

vRealize Automation の構成

2021 年 7 月 21 日

vRealize Automation 7.5

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>)

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴィエムウェア株式会社
105-0013 東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

Copyright © 2015-2021 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

目次

vRealize Automation の構成 6

更新情報 7

1 ブループリント プロビジョニングのための外部環境の準備 8

vRealize Automation の管理に向けた環境の準備 8

NSX ネットワークおよびセキュリティ構成の準備のためのチェックリスト 9

サードパーティ製 IP アドレス管理プロバイダ サポートを提供するためのチェックリスト 14

構成のチェックリスト vRealize Automation のコンテナ 17

vRealize Automation 用の vCloud Director 環境の準備 18

vRealize Automation 用の vCloud Air 環境の準備 19

Amazon AWS 環境の準備 19

Red Hat OpenStack のネットワークとセキュリティの機能の準備 26

SCVMM 環境の準備 27

ネットワークと Azure 間の VPC 接続の設定 28

マシン プロビジョニングの準備 29

準備するマシン プロビジョニング方法の選択 29

プロビジョニング時に Visual Basic スクリプトを実行するためのチェックリスト 32

プロビジョニングでの vRealize Automation ゲスト エージェントの使用 33

クローン作成によるプロビジョニングの準備のためのチェックリスト 42

vCloud Air および vCloud Director のプロビジョニングの準備 55

Linux キックスタート プロビジョニングの準備 56

SCCM プロビジョニングの準備 58

WIM プロビジョニングの準備 60

仮想マシン イメージ プロビジョニングの準備 67

Amazon マシン イメージ プロビジョニングの準備 68

シナリオ：マシンをプロビジョニングするために vSphere リソースを準備する 70

ソフトウェア プロビジョニングの準備 73

ソフトウェアを使用してマシンをプロビジョニングするための準備 74

クローン マシンの vSphere テンプレートとソフトウェア コンポーネント ブループリントを準備 77

シナリオ：Dukes Bank for vSphere サンプル アプリケーション ブループリントをインポートするための準備 81

2 ブループリントのプロビジョニングのためのテナントとリソースの準備 87

テナント設定の構成 87

ディレクトリ管理構成オプションの選択 88

ディレクトリ管理の外部コネクタのアップグレード 149

シナリオ：高可用性 vRealize Automation に対する Active Directory リンクを構成する 157

vRealize Automation でのスマート カードおよびサードパーティ ID プロバイダの認証用外部コネクタの構成	160
マルチ ドメインまたはマルチ フォレストの Active Directory リンクの作成	167
グループとユーザーのロールの構成	169
追加テナントの作成	176
テナントを削除する	178
マルチ テナントのセキュリティ設定	179
カスタム ブランディングの構成	179
通知構成のチェックリスト	181
プロビジョニングされたマシンで RDP 接続をサポートするためのカスタム RDP ファイルの作成	192
シナリオ：複数の拠点にまたがる導入環境向けにデータセンターの場所を追加する	192
vRealize Orchestrator の設定	193
リソースの構成	197
IaaS リソース設定のチェックリスト	198
XaaS リソースの構成	331
コンテナの作成と構成	342
デフォルトの vRealize Orchestrator サーバでの追加プラグインのインストール	365
Active Directory ポリシーの操作	365
通知と代理人のユーザー環境設定	369

3 サービス ブループリントのユーザーへの提供 370

ブループリントの設計	370
デザイン ライブラリの作成	372
マシン ブループリントの設計	374
ソフトウェア コンポーネントの設計	479
XaaS ブループリントおよびリソース アクションの設計	491
ブループリントの公開	552
開発者によるブループリントの連携	553
ブループリントとコンテンツのエクスポートおよびインポート	554
提供されているスタンドアローン ブループリントのダウンロードと構成	560
複数開発者環境でのブループリントおよびその他の IaaS コンテンツの作成	560
複合ブループリントの組み合わせ	561
ネストされたブループリントの動作について	563
ブループリントを組み合わせる際のマシン コンポーネントと ソフトウェア コンポーネントの使用	566
ブループリント コンポーネント間でのプロパティ バインドの作成	567
依存関係の作成とプロビジョニングの順序の制御	568
ブループリント申請フォームのカスタマイズ	569
Active Directory オプションを使用したカスタム申請フォームの作成	572
カスタム フォーム デザイナのフィールド プロパティ	579
カスタム フォーム デザイナでの vRealize Orchestrator アクションの使用	584
カスタム フォーム デザイナでの値ピッカーまたはツリー ピッカー要素の使用	586
カスタム フォーム デザイナでのデータ グリッド要素の使用	587

カスタム フォーム デザイナーでの外部検証の使用	590
失敗したプロビジョニング要求のテストおよびトラブルシューティング	594
再開アクションの動作	597
破棄要求が失敗した後の展開環境の強制破棄	599
vRealize Orchestrator ワークフローが含まれている、失敗した展開のトラブルシューティング	599
サービス カタログの管理	600
サービス カタログ構成用のチェックリスト	601
サービスの作成	602
カタログ アイテムとアクションでの作業	604
資格の作成	607
承認ポリシーの操作	614
パラメータ化されたブループリントを使用したマシン プロビジョニングの申請	637
シナリオ：MySQL を搭載した CentOS アプリケーション ブループリントをサービス カタログで利用できる ようにする	638

4 カタログの使用と導入環境の管理 643

カタログの操作	644
カタログ申請を送信する方法	645
展開の操作	647
プロビジョニング要求の監視	647
展開されたカタログ アイテムの管理	650
受信箱の操作	689

vRealize Automation の構成

『vRealize Automation の構成』では、vRealize Automation を使用したプロビジョニングおよびカタログ管理の準備のための vRealize Automation および外部環境の構成についての情報を提供します。

対象者

この情報は、vRealize Automation 環境の構成を担当する IT プロフェッショナル、および vRealize Automation プロビジョニングに使用する既存のインフラストラクチャを担当するインフラストラクチャ管理者を対象としています。記載されている情報は、Windows および Linux のシステム管理者としての経験があり、仮想マシン テクノロジーおよびデータセンターの運用に詳しいことを前提としています。

更新情報

次の表には、この製品リリースに伴う『vRealize Automation の構成』の変更点が挙げられています。

リビジョン	説明
202X 年 XX TBD	メトリック プロバイダの設定 を更新しました。
2020 年 2 月 14 日	マイナー更新。
2019 年 10 月 24 日	<ul style="list-style-type: none"> ■ フィルタリングの予期しないエントリのトラブルシューティングを追加しました。 ■ マイナー更新。
2019 年 9 月 9 日	<ul style="list-style-type: none"> ■ Microsoft Azure エンドポイントの構成を追加しました。 ■ マイナー更新。
2019 年 7 月 18 日	[ブループリントのプロパティ] 設定 の伝達オプションを明確化しました。
2019 年 6 月 14 日	マイナー更新。
2019 年 5 月 30 日	<ul style="list-style-type: none"> ■ ジャストインタイム ユーザーにワイルドカード一致を使用して対処する方法を説明するトピックを追加しました。ジャストインタイム ユーザーに対するワイルドカードによる一致の使用を参照してください。 ■ Kerberos 認証の構成を更新しました。
2019 年 5 月 7 日	<ul style="list-style-type: none"> ■ いくつかのハイパーリンクを修正しました。 ■ SCCM プロビジョニングの準備を更新し、最近追加された構成プロパティの説明を追加しました。
2019 年 3 月 1 日	ワークロード配置の制限事項 の vSAN ステートメントを改訂しました。
2019 年 2 月 12 日	<ul style="list-style-type: none"> ■ ディレクトリ管理のドキュメントから古いドメイン コントローラのトピックを削除しました。ドメイン コントローラの選択を参照してください。また、OpenLDAP ディレクトリ接続の設定も更新して関連する変更を反映しました。 ■ 他のディレクトリ管理のトピックに対して少量のテキストを編集しました。
2019 年 1 月 25 日	<ul style="list-style-type: none"> ■ クローン ブループリントおよびリンク クローン ブループリントのトラブルシューティングを更新しました。 ■ シナリオ：ゲスト エージェント カスタマイズとソフトウェア コンポーネントを使用できるようにリファレンス マシンを準備するを更新しました。 ■ エンドポイントのソースおよび実行中のデータ収集の確認を更新しました。 ■ 複数開発者環境でのブループリントおよびその他の IaaS コンテンツの作成を更新しました。
2018 年 11 月 13 日	■ vRealize Automation での既存の仮想マシン テンプレートの更新を更新しました。
2018 年 10 月 4 日	<ul style="list-style-type: none"> ■ グループベースのアクセス ポリシーの構成を追加しました。 ■ vRealize Operations Manager を使用した継続的な最適化を更新しました。
2018 年 9 月 20 日	初版リリース。

ブループリント プロビジョニングのための外部環境の準備

1

カタログ アイテムのプロビジョニングをサポートするため、vRealize Automation では外部の環境にいくつかの要素を作成または準備することが必要な場合があります。たとえば、クローン マシンのプロビジョニング用にカタログ アイテムを提供する場合、クローン作成元のハイパーバイザーにテンプレートを作成する必要があります。

この章には、次のトピックが含まれています。

- [vRealize Automation の管理に向けた環境の準備](#)
- [ネットワークと Azure 間の VPC 接続の設定](#)
- [マシン プロビジョニングの準備](#)
- [ソフトウェア プロビジョニングの準備](#)





vRealize Automation の管理に向けた環境の準備

作業環境によっては、何らかの変更を行ってからでないと、vRealize Automation 管理下に環境を配備したり、特定の機能を活用したりできない可能性があります。

表 1-1. vRealize Automation の統合に向けた環境の準備

環境	準備
 NSX for vSphere および NSX-T	vRealize Automation でプロビジョニングした仮想マシンのネットワーク、セキュリティ、およびロード バランサの機能の管理に NSX for vSphere または NSX-T を活用する場合、NSX インスタンスを統合に向けて準備します。 NSX ネットワークおよびセキュリティ構成の準備のためのチェックリスト を参照してください。
 vCloud Director	vCloud Director インスタンスをインストールおよび構成し、vSphere およびクラウド リソースを設定し、適切な認証情報を指定または作成して vRealize Automation が vCloud Director 環境にアクセスできるようにします。 vRealize Automation 用の vCloud Director 環境の準備 を参照してください。

表 1-1. vRealize Automation の統合に向けた環境の準備（続き）

環境	準備
 vCloud Air	vCloud Air アカウントに登録し、vCloud Air 環境を設定し、適切な認証情報を指定または作成して vRealize Automation が環境にアクセスできるようにします。 vCloud Air および vCloud Director のプロビジョニングの準備 を参照してください。
 Amazon AWS	vRealize Automation で使用する Amazon AWS 環境内の要素およびユーザー ロールを準備し、Amazon AWS 機能を vRealize Automation 機能にマッピングする方法について理解します。 Amazon AWS 環境の準備 を参照してください。
Microsoft Azure	Azure ブループリントでソフトウェア コンポーネントをサポートするために VPN トンネリングを使用するネットワークを構成します。 ネットワークと Azure 間の VPC 接続の設定 を参照してください。
 Red Hat OpenStack	vRealize Automation でプロビジョニングしたマシンのネットワークおよびセキュリティ機能の管理に Red Hat OpenStack を活用する場合、Red Hat OpenStack インスタンスを統合に向けて準備します。 Red Hat OpenStack のネットワークとセキュリティの機能の準備 を参照してください。
 SCVMM	ストレージ、ネットワークを構成し、テンプレートおよびハードウェア プロファイルの命名に関する制限について理解します。 SCVMM 環境の準備 を参照してください。
外部 IP アドレス管理プロバイダ	外部 IP アドレス管理プロバイダ パッケージまたはプラグインに登録し、設定ワークフローを実行した後、IP アドレス管理ソリューションを新しい vRealize Automation エンドポイントとして登録します。 サードパーティ製 IP アドレス管理プロバイダ サポートを提供するためのチェックリスト を参照してください。
その他のすべての環境	環境に変更を加える必要はありません。テンプレート、起動環境、またはマシン イメージを作成することで、マシンをプロビジョニングするための準備を行うことができます。 マシン プロビジョニングの準備 を参照してください。

NSX ネットワークおよびセキュリティ構成の準備のためのチェックリスト

vRealize Automation で NSX ネットワークおよびセキュリティのオプションを使用できるようにするには、使用予定の外部の NSX for vSphere または NSX-T ネットワークおよびセキュリティ環境を設定する必要があります。

XaaS を使用して、vRealize Automation と NSX for vSphere の統合を拡張する場合は、vRealize Orchestrator に NSX プラグインをインストールする必要があります。プラグインでは、NSX-T はサポートされません。

vRealize Automation で NSX のネットワーク、セキュリティ、およびロード バランシング機能を使用するには、NSX Manager の認証情報を使用する場合、NSX Manager 管理者アカウントを使用する必要があります。

vRealize Automation では、NSX for vSphere と NSX-T がサポートされています。NSX アプリケーションの関連情報については、[NSX for vSphere 製品のドキュメント](#)または [NSX-T 製品のドキュメント](#)を参照してください。

vRealize Automation で使用する NSX ネットワークおよびセキュリティ設定の大部分は外部で設定され、コンピューティング リソースでのデータ収集が実行された後に使用可能になります。

vRealize Automation ブループリントで構成できる NSX 設定の詳細については、[ネットワークおよびセキュリティ コンポーネントの設定](#)を参照してください。

表 1-2. NSX ネットワークおよびセキュリティのチェックリストの準備

タスク	場所	詳細
<input type="checkbox"/> ゲートウェイおよびトランスポート ゾーンの設定を含む、NSX ネットワーク設定を構成します。	NSX アプリケーションでネットワークを設定します。	お使いの NSX 製品に応じて、以下の NSX ドキュメントの管理関連トピックを参照してください。 <ul style="list-style-type: none"> ■ NSX for vSphere 製品のドキュメント ■ NSX-T 製品のドキュメント
<input type="checkbox"/> NSX セキュリティ ポリシー、タグ、およびグループを作成します。	NSX アプリケーションでセキュリティを設定します。	お使いの NSX 製品に応じて、以下の NSX ドキュメントの管理関連トピックを参照してください。 <ul style="list-style-type: none"> ■ NSX for vSphere 製品のドキュメント ■ NSX-T 製品のドキュメント

表 1-2. NSX ネットワークおよびセキュリティのチェックリストの準備（続き）

タスク	場所	詳細
❑ NSX ロード バランサの設定を構成します。	NSX アプリケーションで NSX ロード バランサを設定します。	<p>お使いの NSX 製品に応じて、以下の NSX ドキュメントの管理関連トピックを参照してください。</p> <ul style="list-style-type: none"> ■ NSX for vSphere 製品のドキュメント ■ NSX-T 製品のドキュメント <p>また、docs.vmware.com にある『カスタムプロパティのリファレンス』(PDF) の「ネットワークのカスタム プロパティ」も参照してください。</p>
❑ NSX for vSphere での Cross-vCenter 展開の場合は、コンピューティング NSX Manager がプライマリ NSX マネージャ ロールを持っていることを確認します。	vRealize Automation プロビジョニングでは、マシンが常駐する領域のコンピューティング NSX Manager がプライマリ NSX マネージャ ロールを持っている必要があります。	<p>NSX for vSphere ユニバーサル オブジェクトをプロビジョニングするための管理者要件を参照してください。</p> <p>複数の仮想センターにまたがった展開、ユニバーサル オブジェクト、およびプライマリ NSX マネージャ ロールについては、NSX for vSphere のドキュメント を参照してください。</p>

vRealize Orchestrator での NSX プラグインのインストール

NSX プラグインをインストールするには、vRealize Orchestrator のインストーラ ファイルをダウンロードし、vRealize Orchestrator 構成インターフェイスを使用してプラグイン ファイルをアップロードし、vRealize Orchestrator サーバにそのプラグインをインストールする必要があります。

プラグインのアップデートおよびトラブルシューティングに関する一般的な情報については、[vRealize Orchestrator 製品のドキュメント](#)を参照してください。

前提条件

XaaS を使用して、vRealize Automation と NSX for vSphere の統合を拡張する場合は、vRealize Orchestrator に NSX プラグインをインストールする必要があります。プラグインでは、NSX-T はサポートされません。

使用している組み込みの vRealize Orchestrator に、インストール済みの NSX プラグインがすでに含まれている場合は、この手順を省略できます。

- サポートされている vRealize Orchestrator インスタンスが実行されていることを確認します。
vRealize Orchestrator の設定の詳細については、[vRealize Orchestrator 製品のドキュメント](#)にある『VMware vRealize Orchestrator のインストールおよび構成』を参照してください。
- vRealize Orchestrator プラグインのインストールおよび vCenter Single Sign-On を介して認証する権限が付与されているアカウントの認証情報があることを確認します。
- vRealize Orchestrator クライアントをインストールしており、管理者の認証情報でログインできることを確認します。
- [vRealize Automation のサポート マトリックス](#)で、NSX プラグインの正しいバージョンを確認します。

手順

- 1 vRealize Orchestrator サーバからアクセス可能な場所にプラグイン ファイルをダウンロードします。
該当するバージョン値を含んだプラグインのファイル名形式は、o11nplugin-nsx-1.n.n.vmoapp です。
NSX for vSphere 用プラグインのインストール ファイルは、[VMware 製品のダウンロード サイト](#)から入手できます。
- 2 ブラウザを開いて vRealize Orchestrator 構成インターフェイスを起動します。
URL 形式は、たとえば `https://orchestrator_server.com:8283` のようになります。
- 3 左側のペインで [プラグイン] をクリックし、[新しいプラグインのインストール] セクションまでスクロールします。
- 4 [プラグイン ファイル] テキスト ボックスで、プラグイン インストーラ ファイルを参照して、[アップロードとインストール] をクリックします。
ファイルは .vmoapp 形式にする必要があります。
- 5 プロンプトが表示されたら、[プラグインのインストール] ペインで使用許諾契約書に同意します。
- 6 [有効] のプラグイン インストール ステータスのセクションで、正しい NSX プラグイン名が指定されていることを確認します。
バージョン情報については、[vRealize Automation のサポート マトリックス](#)を参照してください。
「プラグインは次のサーバ起動時にインストールされます」というステータスが表示されます。
- 7 vRealize Orchestrator サーバ サービスを再起動します。
- 8 vRealize Orchestrator 構成インターフェイスを再起動します。
- 9 [プラグイン] をクリックして、ステータスが「インストール成功」に変更されていることを確認します。
- 10 vRealize Orchestrator クライアント アプリケーションを起動し、ログインして [ワークフロー] タブを使用し、ライブラリを介して NSX フォルダに移動します。
NSX プラグインによって提供されるワークフロー全体を参照することができます。

次のステップ

vRealize Automation でワークフローの実行に使用する vRealize Orchestrator エンドポイントを作成します。
[vRealize Orchestrator エンドポイントの作成](#)を参照してください。

NSX for vSphere ユニバーサル オブジェクトをプロビジョニングするための管理者要件

NSX ユニバーサル オブジェクトを使用する場合、Cross-vCenter NSX 環境でマシンをプロビジョニングするには、NSX コンピュート マネージャがプライマリ ロールを持っている vCenter Server にプロビジョニングする必要があります。

Cross-vCenter NSX for vSphere 環境では、複数の vCenter Server を設定できます。各 vCenter Server は、それぞれの NSX Manager とペアリングされている必要があります。1 つの NSX Manager にプライマリ NSX Manager のロールが割り当てられ、その他の NSX Manager にセカンダリ NSX Manager のロールが割り当てられます。

プライマリ NSX Manager は、ユニバーサル論理スイッチなどのユニバーサル オブジェクトを作成できます。これらのオブジェクトは、セカンダリ NSX Manager に同期されます。セカンダリ NSX Manager では、これらのオブジェクトを表示できますが、編集することはできません。ユニバーサル オブジェクトを管理するには、プライマリ NSX Manager を使用する必要があります。プライマリ NSX Manager を使用して、環境内の任意のセカンダリ NSX Manager を設定できます。

NSX Cross-vCenter 環境の詳細については、[NSX for vSphere 製品のドキュメント](#)にある『NSX 管理ガイド』で、「Cross-vCenter Networking and Security の概要」を参照してください。

プライマリ NSX Manager の NSX エンドポイントに関連付けられている vSphere (vCenter Server) エンドポイントについては、vRealize Automation では、ローカルの論理スイッチ、ローカルの Edge Gateway、およびローカルのロード バランサ、セキュリティ グループ、およびセキュリティ タグなどの NSX ローカル オブジェクトをサポートします。ユニバーサル トランスポート ゾーンを使用した 1 対 1 および 1 対多の NAT ネットワーク、ユニバーサル トランスポート ゾーンおよびユニバーサル分散論理ルーター (DLR) を使用したルーティング ネットワーク、任意のタイプのネットワークを使用したロード バランサもサポートされています。

vRealize Automation では、NSX の既存およびオンデマンドのユニバーサル セキュリティ グループまたはタグがサポートされません。

ローカルのオンデマンド ネットワークをプライマリ NSX Manager としてプロビジョニングするには、vCenter Server 固有のローカル トランスポート ゾーンを使用します。vRealize Automation 予約を設定して、ローカル vCenter Server での展開にローカル トランスポート ゾーンおよび仮想ワイヤを使用することができます。

vSphere (vCenter Server) エンドポイントを、対応するセカンダリ NSX Manager エンドポイントに接続する場合、ローカル オブジェクトのみをプロビジョニングおよび使用できます。

vRealize Automation では、外部ネットワークとして NSX ユニバーサル論理スイッチを使用できます。ユニバーサル スイッチを使用する場合は、展開に含まれる各マシンによって、このデータが収集された後、このスイッチが接続、使用されます。

- ユニバーサル トランスポート ゾーンに、オンデマンド ネットワークをプロビジョニングすると、新しいユニバーサル論理スイッチを作成できます。
- プライマリ NSX Manager 上のユニバーサル トランスポート ゾーンにオンデマンド ネットワークをプロビジョニングすると、ユニバーサル論理スイッチが作成されます。

- セカンダリ NSX Manager 上のユニバーサル トランスポート ゾーンにオンデマンド ネットワークをプロビジョニングすると失敗します。これは、NSX では、セカンダリ NSX Manager 上にユニバーサル論理スイッチを作成できないためです。

NSX ユニバーサル オブジェクトの詳細については、VMware ナレッジベースの記事「Deployment of vRealize Automation blueprints with NSX objects fail (KB2147240)」を参照してください。この記事は、<http://kb.vmware.com/kb/2147240> で参照できます。

サードパーティ製 IP アドレス管理プロバイダ サポートを提供するためのチェックリスト

ネットワーク プロファイル定義で使用する IP アドレスおよび範囲は、サポートされているサードパーティ製 IP アドレス管理プロバイダ（Infoblox など）から取得できます。

vRealize Automation ネットワーク プロファイルの外部 IP アドレス管理プロバイダ エンドポイントを作成して使用するには、最初に vRealize Orchestrator IP アドレス管理プロバイダ プラグインまたはパッケージをダウンロード、または他の方法で入手し、vRealize Orchestrator でそのプラグインまたはパッケージをインポートして、必要なワークフローを実行する必要があります。次に、IP アドレス管理ソリューションを vRealize Automation エンドポイントとして登録する必要があります。

可能な IP アドレスの範囲を提供する外部 IP アドレス管理プロバイダを使用する際のプロビジョニング プロセスの概要については、[サードパーティ製 IP アドレス管理プロバイダを使用した vRealize Automation 環境のプロビジョニング](#)を参照してください。

表 1-3. 外部 IP アドレス管理プロバイダ サポートの準備に関するチェックリスト

タスク	説明	詳細
<input type="checkbox"/> サポートされる外部 IP アドレス管理プロバイダ vRealize Orchestrator プラグインを入手してインポートする。	<p>VMware Solution Exchange (https://solutionexchange.vmware.com/store/category_groups/cloud-management) から、vRealize Orchestrator 用 Infoblox IP アドレス管理プロバイダ プラグインや関連ドキュメントなど、IP アドレス管理プロバイダ プラグインまたはパッケージをダウンロードし、そのプラグインまたはパッケージを vRealize Orchestrator にインポートします。</p> <p>必要な IP アドレス管理プロバイダ パッケージが VMware Solution Exchange に存在しない場合は、サードパーティ製 IP アドレス管理ソリューション プロバイダの SDK と関連ドキュメントを使用して独自に作成できます。</p> <p>vRealize Automation バージョン固有のサードパーティ製 IP アドレス管理ソリューション プロバイダの SDK、vRealize Orchestrator と vRealize Automation に関連するスタータ パッケージは、https://code.vmware.com/sdks または https://code.vmware.com/samples から入手できます。</p>	<p>サードパーティ製 IP アドレス管理プロバイダ パッケージの入手、および vRealize Orchestrator へのインポートを参照してください。</p>
<input type="checkbox"/> 必要な設定ワークフローを実行し、外部 IP アドレス管理ソリューションを vRealize Automation エンドポイントとして登録する。	<p>vRealize Orchestrator 設定ワークフローを実行し、vRealize Orchestrator で IP アドレス管理プロバイダ エンドポイント タイプを登録します。</p>	<p>vRealize Orchestrator でサードパーティ製 IP アドレス管理エンドポイント タイプを登録するワークフローの実行を参照してください。</p>

サードパーティ製 IP アドレス管理プロバイダ パッケージの入手、および vRealize Orchestrator へのインポート

サードパーティ製 IP アドレス管理プロバイダ エンドポイントを定義して使用するための準備として、まずサードパーティ製 IP アドレス管理プロバイダ パッケージを入手し、それを vRealize Orchestrator にインポートする必要があります。

既存のサードパーティ製 IP アドレス管理プロバイダ プラグイン（Infoblox IP アドレス管理など）をダウンロードして使用することが可能です。また、VMware が提供するスタータ パッケージとそれに付属の SDK ドキュメントを使用して、BlueCat などの別のサードパーティ製 IP アドレス管理ソリューション プロバイダで使用するサードパーティ製 IP アドレス管理プラグインやパッケージを独自に作成することも可能です。

- marketplace.vmware.com から、既存の [Infoblox IPAM Plug-in for vRealize Orchestrator](#) と関連ドキュメントを入手します。また、ダウンロードには、プラグインのインストールと使用に関するドキュメントも含まれます。
- サードパーティ製 IP アドレス管理ソリューション プロバイダの SDK、関連ドキュメント、vRealize Orchestrator と vRealize Automation に関連するスタータ パッケージを入手して使用し、独自のサードパーティ製 IP アドレス管理ソリューションを作成します。code.vmware.com/web/sdk の [vRealize Automation のサードパーティ IP アドレス管理パッケージの例](#)を参照してください。

サードパーティ製 IP アドレス管理プロバイダ プラグインまたはパッケージを vRealize Orchestrator にインポートしたら、必要なワークフローを実行し、IP アドレス管理エンドポイント タイプを vRealize Orchestrator に登録します。

プラグインとパッケージのインポート、および vRealize Orchestrator ワークフローの実行の詳細については、『VMware vRealize Orchestrator クライアントの使用』を参照してください。vRealize Orchestrator のプラグイン、パッケージ、およびワークフローで vRealize Automation を拡張する方法の詳細については、『ライフ サイクルの拡張性』を参照してください。

この一連の手順では、例として Infoblox IP アドレス管理プラグインを使用します。手順は、vRealize Automation またはプラグインのバージョンによって異なる場合があります。

前提条件

- marketplace.vmware.com からパッケージまたはプラグインをダウンロードします。
- vRealize Orchestrator プラグインまたはパッケージのインポート、構成、および登録を行うために、管理者特権で vRealize Orchestrator にログインします。

手順

- 1 marketplace.vmware.com サイトを開きます。
- 2 プラグインまたはパッケージを探して、ダウンロードします。

たとえば、サードパーティ製 Infoblox IP アドレス管理エンドポイントをサポートする Infoblox プラグインを vRealize Orchestrator および vRealize Automation 7.1 以降にインポートします。

- a [発行者] カテゴリで [Infoblox] を選択し、[適用] をクリックします。
- b [vRealize Orchestrator 用 Infoblox プラグイン](#)を選択します。
- c [Tech Specs] をクリックして、前提条件を確認します。

- d [試行] をクリックすると、追加情報を確認し、ダウンロードのリンクを含む E メールを受信できます。
- e Eメールの指示に従って、zip ファイルをダウンロードします。

バージョン 4.0 以降のプラグインは vRealize Automation 7.1 以降をサポートしています。zip ファイルには、プラグインに関するドキュメントも含まれます。

- 3 vRealize Orchestrator で、[管理者] タブをクリックし、[パッケージのインポート] をクリックします。
- 4 インポートするパッケージを選択します。
- 5 すべてのワークフローとアーティファクトを選択し、[選択した要素のインポート] をクリックします。

次のステップ

[vRealize Orchestrator でサードパーティ製 IP アドレス管理エンドポイント タイプを登録するワークフローの実行。](#)

vRealize Orchestrator でサードパーティ製 IP アドレス管理エンドポイント タイプを登録するワークフローの実行

vRealize Automation によるサードパーティ製 IP アドレス管理プロバイダの使用をサポートし、vRealize Automation で使用される IP アドレス管理エンドポイント タイプを登録するために、vRealize Orchestrator で登録ワークフローを実行します。

前提条件

- [サードパーティ製 IP アドレス管理プロバイダ パッケージの入手、および vRealize Orchestrator へのインポート](#)
- 登録ワークフローの実行権限を使用して vRealize Orchestrator にログインしていることを確認します。
- 登録ワークフローのプロンプトが表示されたら vRealize Automation 管理者の認証情報を入力できるように、準備をします。vRealize Orchestrator に IP アドレス管理エンドポイントのタイプを登録する場合は、vRealize Automation 管理者の認証情報の入力を求められます。

手順

- 1 vRealize Orchestrator で [設計] タブをクリックし、[管理者] - [ライブラリ] を選択した後、[IP アドレス管理サービス パッケージ SDK] を選択します。

各 IP アドレス管理プロバイダ パッケージには、固有の名前が付いており、固有のワークフローが含まれています。各プロバイダは、独自の登録ワークフローを提供しています。各プロパティ パッケージのワークフロー名は似ていることがありますが、vRealize Orchestrator でのワークフローの場所は異なる場合があります。この場所は、プロバイダごとに設定されています。
- 2 この例では、Register IPAM Endpoint 登録ワークフローを実行し、IP アドレス管理 Infloblox エンドポイント タイプを指定します。

- 3** vRealize Automation 認証情報のプロンプトで、ファブリック管理者の認証情報などの vRealize Automation 管理者の認証情報を入力します。

vRealize Automation システム管理者の認証情報を使用して登録ワークフローを指定する必要があります。システム管理者以外のユーザーが vRealize Orchestrator クライアントにログインしている場合でも、vRealize Automation システム管理者の認証情報をワークフローに提供すると、登録は成功します。

結果

この例では、パッケージは vRealize Automation エンドポイント サービスで Infoblox を新しい IP アドレス管理 エンドポイント タイプとして登録します。これにより、ユーザーが vRealize Automation でエンドポイントを作成または編集するときに、そのエンドポイント タイプが使用可能になります。

注： vRealize Orchestrator コントロール センターで vRealize Orchestrator サーバを再起動した後に、Infoblox IP アドレス管理接続が vRealize Orchestrator の [インベントリ] タブから消える場合があります。この問題を解決するには、[vRO 管理] - [ライブラリ] - [Infoblox] - [vRA] - [ヘルパー] メニューの順に選択して、Create IPAM Connection ワークフローを実行します。次に、vRealize Orchestrator の [インベントリ] タブに移動して [Infoblox IP アドレス管理] を選択し、ページを更新すると、Infoblox IP アドレス管理接続が表示されます。

次のステップ

以上で、IP アドレス管理 Infoblox タイプのエンドポイントと、vRealize Automation で登録したすべてのサードパーティ製パッケージまたはプラグイン用のエンドポイントを作成できるようになりました。[サードパーティの IP アドレス管理プロバイダ エンドポイントの作成](#)を参照してください。

構成のチェックリスト vRealize Automation のコンテナ

コンテナの使用を開始するにあたっては、vRealize Automation のユーザー ロールをサポートするための機能を構成する必要があります。

コンテナ でコンテナの定義を構成した後、ブループリントでコンテナのコンポーネントを追加して構成することができます。

表 1-4. 構成のチェックリスト vRealize Automation のコンテナ

タスク	詳細
コンテナ管理者ロールとコンテナ アーキテクト ロールを割り当てる。	『基盤と概念』でコンテナのロールに関する情報を参照してください。
vRealize Automation の [コンテナ] タブでコンテナの定義を指定する。	『vRealize Automation の構成』を参照してください。
vRealize Automation の [設計] タブでコンテナ コンポーネントとコンテナ ネットワーク コンポーネントをブループリントに追加する。	『vRealize Automation の構成』を参照してください。

vRealize Automation アプライアンスを使用した コンテナ の構成

Xenon サービスの情報には、vRealize AutomationvRealize Automation アプライアンスからアクセスできます ([vRA 設定] - [Xenon])。

ここには、Xenon ホスト仮想マシン、待機ポート、サービス ステータスが表示されます。クラスタ化された Xenon ノードに関する情報も、ここに表示されます。

Xenon Linux サービスは、vRealize Automation アプライアンスから以下の CLI コマンドで管理できます。

Command	説明
service xenon-service status	サービスのステータス（実行中または停止）を表示します。
service xenon-service start	サービスを起動します。
service xenon-service stop	サービスを停止します。
service xenon-service restart	サービスを再起動します。
service xenon-service get_host	サービスが実行されているホストの名前を表示します。
service xenon-service get_port	サービス ポートを表示します。
service xenon-service status_cluster	クラスタ化されているすべてのノードを JSON 形式で表示します。
service xenon-service reset	Xenon のすべての構成ファイルが格納されているディレクトリを削除し、サービスを再起動します。

コンテナのクラスタリング

Xenon サービスを vRealize Automation のコンテナ と連携させることでノードをクラスタに参加させることができます。ノードがクラスタ化されている場合、Xenon サービスがその開始時に他のノードを自動的に接続します。

クラスタのステータスは、vRealize Automation アプライアンスの [Xenon] タブで監視できるほか、CLI から以下のコマンド実行することによって監視することもできます。

```
service xenon-service status_cluster
```

Xenon ではクォーラム ベースのクラスタリングが使用されます。クォーラムは、 $(\text{number of nodes} / 2) + 1$ という式を使って計算されます。

vRealize Automation 用の vCloud Director 環境の準備

vCloud Director を vRealize Automation と統合する前に、vCloud Director インスタンスをインストールして構成し、vSphere とクラウド リソースを設定します。その後、適切な認証情報を指定するか、または作成して vRealize Automation が vCloud Director 環境にアクセスできるようにします。

環境の構成

仮想データセンターやネットワークなどの、vSphere リソースおよびクラウド リソースを構成します。詳細については、『vCloud Director』のドキュメントを参照してください。

統合に必要な認証情報

vRealize Automation IaaS 管理者が vCloud Director 環境をエンドポイントとして vRealize Automation の管理下に置くために使用する、組織管理者またはシステム管理者の認証情報を作成するか、または指定します。

ユーザー ロールの考慮事項

組織の vCloud Director ユーザー ロールは、vRealize Automation ビジネス グループのロールと対応している必要はありません。vCloud Director にユーザー アカウントが存在しない場合、vCloud Director により、関連付けられた LDAP または Active Directory でルックアップが実行され、ID ストアにユーザーが存在していれば、アカウントが作成されます。ユーザー アカウントを作成できない場合、警告がログ記録されますが、プロビジョニング プロセスは失敗しません。次に、プロビジョニングされたマシンは、vCloud Director エンドポイントを構成するために使用されたアカウントに割り当てられます。

vCloud Director のユーザー管理の関連情報については、vCloud Director ドキュメントを参照してください。

vRealize Automation 用の vCloud Air 環境の準備

vCloud Air を vRealize Automation と統合する前に、vCloud Air アカウントを登録、vCloud Air 環境を設定し、適切な認証情報を指定または作成して vRealize Automation が環境にアクセスできるようにする必要があります。

