ハイブリッドクラウド
FlexPod

NetApp
March 25, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/flexpod/hybrid-cloud/fhc-cvoe-solution-overview.html on March 25, 2024. Always check docs.netapp.com for the latest.

目次

ハイブリッドクラウド . . . 1
FlexPod ハイブリッドクラウドとCloud Volumes ONTAP for Epic . . . 1
ネットアップのCloud Volumes ONTAP とCisco Intersightを活用したFlexPod ハイブリッドクラウドfor Google Cloud Platform . . . 38
ネットアップのAstraとCisco Intersightを活用したFlexPod ハイブリッドクラウドをRed Hat OpenShiftに活用 . . . 121
NetApp Cloud Insights for FlexPod の略 . . . 179
FabricPool with FlexPod - Amazon AWS S3 への非アクティブなデータ階層化 . . . 203
IBMクラウドプライベートを使用するFlexPod データセンター . . . 227
FlexPod Datacenter for Hybrid Cloud with Cisco CloudCenter and NetApp Private Storage -設計 . . . 227
Cisco CloudCenterとネットアップデータファブリックを使用したマルチクラウド対応のFlexPod データセンター . . . 227

ハイブリッドクラウド

FlexPod ハイブリッドクラウドとCloud Volumes ONTAP for Epic

TR-4960：『FlexPod Hybrid Cloud with Cloud Volumes ONTAP for Epic』

協力：

Kamini Singh、ネットアップ

デジタル変革を実現するための鍵は、単にデータを活用してより多くのことを行うことにあります。病院では、組織を運営し、患者に効果的にサービスを提供するために、大量のデータが生成され、必要とされています。情報は、患者を治療し、スタッフのスケジュールと医療リソースを管理するときに収集および処理されます。

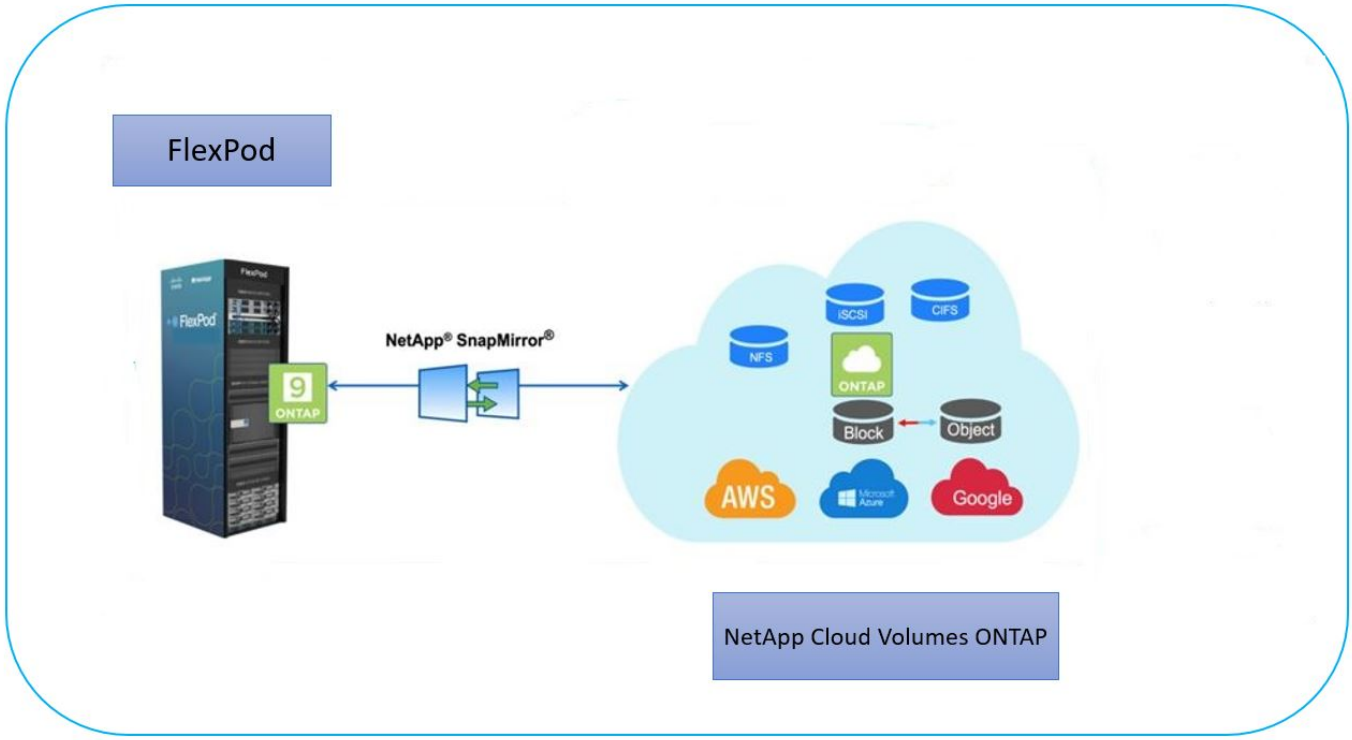
増え続ける医療データと、そのデータから得られる価値あるインサイトによって、医療データサービスとデータ保護が重要な課題となっています。まず、データリカバリ、医療ビジネス継続性、コンプライアンスの要件を満たすためには、医療データの可用性と保護の両方を確保する必要があります。

第2に、医療データを分析のためにすぐに利用できるようにする必要があります。多くの場合、この分析では人工知能（AI）ベースと機械学習（ML）ベースのアプローチを使用して、医療企業がソリューションを改善し、ビジネスバリューを創出できるよう支援します。

第3に、データサービスインフラとデータ保護手法は、医療ビジネスの成長に伴う医療データの増大に対応する必要があります。さらに、データ分析やアーカイブの目的で利用可能なリソースを使用するために、作成されたエッジからコアやクラウドにデータを移動する必要があるため、データモビリティの重要性がますます高まっています。

ネットアップは、ヘルスケアを含むエンタープライズアプリケーション向けに単一のデータ管理解決策 を提供しています。ネットアップは、病院のデジタル変革への道のりを支援することができます。NetApp Cloud Volumes ONTAP は、医療データ管理のための解決策 を提供します。FlexPod データセンターから、AWSなどのパブリッククラウドに導入されたCloud Volumes ONTAP にデータを効率的にレプリケートできます。

Cloud Volumes ONTAP は、対費用効果に優れたセキュアなパブリッククラウドリソースを活用することで、効率性に優れたデータレプリケーション、組み込みのStorage Efficiency機能、シンプルなDRテストによって、クラウドベースのディザスタリカバリ（DR）を強化します。これらのシステムは一元管理され、ドラッグアンドドロップで簡単に管理できるため、あらゆる種類のエラー、障害、災害に対する対費用効果の高い確実な保護が実現します。Cloud Volumes ONTAP は、NetApp SnapMirrorテクノロジをブロックレベルのデータレプリケーション用の解決策 として提供し、差分更新によってデスティネーションを最新の状態に維持します。



対象者

本ドキュメントは、ネットアップ、パートナー様のソリューションエンジニア（SE）、プロフェッショナルサービス担当者を対象としています。ネットアップは、読者が次の知識を有していることを前提としています。

- SANとNASの概念を十分に理解している
- NetApp ONTAP ストレージシステムに関する技術的な知識
- ONTAP ソフトウェアの構成と管理に関する技術的知識

解決策のメリット

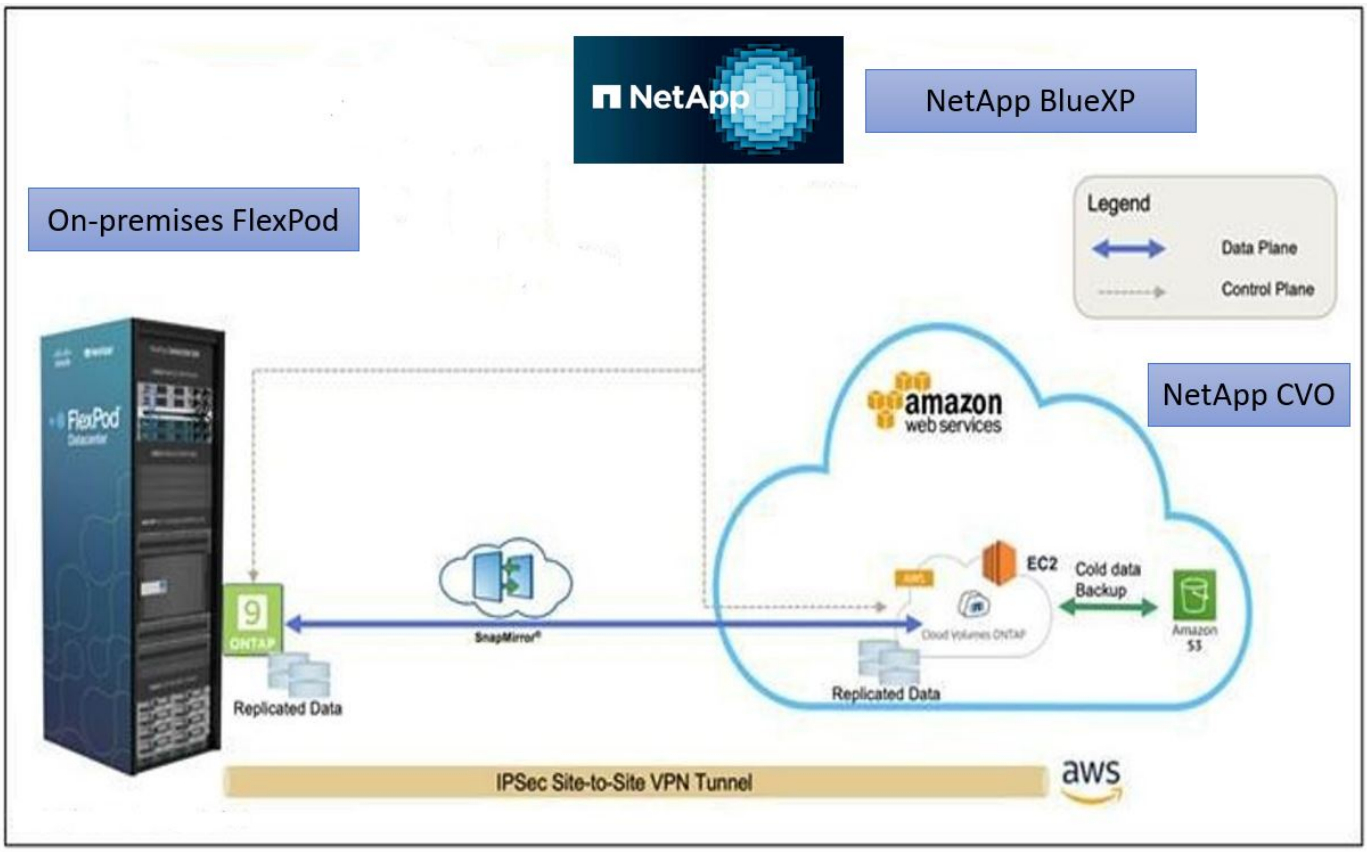
NetApp Cloud Volumes ONTAP と統合されたFlexPod Datacenterは、ヘルスケアワークロードに次のメリットをもたらします。

- カスタマイズされた保護。 Cloud Volumes ONTAP は、ONTAP からクラウドへのブロックレベルのデータレプリケーションを提供し、差分更新によってデスティネーションを最新の状態に維持します。同期スケジュールを指定して、ソースでの変更が転送されるタイミングを決定できます。これにより、あらゆる種類の医療データに対してカスタマイズされた保護が提供されます。
- *フェイルオーバーとフェイルバック*災害が発生した場合、ストレージ管理者はクラウドボリュームへのフェイルオーバーを迅速に設定できます。プライマリサイトがリカバリされると、DR環境で作成された新しいデータがソースボリュームに同期され、セカンダリデータレプリケーションが再確立されます。このようにして、システムを停止することなく医療データを簡単にリカバリできます。
- *効率性。*セカンダリクラウドコピーのストレージスペースとコストは、データ圧縮、シンプロビジョニング、重複排除を使用して最適化されます。医療データは、圧縮と重複排除が適用された形式でブロックレベルで転送されるため、転送速度が向上します。また、データは低コストのオブジェクトストレージに自動的に階層化され、DRシナリオなどでアクセスされたときにのみハイパフォーマンスストレージに戻されます。これにより、継続的なストレージコストを大幅に削減できます。

- ランサムウェア対策。 NetApp BlueXPのランサムウェア対策は、オンプレミス環境とクラウド環境にわたってデータソースをスキャンし、セキュリティの脆弱性を検出し、現在のセキュリティステータスとリスクスコアリングを提供します。次に、さらに調査して修正できる実践的な推奨事項が提示されます。このようにして、医療機関の重要なデータをランサムウェア攻撃から保護できます。

解決策 トポロジ

このセクションでは、解決策 の論理トポロジについて説明します。次の図は、FlexPod オンプレミス環境、Amazon Web Services（AWS）で実行されるNetApp Cloud Volumes ONTAP （CVO）、NetApp BlueXP SaaSプラットフォームで構成される解決策 トポロジを示しています。



コントロールプレーンとデータプレーンは、エンドポイント間で明確に示されます。データプレーンは、セキュアなサイト間VPN接続を利用して、FlexPod のオールフラッシュFAS で実行されるONTAP インスタンスとAWSのNetApp CVOインスタンスの間で実行されます。医療ワークロードのデータをオンプレミスのFlexPod データセンターからNetApp Cloud Volumes ONTAP にレプリケートするには、NetApp SnapMirror レプリケーションを使用します。この解決策 では、NetApp CVOインスタンスにあるコールドデータのバックアップとAWS S3への階層化（オプション）もサポートされています。

"次の例は、解決策 コンポーネントです。"

解決策コンポーネント

"前のページ：解決策 の概要"

FlexPod

FlexPod は、仮想化ソリューションと非仮想化ソリューションの両方の統合基盤となるハードウェアとソフト

ウェアの定義済みセットです。FlexPod には、NetApp ONTAP ストレージ、Cisco Nexusネットワーキング、Cisco MDSストレージネットワーキング、およびCisco Unified Computing System（Cisco UCS）が含まれます。

医療機関は、デジタル変革を容易にし、患者のエクスペリエンスと成果を向上させるための解決策 を求めています。FlexPod を使用すると、安全性と拡張性に優れたプラットフォームを利用して効率性を高め、より多くの情報に基づいた意思決定を迅速に行うことができるため、より優れた患者ケアを提供できます。

FlexPod には次のようなメリットがあるため、医療ワークロードのニーズに最適なプラットフォームです。

- 運用を最適化して分析情報を迅速に取得し、患者の転帰を改善
- 拡張性と信頼性に優れたインフラで画像処理アプリケーションを合理化
- EHRなどの医療に特化したアプリケーション向けの実証済みのアプローチを使用して、迅速かつ効率的に導入できます。

EHR

電子カルテ（EHR）は、中規模および大規模な医療グループ、病院、統合医療組織向けのソフトウェアを作成しています。顧客には、コミュニティ病院、学術施設、子供の組織、セーフティネットプロバイダー、マルチホスピタルシステムも含まれます。EHRに統合されたソフトウェアは、臨床、アクセス、収益の機能にまたがっており、家庭でも利用できます。

医療提供者組織は、業界をリードするEHRへの多額の投資から最大限の利益を得ることを求められ続けています。お客様は、EHRソリューションやミッションクリティカルなアプリケーション向けにデータセンターを設計する際に、データセンターアーキテクチャに関して次のような目標を特定することがよくあります。

- EHRアプリケーションの高可用性
- ハイパフォーマンス
- データセンターへのEHRの導入が容易
- 新しいEHRリリースやアプリケーションで成長を可能にする俊敏性と拡張性
- コスト効率
- 管理性、安定性、および容易なサポート
- 堅牢なデータ保護、バックアップ、リカバリ、ビジネス継続性

FlexPod はEHR検証済みで、Intel Xeonプロセッサ搭載のCisco UCS、Red Hat Enterprise Linux（RHEL）、VMware ESXiによる仮想化を含むプラットフォームをサポートしています。このプラットフォームは、ONTAP を実行するネットアップストレージとしてEHRが評価している「High Comfort Level」と組み合わせることで、お客様は、FlexPod を介してフルマネージドのプライベートクラウドで医療アプリケーションを実行できます。このクラウドは、いずれのパブリッククラウドプロバイダにも接続できます。

NetApp BlueXP

BlueXP（旧称NetApp Cloud Manager）は、エンタープライズクラスのSaaSベースの管理プラットフォームです。ITエキスパートやクラウドアーキテクトは、ネットアップのクラウドソリューションを使用してハイブリッドマルチクラウドインフラを一元管理できます。オンプレミスとクラウドのストレージを表示および管理する一元化されたシステムを提供し、ハイブリッドクラウド、複数のクラウドプロバイダ、アカウントをサポートします。詳細については、を参照してください "BlueXP"。

コネクタ

BlueXPはコネクタインスタンスを使用して、パブリッククラウド環境内のリソースとプロセスを管理できます。BlueXPで提供される機能の多くにはコネクタが必要であり、クラウドまたはオンプレミスのネットワークに導入できます。

Connectorは次の場所でサポートされます。

- Amazon Web Services の
- Microsoft Azure
- Google Cloud
- オンプレミス

コネクタの詳細については、を参照してください "コネクタページ"。

NetApp Cloud Volumes ONTAP の略

NetApp Cloud Volumes ONTAP は、クラウドでONTAP データ管理ソフトウェアを実行し、ファイルワークロードとブロックワークロードに高度なデータ管理を提供するSoftware-Defined Storageソリューションです。Cloud Volumes ONTAP を使用すると、データ保護、セキュリティ、コンプライアンスを強化しながら、クラウドストレージのコストを最適化し、アプリケーションのパフォーマンスを向上させることができます。

主なメリットは次のとおりです。

- * Storage Efficiency。*組み込みのデータ重複排除、データ圧縮、シンプロビジョニング、瞬時のクローニングを活用して、ストレージコストを最小限に抑えます。
- *高可用性*クラウド環境で障害が発生した場合でも、エンタープライズクラスの信頼性と継続的な運用を実現します。
- データ保護。 Cloud Volumes ONTAP は、業界をリードするネットアップのレプリケーションテクノロジであるSnapMirrorを使用してオンプレミスのデータをクラウドにレプリケートするため、複数のユースケースでセカンダリコピーを簡単に利用できます。また、Cloud Volumes ONTAP はCloud Backupと統合して、クラウドデータの保護と長期アーカイブのためのバックアップとリストアの機能を提供します。
- *データ階層化。*アプリケーションをオフラインにすることなく、高パフォーマンスと低パフォーマンスのストレージプールをオンデマンドで切り替えます。
- アプリケーションの整合性。 NetApp SnapCenter テクノロジを使用して、NetApp Snapshotコピーの整合性を提供します。
- データセキュリティ。 Cloud Volumes ONTAP はデータ暗号化をサポートし、ウイルスやランサムウェアからの保護を提供します。
- プライバシーコンプライアンス管理 Cloud Data Senseとの統合により、データのコンテキストを把握し、機密データを特定できます。

詳細については、を参照してください "Cloud Volumes ONTAP"。

NetApp Active IQ Unified Manager の略

NetApp Active IQ Unified Manager では、設計が刷新されたわかりやすい単一のインターフェイスからONTAPストレージクラスタを監視でき、集合知とAI分析から得た情報を提供します。ストレージ環境とストレージ環境で実行されている仮想マシンに関する、運用面、パフォーマンス面、プロアクティブな分析情報を包括的に

提供します。ストレージインフラで問題 が発生すると、Unified Managerから問題 の詳細情報を通知してルート原因 を特定できるようになります。仮想マシンダッシュボードではVMのパフォーマンス統計を確認でき、これにより、ネットワーク経由でダウンしているvSphereホストからストレージへのI/Oパス全体を調査できます。

一部のイベントには、問題 を修正するための対応策も用意されています。問題が発生したときにEメールやSNMPトラップで通知されるように、イベントにカスタムアラートを設定できます。Active IQ Unified Manager を使用すると、容量と使用状況の傾向を予測してユーザのストレージ要件を計画できます。これにより、問題が発生する前に対処できるようになり、長期的に新たな問題につながる可能性のある、短期的な事後的な判断を回避できます。

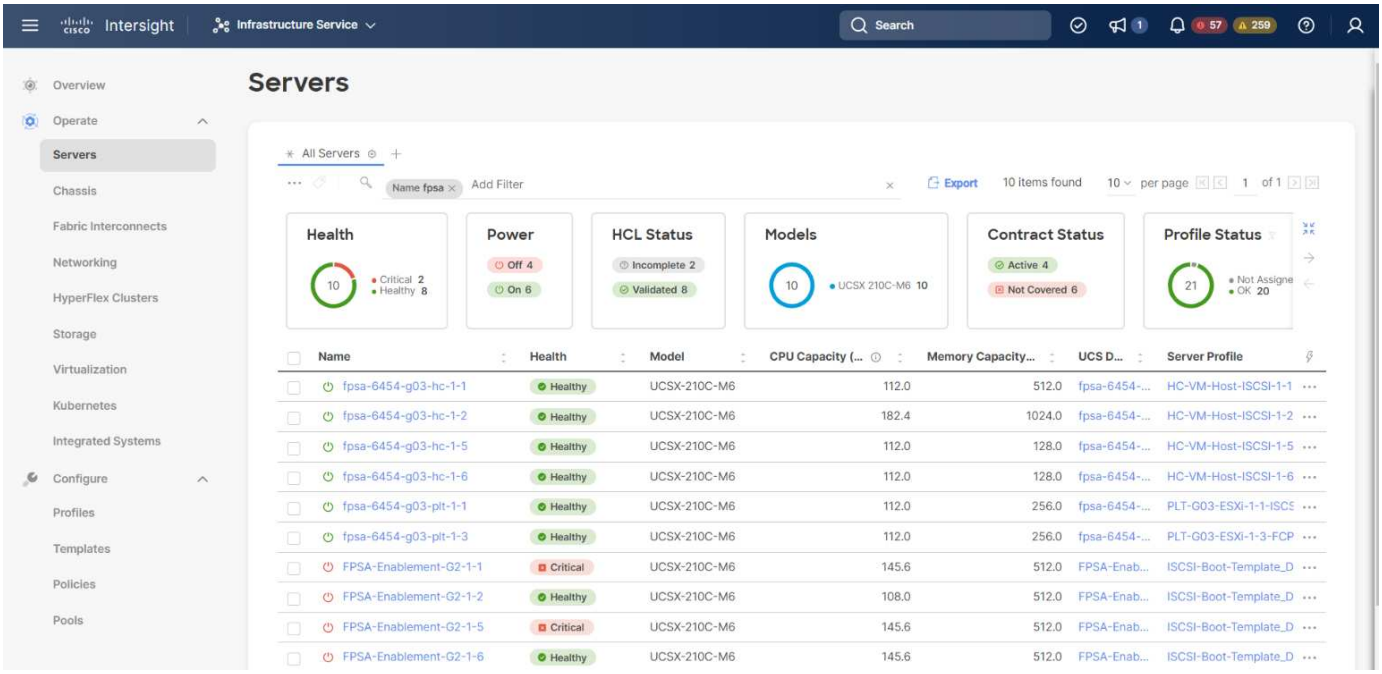
詳細については、を参照してください "Active IQ Unified Manager"。

Cisco Intersightの

Cisco Intersightは、従来のアプリケーションやクラウドネイティブなインフラに向けて、インテリジェントな自動化、オブザーバビリティ、最適化を実現するSaaSプラットフォームです。このプラットフォームは、ITチームの変化を促進し、ハイブリッドクラウド向けに設計された運用モデルを提供します。Cisco Intersightには、次のようなメリットがあります。

- 迅速な提供。 Intersightは、アジャイルベースのソフトウェア開発モデルにより、頻繁な更新と継続的なイノベーションにより、クラウドまたはお客様のデータセンターからサービスとして提供されます。このようにして、お客様は重要なビジネスニーズのサポートに集中できます。
- 運用の簡易化。 Intersightは、SaaSで提供される単一のセキュアなツールと共通のインベントリ、認証、APIを使用してフルスタックとすべての場所で機能し、チーム間のサイロを解消することで、運用を簡易化します。これにより、オンプレミスの物理サーバとハイパーバイザー、VM、Kubernetes、サーバレス、自動化、 オンプレミスとパブリッククラウドの両方で最適化とコスト管理を実現します。
- *継続的な最適化。*すべてのレイヤおよびCisco TACが提供するCisco Intersightのインテリジェンスを使用して、環境を継続的に最適化できます。このインテリジェンスは推奨される自動化可能なアクションに変換されるため、ワークロードの移動や物理サーバの健全性の監視から、使用するパブリッククラウドのコスト削減の推奨まで、あらゆる変更にリアルタイムで適応できます。

Cisco Intersightには、UCSM Managed Mode（UMM）とIntersight Managed Mode（IMM）という2つの管理操作モードがあります。ファブリックインターコネクトの初期セットアップ時に、ファブリック接続Cisco UCSシステムのネイティブUCSM Managed Mode（UMM）またはIntersight Managed Mode（IMM）を選択できます。この解決策 では、ネイティブIMMが使用されます。次の図は、Cisco Intersightダッシュボードを示しています。



ページを示しています。"]

VMware vSphere 7.0

VMware vSphereは、大規模なインフラストラクチャ（CPU、ストレージ、ネットワークなど）をシームレスで汎用性の高い動的な運用環境として包括的に管理するための仮想化プラットフォームです。個 々 のマシンを管理する従来のオペレーティングシステムとは異なり、VMware vSphereはデータセンター全体のインフラストラクチャを集約して、必要なアプリケーションに迅速かつ動的に割り当てることができるリソースを備えた単一のパワーハウスを作成します。

VMware vSphereとそのコンポーネントの詳細については、を参照してください "VMware vSphere の場合"。

VMware vCenter Server の各機能を使用し

VMware vCenter Serverでは、1つのコンソールからすべてのホストとVMを統合的に管理でき、クラスタ、ホスト、およびVMのパフォーマンス監視を集約できます。VMware vCenter Serverを使用すると、管理者は、コンピューティングクラスタ、ホスト、VM、ストレージ、ゲストOS、 仮想インフラストラクチャのその他の重要なコンポーネントVMware vCenterは、VMware vSphere環境で使用できる豊富な機能を管理します。

詳細については、を参照してください "VMware vCenter"。

ハードウェアおよびソフトウェアのリビジョン

このハイブリッドクラウド解決策 は、で定義されている、サポート対象のバージョンのソフトウェア、ファームウェア、ハードウェアを実行している任意のFlexPod 環境に拡張できます "NetApp Interoperability Matrix Tool で確認できます"、 "UCSハードウェアおよびソフトウェアの互換性"および "VMware Compatibility Guide 』を参照してください"。

次の表に、オンプレミスのFlexPod ハードウェアとソフトウェアのリビジョンを示します。

コンポーネント	プロダクト	バージョン
コンピューティング	Cisco UCS X210c M6	5.0（1b）

コンポーネント	プロダクト	バージョン
	Cisco UCSファブリックインターコネクト6454	4.2（2a）
ネットワーク	Cisco Nexus 9336C-FX2 NX-OS	9.3（9）
ストレージ	NetApp AFF A400	ONTAP 9.11.1P2
	NetApp ONTAP Tools for VMware vSphere の略	9.11
	NetApp NFS Plug-in for VMware VAAI	"2.0"
	NetApp Active IQ Unified Manager の略	9.11P1
ソフトウェア	VMware vSphere の場合	7.0（U3）
	VMware ESXi nenic イーサネットドライバ	1.0.35.0
	VMware vCenter Applianceの略	バージョン7.0.3
	Cisco Intersight Assist仮想アプライアンス	1.0.9-342

次の表に、NetApp BlueXPとCloud Volumes ONTAP のバージョンを示します。

ベンダー	プロダクト	バージョン
ネットアップ	BlueXP	3.9.24
	Cloud Volumes ONTAP	ONTAP 9.11

"次の記事：インストールと設定"

インストールと設定

"前の図：解決策 コンポーネント。"

NetApp Cloud Volumes ONTAP の導入

Cloud Volumes ONTAP インスタンスを設定するには、次の手順を実行します。

1. パブリッククラウドサービスプロバイダ環境の準備

   解決策 構成について、パブリッククラウドサービスプロバイダの環境の詳細を確認しておく必要があります。たとえば、Amazon Web Services（AWS）環境の準備では、AWSアクセスキー、AWSシークレットキー、およびその他のネットワークの詳細（リージョン、VPC、サブネットなど）が必要です。

2. VPCエンドポイントゲートウェイを設定します。

   VPCとAWS S3サービスの間の接続を有効にするには、VPCエンドポイントゲートウェイが必要です。これは、ゲートウェイタイプのエンドポイントであるCVOでバックアップを有効にするために使用されます。

3. NetApp BlueXPにアクセスします。

   NetApp BlueXPやその他のクラウドサービスにアクセスするには、に登録する必要があります "NetApp BlueXP"。BlueXPアカウントでワークスペースとユーザを設定するには、をクリックします "こちらをご覧ください"。BlueXPからクラウドプロバイダにコネクタを直接導入する権限を持つアカウントが必要です。BlueXPポリシーはからダウンロードできます "こちらをご覧ください"。

4. コネクタを展開します。

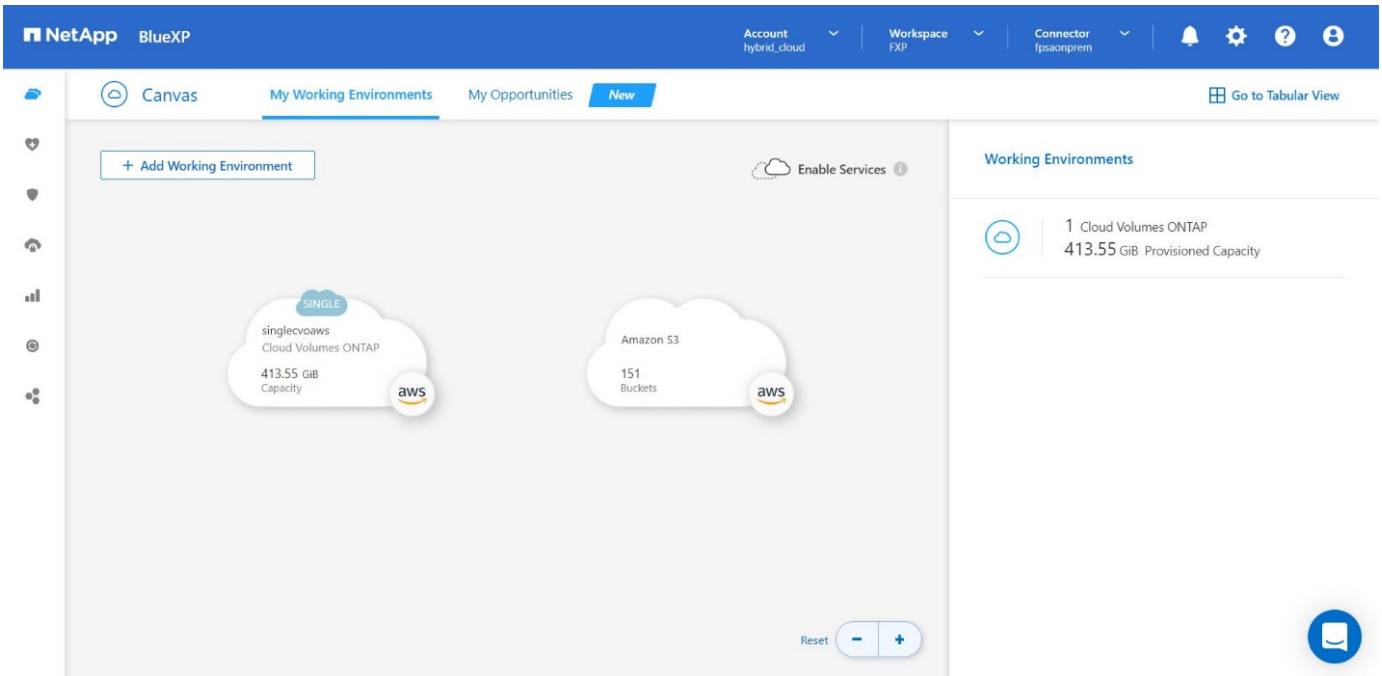
   Cloud Volume ONTAP 作業環境を追加する前に、コネクタを導入する必要があります。コネクタを配置せずに最初のCloud Volumes ONTAP 作業環境を作成しようとすると、プロンプトが表示されます。BlueXPからAWSにコネクタを導入する方法については、こちらを参照してください "リンク"。

5. AWSでCloud Volumes ONTAP を起動します。

   Cloud Volumes ONTAP は単一システム構成で起動することも、 AWS で HA ペアとして起動することもできます。 "ステップバイステップの手順をお読みください"。

   これらの手順の詳細については、を参照してください "AWSでのCloud Volumes ONTAP のクイックスタートガイド"。

   この解決策 では、AWSにシングルノードのCloud Volumes ONTAP システムを導入しました。次の図は、シングルノードCVOインスタンスを使用するNetApp BlueXPダッシュボードを示しています。



画面と[My Working Environments]を示しています。"]

オンプレミスの**FlexPod** 環境

FlexPod とUCS Xシリーズ、VMware、およびNetApp ONTAP の設計の詳細については、を参照してください "FlexPod データセンターとCisco UCS Xシリーズ" 設計ガイド：このドキュメントでは、Cisco Intersightが管理するUCS XシリーズプラットフォームをFlexPod データセンターインフラに組み込むための設計ガイダンスを提供します。

オンプレミスのFlexPod インスタンスの導入については、を参照してください "この導入ガイドを参照してください"。

このドキュメントでは、Cisco Intersightが管理するUCS Xシリーズプラットフォームを FlexPod データセンターインフラに組み込むための導入ガイダンスを提供します。このドキュメントでは、導入を成功させるための構成とベストプラクティスの両方について説明します。

FlexPod は、UCS管理モードとCisco Intersight管理モード（IMM）の両方で導入できます。FlexPod をUCS管理モードで展開する場合は、こちらを参照してください "設計ガイド" そしてこれ "導入ガイド"。

FlexPod の導入は、Ansibleを使用してコードとしてインフラを使用して自動化できます。以下は、エンドツーエンドのFlexPod 展開のためのGitHubリポジトリへのリンクです。

- UCS管理モードでのCisco UCS、NetApp ONTAP 、VMware vSphereを使用したFlexPod のAnsible構成を確認できます "こちらをご覧ください"。
- IMM内のCisco UCS、NetApp ONTAP 、VMware vSphereを使用したFlexPod のAnsible構成を確認できます "こちらをご覧ください"。

オンプレミスの**ONTAP** ストレージ構成

ここでは、この解決策 に固有のONTAP の重要な設定手順をいくつか説明します。

1. iSCSIサービスを実行しているSVMを設定します。

```
1. vserver create –vserver Healthcare_SVM –rootvolume
Healthcare_SVM_root –aggregate aggr1_A400_G0312_01 –rootvolume-security-
style unix
2. vserver add-protocols -vserver Healthcare_SVM -protocols iscsi
3. vserver iscsi create -vserver Healthcare_SVM

   To verify:

   A400-G0312::> vserver iscsi show -vserver Healthcare_SVM
   Vserver: Healthcare_SVM
   Target Name:
   iqn.1992-08.com.netapp:sn.1fbf00f438c111ed866cd039ea91fb56:vs.3
   Target Alias: Healthcare_SVM
   Administrative Status: up
```

   クラスタの構成時にiSCSIライセンスがインストールされなかった場合は、iSCSIサービスを作成する前に必ずライセンスをインストールしてください。

2. FlexVol ボリュームを作成します。

```
1. volume create -vserver Healthcare_SVM -volume hc_iscsi_vol -aggregate
aggr1_A400_G0312_01 -size 500GB -state online -policy default -space
guarantee none
```

3. iSCSIアクセス用のインターフェイスを追加します。

```
1. network interface create -vserver Healthcare_SVM -lif iscsi-lif-01a
-service-policy default-data-iscsi -home-node <st-node01> -home-port
a0a-<infra-iscsi-a-vlan-id> -address <st-node01-infra-iscsi-a-ip>
-netmask <infra-iscsi-a-mask> -status-admin up
2. network interface create -vserver Healthcare_SVM -lif iscsi-lif-01b
-service-policy default-data-iscsi -home-node <st-node01> -home-port
a0a-<infra-iscsi-b-vlan-id> -address <st-node01-infra-iscsi-b-ip>
-netmask <infra-iscsi-b-mask> -status-admin up
3. network interface create -vserver Healthcare_SVM -lif iscsi-lif-02a
-service-policy default-data-iscsi -home-node <st-node02> -home-port
a0a-<infra-iscsi-a-vlan-id> -address <st-node02-infra-iscsi-a-ip>
-netmask <infra-iscsi-a-mask> -status-admin up
4. network interface create -vserver Healthcare_SVM -lif iscsi-lif-02b
-service-policy default-data-iscsi -home-node <st-node02> -home-port
a0a-<infra-iscsi-b-vlan-id> -address <st-node02-infra-iscsi-b-ip>
-netmask <infra-iscsi-b-mask> -status-admin up
```

この解決策 では、4つのiSCSI論理インターフェイス（LIF）を作成しました（各ノードに2つずつ）。

vCenterを導入してFlexPod インスタンスを運用開始し、すべてのESXiホストを追加したら、NetApp ONTAP ストレージに接続してアクセスするサーバとして機能するLinux VMを導入する必要があります。この解決策 では、CentOS 8インスタンスをvCenterにインストールしました。

4. LUNを作成します。

```
1. lun create -vserver Healthcare_SVM -path /vol/hc_iscsi_vol/iscsi_lun1
-size 200GB -ostype linux -space-reserve disabled
```

EHR Operational Database（ODB；EHR運用データベース）、ジャーナル、およびアプリケーションのワークロードについては、ストレージをサーバにiSCSI LUNとして提供することを推奨します。また、対応しているAIXおよびRHELオペレーティングシステムのバージョンがある場合は、FCPとNVMe/FCの使用もサポートされるため、パフォーマンスが向上します。FCPとNVMe/FCは同じファブリックに共存できます。

5. igroupを作成します。

```
1. igroup create –vserver Healthcare_SVM –igroup ehr –protocol iscsi
–ostype linux –initiator iqn.1994-05.com.redhat:8e91e9769336
```

igroupは、サーバからLUNへのアクセスを許可するために使用されます。Linuxホストの場合、サーバIQNはファイルで確認できます `/etc/iscsi/initiatorname.iscsi`。

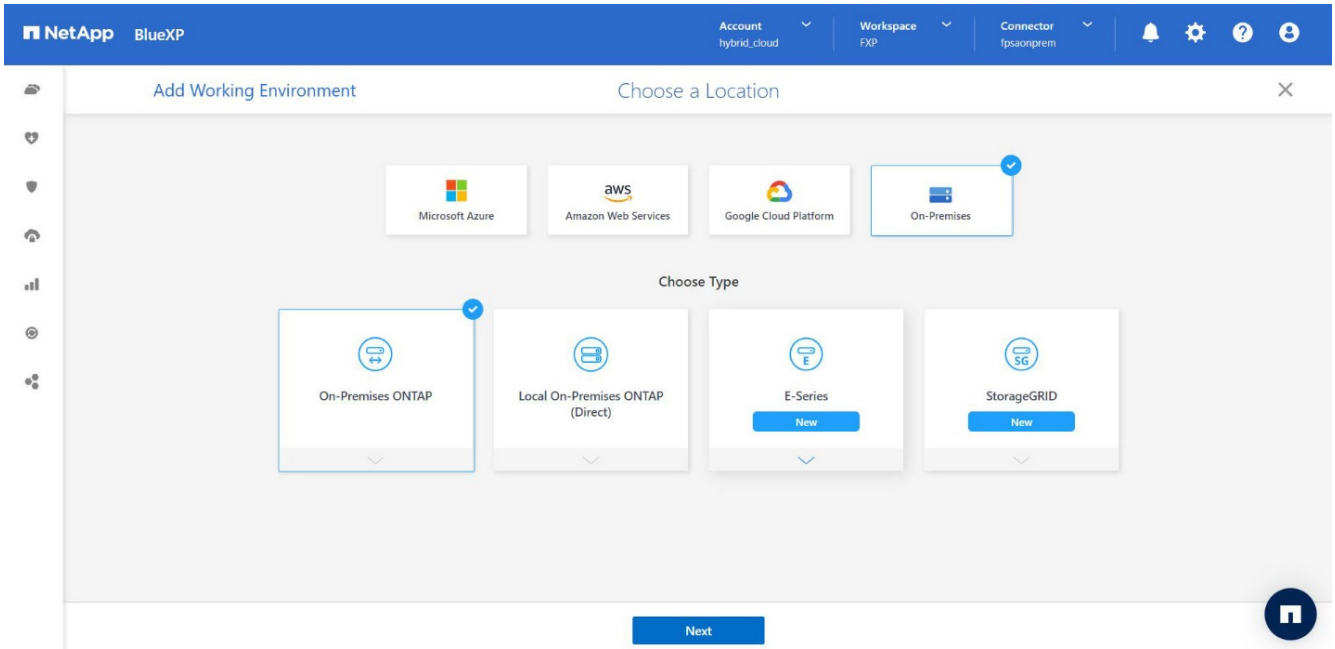
6. LUN を igroup にマッピングします。

```
1. lun mapping create -vserver Healthcare_SVM -path
/vol/hc_iscsi_vol/iscsi_lun1 -igroup ehr -lun-id 0
```

オンプレミスの**FlexPod** ストレージを**BlueXP**に追加

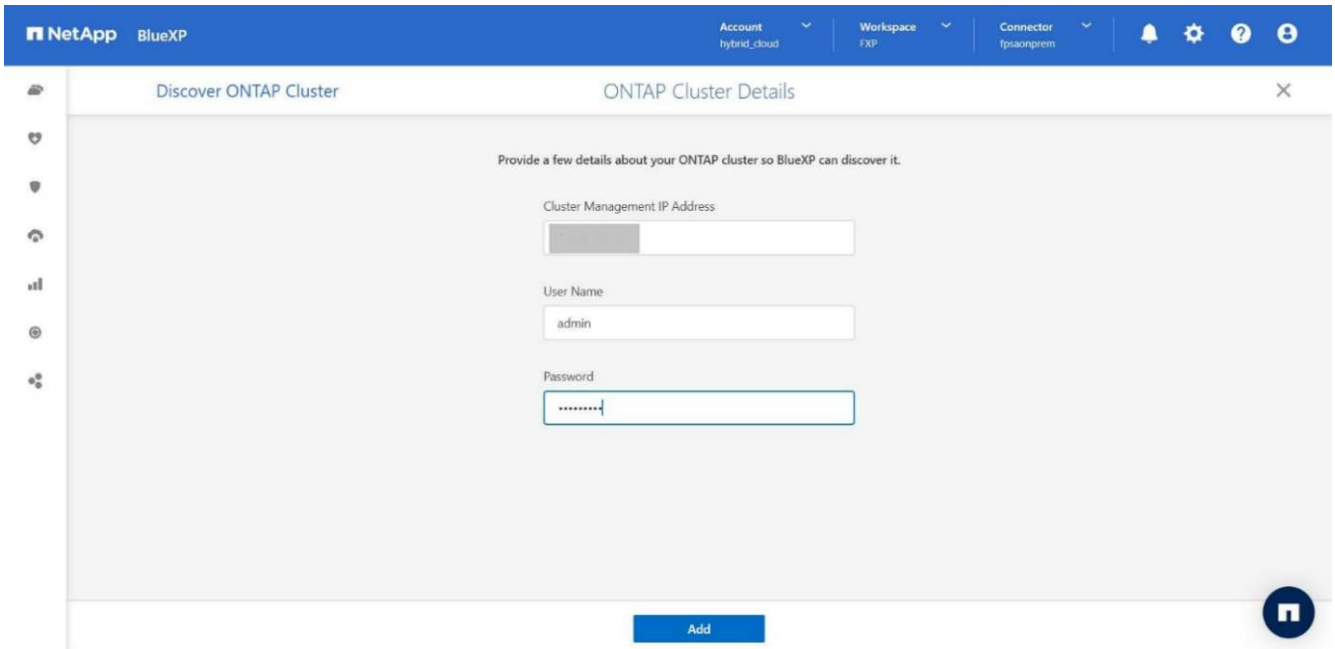
NetApp BlueXPを使用してFlexPod ストレージを作業環境に追加するには、次の手順を実行します。

1. ナビゲーションメニューから、**[**ストレージ**]**>*[キャンバス]*を選択します。
2. キャンバスページで、*作業環境の追加*をクリックし、*オンプレミス*を選択します。
3. オンプレミスONTAP *を選択します。「 * 次へ * 」をクリックします。



ページを示しています。オンプレミスのONTAP が選択されています。"]

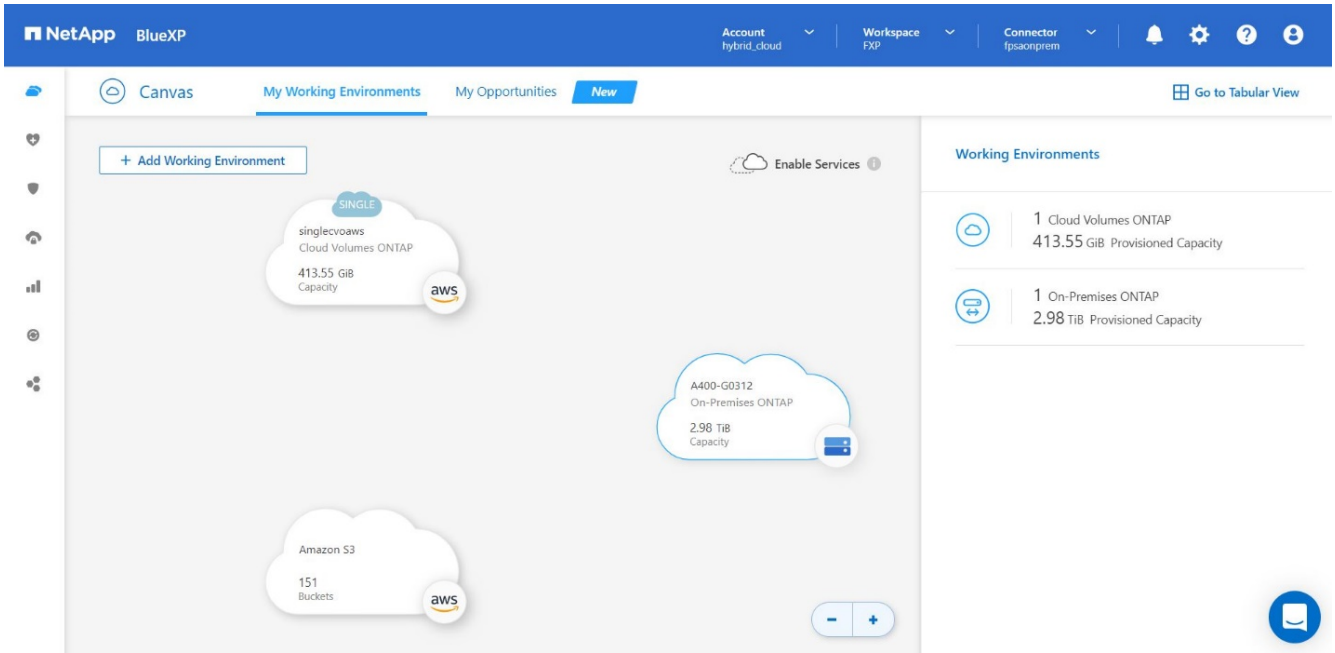
4. ONTAP のクラスタ詳細ページで、クラスタ管理 IP アドレスと admin ユーザアカウントのパスワードを入力します。次に*[追加]*をクリックします。



ページとONTAP の[Cluster Details]エントリを示しています。"]

5. [Details and Credentials]ページで、作業環境の名前と概要 を入力し、*[Go]*をクリックします。

   BlueXPがONTAP クラスタを検出し、Canvasの作業環境として追加します。



ページを示しています。最近追加した作業環境が右側に表示されます。"]

詳細については、ページを参照してください "オンプレミスのONTAP クラスタを検出"。

"次の記事：SANの構成"

SAN の設定

"前の手順：インストールと設定"

このセクションでは、EHRがネットアップストレージとの最適な統合を可能にするために必要なホスト側の構成について説明します。このセグメントでは、Linuxオペレーティングシステムのホスト統合について具体的に説明します。を使用します "ネットアップのInteroperability Matrix Tool （ IMT ）" ソフトウェアとファームウェアのすべてのバージョンを検証します。

以下は、この解決策 で使用したCentOS 8ホストに固有の設定手順です。

NetApp Host Utility Kitの略

ネットアップストレージシステムに接続されてアクセスしているホストのオペレーティングシステムに、NetApp Host Utility Kit（Host Utilities）をインストールすることを推奨します。ネイティブのMicrosoftマルチパスI/O（MPIO）がサポートされています。OSがマルチパス用にAsymmetric Logical Unit Access（ALUA；非対称論理ユニットアクセス）に対応している必要があります。Host Utilitiesをインストールすると、ネットアップストレージのホストバスアダプタ（HBA）が設定されます。

NetApp Host Utilitiesをダウンロードできます "こちらをご覧ください"。この解決策 では、Linux Host Utilities 7.1をホストにインストールしました。

```
[root@hc-cloud-secure-1 ~]# rpm -ivh netapp_linux_unified_host_utilities-
7-1.x86_64.rpm
```

ONTAP ストレージを検出

ログインが発生するはずのときにiSCSIサービスが実行されていることを確認します。ターゲット上の特定のポータルまたはターゲット上のすべてのポータルに対してログインモードを設定するには、を使用します `iscsiadm` コマンドを実行します

```
[root@hc-cloud-secure-1 ~]# rescan-scsi-bus.sh
[root@hc-cloud-secure-1 ~]# iscsiadm -m discovery -t sendtargets -p
<iscsi-lif-ip>
[root@hc-cloud-secure-1 ~]# iscsiadm -m node -L all
```

今、あなたはを使うことができます `sanlun` をクリックして、ホストに接続されているLUNに関する情報を表示します。ホストにrootとしてログインしていることを確認します。

```
[root@hc-cloud-secure-1 ~]# sanlun lun show
controller(7mode/E-Series)/
                                      device    host              lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------------------
---
Healthcare_SVM                         /dev/sdb host33  iSCSI    200g
cDOT
                       /vol/hc_iscsi_vol/iscsi_lun1

Healthcare_SVM                         /dev/sdc host34  iSCSI    200g
cDOT
                       /vol/hc_iscsi_vol/iscsi_lun1
```

マルチパスを設定します

Device Mapper Multipathing（DM-Multipath）は、Linuxの標準マルチパスユーティリティです。冗長性を確保し、パフォーマンスを向上させるために使用できます。サーバとストレージ間の複数のI/Oパスを集約または結合するため、OSレベルで1つのデバイスを作成します。

1. システムにDM-Multipathを設定する前に、システムが更新され、が含まれていることを確認してください `device-mapper-multipath` パッケージ。

```
[root@hc-cloud-secure-1 ~]# rpm -qa|grep multipath
device-mapper-multipath-libs-0.8.4-31.el8.x86_64
device-mapper-multipath-0.8.4-31.el8.x86_64
```

2. 構成ファイルはです `/etc/multipath.conf` ファイル。次のように設定ファイルを更新します。

```
[root@hc-cloud-secure-1 ~]# cat /etc/multipath.conf
defaults {
   path_checker      readsector0
   no_path_retry      fail
}
devices {
   device {
      vendor         "NETAPP  "
      product         "LUN.*"
      no_path_retry     queue
      path_checker      tur
   }
}
```

3. マルチパスサービスを有効にして開始します。

```
[root@hc-cloud-secure-1 ~]# systemctl enable multipathd.service
[root@hc-cloud-secure-1 ~]# systemctl start  multipathd.service
```

4. ロード可能なカーネルモジュールを追加します `dm-multipath` をクリックし、マルチパスサービスを再起動します。最後に、マルチパスのステータスを確認します。

```
[root@hc-cloud-secure-1 ~]# modprobe -v dm-multipath
insmod /lib/modules/4.18.0-408.el8.x86_64/kernel/drivers/md/dm-
multipath.ko.xz

[root@hc-cloud-secure-1 ~]# systemctl restart multipathd.service

[root@hc-cloud-secure-1 ~]# multipath -ll
3600a09803831494c372b545a4d786278 dm-2 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- 33:0:0:0 sdb 8:16 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
`- 34:0:0:0 sdc 8:32 active ready running
```

これらの手順の詳細については、を参照してください "こちらをご覧ください"。

物理ボリュームを作成します

を使用します `pvcreate` 物理ボリュームとして使用するブロックデバイスを初期化するコマンド。初期化は、ファイルシステムのフォーマットに似ています。

```
[root@hc-cloud-secure-1 ~]# pvcreate /dev/sdb
Physical volume "/dev/sdb" successfully created.
```

ボリュームグループを作成します

1つ以上の物理ボリュームからボリュームグループを作成するには、を使用します `vgcreate` コマンドを実行しますこのコマンドは、名前を指定して新しいボリュームグループを作成し、そのグループに少なくとも1つの物理ボリュームを追加します。

```
[root@hc-cloud-secure-1 ~]# vgcreate datavg /dev/sdb
Volume group "datavg" successfully created.
```

。 vgdisplay コマンドを使用すると、ボリュームグループのプロパティ（サイズ、エクステント、物理ボリューム数など）を固定形式で表示できます。

```
[root@hc-cloud-secure-1 ~]# vgdisplay datavg
  --- Volume group ---
  VG Name               datavg
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  1
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                0
  Open LV               0
  Max PV                0
  Cur PV                1
  Act PV                1
  VG Size               <200.00 GiB
  PE Size               4.00 MiB
  Total PE              51199
  Alloc PE / Size       0 / 0
  Free  PE / Size       51199 / <200.00 GiB
  VG UUID               C7jmI0-J0SS-Cq91-t6b4-A9xw-nTfi-RXcy28
```

論理ボリュームを作成します

論理ボリュームを作成すると、ボリュームグループを構成する物理ボリューム上の空きエクステントを使用して、ボリュームグループから論理ボリュームが作成されます。

```
[root@hc-cloud-secure-1 ~]# lvcreate - l 100%FREE -n datalv datavg
Logical volume "datalv" created.
```

このコマンドは、という名前の論理ボリュームを作成します datalv ボリュームグループ内の未割り当てスペースをすべて使用します datavg。

ファイルシステムを作成します

```
[root@hc-cloud-secure-1 ~]# mkfs.xfs -K /dev/datavg/datalv
meta-data=/dev/datavg/datalv     isize=512    agcount=4, agsize=13106944
blks
         =                       sectsz=4096  attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=1, rmapbt=0
         =                       reflink=1    bigtime=0 inobtcount=0
data     =                       bsize=4096   blocks=52427776, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=25599, version=2
         =                       sectsz=4096  sunit=1 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

マウントするフォルダを作成します

```
[root@hc-cloud-secure-1 ~]# mkdir /file1
```

ファイルシステムをマウントします

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1

[root@hc-cloud-secure-1 ~]# df -k
Filesystem                 1K-blocks    Used Available Use% Mounted on
devtmpfs                     8072804       0   8072804   0% /dev
tmpfs                        8103272       0   8103272   0% /dev/shm
tmpfs                        8103272    9404   8093868   1% /run
tmpfs                        8103272       0   8103272   0% /sys/fs/cgroup
/dev/mapper/cs-root         45496624 5642104  39854520  13% /
/dev/sda2                    1038336  258712    779624  25% /boot
/dev/sda1                     613184    7416    605768   2% /boot/efi
tmpfs                        1620652      12   1620640   1% /run/user/42
tmpfs                        1620652       0   1620652   0% /run/user/0
/dev/mapper/datavg-datalv 209608708 1494520 208114188   1% /file1
```

これらのタスクの詳細については、ページを参照してください "CLIコマンドを使用したLVM管理"。

データ生成

`Dgen.pl` は、EHRのI/Oシミュレータ（GenerateIO）用のPerlスクリプトデータジェネレータです。LUN内のデータはEHRを使用して生成されます `Dgen.pl` スクリプト：スクリプトは、EHRデータベース内にあるものと同様のデータを作成するように設計されています。

```
[root@hc-cloud-secure-1 ~]# cd GenerateIO-1.17.3/

[root@hc-cloud-secure-1 GenerateIO-1.17.3]# ./dgen.pl --directory /file1
--jobs 80

[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01  dir05  dir09  dir13  dir17  dir21  dir25  dir29  dir33  dir37
dir41  dir45  dir49  dir53  dir57  dir61  dir65  dir69  dir73  dir77
dir02  dir06  dir10  dir14  dir18  dir22  dir26  dir30  dir34  dir38
dir42  dir46  dir50  dir54  dir58  dir62  dir66  dir70  dir74  dir78
dir03  dir07  dir11  dir15  dir19  dir23  dir27  dir31  dir35  dir39
dir43  dir47  dir51  dir55  dir59  dir63  dir67  dir71  dir75  dir79
dir04  dir08  dir12  dir16  dir20  dir24  dir28  dir32  dir36  dir40
dir44  dir48  dir52  dir56  dir60  dir64  dir68  dir72  dir76  dir80

[root@hc-cloud-secure-1 file1]# df -k .
Filesystem                 1K-blocks  Used       Available  Use%  Mounted
on
/dev/mapper/datavg-datalv  209608708  178167156  31441552   85%   /file1
```

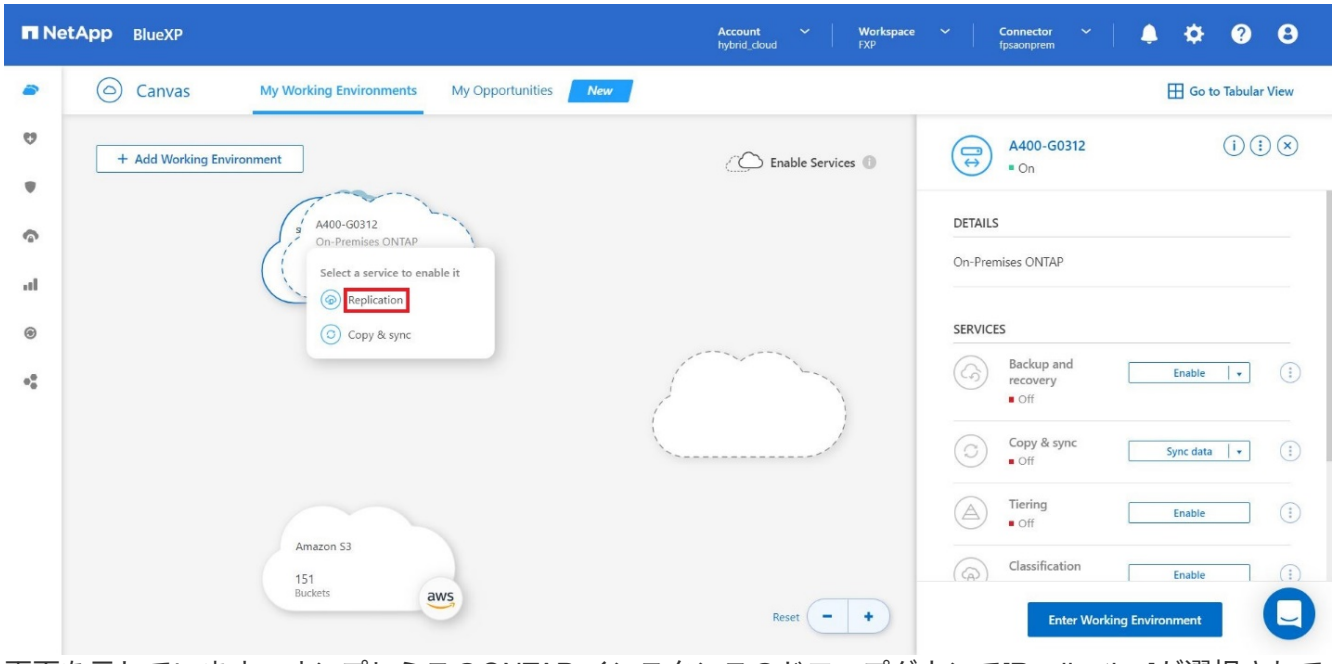
実行中は、 `Dgen.pl` スクリプトは、デフォルトでファイルシステムの85%をデータ生成に使用します。

オンプレミスの**ONTAP** と**Cloud Volumes ONTAP** の間に**SnapMirror**レプリケーションを設定

NetApp SnapMirror は、 LAN または WAN 経由でデータを高速でレプリケートするため、仮想環境と従来の環境の両方で、高いデータ可用性と高速なデータレプリケーションを実現できます。ネットアップストレージシステムにデータをレプリケートし、セカンダリデータを継続的に更新することで、データを最新の状態に保ちながら、必要なときにいつでもデータを利用できるようになります。外部レプリケーションサーバは必要ありません。

オンプレミスのONTAP システムとCVOの間にSnapMirrorレプリケーションを設定するには、次の手順を実行します。

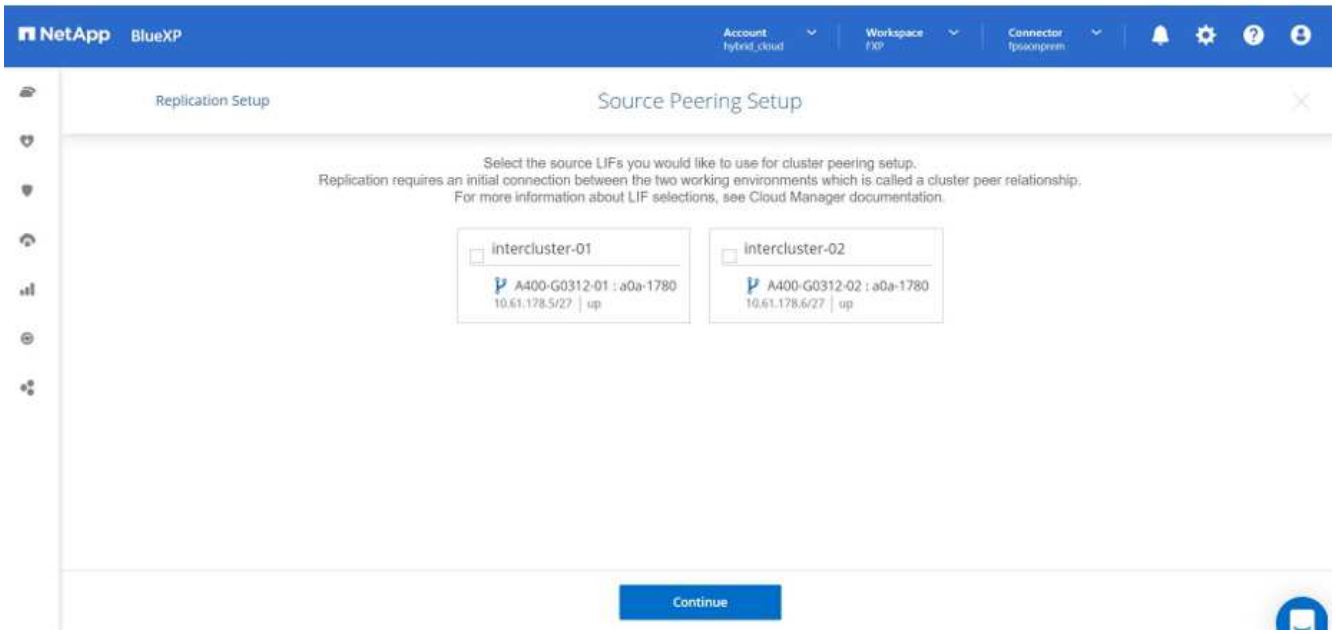
1. ナビゲーションメニューから、**[**ストレージ**]**>*[キャンバス]*を選択します。
2. Canvasで、ソースボリュームが含まれている作業環境を選択し、ボリュームのレプリケート先となる作業環境にソースボリュームをドラッグして、*[レプリケーション]*を選択します。



画面を示しています。オンプレミスのONTAP インスタンスのドロップダウンで[Replication]が選択されています。"]

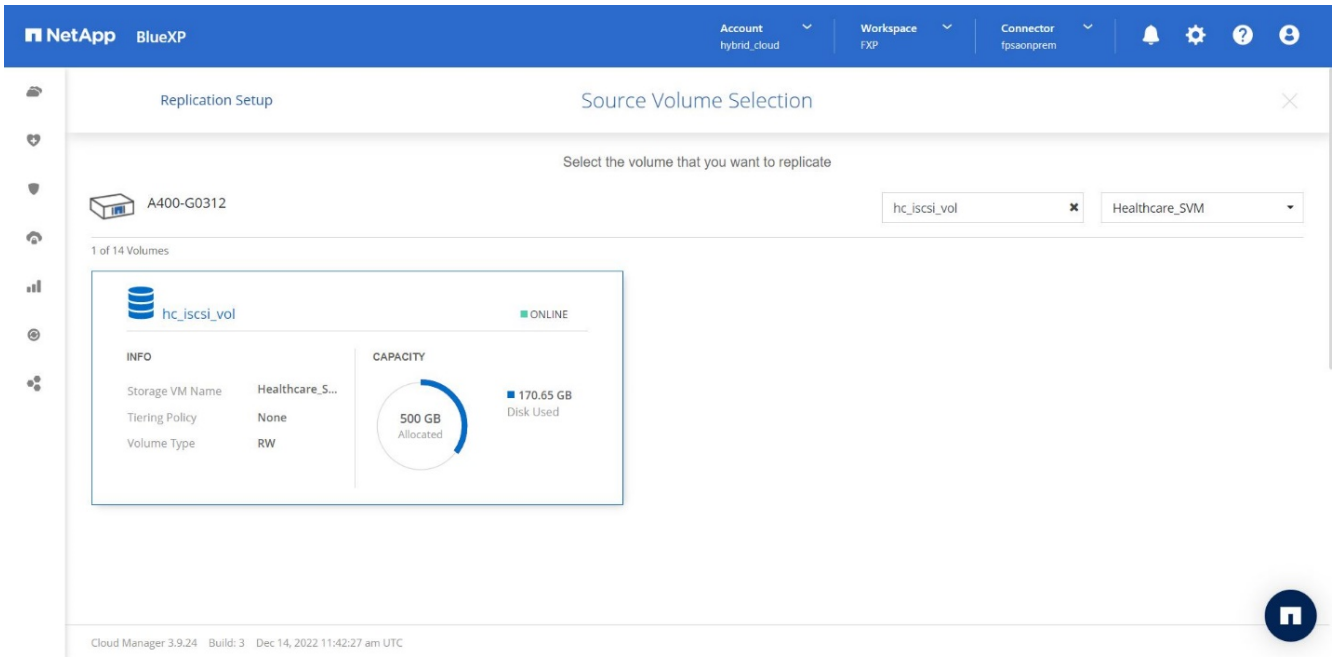
以降の手順では、Cloud Volumes ONTAP クラスタとオンプレミスのONTAP クラスタ間に同期関係を作成する方法について説明します。

3. *ソースとデスティネーションのピアリングのセットアップ。*このページが表示された場合は、クラスタピア関係に使用するすべてのクラスタ間LIFを選択します。



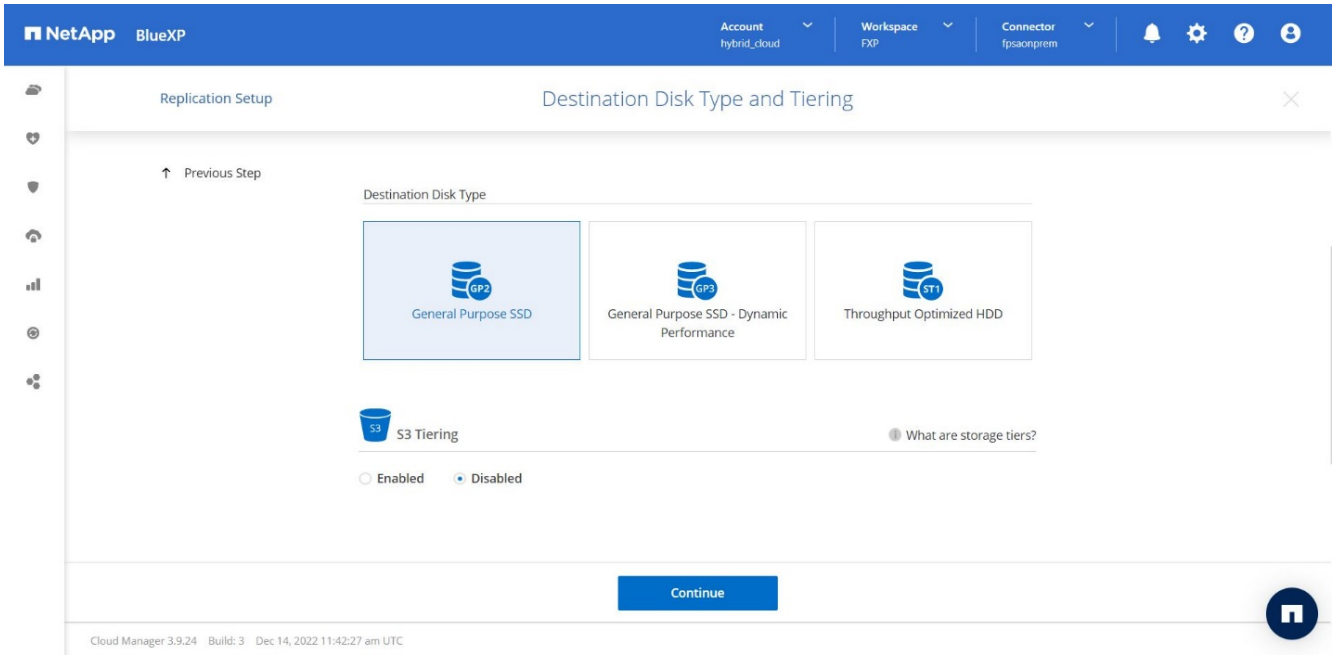
画面を示しています。"]

4. *ソースボリュームの選択。*レプリケートするボリュームを選択します。



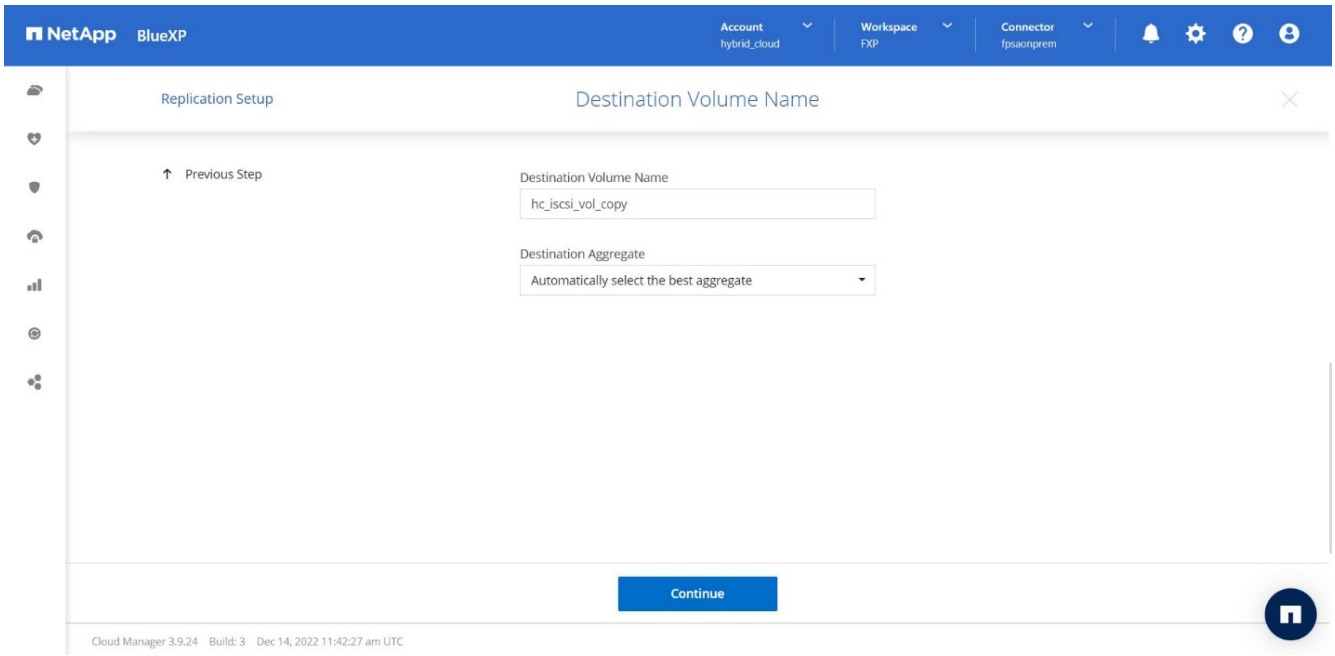
画面を示しています。1つのボリューム（14個）が表示されています。"]

5. *デスティネーションディスクの種類と階層化。*ターゲットがCloud Volumes ONTAP システムの場合は、デスティネーションディスクの種類を選択し、データ階層化を有効にするかどうかを選択します。



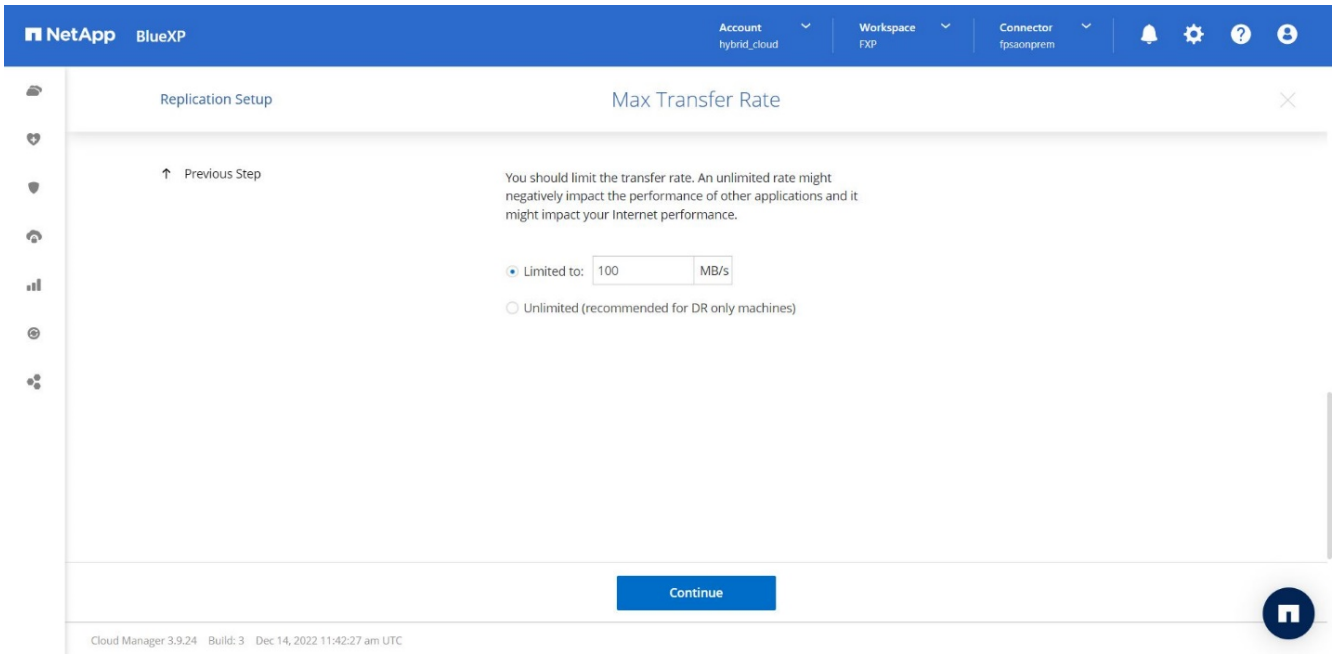
画面を示しています。"]

6. *デスティネーションボリューム名：*デスティネーションボリュームの名前を指定し、デスティネーションアグリゲートを選択してください。デスティネーションが ONTAP クラスタの場合は、デスティネーション Storage VM も指定する必要があります。



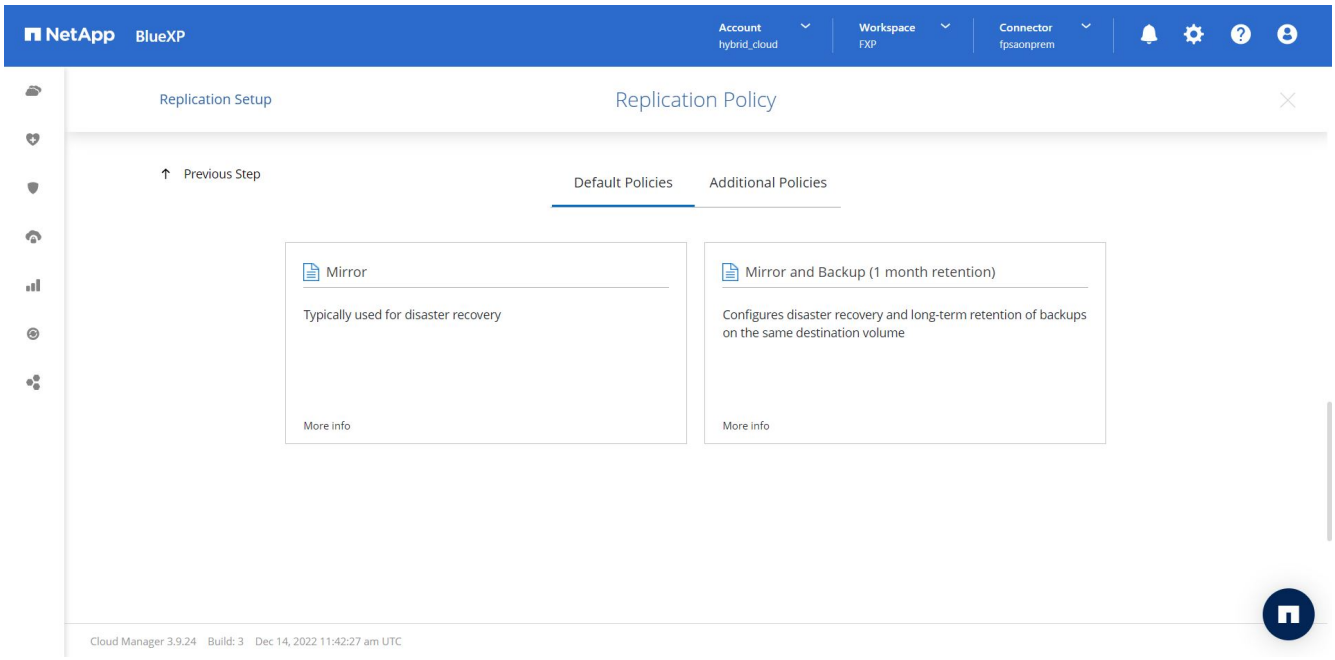
画面を示しています。関連する情報が入力されています。"]

7. *最大転送速度。*データを転送できる最大転送速度（1秒あたりのメガバイト数）を指定します。



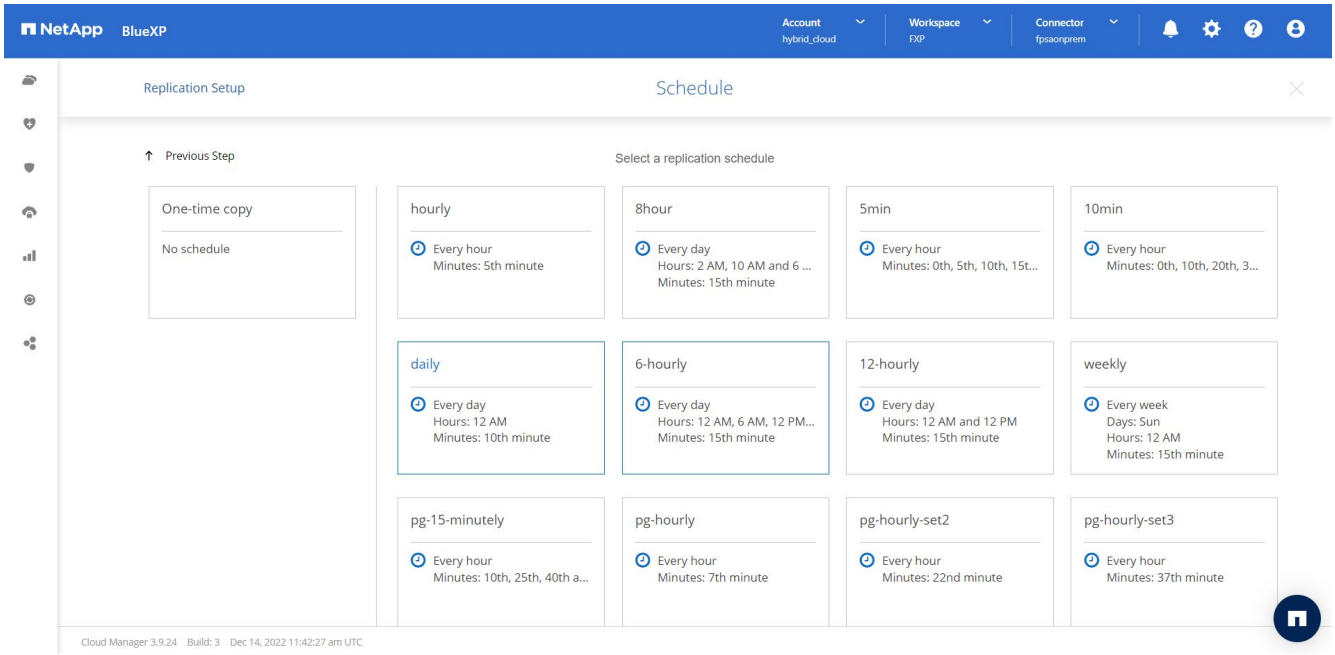
画面を示しています。100MB/sが入力されています。"]

8. レプリケーションポリシー。*デフォルトポリシーを選択するか[その他のポリシー]*をクリックし、いずれかの高度なポリシーを選択します。ヘルプを表示するには、 "レプリケーションポリシーについて説明します"。

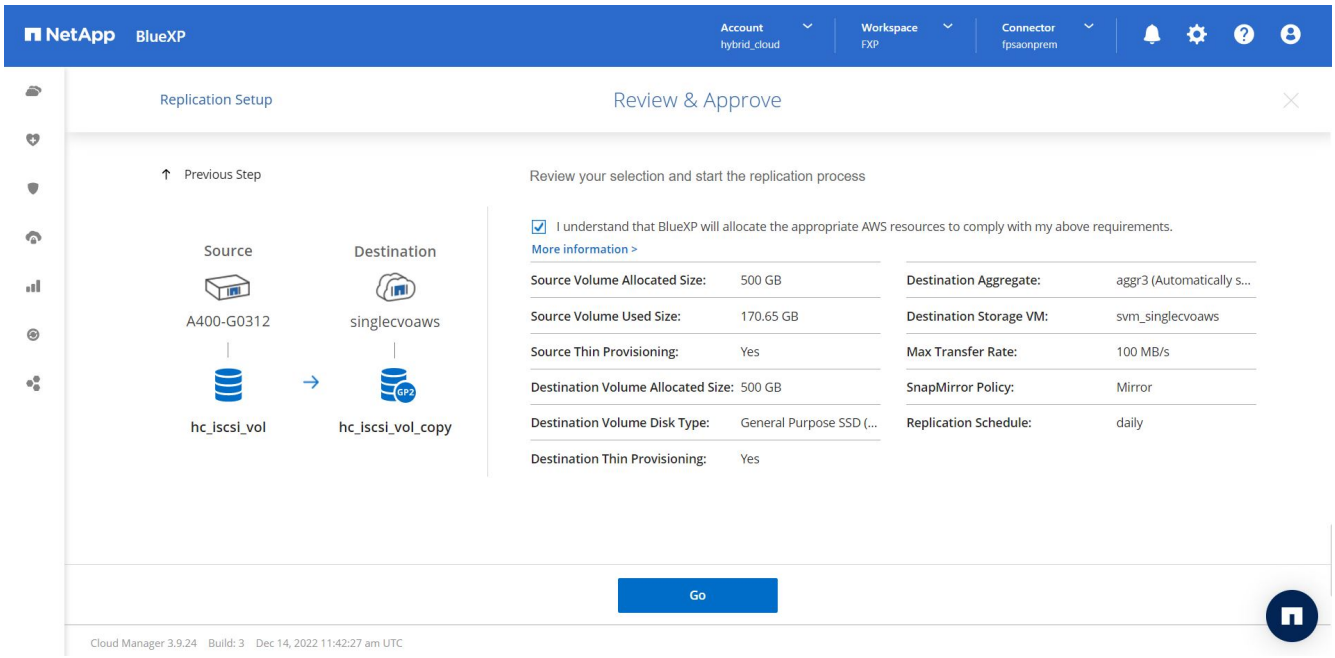


ページを示しています。デフォルトのポリシーである「Mirror」または「Mirror and Backup」が表示されています。"]

9. スケジュール。 1回限りのコピーまたは定期的なスケジュールを選択します。いくつかのデフォルトスケジュールを使用できます。別のスケジュールが必要な場合は、で新しいスケジュールを作成する必要があります `destination cluster` System Manager を使用



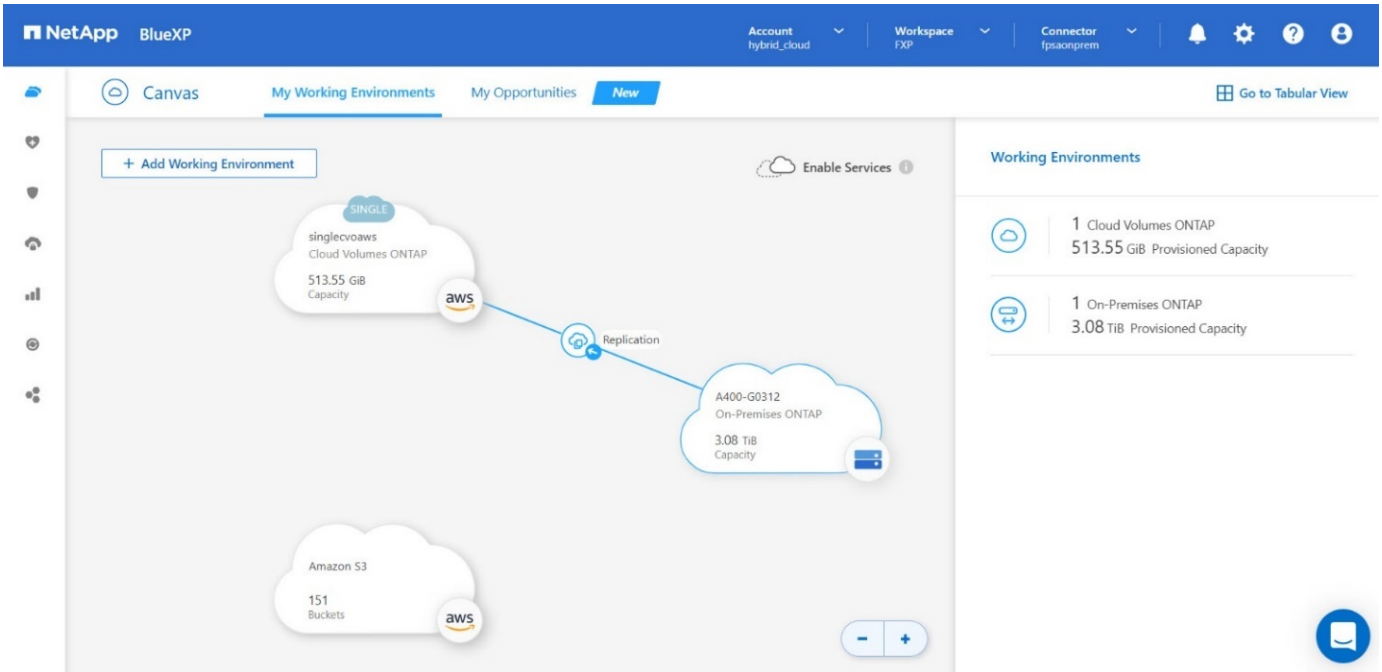
10. *確認。*選択内容を確認し、*移動*をクリックします。



画面を示しています。"]

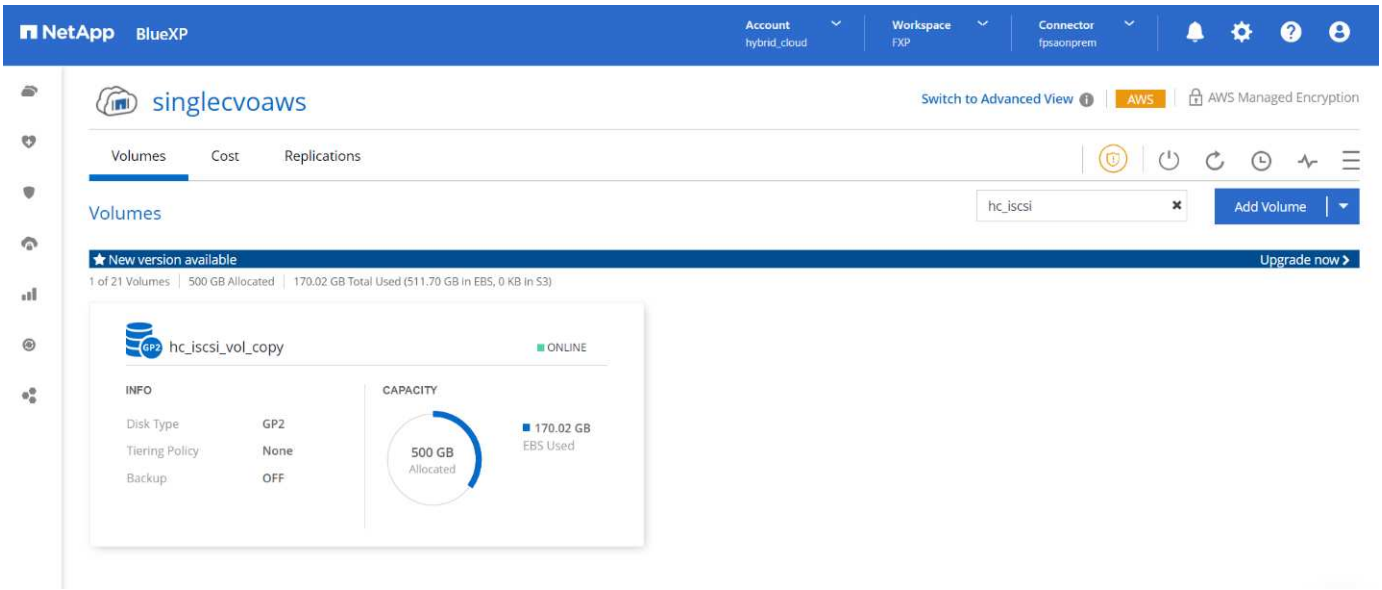
これらの設定手順の詳細については、を参照してください "こちらをご覧ください"。

BlueXPがデータレプリケーションプロセスを開始しますオンプレミスのONTAP システムとCloud Volumes ONTAP の間に確立された*レプリケーション*サービスを確認できます。



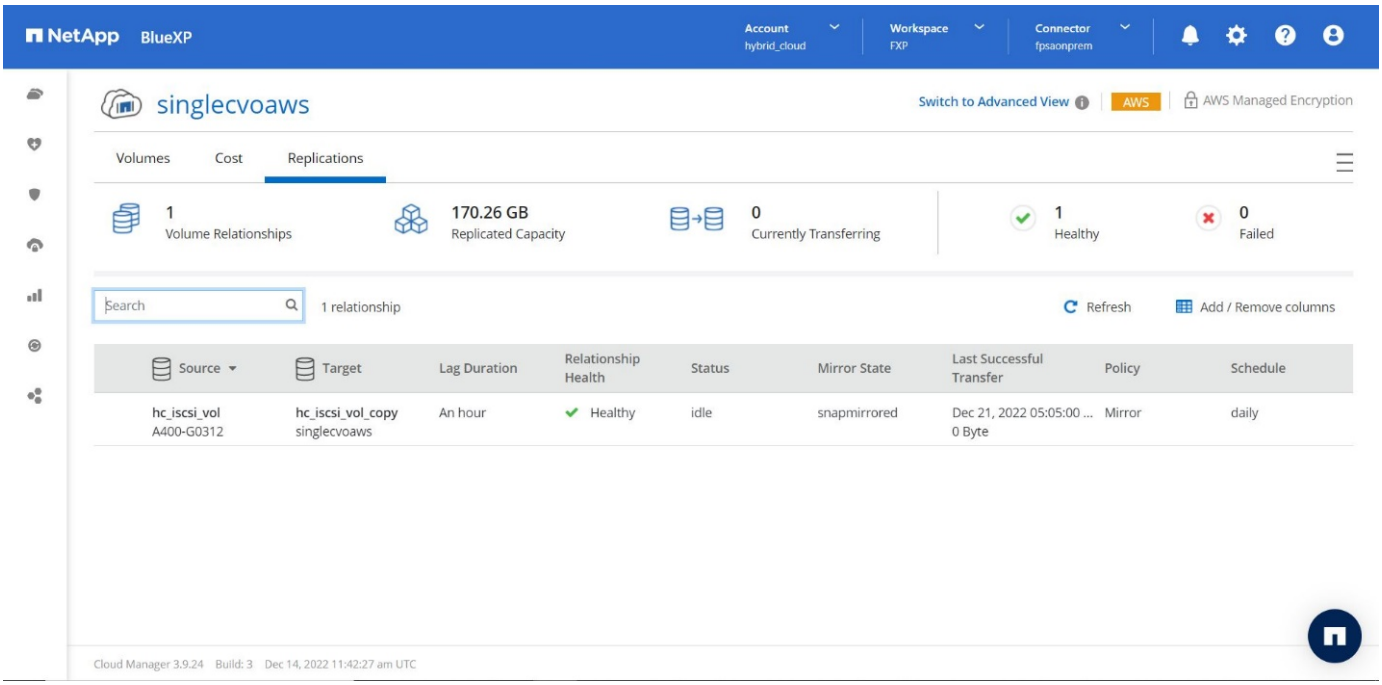
画面を示しています。レプリケーションサービスはCVOインスタンスとオンプレミスのONTAP インスタンスを結ぶ線で示されています。"]

Cloud Volumes ONTAP クラスタでは、新しく作成されたボリュームを確認できます。



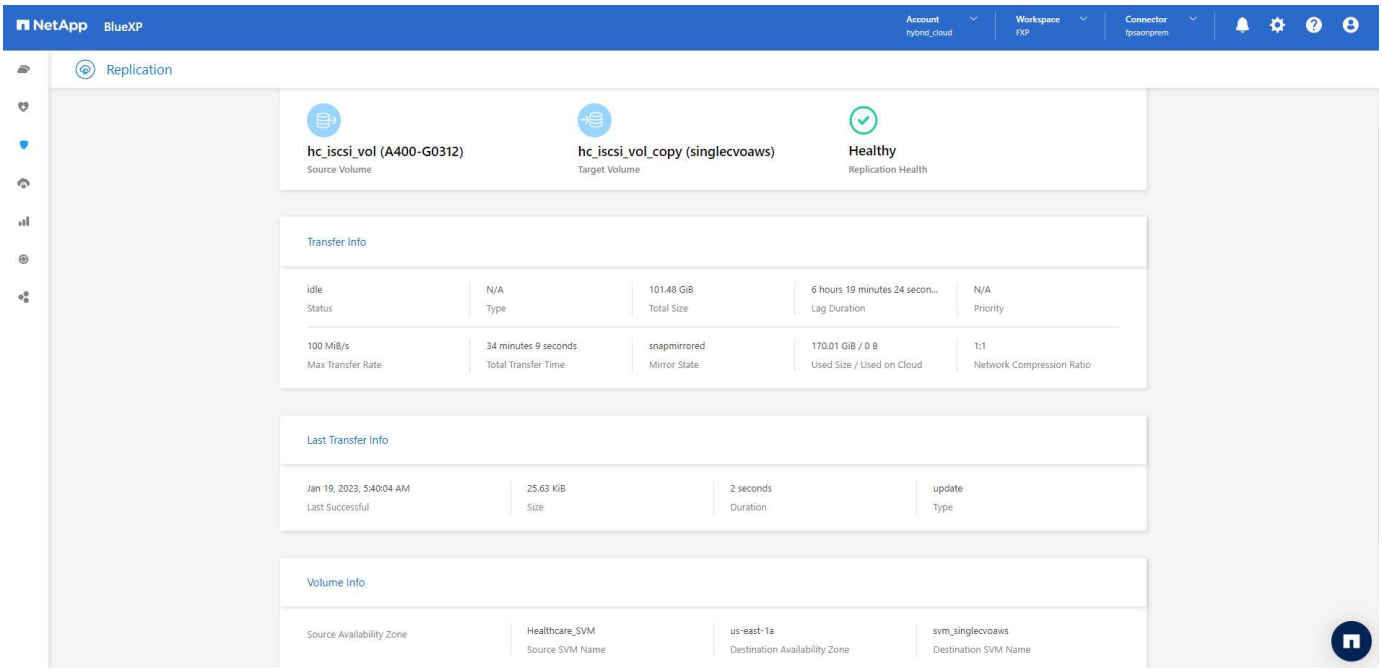
タブを示しています。新しいボリュームが表示されています。"]

オンプレミスボリュームとクラウドボリュームの間にSnapMirror関係が確立されたことを確認することもできます。



タブを示しており、作成したレプリケーション関係に関する情報が表示されています。"]

レプリケーションタスクの詳細については、*[レプリケーション]*タブを参照してください。



タブの下に詳細情報を示しています。"]

"次の例は、解決策の検証です。"

解決策の検証

"前の手順：SAN構成"

このセクションでは、解決策 のユースケースをいくつか確認します。

- SnapMirrorの主なユースケースの1つに、データバックアップがあります。SnapMirrorは、同じクラスタ内またはリモートターゲットにデータをレプリケートすることで、プライマリバックアップツールとして使用できます。
- DR環境を使用したアプリケーション開発テスト（開発とテスト）の実行
- 本番環境で災害が発生した場合のDR。
- データ配信とリモートデータアクセス：

注目すべき点として、この解決策 で検証された比較的少数のユースケースでは、SnapMirrorレプリケーションの全機能を網羅しているわけではありません。

アプリケーションの開発とテスト（開発とテスト）

レプリケートされたデータをDRサイトで迅速にクローニングし、開発/テストアプリケーションに使用することで、アプリケーションの開発期間を短縮できます。DR環境と開発/テスト環境をコロケーションすることで、バックアップやDR施設の利用率を大幅に向上できます。また、オンデマンドの開発/テスト用クローンにより、必要な数のデータコピーを迅速に本番環境に移行できます。

NetApp FlexCloneテクノロジを使用すると、セカンダリコピーの読み取り/書き込みアクセスを許可してすべての本番環境データが利用可能かどうかを確認する場合に、SnapMirrorデスティネーションFlexVol ボリュームの読み取り/書き込みコピーを迅速に作成できます。

DR環境を使用してアプリケーションの開発とテストを実行するには、次の手順を実行します。

1. 本番環境のデータのコピーを作成します。そのためには、オンプレミスボリュームのアプリケーションスナップショットを実行します。アプリケーションスナップショットの作成は、3つのステップで構成されます。 `Lock`、 `Snap`および `Unlock`。

   a. ファイルシステムを休止して、I/Oが中断され、アプリケーションの整合性が維持されるようにします。ファイルシステムにヒットするアプリケーションの書き込みは、手順cで休止解除コマンドが実行されるまで待機状態のままですステップa、b、cは透過的なプロセスまたはワークフローを通じて実行され、アプリケーションのSLAには影響しません。

   ```
   [root@hc-cloud-secure-1 ~]# fsfreeze -f /file1
   ```

   このオプションは、指定されたファイルシステムが新しい変更からフリーズされるように要求します。フリーズされたファイルシステムに書き込みを試みるプロセスは、ファイルシステムがフリーズ解除されるまでブロックされます。

   b. オンプレミスボリュームのSnapshotを作成

   ```
   A400-G0312::> snapshot create -vserver Healthcare_SVM -volume
   hc_iscsi_vol -snapshot kamini
   ```

   c. ファイルシステムを休止解除してI/Oを再開します。

   ```
   [root@hc-cloud-secure-1 ~]# fsfreeze -u /file1
   ```

   このオプションは、ファイルシステムのフリーズを解除し、操作を続行できるようにするために使用します。フリーズによってブロックされたファイルシステムの変更はブロック解除され、完了することができます。

   アプリケーションと整合性のあるSnapshotは、前述のワークフローをSnapCenter の一部として完全にオーケストレーションしたNetApp SnapCenter を使用して実行することもできます。詳細については、を参照してください "こちらをご覧ください"。

2. SnapMirror更新処理を実行して、業務用システムとDRシステムの同期を維持します。

   ```
   singlecvoaws::> snapmirror update -destination-path
   svm_singlecvoaws:hc_iscsi_vol_copy -source-path
   Healthcare_SVM:hc_iscsi_vol

   Operation is queued: snapmirror update of destination
   "svm_singlecvoaws:hc_iscsi_vol_copy".
   ```

   BlueXPのGUIの*[Replication]*タブから、SnapMirrorの更新を実行することもできます。

3. 前の手順で作成したアプリケーションSnapshotに基づいてFlexCloneインスタンスを作成します。

```
singlecvoaws::> volume clone create -flexclone kamini_clone -type RW
-parent-vserver svm_singlecvoaws -parent-volume hc_iscsi_vol_copy
-junction-active true -foreground true -parent-snapshot kamini

[Job 996] Job succeeded: Successful
```

前のタスクでは、新しいSnapshotも作成できますが、アプリケーションの整合性を確保するには、上記と同じ手順を実行する必要があります。

4. FlexCloneボリュームをアクティブ化して、クラウドでEHRインスタンスを起動します。

```
singlecvoaws::> lun mapping create –vserver svm_singlecvoaws –path
/vol/kamini_clone/iscsi_lun1 -igroup ehr-igroup –lun-id 0

singlecvoaws::> lun mapping show
Vserver     Path                                    Igroup    LUN ID
Protocol
---------- -------------- --------------- -----  --------   ------
---------
svm_singlecvoaws
                 /vol/kamini_clone/iscsi_lun1    ehr-igroup   0    iscsi
```

5. クラウドのEHRインスタンスで次のコマンドを実行して、データまたはファイルシステムにアクセスします。
   a. ONTAP ストレージを検出マルチパスのステータスを確認します。

```
sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show

Output:
controller(7mode/E-Series)/         device    host              lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------------
--------
svm_singlecvoaws                    /dev/sda  host2   iSCSI    200g
cDOT
                    /vol/kamini_clone/iscsi_lun1
sudo multipath -ll

Output:
3600a09806631755a452b543041313053 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running
```

b. ボリュームグループをアクティブ化します。

```
sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active
```

c. ファイル・システムをマウントし'ファイル・システム情報の概要を表示します

```
sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                1K-blocks  Used     Available  Use%
Mounted on
/dev/mapper/datavg-datalv  209608708 183987096  25621612  88%
/file1
```

これにより、アプリケーションの開発とテストにDR環境を使用できるかどうかが検証されます。DRストレージでアプリケーションの開発とテストを実行すると、ほとんどの時間アイドル状態になる可

能性のあるリソースをより有効に活用できます。

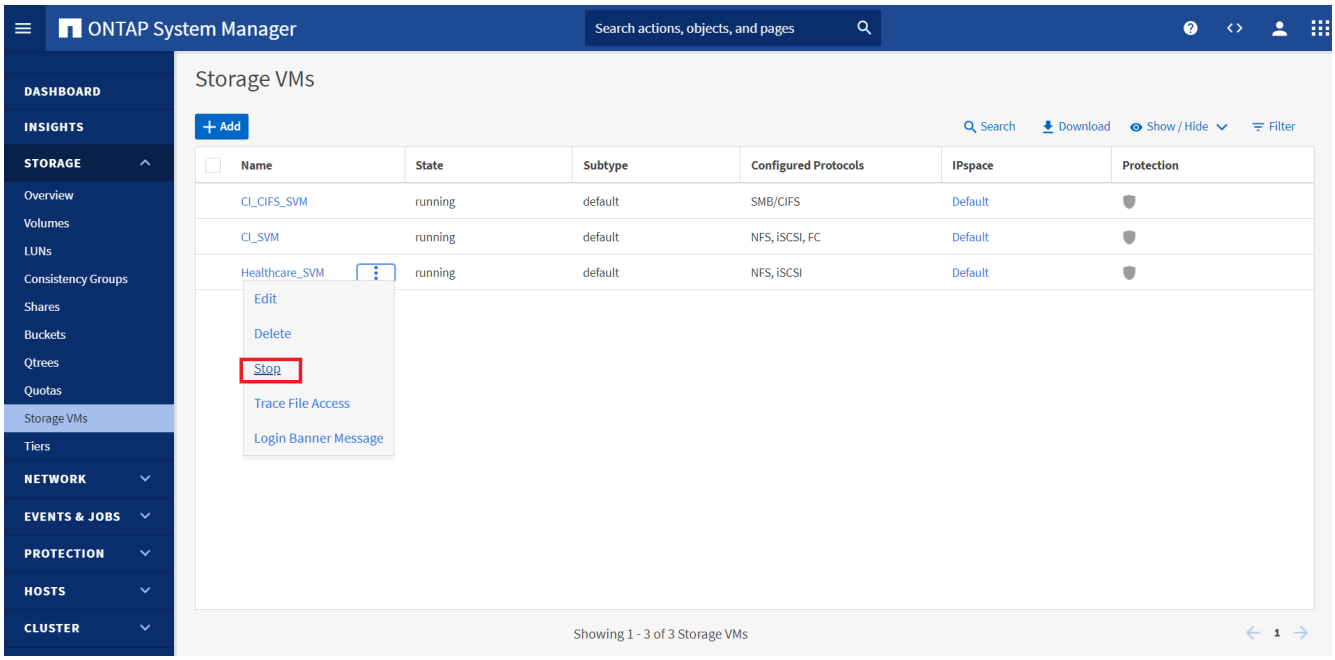
ディザスタリカバリ

SnapMirrorテクノロジは、DR計画の一部としても使用されます。重要なデータが物理的に別の場所にレプリケートされている場合、重大な災害が原因 発生しても、ビジネスクリティカルなアプリケーションで長期間データを使用できなくなることはありません。クライアントは、破損、偶発的な削除、自然災害などから本番サイトをリカバリするまで、レプリケートされたデータにネットワーク経由でアクセスできます。

プライマリサイトへのフェイルバックの場合、SnapMirrorを使用すると、SnapMirror関係をDRサイトからプライマリサイトに反転させるだけで、変更されたデータや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して、DRサイトとDRサイトを効率的に再同期できます。プライマリサイトで通常のアプリケーション運用が再開されると、SnapMirrorは、ベースライン転送をもう1回行わずにDRサイトへの転送を続行します。

DRシナリオが成功するかどうかを検証するには、次の手順を実行します。

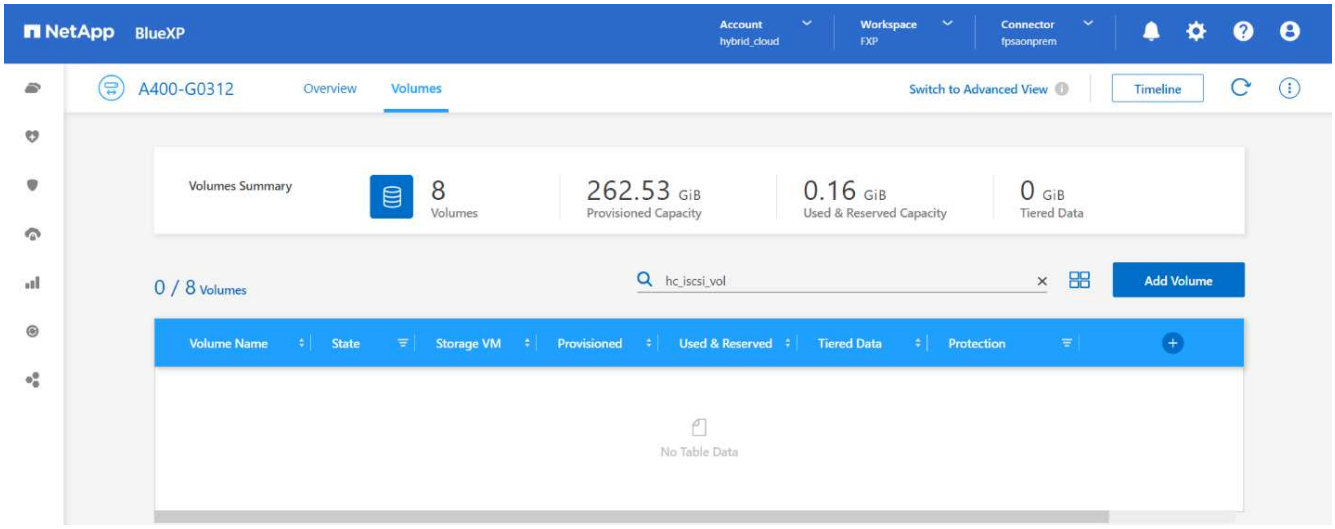
1. オンプレミスのONTAP ボリュームをホストするSVMを停止して、ソース（本番）側で災害をシミュレートします (`hc_iscsi_vol`）。



ドロップダウンにある[stop]オプションを示しています。"]

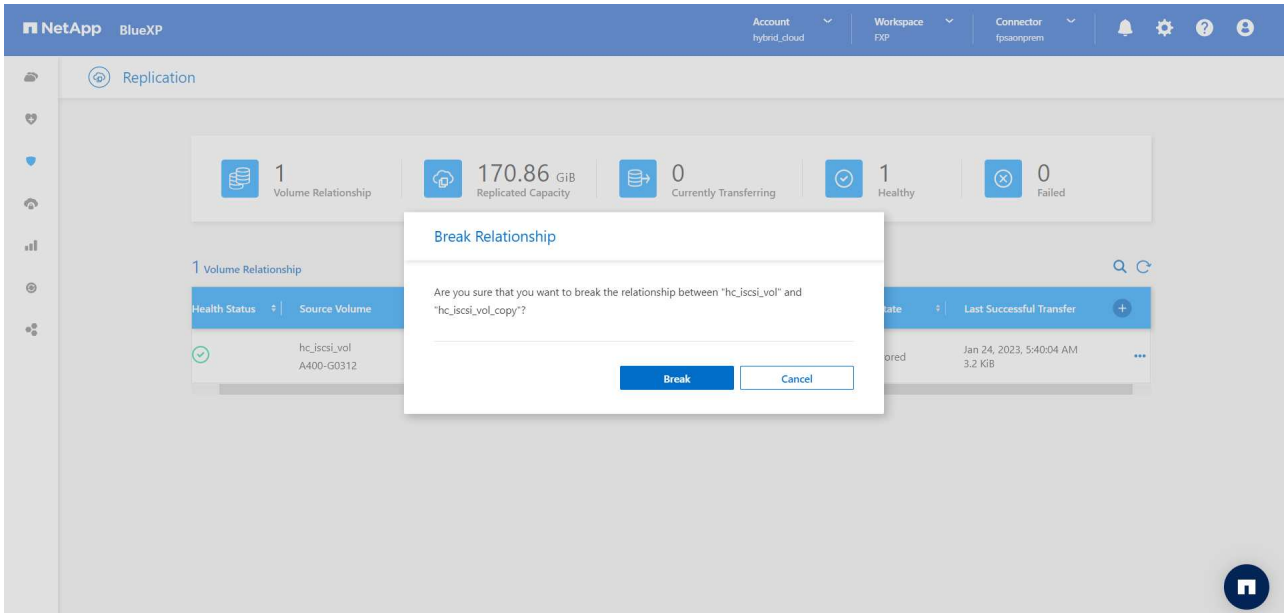
アプリケーションのSnapshotを頻繁に作成できるように、FlexPod インスタンスのオンプレミスONTAPとAWSのCloud Volumes ONTAP の間でSnapMirrorレプリケーションがすでに設定されていることを確認します。