環境の構成

vCloud Air ドキュメントの指示に従って環境を構成します。

統合に必要な認証情報

vRealize Automation Iaas 管理者が vCloud Air 環境をエンドポイントとして vRealize Automation 管理下に置くために使用できる、仮想インフラストラクチャ管理者またはアカウント管理者の認証情報を作成または指定します。

ユーザー ロールの考慮事項

組織の vCloud Air ユーザー ロールは、vRealize Automation ビジネス グループのロールと対応している必要はありません。vCloud Air のユーザー管理の関連情報については、vCloud Air ドキュメントを参照してください。

Amazon AWS 環境の準備

Amazon AWS 環境で要素およびユーザー ロールを準備し、Amazon AWS がゲスト エージェントおよびソフトウェア ブートストラップ エージェントと通信するように準備し、Amazon AWS 機能が vRealize Automation の機能にどのようにマップされているか把握します。

vRealize Automation に必要な Amazon AWS ユーザー ロールと認証情報

vRealize Automation が環境を管理するために必要な権限を持つ認証情報を、Amazon AWS で設定する必要があります。

vRealize Automation では、エンドポイント認証情報のアクセス キーが必要です。ユーザー名とパスワードによる認証はサポートしていません。

- Amazon Web Services におけるロールと権限

AWS の Power User ロールは、AWS Directory Service のユーザーまたはグループに、AWS サービス およびリソースに対するフル アクセス権を与えますが、これは必要ありません。下位の権限を持つユーザー ロールもサポートされます。vRealize Automation 機能のニーズを満たす AWS セキュリティ ポリシーは次のとおりです。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeImages",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeVolumes",

      "ec2:DescribeVpcAttribute",
      "ec2:DescribeAddresses",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeImageAttribute",
      "ec2:DescribeInstanceAttribute",
      "ec2:DescribeVolumeStatus",
      "ec2:DescribeVpnConnections",
      "ec2:DescribeRegions",
      "ec2:DescribeTags",
      "ec2:DescribeVolumeAttribute",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeNetworkInterfaceAttribute",

      "ec2:DisassociateAddress",
      "ec2:GetPasswordData",

      "ec2:ImportKeyPair",
      "ec2:ImportVolume",

      "ec2:CreateVolume",
      "ec2>DeleteVolume",
      "ec2:AttachVolume",
      "ec2:ModifyVolumeAttribute",
      "ec2:DetachVolume",

      "ec2:AssignPrivateIpAddresses",
      "ec2:UnassignPrivateIpAddresses",

      "ec2:CreateKeyPair",
      "ec2>DeleteKeyPair",

      "ec2:CreateTags",
      "ec2:AssociateAddress",
      "ec2:ReportInstanceStatus",
      "ec2:StartInstances",
      "ec2:StopInstances",
```



```

        "ec2:ModifyInstanceAttribute",
        "ec2:MonitorInstances",
        "ec2:RebootInstances",
        "ec2:RunInstances",
        "ec2:TerminateInstances",

        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeInstanceHealth"
    ],
    "Resource": "*"
}
}]

```

■ Amazon Web Services の認証情報

Amazon Identity and Access Management (IAM) ユーザーとグループを管理するには、AWS フル アクセス管理者認証情報を使用するように設定されている必要があります。

vRA で AWS エンドポイントを作成するときは、キーとプライベート キーを入力するように求められます。Amazon エンドポイントを作成するために必要なアクセス キーを取得するには、管理者が AWS フル アクセス管理者認証情報を持つユーザーからキーを申請するか、AWS フル アクセス管理者ポリシーで追加構成される必要があります。 [Amazon エンドポイントの作成](#)を参照してください。

ポリシーとロールを有効化するための詳細については、Amazon Web Services 製品ドキュメントの「AWS Identity and Access Management (IAM)」のセクションを参照してください。

Amazon AWS による ソフトウェア ブートストラップ エージェントとゲスト エージェントとの通信を許可する

ソフトウェアを含むアプリケーション ブループリントをプロビジョニングする場合、またはゲスト エージェントを使用してプロビジョニングしたマシンをさらにカスタマイズする機能を希望する場合、マシンがプロビジョニングされる Amazon AWS 環境と、エージェントがパッケージをダウンロードして命令を受け取る vRealize Automation 環境との間の接続を有効にする必要があります。

vRealize Automation を使用して、vRealize Automation ゲスト エージェントと ソフトウェア ブートストラップ エージェントで Amazon AWS マシンをプロビジョニングする場合、プロビジョニングしたマシンが vRealize Automation に通信を戻してマシンをカスタマイズできるように、ネットワークと Amazon との間の VPC 接続を設定する必要があります。

Amazon AWS VPC 接続オプションの詳細については、Amazon AWS のドキュメントを参照してください。

オプションの Amazon 機能の使用

vRealize Automation では、Amazon Virtual Private Cloud、Elastic ロード バランサー、Elastic IP アドレス、Elastic Block ストレージなどの、いくつかの Amazon 機能がサポートされています。

Amazon のセキュリティ グループの使用

Amazon の予約を作成するときに、1 つ以上のセキュリティ グループを指定します。使用可能な各リージョンには、少なくとも 1 つのセキュリティ グループが指定されている必要があります。

セキュリティ グループは、マシンへのアクセスを制御するファイアウォールとして機能します。各リージョンには、最低 1 つのデフォルトのセキュリティ グループが用意されています。管理者は Amazon Web Services Management Console を使用して、追加のセキュリティ グループの作成、Microsoft Remote Desktop Protocol または SSH のポートの構成、Amazon VPN の仮想プライベート ネットワークの設定を行うことができます。

Amazon の予約を作成したり、ブループリントのマシン コンポーネントを構成するときは、指定された Amazon アカウントのリージョンで使用可能なセキュリティ グループのリストから選択できます。セキュリティ グループは、データ収集時にインポートされます。

Amazon Web Services でのセキュリティ グループの作成と使用に関する詳細については、Amazon のドキュメントを参照してください。

Amazon Web Service のリージョンについて

Amazon Web Services の各アカウントは、クラウド エンドポイントとして表示されます。vRealize Automation に Amazon Elastic Cloud Computing エンドポイントを作成する際に、コンピュート リソースとしてリージョンが収集されます。IaaS 管理者がビジネス グループのコンピュート リソースを選択した後、インベントリおよび状態データの収集が自動的に実行されます。

1 日に 1 回自動的に実行されるインベントリ データの収集では、コンピュート リソース上に存在するものに関するデータが収集されます。収集されるデータの例を以下に示します。

- Elastic IP アドレス
- Elastic ロード バランサ
- Amazon Elastic Block ストレージ ボリューム

状態データの収集は、デフォルトでは、15 分ごとに自動的に実行されます。管理対象インスタンス（vRealize Automation によって作成されたインスタンス）の状態に関する情報が収集されます。以下に、状態データの例を示します。

- Windows パスワード
- ロード バランサ内のマシンの状態
- Elastic IP アドレス

ファブリック管理者は、インベントリ データの収集と状態データの収集の起動、両データ収集の無効化、収集の頻度の変更を実行できます。

Amazon Virtual Private Cloud の使用

Amazon Virtual Private Cloud を使用すると、Amazon Web Services クラウドのプライベート セクションで、Amazon マシン インスタンスをプロビジョニングできます。

Amazon Web Services ユーザーは、Amazon VPC を使用して、仕様に応じた仮想ネットワーク トポロジを設計できます。vRealize Automation で Amazon VPC を割り当てることができます。ただし vRealize Automation は、Amazon VPC の使用コストを追跡しません。

Amazon VPC を使用してプロビジョニングする場合、vRealize Automation は、Amazon がプライマリ IP アドレスを取得する VPC サブネットが存在することを想定します。このアドレスは、インスタンスが終了するまで変更されません。Elastic IP プールを使用して、Elastic IP アドレスを vRealize Automation 内のインスタンスに割り当てることもできます。これによりユーザーは、Amazon Web Services でインスタンスが継続的にプロビジョニングおよび分解される場合に、同じ IP を維持できます。

AWS Management Console を使用して、次の要素を作成します。

- Amazon VPC。インターネット ゲートウェイ、ルーティング テーブル、セキュリティ グループとサブネット、および使用可能な IP アドレスを含みます。
- Amazon Virtual Private Network。ユーザーが AWS Management Console の外部で Amazon マシン インスタンスにログインする必要がある場合。

vRealize Automation ユーザーは、Amazon VPC を使用するとき、次のタスクを実行できます。

- ファブリック管理者は、Amazon VPC をクラウド予約に割り当てることができます。[Amazon EC2 の予約の作成](#)を参照してください。
- マシン所有者は、Amazon マシン インスタンスを Amazon VPC に割り当てることができます。

Amazon VPC の作成の詳細については、Amazon Web Services のドキュメントを参照してください。

Amazon Web Services の Elastic ロード バランサーの使用

Elastic ロード バランサーは、受信アプリケーション トラフィックを Amazon Web Services インスタンス全体に分散させます。Amazon ロード バランシングを使用すると、フォールト トレランスとパフォーマンスが向上します。

Amazon では、Amazon EC2 ブループリントを使用してプロビジョニングされたマシンで Elastic ロード バランシングを使用できます。

Elastic ロード バランサーは、Amazon Web Services、Amazon Virtual Private Network、およびプロビジョニングの場所で使用できる必要があります。たとえば、ロード バランサーが us-east1c で使用でき、マシンの場所が us-east1b である場合、マシンは使用可能なロード バランサーを使用できません。

vRealize Automation は、Elastic ロード バランサーを作成、管理、または監視しません。

Amazon Web Services Management Console を使用して Amazon Elastic ロード バランサーを作成する方法については、Amazon Web Services のドキュメントを参照してください。

Amazon Web Services の Elastic IP アドレスの使用

Elastic IP アドレスを使用すると、動的な Amazon Web Services クラウド環境内で他のマシンにすばやくフェイルオーバーできます。vRealize Automation では、リージョンに対する権限を持つすべてのビジネス グループが Elastic IP アドレスを使用できます。

管理者は、AWS Management Console を使用して、Elastic IP アドレスを Amazon Web Services アカウントに割り当てることができます。任意のリージョンに Elastic IP アドレスのグループが 2 つあり、1 つは Amazon VPC 以外のインスタンス用、もう 1 つは Amazon VPC 用として割り当てられています。Amazon VPC 以外のリージョンにのみアドレスを割り当てた場合、アドレスは Amazon VPC で使用できません。その逆も同じです。アドレスを Amazon VPC にのみ割り当てると、アドレスは Amazon VPC 以外のリージョンで利用できません。

Elastic IP アドレスを、特定のマシンではなく、Amazon Web Services アカウントに関連付けられますが、このアドレスを使用できるのは 1 度に 1 台のマシンのみです。アドレスは、解放されるまで、Amazon Web Services アカウントに関連付けられたままになります。アドレスを開放し、そのアドレスを特定のマシン インスタンスにマッピングできます。

IaaS アーキテクトは、ブループリントにカスタム プロパティを追加し、プロビジョニング中に Elastic IP アドレスをマシンに割り当てることができます。マシンの所有者および管理者は、マシンに割り当てた Elastic IP アドレスを表示できます。さらに、マシンの編集権限を持っている場合は、プロビジョニング後に Elastic IP アドレスを割り当てることもできます。ただし、アドレスがすでにマシン インスタンスに関連付けられ、マシン インスタンスが Amazon Virtual Private Cloud 展開に属している場合、Amazon はアドレスを割り当てません。

Amazon Elastic IP アドレスの作成と使用に関する詳細については、Amazon Web Services のドキュメントを参照してください。

Amazon Web Services の Elastic Block ストレージの使用

Amazon Elastic Block ストレージは、Amazon マシン インスタンスと Amazon Virtual Private Cloud で使用するためのブロック レベルのストレージ ボリュームを提供します。ストレージ ボリュームは、Amazon Web Services クラウド環境内の関連付けられた Amazon マシン インスタンスの有効期限を超えても持続できます。

Amazon Elastic Block ストレージ ボリュームを vRealize Automation と併用する場合は、以下の考慮事項が適用されます。

- マシン インスタンスをプロビジョニングするとき、既存の Elastic Block ストレージ ボリュームは接続できません。ただし、新規ボリュームを作成し、一度に複数のマシンを申請する場合は、ボリュームが作成され各インスタンスに接続されます。たとえば volume_1 という名前のボリュームを 1 つ作成し、3 台のマシンを申請する場合、各マシンに 1 つのボリュームが作成されます。volume_1 という名前の 3 つのボリュームが作成され、各マシンに接続されます。各ボリュームには、一意のボリューム ID が割り当てられます。各ボリュームはサイズが同じで、同じ場所に配置されます。
- ボリュームのオペレーティング システムと場所は、ボリュームを接続するマシンと同じでなければなりません。
- vRealize Automation は、Elastic Block ストレージがサポートするインスタンスのプライマリ ボリュームを管理しません。

Amazon Elastic Block ストレージの詳細、および Amazon Web Services Management Console を使用してそのストレージを有効化する方法の詳細については、Amazon Web Services のドキュメントを参照してください。

事前検証 (POC) 環境でネットワークと Amazon との間に VPC 接続を構成

vRealize Automation を評価する環境をセットアップする IT プロフェッショナルとして、vRealize Automation ソフトウェア 機能をサポートするようにネットワークと Amazon との間の VPC 接続を一時的に構成しようと思います。

ネットワークと Amazon との間の VPC 接続が必要になるのは、ゲスト エージェントを使用してプロビジョニングするマシンをカスタマイズする場合、またはブループリントに ソフトウェア コンポーネントを含める場合のみです。本番環境では Amazon Web Services を経由して正式にこの接続を構成します。ここでは事前検証 (POC) 環境で作業しているため、一時的に Amazon VPC ネットワーク接続を作成します。SSH トンネルを確立し、vRealize Automation で Amazon 予約を構成してトンネルを通るようにします。

前提条件

- TunnelGroup と呼ばれる Amazon AWS セキュリティ グループを作成し、ポート 22 にアクセスできるように構成します。
- Amazon AWS TunnelGroup セキュリティ グループ内の CentOS マシンを作成または特定し、次の構成内容を書き留めます。
 - 管理ユーザー認証情報 (*root* など)。
 - パブリック IP アドレス。
 - プライベート IP アドレス。
- vRealize Automation のインストールと同一のローカル ネットワーク上に CentOS マシンを作成および特定します。
- トンネル マシンの両方に OpenSSH SSHD サーバをインストールします。

手順

- 1 root または同様のユーザーとして Amazon AWS トンネル マシンにログインします。
- 2 iptables を無効にします。

```
# service iptables save
# service iptables stop
# chkconfig iptables off
```

- 3 /etc/ssh/sshd_config を編集し、AllowTCPForwarding および GatewayPorts を有効にします。
- 4 サービスを再起動します。

```
/etc/init.d/sshd restart
```

- 5 vRealize Automation のインストールと同一のローカル ネットワーク上にある CentOS マシンに root ユーザーとしてログインします。
- 6 ローカル ネットワーク マシンと Amazon AWS トンネル マシンとの SSH トンネルを起動します。

```
ssh -N -v -o "ServerAliveInterval 30" -o "ServerAliveCountMax 40" -o "TCPKeepAlive yes" \
```

```
-R 1442:vRealize_automation_appliance_fqdn:5480 \  
-R 1443:vRealize_automation_appliance_fqdn:443 \  
-R 1444:manager_service_fqdn:443 \  
User of Amazon tunnel machine@Public IP Address of Amazon tunnel machine
```

Amazon AWS トンネル マシンから vRealize Automation リソースにアクセスできるようにポート転送を構成しましたが、トンネルを通るように Amazon 予約を構成するまで SSH トンネルは機能しません。

次のステップ

- 1 ソフトウェア ブートストラップ エージェントとゲスト エージェントを Windows または Linux リファレンス マシンにインストールし、IaaS アーキテクトがブループリント作成に使用できる Amazon マシン イメージを作成します。 [ソフトウェア プロビジョニングの準備](#)を参照してください。
- 2 vRealize Automation で Amazon 予約を構成して、SSH トンネルを通るようにします。 [シナリオ：概念実証の環境用の Amazon 予約の作成](#)を参照してください。

Red Hat OpenStack のネットワークとセキュリティの機能の準備

vRealize Automation では、セキュリティ グループや浮動 IP アドレスなどのいくつかの機能を OpenStack でサポートしています。これらの機能を vRealize Automation で使用し、お使いの環境で構成する方法について説明します。

OpenStack セキュリティ グループの使用

セキュリティ グループを使用すると、特定のポートに対するネットワーク トラフィックを制御するためのルールを指定できます。

マシンを要求するときに予約のセキュリティ グループを指定することができます。また、デザイン キャンパスで既存またはオンデマンドの NSX セキュリティ グループを指定することもできます。

セキュリティ グループは、データ収集時にインポートされます。

使用可能な各リージョンには、少なくとも 1 つのセキュリティ グループが指定されている必要があります。予約を作成する際には、そのリージョン内でユーザーが使用可能なセキュリティ グループが表示されます。各リージョンには、最低 1 つのデフォルトのセキュリティ グループが用意されています。

追加のセキュリティ グループは、ソース リソースで管理する必要があります。各種マシンでのセキュリティ グループの管理方法の詳細については、OpenStack のドキュメントを参照してください。

OpenStack での浮動 IP アドレスの使用

OpenStack で実行中の仮想インスタンスには、浮動 IP アドレスを割り当てることができます。

浮動 IP アドレスを割り当てることができるようにするには、Red Hat OpenStack で IP 転送を構成し、浮動 IP プールを作成する必要があります。詳細については、『Red Hat OpenStack』ドキュメントを参照してください。

マシン所有者に対して、[浮動 IP の関連付け] アクションと [浮動 IP の関連付け解除] アクションの資格を付与することができます。その後、資格付与されたユーザーは、浮動 IP アドレス プールから使用可能なアドレスを選択することにより、マシンに接続されている外部ネットワークから、プロビジョニングされたマシンに浮動 IP アドレスを関連付けることができます。浮動 IP アドレスをマシンと関連付けた後、vRealize Automation ユーザーは、[浮動 IP の関連付け解除] オプションを選択して現在割り当てられている浮動 IP アドレスを表示し、マシンからアドレスの関連付けを解除することができます。

SCVMM 環境の準備

vRealize Automation マシンのプロビジョニングに使用する SCVMM テンプレートとハードウェア プロファイルの作成を開始する前に、テンプレート名とハードウェア プロファイル名の命名に関する制限を把握した上で、SCVMM ネットワークおよびストレージ設定を構成します。

環境の準備に関する情報については、『vRealize Automation のインストール』に記載されている SCVMM の要件を参照してください。

マシンのプロビジョニングに関する情報については、[Hyper-V \(SCVMM\) エンドポイントの作成](#)を参照してください。

vRealize Automation は SCVMM のプライベート クラウドの構成を使用する展開環境をサポートしていません。vRealize Automation では現在、SCVMM プライベート クラウドに対してデータ収集、割り当て、プロビジョニングを行うことはできません。

テンプレートとハードウェア プロファイルの命名

SCVMM および vRealize Automation には、テンプレートおよびハードウェア プロファイルに使用される命名規則があるため、テンプレート名またはハードウェア プロファイル名を temporary または profile という単語で始めてはなりません。たとえば、次の用語はデータ収集の際に無視されます。

- TemporaryTemplate
- Temporary Template
- TemporaryProfile
- Temporary Profile
- プロファイル

SCVMM クラスタの必須ネットワーク構成

SCVMM クラスタでは、仮想ネットワークを vRealize Automation のみに公開するため、仮想ネットワークと論理ネットワークの間に 1:1 の関係が必要です。SCVMM コンソールを使用して、各論理ネットワークを仮想ネットワークにマッピングし、仮想ネットワーク経由でマシンにアクセスするよう SCVMM クラスタを構成してください。

SCVMM クラスタの必須ストレージ構成

SCVMM Hyper-V クラスタ上では、共有ボリュームについてのみ、vRealize Automation によりデータの収集およびプロビジョニングが行われます。SCVMM コンソールを使用して、ストレージの共有リソース ボリュームを使用するようにクラスタを構成してください。

スタンドアロン SCVMM ホストの必須ストレージ構成

スタンドアロンの SCVMM ホストの場合、vRealize Automation はデータを収集し、デフォルトの仮想マシンパスにプロビジョニングします。SCVMM コンソールを使用して、スタンドアロン ホストのデフォルトの仮想マシンパスを設定してください。

ネットワークと Azure 間の VPC 接続の設定

Azure ブループリントにソフトウェア コンポーネントを使用する場合は、ネットワークと Azure 間の接続を設定する必要があります。

前提条件

- TunnelGroup と呼ばれる Azure セキュリティ グループを作成し、ポート 22 にアクセスできるように設定します。
- Azure TunnelGroup セキュリティ グループ内の CentOS マシンなどのマシンを作成または特定し、次の設定内容を書き留めます。
 - 管理ユーザー認証情報 (*root* など)。
 - パブリック IP アドレス。
 - プライベート IP アドレス。
- vRealize Automation のインストールと同一のローカル ネットワーク上に CentOS マシンを作成および特定します。
- トンネル マシンの両方に OpenSSH SSHD サーバをインストールします。

手順

- 1 root または同等のユーザーとして Azure トンネル マシンにログインします。
- 2 iptables を無効にします。

```
# service iptables save
# service iptables stop
# chkconfig iptables off
```

- 3 /etc/ssh/sshd_config を編集し、AllowTCPForwarding および GatewayPorts を有効にします。
- 4 サービスを再起動します。

```
/etc/init.d/sshd restart
```

- 5 vRealize Automation のインストールと同一のローカル ネットワーク上にある CentOS マシンに root ユーザーとしてログインします。
- 6 ローカル ネットワーク マシンと Azure トンネル マシンとの SSH トンネルを起動します。

```
ssh -N -v -o "ServerAliveInterval 30" -o "ServerAliveCountMax 40" -o "TCPKeepAlive yes" \
```



```
-R 1442:vRealize_automation_appliance_fqdn:5480 \  
-R 1443:vRealize_automation_appliance_fqdn:443 \  
-R 1444:manager_service_fqdn:443 \  
User of Azure tunnel machine@Public IP Address of Azure tunnel machine
```

Azure トンネル マシンから vRealize Automation リソースにアクセスできるようにポート転送を設定しても、トンネルを通るように Azure 予約を設定するまで SSH トンネルは機能しません。

次のステップ

- 1 ソフトウェア ブートストラップ エージェントとゲスト エージェントを Windows または Linux リファレンス マシンにインストールし、IaaS アーキテクトがブループリント作成に使用できる Azure マシン イメージを作成します。 [ソフトウェア プロビジョニングの準備](#)を参照してください。
- 2 vRealize Automation で Azure 予約を設定して、SSH トンネルを通るようにします。 [Microsoft Azure の予約の作成](#)を参照してください。

マシン プロビジョニングの準備

ご使用の環境およびマシン プロビジョニングの方法によっては、vRealize Automation の外部要素の設定が必要になる場合があります。

たとえば、マシン テンプレートやマシン イメージの構成が必要になる場合があります。

また、NSX 設定の構成や vRealize Orchestrator ワークフローの実行が必要になる場合もあります。

マシンのプロビジョニングの準備中にポートを指定する場合の関連情報については、[vRealize Automation 製品ドキュメント](#)の「リファレンス アーキテクチャ PDF」を参照してください。

準備するマシン プロビジョニング方法の選択

ほとんどのマシン プロビジョニング方法では、vRealize Automation の外部にいくつかの要素を準備する必要があります。

表 1-5. 準備するマシン プロビジョニング方法の選択

シナリオ	サポートされるエンドポイント	エージェント サポート	プロビジョニング方法	プロビジョニング前の準備作業
マシン プロビジョニング前またはプロビジョニング後に、マシン ライフ サイクルの追加手順としてカスタムの Visual Basic スクリプトを実行するよう vRealize Automation を構成する。たとえば、プロビジョニング前のスクリプトを使用して、プロビジョニング前に証明書またはセキュリティ トークンを生成し、マシン プロビジョニング後、プロビジョニング後のスクリプトで証明書およびトークンを使用できます。	Amazon AWS を除く サポートされるすべてのエンドポイントで Visual Basic スクリプトを実行できます。	選択するプロビジョニング方法によります。	任意のプロビジョニング方法で追加手順としてサポートされますが、Amazon AWS マシンで Visual Basic スクリプトを使用することはできません。	プロビジョニング時に Visual Basic スクリプトを実行するためのチェックリスト
Oracle、MySQL、WAR、データベース スキーマなどのミドルウェアおよびアプリケーション展開コンポーネントのインストール、構成、およびライフ サイクル管理を自動化するアプリケーションブループリントをプロビジョニングする。	<ul style="list-style-type: none"> ■ vSphere ■ vCloud Air ■ vCloud Director ■ Amazon AWS 	<ul style="list-style-type: none"> ■ (必須) ゲスト エージェント ■ (必須) ソフトウェア ブートストラップ エージェントおよびゲスト エージェント 	<ul style="list-style-type: none"> ■ クローン作成 ■ クローン作成 (vCloud Air または vCloud Director の場合) ■ リンク クローン ■ Amazon マシン イメージ 	ブループリントで ソフトウェア コンポーネントを使用する場合、ゲスト エージェントと ソフトウェア ブートストラップ エージェントをサポートするプロビジョニング方法を準備します。ソフトウェアの準備の詳細については、 ソフトウェア プロビジョニングの準備 を参照してください。
ゲスト エージェントを使用してプロビジョニングした後にマシンをさらにカスタマイズする。	すべての仮想エンドポイントおよび Amazon AWS。	<ul style="list-style-type: none"> ■ (必須) ゲスト エージェント ■ (オプション) ソフトウェア ブートストラップ エージェントおよびゲスト エージェント 	仮想マシン イメージを除くすべてのプロビジョニング方法でサポートされます。	プロビジョニング後にマシンをカスタマイズする場合、ゲスト エージェントをサポートするプロビジョニング方法を選択します。
ゲスト OS を使用せずにマシンをプロビジョニングします。プロビジョニング後にオペレーティング システムをインストールできます。	すべての仮想マシン エンドポイント。	サポートされません	基本	vRealize Automation 以外でプロビジョニング前に行う必要がある準備作業はありません。

表 1-5. 準備するマシン プロビジョニング方法の選択 (続き)

シナリオ	サポートされるエンドポイント	エージェント サポート	プロビジョニング方法	プロビジョニング前の準備作業
リンク クローンと呼ばれる仮想マシンの容量を効率的に利用したコピーをプロビジョニングします。リンク クローンは、仮想マシンのスナップショットに基づいており、差分ディスクのチェーンを使用して親のマシンとの差異を記録します。	vSphere	<ul style="list-style-type: none"> ■ (オプション) ゲスト エージェント ■ (オプション) ソフトウェア ブートストラップ エージェントおよびゲスト エージェント 	リンク クローン	<p>既存の vSphere 仮想マシンが必要です。</p> <p>ソフトウェア をサポートする場合は、クローンを作成するマシンにゲスト エージェントとソフトウェア ブートストラップ エージェントをインストールする必要があります。</p> <p>ブループリントで識別された仮想マシン スナップショットは、リンク クローン仮想マシンのプロビジョニング前にパワーオフされている必要があります。</p>
Net App FlexClone テクノロジーを使用して、仮想マシンの容量を効率的に利用したコピーをプロビジョニングします。	vSphere	(オプション) ゲスト エージェント	NetApp FlexClone	クローン作成によるプロビジョニングの準備のためのチェックリスト を参照してください。
リファレンス マシンと呼ばれる既存の Windows や Linux マシンおよびカスタマイズ オブジェクトから作成したテンプレート オブジェクトのクローンを作成することで、マシンをプロビジョニングします。	<ul style="list-style-type: none"> ■ vSphere ■ KVM (RHEV) ■ SCVMM 	<ul style="list-style-type: none"> ■ (オプション) ゲスト エージェント ■ (vSphere のみのオプション) ソフトウェア ブートストラップ エージェントおよびゲスト エージェント 	クローン作成	<p>クローン作成によるプロビジョニングの準備のためのチェックリストを参照してください。</p> <p>ソフトウェア をサポートする場合は、クローンを作成する vSphere マシンにゲスト エージェントとソフトウェア ブートストラップ エージェントをインストールする必要があります。</p>
テンプレートとカスタマイズ オブジェクトからクローンを作成することで vCloud Air または vCloud Director マシンをプロビジョニングする。	<ul style="list-style-type: none"> ■ vCloud Air ■ vCloud Director 	<ul style="list-style-type: none"> ■ (オプション) ゲスト エージェント ■ (オプション) ソフトウェア ブートストラップ エージェントおよびゲスト エージェント 	vCloud Air または vCloud Director クローン作成	<p>vCloud Air および vCloud Director のプロビジョニングの準備を参照してください。</p> <p>ソフトウェア をサポートする場合、ゲスト エージェントとソフトウェア ブートストラップ エージェントを含むテンプレートを作成します。vCloud Air では、vRealize Automation 環境と vCloud Air 環境間のネットワーク接続を構成します。</p>
マシンへのオペレーティングシステムのインストールのために、キックスタートまたは autoYaST 構成ファイルおよび Linux 配布イメージを使用し、ISO イメージから起動することでマシンをプロビジョニングします。	<ul style="list-style-type: none"> ■ すべての仮想エンドポイント ■ Red Hat OpenStack 	ゲスト エージェントは準備手順の一部としてインストールされます。	Linux キックスタート	Linux キックスタート プロビジョニングの準備

表 1-5. 準備するマシン プロビジョニング方法の選択 (続き)

シナリオ	サポートされるエンドポイント	エージェント サポート	プロビジョニング方法	プロビジョニング前の準備作業
マシンをプロビジョニングし、ISO イメージからの起動のために SCCM タスク シーケンスへ制御を渡して、Windows オペレーティング システムを展開し、vRealize Automation ゲスト エージェントをインストールします。	すべての仮想マシン エンドポイント。	ゲスト エージェントは準備手順の一部としてインストールされます。	SCCM	SCCM プロビジョニングの準備
既存の Windows リファレンス マシンの Windows Imaging File Format (WIM) イメージを使用して、WinPE 環境で起動したり、オペレーティング システムをインストールすることでマシンをプロビジョニングします。	<ul style="list-style-type: none"> ■ すべての仮想エンドポイント ■ Red Hat OpenStack 	ゲスト エージェントは必須です。WinPE イメージを作成する場合は、ゲスト エージェントを手動で挿入する必要があります。	WIM	WIM プロビジョニングの準備
仮想マシン イメージからインスタンスを起動します。	Red Hat OpenStack	サポートされません	仮想マシン イメージ	仮想マシン イメージ プロビジョニングの準備 を参照してください。
Amazon マシン イメージからインスタンスを起動します。	Amazon AWS	<ul style="list-style-type: none"> ■ (オプション) ゲスト エージェント ■ (オプション) ソフトウェア ブートストラップ エージェントおよびゲスト エージェント 	Amazon マシン イメージ	Amazon マシン イメージとインスタンス タイプを Amazon AWS アカウントと関連付けます。 ソフトウェア をサポートする場合、ゲスト エージェントとソフトウェア ブートストラップ エージェントを含む Amazon マシン イメージを作成し、Amazon AWS と vRealize Automation の環境間に VPC へのネットワーク接続を構成します。

プロビジョニング時に Visual Basic スクリプトを実行するためのチェックリスト

マシン プロビジョニング前またはプロビジョニング後に、マシン ライフサイクルの追加手順としてカスタムの Visual Basic スクリプトを実行するよう vRealize Automation を構成できます。たとえば、プロビジョニング前のスクリプトを使用して、プロビジョニング前に証明書またはセキュリティ トークンを生成し、マシン プロビジョニング後、プロビジョニング後のスクリプトで証明書およびトークンを使用できます。Visual Basic スクリプトは任意のプロビジョニング方法で実行できますが、Amazon AWS マシンで Visual Basic スクリプトを使用することはできません。

表 1-6. プロビジョニング時に Visual Basic スクリプトを実行するためのチェックリスト

タスク	場所	詳細
❑ Visual Basic スクリプトの EPI エージェントをインストールおよび構成する。	通常は Manager Service ホスト	『vRealize Automation のインストール』を参照してください。
❑ Visual Basic スクリプトを作成する。	EPI エージェントがインストールされたマシン	<p>vRealize Automation には、EPI エージェントのインストール ディレクトリのサブディレクトリ <code>Scripts</code> に、サンプル Visual Basic スクリプト <code>PrePostProvisioningExample.vbs</code> が用意されています。このスクリプトには、ディレクトリにすべての引数をロードするヘッダー、関数を追加できる本文、アップデートしたカスタム プロパティを vRealize Automation に返すためのフッターが含まれます。</p> <p>Visual Basic スクリプトを実行する場合、EPI エージェントはすべてのマシン カスタム プロパティを引数としてスクリプトに渡すことができます。アップデートされたプロパティ値を vRealize Automation に返すには、ディクショナリにそれらのプロパティを設定して、vRealize Automation によって提供されている関数を呼び出します。</p>
❑ スクリプトをブループリントに含めるために必要な情報を収集する。	<p>情報を取得してインフラストラクチャ アーキテクトに転送します</p> <p>注: ファブリック管理者は、プロパティ セット <code>ExternalPreProvisioningVbScript</code> および <code>ExternalPostProvisioningVbScript</code> を使用してプロパティ グループを作成し、この必要な情報を提供できます。これにより、ブループリント アーキテクトは、ブループリントに情報を正しく簡単に追加できるようになります。</p>	<ul style="list-style-type: none"> ■ ファイル名と拡張子を含む、Visual Basic スクリプトへの完全パス。たとえば、<code>%System Drive%Program Files (x86)\VMware\VCAC Agents\EPI_Agents\Scripts\SendEmail.vbs</code> と入力します。 ■ プロビジョニング前にスクリプトを実行するには、カスタム プロパティ <code>ExternalPreProvisioningVbScript</code> の値としてスクリプトへの完全なパスを入力するよう、インフラストラクチャ アーキテクトに指示します。プロビジョニング後にスクリプトを実行するには、カスタム プロパティ <code>ExternalPostProvisioningVbScript</code> を使用する必要があります。

プロビジョニングでの vRealize Automation ゲスト エージェントの使用

リファレンス マシンにゲスト エージェントをインストールすると、展開後にマシンをさらにカスタマイズできます。予約されたゲスト エージェントのカスタム プロパティを使用して、ディスクの追加やフォーマットなどの基本的なカスタマイズを実行できます。またプロビジョニングされたマシンのゲスト OS 内でゲスト エージェントが実行する独自のカスタム スクリプトを作成することもできます。

展開が完了し、カスタマイズ仕様が実行された後で（カスタマイズ仕様を提供した場合）、ゲスト エージェントは、展開されたマシンのすべてのカスタム プロパティを含む XML ファイル (c:\VRMGuestAgent\site\workitem.xml) を作成し、ゲスト エージェントのカスタム プロパティを使用して、割り当てられているタスクを完了します。その後、プロビジョニングされたマシンからゲスト エージェント自体を削除します。

展開されたマシンでゲスト エージェントが実行する独自のカスタム スクリプトを作成し、マシン ブループリントのカスタム プロパティを使用して、そのスクリプトの場所とスクリプトが実行される順番を指定できます。マシン ブループリントのカスタム プロパティを使用すると、カスタム プロパティ値をパラメータとしてスクリプトに渡すこともできます。

たとえば、ゲスト エージェントを使用して、展開されたマシン上で次のカスタマイズを行うことができます。

- IP アドレスの変更
- ドライブの追加またはフォーマット
- セキュリティ スクリプトの実行
- 別のエージェント（Puppet や Chef など）の初期化

コマンド ライン引数では暗号化された文字列をカスタム プロパティとして指定することもできます。これにより、ゲスト エージェントが復号化して有効なコマンド ライン引数として認識可能な、暗号化された情報を格納できます。

注： Linux ゲスト エージェントは、Linux キックスタートと PXE プロビジョニングの作成時およびクローニング時に、作業アイテムの vRealize Automation のカスタム プロパティに関連して固定 IP アドレスを割り当てます。ゲスト エージェントは固定 IP アドレスを割り当てる際、Ubuntu 16.x などの新しい一貫したネットワーク命名スキームに対応できません。

カスタム スクリプトはマシンにローカルにインストールする必要はありません。プロビジョニングされたマシンがスクリプトの場所にネットワーク アクセスできる限り、ゲスト エージェントはスクリプトにアクセスして実行できます。これによりテンプレートをすべて再構築しなくてもスクリプトをアップデートできるため、メンテナンス コストが低減されます。

セキュリティ設定を指定するには、予約、ブループリント、またはゲスト エージェント スクリプトで情報を指定します。プロビジョニングするマシンにゲスト エージェントが必要な場合は、その要件を含んだセキュリティ ルールを予約またはブループリントに追加する必要があります。たとえば、すべてのマシン間の通信を拒否するデフォルトのセキュリティ ポリシーを使用したうえで、特定のマシン間の通信を許可するためのセキュリティ ポリシーを別途設けた場合、カスタマイズ段階でゲスト エージェントが vRealize Automation と通信できなくなる可能性があります。このような問題がマシンのプロビジョニング中に発生しないようにするためには、カスタマイズ段階で通信を許可するデフォルトのセキュリティ ポリシーを使用します。

プロビジョニングされたマシンにカスタム スクリプトを実行するゲスト エージェントをインストールする場合は、該当するゲスト エージェントのカスタム プロパティがブループリントに含まれている必要があります。たとえば、クローン作成用のテンプレートにゲスト エージェントをインストールし、プロビジョニングされたマシンの IP アドレスを変更するカスタム スクリプトを作成して、そのスクリプトを共有された場所に配置する場合は、多くのカスタム プロパティをブループリントに含める必要があります。

表 1-7. ゲスト エージェントを使用して、プロビジョニングされたマシンの IP アドレスを変更するためのカスタム プロパティ

カスタム プロパティ	説明
VirtualMachine.Admin.UseGuestAgent	プロビジョニングされたマシンの開始時にゲスト エージェントを初期化する場合は、 true に設定します。
VirtualMachine.Customize.WaitComplete	すべてのカスタマイズが完了するまで、プロビジョニング ワークフローで作業アイテムがゲスト エージェントに送信されないようにする場合は、True に設定します。カスタマイズが完了する前に作業アイテムを作成できるようにするには、False に設定します。

表 1-7. ゲスト エージェントを使用して、プロビジョニングされたマシンの IP アドレスを変更するためのカスタム プロパティ （続き）

カスタム プロパティ	説明
VirtualMachine.SoftwareN.ScriptPath	<p>アプリケーションのインストール スクリプトへの完全パスを指定します。このパスは、ゲスト OS で参照される有効な絶対パスにする必要があります。また、スクリプト ファイル名が含まれている必要があります。</p> <p>パスの文字列に {CustomPropertyName} を挿入することで、カスタム プロパティ値をパラメータとしてスクリプトに渡すことができます。たとえば、名前が ActivationKey で値が 1234 のカスタム プロパティがある場合、スクリプト パスは、D:\InstallApp.bat -key {ActivationKey} となります。ゲスト エージェントはコマンド D:\InstallApp.bat -key 1234 を実行します。その後、この値を受け入れて使用するようにスクリプト ファイルをプログラムできます。</p> <p>マシン所有者名をスクリプトに渡すには、{Owner} を挿入します。</p> <p>また、パスの文字列に {YourCustomProperty} を挿入すると、カスタム プロパティ値をパラメータとしてスクリプトに渡すことができます。たとえば、値</p> <p>\\vra-scripts.mycompany.com\scripts\changeIP.bat を入力すると、共有された場所から changeIP.bat スクリプトが実行されますが、値</p> <p>\\vra-scripts.mycompany.com\scripts\changeIP.bat {VirtualMachine.Network0.Address} を入力すると、changeIP スクリプトが実行され、さらに VirtualMachine.Network0.Address プロパティ値がパラメータとしてスクリプトに渡されます。</p>
VirtualMachine.ScriptPath.Decrypt	<p>適切にフォーマットされた VirtualMachine.SoftwareN.ScriptPath カスタム プロパティ ステートメントとして gagent コマンドラインに渡される暗号化文字列を vRealize Automation が取得できるようにします。</p> <p>パスワードなどの暗号化文字列をコマンドライン引数のカスタム プロパティとして指定することができます。これにより、ゲスト エージェントによる復号化が可能で、有効なコマンドライン引数として認識される、暗号化された情報を格納できます。たとえば、</p> <p>VirtualMachine.Software0.ScriptPath = c:\dosomething.bat <i>password</i> カスタム プロパティ文字列は、実際のパスワードを含むため、安全ではありません。</p> <p>パスワードを暗号化するには、vRealize Automation カスタム プロパティ（たとえば、MyPassword = password）を作成し、チェック ボックスを選択して暗号化を有効にします。ゲスト エージェントは、[MyPassword] エントリをカスタム プロパティ MyPassword の値に復号化し、このスクリプトを c:\dosomething.bat password として実行します。</p> <ul style="list-style-type: none"> ■ カスタム プロパティ MyPassword = password を作成します。ここで、<i>password</i> は、実際のパスワードの値です。チェック ボックスを選択して暗号化を有効にします。 ■ カスタム プロパティ VirtualMachine.ScriptPath.Decrypt を VirtualMachine.ScriptPath.Decrypt = true として設定します。

表 1-7. ゲスト エージェントを使用して、プロビジョニングされたマシンの IP アドレスを変更するためのカスタム プロパティ （続き）

カスタム プロパティ	説明
	<ul style="list-style-type: none"> ■ カスタム プロパティ VirtualMachine.Software0.ScriptPath を VirtualMachine.Software0.ScriptPath = c:\dosomething.bat [MyPassword] として設定します。 VirtualMachine.ScriptPath.Decrypt を false に設定した場合、または VirtualMachine.ScriptPath.Decrypt カスタム プロパティを作成しない場合、角かっこ ([および]) 内の文字列は復号化されません。

ゲスト エージェントで利用できるカスタム プロパティの詳細については、カスタム プロパティのリファレンスを参照してください。

サーバを信頼するゲスト エージェントの構成

サーバを信頼するようにゲスト エージェントを構成する最も安全な方法は、vRealize Automation Manager Service Host のパブリック キーの PEM ファイルを正しいゲスト エージェント フォルダにインストールすることです。

以下に示したのは各テンプレートのゲスト エージェント フォルダの場所です。ここに Manager Service Host の PEM ファイル (cert.pem) をインストールすることによってサーバを信頼します。

- gugent を使用する各テンプレートの Windows ゲスト エージェント フォルダ

```
C:\VRMGuestAgent\cert.pem
```

- gugent を使用する各テンプレートの Linux ゲスト エージェント フォルダ

```
/usr/share/gugent/cert.pem
```

この場所に cert.pem ファイルを置かなかった場合、テンプレートのリファレンス マシンがゲスト エージェントを使用できません。たとえば、スクリプトを変更することによって仮想マシンの起動後にパブリック キーの情報を収集しようとした場合、セキュリティ条件の違反となります。

ご利用の環境の構成によっては、さらに別の考慮事項があります。

- WIM インストールの場合、パブリック キーの PEM ファイルの内容をコンソールの実行可能プログラムとユーザー インターフェイスに追加する必要があります。コンソール フラグは [/cert filename] 形式で指定します。
- RedHat キックスタート インストールの場合、パブリック キーをコピーしてサンプル ファイルに貼り付ける必要があります。それ以外の場合、ゲスト エージェントの実行に失敗します。
- SCCM インストールの場合、cert.pem ファイルが VRMGuestAgent フォルダに格納されている必要があります。

- Linux vSphere インストールの場合、`cert.pem` ファイルが `/usr/share/gugent` フォルダに格納されている必要があります。

注： ソフトウェアとゲスト エージェントと一緒にインストールすることもできます。その場合は、以下のスクリプトを <https://APPLIANCE/software/index.html> からダウンロードしてください。テンプレートを作成する際、SSL 証明書のフィンガープリントの受け入れをこのスクリプトで処理できます。

- Linux

```
prepare_vra_template.sh
```

- Windows

```
prepare_vra_template.ps1
```

ソフトウェアとゲスト エージェントと一緒にインストールした場合、[Linux リファレンス マシンへのゲスト エージェントのインストール](#) や [Windows リファレンス マシンへのゲスト エージェントのインストール](#) の手順を実行する必要があります。

Manager Service ホストから `cert.pem` ファイルを取得する方法

- 1 Manager Service ホストで、管理ツールに移動し、Internet Information Services (IIS) マネージャを開きます。
- 2 左側のツリーで、Manager Service ホストを強調表示します。
- 3 右側で、サーバ証明書を開きます。
- 4 [発行先] が VMware vRA で [発行元] が VMware vRA である証明書を探します。
- 5 その証明書を右クリックし、エクスポートします。
- 6 保存される証明書は PFX 形式になります。PEM に変換するには、コマンドラインで OpenSSL を使用します。

```
openssl pkcs12 -in filename.pfx -out cert.pem -nodes
```

Linux リファレンス マシンへのゲスト エージェントのインストール

リファレンス マシンに Linux ゲスト エージェントをインストールして、展開後にマシンをさらにカスタマイズします。

前提条件

- リファレンス マシンの指定または作成を行います。
- ダウンロードするゲスト エージェント ファイルには、`tar.gz` と RPM の両方のパッケージ形式が含まれています。使用しているオペレーティング システムで `tar.gz` または RPM ファイルをインストールできない場合は、変換ツールを使用してインストール ファイルを適切なパッケージ形式に変換します。
- ゲスト エージェントとマネージャ サービス マシンの間のセキュアな信頼を確立します。[サーバを信頼するゲスト エージェントの構成](#)を参照してください。

手順

- 1 vRealize Automation アプライアンス管理コンソールのページに移動します。

たとえば、`https://va-hostname.domain.com` です。

- 2 ページの vRealize Automation コンポーネントのインストール セクションにある [ゲストおよびソフトウェアのエージェント ページ] をクリックします。

たとえば、`https://va-hostname.domain.com/software/index.html` です。

[ゲストおよびソフトウェアのエージェント インストーラ] ページが開き、利用可能なダウンロードへのリンクが表示されます。

- 3 ページのゲスト エージェント インストーラ セクションにある [Linux ゲスト エージェント パッケージ] をクリックして、`LinuxGuestAgentPkgs.zip` ファイルをダウンロードして保存します。

- 4 ダウンロードした `LinuxGuestAgentPkgs.zip` ファイルを解凍して、`VraLinuxGuestAgent` フォルダを作成します。

- 5 プロビジョニング中に展開するゲスト OS に対応するゲスト エージェント パッケージをインストールします。

- a プロビジョニング中に展開するゲスト OS に対応する `VraLinuxGuestAgent` サブディレクトリに移動します (たとえば、`rhel32`)。

- b 適切なパッケージ形式を見つけるか、パッケージを適切なパッケージ形式に変換します。

- c リファレンス マシンにゲスト エージェント パッケージをインストールします。

たとえば、RPM パッケージからのファイルをインストールするには、`rpm -i gugent-gugent-7.1.0-4201531.i386.rpm` を実行します。

- 6 `installgugent.sh Manager_Service_Hostname_fdqn:portnumber ssl platform` を実行して Manager Service と通信できるように、ゲスト エージェントを構成します。

Manager Service のデフォルト ポート番号は 443 です。受け入れられるプラットフォームの値は `ec2`、`vcd`、`vca`、および `vsphere` です。

オプション	説明
ロード バランサを使用している場合	Manager Service ロード バランサの完全修飾ドメイン名とポートを入力します。例 : <pre>cd /usr/share/gugent ./installgugent.sh load_balancer_manager_service.mycompany.com:443 ssl ec2</pre>
ロード バランサがない場合	Manager Service マシンの完全修飾ドメイン名とポートを入力します。例 : <pre>cd /usr/share/gugent ./installgugent.sh manager_service_machine.mycompany.com:443 ssl vsphere</pre>

- 7 展開したマシンが、Manager Service の SSL 証明書を信頼するようにまだ構成されていない場合は、リファレンス マシンに `cert.pem` ファイルをインストールして信頼関係を確立する必要があります。

- より安全な手段としては、`cert.pem` 証明書を取得し、リファレンス マシンに手動でそのファイルをインストールします。

- より便利な手段としては、Manager Service ロード バランサまたは Manager Service マシンに接続して、cert.pem 証明書をダウンロードすることができます。

オプション	説明
ロード バランサを使用している場合	リファレンス マシンの root ユーザーとして、次のコマンドを実行します。 <pre>echo openssl s_client -connect manager_service_load_balancer.mycompany.com:443 sed -ne '/- BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > cert.pem</pre>
ロード バランサがない場合	リファレンス マシンの root ユーザーとして、次のコマンドを実行します。 <pre>echo openssl s_client -connect manager_service_machine.mycompany.com:443 sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > cert.pem</pre>

- 8 Ubuntu オペレーティング システムにゲスト エージェントをインストールする場合は、次のコマンド セットのいずれかを実行することにより、共有オブジェクトのシンボリック リンクを作成します。

オプション	説明
64 ビット システム	<pre>cd /lib/x86_64-linux-gnu sudo ln -s libssl.so.1.0.0 libssl.so.10 sudo ln -s libcrypto.so.1.0.0 libcrypto.so.10</pre>
32 ビット システム	<pre>cd /lib/i386-linux-gnu sudo ln -s libssl.so.1.0.0 libssl.so.10 sudo ln -s libcrypto.so.1.0.0 libcrypto.so.10</pre>

次のステップ

リファレンス マシンをクローン作成用、Amazon マシン イメージ用、または IaaS アーキテクトがブループリントの作成に使用できるスナップショット用にテンプレートに変換します。

Windows リファレンス マシンへのゲスト エージェントのインストール

Windows サービスとして実行する vRealize Automation Windows ゲスト エージェントを Windows リファレンス マシンにインストールし、マシンの詳細カスタマイズを有効にします。

前提条件

- リファレンス マシンの指定または作成を行います。
- ゲスト エージェントとマネージャ サービス マシンの間のセキュアな信頼を確立します。[サーバを信頼するゲスト エージェントの構成](#)を参照してください。

手順

- 1 次の URL を使用して、vRealize Automation アプライアンスの [ゲストおよびソフトウェア エージェントのインストーラ] ページに移動します。

<https://vrealize-automation-appliance-FQDN/software>

- 2 [ゲスト エージェントのインストーラ] で 32 ビットまたは 64 ビットの実行ファイルをダウンロードして、C: ドライブのルートに保存します。

注： ゲスト エージェントをインストールするためのこの手順には、コマンドラインを使用する代替方法があります。実行可能ファイルをダウンロードする代わりに、[ゲストおよびソフトウェア エージェントのインストーラ] ページの [Windows Software Installers] に移動します。ここで、`prepare_vra_template.ps1` PowerShell スクリプトをダウンロードして実行できます。

```
PowerShell -NoProfile -ExecutionPolicy Bypass -Command prepare_vra_template.ps1
```

- 3 実行ファイルを実行して、Windows ゲスト エージェント ファイルを抽出します。

抽出すると、C:\VRMGuestAgent が作成され、ファイルが追加されます。

C:\VRMGuestAgent の名前を変更しないでください。

- 4 Manager Service と通信するようにゲスト エージェントを構成します。

- a 管理者権限のコマンド プロンプトを開きます。
- b C:\VRMGuestAgent に移動します。
- c 信頼する Manager Service の PEM ファイルを C:\VRMGuestAgent\ ディレクトリに配置し、Manager Service マシンを信頼するように、ゲスト エージェントを設定します。
- d `win service -i -h Manager_Service_Hostname_fdqn:portnumber -p ssl` を実行します。

Manager Service のデフォルト ポート番号は 443 です。

オプション	説明
ロード バランサを使用している場合	Manager Service ロード バランサの完全修飾ドメイン名とポートを入力します。たとえば、 <code>win service -i -h load_balancer_manager_service.mycompany.com:443 -p ssl</code> と入力します。
ロード バランサがない場合	Manager Service マシンの完全修飾ドメイン名とポートを入力します。たとえば、 <code>win service -i -h manager_service_machine.mycompany.com:443 -p ssl</code> と入力します。
Amazon マシン イメージを準備する場合、	Amazon を使用していることを指定する必要があります。たとえば、 <code>win service -i -h manager_service_machine.mycompany.com:443:443 -p ssl -c ec2</code> と指定します。

結果

Windows サービスの名前は VCACGuestAgentService です。インストール ログ VCAC-GuestAgentService.log は、C:\VRMGuestAgent に配置されています。

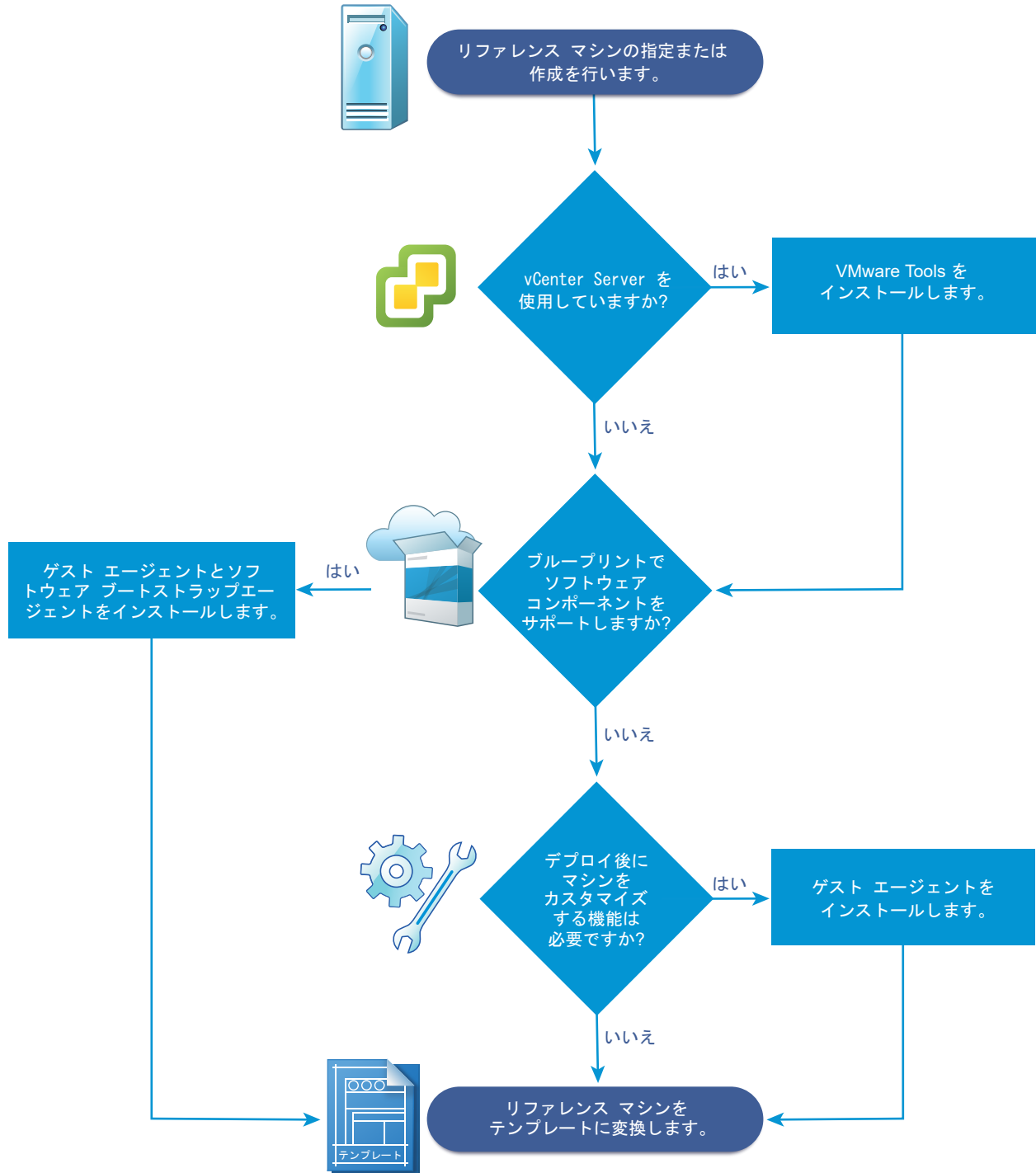
次のステップ

リファレンス マシンをクローン作成用、Amazon マシン イメージ用、またはスナップショット用のテンプレートに変換して、IaaS アーキテクトがブループリントの作成に使用できるようにします。

クローン作成によるプロビジョニングの準備のためのチェックリスト

vRealize Automation の外部で一部の準備を行って、Linux および Windows 仮想マシンのクローン作成に使用するテンプレートおよびカスタマイズ オブジェクトを作成する必要があります。

クローン作成には、リファレンス マシンから作成された、クローン元のテンプレートが必要です。



クローン作成により Windows マシンをプロビジョニングする場合、プロビジョニングされたマシンを Active Directory ドメインに追加する唯一の方法は、vCenter Server のカスタム仕様を使用するか、SCVMM テンプレートでゲスト OS プロファイルを追加することです。クローン作成によりプロビジョニングされるマシンは、プロビジョニング時に Active Directory コンテナ内に配置することはできません。これは、プロビジョニング後に手動で実施する必要があります。

表 1-8. クローン作成によるプロビジョニングの準備のためのチェックリスト

タスク	場所	詳細
<input type="checkbox"/> リファレンス マシンを指定または作成します。	ハイパーバイザー	ハイパーバイザーによって提供されるドキュメントを参照してください。
<input type="checkbox"/> (オプション) クローン テンプレートでソフトウェア コンポーネントをサポートする場合は、vRealize Automation ゲスト エージェントおよびソフトウェア ブートストラップ エージェントをリファレンス マシンにインストールします。	リファレンス マシン	Windows リファレンス マシンについては、 Windows リファレンス マシンで ソフトウェア をサポートするための準備 を参照してください。 Linux リファレンス マシンについては、 Linux リファレンス マシンで ソフトウェア をサポートするための準備 を参照してください。
<input type="checkbox"/> (オプション) クローン テンプレートでソフトウェア コンポーネントをサポートする必要があるものの、展開されたマシンをカスタマイズする機能が必要な場合は、vRealize Automation ゲスト エージェントをリファレンス マシンにインストールします。	リファレンス マシン	プロビジョニングでの vRealize Automation ゲスト エージェントの使用 を参照してください。
<input type="checkbox"/> vCenter Server 環境で作業している場合は、VMware Tools をリファレンス マシンにインストールします。	vCenter Server	VMware Tools のドキュメントを参照してください。
<input type="checkbox"/> リファレンス マシンを使用してクローン作成用のテンプレートを作成します。	ハイパーバイザー	リファレンス マシンはパワーオン/オフのいずれでも可能です。vCenter Server でクローンを作成する場合は、テンプレートを作成せずにリファレンス マシンを直接使用できます。 ハイパーバイザーによって提供されるドキュメントを参照してください。
<input type="checkbox"/> カスタマイズ オブジェクトを作成し、System Preparation Utility の情報または Linux のカスタマイズを適用することにより、クローン作成されたマシンを構成します。	ハイパーバイザー	Linux のクローンを作成する場合は、カスタマイズ オブジェクトを作成する代わりに、Linux ゲスト エージェントをインストールし、外部カスタマイズ スクリプトを使用することができます。vCenter Server を使用してクローン作成する場合、カスタマイズ オブジェクトとしてカスタム仕様を提供する必要があります。 ハイパーバイザーによって提供されるドキュメントを参照してください。
<input type="checkbox"/> テンプレートのクローン作成を行うブループリントを作成するために必要な情報を収集します。	情報を取得して IaaS アーキテクチャに転送します。	クローン作成による仮想プロビジョニング用のワークシート を参照してください。

クローン作成による仮想プロビジョニング用のワークシート

環境内に準備したテンプレート用のクローン ブループリントを作成するために必要なテンプレート、カスタマイズ、およびカスタム プロパティに関する情報を取得するため、ナレッジ転送ワークシートを完成させます。この情報のすべてがすべての実装で必要になるわけではありません。このワークシートはガイドとして使用するか、編集用にワークシートの表をコピーしてワード プロセッシング ツールに貼り付けてください。

必要なテンプレートおよび予約情報

表 1-9. テンプレートおよび予約情報のワークシート

必要な情報	値	詳細
テンプレート名		
テンプレートを使用可能な予約、または適用する予約ポリシー		プロビジョニング時のエラーを回避するには、テンプレートがすべての予約で使用可能なことを確認したり、テンプレートが使用可能な予約に対してブループリントを制限するためにアーキテクトが使用できる予約ポリシーを作成したりします。
(vSphere のみ) このテンプレート用に申請されたクローン作成のタイプ		<ul style="list-style-type: none"> ■ クローン作成 ■ リンク クローン ■ NetApp FlexClone
カスタム仕様 の名前 (固定 IP アドレスでのクローン作成に必要)		<p>vSphere カスタム仕様を使用せずに Windows マシンをカスタマイズすることはできません。</p> <p>Linux マシンを Windows Active Directory ドメインに参加させるを参照してください。</p>
(SCVMM のみ) ISO 名		
(SCVMM のみ) 仮想ハード ディスク		
(SCVMM のみ) プロビジョニングされたマシンに添付するハードウェア プロファイル		

必要なプロパティ グループ

ワークシートのカスタム プロパティ情報セクションを完了させることも、個別に多数のカスタム プロパティを作成する代わりにプロパティ グループを作成し、プロパティ グループをブループリントに追加するようアーキテクトに依頼することもできます。

必要な vCenter Server オペレーティング システム

vCenter Server プロビジョニングにゲスト OS カスタム プロパティを指定する必要があります。

表 1-10. vCenter Server オペレーティング システム

カスタム プロパティ	値	説明
VMware.VirtualCenter.OperatingSystem		vCenter Server がマシンの作成時に使用する vCenter Server ゲスト OS のバージョン (VirtualMachineGuestOsIdentifier) を指定します。このオペレーティング システムのバージョンは、プロビジョニングされたマシンにインストールされるオペレーティング システムのバージョンと一致する必要があります。管理者は、いずれかのプロパティ セット (正しい VMware.VirtualCenter.OperatingSystem 値が含まれるように事前定義された VMware[OS_Version]Properties など) を使用してプロパティ グループを作成できます。これは、仮想プロビジョニング用のプロパティです。

Visual Basic スクリプト情報

マシン ライフ サイクルへの追加手順としてカスタム Visual Basic スクリプトを実行するように vRealize Automation を構成した場合、スクリプトに関する情報をブループリントに含める必要があります。

注： ファブリック管理者は、プロパティ セット ExternalPreProvisioningVbScript および ExternalPostProvisioningVbScript を使用してプロパティ グループを作成し、この必要な情報を提供できます。これにより、ブループリント アーキテクトは、ブループリントに情報を正しく簡単に追加できるようになります。

表 1-11. Visual Basic スクリプト情報

カスタム プロパティ	値	説明
ExternalPreProvisioningVbScript		プロビジョニングの前にスクリプトを実行します。ファイル名と拡張子を含むスクリプトへの完全パスを入力します。 <i>%System Drive %Program Files (x86)\VMware\vCAC Agents\EPI_Agents\Scripts \SendEmail.vbs</i>
ExternalPostProvisioningVbScript		プロビジョニングの後にスクリプトを実行します。ファイル名と拡張子を含むスクリプトへの完全パスを入力します。 <i>%System Drive %Program Files (x86)\VMware\vCAC Agents\EPI_Agents\Scripts \SendEmail.vbs</i>

Linux ゲスト エージェント カスタマイズ スクリプト情報

カスタマイズ スクリプトの実行にゲスト エージェントを使用するように Linux テンプレートを構成した場合、スクリプトに関する情報をブループリントに含める必要があります。

表 1-12. Linux ゲスト エージェント カスタマイズ スクリプト情報のワークシート

カスタム プロパティ	値	説明
Linux.ExternalScript.Name		<p>オペレーティング システムがインストールされた後に、Linux ゲスト エージェントが実行するオプションのカスタマイズ スクリプトの名前を指定します (例: config.sh)。このプロパティは、Linux エージェントがインストールされたテンプレートからクローン作成される Linux マシンで使用可能です。</p> <p>外部スクリプトを指定する場合は、Linux.ExternalScript.LocationType プロパティおよび Linux.ExternalScript.Path プロパティを使用して、その場所も定義する必要があります。</p>
Linux.ExternalScript.LocationType		<p>Linux.ExternalScript.Name プロパティで指定されたカスタマイズ スクリプトの場所タイプを指定します。ローカルまたは NFS のいずれかを指定できます。</p> <p>また、Linux.ExternalScript.Path プロパティを使用してスクリプトの場所を指定する必要もあります。場所タイプが NFS の場合は、Linux.ExternalScript.Server プロパティも使用します。</p>
Linux.ExternalScript.Server		Linux.ExternalScript.Name で指定された Linux 外部カスタマイズ スクリプトが配置される NFS サーバの名前を指定します (例: lab-ad.lab.local)。
Linux.ExternalScript.Path		Linux カスタマイズ スクリプトへのローカルパスまたは NFS サーバ上の Linux カスタマイズへのエクスポートパスを指定します。値はスラッシュから始まり、ファイル名は含みません (例: /scripts/linux/config.sh)。

その他のゲスト エージェント カスタム プロパティ

リファレンス マシンにゲスト エージェントをインストールした場合、カスタム プロパティを使用すると、展開後にマシンをさらにカスタマイズできます。

表 1-13. ゲスト エージェントを使用したクローン マシンのカスタマイズに必要なカスタム プロパティのワークシート

カスタム プロパティ	値	説明
VirtualMachine.Admin.AddOwnerToAdmins		VirtualMachine.Admin.Owner プロパティで指定されたマシンの所有者をマシンのローカル管理者グループに追加する場合は、True（デフォルト）に設定します。
VirtualMachine.Admin.AllowLogin		VirtualMachine.Admin.Owner プロパティでの指定に従ってマシン所有者をローカルのリモート デスクトップ ユーザー グループに追加するには、True（デフォルト）に設定します。
VirtualMachine.Admin.UseGuestAgent		クローン作成用テンプレートのサービスとしてゲスト エージェントがインストールされている場合、マシン ブループリントで True に設定すると、そのテンプレートからクローン作成されたマシンのゲスト エージェント サービスが有効になります。マシンを起動すると、ゲスト エージェント サービスが起動します。ゲスト エージェント を無効にする場合は、False に設定します。False に設定すると、拡張クローン ワークフローでゲスト OS タスクにゲスト エージェントが使用されなくなり、機能が VMwareCloneWorkflow に制限されます。指定しない場合、または False 以外に設定した場合、拡張クローン ワークフローからゲスト エージェントに作業アイテムが送信されます。
VirtualMachine.DiskN.Active		マシンのディスク <i>N</i> が有効であることを指定する場合は、True（デフォルト）に設定します。マシンのディスク <i>N</i> が有効ではないことを指定する場合は、False に設定します。
VirtualMachine.DiskN.Label		マシンのディスク <i>N</i> のラベルを指定します。ディスク ラベルの最大文字数は 32 文字です。ディスク番号は連番にする必要があります。ゲスト エージェントに対して使用する場合は、ゲスト OS 内でマシンのディスク <i>N</i> のラベルを指定します。
VirtualMachine.DiskN.Letter		マシンのディスク <i>N</i> のドライブ文字またはマウント ポイントを指定します。デフォルトは C です。たとえば、ディスク 1 に文字 D を指定するには、カスタム プロパティを VirtualMachine.Disk1.Letter として定義し、値として D と入力します。ディスク番号は連番にする必要があります。ゲスト エージェントと組み合わせて使用する場合、ゲスト エージェントは、この値によって指定されたドライブ文字またはマウント ポイントを使用して、追加ディスク <i>N</i> をゲスト OS にマウントします。

表 1-13. ゲスト エージェントを使用したクローン マシンのカスタマイズに必要なカスタム プロパティのワークシート（続き）

カスタム プロパティ	値	説明
VirtualMachine.Admin.CustomizeGuestOSDelay		カスタマイズが完了してからゲスト OS のカスタマイズが開始するまでの待機時間を指定します。値は HH:MM:SS 形式にする必要があります。値が設定されていない場合、デフォルト値は 1 分 (00:01:00) になります。このカスタム プロパティを含めない場合、ゲスト エージェントの作業アイテムが完了する前に仮想マシンが再起動すると、プロビジョニングに失敗する場合があります。
VirtualMachine.Customize.WaitComplete		すべてのカスタマイズが完了するまで、プロビジョニング ワークフローで作業アイテムがゲスト エージェントに送信されないようにする場合は、True に設定します。カスタマイズが完了する前に作業アイテムを作成できるようにするには、False に設定します。
VirtualMachine.SoftwareN.Name		プロビジョニング中にインストールまたは実行するソフトウェア アプリケーション <i>N</i> やスクリプトの分かりやすい名前を指定します。これは、任意の参照専用プロパティです。このプロパティは、拡張クローン ワークフローやゲスト エージェントでは実質的に機能しませんが、ユーザー インターフェイスでカスタム ソフトウェアを選択する場合や、ソフトウェアの使用状況をレポートする場合に役立ちます。
VirtualMachine.SoftwareN.ScriptPath		<p>アプリケーションのインストール スクリプトへの完全パスを指定します。このパスは、ゲスト OS で参照される有効な絶対パスにする必要があります。また、スクリプト ファイル名が含まれている必要があります。</p> <p>パスの文字列に {CustomPropertyName} を挿入することで、カスタム プロパティ値をパラメータとしてスクリプトに渡すことができます。たとえば、名前が ActivationKey で値が 1234 のカスタム プロパティがある場合、スクリプト パスは、D:\InstallApp.bat -key {ActivationKey} となります。ゲスト エージェントはコマンド D:\InstallApp.bat -key 1234 を実行します。その後、この値を受け入れて使用するようにスクリプト ファイルをプログラムできます。</p>

表 1-13. ゲスト エージェントを使用したクローン マシンのカスタマイズに必要なカスタム プロパティのワークシート（続き）

カスタム プロパティ	値	説明
VirtualMachine.SoftwareN.ISOName		データストアのルートに対する ISO ファイルの相対パスおよびファイル名を指定します。形式は <code>/folder_name/subfolder_name/file_name.iso</code> です。値が設定されていない場合、ISO はマウントされません。
VirtualMachine.SoftwareN.ISOLocation		アプリケーションまたはスクリプトで使用する ISO イメージ ファイルが含まれるストレージバスを指定します。ホスト予約で表示されるバスの形式に設定します（例： <code>netapp-1:it_nfs_1</code> ）。値が設定されていない場合、ISO はマウントされません。

カスタム プロパティのネットワーク

カスタム プロパティを使用することで、マシン上の特定のネットワーク デバイスの構成を指定できます。

一般的なネットワーク関連のカスタム プロパティを次の表に挙げます。その他の関連するカスタム プロパティについては、『カスタム プロパティのリファレンス』の「クローン ブループリント用カスタム プロパティ」および「ネットワークのカスタム プロパティ」を参照してください。

表 1-14. ネットワーク設定のカスタム プロパティ

カスタム プロパティ	値	説明
VirtualMachine.NetworkN.Address		固定 IP アドレスを使用してプロビジョニングされるマシンのネットワーク デバイス <i>N</i> の IP アドレスを指定します。
VirtualMachine.NetworkN.MacAddressType		<p>これにより、ネットワーク デバイス <i>N</i> の MAC アドレスが生成されるのか、またはユーザー定義（固定）なのかを指定します。このプロパティは、クローン作成で使用できます。</p> <p>デフォルト値は <code>generated</code> です。値が <code>static</code> の場合は、<code>VirtualMachine.NetworkN.MacAddress</code> を使用して MAC アドレスも指定する必要があります。</p> <p><code>VirtualMachine.NetworkN</code> カスタム プロパティは、個々のブループリントおよびマシンに固有です。マシンが申請されると、マシンが予約に割り当てられる前に、ネットワークおよび IP アドレスの割り当てが実行されます。ブループリントは特定の予約に割り当てられない可能性もあるため、このプロパティを予約で使用しないでください。このプロパティはオンデマンド NAT ネットワークまたはオンデマンド ルーティング ネットワークではサポートされません。</p>

表 1-14. ネットワーク設定のカスタム プロパティ （続き）

カスタム プロパティ	値	説明
VirtualMachine.NetworkN.MacAddress		<p>ネットワーク デバイス <i>N</i> の MAC アドレスを指定します。このプロパティは、クローン作成で使用できます。</p> <p>VirtualMachine.NetworkN.MacAddressType の値が generated の場合、このプロパティには生成されたアドレスが含まれます。</p> <p>VirtualMachine.NetworkN.MacAddressType の値が static の場合は、このプロパティで MAC アドレスを指定します。ESX Server ホストでプロビジョニングされた仮想マシンの場合、アドレスは、VMware で指定された範囲内に収まっている必要があります。詳細については、vSphere のドキュメントを参照してください。</p> <p>VirtualMachine.NetworkN カスタム プロパティは、個々のブループリントおよびマシンに固有です。マシンが申請されると、マシンが予約に割り当てられる前に、ネットワークおよび IP アドレスの割り当てが実行されます。ブループリントは特定の予約に割り当てられない可能性もあるため、このプロパティを予約で使用しないでください。このプロパティはオンデマンド NAT ネットワークまたはオンデマンド ルーティング ネットワークではサポートされません。</p>

表 1-14. ネットワーク設定のカスタム プロパティ （続き）

カスタム プロパティ	値	説明
VirtualMachine.NetworkN.Name		<p>接続先のネットワークの名前、たとえばマシンの接続先のネットワーク デバイス <i>N</i> を指定します。これは、ネットワーク インターフェイス カード (NIC) と同等です。</p> <p>デフォルトの場合、マシンがプロビジョニングされる予約で利用できるネットワーク バスからネットワークが割り当てられます。</p> <p>[VirtualMachine.NetworkN.Address Type] も参照してください。</p> <p>ネットワーク デバイスが確実に特定のネットワークに接続されるようにするには、このプロパティの値を使用可能な予約のネットワーク名に設定します。たとえば、プロパティを <i>N</i> = 0 および <i>N</i> = 1 と指定すると、関連付けられている予約でネットワークが選択されている場合には、2 つの NIC とその割り当て値が得られます。</p> <p>VirtualMachine.NetworkN カスタム プロパティは、ブループリントおよびマシンに固有です。マシンが申請されると、マシンが予約に割り当てられる前に、ネットワークおよび IP アドレスの割り当てが実行されます。ブループリントは特定の予約に割り当てられない可能性もあるため、このプロパティを予約で使わないでください。このプロパティはオンデマンド NAT ネットワークまたはオンデマンド ルーティング ネットワークではサポートされません。</p> <p>このカスタム プロパティを使用して、定義済みの使用可能なネットワークのリストから利用者の選択に基づいて VirtualMachine.Network0.Name を動的に設定する方法の例については、ブログ記事の Adding a Network Selection Drop-Down in vRA 7 を参照してください。</p>
VirtualMachine.NetworkN.PortID		<p>vSphere Distributed Switch で dvPort グループを使用する場合、ネットワーク デバイス <i>N</i> で使用するポート ID を指定します。</p> <p>VirtualMachine.NetworkN カスタム プロパティは、個々のブループリントおよびマシンに固有です。マシンが申請されると、マシンが予約に割り当てられる前に、ネットワークおよび IP アドレスの割り当てが実行されます。ブループリントは特定の予約に割り当てられない可能性もあるため、このプロパティを予約で使わないでください。このプロパティはオンデマンド NAT ネットワークまたはオンデマンド ルーティング ネットワークではサポートされません。</p>

表 1-14. ネットワーク設定のカスタム プロパティ （続き）

カスタム プロパティ	値	説明
VirtualMachine.NetworkN.NetworkProfileName		<p>ネットワーク プロファイルの名前を指定します。このネットワーク プロファイルに基づいて、固定 IP アドレスをネットワーク デバイス <i>N</i> に割り当てたり、クローン作成されたマシンのネットワーク デバイス <i>N</i> に割り当て可能な固定 IP アドレスの範囲を取得したりします。ここで、最初のデバイスでは <i>N</i>=0、2 番目のデバイスは 1、以降同様に指定していきます。</p> <p>プロパティが示すネットワーク プロファイルは、IP アドレスを割り当てるために使用されます。このプロパティにより、マシンの接続先ネットワークが予約に基づいて決定されます。</p>
■ VirtualMachine.NetworkN.SubnetMask		<p>名前を追加すると、複数のバージョンのカスタム プロパティを作成できます。たとえば、次のプロパティでは、一般用途向けに設定されるロード バランシング プールや、高、中、低のパフォーマンス要件があるマシンに設定されるロード バランシング プールを一覧表示できます。</p> <ul style="list-style-type: none"> ■ VCNS.LoadBalancerEdgePool.Names ■ VCNS.LoadBalancerEdgePool.Names.moderate ■ VCNS.LoadBalancerEdgePool.Names.high ■ VCNS.LoadBalancerEdgePool.Names.low <p>VirtualMachine.NetworkN.NetworkProfileName で指定されたネットワーク プロファイルの属性を構成します。</p>
■ VirtualMachine.NetworkN.Gateway		
■ VirtualMachine.NetworkN.PrimaryDns		
■ VirtualMachine.NetworkN.SecondaryDns		
■ VirtualMachine.NetworkN.PrimaryWins		
■ VirtualMachine.NetworkN.SecondaryWins		
■ VirtualMachine.NetworkN.DnsSuffix		
■ VirtualMachine.NetworkN.DnsSearchSuffixes		

表 1-14. ネットワーク設定のカスタム プロパティ （続き）

カスタム プロパティ	値	説明
VCNS.LoadBalancerEdgePool.Names.name		<p>プロビジョニング中に仮想マシンが割り当てられる NSX ロード バランシング プールを指定します。仮想マシンは、指定したすべてのプールの全サービス ポートに割り当てられます。値は <i>edge/pool</i> 名またはコンマで区切られた <i>edge/pool</i> 名のリストになります。名前の大文字と小文字は区別されます。</p> <p>名前を追加すると、複数のバージョンのカスタム プロパティを作成できます。たとえば、次のプロパティでは、一般用途向けに設定されるロード バランシング プールや、高、中、低のパフォーマンス要件があるマシンに設定されるロード バランシング プールを一覧表示できます。</p> <ul style="list-style-type: none"> ■ VCNS.LoadBalancerEdgePool.Names ■ VCNS.LoadBalancerEdgePool.Names.moderate ■ VCNS.LoadBalancerEdgePool.Names.high ■ VCNS.LoadBalancerEdgePool.Names.low

表 1-14. ネットワーク設定のカスタム プロパティ （続き）

カスタム プロパティ	値	説明
VCNS.SecurityGroup.Names. <i>name</i>		<p>プロビジョニング中に仮想マシンが割り当てられる 1 つ以上の NSX セキュリティ グループを指定します。値はセキュリティ グループ名またはコンマで区切られた名前のリストになります。名前の大文字と小文字は区別されます。</p> <p>名前を追加すると、複数のバージョンのプロパティを作成できます。これは、個別に使用することも、組み合わせて使用することもできます。たとえば、次のプロパティでは、一般用途、販売部、およびサポートのためのセキュリティ グループを一覧表示できます。</p> <ul style="list-style-type: none"> ■ VCNS.SecurityGroup.Names ■ VCNS.SecurityGroup.Names.sales ■ VCNS.SecurityGroup.Names.support
VCNS.SecurityTag.Names. <i>name</i>		<p>プロビジョニング中に仮想マシンが関連付けられる 1 つ以上の NSX セキュリティ タグを指定します。この値は、セキュリティ タグの 1 つの名前、またはコンマ区切りの名前のリストです。名前の大文字と小文字は区別されます。</p> <p>名前を追加すると、複数のバージョンのプロパティを作成できます。これは、個別に使用することも、組み合わせて使用することもできます。たとえば、次のプロパティでは、一般用途、販売部、およびサポートのためのセキュリティ タグを一覧表示できます。</p> <ul style="list-style-type: none"> ■ VCNS.SecurityTag.Names ■ VCNS.SecurityTag.Names.sales ■ VCNS.SecurityTag.Names.support

Linux マシンを Windows Active Directory ドメインに参加させる

マシンをプロビジョニングする際に、Linux マシンを Windows Active Directory ドメインに参加させる方法はいくつかあります。

- クローン作成によってプロビジョニングする場合は、カスタム仕様を使用するか（vSphere マシンのプロビジョニングの場合）、SCVMM テンプレートにゲスト OS プロファイルを含める必要があります。マシンをプロビジョニングすると、指定したドメインにマシンが参加します。
- クローン作成によってプロビジョニングしない場合は、ブループリントで関連付けられたネットワーク プロファイルの DNS サフィックス設定を使用して、ドメインを特定できます。ただし、Windows をクローン作成するプロビジョニングで、固定 IP アドレス割り当てを使用する場合は、vSphere のカスタム仕様を使用する必要があります。

- vSphere のカスタム仕様を使用する場合、プロビジョニングされたマシンは、ブループリントで関連付けられたネットワーク プロファイルの DNS サフィックス設定によって指定されるドメインではなく、カスタム仕様で特定されたドメインに参加します。

vSphere のカスタム仕様は、Windows および Linux ゲスト OS の設定に関して事前定義された条件のセットを含んでいる vSphere オブジェクトです。マシンの [ビルド情報] タブで [カスタム仕様] 設定を使用することにより、カスタム仕様の名前を vRealize Automation ブループリントに追加できます。

vSphere でのカスタム仕様の作成については、[vSphere 製品のドキュメント](#) で、カスタム仕様の作成と管理などのカスタム仕様に関するトピックを参照してください。

vCloud Air および vCloud Director のプロビジョニングの準備

vCloud Air および vCloud Director マシンのプロビジョニングの準備を vRealize Automation を使用して行うには、テンプレートとカスタム オブジェクトで組織の仮想データセンターを構成する必要があります。

vRealize Automation を使用して vCloud Air および vCloud Director のリソースをプロビジョニングするには、組織に 1 つ以上のマシン リソースから構成されるクローン作成元のテンプレートが必要です。

組織間で共有するテンプレートは公開されている必要があります。 予約されたテンプレートのみが、クローン作成ソースとして vRealize Automation で使用できます。

注： テンプレートからのクローン作成でブループリントを作成する場合、そのテンプレート固有の ID はブループリントと関連付けられます。ブループリントが vRealize Automation カタログに公開され、プロビジョニングとデータ収集プロセスで使用される場合、関連付けられたテンプレートが認識されます。vCloud Air または vCloud Director でテンプレートを削除すると、その後の vRealize Automation のプロビジョニングとデータ収集は、関連付けられたテンプレートが存在しないために失敗します。テンプレートを削除して再作成するのではなく、たとえばアップデートされたバージョンをアップロードするために、vCloud Air または vCloud Director のテンプレート置換プロセスを使用してテンプレートを置換します。テンプレートの削除や再作成ではなく、vCloud Air または vCloud Director を使用してテンプレートを置換すると、テンプレート固有の ID が変更されないため、プロビジョニングとデータ収集が継続して機能します。

次の概要では、vRealize Automation を使用してエンドポイントを作成し、予約とブループリントを定義する前に実行する必要のある手順を説明します。これらの管理タスクの詳細については、vCloud Air および vCloud Director の製品ドキュメントを参照してください。

- 1 vCloud Air または vCloud Director で、クローン作成のテンプレートを作成し、組織カタログに追加します。
- 2 vCloud Air または vCloud Director で、テンプレートを使用して、各マシン上のゲスト OS のパスワード、ドメイン、スクリプトなどのカスタム設定を指定します。

vRealize Automation を使用して、これらの設定の一部をオーバーライドできます。

カスタマイズは、リソースのゲスト OS により異なることがあります。

- 3 vCloud Air または vCloud Director で、カタログを構成し、組織の全員で共有できるようにします。

vCloud Air または vCloud Director で、アカウント管理者用に該当する組織へのアクセスを構成し、組織のすべてのユーザーとグループがカタログにアクセスできるようにします。この共有設計をしないと、vRealize Automation のエンドポイントまたはブループリントのアーキテクトにはカタログ テンプレートが表示されません。

4 以下の情報を収集して、その情報をブループリントに含めることができますようにします。

- vCloud Air または vCloud Director のテンプレート名。
- テンプレート用に指定した合計ストレージ容量。

Linux キックスタート プロビジョニングの準備

Linux キックスタート プロビジョニングでは、構成ファイルを使用して、新しくプロビジョニングされたマシンに Linux を自動的にインストールします。プロビジョニングを準備するには、起動可能な ISO イメージとキックスタート、または AutoYaST 構成ファイルを作成する必要があります。

Linux キックスタート プロビジョニングの準備に必要な手順の概要は次のとおりです。

- 1 DHCP サーバがネットワーク上で使用可能なことを確認します。DHCP を使用しない限り、vRealize Automation は、Linux キックスタート プロビジョニングを使用してマシンをプロビジョニングできません。
- 2 構成ファイルを準備します。構成ファイルでは、vRealize Automation サーバおよび Linux エージェント インストール パッケージの場所を指定する必要があります。[Linux キックスタート構成サンプル ファイルの準備](#) を参照してください。
- 3 `isolinux/isolinux.cfg` または `loader/isolinux.cfg` を編集して、構成ファイルおよび Linux の適切な配布ソースの名前と場所を指定します。
- 4 起動 ISO イメージを作成して、仮想化プラットフォームが要求する場所に保存します。必要な場所の詳細については、ハイパーバイザーによって提供されるドキュメントを参照してください。
- 5 (オプション) カスタマイズ スクリプトを追加します。
 - a 構成ファイルでインストール後のカスタマイズ スクリプトを指定するには、[キックスタート/autoYaST 構成ファイルでのカスタム スクリプトの指定](#)を参照してください。
 - b ブループリントで Visual Basic スクリプトを呼び出すには、[プロビジョニング時に Visual Basic スクリプトを実行するためのチェックリスト](#)を参照してください。
- 6 以下の情報を収集して、ブループリントのアーキテクトが自分のブループリントにその情報を含めることができますようにします。
 - a ISO イメージの名前および場所。
 - b vCenter Server を統合する場合、vCenter Server がマシンを作成するための vCenter Server ゲスト OS のバージョン。

注： プロパティ セットが `BootIsoProperties` のプロパティ グループを作成して、必要な ISO 情報を含めることができます。これにより、ブループリントにこの情報を正確に含めることが容易になります。

Linux キックスタート構成サンプル ファイルの準備

vRealize Automation は、ニーズに応じて変更と編集ができるサンプル構成ファイルを提供します。使用可能なファイルを作成するにはいくつか変更する必要があります。

手順

- 1 vRealize Automation アプライアンス管理コンソールのページに移動します。
たとえば、`https://va-hostname.domain.com` です。
- 2 ページの vRealize Automation コンポーネントのインストール セクションにある [ゲストおよびソフトウェアのエージェント ページ] をクリックします。
たとえば、`https://va-hostname.domain.com/software/index.html` です。
[ゲストおよびソフトウェアのエージェント インストーラ] ページが開き、利用可能なダウンロードへのリンクが表示されます。
- 3 ページのゲスト エージェント インストーラ セクションにある [Linux ゲスト エージェント パッケージ] をクリックして、`LinuxGuestAgentPkgs.zip` ファイルをダウンロードして保存します。
- 4 ダウンロードした `LinuxGuestAgentPkgs.zip` ファイルを解凍して、`VraLinuxGuestAgent` フォルダを作成します。
- 5 プロビジョニング中に展開するゲスト OS に対応する `VraLinuxGuestAgent` サブディレクトリに移動します。
たとえば、`rhel32` です。
- 6 ターゲット システムに対応するサンプルのサブディレクトリにあるファイルを開きます。
たとえば、`samples/sample-https-rhel6-x86.cfg` です。
- 7 文字列 `host=dcac.example.net` のすべてのインスタンスを、Manager Service または Manager Service のロード バランサの IP アドレスまたは完全修飾ドメイン名とポート番号に置き換えます。

プラットフォーム	必要なフォーマット
vSphere ESXi	たとえば、IP アドレスは <code>--host=172.20.9.59</code> と入力します。
vSphere ESX	たとえば、IP アドレスは <code>--host=172.20.9.58</code> と入力します。
SUSE 10	たとえば、IP アドレスは <code>--host=172.20.9.57</code> と入力します。
その他すべて	たとえば、FQDN は <code>--host=mycompany-host1.mycompany.local:443</code> と入力します。

- 8 `gugent.rpm` または `gugent.tar.gz` の各インスタンスを特定し、この URL `rpm.example.net` をゲスト エージェント パッケージの場所に置き換えます。

例：