SVMが停止したあと、 `hc_iscsi_vol` ボリュームはBlueXPに表示されません。



2. CVOでDRをアクティブ化

   a. オンプレミスのONTAP とCloud Volumes ONTAP の間のSnapMirrorレプリケーション関係を解除し、CVOのデスティネーションボリュームを昇格します (`hc_iscsi_vol_copy`）を本番環境に移行します。



   SnapMirror関係を解除すると、デスティネーションボリュームのタイプがデータ保護（DP）から読み書き可能（rw）に変わります。

```
singlecvoaws::> volume show -volume hc_iscsi_vol_copy -fields typev
server          volume              type
--------------- ------------------- ----
svm_singlecvoaws hc_iscsi_vol_copy RW
```

   b. Cloud Volumes ONTAP でデスティネーションボリュームをアクティブ化し、クラウド内のEC2インスタンスでEHRインスタンスを起動します。

```
singlecvoaws::> lun mapping create –vserver svm_singlecvoaws –path
/vol/hc_iscsi_vol_copy/iscsi_lun1 -igroup ehr-igroup –lun-id 0

singlecvoaws::> lun mapping show
Vserver     Path                                  Igroup   LUN ID
Protocol
---------- ----------------------------------  --------  ------
---------
svm_singlecvoaws
            /vol/hc_iscsi_vol_copy/iscsi_lun1  ehr-igroup  0    iscsi
```

c. クラウド内のEHRインスタンス上のデータとファイルシステムにアクセスするには、まずONTAP ストレージを検出し、マルチパスのステータスを確認します。

```
sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show
Output:
controller(7mode/E-Series)/         device    host              lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------------
--------
svm_singlecvoaws                    /dev/sda  host2   iSCSI    200g
cDOT
                  /vol/hc_iscsi_vol_copy/iscsi_lun1
sudo multipath -ll
Output:
3600a09806631755a452b543041313051 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running
```

d. ボリュームグループをアクティブ化します。

```
sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active
```

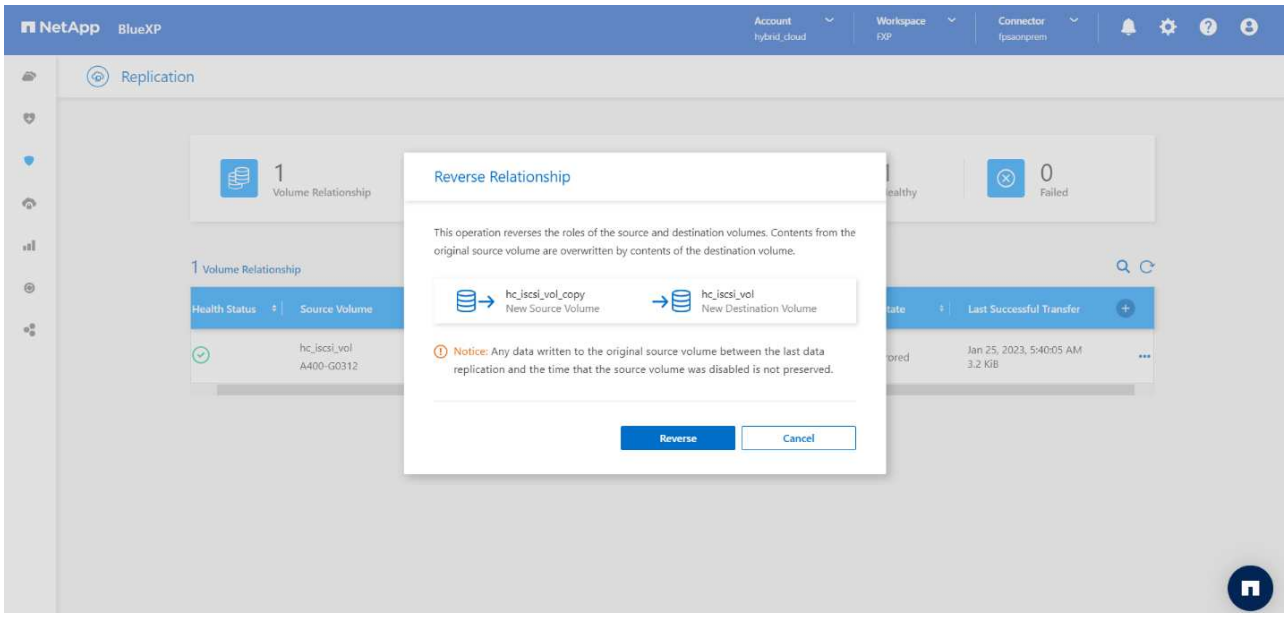
e. 最後に、ファイルシステムをマウントし、ファイルシステム情報を表示します。

```
sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                 1K-blocks  Used      Available  Use%
Mounted on
/dev/mapper/datavg-datalv  209608708  183987096  25621612  88%
/file1
```

この出力は、災害から本番サイトがリカバリされるまで、ユーザがネットワーク経由でレプリケートされたデータにアクセスできることを示しています。

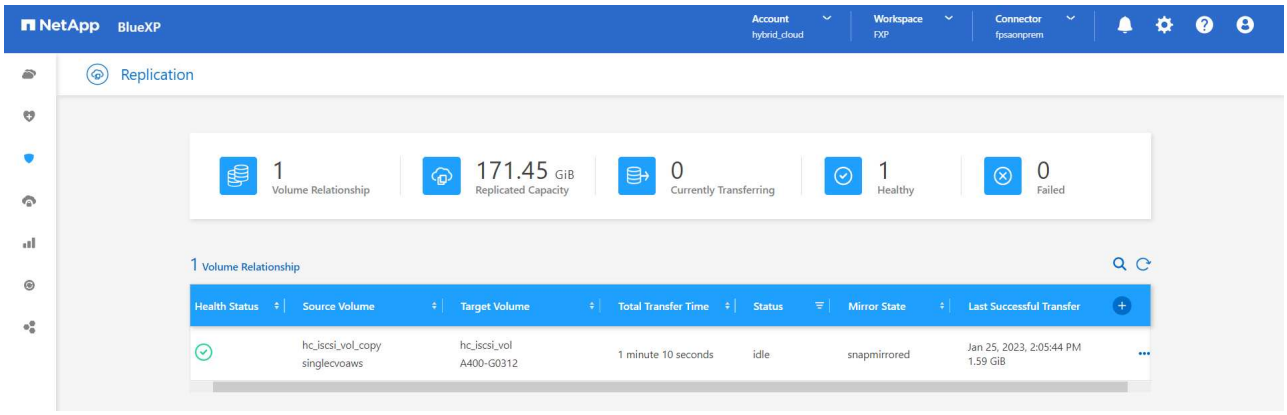
f. SnapMirror関係を反転します。この処理では、ソースボリュームとデスティネーションボリュームの役割が入れ替わります。



ボックスを示しています。"]

この処理を実行すると、元のソースボリュームの内容がデスティネーションボリュームの内容で上書きされます。これは、オフラインになったソースボリュームを再アクティブ化する場合に役立ちます。

CVOボリュームに移動します (`hc_iscsi_vol_copy`）がソースボリュームになり、オンプレミスボリュームになります (`hc_iscsi_vol`）がデスティネーションボリュームになります。



前回のデータレプリケーションからソースボリュームが無効になったまでの間に元のソースボリュームに書き込まれたデータは保持されません。

a. CVOボリュームへの書き込みアクセスを確認するには、クラウドのEHRインスタンスに新しいファイルを作成します。

```
cd /file1/
sudo touch newfile
```

業務用サイトが停止しても、クライアントは引き続きデータにアクセスし、Cloud Volumes ONTAP ボリューム（現在はソースボリューム）への書き込みも実行できます。

プライマリサイトへのフェイルバックの場合、SnapMirrorを使用すると、SnapMirror関係をDRサイトからプライマリサイトに反転させるだけで、変更されたデータや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して、DRサイトとDRサイトを効率的に再同期できます。プライマリサイトで通常のアプリケーション運用が再開されると、SnapMirrorは、ベースライン転送をもう1回行わずにDRサイトへの転送を続行します。

このセクションでは、業務用サイトで災害が発生した場合のDRシナリオの適切な解決方法について説明します。これで、ソースサイトのリストア中にクライアントにサービスを提供できるアプリケーションが、データを安全に消費できるようになります。

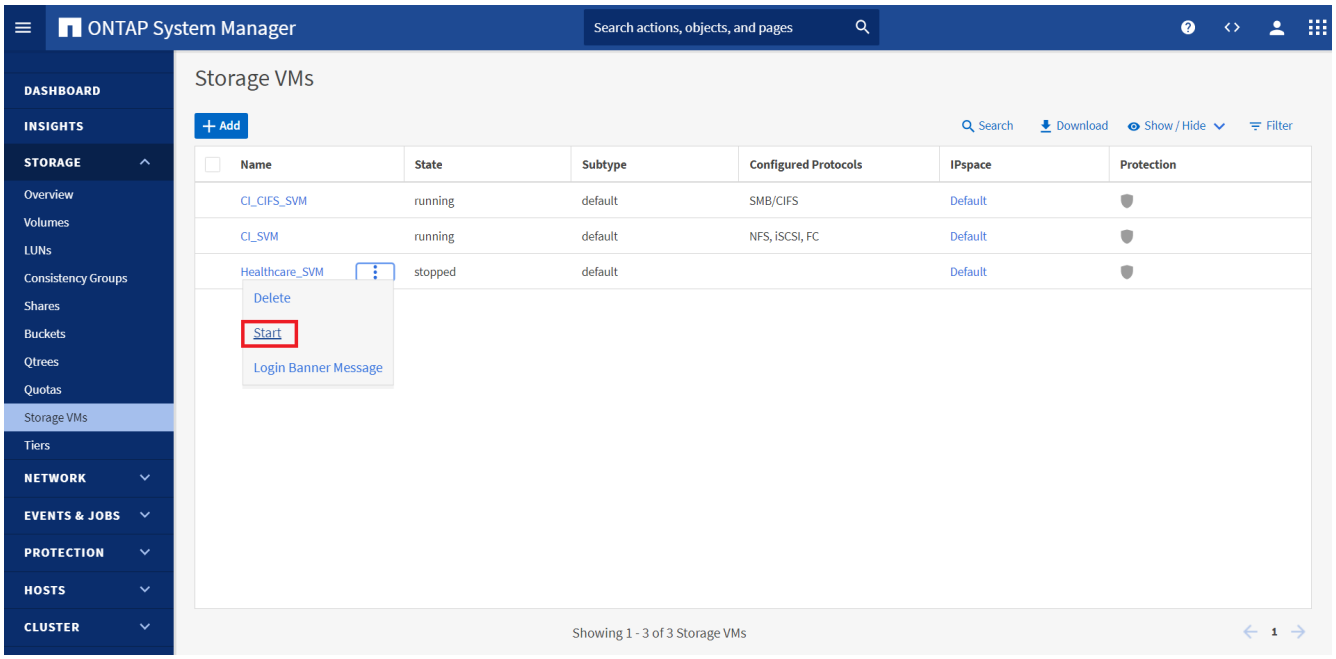
本番サイトでのデータの検証

業務用サイトをリストアしたら、元の構成がリストアされ、クライアントがソースサイトのデータにアクセスできることを確認する必要があります。

このセクションでは、ソースサイトを立ち上げ、オンプレミスのONTAP とCloud Volumes ONTAP 間のSnapMirror関係をリストアし、最後にソース側でデータ整合性チェックを実行します

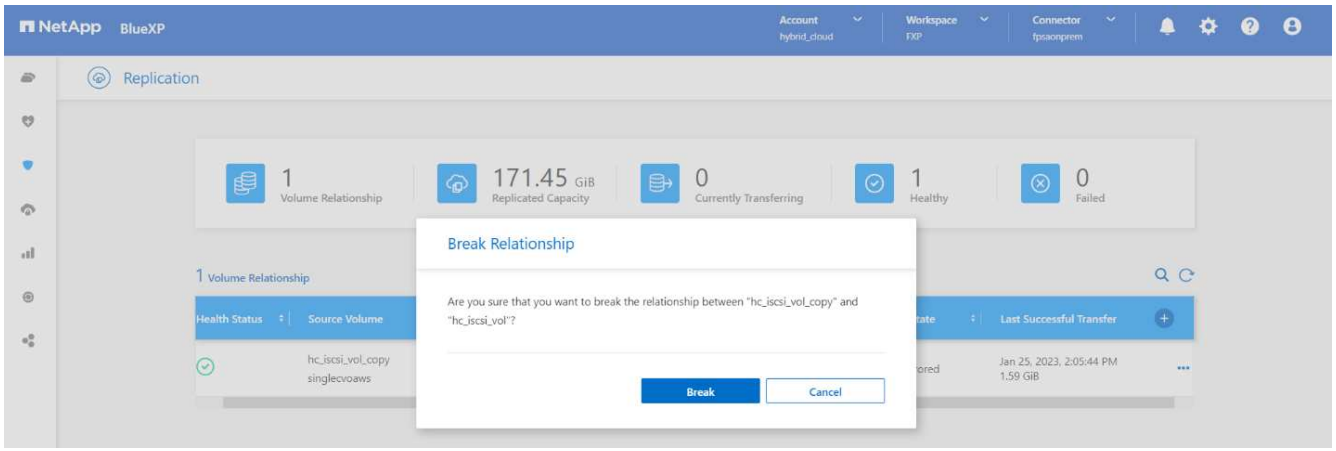
業務用サイトでは、次の手順 を使用してデータを検証できます。

1. ソースサイトが稼働していることを確認します。これを行うには、オンプレミスのONTAP ボリュームをホストするSVMを起動します (`hc_iscsi_vol`）。



ページのドロップダウンメニューを使用して特定のVMを起動する方法を示しています。"]

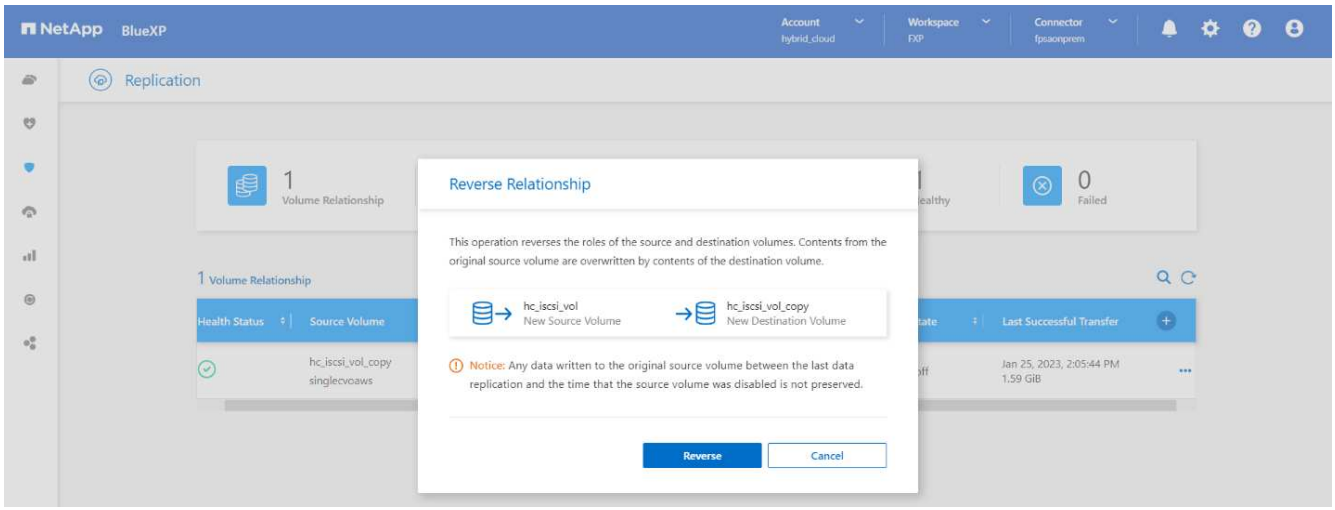
2. Cloud Volumes ONTAP とオンプレミスのONTAP 間のSnapMirrorレプリケーション関係を解除し、オンプレミスボリュームを昇格 (`hc_iscsi_vol`）を本番環境に戻します。



SnapMirror関係を解除すると、オンプレミスのボリュームタイプがデータ保護（DP）から読み取り/書き込み（RW）に変わります。

```
A400-G0312::> volume show -volume hc_iscsi_vol -fields type
vserver         volume        type
--------------- ------------- ----
Healthcare_SVM hc_iscsi_vol RW
```

3. SnapMirror関係を反転します。今度はオンプレミスのONTAP ボリュームです (`hc_iscsi_vol`）がソースボリュームになり、Cloud Volumes ONTAP ボリュームになります (`hc_iscsi_vol_copy`）がデスティネーションボリュームになります。



これらの手順を実行することで、元の構成が正常に復元されました。

4. オンプレミスのEHRインスタンスをリブートします。ファイルシステムをマウントし、を確認します `newfile` 本番環境がダウンしていたときにクラウドのEHRインスタンスに作成したものもここに存在します。