```
rpm -i nfs:172.20.9.59/suseagent/gugent.rpm
```

- 9 新しくプロビジョニングされたマシンにアクセス可能な場所にファイルを保存します。

キックスタート/autoYaST 構成ファイルでのカスタム スクリプトの指定

構成ファイルを変更し、新たにプロビジョニングされたマシンにカスタム スクリプトをコピーまたはインストールすることができます。Linux エージェントは、ワークフローで指定されたポイントでスクリプトを実行します。

スクリプトで `/properties.xml` ファイル (`/usr/share/gugent/site/workitem` ディレクトリ内) のいずれかを参照することができます。

前提条件

- キックスタートまたは autoYaST 構成ファイルを準備する。[Linux キックスタート構成サンプル ファイルの準備](#)を参照してください。
- マシン プロビジョニングの失敗を防ぐため、このスクリプトは失敗時にゼロ以外の値を返す必要があります。

手順

1 使用するスクリプトを作成するか、または特定します。

2 このスクリプトを `NN_scriptname` として保存します。

`NN` は 2 桁の数値です。スクリプトの実行は、最小の数値から最大へ、順に行われます。2 つのスクリプトに同じ数値が指定されている場合は、`scriptname` に基づいてアルファベット順となります。

3 スクリプトを実行可能にします。

4 キックスタートまたは autoYaST 構成ファイルのインストール後処理についてのセクションを見つけます。

キックスタートでは、これは `%post` で示されます。autoYaST では、これは `post-scripts` で示されます。

5 選択した `/usr/share/gugent/site/workitem` ディレクトリにスクリプトをコピーまたはインストールするように構成ファイルのインストール後セクションを変更します。

仮想スタートまたは autoYaST の場合、カスタム スクリプトは一般に作業アイテム SetupOS (作成プロビジョニング用) および CustomizeOS (クローン プロビジョニング用) とともに実行されますが、ワークフロー内の任意のポイントで実行することもできます。

たとえば、構成ファイルを変更し、次のコマンドを使用して、新たにプロビジョニングされたマシン上の `/usr/share/gugent/site/SetupOS` ディレクトリにスクリプト `11_addusers.sh` をコピーできます。

```
cp nfs:172.20.9.59/linuxscripts/11_addusers.sh /usr/share/gugent/site/SetupOS
```

結果

Linux エージェントは、作業アイテム ディレクトリとスクリプト ファイル名で指定された順にスクリプトを実行します。

SCCM プロビジョニングの準備

vRealize Automation は、ISO イメージから新しくプロビジョニングされたマシンを起動し、指定された SCCM タスク シーケンスに制御を渡します。

SCCM プロビジョニングは、Windows オペレーティング システムの展開でサポートされています。Linux はサポートされていません。ソフトウェアの配布およびアップデートはサポートされていません。

デフォルトでは、SCCM マシンは、該当する収集のメンバーシップをプロビジョニング以降 10 秒間隔で確認するように構成されています。場合によっては、この間隔では登録プロセスで問題が発生する可能性があります。確認プロセスをカスタマイズするには、2 つのプロパティを使用できます。1 つは SCCM `refresh collection setting` というプロパティです。デフォルトでは、このプロパティは `true` に設定され、マシンがメンバーシップ チェックを

実行していることを確認します。必要に応じて、この設定を `false` に変更し、メンバーシップチェックをスキップするようにマシンを構成できます。もう 1 つは `SCCM machine membership check interval` というプロパティです。前述のとおりデフォルトは 10 秒ですが、登録で問題が発生する場合は、別の値を指定して再トリガの時間枠を拡張することができます。これらのプロパティは両方とも、[インフラストラクチャ] - [管理] - [グローバル設定] の `laaS` グローバル設定に含まれています。

SCCM プロビジョニングの準備に必要な手順の概要は次のとおりです。

- 1 SCCM との通信には、SCCM サーバの NetBIOS 名が必要です。

ネットワーク管理者と連携して、少なくとも 1 つの Distributed Execution Manager (DEM) が SCCM サーバの FQDN を NetBIOS 名に解決できるようにします。

DEM を SCCM サーバと同じネットワークに直接配置する必要はありませんが、DEM が IP 経由で SCCM サーバに到達できる必要があります。

- 2 vRealize Automation ゲスト エージェントを含むソフトウェア パッケージを作成します。 [SCCM プロビジョニング用のソフトウェア パッケージの作成](#) を参照してください。
- 3 SCCM で、マシンをプロビジョニングするために必要なタスク シーケンスを作成します。最後の手順として、vRealize Automation ゲスト エージェントを含むように作成したソフトウェア パッケージをインストールする必要があります。タスク シーケンスの作成およびソフトウェア パッケージのインストールの詳細については、SCCM のドキュメントを参照してください。
- 4 タスク シーケンス用のゼロ タッチ起動 ISO イメージを作成します。デフォルトの場合、SCCM はライト タッチ起動 ISO イメージを作成します。ゼロ タッチ ISO イメージに関する SCCM の構成の詳細については、SCCM のドキュメントを参照してください。
- 5 仮想化プラットフォームが要求する場所に ISO イメージをコピーします。適切な場所が分からない場合は、ハイパーバイザーによって提供されるドキュメントを参照してください。
- 6 以下の情報を収集して、ブループリントのアーキテクトがその情報をブループリントに含めることができるようにします。
 - a タスク シーケンスが含まれるコレクションの名前。
 - b シーケンスを含むコレクションのある SCCM サーバの完全修飾ドメイン名。
 - c SCCM サーバのサイト コード。
 - d SCCM サーバの管理者レベルの認証情報。
 - e (オプション) SCVMM 統合の場合、プロビジョニングされたマシンに添付する ISO、仮想ハード ディスク、またはハードウェア プロファイル。

SCCM プロビジョニング用のソフトウェア パッケージの作成

SCCM タスク シーケンスの最後の手順として、vRealize Automation ゲスト エージェントを含むソフトウェア パッケージをインストールする必要があります。

手順

- 1 vRealize Automation アプライアンス管理コンソールのページに移動します。

たとえば、`https://va-hostname.domain.com` です。

- 2 ページの vRealize Automation コンポーネントのインストール セクションにある [ゲストおよびソフトウェアのエージェント ページ] をクリックします。

たとえば、<https://va-hostname.domain.com/software/index.html> です。

[ゲストおよびソフトウェアのエージェント インストーラ] ページが開き、利用可能なダウンロードへのリンクが表示されます。

- 3 ページのコンポーネント インストール セクションにある Windows ゲスト エージェント ファイル ([32 ビット]) または ([64 ビット]) をクリックして、GuestAgentInstaller.exe または GuestAgentInstaller_x64.exe ファイルをダウンロードおよび保存します。
- 4 Windows ゲスト エージェント ファイルを SCCM で使用できる場所に展開します。
この操作で、ディレクトリ C:\VRMGuestAgent が作成されます。このディレクトリの名前は変更しないでください。
- 5 定義ファイル SCCMPackageDefinitionFile.sms からソフトウェア パッケージを作成します。
- 6 ソフトウェア パッケージを自分の分散ポイントで使用できるようにします。
- 7 抽出した Windows ゲスト エージェント ファイルのコンテンツをソース ファイルとして選択します。

WIM プロビジョニングの準備

WinPE 環境で起動してマシンをプロビジョニングし、既存の Windows リファレンス マシンの Windows イメージ ファイル形式 (WIM) イメージを使用して、オペレーティング システムをインストールします。

WIM プロビジョニングの準備に必要な手順の概要は次のとおりです。

- 1 ステージング エリアの指定または作成を行います。ステージング領域は、次によって UNC パスとして指定できる、またはネットワーク ドライブとしてマウントできる、ネットワーク ディレクトリである必要があります。
 - 参照マシン。
 - WinPE イメージをビルドするシステム。
 - マシンをプロビジョニングする仮想化ホスト。
- 2 ネットワークに DHCP サーバがあることを確認します。DHCP が使用できないと、vRealize Automation は WIM イメージを使用してマシンをプロビジョニングできません。
- 3 プロビジョニングに使用する仮想プラットフォーム内でリファレンス マシンの指定または作成を行います。
vRealize Automation の要件については、[WIM プロビジョニングのリファレンス マシンの要件](#) を参照してください。リファレンス マシンの作成については、ハイパーバイザーにより提供されたドキュメントを参照してください。
- 4 System Preparation Utility for Windows を参照して、リファレンス マシンのオペレーティング システムの展開を準備します。[リファレンス マシンの SysPrep 要件](#) を参照してください。
- 5 リファレンス マシンの WIM イメージを作成します。WIM イメージ ファイル名にスペースを入れないでください。さもないとプロビジョニングが失敗します。

6 vRealize Automation ゲスト エージェントを含む WinPE イメージを作成します。

- (オプション) プロビジョニングされたマシンのカスタマイズに使用するカスタム スクリプトを作成し、適切な作業アイテム ディレクトリにそのスクリプトを配置します。
- ネットワークまたはストレージのインターフェイスに VirtIO を使用している場合、必要なドライバが WinPE イメージと WIM イメージに含まれていることを確認する必要があります。[VirtIO ドライバを使用した WIM プロビジョニングの準備](#)を参照してください。

WinPE イメージを作成する場合は、vRealize Automation ゲスト エージェントを手動で挿入する必要があります。[WinPE イメージへのゲスト エージェントの手動挿入](#)を参照してください。

- 7 仮想プラットフォームが必要とする場所に WinPE イメージを配置します。場所が分からない場合は、ハイパーバイザーのドキュメントを参照してください。
- 8 ブループリントに含める次の情報を収集します。
 - a WinPE ISO イメージの名前および場所。
 - b WIM ファイルの名前、WIM への UNC パス、および WIM ファイルから必要なイメージを展開するために使用されるインデックス。
 - c プロビジョニングされたマシン上のネットワーク ドライブに WIM イメージ パスをマッピングするためのユーザー名およびパスワード。
 - d (オプション) デフォルト K を使用しない場合、プロビジョニングされたマシンに WIM イメージ パスをマッピングするドライブ文字。
 - e vCenter Server を統合する場合、vCenter Server がマシンを作成するための vCenter Server ゲスト OS のバージョン。
 - f (オプション) SCVMM 統合の場合、プロビジョニングされたマシンに添付する ISO、仮想ハード ディスク、またはハードウェア プロファイル。

注： プロパティ グループを作成して、この必要な情報のすべてを含めることができます。プロパティ グループを使用すると、ブループリントにすべての情報を正しく含めることがより簡単になります。

手順

1 [WIM プロビジョニングのリファレンス マシンの要件](#)

WIM プロビジョニングでは、リファレンス マシンから WIM イメージを作成します。リファレンス マシンは、vRealize Automation でプロビジョニングが機能するために、WIN イメージの基本的な要件を満たす必要があります。

2 [リファレンス マシンの SysPrep 要件](#)

SysPrep 応答ファイルには、WIM プロビジョニングで使用するのに必要な複数の設定が含まれます。

3 [VirtIO ドライバを使用した WIM プロビジョニングの準備](#)

ネットワークまたはストレージのインターフェイスに VirtIO を使用している場合、必要なドライバが WinPE イメージと WIM イメージに含まれていることを確認する必要があります。VirtIO は一般に、KVM (RHEV) でプロビジョニングする場合に高いパフォーマンスを提供します。

4 WinPE イメージへのゲスト エージェントの手動挿入

WinPE イメージに vRealize Automation のゲスト エージェントを手動で挿入する必要があります。

WIM プロビジョニングのリファレンス マシンの要件

WIM プロビジョニングでは、リファレンス マシンから WIM イメージを作成します。リファレンス マシンは、vRealize Automation でプロビジョニングが機能するために、WIN イメージの基本的な要件を満たす必要があります。

リファレンス マシンの準備に必要な手順の概要は次のとおりです。

- 1 リファレンス マシンのオペレーティング システムが、Windows Server 2008 R2、Windows Server 2012、Windows 7、または Windows 8 の場合、デフォルト インストールでは、メイン パーティションに加えて、システムのハード ディスクに小さなパーティションが作成されます。vRealize Automation では、このように複数のパーティションに分割されたリファレンス マシン上に作成した WIM イメージの使用はサポートしません。インストール プロセス時には、このパーティションを削除する必要があります。
- 2 NET 4.5 および Windows 7 用の Windows Automated Installation Kit (AIK) (WinPE 3.0 を含む) をリファレンス マシンにインストールします。
- 3 リファレンス マシンのオペレーティング システムが Windows Server 2003 または Windows XP の場合は、管理者パスワードをリセットして空にします。(パスワードはありません。)
- 4 (オプション) XenDesktop 統合を有効にする場合は、Citrix Virtual Desktop Agent をインストールして構成します。
- 5 (オプション) Windows Management Instrumentation (WMI) エージェントは、マシン所有者の Active Directory のステータスなど、vRealize Automation により管理される Windows マシンから特定のデータを収集する必要があります。Windows マシンを正常に管理するには、(通常は Manager Service ホスト上の) WMI エージェントをインストールし、このエージェントを有効にして Windows マシンからデータを収集する必要があります。『vRealize Automation のインストール』を参照してください。

リファレンス マシンの SysPrep 要件

SysPrep 応答ファイルには、WIM プロビジョニングで使用するのに必要な複数の設定が含まれます。

表 1-15. Windows Server または Windows XP リファレンス マシンに必要な SysPrep 設定値

GuiUnattended の設定値	値
AutoLogon	Yes
AutoLogonCount	1
AutoLogonUsername	username (username と password は、新たにプロビジョニングされたマシンがゲスト OS で起動するときに自動ログオンに使用される認証情報です。通常は管理者が使用されます。)
AutoLogonPassword	password は AutoLogonUsername に対応します。

表 1-16. Windows Server 2003 または Windows XP を使用していないリファレンス マシンに必要な SysPrep 設定値

AutoLogon の設定値	値
Enabled	Yes
LogonCount	1
Username	username (username と password は、新たにプロビジョニングされたマシンがゲスト OS で起動するときに自動ログオンに使用される認証情報です。通常は管理者が使用されます。)
Password	password (username と password は、新たにプロビジョニングされたマシンがゲスト OS で起動するときに自動ログオンに使用される認証情報です。通常は管理者が使用されます。) 注: Windows Server 2003 または Windows XP よりも新しい Windows プラットフォームを使用するリファレンス マシンの場合は、カスタム プロパティ Sysprep.GuiUnattended.AdminPassword を使用して自動ログオン パスワードを設定する必要があります。この設定を確実に行うには、このカスタム プロパティを含むプロパティ グループを作成し、テナント管理者とビジネス グループ マネージャがこの情報をブループリントに正しく含めることができるようにするのが簡単です。

VirtIO ドライバを使用した WIM プロビジョニングの準備

ネットワークまたはストレージのインターフェイスに VirtIO を使用している場合、必要なドライバが WinPE イメージと WIM イメージに含められていることを確認する必要があります。VirtIO は一般に、KVM (RHEV) でプロビジョニングする場合に高いパフォーマンスを提供します。

VirtIO 用の Windows ドライバは Red Hat Enterprise Virtualization の一部として含まれており、Red Hat Enterprise Virtualization Manager のファイル システム上の /usr/share/virtio-win ディレクトリに置かれています。ドライバは、/usr/share/rhev-guest-tools-iso/rhev-tools-setup.iso に置かれている Red Hat Enterprise Virtualization ゲスト ツールにも含まれています。

VirtIO ドライバを使用して WIM ベースのプロビジョニングを有効にする手順の概要は次のとおりです。

- 1 VirtIO ドライバがインストールされた Windows リファレンス マシンから WIM イメージを作成するか、またはドライバを既存の WIM イメージに挿入します。
- 2 VirtIO ドライバ ファイルをコピーし、WinPE イメージにドライバを挿入します。
- 3 rhevm-iso-uploader コマンドを使用し、Red Hat Enterprise Virtualization ISO ストレージ ドメインに WinPE イメージ ISO をアップロードします。RHEV で ISO イメージを管理する方法については、Red Hat のドキュメントを参照してください。
- 4 WIM プロビジョニング用の KVM (RHEV) ブループリントを作成し、WinPE ISO オプションを選択します。値 **VirtIO** とともにカスタム プロパティ VirtualMachine.Admin.DiskInterfaceType を含める必要があります。ファブリック管理者は、プロパティ グループにこの情報を含め、ブループリントに含めるようにすることができます。

カスタム プロパティ `Image.ISO.Location` と `Image.ISO.Name` は、KVM (RHEV) ブループリントには使用されません。

WinPE イメージへのゲスト エージェントの手動挿入

WinPE イメージに vRealize Automation のゲスト エージェントを手動で挿入する必要があります。

前提条件

- 準備したステージング エリアにアクセスできる Windows システム、および .NET 4.5 と Windows 7 用の Windows Automated Installation Kit (AIK) (WinPE 3.0 を含む) がインストールされている Windows システムを選択する。
- WinPE を作成する。

手順

1 WinPE へのゲスト エージェントのインストール

ゲスト エージェント ファイルを WinPE イメージに手動でコピーする必要があります。

2 `doagent.bat` ファイルの構成

`doagent.bat` ファイルを手動で構成する必要があります。

3 `doagentc.bat` ファイルの構成

`doagentc.bat` ファイルを手動で構成する必要があります。

4 ゲスト エージェント プロパティ ファイルの構成

ゲスト エージェント プロパティ ファイルを手動で構成する必要があります。

手順

1 WinPE へのゲスト エージェントのインストール。

2 `doagent.bat` ファイルの構成。

3 `doagentc.bat` ファイルの構成。

4 ゲスト エージェント プロパティ ファイルの構成。

WinPE へのゲスト エージェントのインストール

ゲスト エージェント ファイルを WinPE イメージに手動でコピーする必要があります。

前提条件

- 準備したステージング エリアにアクセスできる Windows システム、および .NET 4.5 と Windows 7 用の Windows Automated Installation Kit (AIK) (WinPE 3.0 を含む) がインストールされている Windows システムを選択する。
- WinPE を作成する。

手順

- ◆ vRealize Automation ゲスト エージェントを、https://vRealize_VA_Hostname_fqdn/software/index.html からダウンロードしてインストールします。
 - a `GugentZip_version` を、リファレンス マシンの C ドライブにダウンロードします。
ご使用のオペレーティング システムに応じて、`GuestAgentInstaller.exe` (32 ビット) または `GuestAgentInstaller_x64.exe` (64 ビット) を選択します。
 - b ファイルを右クリックして [プロパティ] を選択します。
 - c [全般] をクリックします。
 - d [ブロック解除] をクリックします。
 - e ファイルを C:\ に解凍します。
この操作で、ディレクトリ `C:\VRMGuestAgent` が作成されます。このディレクトリの名前は変更しないでください。

次のステップ

[doagent.bat ファイルの構成。](#)

doagent.bat ファイルの構成

doagent.bat ファイルを手動で構成する必要があります。

前提条件

[WinPE へのゲスト エージェントのインストール。](#)

手順

- 1 WinPE イメージ内の `VRMGuestAgent` ディレクトリに移動します。
例: `C:\Program Files (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent`。
- 2 `doagent-template.bat` ファイルのコピーを作成し、`doagent.bat` と名前を付けます。
- 3 `doagent.bat` をテキスト エディタで開きます。
- 4 文字列 `#Dcac Hostname#` のすべてのインスタンスを `IaaS Manager Service` ホストの完全修飾ドメイン名とポート番号で置き換えます。

オプション	説明
ロード バランサを使用している場合	IaaS Manager Service のロード バランサの完全修飾ドメイン名とポートを入力します。 例、 <code>manager_service_LB.mycompany.com:443</code>
ロード バランサがない場合	IaaS Manager Service がインストールされているマシンの完全修飾ドメイン名とポートを入力します。 例、 <code>manager_service.mycompany.com:443</code>

- 5 文字列 #Protocol# のすべてのインスタンスを文字列 /ssl に置き換えます。
- 6 文字列 #Comment# のすべてのインスタンスを REM （REM の末尾にスペースが必要）に置き換えます。
- 7 （オプション） 自己署名証明書を使用している場合は、openssl コマンドをコメント解除します。

```
echo QUIT | c:\VRMGuestAgent\bin\openssl s_client -connect
```

- 8 ファイルを保存して閉じます。
- 9 WinPE の Startnet.cmd スクリプトを編集し、カスタム スクリプトとして doagentc.bat を含めます。

次のステップ

[doagentc.bat ファイルの構成。](#)

doagentc.bat ファイルの構成

doagentc.bat ファイルを手動で構成する必要があります。

前提条件

[doagentc.bat ファイルの構成。](#)

手順

- 1 WinPE イメージ内の VRMGuestAgent ディレクトリに移動します。
例 : C:\Program Files (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent。
- 2 doagentsvc-template.bat ファイルのコピーを作成し、doagentc.bat と名前を付けます。
- 3 doagentc.bat をテキスト エディタで開きます。
- 4 文字列 #Comment# のすべてのインスタンスを削除します。
- 5 文字列 #Dcac Hostname# のすべてのインスタンスを Manager Service ホストの完全修飾ドメイン名とポート番号で置き換えます。

Manager Service のデフォルト ポートは 443 です。

オプション	説明
ロード バランサを使用している場合	Manager Service のロード バランサの完全修飾ドメイン名とポートを入力します。 例、 load_balancer_manager_service.mycompany.com:443
ロード バランサがない場合	Manager Service の完全修飾ドメイン名とポートを入力します。 例、 manager_service.mycompany.com:443

- 6 文字列 #errorlevel# のすべてのインスタンスを文字列 1 に置き換えます。
- 7 文字列 #Protocol# のすべてのインスタンスを文字列 /ssl に置き換えます。
- 8 ファイルを保存して閉じます。

次のステップ

[ゲスト エージェント プロパティ ファイルの構成。](#)

ゲスト エージェント プロパティ ファイルの構成

ゲスト エージェント プロパティ ファイルを手動で構成する必要があります。

前提条件

[doagentc.bat ファイルの構成。](#)

手順

- 1 WinPE イメージ内の VRMGuestAgent ディレクトリに移動します。
例 : C:\Program Files (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent.
- 2 ファイル gument.properties のコピーを作成し、そのコピーに gument.properties.template という名前を付けます。
- 3 ファイル gument.properties.template のコピーを作成し、そのコピーに gumentc.properties という名前を付けます。
- 4 gument.properties をテキスト エディタで開きます。
- 5 文字列 GuestAgent.log のすべてのインスタンスを文字列 X:/VRMGuestAgent/GuestAgent.log に置き換えます。
- 6 ファイルを保存して閉じます。
- 7 gumentc.properties をテキスト エディタで開きます。
- 8 文字列 GuestAgent.log のすべてのインスタンスを文字列 C:/VRMGuestAgent/GuestAgent.log に置き換えます。
- 9 ファイルを保存して閉じます。

仮想マシン イメージ プロビジョニングの準備

OpenStack を使用してインスタンスをプロビジョニングする前に、仮想マシン イメージが作成済みであり、OpenStack プロバイダによってフレーバーが構成済みである必要があります。

仮想マシン イメージ

OpenStack リソースのブループリントの作成時に、使用可能なイメージのリストから仮想マシン イメージを選択できます。

仮想マシン イメージは、オペレーティング システムなどのソフトウェア構成を含むテンプレートです。仮想マシン イメージは OpenStack プロバイダによって管理され、データ収集中にインポートされます。

ブループリントで使用されるイメージが後で OpenStack プロバイダから削除されると、そのイメージはブループリントからも削除されます。ブループリントからすべてのイメージが削除された場合、ブループリントは無効になり、編集して 1 つ以上のイメージを追加するまでマシン申請に使用できません。

OpenStack フレーバー

OpenStack ブループリントを作成するときに、1つ以上のフレーバーを選択することができます。

OpenStack フレーバーは、OpenStack でプロビジョニングされたインスタンスのマシン リソース仕様を定義する仮想ハードウェア テンプレートです。フレーバーは、OpenStack プロバイダによって管理され、データ収集中にインポートされます。

Amazon マシン イメージ プロビジョニングの準備

vRealize Automation でのプロビジョニングのために Amazon マシン イメージおよびインスタンス タイプを準備します。

Amazon マシン イメージについて

Amazon マシンのブループリントを作成するときは、使用可能なイメージのリストから Amazon マシン イメージを選択できます。

Amazon マシン イメージは、オペレーティング システムなどのソフトウェア構成を含むテンプレートです。Amazon Web Services アカウントにより管理されます。vRealize Automation では、プロビジョニングに対応しているインスタンス タイプを管理します。

Amazon マシン イメージとインスタンス タイプは、Amazon のリージョンで利用できる必要があります。すべてのインスタンス タイプがすべてのリージョンで利用できるわけではありません。

Amazon Web Services、ユーザー コミュニティ、または AWS Marketplace サイトが提供する Amazon マシン イメージを選択できます。また独自に Amazon マシン イメージを作成したり、必要に応じてそのイメージを共有したりすることもできます。1つの Amazon マシン イメージを使用して、1つのインスタンスや多くのインスタンスを起動できます。

クラウド マシンをプロビジョニングする Amazon Web Services アカウントの Amazon マシン イメージには、次の考慮事項が適用されます。

- ブループリントごとに Amazon マシン イメージを指定する必要があります。

プライベート Amazon マシン イメージは、特定のアカウントとそのアカウントのすべてのリージョンで利用できます。パブリック Amazon マシン イメージは、すべてのアカウントと、各アカウントの特定のリージョンでのみ利用できます。

- ブループリントが作成されるとき、指定された Amazon マシン イメージが、データ収集元のリージョンから選択されます。複数の Amazon Web Services アカウントを利用できる場合、ビジネス グループ マネージャはプライベート Amazon マシン イメージに対する権限が必要になります。Amazon マシン イメージのリージョンと指定されたユーザーの場所により、プロビジョニングの申請が、その同じリージョンと場所に対応する予約に制限されます。
- 予約とポリシーを使用して、Amazon Web Services アカウントの Amazon マシン イメージを配布します。ポリシーを使用して、ブループリントからのプロビジョニングを特定の一連の予約に制限します。
- vRealize Automation は、クラウド マシンでユーザー アカウントを作成できません。マシン所有者は初めてクラウド マシンに接続するとき、管理者としてログインし、自分の vRealize Automation ユーザー認証情報を追加する必要があります。または、マシン所有者の代わりに管理者がこの操作を実行する必要があります。マシン所有者は、その後、自分の vRealize Automation ユーザー認証情報を使用してログインできます。

Amazon マシン イメージにより、起動のたびに管理者パスワードが作成される場合、[マシン レコードの編集] ページにパスワードが表示されます。表示されない場合、Amazon Web Services アカウントでパスワードを確認できます。起動のたびに管理者パスワードを生成するように、すべての Amazon マシン イメージを構成できます。また、他のユーザーに代わってマシンをプロビジョニングするユーザーをサポートするために、管理者パスワード情報を提供することもできます。

- Amazon Web Services アカウントでプロビジョニングされたクラウド マシン上でリモート Microsoft Windows Management Instrumentation (WMI) 申請を許可するには、Microsoft Windows Remote Management (WinRM) エージェントが、vRealize Automation によって管理される Windows マシンからデータを収集できるようにします。『vRealize Automation のインストール』を参照してください。
- プライベート Amazon マシン イメージは、テナント全体に表示できます。

詳細については、Amazon のドキュメントの「*Amazon マシン イメージ (AMI)*」のトピックを参照してください。

Amazon インスタンス タイプについて

IaaS アーキテクトは、Amazon EC2 ブループリントを作成するときに、1 つ以上の Amazon インスタンス タイプを選択します。IaaS 管理者は、インスタンス タイプを追加または削除して、アーキテクトが使用できる選択肢を管理できます。

Amazon EC2 インスタンスは、Amazon Web Services でアプリケーションを実行できる仮想サーバです。インスタンスは、適切なインスタンス タイプを選択することで、Amazon マシン イメージから作成されます。

Amazon Web Services アカウントでマシンをプロビジョニングするために、指定された Amazon マシン イメージにインスタンス タイプが適用されます。アーキテクトが Amazon EC2 ブループリントを作成するときに、利用可能なインスタンス タイプが一覧表示されます。アーキテクトは 1 つ以上のインスタンス タイプを選択します。また、それらのインスタンス タイプは、ユーザーがマシンをプロビジョニングするよう申請したときに利用可能な選択肢となります。インスタンス タイプは、指定されたリージョンでサポートされている必要があります。

詳細については、Amazon のドキュメントの「*インスタンス タイプの選択*」および「*Amazon EC2 インスタンスの詳細*」のトピックを参照してください。

Amazon インスタンス タイプの追加

vRealize Automation には、Amazon ブループリントとともに使用するための複数のインスタンス タイプが用意されています。管理者は、インスタンス タイプを追加および削除できます。

IaaS 管理者によって管理されるマシン インスタンス タイプは、ブループリント アーキテクトが Amazon ブループリントを作成または編集するときにブループリント アーキテクトに対して利用可能になります。Amazon マシン イメージおよびインスタンス タイプは、Amazon Web Services 製品を介して利用可能になります。

前提条件

IaaS 管理者として vRealize Automation にログインします。

手順

- 1 [インフラストラクチャ] - [管理] - [インスタンス タイプ] をクリックします。
- 2 [新規] をクリックします。

3 新規インスタンス タイプを追加し、次のパラメータを指定します。

これらのパラメータに指定できる、利用可能な Amazon インスタンス タイプおよび設定値の詳細については、aws.amazon.com/ec2 の EC2 Instance Types - Amazon Web Services (AWS) および docs.aws.amazon.com の Instance Types にある Amazon Web Services のドキュメントから入手できます。

- 名前
- API 名
- タイプ名
- IO パフォーマンス名
- CPU
- メモリ (GB)
- ストレージ (GB)
- 計算単位

4 [保存] アイコン (👍) をクリックします。

結果

IaaS アーキテクトは、Amazon Web Services ブループリントを作成するとき、カスタムのインスタンス タイプを使用できます。

次のステップ

エンドポイントからファブリック グループにコンピュート リソースを追加します。[ファブリック グループの作成](#)を参照してください。

シナリオ：マシンをプロビジョニングするために vSphere リソースを準備する

あなたは vSphere 管理者で、vRealize Automation のテンプレートを作成しています。vSphere Web Client を使用して、vRealize Automation で CentOS マシンのクローンを作成する準備をしようとしています。

また、あなたとアーキテクトが vRealize Automation で CentOS マシンのクローン作成用ブループリントを作成できるように、既存の CentOS リファレンス マシンを vSphere テンプレートに変換する予定です。さらに、同一の設定で複数の仮想マシンを展開することにより生じる競合を防ぐために、あなたとアーキテクトが Linux テンプレートのクローン ブループリントを作成する際に使用できる一般的なカスタム仕様 も作成したいと思っています。

前提条件

VMware Tools がインストールされている Linux CentOS リファレンス マシンを特定または作成します。インターネット接続を提供するネットワーク アダプタを少なくとも 1 つ含めます。

手順

1 シナリオ : CentOS リファレンス マシンを Rainpole 用のテンプレートに変換する

vSphere Client を使用して、既存の CentOS リファレンス マシンを vSphere テンプレートに変換し、vRealize Automation IaaS アーキテクトが自分のクローン ブループリントのベースとして参照できるようにします。

2 シナリオ : Linux マシンのクローン作成用のカスタム仕様 を作成する

vSphere Client を使用して、標準的なカスタマイズ仕様を作成します。vRealize Automation IaaS アーキテクトは、Linux マシン用のクローン ブループリントを作成するときにこれを利用できます。

シナリオ : CentOS リファレンス マシンを Rainpole 用のテンプレートに変換する

vSphere Client を使用して、既存の CentOS リファレンス マシンを vSphere テンプレートに変換し、vRealize Automation IaaS アーキテクトが自分のクローン ブループリントのベースとして参照できるようにします。

手順

1 root ユーザーとしてリファレンス マシンにログインして、マシンを変換する準備をします。

- a udev 持続性ルールを削除します。

```
/bin/rm -f /etc/udev/rules.d/70*
```

- b このテンプレートからクローン作成されたマシンに一意の識別子を割り当てられるようにします。

```
/bin/sed -i '/^\(HWADDR\|UUID\)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- c マシンをパワーオフします。

```
shutdown -h now
```

2 vSphere Web Client に管理者としてログインします。

3 [仮想マシン オプション] タブをクリックします。

4 参照マシンを右クリックして、[設定の編集] を選択します。

5 [仮想マシン名] テキスト ボックスに、**Rainpole_centos_63_x86** と入力します。

6 リファレンス マシンでゲスト OS として CentOS が動作している場合でも、[ゲスト OS のバージョン] ドロップダウン メニューから [Red Hat Enterprise Linux 6 (64-bit)] を選択します。

CentOS を選択すると、テンプレートとカスタム仕様 が期待どおりに動作しないことがあります。

7 vSphere Web Client で [Rainpole_centos_63_x86] リファレンス マシンを右クリックして、[テンプレート] - [テンプレートに変換] を選択します。

結果

vCenter Server で、Rainpole_centos_63_x86 reference リファレンス マシンにテンプレートのマークが付けられ、[最近のタスク] ペインにタスクが表示されます。

次のステップ

同一の設定を使用して複数の仮想マシンを展開すると競合が生じる場合があります。自分や他の Rainpole アーキテクトのために、Linux テンプレート用のクローン ブループリントの作成に利用できる汎用的なカスタマイズ仕様を作成しておけば、これを防ぐことができます。

シナリオ：Linux マシンのクローン作成用のカスタム仕様 を作成する

vSphere Client を使用して、標準的なカスタマイズ仕様を作成します。vRealize Automation IaaS アーキテクトは、Linux マシン用のクローン ブループリントを作成するときにこれを利用できます。

手順

- 1 ホーム ページの [カスタム仕様 マネージャ] をクリックしてウィザードを開きます。
- 2 [新規] アイコンをクリックします。
- 3 プロパティを指定します。
 - a [ターゲット仮想マシン オペレーティング システム] ドロップダウン メニューから [Linux] を選択します。
 - b [カスタム仕様 名] テキスト ボックスに **Linux** と入力します。
 - c [説明] テキスト ボックスに、**Rainpole Linux cloning with vRealize Automation** と入力します。
 - d [次へ] をクリックします。
- 4 コンピュータ名を設定します。
 - a [仮想マシン名を使用] を選択します。
 - b [ドメイン名] テキスト ボックスに、プロビジョニングする予定の、クローン作成されたマシンのドメインを入力します。
 - c [次へ] をクリックします。
- 5 タイム ゾーン設定を構成します。
- 6 [次へ] をクリックします。
- 7 [ゲスト OS に標準ネットワーク設定を使用します (すべてのネットワーク インターフェイスで DHCP を有効化など)] を選択します。
- 8 プロンプトの指示に従って残りの必須情報を入力します。
- 9 [完了前の確認] ページで選択内容を確認し、[終了] をクリックします。

ソフトウェア プロビジョニングの準備

ソフトウェア を使用し、vSphere、vCloud Director、vCloud Air、Amazon Web Services、Microsoft Azure の各マシンの vRealize Automation プロビジョニング手順の一環として、アプリケーションおよびミドルウェアを展開します。

ブループリントが ソフトウェア をサポートする場合、またはゲスト エージェントとソフトウェア ブートストラップ エージェントをテンプレート、スナップショット、マシン イメージに変換する前にリファレンス マシンにインストールした場合は、ソフトウェア をマシンに展開できます。

マシンのプロビジョニングの準備中にポートを指定する場合の関連情報については、[vRealize Automation 製品ドキュメント](#)の「リファレンス アーキテクチャ PDF」を参照してください。

表 1-17. ソフトウェア をサポートするプロビジョニングの方法

マシン タイプ	準備
vSphere	クローン ブループリントは、vCenter Server 仮想マシン テンプレートに基づいて、完全な独立型の仮想マシンをプロビジョニングします。クローン作成用テンプレートで ソフトウェア コンポーネントをサポートする場合は、クローン作成用テンプレートを準備するときに、ゲスト エージェントとソフトウェア ブートストラップ エージェントをリファレンス マシン上にインストールします。 クローン作成によるプロビジョニングの準備のためのチェックリスト を参照してください。
vSphere	リンク クローン ブループリントは、差分ディスクのチェーンを使用して親マシンとの差異を追跡し、スナップショットに基づいて vSphere マシンの容量を効率的に利用したコピーをプロビジョニングします。リンク クローン ブループリントで ソフトウェア コンポーネントをサポートする場合は、スナップショットを作成する前に、ゲスト エージェントおよびソフトウェア ブートストラップ エージェントをマシン上にインストールします。ソフトウェア をサポートするテンプレートからスナップショット マシンをクローン作成した場合は、必要なエージェントがすでにインストールされています。
vCloud Director	クローン ブループリントは、vCenter Server 仮想マシン テンプレートに基づいて、完全な独立型の仮想マシンをプロビジョニングします。クローン作成用テンプレートで ソフトウェア コンポーネントをサポートする場合は、クローン作成用テンプレートを準備するときに、ゲスト エージェントとソフトウェア ブートストラップ エージェントをリファレンス マシン上にインストールします。 クローン作成によるプロビジョニングの準備のためのチェックリスト を参照してください。
vCloud Air	クローン ブループリントは、vCenter Server 仮想マシン テンプレートに基づいて、完全な独立型の仮想マシンをプロビジョニングします。クローン作成用テンプレートで ソフトウェア コンポーネントをサポートする場合は、クローン作成用テンプレートを準備するときに、ゲスト エージェントとソフトウェア ブートストラップ エージェントをリファレンス マシン上にインストールします。 クローン作成によるプロビジョニングの準備のためのチェックリスト を参照してください。
Amazon Web Services	Amazon マシン イメージは、オペレーティング システムなどのソフトウェア構成を含むテンプレートです。ソフトウェア をサポートする Amazon マシン イメージを作成する場合、ルート デバイスの EBS ボリュームを使用する実行中の Amazon Web Services インスタンスに接続します。ゲスト エージェントおよびソフトウェア ブートストラップ エージェントをリファレンス マシン上にインストールし、インスタンスから Amazon マシン イメージを作成します。 プロビジョニングされたマシン上で機能するゲスト エージェントおよび ソフトウェア ブートストラップ エージェントについては、VPC へのネットワーク接続を構成する必要があります。 Amazon EBS に対応する AMI を作成する方法については、Amazon Web Services のドキュメントを参照してください。
Microsoft Azure	詳細については、 ソフトウェア コンポーネントの設定 、 Microsoft Azure 用のブループリントの作成 、および Microsoft Azure 製品のドキュメントを参照してください。

ソフトウェアを使用してマシンをプロビジョニングするための準備

ソフトウェア コンポーネントをサポートするには、クローン作成用のテンプレートの変換、Amazon マシン イメージの作成、またはスナップショットの取得の前に、ゲスト エージェントおよびソフトウェア ブートストラップ エージェントをリファレンス マシンにインストールする必要があります。

Windows リファレンス マシンで ソフトウェア をサポートするための準備

Windows リファレンス マシンに、Java Runtime Environment、ゲスト エージェント、ソフトウェア ブートストラップ エージェントを単一のスクリプトを使用してインストールします。リファレンス マシンから、クローン作成、スナップショット、ソフトウェア コンポーネントをサポートする Amazon マシン イメージに使用するテンプレートを作成できます。

ソフトウェア は、Windows CMD および PowerShell 2.0 によるスクリプトをサポートしています。

重要： 起動処理を中断しないようにします。ログイン プロンプトに到達する前に仮想マシン起動処理が一時停止されないように仮想マシンを設定します。たとえば、仮想マシンの起動中に、ユーザーの操作を求めるプロセスやスクリプトが表示されないようにします。

前提条件

- Windows リファレンス マシンを特定または作成します。
- リファレンス マシンと IaaS Manager Service ホスト間のセキュアな信頼を確立します。[サーバを信頼するゲスト エージェントの構成](#)を参照してください。
- トラブルシューティングなどの理由で、マシンにリモートでアクセスする場合は、リモート デスクトップ サービス (RDS) をインストールします。
- ネットワーク構成ファイルからネットワーク構成のアーティファクトを削除します。

手順

- 1 Windows リファレンス マシンに管理者としてログインします。
- 2 vRealize Automation アプライアンスのブラウザでソフトウェアのダウンロード ページを開きます。
`https://vrealize-automation-appliance-FQDN/software`
- 3 テンプレートの ZIP を Windows サーバに保存します。
`prepare_vra_template_windows.zip`
- 4 ZIP コンテンツをフォルダに抽出して、バッチ ファイルを実行します。
`.\prepare_vra_template.bat`
- 5 プロンプトの指示に従います。
- 6 完了したら、Windows 仮想マシンをシャットダウンします。

結果

以前のホストまたは ソフトウェア ブートストラップ エージェントがある場合はスクリプトによって削除され、Java Runtime Environment のサポートされているバージョン、ゲスト エージェント、および ソフトウェア ブートストラップ エージェントがインストールされます。

次のステップ

リファレンス マシンを、クローン作成、スナップショット、または Amazon マシン イメージに使用するテンプレートに変換します。各テンプレートが ソフトウェア コンポーネントをサポートし、インフラストラクチャ アーキテククトは、ブループリントの作成時にこれを使用することができます。

Linux リファレンス マシンで ソフトウェア をサポートするための準備

Linux リファレンス マシンに、Java Runtime Environment、ゲスト エージェント、ソフトウェア ブートストラップ エージェントを単一のスクリプトを使用してインストールします。リファレンス マシンから、クローン作成、スナップショット、ソフトウェア コンポーネントをサポートする Amazon マシン イメージに使用するテンプレートを作成できます。

ソフトウェア では、Bash によるスクリプトをサポートしています。

重要： ブート処理を中断しないようにします。ログイン プロンプトに到達する前に仮想マシンのブート処理が一時停止されないように仮想マシンを設定します。たとえば、仮想マシンの起動中に、ユーザーの操作を求めるプロセスやスクリプトが表示されないようにします。

前提条件

- Linux リファレンス マシンを指定または作成を行います。
- Linux システムに応じて、次のコマンドを使用できることを確認します。
 - yum または apt-get
 - wget または curl
 - python
 - dmidecode (クラウド プロバイダによって必要な場合)
 - Linux ディストリビューションに応じた、sed、awk、perl、chkconfig、unzip、grep などの一般的な要件

エディタを使用して、ダウンロードした `prepare_vra_template.sh` スクリプトを調べ、使用されているコマンドを特定することもできます。

- トラブルシューティングなどの理由で、マシンにリモートでアクセスする場合は、OpenSSH をインストールします。
- ネットワーク構成ファイルからネットワーク構成のアーティファクトを削除します。

手順

- 1 root としてリファレンス マシンにログインします。

- 2 vRealize Automation アプライアンスからテンプレートの tar.gz パッケージをダウンロードします。

```
wget https://vrealize-automation-appliance-FQDN/software/download/
prepare_vra_template_linux.tar.gz
```

環境内で自己署名証明書を使用している場合、`--no-check-certificate` オプションが必要になる場合があります。

```
wget --no-check-certificate https://vrealize-automation-appliance-FQDN/software/download/
prepare_vra_template_linux.tar.gz
```

- 3 tar パッケージを解凍します。

```
tar -xvf prepare_vra_template_linux.tar.gz
```

- 4 解凍の出力でインストーラ スクリプトを見つけて、実行可能の状態にします。

```
chmod +x prepare_vra_template.sh
```

- 5 インストーラ スクリプトを実行します。

```
./prepare_vra_template.sh
```

非対話型のオプションおよび想定される値に関する情報が必要な場合、スクリプトのヘルプを参照してください。

```
./prepare_vra_template.sh --help
```

- 6 プロンプトの指示に従います。

インストールが成功すると、確認が表示されます。エラーとログが表示された場合は、エラーを解決してスクリプトを再実行します。

- 7 完了したら、Linux 仮想マシンをシャットダウンします。

結果

以前のホストまたは ソフトウェア ブートストラップ エージェントがある場合はスクリプトによって削除され、Java Runtime Environment のサポートされているバージョン、ゲスト エージェント、および ソフトウェア ブートストラップ エージェントがインストールされます。

次のステップ

ハイパーバイザーまたはクラウド プロバイダで、リファレンス マシンを、クローン作成、スナップショット、または Amazon マシン イメージに使用するテンプレートに変換します。各テンプレートが ソフトウェア コンポーネントをサポートし、インフラストラクチャ アーキテクトは、ブループリントの作成時にこれを使用することができます。

vRealize Automation での既存の仮想マシン テンプレートの更新

最新バージョンの Windows ソフトウェア ブートストラップ エージェントのテンプレート、Amazon マシン イメージ、スナップショットをアップデートする場合、または `prepare_vra_template.sh` スクリプトを使用する代わりに、最新の Linux ソフトウェア ブートストラップ エージェントに手動でアップデートする場合、すべての既存のバージョンを削除し、あらゆるログを削除する必要があります。

Linux

Linux リファレンス マシンの場合、`prepare_vra_template.sh` スクリプトを実行すると、エージェントがリセットされ、再インストールの前にすべてのログが削除されます。ただし、手動でインストールする場合は、root ユーザーとしてリファレンス マシンにログインし、リセットのコマンドを実行して製品を削除する必要があります。

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

Windows

Windows リファレンス マシンの場合、既存の ソフトウェア エージェント ブートストラップおよび vRealize Automation 6.0 以降のゲスト エージェントを削除し、すべての既存のランタイム ログ ファイルを削除します。PowerShell コマンド ウィンドウで、コマンドを実行して、エージェントおよび製品を削除します。

```
c:\opt\vmware-appdirector\agent-bootstrap\appd_bootstrap_removal.bat
```

クローン マシンの vSphere テンプレートとソフトウェア コンポーネント ブループリントを準備

vCenter Server 管理者として、vRealize Automation アーキテクトが Linux CentOS マシンなどのクローンを作成する際に使用できる vSphere テンプレートを準備したいと考えています。テンプレートでソフトウェア コンポーネントを持つブループリントをサポートできるようにしたいと考えているため、リファレンス マシンをテンプレートに変換する前に、ゲスト エージェントおよびソフトウェア ブートストラップ エージェントをインストールします。

前提条件

- VMware Tools がインストールされている Linux CentOS リファレンス マシンを特定または作成します。1 つ以上のネットワーク アダプタを追加し、ブループリント アーキテクトによってこの機能がブループリント レベルで追加されない場合にインターネット接続を提供します。仮想マシンの作成に関する詳細については、vSphere のドキュメントを参照してください。
- 仮想マシンをテンプレートに変換するには、vCenter Server に接続されている必要があります。vSphere Client を直接 vSphere ESXi ホストに接続した場合、テンプレートを作成することはできません。

手順

1 シナリオ：ゲスト エージェント カスタマイズとソフトウェア コンポーネントを使用できるようにリファレンス マシンを準備する

テンプレートでソフトウェア コンポーネントをサポートできるようにするために、ソフトウェア ブートストラップ エージェントとその前提条件であるゲスト エージェントをリファレンス マシンにインストールします。これらのエージェントにより、テンプレートを使用する vRealize Automation アーキテクトは、ブループリントにソフトウェア コンポーネントを確実に含めることができます。

2 シナリオ：CentOS リファレンス マシンをテンプレートに変換する

ゲスト エージェントとソフトウェア ブートストラップ エージェントをリファレンス マシンにインストールしたら、リファレンス マシンをテンプレートに変換して、vRealize Automation アーキテクトがクローン マシン ブループリントの作成に使用できるようにします。

3 シナリオ：vSphere クローン作成用のカスタム仕様を作成する

ブループリント アーキテクトが cpb_centos_63_x84 テンプレートで利用できるカスタム仕様を作成します。

結果

Linux CentOS マシンのクローンを作成する vRealize Automation ブループリントの作成にブループリント アーキテクトが使用できるリファレンス マシンから、テンプレートおよびカスタム仕様を作成しました。ソフトウェア ブートストラップ エージェントおよびゲスト エージェントをリファレンス マシンにインストールしているため、アーキテクトはテンプレートを使用し、スクリプトの実行やディスクのフォーマットなど、ソフトウェア コンポーネントまたは他のゲスト エージェントのカスタマイズを含む高度なカタログ アイテム ブループリントを作成できます。また、VMware Tools をインストールしているため、アーキテクトおよびカタログ管理者は、再構成、スナップショット、再起動などのアクションをマシンに対して実行する許可をユーザーに付与できます。

次のステップ

vRealize Automation のユーザー、グループ、およびリソースを設定したら、テンプレートとカスタム仕様を使用して、クローン作成用のマシン ブループリントを作成することができます。『[マシンのブループリントの設定](#)』を参照してください。

シナリオ：ゲスト エージェント カスタマイズとソフトウェア コンポーネントを使用できるようにリファレンス マシンを準備する

テンプレートでソフトウェア コンポーネントをサポートできるようにするために、ソフトウェア ブートストラップ エージェントとその前提条件であるゲスト エージェントをリファレンス マシンにインストールします。これらのエージェントにより、テンプレートを使用する vRealize Automation アーキテクトは、ブループリントにソフトウェア コンポーネントを確実に含めることができます。

このプロセスを簡素化するために、個々のパッケージをダウンロードしてインストールするのではなく、両方のエージェントをインストールする vRealize Automation スクリプトをダウンロードして実行します。

このスクリプトは、Manager Service インスタンスに接続して SSL 証明書のダウンロードも行います。これにより、テンプレートから展開されたマシンと Manager Service 間に信頼関係が確立されます。スクリプトで証明書をダウンロードする方法は、手動で Manager Service SSL 証明書を取得して、リファレンス マシンの `/usr/share/gugent/cert.pem` にインストールする方法よりもセキュリティが低下することに注意してください。

手順

- 1 ブラウザを開き、vRealize Automation アプライアンス ソフトウェア ページにアクセスします。

`https://vrealize-automation-appliance-FQDN/software`

- 2 [Linux Software Installers] で圧縮された tar ファイルをダウンロードします。

`prepare_vra_template_linux.tar.gz`

- 3 tar ファイルを Linux リファレンス マシンの一時ディレクトリに移動します。

ファイルを転送するには、WinSCP などのツールを実行するか、使い慣れた他の方法を使用します。

- 4 Linux リファレンス マシンのコマンド プロンプトに root としてログインします。

ターミナルを開くには、vRealize Automation 内からマシンのリモート コンソールを起動するか、使い慣れている他の方法を使用します。

- 5 一時ディレクトリから tar ファイルを抽出します。

```
gunzip prepare_vra_template_linux.tar.gz
```

- 6 tar ファイルの内容を抽出します。

```
tar xvf prepare_vra_template_linux.tar
```

- 7 スクリプト ディレクトリに移動します。

```
cd prepare_vra_template_linux
```

- 8 スクリプトをクリックし、表示される指示に従います。

```
/prepare_vra_template.sh
```

オプションと値に関して、対話形式以外の情報が必要な場合は、 と入力します。/prepare_vra_template.sh --help.