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1
[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01  dir05  dir09  dir13  dir17  dir21  dir25  dir29  dir33  dir37  dir41  dir45  dir49  dir53  dir57  dir61  dir65  dir69  dir73  dir77  kamini
dir02  dir06  dir10  dir14  dir18  dir22  dir26  dir30  dir34  dir38  dir42  dir46  dir50  dir54  dir58  dir62  dir66  dir70  dir74  dir78  latest_file
dir03  dir07  dir11  dir15  dir19  dir23  dir27  dir31  dir35  dir39  dir43  dir47  dir51  dir55  dir59  dir63  dir67  dir71  dir75  dir79  newfile
dir04  dir08  dir12  dir16  dir20  dir24  dir28  dir32  dir36  dir40  dir44  dir48  dir52  dir56  dir60  dir64  dir68  dir72  dir76  dir80
```

ソースからデスティネーションへのデータレプリケーションが正常に完了し、データの整合性が維持されていると推測できます。これで、本番サイトでのデータの検証は完了です。

"次は終わりです"

まとめ

"前のバージョン：解決策 の検証。"

ほとんどの医療機関では、ハイブリッドクラウドの構築が、いつでもデータにアクセスできるようにすることを目標としています。この解決策 では、Cloud Volumes ONTAP を備えたFlexPod ハイブリッドクラウド解決策 を実装し、ネットアップのSnapMirrorレプリケーションテクノロジを活用して、ヘルスケアアプリケーションとワークロードのバックアップとリカバリのいくつかのユースケースを検証しました。

FlexPod は、Ciscoとネットアップの戦略的パートナーシップが提供する厳格なテストと検証済みの統合インフラです。予測可能な低レイテンシのシステムパフォーマンスと高可用性を実現するように設計されています。このアプローチにより、EHRの快適性レベルが高くなり、最終的にEHRシステムのユーザーにとって最適な応答時間が得られます。

ネットアップなら、オンプレミスのデータセンターでネットアップのストレージ機能を実行するのと同じように、本番環境のEHR、ディザスタリカバリ、バックアップ、階層化をクラウドで実行できます。ネットアップは、NetApp Cloud Volumes ONTAP を使用して、クラウドでEHRを効果的に実行するために必要なエンタープライズクラスの機能とパフォーマンスを提供します。ネットアップのクラウドオプションは、iSCSI経由のブロックとNFSまたはSMB経由のファイルを提供します。

この解決策 は、医療機関のニーズに応え、デジタル変革に向けた一歩を踏み出すためのものです。また、アプリケーションやワークロードを効率的に管理するのにも役立ちます。

"次へ：追加情報の検索場所。"

追加情報の参照先

"前へ：終わりに。"

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

- FlexPod ホームページ

  "https://www.flexpod.com"

- FlexPod のシスコ検証済み設計および導入ガイド

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- NetApp BlueXP

  "https://bluexp.netapp.com/"

- NetApp Cloud Volumes ONTAP の略

  "https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/concept-overview-cvo.html"

- AWS での Cloud Volumes ONTAP のクイックスタート

  "https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-aws.html"

- SnapMirror レプリケーション

  "https://docs.netapp.com/us-en/cloud-manager-replication/concept-replication.html"

- TR-3928：『NetApp Best Practices for Epic』

  https://www.netapp.com/pdf.html?item=/media/17137-tr3928pdf.pdf

- TR-4693 ：『 FlexPod Datacenter for Epic EHR Deployment Guide 』

  "https://www.netapp.com/media/10658-tr-4693.pdf"

- FlexPod for Epicの略

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmw_epic.html"

- NetApp Interoperability Matrix Tool で確認できます

  "http://support.netapp.com/matrix/"

- Cisco UCS ハードウェアおよびソフトウェア相互運用性ツール

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- VMware Compatibility Guide 』を参照してください

  "http://www.vmware.com/resources/compatibility/search.php"

バージョン履歴

バージョン	日付	ドキュメントのバージョン履歴
バージョン 1.0 以降	2023年3月	初版

ネットアップのCloud Volumes ONTAP とCisco Intersightを活用したFlexPod ハイブリッドクラウドfor Google Cloud Platform

TR-4939：『FlexPod Hybrid Cloud for Google Cloud Platform with NetApp Cloud Volumes ONTAP and Cisco Intersight』

Ruchika Lahoti、ネットアップ

はじめに

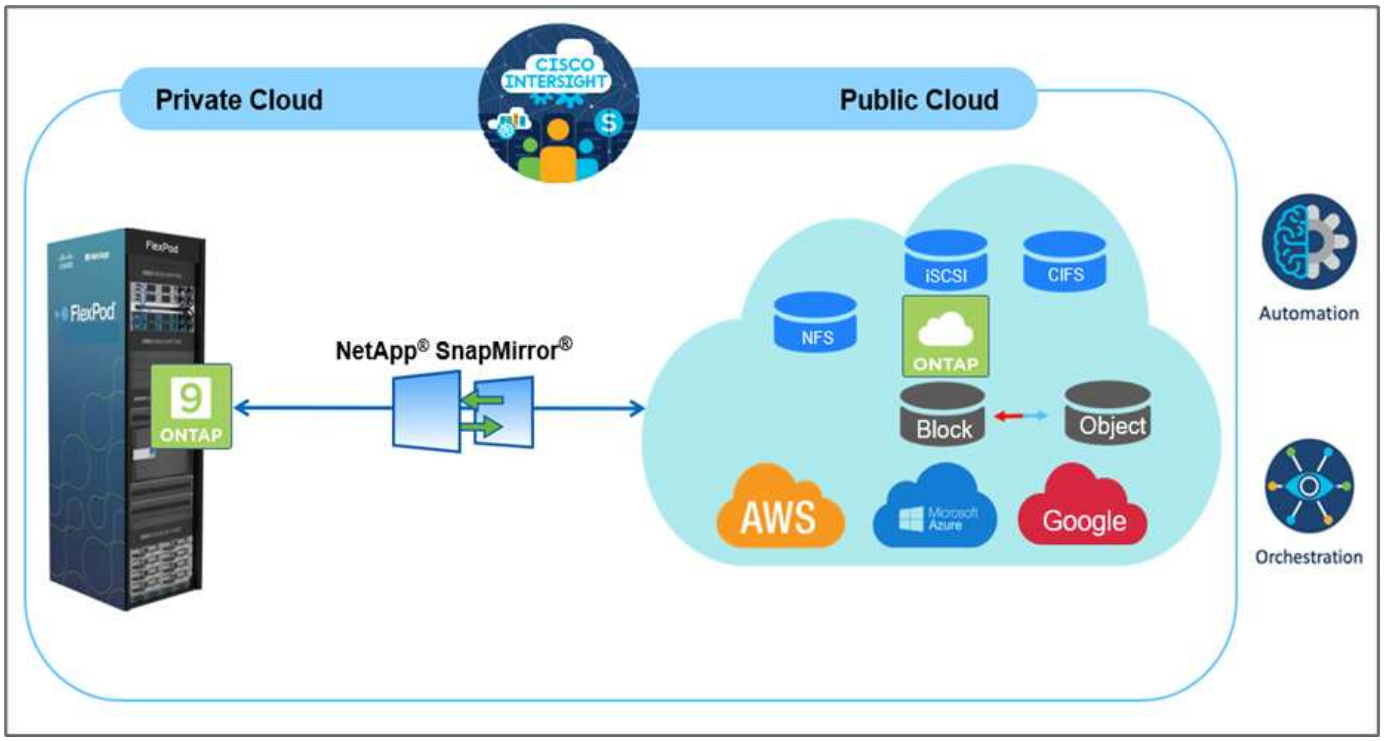
企業の継続性を確保するうえで重要な目標は、ディザスタリカバリ（DR）によってデータを保護することです。DRを使用すると、企業は業務をセカンダリサイトにフェイルオーバーし、あとでプライマリサイトに効率的かつ確実にリカバリおよびフェイルバックできます。自然災害、ネットワーク障害、ソフトウェアの脆弱性、人為的ミスなど、さまざまな懸念があるため、DR戦略を開発することがITの最優先事項となっています。

DRに関しては、プライマリサイトで実行しているすべてのワークロードを、DRサイトで忠実に再現する必要があります。組織には、データベース、ファイルサービス、NFS、iSCSIストレージなど、すべてのエンタープライズデータの最新コピーも必要です。本番環境のデータは常に更新されるため、変更は定期的にDRサイトに転送する必要があります。

DR環境の導入は、インフラやサイトに依存しないことが求められるため、ほとんどの組織にとって困難な課題です。必要なリソースの数や、セカンダリデータセンターのセットアップ、テスト、メンテナンスにかかるコストは、通常、本番環境全体のコストに迫ることがあります。データを継続的に同期し、シームレスなフェイルオーバーとフェイルバックを確立しながら、最小限のデータ容量で十分な保護を維持することは困難です。DRサイトを構築したら、本番環境からデータをレプリケートし、それを同期して先に進めるという課題に直面します。

このテクニカルレポートでは、FlexPod コンバージドインフラ解決策 、Google Cloud上のNetApp Cloud Volumes ONTAP 、およびCisco Intersightを統合して、DR用のハイブリッドクラウドデータセンターを形成しています。この解決策 では、Cisco Intersight Cloud Orchestratorを使用したオンプレミスONTAP ワークフローの設計と実行について説明します。また、ネットアップCloud Volumes ONTAP の導入、FlexPod とCloud Volumes ONTAP 間のデータレプリケーションおよびDRのオーケストレーションと自動化についても、Cisco Intersight Service for橋(Cisco Intersight Service for橋Corp Terraform)を使用して説明します。

次の図は、解決策 の概要を示しています。



この解決策 には、次のような複数の利点があります。

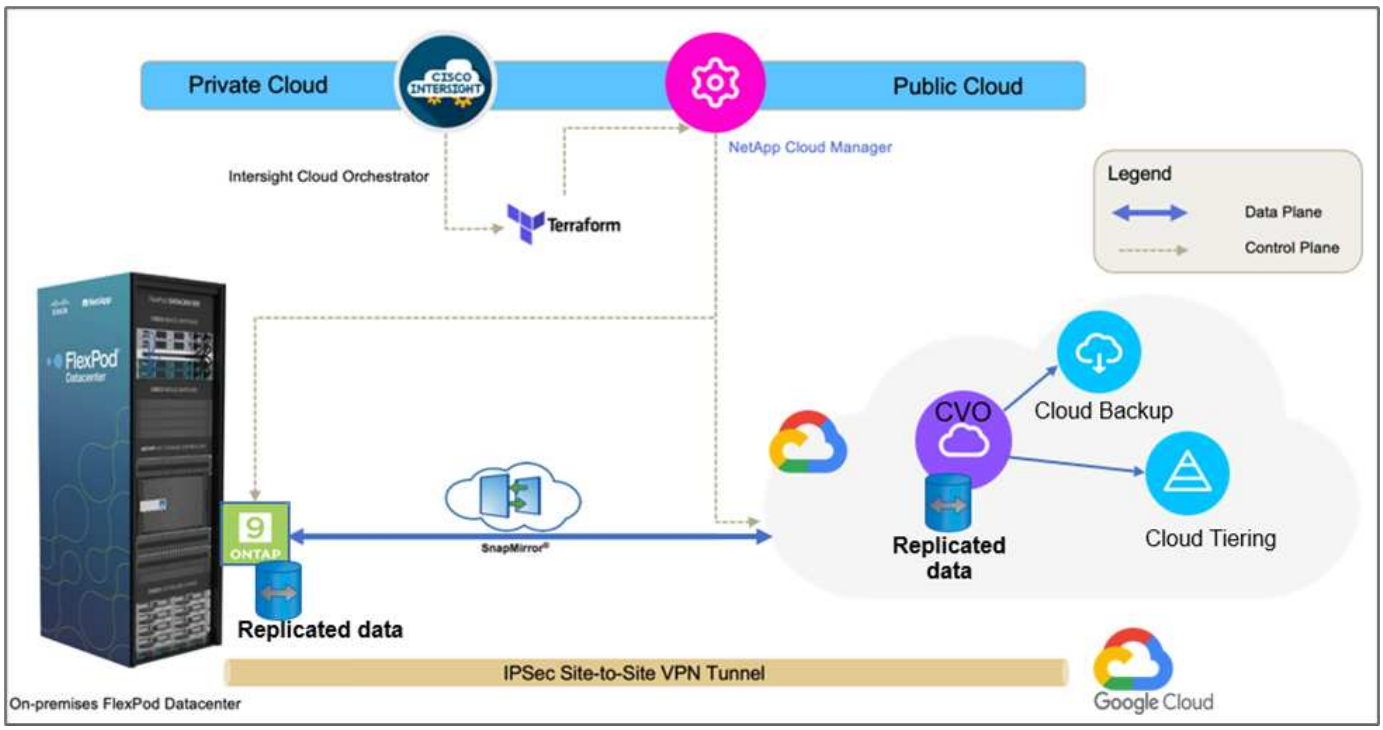
- オーケストレーションと自動化。 Cisco Intersightは、自動化を通じて提供される一貫したオーケストレーションフレームワークを提供することで、FlexPod ハイブリッドクラウドインフラの日常的な運用を簡易化します。
- カスタマイズされた保護。 Cloud Volumes ONTAP は、ONTAP からクラウドへのブロックレベルのデータレプリケーションを提供し、差分更新によってデスティネーションを最新の状態に維持します。ユーザは、たとえば、転送されるソースでの変更に基づいて、5分ごとまたは1時間ごとに同期スケジュールを指定できます。
- *シームレスなフェイルオーバーとフェイルバック。*災害が発生した場合、ストレージ管理者はCloud Volume に迅速にフェイルオーバーできます。プライマリサイトがリカバリされると、DR環境で作成された新しいデータがソースボリュームと同期され、セカンダリデータレプリケーションが再確立されます。
- *効率性：*データ圧縮、シンプロビジョニング、重複排除により、セカンダリクラウドコピー用のストレージスペースとコストを最適化します。データは圧縮と重複排除が行われた形式でブロックレベルで転送されるため、転送速度が向上します。また、データは低コストのオブジェクトストレージに自動的に階層化され、DRシナリオなどでアクセスされたときにのみハイパフォーマンスストレージに戻されます。これにより、継続的なストレージコストを大幅に削減できます。
- * ITの生産性向上。* Intersightをインフラストラクチャおよびアプリケーションのライフサイクル管理向けの単一のセキュアなエンタープライズクラスのプラットフォームとして使用することで、解決策 の構成管理と手動タスクの自動化が容易になります。

対象者

本ドキュメントが対象とする主な読者は、セールスエンジニア、フィールドコンサルタント、プロフェッショナルサービス、ITマネージャ、 パートナー様のエンジニア、サイト信頼性エンジニア、クラウドアーキテクト、クラウドエンジニア、お客様が、ITの効率化とITイノベーションの実現のために構築されたインフラを活用したいと考えています。

解決策 トポロジ

このセクションでは、解決策 の論理トポロジについて説明します。次の図は、オンプレミスのFlexPod 環境、Google Cloudで実行されているNetApp Cloud Volumes ONTAP 、Cisco Intersight、NetApp Cloud Managerの解決策 トポロジを示しています。



コントロールプレーンとデータプレーンは、エンドポイント間で明確に示されます。データプレーンは、セキュアなサイト間VPN接続を使用して、FlexPod All Flash FAS で実行されているONTAP インスタンスをGoogle Cloud上のNetApp Cloud Volumes ONTAP インスタンスに接続します。

FlexPod からNetApp Cloud Volumes ONTAP へのワークロードデータのレプリケーションはNetApp SnapMirrorによって処理され、オンプレミス環境とクラウド環境の両方でCisco Intersight Cloud Orchestratorを使用して全体的なプロセスが調整されます。Cisco Intersight Cloud OrchestratorはNetApp Cloud Managerのリソースプロバイダとして、NetApp Cloud Volumes ONTAP の導入に関連する処理を実行し、データレプリケーション関係を確立します。

この解決策 では、NetApp Cloud Volumes ONTAP インスタンスにあるコールドデータのバックアップと階層化もオプションでサポートされています。

"次の例は、解決策 コンポーネントです。"

解決策コンポーネント

"Previous ：解決策の概要を示します。"

FlexPod

FlexPod は、仮想化ソリューションと非仮想化ソリューションの両方の統合基盤となるハードウェアとソフトウェアの定義済みセットです。FlexPod には、NetApp ONTAP ストレージ、Cisco Nexusネットワーク、Cisco MDSストレージネットワーク、Cisco Unified Computing System（Cisco UCS）が含まれています。この設計は、ネットワーク、コンピューティング、ストレージを1つのデータセンターラックに収容でき

る柔軟性を備えています。また、お客様のデータセンター設計に従って導入することもできます。ポート密度を使用すると、ネットワークコンポーネントは複数の構成に対応できます。

Cisco Intersightの

Cisco Intersightは、従来のアプリケーションやクラウドネイティブなインフラに向けて、インテリジェントな自動化、オブザーバビリティ、最適化を実現するSaaSプラットフォームです。このプラットフォームは、ITチームの変化を促進し、ハイブリッドクラウド向けに設計された運用モデルを提供します。Cisco Intersightには、次のようなメリットがあります。

- *迅速な提供。*俊敏性に優れたソフトウェア開発モデルにより、クラウドまたはお客様のデータセンターからサービスとして提供され、頻繁な更新と継続的な技術革新を実現します。このようにして、お客様は基幹業務へのサービス提供の高速化に注力できます。
- *運用の簡素化。*共通のインベントリ、認証、APIを備えた単一のセキュアなSaaS提供ツールを使用して、スタック全体とすべての場所で作業できるようにし、チーム間のサイロを排除し、運用を簡素化します。オンプレミスの物理サーバやハイパーバイザーの管理からVM、Kubernetes、サーバレス、自動化、オンプレミスとパブリッククラウドの両方にわたって最適化とコスト管理を実現
- 継続的な最適化。 Cisco Intersightが提供するインテリジェンスを、Cisco TACだけでなくすべてのレイヤで使用して、環境を継続的に最適化します。このインテリジェンスは、推奨される自動化可能なアクションに変換されるため、ワークロードの移動や物理サーバの状態の監視から、コスト削減へと、お客様が使用するパブリッククラウドの推奨まで、あらゆる変化にリアルタイムで適応できます。

Cisco Intersightには、UCSM Managed Mode（UMM）とIntersight Managed Mode（IMM）という2つの管理操作モードがあります。ファブリックインターコネクトの初期セットアップ中に、ファブリック接続Cisco UCSシステムにネイティブUmmまたはIMMを選択できます。この解決策 では、ネイティブIMMが使用されます。

Cisco Intersightのライセンス

Cisco Intersightは、複数の階層を含むサブスクリプションベースのライセンスを使用しています。

Cisco Intersightのライセンスレベルは次のとおりです。

- * Cisco Intersight Essential.*には、すべての基本機能に加えて次の機能が含まれています。
  - Cisco UCS Centralの特長です
  - Cisco IMC Supervisorの使用権
  - サーバプロファイルを使用したポリシーベースの設定
  - ファームウェア管理
  - ハードウェア互換性リスト（HCL）との互換性の評価
- * Cisco Intersight Advantage *には、Essentials階層の機能に加え、次の機能が含まれます。
  - 物理コンピューティング、ネットワーク、ストレージ、VMware仮想化、AWSパブリッククラウド全体で、ウィジェット、インベントリ、容量、利用率、ドメイン間のインベントリ相関関係を確認できます。
  - お客様が重要なセキュリティアラートを受信し、影響を受けるエンドポイントデバイスに関するフィールド通知を受け取ることができるシスコセキュリティアドバイザリサービス。
- * Cisco Intersight Premierは、Advantageレベルで提供される機能に加えて、次の機能を提供します。
  - Ciscoとサードパーティのコンピューティング、ネットワーク、ストレージ、統合システム、仮想化向

けのIntersight Cloud Orchestrator（ICO） コンテナ、パブリッククラウドの各プラットフォームで実現できます

- Cisco UCS Directorのフルサブスクリプションを追加料金なしでご利用いただけます。

Intersightのライセンスと各ライセンスでサポートされる機能の詳細については、こちらをご覧ください "こちらをご覧ください"。

> この解決策 では、インテル®Intersightクラウド・オーケストレーション・サービスとインテル®Intersightサービスを使用して、これらの機能は、Intersight Premierライセンスを持つユーザが利用できるため、このライセンス層を有効にする必要があります。

クラウドと**ICO**の統合

Cisco Intersight Cloud Orchestrator（ICO）を使用すると、Terraform Cloud（TFC）APIと呼ばれるワークフローを作成、実行できます。Web API要求の呼び出しタスクは、Terraform Cloudをターゲットとしてサポートし、HTTPメソッドを使用してTerraform Cloud APIで構成できます。そのため、このワークフローでは、汎用のAPIタスクやその他の操作を使用して、複数のTerraform Cloud APIを呼び出すタスクを組み合わせることができます。ICO機能を使用するには、プレミアライセンスが必要です。

Cisco Intersight Assistの導入

Cisco Intersight Assistを使用すると、エンドポイントデバイスをCisco Intersightに追加できます。データセンターには、Cisco Intersightに直接接続できない複数のデバイスが存在する場合があります。Cisco Intersightでサポートされているが、直接接続されていないデバイスには、接続メカニズムが必要です。Cisco Intersight Assistは、この接続メカニズムを提供し、Cisco Intersightへのデバイスの追加を支援します。

Cisco Intersight Assistは、Cisco Intersight Virtual Appliance内で利用できます。これは、Open Virtual Appliance（OVA；オープン仮想アプライアンス）ファイル形式に含まれる展開可能な仮想マシンとして配布されます。アプライアンスはESXiサーバにインストールできます。詳細については、を参照してください "『Cisco Intersight Virtual Appliance Getting Started Guide』"。

Intersight AssistをIntersightに請求した後、[Claim Through Intersight Assist]オプションを使用してエンドポイントデバイスを請求できます。詳細については、を参照してください "はじめに"。

NetApp Cloud Volumes ONTAP の略

- 組み込みのデータ重複排除、データ圧縮、シンプロビジョニング、クローニングを活用して、ストレージコストを最小限に抑えます。
- クラウド環境で障害が発生した場合でも、エンタープライズクラスの信頼性と継続的な運用を実現します。
- Cloud Volumes ONTAP では、業界をリードするレプリケーションテクノロジであるNetApp SnapMirrorを使用して、オンプレミスのデータをクラウドにレプリケートすることで、複数のユースケースでセカンダリコピーを簡単に利用できます。
- また、Cloud Volumes ONTAP はCloud Backup Service との統合により、クラウドデータの保護と長期保管のためのバックアップおよびリストア機能も提供します。
- アプリケーションをオフラインにすることなく、ハイパフォーマンスとローパフォーマンスのストレージプールをオンデマンドで切り替えます。
- NetApp SnapCenter を使用してSnapshotコピーの整合性を確保する。
- Cloud Volumes ONTAP は、データ暗号化をサポートし、ウィルスやランサムウェアからの保護を提供し

ます。

- クラウドデータセンスとの統合により、データコンテキストを把握し、機密データを識別できます。

Cloud Central にアクセスできます

Cloud Centralは、ネットアップのクラウドデータサービスにアクセスして管理するための一元的な場所を提供します。これらのサービスを利用すると、重要なアプリケーションをクラウドで実行したり、自動化されたDR サイトを作成したり、 SaaS データをバックアップしたり、複数のクラウド間でデータを効果的に移行および制御したりすることができます。詳細については、を参照してください "Cloud Central にアクセスできます"。

クラウドマネージャ

Cloud Managerは、エンタープライズクラスのSaaSベースの管理プラットフォームです。ITエキスパートやクラウドアーキテクトは、ネットアップのクラウドソリューションを使用してハイブリッドマルチクラウドインフラを一元管理できます。オンプレミスとクラウドのストレージを表示および管理する一元化されたシステムを提供し、複数のハイブリッドクラウドプロバイダとアカウントをサポートします。詳細については、を参照してください "クラウドマネージャ"。

コネクタ

Connectorを使用すると、Cloud Managerでパブリッククラウド環境内のリソースやプロセスを管理できます。コネクタインスタンスは、Cloud Managerが提供するさまざまな機能を使用するために必要です。クラウドまたはオンプレミスのネットワークに導入できます。Connectorは次の場所でサポートされます。

- AWS
- Microsoft Azure
- Google Cloud
- オンプレミス

NetApp Active IQ Unified Manager の略

NetApp Active IQ Unified Manager では、設計を一新したわかりやすいインターフェイスからONTAP ストレージクラスタを監視でき、集合知やAI分析から得た情報を活用できます。運用、パフォーマンス、プロアクティブな分析情報を提供し、ストレージ環境と仮想マシン上で実行される環境を包括的に分析します。ストレージインフラで問題 が発生すると、Unified Managerから問題 の詳細情報を通知してルート原因 を特定できるようになります。仮想マシンダッシュボードではVMのパフォーマンス統計を確認でき、これにより、ネットワーク経由でダウンしているvSphereホストからストレージへのI/Oパス全体を調査できます。

一部のイベントには、問題 を修正するための対応策も用意されています。問題が発生したときにEメールやSNMPトラップで通知されるように、イベントにカスタムアラートを設定できます。Active IQ Unified Manager を使用すると、容量や使用状況の傾向を予測して問題が発生する前にプロアクティブに対処することができるため、長期的な問題につながる短期的な事後対処策を実施する必要がなくなり、ユーザのストレージ要件に合わせて計画を立てることができます。

VMware vSphere の場合

VMware vSphereは、大量のインフラ（CPU、ストレージ、ネットワークなどのリソース）をシームレスで汎用性に優れた動的な運用環境として包括的に管理する仮想化プラットフォームです。個々のマシンを管理する従来のオペレーティングシステムとは異なり、VMware vSphereはデータセンター全体のインフラストラクチャを集約して、必要なアプリケーションに迅速かつ動的に割り当てられるリソースを備えた単一の強力なサー

バを作成します。

VMware vSphereの詳細については、を参照してください "リンクをクリックしてください"。

VMware vSphere vCenterの場合

VMware vCenter Serverでは、1つのコンソールからすべてのホストとVMを統合的に管理でき、クラスタ、ホスト、およびVMのパフォーマンス監視を集約できます。VMware vCenter Serverを使用すると、管理者は、コンピューティングクラスタ、ホスト、VM、ストレージ、ゲストOS、 仮想インフラストラクチャのその他の重要なコンポーネントVMware vCenterは、VMware vSphere環境で使用できる豊富な機能を管理します。

ハードウェアとソフトウェアのバージョン

このハイブリッドクラウド解決策 は、サポート対象のバージョンのソフトウェア、ファームウェア、ハードウェアを実行しているFlexPod 環境に拡張できます。このバージョンは、NetApp Interoperability Matrix ToolおよびCisco UCSハードウェア互換性リストで定義されています。

ネットアップのオンプレミス環境でベースラインプラットフォームとして使用されているFlexPod 解決策は、前述のガイドラインと仕様に従って導入されています "こちらをご覧ください"。

この環境内のネットワークはACIベースです。詳細については、を参照してください "こちらをご覧ください"。

- 詳細については、次のリンクを参照してください。
- "NetApp Interoperability Matrix Tool で確認できます"
- "VMware Compatibility Guide 』を参照してください"
- "Cisco UCS ハードウェアおよびソフトウェア相互運用性ツール"

次の表に、FlexPod のハードウェアとソフトウェアのリビジョンを示します。

コンポーネント	プロダクト	バージョン
コンピューティング	Cisco UCS X210-M6	5.0（1b）
	Cisco UCSファブリックインターコネクト6454	4.2（2a）
ネットワーク	Cisco Nexus 9332C（スパイン）	14.2（7秒）
	Cisco Nexus 9336C-FX2（リーフ）	14.2（7秒）
	Cisco ACI	4.2（7秒）
ストレージ	NetApp AFF A220	9.11.1
	NetApp ONTAP Tools for VMware vSphere の略	9.10
	NetApp NFS Plugin for VMware VAAI	2.0-15
	Active IQ Unified Manager	9.11
ソフトウェア	vSphere ESXiの場合	7.0（U3）

コンポーネント	プロダクト	バージョン
	VMware vCenter Applianceの略	バージョン7.0.3
	Cisco Intersight Assist仮想アプライアンス	1.0.11-306

Terraformの構成の実行は、Terraform Cloud for Businessアカウントで行われます。Terraformの構成では、NetApp Cloud ManagerのTerraformプロバイダを使用しています。

次の表に、ベンダー、製品、およびバージョンを示します。

コンポーネント	プロダクト	バージョン
橋本（橋本	テラフォーム	1.2.7

次の表に、Cloud ManagerとCloud Volumes ONTAP のバージョンを示します。

コンポーネント	プロダクト	バージョン
ネットアップ	Cloud Volumes ONTAP	9.11
	クラウドマネージャ	3.9.21

"次の手順：インストールと設定- FlexPod を導入します。"

インストールと設定

FlexPod を導入します

"前の図：解決策 コンポーネント。"

設計のさまざまな要素の構成や関連するベストプラクティスなど、FlexPod の設計および導入の詳細については、を参照してください "FlexPod 向けのシスコ検証済み設計"。

FlexPod は、UCS管理モードとCisco Intersight管理モードの両方に導入できます。FlexPod をUCS管理モードで導入している場合は、最新のCisco Validated Designが見つかります "こちらをご覧ください"。

Cisco Unified Compute System（Cisco UCS）Xシリーズは、まったく新しいモジュラ型コンピューティングシステムであり、クラウドから構成、管理できます。最新のアプリケーションのニーズを満たし、柔軟性に優れた、将来に対応できるモジュラ設計によって運用効率、即応性、拡張性を向上させるように設計されています。Cisco Intersightが管理するUCS XシリーズプラットフォームをFlexPod インフラに組み込むための設計ガイダンスを提供します "こちらをご覧ください"。

FlexPod とCisco ACIの導入方法が用意されています "こちらをご覧ください"。

"次の例は、Cisco Intersightの設定です。"

Cisco Intersightの設定

"前の手順：FlexPod を導入します。"

Cisco IntersightとIntersight Assistを設定する方法については、「Cisco Validated Design

for FlexPod 」を参照してください "こちらをご覧ください"。

"次のステップ：クラウド統合とICOの統合の前提条件"

クラウド統合とICOの統合の前提条件

"前の手順：Cisco Intersightの設定。"

手順 1：Cisco IntersightとTerraform Cloudを接続します

1. Terraform Cloudアカウントの詳細情報を提供して、クラウドターゲットを請求または作成します。
2. プライベートクラウド用のTerraform Cloud Agentターゲットを作成して、お客様がデータセンターにエージェントをインストールし、Terraform Cloudと通信できるようにします。

   詳細については、を参照してください "リンクをクリックしてください"。

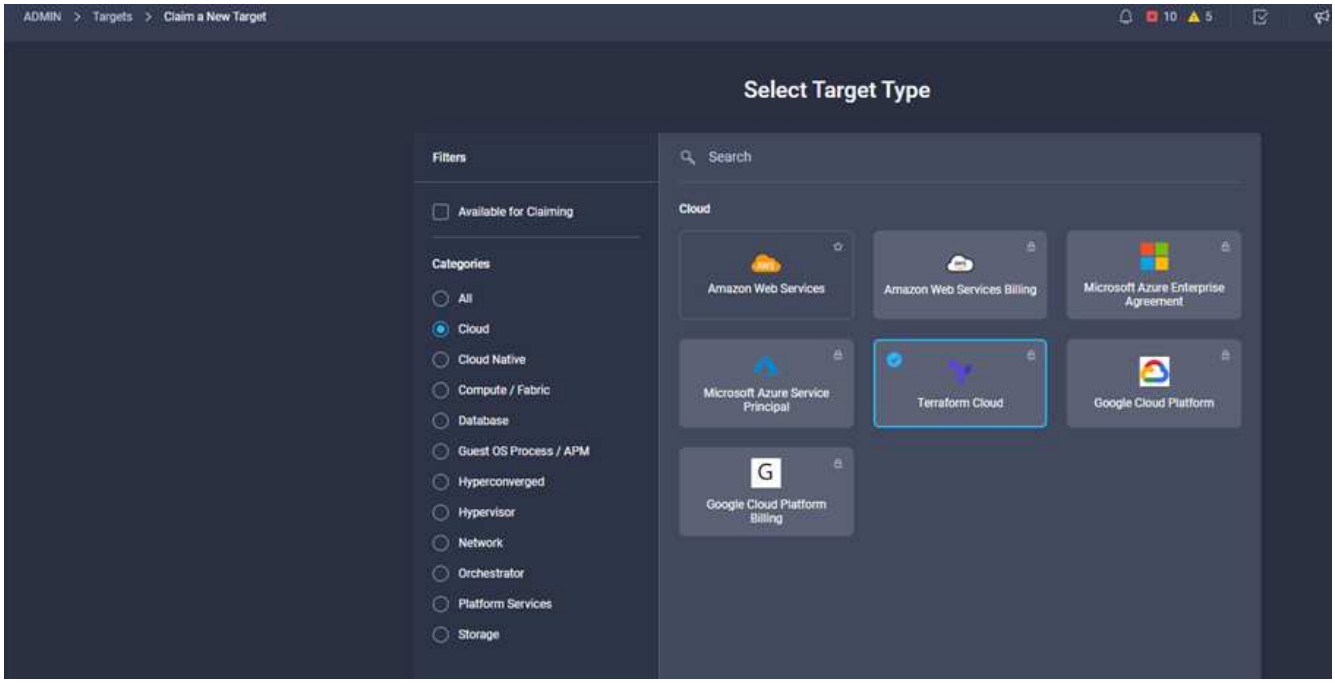
手順 2:ユーザートークンを生成します

Terraform Cloudのターゲットを追加する際には、Terraform Cloud設定ページからユーザー名とAPIトークンを入力する必要があります。

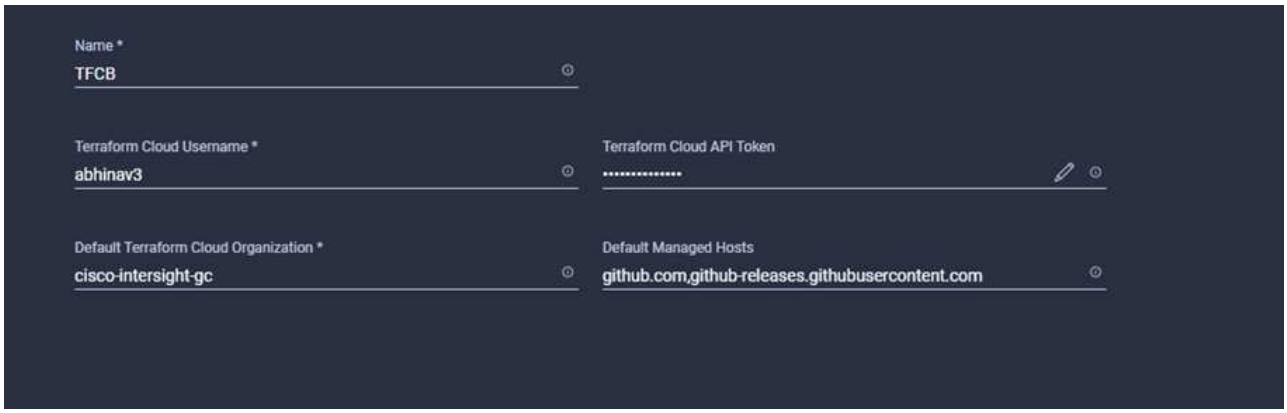
1. Terraform Cloudにログインし、* User Tokens *にアクセスします。 "https://app.terraform.io/app/settings/tokens"。
2. [新しいAPIトークンの作成]をクリックします。
3. トークンを覚えて安全な場所に保存するための名前を割り当てます。

手順 3：クラウドターゲットを要求

1. アカウント管理者、デバイス管理者、またはデバイス技術者の権限でIntersightにログインします。
2. [管理者]、[ターゲット]、[新しいターゲットの請求]の順に移動します。*
3. 「カテゴリ」で、「クラウド」をクリックします。
4. [**Terraform Cloud**]をクリックし、[**Start**]をクリックします。



5. 次の図に示すように、ターゲットの名前、Terraform Cloudのユーザー名、APIトークン、およびTerraform Cloudのデフォルトの組織を入力します。
6. [*Default Managed Hosts]フィールドに、他の管理対象ホストと一緒に次のリンクを追加してください。
   - github.com
   - github-releases.githubusercontent.com



すべてが正しく入力されていれば、[* Intersight Targets]セクションにTerraform Cloudターゲットが表示されます。

手順 **4**：クラウドエージェントを追加します

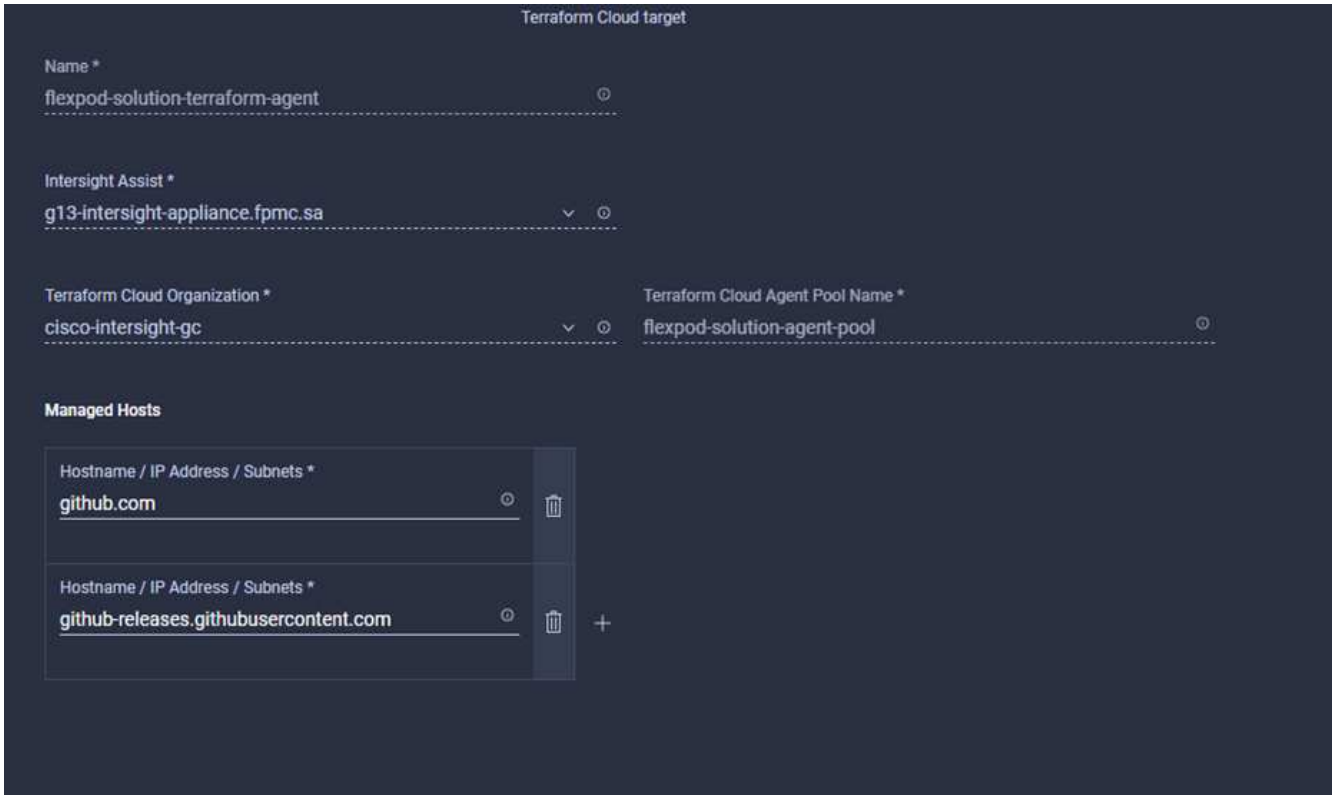
前提条件

- クラウドのターゲットをクラウド化
- Terraform Cloud Agentを展開する前に、Intersight AssistをIntersightに主張。

各アシストに対して請求できるエージェントは5人だけです。

Terraformへの接続を作成したら、Terraform Agentをスピンアップしてterraformコードを実行する必要があります。

1. Terraform Cloudターゲットのドロップダウンリストから*Claim Terraform Cloud Agent *をクリックします。
2. Terraformクラウドエージェントの詳細を入力します。次のスクリーンショットは、Terraformエージェントの構成の詳細を示しています。



任意のTerraform Agentプロパティを更新できます。ターゲットが「接続されていない」状態で、「接続されていない」状態になっていない場合、Terraformエージェントに対してトークンが生成されていません。

エージェントの検証が成功し、エージェントトークンが生成された後、組織やエージェントプールを再構成することはできません。Terraformエージェントが正常に配備された場合、ステータスは* Connected *と表示されます。

Terraform Cloud統合を有効にして主張したら、Cisco Intersight Assistで1つ以上のTerraform Cloudエージェントを導入できます。Terraform Cloudエージェントは、クラウドターゲットの子ターゲットとしてモデル化されています。エージェント目標を要求すると、ターゲット請求が進行中であることを示すメッセージが表示されます。

数秒後、ターゲットは「接続済み」状態に移行し、Intersightプラットフォームはエージェントからterraform CloudゲートウェイにHTTPSパケットをルーティングします。

Terraform Agentは正しく請求され、ターゲットの下に「* Connected *」と表示されます。

"次の手順：パブリッククラウドサービスプロバイダを設定します。"

パブリッククラウドサービスプロバイダを設定

"前：Terraform Cloud Integration with ICOの前提条件"

手順 **1**：**NetApp Cloud Manager**にアクセスします

NetApp Cloud Managerおよびその他の クラウド サービス にアクセスするには、にサインアップする必要があります "NetApp Cloud Central"。

Cloud Centralアカウントでワークスペースとユーザを設定する場合は、をクリックします "こちらをご覧ください"。

手順 **2**：コネクタを配置します

Google CloudにConnectorを導入するには、こちらを参照してください "リンク"。

"次のステップ：ハイブリッドクラウドネットアップストレージの自動導入"

ハイブリッドクラウドネットアップストレージの導入を自動化

"前のページ：パブリッククラウドサービスプロバイダを設定"

Google Cloud

最初にAPIを有効にし、コネクタまたは異なるプロジェクトにあるCloud Volumes ONTAP システムを導入および管理する権限をCloud Managerに付与するサービスアカウントを作成する必要があります。

Google CloudプロジェクトにConnectorを導入する前に、Connectorがオンプレミスまたは別のクラウドプロバイダで実行されていないことを確認してください。

Cloud Manager からコネクタを直接導入するには、次の 2 組の権限が必要です。

- Cloud ManagerからConnector VMインスタンスを起動する権限があるGoogleアカウントを使用してConnectorを導入する必要があります。
- Connectorを導入する場合は、VMインスタンスを選択するよう求められます。Cloud Manager は、サービスアカウントから権限を取得して、 Cloud Volumes ONTAP システムを代わりに作成および管理します。権限は、サービスアカウントにカスタムロールを割り当てることによって提供されます。ユーザーとサービスアカウントに必要な権限を含むYAMLファイルを2つ設定する必要があります。の使用方法について説明します "権限を設定するYAMLファイル" こちらをご覧ください。

を参照してください "この詳細なビデオをご覧ください" を参照してください。

Cloud Volumes ONTAP の導入モードとアーキテクチャ

Cloud Volumes ONTAP は、シングルノードシステムとして、またハイアベイラビリティ（HA）ペアのノードとしてGoogle Cloudで利用できます。要件に基づいて、Cloud Volumes ONTAP 導入モードを選択できます。シングルノードシステムの HA ペアへのアップグレードはサポートされていません。シングルノードシステムとHAペアを切り替える場合は、新しいシステムを導入し、既存のシステムから新しいシステムにデータをレプリケートする必要があります。

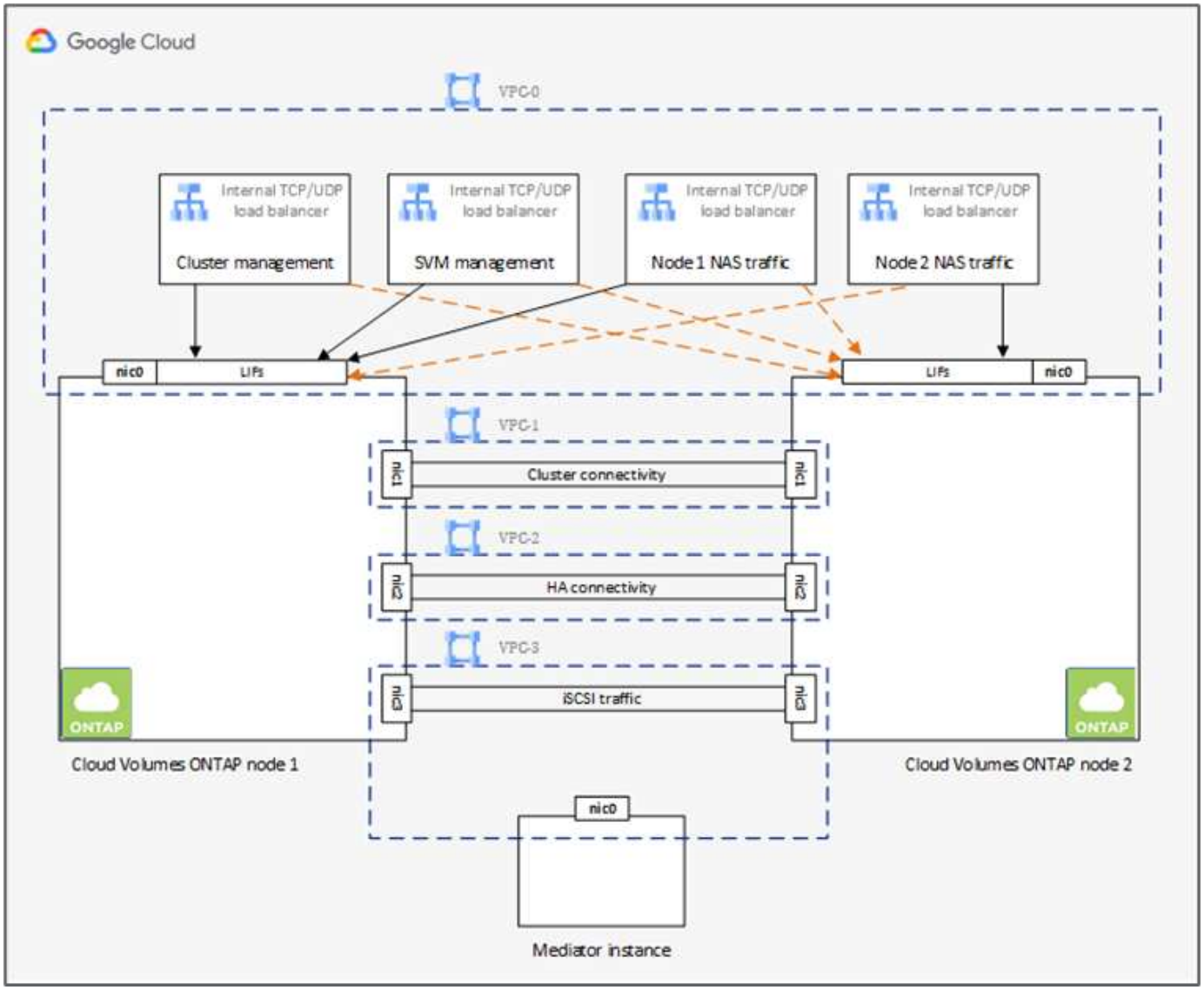
Google Cloudの高可用性Cloud Volumes ONTAP

Google Cloudでは、複数の地域や1つの地域内の複数のゾーンにまたがるリソースの導入をサポートしています。HA導入は、Google Cloudで利用できる強力なn1-standardまたはn2標準のマシンタイプを使用する2つのONTAP ノードで構成されます。2つのCloud Volumes ONTAP ノード間でデータが同期的にレプリケートされ、障害発生時の可用性が確保されます。Cloud Volumes ONTAP のHA導入では、VPCごとに4つのVPCとプライベートサブネットが必要です。4つのVPC内のサブネットは、重複しないCIDR範囲でプロビジョニングする必要があります。

4つのVPCは次の目的に使用されます。

- vPC 0は、データノードおよびCloud Volumes ONTAP ノードへのインバウンド通信を可能にします。
- vPC 1は、Cloud Volumes ONTAP ノード間のクラスタ接続を提供します。
- vPC 2を使用すると、ノード間でNVRAM（不揮発性RAM）レプリケーションを実行できます。
- vPC 3は、HAメディエーターインスタンスへの接続、およびノードの再構築のためのディスクレプリケーショントラフィックに使用されます。

次の図は、Goggle Cloudで高可用性Cloud Volumes ONTAP を示しています。



詳細については、を参照してください "リンクをクリックしてください"。

Google CloudでのCloud Volumes ONTAP のネットワーク要件については、を参照してください "リンクをクリックしてください"。

データ階層化の詳細については、を参照してください "リンクをクリックしてください"。

環境の前提条件を設定する

Cloud Volumes ONTAP クラスタの自動作成、オンプレミスボリュームとクラウドボリューム間のSnapMirror設定、クラウドボリュームの作成などが、Terraform設定を使用して実行されます。これらのTerraform構成は、Terraform Cloud for Businessアカウントでホストされています。Intersight Cloud Orchestratorを使用すると、Terraform Cloud for Businessアカウントでのワークスペースの作成、ワークスペースへの必要な変数の追加、Terraformプランの実行などのタスクをオーケストレーションできます。

これらの自動化タスクとオーケストレーションタスクには、以降のセクションで説明するように、いくつかの要件とデータが必要になります。

GitHub リポジトリ

TerraformコードをホストするにはGitHubアカウントが必要です。Intersight Orchestratorは、Terraform Cloud for Businessアカウントに新しいワークスペースを作成します。このワークスペースには、バージョン管理ワークフローが設定されています。そのためには、Terraformの構成をGitHubリポジトリに保持し、ワークスペースの作成時に入力として提供する必要があります。

"このGitHubリンク" は、さまざまなリソースを使用したTerraformの構成を提供します。このリポジトリを作成し、GitHubアカウントにコピーを作成できます。

このリポジトリでは'providator.tf'は'必要なTerraformプロバイダの定義を持っていますNetApp Cloud ManagerのTerraformプロバイダが使用されています。

「variable.tf」には、すべての変数宣言が含まれています。これらの変数の値は、Intersight Cloud Orchestratorのワークフロー入力として入力されます。これにより、値をワークスペースに渡し、Terraform設定を実行するのに便利な方法が提供されます。

「resources.tf」では、作業環境へのオンプレミスONTAP の追加、Google CloudでのシングルノードCloud Volumes ONTAP クラスタの作成、オンプレミスとCloud Volumes ONTAP 間のSnapMirror関係の確立、Cloud Volumes ONTAP でのクラウドボリュームの作成などに必要なさまざまなリソースを定義します。

このリポジトリの内容は次のとおりです

- 「providator.tf」には、必要なTerraformプロバイダの定義としてNetApp Cloud Managerが含まれています。
- 「variables .tf」には、Intersight Cloud Orchestratorワークフローの入力として使用される変数宣言が含まれています。これにより、値をワークスペースに渡し、Terraform設定を実行する便利な方法が提供されます。
- 「resources.tf」では、オンプレミスONTAP を作業環境に追加するためのさまざまなリソースを定義し、Google Cloud上でシングルノードCloud Volumes ONTAP クラスタを作成し、オンプレミスとCloud Volumes ONTAP 間のSnapMirror関係を確立し、Cloud Volumes ONTAP 上にクラウドボリュームを作成します。

Cloud Volumes ONTAP 上に複数のボリュームを作成する場合は'リソース・ブロックを追加するか'Terraform

構造体ごとにcountまたは'for _を使用できます

Terraformのワークスペース、モジュール、およびポリシーセットを、Terraformの構成を含むgitリポジトリに接続するには、Terraform CloudがGitHubレポジトリにアクセスする必要があります。

クライアントを追加すると、そのクライアントのOAuthトークンIDがIntersight Cloud Orchestratorのワークフロー入力の1つとして使用されます。

1. Terraform Cloud for Businessアカウントにログインします。[設定]>[プロバイダ]に移動します。
2. [VCSプロバイダの追加*]をクリックします。
3. バージョンを選択します。
4. 「プロバイダの設定」の手順に従います。
5. 追加したクライアントが* VCS Providers *に表示されます。OAuthトークンIDをメモします。

NetApp Cloud Manager API処理のトークンを更新します

Cloud Manager には、 Web ブラウザインターフェイスに加えて、 SaaS インターフェイスを介して Cloud Manager 機能に直接アクセスできるようにする REST API が用意されています。Cloud Manager サービスは、拡張可能な開発プラットフォームをまとめた複数のコンポーネントで構成されます。リフレッシュトークンを使用すると、API呼び出しごとにAuthorizationヘッダーに追加するアクセストークンを生成できます。

APIを直接呼び出すことなく、cloudmanagerプロバイダは更新トークンを使用し、Terraformリソースを対応するAPI呼び出しに変換します。NetApp Cloud Manager API処理の更新トークンを生成する必要があります "NetApp Cloud Central"。

Cloud Volumes ONTAP クラスタの作成、SnapMirrorの設定などのリソースをCloud Managerで作成するには、Cloud Manager ConnectorのクライアントIDが必要です。

1. Cloud Managerにログインします。 "https://cloudmanager.netapp.com/"。
2. コネクター（ * Connector ）をクリックします。
3. [* コネクターの管理 *] をクリックします。
4. 省略記号をクリックし、コネクタIDをコピーします。

Cisco Intersight Cloud Orchestratorのワークフローの開発

Cisco Intersight Cloud Orchestratorは、次の場合にCisco Intersightで利用できます。

- Intersight Premierのライセンスがインストールされている。
- お客様は、アカウント管理者、ストレージ管理者、仮想化管理者、またはサーバ管理者であり、少なくとも1台のサーバを割り当て済みであることが必要です。

ワークフローデザイナ

ワークフローデザイナを使用すると、新しいワークフロー(タスクおよびデータ型)の作成や、既存のワークフローの編集を行って、Cisco Intersightでターゲットを管理できます。

Workflow Designerを起動するには、[* Orchestration（オーケストレーション）**]>[Workflows ***（ワークフロー）]ダッシュボードには、[マイワークフロー*]、[サンプルワークフロー*]、[すべてのワークフロー*]タブの下に以下の詳細が表示されます。

- 検証ステータス
- 前回の実行ステータス
- 実行数別上位ワークフロー
- 上位のワークフローカテゴリ
- システム定義ワークフローの数
- Top Workflows by Targets（ターゲット別の上位ワークフロー

ダッシュボードを使用すると、タブを作成、編集、クローニング、または削除できます。独自のカスタムビュータブを作成するには、*+*をクリックし、名前を指定し、列、タグ列、ウィジェットに表示する必要があるパラメータを選択します。タブに*ロック*アイコンがない場合は、タブの名前を変更できます。

ダッシュボードの下には、次の情報を表示するワークフローが表形式のリストとして表示されます。

- 表示名
- 説明
- システム定義
- デフォルトバージョン
- 実行
- 前回の実行ステータス
- 検証ステータス
- 前回の更新
- 組織

Actionsカラムでは、次の操作を実行できます。

- *実行。*ワークフローを実行します。
- *履歴。*ワークフローの実行履歴を表示します。
- *バージョンの管理。*ワークフローのバージョンを作成および管理します。
- *削除。*ワークフローを削除します。
- *再試行*失敗したワークフローを再試行します。

ワークフロー

次の手順で構成されるワークフローを作成します。

- *ワークフローの定義。*表示名、概要 、およびその他の重要な属性を指定します。
- *ワークフローの入力とワークフローの出力を定義します。*ワークフローの実行に必要な入力パラメータと、正常に実行されたときに生成される出力を指定します
- *ワークフロータスクを追加します。*ワークフローデザイナで、ワークフローの機能を実行するために必要なワークフロータスクを1つ以上追加します。
- *ワークフローを検証します。*ワークフローを検証して、タスク入出力の接続にエラーがないことを確認します。

オンプレミスの**FlexPod** ストレージ用のワークフローを作成

オンプレミスのFlexPod ストレージのワークフローを設定するには、を参照してください "リンクをクリックしてください"。

"次：DRワークフロー："

DRワークフロー

"前：ハイブリッドクラウドネットアップストレージの自動導入。"

手順は次のとおりです。

1. ワークフローを定義します。
   - ディザスタリカバリワークフローなど、ワークフローにわかりやすい短い名前を作成します。
2. ワークフローの入力を定義します。このワークフローでは、以下の情報を入力します。
   - ボリュームオプション（ボリューム名、マウントパス）
   - ボリューム容量
   - 新しいデータストアに関連付けられているデータセンター
   - データストアがホストされているクラスタ
   - vCenterで作成する新しいデータストアの名前
   - 新しいデータストアのタイプとバージョン
   - Terraform組織の名前
   - Terraformワークスペース
   - Terraformワークスペースの概要
   - Terraform設定を実行するために必要な変数（機密性および非機密）
   - 計画を開始する理由
3. ワークフロータスクを追加します。

   FlexPod の処理に関連するタスクは次のとおりです。

   - FlexPod でボリュームを作成します。
   - 作成したボリュームにストレージエクスポートポリシーを追加します。
   - VMware vCenterで、新しく作成したボリュームをデータストアにマッピングします。

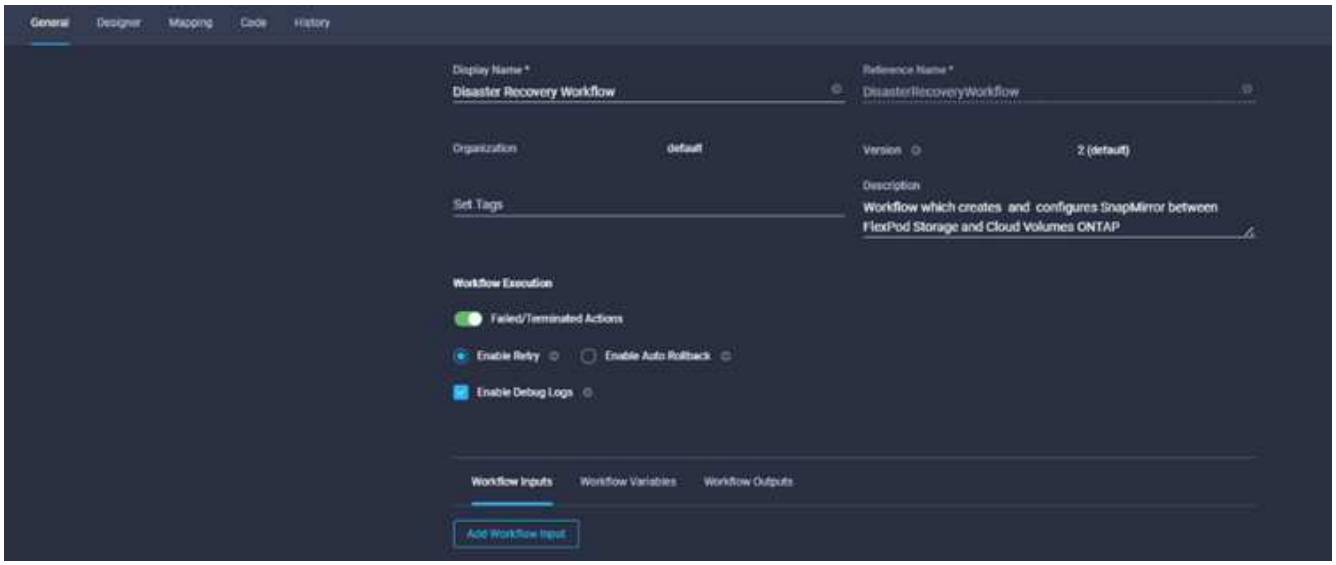
     Cloud Volumes ONTAP クラスタの作成に関連するタスクは次のとおりです。

   - Terraformワークスペースを追加します
   - Terraform変数を追加します
   - Terraformの機密変数を追加します
   - 新しいTerraformプランを開始します
   - Terraformの実行を確認します

4. ワークフローを検証します。

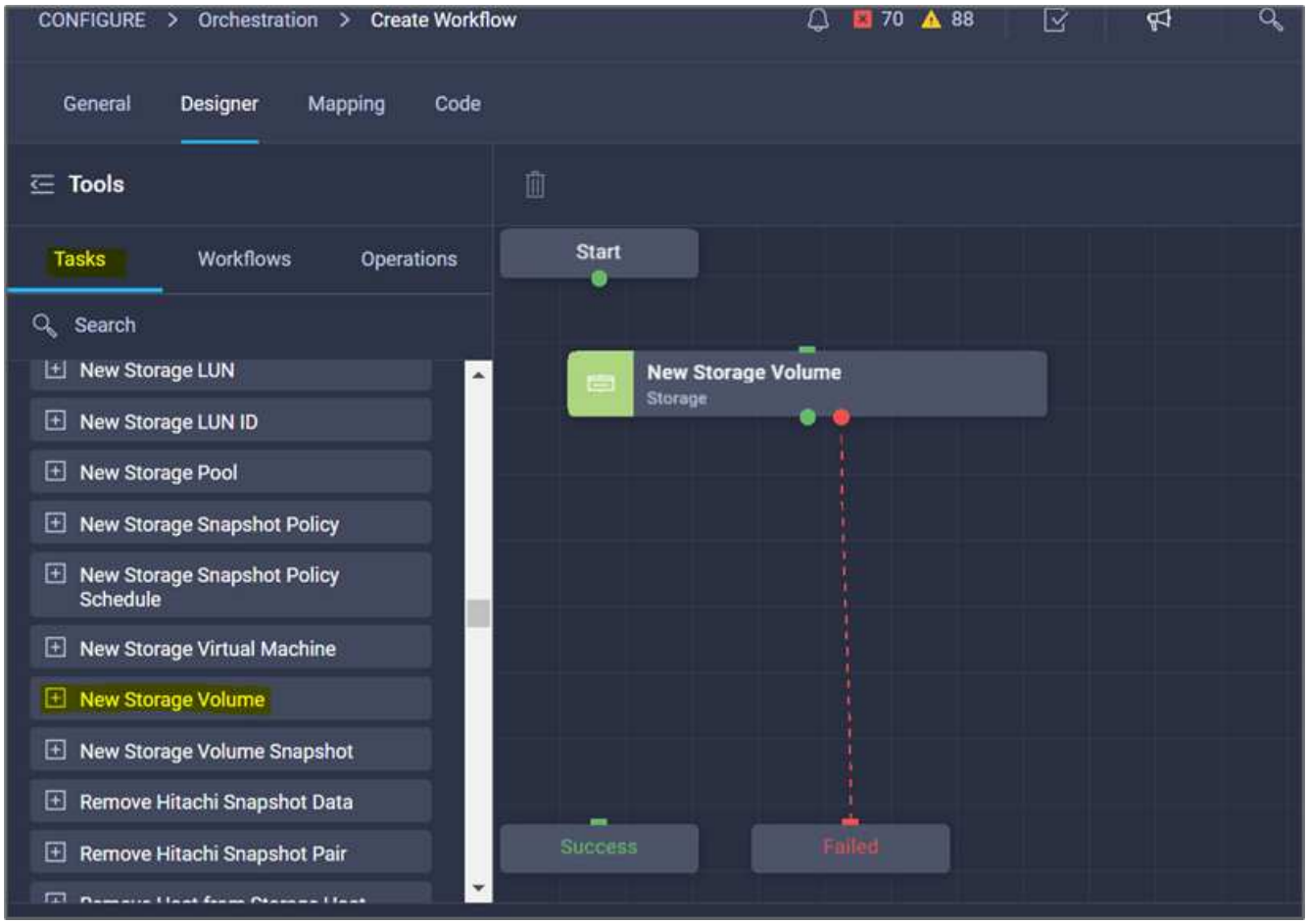
手順 **1**：ワークフローを作成します

1. 左側のナビゲーションペインで[* Orchestration（オーケストレーション）**]**をクリックし、**[** Create Workflow*]をクリックします。
2. [一般*（General *）]タブで、次のように
   a. 表示名を指定します（ディザスタリカバリワークフロー）。
   b. 組織を選択し、タグを設定し、概要 を指定します。
3. [保存] をクリックします .

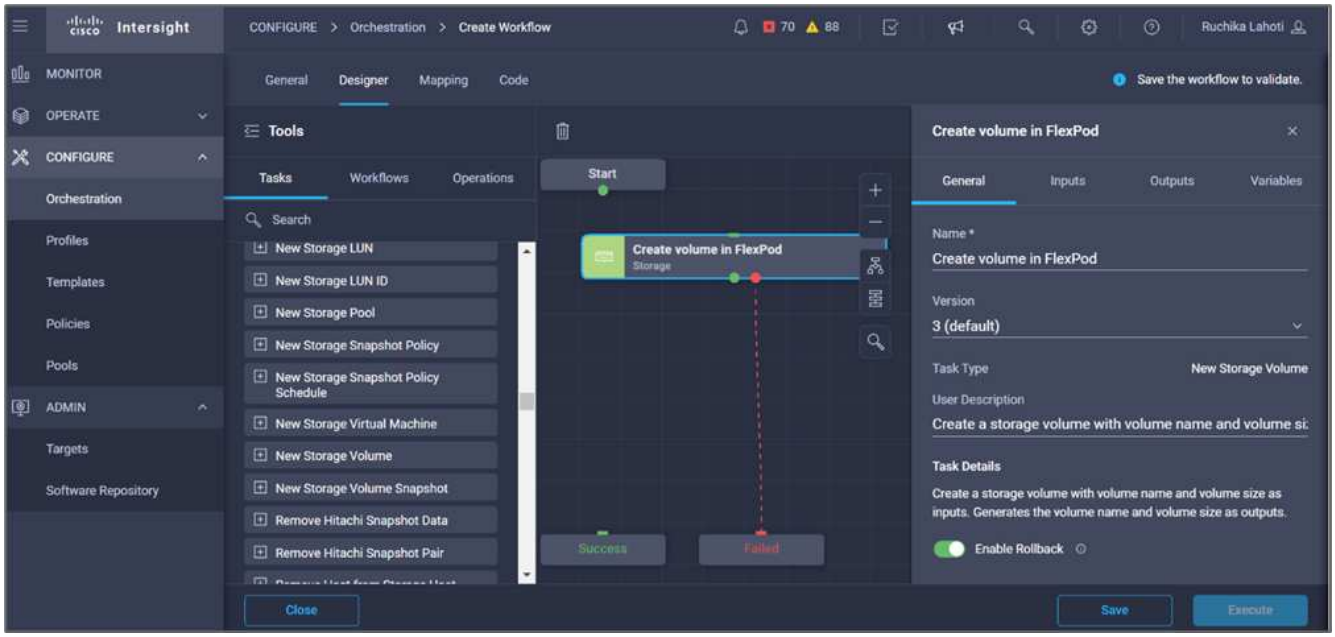


手順 **2.FlexPod** で新しいボリュームを作成します

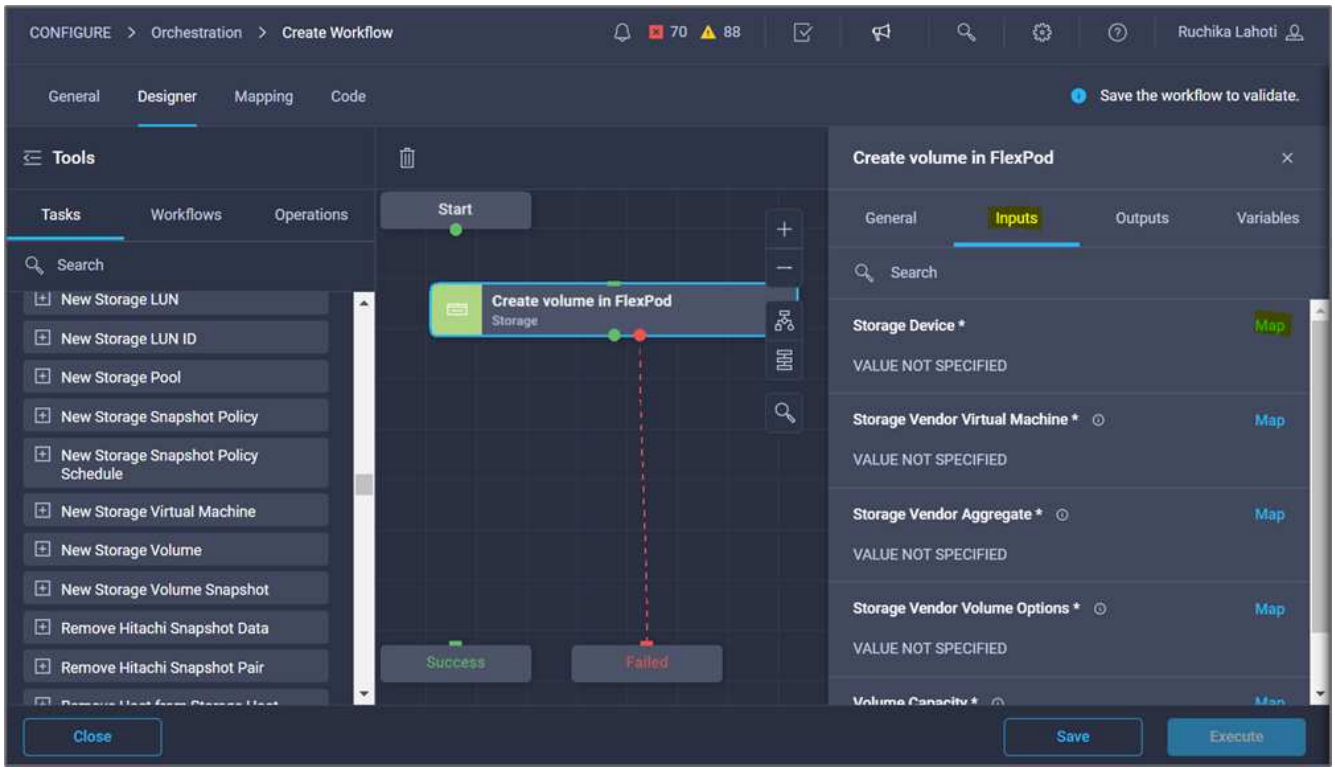
1. [*Designer]タブに移動し、[*Tools]セクションから[*Tasks]をクリックします。
2. [ツール]セクションから[デザイン]領域に*ストレージ>新規ストレージボリューム*タスクをドラッグアンドドロップします。
3. [New Storage Volume]をクリックします。



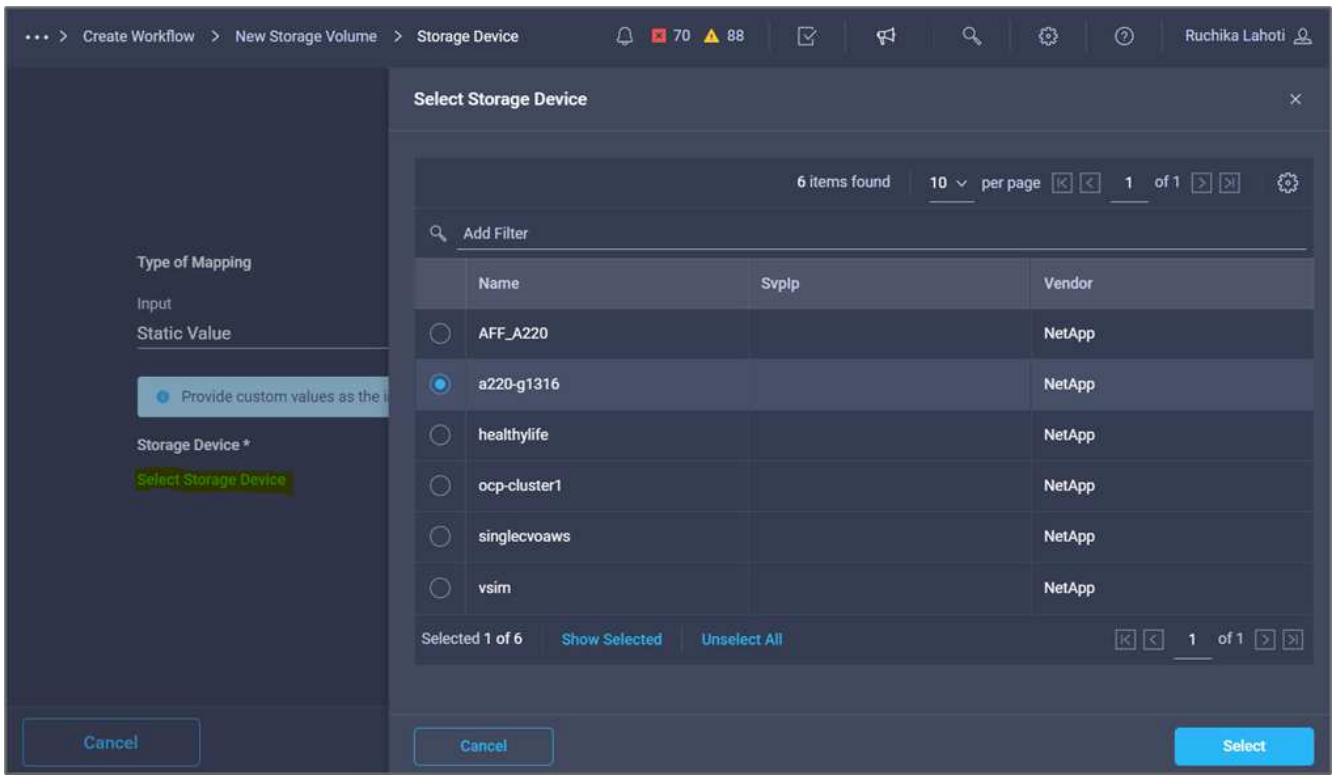
4. [タスクのプロパティ]領域で、[一般]タブをクリックします。必要に応じて、このタスクの名前と概要 を変更できます。この例では、タスクの名前は* FlexPod でのボリュームの作成*です。



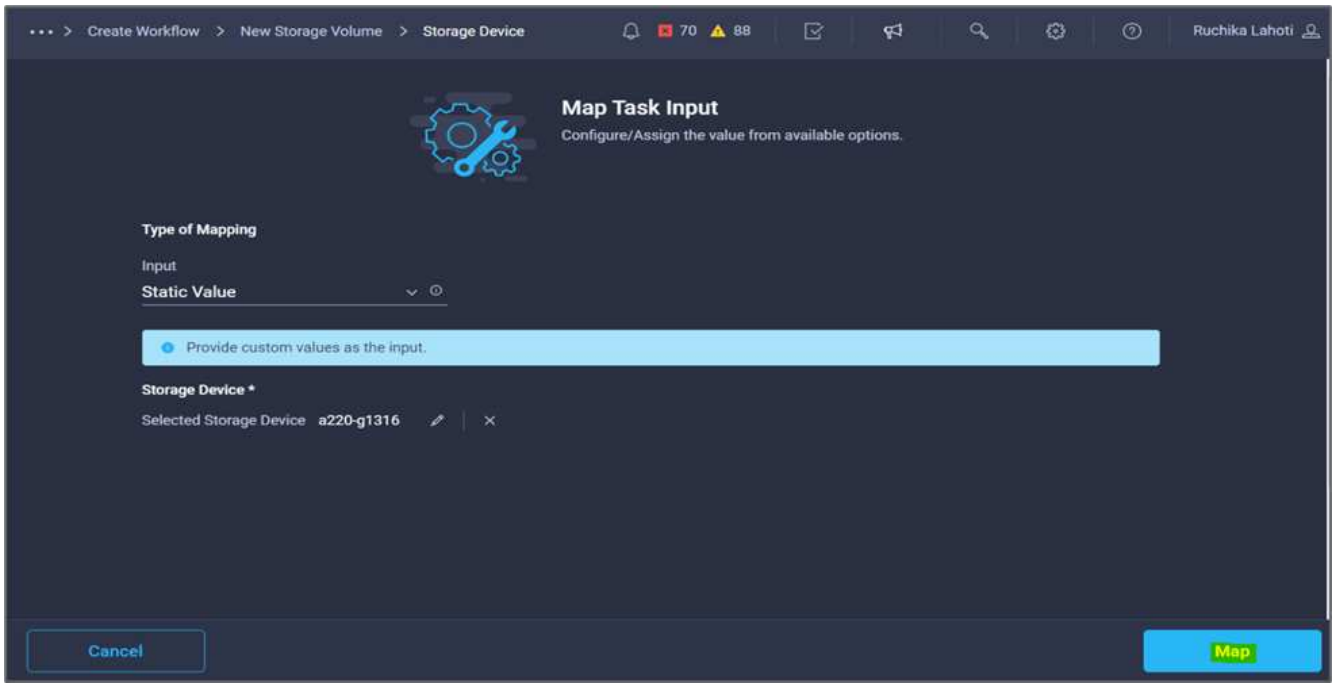
5. [タスクプロパティ（Task Properties ）]領域で、[*入力（Inputs *）]をクリックする
6. [ストレージデバイス]フィールドで[マップ]をクリックします。



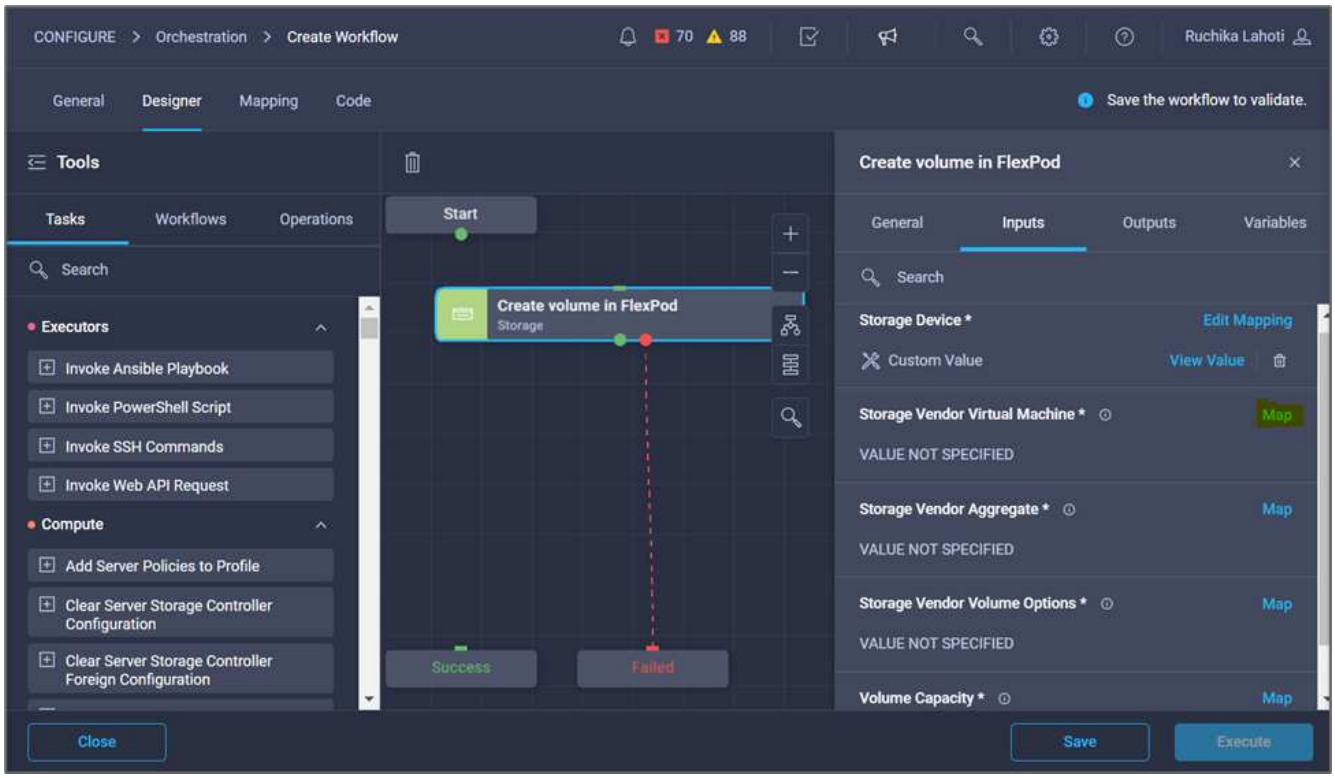
7. 「* Static Value 」を選択し、「 Select Storage Device *」をクリックします。
8. 追加したストレージターゲットをクリックし、* Select *をクリックします。



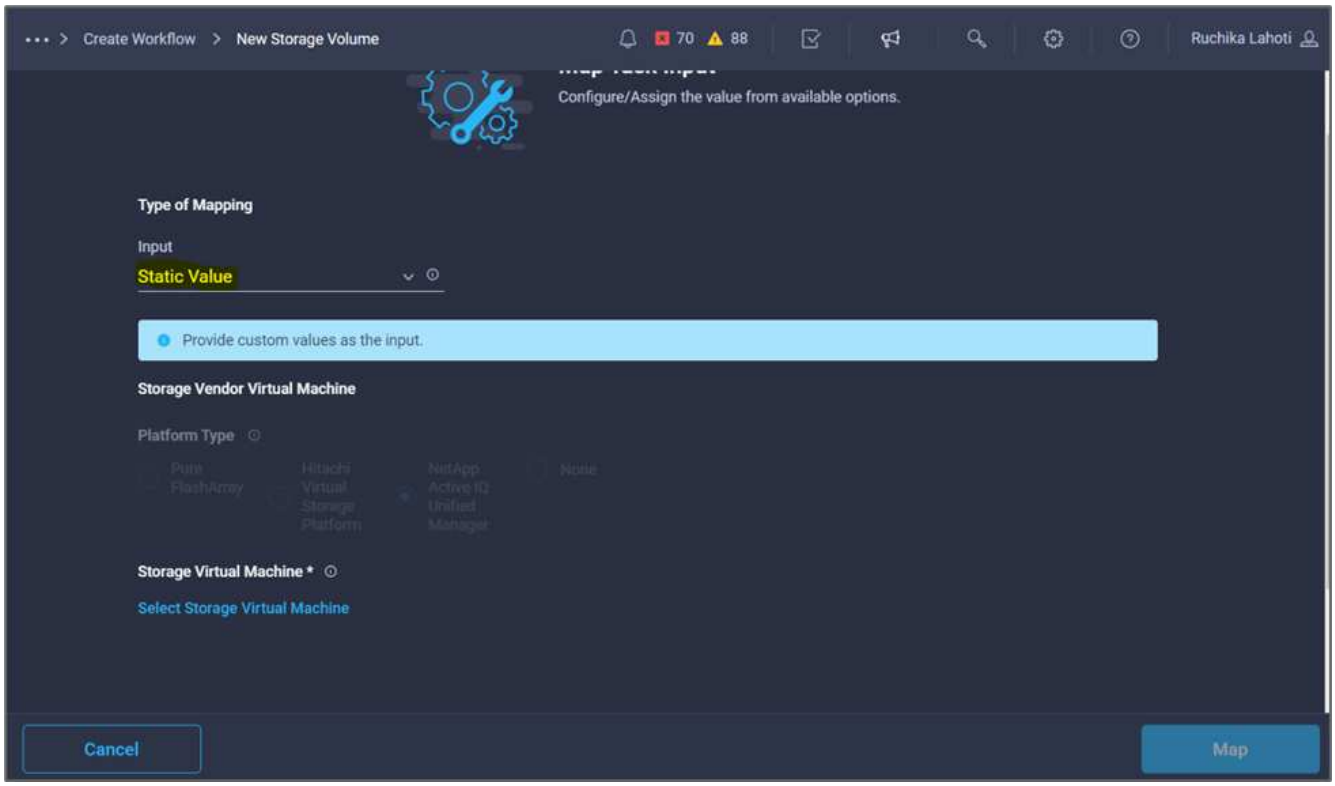
9. [マップ]をクリックします。



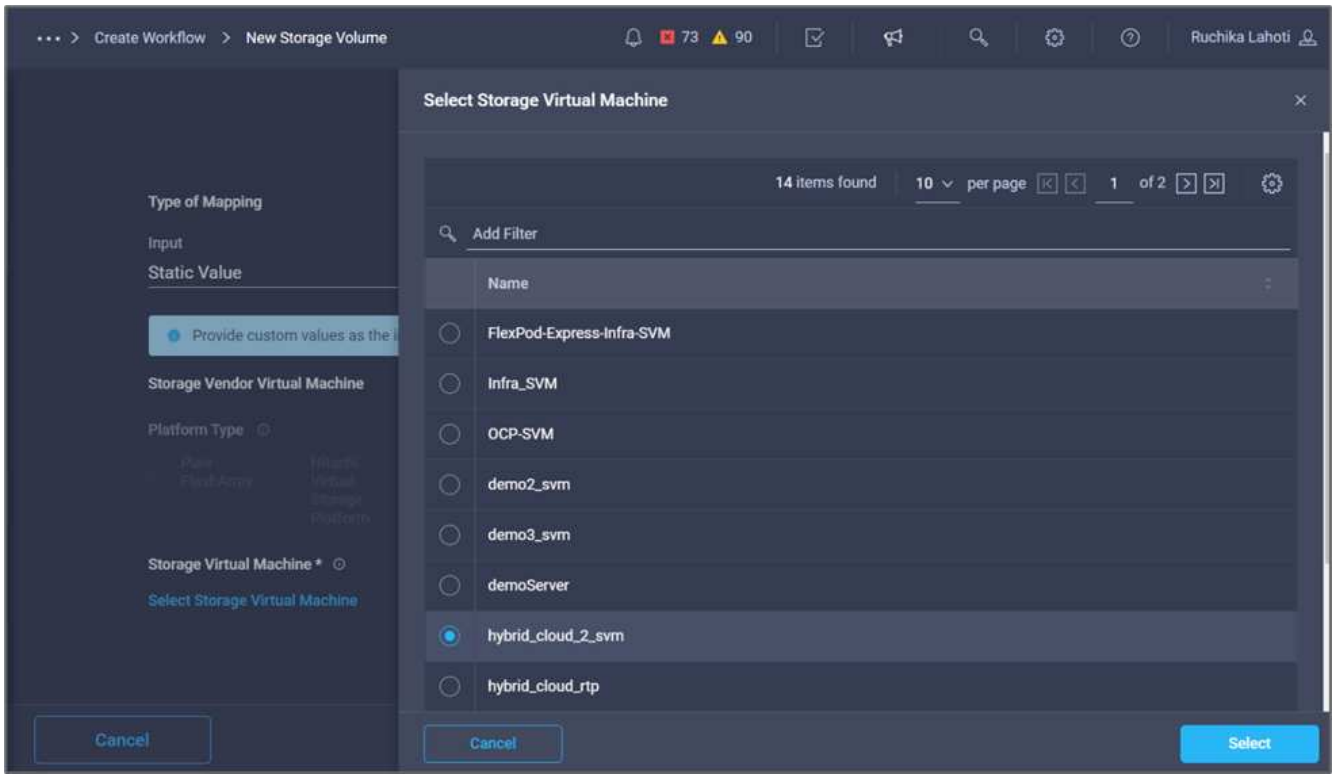
10. Storage Vendor Virtual Machine フィールドで Map *をクリックします。



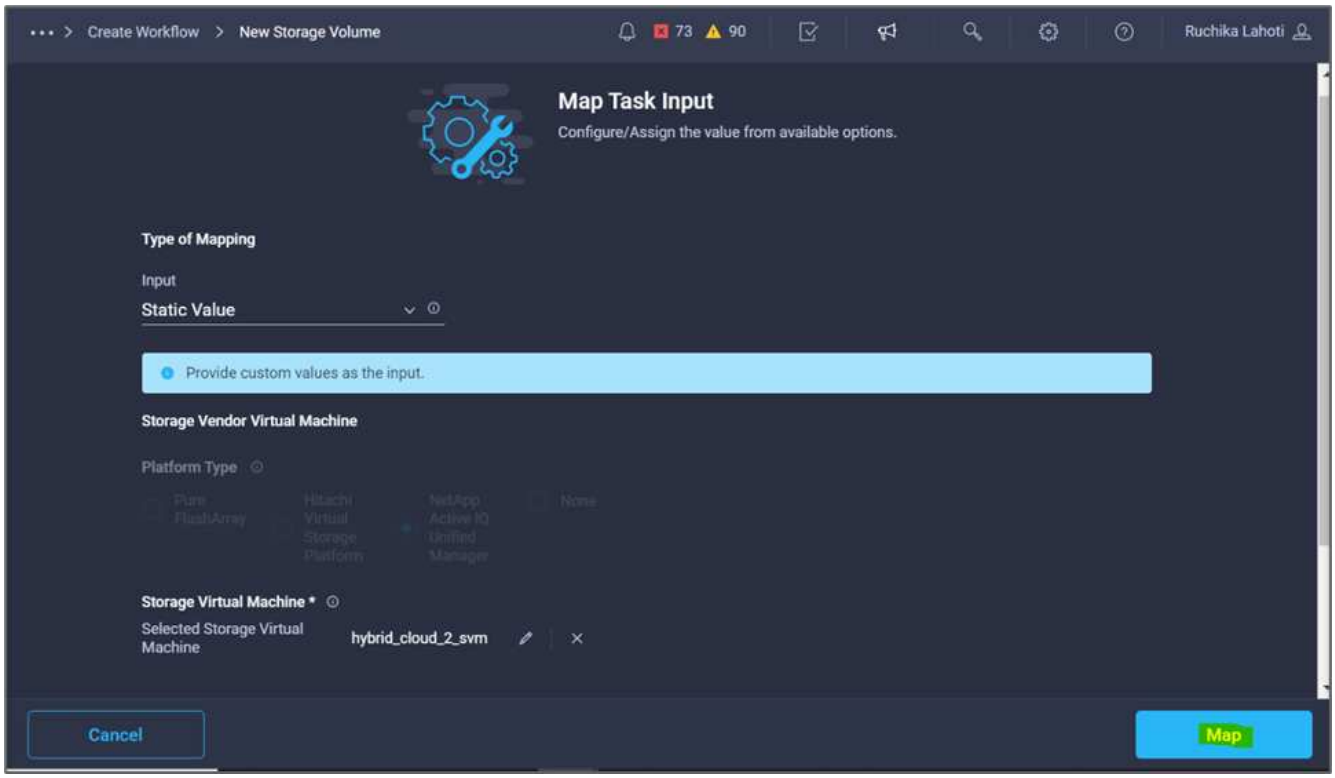
11. 「* Static Value 」を選択し、「 Storage Virtual Machineの選択*」をクリックします。



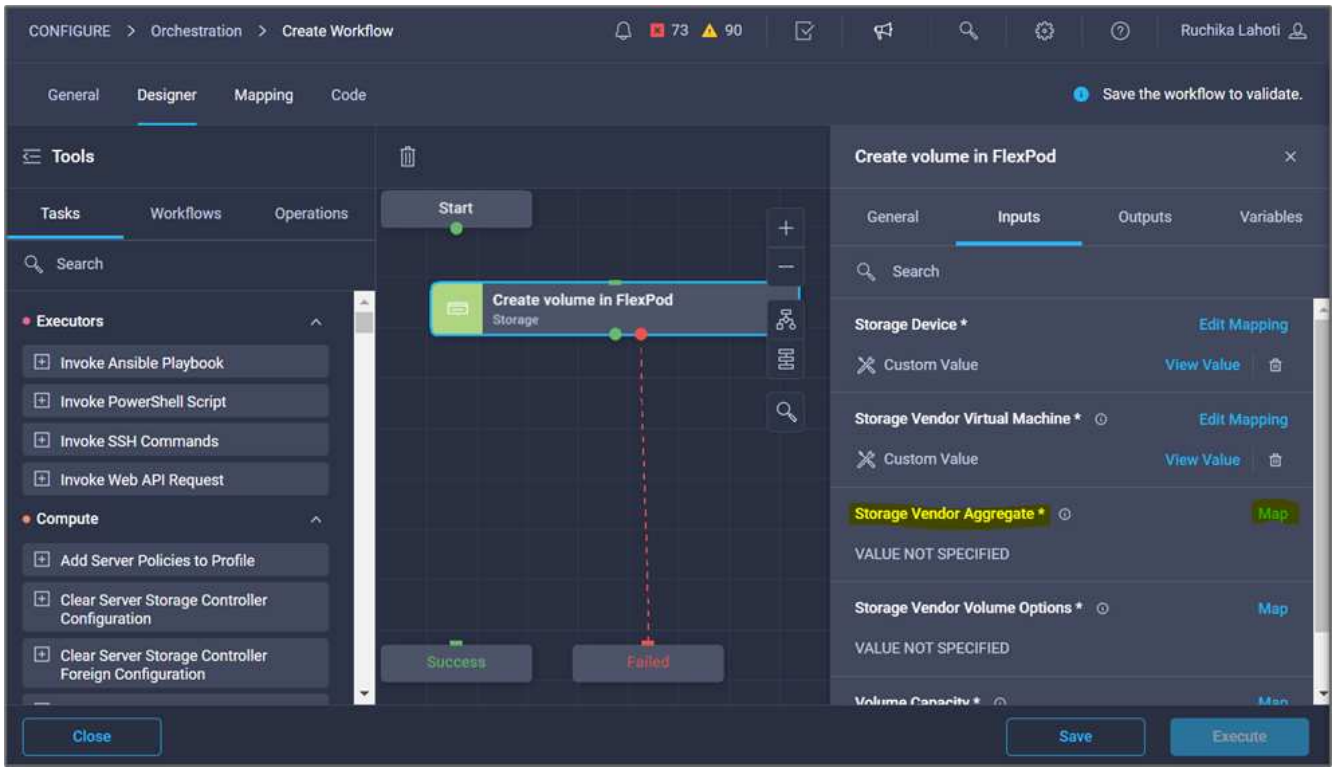
12. ボリュームを作成するStorage Virtual Machineを選択し、* Select *をクリックします。



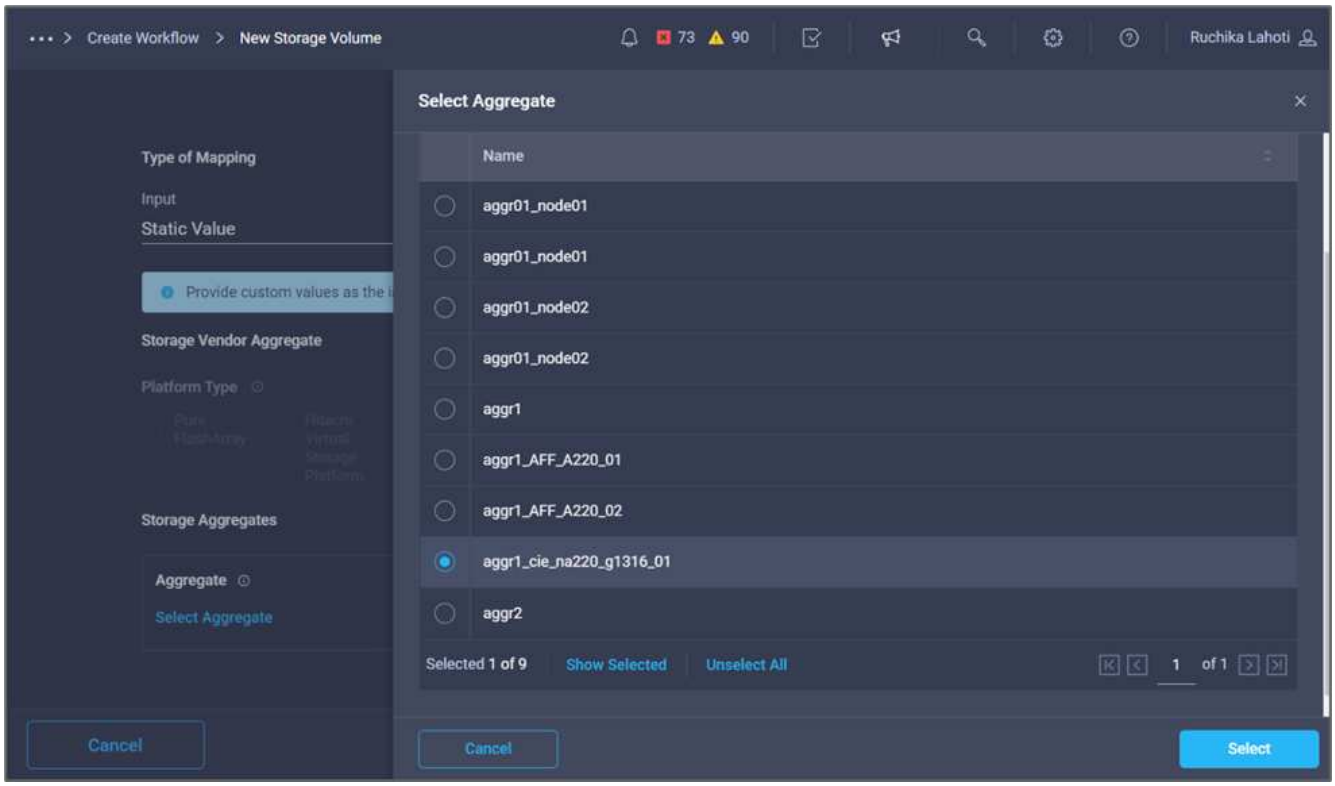
13. [マップ]をクリックします。



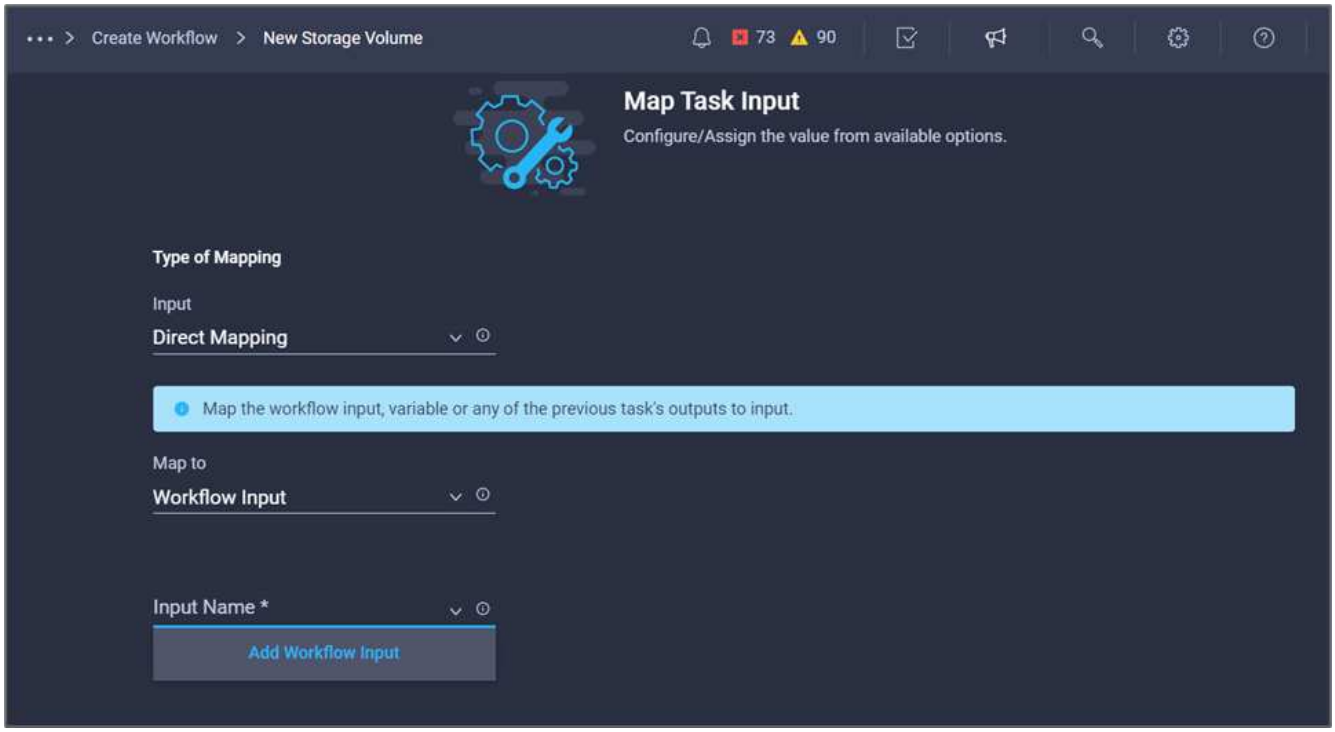
14. Storage Vendor Aggregate フィールドで Map *をクリックします。



15. 「静的値」を選択し、「*ストレージアグリゲートの選択」をクリックします。アグリゲートを選択し、Select *をクリックします。

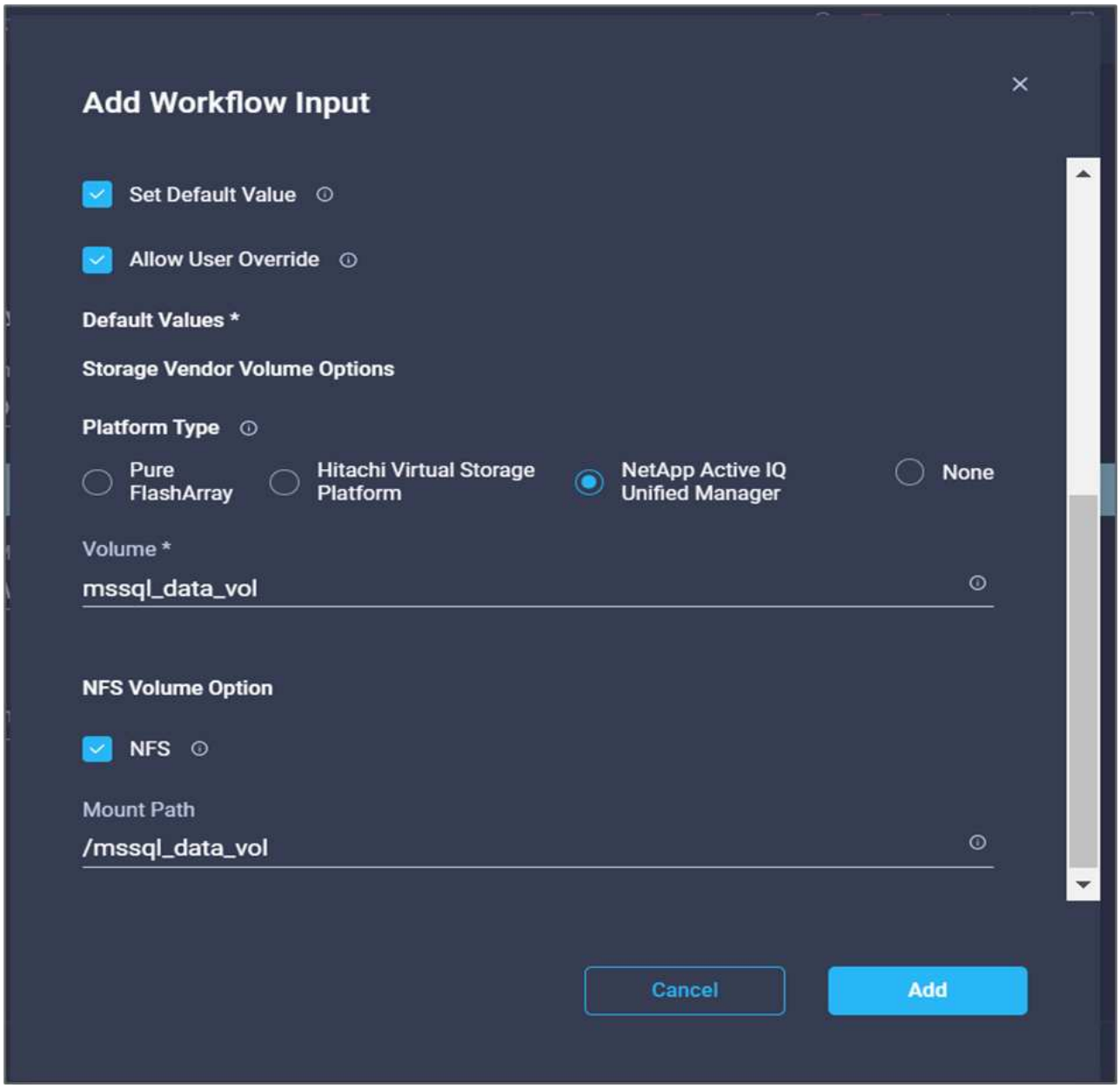


16. [マップ]をクリックします。
17. Storage Vendor Volume Options （ストレージベンダーボリュームオプション）フィールドで* Map *をクリックします。
18. [直接マッピング]を選択し、[ワークフロー入力]をクリックします。



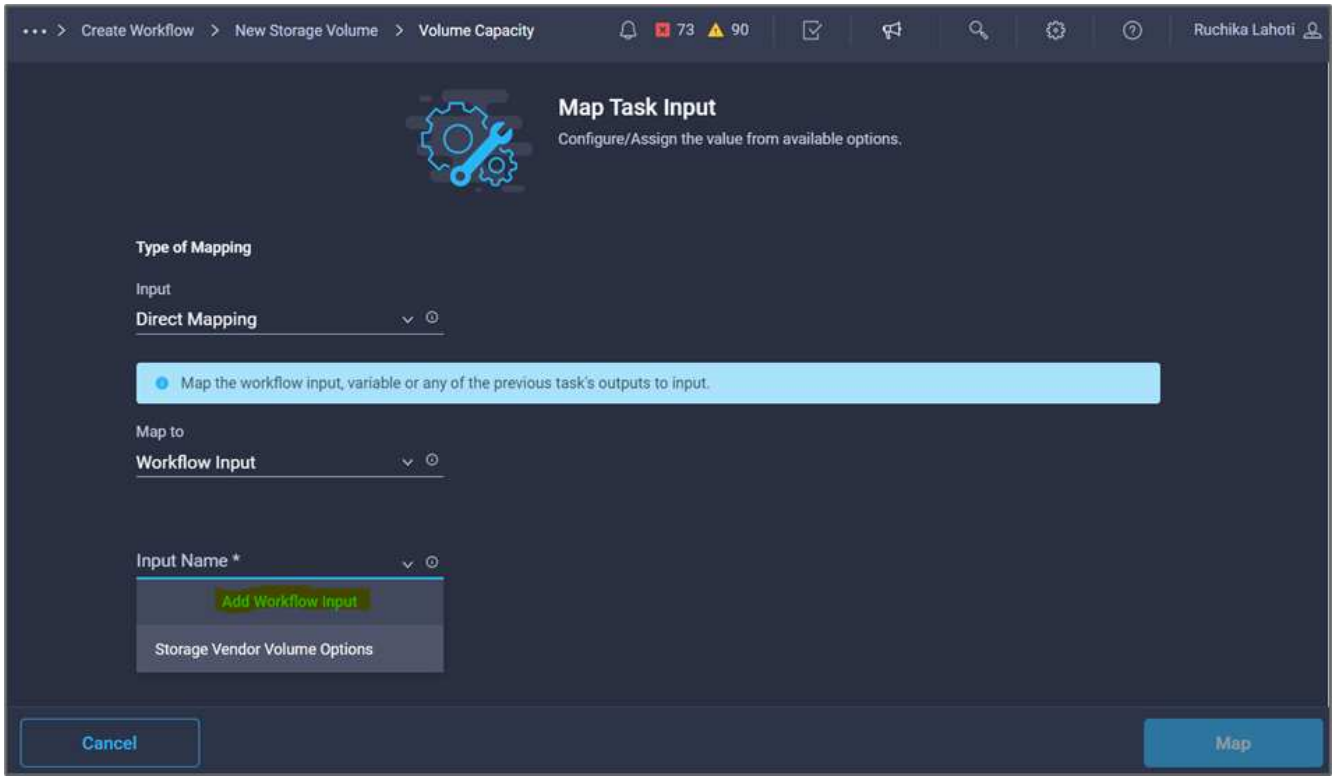
19. 入力の追加ウィザードで、次の手順を実行します。
    a. 表示名と参照名を指定します（オプション）。

b. タイプ*でストレージ・ベンダーのボリューム・オプション*が選択されていることを確認します。
c. [デフォルト値の設定]と[オーバーライド*]をクリックします。
d. [必須]をクリックします。
e. プラットフォームのタイプ*をNetApp Active IQ Unified Manager *に設定します。
f. 作成したボリュームのデフォルト値を* Volume *で指定します。
g. [**NFS**]をクリックします。NFSが設定されている場合は、NFSボリュームが作成されます。この値をfalseに設定すると、SANボリュームが作成されます。
h. マウントパスを指定し、* Add *をクリックします。

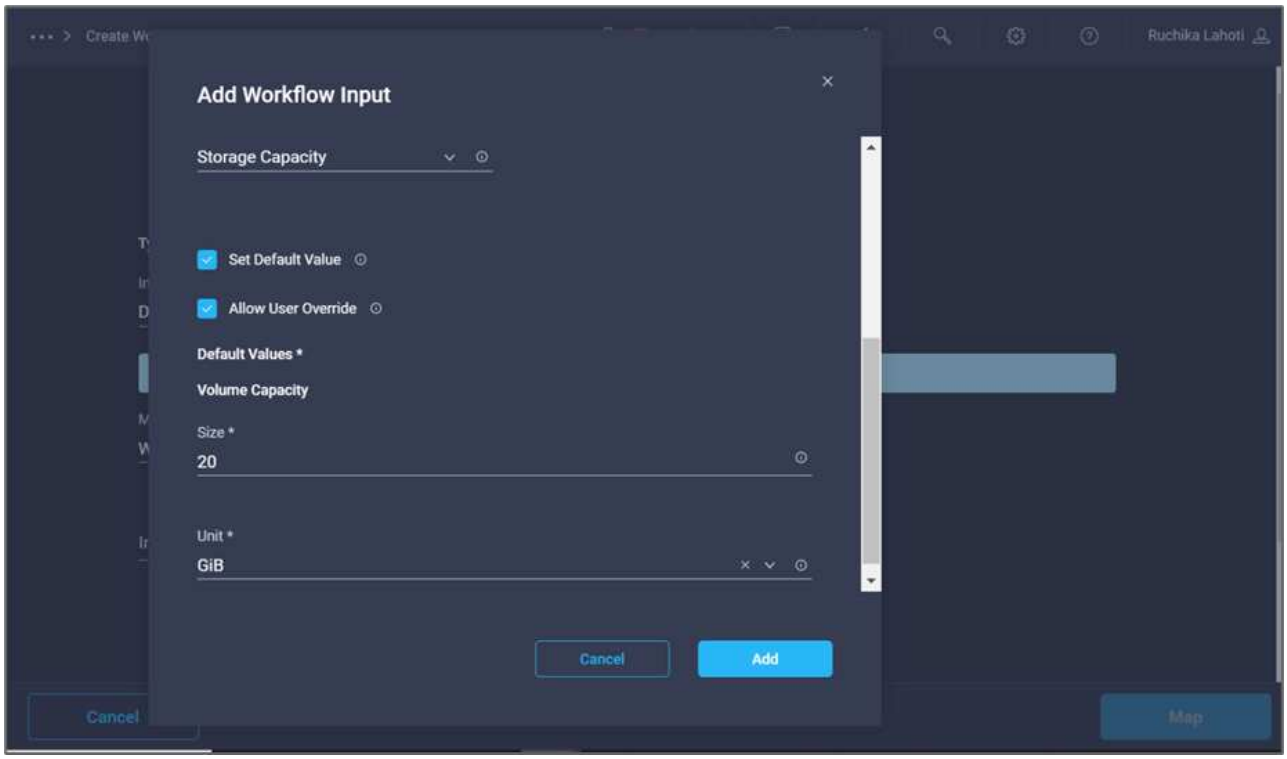


20. [マップ]をクリックします。
21. [* Volume Capacity*（ボリューム容量*）]フィールドで[* Map]*をクリックします。
22. [直接マッピング]を選択し、[ワークフロー入力]をクリックします。

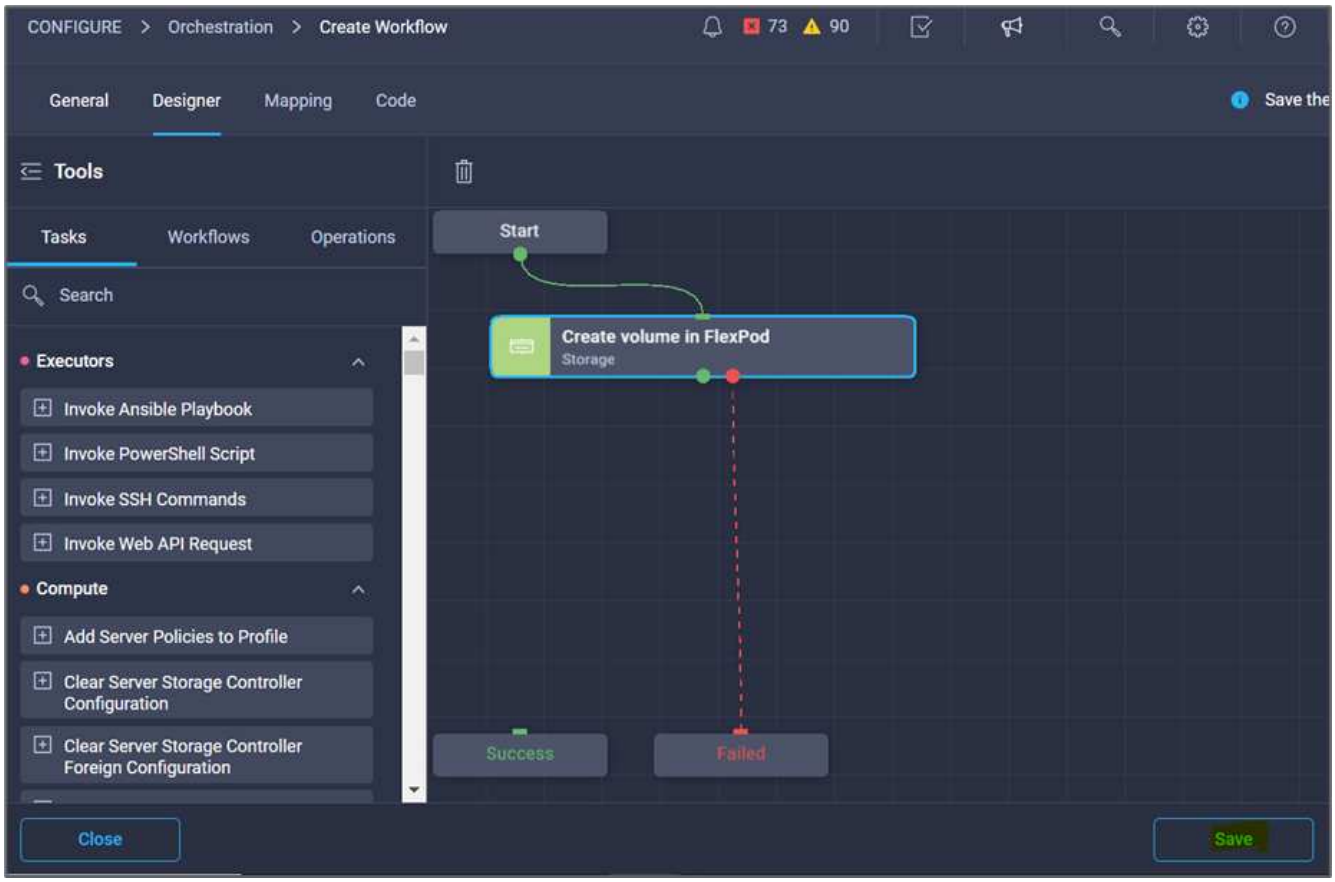
23. [入力名]および[ワークフロー入力の作成]をクリックします。



24. 入力の追加ウィザードで、次の操作を行います。
    a. 表示名と参照名を入力します（オプション）。
    b. [必須]をクリックします。
    c. 「タイプ」で、「ストレージ容量」を選択します。
    d. [デフォルト値の設定]と[オーバーライド*]をクリックします。
    e. ボリュームのサイズと単位をデフォルトで指定します。
    f. [追加（ Add ）] をクリックします。



25. [マップ]をクリックします。
26. コネクターを使用して、FlexPod *タスクで*スタート*と*ボリュームの作成*の間に接続を作成し、*保存*をクリックします。

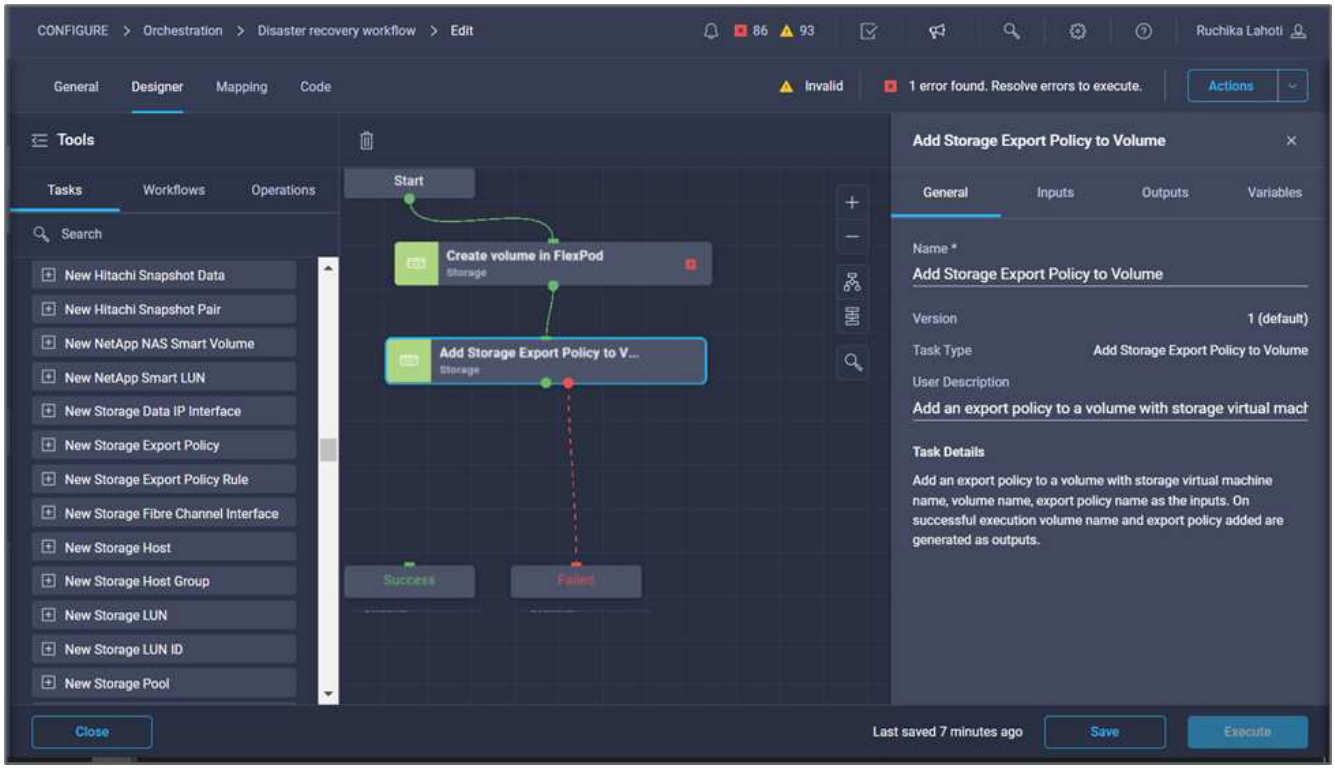


と[ボリュームの作成]の間に接続を作成する方法を示しています。"]

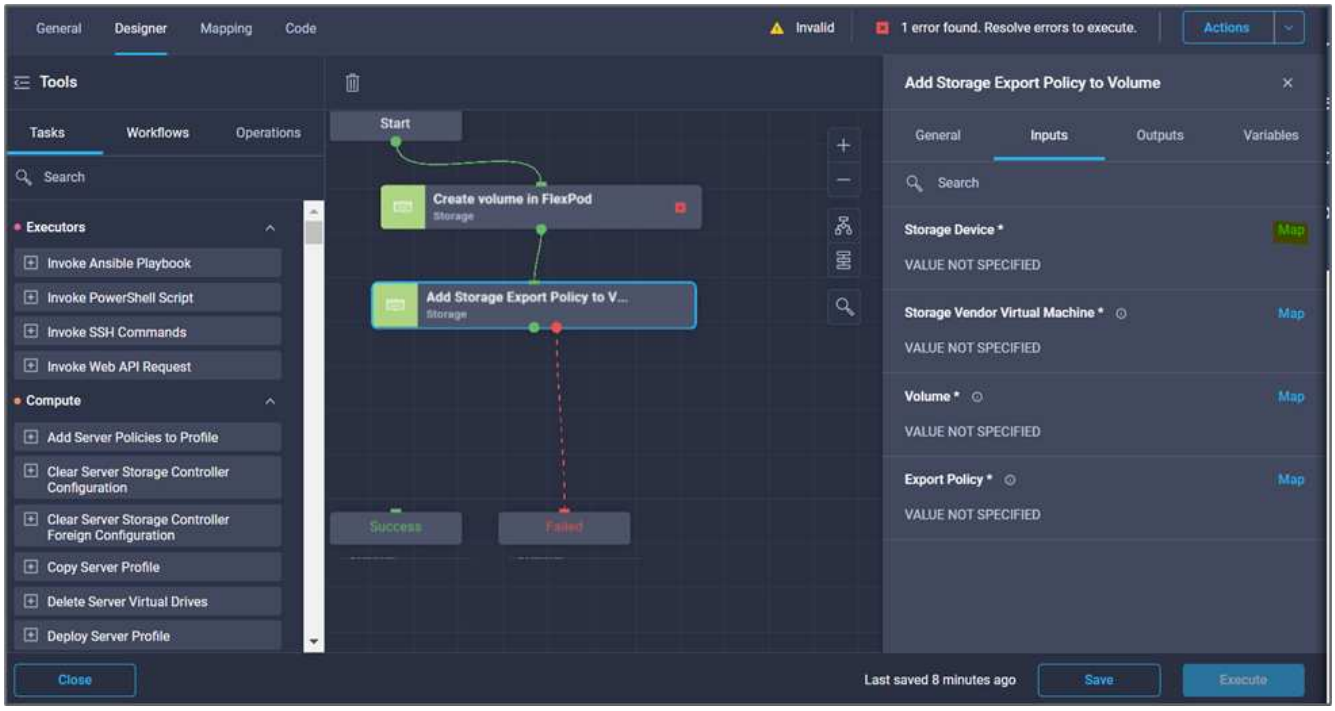
今はエラーを無視してください。このエラーは、成功した移行を指定するために必要なタスク* FlexPod でのボリュームの作成*と* Success *の間に接続がないことが原因で表示されます。

手順 **3**：ストレージエクスポートポリシーを追加します

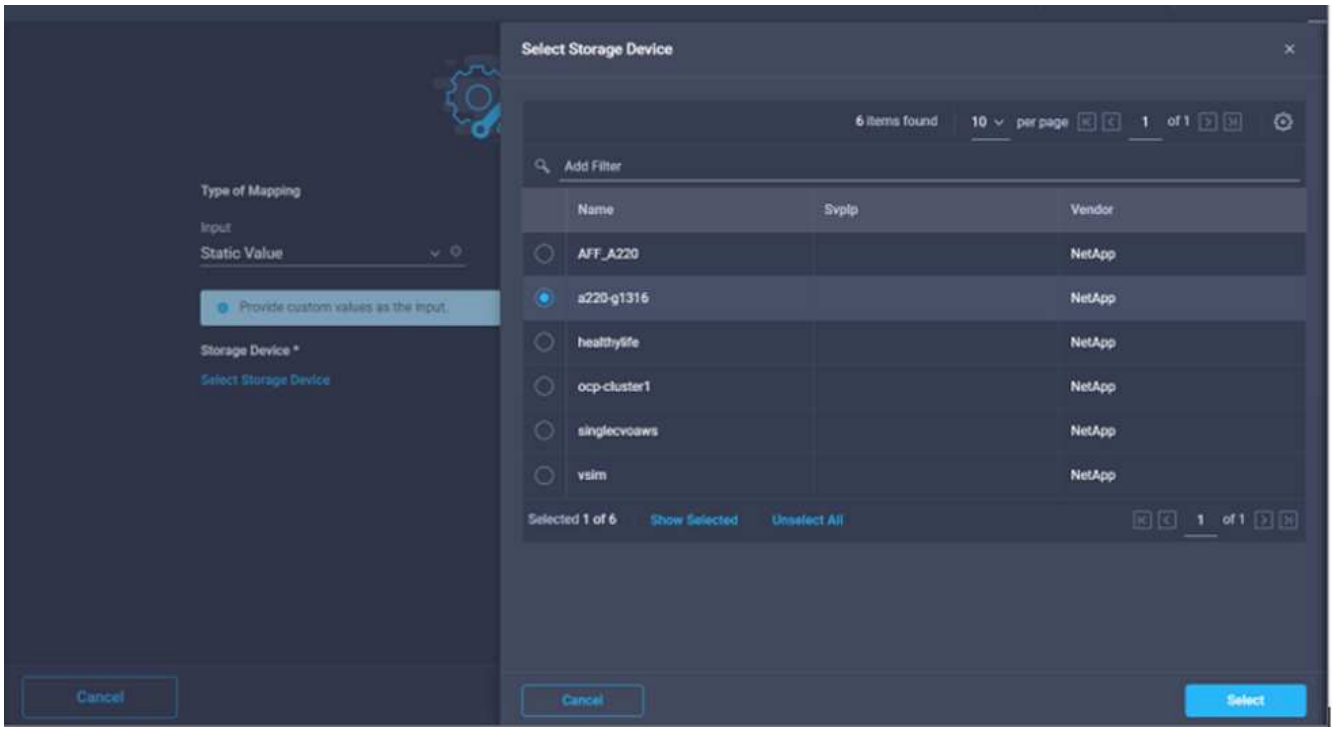
1. [*Designer]タブに移動し、[*Tools]セクションから[*Tasks]をクリックします。
2. デザイン*領域の*ツール*セクションから、*ストレージ>ボリュームへのストレージエクスポートポリシーの追加タスクをドラッグ・アンド・ドロップします。
3. Add Storage Export Policy to Volume（ボリュームへのストレージエクスポートポリシーの追加）をクリックします。[タスクのプロパティ]領域で、[一般]タブをクリックします。必要に応じて、このタスクの名前と概要 を変更できます。この例では、タスクの名前はAdd Storage Export Policyです。
4. コネクターを使用して、FlexPod *でのタスク*ボリュームの作成と*ストレージエクスポートポリシーの追加*との間に接続を確立します。[保存（ Save ）] をクリックします。



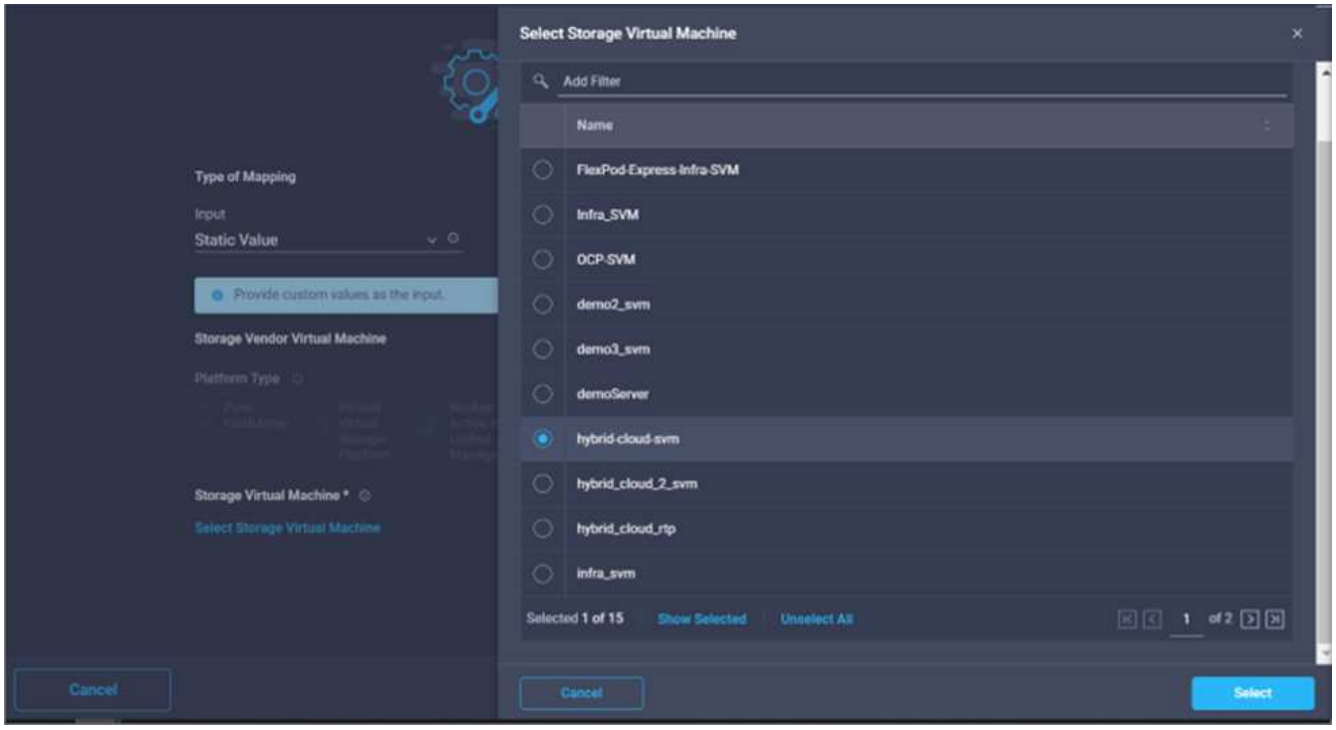
5. [タスクプロパティ（Task Properties ）]領域で、[*入力（Inputs *）]をクリックする
6. [ストレージデバイス]フィールドで[マップ]をクリックします。



7. 「* Static Value 」を選択し、「 Select Storage Device *」をクリックします。新しいストレージボリュームを作成する前のタスクで追加したのと同じストレージターゲットを選択します。
8. [マップ]をクリックします。

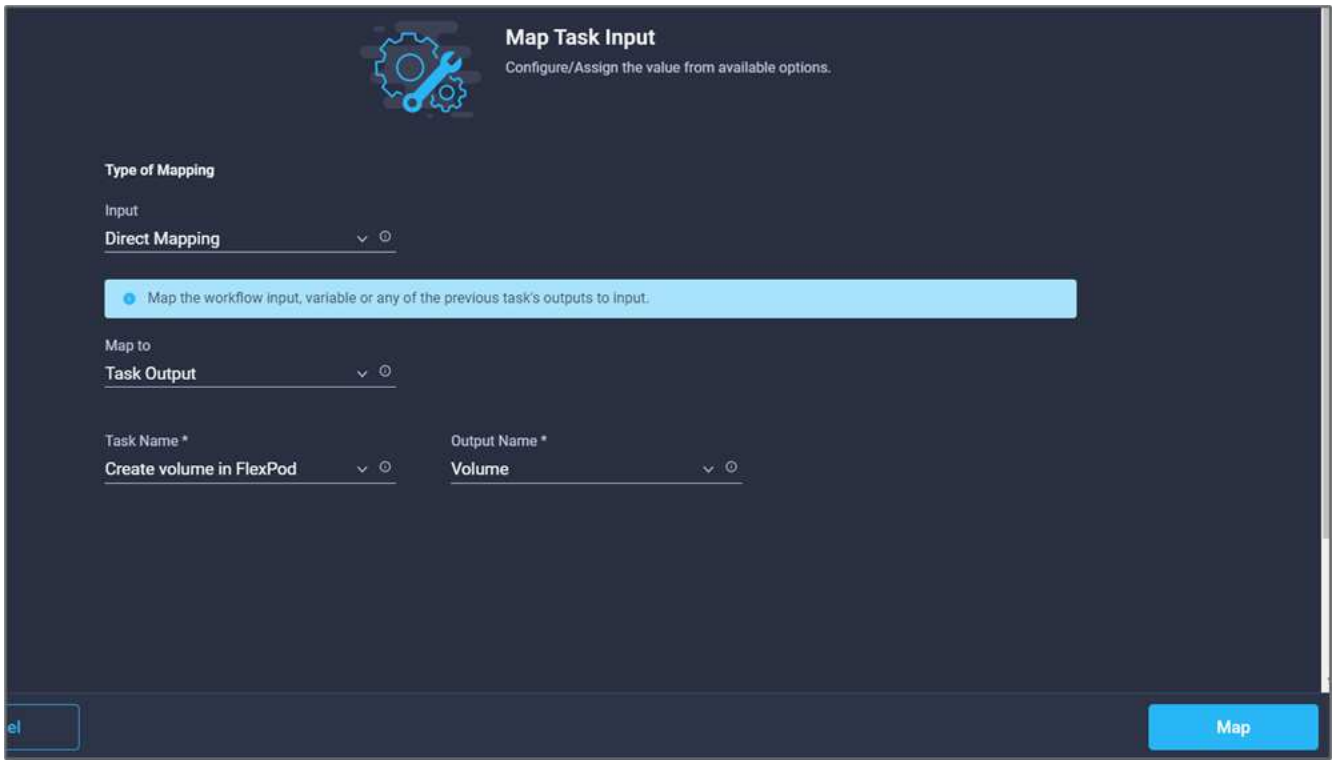


9. Storage Vendor Virtual Machine フィールドで Map *をクリックします。
10. 「* Static Value 」を選択し、「 Storage Virtual Machineの選択*」をクリックします。新しいストレージボリュームを作成する前のタスクの作成時に追加したのと同じStorage Virtual Machineを選択してください。

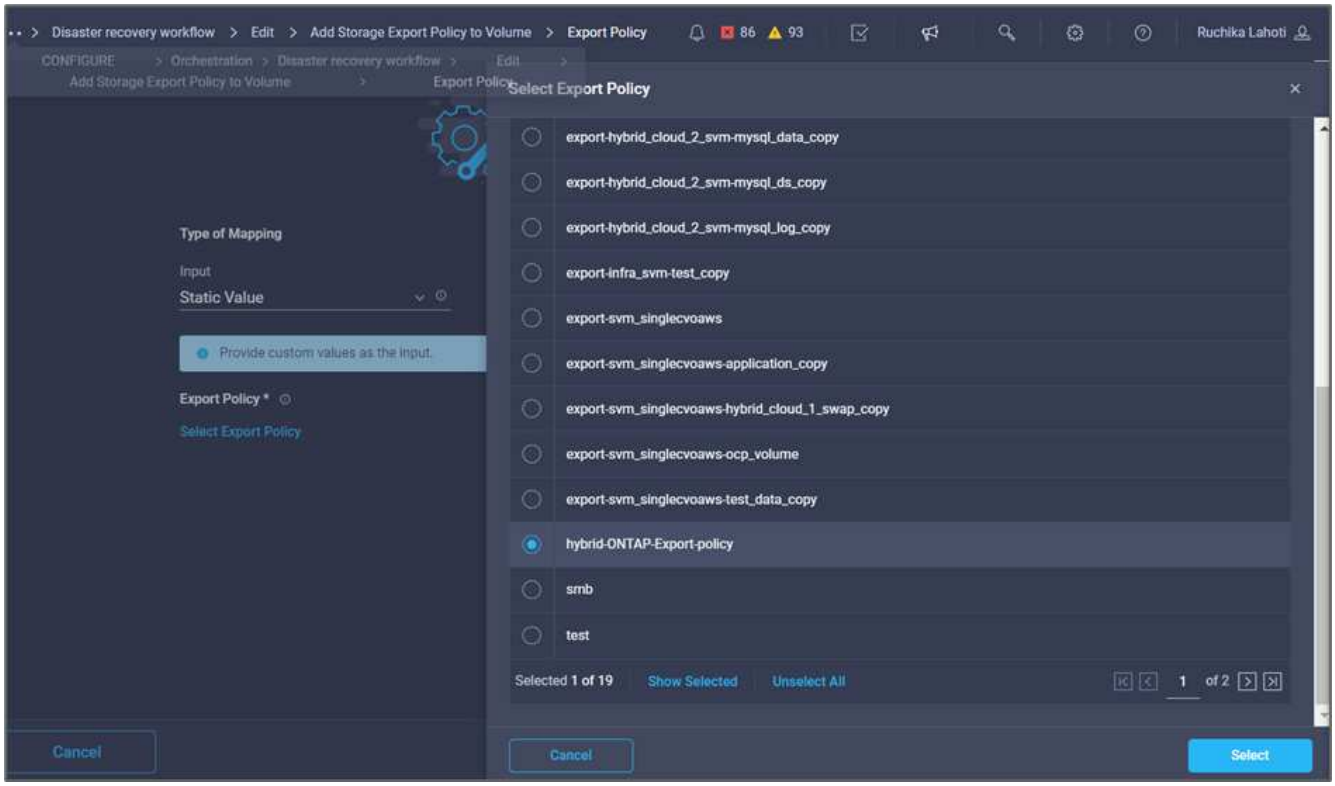


11. [マップ]をクリックします。
12. [* Volume*（ボリューム*）]フィールドの[マップ（* Map *）]をクリック
13. タスク名*をクリックし、FlexPod でボリュームを作成をクリックします。[*出力名]、[ボリューム]の順にクリックします。

> Cisco Intersight Cloud Orchestratorでは、前のタスクの出力を新しいタスクの入力として指定できます。この例では、「FlexPod でのボリュームの作成」タスクの入力として「ボリューム」の詳細がタスク*ストレージエクスポートポリシーの追加」から提供されています。



14. [マップ]をクリックします。
15. [エクスポートポリシー]フィールドで[マップ]をクリックします。
16. 「* Static Value 」を選択し、「*エクスポートポリシーの選択」をクリックします。作成したエクスポートポリシーを選択します。

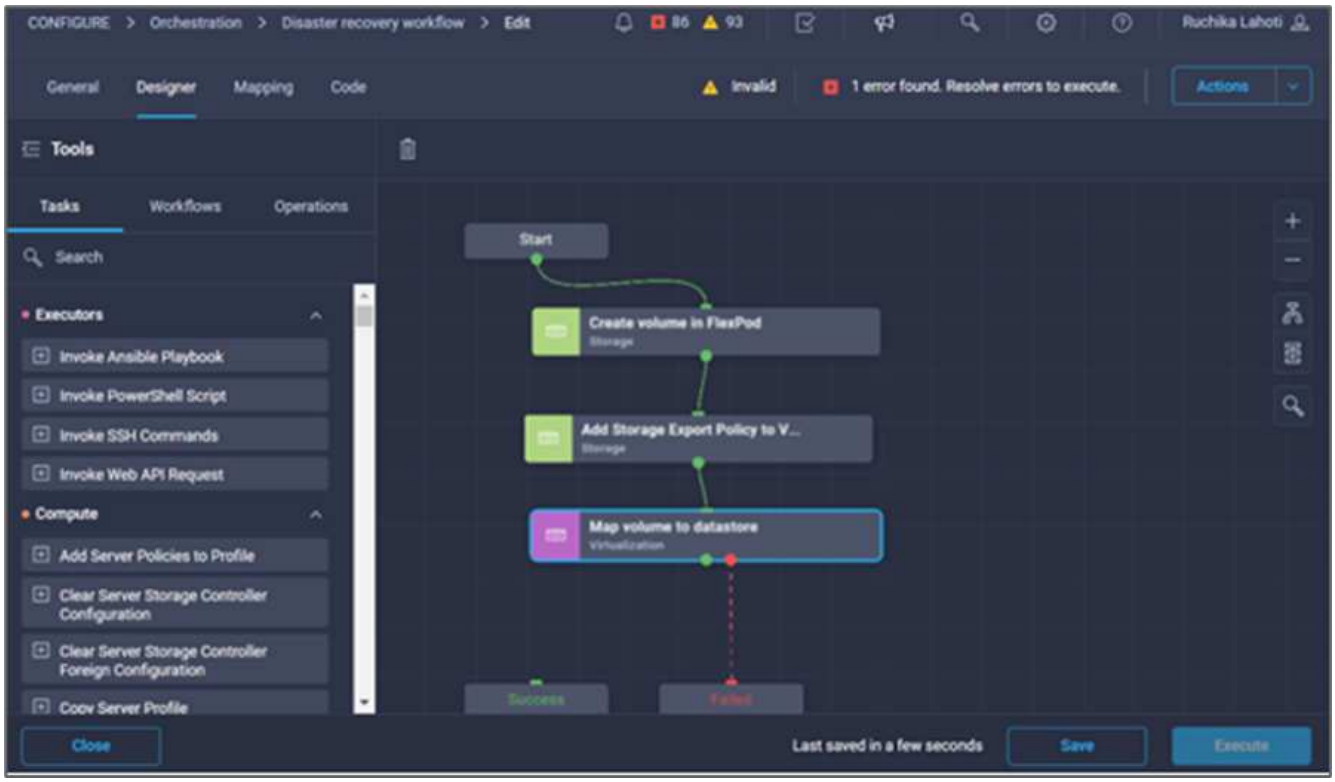


17. [マップ]、[保存]の順にクリックします。

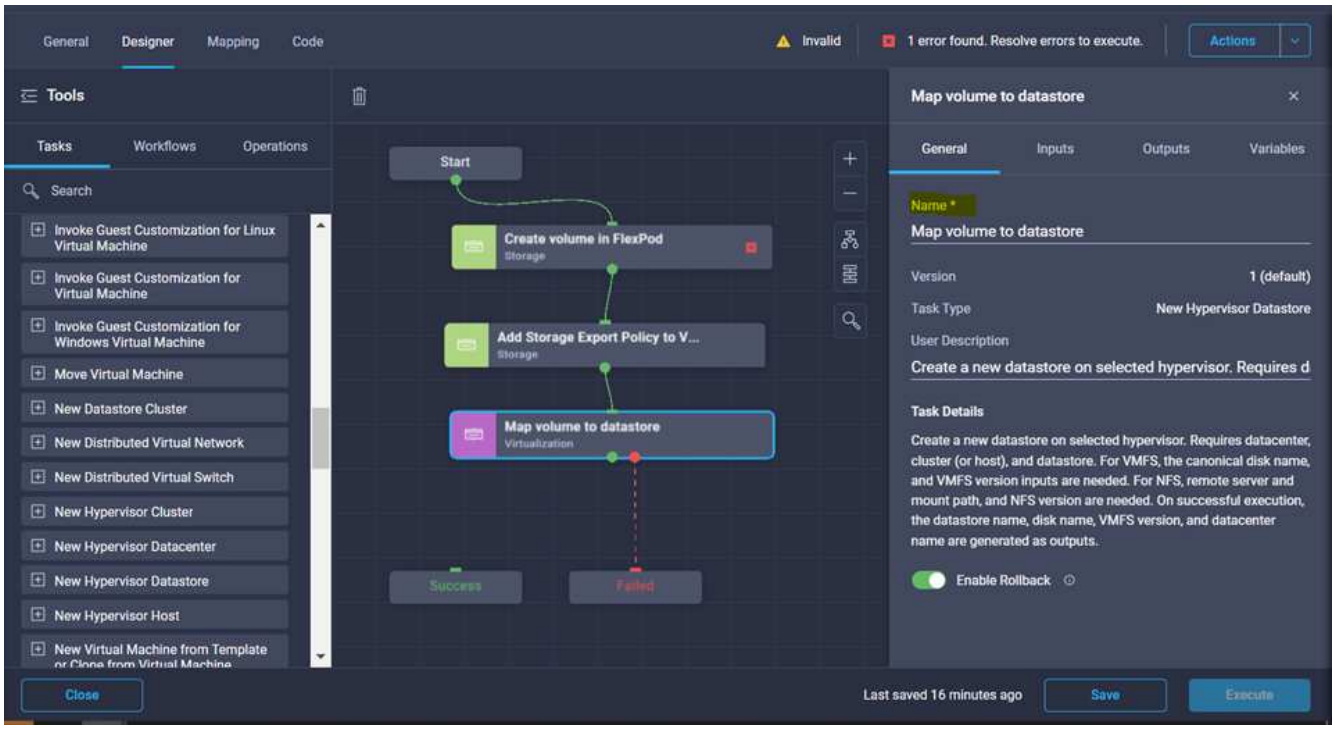
これで、ボリュームへのエクスポートポリシーの追加は完了です。次に、作成したボリュームをマッピングする新しいデータストアを作成します。

手順 **4**：**FlexPod** ボリュームをデータストアにマッピングする

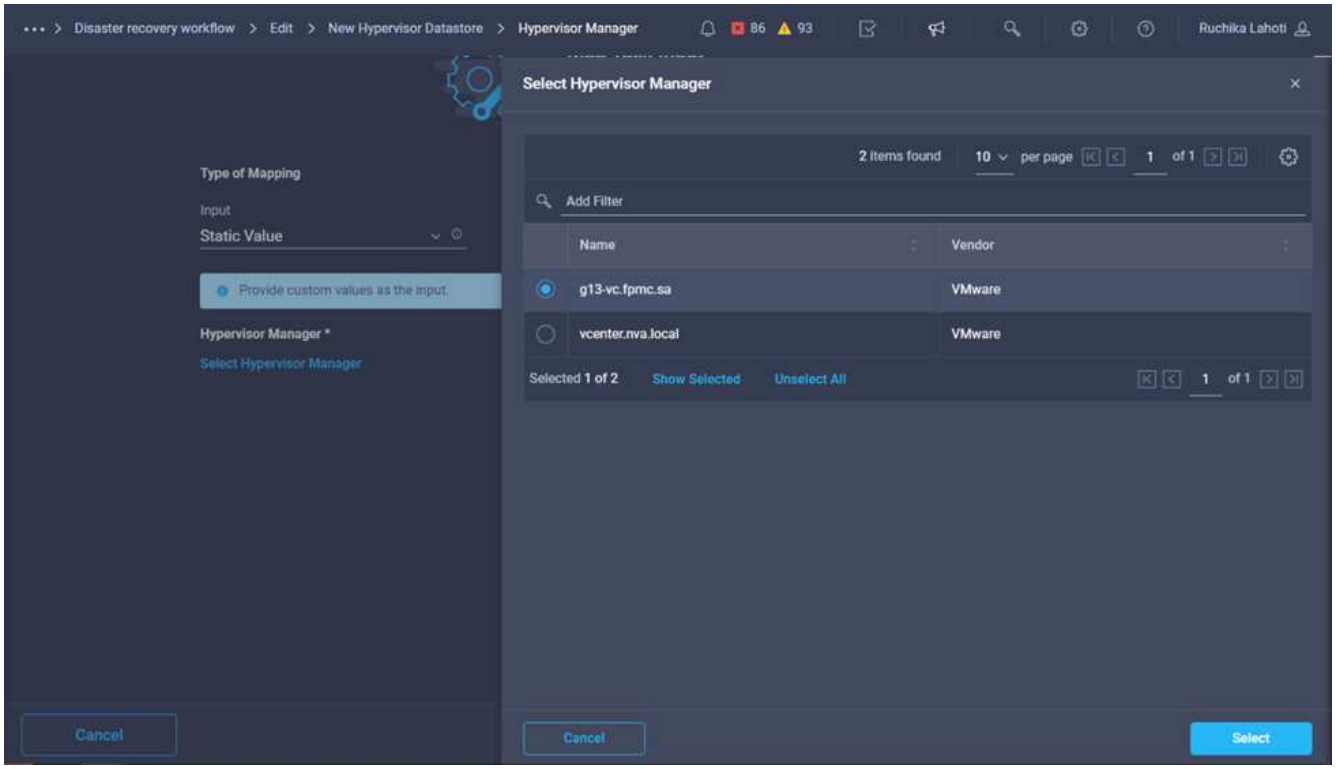
1. [*Designer]タブに移動し、[*Tools]セクションから[*Tasks]をクリックします。
2. 「デザイン」領域の「ツール*」セクションから*「仮想化」>「新しいハイパーバイザー・データストア*」タスクをドラッグアンド・ドロップします。
3. コネクタを使用して、*ストレージエクスポートポリシーの追加*タスクと*新しいハイパーバイザーデータストア*タスクを接続します。[保存（ Save ）] をクリックします。



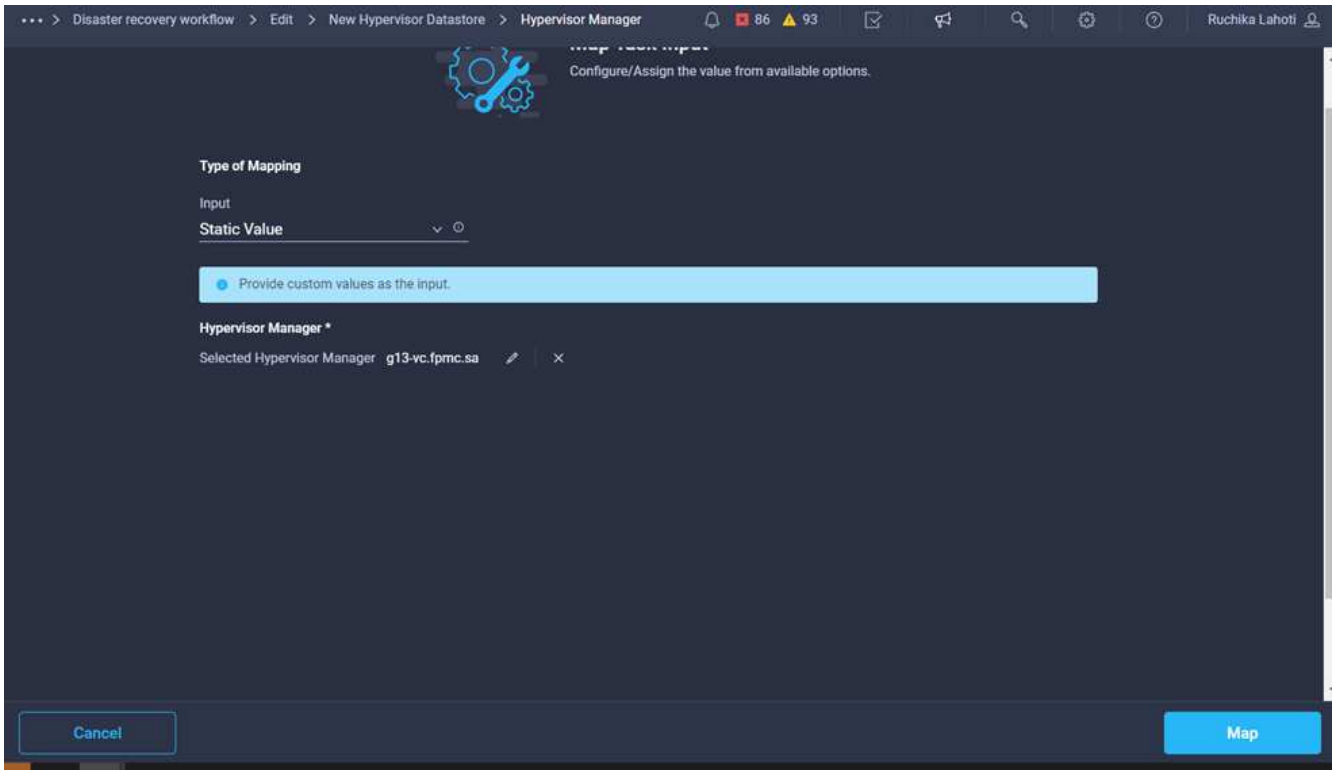
4. [New Hypervisor Datastore]をクリックします。[タスクのプロパティ]領域で、[一般]タブをクリックします。必要に応じて、このタスクの名前と概要 を変更できます。この例では、タスクの名前は*ボリュームをデータストアにマッピング*です。



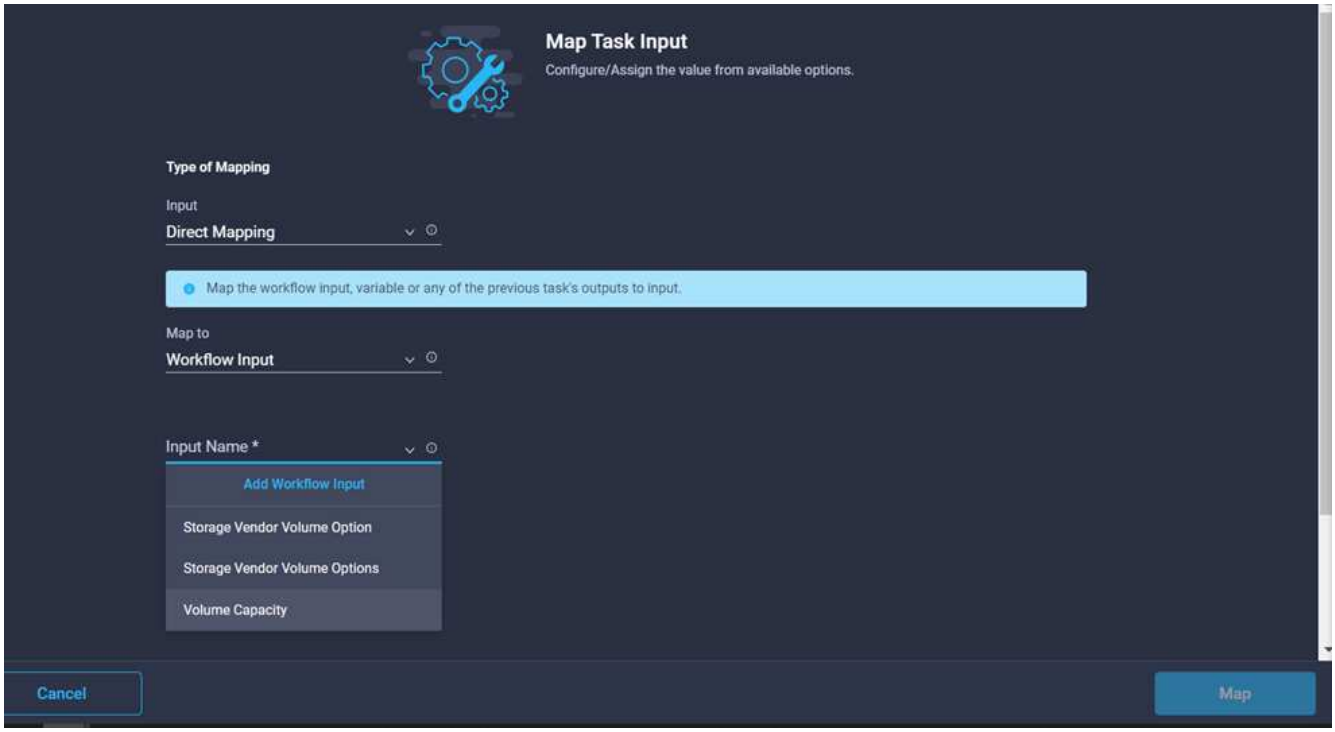
5. [タスクプロパティ（Task Properties ）]領域で、[*入力（Inputs *）]をクリックする
6. [* Hypervisor Manager*]フィールドで[* Map]をクリックします。
7. 「* Static Value 」を選択し、「*ハイパーバイザーマネージャーの選択」をクリックします。VMware vCenterターゲットをクリックします。



8. [マップ]をクリックします。



9. [データセンター]フィールドで[マップ]をクリックします。新しいデータストアに関連付けられているデータセンターです。
10. [直接マッピング]を選択し、[ワークフロー入力]をクリックします。
11. [入力名]、[ワークフロー入力の作成]の順にクリックします。



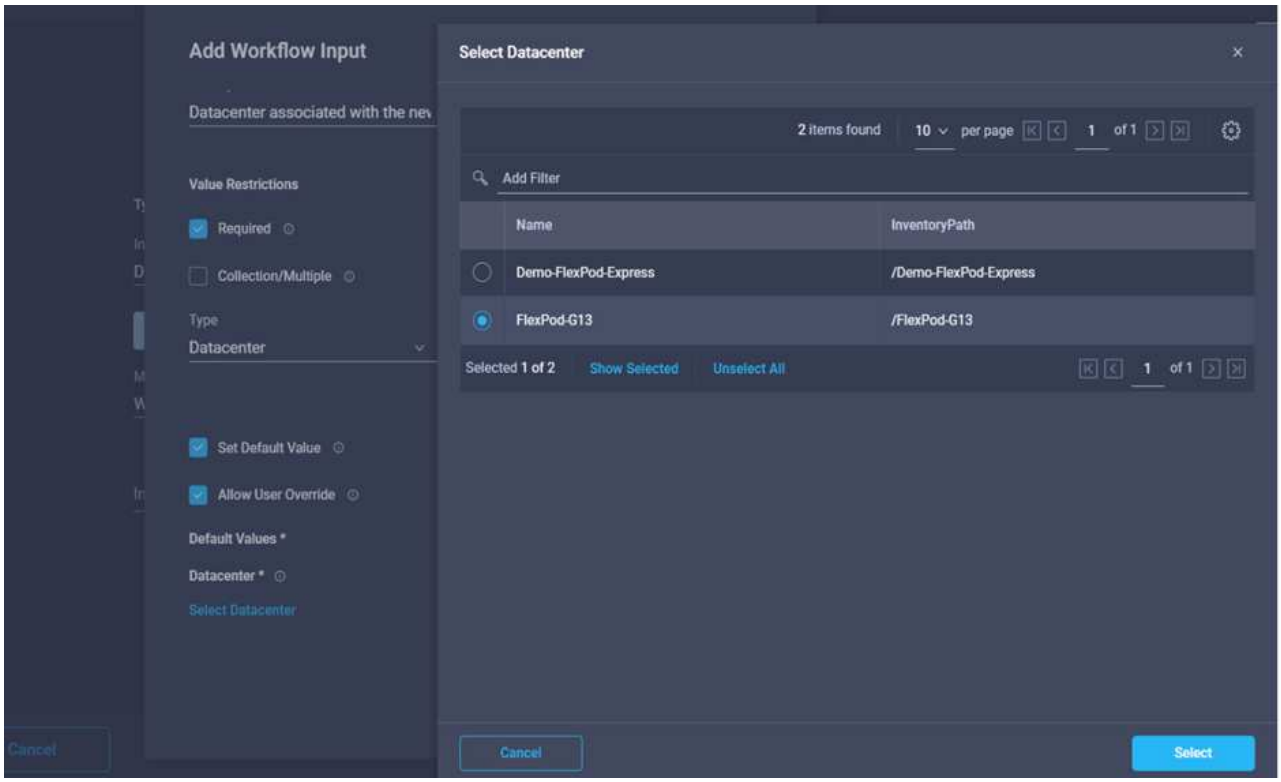
12. 入力の追加ウィザードで、次の手順を実行します。
    a. 表示名と参照名を指定します（オプション）。

b. タイプとして* Datacenter *を選択します。

c. [デフォルト値の設定]と[オーバーライド*]をクリックします。

d. [データセンターの選択]をクリックします。

e. 新しいデータストアに関連付けられているデータセンターをクリックし、* Select *をクリックします。

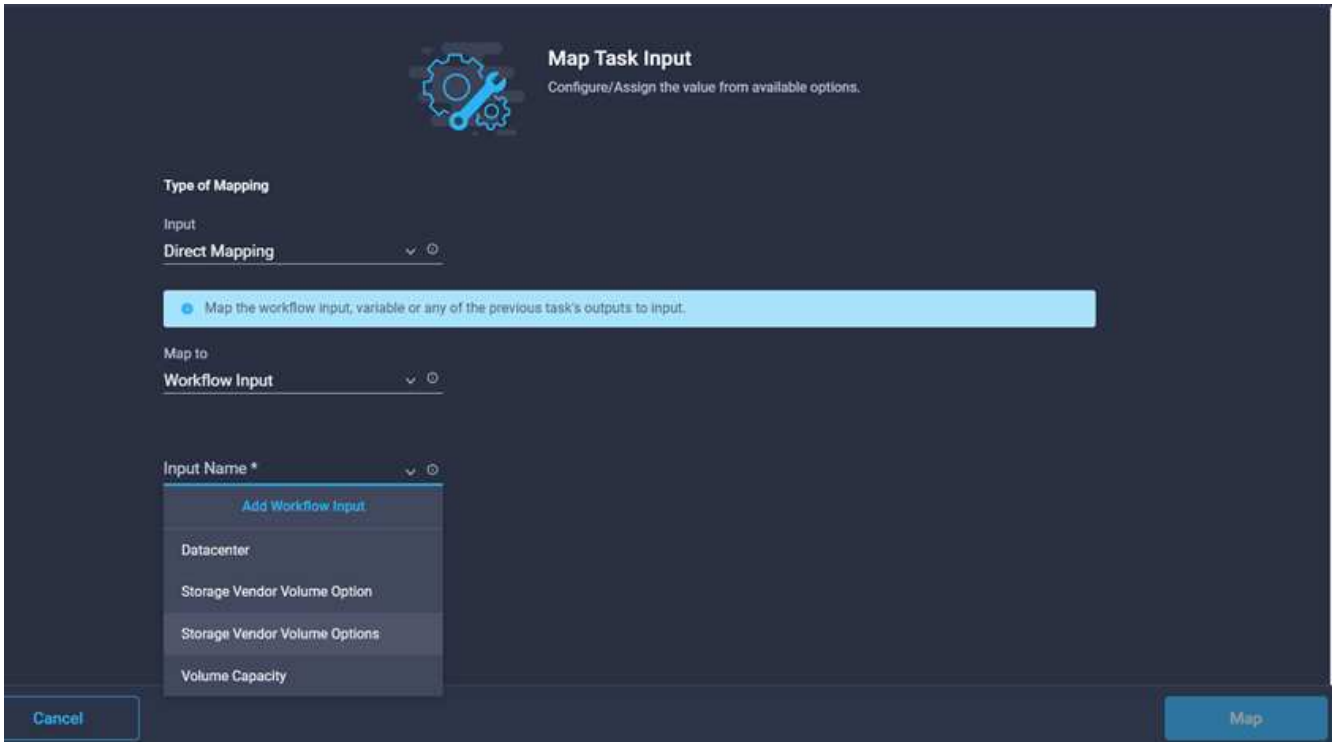


- [追加（ Add ）] をクリックします。

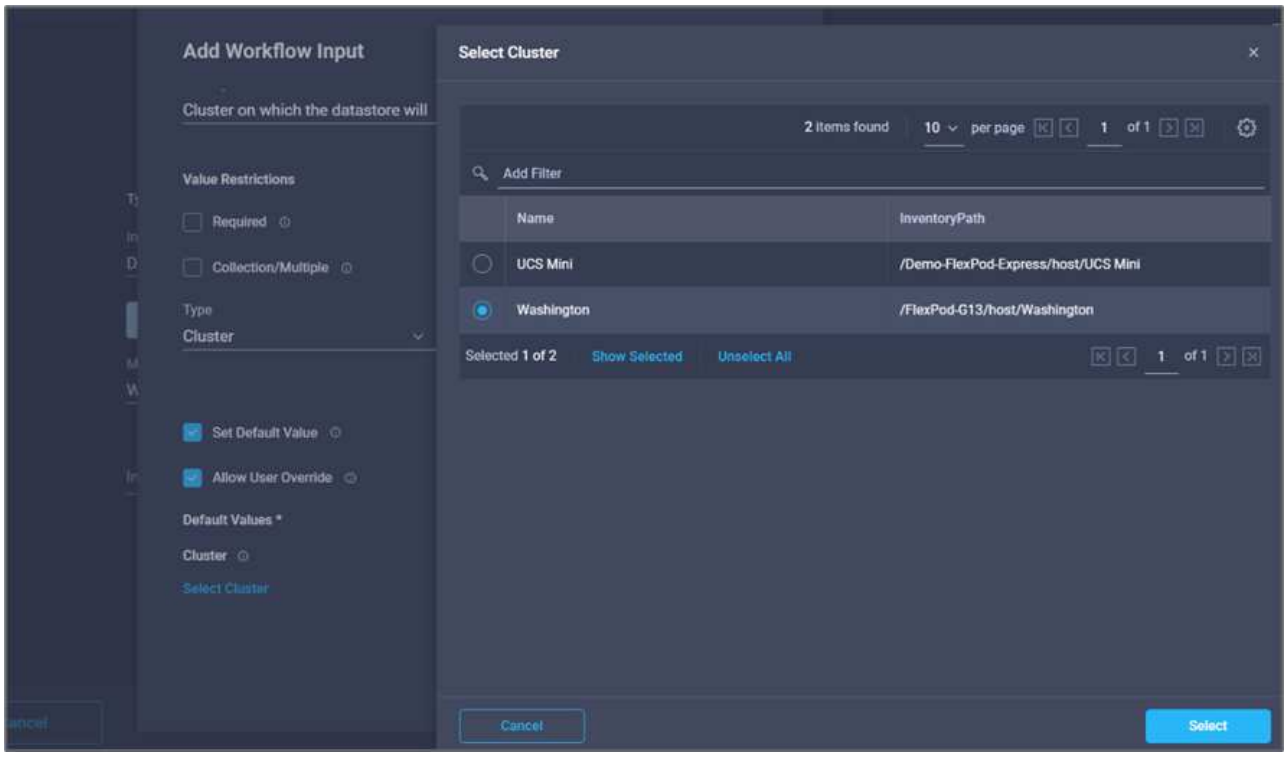
13. [マップ]をクリックします。

14. [**Cluster**]フィールドで[**Map**]をクリックします。

15. [直接マッピング]を選択し、[ワークフロー入力]をクリックします。

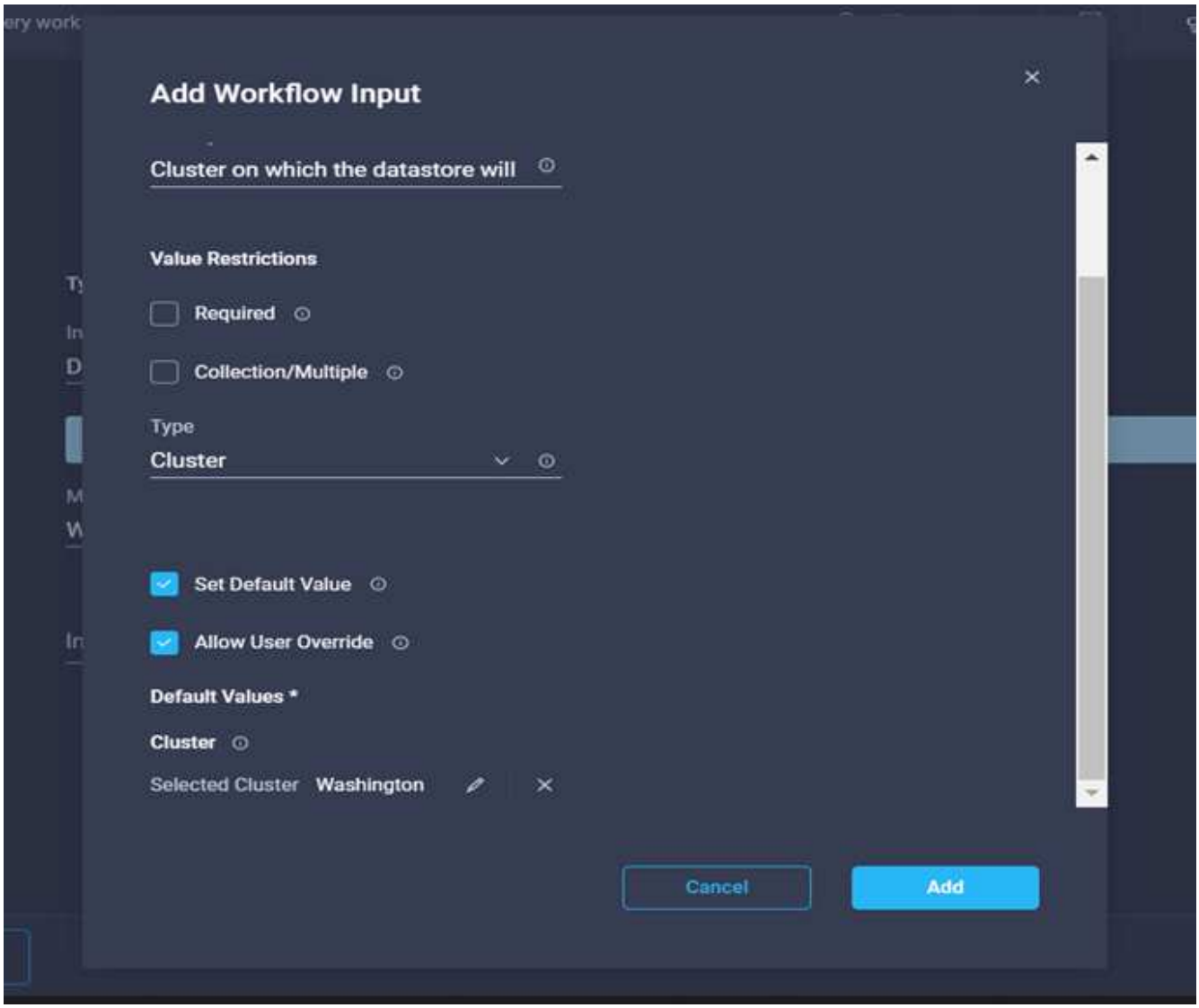


16. 入力の追加ウィザードで、次の手順を実行します。
    a. 表示名と参照名を指定します（オプション）。
    b. [必須]をクリックします。
    c. タイプとしてClusterを選択します。
    d. [デフォルト値の設定]と[オーバーライド*]をクリックします。
    e. Select Cluster（クラスタの選択）*をクリックします。
    f. 新しいデータストアに関連付けられているクラスタをクリックします。
    g. [* 選択 *] をクリックします。

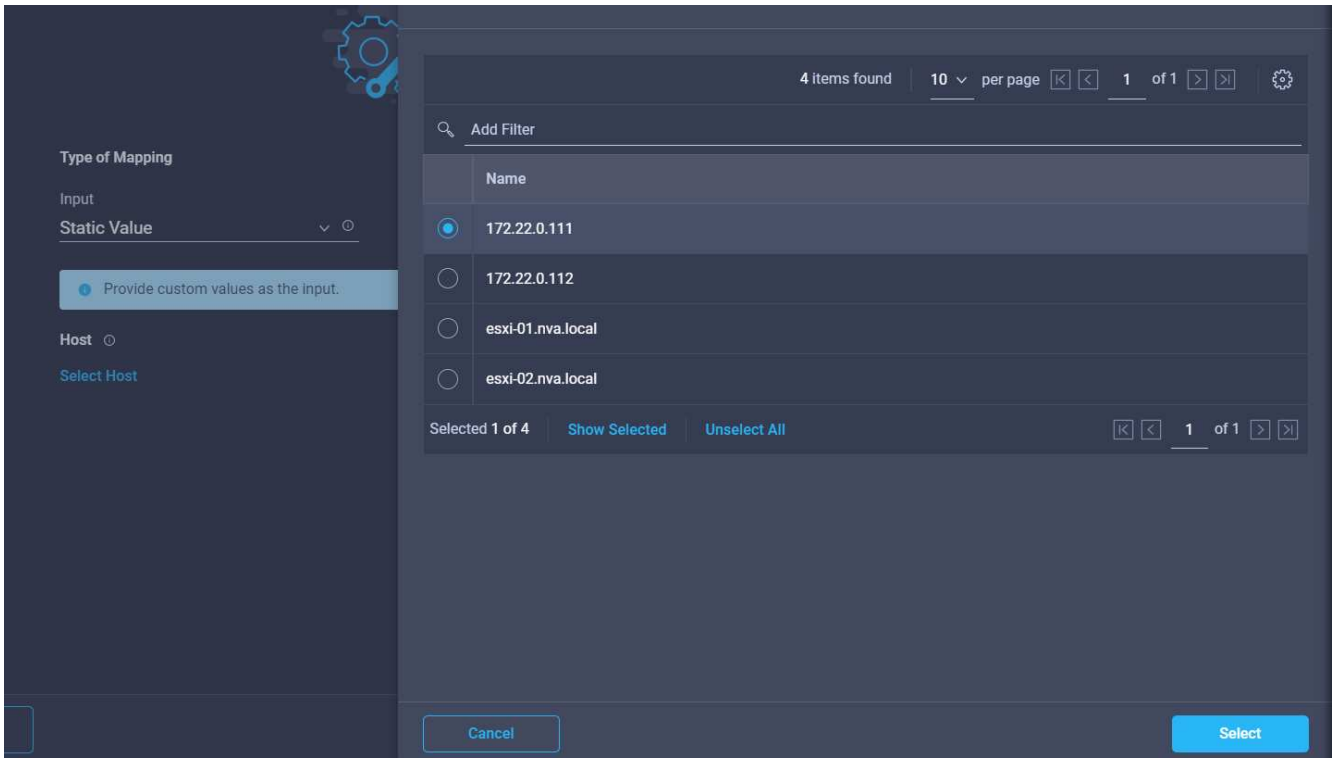


h. [追加（ Add ）] をクリックします。

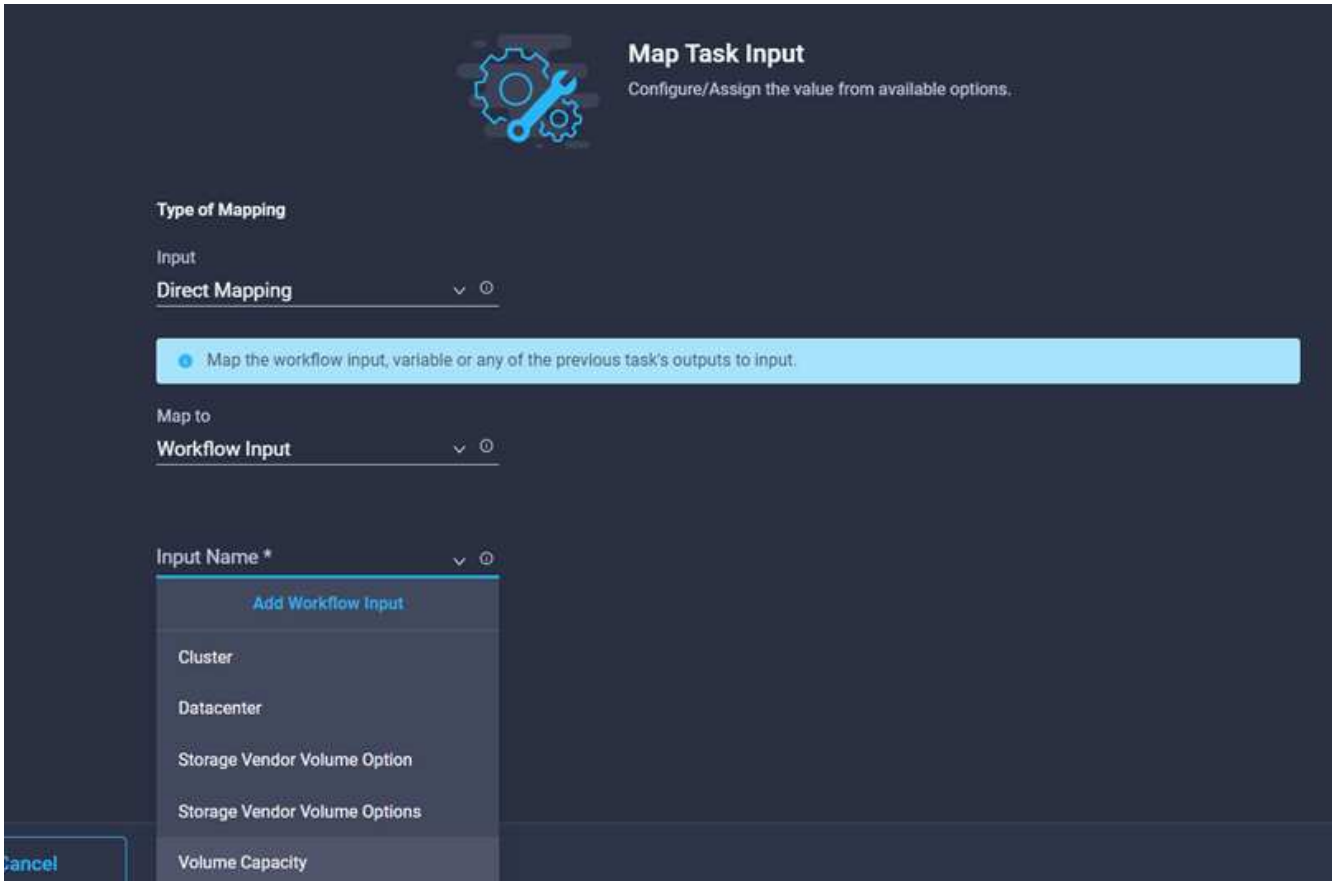
17. [マップ]をクリックします。
18. [**Host**]フィールドの[**Map**]をクリックします。



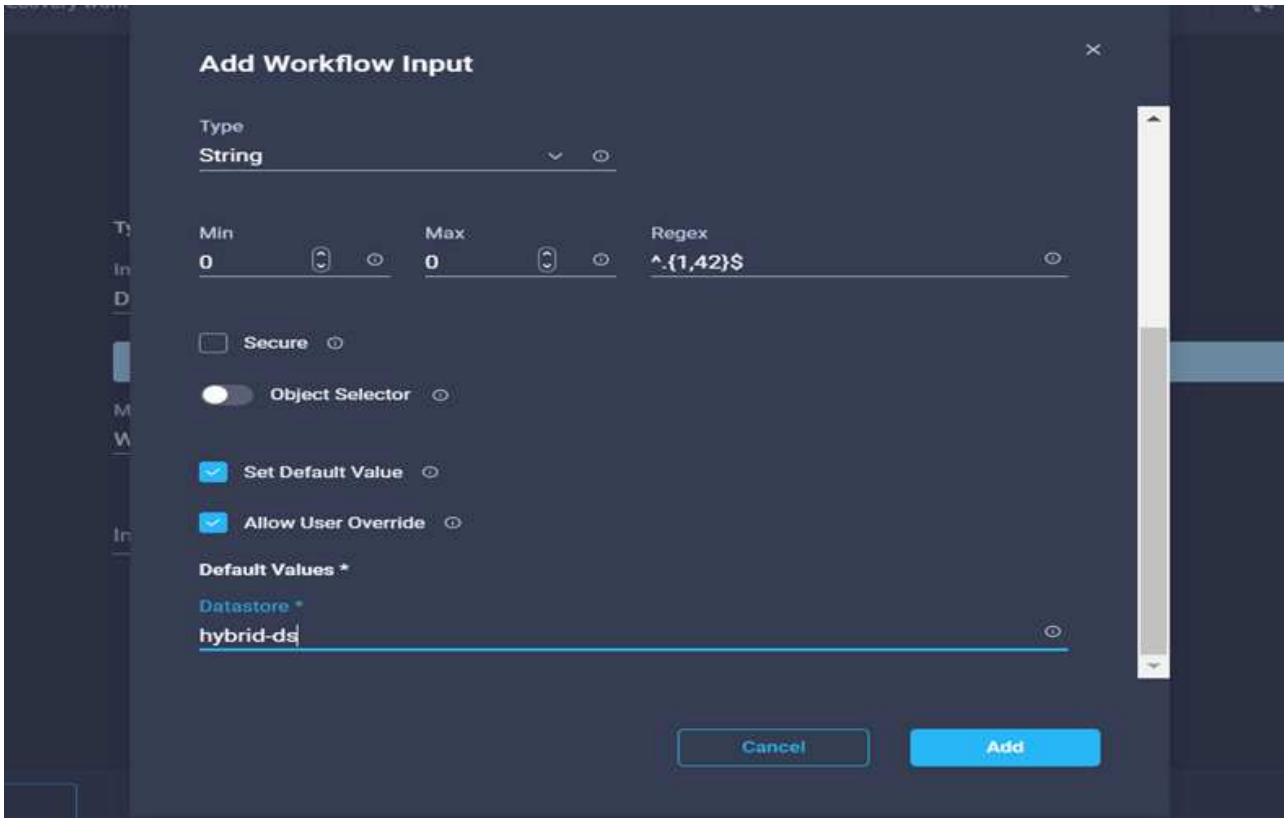
19. 「* Static Value *」を選択し、データストアをホストするホストをクリックします。クラスタを指定した場合、ホストは無視されます。



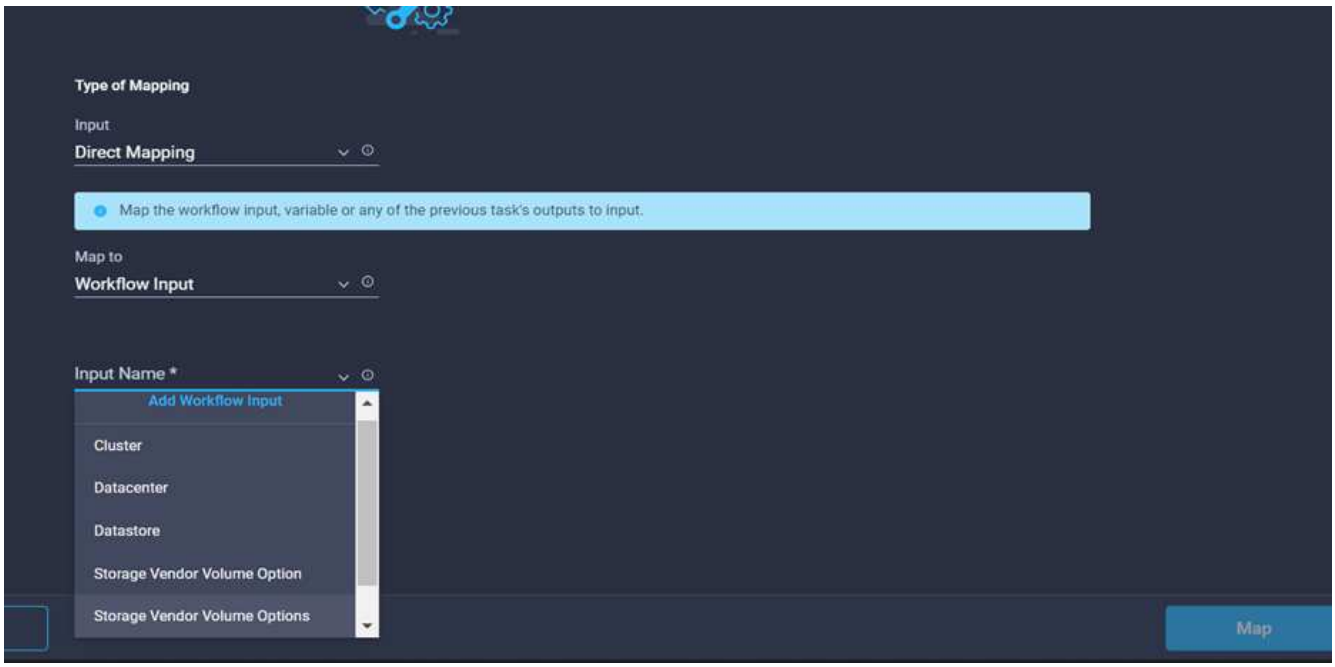
20. [選択してマップ]をクリックします。
21. **[Datastore](**データストア**)**フィールドで**[*Map](**マップ)をクリックします。
22. [直接マッピング]を選択し、[ワークフロー入力]をクリックします。
23. [入力名]および[ワークフロー入力の作成]をクリックします。



24. 入力の追加ウィザードで、次の操作を行います。
    a. 表示名と参照名を指定します（オプション）。
    b. [必須]をクリックします。
    c. [デフォルト値の設定]と[オーバーライド*]をクリックします。
    d. データストアのデフォルト値を指定し、* Add *をクリックします。

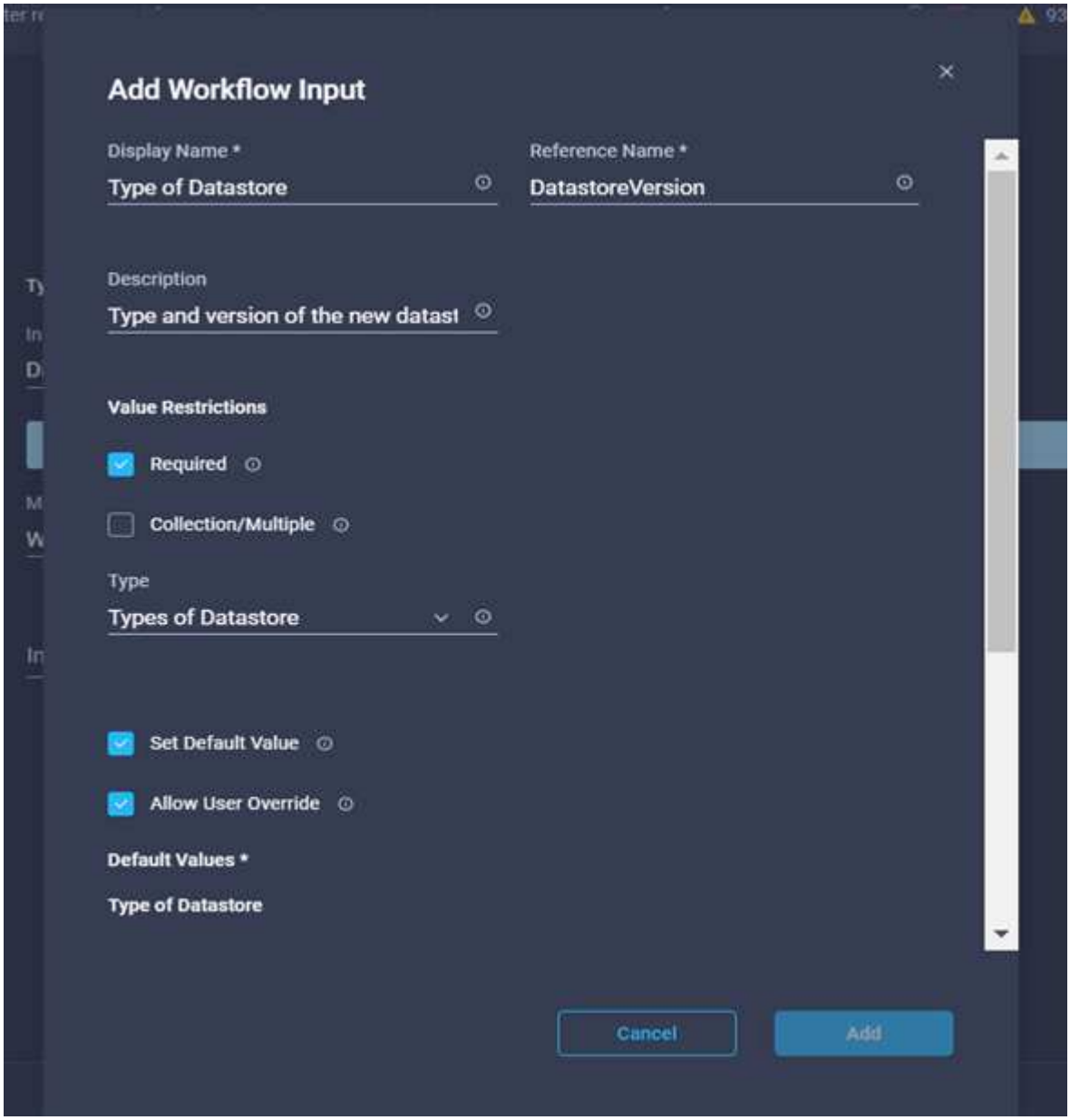


25. [マップ]をクリックします。
26. 入力フィールド*データストアのタイプ*で*マップ*をクリックします。
27. [直接マッピング]を選択し、[ワークフロー入力]をクリックします。
28. [入力名]および[ワークフロー入力の作成]をクリックします。



29. 入力の追加ウィザードで、次の手順を実行します。
    a. 表示名と参照名を入力し（オプション）、*必須*をクリックします。

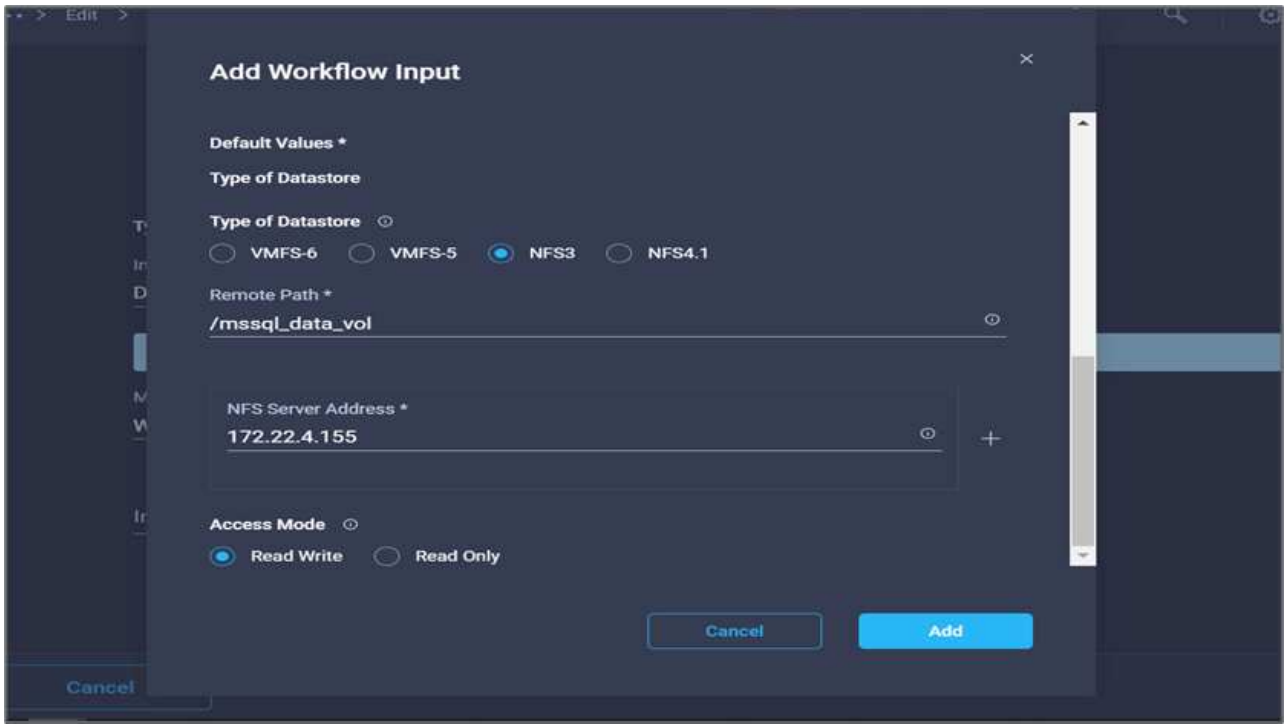
b. タイプ*タイプのデータストア*を選択し、*デフォルト値の設定と上書き*をクリックしてください。



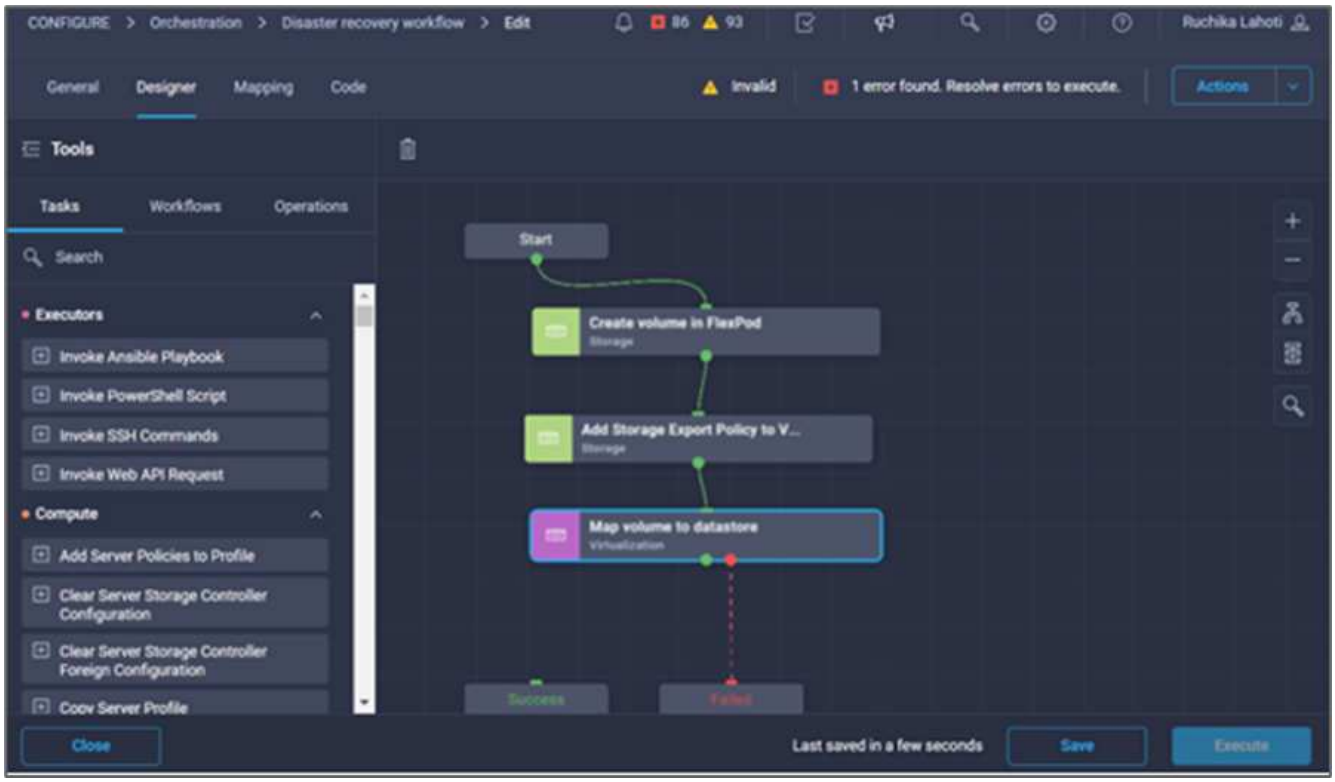
c. リモートパスを指定します。NFSマウントポイントのリモートパスです。

d. NFSサーバアドレスにリモートNFSサーバのホスト名またはIPアドレスを入力します。

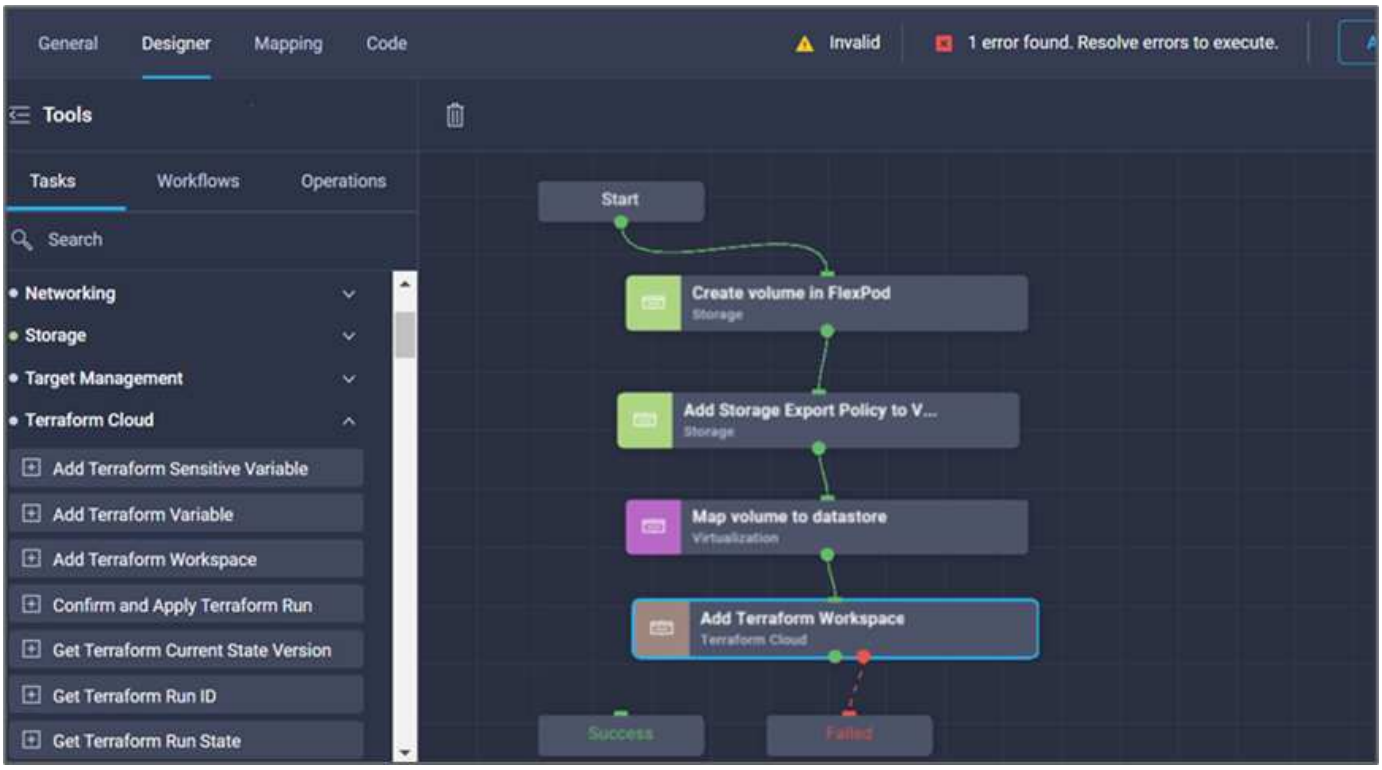
e. [アクセスモード*]をクリックします。アクセスモードはNFSサーバ用です。ボリュームが読み取り専用としてエクスポートされている場合は、[読み取り専用]をクリックします。[追加（ Add ）] をクリックします。



30. [マップ]をクリックします。
31. [保存（ Save ）] をクリックします。

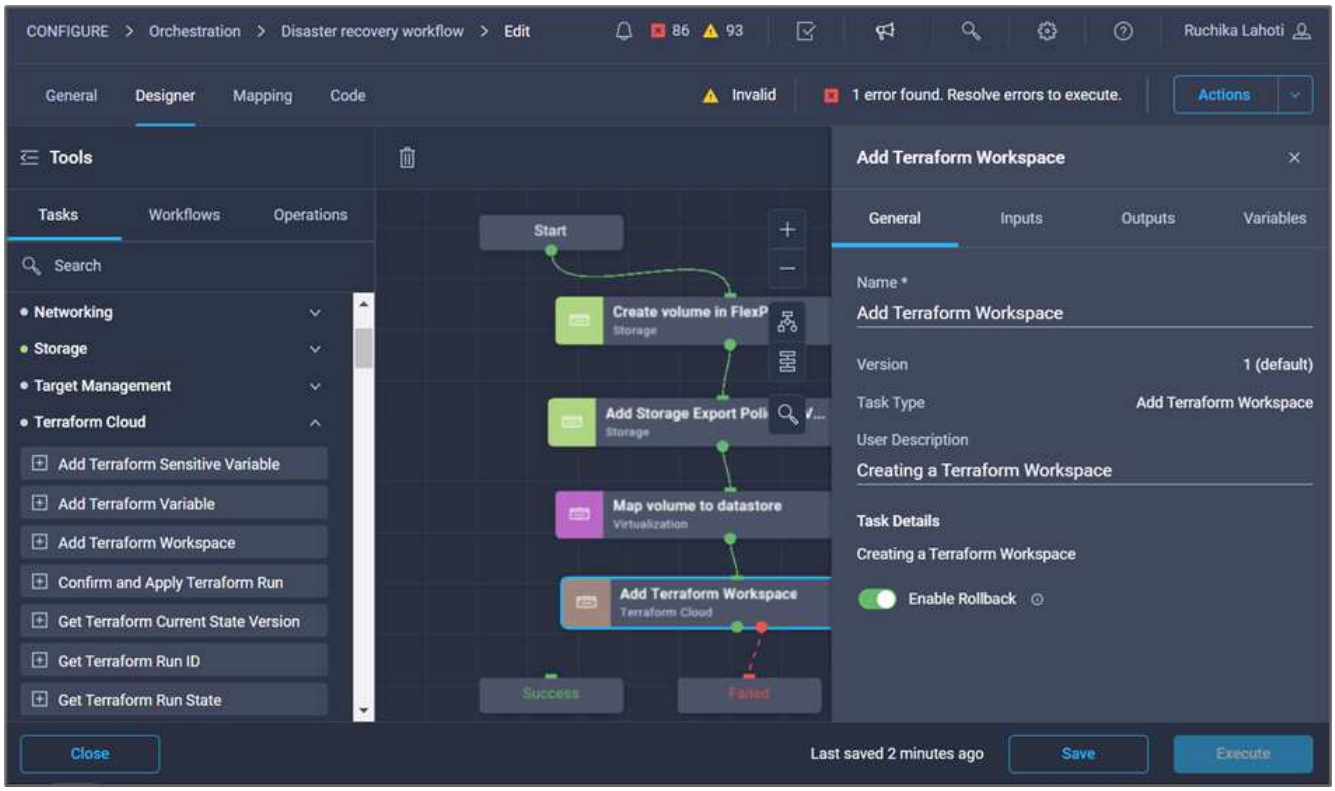


これでデータストアの作成は完了です。オンプレミスのFlexPod データセンターで実行されるすべてのタスクが完了します。

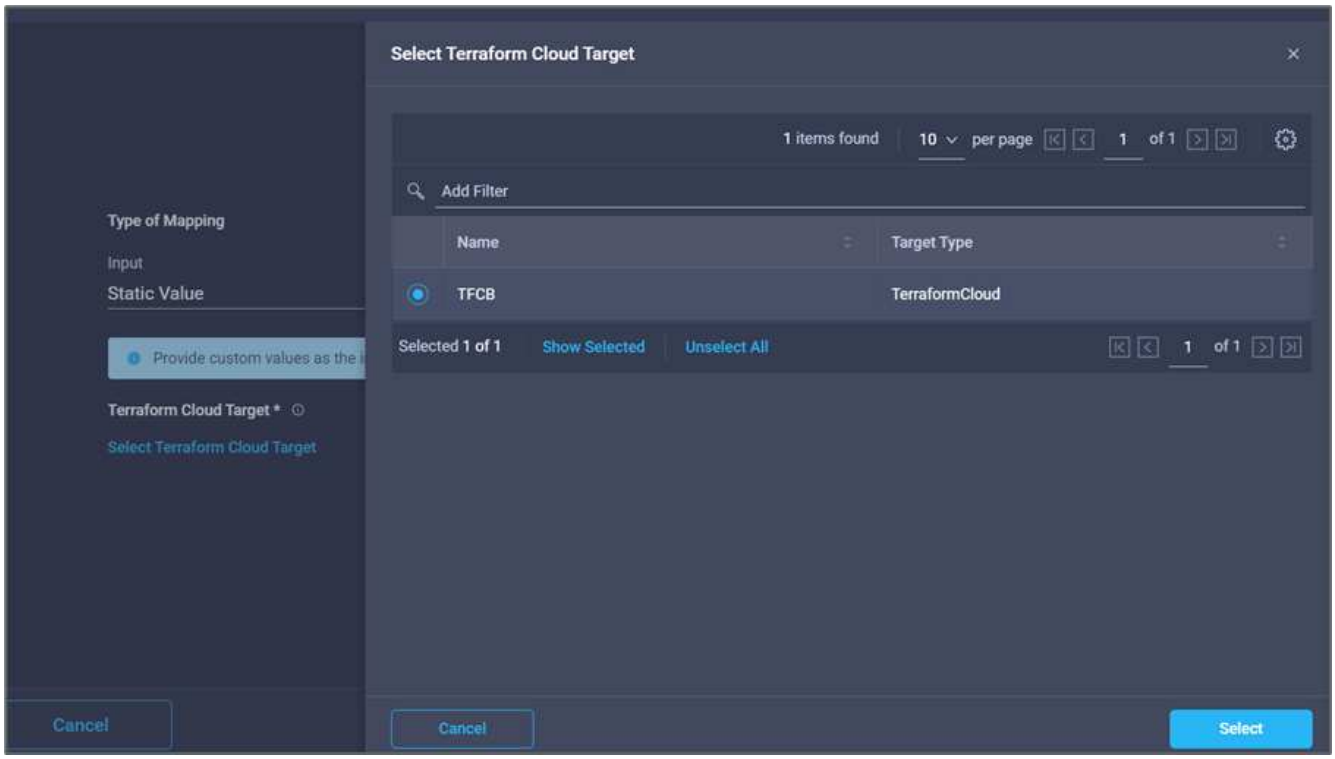


手順 **5:**新しい**Terraform**ワークスペースを追加します

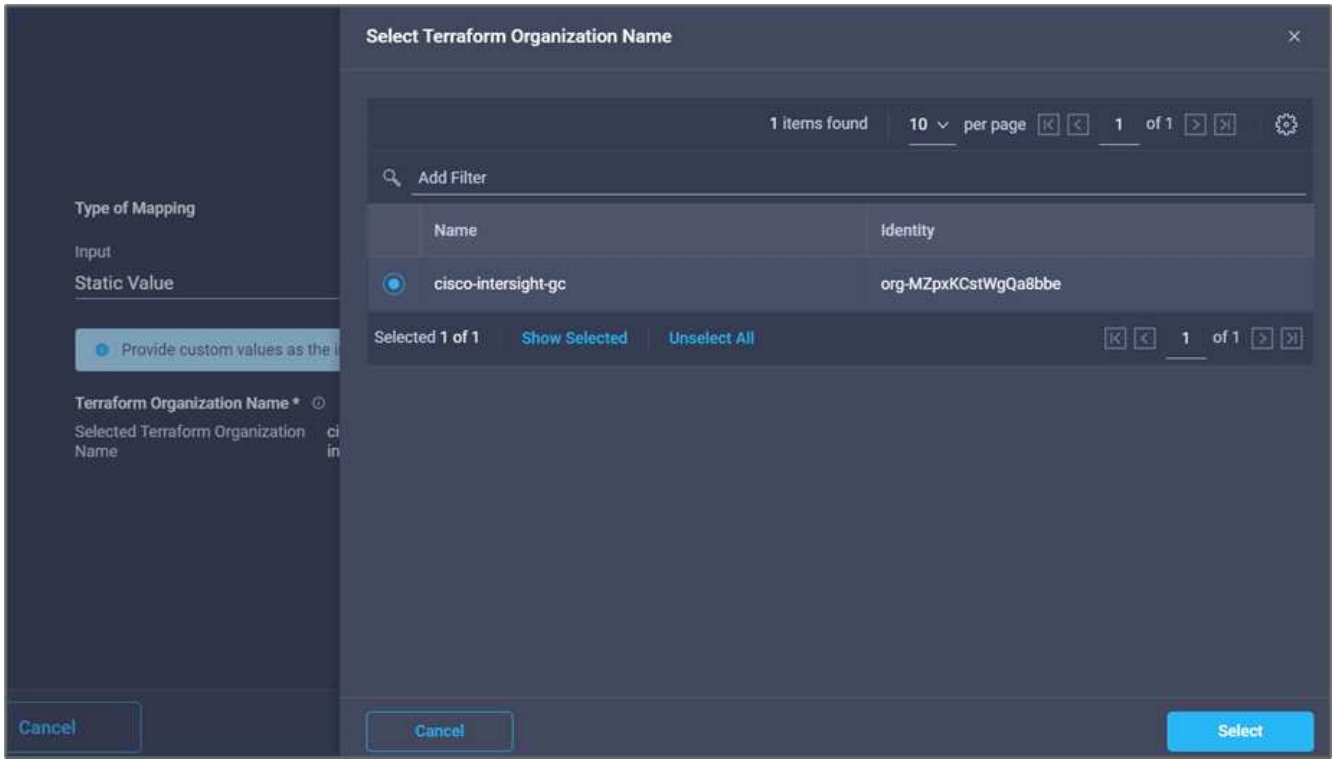
1. [*Designer]タブに移動し、[*Tools]セクションから[*Tasks]をクリックします。
2. [デザイン]領域の[ツール]セクションから、[*Terraform Cloud]>[Add Terraform Workspace]タスクをドラッグアンドドロップします。
3. コネクターを使用して、*マップボリュームをデータストア*に接続し、*テラフォームワークスペースの追加*タスクを実行し、*保存*をクリックします。
4. [**Add Terraform Workspace]**をクリックします。**[**タスクのプロパティ**]**領域で、**[**一般]タブをクリックします。必要に応じて、このタスクの名前と概要 を変更できます。



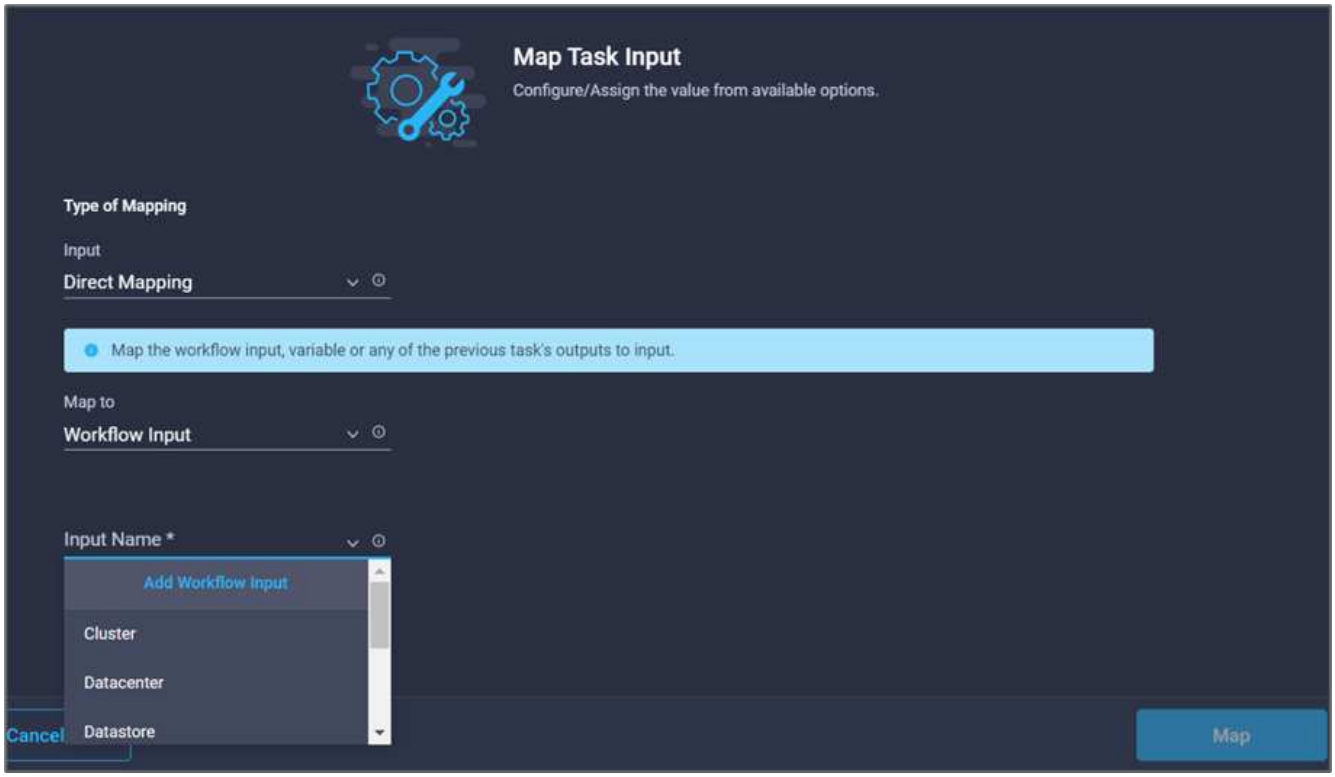
5. [タスクプロパティ]領域で、[入力]をクリックします。
6. 入力フィールド* Terraform Cloud Target で Map *をクリックします。
7. *静的値*を選択し、*テラフォームクラウドターゲットの選択*をクリックします。の説明に従って追加された、Terraform Cloud for Businessアカウントを選択します "Cisco Intersight Service for橋のTerraformを設定します"。」。



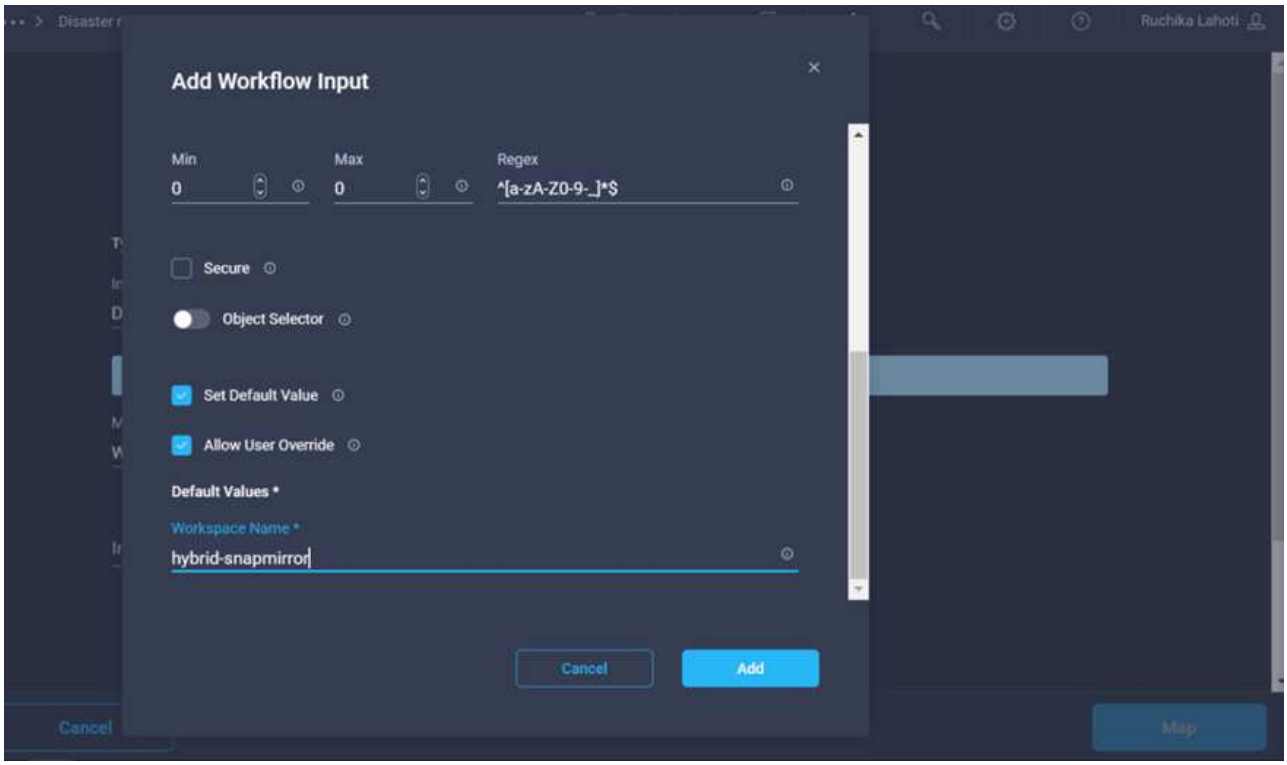
8. [マップ]をクリックします。
9. 入力フィールド*Terraform組織名*の*Map*をクリックします。
10. [静的値*]を選択し、[**Select Terraform Organization**]をクリックします。Terraform Cloud for Businessアカウントに含まれるTerraform Organizationの名前を選択します。



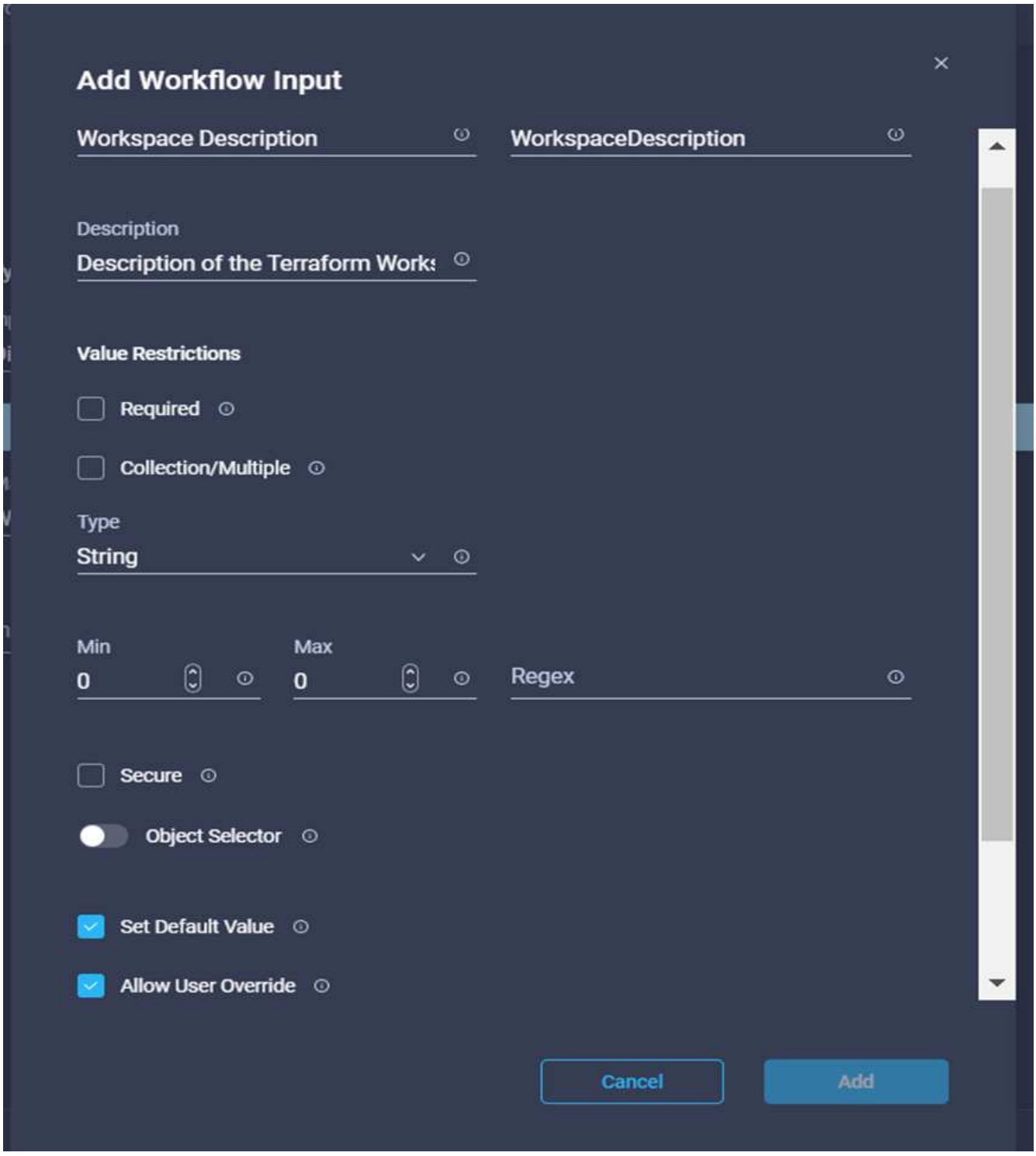
11. [マップ]をクリックします。
12. [**Terraform**ワークスペース名]フィールドの[**Map**]をクリックします。これは、Terraform Cloud for Businessアカウントの新しいワークスペースです。
13. [直接マッピング]を選択し、[ワークフロー入力]をクリックします。
14. [入力名]および[ワークフロー入力の作成]をクリックします。



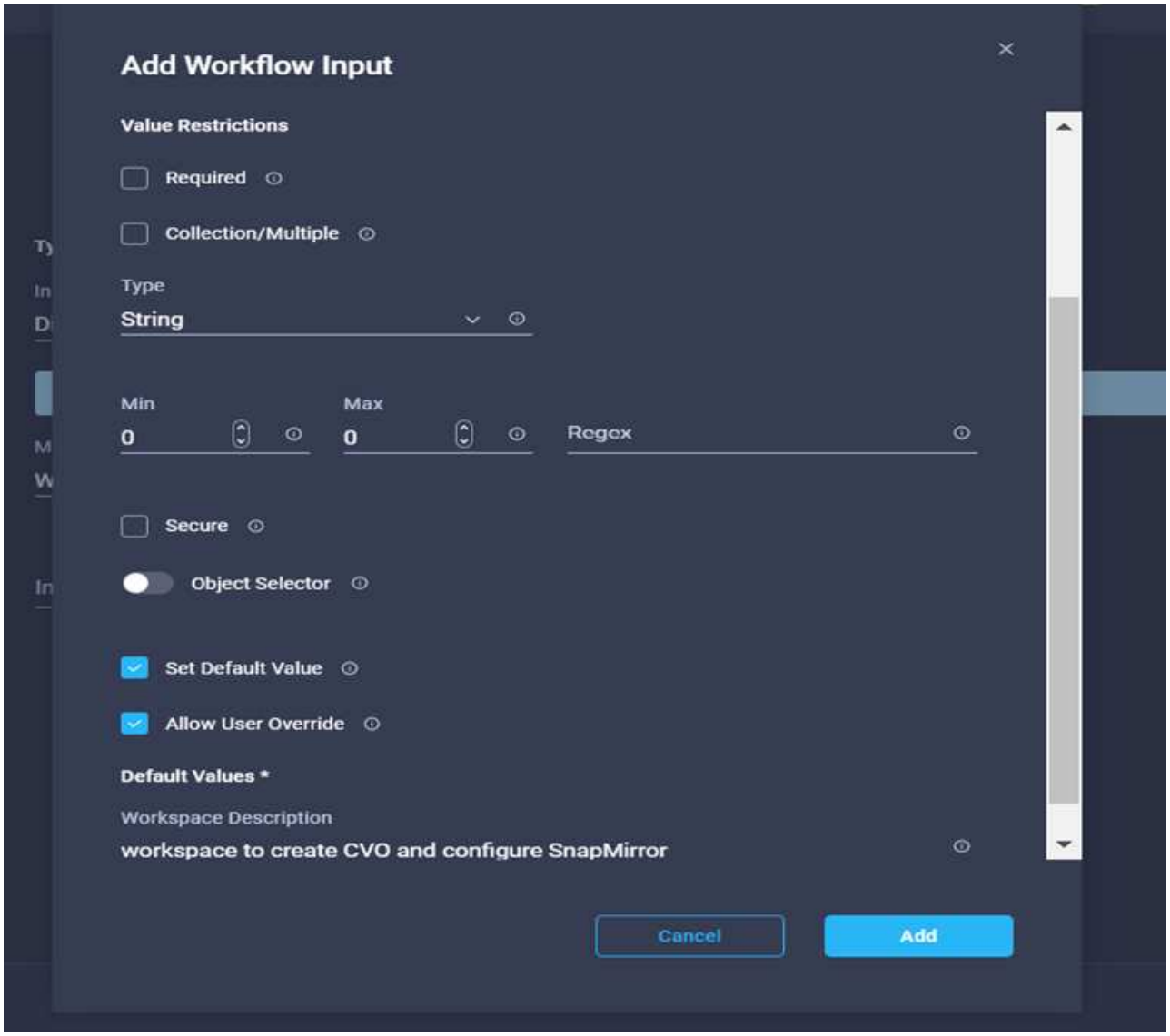
15. 入力の追加ウィザードで、次の手順を実行します。
    a. 表示名と参照名を指定します（オプション）。
    b. [必須]をクリックします。
    c. [タイプ（* Type）]に[文字列（* String）]を選択してください。
    d. [デフォルト値の設定]と[オーバーライド*]をクリックします。
    e. ワークスペースのデフォルト名を指定します。
    f. [追加（ Add ）] をクリックします。



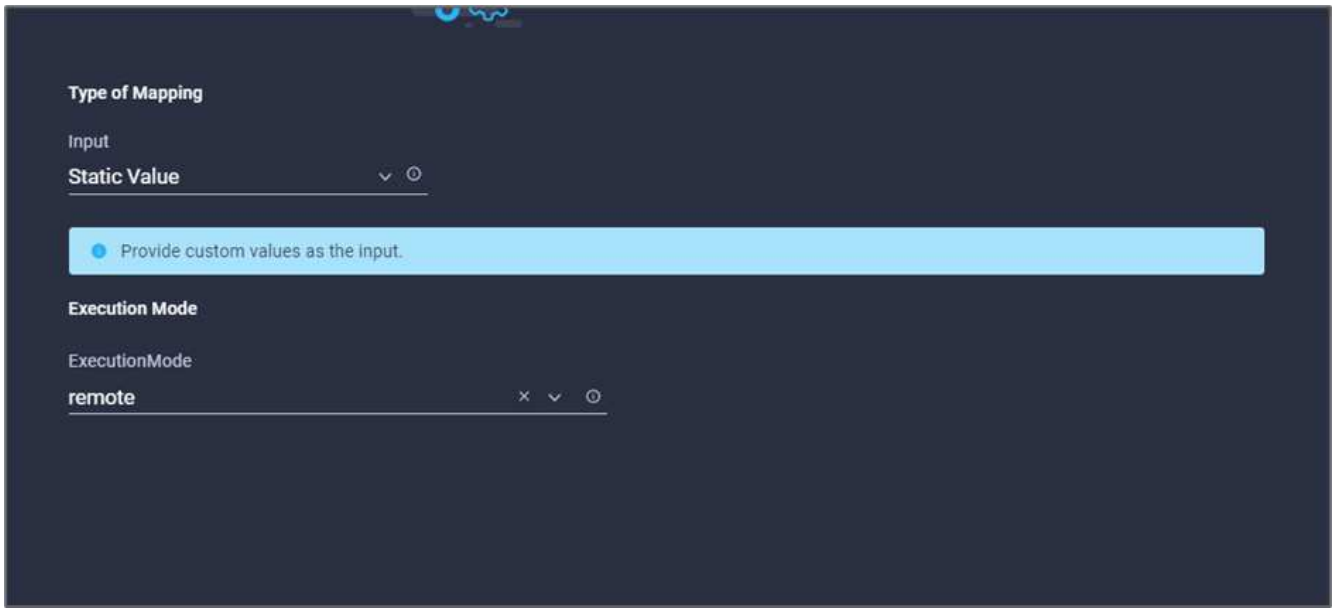
16. [マップ]をクリックします。
17. [* Workspace概要 （ワークスペースのマップ）]フィールドで[マップ]をクリックします。
18. [直接マッピング]を選択し、[ワークフロー入力]をクリックします。
19. [入力名]および[ワークフロー入力の作成]をクリックします。



20. 入力の追加ウィザードで、次の手順を実行します。
    a. 表示名と参照名を指定します（オプション）。
    b. [タイプ（* Type）]に[文字列（* String）]を選択してください。
    c. [デフォルト値の設定]と[オーバーライド*]をクリックします。
    d. ワークスペース概要 を提供し、*追加*をクリックします。



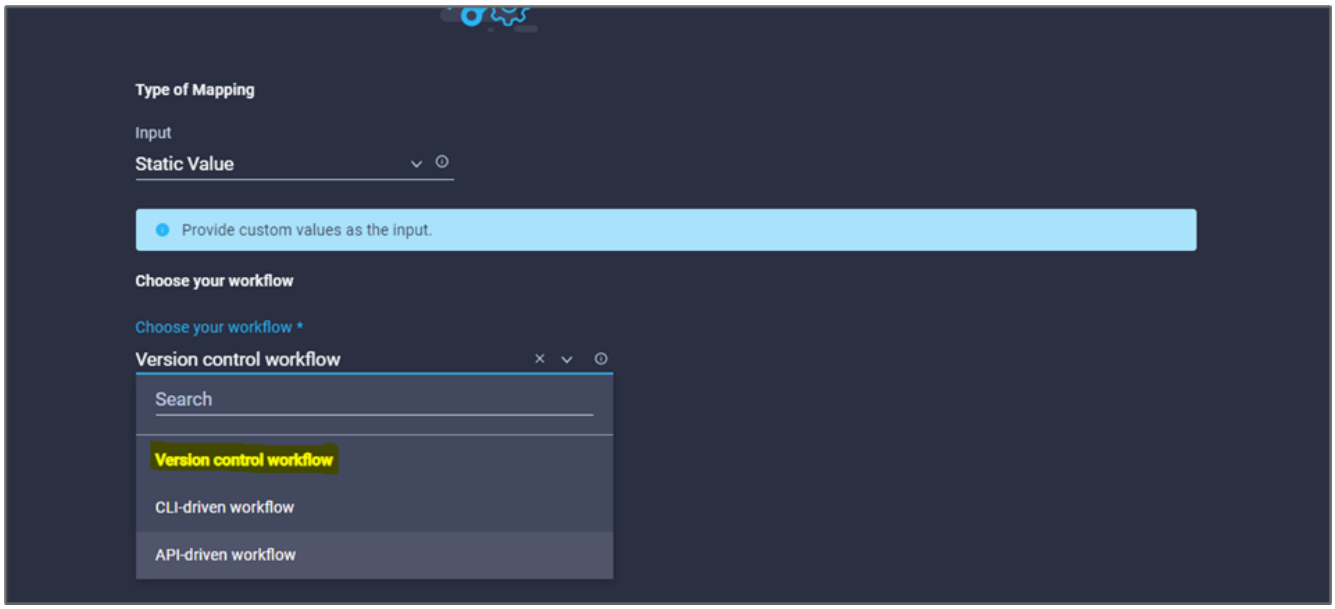
21. [マップ]をクリックします。
22. [実行モード*]フィールドの[マップ*]をクリックします。
23. *静的値*を選択し、*実行モード*をクリックして、*リモート*をクリックします。



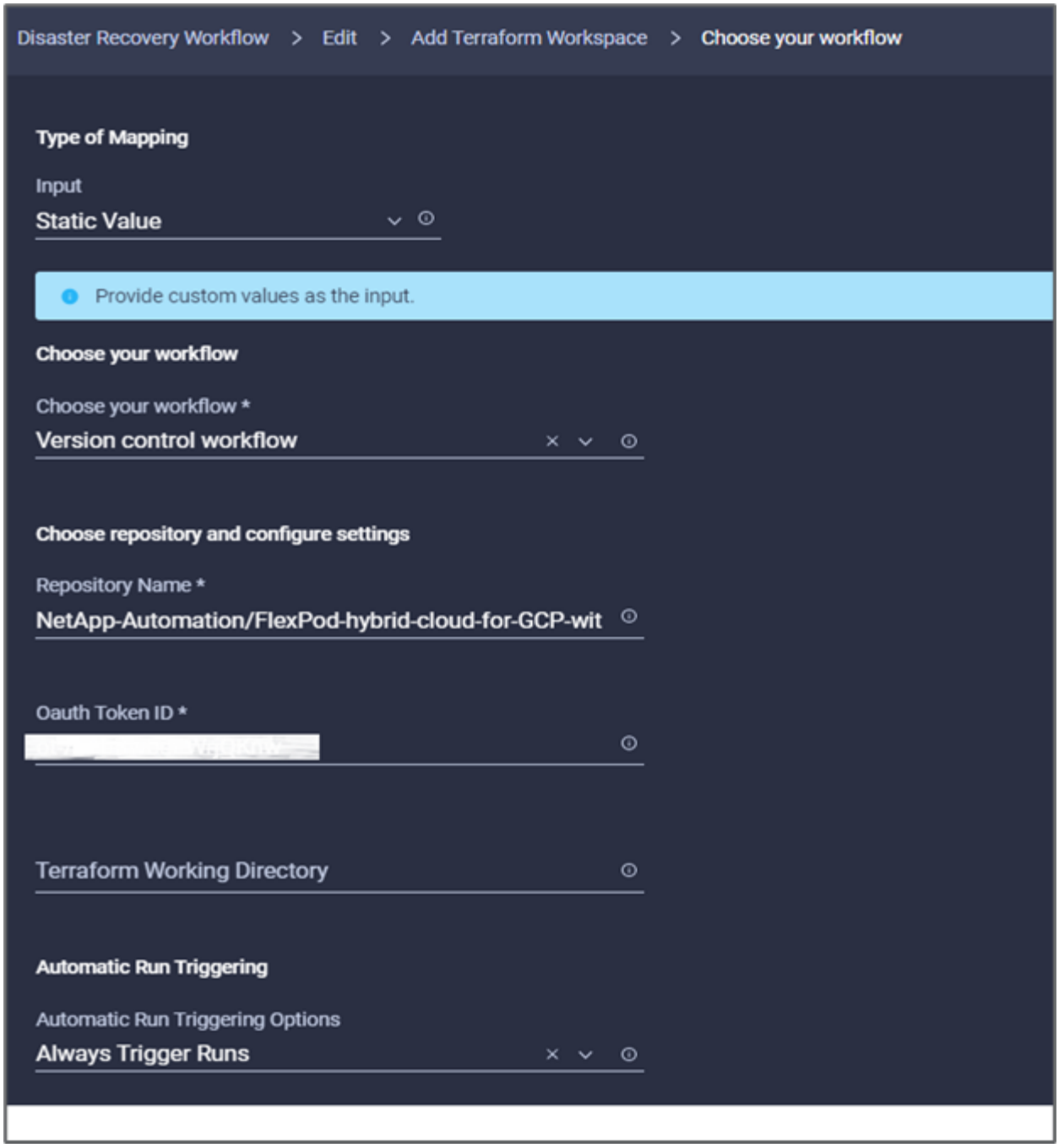
24. [マップ]をクリックします。
25. [メソッドの適用]フィールドで[マップ]をクリックします。
26. 「* Static Value 」を選択し、「 Apply Method *」をクリックします。*手動適用*をクリックします。

27. [マップ]をクリックします。
28. [ユーザーインタフェース]フィールドで[マップ]をクリックします。
29. 「* Static Value 」を選択し、「 User Interface 」をクリックします。**[***コンソール**UI**]をクリックします。

30. [マップ]をクリックします。
31. 入力フィールドで*マップ*をクリックし、ワークフローを選択します。
32. 「静的値」を選択し、「ワークフローの選択」をクリックします。[バージョン管理ワークフロー]をクリックします。



33. GitHubリポジトリについて、次の詳細情報を入力します。
    a. [リポジトリ名*]に'セクションで詳細に説明したリポジトリの名前を入力します "「環境の前提条件の設定」"。
    b. セクションの説明に従って、OAuthトークンIDを指定します "「環境の前提条件の設定」"。
    c. [自動実行トリガー（* Automatic Run Triggering）]オプションを選択します。



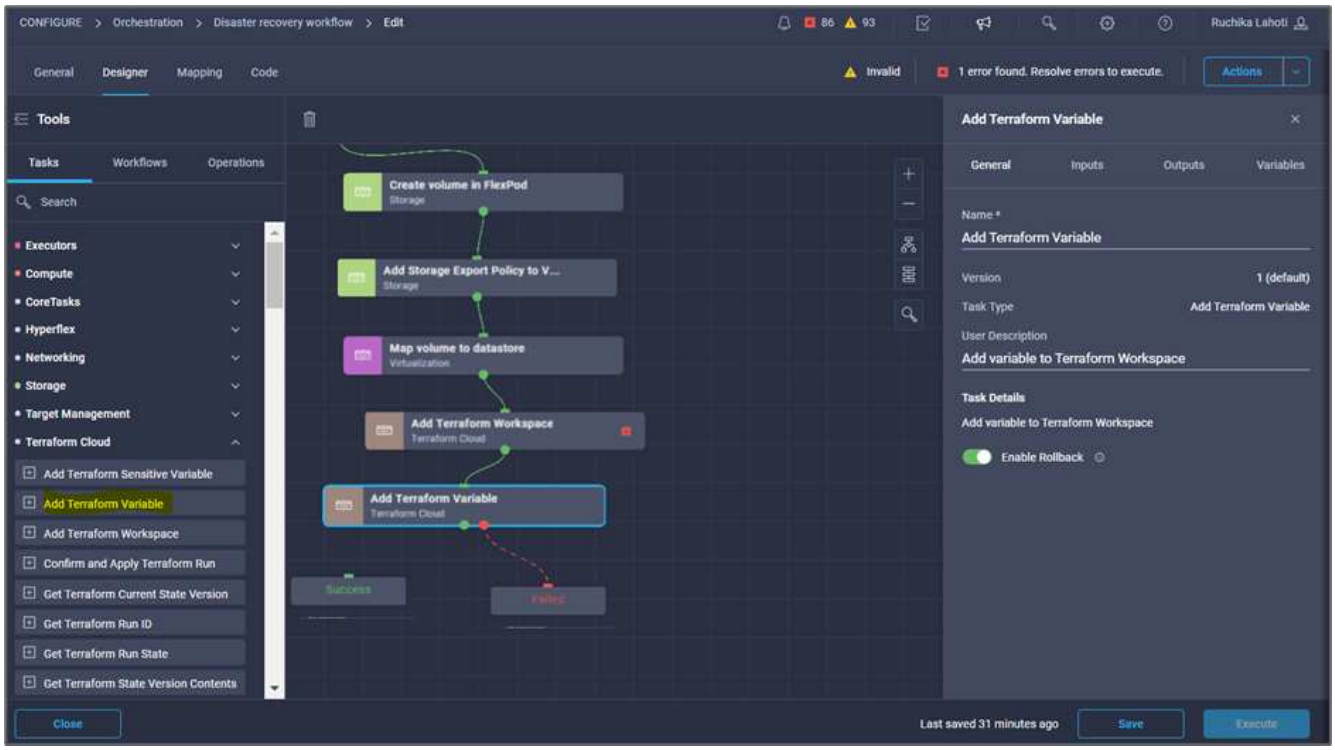
34. [マップ]をクリックします。
35. [保存（ Save ）] をクリックします。

これで、Terraform Cloud for Businessアカウントでワークスペースを作成するタスクは完了です。

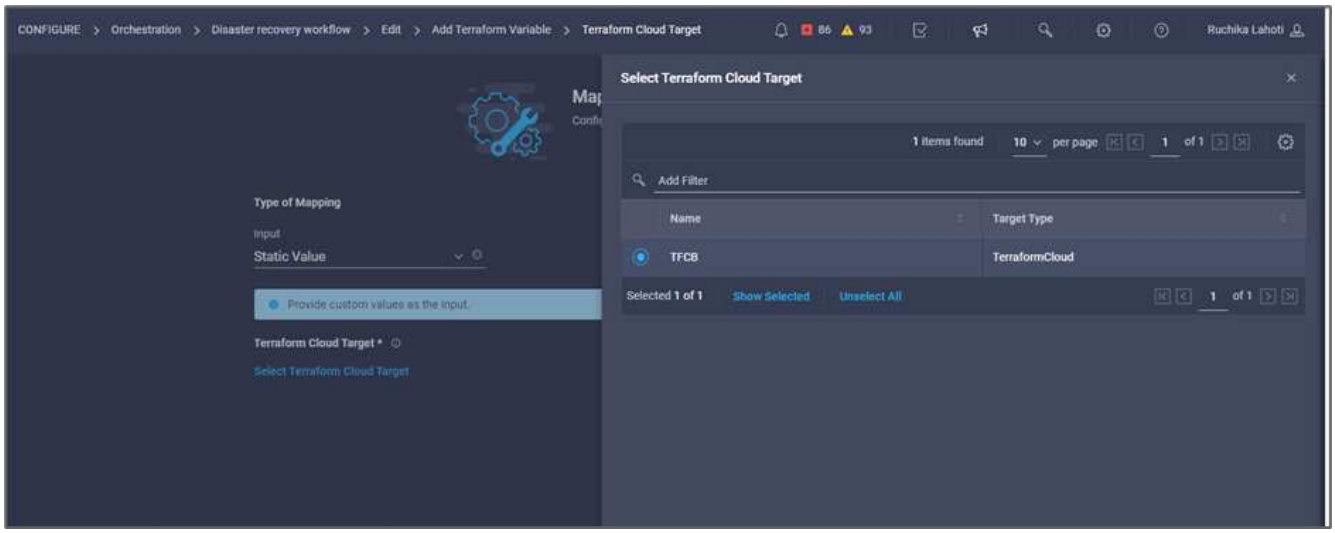
手順 **6**：ワークスペースに非機密変数を追加します

1. **[Designer]**タブに移動し、**[**ツールからのワークフロー]セクションをクリックします。
2. [**Design**]領域の[**Tools**]セクションから、[**Terraform]>[Add Terraform Variables**]ワークフローをドラッグアンドドロップします。
3. コネクターを使用して、*テラフォームワークスペースの追加*および*テラフォーム変数の追加*タスクを接続します。[保存（ Save ）] をクリックします。

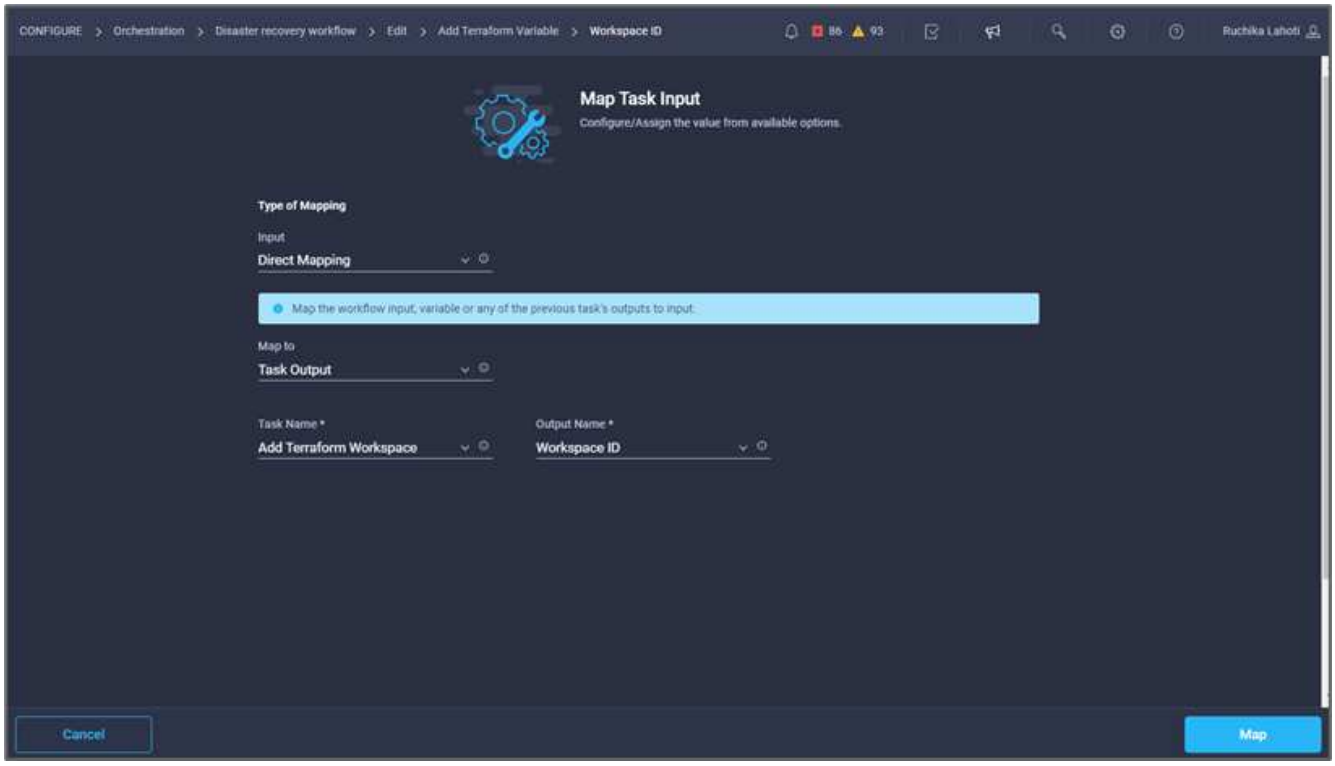
4. [**Add Terraform Variables**]をクリックします。[ワークフローのプロパティ*]領域で、[一般*]タブをクリックします。必要に応じて、このタスクの名前と概要 を変更できます。



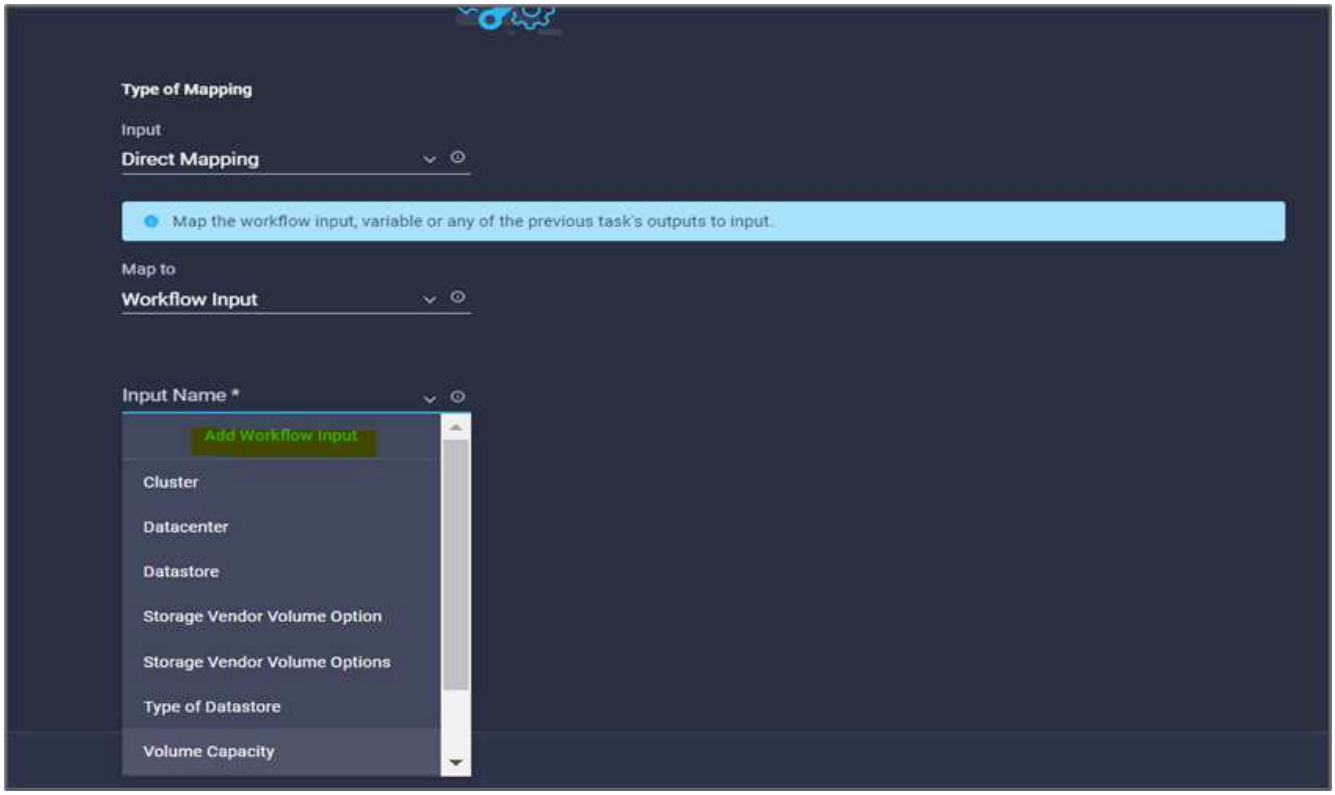
5. [ワークフロープロパティ]領域で、[入力]をクリックします。
6. [**Terraform Cloud Target**]フィールドの[**Map**]をクリックします。
7. *静的値*を選択し、*テラフォームクラウドターゲットの選択*をクリックします。の説明に従って追加された、Terraform Cloud for Businessアカウントを選択します "Cisco Intersight Service for橋のTerraformを設定します"。」。



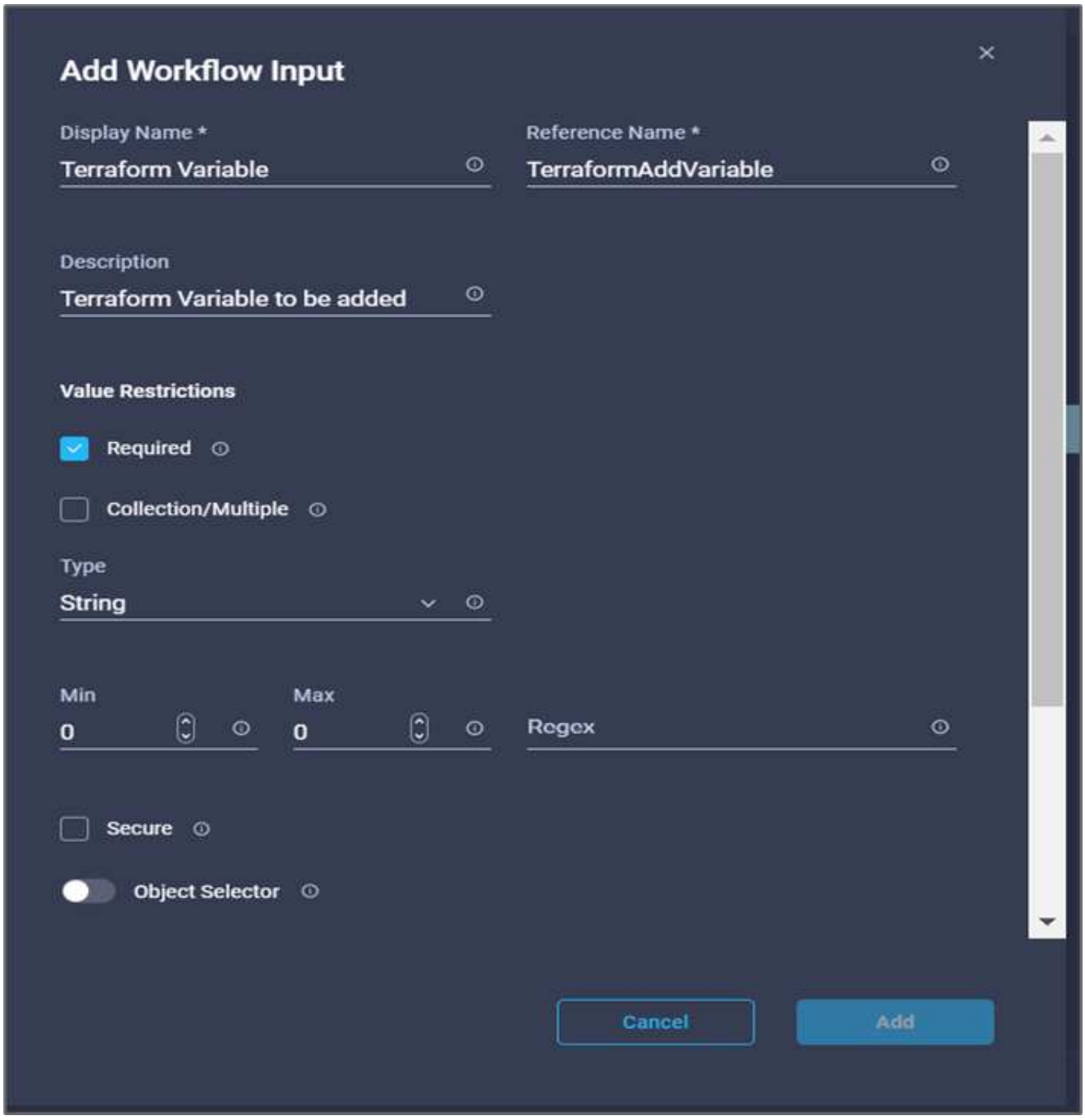
8. [マップ]をクリックします。
9. [**Terraform Organization Name**]フィールドの[**Map**]をクリックします。
10. 「静的値」を選択し、「テラフォームの組織を選択」をクリックします。Terraform Cloud for Businessアカウントに含まれるTerraform Organizationの名前を選択します。



11. [マップ]をクリックします。
12. [**Terraform**ワークスペース名]フィールドの[**Map**]をクリックします。
13. [直接マッピング]を選択し、[タスク出力]をクリックします。
14. タスク名*をクリックし、*テラフォームワークスペースの追加*をクリックします。



15. 出力名*をクリックし、*ワークスペース名*をクリックします。
16. [マップ]をクリックします。
17. [変数オプションの追加*]フィールドで[**Map**]をクリックします。
18. [直接マッピング]を選択し、[ワークフロー入力]をクリックします。
19. [入力名]および[ワークフロー入力の作成]をクリックします。



20. 入力の追加ウィザードで、次の手順を実行します。
    a. 表示名と参照名を指定します（オプション）。
    b. [タイプ（* Type）]に[文字列（ String）]を選択してください。

c. [デフォルト値の設定]と[オーバーライド*]をクリックします。

d. 変数タイプ*をクリックし、*非機密変数*をクリックします。

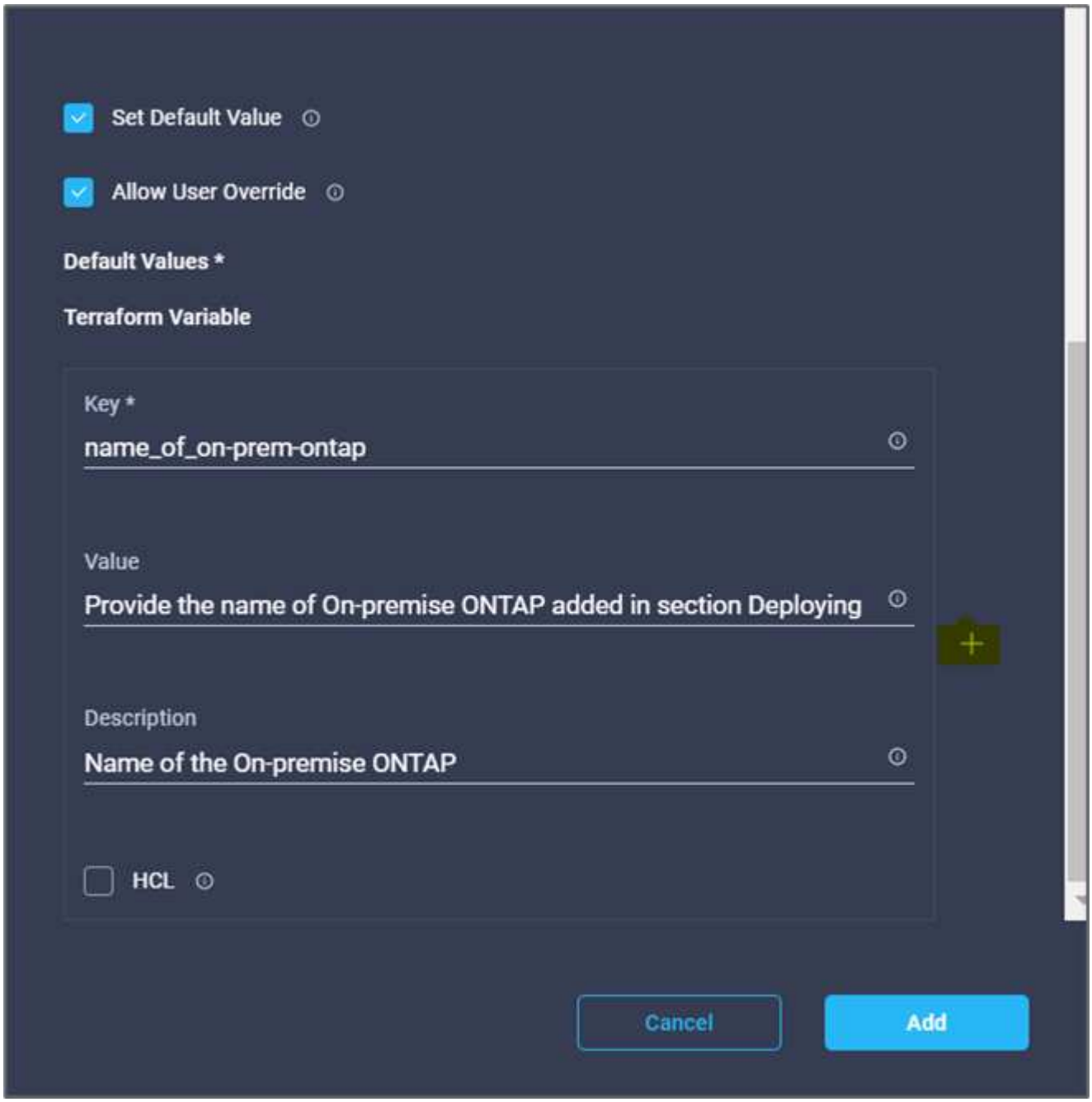
21. [**Add Terraform Variables**]セクションで、次の情報を入力します。

   ◦ * Key.*'name_OF_OF_OLIプレ ミス-ONTAP'

   ◦ *値。*オンプレミスONTAP の名前を指定します。

   ◦ *概要 。*オンプレミスONTAP の名前。

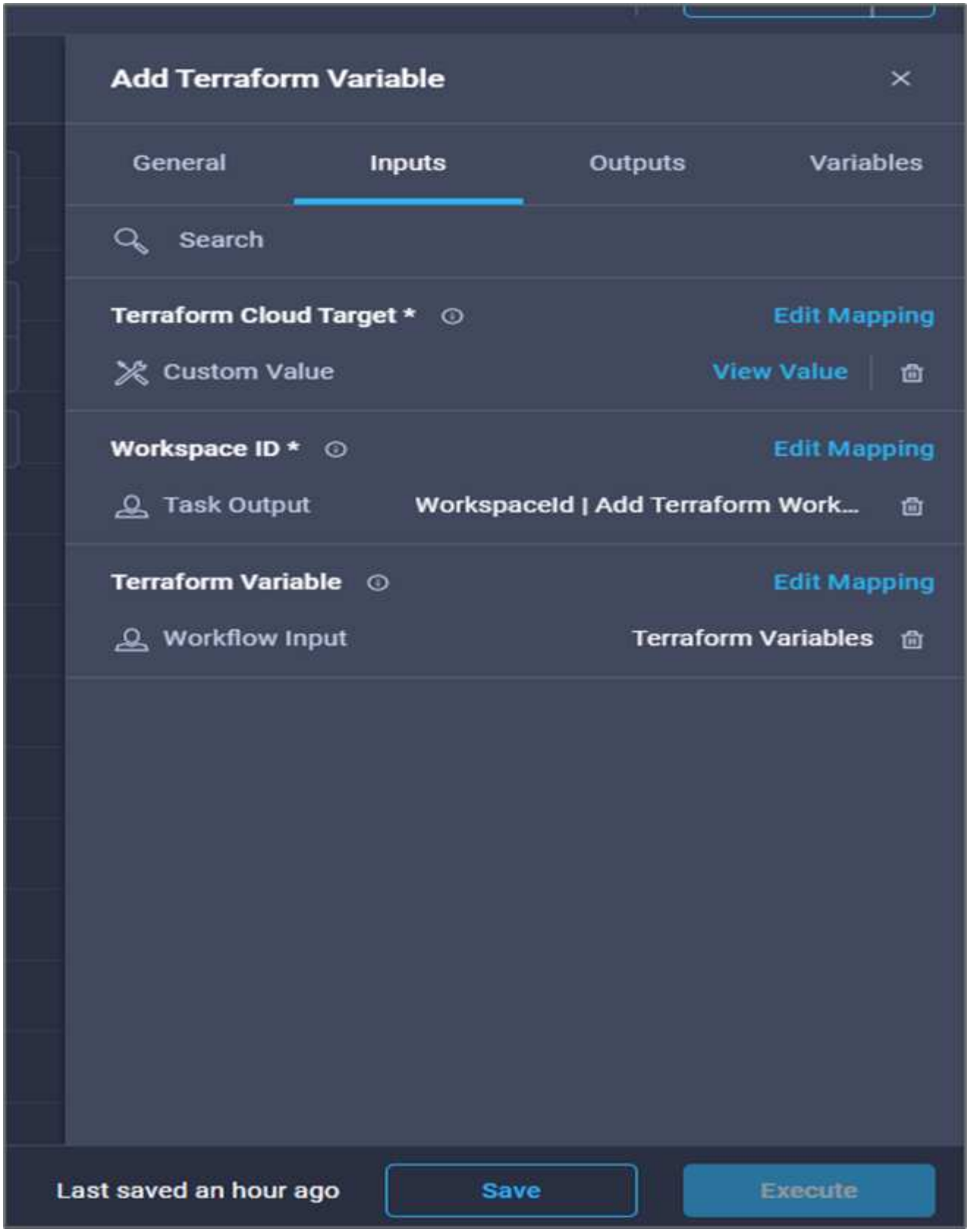
22. 追加の変数を追加するには、*+*をクリックします。



23. 次の表に示すように、すべてのTerraform変数を追加します。デフォルト値を指定することもできます。

Terraform変数名	説明
名前オンプレミス- ONTAP	オンプレミスONTAP （FlexPod ）の名前
オンプレミス- ONTAP_cluster_IP	ストレージクラスタ管理インターフェイスのIPアドレスです
オンプレミス- ONTAP_user_name	ストレージクラスタの管理ユーザ名
ゾーン	作業環境を作成するGCPリージョン
subnet_idの値	作業環境を作成するGCPサブネットID
vPC_id	作業環境を作成するVPC ID
capacity_package_nameのようになりました	使用するライセンスのタイプ
source_volumeを指定します	ソースボリュームの名前
source_storage_vm_name	ソースSVMの名前
destination_volumeに指定します	Cloud Volumes ONTAP 上のボリュームの名前
レプリケーションのスケジュール	デフォルトは1時間です
name_OF_VOLUME _TO _CREATE _on_CVO	クラウドボリュームの名前
Workspace_idをクリックします	作業環境を作成するワークスペースID
project_idに割り当てられます	作業環境を作成するproject_id
名前_OF_CVO-cluster	Cloud Volumes ONTAP 作業環境の名前
GCP_SERVICE_ACCOUNT	Cloud Volumes ONTAP 作業環境のGCP_SERVICE_ACCOUNT

24. [マップ]、[保存]の順にクリックします。



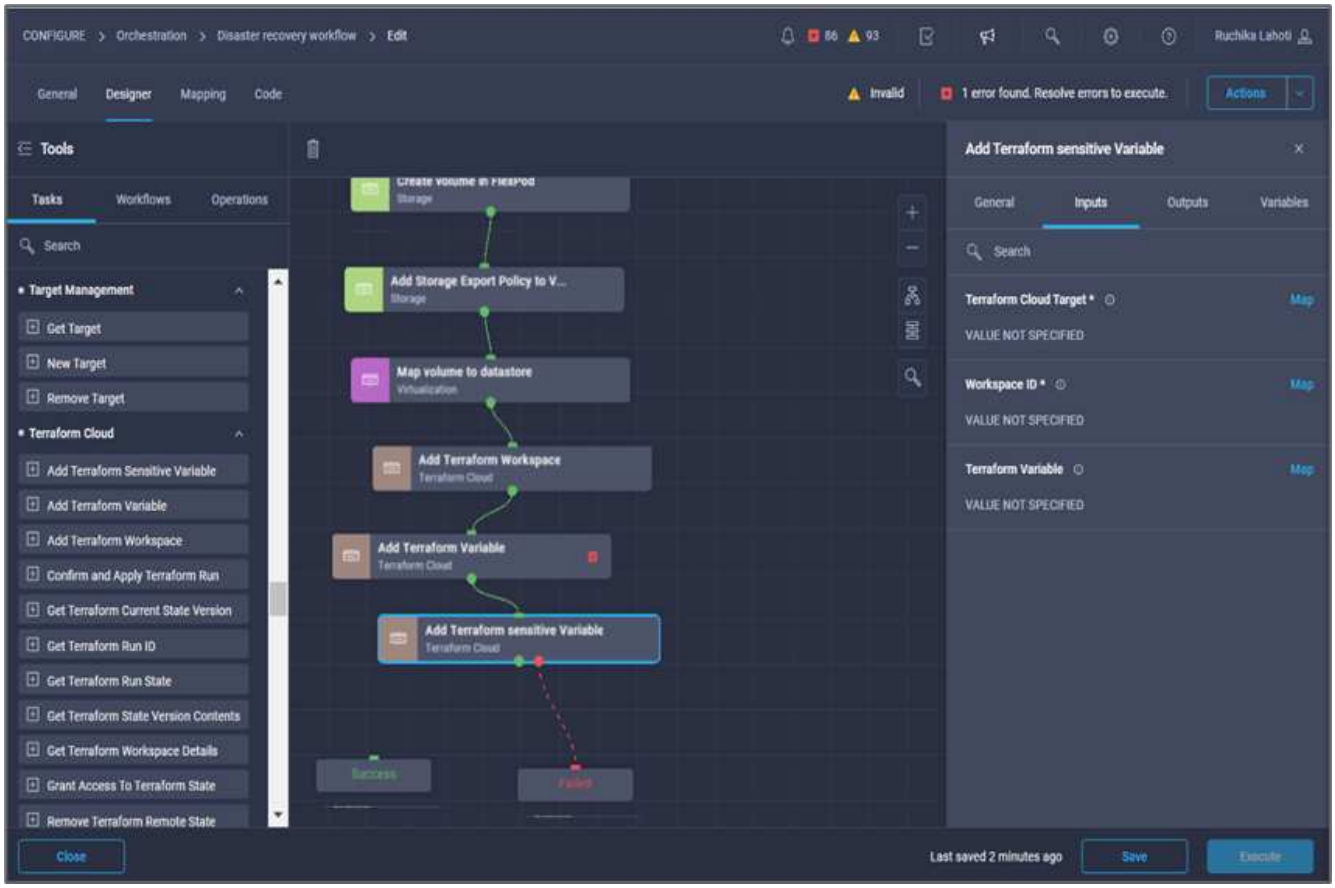
これで、必要なTerraform変数をワークスペースに追加する作業は完了です。次に、必要なセンシティブTerraform変数をワークスペースに追加します。両方を1つのタスクに組み合わせることもできます。

手順 **7:**ワークスペースに機密変数を追加します

1. [*Designer]タブに移動し、[*Tools]セクションから[*Workflows]をクリックします。
2. [**Design**]領域の[**Tools**]セクションから、[**Terraform]>[Add Terraform Variables**]ワークフローをドラッグアンドドロップします。
3. コネクターを使用して、2つの*テラフォームワークスペースの追加*タスクを接続します。[保存（ Save ）] をクリックします。

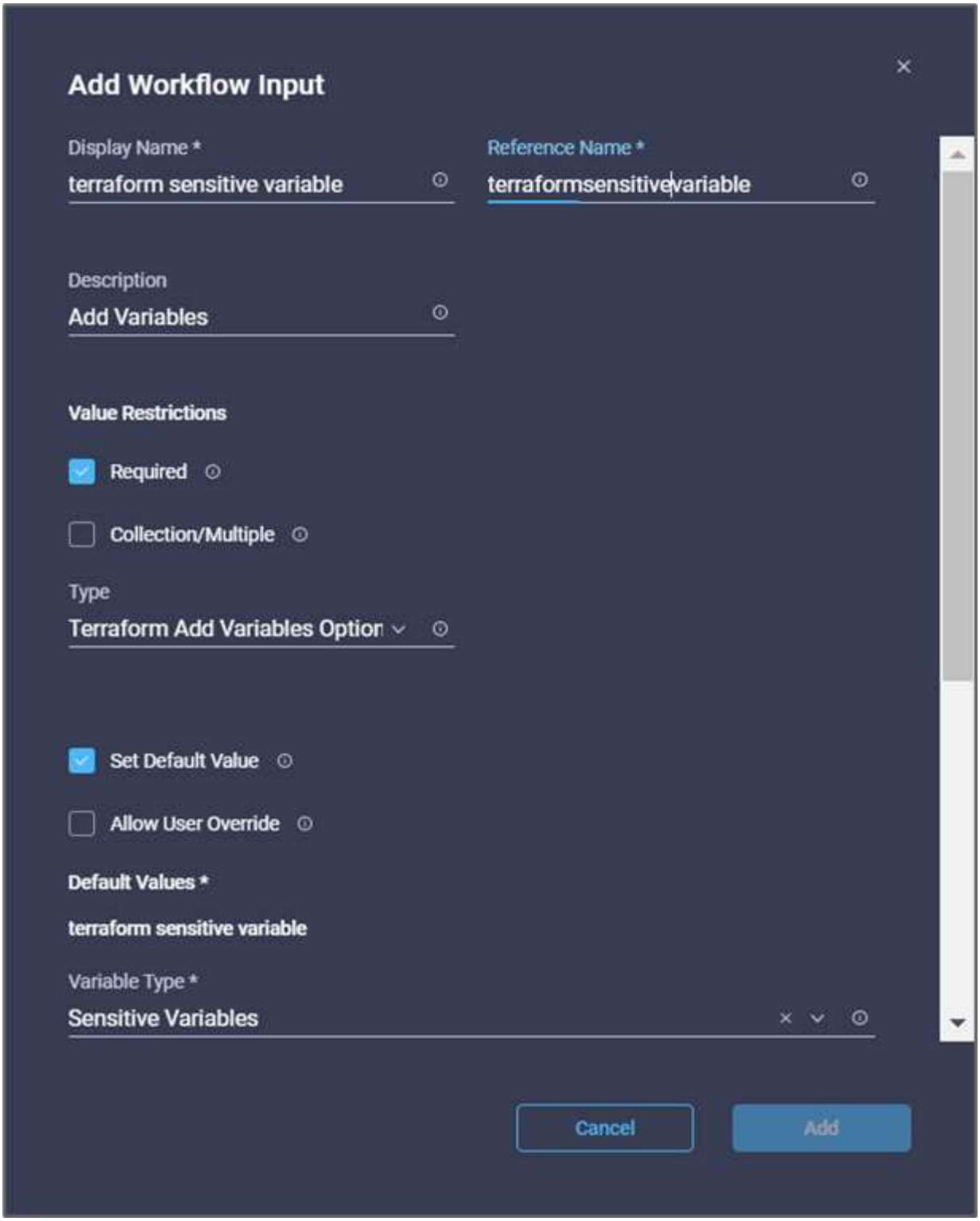
   2つのタスクの名前が同じであることを示す警告が表示されます。次の手順でタスク名を変更したため、エラーは無視してください。

4. [**Add Terraform Variables**]をクリックします。[ワークフローのプロパティ*]領域で、[一般*]タブをクリックします。名前を*Add Terraform Sensitive Variables*に変更します。



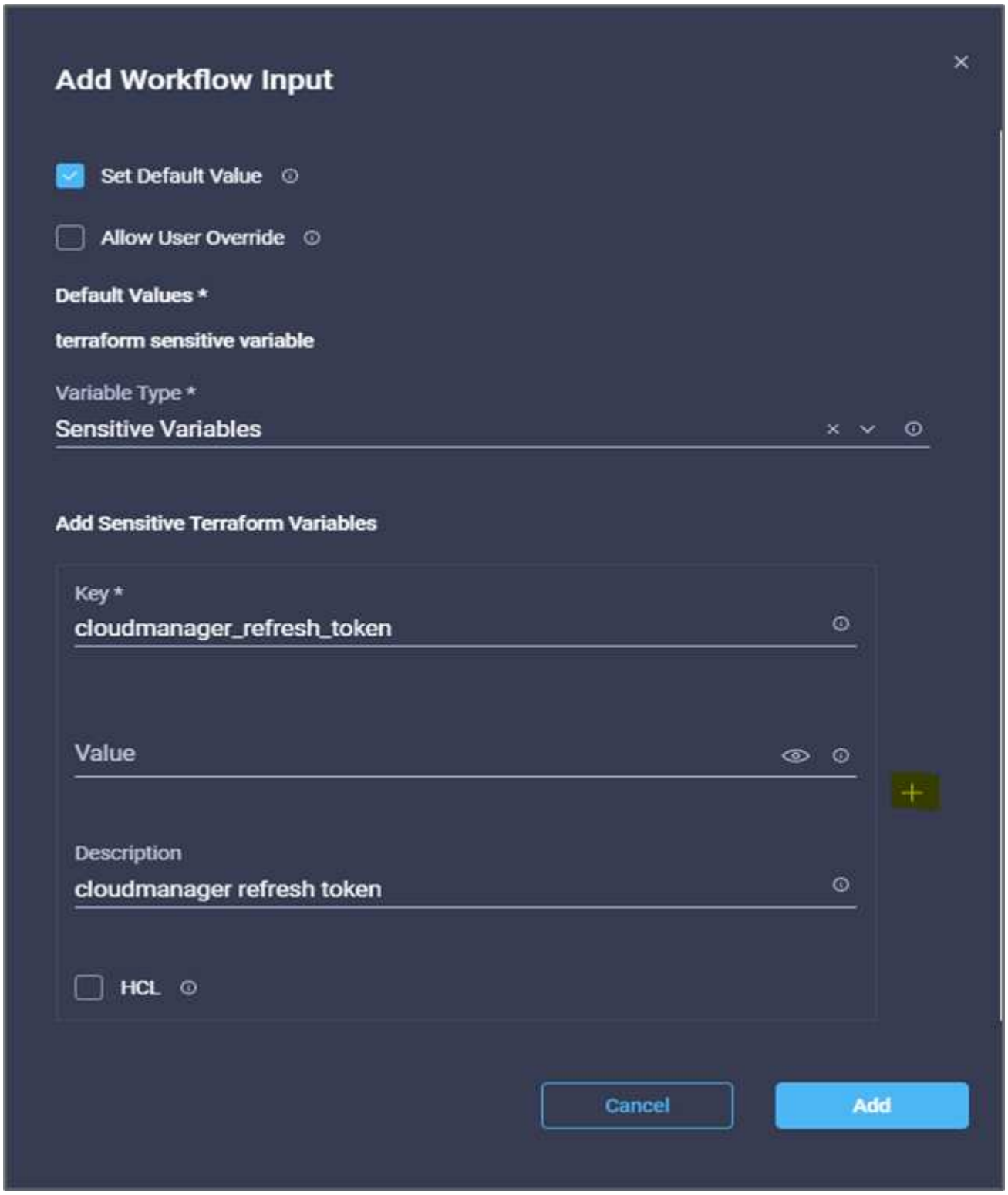
5. [ワークフロープロパティ]領域で、[入力]をクリックします。
6. [**Terraform Cloud Target**]フィールドの[**Map**]をクリックします。
7. *静的値*を選択し、*テラフォームクラウドターゲットの選択*をクリックします。セクションに追加されたTerraform Cloud for Businessアカウントを選択します "Cisco Intersight Service for橋のTerraformを設定します"」
8. [マップ]をクリックします。
9. [**Terraform Organization Name**]フィールドの[**Map**]をクリックします。
10. 「静的値」を選択し、「テラフォームの組織を選択」をクリックします。Terraform Cloud for Businessアカウントに含まれるTerraform Organizationの名前を選択します。

11. [マップ]をクリックします。
12. [**Terraform**ワークスペース名]フィールドの[**Map**]をクリックします。
13. [直接マッピング]を選択し、[タスク出力]をクリックします。
14. [タスク名*]をクリックし、[**Add Terraform Workspace**]をクリックします。
15. 出力名*をクリックし、出力*ワークスペース名*をクリックします。
16. [マップ]をクリックします。
17. [変数オプションの追加*]フィールドで[**Map**]をクリックします。
18. [直接マッピング]を選択し、[ワークフロー入力]をクリックします。
19. [入力名]および[ワークフロー入力の作成]をクリックします。
20. 入力の追加ウィザードで、次の手順を実行します。
    a. 表示名と参照名を指定します（オプション）。
    b. タイプには必ず* Terraform「変数オプションを追加」*を選択してください。
    c. *デフォルト値の設定*をクリックします。
    d. [変数の種類*]をクリックし、[変数の影響を受ける変数]をクリックします。
    e. [追加（ Add ）] をクリックします。



21. [**Add Terraform Variables**]セクションで、次の情報を入力します。
    - * Key.*`cloudmanager_refresh_ctoken`.
    - 値。 NetApp Cloud Manager API処理の更新トークンを入力します。
    - *概要 。*リフレッシュトークン。

NetApp Cloud Manager API処理用の更新トークンの取得方法の詳細については、セクションを参照してください "「環境の前提条件を設定する」"



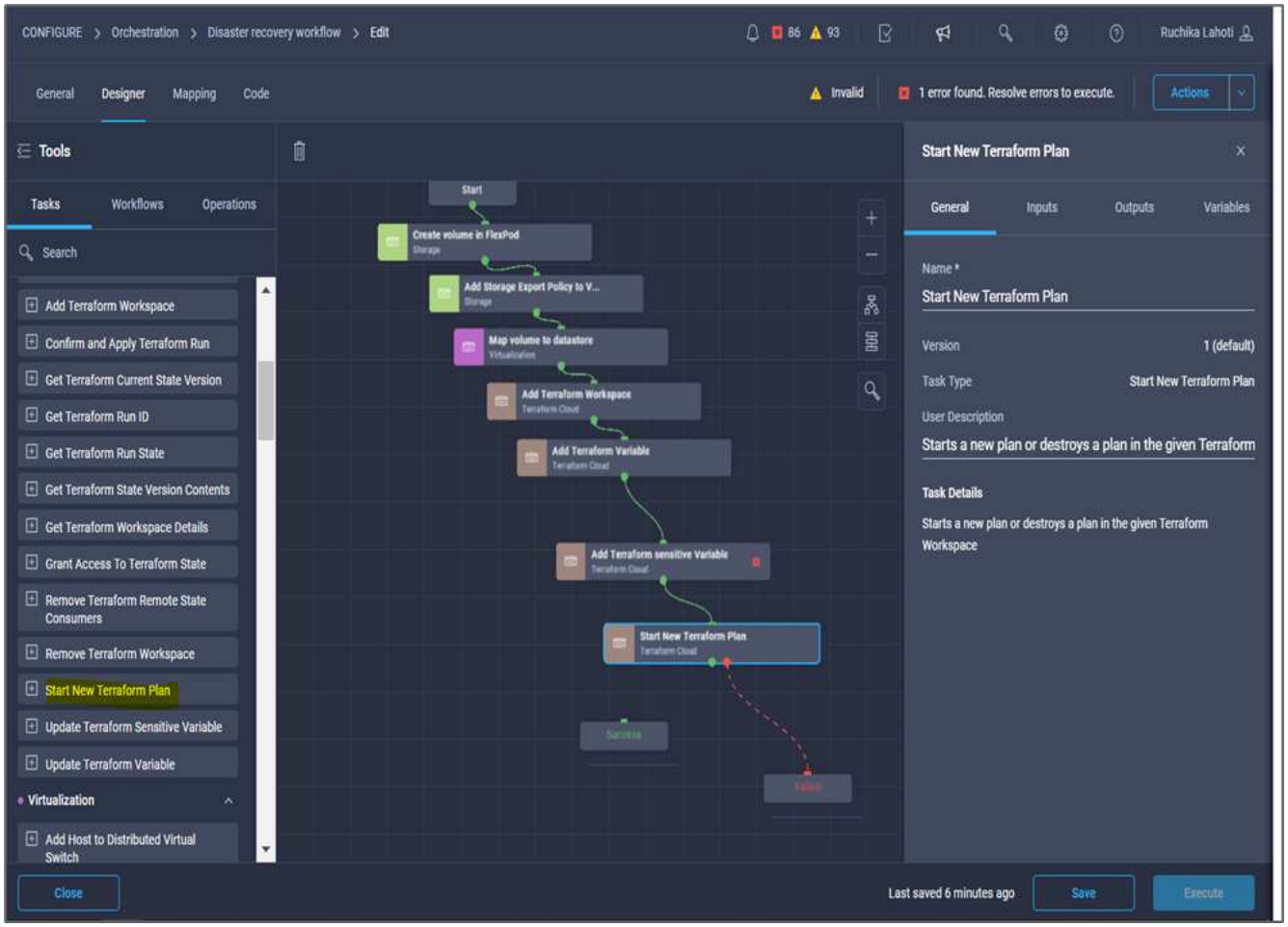
22. 次の表に示すように、すべてのTerraform機密変数を追加します。デフォルト値を指定することもできます。

Terraformの変数名	説明
cloudmanager_refresh_ctoken	トークンをリフレッシュします。次の場所から入手してください。
connector_id	Cloud Manager ConnectorのクライアントID。から入手します
CVO-admin_passwordのように入力します	Cloud Volumes ONTAP の管理パスワード
オンプレミス- ONTAP_user_password	ストレージクラスタの管理パスワード

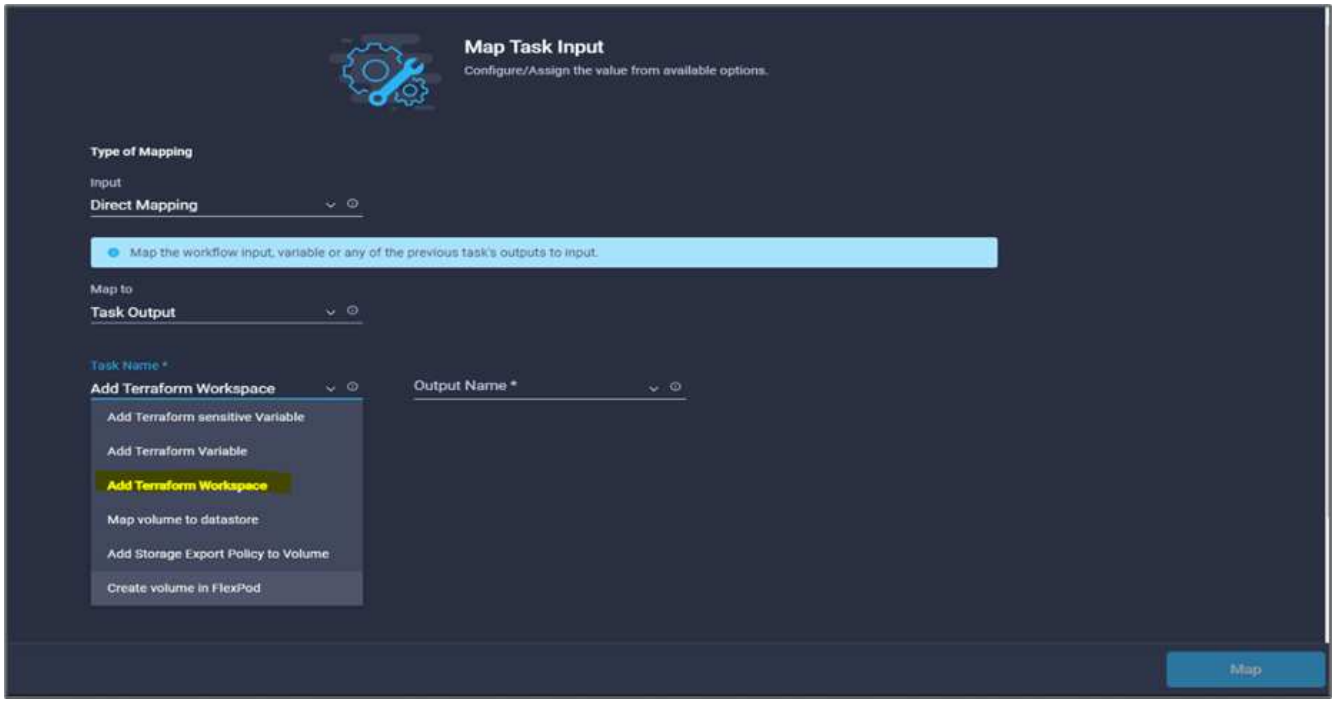
23. [**Map**]をクリックします。これで、必要なTerraformの機密変数をワークスペースに追加するタスクが完了します。次に、設定したワークスペースで新しいTerraformプランを開始します。

手順 **8:**新しい**Terraform**計画を開始します

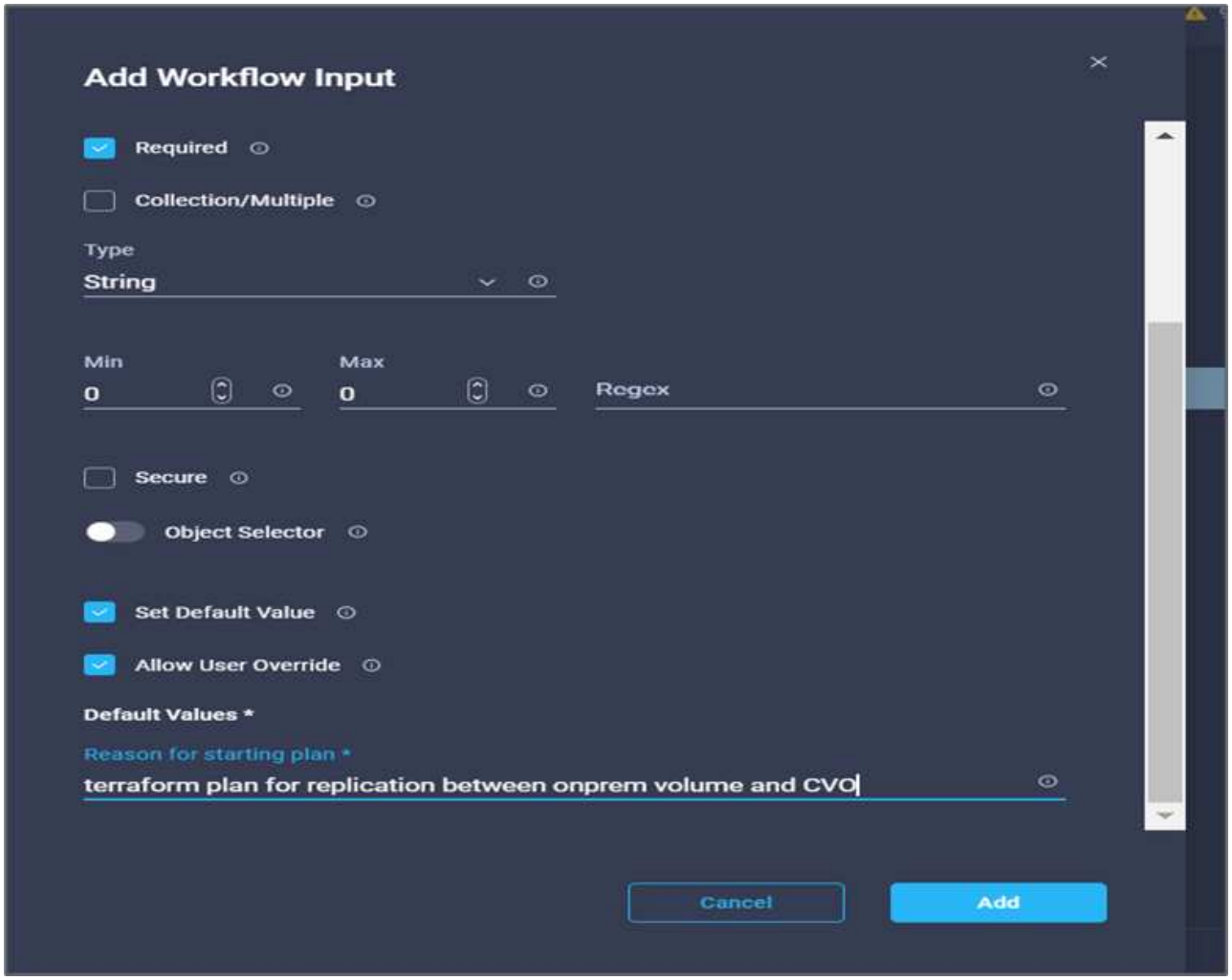
1. [*Designer]タブに移動し、[*Tools]セクションから[*Tasks]をクリックします。
2. デザイン*領域の*ツール*セクションから*テラフォーム・クラウド>新規テラフォームプラン開始*タスクをドラッグ・アンド・ドロップします。
3. コネクターを使用して、タスク*テラフォームのセンシティブ変数の追加*と*新しいTerraformプランタスクの開始*を接続します。[保存（ Save ）] をクリックします。
4. [新しいTerraformプランを開始する*]をクリックします。[タスクのプロパティ]領域で、[一般]タブをクリックします。必要に応じて、このタスクの名前と概要 を変更できます。



5. [タスクプロパティ（Task Properties ）]領域で、[*入力（Inputs *）]をクリックする
6. [**Terraform Cloud Target**]フィールドの[**Map**]をクリックします。
7. *静的値*を選択し、*テラフォームクラウドターゲットの選択*をクリックします。「Configuring Cisco Intersight Service for Corp'Terraform」の項に追加されたTerraform Cloud for Businessアカウントを選択します。
8. [マップ]をクリックします。
9. [ワークスペース**ID**]フィールドで[マップ]をクリックします。
10. [直接マッピング]を選択し、[タスク出力]をクリックします。
11. [タスク名*]をクリックし、[**Add Terraform Workspace**]をクリックします。



12. [出力名*]、[ワークスペース**ID**]、[マップ]の順にクリックします。
13. [開始計画の理由*]フィールドで[**Map**]をクリックします。
14. [直接マッピング]を選択し、[ワークフロー入力]をクリックします。
15. [入力名]、[ワークフロー入力の作成]の順にクリックします。
16. 入力の追加ウィザードで、次の手順を実行します。
    a. 表示名と参照名を指定します（オプション）。
    b. [タイプ（* Type）]に[文字列（ String）]を選択してください。
    c. [デフォルト値の設定]と[オーバーライド*]をクリックします。
    d. 開始計画の理由*のデフォルト値を入力し、*追加*をクリックします。



17. [マップ]をクリックします。
18. [計画操作]フィールドで[マップ]をクリックします。
19. 「静的値」を選択し、「計画操作」をクリックします。[新しい計画*]をクリックします。

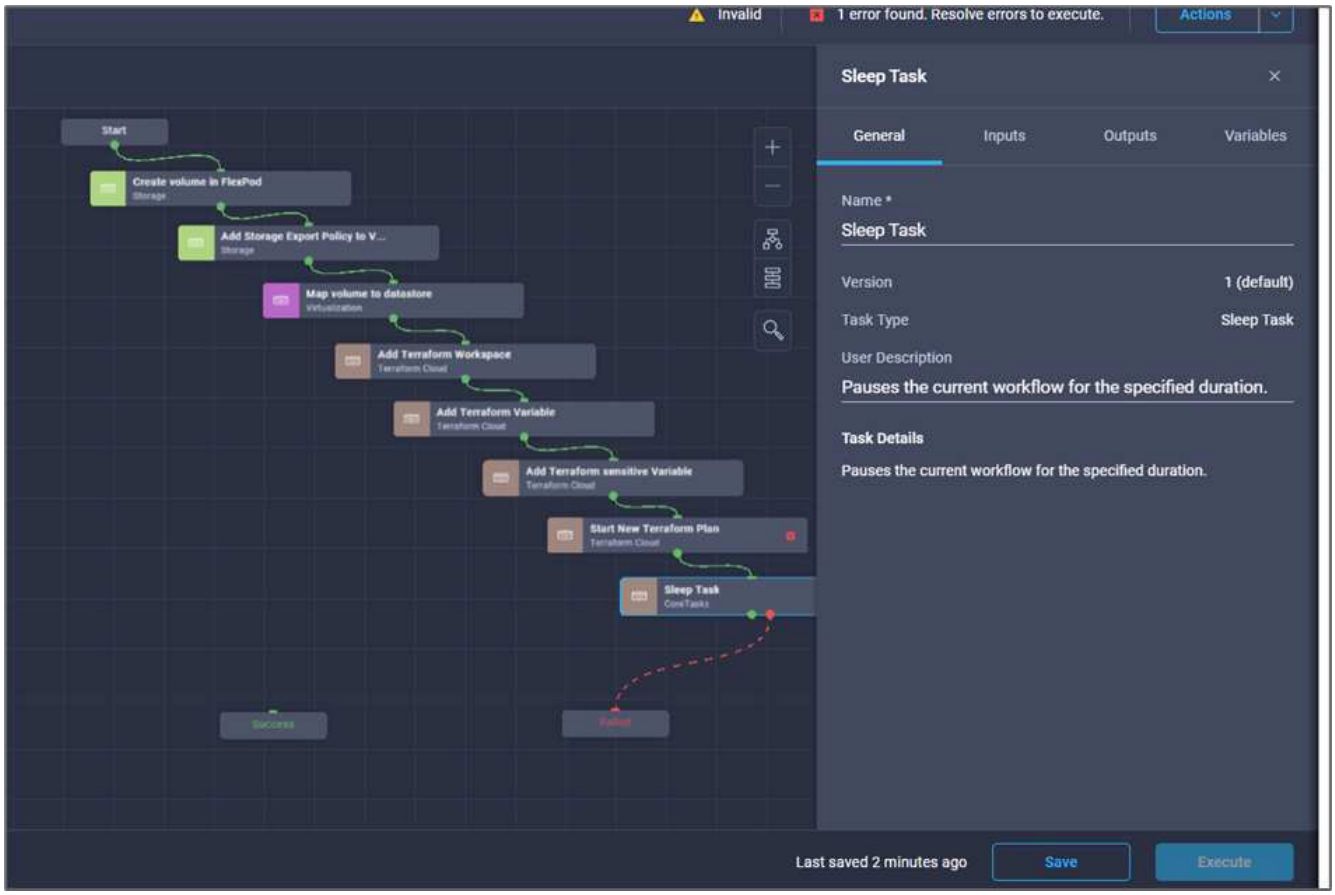
20. [マップ]をクリックします。
21. [保存（ Save ）] をクリックします。

これで、Terraform Cloud for BusinessアカウントにTerraformプランを追加する作業は完了です。次に、スリープタスクを数秒間作成します。

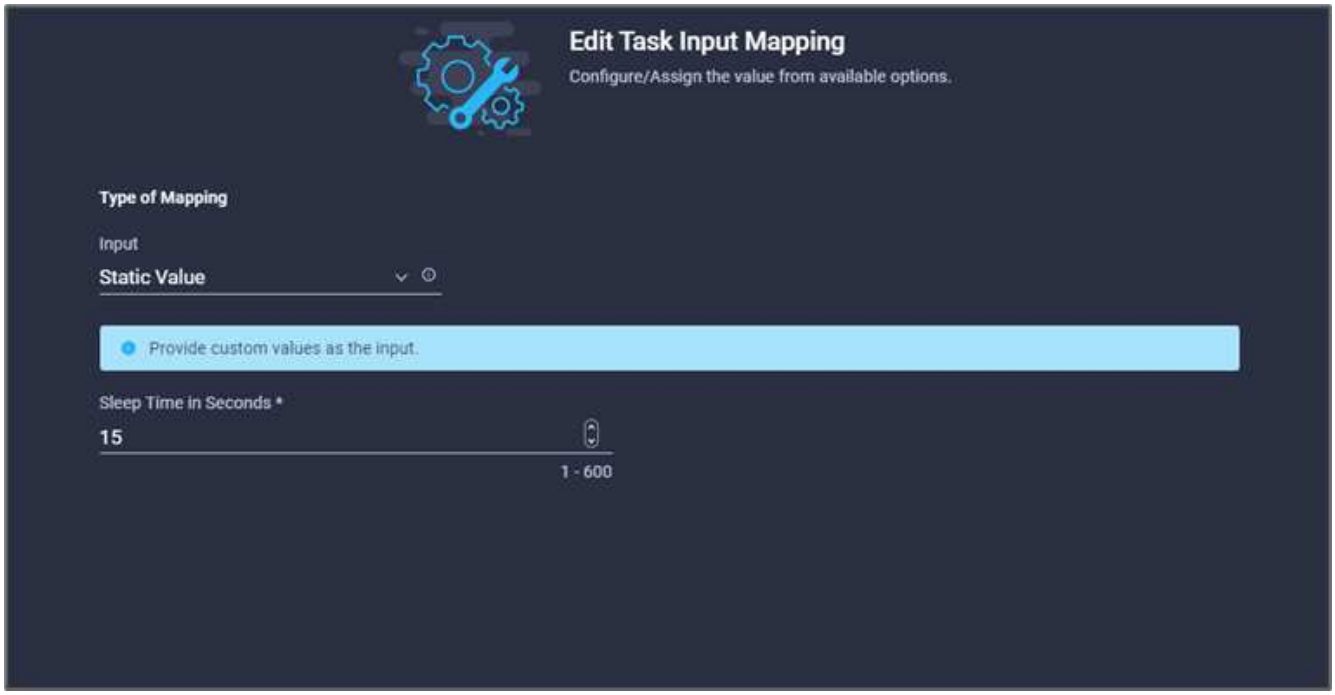
手順 **9**：同期のためのスリープタスク

Terraform ApplyにはRunIDが必要です。RunIDはTerraform Planタスクの一部として生成されます。Terraform PlanとTerraform Applyアクションの間に数秒待機することで、タイミングの問題を回避できます。

1. [*Designer]タブに移動し、[*Tools]セクションから[*Tasks]をクリックします。
2. デザイン*領域の*ツール*セクションから*コアタスク>スリープ・タスク*をドラッグ・アンド・ドロップします。
3. コネクターを使用して、タスク*新しいTerraformプランの開始*と*スリープタスク*を接続します。[保存（ Save ）] をクリックします。



4. スリープタスク*をクリックします。[タスクのプロパティ]領域で、[一般]タブをクリックします。必要に応じて、このタスクの名前と概要 を変更できます。この例では、タスクの名前は* Synchronize *です。
5. [タスクプロパティ（Task Properties ）]領域で、[*入力（Inputs *）]をクリックする
6. スリープ時間（秒）*フィールドで*マップ*をクリックします。
7. スリープ時間（秒）*に*静的値*と入力 15 *を選択します。

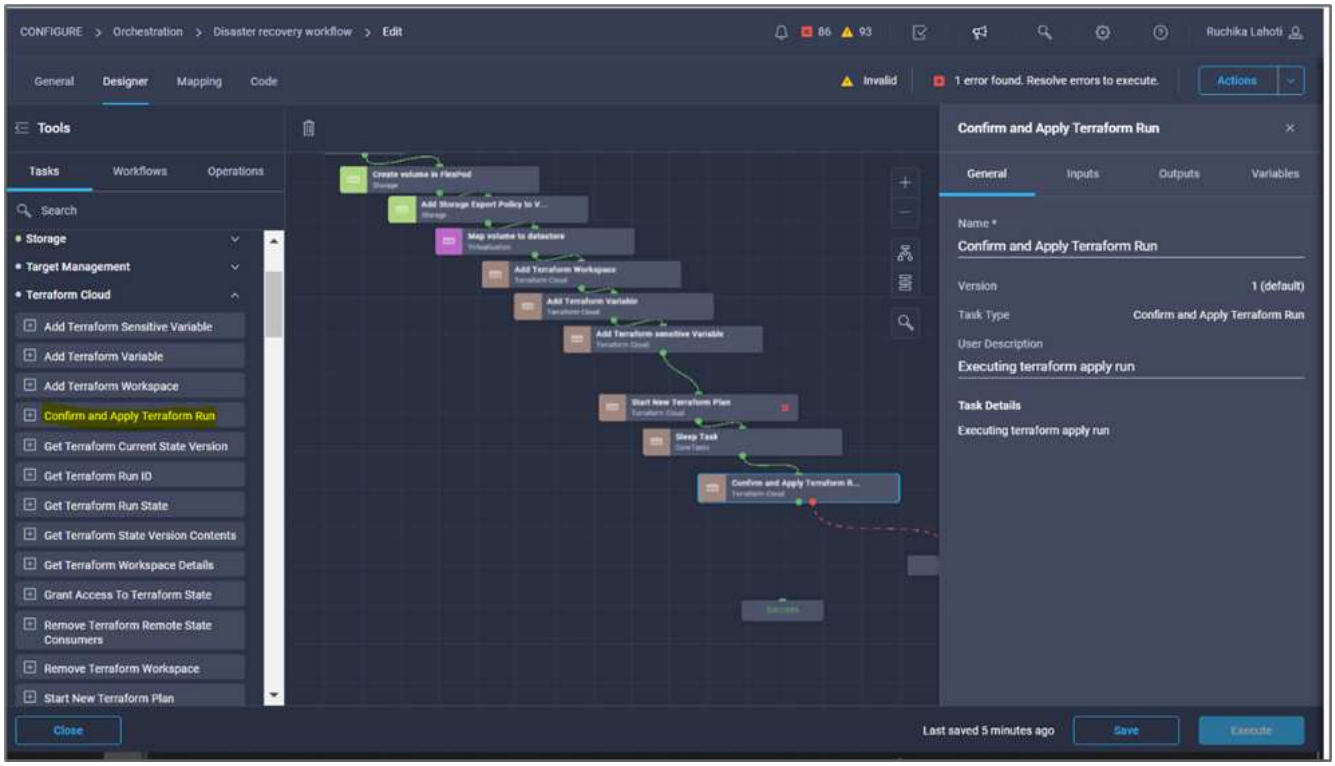


8. [マップ]をクリックします。
9. [保存（ Save ）] をクリックします。

これでスリープタスクは完了です。次に、このワークフローの最後のタスクを作成し、Terraform Runを確認して適用します。

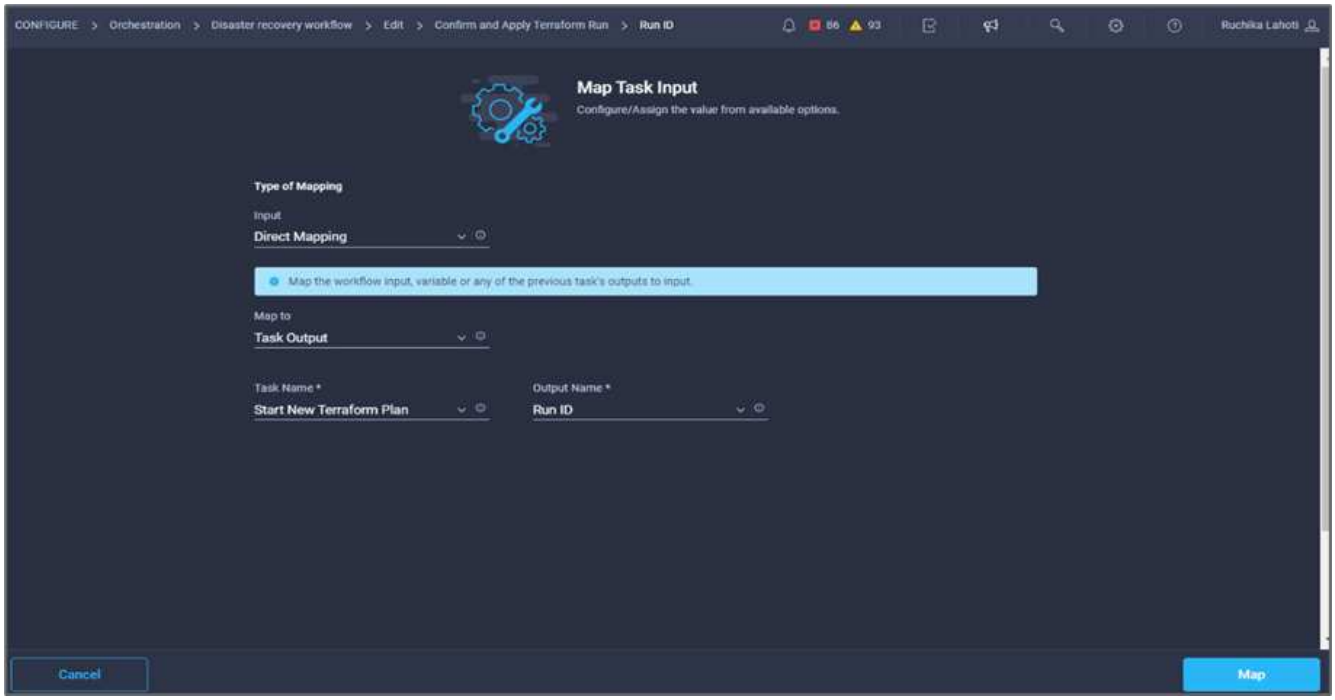
手順 **10: Terraform Run**を確認して適用します

1. [*Designer]タブに移動し、[*Tools]セクションから[*Tasks]をクリックします。
2. [**Design**]領域の[**Tools**]セクションから**[*Terraform Cloud]>[Confirm and Apply Terraform Run**]タスクをドラッグアンドドロップします。
3. コネクターを使用して、タスク*同期化*および*確認とテラフォーム実行の適用*を接続します。[保存（ Save ）] をクリックします。
4. [確認]と[* Terraform実行の適用*]をクリックします。[タスクのプロパティ]領域で、[一般]タブをクリックします。必要に応じて、このタスクの名前と概要 を変更できます。

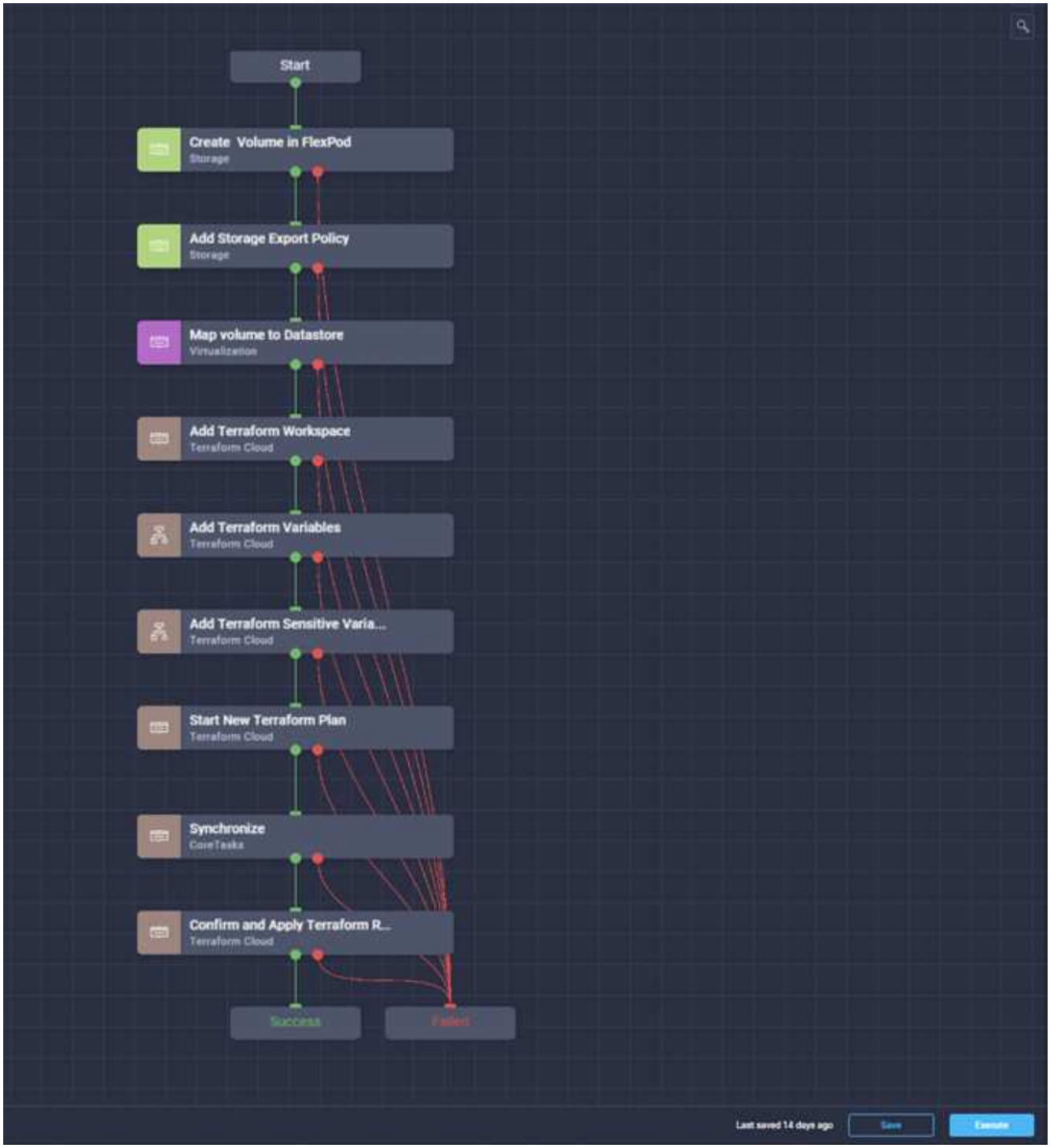


5. [タスクプロパティ（Task Properties ）]領域で、**[***入力（Inputs *）]をクリックする
6. [**Terraform Cloud Target**]フィールドの[**Map**]をクリックします。
7. *静的値*を選択し、*テラフォームクラウドターゲットの選択*をクリックします。で追加したTerraform Cloud for Businessアカウントを選択します "Cisco Intersight Service for橋のTerraformを設定します"」
8. [マップ]をクリックします。
9. [ファイル名を指定して実行ID]フィールドの**[*Map**]をクリックします。
10. [直接マッピング]を選択し、[タスク出力]をクリックします。
11. [タスク名*]をクリックし、[新しいTerraformプランの開始*]をクリックします。

12. [出力名*]をクリックし、[**Run ID**]をクリックします。



13. [マップ]をクリックします。
14. [保存（ Save ）] をクリックします。
15. すべてのタスクが整列されるように、*ワークフローの自動整列*をクリックします。[保存（ Save ）] をクリックします。



これで、確認と実行の適用タスクは完了です。コネクターを使用して、**Confirm**タスクと**Apply Terraform Run***タスクと***Success**/*Failed*タスクを接続します。

手順 **11**：シスコが構築したワークフローをインポートします

Cisco Intersight Cloud Orchestratorを使用すると、ワークフローをCisco Intersightアカウントからシステムにエクスポートし、別のアカウントにインポートできます。JSONファイルは、アカウントにインポート可能なビルドワークフローをエクスポートすることで作成されました。

ワークフローコンポーネントのJSONファイルは、で確認できます "GitHub リポジトリ"。

"次の例は、コントローラからのTerraformの実行です。"

コントローラからの**Terraform**の実行

"前の手順：DRワークフロー"

コントローラを使用してTerraformプランを実行できます。ICOワークフローを使用してTerraformプランをすでに実行している場合は、このセクションを省略できます。

前提条件

解決策 のセットアップは、まずインターネットにアクセスできる管理ワークステーションと、Terraformの実際のインストールから始まります。

Terraformをインストールするためのガイドがあります "こちらをご覧ください"。

クローン**GitHub**リポジトリをリポジトリします

このプロセスの最初のステップでは、GitHubリポジトリを管理ワークステーションの新しい空のフォルダにクローニングします。GitHubリポジトリのクローンを作成するには、次の手順を実行します。

1. 管理ワークステーションから、プロジェクトの新しいフォルダを作成します。このフォルダ内に'/root/snapmirror-CVO'という名前の新しいフォルダを作成し'GitHubリポジトリをクローンします
2. 管理ワークステーションでコマンドラインインターフェイスまたはコンソールインターフェイスを開き、作成した新しいフォルダにディレクトリを変更します。
3. 次のコマンドを使用してGitHubコレクションをクローニングします。

```
Git clone https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO
```

1. ディレクトリを「snapmirror-CVO'」という新しいフォルダに変更します。
    - Terraformの実行*

- * Init.*(local) Terraform環境を初期化します。通常、1回のセッションで1回のみ実行されます。
- *計画。*テラフォームの状態をクラウドの現状と比較し、実行計画を作成して表示します。これによって導入環境が変更されることはありません（読み取り専用）。
- *適用。*計画フェーズから計画を適用します。これにより、導入環境（読み取りと書き込み）が変更される可能性があります。
- *破棄。*この特定のテラフォーム環境によって管理されるすべてのリソース。

詳細については、を参照してください "こちらをご覧ください"。

"次の例は、解決策の検証です。"

解決策の検証

"前のバージョン：コントローラからのTerraformの実行。"

このセクションでは、サンプルのデータレプリケーションワークフローを使用して解決策 を再確認し、測定値をいくつか確認して、FlexPod で実行されているNetApp ONTAP インスタンスからGoogle Cloudで実行されているNetApp Cloud Volumes ONTAP へのデータレプリケーションの整合性を検証します。

この解決策 では、Cisco Intersightワークフローオーケストレーションツールを使用しており、今回のユースケースで引き続き使用します。

特に、この解決策 で使用される限定的なCisco Intersightのワークフローは、Cisco Intersightに含まれるすべてのワークフローを表しているわけではありません。独自の要件に基づいてカスタムワークフローを作成し、Cisco Intersightからトリガーされるようにすることができます。

DRシナリオが成功するかどうかを検証するために、最初にSnapMirrorを使用して、FlexPod に含まれるONTAP のボリュームからCloud Volumes ONTAP にデータを移動します。その後、Googleクラウドコンピューティングインスタンスからデータにアクセスし、データ整合性チェックを実行できます。

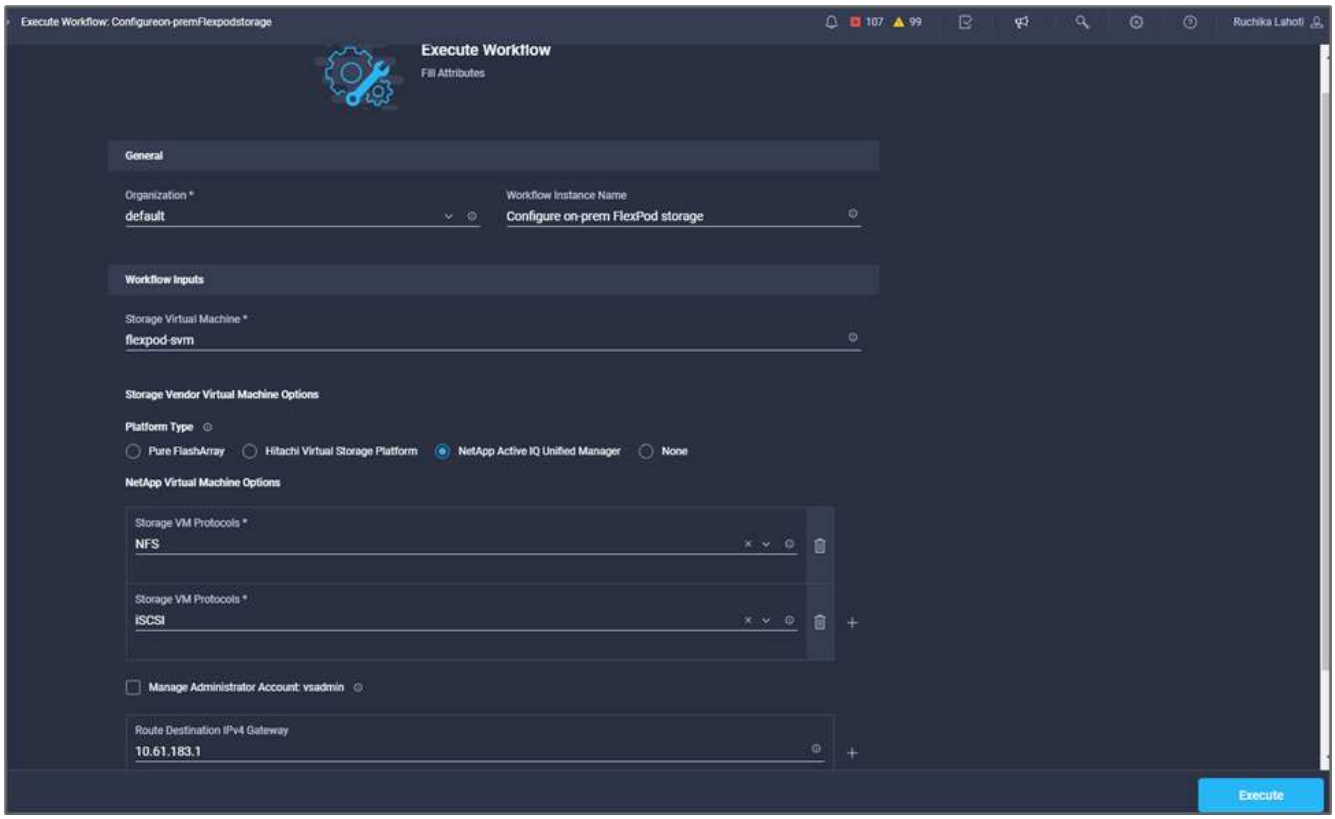
次に、この解決策 の成功基準を確認する手順の概要を示します。

1. FlexPod のONTAP ボリュームにあるサンプルデータセットでSHA256チェックサムを生成します。
2. FlexPod のONTAP とCloud Volumes ONTAP の間にVolume SnapMirror関係を設定します。
3. サンプルデータセットをFlexPod からCloud Volumes ONTAP にレプリケートします。
4. SnapMirror関係を解除し、Cloud Volumes ONTAP 内のボリュームを本番環境に昇格します。
5. Cloud Volumes ONTAP ボリュームとデータセットをGoogle Cloudのコンピューティングインスタンスにマッピングします。
6. Cloud Volumes ONTAP のサンプルデータセットでSHA256チェックサムを生成します。
7. ソースとデスティネーションのチェックサムを比較します。両方のチェックサムが一致していると考えられます。

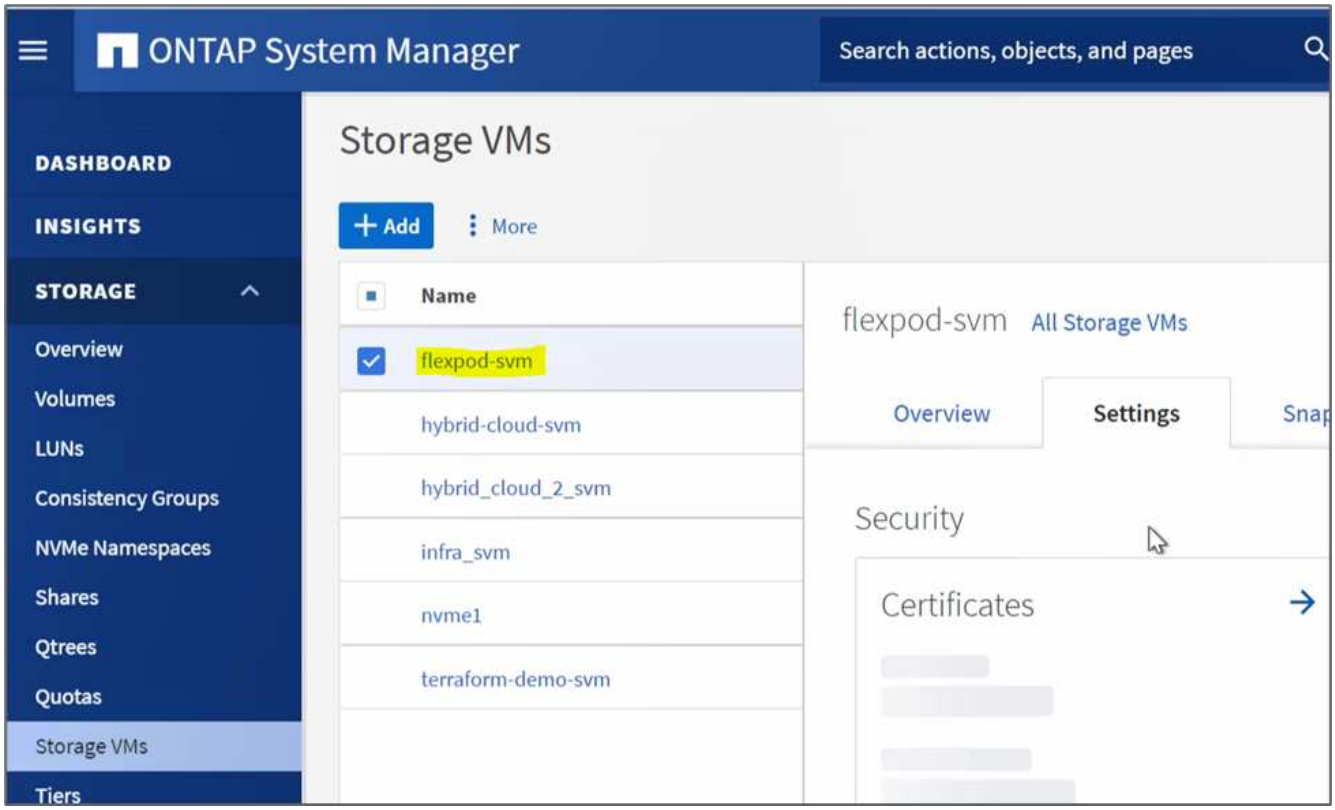
オンプレミスワークフローを実行するには、次の手順を実行します。

1. オンプレミスFlexPod のIntersightでワークフローを作成

2. 必要な入力を指定し、ワークフローを実行します。

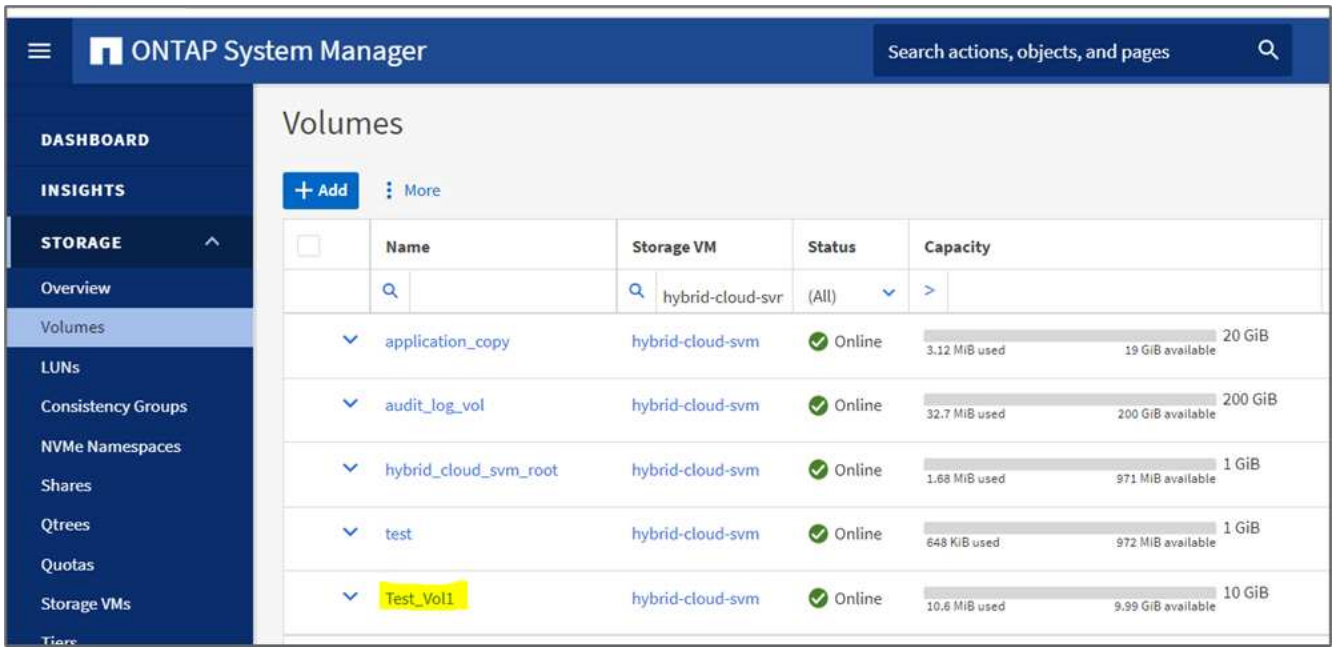


3. システムマネージャで、新しく作成したSVMを確認します。



4. 別のディザスタリカバリワークフローを作成して実行し、オンプレミスのFlexPod にボリュームを作成して、FlexPod とCloud Volumes ONTAP でこのボリューム間にSnapMirror関係を確立します。

5. ONTAP システムマネージャで、新しく作成したボリュームを確認します。

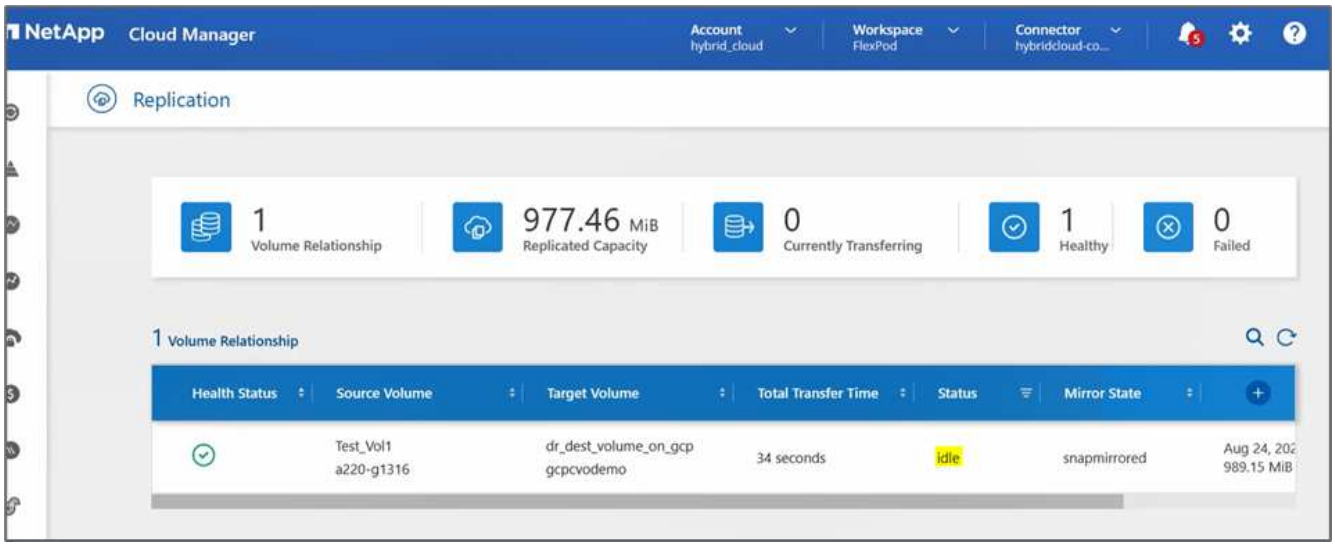


6. 同じNFSボリュームをオンプレミスの仮想マシンにマウントし、サンプルデータセットをコピーしてチェックサムを実行します。