結果

インストールが完了すると、確認メッセージが表示されます。エラー メッセージとログが表示された場合は、問題を解消してから、スクリプトを再実行します。

シナリオ : CentOS リファレンス マシンをテンプレートに変換する

ゲスト エージェントとソフトウェア ブートストラップ エージェントをリファレンス マシンにインストールしたら、リファレンス マシンをテンプレートに変換して、vRealize Automation アーキテクトがクローン マシン ブループリントの作成に使用できるようにします。

リファレンス マシンをテンプレートに変換したら、それを変換して仮想マシンに戻さないかぎり、そのテンプレートは編集することもパワーオンすることもできません。

手順

- 1 root ユーザーとしてリファレンス マシンにログインして、マシンを変換する準備をします。

- a udev 持続性ルールを削除します。

```
/bin/rm -f /etc/udev/rules.d/70*
```

- b このテンプレートからクローン作成されたマシンに一意の識別子を割り当てられるようにします。

```
/bin/sed -i '/^\(HWADDR\|UUID\)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- c ソフトウェア ブートストラップ エージェントのインストール後にリファレンス マシンを再起動または再構成した場合は、エージェントをリセットします。

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

- d マシンをパワーオフします。

```
shutdown -h now
```

- 2 vSphere Web Client に管理者としてログインします。
- 3 参照マシンを右クリックして、[設定の編集] を選択します。
- 4 [仮想マシン名] テキスト ボックスに **cpb_centos_63_x84** と入力します。
- 5 リファレンス マシンでゲスト OS として CentOS が動作している場合でも、[ゲスト OS のバージョン] ドロップダウン メニューから [Red Hat Enterprise Linux 6 (64-bit)] を選択します。
CentOS を選択すると、テンプレートとカスタム仕様 が期待どおりに動作しないことがあります。
- 6 vSphere Web Client でリファレンス マシンを右クリックして、[テンプレート] - [テンプレートに変換] を選択します。

結果

vCenter Server は、cpb_centos_63_x84 リファレンス マシンにテンプレートとしてマークを付け、[最近のタスク] ペインにタスクを表示します。すでに vSphere 環境が vRealize Automation の管理下にある場合は、テンプレートが次の自動データ収集時に検出されます。vRealize Automation をまだ構成していない場合、テンプレートはそのとき実行中のプロセスで収集されます。

シナリオ：vSphere クローン作成用のカスタム仕様 を作成する

ブループリント アーキテクトが cpb_centos_63_x84 テンプレートで利用できるカスタム仕様 を作成します。

手順

- 1 vSphere Web Client に管理者としてログインします。
- 2 ホーム ページの [カスタム仕様 マネージャ] をクリックしてウィザードを開きます。
- 3 [新規] アイコンをクリックします。
- 4 [新規] アイコンをクリックします。
- 5 プロパティを指定します。
 - a [ターゲット仮想マシン オペレーティング システム] ドロップダウン メニューから [Linux] を選択します。
 - b [カスタム仕様 名] テキスト ボックスに **Customspecs** と入力します。
 - c [説明] テキスト ボックスに **cpb_centos_63_x84 cloning with vRealize Automation** と入力します。
 - d [次へ] をクリックします。

6 コンピュータ名を設定します。

- a [仮想マシン名を使用] を選択します。
- b [ドメイン名] テキスト ボックスに、プロビジョニングする予定の、クローン作成されたマシンのドメインを入力します。
- c [次へ] をクリックします。

7 タイム ゾーン設定を構成します。**8** [次へ] をクリックします。**9** [ゲスト OS に標準ネットワーク設定を使用します (すべてのネットワーク インターフェイスで DHCP を有効化など)] を選択します。

ファブリック管理者とインフラストラクチャ アーキテクトは、vRealize Automation のネットワーク プロファイルを作成および使用して、プロビジョニングされたマシンのネットワーク設定を行います。

10 プロンプトの指示に従って残りの必須情報を入力します。**11** [完了前の確認] ページで選択内容を確認し、[終了] をクリックします。**結果**

シナリオ : Dukes Bank for vSphere サンプル アプリケーション ブループリントをインポートするための準備

vCenter Server 管理者として、vRealize Automation Dukes Bank サンプル アプリケーションのプロビジョニングに使用する vSphere CentOS 6.x Linux テンプレートとカスタマイズ仕様を準備しようとしています。

テンプレートで、サンプル アプリケーション ソフトウェア コンポーネントを確実にサポートするため、Linux リファレンス マシンにゲスト エージェントとソフトウェア ブートストラップ エージェントをインストールしてから、そのリファレンス マシンをテンプレートに変換して、カスタマイズ仕様を作成します。リファレンス マシンで SELinux を無効にして、Dukes Bank サンプル アプリケーションで使用されている特定の MySQL の実装をテンプレートがサポートするようにします。

前提条件

- VMware Tools がインストールされている CentOS 6.x Linux リファレンス マシンを特定または作成します。仮想マシンの作成に関する詳細については、vSphere のドキュメントを参照してください。

- 仮想マシンをテンプレートに変換するには、vCenter Server に接続されている必要があります。vSphere Client を直接 vSphere ESXi ホストに接続した場合、テンプレートを作成することはできません。

手順

1 シナリオ : Dukes Bank vSphere サンプル アプリケーションをサポートできるようにリファレンス マシンを準備する

テンプレートで Dukes Bank サンプル アプリケーションをサポートするため、ゲスト エージェントとソフトウェア ブートストラップ エージェントの両方をリファレンス マシンにインストールして、vRealize Automation がソフトウェア コンポーネントをプロビジョニングできるようにする必要があります。プロセスを単純化するため、パッケージを個別にダウンロードおよびインストールする代わりに、ゲスト エージェントとソフトウェア ブートストラップ エージェントの両方をインストールする vRealize Automation スクリプトをダウンロードして実行します。

2 シナリオ : リファレンス マシンを Dukes Bank vSphere アプリケーションのテンプレートに変換する

リファレンス マシンにゲスト エージェントとソフトウェア ブーストラップ エージェントをインストールした後は、SELinux を無効にして、Dukes Bank サンプル アプリケーションで使用されている特定の MySQL の実装をテンプレートがサポートするようにします。リファレンス マシンを、Dukes Bank vSphere サンプル アプリケーションのプロビジョニングに使用できるテンプレートにします。

3 シナリオ : Dukes Bank vSphere サンプル アプリケーション マシンのクローン作成のためのカスタマイズ仕様を作成する

Dukes Bank マシン テンプレートで使用するカスタマイズ仕様を作成します。

結果

vRealize Automation Dukes Bank サンプル アプリケーションをサポートしているリファレンス マシンからテンプレートとカスタム仕様を作成しました。

シナリオ : Dukes Bank vSphere サンプル アプリケーションをサポートできるようにリファレンス マシンを準備する

テンプレートで Dukes Bank サンプル アプリケーションをサポートするため、ゲスト エージェントとソフトウェア ブートストラップ エージェントの両方をリファレンス マシンにインストールして、vRealize Automation がソフトウェア コンポーネントをプロビジョニングできるようにする必要があります。プロセスを単純化するため、パッケージを個別にダウンロードおよびインストールする代わりに、ゲスト エージェントとソフトウェア ブートストラップ エージェントの両方をインストールする vRealize Automation スクリプトをダウンロードして実行します。

手順

- 1 root ユーザーとしてリファレンス マシンにログインします。
- 2 vRealize Automation アプライアンスからインストール用スクリプトをダウンロードします。

```
wget https://vRealize_VA_Hostname_fqdn/software/download/prepare_vra_template.sh
```

環境で自己署名証明書を使用している場合は、wget オプション `--no-check-certificate` を使用しなければならない場合があります。例：

```
wget --no-check-certificate https://vRealize_VA_Hostname_fqdn/software/download/prepare_vra_template.sh
```

- 3 `prepare_vra_template.sh` スクリプトを実行可能にします。

```
chmod +x prepare_vra_template.sh
```

- 4 `prepare_vra_template.sh` インストーラ スクリプトを実行します。

```
./prepare_vra_template.sh
```

非対話オプションおよび期待値の詳細を確認するには、ヘルプ コマンド `./prepare_vra_template.sh --help` を実行します。

- 5 プロンプトの指示に従って、インストールを完了します。

インストールが正常に完了すると、確認メッセージが表示されます。コンソールにエラー メッセージとログが表示されたら、エラーを解決して、インストール用スクリプトを再実行してください。

結果

ソフトウェア ブートストラップ エージェントと、その前提条件として必要なゲスト エージェントをインストールしました。これにより、Dukes Bank サンプル アプリケーションによって正常にソフトウェア コンポーネントがプロビジョニングされます。このスクリプトは Manager Service インスタンスにも接続し、SSL 証明書もダウンロードして、Manager Service とテンプレートから展開されたマシン間に信頼関係を確立しました。セキュリティという観点から見ると、この方法よりも、Manager Service SSL 証明書を取得して、`/usr/share/gugent/cert.pem` にあるリファレンス マシンに手動でインストールしたほうが安全です。セキュリティ保護の優先度が高い場合は、今すぐこの証明書を手動で置換することもできます。

シナリオ：リファレンス マシンを Dukes Bank vSphere アプリケーションのテンプレートに変換する

リファレンス マシンにゲスト エージェントとソフトウェア ブーストラップ エージェントをインストールした後は、SELinux を無効にして、Dukes Bank サンプル アプリケーションで使用されている特定の MySQL の実装をテンプレートがサポートするようにします。リファレンス マシンを、Dukes Bank vSphere サンプル アプリケーションのプロビジョニングに使用できるテンプレートにします。

リファレンス マシンをテンプレートに変換したら、それを変換して仮想マシンに戻さないかぎり、そのテンプレートは編集することもパワーオンすることもできません。

手順

- 1 root ユーザーとしてリファレンス マシンにログインします。

- a /etc/selinux/config ファイルを編集し、SELinux を無効にします。

```
SELINUX=disabled
```

SELinux を無効にしないと、Dukes Bank のサンプル アプリケーションの MySQL ソフトウェア コンポーネントが意図したとおりに動作しない場合があります。

- b udev 持続性ルールを削除します。

```
/bin/rm -f /etc/udev/rules.d/70*
```

- c このテンプレートからクローン作成されたマシンに一意的識別子を割り当てられるようにします。

```
/bin/sed -i '/^\(HWADDR\|UUID\)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- d ソフトウェア ブートストラップ エージェントのインストール後にリファレンス マシンを再起動または再構成した場合は、エージェントをリセットします。

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

- e マシンをパワーオフします。

```
shutdown -h now
```

- 2 vSphere Web Client に管理者としてログインします。

- 3 参照マシンを右クリックして、[設定の編集] を選択します。

- 4 [仮想マシン名] テキスト ボックスに、**dukes_bank_template** と入力します。

- 5 リファレンス マシンでゲスト OS として CentOS が稼動している場合は、[ゲスト OS のバージョン] ドロップダウン メニューから [Red Hat Enterprise Linux 6 (64-bit)] を選択します。

CentOS を選択すると、テンプレートとカスタム仕様 が期待どおりに動作しないことがあります。

- 6 [OK] をクリックします。

- 7 vSphere Web Client でリファレンス マシンを右クリックして、[テンプレート] - [テンプレートに変換] を選択します。

結果

vCenter Server は、dukes_bank_template リファレンス マシンにテンプレートとしてマークを付け、[最近のタスク] ペインにタスクを表示します。すでに vSphere 環境が vRealize Automation の管理下にある場合は、テンプレートが次の自動データ収集時に検出されます。vRealize Automation をまだ構成していない場合、テンプレートはそのとき実行中のプロセスで収集されます。

シナリオ: Dukes Bank vSphere サンプル アプリケーション マシンのクローン作成のためのカスタマイズ仕様を作成する

Dukes Bank マシン テンプレートで使用するカスタマイズ仕様を作成します。

手順

- 1 vSphere Web Client に管理者としてログインします。
- 2 ホーム ページの [カスタム仕様 マネージャ] をクリックしてウィザードを開きます。
- 3 [新規] アイコンをクリックします。
- 4 プロパティを指定します。
 - a [ターゲット仮想マシン オペレーティング システム] ドロップダウン メニューから [Linux] を選択します。
 - b [カスタマイズ仕様名] テキスト ボックスに **Customspecs_sample** と入力します。
 - c [説明] テキスト ボックスに **Dukes Bank customization spec** と入力します。
 - d [次へ] をクリックします。
- 5 コンピュータ名を設定します。
 - a [仮想マシン名を使用] を選択します。
 - b [ドメイン名] テキスト ボックスに、Dukes Bank サンプル アプリケーションのプロビジョニング先ドメインを入力します。
 - c [次へ] をクリックします。
- 6 タイム ゾーン設定を構成します。
- 7 [次へ] をクリックします。
- 8 [ゲスト OS に標準ネットワーク設定を使用します (すべてのネットワーク インターフェイスで DHCP を有効化など)] を選択します。

 ファブリック管理者とインフラストラクチャ アーキテクトは、vRealize Automation のネットワーク プロファイルを作成および使用して、プロビジョニングされたマシンのネットワーク設定を行います。
- 9 プロンプトの指示に従って残りの必須情報を入力します。
- 10 [完了前の確認] ページで選択内容を確認し、[終了] をクリックします。

結果

Dukes Bank サンプル アプリケーションのプロビジョニングに使用するテンプレートとカスタマイズ仕様を作成しました。

次のステップ

- 1 外部ネットワーク プロファイルを作成して、ゲートウェイと IP アドレスの範囲を指定します。 [サードパーティの IP アドレス管理プロバイダを使用した外部ネットワーク プロファイルの作成](#)を参照してください。

- 2 外部ネットワーク プロファイルを vSphere 予約にマップします。[Hyper-V](#)、[KVM](#)、[SCVMM](#)、[vSphere](#)、[XenServer](#) の[予約の作成](#)を参照してください。サンプル アプリケーションは、外部ネットワーク プロファイルがないとプロビジョニングを正常に行うことができません。
- 3 Duke's Bank サンプル アプリケーションを環境内にインポートします。[シナリオ：Dukes Bank for vSphere](#) サンプル アプリケーションをインポートし、[環境に合わせて構成する](#)を参照してください。

ブループリントのプロビジョニングのためのテナントとリソースの準備

2

複数のテナント環境を構成し、それぞれの環境で独自のユーザー グループと vRealize Automation の管理下に置いたリソースに対する固有のアクセス権を設定できます。

この章には、次のトピックが含まれています。

- [テナント設定の構成](#)
- [リソースの構成](#)
- [通知と代理人のユーザー環境設定](#)

テナント設定の構成

テナント管理者は、ユーザー認証などのテナント設定を構成し、ユーザー ロールとビジネス グループを管理します。システム管理者とテナント管理者は、通知を処理するメール サーバ、vRealize Automation コンソールのブランディングなどのオプションを構成します。

テナント設定の構成のチェックリストを使用すると、テナント設定の構成に必要な手順の概要を確認できます。

表 2-1. テナント設定の構成のチェックリスト

タスク	vRealize Automation	ロール	詳細
<input type="checkbox"/> ローカル ユーザー アカウントを作成し、テナント管理者を割り当てます。	システム管理者		デフォルト テナントへのアクセスの構成
<input type="checkbox"/> ディレクトリ管理を構成して、テナント ID 管理とアクセス コントロールの設定を行います。	テナント管理者		ディレクトリ管理構成オプションの選択
<input type="checkbox"/> ビジネス グループとカスタム グループを作成し、vRealize Automation コンソールへのユーザー アクセス権を付与します。	テナント管理者		グループとユーザーのロールの構成
<input type="checkbox"/> (オプション) 追加のテナントを作成して、ユーザーが、割り当てられた作業を完了するために必要なアプリケーションやリソースにアクセスできるようにします。	システム管理者		追加テナントの作成
<input type="checkbox"/> (オプション) vRealize Automation コンソールのテナント ログイン ページとアプリケーション ページのカスタム ブランディングを構成します。	<ul style="list-style-type: none">■ システム管理者■ テナント管理者		カスタム ブランディングの構成
<input type="checkbox"/> (オプション) 特定のイベントの発生時にユーザー通知を送信するように vRealize Automation を構成します。	<ul style="list-style-type: none">■ システム管理者■ テナント管理者		通知構成のチェックリスト

表 2-1. テナント設定の構成のチェックリスト（続き）

タスク	vRealize Automation ロール	詳細
<input type="checkbox"/> （オプション）XaaS およびその他の拡張機能をサポートするように vRealize Orchestrator を構成します。	<ul style="list-style-type: none"> ■ システム管理者 ■ テナント管理者 	vRealize Orchestrator の設定
<input type="checkbox"/> （オプション）RDP 設定を構成するために IaaS アーキテクトがブループリントで使用するカスタム リモート デスクトップ プロトコル ファイルを作成します。	システム管理者	プロビジョニングされたマシンで RDP 接続をサポートするためのカスタム RDP ファイルの作成
<input type="checkbox"/> （オプション）ユーザーがマシンを申請するときにプロビジョニングに適切な場所を選択できるようにするためにファブリック管理者や IaaS アーキテクトが利用できる、データセンターの場所を定義します。	システム管理者	データセンターの場所を追加する例については、 シナリオ: 複数の拠点にまたがる導入環境向けにデータセンターの場所を追加する を参照してください。

ディレクトリ管理構成オプションの選択

vRealize Automation のディレクトリ管理機能を使用し、ユーザー認証要件に従って Active Directory リンクを構成できます。

ディレクトリ管理には、ユーザー認証を高度にカスタマイズできるように多くのオプションが用意されています。

表 2-2. ディレクトリ管理構成オプションの選択

構成オプション	手順
Active Directory へのリンクを構成します。	<ol style="list-style-type: none"> 1 Active Directory へのリンクを構成します。Active Directory over LDAP/IWA リンクの構成 を参照してください。 2 vRealize Automation を高可用性向けに構成した場合は、高可用性を実現するためのディレクトリ管理の構成 を参照してください。
（オプション）Active Directory フェデレーション サービスと双方向で連携することで、ユーザー ID とパスワードを使用したディレクトリリンクのセキュリティを強化します。	vRealize Automation と Active Directory 間で双方向の信頼関係を構築
（オプション）既存の Active Directory リンクにユーザーおよびグループを追加します。	Active Directory 接続へのユーザーまたはグループの追加。
（オプション）デフォルト ポリシーを編集し、Active Directory リンクにカスタム ルールを適用します。	ユーザー アクセス ポリシーの管理。
（オプション）ネットワーク範囲を設定して、ユーザーがシステムへのログインに使用する IP アドレスを制限し、ログイン制限（タイムアウト、ロックアウトされるまでのログイン試行回数）を管理します。	ネットワーク範囲の追加または編集。

ディレクトリ管理の概要

テナント管理者は、vRealize Automation アプリケーション コンソールのディレクトリ管理オプションを使用してテナントの ID 管理とアクセス コントロール設定を構成できます。

[管理] - [ディレクトリ管理] タブから次の設定を管理できます。

表 2-3. ディレクトリ管理の設定

設定	説明
ディレクトリ	<p>[ディレクトリ] ページは、アクティブ ディレクトリ リンクを作成および管理して、vRealize Automation テナント ユーザーの認証と権限をサポートできるようにします。1 つ以上のディレクトリを作成してから、Active Directory を展開した環境とこれらのディレクトリを同期します。このページには、ディレクトリと同期されたグループとユーザーの数と最後に同期された時間が表示されます。[今すぐ同期] をクリックして、ディレクトリの同期を手動にて開始できます。</p> <p>ディレクトリ管理による Active Directory リンクの作成を参照してください。</p> <p>ディレクトリをクリックして [同期設定] をクリックすると、同期設定の編集、ID プロバイダ ページの移動、および同期ログの表示ができます。</p> <p>ディレクトリ同期設定のページから、同期頻度をスケジュールできます。このディレクトリに関連付けられているドメインリストの表示、マッピングされている属性のリストを変更、同期するユーザーとグループのリストのアップデート、およびセーフガードのターゲット設定をします。</p>
コネクタ	<p>[コネクタ] ページには、エンタープライズ ネットワークの展開されたコネクタが一覧表示されます。コネクタは、Active Directory とディレクトリ管理サービス間でユーザーとグループ データを同期し、ID プロバイダとして使用される場合には、サービスに対してユーザーを認証します。デフォルトで、各 vRealize Automation アプライアンスにはコネクタが含まれます。コネクタとコネクタ クラスターの管理を参照してください。</p>
ユーザー属性	<p>[ユーザー属性] ページには、このディレクトリと同期するデフォルトのユーザー属性が表示され、他の属性を追加して、Active Directory の属性にマッピングできます。ディレクトリと同期する属性の選択を参照してください。</p>
ネットワーク範囲	<p>このページには、システムに構成されているネットワーク範囲が一覧表示されます。ネットワーク範囲を構成し、これらの IP アドレスを介したユーザー アクセスを許可します。ネットワーク範囲の追加や、既存の範囲の編集ができます。ネットワーク範囲の追加または編集を参照してください。</p>
ID プロバイダ	<p>[ID プロバイダ] ページには、システムで使用可能な ID プロバイダが一覧表示されます。vRealize Automation システムには、デフォルトの ID プロバイダとして予約し、多数のユーザーのニーズを満たすコネクタが含まれます。サードパーティの ID プロバイダ インスタンスを追加したり、両方を組み合わせて使用できます。</p> <p>サードパーティ ID プロバイダの接続の構成を参照してください。</p>
ポリシー	<p>[ポリシー] ページには、デフォルトのアクセス ポリシーとユーザーが作成した他の Web アプリケーションのアクセス ポリシーが表示されます。ポリシーとは、アプリケーション ポータルにアクセスしたり、ユーザー向けに有効になっている Web アプリケーションを起動したりするユーザーが満たす必要がある条件を指定する一連のルールです。デフォルトのポリシーは、ほとんどの vRealize Automation 展開に適している必要がありますが、必要に応じて編集できます。ユーザー アクセス ポリシーの管理を参照してください。</p>

Active Directory に関連する重要な概念

Directories Management が Active Directory 環境を統合する方法を理解するうえで、Active Directory に関するいくつかの概念を把握しておく必要があります。

コネクタ

このサービスのコンポーネントである コネクタ は、次の機能を実行します。

- Active Directory とサービス間でユーザーとグループを同期します。
- ID プロバイダとして使用される場合、サービスに対してユーザーを認証します。

コネクタ は、デフォルト ID プロバイダになります。コネクタ でサポートしている認証方法については、『VMware Identity Manager の管理』を参照してください。SAML 2.0 プロトコルをサポートするサードパーティ ID プロバイダを使用することもできます。企業のセキュリティ ポリシーにとってサードパーティ ID プロバイダが適切である場合には、コネクタ がサポートしていない認証タイプまたは コネクタ がサポートする認証タイプにサードパーティ ID プロバイダを使用します。

注： サードパーティ ID プロバイダを使用する場合であっても、コネクタ を構成してユーザーとグループ データを同期する必要があります。

ディレクトリ

Directories Management サービスには、ディレクトリに関する独自の概念があり、Active Directory の属性とパラメータを使用して、ユーザーとグループを定義します。1つ以上のディレクトリを作成してから、Active Directory を展開した環境とこれらのディレクトリを同期します。サービスでは次のディレクトリ タイプを作成できます。

- LDAP 経由の Active Directory 単一の Active Directory ドメイン環境に接続する計画である場合には、このディレクトリ タイプを作成します。LDAP 経由の Active Directory のディレクトリ タイプでは、コネクタ は単純なバインド認証を使用して Active Directory をバインドします。
- Active Directory、統合 Windows 認証マルチドメインまたはマルチフォレストの Active Directory ドメイン環境に接続する計画である場合には、このディレクトリ タイプを作成します。コネクタ は、統合 Windows 認証を使用して Active Directory をバインドします。

単一ドメインかマルチドメインか、ドメイン間で使用される信頼のタイプなど、ユーザーの Active Directory 環境によって、作成するディレクトリのタイプと数は変わります。通常環境では、作成するディレクトリは1つになります。

このサービスは、Active Directory に直接アクセスしません。コネクタ だけが、Active Directory に直接アクセスします。したがって、コネクタ インスタンスとこのサービスで作成された各ディレクトリを関連付けます。

ワーカー

コネクタ インスタンスをディレクトリに関連付けるときに、コネクタは、ワーカーと呼ばれる、関連付けられたディレクトリのパーティションを作成します。コネクタ インスタンスには、複数のワーカーを関連付けることができます。各ワーカーは、ID プロバイダとして動作します。ワーカー毎に認証方法を定義および構成します。

コネクタは、1つ以上のワーカーを介して Active Directory とサービス間でユーザーとグループを同期します。

同じコネクタ インスタンスでは、統合 Windows 認証タイプの 2 つのワーカーを使用することはできません。

Active Directory 環境

このサービスは、単一の Active Directory ドメイン、単一の Active Directory フォレスト内の複数のドメイン、または複数の Active Directory フォレストにわたる複数のドメインを持つ Active Directory 環境と統合できます。

単一の Active Directory ドメイン環境

単一の Active Directory 環境では、単一の Active Directory ドメインのユーザーとグループを同期できます。

[Active Directory over LDAP/IWA リンクの構成](#) を参照してください。この環境で、サービスにディレクトリを追加するときには、LDAP 経由の Active Directory オプションを選択します。

マルチ ドメイン、シングル フォレストの Active Directory 環境

マルチドメイン、シングル フォレストの Active Directory 環境では、単一フォレスト内の複数の Active Directory ドメインのユーザーとグループを同期できます。

Active Directory 環境向けのサービスは、単一の Active Directory、統合 Windows 認証のディレクトリ タイプとして、または、グローバル カタログ オプションで構成される LDAP 経由の Active Directory のディレクトリ タイプとして構成できます。

- 推奨されるオプションは、単一の Active Directory、統合 Windows 認証のディレクトリ タイプです。

[Active Directory over LDAP/IWA リンクの構成](#) を参照してください。この環境にディレクトリを追加するときに、[Active Directory (統合 Windows 認証)] オプションを選択します。

信頼関係があるマルチフォレスト Active Directory 環境

信頼関係があるマルチフォレスト Active Directory の展開では、ドメイン間に双方向の信頼が存在するフォレスト全体で複数の Active Directory ドメインのユーザーとグループを同期できます。

[Active Directory over LDAP/IWA リンクの構成](#) を参照してください。この環境にディレクトリを追加するときには、Active Directory (統合 Windows 認証) オプションを選択します。

信頼関係がないマルチフォレスト Active Directory 環境

信頼関係がないマルチフォレスト Active Directory の展開では、ドメイン間に信頼関係がないフォレスト全体で複数の Active Directory ドメインのユーザーとグループを同期できます。この環境では、各フォレストに対して1つディレクトリを作成し、サービス内で複数のディレクトリを作成します。

[Active Directory over LDAP/IWA リンクの構成](#) を参照してください。サービスで作成するディレクトリのタイプは、フォレストによって変わります。複数のドメインがあるフォレストでは、Active Directory (統合 Windows 認証) オプションを選択します。単一ドメインのフォレストでは、LDAP 経由の Active Directory オプションを選択します。

ディレクトリ管理による Active Directory リンクの作成

vRealize Automation テナントを作成したら、テナント管理者としてシステム コンソールにログインし、ユーザー認証をサポートする Active Directory リンクを作成する必要があります。

ディレクトリ管理を使用して Active Directory 接続を構成する際、3 つの Active Directory 通信プロトコルのオプションがあります。

- LDAP 経由の Active Directory - LDAP 経由の Active Directory プロトコルでは、デフォルトで DNS サービス ロケーション検索がサポートされます。
- Active Directory (統合 Windows 認証) - Active Directory (統合 Windows 認証) では、参加するドメインを構成します。LDAP 経由の Active Directory は、単一ドメインの展開に適しています。マルチドメインおよびマルチフォレストの展開には、Active Directory (統合 Windows 認証) を使用します。
- OpenLDAP - LDAP のオープン ソース版を使用してディレクトリ管理のユーザー認証をサポートできます。

通信プロトコルを選択して Active Directory リンクを構成した後、Active Directory 構成で使用するドメインを指定したうえで、指定した構成との同期を取るユーザーやグループを選択することができます。

Active Directory over LDAP/IWA リンクの構成

ユーザー認証に対応するには、Active Directory over LDAP/IWA リンクを構成します。Directories Management 機能を使用して Active Directory とのリンクを構成し、すべてのテナントを対象にユーザー認証をサポートしたうえで、Directories Management ディレクトリとの間で同期するユーザーおよびグループを選択します。

ディレクトリ管理での OpenLDAP の使用に関する情報と手順については、[OpenLDAP ディレクトリ接続の設定](#)を参照してください。

Active Directory（統合 Windows 認証）では、マルチフォレスト Active Directory を構成し、ドメイン ローカル グループに異なるフォレストのドメイン メンバーが含まれる場合、ドメイン ローカル グループが存在するドメインの管理者グループにバインド ユーザーを必ず追加してください。この操作を実行できない場合、これらのメンバーはドメイン ローカル グループ内に存在しなくなります。

注： 最初にデフォルト テナントの Active Directory IWA ディレクトリを構成し、その後で他のテナントにそれらを追加することができます。

前提条件

- [ユーザー属性] ページで必須のデフォルト属性を選択し、その他の属性を追加します。[ディレクトリと同期する属性の選択](#)を参照してください。
- Active Directory から同期する Active Directory のグループとユーザーのリスト。
- Active Directory が SSL または STARTTLS 経由のアクセスを必要とする場合は、Active Directory ドメイン コントローラのルート CA 証明書が必要となります。
- テナント管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [ディレクトリ管理] - [ディレクトリ] を選択します。
- 2 [ディレクトリを追加] をクリックし、[Active Directory over LDAP/IWA の追加] を選択します。
- 3 [ディレクトリの追加] ページの [ディレクトリ名] テキスト ボックスで Active Directory サーバの IP アドレスを指定します。
- 4 [ディレクトリ名] テキスト ボックスの下にあるラジオ ボタンを使用して、適切な Active Directory 通信プロトコルを選択します。

オプション	説明
Windows 認証	[Active Directory（統合 Windows 認証）] を選択します。Active Directory（統合 Windows 認証）では、ドメインのバインド ユーザー UPN アドレスとパスワードなどの情報が必要となります。
LDAP	[LDAP 経由の Active Directory] を選択します。LDAP 経由の Active Directory の場合、ベース DN、バインド DN、およびバインド DN パスワードなどの情報が必要となります。

5 [ディレクトリの同期と認証] セクションで、Active Directory から VMware Directories Management ディレクトリにユーザーを同期するコネクタを構成します。

オプション	説明
同期コネクタ	お使いのシステムに適したコネクタを選択します。各 vRealize Automation アプライアンスにはデフォルトのコネクタが含まれています。適切なコネクタの選択について不明な点がある場合は、システム管理者に問い合わせてください。
認証	<p>適切なラジオ ボタンをクリックして、選択したコネクタで認証も行うかどうかを指定します。</p> <p>サード パーティの ID プロバイダとともに Active Directory (統合 Windows 認証) を使用してユーザーを認証している場合は、[いいえ] をクリックします。ユーザーとグループを同期するように Active Directory 接続を設定したら、[ID プロバイダ] ページを使用して、認証に使用するサードパーティ ID プロバイダを追加します。</p> <p>PasswordIpddAdapter、SecurIDAdapter、RadiusAuthAdapter などの認証アダプタを使用する方法の詳細については、『VMware Identity Manager 管理ガイド』を参照してください。</p>
ディレクトリ検索属性	<p>ユーザー名を含む適切なアカウント属性を選択します。userPrincipleName ではなく sAMAccount 属性を使用することをお勧めします。同期に userPrincipleName を使用すると、ユーザー名を必要とするセカンドおよびサードパーティ製のソフトウェアとの統合が正しく機能しない場合があります。</p> <p>注： 「サーバの場所」領域の [このディレクトリにグローバル カタログがある] チェック ボックスを選択して示されるグローバル カタログを使用する際、sAMAccountName を選択すると、ユーザーはログインできません。</p>

- 6 LDAP 経由の Active Directory を選択した場合は「サーバの場所」のテキスト ボックスに、または Active Directory (統合 Windows 認証) を選択した場合は「ドメインへの参加の詳細」テキスト ボックスに適切な情報を入力します。

オプション	説明
サーバの場所として、LDAP 経由の Active Directory を選択した場合に表示されます	<ul style="list-style-type: none"> ■ DNS サービスの場所を使用して Active Directory ドメインを検索する場合は、[このディレクトリは DNS サービスの場所をサポートする] チェック ボックスをオンのままにします。 <p>注： このオプションを選択する場合は、ポート割り当てを 636 に変更できません。</p> <p>ドメイン コントローラのリストが自動入力された domain_krb.properties ファイルが、ディレクトリと共に作成されます。ドメイン コントローラの選択を参照してください。</p> <p>Active Directory が STARTTLS 暗号化を必要とする場合は、[証明書] セクションの [このディレクトリには STARTTLS を使用するすべての接続が必要です] チェック ボックスを選択し、Active Directory のルート CA 証明書をコピーして [SSL 証明書] フィールドにペーストします。</p> <ul style="list-style-type: none"> ■ 指定した Active Directory が DNS サービスの場所検索を使用しない場合、サーバの場所フィールドの [このディレクトリは DNS サービスの場所をサポートする] の横にあるチェック ボックスを選択解除し、適切なテキスト ボックスに Active Directory サーバ ホスト名とポート番号を入力します。 <p>関連付けられている Active Directory がグローバル カタログを使用する場合は、[このディレクトリにグローバル カタログがある] チェック ボックスを選択します。グローバル カタログには、マルチ ドメイン Active Directory フォレスト内のすべてのドメイン内にあるすべてのオブジェクトの表現が含まれています。</p> <p>グローバル カタログとしてディレクトリを設定するには、Active Directory 環境 の「マルチドメイン、シングル フォレストの Active Directory 環境」セクションを参照してください。</p> <p>SSL を介して Active Directory にアクセスする必要がある場合は、[証明書] の下の [このディレクトリではすべての接続に SSL を使用する必要がある] チェック ボックスをオンにして、Active Directory SSL 証明書を指定します。</p> <p>このオプションを選択すると、ポート 636 が自動的に使用され、変更できません。</p> <p>証明書が PEM 形式であり、BEGIN CERTIFICATE と END CERTIFICATE の行を含んでいることを確認します。</p>
ドメインへの参加の詳細 - Active Directory (統合 Windows 認証) を選択した場合に表示されます	<p>[ドメイン名]、[ドメイン管理者ユーザー名]、および [ドメイン管理者パスワード] の各テキスト ボックスに適切な認証情報を入力します。</p> <p>Active Directory が STARTTLS 暗号化を必要とする場合は、[証明書] セクションの [このディレクトリには STARTTLS を使用するすべての接続が必要です] チェック ボックスを選択し、Active Directory のルート CA 証明書をコピーして [SSL 証明書] フィールドにペーストします。</p> <p>証明書が PEM 形式であり、BEGIN CERTIFICATE と END CERTIFICATE の行を含んでいることを確認します。</p> <p>ディレクトリで複数のドメインを使用している場合は、ルート CA 証明書をすべてのドメインに 1 つずつ追加していきます。</p> <p>注： Active Directory が STARTTLS を必要とする場合、証明書がなければディレクトリを作成できません。</p>

- 7 バインド ユーザーの詳細セクションで、ディレクトリ同期を促進するための適切な認証情報を入力します。

LDAP 経由の Active Directory の場合：

オプション	説明
ベース DN	検索ベース識別名を入力します。たとえば、 cn=users,dc=corp,dc=local と入力します。
バインド DN	バインド識別名を入力します。たとえば、 cn=fritz infra,cn=users,dc=corp,dc=local と入力します。

Active Directory（統合 Windows 認証）の場合：

オプション	説明
バインド ユーザー UPN	そのドメインで認証できるユーザーのユーザー プリンシパル名を入力します。たとえば、UserName@example.com のように入力します。
バインド DN パスワード	バインド ユーザーのパスワードを入力します。

- 8 [接続をテスト] をクリックし、構成したディレクトリへの接続をテストします。

Active Directory（統合 Windows 認証）を選択した場合、このボタンは表示されません。

- 9 [保存して次へ] をクリックします。

[ドメインの選択] ページにドメインのリストが表示されます。

- 10 この Active Directory 接続に対して表示されるドメインを確認および更新します。

- [Active Directory（統合 Windows 認証）] で、この Active Directory 接続に関連付ける必要があるドメインを選択します。
- LDAP 経由の Active Directory では、使用可能なドメインにチェックマークが付けられて表示されます。


注： ディレクトリが作成された後に信頼するドメインを追加する場合、サービスは新規に追加されたドメインを自動的に検出しません。サービスによるドメインの検出を有効にするには、コネクタ をドメインから切り離してから、ドメインに再度参加させる必要があります。コネクタ がドメインに再度参加すると、信頼するドメインがリストに表示されます。

- 11 [次へ] をクリックします。

- 12 Directories Management のディレクトリ属性名が、正しい Active Directory 属性にマッピングされていることを確認します。

適切にマッピングされていない場合は、ドロップダウン メニューから正しい Active Directory 属性を選択します。

- 13 [次へ] をクリックします。


- 14  をクリックして、Active Directory とこのディレクトリを同期するグループを選択します。

Active Directory からグループを追加するときに、そのグループのメンバーがユーザー リストに含まれていない場合、これらのメンバーが追加されます。グループを同期する際、Active Directory のプライマリ グループである Domain Users に属していないユーザーの同期は行われません。

注： Directories Management のユーザー認証システムでは、グループやユーザーを追加する場合 Active Directory からデータをインポートするため、その処理速度は Active Directory の機能によって制限されます。その結果、追加するグループとユーザーの数に応じて、インポート処理にかなりの時間がかかる場合があります。遅延または問題の発生を最小限に抑えるには、グループとユーザーを vRealize Automation の運用上必要な数に制限します。


システム パフォーマンスの低下またはエラーが発生した場合は、不要なアプリケーションをすべて閉じて、Active Directory に十分なメモリが割り当てられるようにしてください。問題が解決されない場合は、必要に応じて Active Directory に割り当てるメモリを増やしてください。多数のユーザーおよびグループを持つシステムでは、場合によっては Active Directory に割り当てるメモリを最大 24 GB まで増やす必要があります。