```
root@hybridcloudbackup:/snapmirror_demo# mount -t nfs 172.22.4.157:/Test_Vol1 /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo# df -kh
Filesystem                Size  Used Avail Use% Mounted on
udev                      1.9G     0  1.9G   0% /dev
tmpfs                     394M  1.1M  393M   1% /run
/dev/sda2                  16G   11G  4.2G  72% /
tmpfs                     2.0G     0  2.0G   0% /dev/shm
tmpfs                     5.0M     0  5.0M   0% /run/lock
tmpfs                     2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/loop1                 55M   55M     0 100% /snap/core18/1705
/dev/loop2                 69M   69M     0 100% /snap/lxd/14804
/dev/loop0                 28M   28M     0 100% /snap/snapd/7264
172.22.4.157:/Test_Vol1    10G  512K   10G   1% /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo#
```

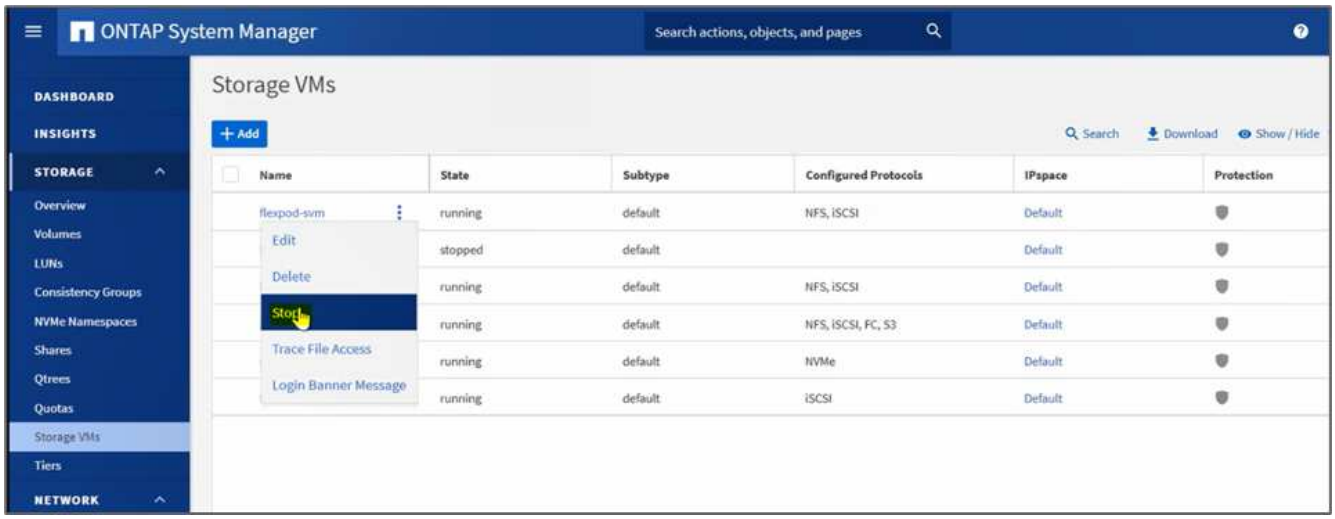
```
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo# sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo#
```

7. Cloud Managerでレプリケーションステータスを確認します。データのサイズによっては、データ転送に数分かかることがあります。完了すると、SnapMirrorのステータスが* Idle *と表示されます。

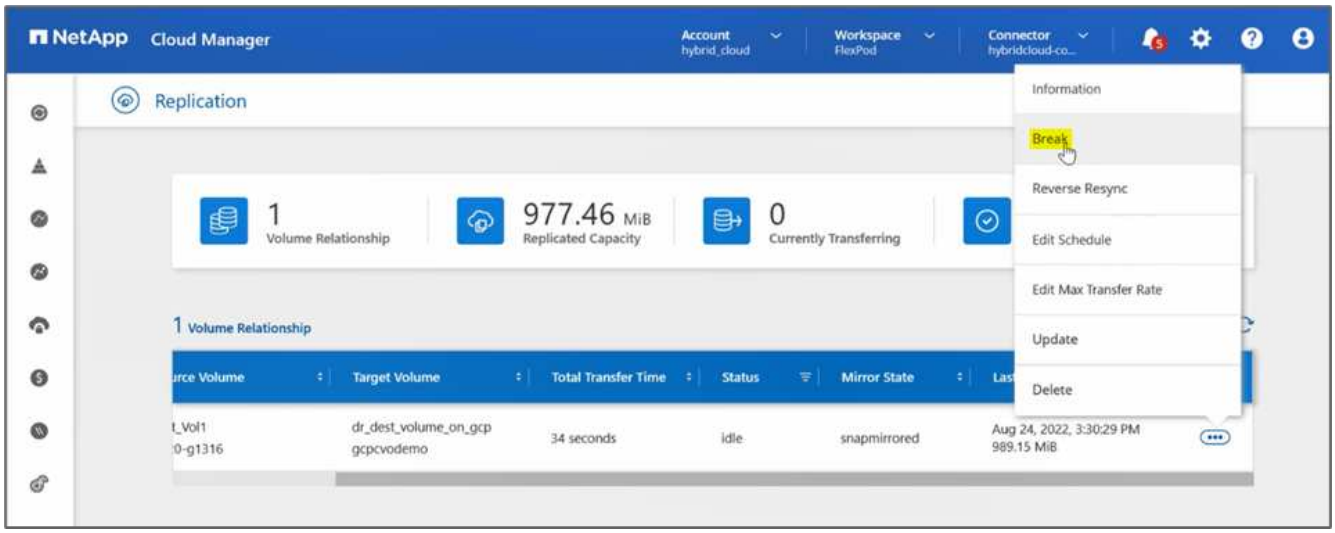


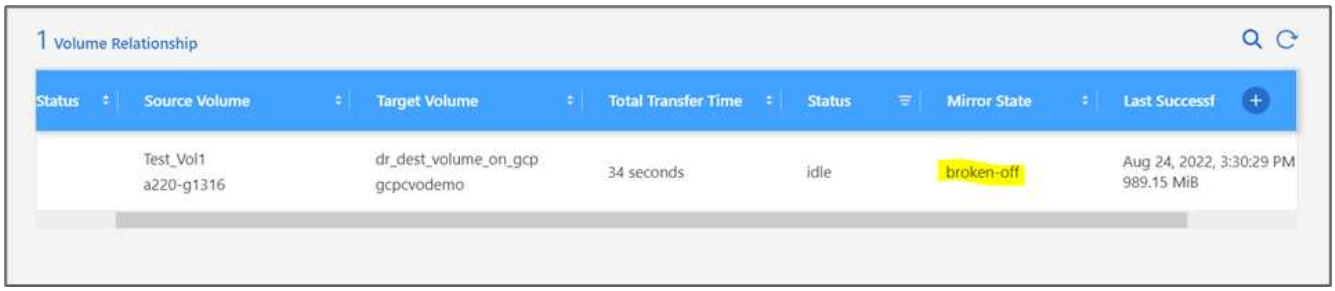
8. データ転送が完了したら、「Test_vol1」ボリュームをホストしているSVMを停止して、ソース側の災害をシミュレートします。

   SVMの停止後、「Test_vol1」ボリュームはCloud Managerに表示されません。

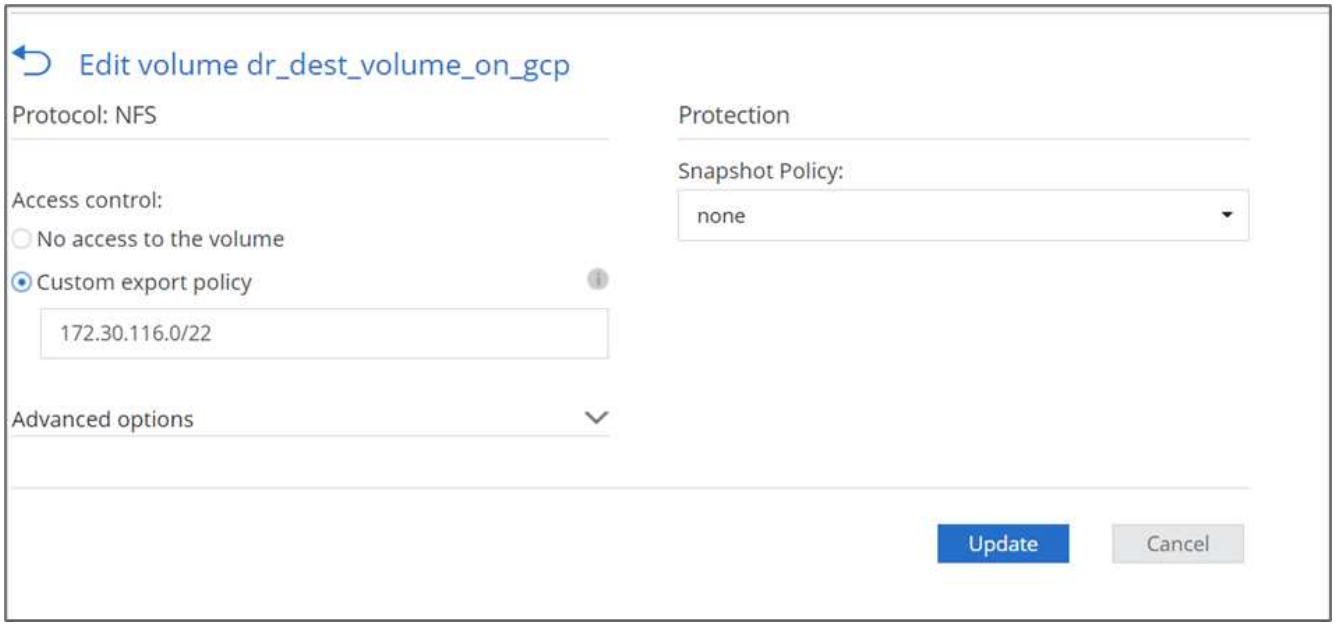


9. レプリケーション関係を解除し、Cloud Volumes ONTAP デスティネーションボリュームを本番環境に昇格

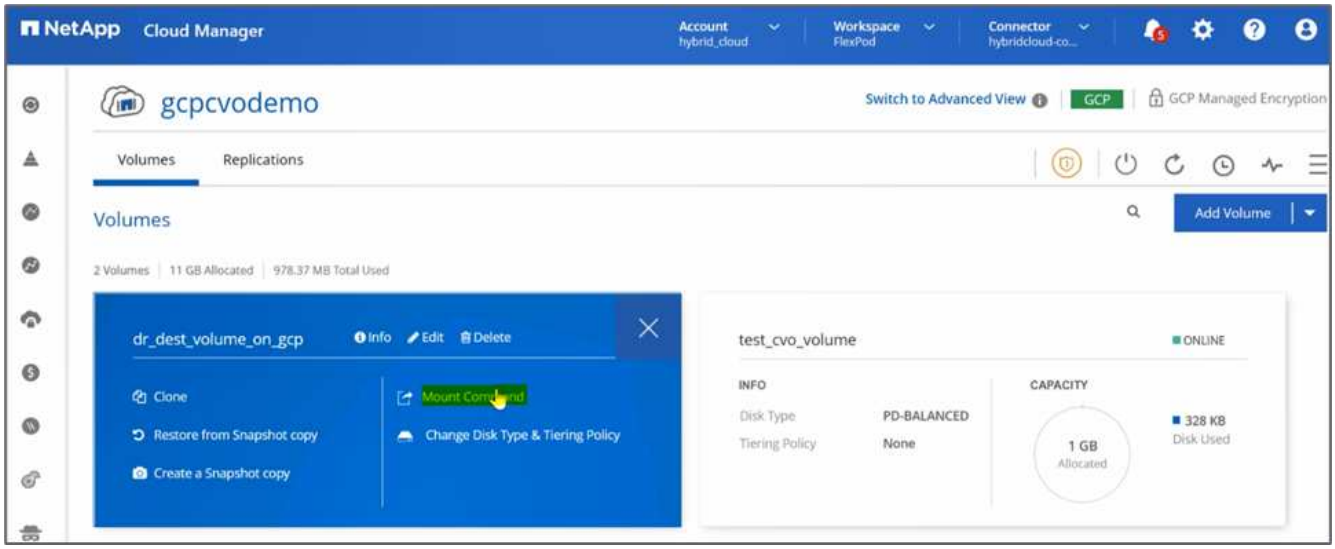




10. ボリュームを編集し、エクスポートポリシーに関連付けてクライアントアクセスを有効にします。



11. ボリュームの使用準備が完了しているマウントコマンドを取得します。



12. コンピューティング・インスタンスにボリュームをマウントし'デスティネーション・ボリュームにデータが存在することを確認して'sample_dataset_s2GB'ファイルのSHA256チェックサムを生成します

```
drwxr-xr-x 21 root   root            4096 Aug 24 10:20 ../
-rwxr-xr-x  1 nobody 4294967294 1015306240 Aug 24 09:59 test.zip*
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$ sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
```

13. ソース（FlexPod ）とデスティネーション（Cloud Volumes ONTAP ）の両方でチェックサム値を比較します。
14. チェックサムはソースとデスティネーションのチェックサムと同じです。

ソースからデスティネーションへのデータレプリケーションが正常に完了し、データの整合性が維持されていることを確認できます。このデータは、ソースサイトがリストアを実行している間に、アプリケーションがクライアントにデータを提供するために安全に使用できるようになりました。

"次は終わりです"

まとめ

"前のバージョン：解決策 の検証。"

この解決策 では、ネットアップのクラウドデータサービス、Cloud Volumes ONTAP 、FlexPod データセンターインフラを使用して、Cisco Intersightクラウドオーケストレーションツールを基盤とするパブリッククラウドを使用したDR解決策 を構築しました。FlexPod 解決策 は絶えず進化しており、お客様はアプリケーションやビジネス提供プロセスを最新化できるようになっています。この解決策 を使用すると、DR解決策 のコストを低く抑えながら、短期またはフルタイムのDR計画のための移動先としてパブリッククラウドを使用してBCDR計画を構築できます。

オンプレミスのFlexPod とNetApp Cloud Volumes ONTAP 間のデータレプリケーションは、実績のあるSnapMirrorテクノロジによって処理されましたが、お客様のデータ移動要件には、Cloud Sync などの他のネットアップのデータ転送ツールや同期ツールも選択できます。TLS/AESをベースとする暗号化テクノロジが組み込まれているため、転送中のデータのセキュリティを確保できます。

アプリケーション向けの一時的なDRプランでも、企業向けのフルタイムのDRプランでも、この解決策 で使用される製品ポートフォリオは、両方の要件を大規模に満たすことができます。Cisco Intersight Workflow Orchestratorを活用することで、構築済みのワークフローを利用して同じワークフローを自動化できます。プロセスの再構築が不要になるだけでなく、BCDRプランの実装も高速化されます。

解決策 を使用すると、Cisco Intersight Cloud Orchestratorが提供する自動化とオーケストレーションによって、ハイブリッドクラウド全体でFlexPod オンプレミスとデータレプリケーションを非常に簡単かつ便利に管理できます。

追加情報の参照先

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

GitHub

- 使用されているすべてのTerraform設定

  "https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO"

- ワークフローをインポートするためのJSONファイル

  "https://github.com/ucs-compute-solutions/FlexPod_DR_Workflows"

Cisco Intersightの

- Cisco Intersightのヘルプセンター

  "https://intersight.com/help/saas/home"

- Cisco Intersight Cloud Orchestratorのドキュメント：

  "https://intersight.com/help/saas/features/orchestration/configure#intersight_cloud_orchestrator"

- Cisco Intersight Service for橋（橋本）Terraform Documentation

  "https://intersight.com/help/saas/features/terraform_cloud/admin"

- Cisco Intersightのデータシート

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html"

- Cisco Intersight Cloud Orchestratorデータシート

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-cloud-orch-aag-cte-en.html"

- Cisco Intersight Service for橋（Cisco Intersight Service for橋）Terraformデータシート

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-terraf-ser-aag-cte-en.html"

FlexPod

- FlexPod ホームページ

  "https://www.flexpod.com"

- FlexPod のシスコ検証済み設計および導入ガイド

  "UCS 管理モードの FlexPod データセンター、 VMware vSphere 7.0 U2 、および NetApp ONTAP 9.9 設計ガイド"

- FlexPod データセンターとCisco UCS Xシリーズ

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_esxi7u2_design.html"

相互運用性

- NetApp Interoperability Matrix Tool で確認できます

  "http://support.netapp.com/matrix/"

- Cisco UCS ハードウェアおよびソフトウェア相互運用性ツール

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- VMware Compatibility Guide 』を参照してください

  "http://www.vmware.com/resources/compatibility/search.php"

NetApp Cloud Volumes ONTAP の参考資料

- NetApp Cloud Manager の略

"https://docs.netapp.com/us-en/occm/concept_overview.html"

- Cloud Volumes ONTAP

  https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-gcp.html

- Cloud Volumes ONTAP TCO計算ツール

  https://cloud.netapp.com/google-cloud-calculator

- Cloud Volumes ONTAP サイジングツール

  "https://cloud.netapp.com/cvo-sizer"

- クラウド評価ツール

  https://cloud.netapp.com/assessments

- ネットアップのハイブリッドクラウド

  https://cloud.netapp.com/hybrid-cloud

- Cloud Manager API ドキュメント

  "https://docs.netapp.com/us-en/occm/reference_infrastructure_as_code.html"

問題のトラブルシューティング

"https://kb.netapp.com/Advice_and_Troubleshooting/Cloud_Services/Cloud_Volumes_ONTAP_(CVO)"

テラフォーム

- クラウドをテラフォーム

  "https://www.terraform.io/cloud"

- Terraformドキュメント

  "https://www.terraform.io/docs/"

- NetApp Cloud Managerレジストリ

  "https://registry.terraform.io/providers/NetApp/netapp-cloudmanager/lates"

GCP

- GCPのONTAP ハイアベイラビリティ

  "https://cloud.netapp.com/blog/gcp-cvo-blg-what-makes-cloud-volumes-ontap-high-availability-for-gcp-tick"

- GCPの永続的なサイト

  https://netapp.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=f3d0368b-7165-4d43-a76e-ae01011853d6

ネットアップのAstraとCisco Intersightを活用したFlexPod ハイブリッドクラウドをRed Hat OpenShiftに活用

TR-4936：『FlexPod hybrid cloud with NetApp Astra and Cisco Intersight for Red Hat OpenShift』

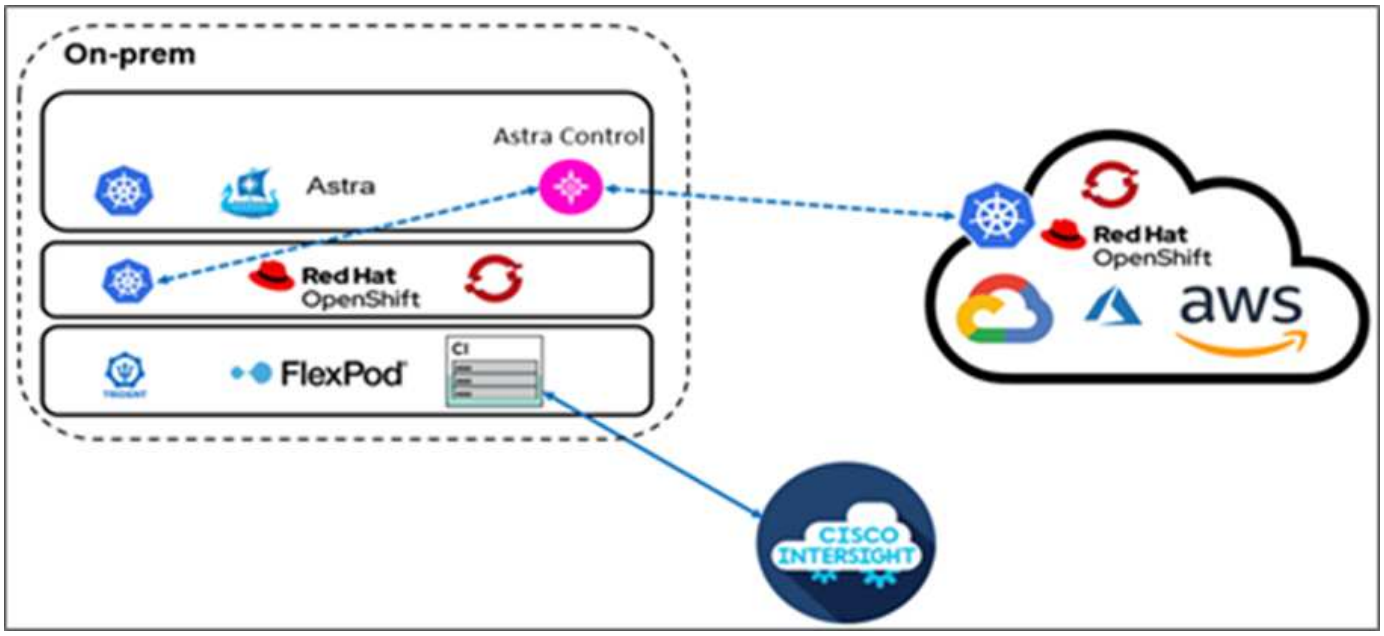
Abhinav Singhの

はじめに

コンテナ化されたアプリケーションの開発、導入、実行、管理、拡張のための事実上の選択肢となるコンテナとKubernetesは、ビジネスクリティカルなアプリケーションを実行する企業の増加に伴いつつあります。ビジネスクリティカルなアプリケーションは、状態に大きく依存しています。ステートフルアプリケーションには、状態、データ、および設定情報が関連付けられており、ビジネスロジックを実行する前のデータトランザクションに依存します。Kubernetes上で実行されるビジネスクリティカルなアプリケーションには、従来型アプリケーションのような可用性とビジネス継続性の要件が引き続きあります。サービスの停止は、収益の損失、生産性、会社の評判に深刻な影響を与える可能性があります。そのため、Kubernetesワークロードをクラスタ、オンプレミスデータセンター、ハイブリッドクラウド環境内およびクラスタ間で迅速かつ容易に保護、リカバリ、移動することが非常に重要です。企業は、ビジネスをハイブリッドクラウドモデルに移行し、アプリケーションをクラウドネイティブなフォームファクタに刷新するメリットを高く挙げています。

このテクニカルレポートでは、FlexPod コンバージドインフラ解決策 上にNetApp Astra Control CenterとRed Hat OpenShift Container Platformを統合し、Amazon Web Services（AWS）に拡張してハイブリッドクラウドデータセンターを構築しました。使い慣れたことに基づいて作成されています "FlexPod とRed Hat OpenShift"このドキュメントでは、ネットアップのAstra Control Centerについて説明します。インストール、設定、アプリケーション保護ワークフロー、オンプレミスとクラウド間でのアプリケーション移行から始まります。また、Red Hat OpenShiftで実行されるコンテナ化アプリケーションにNetApp Astra Control Centerを使用する場合の、アプリケーション対応データ管理機能（バックアップとリカバリ、ビジネス継続性など）の利点についても説明します。

次の図に、解決策 の概要を示します。



対象者

このドキュメントは、CTO（最高技術責任者）、アプリケーション開発者、クラウド解決策 アーキテクト、サイト信頼性エンジニア（SRE）、DevOpsエンジニア、ITOps、コンテナ化されたアプリケーションの設計、ホスティング、管理に重点を置いたプロフェッショナルサービスチームなど、読者を想定しています。

NetApp Astra Control–主なユースケース

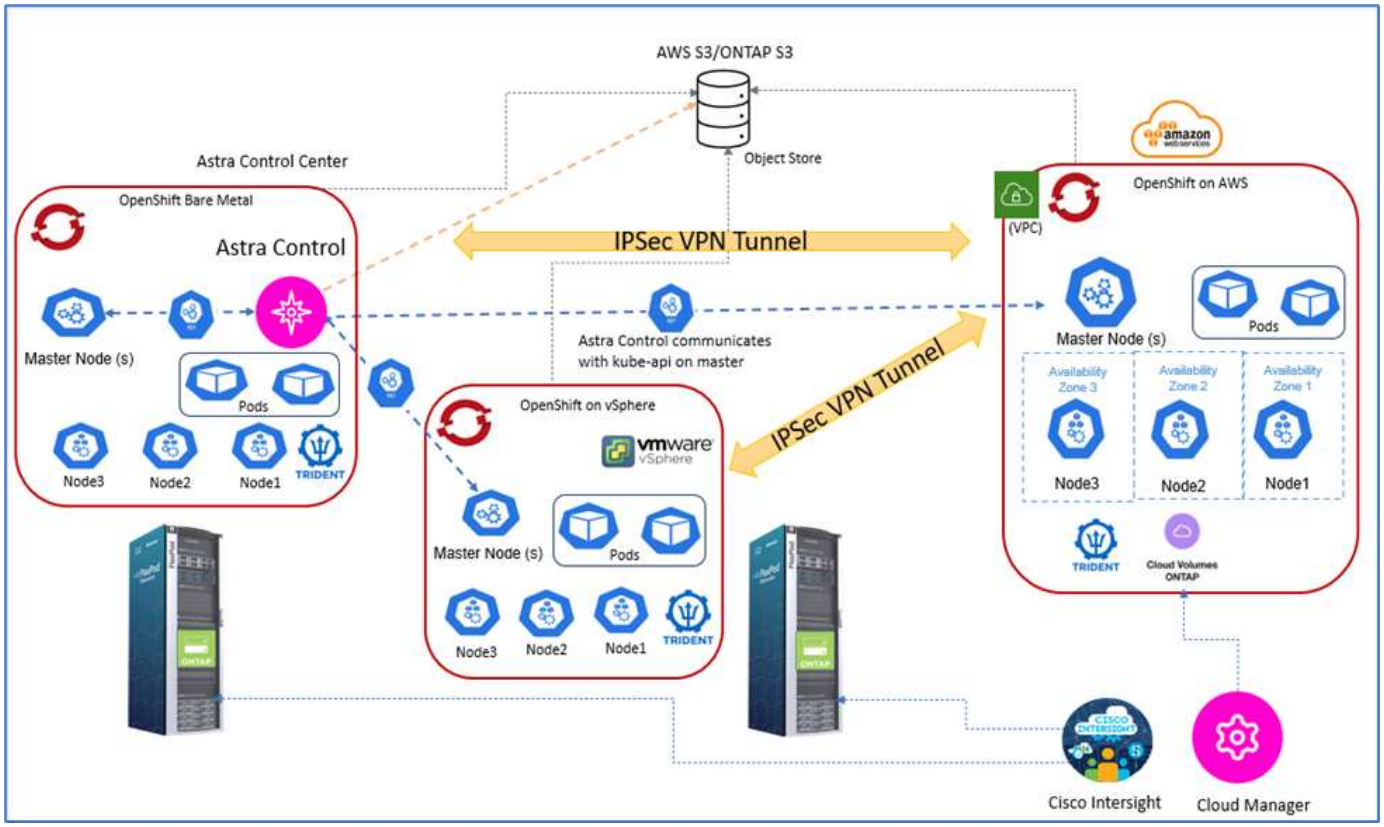
ネットアップのAstra Controlは、クラウドネイティブなマイクロサービスを利用するお客様にアプリケーション保護を簡易化することを目的としています。

- スナップショットを使用したポイントインタイム（**PiT**）アプリケーションリプレゼンテーション。 Astra Controlを使用すると、Kubernetesで実行されているアプリケーションの構成の詳細や、関連付けられた永続的ストレージを含む、コンテナ化されたアプリケーションのエンドツーエンドのスナップショットを作成できます。インシデントが発生した場合は、ボタンクリックでアプリケーションを正常な状態に復元できます。
- フルコピー・アプリケーション・バックアップ Astra Controlを使用すると’事前に定義されたスケジュールでフル・アプリケーション・バックアップを実行できますこのスケジュールを使用すると’アプリケーションを同じKubernetesクラスタにリストアしたり’別のKubernetesクラスタにオンデマンドで自動化された方法でリストアしたりできます
- クローンを使用したアプリケーションの移植と移行 Astra Controlを使用すると、アプリケーション全体をKubernetesクラスタ間または同じKubernetesクラスタ内のデータとともにクローニングできます。この機能は、クラスタがどこにあるかに関係なく、Kubernetesクラスタ間でアプリケーションを移植または移行する場合にも役立ちます（クローニング後にソースアプリケーションインスタンスを削除するだけです）。
- アプリケーションの一貫性をカスタマイズできます。 Astra Controlを使用すると、実行フックを活用してアプリケーションの休止状態を定義できます。「実行前」と「実行後」のフックをスナップショットおよびバックアップのワークフローにドロップすると、スナップショットまたはバックアップが作成される前に、アプリケーションが独自の方法で休止されます。
- アプリケーションレベルのディザスタリカバリ（**DR**）を自動化。 Astra Controlを使用すると、コンテナ化されたアプリケーション用にBCDR（ビジネス継続性ディザスタリカバリ）計画を設定できます。NetApp SnapMirrorはバックエンドで使用されるため、DRワークフローの実装はすべて自動化されます。

解決策 トポロジ

このセクションでは、解決策 の論理トポロジについて説明します。

次の図は、OpenShift Container Platformクラスタを実行するFlexPod オンプレミス環境と、NetApp Cloud Volumes ONTAP 、Cisco Intersight、NetApp Cloud Manager SaaSプラットフォームを使用するAWS上の自己管理型OpenShift Container Platformクラスタからなる解決策 トポロジを示しています。



最初のOpenShift Container PlatformクラスタはFlexPod 上にベアメタルインストールされ、2番目のOpenShift Container PlatformクラスタはFlexPod 上で実行されるVMware vSphereに導入され、3番目のOpenShift Container Platformクラスタはとして導入されます "プライベートクラスタ" 自社で管理するインフラとして、AWS上の既存の仮想プライベートクラウド（VPC）に導入できます。

この解決策 では、FlexPod はサイト間VPNを介してAWSに接続されますが、直接接続の実装を使用してハイブリッドクラウドに拡張することもできます。Cisco Intersightは、FlexPod インフラストラクチャコンポーネントの管理に使用されます。

この解決策 では、Astra Control Centerが、FlexPod およびAWSで実行されているOpenShift Container Platformクラスタでホストされているコンテナ化アプリケーションを管理します。FlexPod で実行されているOpenShiftベアメタルインスタンスにAstraコントロールセンターをインストールします。Astra Controlは、マスターノードのkube-APIと通信し、Kubernetesクラスタの変更を継続的に監視します。Kubernetesクラスタに追加した新しいアプリケーションは自動的に検出され、管理用に使用できるようになります。

コンテナ化されたアプリケーションのPiT表現は、Astra Control Centerを使用してスナップショットとしてキャプチャできます。アプリケーションスナップショットは、スケジュールされた保護ポリシーまたはオンデマンドで開始できます。Astraがサポートしているアプリケーションの場合、スナップショットはクラッシュ整合性があります。アプリケーションスナップショットは、永続ボリューム内のアプリケーションデータのスナップショットと、そのアプリケーションに関連付けられているさまざまなKubernetesリソースのアプリケーションメタデータを構成します。

アプリケーションのフルコピーバックアップは、事前定義されたバックアップスケジュールまたはオンデマンドを使用して、Astra Controlを使用して作成できます。オブジェクトストレージは、アプリケーションデータのバックアップを格納するために使用されます。NetApp ONTAP S3、NetApp StorageGRID 、および汎用のS3実装をオブジェクトストアとして使用できます。

"次の例は、解決策 コンポーネントです。"

解決策コンポーネント

"Previous ：解決策の概要を示します。"

FlexPod

FlexPod は、仮想化ソリューションと非仮想化ソリューションの両方の統合基盤となるハードウェアとソフトウェアの定義済みセットです。FlexPod には、NetApp ONTAP ストレージ、Cisco Nexusネットワーク、Cisco MDSストレージネットワーク、Cisco Unified Computing System（Cisco UCS）が含まれています。この設計は、ネットワーク、コンピューティング、ストレージを1つのデータセンターラックに収容できる柔軟性を備えています。また、お客様のデータセンター設計に従って導入することもできます。ポート密度を使用すると、ネットワークコンポーネントは複数の構成に対応できます。

Astra Control の略

Astra Controlは、パブリッククラウドとオンプレミスの両方でホストされるクラウドネイティブアプリケーションに対して、アプリケーション対応のデータ保護サービスを提供します。Astra Controlは、Kubernetesで実行されるコンテナ化されたアプリケーションに、データ保護、ディザスタリカバリ、移行の機能を提供します。

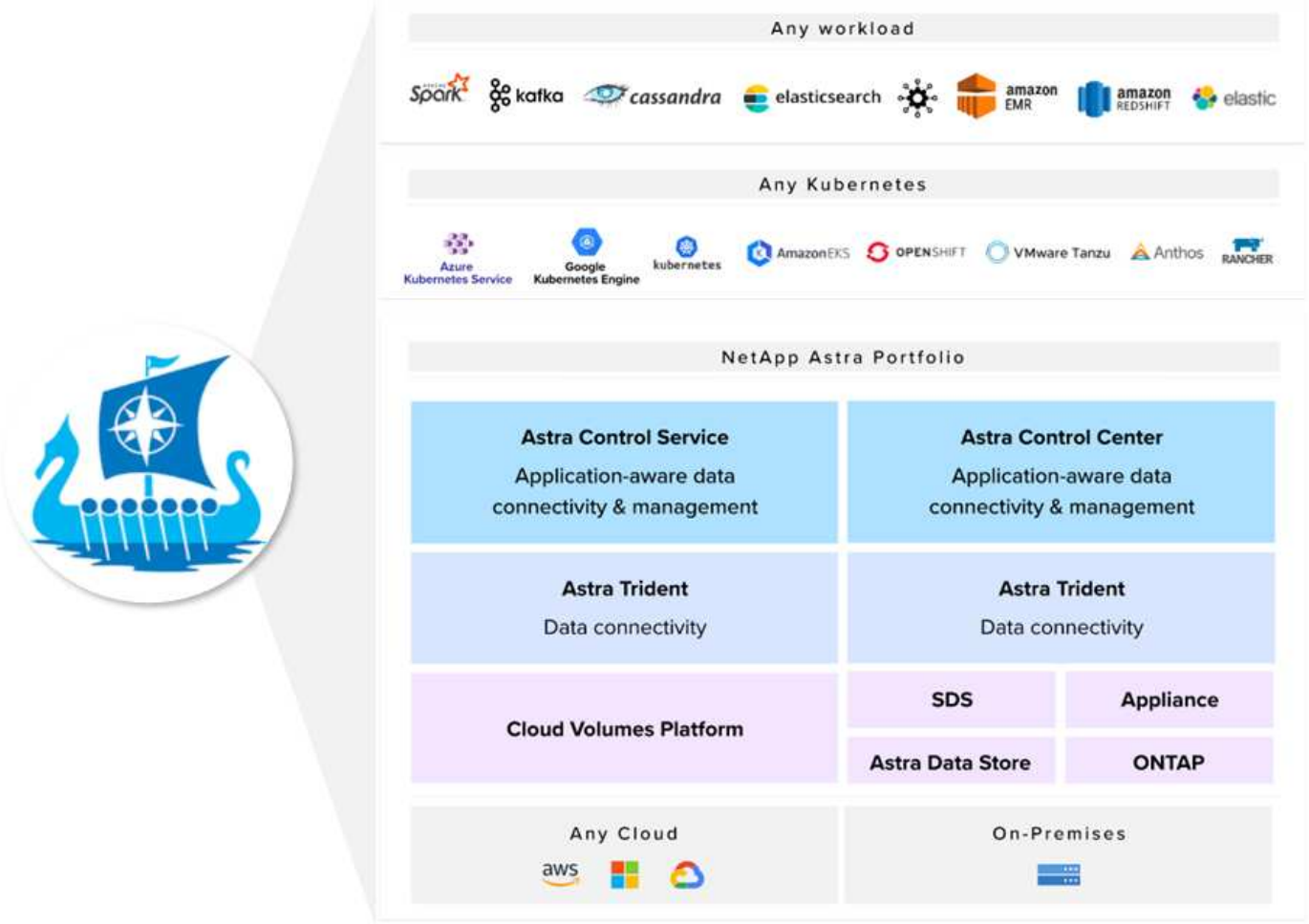
の機能

Astra Control は、 Kubernetes アプリケーションデータのライフサイクル管理に不可欠な機能を提供

- 永続的ストレージを自動的に管理
- アプリケーションと整合性のあるオンデマンドのSnapshotとバックアップを作成
- ポリシーベースのスナップショット処理とバックアップ処理を自動化
- ハイブリッドクラウド環境で、アプリケーションと関連データをKubernetesクラスタから別のクラスタに移行する
- 同じKubernetesクラスタまたは別のKubernetesクラスタにアプリケーションをクローニングする
- アプリケーション保護ステータスを視覚化します
- グラフィカルユーザインターフェイスとすべての保護ワークフローを社内ツールから実装するためのREST APIの完全なリストを提供します。

Astra Controlを使用すると、Kubernetesクラスタで作成された関連リソースの情報を含む、コンテナ化されたアプリケーションを一元的に可視化できます。すべてのクラスタ、すべてのアプリケーション、すべてのクラウド、またはすべてのデータセンターを1つのポータルで表示できます。オンプレミスまたはパブリッククラウドのすべての環境でAstra Control APIを使用して、データ管理ワークフローを実装できます。

次の図は、Astra Controlの機能を示しています。



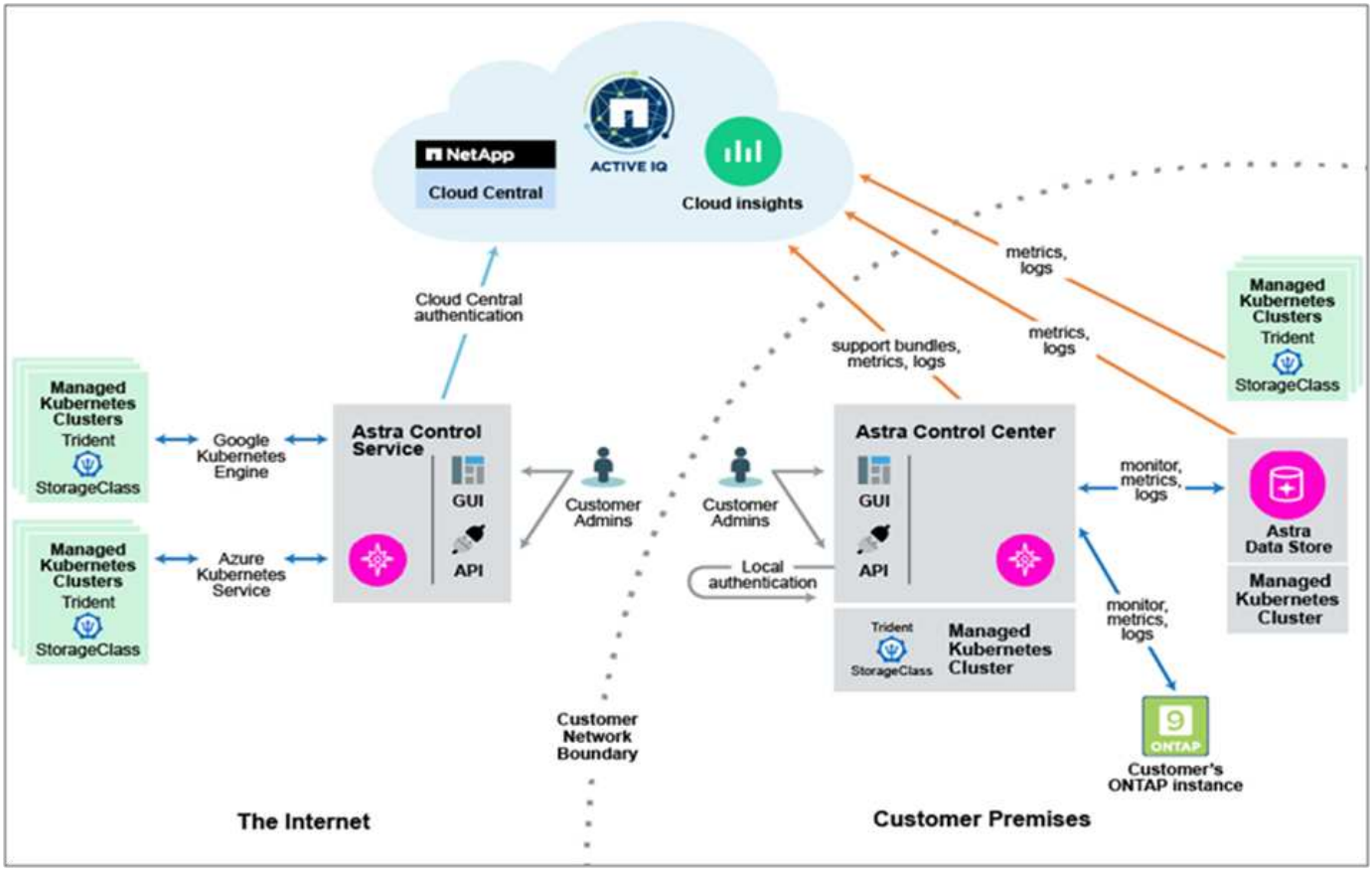
Astra Control消費モデル

Astra Controlには、次の2つの消費モデルがあります。

- * Astra Control Service。ネットアップがホストするフルマネージドサービス。Google Kubernetes Engine（GKE）、Azure Kubernetes Service（AKS）でKubernetesクラスタのアプリケーション対応データ管理を実現します。
- * Astra Control Center。*オンプレミスおよびハイブリッドクラウド環境で実行されるKubernetesクラスタのアプリケーション対応データ管理を提供する、自己管理ソフトウェアです。

このテクニカルレポートでは、Kubernetesで実行されるクラウドネイティブアプリケーションを管理するために、Astra Control Centerを活用しています。

次の図は、Astra Controlアーキテクチャを示しています。



Astra Trident

Astra Tridentは、コンテナやKubernetesディストリビューション向けの、完全にサポートされているオープンソースのストレージオーケストレーションツールです。コンテナ化されたアプリケーションの永続性に対する要求を、業界標準のインターフェイス（など）を使用して満たすことができるように、最初から設計されています "CSI（Container Storage Interface）"。Astra Tridentを使用すると、マイクロサービスやコンテナ化されたアプリケーションを利用して、ネットアップのストレージシステムポートフォリオが提供するエンタープライズクラスのストレージサービスを活用できます。

Kubernetesクラスタにポッドとして導入されるAstra Tridentは、Kubernetesワークロードに動的なストレージオーケストレーションサービスを提供します。コンテナ化されたアプリケーションは、NetApp ONTAP（NetApp AFF 、NetApp FAS 、NetApp ONTAP Select 、Cloudなど）を含むネットアップの幅広いポートフォリオから、永続的ストレージをすばやく簡単に消費できます。 さらに、Amazon FSX for NetApp ONTAP ）、NetApp Element ソフトウェア（NetApp SolidFire ）、Azure NetApp Files サービス、Google Cloud上のクラウドボリュームサービス、AWS上のクラウドボリュームサービスも利用できます。FlexPod 環境では、Astra Tridentを使用して、ネットアップのFlexVol ボリュームをベースとするコンテナや、ONTAP AFFやFAS システム、Cloud Volumes ONTAP などのストレージプラットフォームでホストされるLUNに対応するコンテナの永続的ボリュームを動的にプロビジョニングおよび管理できます。Tridentは、Astra Controlが提供するアプリケーション保護スキームの実装においても重要な役割を果たします。Astra Tridentの詳細については、を参照してください "Astra Tridentのドキュメント"

ストレージバックエンド

Astra Tridentを使用するには、サポートされているストレージバックエンドが必要です。Tridentバックエンドは、Tridentとストレージシステムの関係を定義します。Tridentは、そのストレージシステムとの通信方法や、Tridentがそのシステムからボリュームをプロビジョニングする方法を解説します。Tridentは、あるストレージクラスが定義した要件を満たしたストレージプールをバックエンドから自動的に提供します。

- ONTAP AFF と FAS のストレージバックエンド。ONTAP は、ストレージソフトウェアおよびハードウェアプラットフォームとして、コアストレージサービス、複数のストレージアクセスプロトコルのサポート、およびネットアップのSnapshotコピーやミラーリングなどのストレージ管理機能を提供します。
- Cloud Volumes ONTAP ストレージバックエンド
- "Astra データストア" ストレージバックエンド

NetApp Cloud Volumes ONTAP の略

NetApp Cloud Volumes ONTAP は、ファイルワークロードとブロックワークロードに高度なデータ管理機能を提供するSoftware-Defined Storageです。Cloud Volumes ONTAP を使用すると、データ保護、セキュリティ、コンプライアンスを強化しながら、クラウドストレージのコストを最適化し、アプリケーションのパフォーマンスを向上させることができます。

主なメリットは次のとおりです。

- 組み込みのデータ重複排除、データ圧縮、シンプロビジョニング、クローニングを活用して、ストレージコストを最小限に抑えます。
- クラウド環境で障害が発生した場合でも、エンタープライズクラスの信頼性と継続的な運用を確保できます。
- Cloud Volumes ONTAP は、業界をリードするネットアップのレプリケーションテクノロジであるSnapMirrorを活用して、オンプレミスのデータをクラウドにレプリケートします。これにより、複数のユースケースでセカンダリコピーを簡単に利用できます。
- また、 Cloud Volumes ONTAP は Cloud Backup Service との統合により、保護のためのバックアップとリストア機能、およびクラウドデータの長期アーカイブ機能を提供します。
- アプリケーションをオフラインにすることなく、ハイパフォーマンスとローパフォーマンスのストレージプールをオンデマンドで切り替えます。
- NetApp SnapCenter を使用してSnapshotコピーの整合性を確保します。
- Cloud Volumes ONTAP は、データ暗号化をサポートし、ウィルスやランサムウェアからの保護を提供します。
- クラウドデータセンスとの統合により、データコンテキストを把握し、機密データを識別できます。

Cloud Central にアクセスできます

Cloud Centralは、ネットアップのクラウドデータサービスにアクセスして管理するための一元的な場所を提供します。これらのサービスにより、重要なアプリケーションのクラウドでの実行、自動化されたDRサイトの作成、データのバックアップ、複数のクラウド間でのデータの効果的な移行と制御が可能になります。詳細については、を参照してください "Cloud Centralにアクセスできます。"

クラウドマネージャ

Cloud Managerは、エンタープライズクラスのSaaSベースの管理プラットフォームです。ITエキスパートとクラウドアーキテクトは、ネットアップのクラウドソリューションを使用して、ハイブリッドマルチクラウドインフラを一元管理できます。オンプレミスとクラウドのストレージを表示および管理する一元化されたシステムを提供し、ハイブリッドクラウド、複数のクラウドプロバイダ、アカウントをサポートします。詳細については、を参照してください "クラウドマネージャ"。

コネクタ

Connectorは、Cloud Managerがパブリッククラウド環境内のリソースとプロセスを管理できるようにするインスタンスです。Cloud Managerのさまざまな機能を使用するには、コネクタが必要です。コネクタは、クラウドまたはオンプレミスネットワークに導入できます。

Connectorは次の場所でサポートされます。

- AWS
- Microsoft Azure
- Google Cloud
- オンプレミス

コネクタの詳細については、を参照してください "リンクをクリックしてください"

NetApp Cloud Insights の略

ネットアップのクラウドインフラ監視ツールであるCloud Insights を使用すると、Astra Control Centerで管理されるKubernetesクラスタのパフォーマンスと利用率を監視できます。Cloud Insights ：ストレージ使用率とワークロードの相関関係を示します。Cloud Insights 接続を Astra コントロールセンターで有効にすると、テレメータの情報が Astra コントロールセンターの UI ページに表示されます。

NetApp Active IQ Unified Manager の略

NetApp Active IQ Unified Manager では、デザインが一新され、直感的に操作できるインターフェイスからONTAP ストレージクラスタを監視できます。コミュニティの情報やAI分析から得た情報を活用できます。運用、パフォーマンス、プロアクティブな分析情報を提供し、ストレージ環境と仮想マシン（VM）で実行される環境を包括的に分析します。ストレージインフラで問題 が発生すると、Unified Managerから問題 の詳細情報を通知して、ルート原因 の特定に役立てることができます。VMダッシュボードにはVMのパフォーマンス統計が表示されるため、VMware vSphereホストからネットワーク経由で最後にストレージへのI/Oパス全体を調査できます。一部のイベントには、問題 を修正するための対応策も用意されています。問題が発生したときにEメールやSNMPトラップで通知されるように、イベントにカスタムアラートを設定できます。Active IQ Unified Manager を使用すると、容量や使用状況の傾向を予測して問題が発生する前にプロアクティブに対処することができるため、長期的な問題につながる短期的な事後対処策を実施する必要がなくなり、ユーザのストレージ要件に合わせて計画を立てることができます。

Cisco Intersightの

Cisco Intersightは、従来のアプリケーションやクラウドネイティブなインフラに向けて、インテリジェントな自動化、オブザーバビリティ、最適化を実現するSaaSプラットフォームです。このプラットフォームは、ITチームの変化を促進し、ハイブリッドクラウド向けに設計された運用モデルを提供します。

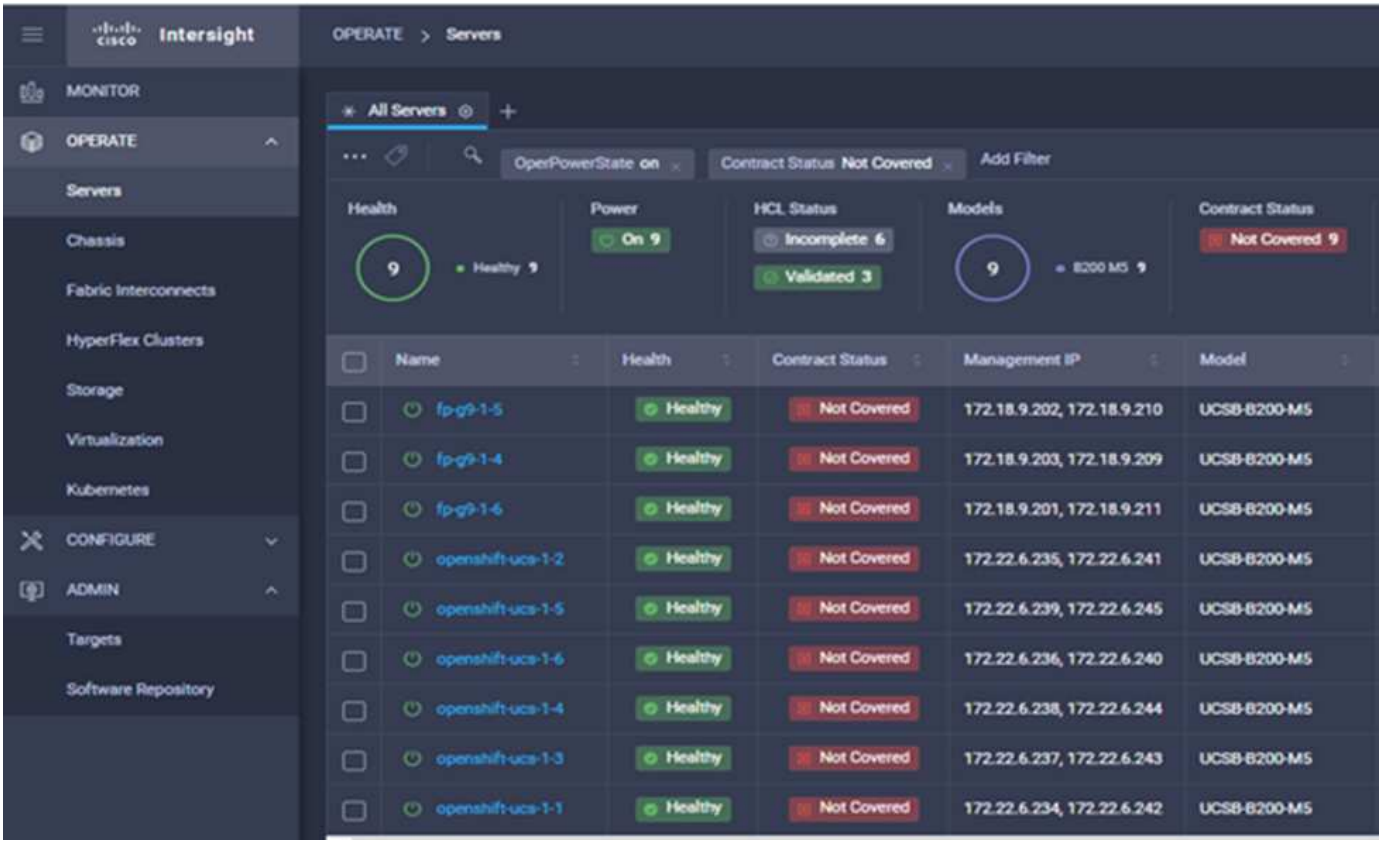
Cisco Intersightには、次のようなメリットがあります。

- *迅速な提供。*俊敏性に優れたソフトウェア開発モデルにより、クラウドまたはお客様のデータセンターからサービスとして提供され、頻繁な更新と継続的な技術革新を実現します。このようにして、お客様は基幹業務の提供を加速することに集中できます。
- *運用の簡素化。*共通のインベントリ、認証、APIを備えた単一のセキュアなSaaS提供ツールを使用して、スタック全体とすべての場所で作業し、チーム間のサイロを排除し、運用を簡素化します。オンプレミスの物理サーバやハイパーバイザーの管理からVM、Kubernetes、サーバレス、自動化、 オンプレミスとパブリッククラウドの両方にわたって最適化とコスト管理を実現

- 継続的な最適化。 Cisco Intersightが提供するインテリジェンスを、Cisco TACだけでなくすべてのレイヤで使用して、環境を継続的に最適化します。このインテリジェンスは、推奨される自動化可能なアクションに変換されるため、ワークロードの移動や物理サーバの稼働状態の監視からKubernetesクラスタの自動サイジングまで、あらゆる変更にリアルタイムで対応できます。また、コスト削減のために、作業中のパブリッククラウドが推奨されます。

Cisco Intersightには、UCSM Managed Mode（UMM）とIntersight Managed Mode（IMM）という2つの管理操作モードがあります。ファブリックインターコネクトの初期セットアップ中に、ファブリック接続Cisco UCSシステムのネイティブUmmまたはIMMを選択できます。この解決策 では、ネイティブUmmが使用されます。

次の図は、Cisco Intersightのダッシュボードを示しています。



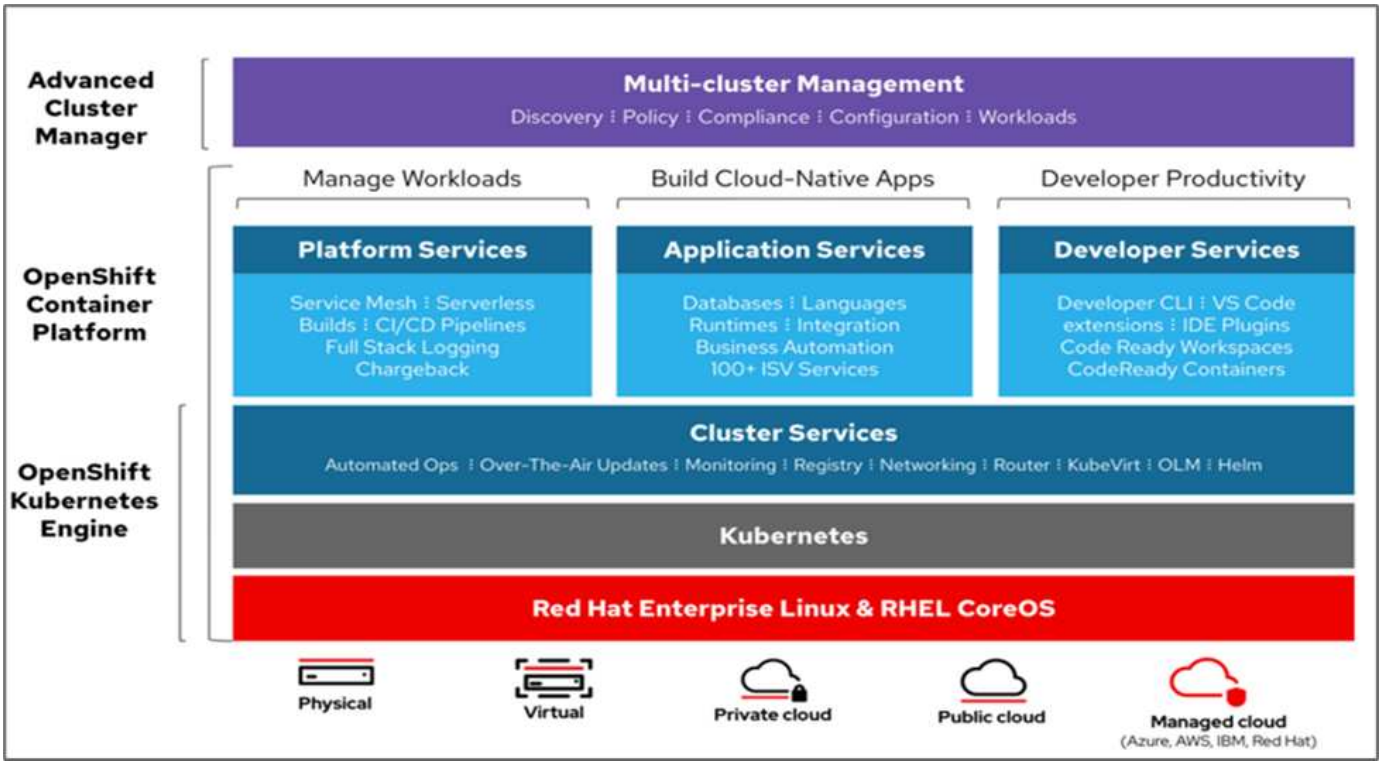
Red Hat OpenShift Container Platform

Red Hat OpenShift Container Platformは、CRI-OとKubernetesを統合し、これらのサービスを管理するためのAPIとWebインターフェイスを提供するコンテナアプリケーションプラットフォームです。CRI-Oは、Kubernetes Container Runtime Interface（CRI）を実装したもので、Open Container Initiative（OCI）互換のランタイムを使用した実行を可能にします。Kubernetesの実行時にDockerを使用する代わりに、軽量なソリューションです。

OpenShift Container Platformにより、お客様はコンテナを作成および管理できます。コンテナは、オペレーティングシステムや基盤のインフラとは無関係に、それぞれの環境で実行されるスタンドアロンプロセスです。OpenShift Container Platformは、コンテナベースのアプリケーションの開発、導入、管理を支援します。アプリケーションをオンデマンドで作成、変更、および導入できるセルフサービスプラットフォームを提供し、開発とリリースのライフサイクルを短縮します。OpenShift Container Platformには、より小規模で分離されたユニットで構成されるマイクロサービスベースのアーキテクチャがあり、連携して機能します。Kubernetesクラスタ上で実行され、信頼性の高いクラスタキーバリュー型データストアであるetcdに格納

されているオブジェクトに関するデータが含まれます。

次の図は、Red Hat OpenShift Containerプラットフォームの概要を示しています。



Kubernetesインフラ

Kubernetesは、OpenShift Container Platform内で、コンテナ化されたアプリケーションを一連のCRI-Oランタイムホスト全体で管理し、導入、メンテナンス、アプリケーション拡張のためのメカニズムを提供します。CRI-Oサービスは、コンテナ化されたアプリケーションをインスタンス化し、実行します。

Kubernetesクラスタは、1つ以上のマスターノードと一連のワーカーノードで構成されます。この解決策 設計には、ハードウェアのハイアベイラビリティ（HA）機能とソフトウェアスタックが含まれています。Kubernetesクラスタは、3つのマスターノードと最低2つのワーカーノードでHAモードで実行されるように設計されており、クラスタに単一点障害がないようにします。

Red Hatコア**OS**

OpenShift Container Platformは、Red Hat Enterprise Linux CoreOS（RHCOS）を使用します。RHCOSは、CoreOSとRed Hat Atomic Host OSの優れた機能を組み合わせたコンテナ指向のオペレーティングシステムです。RHCOSは、コンテナ化されたアプリケーションをOpenShift Container Platformから実行できるように特別に設計されており、新しいツールと連携して、迅速なインストール、オペレータベースの管理、簡単なアップグレードを実現します。

RHCOSには次の機能があります。

- イグニションは、最初にマシンを起動して構成する際に、OpenShift Container Platformが最初のブートシステム構成として使用するものです。
- Kubernetesネイティブのコンテナランタイム実装であるCRI-Oは、オペレーティングシステムと緊密に統合して、Kubernetes環境を効率的かつ最適化します。CRI-Oには、コンテナの実行、停止、再起動を行う機能があります。これは、OpenShift Container Platform 3で使用されていたDocker Container Engineに完

全に代わるものです。

- Kubernetesの主要ノードエージェントであるKubeletはコンテナの起動と監視を担当しています。

VMware vSphere 7.0

VMware vSphereは、大量のインフラ（CPU、ストレージ、ネットワークなどのリソース）をシームレスで汎用性に優れた動的な運用環境として包括的に管理する仮想化プラットフォームです。個々のマシンを管理する従来のオペレーティングシステムとは異なり、VMware vSphereはデータセンター全体のインフラストラクチャを集約して、必要なアプリケーションに迅速かつ動的に割り当てられるリソースを備えた単一の強力なサーバを作成します。

詳細については、を参照してください "VMware vSphere の場合"。

VMware vSphere vCenterの場合

VMware vCenter Serverでは、1つのコンソールからすべてのホストとVMを統合的に管理でき、クラスタ、ホスト、およびVMのパフォーマンス監視を集約できます。VMware vCenter Serverを使用すると、管理者は、コンピューティングクラスタ、ホスト、VM、ストレージ、ゲストOS、 仮想インフラストラクチャのその他の重要なコンポーネントVMware vCenterは、VMware vSphere環境で使用できる豊富な機能を管理します。

ハードウェアおよびソフトウェアのリビジョン

この解決策 は、で定義されている、サポートされているバージョンのソフトウェア、ファームウェア、およびハードウェアを実行している任意のFlexPod 環境に拡張できます "NetApp Interoperability Matrix Tool で確認できます" および "Cisco UCSハードウェア互換性リスト。" OpenShiftクラスタは、VMware vSphereだけでなくベアメタル方式でFlexPod にインストールされます。

複数のOpenShift（k8s）クラスタを管理するために必要なのはAstra Control Centerの1つのインスタンスだけです。各OpenShiftクラスタにはTrident CSIがインストールされています。Astra Control Centerは、このようなOpenShiftクラスタのいずれにもインストールできます。この解決策 では、OpenShiftベアメタルクラスタにAstraコントロールセンターをインストールします。

次の表に、OpenShift用のFlexPod ハードウェアおよびソフトウェアのリビジョンを示します。

コンポーネント	プロダクト	バージョン
コンピューティング	Cisco UCSファブリックインターコネクト6454	4.1（3c）
	Cisco UCS B200 M5サーバ	4.1（3c）
ネットワーク	Cisco Nexus 9336C-FX2 NX-OS	9.3（8）
ストレージ	NetApp AFF A700	9.11.1
	ネットアップアストラコントロールセンター	22.04.0
	NetApp Astra Trident CSIプラグイン	22.04.0
	NetApp Active IQ Unified Managerの略	9.11
ソフトウェア	VMware ESXi nenic イーサネットドライバ	1.0.35.0

コンポーネント	プロダクト	バージョン
	vSphere ESXiの場合	7.0（U2）
	VMware vCenter Applianceの略	7.0 U2b
	Cisco Intersight Assist仮想アプライアンス	1.0.9-342
	OpenShift Container Platform	4.9
	OpenShift Container Platformマスターノード	RHCOS 4.9
	OpenShift Container Platform Workerノード	RHCOS 4.9

次の表に、AWS上のOpenShift用のソフトウェアバージョンを示します。

コンポーネント	プロダクト	バージョン
コンピューティング	マスターインスタンスタイプ：m5.xlarge	該当なし
	ワーカーインスタンスタイプ：m5.large	該当なし
ネットワーク	Virtual Private Cloud Transit Gatewayの略	該当なし
ストレージ	NetApp Cloud Volumes ONTAP の略	9.11.1
	NetApp Astra Trident CSIプラグイン	22.04.0
ソフトウェア	OpenShift Container Platform	4.9
	OpenShift Container Platformマスターノード	RHCOS 4.9
	OpenShift Container Platform Workerノード	RHCOS 4.9

"次の例：FlexPod for OpenShift Container Platform 4ベアメタルインストール"

インストールと設定

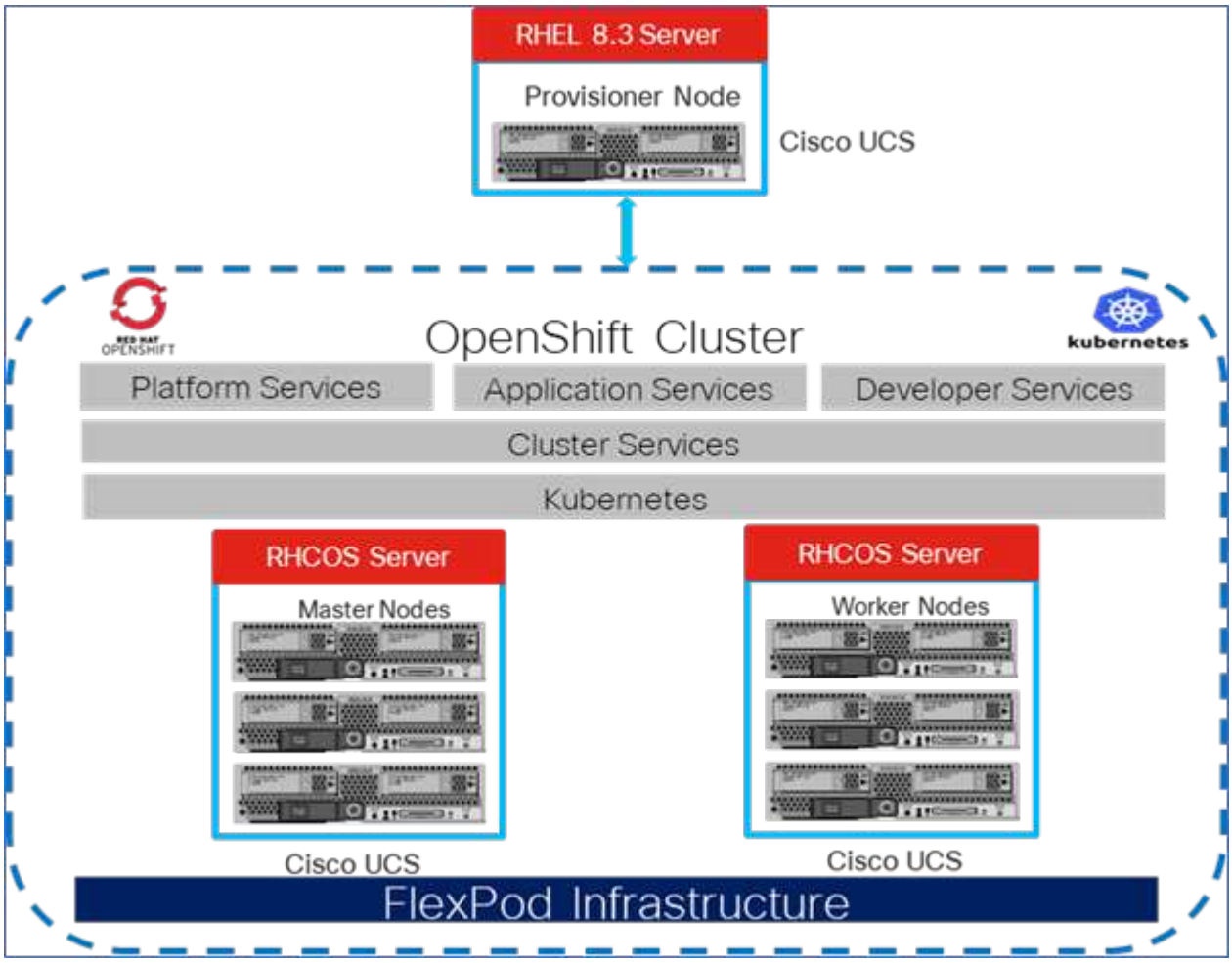
FlexPod for OpenShift Container Platform 4ベアメタルインストール

"前の図：解決策 コンポーネント。"

FlexPod for OpenShift Container Platform 4のベアメタル設計、導入の詳細、およびNetApp Astra Tridentのインストールと設定については、を参照してください "FlexPod with OpenShift Cisco Validated Design and Deploymentガイド（CVD）"。このCVDでは、Ansibleを使用したFlexPod およびOpenShift Container Platformの導入について説明します。CVDには、ワーカーノード、Astra Tridentインストール、ストレージバックエンド、ストレージクラス構成の準備に関する詳細も記載されています。この構成

は、Astra Control Centerの導入と構成を行うためのいくつかの前提条件です。

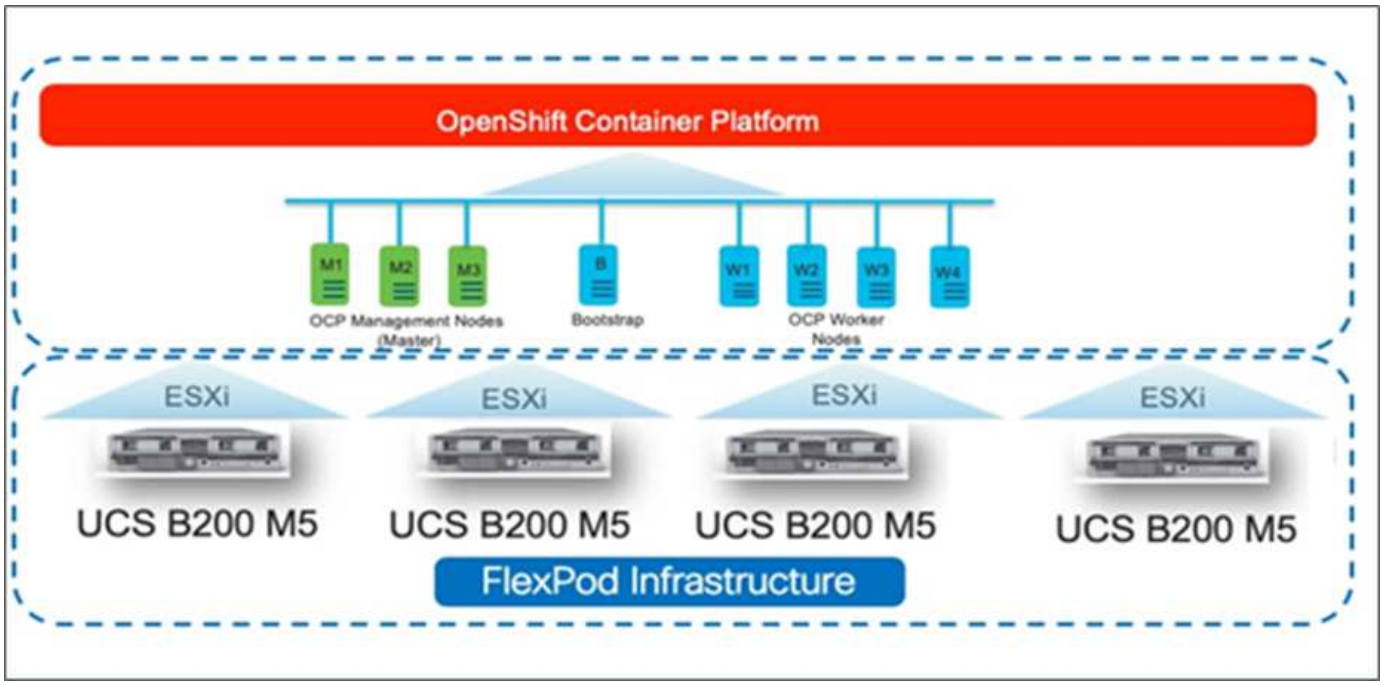
次の図は、FlexPod 上のOpenShift Container Platform 4ベアメタルを示しています。



VMware環境に実装された**OpenShift Container Platform 4**用**FlexPod**

VMware vSphereを実行しているFlexPod にRed Hat OpenShift Container Platform 4を導入する方法については、を参照してください "OpenShift Container Platform 4のFlexPod データセンター"。

次の図は、vSphere上のOpenShift Container Platform 4のFlexPod を示しています。

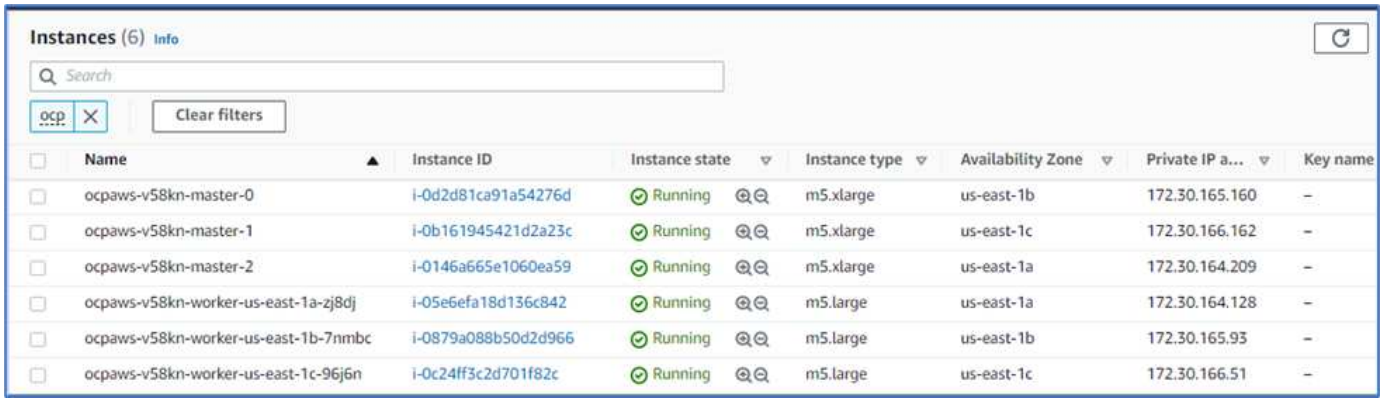


"次の例は、AWSでRed Hat OpenShiftを実装したものです。"

AWSに**Red Hat OpenShift**を実装しました

"従来：FlexPod for OpenShift Container Platform 4ベアメタルインストール"

DRサイトとしてAWSに実装された、独立した自己管理OpenShift Container Platform 4クラスタです。マスターノードとワーカーノードは、3つのアベイラビリティゾーンにまたがって配置されるため、高可用性が実現します。



```
[ec2-user@ip-172-30-164-92 ~]$ oc get nodes
NAME                                STATUS   ROLES    AGE   VERSION
ip-172-30-164-128.ec2.internal   Ready    worker   29m   v1.22.8+f34b40c
ip-172-30-164-209.ec2.internal   Ready    master   36m   v1.22.8+f34b40c
ip-172-30-165-160.ec2.internal   Ready    master   33m   v1.22.8+f34b40c
ip-172-30-165-93.ec2.internal    Ready    worker   30m   v1.22.8+f34b40c
ip-172-30-166-162.ec2.internal   Ready    master   36m   v1.22.8+f34b40c
ip-172-30-166-51.ec2.internal    Ready    worker   28m   v1.22.8+f34b40c
```

OpenShiftはとして導入されます "プライベートクラスタ" AWS上の既存のVPCに接続できます。プライベートOpenShift Container Platformクラスタは外部エンドポイントを公開しないため、内部ネットワークからのみアクセスでき、インターネットには表示されません。シングルノードのNetApp Cloud Volumes ONTAPは、NetApp Cloud Managerを使用して導入されます。これにより、TridentからAstraにバックエンドとしてストレージが提供されます。

AWSへのOpenShiftのインストールの詳細については、を参照してください "OpenShiftのドキュメント"。

"次のステップ：NetApp Cloud Volumes ONTAP"

NetApp Cloud Volumes ONTAP の略

"以前は、AWSでRed Hat OpenShiftを利用していました。"

NetApp Cloud Volumes ONTAP インスタンスはAWSに導入され、Astra Tridentのバックエンドストレージとして機能します。Cloud Volumes ONTAP 作業環境を追加する前に、コネクタを配置する必要があります。コネクタを配置せずにCloud Volumes ONTAP の最初の作業環境を作成するかどうかを確認するメッセージが表示されます。AWSにコネクタを導入するには、を参照してください "コネクタを作成します"。

AWSにCloud Volumes ONTAP を導入する手順については、を参照してください "AWSでのクイックスタート"。

Cloud Volumes ONTAP を導入したら、Astra Tridentをインストールし、OpenShift Container Platformクラスタでストレージバックエンドとスナップショットクラスを設定できます。

"次は、OpenShift Container PlatformにAstra Control Centerをインストールする方法です。"

OpenShift Container Platformに**Astra Control Center**をインストールします

"Previous：NetApp Cloud Volumes ONTAP の略。"

FlexPod で実行されているOpenShiftクラスタ、またはCloud Volumes ONTAP ストレージバックエンドを使用するAWSにAstraコントロールセンターをインストールできます。この解決策 では、OpenShiftベアメタルクラスタにAstraコントロールセンターを導入します。

Astra Control Centerは、説明されている標準的なプロセスを使用してインストールできます "こちらをご覧ください" または、Red Hat OpenShift OperatorHubから入手してください。Astra Control Operatorは、Red Hat

認定オペレータです。この解決策 では、AstraコントロールセンターはRed Hat OperatorHubを使用してインストールされます。

環境要件

- Astra Control Centerは複数のKubernetesディストリビューションをサポートします。Red Hat OpenShiftでは、Red Hat OpenShift Container Platform 4.8または4.9がサポートされます。
- Astra Control Centerでは、環境およびエンドユーザーのアプリケーションリソース要件に加えて、次のリソースが必要です。

コンポーネント	要件
ストレージバックエンドの容量	500GB以上の容量があります
ワーカーノード	少なくとも3つのワーカーノードがあり、それぞれ4つのCPUコアと12GBのRAMが搭載されています
Fully Qualified Domain Name（FQDN；完全修飾ドメイン名）アドレス	Astra Control Center の FQDN アドレス
Astra Trident	Astra Trident 21.04 以降がインストールおよび設定されている
入力コントローラまたはロードバランサ	入力コントローラでURLまたはロードバランサを使用してAstra Control Centerを公開し、FQDNに解決されるIPアドレスを提供するように設定します

- 既存のプライベートイメージレジストリが必要です。このレジストリには、Astra Control Centerビルドイメージをプッシュできます。イメージをアップロードするイメージレジストリのURLを指定する必要があります。

一部のイメージは特定のワークフローの実行中にプルされ、必要に応じてコンテナが作成および破棄されます。

- Astra Control Center を使用するには、ストレージクラスを作成してデフォルトのストレージクラスとして設定する必要があります。Astra Control Center は、 Astra Trident が提供する次の ONTAP ドライバをサポートしています。
  - ONTAP - NAS
  - ONTAP-NAS-flexgroup
  - ONTAP - SAN
  - ONTAP - SAN - 経済性

導入したOpenShiftクラスタにAstra Tridentがインストールされ、ONTAP バックエンドで設定されているとします。また、デフォルトのストレージクラスも定義されています。

- OpenShift環境でアプリケーションクローニングを行う場合、Astra Control CenterはOpenShiftでボリュームをマウントし、ファイルの所有権を変更できるようにする必要があります。これらの処理を許可するようにONTAP エクスポートポリシーを変更するには、次のコマンドを実行します。

```
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -superuser sys
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -anon 65534
```

管理対象のコンピューティングリソースとして2つ目のOpenShift運用環境を追加するには、Astra Tridentボリュームスナップショット機能が有効になっていることを確認します。Tridentを使用してボリュームSnapshotを有効にし、テストする方法については、を参照してください "Astra Tridentの手順"。

- A "VolumeSnapClass" アプリケーションの管理元であるすべてのKubernetesクラスタで設定する必要があります。Astra Control Centerがインストールされているクラスタも含めることができます。Astra Control Centerでは、実行中のKubernetesクラスタ上のアプリケーションを管理できます。

アプリケーション管理の要件

- ライセンス。 Astra Control Centerを使用してアプリケーションを管理するには、Astra Control Centerライセンスが必要です。
- *名前空間。*名前空間は、Astra Control Centerによってアプリケーションとして管理できる最大のエンティティです。既存のネームスペース内のアプリケーションラベルとカスタムラベルに基づいてコンポーネントを除外し、リソースのサブセットをアプリケーションとして管理できます。
- * StorageClass.* StorageClassが明示的に設定されたアプリケーションをインストールし、アプリケーションのクローンを作成する必要がある場合、クローン処理のターゲットクラスタに最初に指定されたStorageClassが必要です。明示的にStorageClassを設定したアプリケーションを、同じストレージクラスを持たないクラスタにクローニングすると失敗します。
- * Kubernetesのリソース。* Astra Controlではキャプチャされないkubernetesリソースを使用するアプリケーションには、アプリケーションデータの完全な管理機能が備わっていない可能性があります。Astra Controlでは、次のKubernetesリソースをキャプチャできます。

Kubernetesのリソース		
クラスタロール	ClusterRoleBinding	ConfigMap
CustomResourceDefinition の場合	CustomResource の場合	cronjob
デモンセット（ DemonSet ）	HorizontalPodAutoscaler のように表示されます	入力
DeploymentConfig	MutingWebhook	PersistentVolumeClaim のように表示され
ポッド	PodDisruptionBudget （予算の廃止）	PodTemplate
ネットワークポリシー	ReplicaSet	ロール
RoleBinding です	ルート	秘密
検証 Webhook		

OpenShift OperatorHub を使用して **Astra Control Center** をインストールします

次の手順 は、Red Hat OperatorHubを使用してAstraコントロールセンターをインストールします。この解決策 では、FlexPod 上で動作するベアメタルOpenShiftクラスタにAstraコントロールセンターをインストールします。

1. から Astra Control Center バンドル（「 Astra - control-ccenter-[version].tar.gz` ）をダウンロードします "NetApp Support Site"。
2. からAstra Control Centerの証明書とキーの.zipファイルをダウンロードします "NetApp Support Site"。
3. バンドルの署名を確認します。

```
openssl dgst -sha256 -verify astra-control-center[version].pub
-signature <astra-control-center[version].sig astra-control-
center[version].tar.gz
```

4. Astraの画像を抽出します。

```
tar -vxzf astra-control-center-[version].tar.gz
```

5. Astra ディレクトリに移動します。

```
cd astra-control-center-[version]
```

6. イメージをローカルレジストリに追加します。

```
For Docker:
docker login [your_registry_path]OR
For Podman:
podman login [your_registry_path]
```

7. 適切なスクリプトを使用して、イメージをロードし、イメージにタグを付け、ローカルレジストリにプッシュします。

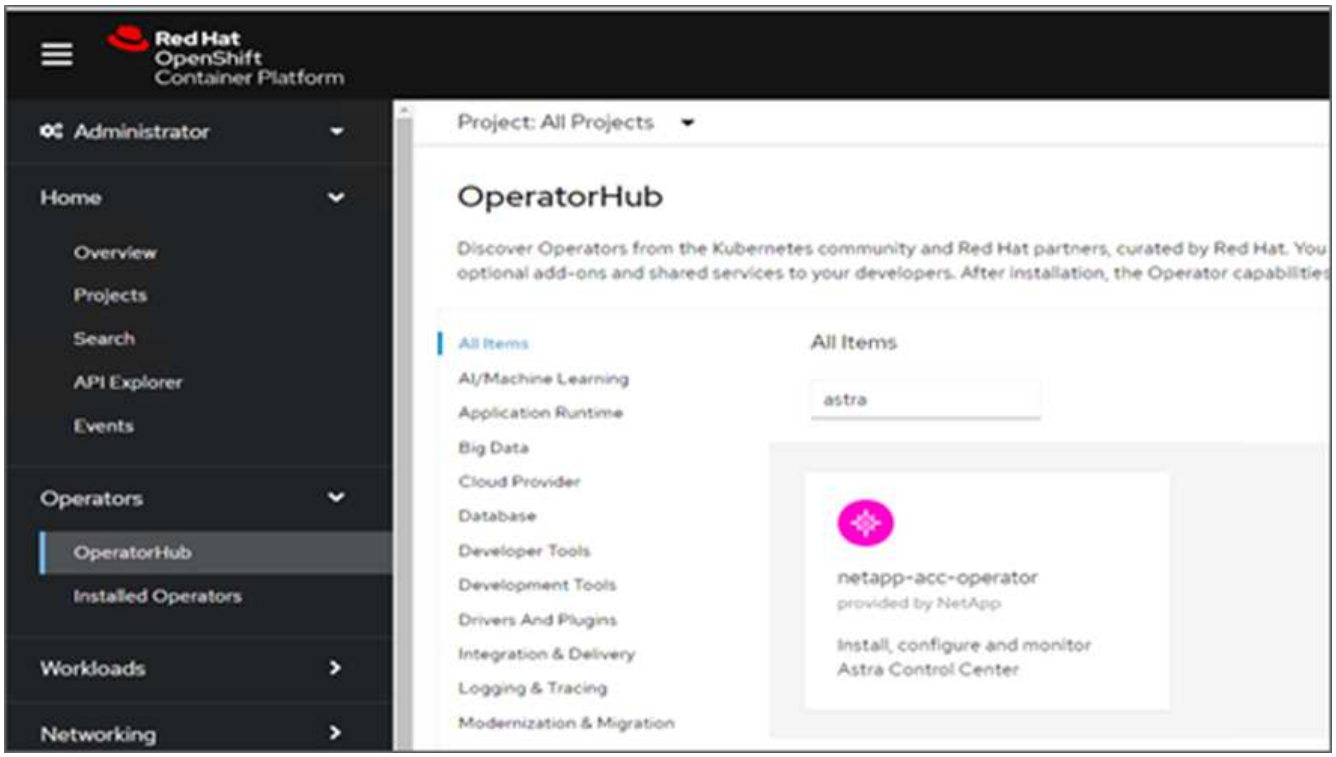
   Docker の場合：

```
export REGISTRY=[Docker_registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(docker load --input ${astraImageFile} | sed 's/Loaded
image: //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  docker tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  docker push ${REGISTRY}/${astraImage}
done
```

Podman の場合：

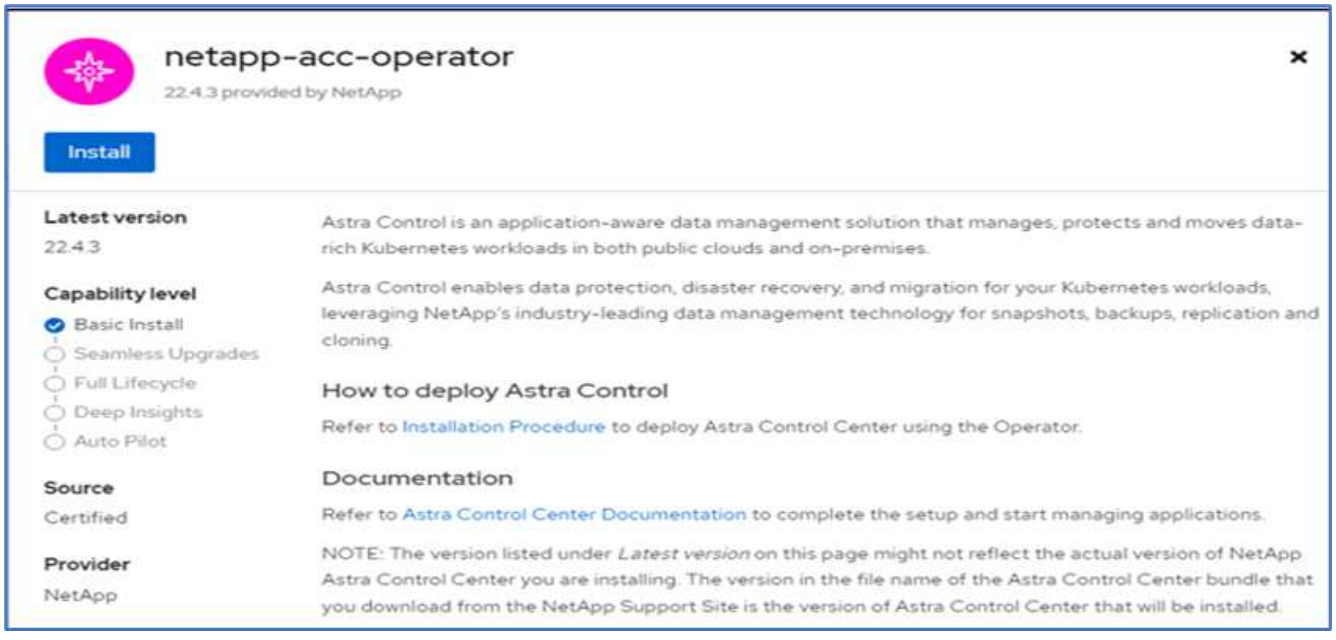
```
export REGISTRY=[Registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  podman push ${REGISTRY}/${astraImage}
done
```

8. ベアメタルOpenShiftクラスタのWebコンソールにログインします。サイドメニューから、[演算子]>[演算子ハブ]を選択します。「stra」と入力して、「NetApp-acc-operator」のリストを表示します。

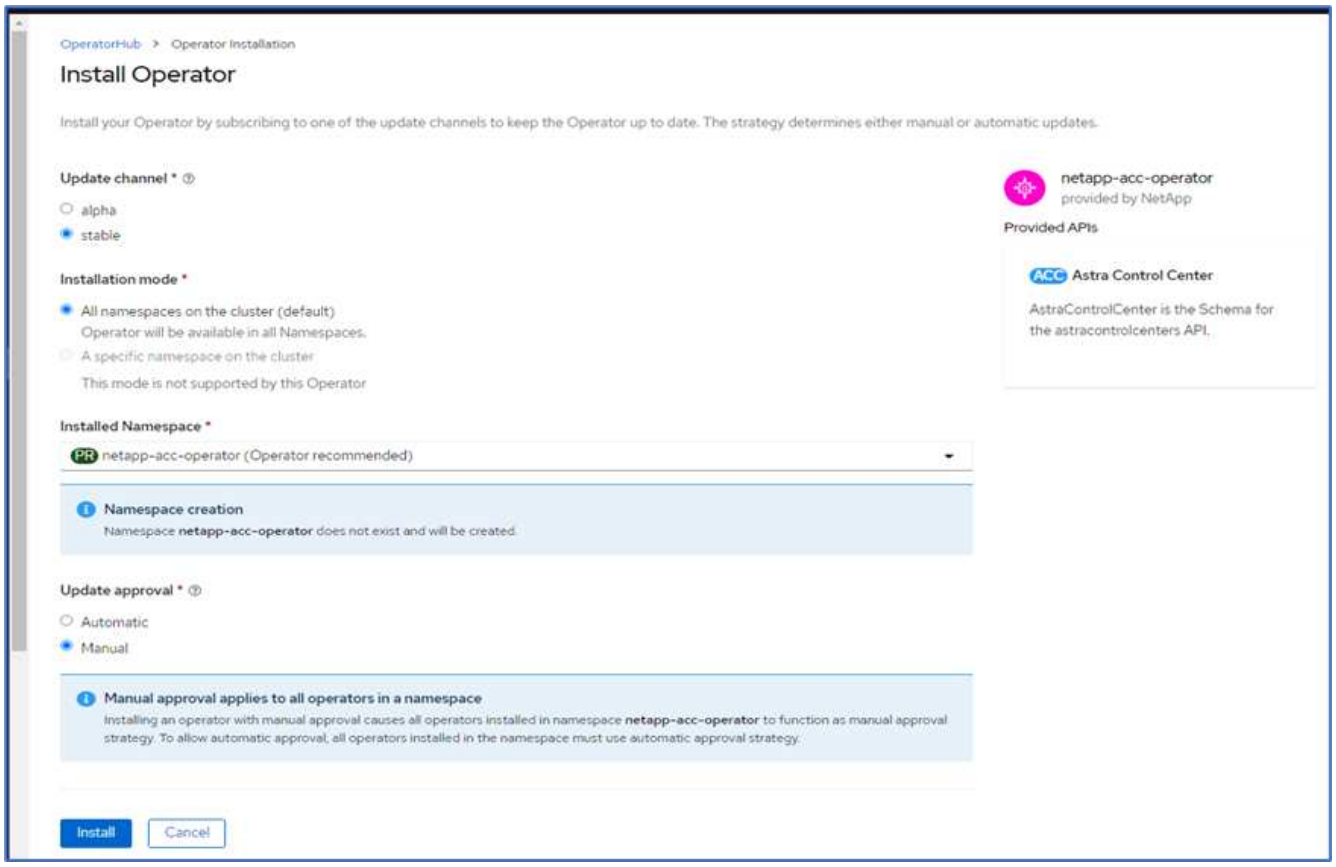


「NetApp-acc-operator」は、Red Hat OpenShift Operatorの認定を受けたもので、OperatorHubカタログの下にリストされています。

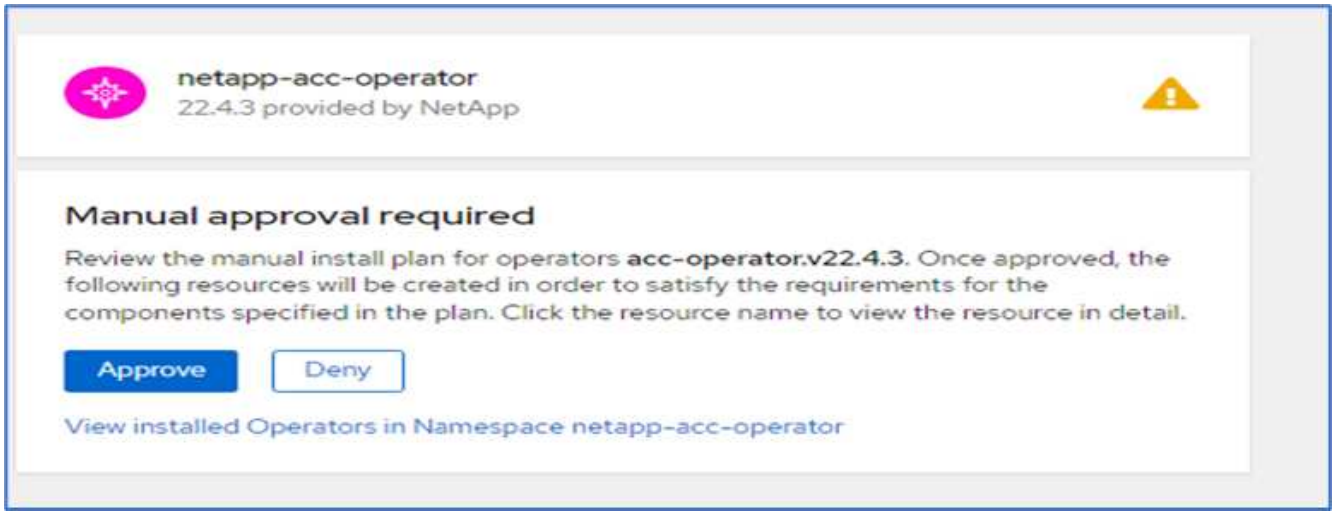
9. 「NetApp-acc-operator」を選択し、「Install」をクリックします。



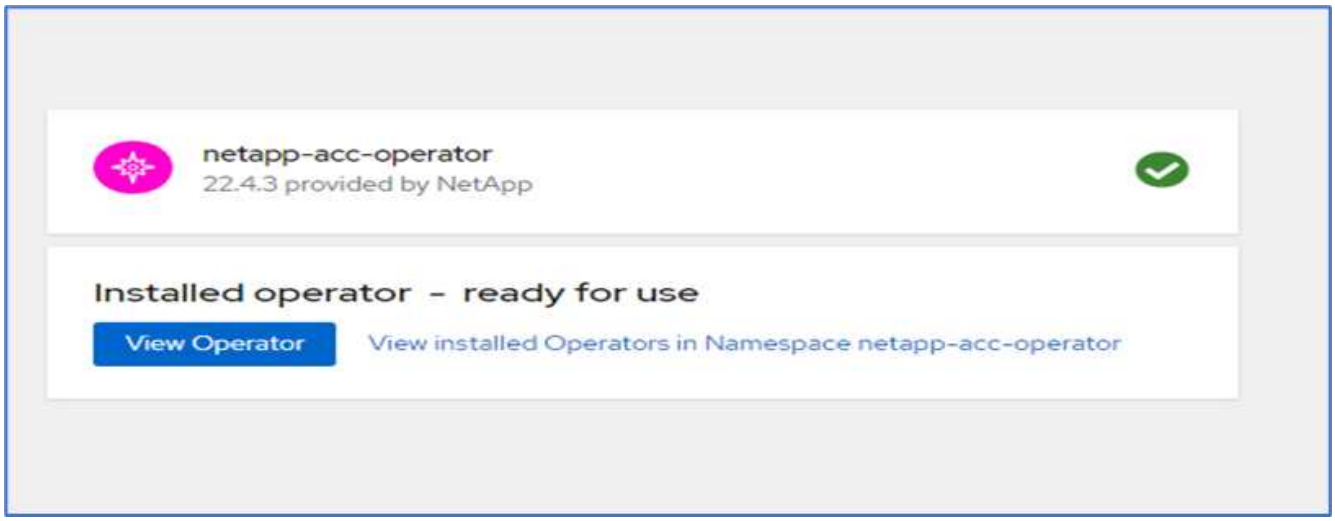
10. 適切なオプションを選択し、[インストール]をクリックします。



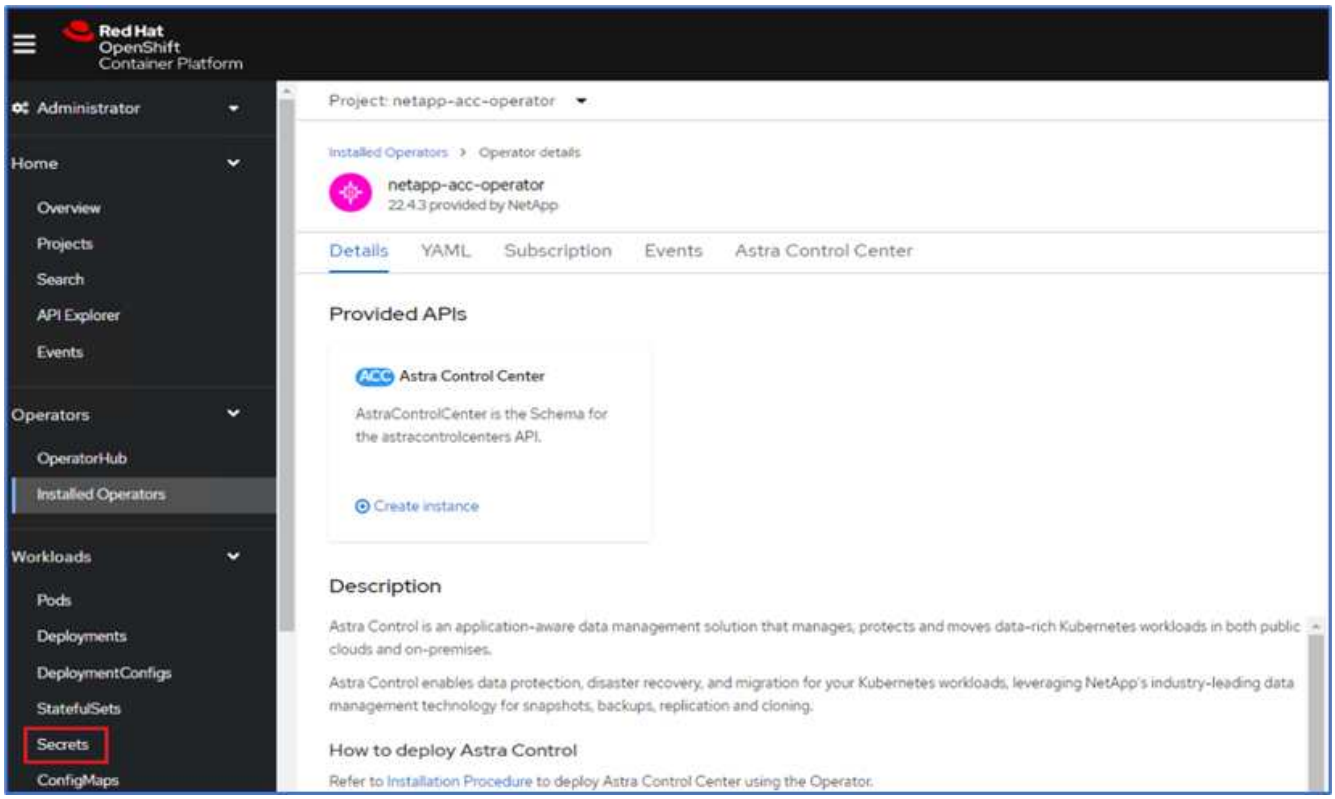
11. インストールを承認し、オペレータがインストールされるまで待ちます。



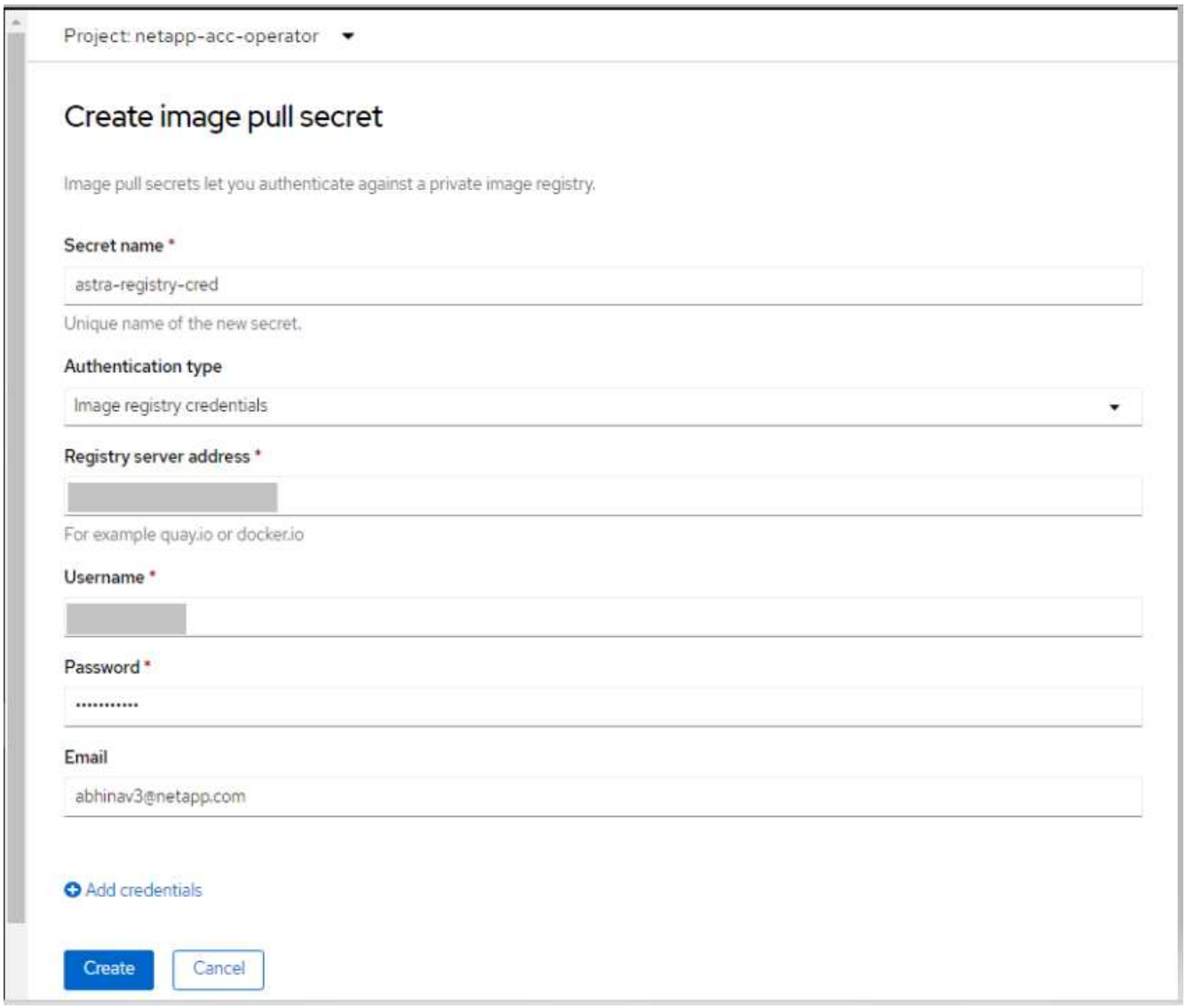
12. この段階で、オペレータは正常にインストールされ、使用可能な状態になります。View Operator（オペレーターの表示）をクリックして、Astra Control Centerのインストールを開始します。



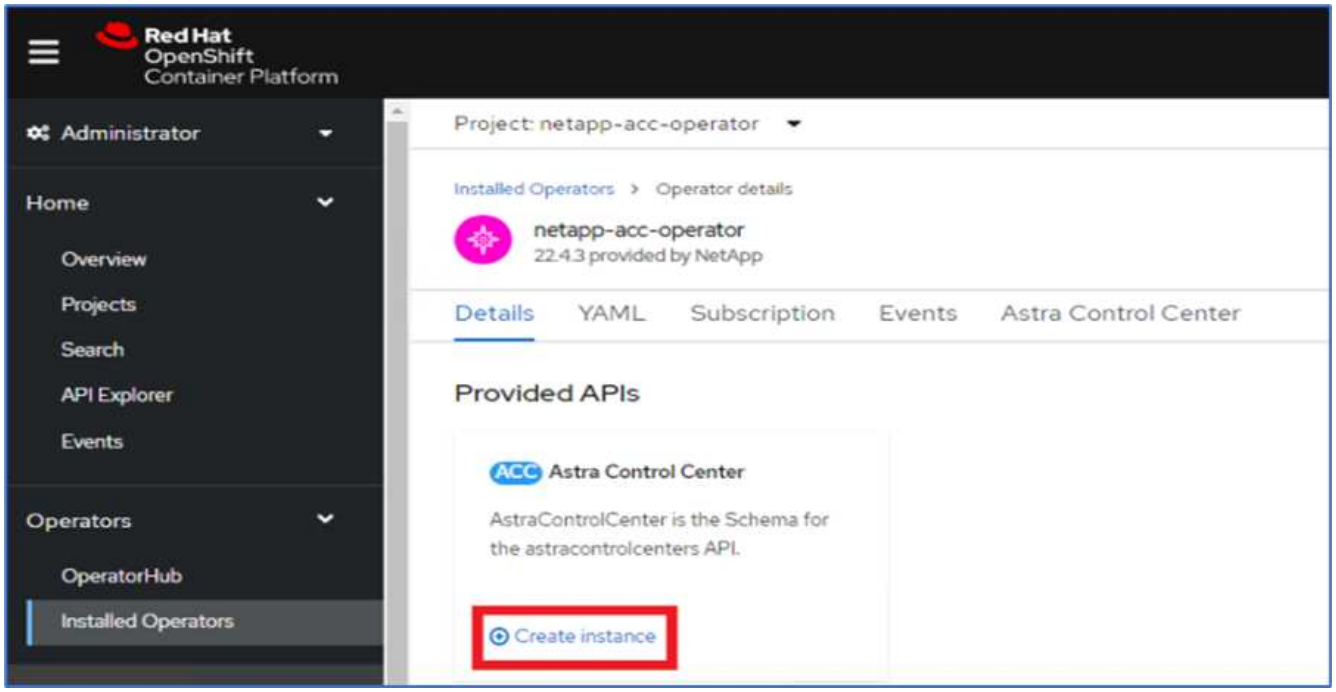
13. Astra Control Centerをインストールする前に、事前にプッシュしたDockerレジストリからAstraイメージをダウンロードするプルシークレットを作成します。



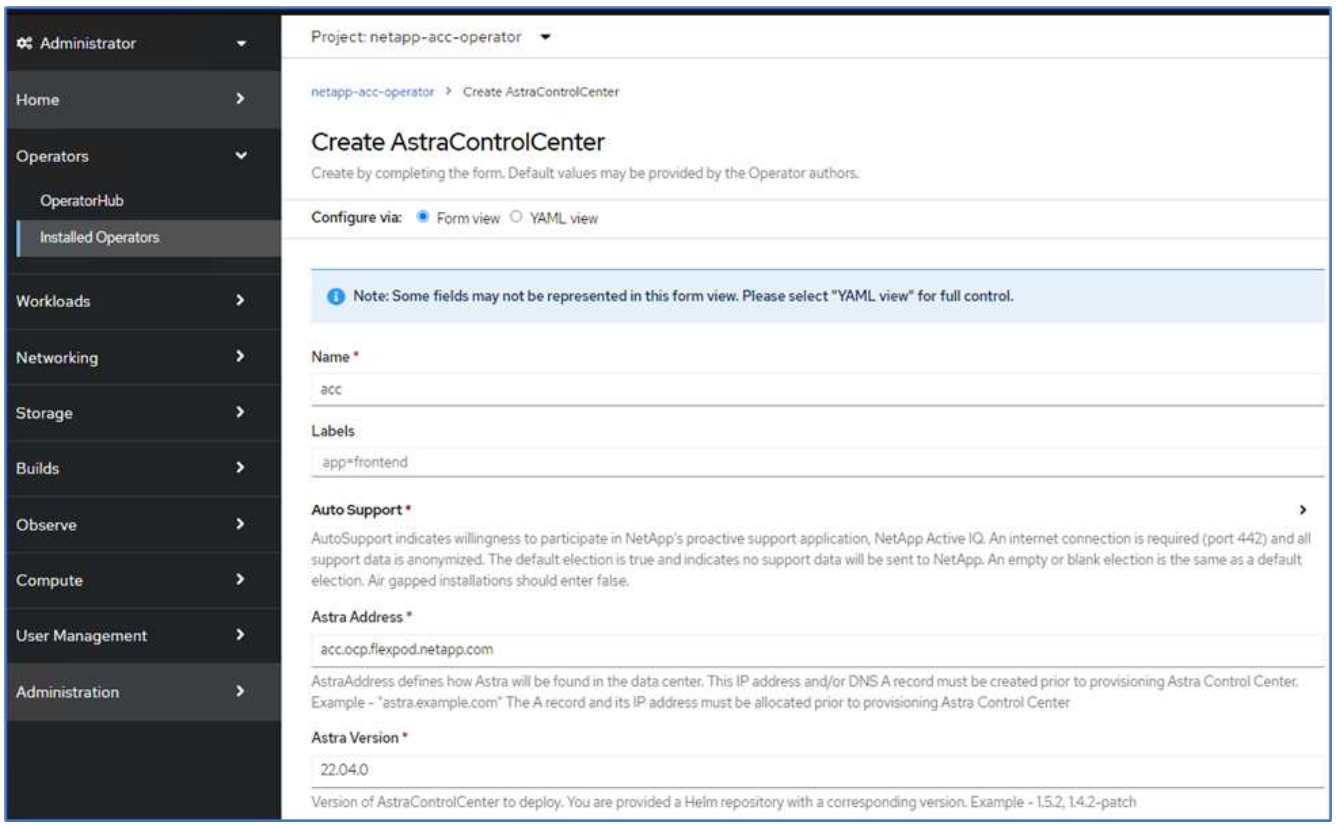
14. Astra Control Centerのイメージを Docker private repoから取得するには、NetApp-acc-operator'ネームスペースにシークレットを作成します。このシークレット名は、後の手順でAstra Control Center YAMLマニフェストに表示されます。



15. サイドメニューから、[演算子]>[インストールされた演算子]を選択し、[提供されたAPI]セクションの下にある[インスタンスの作成]をクリックします。



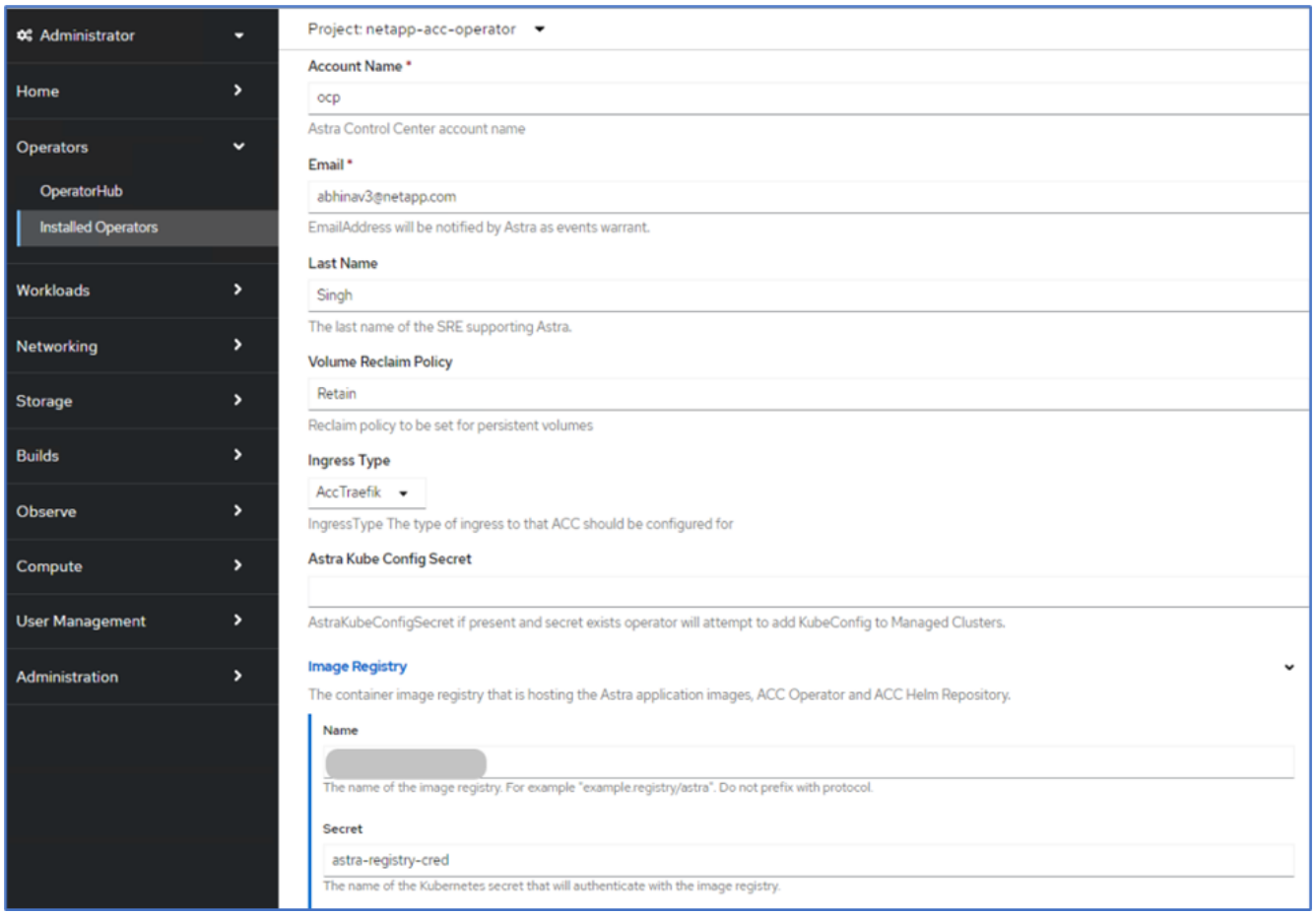
16. Create AstraControlCenterフォームに入力します名前、Astraアドレス、Astraバージョンを入力します。



[Astra Address]で、Astra Control CenterのFQDNアドレスを入力します。このアドレスは、Astra Control CenterのWebコンソールにアクセスするために使用されます。FQDNは、到達可能なIPネットワークにも解決される必要があり、DNSで設定する必要があります。

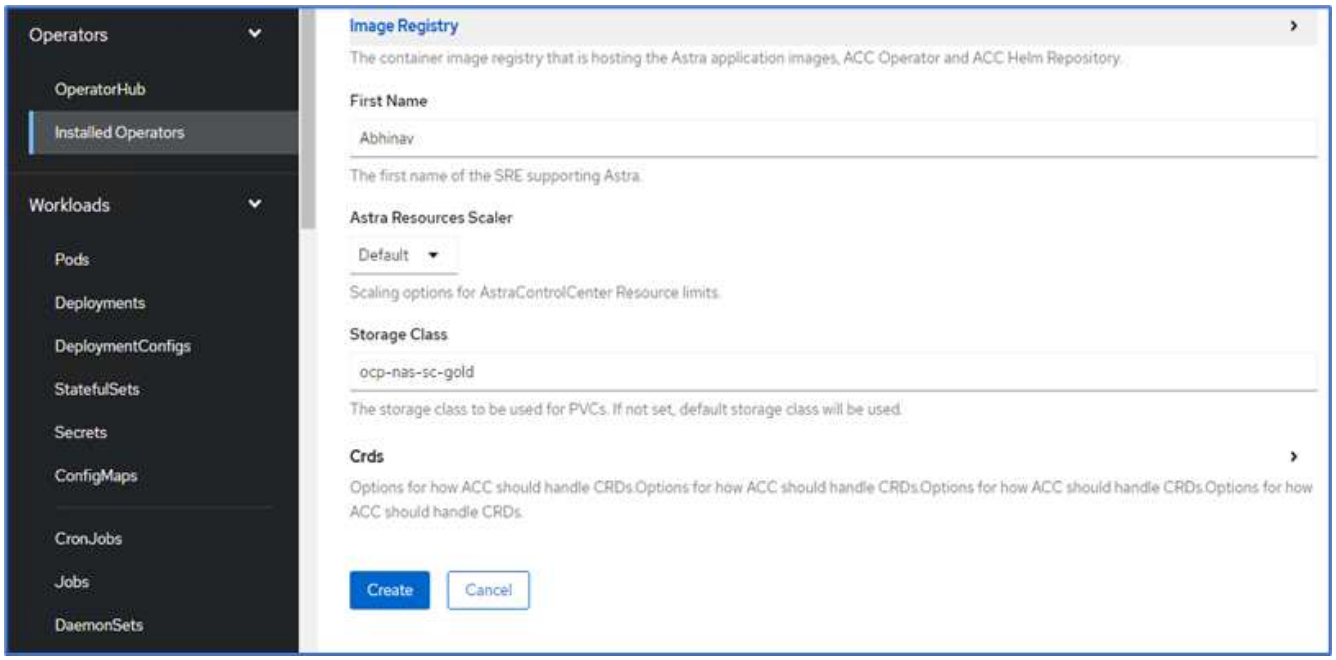
17. アカウント名、Eメールアドレス、管理者の姓を入力し、デフォルトのボリューム再利用ポリシーをその

まま使用します。ロードバランサを使用している場合は、入力タイプを「AccTraefik」に設定します。それ以外の場合は、「Ingress .Controller」で「Generic」を選択します。イメージレジストリで、コンテナイメージのレジストリパスとシークレットを入力します。

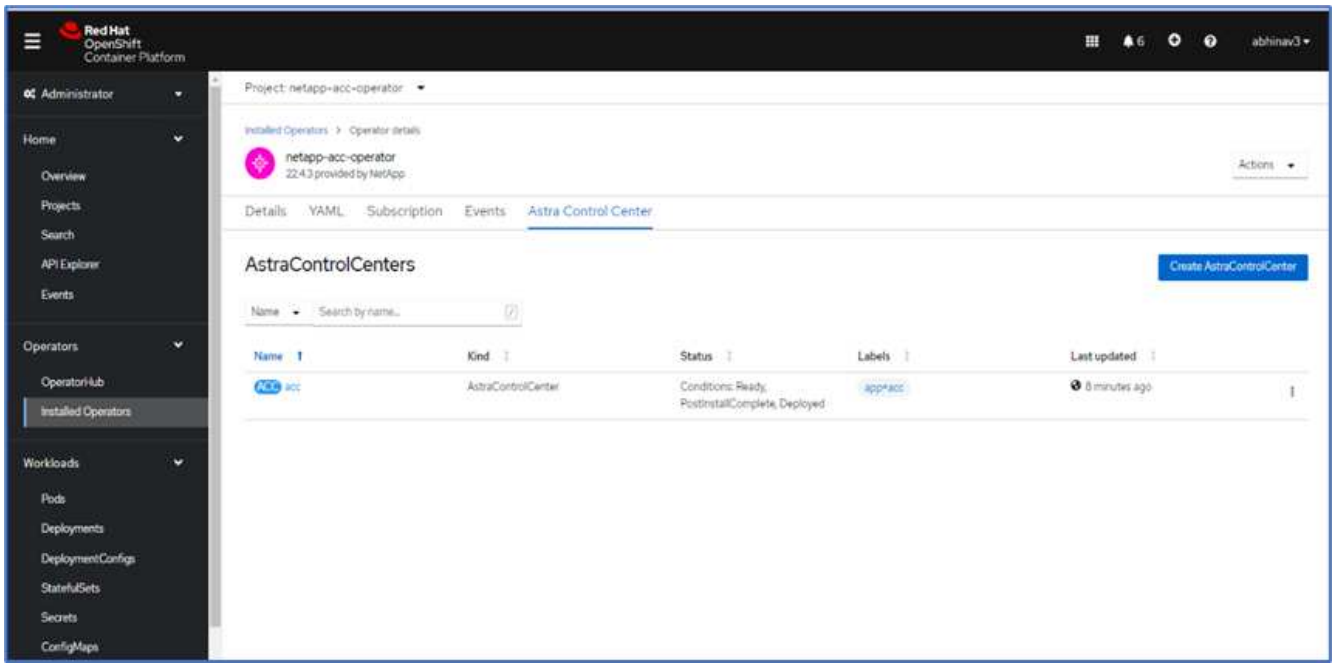


この解決策 では、Metallbロードバランサが使用されます。したがって、入力タイプはAccTraefikです。これにより、Astra Control Center traefikゲートウェイが、LoadBalancerタイプのKubernetesサービスとして公開されます。

18. 管理者の名を入力し、リソースの拡張を設定して、ストレージクラスを指定します。Create をクリックします。 .



Astra Control Centerインスタンスのステータスは、[Deploying]から[Ready]に変わります。



19. すべてのシステムコンポーネントが正常にインストールされ、すべてのポッドが実行されていることを確認します。

```
root@abhinav-ansible# oc get pods -n netapp-acc-operator
NAME                                               READY   STATUS
RESTARTS   AGE
acc-helm-repo-77745b49b5-7zg2v                     1/1     Running   0
10m
acc-operator-controller-manager-5c656c44c6-tqnmn   2/2     Running   0
13m
```

```
activity-589c6d59f4-x2sfs                          1/1     Running   0
6m4s
api-token-authentication-4q5lj                     1/1     Running   0
5m26s
api-token-authentication-pzptd                     1/1     Running   0
5m27s
api-token-authentication-tbtg6                     1/1     Running   0
5m27s
asup-669df8d49-qps54                               1/1     Running   0
5m26s
authentication-5867c5f56f-dnpp2                    1/1     Running   0
3m54s
bucketservice-85495bc475-5zcc5                     1/1     Running   0
5m55s
cert-manager-67f486bbc6-txhh6                      1/1     Running   0
9m5s
cert-manager-cainjector-75959db744-4l5p5           1/1     Running   0
9m6s
cert-manager-webhook-765556b869-g6wdf              1/1     Running   0
9m6s
cloud-extension-5d595f85f-txrfl                    1/1     Running   0
5m27s
cloud-insights-service-674649567b-5s4wd            1/1     Running   0
5m49s
composite-compute-6b58d48c69-46vhc                 1/1     Running   0
6m11s
composite-volume-6d447fd959-chnrt                  1/1     Running   0
5m27s
credentials-66668f8ddd-8qc5b                       1/1     Running   0
7m20s
entitlement-fd6fc5c58-wxnmh                        1/1     Running   0
6m20s
features-756bbb7c7c-rgcrm                          1/1     Running   0
5m26s
fluent-bit-ds-278pg                                1/1     Running   0
3m35s
fluent-bit-ds-5pqc6                                1/1     Running   0
3m35s
fluent-bit-ds-8l7cq                                1/1     Running   0
3m35s
fluent-bit-ds-9qbft                                1/1     Running   0
3m35s
fluent-bit-ds-nj475                                1/1     Running   0
3m35s
fluent-bit-ds-x9pd8                                1/1     Running   0
3m35s
```

```
graphql-server-698d6f4bf-kftwc                    1/1     Running   0
3m20s
identity-5d4f4c87c9-wjz6c                         1/1     Running   0
6m27s
influxdb2-0                                       1/1     Running   0
9m33s
krakend-657d44bf54-8cb56                          1/1     Running   0
3m21s
license-594bbdc-rghdg                             1/1     Running   0
6m28s
login-ui-6c65fbbbd4-jg8wz                         1/1     Running   0
3m17s
loki-0                                            1/1     Running   0
9m30s
metrics-facade-75575f69d7-hnlk6                   1/1     Running   0
6m10s
monitoring-operator-65dff79cfb-z78vk              2/2     Running   0
3m47s
nats-0                                            1/1     Running   0
10m
nats-1                                            1/1     Running   0
9m43s
nats-2                                            1/1     Running   0
9m23s
nautilus-7bb469f857-4hlc6                         1/1     Running   0
6m3s
nautilus-7bb469f857-vz94m                         1/1     Running   0
4m42s
openapi-8586db4bcd-gwwvf                          1/1     Running   0
5m41s
packages-6bdb949cfb-nrq8l                         1/1     Running   0
6m35s
polaris-consul-consul-server-0                    1/1     Running   0
9m22s
polaris-consul-consul-server-1                    1/1     Running   0
9m22s
polaris-consul-consul-server-2                    1/1     Running   0
9m22s
polaris-mongodb-0                                 2/2     Running   0
9m22s
polaris-mongodb-1                                 2/2     Running   0
8m58s
polaris-mongodb-2                                 2/2     Running   0
8m34s
polaris-ui-5df7687dbd-trcnf                       1/1     Running   0
3m18s
```

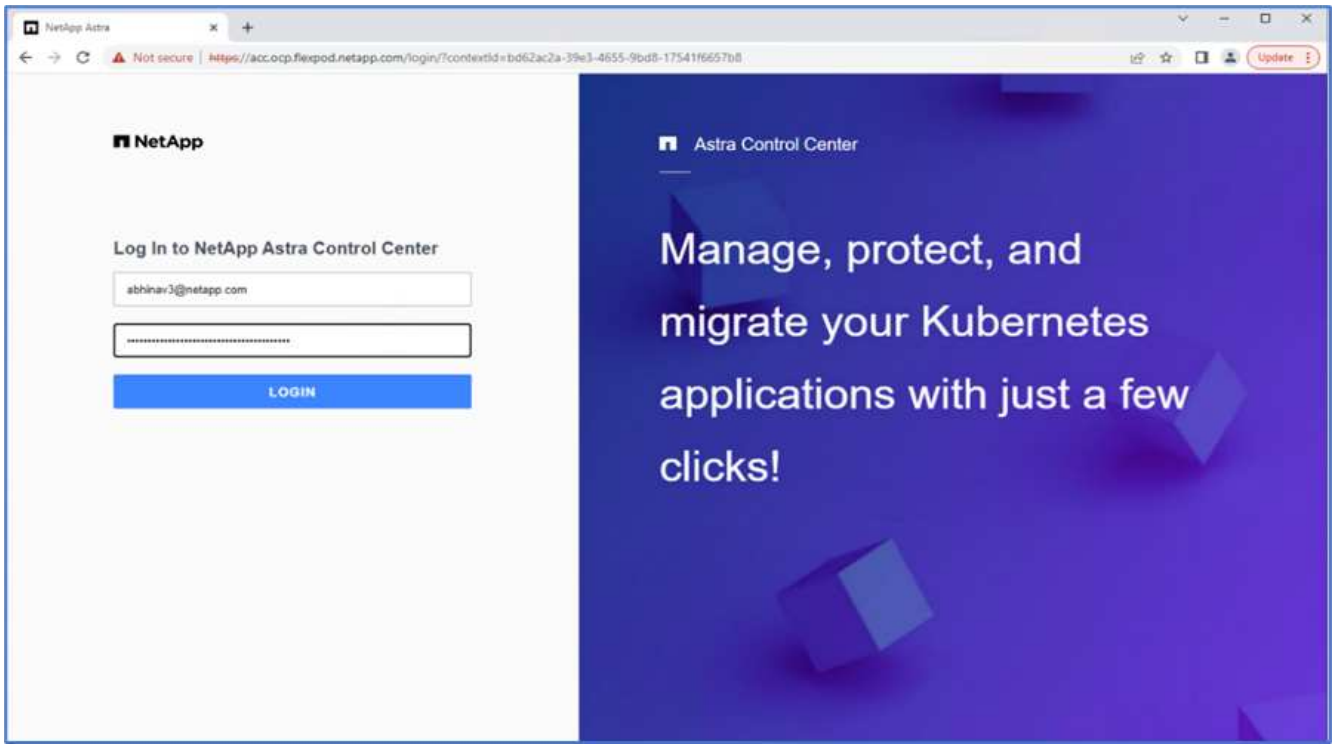
```
polaris-vault-0                                   1/1     Running   0
9m18s
polaris-vault-1                                   1/1     Running   0
9m18s
polaris-vault-2                                   1/1     Running   0
9m18s
public-metrics-7b96476f64-j88bw                   1/1     Running   0
5m48s
storage-backend-metrics-5fd6d7cd9c-vcb4j          1/1     Running   0
5m59s
storage-provider-bb85ff965-m7qrq                  1/1     Running   0
5m25s
telegraf-ds-4zqgz                                 1/1     Running   0
3m36s
telegraf-ds-cp9x4                                 1/1     Running   0
3m36s
telegraf-ds-h4n59                                 1/1     Running   0
3m36s
telegraf-ds-jnp2q                                 1/1     Running   0
3m36s
telegraf-ds-pdz5j                                 1/1     Running   0
3m36s
telegraf-ds-znqtp                                 1/1     Running   0
3m36s
telegraf-rs-rt64j                                 1/1     Running   0
3m36s
telemetry-service-7dd9c74bfc-sfkzt                1/1     Running   0
6m19s
tenancy-d878b7fb6-wf8x9                           1/1     Running   0
6m37s
traefik-6548496576-5v2g6                          1/1     Running   0
98s
traefik-6548496576-g82pq                          1/1     Running   0
3m8s
traefik-6548496576-psn49                          1/1     Running   0
38s
traefik-6548496576-qrkfd                          1/1     Running   0
2m53s
traefik-6548496576-srs6r                          1/1     Running   0
98s
trident-svc-679856c67-78kbt                       1/1     Running   0
5m27s
vault-controller-747d664964-xmn6c                 1/1     Running   0
7m37s
```

各ポッドのステータスが「Running」である必要があります。システムのポッドが導入されるまでに数分かかることがあります。

20. すべてのポッドが実行中の場合は、次のコマンドを実行して1回限りのパスワードを取得します。出力のYAMLバージョンで、「status.deploymentState`」フィールドで展開された値を確認し、「status.uuid」値をコピーします。パスワードは「ACC-」で、その後にUUID値が続きます。（ACC -[UUID]）。

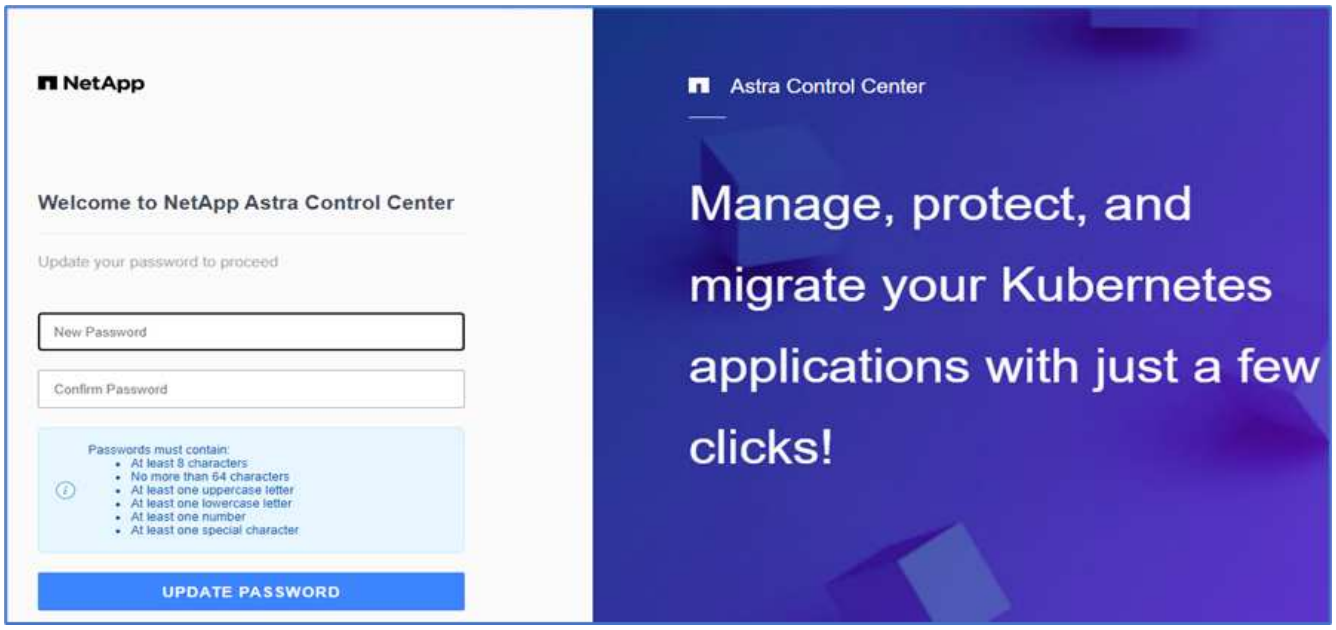
```
root@abhinav-ansible# oc get acc -o yaml -n netapp-acc-operator
```

21. ブラウザで、指定したFQDNを使用してURLに移動します。
22. デフォルトのユーザ名（インストール時に指定したEメールアドレス）とワンタイムパスワードACC-[UUID]を使用してログインします。



誤ったパスワードを3回入力すると、管理者アカウントは15分間ロックされます。

23. パスワードを変更して次に進みます。

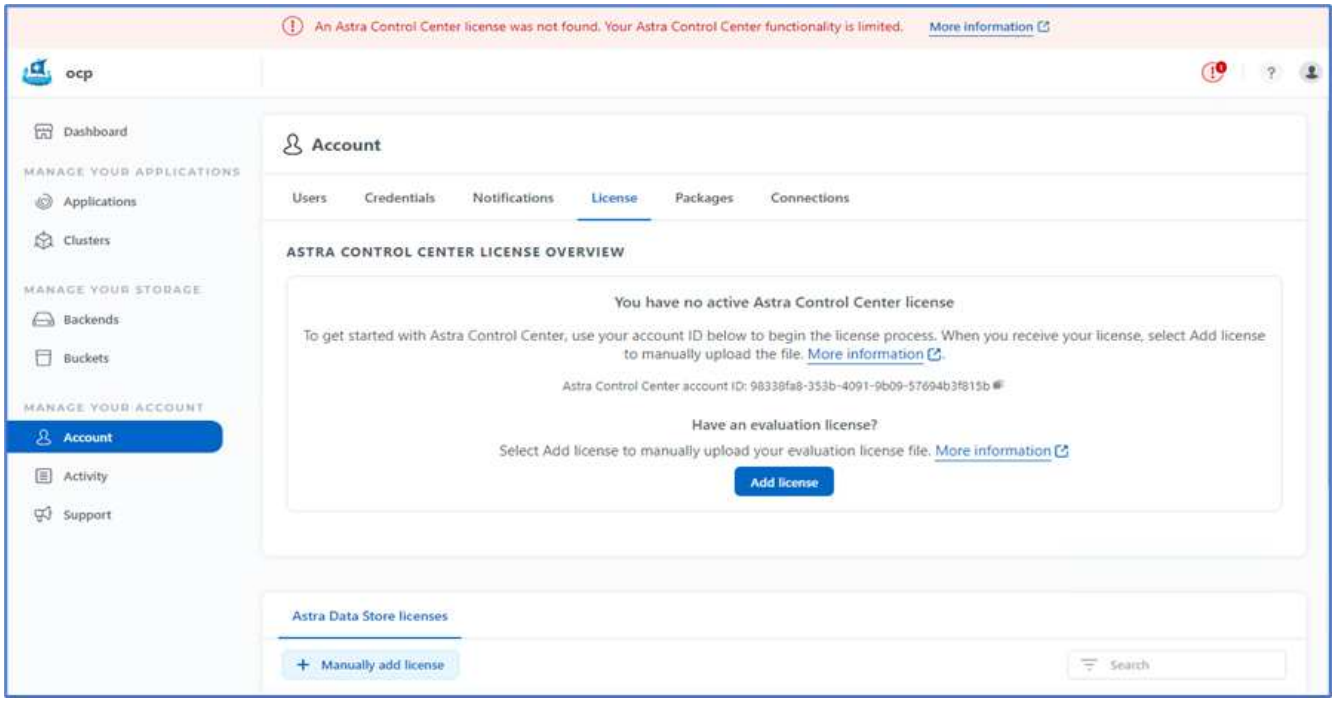


Astra Control Centerのインストールの詳細については、を参照してください "Astra Control Centerのインストールの概要" ページ

Astra Control Center をセットアップします

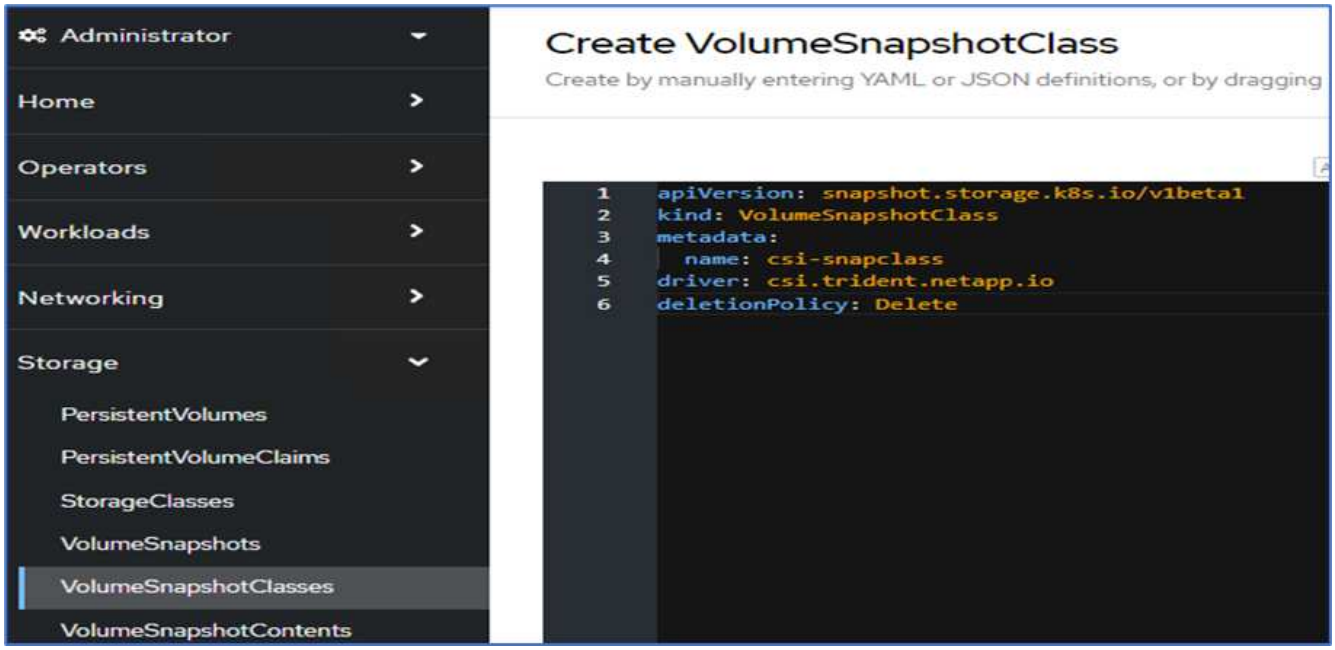
Astra Control Centerをインストールしたら、UIにログインし、ライセンスのアップロード、クラスタの追加、ストレージの管理、バケットの追加を行います。

1. [アカウント]の下のホームページで、[ライセンス]タブに移動し、[ライセンスの追加]を選択してAstraライセンスをアップロードします。

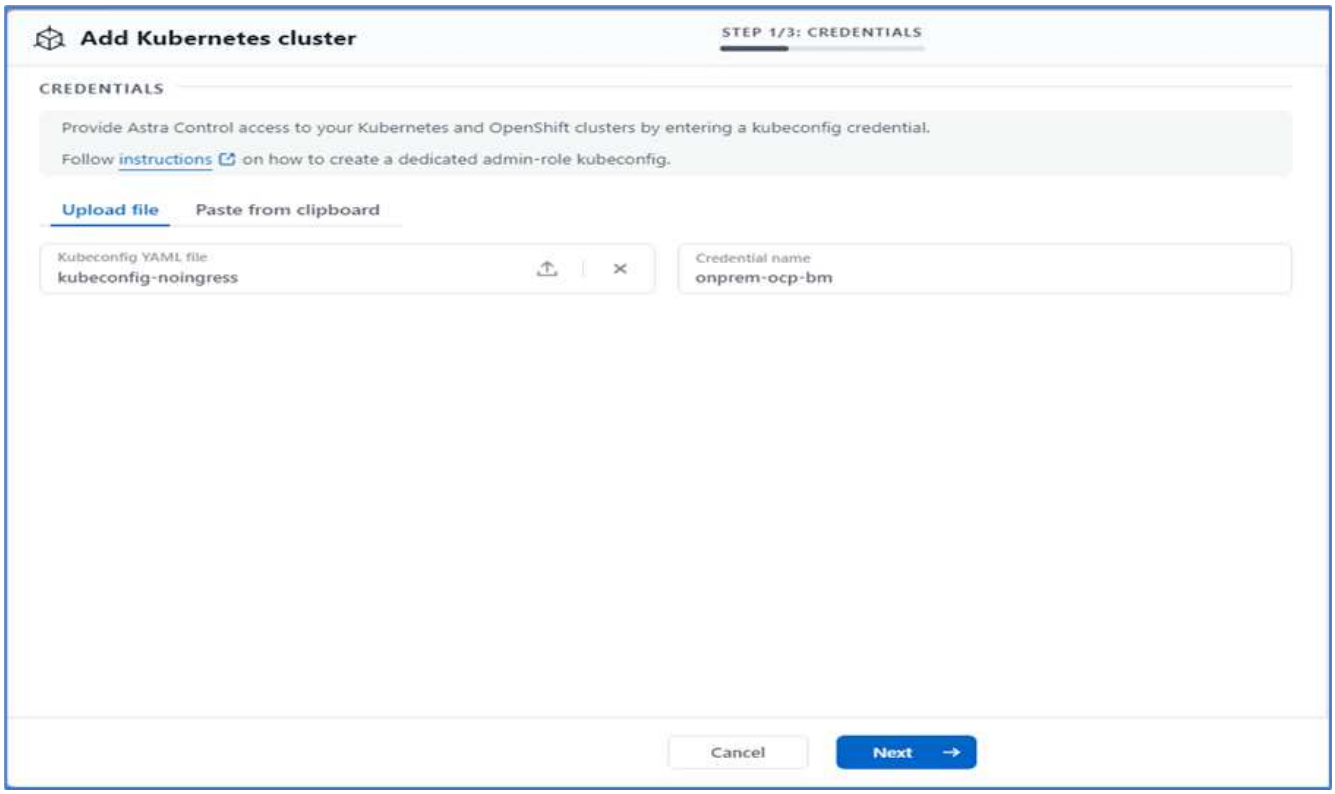


2. OpenShiftクラスタを追加する前に、OpenShift WebコンソールからAstra Tridentボリュームスナップショットクラスを作成します。Volumeスナップショット・クラスには'csi.trident.netapp.io`ドライバが設定さ

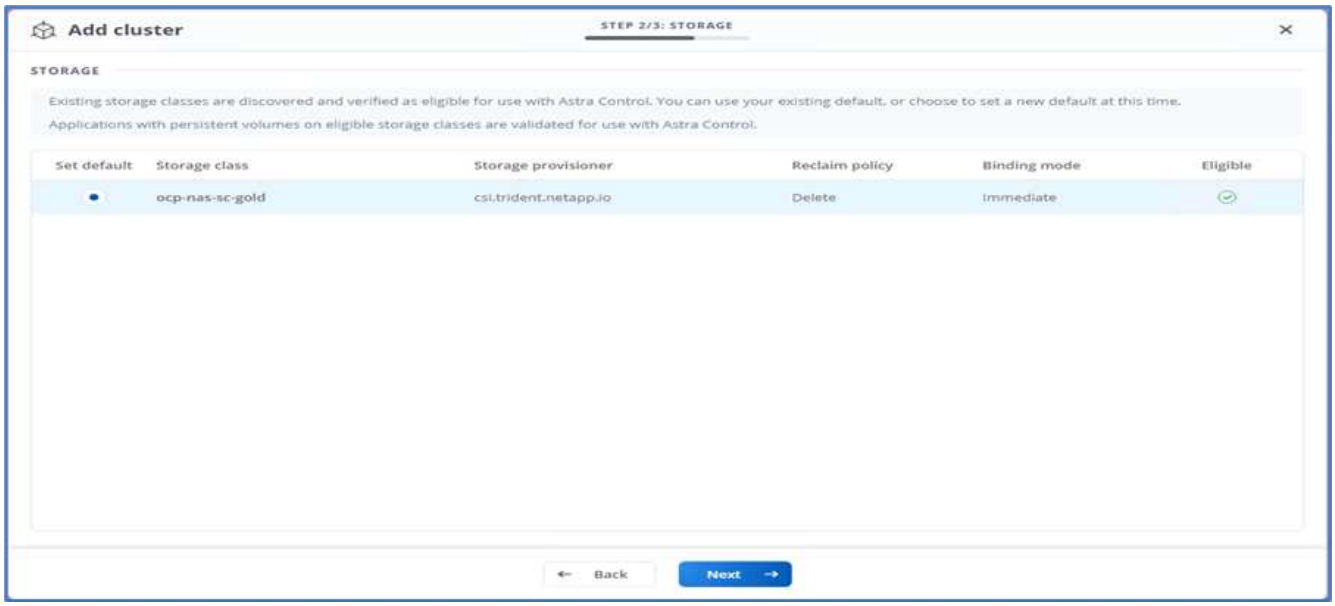
れています



3. Kubernetesクラスタを追加するには、ホームページでクラスタに移動し、Kubernetesクラスタを追加をクリックします。次に、クラスタの「kubeconfig」ファイルをアップロードし、クレデンシャル名を指定します。次へをクリックします。



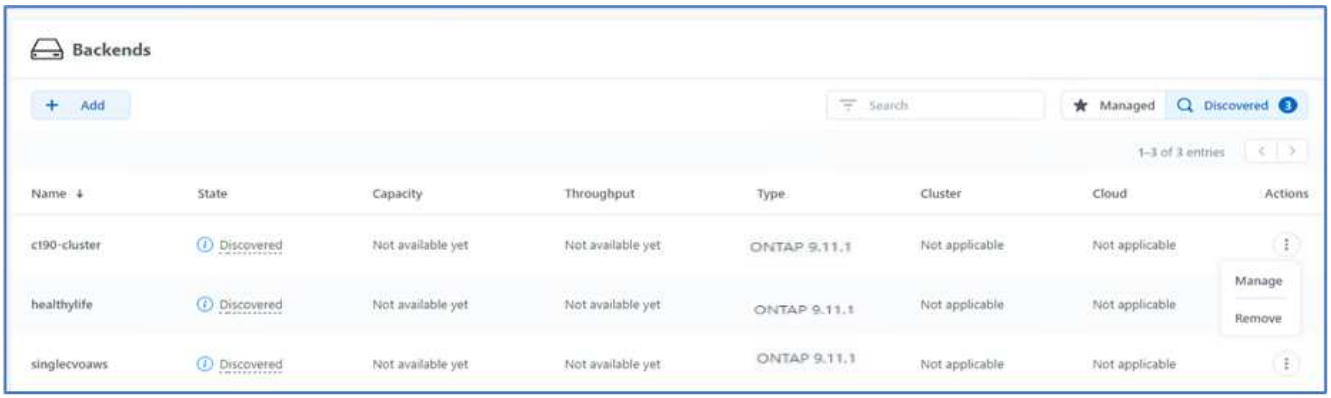
4. 既存のストレージクラスは自動的に検出されます。デフォルトのストレージクラスを選択し、Next（次へ）をクリックし、Add cluster（クラスタの追加）をクリックします。



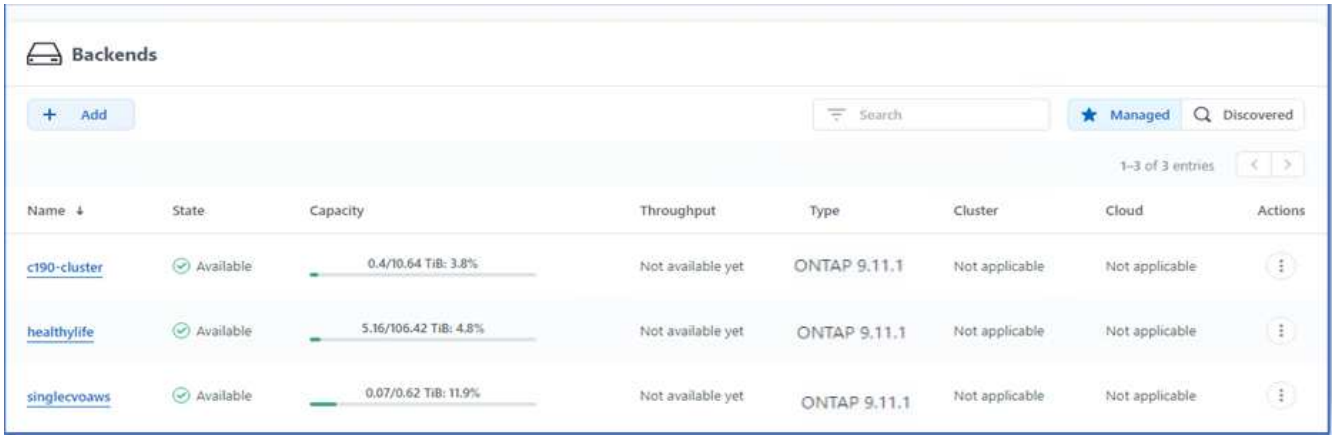
5. クラスタは数分で追加されます。OpenShift Container Platformクラスタを追加するには、手順1~4を繰り返します。

> 管理対象のコンピューティングリソースとしてOpenShift運用環境を追加するには、Astra Tridentを実行してください "VolumeSnapshotClassオブジェクト" が定義されている。

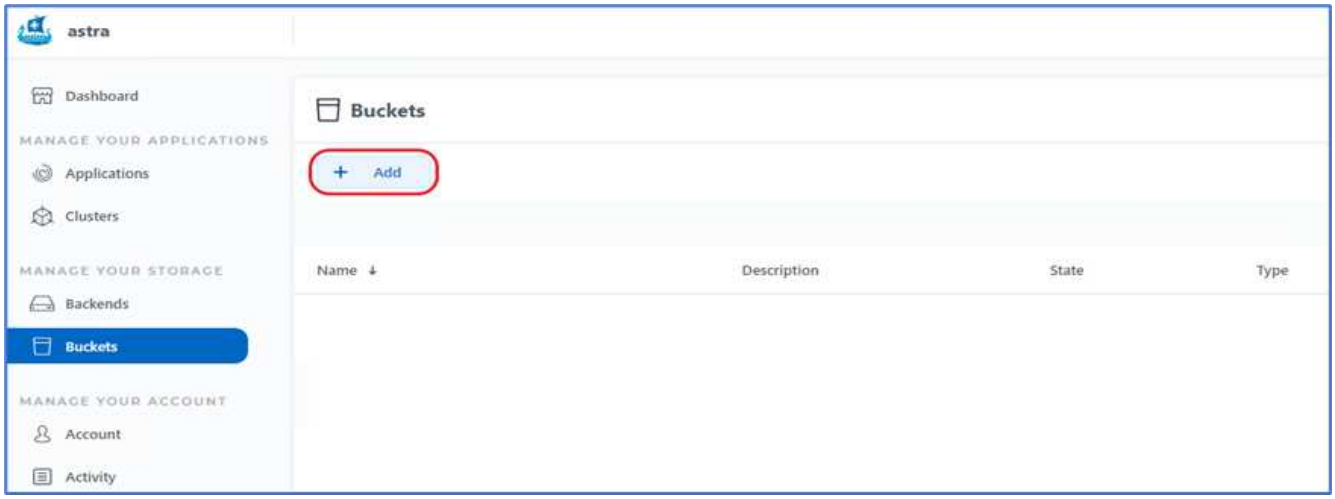
6. ストレージを管理するには、バックエンドに移動し、管理するバックエンドに対する処理の下にある3つのドットをクリックします。[管理]をクリックします



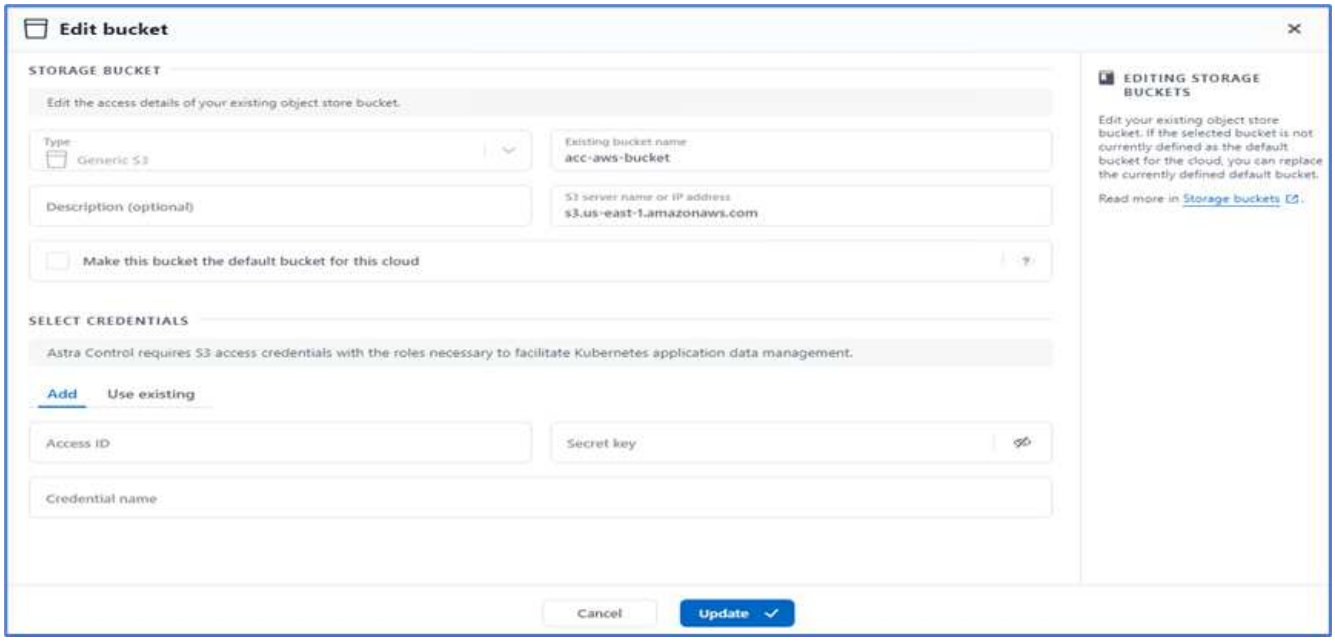
7. ONTAP の資格情報を入力し、[次へ]をクリックします。情報を確認し、[管理]をクリックします。バックエンドは次の例のようになります。



8. Astra Controlにバケットを追加するには、バケットを選択して追加をクリックします。

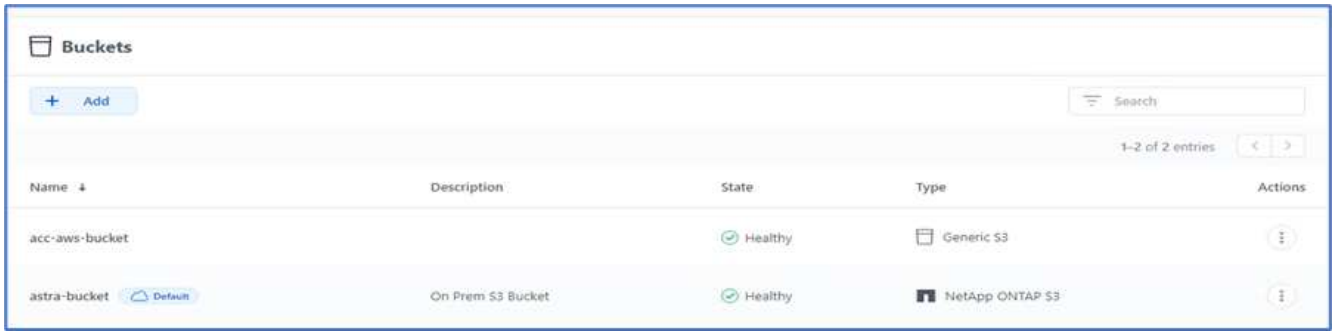


9. バケットタイプを選択し、バケット名、S3サーバ名、またはIPアドレスとS3クレデンシャルを指定します。更新をクリックします。



この解決策 では、AWS S3バケットとONTAP S3バケットの両方が使用されます。StorageGRID を使用することもできます。

バケットは正常な状態である必要があります。



アプリケーション対応データ管理用のAstra Control CenterへのKubernetesクラスタ登録の一部として、Astra Controlは、ロールバインドとネットアップ監視ネームスペースを自動的に作成し、アプリケーションポッドとワーカーノードから指標とログを収集します。サポートされているONTAPベースのストレージクラスのいずれかをデフォルトにします。

お先にどうぞ "Astra Control 管理にクラスタを追加"では、クラスターにアプリケーションをインストールし（Astra Controlの外部）、Astra Controlの[アプリ]ページに移動して、アプリケーションとそのリソースを管理できます。Astraを使用したアプリケーションの管理の詳細については、を参照してください "アプリケーション管理の要件"。

"次：解決策 の検証の概要"

解決策の検証

概要

"前のレポート：OpenShift Container PlatformにAstra Control Centerをインストールしました。"

このセクションでは、いくつかのユースケースで解決策 を復習します。

- リモートバックアップから、クラウドで実行されている別のOpenShiftクラスタへのステートフルアプリケーションのリストア。
- OpenShiftクラスタ内の同じネームスペースへのステートフルアプリケーションのリストア。
- あるFlexPod システム（OpenShift Container Platformベアメタル）から別のFlexPod システム（VMware上のOpenShift Container Platform）にクローニングすることでアプリケーションを移動できます。

特に、この解決策 で検証されるのはユースケースが少ないことがわかります。この検証は、Astra Control Centerの全機能を表しているわけではありません。

"Next：リモートバックアップを使用したアプリケーションのリカバリ。"

リモートバックアップによるアプリケーションのリカバリ

"Previous：解決策 の検証の概要を示します。"

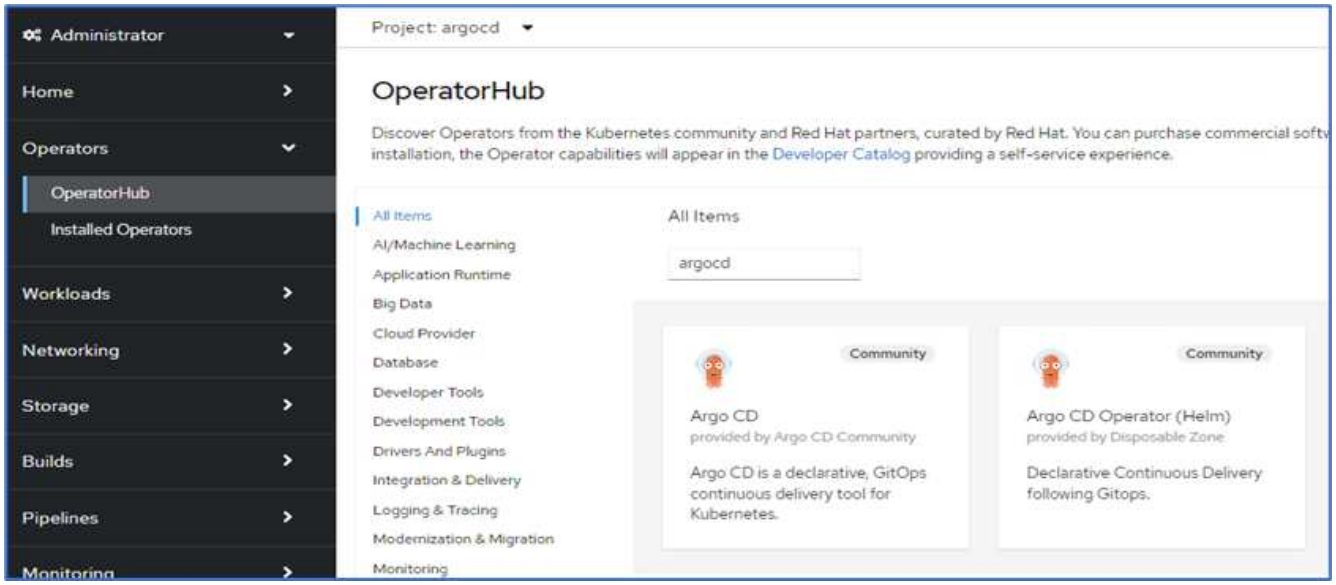
Astraでは、アプリケーションと整合性のあるフルバックアップを作成できます。このバックアップを使用すると、アプリケーションのデータを使用して、オンプレミスのデータセンターやパブリッククラウドで実行されている別のKubernetesクラスタにリストアできます。

アプリケーションのリカバリが正常に行われるかどうかを検証するには、FlexPod システムで実行されているアプリケーションのオンプレミス障害をシミュレートし、リモートバックアップを使用してクラウドで実行されているKubernetesクラスタにアプリケーションをリストアします。

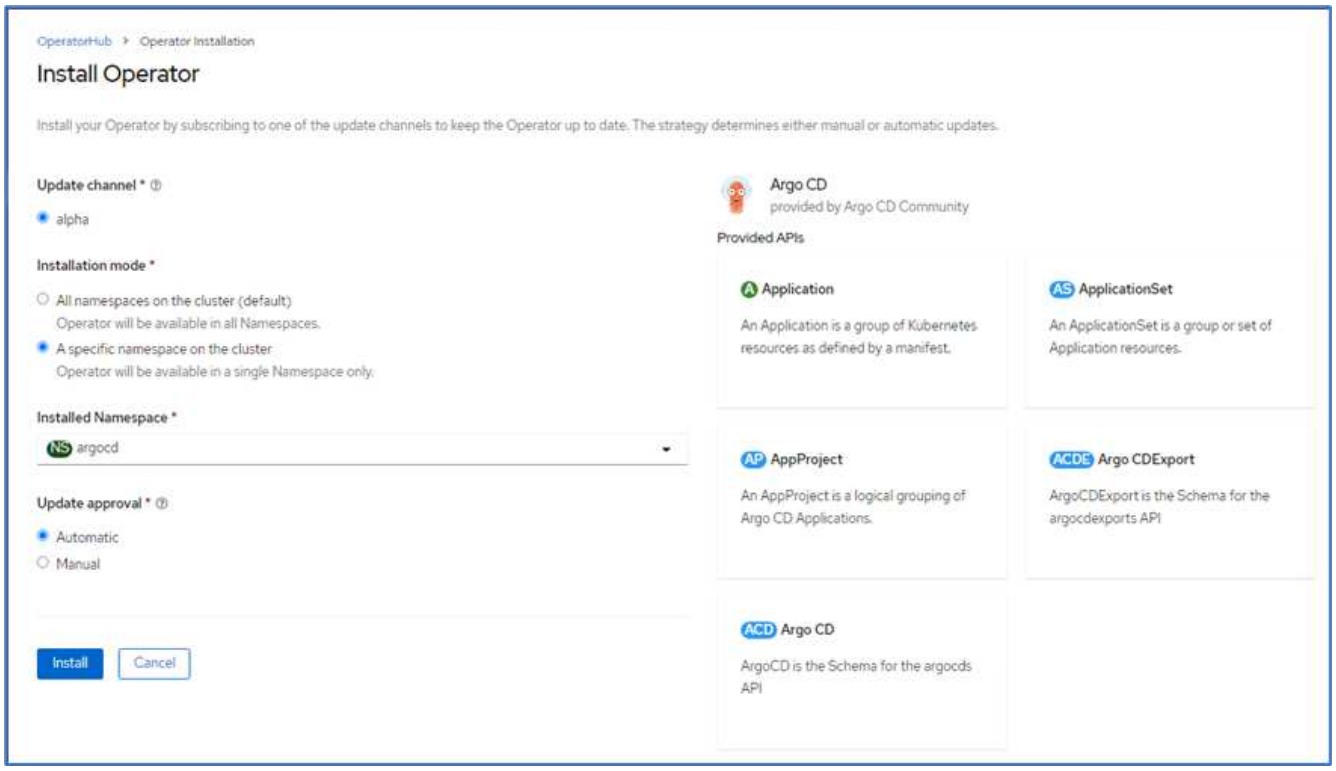
サンプルアプリケーションは、データベースにMySQLを使用する価格表アプリケーションです。導入を自動化するために、を使用しました "Argo CD" ツール。Argo CDは、Kubernetes向けの宣言型、GitOps、継続的デリバリーツールです。

1. オンプレミスOpenShiftクラスタにログインし、「argocd」という名前の新しいプロジェクトを作成します。

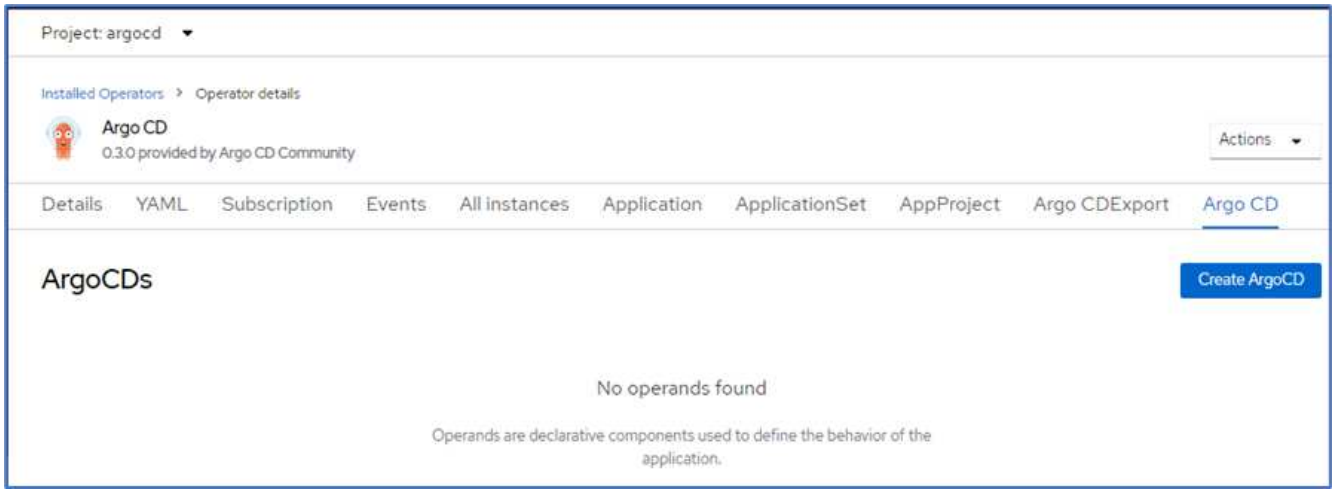
2. OperatorHubで'argocd'を検索し'Argo CD operatorを選択します



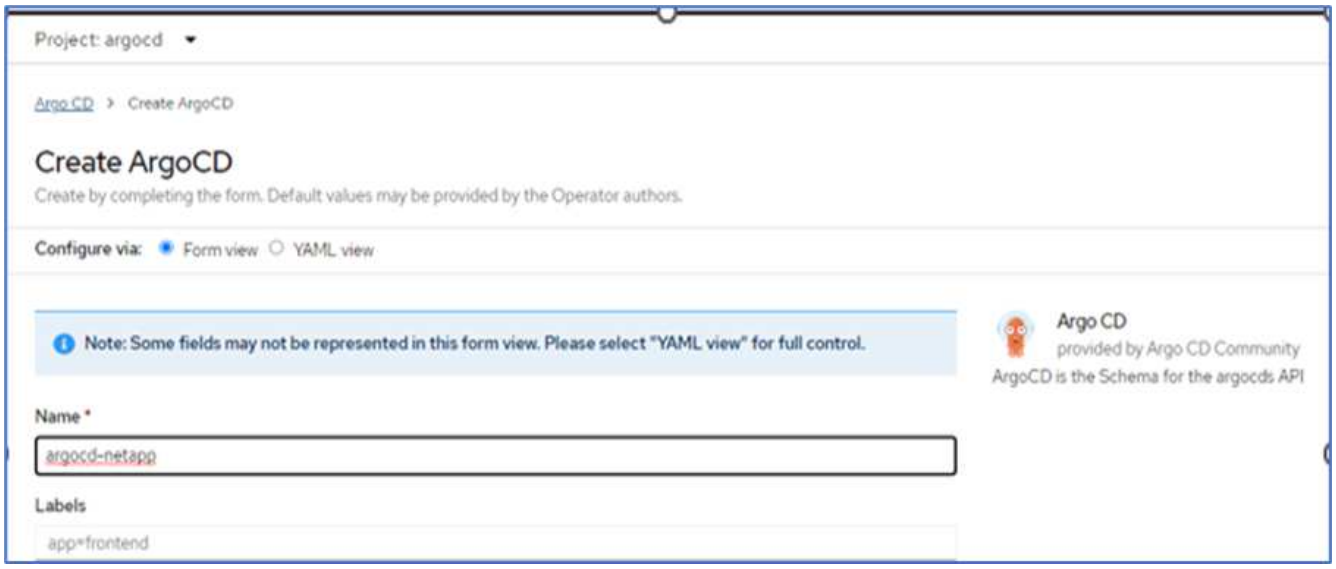
3. 「argocd」名前空間に演算子をインストールします。



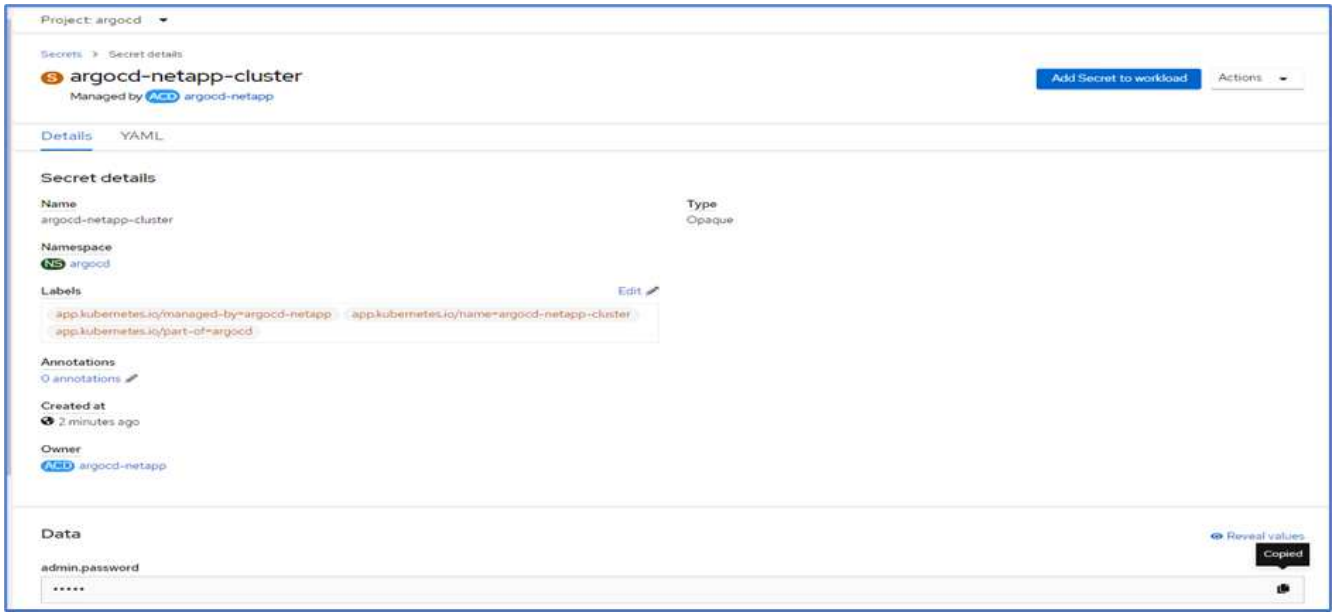
4. オペレータに移動し、Create ArgCDをクリックします。



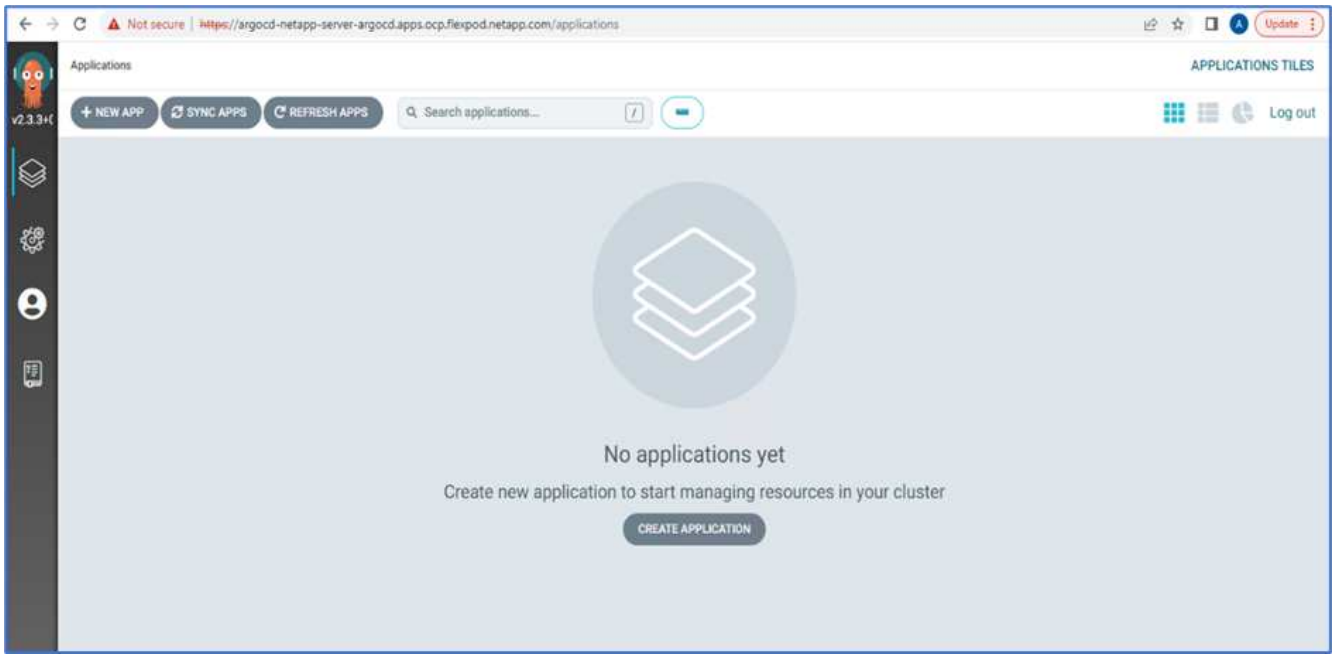
5. Argo CDインスタンスを'argocd'プロジェクトに配備するには'名前を指定してCreateをクリックします



6. Argo CDにログインするには、デフォルトのユーザはadminで、パスワードは「argocd -NetApp-cluster」という名前のシークレットファイルに含まれています。



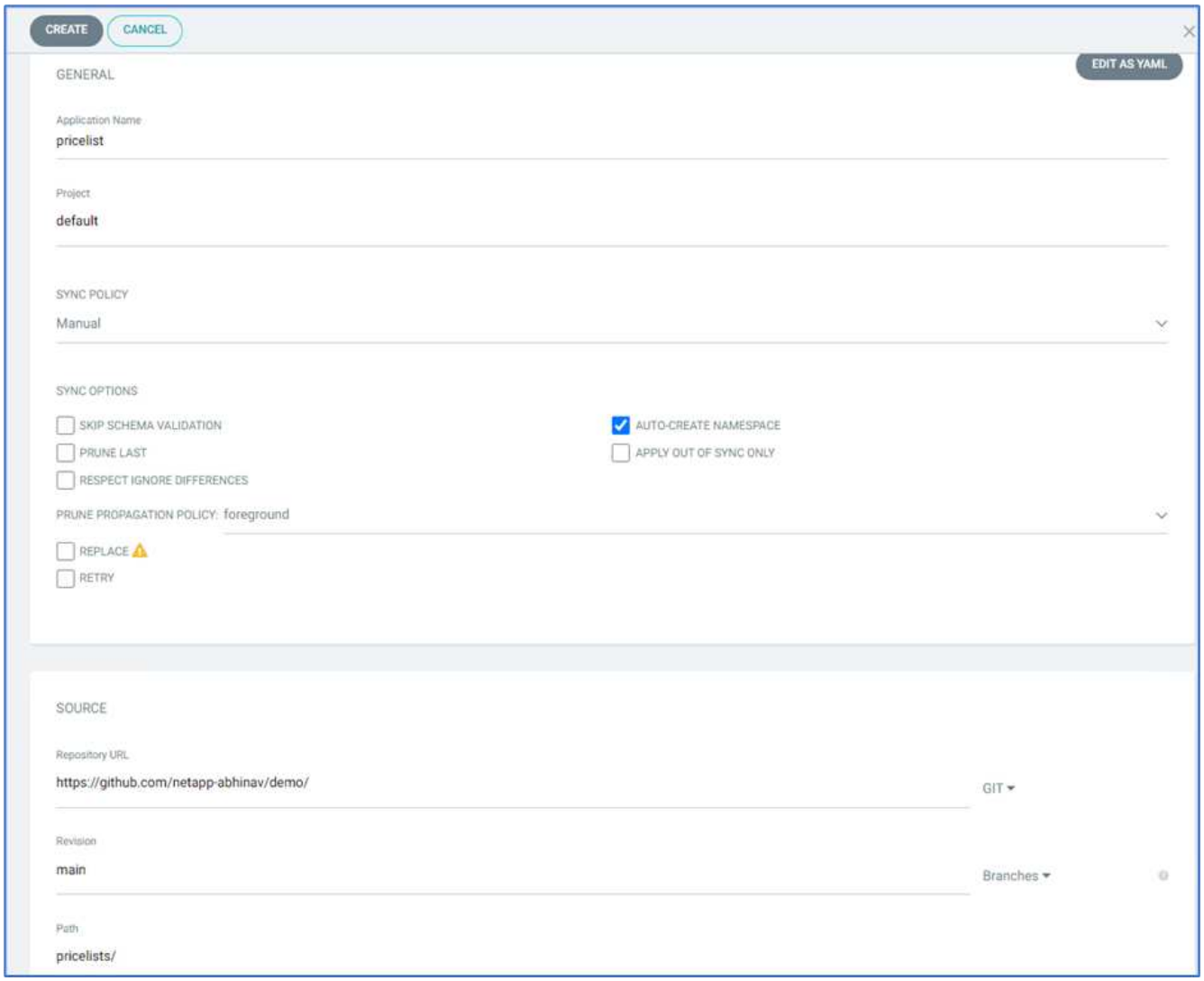
7. サイド・メニューから'ルート>ロケーションを選択し'argocd'ルートのURLをクリックしますユーザ名とパスワードを入力します。



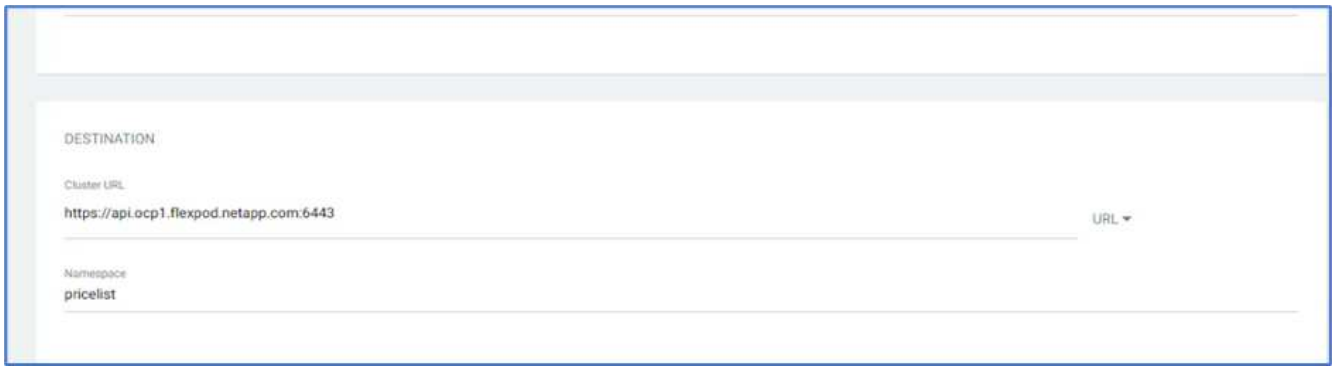
8. CLIを使用して、Argo CDにオンプレミスOpenShiftクラスタを追加します。