- 15 [次へ] をクリックします。

- 16  をクリックしてさらにユーザーを追加します。

適切な値は次のとおりです。

- 単一ユーザー：CN=*username*,CN=Users,OU=Users,DC=myCorp,DC=com
- 複数ユーザー：OU=Users,OU=myUnit,DC=myCorp,DC=com

ユーザーを除外するには、 をクリックして特定のタイプのユーザーを除外するフィルタを作成します。フィルタリングの基準となるユーザー属性、クエリ ルールおよび値を選択します。

- 17 [次へ] をクリックします。

- 18 このページで、ディレクトリと同期しているユーザー数とグループ数を確認します。

ユーザー数とグループ数を変更する場合には、[編集] リンクをクリックします。

注： 以前に指定したベース DN の下にあるユーザー DN を指定していることを確認します。ユーザー DN がベース DN に含まれない場合、その DN のユーザーは、同期はされますがログインすることはできません。

- 19 [Workspace にプッシュ] をクリックして、ディレクトリとの同期を開始します。

結果

Active Directory への接続が完了し、選択したユーザーとグループがディレクトリに追加されます。これで、[管理] - [ユーザーとグループ] - [ディレクトリ ユーザーとディレクトリ グループ]を選択してユーザーとグループを適切な vRealize Automation ロールに割り当てることができます。詳細については、[ディレクトリ ユーザーまたはグループへのロールの割り当て](#) を参照してください。

次のステップ

vRealize Automation 環境に高可用性が構成されている場合は、ディレクトリ管理も高可用性向けに構成する必要があります。[高可用性を実現するためのディレクトリ管理の構成](#)を参照してください。

- 認証方法を設定します。コネクタを認証にも使用している場合、ユーザーとグループがディレクトリと同期された後に、コネクタ上で認証方法を設定できます。サードパーティの認証 ID プロバイダを使用している場合、コネクタ上で該当の ID プロバイダを設定します。
- デフォルトのアクセス ポリシーを確認します。デフォルトのアクセス ポリシーでは、すべてのネットワーク範囲にあるすべてのアプライアンスに対し、Web ブラウザにアクセスする場合のセッション タイムアウトを 8 時間に設定します。また、クライアント アプリケーションにアクセスする場合のセッション タイムアウトを、2,160 時間（90 日間）に設定します。デフォルトのアクセス ポリシーは変更が可能です。Web アプリケーションをカタログに追加するときに、新しいアクセス ポリシーを作成することができます。
- 管理コンソール、ユーザー ポータルおよびサインイン画面にカスタム ブランディングを適用します。

OpenLDAP ディレクトリ接続の設定

OpenLDAP ディレクトリ接続は、ディレクトリ管理機能を使用して設定できます。

LDAP プロトコルにはいくつかの種類がありますが、OpenLDAP は vRealize Automation のディレクトリ管理機能での使用に関してテスト、認定されているのはプロトコルだけです。

LDAP ディレクトリを統合するには、対応する Directories Management ディレクトリを作成し、ユーザーとグループを LDAP ディレクトリから Directories Management ディレクトリに同期します。後続の更新のために定期的な同期スケジュールを設定することができます。

また、ユーザーのために同期させる LDAP 属性を選択し、Directories Management 属性にマップします。

LDAP ディレクトリ構成はデフォルトのスキーマをベースにすることができますが、カスタムのスキーマを作成することもできます。また、カスタムの属性を定義することもできます。Directories Management で、LDAP ディレクトリを検索してユーザーまたはグループ オブジェクトを取得できるようにするには、LDAP ディレクトリに適用可能な LDAP 検索フィルタおよび属性名を指定する必要があります。

具体的には、次の情報を指定する必要があります。

- グループ、ユーザーおよびバインド ユーザーを取得するための LDAP 検索フィルタ
- グループ メンバーシップ、UUID および識別名のための LDAP 属性名

注： ディレクトリ管理では、LDAP クエリに 1,500 のデフォルト ページ サイズが使用されます。OpenLDAP ディレクトリ接続を設定する場合は、OpenLDAP のシンプルなページ結果制御の拡張機能を有効にして、表示される結果の数を制限する必要があります。この拡張機能を使用しないと、ユーザーおよびグループの同期エラーが発生することがあります。

前提条件

- [ユーザー属性] ページで設定を確認し、他に同期する属性を追加します。ディレクトリを作成するときは、Directories Management 属性を LDAP ディレクトリ属性にマッピングします。これらの属性はディレクトリ内のユーザーに対して同期されます。

注： ユーザー属性を変更する場合は、サービスの他のディレクトリに対する影響を考慮してください。Active Directory と LDAP ディレクトリの両方を追加する計画の場合は、[userName] を除いて、属性には必須のマークが付いていないことを確認してください。[ユーザー属性] ページの設定はサービスのすべてのディレクトリに適用されます。属性に必須のマークが付いている場合は、その属性を持たないユーザーは Directories Management サービスに同期されません。

- バインド DN ユーザー アカウント。有効期限のないパスワードを持つバインド DN ユーザー アカウントを使用することを推奨します。
- LDAP ディレクトリでは、ユーザーとグループの UUID はプレーン テキスト形式である必要があります。
- LDAP ディレクトリには、すべてのユーザーおよびグループに対するドメイン属性が存在する必要があります。Directories Management ディレクトリを作成するときは、この属性を Directories Management の [domain] 属性にマップします。
- ユーザー名にスペースを含めることはできません。ユーザー名にスペースが含まれていると、ユーザーは同期されますが、資格を利用できません。
- 証明書認証を使用する場合、ユーザーは userPrincipalName とメール アドレス属性の値を持っている必要があります。

手順

- 1 [管理] - [ディレクトリ管理] - [ディレクトリ] を選択します。
- 2 [ディレクトリを追加] をクリックし、[LDAP ディレクトリの追加] をクリックします。

3 [LDAP ディレクトリを追加] ページに必要な情報を入力します。

オプション	説明
ディレクトリ名	Directories Management ディレクトリの名前を入力します。
ディレクトリの同期と認証	<p>a [コネクタを同期] フィールドで、LDAP ディレクトリから Directories Management ディレクトリにユーザーとグループを同期するためのコネクタを選択します。</p> <p>コネクタ コンポーネントは、デフォルトでは Directories Management サービスで常に利用できます。このコネクタは、ドロップダウン リストに表示されます。高可用性を実現するために複数の Directories Management アプライアンスを展開すると、それぞれのコネクタ コンポーネントがリストに表示されます。</p> <p>LDAP ディレクトリ用の個別のコネクタは必要ありません。コネクタは、Active Directory であるか LDAP ディレクトリであるかにかかわらず複数のディレクトリをサポートすることができます。</p> <p>b この LDAP ディレクトリを使用してユーザー認証を行う場合は、[認証] フィールドで [はい] を選択します。</p> <p>サードパーティの ID プロバイダを使用してユーザーを認証する場合は、[いいえ] を選択します。ユーザーとグループを同期するようにディレクトリ接続を追加したら、[管理] - [ディレクトリ管理] - [ID プロバイダ] ページの順に移動して、認証に使用するサードパーティの ID プロバイダを追加します。</p> <p>c [ディレクトリ検索属性] テキスト ボックスは、ほとんどの構成で、デフォルトで選択される [カスタム] のままにしてください。[カスタム ディレクトリ検索属性] フィールドで、ユーザー名とグループ名に使用する LDAP ディレクトリ属性を指定します。ユーザーやグループなど LDAP サーバのエンティティが、この属性によって一意に識別されます。たとえば、cn です。</p> <p>d Active Directory で DNS サービス ロケーション ルックアップを使用する場合は、次の項目を選択します。</p> <ul style="list-style-type: none"> ■ [サーバの場所] セクションで、[このディレクトリは DNS サービス ロケーションをサポートします] チェック ボックスを選択します。 <p>ディレクトリ管理が、最適なドメイン コントローラを検索して使用します。最適化されたドメイン コントローラの選択を使用しない場合は、手順 e に進みます。</p> <ul style="list-style-type: none"> ■ Active Directory に STARTTLS 暗号化が必要な場合は、[証明書] セクションの [このディレクトリには SSL を使用するすべての接続が必要です] チェック ボックスを選択し、Active Directory のルート CA 証明書をコピーして [SSL 証明書] テキスト ボックスに貼り付けます。 <p>証明書が PEM 形式であり、[BEGIN CERTIFICATE] と [END CERTIFICATE] の行を含んでいることを確認します。</p> <p>注： Active Directory が STARTTLS を必要とする場合、証明書がなければディレクトリを作成できません。</p> <p>e Active Directory の DNS サービス ロケーション ルックアップを使用しない場合は、次の項目を選択します。</p> <ul style="list-style-type: none"> ■ [サーバの場所] セクションで、[このディレクトリは DNS サービス ロケーションをサポートします] チェック ボックスが選択されていないことを確認して、Active Directory サーバのホスト名とポート番号を入力します。グローバル カタログとしてディレクトリを設定するには、Active Directory 環境 の「マルチドメイン、シングルフォレストの Active Directory 環境」セクションを参照してください。 ■ Active Directory が SSL 経由のアクセスを必要とする場合は、[証明書] セクションの [このディレクトリには SSL を使用するすべての接続が必要です] チェック ボックスを選択し、Active Directory のルート CA 証明書をコピーして [SSL 証明書] フィールドにペーストします。

オプション	説明
	<p>証明書が PEM 形式であり、「BEGIN CERTIFICATE」と「END CERTIFICATE」の行を含んでいることを確認します。</p> <p>注： Active Directory が STARTTLS を必要とする場合、証明書がなければディレクトリを作成できません。</p>
サーバの場所	<p>LDAP ディレクトリ サーバのホスト名とポート番号を入力します。サーバ ホストには、完全修飾ドメイン名または IP アドレスのいずれかを指定することができます。たとえば、myLDAPserver.example.com または 100.00.00.0 のように入力します。</p> <p>ロード バランサの背後にサーバのクラスタがある場合は、代わりにロード バランサの情報を入力します。</p>
LDAP の設定	<p>Directories Management が LDAP ディレクトリのクエリに使用することができる LDAP 検索フィルタおよび属性を指定します。デフォルト値はコア LDAP スキーマに基づいて提供されます。</p> <p>[フィルタ クエリ]</p> <ul style="list-style-type: none"> ■ [グループ]：グループ オブジェクトを取得するための検索フィルタ。 <p>例：(objectClass=group)</p> <ul style="list-style-type: none"> ■ [バインド ユーザー]：バインド ユーザー オブジェクト、つまりディレクトリにバインドすることができるユーザーを取得するための検索フィルタ。 <p>例：(objectClass=person)</p> <ul style="list-style-type: none"> ■ [ユーザー]：同期するユーザーを取得するための検索フィルタ。 <p>例：(&(objectClass=user)(objectCategory=person))</p> <p>[属性]</p> <ul style="list-style-type: none"> ■ [メンバーシップ]：グループのメンバーを定義するために LDAP ディレクトリで使われる属性。 <p>例：member</p> <ul style="list-style-type: none"> ■ [オブジェクト UUID]：ユーザーまたはグループの UUID を定義するために LDAP ディレクトリで使われる属性。 <p>例：entryUUID</p> <ul style="list-style-type: none"> ■ [識別名]：LDAP ディレクトリでユーザーまたはグループの識別名に使用される属性。 <p>例：entryDN</p>

オプション	説明
証明書	<p>LDAP ディレクトリが SSL 経由のアクセスを必要とする場合は、[このディレクトリには SSL を使用するすべての接続が必要です] チェック ボックスをオンにします。そのうえで、LDAP ディレクトリ サーバのルート CA SSL 証明書をコピーして [SSL 証明書] テキスト ボックスに貼り付けます。証明書が PEM 形式であり、「BEGIN CERTIFICATE」と「END CERTIFICATE」の行を含んでいることを確認します。</p> <p>ディレクトリに複数のドメインがある場合は、すべてのドメインのルート CA 証明書を順番に追加します。</p> <p>最後に、このページの [サーバの場所] セクションの [サーバのポート] フィールドに適切なポート番号が指定されていることを確認します。</p>
バインド ユーザーの詳細	<p>[ベース DN] : 検索を開始する DN を入力します。たとえば、cn=users,dc=example,dc=com のように入力します。</p> <p>該当するすべてのユーザーがベース DN 下に存在している必要があります。ベース DN に特定のユーザーが存在しない場合、そのユーザーは、ベース DN 下に存在するグループのメンバーであってもログインできなくなります。</p> <p>[バインド DN] : LDAP ディレクトリにバインドするために使用する DN を入力します。ユーザー名を入力することもできますが、ほとんどの環境では DN の方が適しています。</p> <p>注： 有効期限のないパスワードを持つバインド DN ユーザー アカウントを使用することを推奨します。</p> <p>[バインド DN パスワード] : バインド DN ユーザーのパスワードを入力します。</p>

- 4 LDAP ディレクトリ サーバへの接続をテストするには、[接続をテスト] をクリックします。

接続に成功しない場合は、入力した情報を確認して、適切な変更を行います。

- 5 [保存して次へ] をクリックします。

- 6 [ドメインの選択] ページで正しいドメインが選択されていることを確認し、[次へ] をクリックします。

- 7 [属性をマップ] ページで、Directories Management 属性が正しい LDAP 属性にマップされていることを確認します。

これらの属性がユーザーに対して同期されます。

重要： [domain] 属性のマッピングを指定する必要があります

属性は [ユーザー属性] ページからリストに追加することができます。

- 8 [次へ] をクリックします。

- 9 [+] をクリックし、[同期するグループ（ユーザー）の選択] ページで、LDAP ディレクトリから Directories Management ディレクトリに同期するグループを選択します。

LDAP ディレクトリに同じ名前のグループが複数ある場合は、グループ ページ内でグループに一意の名前を指定する必要があります。

Active Directory からグループを追加するときに、そのグループのメンバーがユーザー リストに含まれていない場合、これらのメンバーが追加されます。グループを同期する際、Active Directory のプライマリ グループである Domain Users に属していないユーザーの同期は行われません。

[ネストされたグループ メンバーを同期] オプションは、デフォルトで有効になっています。このオプションが有効になっているときは、選択したグループに直接属するすべてのユーザーと、その下にネストされたグループに属するすべてのユーザーが同期されます。ネストされたグループ自体は同期されないことに注意してください。同期されるのは、ネストされたグループに属するユーザーのみです。Directories Management ディレクトリでは、これらのユーザーは同期対象として選択したトップレベルのグループのメンバーとして表示されます。実際には、選択されたグループの階層がフラット化され、すべてのレベルのユーザーが選択されたグループのメンバーとして Directories Management に表示されます。

このオプションが無効になっている場合、同期するグループを指定すると、そのグループに直接属するすべてのユーザーが同期されます。その下のネストされたグループに属するユーザーは同期されません。グループ ツリーのスキャンに多くのリソースが消費され時間がかかる大規模なディレクトリ構成では、このオプションを無効にすると、時間を短縮できます。このオプションを無効にする場合は、同期するユーザーが属するグループをすべて選択してください。

注： Directories Management のユーザー認証システムでは、グループやユーザーを追加する場合 Active Directory からデータをインポートするため、その処理速度は Active Directory の機能によって制限されます。その結果、追加するグループとユーザーの数に応じて、インポート処理にかなりの時間がかかる場合があります。遅延または問題の発生を最小限に抑えるには、グループとユーザーを vRealize Automation の運用上必要な数に制限します。

システム パフォーマンスの低下またはエラーが発生した場合は、不要なアプリケーションをすべて閉じて、ディレクトリ管理に十分なメモリが割り当てられるようにしてください。問題が解決されない場合は、必要に応じてディレクトリ管理に割り当てるメモリを増やしてください。多数のユーザーおよびグループを持つシステムでは、場合によってはディレクトリ管理に割り当てるメモリを最大 24 GB まで増やす必要があります。

10 [次へ] をクリックします。

11 [+] をクリックして、別のユーザーを追加します。たとえば、**CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com** と入力します。

ここには組織単位のほか、個別にユーザーを追加することができます。

特定のタイプのユーザーを除外するフィルタを作成できます。フィルタリングの基準となるユーザー属性、クエリ ルールおよび値を選択します。

12 [次へ] をクリックします。

13 ディレクトリに同期するユーザーとグループの数や、デフォルトの同期スケジュールをページで確認します。

ユーザーとグループや、同期の頻度に変更を加えるには、[編集] リンクをクリックします。

14 [ディレクトリを同期] をクリックして、ディレクトリ同期を開始します。

結果

LDAP ディレクトリへの接続が確立され、ユーザーとグループは LDAP ディレクトリから Directories Management ディレクトリに同期されます。

これで、[管理] - [ユーザーとグループ] - [ディレクトリ ユーザーとディレクトリ グループ]を選択してユーザーとグループを適切な vRealize Automation ロールに割り当てることができます。詳細については、[ディレクトリ ユーザーまたはグループへのロールの割り当て](#) を参照してください。

LDAP ディレクトリ統合の制限

ディレクトリ管理への LDAP Directory 統合に関連して、いくつかの重要な制限があります。

- 単一ドメインの LDAP ディレクトリ環境のみを統合することができます。

LDAP ディレクトリから複数のドメインを統合するには、ドメインごとに追加の Directories Management ディレクトリを1つずつ作成する必要があります。
- Directories Management ディレクトリのタイプが LDAP ディレクトリの場合、次の認証方法はサポートされません。
 - Kerberos 認証
 - RSA Adaptive Authentication
 - サードパーティ ID プロバイダとしての ADFS
 - SecurID
 - Vasco および SMS パスコード サーバによる Radius 認証
- LDAP ドメインに参加することはできません。
- Directories Management ディレクトリのタイプが LDAP ディレクトリの場合、View または Citrix 公開リソースとの統合はサポートされません。
- ユーザー名にスペースを含めることはできません。ユーザー名にスペースが含まれていると、ユーザーは同期されますが、資格を利用できません。
- Active Directory と LDAP ディレクトリの両方を追加する計画の場合は、必須のマークを付けることができる userName を除いて、[ユーザー属性] ページで属性には必須のマークが付いていないことを確認してください。[ユーザー属性] ページの設定はサービスのすべてのディレクトリに適用されます。属性に必須のマークが付いている場合は、その属性を持たないユーザーは Directories Management サービスに同期されません。
- LDAP ディレクトリに同じ名前のグループが複数ある場合は、Directories Management サービスでグループに一意的な名前を指定する必要があります。同期するグループを選択するときに名前を指定することができます。
- ユーザーが有効期限の切れたパスワードをリセットするオプションは利用できません。
- domain_krb.properties ファイルはサポートされません。

高可用性を実現するためのディレクトリ管理の構成

ディレクトリ管理を使用すると、vRealize Automation で Active Directory 接続の高可用性を構成できます。

各 vRealize Automation アプライアンスにはユーザー認証をサポートするコネクタが含まれていますが、通常、ディレクトリの同期用にコネクタを1つ構成します。同期用に選択するコネクタは、どのコネクタでもかまいません。ディレクトリ管理の高可用性をサポートするには、セカンダリ vRealize Automation アプライアンスに対応する別のコネクタを手動で設定する必要があります。このコネクタは、ID プロバイダに接続して同一の Active Directory を指定します。このように構成すると、1台目の vRealize Automation Appliance が故障しても、もう一方がユーザー認証の管理を引き継ぎます。

高可用性環境では、すべてのノードで、同一の Active Directory、ユーザー、認証方法などの設定を使用する必要があります。最も直接的な実現方法は、ID プロバイダ ホストとしてロード バランサ ホストを設定し、ID プロバイダをクラスタに昇格させることです。このように構成すると、すべての認証要求はロード バランサに送られ、必要に応じていずれかのコネクタにこの要求が転送されます。

コネクタは、ユーザーの同期にも使用されます。ただし、ディレクトリの同期を実行するために設定されるコネクタは 1 つだけです。同期されたユーザーは、クラスタ化されたすべてのノードから読み取ることができるアプライアンス データベースに保存されます。ディレクトリ同期用のコネクタが接続に失敗した場合、ディレクトリ同期は機能しなくなります。同期を回復するには、テナント管理者が vRealize Automation ユーザー インターフェイスを使用して別のコネクタでディレクトリ同期を実行するように手動で設定する必要があります。[セカンダリ コネクタでのディレクトリの同期の有効化](#)を参照してください。

コネクタの使用の詳細については、[コネクタとコネクタ クラスタの管理](#)を参照してください。

前提条件

- vRealize Automation アプライアンスのインスタンスを 2 つ以上使用して、vRealize Automation の展開を構成します。
- vRealize Automation アプライアンスのインスタンスを 2 つ使用して、単一ドメインで稼動するエンタープライズ モードで vRealize Automation をインストールします。
- vRealize Automation の展開でできるように最適なロード バランサをインストールおよび構成します。
- インストールした vRealize Automation アプライアンスのインスタンスに付属するコネクタのいずれかを使用して、テナントおよびディレクトリ管理を構成します。テナントの構成の詳細については、[テナント設定の構成](#)を参照してください。

手順

- 1 テナント管理者として、vRealize Automation の展開のロード バランサにログインします。
ロード バランサの URL は <load balancer address>/vcac/org/*tenant_name* です。
- 2 [管理] - [ディレクトリ管理] - [ID プロバイダ] の順に選択します。
- 3 システムで現在使用している ID プロバイダをクリックします。
システムに基本的な ID 管理を提供する既存のディレクトリとコネクタが表示されます。
- 4 [ID プロバイダ プロパティ] ページで、[コネクタの追加] ドロップダウン リストをクリックし、セカンダリ vRealize Automation アプライアンスに対応するコネクタを選択します。
- 5 コネクタを選択すると表示される [バインド DN パスワード] テキスト ボックスに適切なパスワードを入力します。
- 6 [コネクタの追加] をクリックします。
- 7 デフォルトでは、メインのコネクタが [IdP ホスト名] テキスト ボックスに表示されます。ロード バランサをポイントするようにホスト名を変更します。

セカンダリ コネクタでのディレクトリの同期の有効化

プライマリ コネクタで障害が発生した場合、認証は自動的に別のコネクタ インスタンスによって処理されます。障害が発生した場合、ディレクトリの同期については、[ディレクトリ管理] で、適切なセカンダリ コネクタ インスタ

ンスを使用するようにディレクトリ設定を変更する必要があります。ディレクトリの同期を有効にできるコネクタは一度に 1 つだけです。

手順

- 1 [管理] - [ディレクトリ管理] - [ディレクトリ] を選択します。
- 2 元のコネクタ インスタンスに関連付けられているディレクトリを選択します。

注： この情報は、[ディレクトリ] - [コネクタ] ページで確認できます。

- 3 [ディレクトリ] ページの [ディレクトリの同期と認証] セクションにある [コネクタを同期] ドロップダウン リストで別のコネクタ インスタンスを選択します。
- 4 [バインド ユーザーの詳細] セクションの [バインド DN パスワード] テキスト ボックスに、Active Directory バインド アカウントのパスワードを入力します。
- 5 [保存] をクリックします。

vRealize Automation と Active Directory 間で双方向の信頼関係を構築

ID プロバイダと Active Directory フェデレーション サービス間の双方向信頼関係を構成することによって、基本的な vRealize Automation Active Directory 接続のシステム セキュリティを強化できます。

vRealize Automation と Active Directory 間の双方向の信頼関係を構成するには、カスタム ID プロバイダを作成し、このプロバイダに Active Directory のメタデータを追加する必要があります。また、vRealize Automation 環境で使用するデフォルト ポリシーの変更も必要です。最後に、ID プロバイダを認識するように Active Directory を構成します。

前提条件

- Active Directory の基本的なユーザー ID とパスワード認証をサポートする、適切な Active Directory リンクが設定された vRealize Automation 環境でテナントを構成したことを確認します。
- 使用するネットワークに Active Directory をインストールおよび構成します。
- 適切な Active Directory フェデレーション サービス (AD FS) メタデータを取得します。
- テナント管理者として vRealize Automation にログインします。

手順

- 1 フェデレーション メタデータ ファイルを取得します。

このファイルは次のリンクからダウンロードできます。 <https://servername.domain/FederationMetadata/2007-06/FederationMetadata.xml>

- 2 logout という用語を検索し、`https://servername.domain/adfs/ls/logout.aspx` を指し示すように各インスタンスの場所を編集します。

たとえば、

```
SingleLogoutService
  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Location="https://servername.domain/adfs/ls/ "/>
```

上記のアドレスを次のように変更します。

```
SingleLogoutService
  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Location="https://servername.domain/adfs/ls/logout.aspx"/>
```

- 3 環境に適した新しい ID プロバイダを作成します。
 - a [管理] - [ディレクトリ管理] - [ID プロバイダ] の順に選択します。
 - b [ID プロバイダの追加] をクリックして、必要に応じてフィールドに記入します。

オプション	説明
ID プロバイダ名	新しい ID プロバイダの名前を入力します。
ID プロバイダ メタデータ (URL または XML)	Active Directory フェデレーション サービスのメタデータ ファイルのコンテンツをここに貼り付けます。
SAML 要求の名前 ID ポリシー (オプション)	必要に応じて、ID ポリシーの SAML 要求の名前を入力します。
ユーザー	ユーザーにアクセス権限を許可するドメインを選択します。
IDP メタデータの処理	クリックして、追加したメタデータ ファイルを処理します。
ネットワーク	ユーザーにアクセスを許可するネットワーク範囲を選択します。
認証方法	この ID プロバイダが使用する認証方法の名前を入力します。
SAML コンテキスト	システムに適切なコンテキストを選択します。
SAML 署名証明書	SAML メタデータの見出しの横のリンクをクリックして、ディレクトリ管理メタデータをダウンロードします。

- c ディレクトリ管理メタデータ ファイルは `sp.xml` として保存します。
 - d [追加] をクリックします。
- 4 デフォルト ポリシーにルールを追加します。
 - a [管理] - [ディレクトリ管理] - [ポリシー] の順に選択します。
 - b デフォルトのポリシー名をクリックします。

- c [ポリシー ルール] の見出しの中にある [+] アイコンをクリックし、新しいルールを追加します。

[ポリシー ルールの追加] ページのオプションを使用し、特定のネットワーク範囲とデバイスでの使用に適したプライマリ認証方法およびセカンダリ認証方法を指定するルールを作成します。

たとえば、ネットワーク範囲が「**マイ マシン**」で、「**すべてのデバイス タイプ**」のコンテンツにアクセスする必要がある場合、一般的な展開では、**ADFS のユーザー名とパスワード**で認証する必要があります。

- d ポリシーの変更を保存するには、[OK] をクリックします。

- e [デフォルト ポリシー] ページで、既存のルールよりも優先されるように新しいルールを表の先頭にドラッグします。

- 5 Active Directory フェデレーション サービスの管理コンソールまたは他の適切なツールを使用して、vRealize Automation ID プロバイダとの証明書利用者信頼を設定します。

これを設定するには、以前にダウンロードしたディレクトリ管理メタデータをインポートする必要があります。Active Directory フェデレーション サービスで双方向の信頼関係を構成する際の詳細については、Microsoft Active Directory のドキュメントを参照してください。この手順では、次の項目を実行する必要があります。

- 証明書利用者信頼を設定します。これを設定した場合は、コピーおよび保存しておいた、VMware ID プロバイダのサービス プロバイダ メタデータ XML ファイルをインポートする必要があります。
- 属性取得ルールで LDAP から取得した属性を指定した SAML 形式に変換する要求ルールを作成します。ルールを作成した後、次のテキストを追加してルールを編集します。