```
####Login to Argo CD####
abhinav3@abhinav-ansible$ argocd-linux-amd64 login argocd-netapp-server-
argocd.apps.ocp.flexpod.netapp.com --insecure
Username: admin
Password:
'admin:login' logged in successfully
Context'argocd-netapp-server-argocd.apps.ocp.flexpod.netapp.com' updated
####List the On-Premises OpenShift cluster####
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add
ERRO[0000] Choose a context name from:
CURRENT  NAME
CLUSTER              SERVER
*        default/api-ocp-flexpod-netapp-com:6443/abhinav3
api-ocp-flexpod-netapp-com:6443
https://api.ocp.flexpod.netapp.com:6443
         default/api-ocp1-flexpod-netapp-com:6443/abhinav3
api-ocp1-flexpod-netapp-com:6443
https://api.ocp1.flexpod.netapp.com:6443
####Add On-Premises OpenShift cluster###
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add default/api-
ocp1-flexpod-netapp-com:6443/abhinav3
WARNING: This will create a service account `argocd-manager` on the
cluster referenced by context `default/api-ocp1-flexpod-netapp-
com:6443/abhinav3` with full cluster level admin privileges. Do you want
to continue [y/N]? y
INFO[0002] ServiceAccount "argocd-manager" already exists in namespace
"kube-system"
INFO[0002] ClusterRole "argocd-manager-role" updated
INFO[0002] ClusterRoleBinding "argocd-manager-role-binding" updated
Cluster 'https://api.ocp1.flexpod.netapp.com:6443' added
```

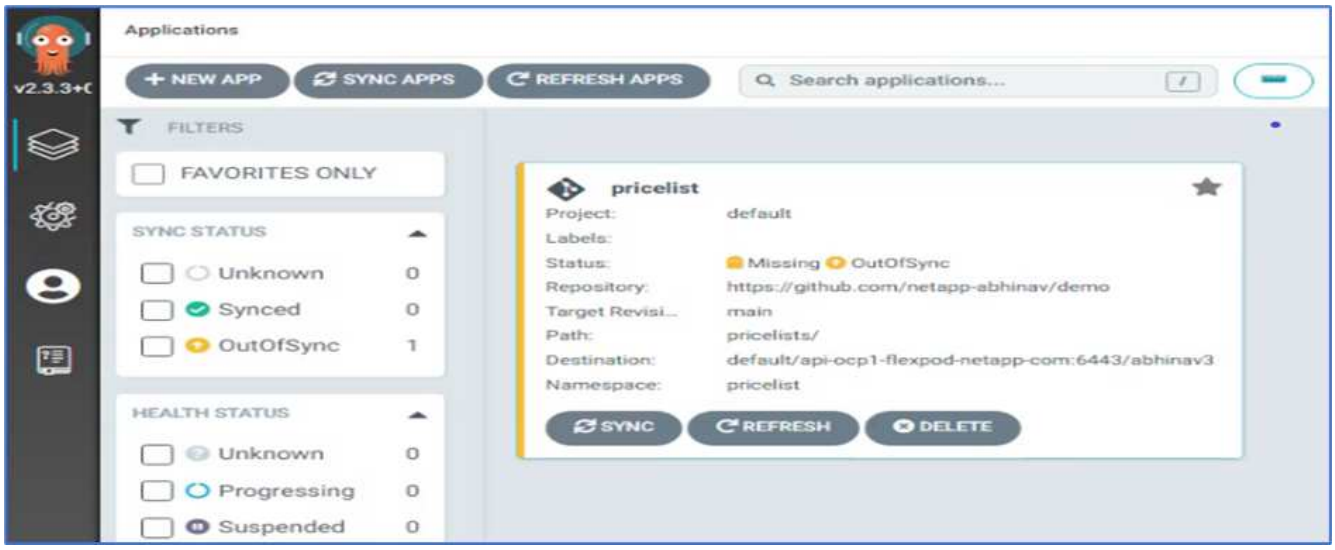
9. ArgodCD UIで、[新しいアプリ]をクリックし、アプリ名とコードリポジトリの詳細を入力します。



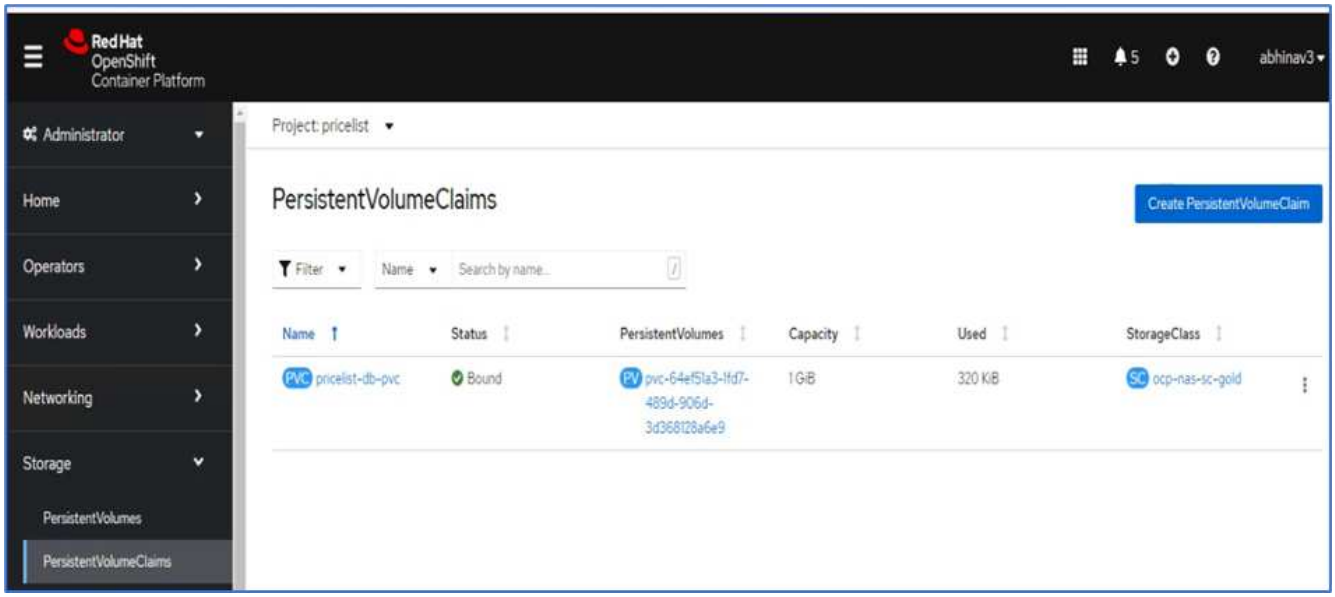
10. ネームスペースとともにアプリケーションを導入するOpenShiftクラスタを入力します。



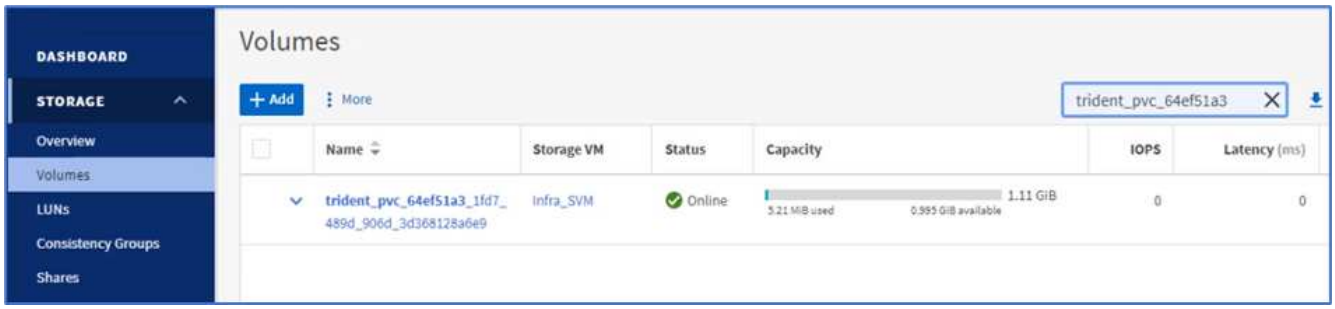
11. オンプレミスOpenShiftクラスタにアプリを導入するには、[同期]をクリックします。



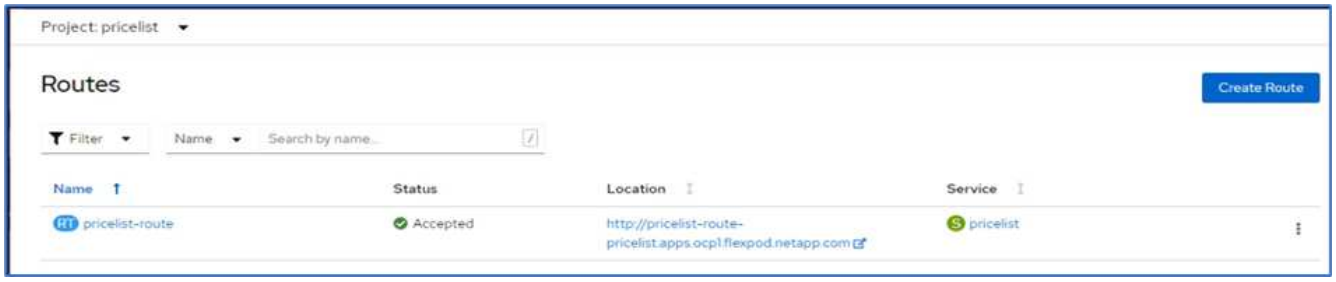
12. OpenShift Container Platformコンソールで、プロジェクト価格表に移動し、ストレージでPVCの名前とサイズを確認します。



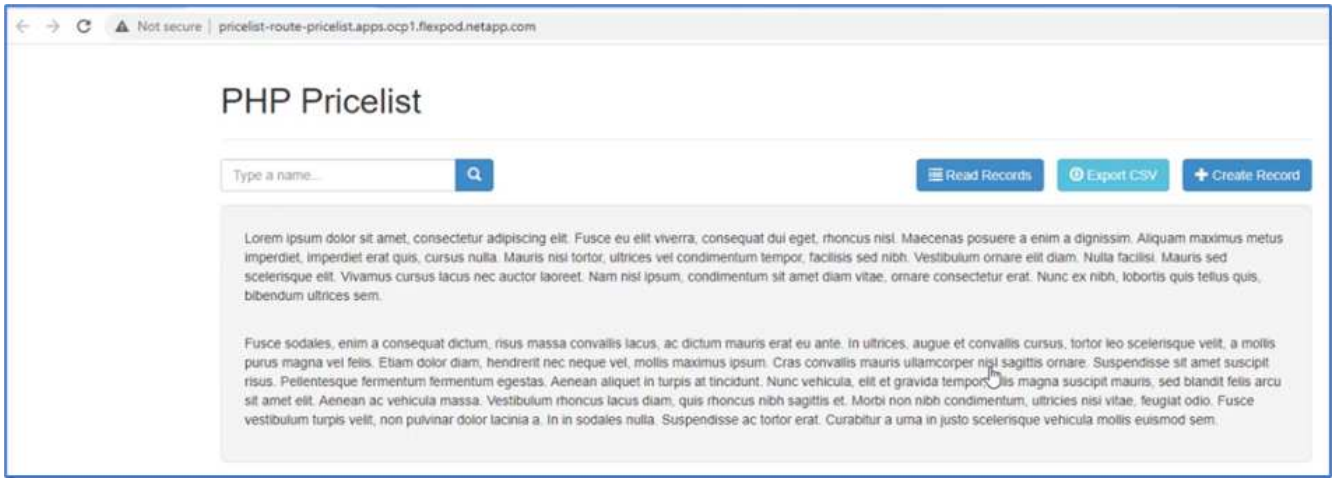
13. System Managerにログインし、PVCを確認します。



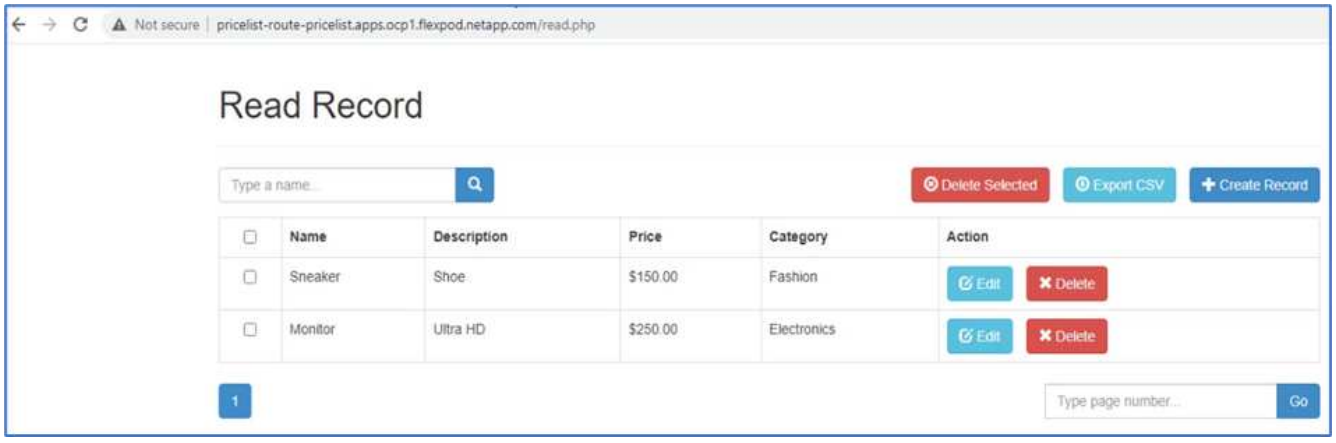
14. ポッドが実行されたら、サイドメニューからネットワーキング／ルートを選択し、「場所」の下のURLをクリックします。



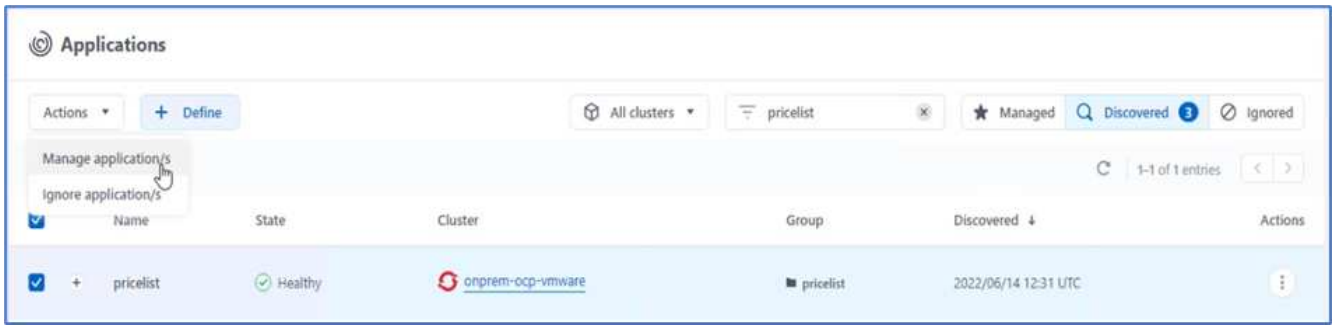
15. 価格表アプリのホームページが表示されます。



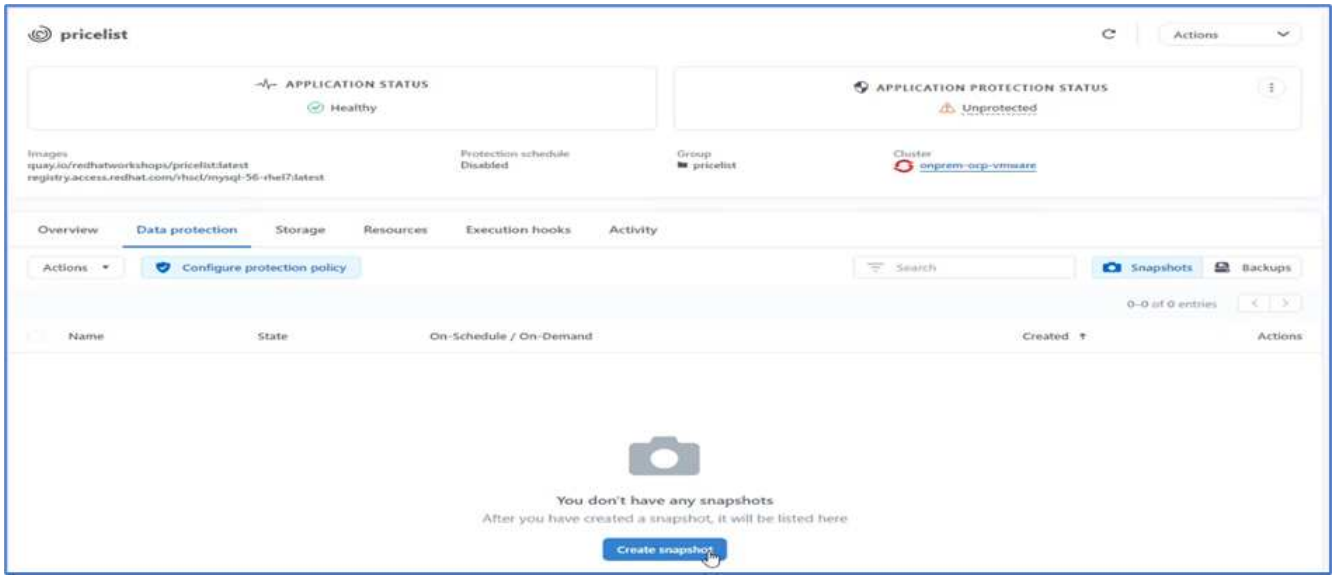
16. Webページにレコードをいくつか作成します。



17. アプリケーションはAstra Control Centerで検出されます。アプリを管理するには、[アプリケーション]>[検出済み]に移動し、価格表アプリを選択して、[アクション]の[アプリケーションの管理]をクリックします。

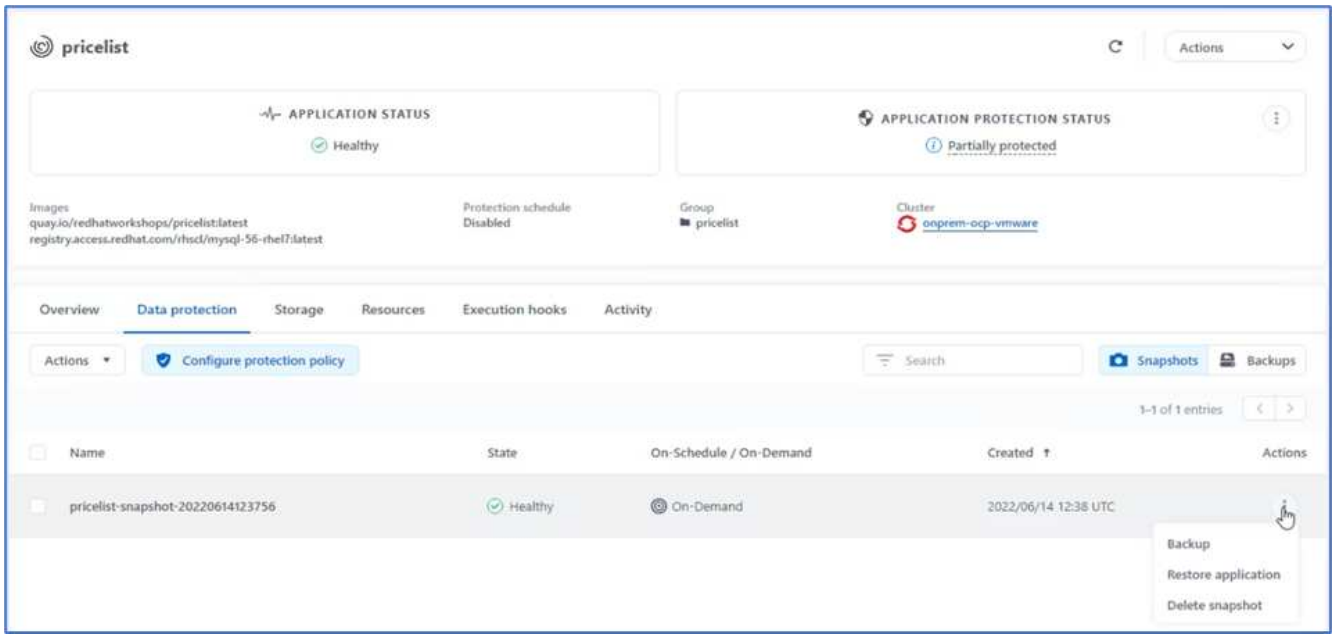


18. 価格表アプリをクリックし、[データ保護]を選択します。この時点では、Snapshotやバックアップは作成されていません。スナップショットの作成をクリックして、オンデマンドスナップショットを作成します。

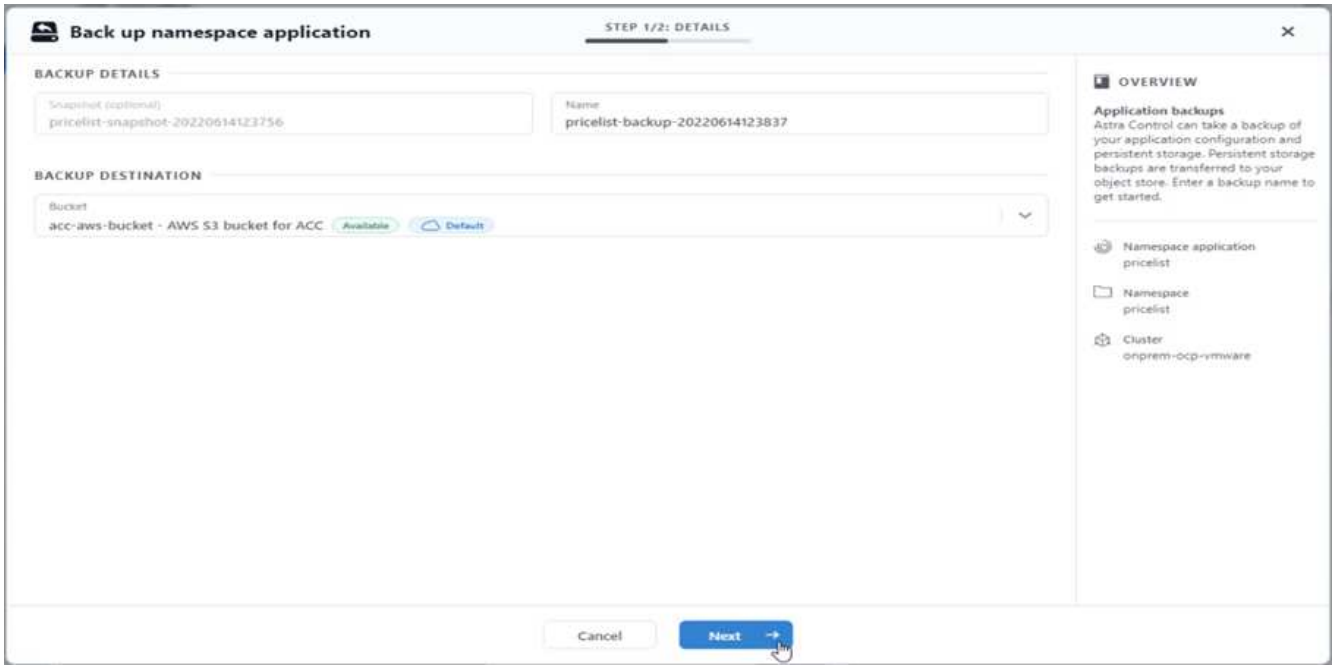


NetApp Astra Control Centerは、オンデマンドおよびスケジュールされたスナップショットとバックアップの両方をサポートします。

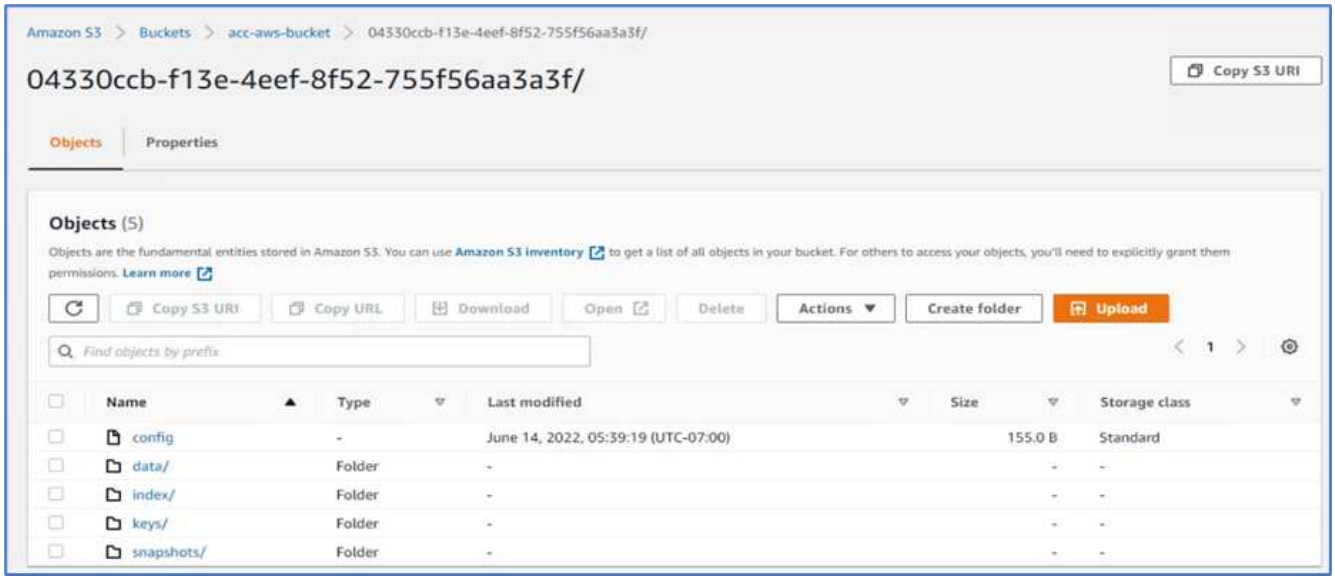
19. スナップショットが作成され、状態が正常になったら、そのスナップショットを使用してリモートバックアップを作成します。このバックアップはS3バケットに格納されます。



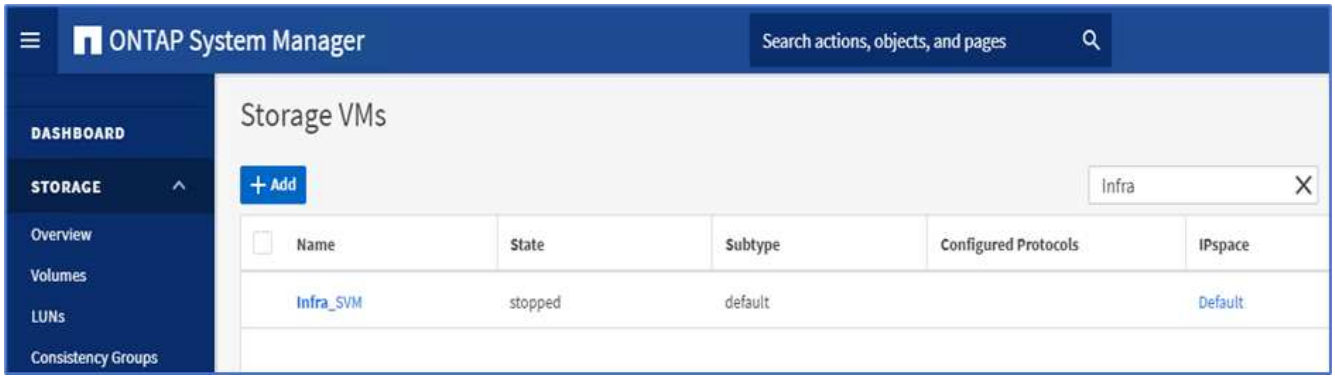
20. AWS S3バケットを選択してバックアップ処理を開始します。



21. バックアップ処理では、AWS S3バケットに複数のオブジェクトを含むフォルダを作成する必要があります。



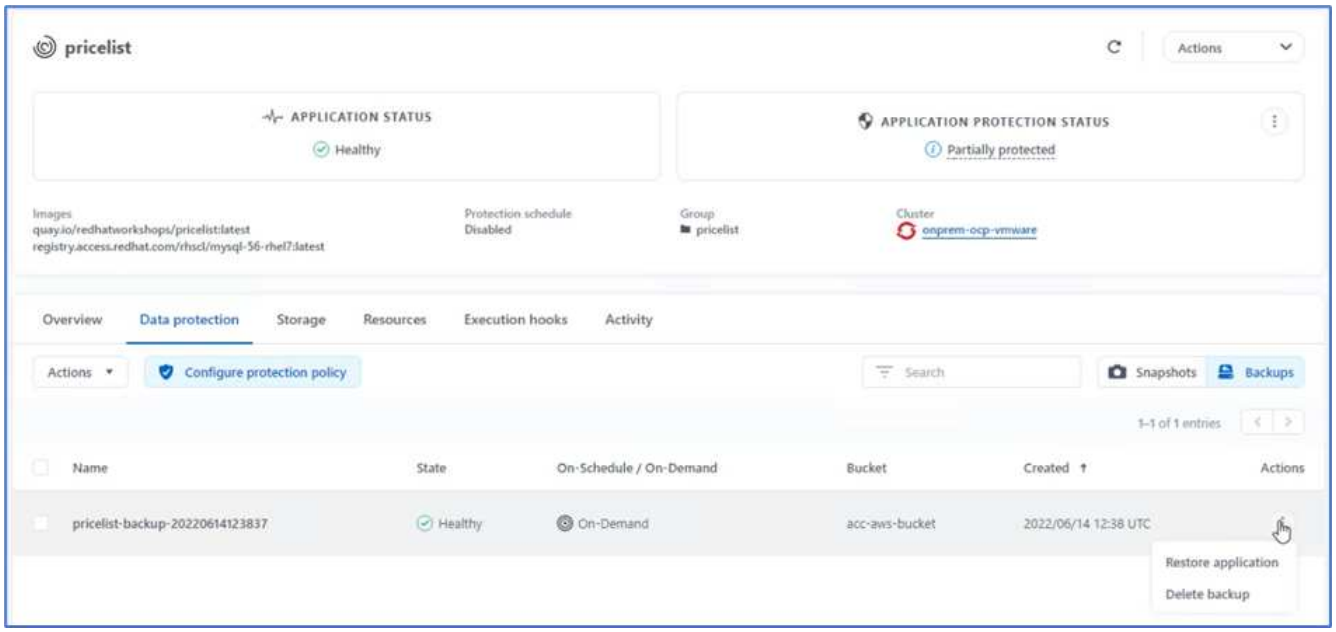
22. リモートバックアップが完了したら、PVの元のボリュームをホストするStorage Virtual Machine（SVM）を停止して、オンプレミスでの災害をシミュレートします。



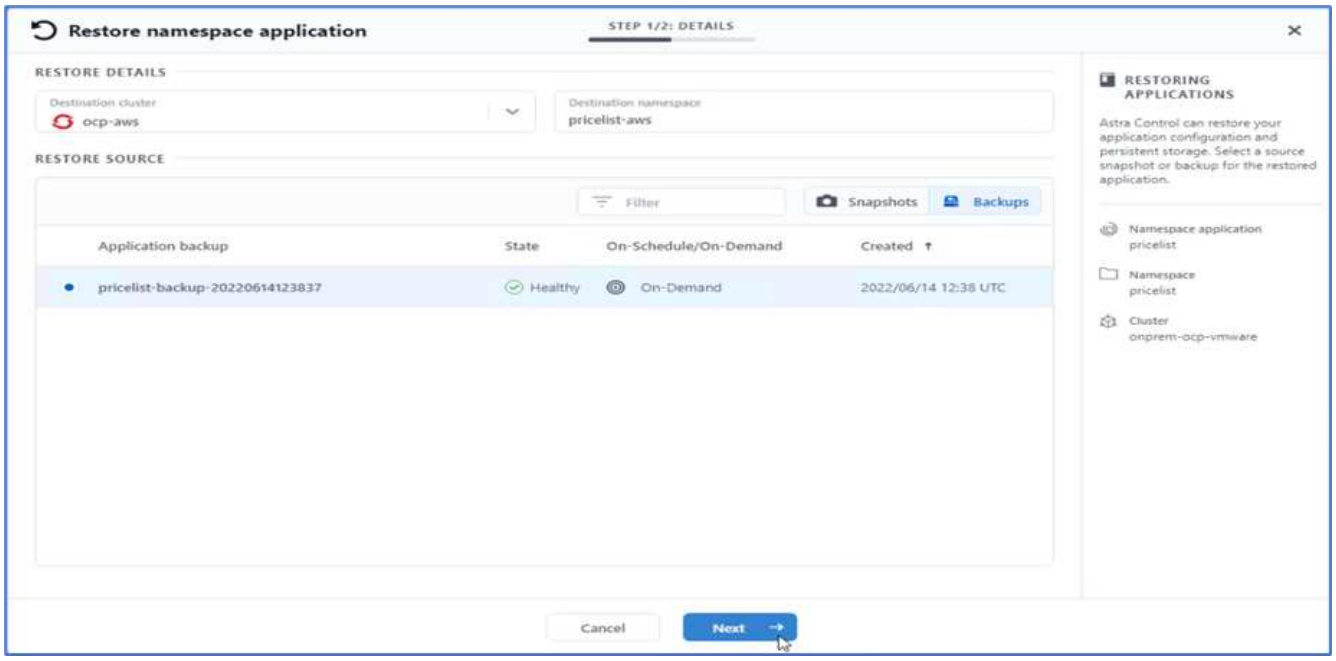
23. Webページを更新してシステム停止を確認します。Webページは使用できません。

ウェブサイトは予想どおりに停止しているので、AWSで実行されているOpenShiftクラスタにAstraを使用して、リモートバックアップからアプリケーションを迅速にリカバリしてみましょう。

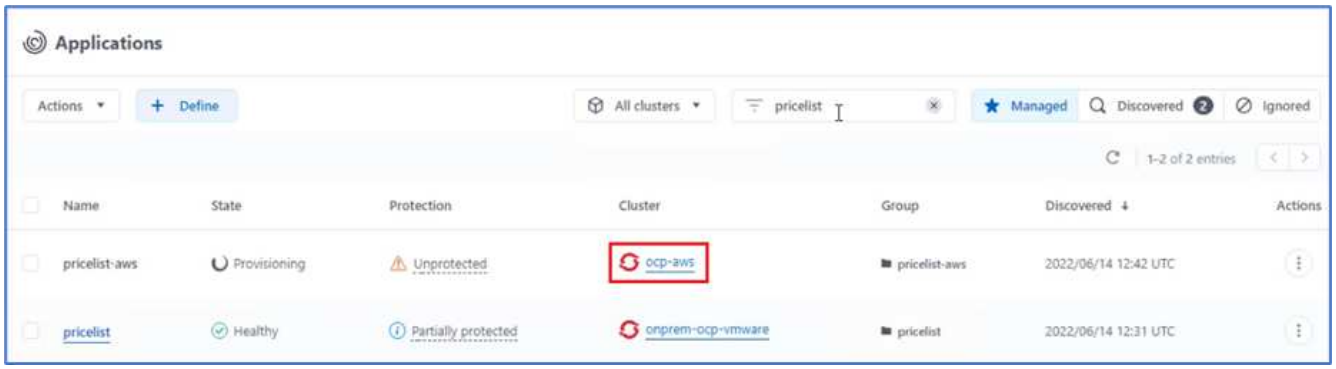
24. Astra Control Centerで、価格表アプリをクリックし、[データ保護]>[バックアップ]を選択します。バックアップを選択し、[操作]の下の[アプリケーションの復元]をクリックします。



25. デスティネーションクラスタとして「OCP-AWS」を選択し、ネームスペースに名前を付けます。[オンデマンドバックアップ]、[次へ]、[復元]の順にクリックします。

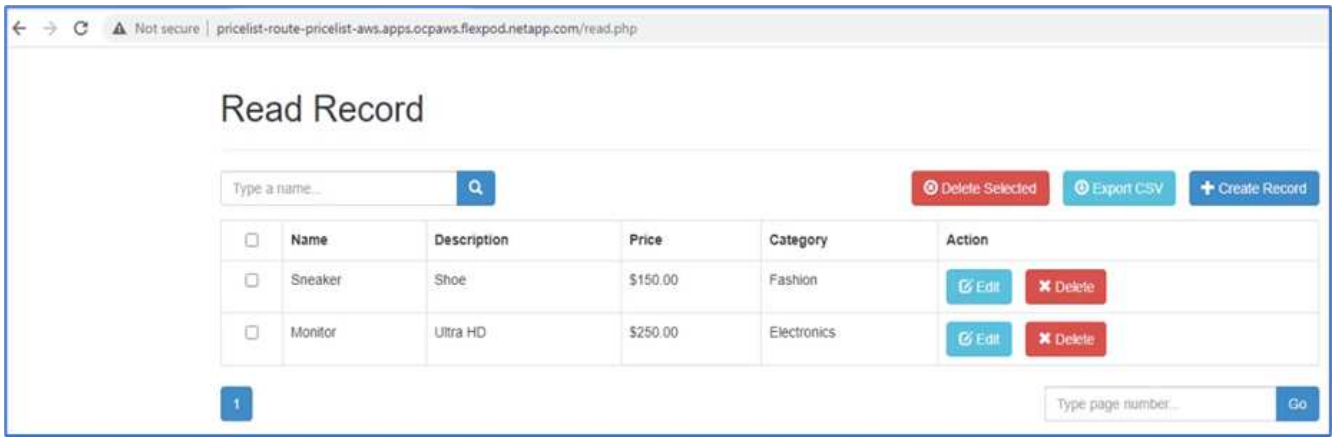


26. 「pricelist-app」という名前の新しいアプリケーションは、AWSで実行されるOpenShiftクラスタでプロビジョニングされます。



27. OpenShift Webコンソールで同じことを確認します。

28. 「pricelist -aws」プロジェクトの下のポッドがすべて実行されたら、「Routes」に移動し、URLをクリックしてWebページを起動します。



このプロセスでは、貴重なアプリケーションが正常に復元され、Astra Control Centerを利用してAWS上でシームレスに実行されるOpenShiftクラスタでデータの整合性が維持されていることを検証します。

Snapshotコピーと**DevTest**のアプリケーション移動によるデータ保護

この使用事例は、次のセクションで説明する2つの部分で構成されています。

パート**1**

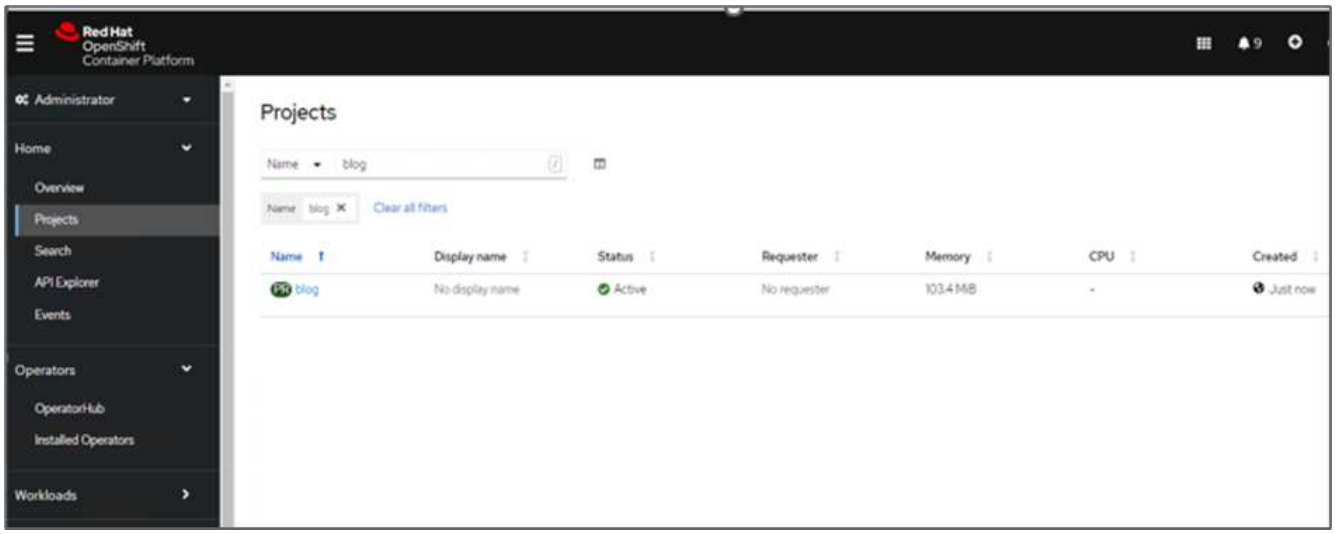
Astra Control Centerを使用すると、アプリケーション対応のスナップショットを作成してローカルデータを

保護できます。データを誤って削除したり破損したりした場合は、以前に記録したスナップショットを使用して、アプリケーションおよび関連データを既知の正常な状態に戻すことができます。

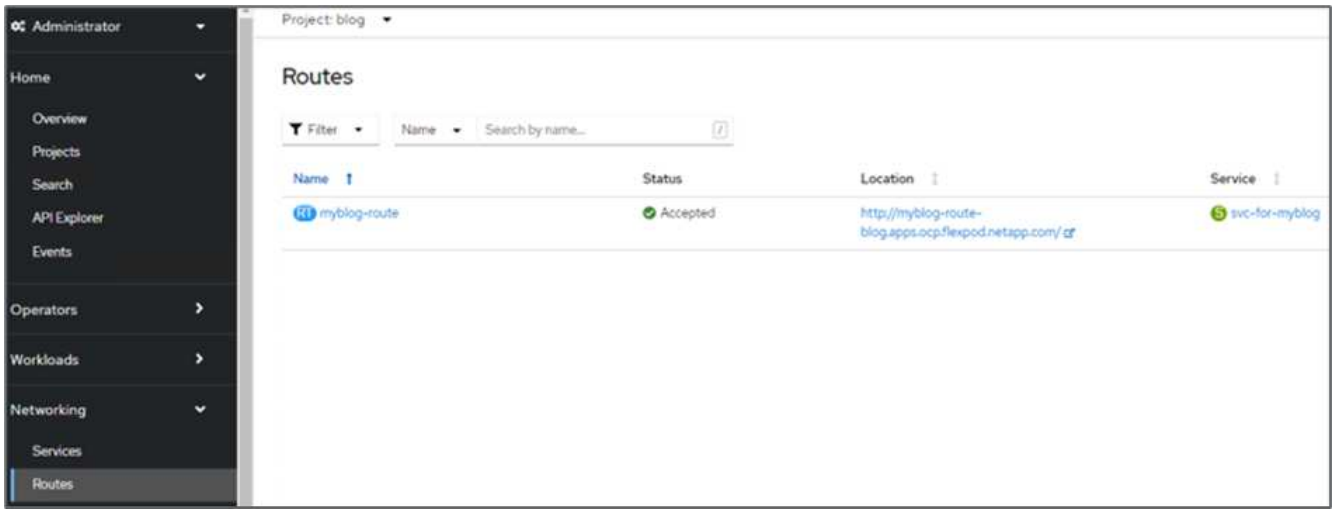
このシナリオでは、開発とテスト（DevTest）チームが、Ghostブログアプリケーションであるサンプルのステートフルアプリケーション（ブログサイト）を導入し、コンテンツを追加し、アプリケーションを最新バージョンにアップグレードします。Ghostアプリケーションでは、データベースにSQLiteを使用します。アプリケーションをアップグレードする前に、Astra Control Centerを使用してスナップショット（オンデマンド）を作成し、データを保護します。詳細な手順は次のとおりです。

1. サンプルブログアプリをデプロイし、ArgoCDから同期します。

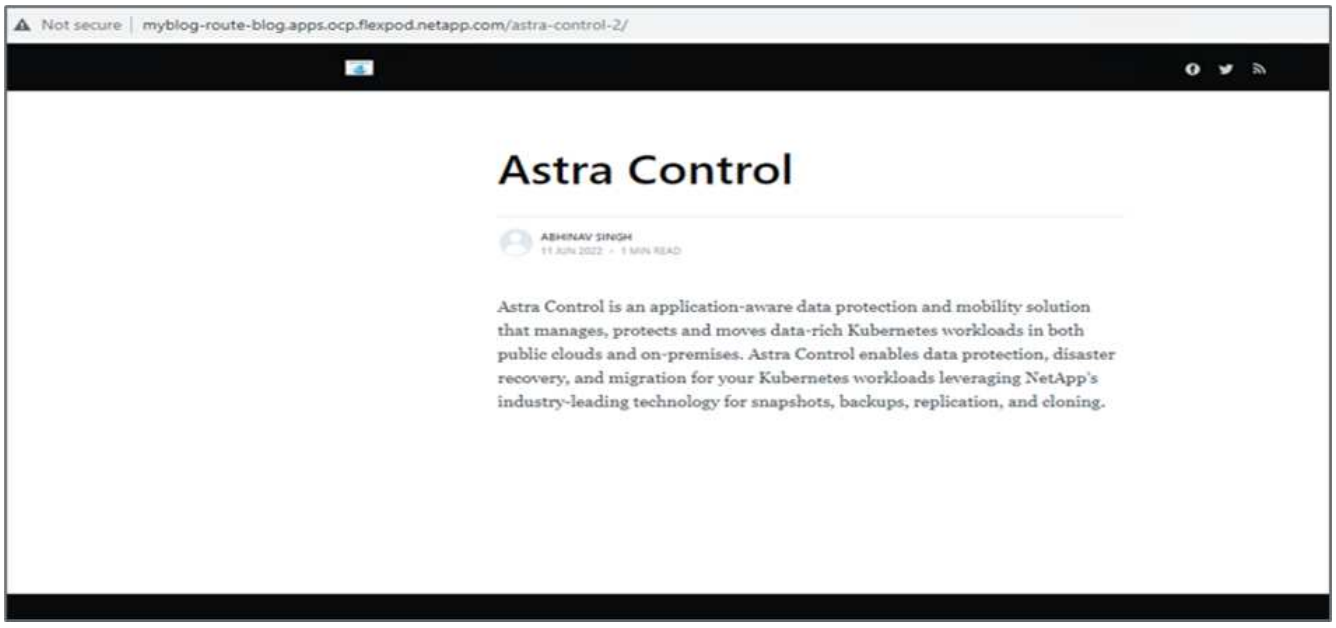
2. 最初のOpenShiftクラスタにログインし、Projectに移動して、検索バーにBlogと入力します。



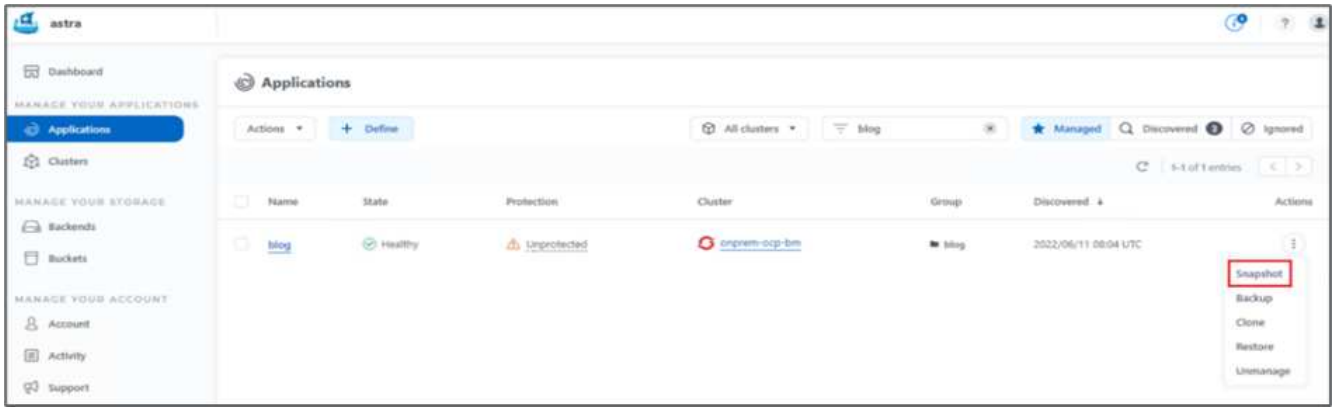
3. サイドメニューから、[Networking]>[Routes]の順に選択し、URLをクリックします。



4. ブログのホームページが表示されます。ブログサイトにコンテンツを追加して公開します。



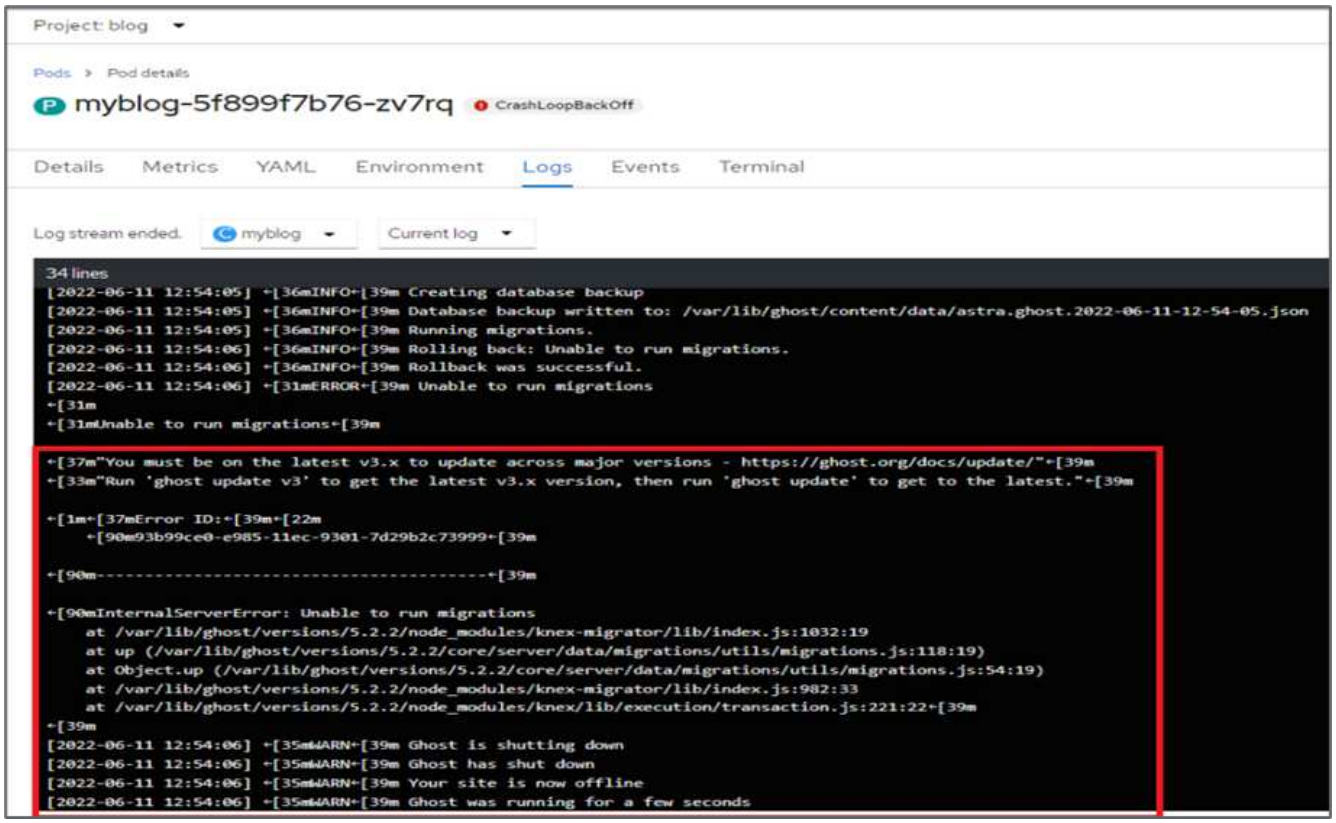
5. Astra Control Centerにアクセスします。最初に検出タブからアプリケーションを管理してから、Snapshotコピーを作成します。



定義したスケジュールでスナップショット、バックアップ、またはその両方を作成することで、アプリケーションを保護することもできます。詳細については、を参照してください "Snapshot とバックアップでアプリケーションを保護"。

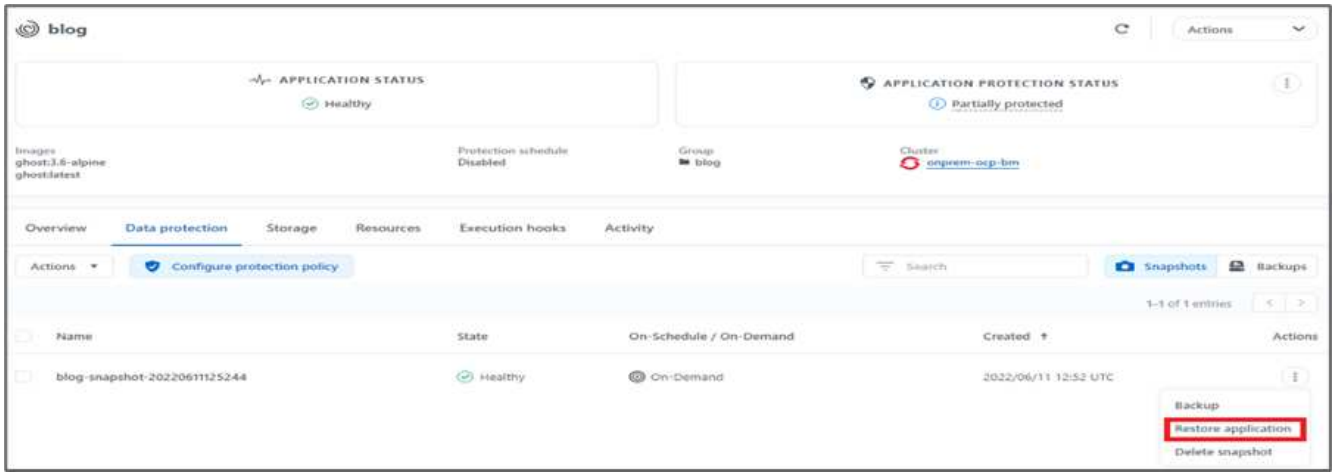
6. オンデマンドスナップショットが正常に作成されたら、アプリケーションを最新バージョンにアップグレードします。現在のイメージのバージョンは「ghost:3.6 -アルパイン」で、ターゲットのバージョンは「ghost:latest」です。アプリをアップグレードするには、Gitリポジトリに直接変更を加え、Argo CDに同期します。

7. ブログサイトがダウンし、アプリケーション全体が破損しているために、最新バージョンへの直接アップグレードがサポートされていないことがわかります。

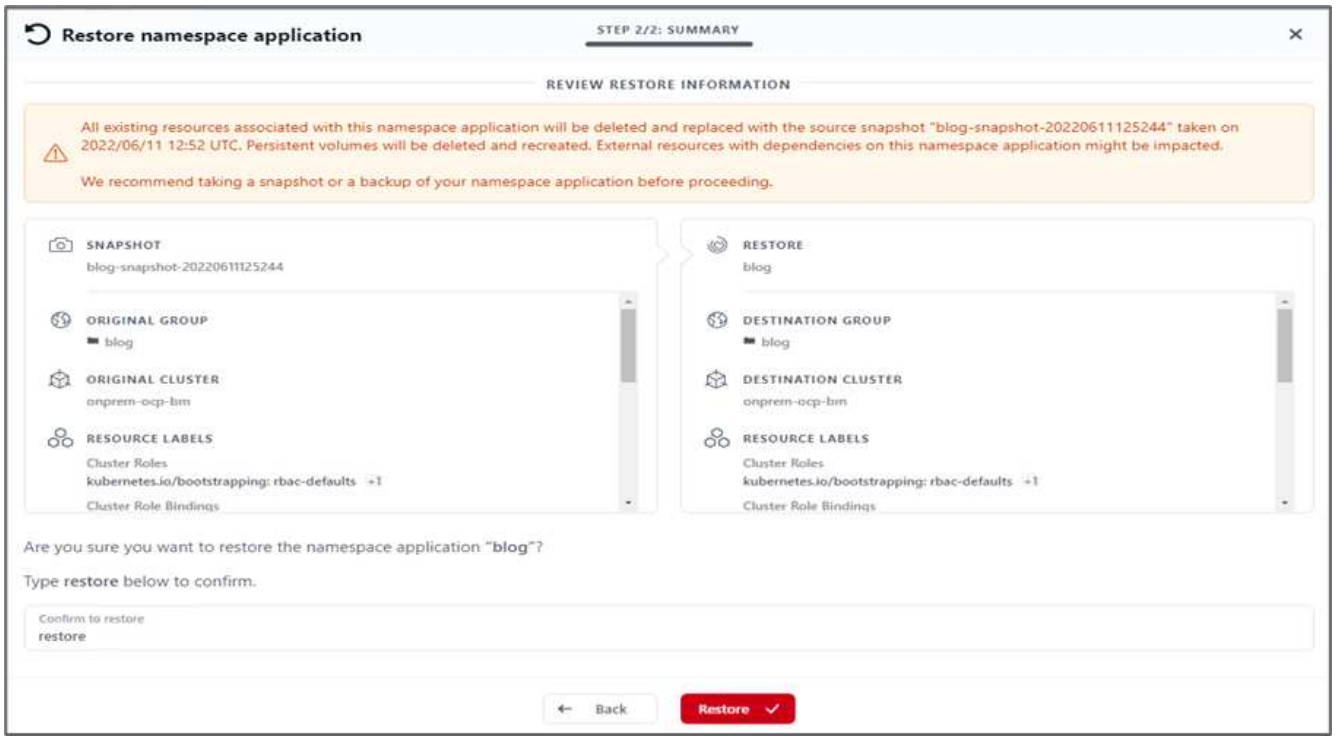


8. ブログサイトが利用できないことを確認するには、URLを更新します。

9. スナップショットからアプリケーションを復元します。

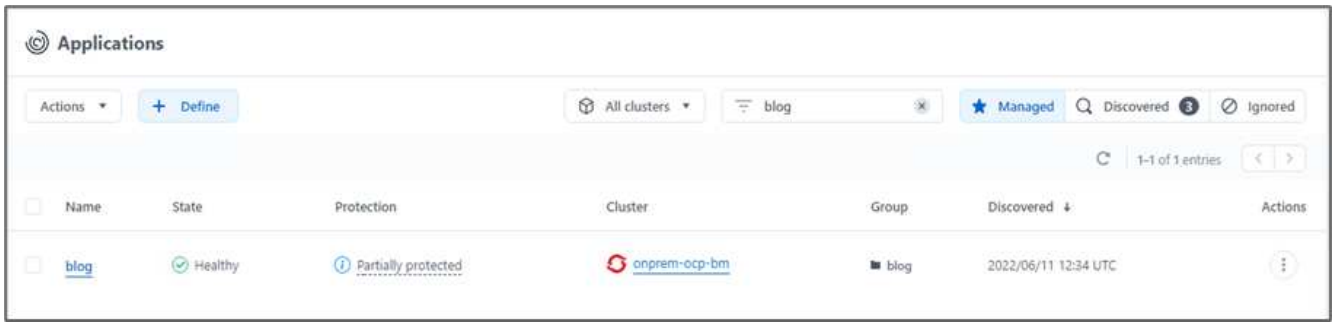


10. アプリケーションは同じOpenShiftクラスタにリストアされます。

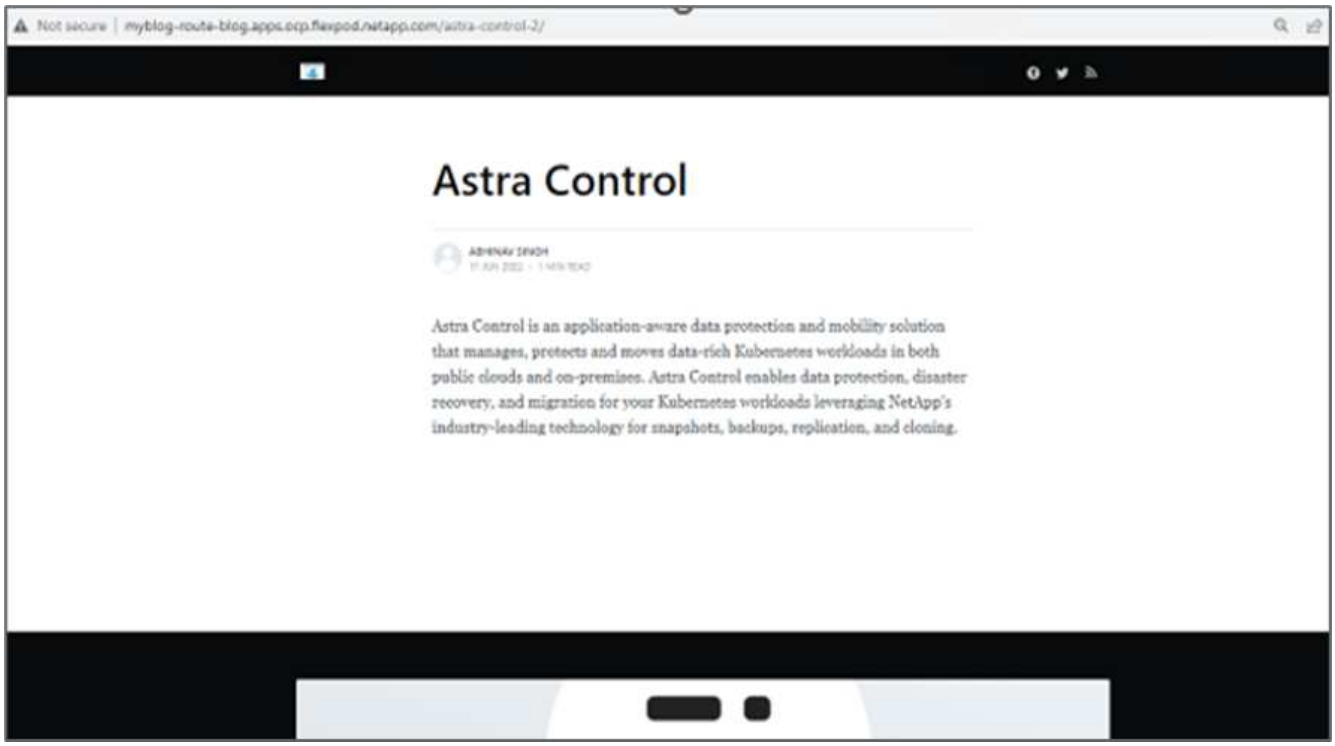


11. アプリケーションのリストアプロセスがただちに開始されます。

12. 数分後に、使用可能なスナップショットからアプリケーションが正常にリストアされます。



13. Webページが表示されるかどうかを確認するには、URLを更新します。

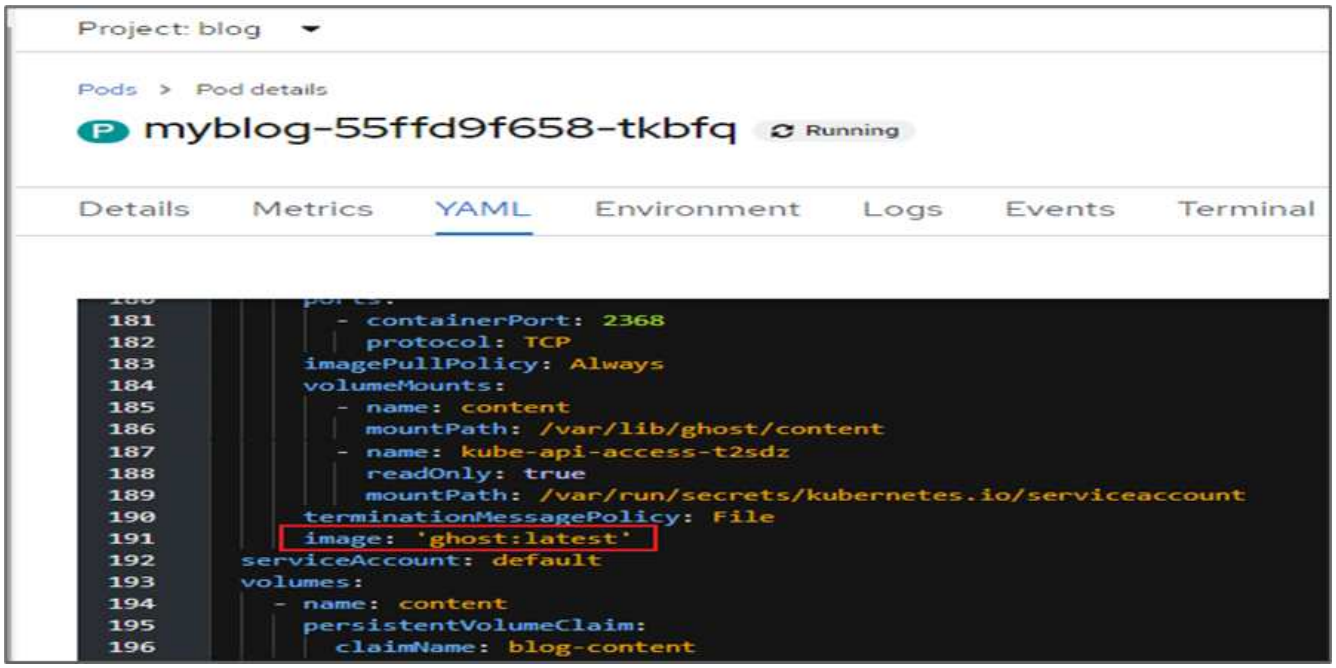


DevTestチームは、Astra Control Centerを活用して、ブログサイトアプリとその関連データをスナップショットを使用して正常にリカバリできます。

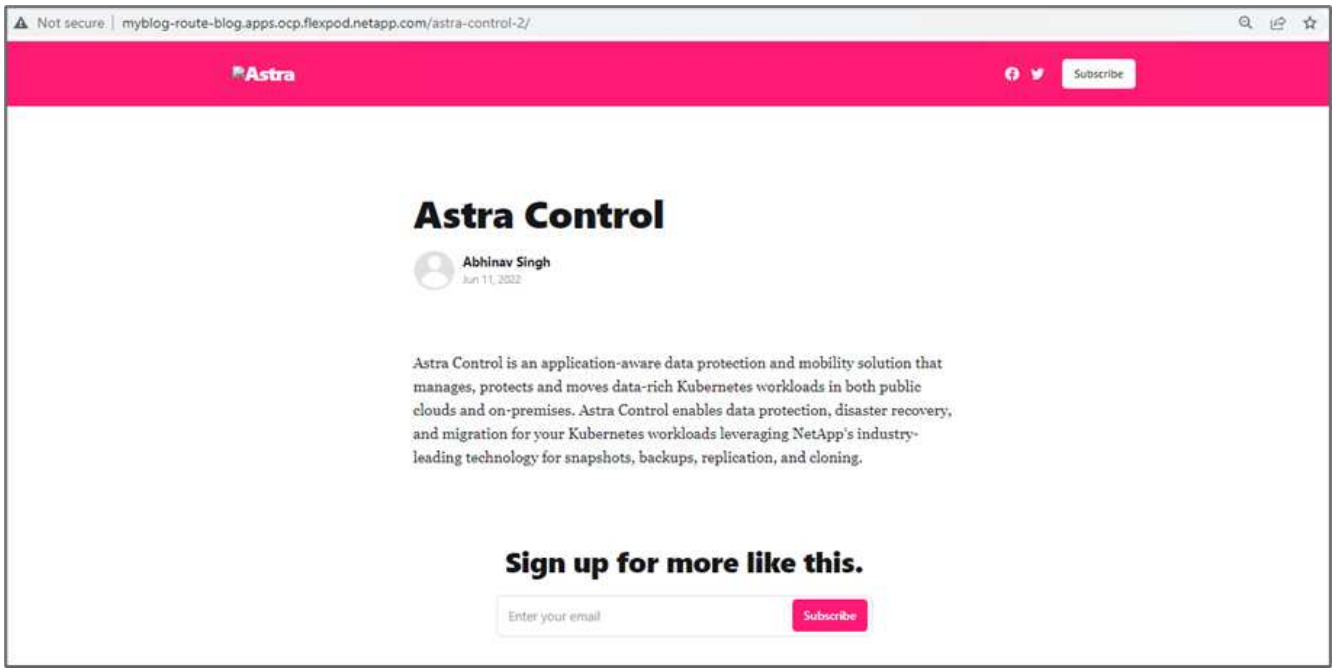
パート**2**

Astra Control Centerを使用すると、クラウド上またはオンプレミスで、クラウド上のどの場所にあるかに関係なく、アプリケーション全体をKubernetesクラスタ間でデータとともに移動できます。

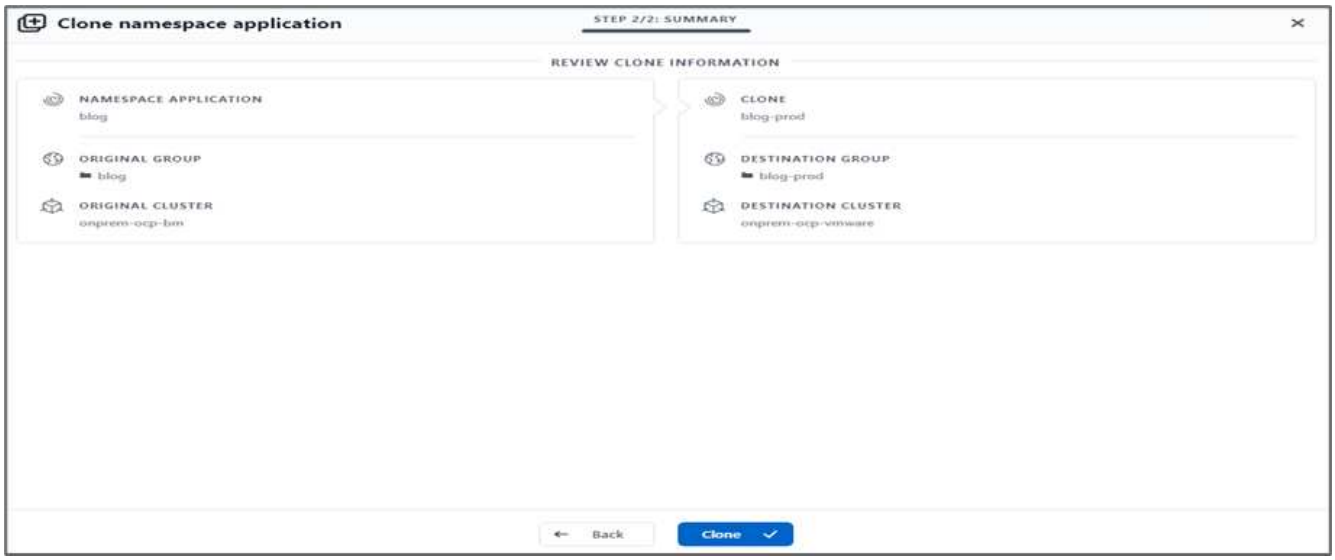
1. DevTestチームは、アプリケーションを最初にサポートされているバージョン（「ゴースト- 4.6 -アルプス」）にアップグレードしてから、最終バージョン（「ゴースト-最新」）にアップグレードして、本番環境を準備します。その後、別のFlexPod システムで実行されている本番環境のOpenShiftクラスタにクローニングされているアプリケーションをアップグレードします。
2. この時点で、アプリケーションが最新バージョンにアップグレードされ、本番環境のクラスタにクローニングできる状態になります。



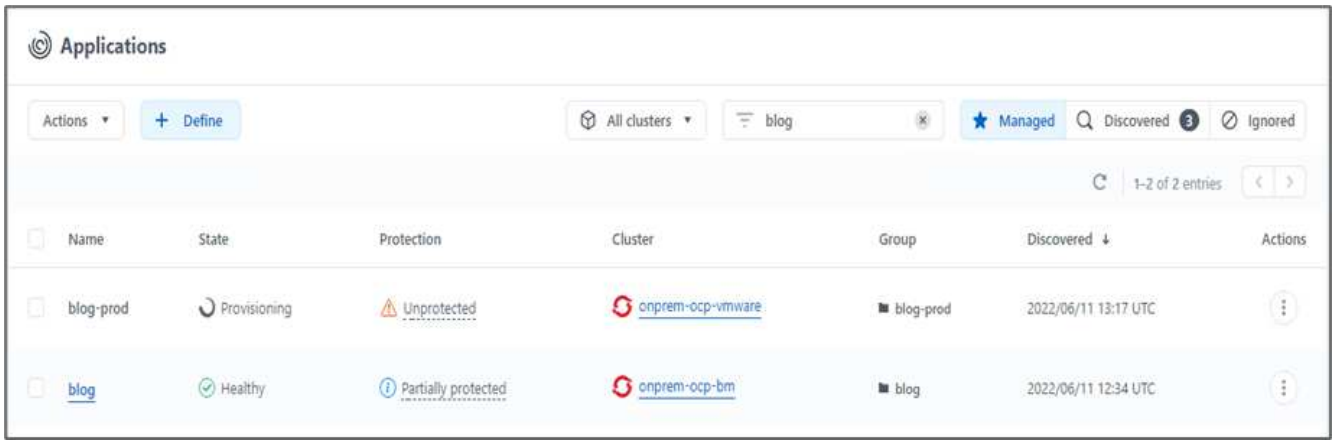
3. 新しいテーマを確認するには、ブログサイトを更新します。



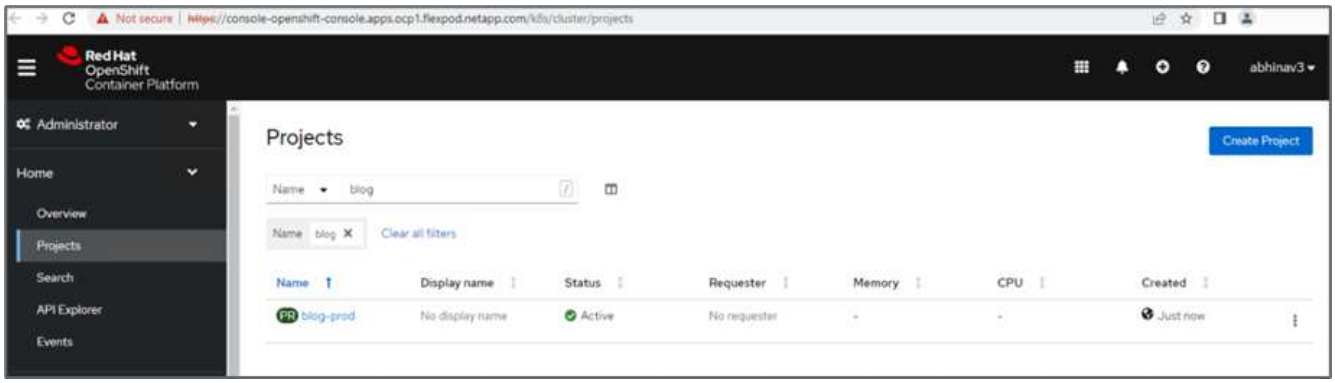
4. Astra Control Centerから、VMware vSphereで実行されている他の本番環境OpenShiftクラスタにアプリケーションをクローニングします。



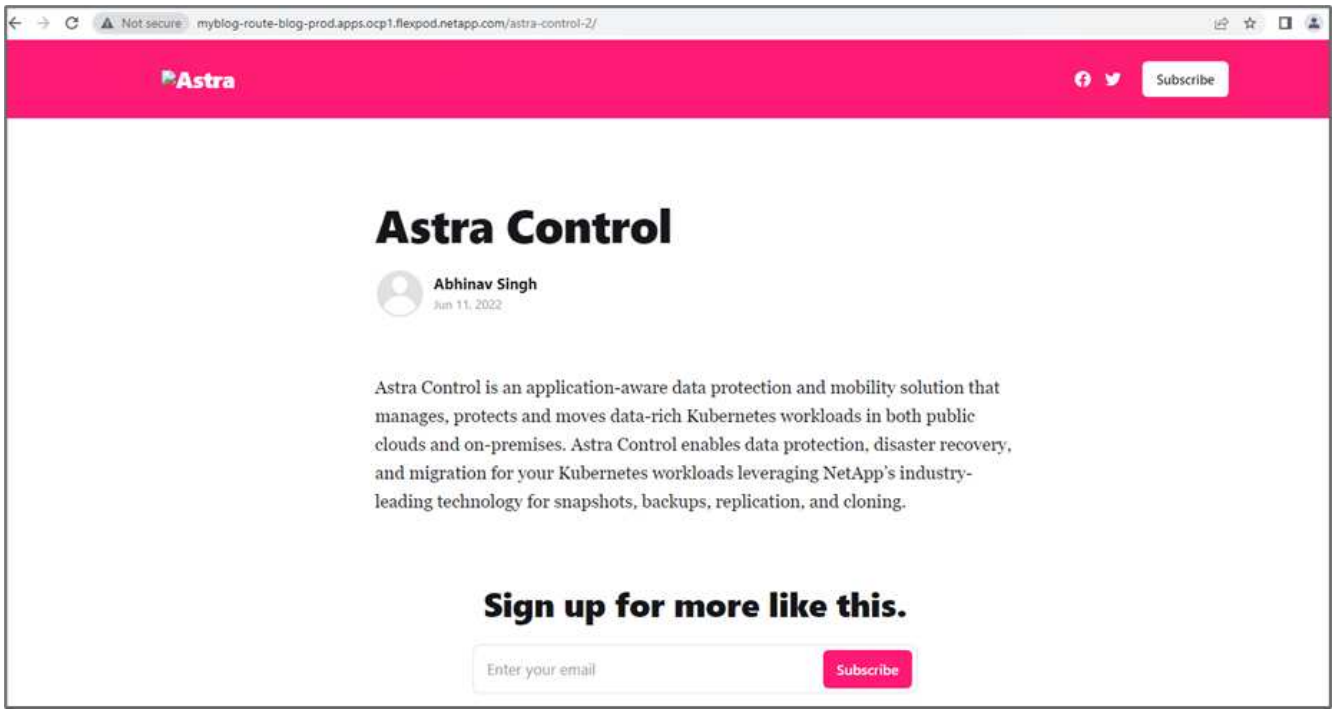
これで、本番環境のOpenShiftクラスタで新しいアプリケーションクローンがプロビジョニングされます。



5. 本番環境のOpenShiftクラスタにログインし、プロジェクトブログを検索します。



6. サイドメニューから、Networking > Routesを選択し、Locationの下のURLをクリックします。同じホームページとコンテンツが表示されます。



これでAstra Control Center解決策 の検証は終了です。Kubernetesクラスタが配置されている場所に関係なく、アプリケーション全体とそのデータを1つのKubernetesクラスタから別のクラスタにクローニングできるようになりました。

"次は終わりです"

まとめ

"Previous：リモートバックアップを使用したアプリケーションのリカバリ。"

この解決策 では、ネットアップのAstraポートフォリオを使用して、FlexPod とAWSで実行されるコンテナ化アプリケーション向けの保護計画を実装しました。ネットアップのAstra Control CenterとAstra Tridentは、Cloud Volumes ONTAP 、Red Hat OpenShift、FlexPod インフラとともに、この解決策 のコアコンポーネントを形成しました。

Snapshotをキャプチャしてアプリケーションの保護を実証し、クラウド環境とオンプレミス環境で実行されているKubernetesクラスタ間でアプリケーションをリストアするフルコピーバックアップを実行しました。

また、Kubernetesクラスタ間でアプリケーションのクローニングを実演し、お客様が希望する場所で選択したKubernetesクラスタにアプリケーションを移行できるようにする方法についても説明しました。

FlexPod は絶えず進化しているため、お客様はアプリケーションやビジネス提供プロセスを最新化できます。この解決策 を使用することで、FlexPod のお客様は、解決策 のコストを低く抑えながら、短期またはフルタイムのDRプランを作成できる場所としてパブリッククラウドを使用して、クラウドネイティブアプリケーション向けのBCDRプランを自信を持って構築できます。

Astra Controlを使用すると、クラスタの配置場所に関係なく、アプリケーション全体をKubernetesクラスタ間でデータとともに移動できます。また、クラウドネイティブアプリケーションの導入、運用、保護を高速化するのにも役立ちます。

トラブルシューティング

トラブルシューティングのガイダンスについては、を参照してください "オンラインドキュメント"。

追加情報の参照先

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

- FlexPod ホームページ

  "https://www.flexpod.com"

- FlexPod のシスコ検証済み設計および導入ガイド

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- Ansibleを使用して、VMwareのコードとしてInfrastructureを使用したFlexPod の導入

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2.html#AnsibleAutomationWorkflowandSolutionDeployment"

- Ansibleを使用したRed Hat OpenShift Bare Metalのコードとしてのインフラを使用したFlexPod 導入

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_iac_redhat_openshift.html"

- Cisco UCS ハードウェアおよびソフトウェア相互運用性ツール

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- Cisco Intersightのデータシート

  "https://intersight.com/help/saas/home"

- ネットアップAstraのドキュメント

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- ネットアップアストラコントロールセンター

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- ネットアップアストラト Trident

  "https://docs.netapp.com/us-en/trident/index.html"

- NetApp Cloud Manager の略

  "https://docs.netapp.com/us-en/occm/concept_overview.html"

- NetApp Cloud Volumes ONTAP の略

"https://docs.netapp.com/us-en/occm/task_getting_started_aws.html"

- Red Hat OpenShift のサービスです

  "https://www.openshift.com/"

- NetApp Interoperability Matrix Tool で確認できます

  "http://support.netapp.com/matrix/"

バージョン履歴

バージョン	日付	ドキュメントのバージョン履歴
バージョン 1.0 以降	2022年7月	ACC 22.04.0用リリース。

NetApp Cloud Insights for FlexPod の略

TR-4868 ：『 NetApp Cloud Insights for FlexPod 』

ネットアップ、 Alan Cowles 氏

協力：

このテクニカルレポートで詳述されている解決策は、 ONTAP データセンター解決策の一部として導入されている NetApp AFF を実行している NetApp Cloud Insights A800 ストレージシステムを監視するために、 NetApp FlexPod サービスを設定する方法を示しています。

お客様にもたらされる価値

ここで詳述する解決策は、フル機能を備えたハイブリッドクラウド環境向けの監視解決策に関心があり、 ONTAP をプライマリストレージシステムとして導入するお客様に価値を提供します。これには、ネットアップの AFF および FAS ストレージシステムを使用する FlexPod 環境が含まれます。

ユースケース

この解決策環境のユースケースは次のとおりです。

- FlexPod 解決策の一部として導入された ONTAP ストレージシステムのさまざまなリソースと使用率を監視する必要がある組織。
- AFF または FAS システムを使用して FlexPod 解決策で発生したインシデントのトラブルシューティングを行い、解決時間を短縮したいと考えている組織。
- コストの最適化を検討している組織では、無駄なリソースに関する詳細な情報を提供するカスタマイズされたダッシュボードや、 ONTAP などの FlexPod 環境でコスト削減を実現できる場所などが挙げられます。

対象読者

解決策の対象となるグループは次のとおりです。

- コストの最適化とビジネス継続性に関心を持つ IT エグゼクティブとその関係者。
- データセンターやハイブリッドクラウドの設計と管理に関心のあるソリューションアーキテクト。
- トラブルシューティングとインシデント解決を担当するテクニカルサポートエンジニア。

Cloud Insights は、計画、トラブルシューティング、メンテナンス、およびビジネス継続性の確保に役立ついくつかの有用なデータタイプを提供するように設定できます。FlexPod Datacenter 解決策 with Cloud Insights を監視し、集計データをわかりやすいカスタマイズされたダッシュボードに表示することで、 ニーズに応じて環境内のリソースをいつ拡張する必要があるかを予測できるだけでなく、システム内で問題の原因となっている特定のアプリケーションやストレージボリュームを特定することもできます。これにより、監視対象のインフラストラクチャが予測可能で、期待どおりに動作することが保証されます。これにより、組織は定義済みの SLA を提供し、必要に応じてインフラストラクチャを拡張できるようになり、無駄と追加コストを削減できます。

アーキテクチャ

このセクションでは、 Cloud Insights で監視される NetApp AFF A800 システムを含む、 FlexPod データセンター統合インフラのアーキテクチャについて説明します。

解決策テクノロジ

FlexPod Datacenter 解決策には、次に示す最小コンポーネントが含まれており、可用性が高く、拡張性に優れ、検証済みで、サポートされている統合インフラ環境を構築できます。

- NetApp ONTAP ストレージノード × 2 （ HA ペア × 1 ）
- Cisco Nexus データセンターネットワークスイッチ × 2
- Cisco MDS ファブリックスイッチ × 2 （ FC 環境ではオプション）
- Cisco UCS ファブリックインターコネクト × 2
- 1 台の Cisco UCS ブレードシャーシに 2 台の Cisco UCS B シリーズブレードサーバを搭載

または

- Cisco UCS C シリーズラックマウントサーバ × 2

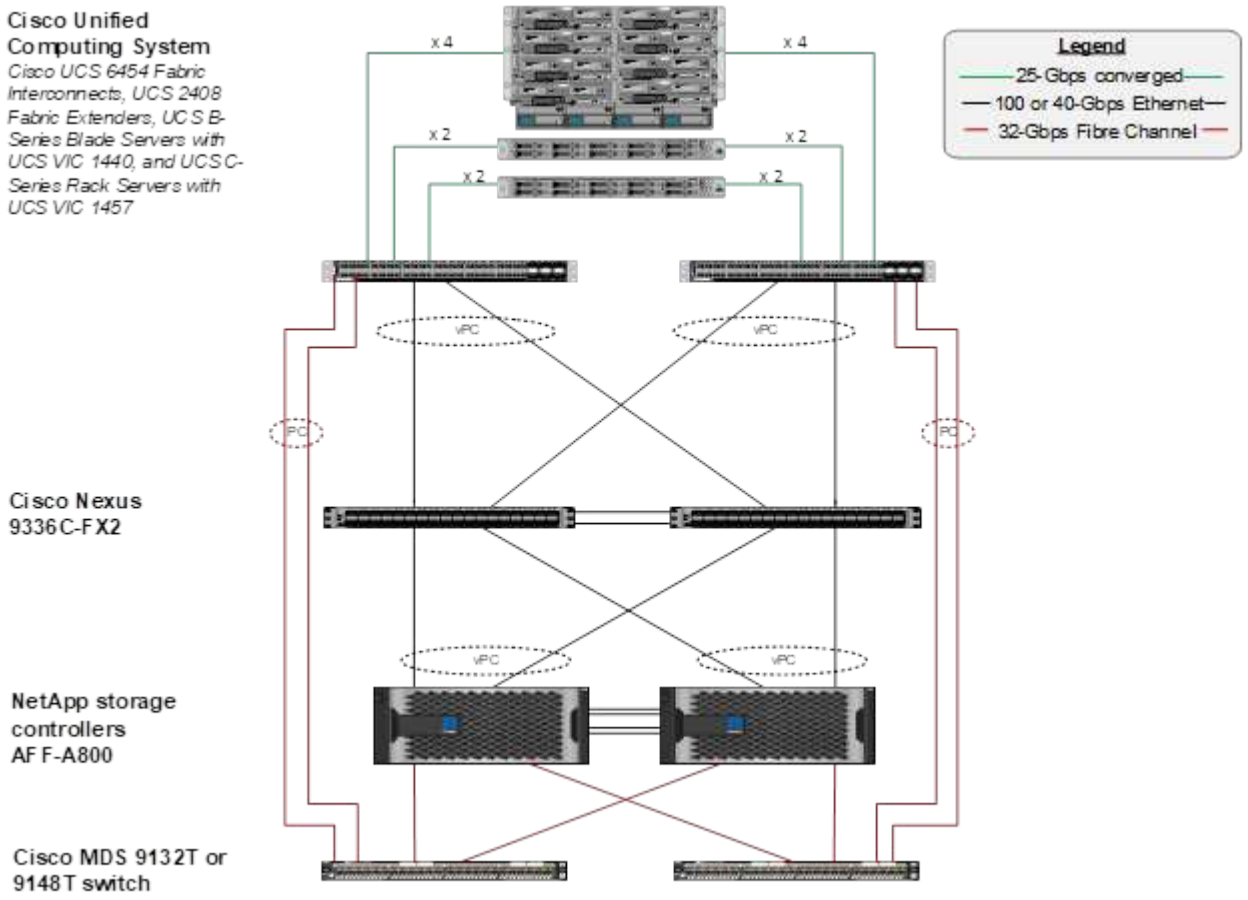
Cloud Insights でデータを収集するには、 FlexPod データセンター環境内、またはデータを収集するコンポーネントにアクセスできる場所に、仮想マシンまたは物理マシンとして Acquisition Unit を導入する必要があります。Acquisition Unit ソフトウェアは、サポートされている複数の Windows または Linux オペレーティングシステムを実行するシステムにインストールできます。次の表に、このソフトウェアの解決策コンポーネントを示します。

オペレーティングシステム	バージョン
Microsoft Windows の場合	10.
Microsoft Windows Server の場合	2012 、 2012 R2 、 2016 、 2019
Red Hat Enterprise Linux の場合	7.2 – 7.6

オペレーティングシステム	バージョン
CentOS の場合	7.2 – 7.6
Oracle Enterprise Linux の場合	7.5
Debian	9.
Ubuntu	18.04 LTS

アーキテクチャ図

次の図に、解決策のアーキテクチャを示します。



ハードウェア要件

次の表に、解決策の実装に必要なハードウェアコンポーネントを示します。解決策の特定の実装で使用されるハードウェアコンポーネントは、お客様の要件に応じて異なる場合があります。

ハードウェア	数量
Cisco Nexus 9336C-FX2	2.
Cisco UCS 6454 ファブリックインターコネクト	2.
Cisco UCS 5108 ブレードシャーシ	1.
Cisco UCS 2408 ファブリックエクステンダ	2.

ハードウェア	数量
Cisco UCS B200 M5 ブレード	2.
NetApp AFF A800	2.

ソフトウェア要件

次の表に、解決策の実装に必要なソフトウェアコンポーネントを示します。解決策の特定の実装で使用されるソフトウェアコンポーネントは、お客様の要件に応じて異なる場合があります。

ソフトウェア	バージョン
Cisco Nexus ファームウェア	9.3 （ 5 ）
Cisco UCS のバージョン	4.1 （ 2a ）
NetApp ONTAP のバージョン	9.7
NetApp Cloud Insights のバージョン	2020 年 9 月、基本
Red Hat Enterprise Linux の場合	7.6
VMware vSphere の場合	6.7U3

ユースケースの詳細

この解決策環境のユースケースは次のとおりです。

- NetApp Active IQ デジタルアドバイザに提供されたデータを基に環境を分析し、ストレージシステムのリスクとストレージ最適化に関する推奨事項を評価します。
- FlexPod Datacenter 解決策に導入された ONTAP ストレージ・システムの問題をトラブルシューティングするには、システム統計情報をリアルタイムで調べます。
- ONTAP データセンター統合インフラに導入された FlexPod ストレージシステムの特定の関心ポイントを簡単に監視できるように、カスタマイズしたダッシュボードを生成できます。

設計上の考慮事項

FlexPod Datacenter 解決策は、シスコとネットアップが設計した統合インフラです。エンタープライズワークロードを実行するための、動的で可用性が高く、拡張性に優れたデータセンター環境を提供します。解決策のコンピューティングリソースとネットワークリソースは Cisco UCS および Nexus 製品から提供され、ストレージリソースは ONTAP ストレージシステムから提供されます。解決策設計は、更新されたハードウェアモデルまたはソフトウェアとファームウェアのバージョンが利用可能になったときに、定期的に拡張されます。これらの詳細情報に加え、解決策の設計と導入に関するベストプラクティスも、 Cisco Validated Design （ CVD ）または NetApp Verified Architecture （ NVA ）ドキュメントにキャプチャされ、定期的に公開されています。

FlexPod Datacenter 解決策の設計に関する最新の CVD ドキュメントを参照できます "こちらをご覧ください"。

Cloud Insights for FlexPod を導入します

解決策を導入するには、次のタスクを実行する必要があります。

1. Cloud Insights サービスに登録します
2. Acquisition Unit として設定する VMware 仮想マシン（ VM ）を作成します
3. Red Hat Enterprise Linux （ RHEL ）ホストをインストールします
4. Cloud Insights ポータルで Acquisition Unit インスタンスを作成し、ソフトウェアをインストールします
5. FlexPod データセンターから Cloud Insights に監視対象のストレージシステムを追加します。

NetApp Cloud Insights サービスに登録します

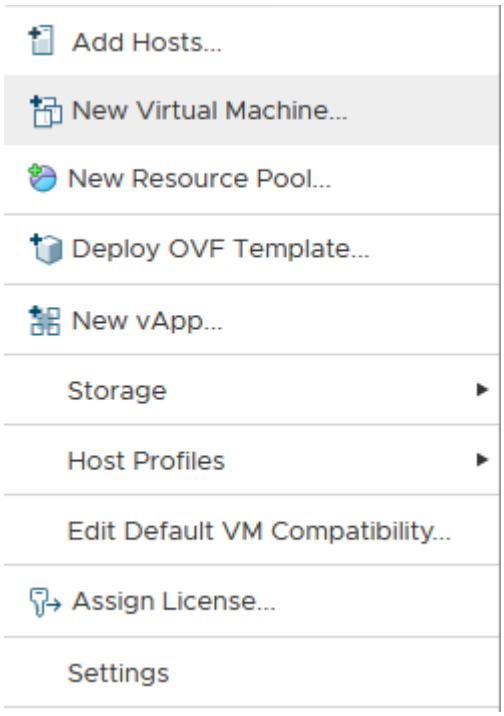
NetApp Cloud Insights サービスに登録するには、次の手順を実行します。

1. に進みます "https://cloud.netapp.com/cloud-insights"
2. 画面の中央にあるボタンをクリックして 14 日間の無償トライアルを開始するか、右上にあるリンクをクリックして、既存の NetApp Cloud Central アカウントに登録またはログインします。

Acquisition Unit として設定する VMware 仮想マシンを作成する

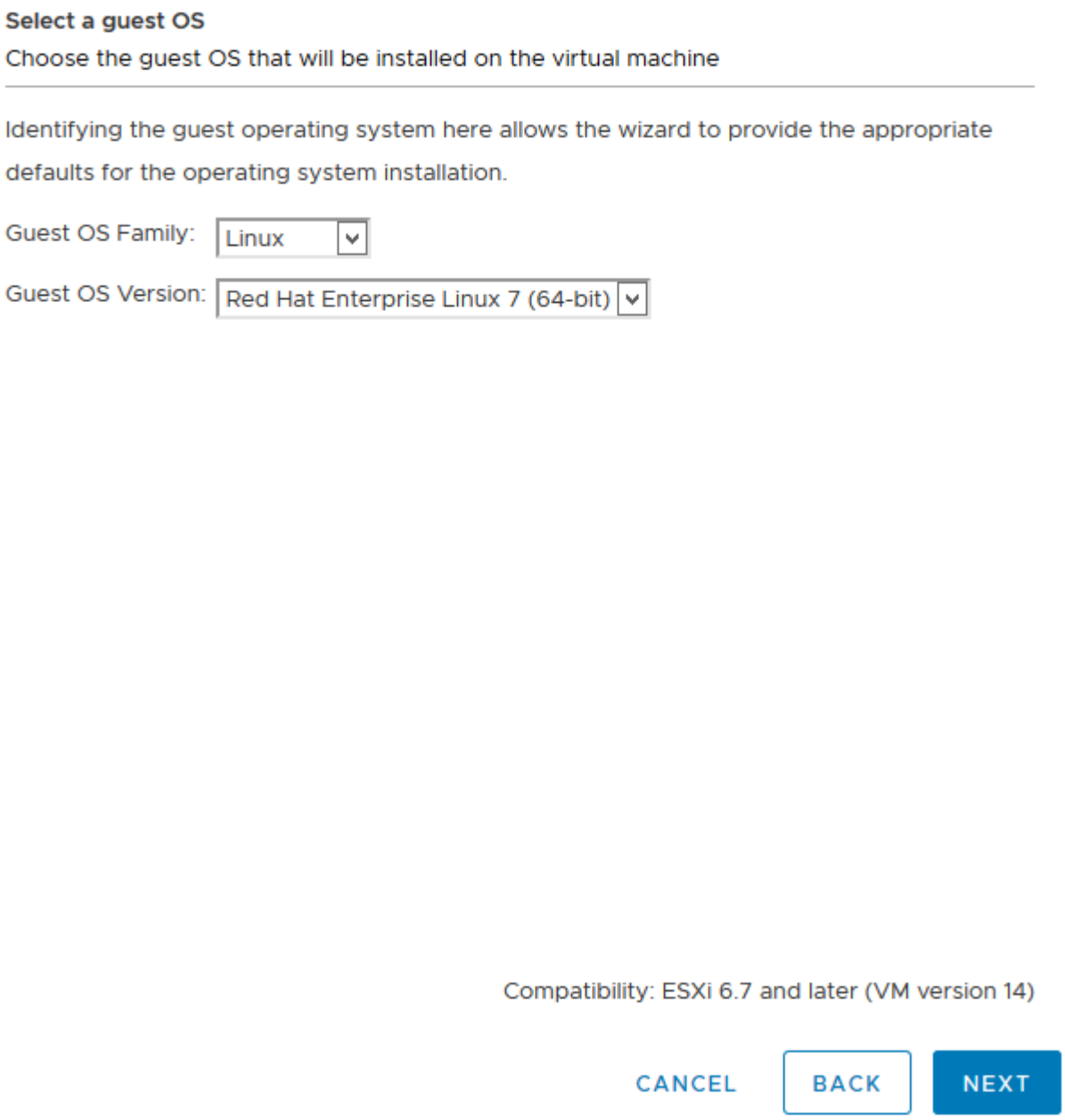
VMware VM を作成して Acquisition Unit として設定するには、次の手順を実行します。

1. Web ブラウザを起動して VMware vSphere にログインし、 VM をホストするクラスタを選択します。
2. そのクラスタを右クリックし、メニューから [仮想マシンの作成] を選択します。



3. 新規仮想マシンウィザードで、次へをクリックします。
4. VM の名前を指定し、インストール先のデータセンターを選択して、 Next （次へ）をクリックします。

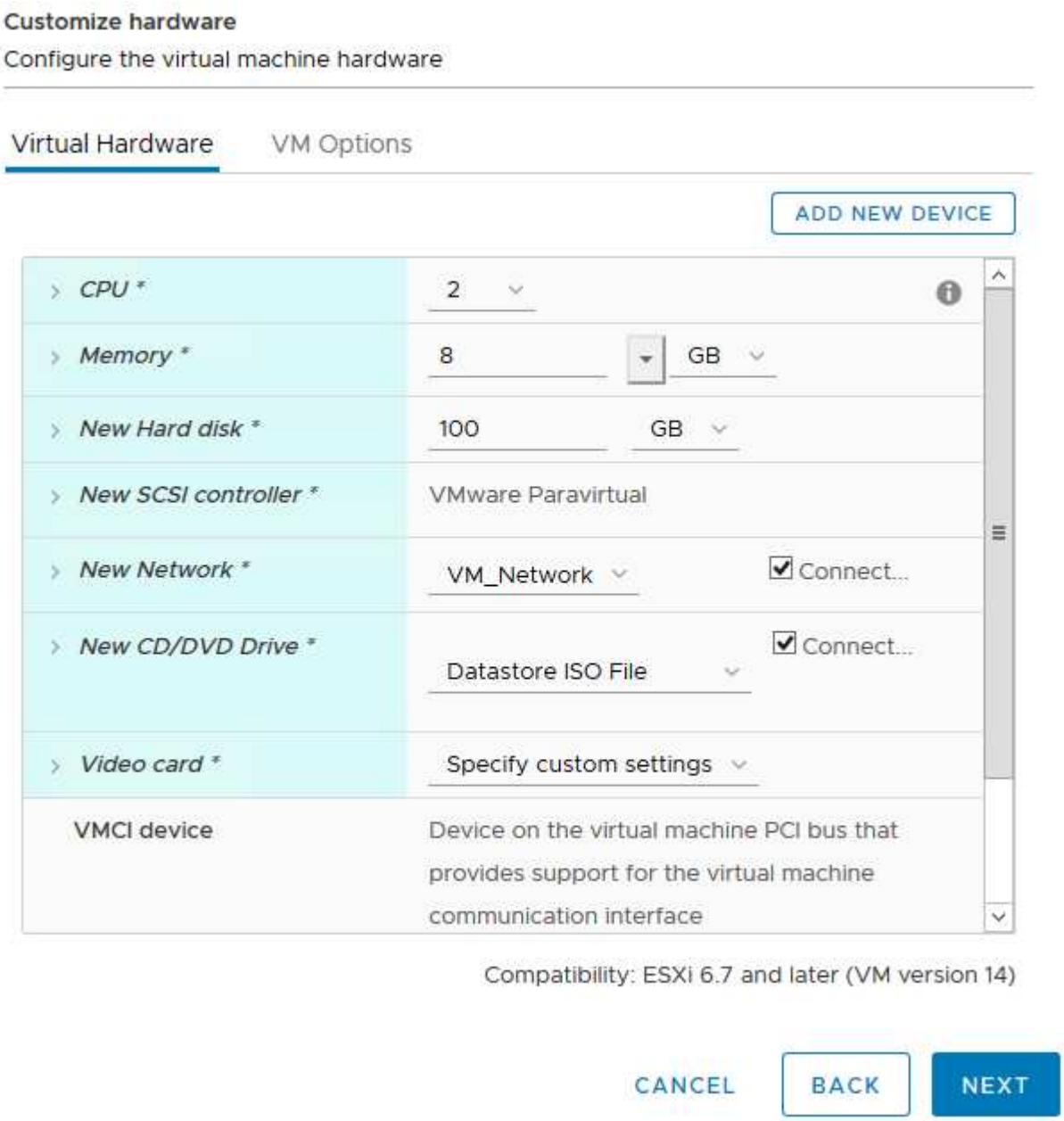
5. 次のページで、 VM のインストール先となるクラスタ、ノード、またはリソースグループを選択し、 [次へ] をクリックします。
6. VM をホストする共有データストアを選択し、 Next （次へ）をクリックします。
7. VM の互換性モードが ESXi 6.7 以降に設定されていることを確認し '[次へ] をクリックします
8. [Guest OS Family Linux, Guest OS Version: Red Hat Enterprise Linux 7 (64 bit)] を選択します。



9. 次のページでは、 VM のハードウェアリソースをカスタマイズできます。Cloud Insights Acquisition Unit には、次のリソースが必要です。リソースを選択したら、 [次へ] をクリックします。
   a. CPU × 2
   b. 8GB の RAM
   c. 100GB のハードディスクスペースが必要です

d. ポート 443 で SSL 接続を介して FlexPod データセンターおよび Cloud Insights サーバのリソースにアクセスできるネットワーク。

e. 選択した Linux ディストリビューション（ Red Hat Enterprise Linux ）の ISO イメージをブート元として指定します。

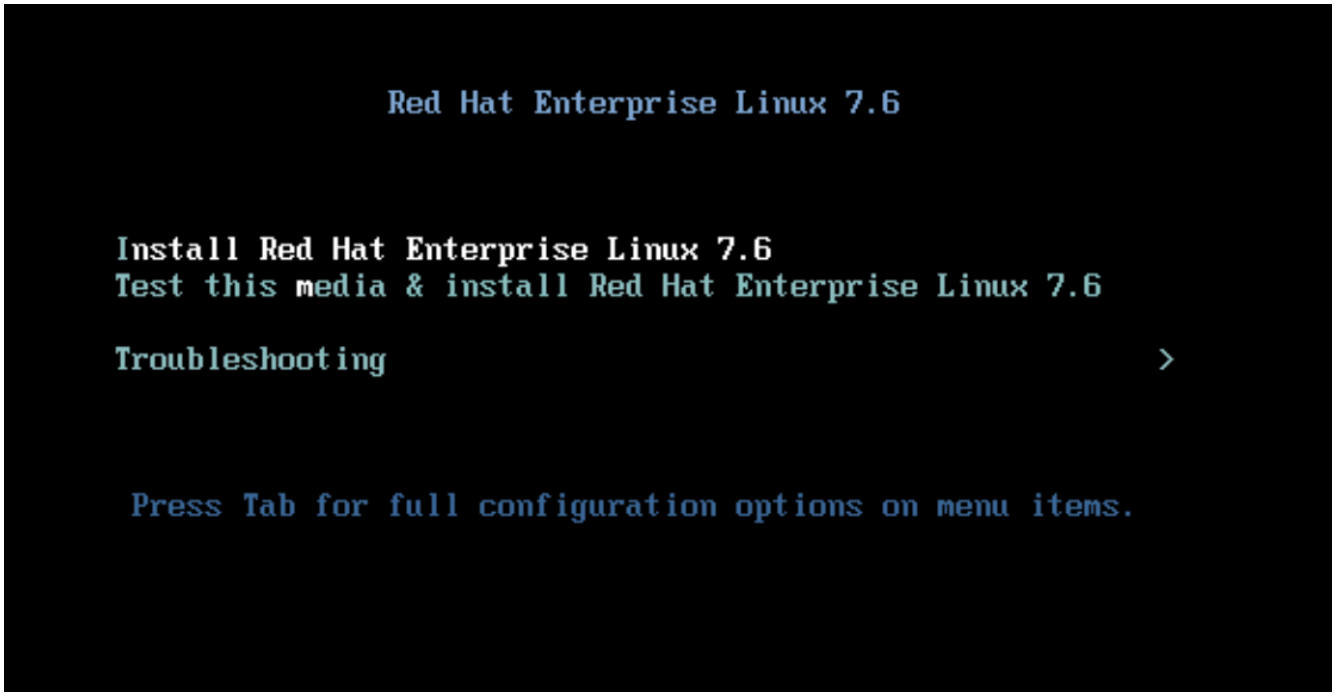


10. VM を作成するには、 [Ready to Complete] ページで設定を確認し、 [Finish] をクリックします。

Red Hat Enterprise Linux をインストールします

Red Hat Enterprise Linux をインストールするには、次の手順を実行します。

1. VM の電源をオンにし、ウィンドウをクリックして仮想コンソールを起動し、 Red Hat Enterprise Linux 7.6 をインストールするオプションを選択します。



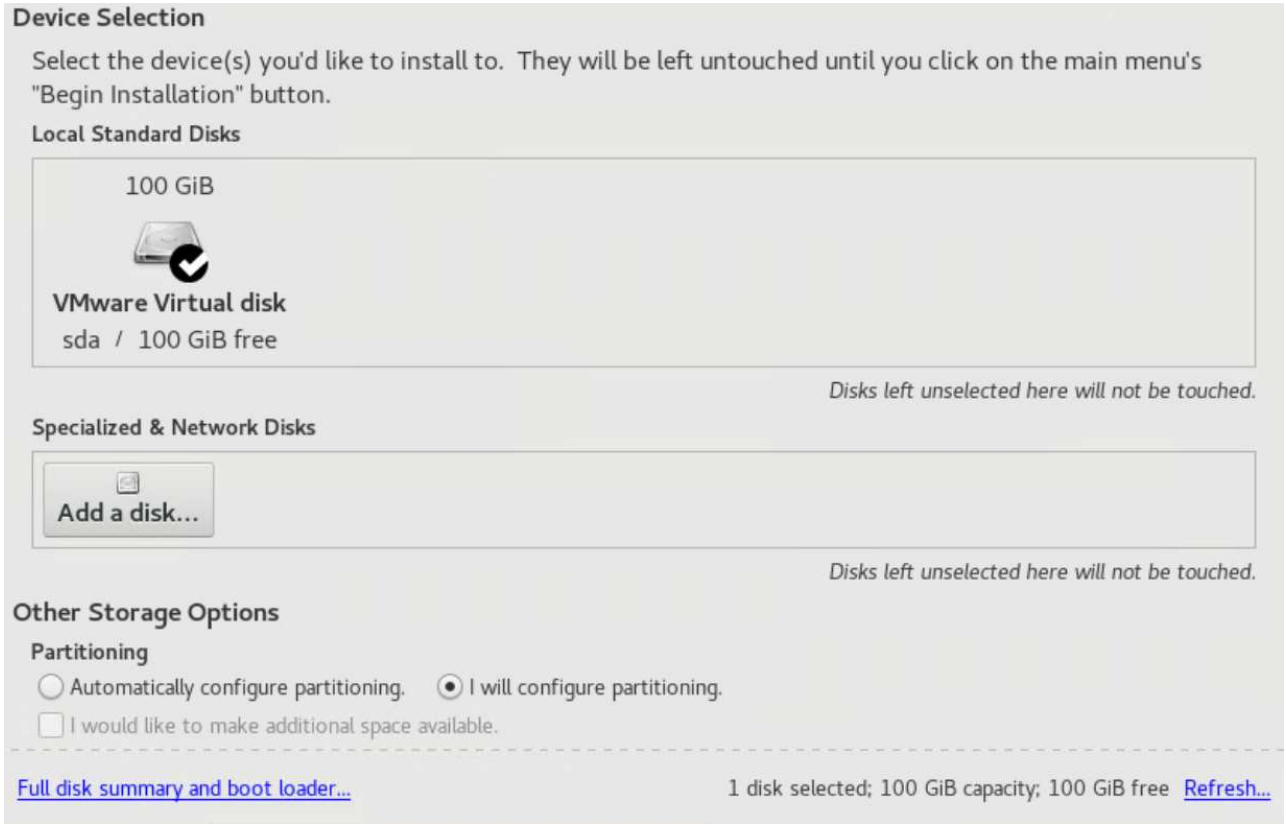
2. 使用する言語を選択し、 [続行] をクリックします。

   次のページはインストールの概要です。これらのオプションのほとんどはデフォルト設定のままでかまいません。

3. 次のオプションを実行して、ストレージレイアウトをカスタマイズする必要があります。

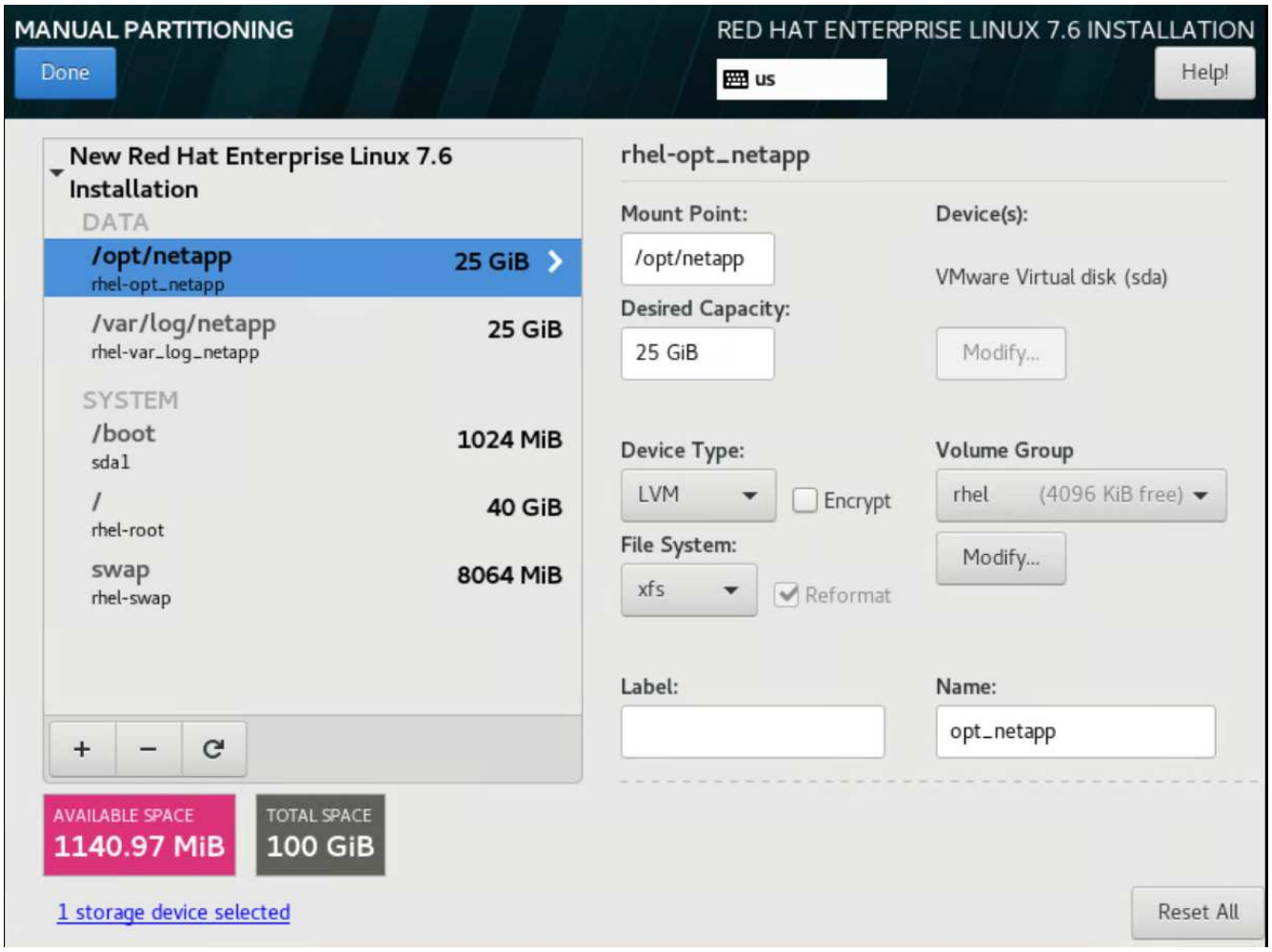
   a. サーバのパーティションをカスタマイズするには、インストール先をクリックします。

   b. VMware 仮想ディスク 100GiB がブラックチェックマークで選択されていることを確認し、 [I will Configure Partitioning （パーティションの設定）] オプションボタンを選択します。



c. 完了をクリックします。

新しいメニューが表示され、パーティションテーブルをカスタマイズできます。それぞれ 25 GB を '/opt/NetApp' と '/var/log/netapp' 専用にします残りのストレージをシステムに自動的に割り当てることができます。

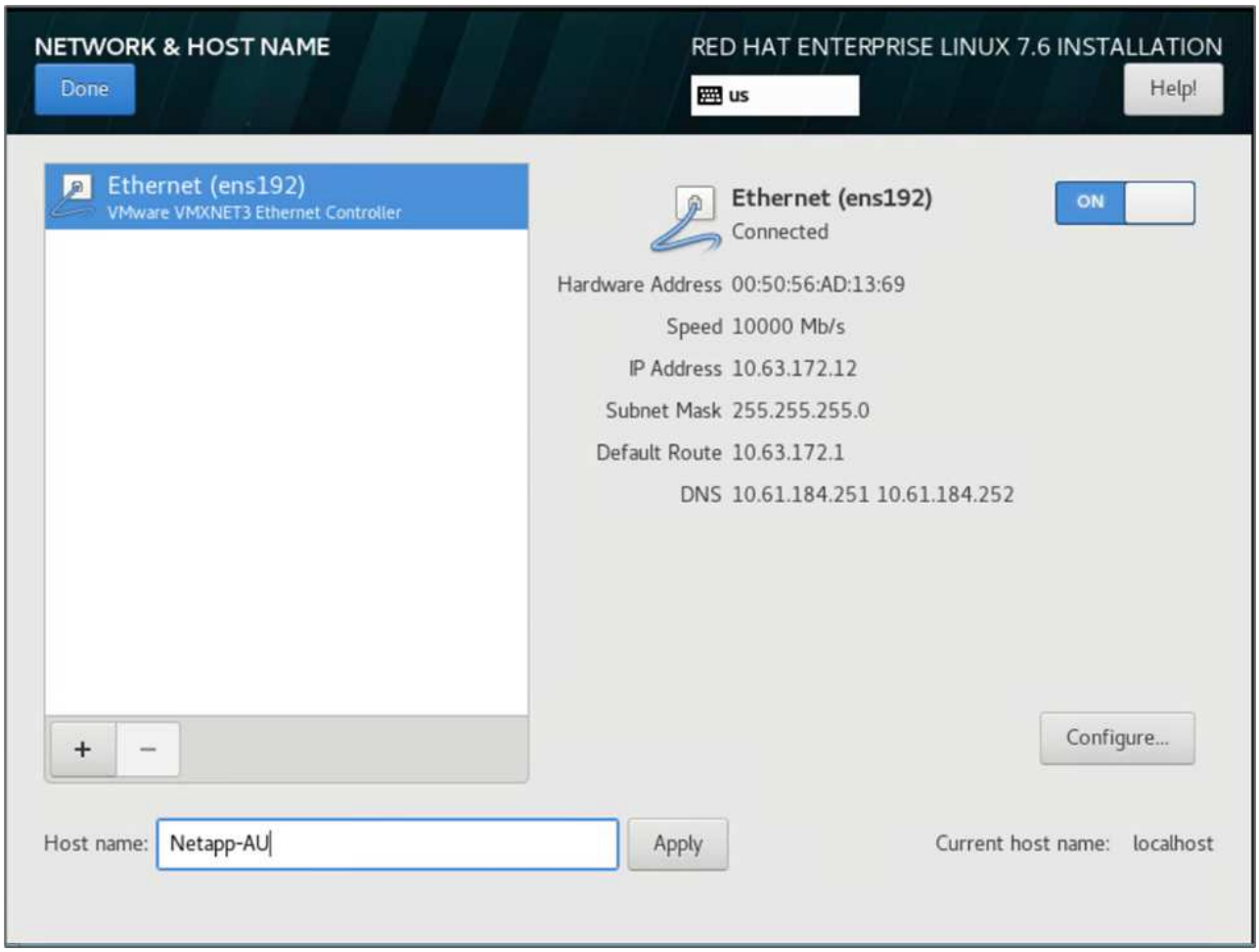


a. [インストールの概要] に戻るには、 [完了] をクリックします。

4. [ネットワークとホスト名] をクリックします。

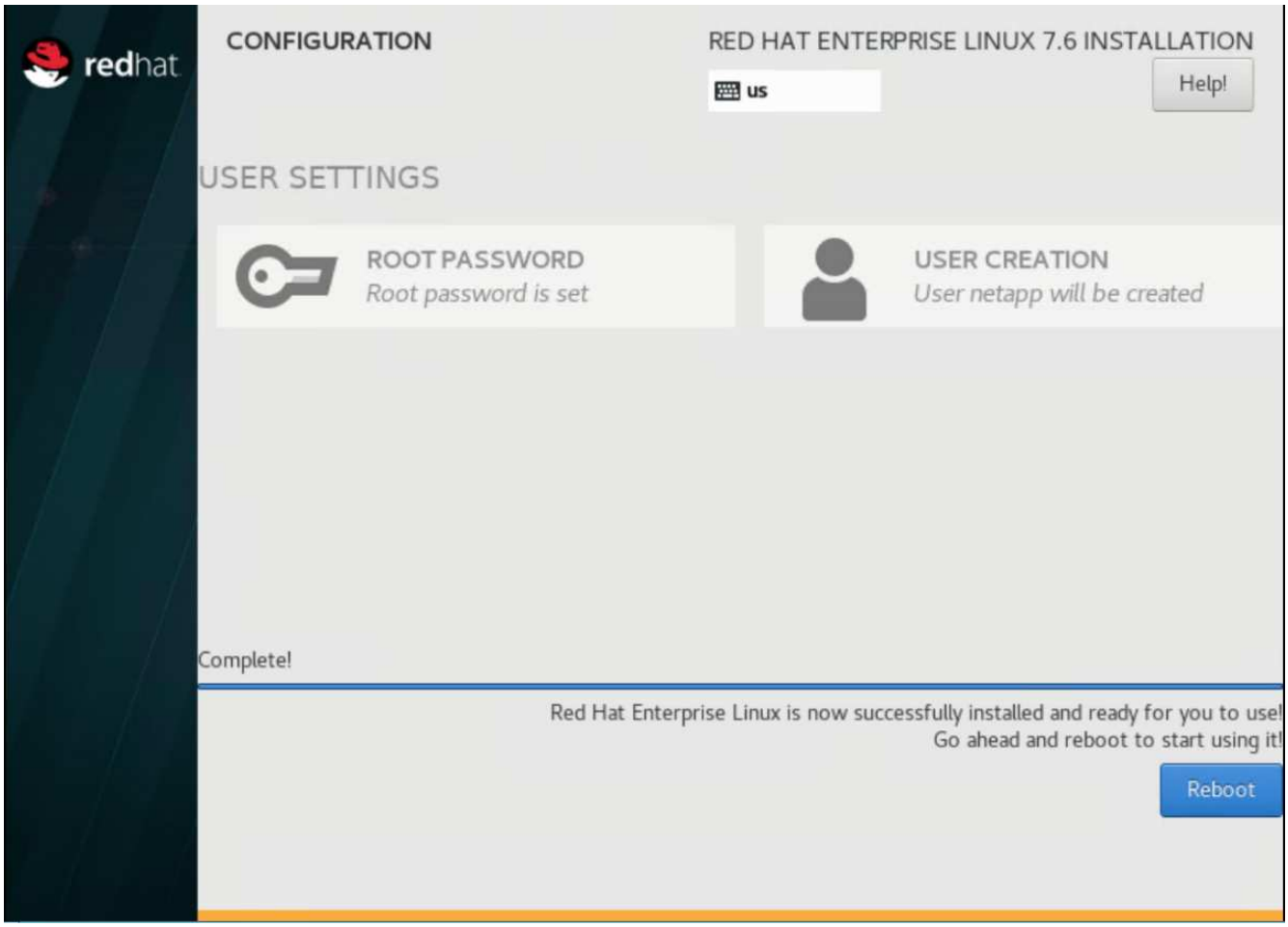
a. サーバのホスト名を入力します。

b. スライダボタンをクリックして、ネットワークアダプタの電源をオンにします。ネットワークに Dynamic Host Configuration Protocol （ DHCP ；動的ホスト構成プロトコル）が設定されている場合は、 IP アドレスが割り当てられます。表示されない場合は、 Configure （設定）をクリックし、アドレスを手動で割り当てます。



c. 。[完了] をクリックして、 [インストールの概要] に戻ります。

5. [インストールの概要] ページで、 [インストールの開始] をクリックします。
6. インストールの進行状況ページで、 root パスワードを設定するか、ローカルユーザーアカウントを作成できます。インストールが完了したら、 Reboot （再起動）をクリックしてサーバを再起動します。



7. システムが再起動したら、サーバにログインし、 Red Hat Subscription Manager に登録します。

```
[root@Netapp-AU ~]# subscription-manager register
Registering to: subscription.rhsm.redhat.com:443/subscription
Username: alan.cowles@netapp.com
Password:
The system has been registered with ID: a47f2e7b-81cd-4757-85c7-eb1818c2c2a1
The registered system name is: Netapp-AU
[root@Netapp-AU ~]#
```

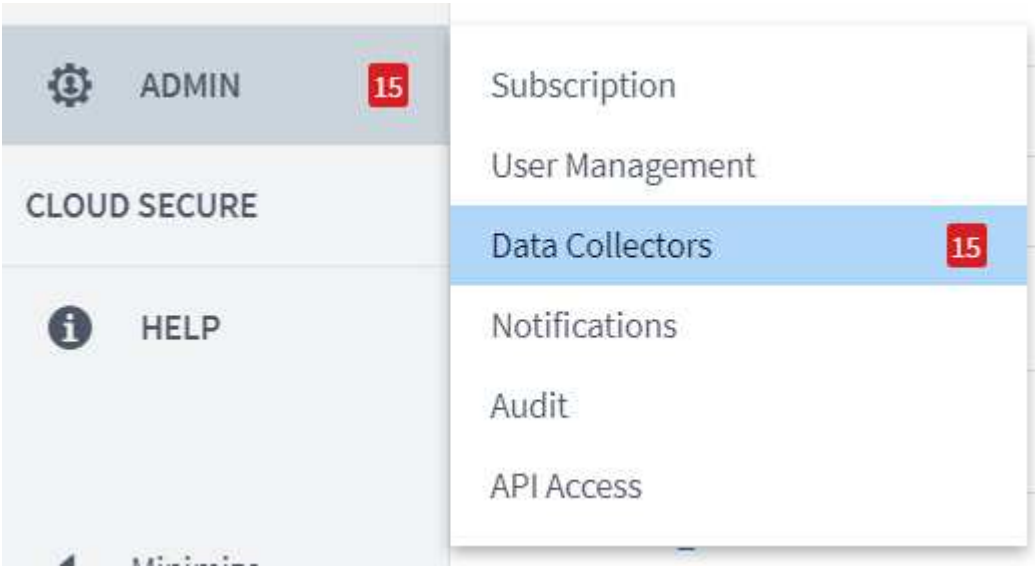
8. Red Hat Enterprise Linux のサブスクリプションを追加します。

```
[root@Netapp-AU ~]# subscription-manager attach --pool=8a85f99b710f3b1901713b90b9e154cf
Successfully attached a subscription for: Red Hat Enterprise Linux, Standard Support (128 Sockets, NFR, Partner Only)
[root@Netapp-AU ~]#
```

Cloud Insights ポータルで **Acquisition Unit** インスタンスを作成し、ソフトウェアをインストールする

Cloud Insights ポータルで Acquisition Unit インスタンスを作成してソフトウェアをインストールするには、次の手順を実行します。

1. Cloud Insights のホームページで、左側のメインメニューの Admin エントリにカーソルを合わせ、メニューから Data Collectors を選択します。

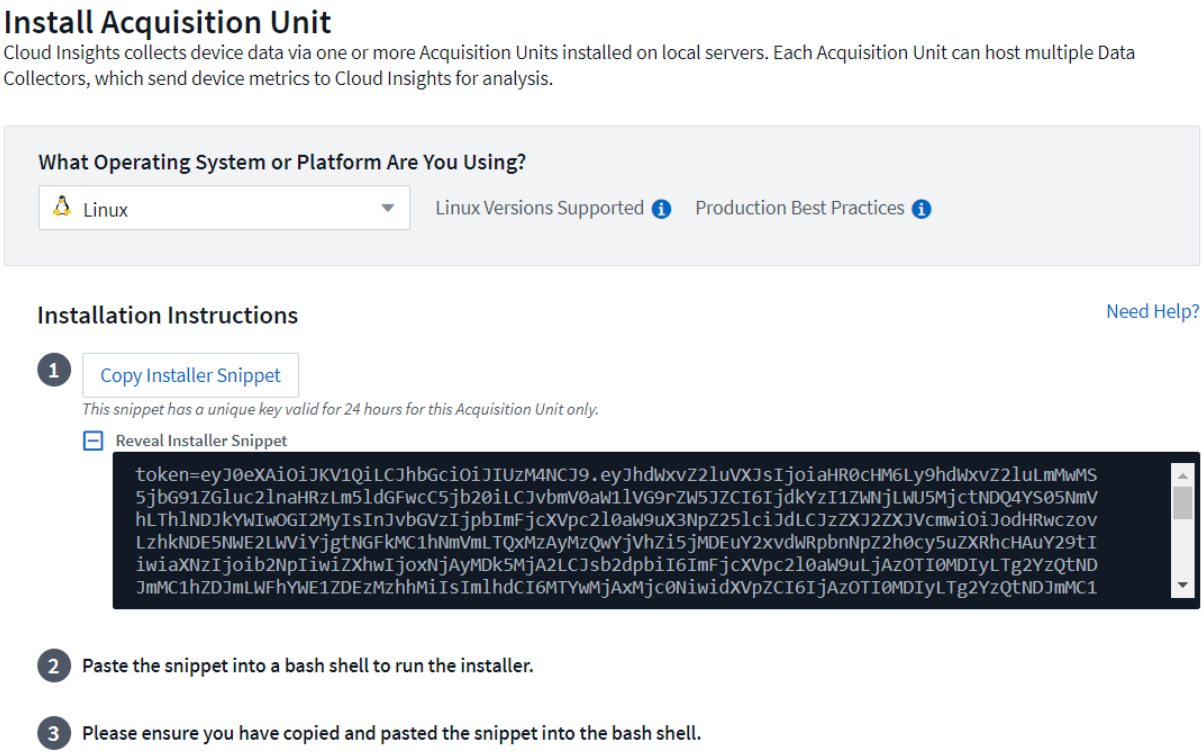


2. データコレクタページの上部中央で、 Acquisition Unit のリンクをクリックします。

3. 新しい Acquisition Unit を作成するには、右側のボタンをクリックします。

4. Acquisition Unit のホストとして使用するオペレーティングシステムを選択し、 Web ページからインストールスクリプトをコピーする手順に従います。

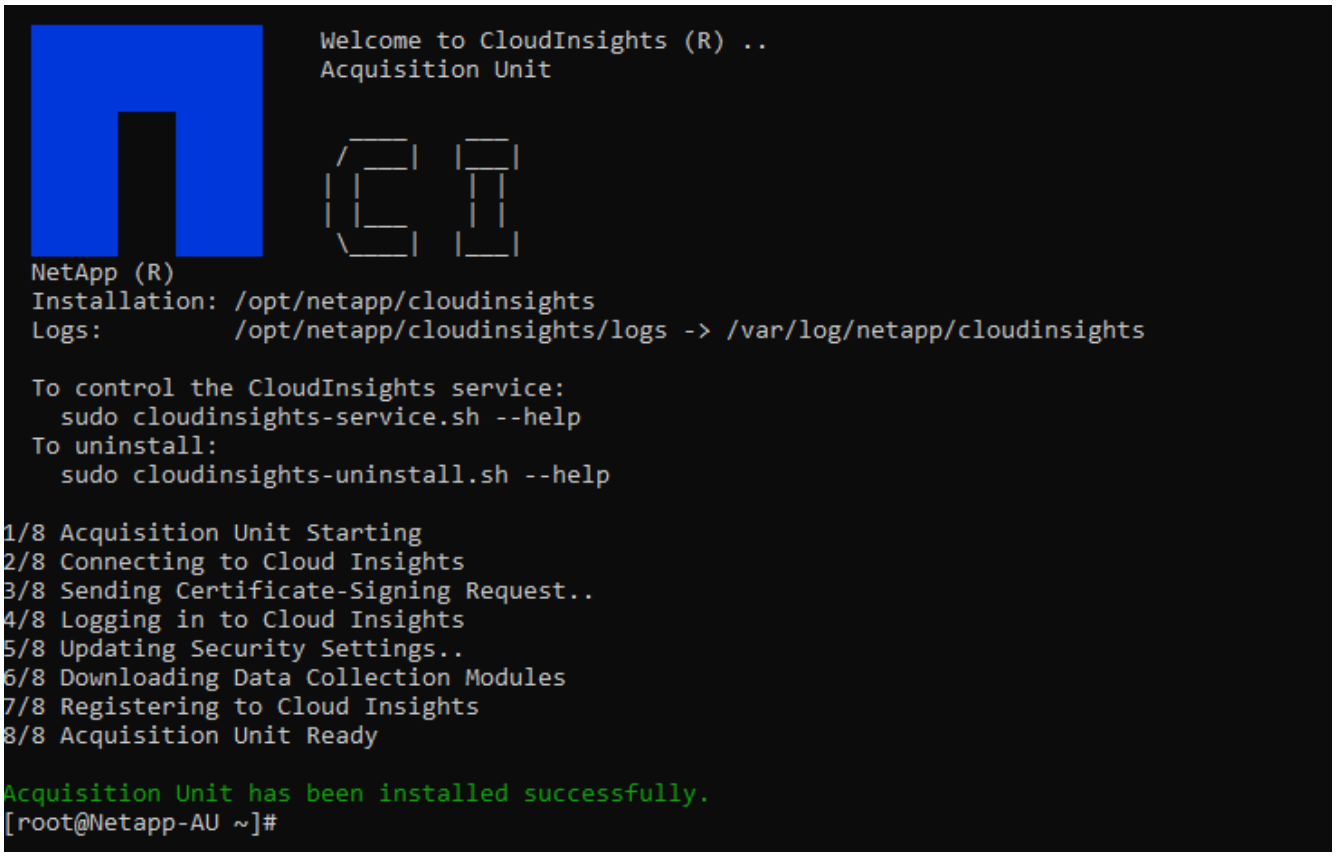
   この例では、 Linux サーバを使用しています。これは、スニペットとトークンを提供し、ホストの CLI に貼り付けます。Web ページは Acquisition Unit への接続を待機します。



5. プロビジョニングされた Red Hat Enterprise Linux マシンの CLI にスニペットを貼り付け、 Enter キーを押します。

```
[root@Netapp-AU ~]# token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzM4NCJ9.eyJhdWxvZ2luVXJsIjoiaHR0cHM6Ly9hdWxvZ2luLmMwMS5jbG91ZGluc
2lnaHRzLm5ldGFwcC5jb20iLCJvbmV0aW1lVG9rZW5JZCI6IjQ5ZTY0MGM5LTY5MTItNDQ4Yi04YmI4LTIwNGY2OTQ2YzY1YSIsInJvbGVzIjpbImFjcXVpc
2l0aW9uX3NpZ25lciJdLCJzZXJ2ZXJVcmwiOiJodHRwczovLzhkNDE5NWE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZi5jMDEuY2xvdWRpbnNpZ2h0c
y5uZXRhcHAuY29tIiwiaXNzIjoib2NpIiwiZXhwIjoxNjAyMTgyNzg2LCJsb2dpbiI6ImFjcXVpc2l0aW9uLjc4MTliZGI3LTk5OWQtNGNiYS05YmU1LTMwZ
TcxZjk0ODRiZCIsImlhdCI6MTYwMjA5NjMyNiwidXVpZCI6Ijc4MTliZGI3LTk5OWQtNGNiYS05YmU1LTMwZTcxZjk0ODRiZCIsInRlbmFudCI6IjhkNDE5N
WE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZiIsInRlbmFudFN1YmRvbWFpbiI6InBzMTMyNSJ9.RvWLR3wH1_k6fIOCiO_h-Wok2STfFPDj7VksmXqw
-GZ-JqSIe8SZE4Sv3DuWrWM6 domainUrl=https://8d4195a6-ebb8-4ad0-a6ef-41302340b5af.c01.cloudinsights.netapp.com/rest/v1/au
version=1.253.0 bootstrap=cloudinsights-au-install-bootstrap.sh && curl $proxy_auth_scheme -H "Authorization: Bearer $to
ken" -o $bootstrap $domainUrl/installerBootstrap && sudo chmod 755 $bootstrap && sudo /bin/bash -c "TOKEN=$token HTTPS_P
ROXY=$https_proxy PROXY_AUTH_SCHEME=$proxy_auth_scheme AU_VERSION=$version INSTALLER_NAME=cloudinsights-linux-au-install
er-$version INSTALLER_URL=$domainUrl/installers/linux/$version ./$bootstrap"
```

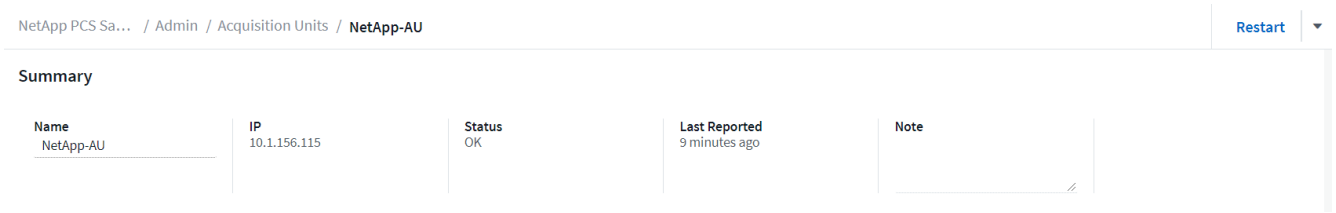
インストールプログラムは、圧縮パッケージをダウンロードしてインストールを開始します。インストールが完了すると、 Acquisition Unit が NetApp Cloud Insights に登録されたことを示すメッセージが表示されます。



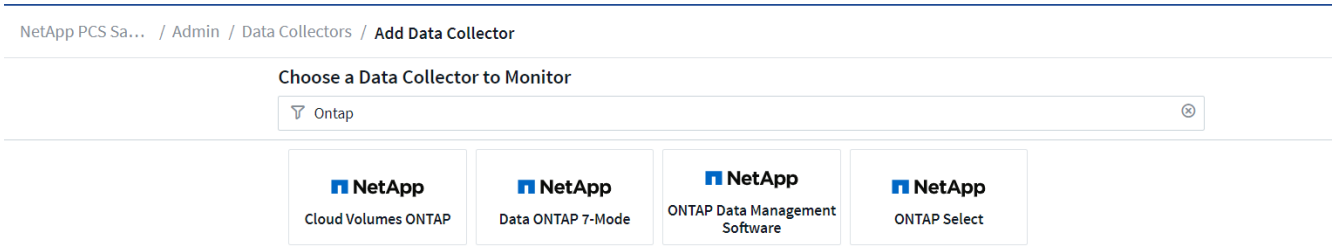
FlexPod データセンターから **Cloud Insights** に監視対象のストレージシステムを追加します

FlexPod 環境から ONTAP ストレージシステムを追加するには、次の手順を実行します。

1. Cloud Insights ポータルの Acquisition Unit ページに戻り、新たに登録されたユニットを探します。ユニットのサマリーを表示するには、ユニットをクリックします。

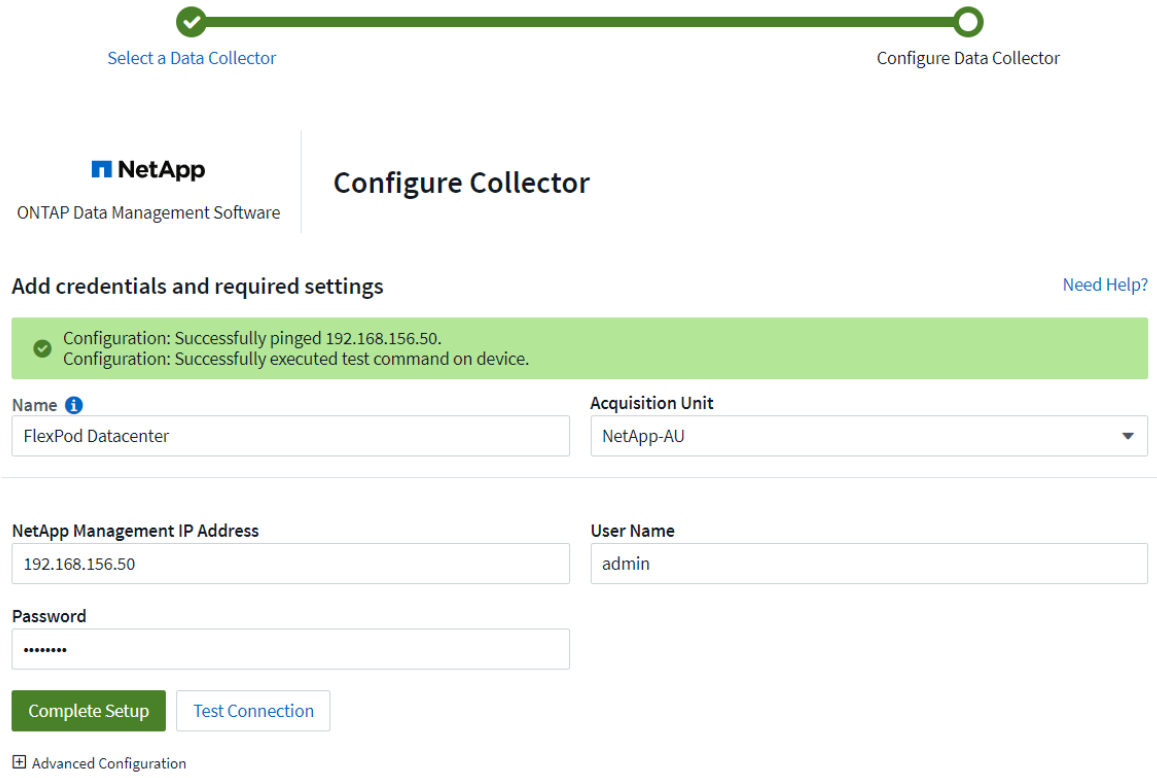


2. ストレージシステムを追加するウィザードを開始するには、概要ページでデータコレクタを作成するボタンをクリックします。最初のページには、データの収集元となるすべてのシステムが表示されます。検索バーを使用して ONTAP を検索します。



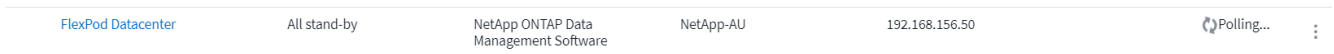
3. ONTAP データ管理ソフトウェアを選択します。

   導入環境の名前を指定し、使用する Acquisition Unit を選択するためのページが表示されます。ONTAP システムの接続情報とクレデンシャルを指定し、接続をテストして確認できます。



4. [セットアップの完了] をクリックします

   ポータルが Data Collectors ページに戻り、 Data Collector は最初のポーリングを開始して、 FlexPod データセンターの ONTAP ストレージシステムからデータを収集します。



ユースケース

FlexPod をセットアップし、解決策 Datacenter Cloud Insights を監視するように設定す

ると、ダッシュボードで実行できるいくつかのタスクを確認して、環境を評価および監視することができます。このセクションでは、 Cloud Insights の主なユースケースを 5 つ紹介します。

- Active IQ 統合
- リアルタイムダッシュボードの表示
- カスタムダッシュボードの作成
- 高度なトラブルシューティング
- ストレージの最適化

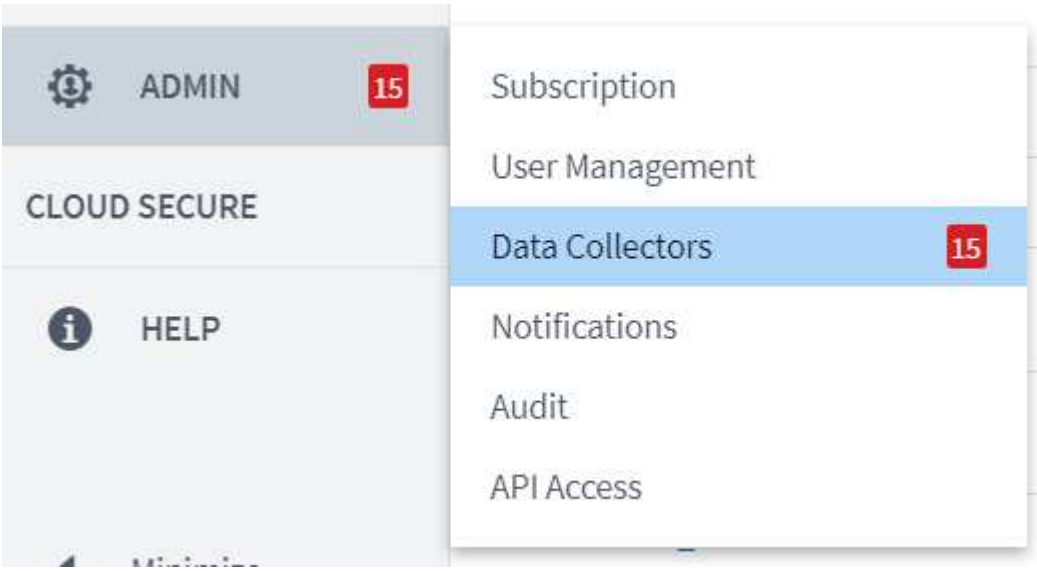
Active IQ 統合

Cloud Insights は、 Active IQ ストレージ監視プラットフォームに完全に統合されています。FlexPod Datacenter 解決策の一部として導入された ONTAP システムは、各システムに組み込まれている AutoSupport 機能を通じてネットアップに情報を送信するように、自動的に設定されます。これらのレポートは、スケジュールに基づいて生成されるか、システムで障害が検出されると動的に生成されます。AutoSupport 経由で送信されたデータは、 Cloud Insights の Active IQ メニューにある簡単にアクセスできるダッシュボードに集約されて表示されます。

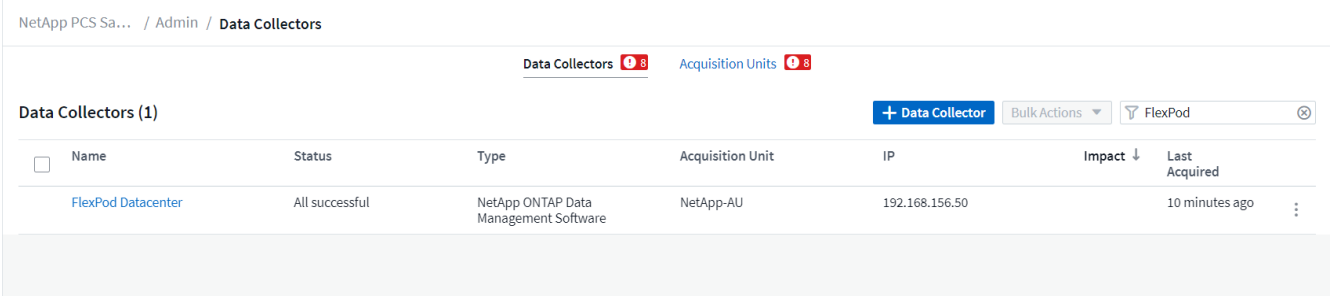
Active IQ ダッシュボードから Cloud Insights 情報にアクセスします

Cloud Insights ダッシュボードから Active IQ 情報にアクセスするには、次の手順を実行します。

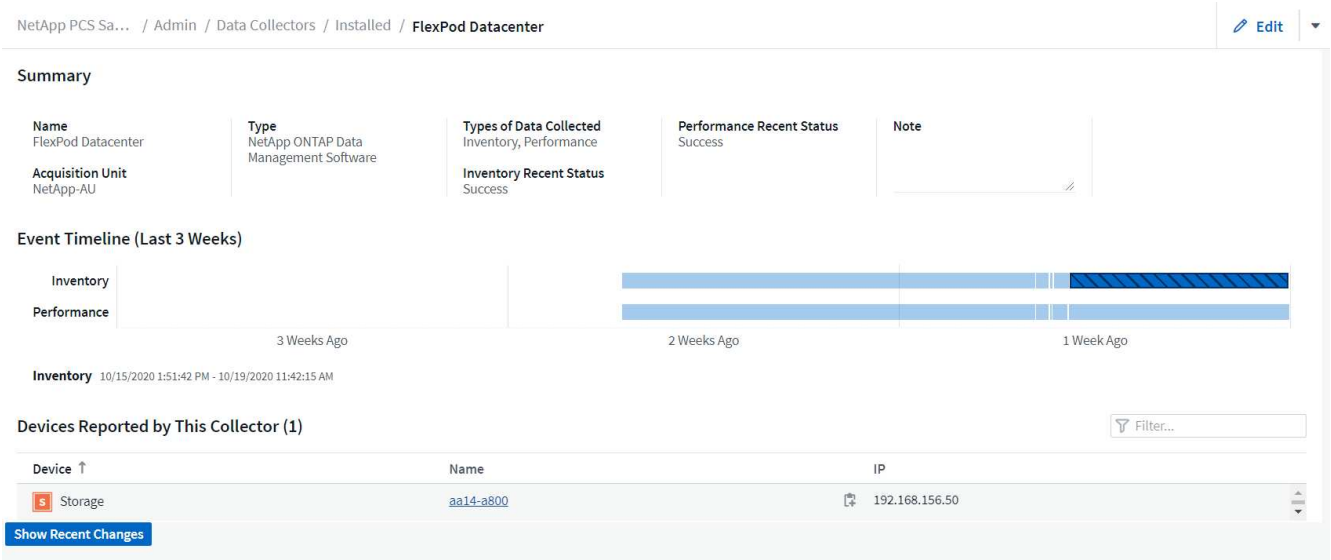
1. 左側の Admin メニューの下にある Data Collector オプションをクリックします。



2. 環境内の特定の Data Collector にフィルタを適用します。この例では、 FlexPod でフィルタリングしています。

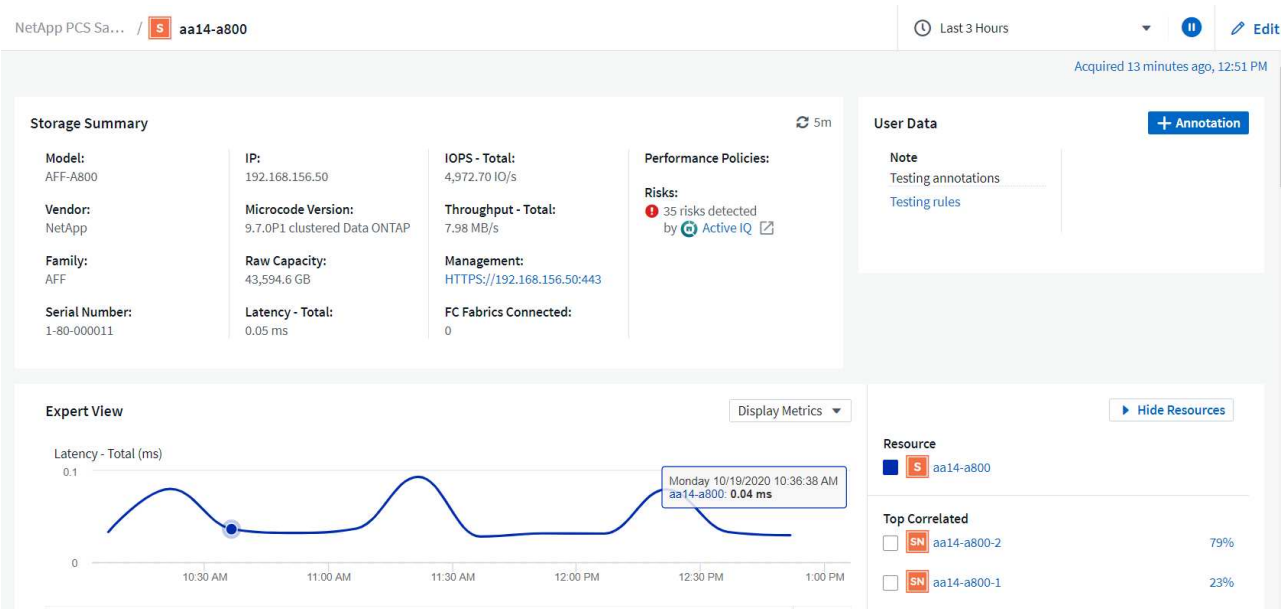


3. Data Collector をクリックして、その Collector によって監視されている環境とデバイスの概要を取得します。

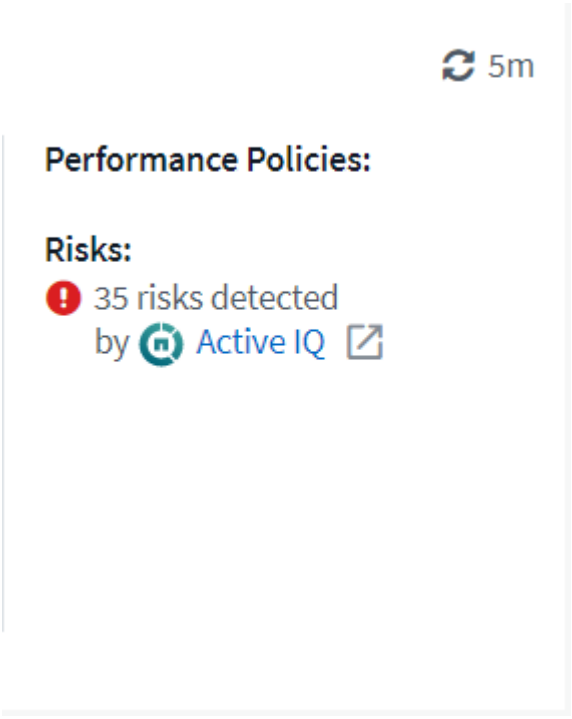


下部のデバイスリストで、監視対象の ONTAP ストレージシステムの名前をクリックします。システムに関して収集された情報を示すダッシュボードが表示されます。これには次の情報が含まれます。

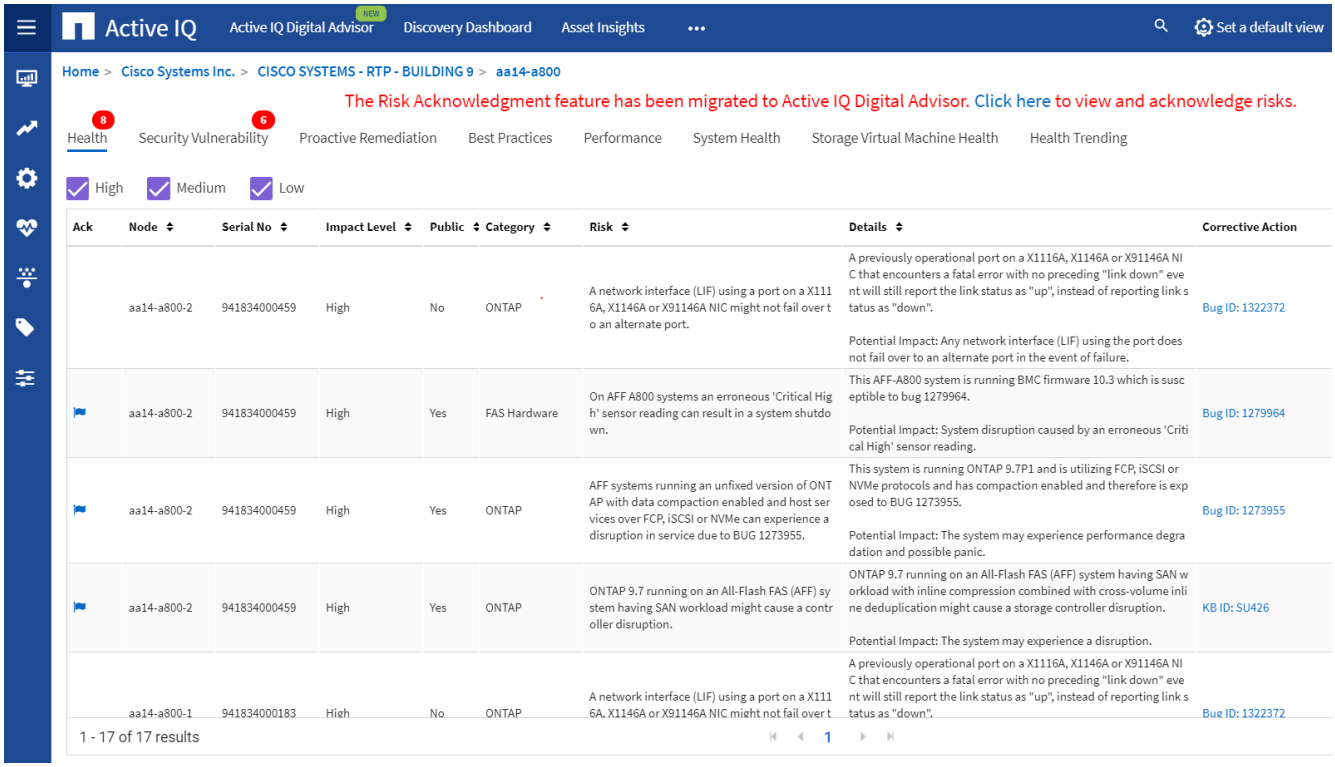
- モデル
- ファミリー
- ONTAP バージョン
- 物理容量
- 平均 IOPS
- 平均レイテンシ
- 平均スループット



また、このページのパフォーマンスポリシーのセクションで、 NetApp Active IQ へのリンクを確認できます。



4. ブラウザの新しいタブを開き、リスク軽減ページに移動します。このページには、影響を受けるノード、リスクがどの程度重要か、特定された問題を修正するために実行する必要がある適切なアクションが表示されます。 Active IQ のリンクをクリックします。

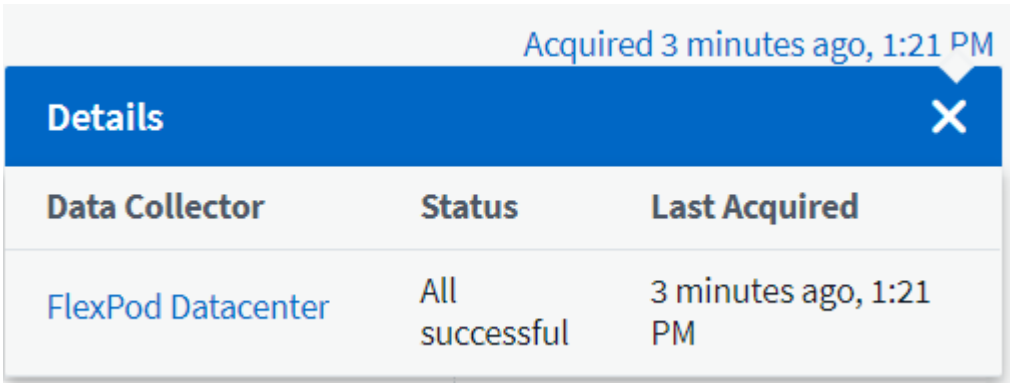


リアルタイムダッシュボードを確認する

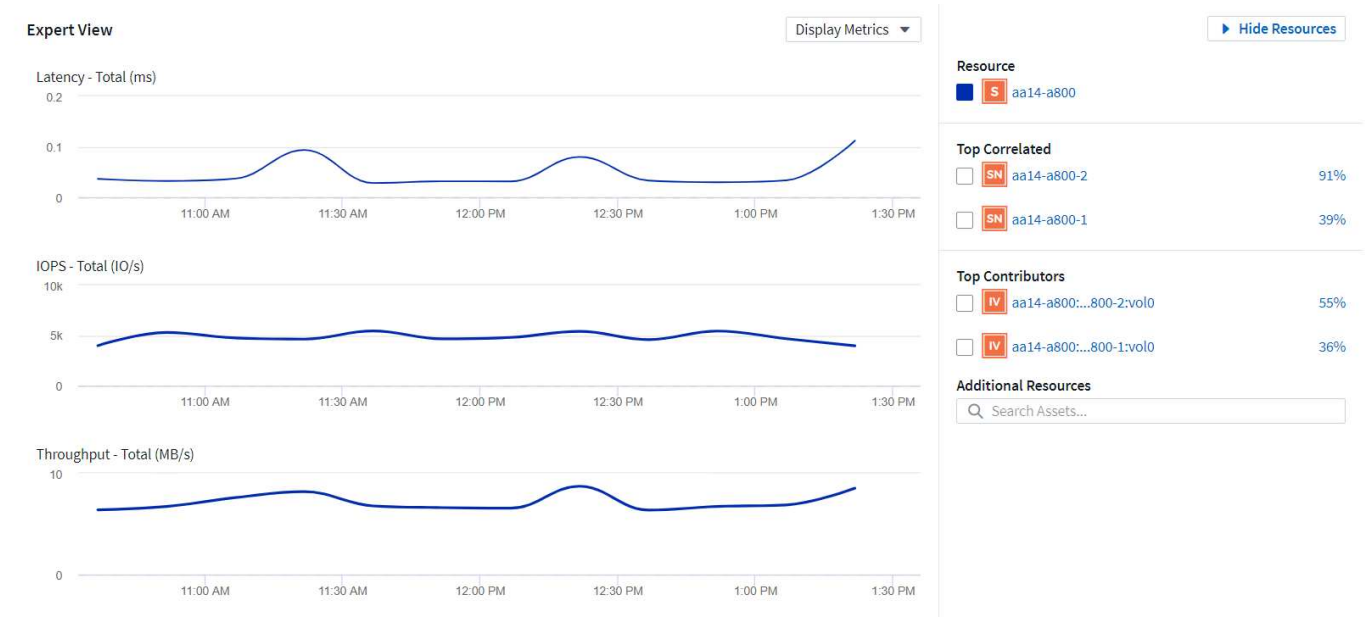
Cloud Insights では、 FlexPod データセンター解決策に導入された ONTAP ストレージシステムでポーリングされた情報のダッシュボードをリアルタイムで表示できます。Cloud Insights Acquisition Unit では、定期的にデータが収集され、デフォルトのストレージシステムダッシュボードに収集された情報が読み込まれます。

Cloud Insights ダッシュボードからリアルタイムグラフにアクセスできます

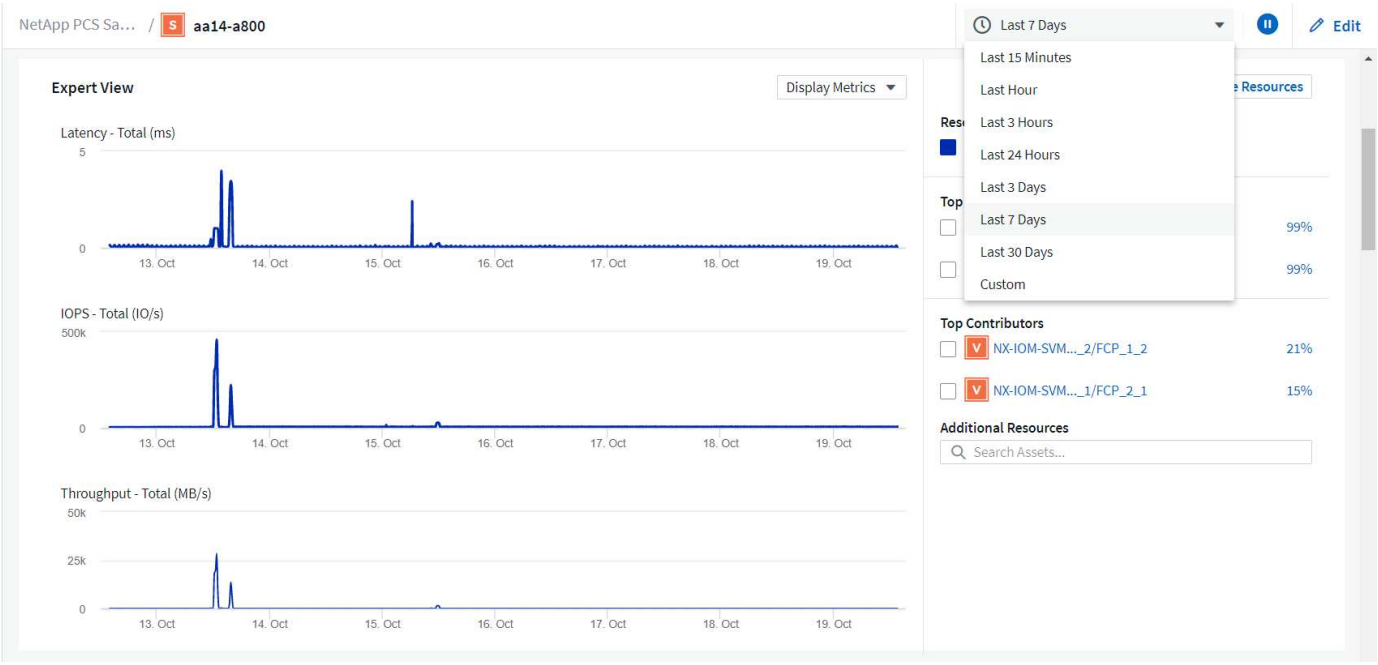
ストレージ・システムのダッシュボードから 'Data Collector が情報を最後に更新した時刻を確認できますこの例を次の図に示します。



デフォルトでは、ストレージシステムダッシュボードのエキスパートビューセクションに、ポーリング対象のストレージシステム、または個々のノードからのシステム全体の指標（レイテンシ、 IOPS 、スループットなど）を示す対話型グラフがいくつか表示されます。これらのデフォルトのグラフの例を次の図に示します。



デフォルトでは、過去 3 時間の情報がグラフに表示されますが、ストレージシステムダッシュボードの右上にあるドロップダウンリストからさまざまな値またはカスタム値に設定できます。これを次の図に示します。



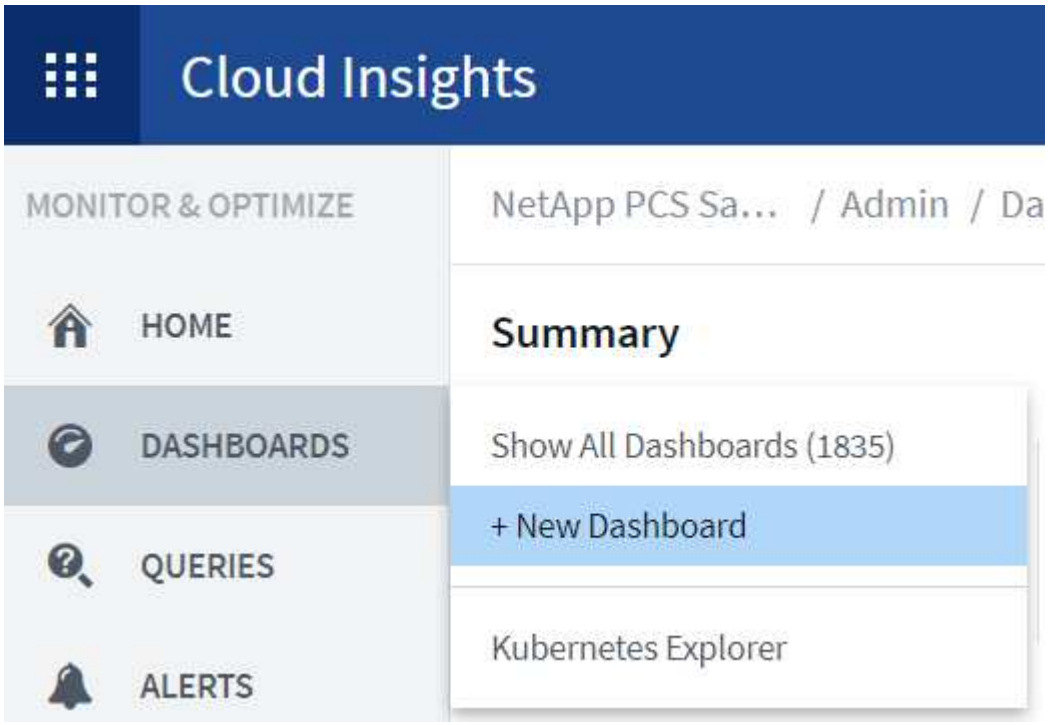
カスタムダッシュボードを作成する

システム全体の情報を表示するデフォルトのダッシュボードを利用する以外に、 Cloud Insights を使用して完全にカスタマイズされたダッシュボードを作成し、 FlexPod Datacenter 解決策の特定のストレージボリュームを対象としたリソースの使用に専念できるようにすることができます。 また、コンバージドインフラに導入されているアプリケーションは、それらのボリュームに依存して効果的に実行されます。これにより、特定のアプリケーションと、データセンター環境で消費されるリソースを視覚的に確認することができます。

カスタマイズしたダッシュボードを作成して、ストレージリソースを評価できます

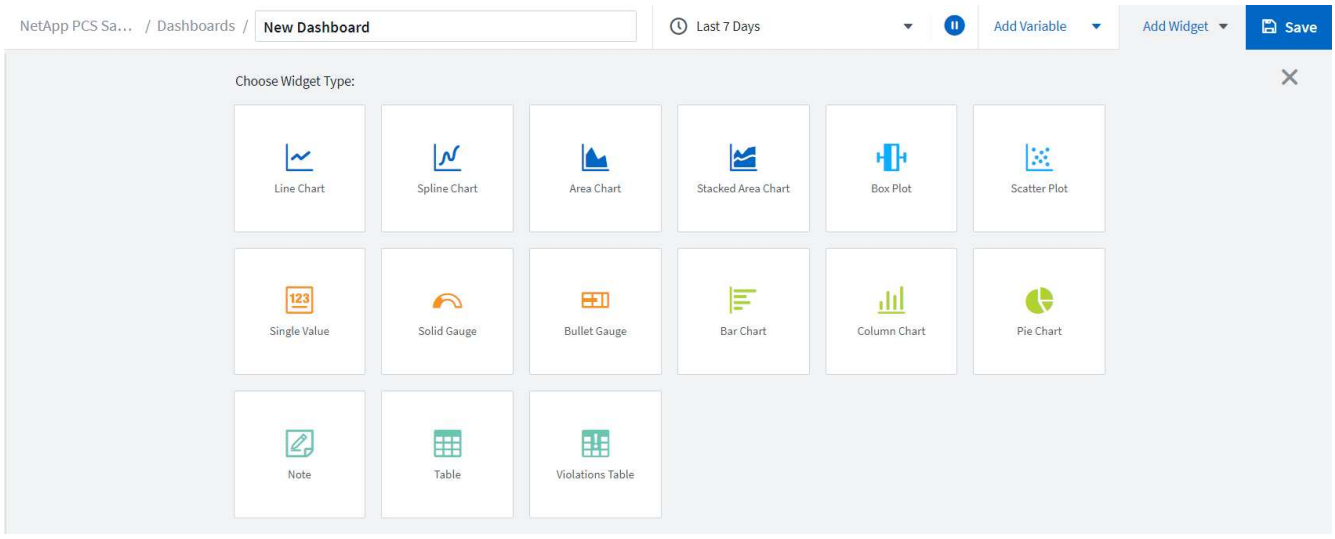
ストレージリソースを評価するためにカスタマイズしたダッシュボードを作成するには、次の手順を実行します。

1. カスタマイズされたダッシュボードを作成するには、 Cloud Insights のメインメニューの [Dashboards] にカーソルを合わせ、ドロップダウンリストで [+] [New Dashboard] をクリックします。



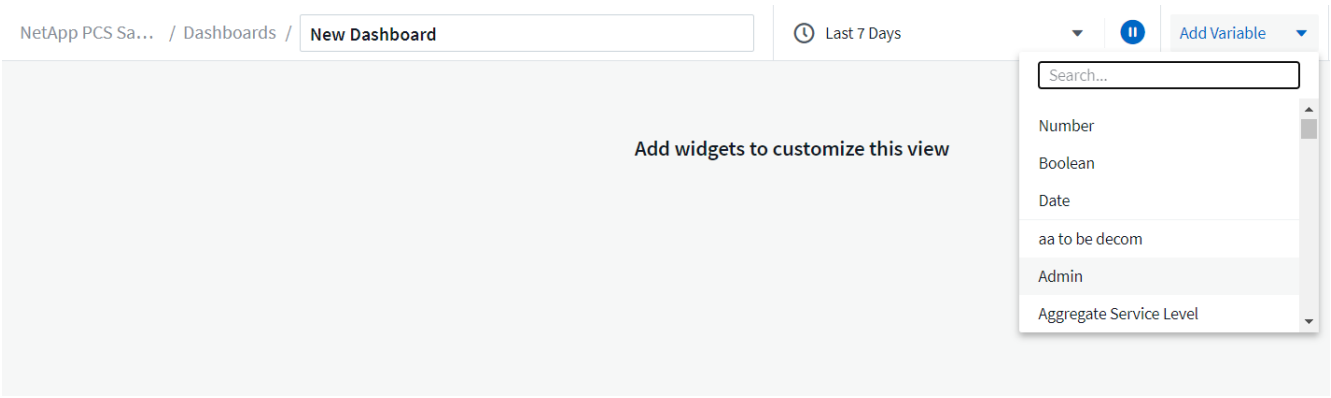
[新しいダッシュボード] ウィンドウが開きます。

2. ダッシュボードに名前を付け、データの表示に使用するウィジェットのタイプを選択します。収集したデータを表示するグラフの種類を選択することも、メモやテーブルの種類を選択することもできます。



3. [変数の追加] メニューから [カスタマイズされた変数] を選択します。

これにより、提示されるデータに集中して、より具体的な、または特殊な要因を表示できます。



4. カスタムダッシュボードを作成するには、使用するウィジェットタイプを選択します。たとえば、円グラフでボリューム別のストレージ利用率を表示します。

   a. [ウィジェットの追加] ドロップダウンリストから [円グラフ] ウィジェットを選択します。

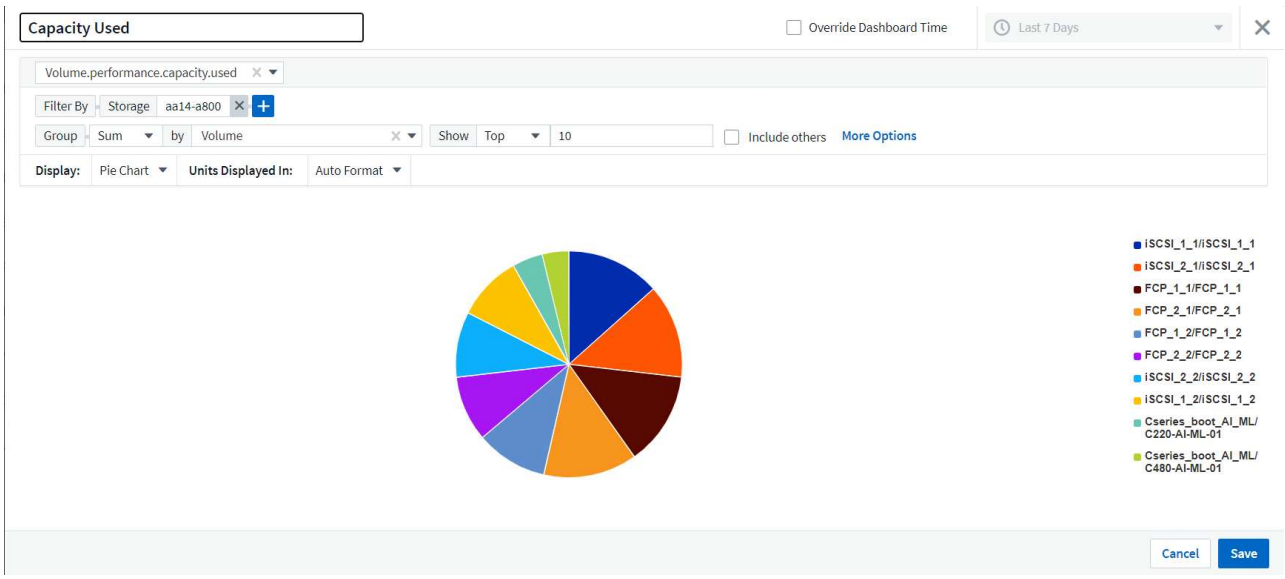
   b. ウィジェットに「 Capacity Used 」などのわかりやすい識別子を付けます。

   c. 表示するオブジェクトを選択します。たとえば、キーワード volume で検索し、「 volume.performance.capacity.used` 」を選択できます。

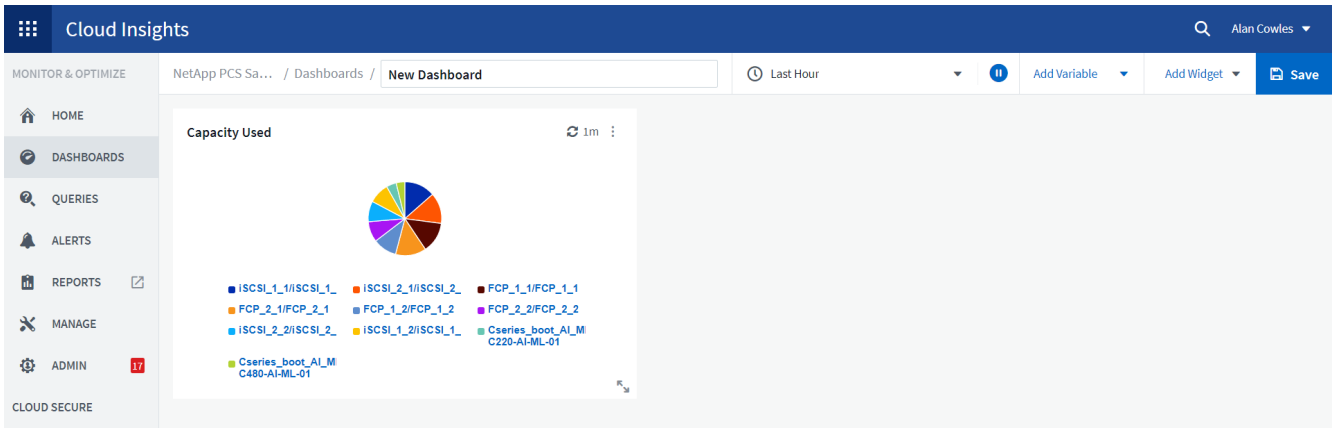
   d. ストレージシステムでフィルタリングするには、 FlexPod Datacenter 解決策で、フィルタを使用してストレージシステムの名前を入力します。

   e. 表示する情報をカスタマイズします。デフォルトでは、 ONTAP データボリュームが表示され、上位 10 個のが表示されます。

   f. カスタマイズしたダッシュボードを保存するには、 [保存] をクリックします。



   カスタムウィジェットを保存すると、ブラウザは新しいダッシュボードページに戻ります。このページには、新しく作成したウィジェットが表示され、データポーリング期間の変更などの対話型アクションを実行できます。



高度なトラブルシューティング

Cloud Insights を使用すると、 FlexPod データセンターコンバージドインフラのどのストレージ環境にも高度なトラブルシューティング方法を適用できます。前述した各機能のコンポーネントを使用： Active IQ 統合、リアルタイム統計を表示するデフォルトダッシュボード、カスタマイズされたダッシュボードなど、発生する可能性のある問題は早期に検出されて迅速に解決されます。Active IQ のリスクリストを使用すると、問題につながる可能性のある報告済みの構成エラーを発見したり、報告済みのコードバージョンやパッチが適用されたコードのバージョンを発見したりできます。Cloud Insights ホームページ上のリアルタイムダッシュボードを観察することで、システムパフォーマンスのパターンを発見し、問題の早期発見や早期解決に役立てることができます。最後に、カスタマイズしたダッシュボードを作成することで、お客様はインフラ内の最も重要な資産に集中し、それらを直接監視して、ビジネス継続性の目標を達成できるようになります。

ストレージの最適化

トラブルシューティングに加えて、 Cloud Insights で収集されたデータを使用することで、 FlexPod データセンターコンバージドインフラ解決策に導入されている ONTAP ストレージシステムを最適化することができます。高レイテンシが発生しているボリュームについては、たとえば、高パフォーマンスが求められる複数の VM が同じデータストアを共有している場合など、 Cloud Insights ダッシュボードにその情報が表示されます。ストレージ管理者は、この情報を使用して、 1 つ以上の VM を別のボリュームに移行したり、アグリゲート間や ONTAP ストレージシステムのノード間で移行したりできます。その結果、パフォーマンスが最適化された環境になります。Cloud Insights と Active IQ の統合から収集された情報は、想定よりもパフォーマンスが低下する構成の問題を明らかにし、問題を解決して最適に調整されたストレージシステムを確保するための推奨される対処方法を提供します。

ビデオとデモ

ビデオでは、 NetApp Cloud Insights を使用してオンプレミス環境内のリソースを評価する方法を紹介しています "こちらをご覧ください"。

NetApp Cloud Insights を使用してインフラを監視し、インフラのアラートしきい値を設定する方法を紹介するビデオをご覧ください "こちらをご覧ください"。

環境内の個々のアプリケーションの評価には、 NetApp Cloud Insights の使用方法を示すビデオが視聴できます "こちらをご覧ください"。

追加情報

このドキュメントに記載されている情報の詳細については、次の Web サイトを参照して

ください。

- シスコ製品マニュアル

  "https://www.cisco.com/c/en/us/support/index.html"

- FlexPod データセンター

  "https://www.flexpod.com"

- NetApp Cloud Insights の略

  "https://cloud.netapp.com/cloud-insights"

- ネットアップの製品マニュアル

  "https://docs.netapp.com"

FabricPool with FlexPod - Amazon AWS S3 への非アクティブなデータ階層化

TR-4801 ：『 FlexPod with FabricPool - Inactive Data Tiering to Amazon AWS S3 』

ネットアップ、 Scott Kovacs 氏

フラッシュストレージの価格は下落し続けているため、これまでフラッシュストレージの候補とみなされていなかったワークロードやアプリケーションで利用できます。しかし、 IT 管理者にとっては、ストレージへの投資を最も効率的に活用することが非常に重要です。IT 部門は、予算をほとんど増やすことなく、パフォーマンスの高いサービスを提供し続ける必要があります。このようなニーズに対応するために、 NetApp FabricPool では、使用頻度の低いデータをオンプレミスの高価なフラッシュストレージからパブリッククラウドの対費用効果の高いストレージ階層に移動することで、クラウドの経済性を活用できます。アクセス頻度の低いデータをクラウドに移動することで、AFF システムや FAS システム上の貴重なフラッシュストレージスペースが解放され、ビジネスクリティカルなワークロードに対応できる容量がハイパフォーマンスのフラッシュ階層に追加されます。

このテクニカルレポートでは、ネットアップと Cisco が提供する FlexPod コンバージドインフラアーキテクチャに関連して、 ONTAP FabricPool のデータ階層化機能について説明します。このテクニカルレポートで説明する概念を最大限に活用するには、 FlexPod データセンター統合インフラアーキテクチャと ONTAP ストレージソフトウェアについて理解しておく必要があります。FlexPod と ONTAP に精通していることを前提に、 FabricPool とその仕組み、オンプレミスのフラッシュストレージをより効率的に使用するための の使用方法について説明します。このレポートの内容の大部分については、で詳しく説明します "TR-4598 ：『 FabricPool Best Practices 』" およびその他の ONTAP 製品ドキュメントを参照してください。このコンテンツは FlexPod インフラのために集約されており、 FabricPool のすべてのユースケースを網羅しているわけではありません。ONTAP 9.6 では、すべての機能と概念が使用可能です。

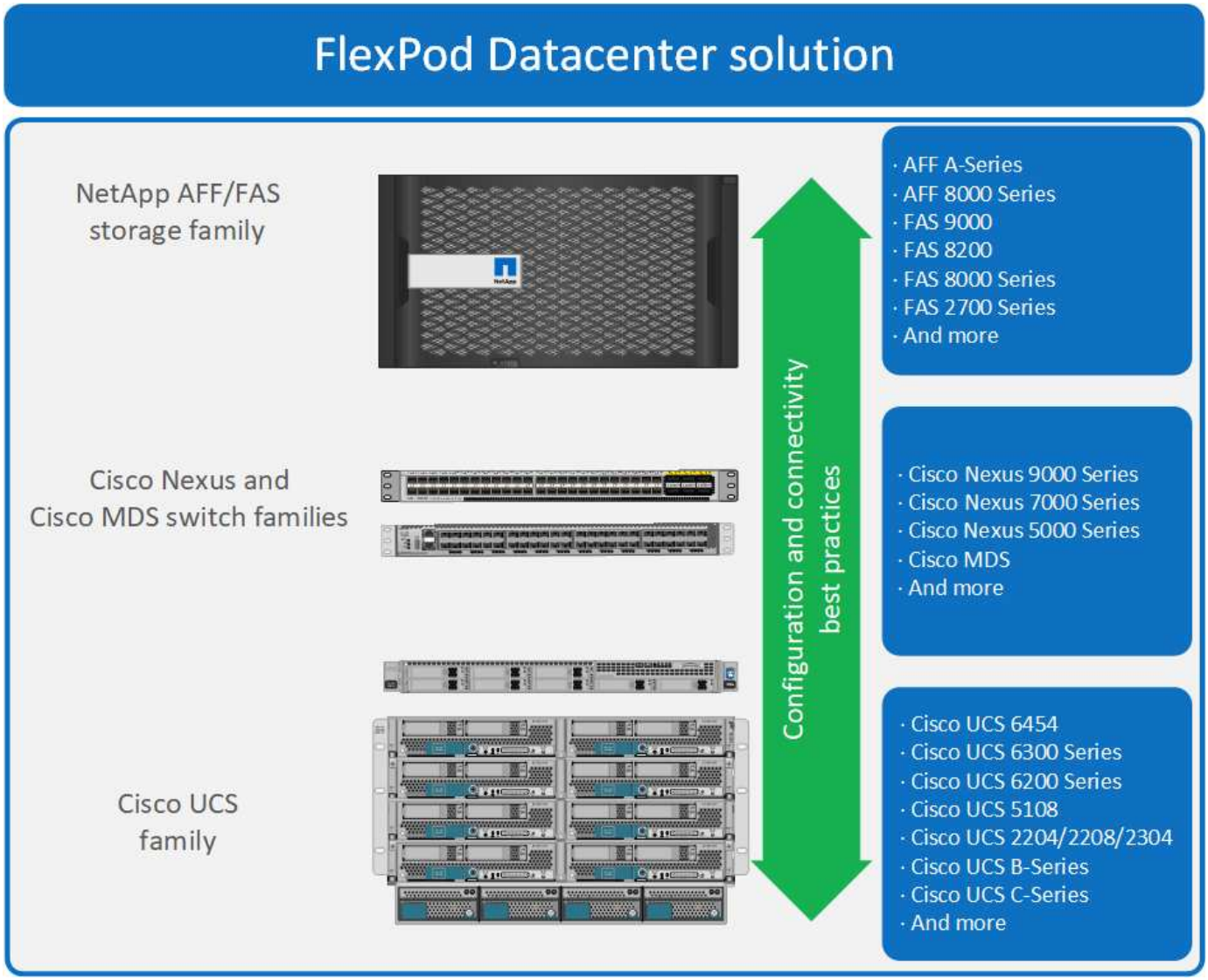
追加情報 About FlexPod をに示します "TR-4036 『 FlexPod データセンター技術仕様』"。

FlexPod の概要とアーキテクチャ

FlexPod の概要

FlexPod は、仮想化ソリューションと非仮想化ソリューションの両方の統合基盤となるハードウェアとソフトウェアの定義済みセットです。FlexPod には、 NetApp AFF ストレージ、 Cisco Nexus ネットワーク、 Cisco MDS ストレージネットワーク、 Cisco Unified Computing System （ Cisco UCS ）、 VMware vSphere ソフトウェアが 1 つのパッケージに含まれています。この設計は柔軟性に優れており、ネットワーク、コンピューティング、ストレージを 1 つのデータセンターラックに収容することも、お客様のデータセンター設計に従って導入することもできます。ポート密度を使用すると、ネットワークコンポーネントは複数の構成に対応できます。

FlexPod アーキテクチャのメリットの 1 つは、お客様の要件に合わせて環境をカスタマイズしたり柔軟に設定したりできることです。FlexPod ユニットは、要件や需要の変化に応じて簡単に拡張できます。ユニットは、スケールアップ（ FlexPod ユニットにリソースを追加）とスケールアウト（ FlexPod ユニットを追加）の両方に対応しています。FlexPod リファレンスアーキテクチャでは、ファイバチャネルおよび IP ベースのストレージ解決策の耐障害性、コスト上のメリット、および導入の容易さを強調しています。単一のインターフェイスから複数のプロトコルに対応できるストレージシステムなら、選択肢が広がり、投資が無駄にならずに保護されます。これは、まさに Wire-Once アーキテクチャだからです。次の図に、 FlexPod の多くのハードウェアコンポーネントを示します。

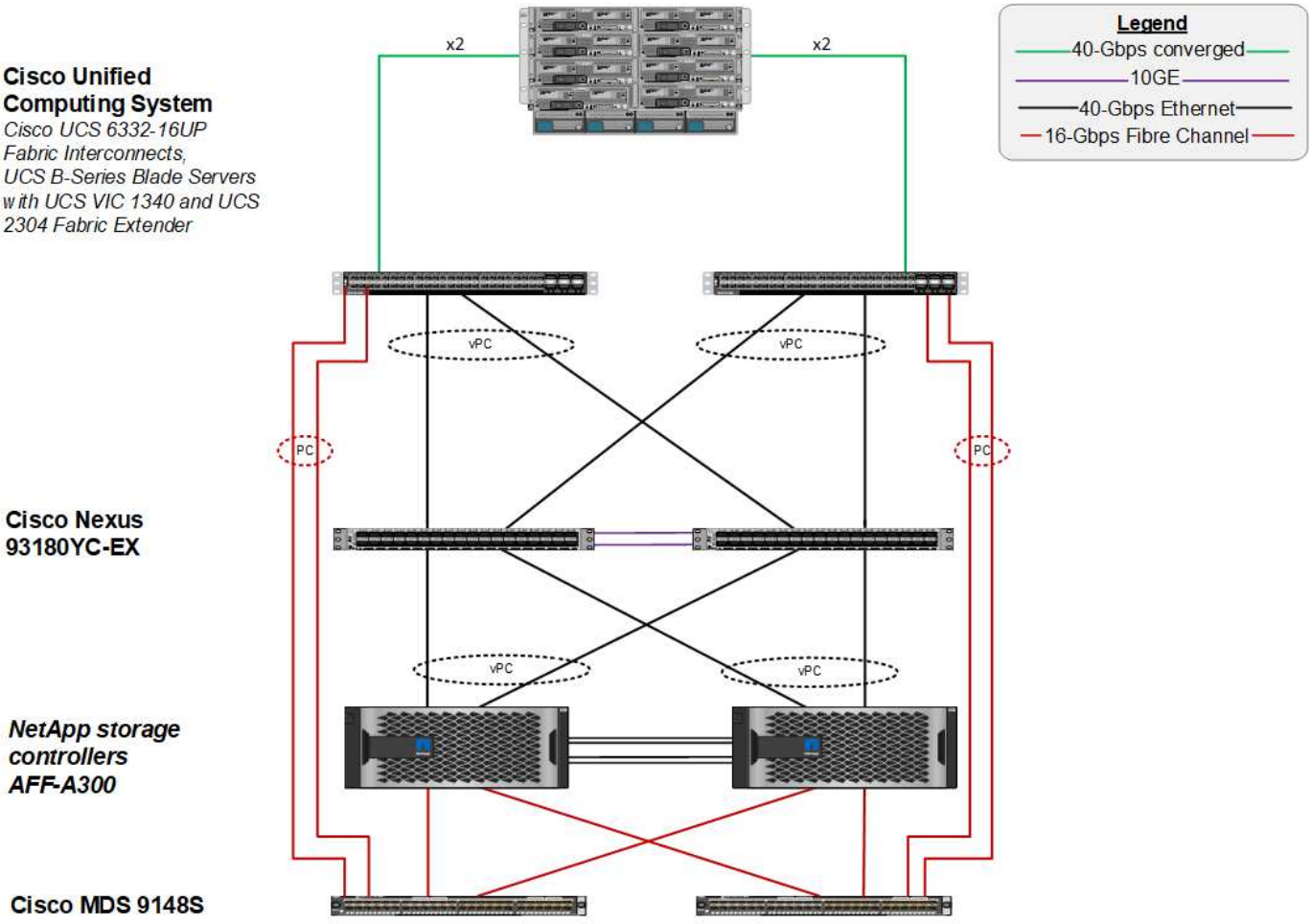


FlexPod アーキテクチャ

次の図に、 VMware vSphere と FlexPod 解決策のコンポーネントと、 Cisco UCS 6454 ファブリックインターコネクトに必要なネットワーク接続を示します。この設計には、次のコンポーネントがあります。

- Cisco UCS 5108 ブレードシャーシと Cisco UCS ファブリックインターコネクト間のポートチャネル 40GB イーサネット接続
- Cisco UCS ファブリックインターコネクトと Cisco Nexus 9000 間の 40GB イーサネット接続
- Cisco Nesxus 9000 と NetApp AFF A300 ストレージアレイ間に 40GB イーサネット接続

これらのインフラオプションは、 Cisco UCS ファブリックインターコネクトと NetApp AFF A300 の間に Cisco MDS スイッチが配置されたことで拡張されました。この構成では、 16Gb FC ブートホストに、共有ストレージへのブロックレベルのアクセスを提供します。これは、アーキテクチャにストレージを追加する場合に、ホストから Cisco UCS ファブリックインターコネクトへのケーブルの再接続が不要になるため、リファレンスアーキテクチャによって wire-once 戦略が強化されることを意味します。



FabricPool

FabricPool の概要

FabricPool は、オールフラッシュ（ SSD ）アグリゲートをパフォーマンス階層として使用し、オブジェクトストアをパブリッククラウドサービスにクラウド階層として使用する、 ONTAP のハイブリッドストレージ解決策です。この構成では、アクセス頻度に応じてポリシーベースのデータ移動が可能です。FabricPool は、

FAS プラットフォームの AFF アグリゲートとオール SSD アグリゲートの両方で ONTAP でサポートされています。データ処理はブロックレベルで実行され、アクセス頻度が高いデータブロックがオールフラッシュのパフォーマンス階層にあり、コールドとしてタグ付けされ、アクセス頻度が低いブロックとホットタグ付けされます。

FabricPool を使用すると、パフォーマンス、効率、セキュリティ、保護を犠牲にすることなくストレージコストを削減できます。FabricPool は、エンタープライズアプリケーションに対して透過的であり、アプリケーションインフラを再設計することなくストレージの TCO を削減することで、クラウドの効率性を活用します。

FlexPod は、 FabricPool のストレージ階層化機能を活用して、 ONTAP フラッシュストレージをより効率的に使用できます。NetApp SnapCenter for vSphere からアクセス頻度の低い仮想マシン（ VM ）、使用頻度の低い VM テンプレート、および VM のバックアップを取得すると、データストアボリュームのスペースを貴重に使用することができます。コールドデータをクラウド階層に移動することで、 FlexPod インフラにホストされているミッションクリティカルなハイパフォーマンスアプリケーションのスペースとリソースを解放できます。

> 一般に、 Fibre Channel および iSCSI プロトコルは、タイムアウト（ 60 ～ 120 秒）が発生するまでに時間がかかりますが、 NAS プロトコルと同じ方法で接続の確立を再試行することはありません。SAN プロトコルがタイムアウトした場合は、アプリケーションを再起動する必要があります。パブリッククラウドへの接続を保証する方法がないため、 SAN プロトコルを使用した本番アプリケーションの停止は、短時間であっても非常に深刻な事態になる可能性があります。この問題を回避するには、 SAN プロトコルがアクセスするデータを階層化するときにプライベートクラウドを使用することを推奨します。

ONTAP 9.6 で FabricPool は、 Alibaba Cloud Object Storage Service 、 Amazon AWS S3 、 Google Cloud Storage 、 IBM Cloud Object Storage 、 Microsoft Azure Blob Storage など、主要なすべてのパブリッククラウドプロバイダと統合されます。本レポートでは、選択するクラウドオブジェクト階層として Amazon AWS S3 ストレージを中心に説明します。

複合アグリゲート

ONTAP インスタンスを作成するには、 FabricPool フラッシュアグリゲートを AWS S3 バケットなどのクラウドオブジェクトストアに関連付けて複合アグリゲートを作成します。ボリュームを複数のアグリゲート内に作成すると、 FabricPool の階層化機能を利用できます。データがボリュームに書き込まれると、 ONTAP は各データブロックに温度を割り当てます。最初に書き込まれたブロックには、ホットの温度が割り当てられます。時間が経過すると、データにアクセスできない場合は、最後にコールドステータスが割り当てられるまでクーリングプロセスが実行されます。アクセス頻度の低いデータブロックは、パフォーマンス SSD アグリゲートからクラウドオブジェクトストアに階層化されます。

ブロックがコールドとして指定され、クラウドオブジェクトストレージに移動されるまでの期間は、 ONTAP のボリューム階層化ポリシーによって変更されます。さらにきめ細かい設定は、ブロックがコールドになるまでに必要な日数を制御する ONTAP 設定を変更することで実現します。データ階層化の対象となるのは、従来のボリューム Snapshot 、 vSphere VM バックアップ用の SnapCenter 、およびその他の NetApp Snapshot ベースのバックアップです。また、 VM テンプレートやアクセス頻度の低い VM データなど、 vSphere データストア内の使用頻度の低いブロックも対象となります。

Inactive Data Reporting の実行

ONTAP では、アグリゲートから階層化できるコールドデータの量を評価するのに役立つ Inactive Data Reporting （ IDR ）を利用できます。ONTAP 9.6 では、 IDR がデフォルトで有効になっており、 31 日間のデフォルトのクーリングポリシーを使用してアクセス頻度の低いデータが特定されます。

階層化されるコールドデータの量は、ボリュームに設定されている階層化ポリシーによって異なります。この量は、デフォルトの 31 日間のクーリング期間を使用して、 IDR によって検出されたコールドデータの量とは異なる場合があります。

オブジェクトの作成とデータの移動

FabricPool は、 NetApp WAFL のブロックレベルで動作し、ブロックを冷却し、ストレージオブジェクトに連結し、それらのオブジェクトをクラウド階層に移行します。各 FabricPool オブジェクトは 4MB で、 1 、 024 個の 4KB ブロックで構成されています。オブジェクトサイズは、主要なクラウドプロバイダからの推奨パフォーマンスに基づいて、 4MB に固定されており、変更できません。コールドブロックが読み取られてホットにされると、 4MB オブジェクト内の要求されたブロックのみが取得され、パフォーマンス階層に戻されます。オブジェクト全体もファイル全体も移行されません。必要なブロックのみが移行されます。

ONTAP は、シーケンシャルな先読みの機会を検出すると、パフォーマンスを向上させるために、読み取り前にブロックをクラウド階層に要求します。

デフォルトでは、パフォーマンスアグリゲートの使用率が 50% を超えている場合にのみ、データがクラウド階層に移動されます。このしきい値を低い割合に設定すると、パフォーマンスフラッシュ階層のデータストレージの量を少なくしてクラウドに移動できます。これは、アグリゲートの容量が上限に近づいている場合にのみコールドデータを移動する階層化戦略がある場合に役立ちます。

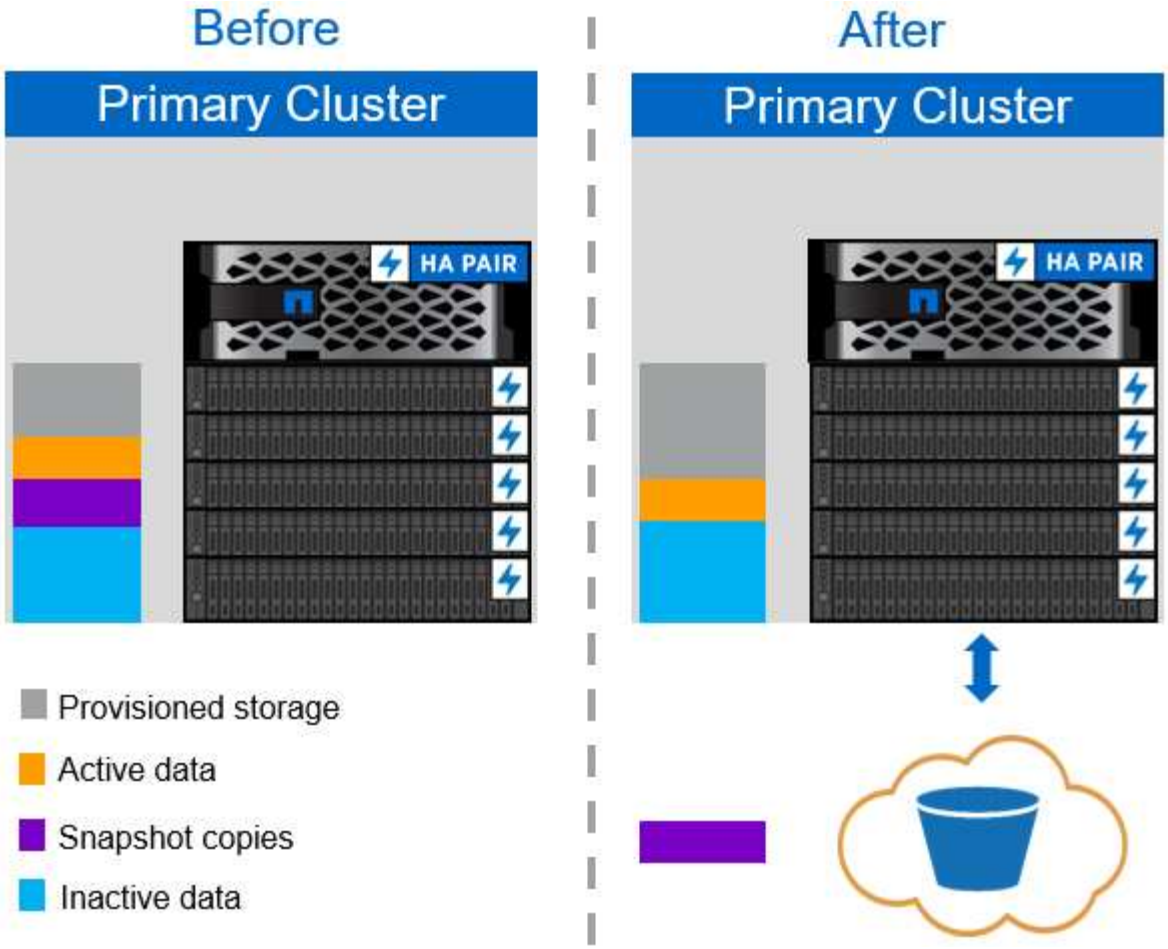
パフォーマンス階層の使用率が 70% を超える場合、コールドデータはパフォーマンス階層に書き戻されることなく、クラウド階層から直接読み取られます。FabricPool では、使用頻度の高いアグリゲートでのコールドデータの書き戻しを防止することで、アクティブデータのアグリゲートが保持されます。

パフォーマンス階層のスペースを再生します

前述したように、 FabricPool の主なユースケースは、ハイパフォーマンスのオンプレミスフラッシュストレージを最も効率的に使用できるようにすることです。FlexPod 仮想インフラのボリューム Snapshot および VM バックアップという形で作成されたコールドデータは、高価なフラッシュストレージを大量に消費している可能性があります。Snapshot のみまたは自動の 2 つの階層化ポリシーのいずれかを実装すると、重要なパフォーマンス階層のストレージを解放できます。

snapshot-only 階層化ポリシー

次の図に示す「 Snapshot のみ」の階層化ポリシーは、ボリュームのコールドスナップショットデータと、スペースを占有しているがアクティブなファイルシステムとブロックを共有していない VM の SnapCenter for vSphere バックアップをクラウドオブジェクトストアに移動します。「 Snapshot のみ」の階層化ポリシーは、コールドデータブロックをクラウド階層に移動します。リストアが必要な場合、クラウド内のコールドブロックがホットになり、オンプレミスのパフォーマンスフラッシュ階層に戻ります。

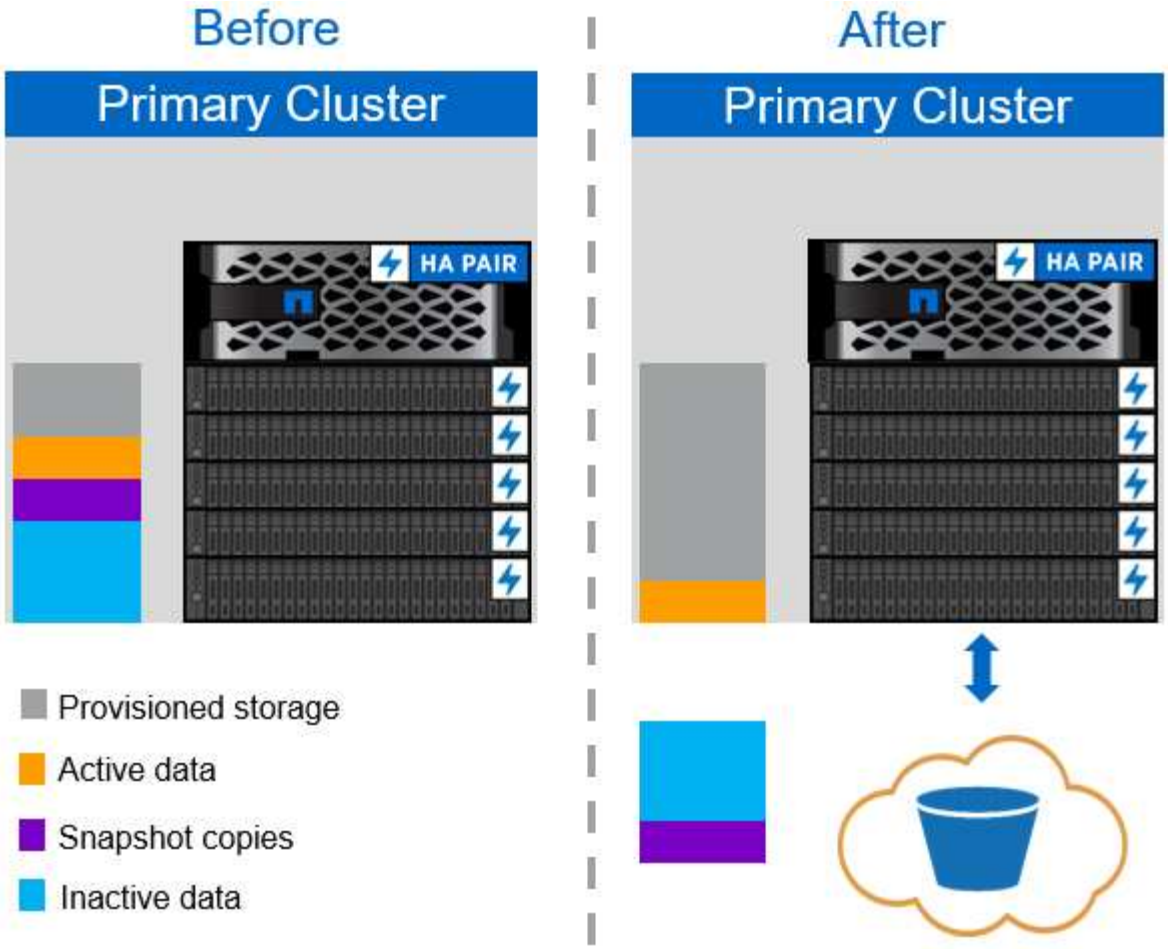


auto 階層化ポリシー

次の図に示す FabricPool の自動階層化ポリシーは、コールドスナップショットのデータブロックをクラウドに移動するだけでなく、アクティブファイルシステムのコールドブロックも移動します。これには、 VM テンプレートと、データストアボリューム内の未使用の VM データが含まれることがあります。どのコールドブロックを移動するかは ' ボリュームの階層化最小冷却日数設定によって制御されますクラウド階層のコールドブロックがアプリケーションによってランダムに読み取られると、それらのブロックがホットになり、パフォーマンス階層に戻ります。ただし、ウィルス対策スキャナなどのプロセスによってコールドブロックが読み取られた場合、ブロックはコールドのままクラウドオブジェクトストアに残り、パフォーマンス階層に戻されることはありません。

auto 階層化ポリシーを使用している場合、ホットに設定されたアクセス頻度の低いブロックは、クラウド接続の速度でクラウド階層から戻されます。これは、レイテンシの影響を受けやすいアプリケーションの場合、VM のパフォーマンスに影響を及ぼす可能性があります。レイテンシが影響を受ける場合は、データストアで自動階層化ポリシーを使用する前に考慮する必要があります。十分なパフォーマンスを確保するために、インタークラスタ LIF は 10GbE の速度のポートに配置することを推奨します。

オブジェクトストレージプロファイラは、オブジェクトストアを FabricPool アグリゲートに接続する前に、オブジェクトストアに対するレイテンシとスループットをテストするために使用します。



all 階層化ポリシー

「自動」および「 Snapshot のみ」のポリシーとは異なり、「すべて」の階層化ポリシーは、データボリューム全体をただちにクラウド階層に移動します。このポリシーは、セカンダリデータ保護ボリュームまたはアーカイブボリュームに適しています。アーカイブボリュームのデータは、履歴データや規制上の目的で保持する必要があり、ほとんどアクセスされません。VMware データストアボリュームに書き込まれたデータはすぐにクラウド階層に移動されるため、「すべて」のポリシーは推奨されません。以降の読み取り処理はクラウドから実行されるため、データストアボリュームに配置されている VM やアプリケーションでパフォーマンスの問題が発生する可能性があります。

セキュリティ

クラウドと FabricPool では、セキュリティが一元的に懸念されます。ONTAP に標準で搭載されているセキュリティ機能はすべて高パフォーマンス階層でサポートされており、データの移動はクラウド階層に転送される際にセキュリティで保護されます。FabricPool では、を使用します "AES-256-GCM" パフォーマンス階層で暗号化アルゴリズムを使用して、この暗号化をエンドツーエンドでクラウド階層に維持します。クラウドオブジェクトストアに移動されるデータブロックは、ストレージ階層間のデータの機密性と整合性を維持するために、 Transport Layer Security （ TLS ） v1.2 で保護されます。

暗号化されていない接続を介したクラウドオブジェクトストアとの通信はサポートされていますが、ネットアップでは推奨していません

データ暗号化は、知的財産、取引情報、個人を特定できる顧客情報の保護に不可欠です。FabricPool は、既存のデータ保護戦略を維持するために、 NetApp Volume Encryption （ NVE ）と NetApp Storage Encryption （ NSE ）の両方を完全にサポートしています。クラウド階層に移動した場合、パフォーマンス階層で暗号化されたすべてのデータは暗号化されたままになります。クライアント側の暗号化キーは ONTAP によって所有され、サーバ側のオブジェクトストアの暗号化キーはそれぞれのクラウドオブジェクトストアによって所有されます。NVE で暗号化されていないデータは、 AES-256-GCM アルゴリズムで暗号化されます。それ以外の AES-256 暗号はサポートされません。

NSE または NVE の使用はオプションで、 FabricPool を使用する必要はありません。

FabricPool の要件

FabricPool を使用するには、 ONTAP 9.2 以降と、このセクションに記載されたプラットフォームのいずれかで SSD アグリゲートを使用する必要があります。追加の FabricPool 要件は、接続するクラウド階層によって異なります。NetApp AFF C190 など、容量が比較的小さい、固定レベルの AFF プラットフォームでは、アクセス頻度の低いデータをクラウド階層に移動する場合に FabricPool を使用すると効果的です。

プラットフォーム

FabricPool は、次のプラットフォームでサポートされます。

- NetApp AFF
  - A800
  - A700S 、 A700
  - A320 、 A300
  - A220 、 A200
  - C190
  - AFF8080 、 AFF8060 、および AFF8040
- NetApp FAS
  - FAS9000
  - FAS8200
  - FAS8080 、 FAS8060 、および FAS8040
  - FAS2750 、 FAS2720
  - FAS2650 、 FAS2620

FabricPool を使用できるのは、 FAS プラットフォーム上の SSD アグリゲートのみです。

- クラウド階層
  - Alibaba Cloud Object Storage Service （標準、低頻度アクセス）
  - Amazon S3 （標準、標準 -IA 、 1 ゾーン -IA 、インテリジェント階層化）

- Amazon Commercial クラウドサービス（ C2S ）
- Google Cloud Storage （マルチリージョン、リージョナル、ニアライン、コールドライン）
- IBM Cloud Object Storage （ Standard 、 Vault 、 Cold Vault 、 Flex ）
- Microsoft Azure Blob Storage （ホットおよびクール）

クラスタ間 **LIFs**

FabricPool を使用するクラスタのハイアベイラビリティ（ HA ）ペアでは、クラウド階層と通信するために 2 つのクラスタ間 LIF が必要です。ネットアップでは、追加の HA ペアでクラスタ間 LIF を作成して、これらのノードのアグリゲートにもクラウド階層をシームレスに接続することを推奨しています。

ONTAP が AWS S3 オブジェクトストアとの接続に使用する LIF は、 10Gbps ポート上に配置する必要があります。

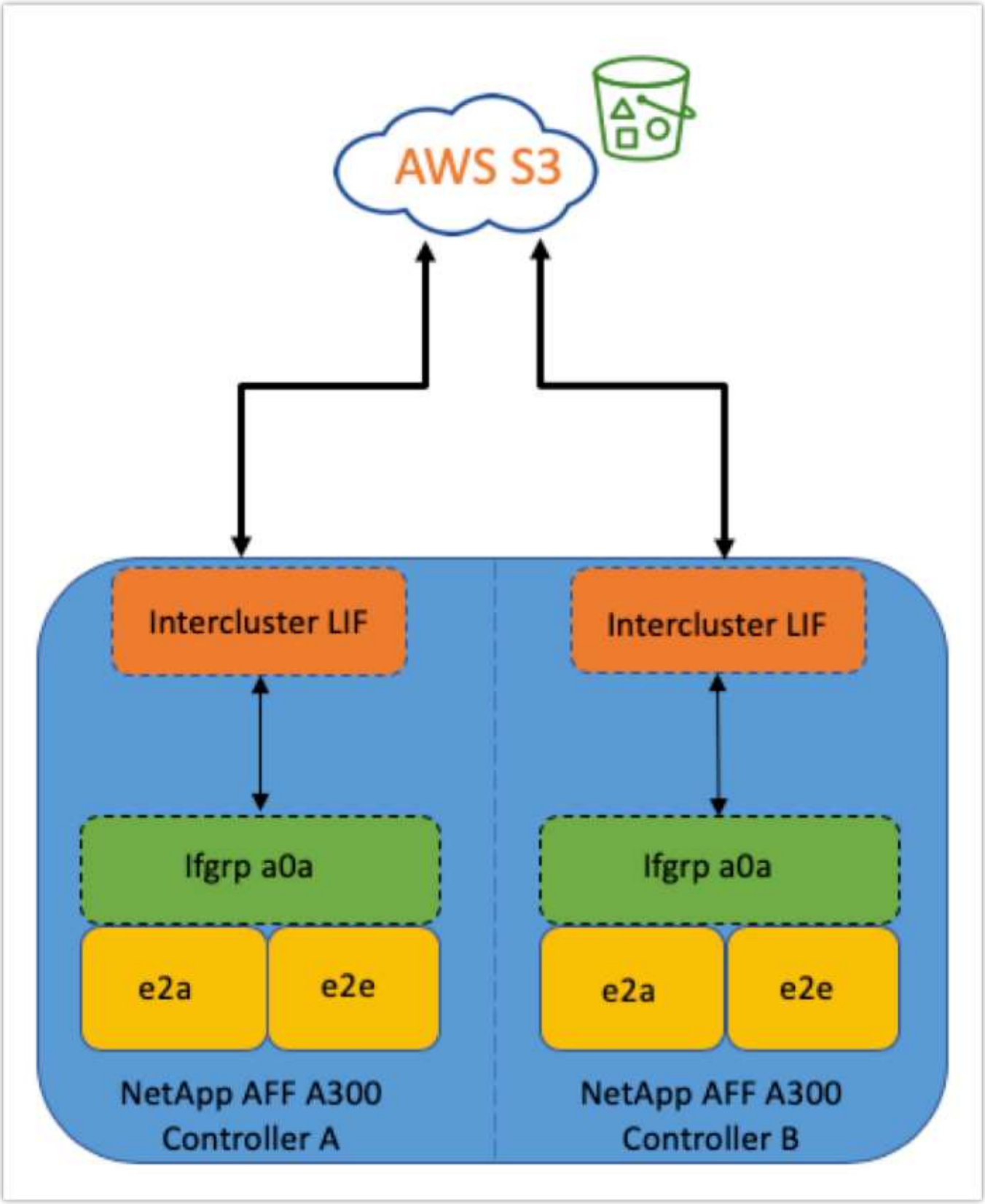
ルーティングが異なるノードで複数の Intercluser LIF を使用する場合は、異なる IPspace に配置することを推奨します。FabricPool では設定時に複数の IPspace から選択できますが、 IPspace 内の特定のクラスタ間 LIF を選択することはできません。

クラスタ間 LIF を無効化または削除すると、クラウド階層への通信が中断されます。

接続性

FabricPool 読み取りレイテンシは、クラウド階層への接続機能です。次の図に示すように、 10Gbps ポートを使用するクラスタ間 LIF は、十分なパフォーマンスを提供します。特定のネットワーク環境のレイテンシとスループットを検証して、 FabricPool のパフォーマンスに与える影響を判断することを推奨します。

低パフォーマンスの環境で FabricPool を使用する場合は、クライアントアプリケーションの最小パフォーマンス要件を引き続き満たし、それに応じてリカバリ時間の目標を調整する必要があります。



オブジェクトストアプロファイラ

次に示すオブジェクトストアプロファイラの例は ONTAP の CLI から実行でき、 FabricPool アグリゲートに接続する前にオブジェクトストアのレイテンシとスループットのパフォーマンスをテストします。

クラウド階層は、オブジェクトストレージプロファイラで使用する前に ONTAP に追加する必要があります。

次のコマンドを使用して、 ONTAP の advanced 権限モードからオブジェクトストアプロファイラを開始します。

```
storage aggregate object-store profiler start -object-store-name <name>
-node <name>
```

結果を表示するには、次のコマンドを実行します。

```
storage aggregate object-store profiler show
```

クラウド階層では、パフォーマンス階層のようなパフォーマンスは提供されません（通常は毎秒 GB ）。FabricPool アグリゲートは、 SATA のようなパフォーマンスを簡単に提供できますが、 SATA のようなパフォーマンスを必要としない階層化ソリューションでは、 10 秒という高いレイテンシと低いスループットも許容できます。

```
bb09-a300-2::*> storage aggregate object-store profiler show
Object store config name: aws_infra_fp_bk_1
Node name: bb09-a300-2-1
Status: Active. Issuing GETs
Start time: 10/3/2019 12:37:24

Op      Size       Total     Failed            Latency(ms)          Throughput
                                        min       max       avg
-------------------------------------------------------------------------------
PUT     4MB        1084      0         336       5951      2817     69.55MB
GET     4KB        158636    0         27        1132      41       32.22MB
GET     8KB        0         0         0         0         0        0B
GET     32KB       0         0         0         0         0        0B
GET     256KB      0         0         0         0         0        0B
5 entries were displayed.
```

個のボリューム

ストレージシンプロビジョニングは、 FlexPod 仮想インフラ管理者向けの標準的な手法です。NetApp Virtual Storage Console （ VSC ）では、 VMware データストアのストレージボリュームを、スペースギャランティ（シンプロビジョニング）なしでプロビジョニングできます。また、ネットアップのベストプラクティスに従って、ストレージ効率の設定が最適化されます。VSC を使用して VMware データストアを作成する場合は、データストアボリュームにスペースギャランティを割り当てる必要がないため追加の操作は必要ありません。

FabricPool は、「なし」以外のスペースギャランティを使用するボリュームを含むアグリゲート（「ボリューム」など）にクラウド階層を接続できません。

```
volume modify -space-guarantee none
```

'pace guarantee none' パラメータを設定すると ' ボリュームのシン・プロビジョニングが行われますこのギャランティタイプのボリュームで使用されるスペースの量は、初期ボリュームサイズで決定されるのではなく、データが追加されるにつれて増加します。このアプローチは FabricPool にとって不可欠です。ボリュームがホットになりパフォーマンス階層に戻されるクラウド階層データをサポートする必要があるためです。

ライセンス

FabricPool では、サードパーティのオブジェクトストレージプロバイダ（ Amazon S3 など）を AFF および FAS ハイブリッドフラッシュシステムのクラウド階層として接続する場合、容量ベースのライセンスが必要です。

FabricPool ライセンスには恒久ライセンスとタームベースライセンス（ 1 年または 3 年）があります。

クラウド階層に格納されているデータの量（使用容量）がライセンス容量に達すると、クラウド階層への階層化が停止します。「すべて」の階層化ポリシーを使用したボリュームへの SnapMirror コピーを含む追加データは、ライセンス容量が増加するまで階層化できません。階層化は停止しますが、クラウド階層のデータには引き続きアクセスできます。ライセンスされた容量が増えるまで、追加のコールドデータは SSD に残ります。

新しい ONTAP 9.5 以降のクラスタを購入すると、無料の 10TB 容量のタームベースの FabricPool ライセンスが付属しますが、追加のサポートコストが適用される場合があります。FabricPool ライセンス（既存のライセンスの追加容量を含む）は、 1TB 単位で購入できます。

FabricPool ライセンスは、 FabricPool アグリゲートを含まないクラスタからのみ削除できます。

FabricPool ライセンスはクラスタ全体に適用されます。ライセンスの購入時にUUIDを用意しておく必要があります (`cluster identify show`）。追加のライセンス情報については、を参照してください "ネットアップナレッジベース"。

設定

ソフトウェアのリビジョン

次の表に、検証済みのハードウェアとソフトウェアのバージョンを示します。

レイヤー（ **Layer** ）	デバイス	イメージ（ **Image** ）	コメント
ストレージ	NetApp AFF A300	ONTAP 9.6P2	
コンピューティング	Cisco UCS B200 M5 ブレードサーバ、 Cisco UCS VIC 1340	リリース 4.0 （ 4b ）	
ネットワーク	Cisco Nexus 6332-16UP ファブリックインターコネクト	リリース 4.0 （ 4b ）	
	NX-OS スタンドアロンモードの Cisco Nexus 93180YC-EX スイッチ	リリース 7.0(3) i7(6)	
ストレージネットワーク	Cisco MDS 9148S	リリース 8.3(2)	

レイヤー（ **Layer** ）	デバイス	イメージ（ **Image** ）	コメント
ハイパーバイザー		VMware vSphere ESXi 6.7U2	ESXi 6.7.0,13006603.
		VMware vCenter Server の各機能を使用し	vCenter サーバ 6.7.0.30000 ビルド 13639309
クラウドプロバイダ		Amazon AWS S3	デフォルトオプションを使用する標準の S3 バケット

FabricPool の基本要件については、を参照してください "FabricPool の要件"。基本的な要件をすべて満たしたら、次の手順を実行して FabricPool を設定します。

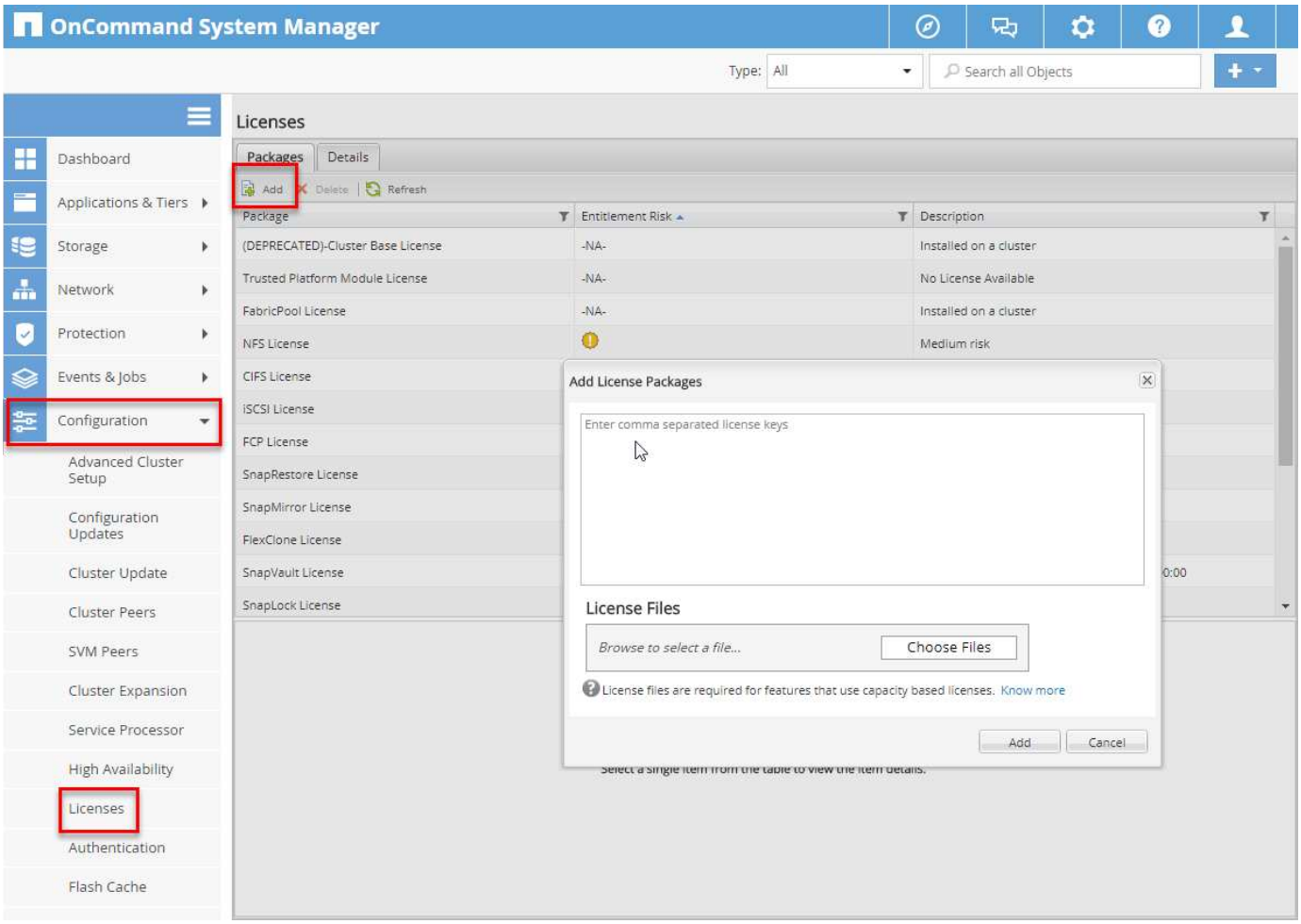
1. FabricPool ライセンスをインストールする。
2. AWS S3 オブジェクトストアバケットを作成する。
3. ONTAP にクラウド階層を追加します。
4. クラウド階層をアグリゲートに接続する。
5. ボリューム階層化ポリシーを設定

"次の手順： FabricPool ライセンスをインストールします。"

FabricPool ライセンスをインストールする

ネットアップライセンスファイルを取得したら、 OnCommand System Manager でインストールできます。ライセンスファイルをインストールするには、次の手順を実行します。

1. 構成をクリックします
2. クラスタをクリックします。
3. [ライセンス] をクリックします
4. 追加をクリックします。
5. [ファイルの選択] をクリックして、ファイルを参照して選択します。
6. 追加をクリックします。



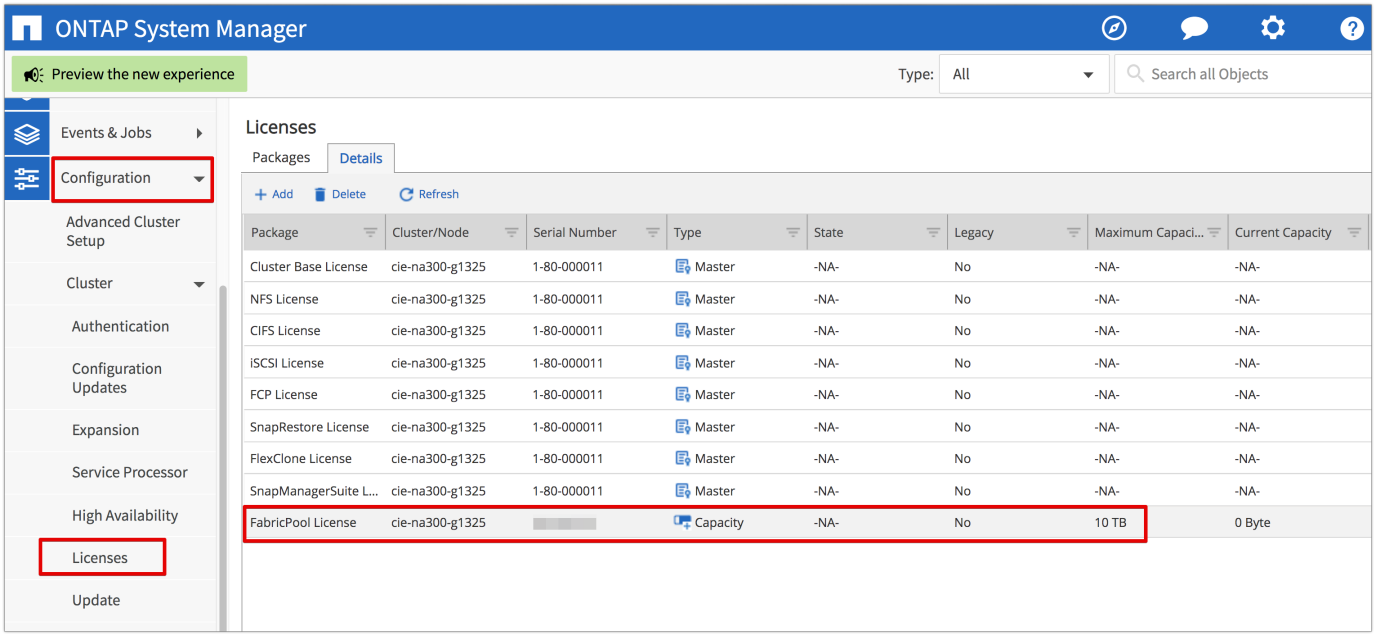
ライセンス容量

ライセンス容量を表示するには、 ONTAP CLI または OnCommand System Manager を使用します。ライセンス容量を確認するには、 ONTAP CLI で次のコマンドを実行します。

```
system license show-status
```

OnCommand システムマネージャで、次の手順を実行します。

1. 構成をクリックします
2. [ライセンス] をクリックします
3. [詳細] タブをクリックします。



FabricPool ライセンスの行には、最大容量と現在の容量が表示されます。

"次： AWS S3 バケットを作成します。"

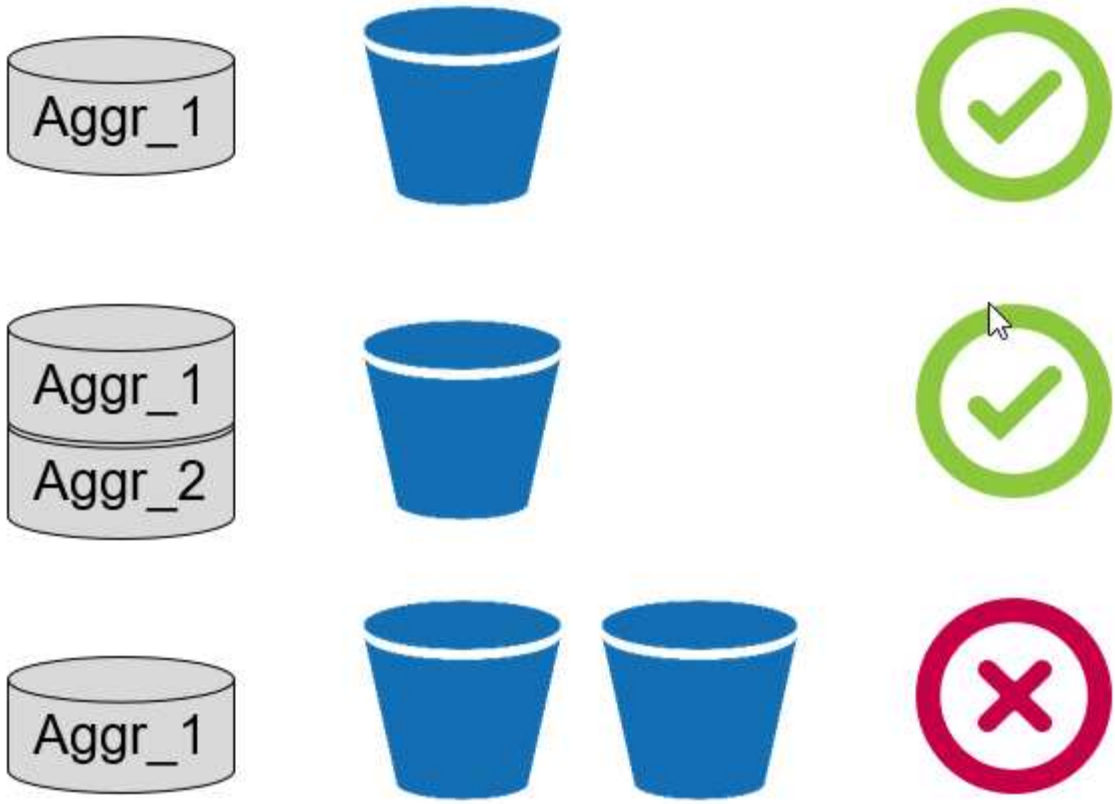
AWS S3 バケットを作成する

バケットは、データを保持するオブジェクトストレージコンテナです。データをクラウド階層としてアグリゲートに追加する前に、データが格納されているバケットの名前と場所を指定する必要があります。

バケットは、 OnCommand システムマネージャ、 OnCommand Unified Manager 、または ONTAP を使用して作成することはできません。

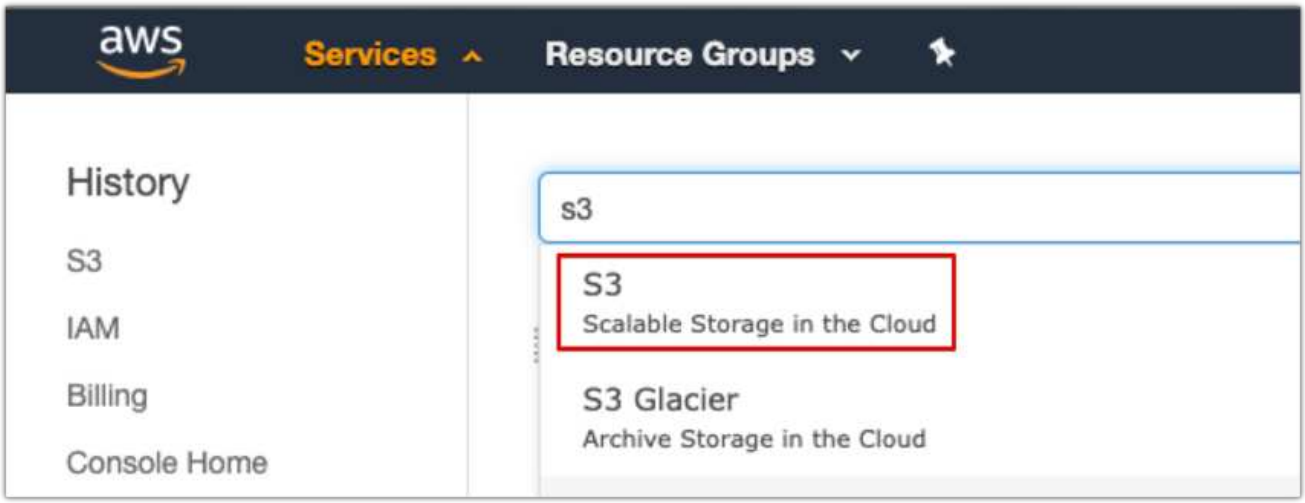
次の図に示すように、 FabricPool ではアグリゲートごとに 1 つのバケットの接続がサポートされます。1 つのバケットを 1 つのアグリゲートに接続し、 1 つのバケットを複数のアグリゲートに接続できます。ただし、 1 つのアグリゲートを複数のバケットに接続することはできません。1 つのバケットをクラスタ内の複数のアグリゲートに接続することはできますが、複数のクラスタ内のアグリゲートに 1 つのバケットを接続することは推奨されません。

ストレージアーキテクチャを計画する際は、バケットとアグリゲートの関係がパフォーマンスにどのように影響するかを検討してください。多くのオブジェクトストレージプロバイダは、サポートされる IOPS の最大数をバケットレベルまたはコンテナレベルで設定しています。最大のパフォーマンスを必要とする環境では、複数のバケットを使用して、オブジェクトストレージの IOPS 制限が複数の FabricPool アグリゲートのパフォーマンスに影響する可能性を軽減する必要があります。クラスタ内のすべての FabricPool アグリゲートに単一のバケットまたはコンテナを接続すると、クラウド階層のパフォーマンスよりも管理性の高い環境が有利になることがあります。

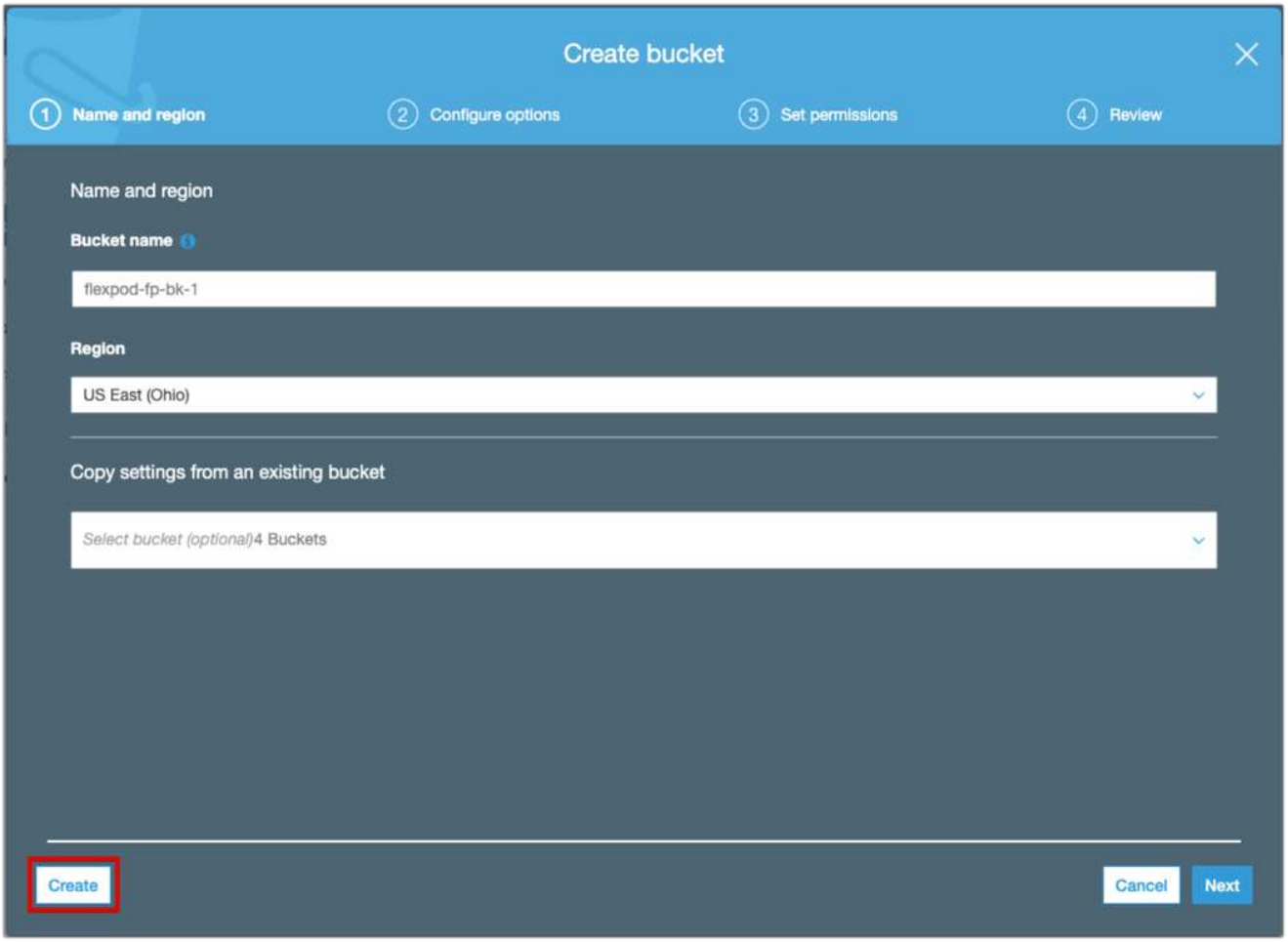


S3 バケットを作成します。

1. ホームページから AWS 管理コンソールの検索バーに「 S3 」と入力します。
2. クラウドで S3 Scalable Storage を選択します。



3. S3 ホームページで、バケットの作成を選択します。
4. DNS 準拠の名前を入力し、バケットを作成するリージョンを選択します。



5. Create をクリックしてオブジェクトストアバケットを作成します。

"次： ONTAP にクラウド階層を追加します"

ONTAP にクラウド階層を追加します

オブジェクトストレージをアグリゲートに接続する前に、オブジェクトストレージを追加し、 ONTAP で識別する必要があります。このタスクは、 OnCommand システムマネージャまたは ONTAP CLI のどちらかで実行できます。

FabricPool は、クラウド階層として Amazon S3 、 IBM Object Cloud Storage 、および Microsoft Azure Blob Storage オブジェクトストアをサポートしています。

次の情報が必要です。

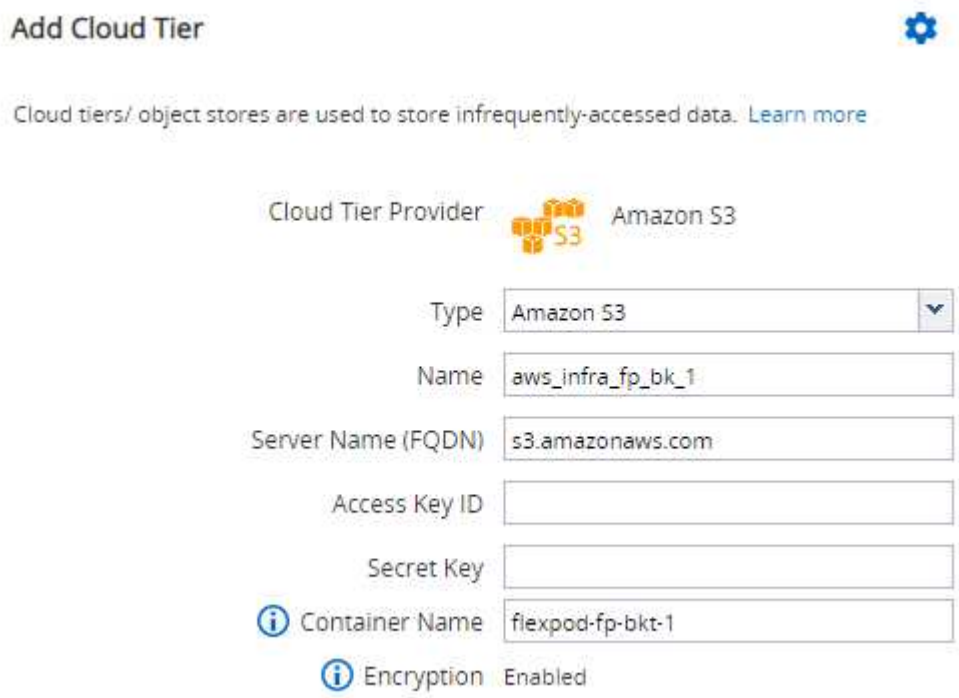
- サーバ名（ FQDN ）。例：「 3.amazonaws.com 」
- アクセスキー ID
- シークレットキー
- コンテナ名（バケット名）

OnCommand システムマネージャ

OnCommand System Manager を使用してクラウド階層を追加するには、次の手順を実行します。

1. OnCommand System Manager を起動します。
2. [ストレージ] をクリックします
3. アグリゲートとディスクをクリックします。
4. クラウド階層をクリックします。
5. オブジェクトストアプロバイダを選択します。
6. オブジェクトストアプロバイダの必要に応じてテキストフィールドを入力します。

   Container Name フィールドに、オブジェクトストアのバケット名またはコンテナ名を入力します。
7. アグリゲートを保存して接続をクリックします。



ONTAP CLI

ONTAP CLI を使用してクラウド階層を追加するには、次のコマンドを入力します。

```
object-store config create
-object-store-name <name>
-provider-type <AWS>
-port <443/8082> (AWS)
-server <name>
-container-name <bucket-name>
-access-key <string>
-secret-password <string>
-ssl-enabled true
-ipspace default
```

"次：クラウド階層を ONTAP アグリゲートに接続します。"

ONTAP アグリゲートにクラウド階層を接続する

ONTAP でオブジェクトストアを追加して識別したら、そのオブジェクトストアをアグリゲートに接続して FabricPool を作成する必要があります。このタスクは、 OnCommand システムマネージャまたは ONTAP CLI を使用して実行できます。

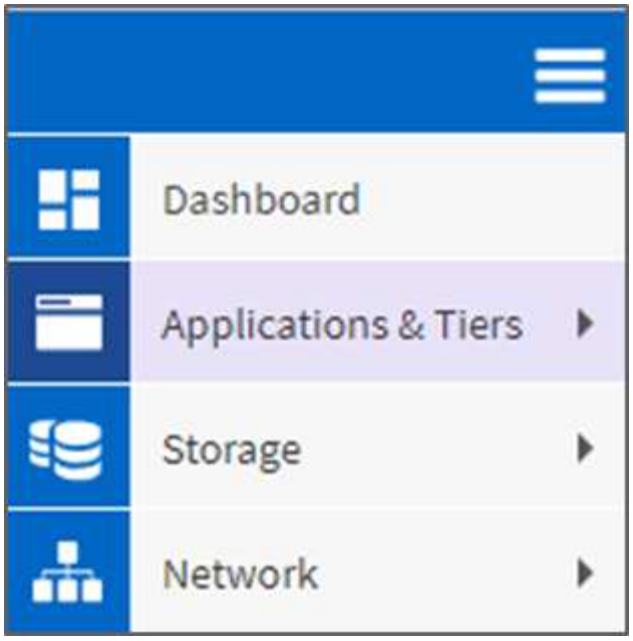
1 つのクラスタに複数のタイプのオブジェクトストアを接続できますが、各アグリゲートに接続できるオブジェクトストアのタイプは 1 つだけです。たとえば、 1 つのアグリゲートで Google Cloud を使用でき、別のアグリゲートで Amazon S3 を使用できますが、 1 つのアグリゲートを両方に接続することはできません。

クラウド階層をアグリゲートに接続することは、永続的なアクションです。クラウド階層は、接続されているアグリゲートから接続を解除することはできません。

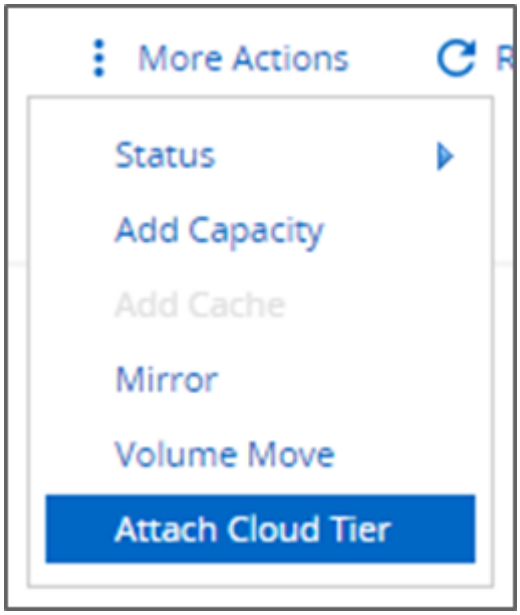
OnCommand システムマネージャ

OnCommand System Manager を使用してクラウド階層をアグリゲートに接続するには、次の手順を実行します。

1. OnCommand System Manager を起動します。
2. [アプリケーションと階層] をクリックします。



3. [ストレージ階層] をクリックします。
4. アグリゲートをクリックします。
5. アクションをクリックし、クラウド階層の接続を選択します。



6. クラウド階層を選択します。
7. アグリゲート上のボリュームの階層化ポリシーを表示および更新します（オプション）。デフォルトでは、ボリューム階層化ポリシーは「 Snapshot のみ」に設定されています。
8. [保存] をクリックします .

ONTAP CLI

ONTAP CLI を使用してアグリゲートにクラウド階層を接続するには、次のコマンドを実行します。

```
storage aggregate object-store attach
-aggregate <name>
-object-store-name <name>
```

例

```
storage aggregate object-store attach -aggregate aggr1 -object-store-name
- aws_infra_fp_bk_1
```

"次：ボリューム階層化ポリシーを設定します。"

ボリューム階層化ポリシーを設定します

デフォルトでは、ボリュームは「なし」ボリューム階層化ポリシーを使用します。ボリュームの作成後、 OnCommand システムマネージャまたは ONTAP CLI を使用してボリューム階層化ポリシーを変更できます。

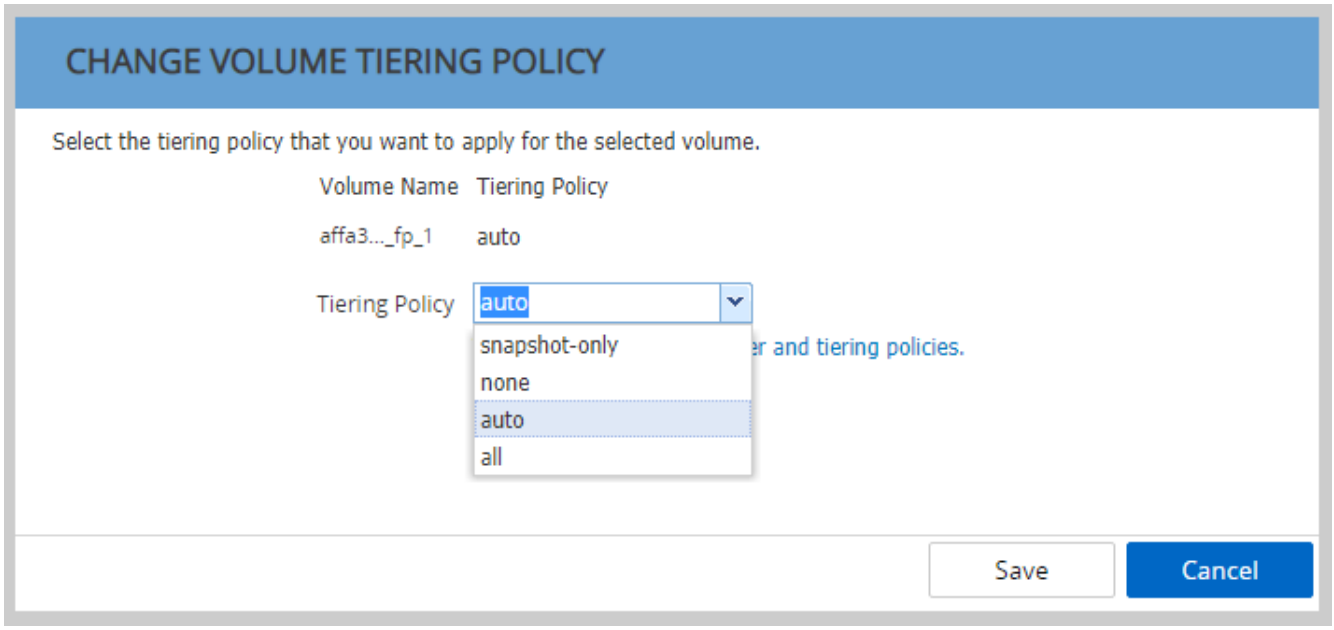
FlexPod で使用する場合、 FabricPool には、「自動」、「 Snapshot のみ」、「なし」の 3 つのボリューム階層化ポリシーが用意されています。

- * 自動 *
  - ボリューム内のすべてのコールドブロックがクラウド階層に移動されます。アグリゲートの使用率が 50% を超えている場合、非アクティブなブロックがコールドになるまでに約 31 日かかります。自動クーリング期間は、「 tiering-minimum-cooling-days 」設定を使用して、 2 日から 63 日の間で調整できます。
  - 階層化ポリシーが「自動」に設定されているボリューム内のコールドブロックがランダムに読み取られると、ブロックがホットになり、パフォーマンス階層に書き込まれます。
  - 階層化ポリシーが「自動」に設定されているボリューム内のコールドブロックが順番に読み取られると、コールドブロックのままクラウド階層に残ります。パフォーマンス階層には書き込まれません。
- * Snapshot のみ *
  - アクティブなファイルシステムと共有されていないボリューム内のコールドスナップショットブロックはクラウド階層に移動されます。アグリゲートの使用率が 50% を超えている場合、非アクティブな Snapshot ブロックがコールドになるまでに約 2 日かかります。「 tiering-minimum-cooling-days 」設定を使用すると、 Snapshot のみのクーリング期間を 2 日から 63 日に調整できます。
  - 階層化ポリシーが「 Snapshot のみ」に設定されているボリューム内のコールドブロックが読み取られるとホットになり、パフォーマンス階層に書き込まれます。
- * なし（デフォルト） *
  - 階層化ポリシーで「なし」を使用するように設定されたボリュームは、コールドデータをクラウド階層に階層化しません。
  - 階層化ポリシーを「なし」に設定すると、新しい階層化が防止されます。
  - 以前にクラウド階層に移動したボリュームデータは、ホットになるまでクラウド階層に残り、パフォーマンス階層に自動的に戻ります。

OnCommand システムマネージャ

OnCommand システムマネージャを使用してボリュームの階層化ポリシーを変更するには、次の手順を実行します。

1. OnCommand System Manager を起動します。
2. ボリュームを選択します。
3. その他の操作をクリックし、階層化ポリシーの変更を選択します。
4. ボリュームに適用する階層化ポリシーを選択します。
5. [保存] をクリックします .



ONTAP CLI

ONTAP CLI を使用してボリュームの階層化ポリシーを変更するには、次のコマンドを実行します。

```
volume modify -vserver <svm_name> -volume <volume_name>
-tiering-policy <auto|snapshot-only|all|none>
```

"次の手順：ボリューム階層化の最小クーリング日数を設定します。"

ボリューム階層化の最小クーリング日数を設定します

「 tiering-minimum-cooling-days 」設定では、ボリューム内のアクセス頻度の低いデータがコールドとみなされて階層化の対象になるまでの日数を指定します。

自動

Auto 階層化ポリシーのデフォルトの「 tiering-minimum-cooling-days 」設定は 31 日です。

読み取りではブロック温度がホットになるため、この値を大きくすると、階層化の対象となるデータ量が減り、パフォーマンス階層に保持されるデータ量が増加する可能性があります。

この値をデフォルトの 31 日間から減らす場合は、コールドとしてマークされる前にデータをアクティブにしないようにしてください。たとえば ' 複数日のワークロードが 7 日目にかなりの数の書き込みを実行すると予想される場合 ' ボリュームの「 tiering-minimum-cooling-days 」設定は 8 日以上に設定する必要があります

> オブジェクトストレージは、ファイルやブロックストレージのようにトランザクション可能ではありません。ボリュームにオブジェクトとして保存されているファイルを変更してクーリング日数を最小限に抑えると、新しいオブジェクトの作成、既存のオブジェクトの断片化、およびストレージの非効率性の追加につながる可能性があります。

Snapshot のみ

スナップショット専用階層化ポリシーのデフォルトの「 tiering-minimum-cooling-days 」設定は 2 日です。最小値を 2 日間に設定すると、バックグラウンドプロセスの時間が長くなり、ストレージ効率が最大限に向上します。また、日々のデータ保護プロセスがクラウド階層からデータを読み取る必要がなくなります。

ONTAP CLI

ONTAP CLI を使用してボリュームの「 tiering-minimum-cooling-days 」設定を変更するには、次のコマンドを実行します。

```
volume modify -vserver <svm_name> -volume <volume_name> -tiering-minimum
-cooling-days <2-63>
```

advanced 権限レベルが必要です。

> 階層化ポリシーを「自動」と「 Snapshot のみ」（またはその逆）の間で変更すると、パフォーマンス階層のブロックの非アクティブ期間がリセットされます。たとえば、「自動」ボリューム階層化ポリシーを使用し、 20 日間非アクティブだったパフォーマンス階層のデータを含むボリュームでは、階層化ポリシーが「 Snapshot のみ」に設定されている場合、パフォーマンス階層のデータが非アクティブになる日数は 0 日にリセットされます。

パフォーマンスに関する考慮事項

高パフォーマンス階層のサイズを設定します

サイジングを検討する場合は、パフォーマンス階層で次のタスクを実行できる必要があります。

- ホットデータのサポート
- 階層化スキャンによってデータがクラウド階層に移動されるまでコールドデータのサポート
- ホットになりパフォーマンス階層に書き戻されるクラウド階層データのサポート
- 接続されたクラウド階層に関連付けられた WAFL メタデータをサポートしています

ほとんどの環境では、 FabricPool アグリゲートのパフォーマンスと容量の比率は 1 ： 10 で、非常に控えめであるため、ストレージを大幅に節約できます。たとえば、 200TB をクラウド階層に階層化する場合、パフォーマンス階層アグリゲートは少なくとも 20TB にする必要があります。

パフォーマンス階層の容量が 70% を超える場合、クラウド階層からパフォーマンス階層への書き込みは無効になります。この場合、ブロックはクラウド階層から直接読み取られます。

クラウド階層のサイズを設定する

サイジングを検討する場合、クラウド階層として機能するオブジェクトストアは次のタスクを実行できる必要があります。

- 既存のコールドデータの読み取りをサポートします
- 新しいコールドデータの書き込みをサポートします
- オブジェクトの削除とデフラグをサポートしています

所有コスト

。 "FabricPool 経済計算ツール" 独立した IT アナリスト企業の Evaluator Group が、オンプレミスとクラウドの間でコールドデータストレージのコスト削減を予測できるよう支援します。この計算ツールは、アクセス頻度の低いデータをパフォーマンス階層に格納するコストと、残りのデータライフサイクルについてクラウド階層に送信するコストを算出するシンプルなインターフェイスです。5 年間の計算に基づいて、ソース容量、データ増加率、スナップショット容量、コールドデータの割合の 4 つの主要な要素を使用して、その期間におけるストレージコストを決定します。

まとめ

クラウドへの移行は、組織ごと、ビジネスユニットごと、組織内のビジネスユニット間で異なります。一部は急速な導入を選択し、その他はより控えめなアプローチを採用しています。FabricPool は、組織の規模やクラウドの導入速度に関係なく、組織のクラウド戦略に適合し、 FlexPod インフラの効率性と拡張性のメリットをさらに実証します。

追加情報の参照先

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

- FabricPool のベストプラクティス

  "www.netapp.com/us/media/tr-4598.pdf"

- ネットアップの製品マニュアル

  "https://docs.netapp.com"

- TR-4036 ：『 FlexPod データセンター技術仕様』

  "https://www.netapp.com/us/media/tr-4036.pdf"

IBMクラウドプライベートを使用するFlexPod データセンター

Sreenivasa Edula、Cisco Thanachit Wichianchai、IBM Jacky Ben-Bassat、IBM Global Alliance、ネットアップ

IBM Cloud Private（ICP）は、クラウドネイティブやアプリケーション最新化のユースケース向けにコンテナ化されたアプリケーションを開発、管理するためのオンプレミスプラットフォームです。コンテナオーケストレーションとしてKubernetes上に構築された統合環境で、Dockerコンテナ用のプライベートイメージリポジトリ、管理コンソール、監視フレームワーク、多くのオープンソースベースおよびIBMコンテナ化アプリケーションなどが含まれます。Ciscoとネットアップが提供する統合インフラであるFlexPod とICPを組み合わせることで、インフラの導入と管理が簡易化されます。また、ストレージ効率の向上、データ保護の強化、リスクの軽減、この可用性に優れたエンタープライズクラスのインフラスタックを柔軟に拡張できるというメリットも得られ、新しいビジネス要件や長期的なその他の変化に対応できます。

"IBMクラウドプライベートを使用するFlexPod データセンター"

FlexPod Datacenter for Hybrid Cloud with Cisco CloudCenter and NetApp Private Storage -設計

ネットアップ、Haseeb Niazi、Cisco David Arnette

Cisco Validated Design（CVD）は、お客様の導入を促進および改善するために設計、テスト、文書化されたシステムとソリューションを提供します。これらの設計では、お客様のビジネスニーズに対応し、設計から導入までを支援するために開発されたソリューションポートフォリオに、幅広いテクノロジと製品が組み込まれています。

"FlexPod Datacenter for Hybrid Cloud with Cisco CloudCenter and NetApp Private Storage -設計"

Cisco CloudCenterとネットアップデータファブリックを使用したマルチクラウド対応のFlexPod データセンター

ネットアップ、Haseeb Niazi、Cisco David Arnette

本ドキュメントでは、FlexPod Datacenter for Hybrid Cloudをセットアップするための設定と実装の詳細なガイドラインを提供します。次の設計要素は、このバージョンのFlexPod を以前のモデルと区別します。

- Cisco CloudCenterとFlexPod データセンターの統合（ACIをプライベートクラウドとして使用
- Cisco CloudCenterとAmazon Web Services（AWS）およびMicrosoft Azure Resource Manager（MS Azure RM）パブリッククラウドの統合
- FlexPod データセンターとパブリッククラウドの間にセキュアな接続を提供し、仮想マシン（VM）間のトラフィックをセキュアに保護
- データレプリケーショントラフィック用に、FlexPod データセンターとNetApp Private Storage（NPS）

の間にセキュアな接続を提供します

- パブリッククラウドまたはプライベートクラウドにアプリケーションインスタンスを導入し、Cisco CloudCenterによるオーケストレーションを通じて最新のアプリケーションデータをこれらのインスタンスで利用できるようにする機能
- この新しいハイブリッドクラウドモードで、開発およびテスト環境の運用面をセットアップ、検証、強調します。

"Cisco CloudCenterとネットアップデータファブリックを使用したマルチクラウド対応のFlexPod データセンター"

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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

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

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

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

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

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、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。