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/
format"] = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress", Properties["http://
schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"vmwareidentity.domain.com");
```

Directories Management と SSO2 間の SAML フェデレーションの構成

vRealize Automation Directories Management と、SSO2 を使用してシングル サインオンをサポートしているシステムとの間に SAML フェデレーションを確立できます。

ディレクトリ管理と SSO2 の間で SAML 接続を作成し、Directories Management と SSO2 間のフェデレーションを確立します。現在、唯一サポートされている End-to-End のフローでは、SSO2 が ID プロバイダ (IdP) として機能し、Directories Management がサービス プロバイダ (SP) として機能します。

SSO2 のユーザー認証のために、Directories Management と SSO2 の両方に同じアカウントが存在する必要があります。少なくとも両者の間で、ユーザーのユーザー プリンシパル名 (UPN) が一致する必要があります。他の属性は、SAML 件名の識別に必要なものであるため、違っていてもかまいません。

admin@vsphere.local など、SSO2 のローカル ユーザーの場合、対応する（少なくともユーザーの UPN が一致する）アカウントが Directories Management に存在する必要があります。これらのアカウントは手動で作成することも、Directories Management ローカル ユーザー作成 API を使用してスクリプトで作成することもできます。

SSO2 と Directories Management 間の SAML を設定するには、ディレクトリ管理と SSO コンポーネントを構成します。

表 2-4. SAML フェデレーションのコンポーネントの構成

コンポーネント	構成
ディレクトリ管理	SSO2 を Directories Management のサード パーティ ID プロバイダとして構成し、デフォルトの認証ポリシーを更新します。自動スクリプトを作成して Directories Management を設定できます。
SSO2 コンポーネント	Directories Management の <code>sp.xml</code> ファイルをインポートして、Directories Management をサービス プロバイダとして構成します。このファイルにより、Directories Management をサービス プロバイダ (SP) として使用するように SSO2 を構成できます。

前提条件

- vRealize Automation 展開のテナントを構成します。[追加テナントの作成](#)を参照してください。
- 適切な Active Directory リンクを設定して、基本的な Active Directory ユーザー ID とパスワードの認証をサポートします。
- テナント管理者として vRealize Automation にログインします。

手順

- 1 SSO2 ユーザー インターフェイスを使用して、SSO2 の ID プロバイダ メタデータをダウンロードします。
 - a `https://<cloudvm-hostname>/` で、管理者として vCenter Server にログインします。
 - b [vSphere Web Client へのログイン] リンクをクリックします。
 - c 左側のナビゲーション ペインで、[管理] - [Single Sign On] - [構成] の順に選択します。
 - d [SAML サービス プロバイダのメタデータ] の横にある [ダウンロード] をクリックします。
vsphere.local.xml ファイルのダウンロードが開始されます。
 - e vsphere.local.xml ファイルの内容をコピーします。
- 2 [vRealize Automation ディレクトリ管理 ID プロバイダ] ページで新しい ID プロバイダを作成します。
 - a テナント管理者として vRealize Automation にログインします。
 - b [管理] - [ディレクトリ管理] - [ID プロバイダ] の順に選択します。

- c [ID プロバイダを追加] をクリックして、構成情報を入力します。

オプション	アクション
[ID プロバイダ名]	新しい ID プロバイダの名前を入力します。
[ID プロバイダ メタデータ (URI または XML)] テキスト ボックス	SSO2 idp.xml メタデータ ファイルの内容をテキスト ボックスに貼り付けて、[IDP メタデータの処理] をクリックします。
[SAML 要求の名前 ID ポリシー (オプション)]	http://schemas.xmlsoap.org/claims/UPN.
[ユーザー]	ユーザーにアクセス権限を許可するドメインを選択します。
[ネットワーク]	ユーザーにアクセス権限を付与するネットワーク範囲を選択します。 IP アドレスでユーザーを認証する場合は、[全範囲] を選択します。
[認証方法]	認証方法の名前を入力します。右側の [SAML コンテキスト] ドロップダウン メニューを使用し、認証方法を urn:oasis:names:tc:SAML:2.0:ac:classes:Password にマッピングします。
[SAML 署名証明書]	SAML メタデータの見出しの横のリンクをクリックして、ディレクトリ管理メタデータをダウンロードします。

- d ディレクトリ管理メタデータ ファイルは sp.xml として保存します。

- e [追加] をクリックします。

- 3 [ディレクトリ管理ポリシー] ページを使用して関連認証ポリシーを更新し、サード パーティ SSO2 ID プロバイダに認証をリダイレクトします。

- a [管理] - [ディレクトリ管理] - [ポリシー] の順に選択します。
- b デフォルトのポリシー名をクリックします。
- c [ポリシー ルール] の見出しの下にある認証方法をクリックし、既存の認証ルールを編集します。
- d [ポリシー ルールの編集] ページで、パスワードの認証方法を適切な認証方法に変更します。

この場合、方法を SSO2 に変更します。

- e ポリシーの変更を保存するには [保存] をクリックします。

- 4 左側のナビゲーション ペインで、[管理] - [Single Sign On] - [構成] の順に選択し、[更新] をクリックして、sp.xml ファイルを vSphere にアップロードします。

Active Directory 接続へのユーザーまたはグループの追加

既存の Active Directory 接続にユーザーまたはグループを追加できます。

ディレクトリ管理のユーザー認証システムでは、グループおよびユーザーを追加するときに Active Directory からデータをインポートします。データ転送の速度は、Active Directory の機能によって制限されます。その結果、追加するグループおよびユーザーの数によっては、アクションに時間がかかる場合があります。問題を最小限に抑えるためには、グループとユーザーを、vRealize Automation のアクションに必要なグループとユーザーのみに制限します。問題が発生した場合は、不要なアプリケーションを終了し、展開で適切なメモリが Active Directory に割り当てられていることを確認します。問題が引き続き発生する場合は、Active Directory のメモリ割り当てを増やします。多数のユーザーおよびグループを展開する環境では、必要に応じて、Active Directory に割り当てるメモリを最大 24 GB まで増やします。

多数のユーザーおよびグループを展開する vRealize Automation 環境を同期する場合、SyncLog の詳細が利用できるまでに遅延が発生することがあります。ログ ファイルのタイム スタンプが、コンソールに表示される完了時刻と異なる場合があります。

グループのメンバーがユーザー リストに含まれていない場合、Active Directory からグループを追加すると、そのメンバーがリストに追加されます。グループを同期する際、Active Directory のプライマリ グループである Domain Users に属していないユーザーの同期は行われません。

注： 同期アクションは、アクションの開始後にキャンセルできません。

前提条件

- コネクタ がインストールされ、アクティベーション コードで有効になっている必要があります。[ユーザー属性] ページで必須のデフォルト属性を選択し、その他の属性を追加します。
- Active Directory から同期する Active Directory のグループとユーザーのリスト。
- LDAP 経由の Active Directory の場合、ベース DN、バインド DN、およびバインド DN パスワードなどの情報が必要となります。
- Active Directory (統合 Windows 認証) では、ドメインのバインド ユーザー UPN アドレスとパスワードなどの情報が必要となります。
- SSL を介して Active Directory にアクセスする場合、SSL 証明書のコピーが必要です。
- Windows 認証と統合されたマルチ フォレスト Active Directory があり、ドメイン ローカル グループに異なるフォレストのメンバーが含まれている場合は、次の操作を実行します。バインド ユーザーをドメイン ローカル グループの管理者グループに追加します。バインド ユーザーを追加しない場合、これらのメンバーはドメイン ローカル グループに含まれません。
- テナント管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [ディレクトリ管理] - [ディレクトリ] を選択します。
- 2 目的のディレクトリ名をクリックします。
- 3 [同期設定] をクリックして、同期オプションのダイアログ ボックスを開きます。
- 4 ユーザーまたはグループの構成を変更するかどうかに応じて、適切なアイコンをクリックします。

グループ構成を編集するには：

- グループを追加するには、[+] アイコンをクリックし、グループ DN 定義に行を追加して、適切なグループ DN を入力します。
- グループ DN 定義を削除するには、目的のグループ DN の [x] アイコンをクリックします。

ユーザー構成を編集するには：

- ◆ ユーザーを追加するには、[+] アイコンをクリックし、ユーザー DN 定義に行を追加して、適切なユーザー DN を入力します。

ユーザー DN 定義を削除するには、目的のユーザー DN の [x] アイコンをクリックします。

- 5 更新をすぐに同期せずに変更内容を保存するには、[保存] をクリックします。変更内容を保存して更新をすぐに同期するには、[保存して同期] をクリックします。

ディレクトリと同期する属性の選択

Active Directory と同期するように Directories Management ディレクトリをセットアップするときに、ディレクトリと同期するユーザー属性を指定します。ディレクトリをセットアップする前に、[ユーザー属性] ページで、必要となるデフォルト属性を指定し、Active Directory 属性にマッピングするその他の属性を適宜追加できます。

ディレクトリが作成される前に [ユーザー属性] ページを構成するときに、必須にするデフォルト属性を変更したり、属性を必須としてマークしたり、カスタム属性を追加したりできます。

デフォルトでマッピングされている属性のリストについては、[Active Directory で同期されるユーザー属性の管理](#) を参照してください。

ディレクトリが作成された後で、必須の属性を変更したり、カスタム属性を削除したりできます。ある属性を必須属性に変更することはできません。

ディレクトリと同期する別の属性を追加するときには、ディレクトリが作成された後に、ディレクトリの [マップされた属性] ページに移動して、これらの属性を Active Directory の属性にマッピングします。

手順

- 1 vRealize Automation にシステムまたはテナント管理者としてログインします。
- 2 [管理] タブをクリックします。
- 3 [ディレクトリ管理] - [ユーザー属性] を選択します。
- 4 [デフォルト属性] セクションで、必須属性のリストを確認して、必須にする必要がある属性が反映されるように必要な変更を加えます。
- 5 [属性] セクションで、Directories Management ディレクトリの属性名をリストに追加します。
- 6 [保存] をクリックします。

デフォルト属性のステータスがアップデートされ、追加した属性が、ディレクトリの [マップされた属性] リストに追加されます。
- 7 ディレクトリが作成された後に、[ID ストア] ページに移動して、ディレクトリを選択します。
- 8 [同期設定] - [マップされた属性] をクリックします。
- 9 追加した属性のドロップダウン メニューで、マップ先の Active Directory 属性を選択します。
- 10 [保存] をクリックします。

結果

ディレクトリは、Active Directory と次回同期されるときにアップデートされます。

ディレクトリ管理へのメモリの追加

多数のユーザーまたはグループを含む Active Directory と接続している場合、Directories Management へのメモリ追加が必要になる可能性があります。

デフォルトでは、4 GB のメモリが Directories Management サービスに割り当てられています。多くの小規模から中規模の環境では、これで十分です。多数のユーザーまたはグループを使用する Active Directory 接続がある場合、メモリの増加が必要になる可能性があります。10 万人以上のユーザーがそれぞれ 30 グループ、全体で 750 のグループある場合、メモリ割り当てを増やすことをお勧めします。このシステムの例では、VMware は Directories Management のメモリ割り当てを 6 GB に増やすことを推奨します。

ディレクトリ管理メモリは、vRealize Automation アプライアンスに割り当てたメモリ合計に基づいて算出されます。次の表は、関連するコンポーネントのメモリ割り当てを示しています。

表 2-5. vRealize Automation アプライアンスのメモリ割り当て

仮想アプライアンス メモリ	vRA サービス メモリ	vIDM サービス メモリ
18 GB	3.3 GB	4 GB
24 GB	4.9 GB	6 GB
30 GB	7.4 GB	9.1 GB

注： 上記の割り当ては、すべてのデフォルト サービスが有効であり、仮想アプライアンス上で機能することを前提としています。サービスの一部が停止した場合は、割り当てを変更する場合があります。

前提条件

- 適切な Active Directory 接続が構成されており、vRealize Automation 導入環境で機能しています。

手順

- 1 vRealize Automation アプライアンスが稼動している各マシンを停止します。
- 2 各マシンの仮想アプライアンスのメモリ割り当てを増やします。
18 GB のデフォルトのメモリ割り当てを使用している場合は、VMware はメモリ割り当てを 24 GB に増やすことをお勧めします。
- 3 vRealize Automation アプライアンスのマシンを再起動します。

ドメイン ホスト参照ファイルを作成して DNS Service Location (SRV) 参照をオーバーライドする

統合 Windows 認証を有効にすると、[ディレクトリ] の構成は [DNS サービスの場所] フィールドを有効にするように変更されます。コネクタ サービスの場所の参照は、サイトを認識しません。ランダムな DC 選択をオーバーライドするには、domain_krb.properties というファイルを作成し、SRV 参照より優先されるホスト値にドメインを追加できます。

手順

- 1 appliance-va コマンド ラインで、root 権限を保有するユーザーとしてログインします。
- 2 /usr/local/horizon/conf ディレクトリに移動し、domain_krb.properties というファイルを作成します。

- 3 domain_krb.properties ファイルを編集して、ホスト値にドメインのリストを追加します。この情報は、<AD Domain>=<host:port>, <host2:port2>, <host2:port2> のように追加します。

たとえば、リストを example.com=examplehost.com:636, examplehost2.example.com:389 のように入力します。
- 4 domain_krb.properties ファイルの所有者を horizon に変更し、グループを www に変更します。
chown horizon:www /usr/local/horizon/conf/domain_krb.properties と入力します。
- 5 サービスを再起動します。**service horizon-workspace restart** と入力します。

ジャストインタイム ユーザー プロビジョニングの設定

ジャストインタイム (JIT) プロビジョニングを設定することで、Active Directory から同期することなくユーザーを追加できます。

ジャストインタイム プロビジョニングをサポートするには、サードパーティ ID プロバイダを追加し、vRealize Automation 環境内でそのサードパーティ ID プロバイダとの接続を設定して、SAML プロトコルを介して他の SSO プロバイダとディレクトリ管理を連携させる必要があります。また、JIT ディレクトリなどの適切な名前を持つ新しいディレクトリを作成する必要があります。

ジャストインタイム プロビジョニングを有効にすると、指定したカスタム グループにジャストインタイム ユーザーを追加できます。この機能をサポートするには、適切なメンバーで構成されたカスタム グループを作成します。[カスタム グループとルールを使用したジャストインタイム ユーザーの追加](#)を参照してください。

注： ベスト プラクティスとして、デフォルトの vsphere.local テナントにはジャストインタイム プロビジョニングを設定しないでください。

前提条件

JIT プロビジョニングで使用するための適切なサードパーティ ID プロバイダを設定します。

手順

- 1 ジャストインタイム プロビジョニングのための ID プロバイダを作成します。
 - a [管理] - [ディレクトリ管理] - [ID プロバイダ] の順に選択します。
 - b [ID プロバイダを追加] ボタンをクリックして、ID プロバイダ インスタンスの設定を必要に応じて編集します。
 - ジャストインタイム プロビジョニング用にサードパーティの ID プロバイダを作成します。
 - [ジャストインタイム ディレクトリの作成] セクションで、ディレクトリと 1 つ以上のドメインの名前を入力します。
 - サードパーティの ID プロバイダの構成のためにネットワークを選択する必要があります。
 - 外部 VMware Identity Manager をサードパーティの ID プロバイダとして使用していて、userPrincipleName を使用してユーザーの認証を行っている場合は、userPrincipleName の名前 ID のマッピングの設定をデフォルトの x509SubjectName から unspecified に変更する必要があります。

ID プロバイダの作成の詳細については、[サードパーティ ID プロバイダの接続の構成](#)を参照してください。

2 ジャストインタイム ID プロバイダに SAML を設定します。

- a ID プロバイダから IdP メタデータをコピーします。
- b vRealize Automation で、ID プロバイダを選択し、IdP メタデータを [ID プロバイダ メタデータ (URL または XML)] テキスト ボックスに貼り付けます。
- c [保存] をクリックします。
- d [SAML 要求の名前 ID ポリシー (オプション)] ドロップダウン メニューで、適切な形式を選択します。
たとえば、メール アドレスを一意的ユーザー識別子として使用している場合は、
`urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress` を選択します。
- e [ユーザー] の見出しの下で、適切なディレクトリを選択します。
- f [ネットワーク] の見出しの下で、この ID プロバイダで使用するネットワークを選択します。
- g [認証方法] テキスト ボックスに、適切な名前を指定します。
- h [SAML コンテキスト] ドロップ ダウンで、
`urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport` を選択します。
- i [サービス プロバイダ (SP) メタデータ] リンクを右クリックし、別のブラウザ タブで開きます。
- j このメタデータを使用して、ID プロバイダの SAML 接続を設定します。

VMware Identity Manager を使用している場合は、SAML を設定する完全な手順について、VMware Identity Manager のドキュメントを参照してください。

3 [追加] をクリックします。

指定したディレクトリ名を使用して新しいディレクトリが作成されます。

4 vRealize Automation アクセス ポリシーを設定します。

- a [管理] - [ポリシー] の順に選択します。
- b ポリシー ルール テーブルの右上にある緑色の + アイコンをクリックします。
- c 該当する範囲とデバイス タイプに適用するポリシー ルールを設定します。
- d 認証方法の JIT プロビジョニングのためのサード パーティ ID プロバイダを設定するときに作成した認証方法を選択します。

Active Directory で同期されるユーザー属性の管理

ディレクトリ管理の [ユーザー属性] ページには、Active Directory 接続に同期するユーザー属性が一覧表示されません。

[ユーザー属性] ページで実行および保存された変更は、Directories Management ディレクトリの [マップされた属性] ページに追加されます。属性の変更は、Active Directory を次回同期するときに、ディレクトリでアップデートされます。

[ユーザー属性] ページには、Active Directory 属性にマッピングできるデフォルトのディレクトリ属性が表示されます。必須の属性を選択します。ディレクトリと同期するその他の Active Directory 属性を追加することができます。

表 2-6. ディレクトリと同期するデフォルトの Active Directory 属性

ディレクトリの属性名	Active Directory 属性とのデフォルトのマッピング
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeid	employeeID
ドメイン	canonicalName。オブジェクトの完全修飾ドメイン名を追加します。
disabled (external user disabled)	userAccountControl。UF_Account_Disable でフラグが設定されます。 アカウントが無効になると、ユーザーはログインしてアプリケーションとリソースにアクセスすることができません。ユーザーに使用資格が付与されているリソースはアカウントから削除されないため、フラグがアカウントから削除されても、ユーザーはログインして資格が付与されているリソースにアクセスすることができます。
phone	telephoneNumber
lastName	sn
firstName	givenName
email	mail
userName	sAMAccountName

[ユーザー属性] ページには、Active Directory 属性にマッピングできるデフォルトのディレクトリ属性が表示されます。必須の属性を選択します。ディレクトリと同期するその他の Active Directory 属性を追加することができます。

表 2-7. ディレクトリと同期するデフォルトの Active Directory 属性

ディレクトリの属性名	Active Directory 属性とのデフォルトのマッピング
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeid	employeeID
ドメイン	canonicalName。オブジェクトの完全修飾ドメイン名を追加します。
disabled (external user disabled)	userAccountControl。UF_Account_Disable でフラグが設定されます。 アカウントが無効になると、ユーザーはログインしてアプリケーションとリソースにアクセスすることができません。ユーザーに使用資格が付与されているリソースはアカウントから削除されないため、フラグがアカウントから削除されても、ユーザーはログインして資格が付与されているリソースにアクセスすることができます。
phone	telephoneNumber
lastName	sn

表 2-7. ディレクトリと同期するデフォルトの Active Directory 属性（続き）

ディレクトリの属性名	Active Directory 属性とのデフォルトのマッピング
firstName	givenName
email	mail
userName	sAMAccountName

コネクタとコネクタ クラスタの管理

[コネクタ] ページには、エンタープライズ ネットワークの展開されたコネクタが一覧表示されます。コネクタは、Active Directory とディレクトリ管理サービス間でユーザーとグループ データを同期し、ID プロバイダとして使用される場合には、サービスに対してユーザーを認証します。

vRealize Automation では、各 vRealize Automation アプライアンス にそれ自体のコネクタが含まれており、これらのコネクタはほとんどの展開に適しています。

コネクタ インスタンスをディレクトリに関連付けるときに、コネクタは、ワーカーと呼ばれる、関連付けられたディレクトリのパーティションを作成します。コネクタ インスタンスは、複数の関連付けられたワーカーを持つことができます。各ワーカーは、ID プロバイダとして動作します。コネクタは、1 つ以上のワーカーを介して Active Directory とサービス間でユーザーとグループを同期します。ワーカーごとに認証方法を定義および構成します。

[コネクタ] ページから Active Directory リンクのさまざまな特性を管理できます。このページには、各種管理タスクの完了を有効にするテーブルといくつかのボタンが含まれます。

- [ワーカー] 列で、ワーカーを選択してコネクタの情報を表示し、[認証アダプタ] ページに移動して、利用可能な認証方法のステータスを確認します。認証に関する情報については、[代替ユーザー認証製品とディレクトリ管理との統合](#)を参照してください。
- [ID プロバイダ] 列で、表示、編集、または無効にする IdP を選択します。[サード パーティ ID プロバイダの接続の構成](#)を参照してください。
- [関連付けられたディレクトリ] 列で、このワーカーに関連付けられているディレクトリにアクセスします。
- [ドメインに参加] をクリックして、コネクタを特定の Active Directory ドメインに参加させます。たとえば、Kerberos 認証を構成するときには、ユーザーを含む Active Directory ドメインか、ユーザーを含むドメインと信頼関係のある Active Directory ドメインに参加する必要があります。
- Active Directory（統合 Windows 認証）でディレクトリを構成するときには、構成の情報に従ってコネクタをドメインに参加させます。

クラスタ化環境のコネクタ

分散型の vRealize Automation 展開では、使用可能なすべてのコネクタが必要なユーザー認証を実行する一方で、指定された 1 つのコネクタはすべての構成の同期を処理します。通常、同期にはユーザー構成の追加、削除、または変更が含まれ、すべてのコネクタが使用可能な限り、同期は自動的に行われます。自動同期が発生しない特定の状況がいくつかあります。

ベース DN などのディレクトリ構成に関連する変更については、vRealize Automation はクラスタ内のすべてのコネクタに更新を自動的にプッシュしようとします。何らかの理由でコネクタが動作しない場合、または到達できない場合、そのコネクタがオンライン操作を再開した場合でも、更新を受信しません。構成変更を自動的に受信していない可能性があるコネクタに構成変更を実装するには、システム管理者が該当するすべてのコネクタに変更を手動で保存する必要があります。

変更に関するディレクトリ同期プロファイルについても、vRealize Automation は更新をすべてのコネクタに自動的にプッシュしようとします。同期コネクタが動作している場合は、更新が保存され、すべての使用可能な承認コネクタにプッシュされます。1つ以上のコネクタに到達できない場合、システム管理者は、すべてのコネクタが更新されなかったことを示す警告を受け取ります。同期コネクタが動作しない場合、更新が失敗して、エラーが発生します。システム管理者が同期コネクタとして指定されているコネクタを変更すると、新しい同期コネクタが最新の使用可能なプロファイル情報を受信し、この情報がすべての該当する使用可能なコネクタにプッシュされます。

コネクタ マシンをドメインに参加させる

状況に応じて、ディレクトリ管理コネクタを含むマシンをドメインに参加させる必要があります。

LDAP ディレクトリ経由の Active Directory については、ディレクトリを作成した後でドメインに参加させることができます。Active Directory (統合 Windows 認証) ディレクトリについては、ディレクトリを作成すると自動的にコネクタがドメインに参加します。どちらの場合も、適切な認証情報を指定する必要があります。

コネクタをドメインに参加させるには、Active Directory の「AD ドメインにコンピュータを参加させる」権限を含む証明書が必要です。これは、次の権限を使用して Active Directory に構成されます。

- コンピュータ オブジェクトの作成
- コンピュータ オブジェクトの削除

ドメインに参加させるときには、Active Directory 内のデフォルトの場所にコンピュータ オブジェクトが作成されます。

ドメインに参加させる権限を持たない場合、または企業ポリシーによってコンピュータ オブジェクト用にカスタムの場所が必要となる場合は、オブジェクトを作成するよう管理者に依頼し、その後コネクタ マシンをドメインに参加させる必要があります。

手順

- 1 Active Directory 内で企業ポリシーで指定された場所にコンピュータ オブジェクトを作成するよう、Active Directory の管理者に依頼します。コネクタのホスト名を指定する必要があります。必ず完全修飾ドメイン名 (例: `server.example.com`) を指定してください。

ホスト名は、管理コンソールの [コネクタ] ページで [ホスト名] 列に表示されます。[管理] - [ディレクトリ管理] - [コネクタ] の順に選択します。

- 2 コンピュータ オブジェクトが作成されたら、[コネクタ] ページの [ドメインに参加させる] をクリックし、ディレクトリ管理で利用可能なドメイン ユーザー アカウントを使用してドメインに参加させます。

ドメイン コントローラの選択

ユーザー構成を必要としないドメイン コントローラの動的リストは、ディレクトリ管理によって維持されます。

ディレクトリ管理は LDAP Ping に基づいてドメイン コントローラを定期的に更新し、再検出し、並べ替えて、domain_krb プロパティ ファイルとカスタム krb5.conf ファイルに格納します。最適なドメイン コントローラが最初に表示されるため、認証操作や同期操作などのすべての目的に使用されます。このドメイン コントローラが 10 ミリ秒以内に応答しない場合は、ドメイン コントローラのリストが再更新されます。これにより、ドメイン コントローラに障害が発生しているときでも、ディレクトリ管理では最適なドメイン コントローラを一貫して使用することができます。

アクセス ポリシーの管理

Directories Management のポリシーとは一連のルールで、マイ アプリ ポータルへのアクセスしたり、有効な Web アプリケーションを起動する場合に、ユーザーが満たす必要がある条件を指定します。

ポリシーの一部としてルールを作成します。ポリシーの各ルールでは、次の情報を指定できます。

- 企業ネットワークの内部または外部などのユーザーがログインできるネットワーク範囲。
- このポリシーによってアクセスが許可されるデバイス タイプ。
- 有効な認証方法が適用される順序。
- 認証の有効時間数。
- カスタムのアクセス拒否メッセージ。

注： ポリシーは、Web アプリケーションのセッションの持続時間の長さを制御しません。ポリシーは、ユーザーが Web アプリケーションを起動するのに必要な時間を制御します。

Directories Management サービスには、編集可能なデフォルトのポリシーが含まれています。このポリシーは、サービス全体へのアクセスを制御します。[デフォルトのアクセス ポリシーの適用](#)を参照してください。追加のポリシーを作成して、特定の Web アプリケーションへのアクセスを制御できます。Web アプリケーションにポリシーを適用しない場合、デフォルトのポリシーが適用されます。

アクセス ポリシー設定の構成

ポリシーには 1 つ以上のアクセス ルールが含まれます。各ルールは、アプリケーション ポータルに対する全体としてのユーザー アクセスまたは指定された Web アプリケーションへのユーザー アクセスを管理するために構成できる設定値の集まりです。

ネットワーク範囲

各ルールについて、ネットワーク範囲を指定してユーザー ペースを決定します。ネットワーク範囲は、1 つ以上の IP 範囲から構成されます。アクセス ポリシー セットを構成する前に、[セットアップ] > [ネットワーク範囲] ページの [ID とアクセス管理] タブでネットワーク範囲を作成します。

デバイス タイプ

このルールで管理するデバイス タイプを選択します。クライアント タイプには、[Web ブラウザ]、[Identity Manager Client アプリ]、[iOS]、[Android]、および [すべてのデバイス タイプ] があります。

グループを追加

ユーザーのグループ メンバーシップに基づいて、認証に異なるポリシーを適用することができます。特定の認証フローを使用してログインするユーザーのグループを割り当てる場合、グループをアクセス ポリシー ルールに追加することができます。グループをエンタープライズ ディレクトリ、または管理コンソールで作成したローカル グループと同期することができます。グループ名は、1つのドメイン内で一意である必要があります。

アクセス ポリシー ルールでグループを使用するには、[ディレクトリ管理] > [ポリシー] ページで新しいポリシーを構成し、そのポリシーに必要なグループを選択します。ポリシーは [ユーザー属性] ページでマップしてから、ディレクトリと同期する必要があります。

アクセス ポリシー ルールでグループを使用する場合、ユーザーのログイン エクスペリエンスは通常と異なります。ドメインの選択と認証情報の入力求められる代わりに、一意の ID の入力を求めるページが表示されます。Directories Management で一意の ID に基づいて内部データベースからユーザーが見つけれられ、該当のルールで設定された認証ページが表示されます。

グループが選択されていない場合は、アクセス ポリシー ルールがすべてのユーザーに適用されます。グループに基づくルールとすべてのユーザーに対するルールが含まれるアクセス ポリシー ルールを設定する場合は、すべてのユーザーに対して指定されたルールがポリシーの [ポリシー ルール] セクションの最後にリストされるようにしてください。

ユーザーにルールを適用する方法の詳細については、VMware Identity Manager ドキュメントの「一意の識別子を使用したログイン エクスペリエンス」を参照してください。

認証方法

ポリシー ルールについて認証方法の優先順位を設定します。認証方法は、表示されている順序で適用されます。ポリシーの認証方法とネットワーク範囲の構成と一致する最初の ID プロバイダ インスタンスが選択され、ユーザー認証要求は、その ID プロバイダ インスタンスに転送され認証が行われます。認証が失敗すると、リストに表示されている次の認証方法が選択されます。証明書によって認証する場合、この認証方法をリストの最初に表示する必要があります。

2つの認証方法を使用してユーザーの認証情報を検証し、パスしなければユーザーがサインインできないようにするアクセス ポリシー ルールを構成できます。1つまたは両方の認証方法が失敗し、フォールバック方法も構成されている場合、ユーザーは構成されている次の認証方法の認証情報を入力するように求められます。次の2つのシナリオから、認証チェーンがどのように機能するかを把握できます。

- 最初のシナリオでは、パスワードと Kerberos の認証情報を使用してユーザーを認証することを求めるアクセス ポリシー ルールが構成されています。認証にパスワードと RADIUS の認証情報を求めるフォールバック認証がセットアップされています。ユーザーはパスワードを正しく入力しましたが、正しい Kerberos の認証情報を入力していません。ユーザーは正しいパスワードを入力したため、フォールバック認証で、RADIUS の認証情報だけが要求されます。ユーザーはパスワードを再入力する必要はありません。
- 2番目のシナリオでは、パスワードと Kerberos の認証情報を使用してユーザーを認証することを求めるアクセス ポリシー ルールが構成されています。認証に RSA SecurID と RADIUS を求めるフォールバック認証がセットアップされています。ユーザーはパスワードを正しく入力しましたが、正しい Kerberos の認証情報を入力していません。フォールバック認証では、認証に RSA SecurID の認証情報と RADIUS の認証情報の両方が要求されます。

認証セッションの時間の長さ

各ルールについて、認証が有効となる時間の長さを設定します。この値は、ユーザーがポータルにアクセスするか、または特定の Web アプリケーションを起動した前回の認証イベント以来の最長時間を決定します。たとえば、Web アプリケーション ルールに値 4 を指定すると、ユーザーが別の認証イベントを開始して時間が延長される場合を除いて、Web アプリケーションを 4 時間起動できます。

カスタムのアクセス拒否エラー メッセージ

無効な認証情報、誤った構成、またはシステム エラーによってユーザーのログイン試行が失敗すると、アクセス拒否のメッセージが表示されます。デフォルトのメッセージは、以下のとおりです。

有効な認証方法が見つからなかったため、アクセスは拒否されました。

各アクセス ポリシー ルールに、デフォルトのメッセージをオーバーライドするカスタム エラー メッセージを作成できます。このカスタム メッセージには、アクション メッセージを呼び出すテキストおよびリンクを含めることができます。たとえば、管理するモバイル デバイス用のポリシー ルールで、ユーザーが未登録のデバイスからログインしようとする場合に次のカスタム エラー メッセージが表示されることがあります。

社内リソースにアクセスするには、このメッセージの最後にあるリンクをクリックしてデバイスを登録してください。デバイスが既に登録されている場合は、サポートにお問い合わせください。

デフォルト ポリシーの例

次のポリシーは、デフォルトのポリシーを構成してアプリ ポータルへのアクセスを制御する方法の例として参考になります。[ユーザー アクセス ポリシーの管理](#)を参照してください。

ポリシー ルールは、表示されている順序で評価されます。[ポリシー ルール] セクションでルールをドラッグ アンドドロップして、ポリシーの順序を変更できます。

次の使用事例では、このポリシーの例は、すべてのアプリケーションに適用されています。

ポリシー ルール

上記の Web アプリケーションにアクセスするルールのリストを作成できます。ルールごとに、IP ネットワーク範囲、アプリケーションにアクセスできるデバイスのタイプ、方法および認証順序、再認証前にユーザーがアプリケーションを使用できる最大時間数を選択します。

ネットワーク範囲	デバイス タイプ	認証方式	再認証	
すべての範囲	Web ブラウザ	Password	8 時間	✖ +
すべての範囲	Identity Manager Client アプリ	Password	2160 時間	✖ +

- 社内ネットワーク（内部ネットワーク範囲）の場合、Kerberos とパスワード認証という 2 つの認証方法がフォールバック方法として、ルールに構成されます。社内ネットワークからアプリケーション ポータルにアクセスするため、サービスはまず Kerberos によるユーザー認証を試行します。これは、ルールで最初に記載されている認証方法であるためです。それが失敗すると、ユーザーは Active Directory のパスワードを入力するよう求められます。ユーザーはブラウザを使用してログインし、8 時間のセッション期限までユーザー ポータルにアクセスできます。

- 外部ネットワーク（全ての範囲）からのアクセスの場合、構成される認証方法は RSA SecurID の 1 つだけです。外部ネットワークからアプリケーション ポータルにアクセスする際、ユーザーは SecurID でログインするよう要求されます。ユーザーがブラウザを使用してログインすると、4 時間のセッション期限までアプリケーション ポータルにアクセスできます。
- 2 ユーザーがリソースへのアクセスを試みると、Web アプリケーション固有のポリシーが適用されている Web アプリケーションを除いて、デフォルトのポータル アクセス ポリシーが適用されます。

たとえば、このようなリソースの再認証の時間は、デフォルトのアクセス ポリシー ルールの再認証の時間と同一になります。アプリ ポータルにログインしているユーザーの時間がデフォルトのアクセス ポリシー ルールに従って 8 時間である場合、ユーザーがセッション中にリソースを起動しようとする、アプリケーションはユーザーに再認証を求めずに起動します。

グループベースのアクセス ポリシーの構成

グループベースのアクセス ポリシーを構成して、グループの割り当てに基づいてログイン権限を制御することができます。

ディレクトリ管理には、すべてのグループとすべてのネットワーク範囲をサポートするデフォルトのアクセス ポリシーが含まれています。これらのポリシーを変更してより限定的にすることも、異なるログイン ポリシーをサポートする新しいポリシーを作成することもできます。

手順

- 1 目的のポリシーにグループを追加します。

- a [管理] - [ディレクトリ管理] - [ポリシー] の順に選択します。
- b デフォルトのアクセス ポリシーを開くか、新しいアクセス ポリシーを作成します。
- c Web ブラウザのデバイス タイプで構成されているポリシー ルールを編集します。

ポリシーを編集するには、その認証方法をクリックします。デフォルトでは、すべての IP アドレスとすべてのユーザーに適用される 2 つのポリシー ルールがあります。

選択したポリシーの [ポリシー ルールの編集] ページが開きます。ネットワーク範囲、デバイス タイプ、認証方法、およびポリシーに対するその他のルール パラメータなど、各種のパラメータを編集できます。

- d [ポリシー ルールの編集] ページで [グループの編集] をクリックすると、ポリシーで使用できるすべてのグループが表示されます。

このページには、テナントに関連付けられているすべてのグループが表示されます。

- e ポリシーに関連付けるグループを選択します。
- f [OK] をクリックします。

[ポリシー ルールの編集] ページに選択したグループが表示されます。

- g [ポリシー ルールの編集] ページで [OK] をクリックし、ポリシー ルールへの変更を保存します。

[ポリシー] ページが表示され、ポリシーに対して選択されたグループの数を示されます。

- h [ポリシー] ページで [保存] をクリックします。

2 グループ ポリシーのネットワーク範囲を構成します。

- a [管理] - [ディレクトリ管理] - [ネットワーク範囲] の順に選択します。

デフォルトでは、すべてのネットワーク範囲のすべての IP アドレスをカバーする All Ranges の事前定義された設定があります。新しいネットワーク範囲を作成することも、既存のネットワーク範囲の 1 つを編集することもできます。

- b [ネットワーク範囲の追加] をクリックします。

[ネットワーク範囲の編集] ページが開きます。

- c 新しいネットワーク範囲の [名前] を入力し、必要に応じて [説明] を追加します。

結果

ユーザーが vRealize Automation にログインするときは、ドメインを選択し、有効なユーザー名とパスワードを入力する必要があります。該当のポリシーでグループが指定されている場合でも、有効なユーザーのユーザー名とパスワードを入力する必要があります。

Web アプリケーション固有のポリシーの管理

Web アプリケーションをカタログに追加する際に、Web アプリケーション固有のアクセス ポリシーを作成できます。たとえば、特定の Web アプリケーションについて、そのアプリケーションにアクセスできる IP アドレス、使用する認証方法、および再認証が必要になるまでの期間を指定するルール付きのポリシーを作成できます。

次の Web アプリケーション固有のポリシーは、指定した Web アプリケーションへのアクセスを制御するために作成できるポリシーの例です。

例 1: 厳格な Web アプリケーション固有のポリシー

この例では、新しいポリシーが作成され、機密性の高い Web アプリケーションに適用されます。

Sensitive Web Application
To be applied to Web application that should have limited access.

ポリシーの削除

ポリシー名*

Sensitive Web Application

説明

To be applied to Web application that should have limited access.

適用先

このポリシーの適用先のカテゴリからアプリケーションを選択します。

AirWatch
Content Locker

アプリを編集

ポリシー ルール

上記のアプリケーションに対するアクセスのルールを作成できます。ルールごとに、IP ネットワーク範囲、アプリケーションにアクセスできるデバイスのタイプ、方法および認証順序、再認証までにユーザーがアプリケーションを使用できる最大セッション数を選択します。

ネットワーク...	デバイス...	認証方法	再認証	グループ	
Internal Network	Web ブラウザ	まず、次を試行: Kerberos さらに 1 以上の フォールバック...	8 時間	すべてのユーザー	✖ +
すべての範囲	Web ブラウザ	SecurID	4 時間	すべてのユーザー	✖ +

保存

キャンセル

- 1 企業ネットワークの外部からサービスにアクセスするには、ユーザーは RSA SecurID を使用してログインする必要があります。ユーザーはブラウザを使用してログインし、デフォルトのアクセス ルールに指定されているように、4 時間のセッションまでアプリ ポータルにアクセスできます。
- 2 4 時間後に、ユーザーは機密性の高い Web アプリケーション ポリシー セットが適用された Web アプリケーションを起動しようとしています。
- 3 サービスは、ポリシーのルールをチェックし、ユーザー リクエストが Web ブラウザと全範囲ネットワーク範囲から来ているため、全範囲ネットワーク範囲のポリシーを適用します。

このユーザーは、RSA SecurID の認証方法でログインしていますが、セッションがちょうど失効しました。このユーザーは再認証にリダイレクトされます。再認証により、ユーザーには再度 4 時間のセッションが与えられ、アプリケーションの起動が許可されます。これに続く 4 時間、ユーザーは再認証する必要なしにアプリケーションを起動し続けることができます。

例 2：さらに厳格な Web アプリケーション固有のポリシー

極めて機密性の高い Web アプリケーションに適用するさらに厳格なルールの場合は、デバイスを問わず、1 時間後に SecureID を使用した再認証を必要とします。次の例は、このタイプのポリシー アクセス ルールの実装方法を示しています。

- 1 パスワードによる認証方法で企業ネットワークの内部からユーザーがログインします。
今、例 1 でセットアップしたように、ユーザーは 8 時間アプリ ポータルにアクセスできます。
- 2 ユーザーは、例 2 のポリシー ルールが適用された Web アプリケーションを直ちに起動しようとしています。このためには RSA SecurID 認証が必要です。
- 3 このユーザーは、RSA SecurID を提供する ID プロバイダにリダイレクトされます。
- 4 ユーザーがログインに成功すると、サービスによりアプリケーションが起動され、認証イベントが保存されます。

ユーザーはこのアプリケーションを最大 1 時間起動し続けることができますが、1 時間後、ポリシー ルールの指示通りに再認証を求められます。

ユーザー アクセス ポリシーの管理

vRealize Automation では、アプリケーションにアクセスするテナントを管理するため、デフォルトでユーザー アクセス ポリシーが提供されます。これはそのまま使用するか、あるいは必要に応じて編集することができます。

vRealize Automation にはデフォルトのユーザー アクセス ポリシーが付属しており、新しいポリシーは追加できません。既存のポリシーを編集して、ルールを追加することはできます。

前提条件

- 環境に適した ID プロバイダを選択または構成します。 [サードパーティ ID プロバイダの接続の構成](#)を参照してください。
- 環境に適したネットワーク範囲を構成します。 [ネットワーク範囲の追加または編集](#)を参照してください。
- 環境に適した認証方法を構成します。 [代替ユーザー認証製品とディレクトリ管理との統合](#)を参照してください。
- サービスへのユーザー アクセスを全体的に制御するため、デフォルト ポリシーを編集する場合、Web アプリケーション固有のポリシーを作成する前にデフォルト ポリシーを構成します。
- Web アプリケーションをカタログに追加します。Web アプリケーションが [カタログ] ページに表示されていないと、ポリシーを追加することはできません。
- テナント管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [ディレクトリ管理] - [ポリシー] の順に選択します。
- 2 [ポリシーの編集] をクリックし、新しいポリシーを追加します。
- 3 該当のテキスト ボックスにポリシーの名前と説明を追加します。
- 4 適用先のセクションで、[選択] をクリックし、表示されるページで、このポリシーに関連付けられている Web アプリケーションを選択します。
- 5 ポリシー ルールのセクションで、[+] をクリックしてルールを追加します。
 ポリシー ルールを追加するページが表示されます。
 - a このルールに適用するネットワーク範囲を選択します。
 - b このルールで Web アプリケーションにアクセスできるデバイス タイプを選択します。
 - c 適用する順番で使用する認証方法を選択します。
 - d Web アプリケーション セッションを開いている時間数を指定します。
 - e [保存] をクリックします。
- 6 必要に応じて、追加のルールを構成します。
- 7 [保存] をクリックします。

追加の ID プロバイダの接続の構成

追加の組み込み ID プロバイダや、サードパーティの ID プロバイダなどのさまざまな ID 管理のシナリオに対応するため、必要に応じて、追加の ID プロバイダの接続を構成できます。

ディレクトリ管理を使用して、3 つのタイプの ID プロバイダの接続を作成できます。

- サードパーティ IDP を作成 - このアイテムを使用すると、外部のサードパーティ ID プロバイダへの接続を作成できます。サードパーティ ID プロバイダのインスタンスを追加する前に、次の項目を確認してください。
 - サードパーティ インスタンスが SAML 2.0 互換であり、サービスがサードパーティ インスタンスにアクセスできることを確認します。
 - 管理コンソールで ID プロバイダを構成するときに追加する、適切なサードパーティ メタデータ情報を取得します。サードパーティ インスタンスから取得するメタデータ情報は、メタデータへの URL または実際のメタデータのいずれかです。
- Workspace IDP を作成 - ディレクトリ管理の構成時にコネクタでユーザーを認証できるようにする場合、Workspace IDP は ID プロバイダとして作成され、パスワード認証が有効になります。さまざまなロード バランサの背後に追加の Workspace ID プロバイダを構成できます。
- 組み込み IDP を作成 - 組み込み ID プロバイダでは、内部のディレクトリ管理メカニズムを使用して、認証をサポートします。組み込み ID プロバイダを構成すると、オンプレミス コネクタが不要な認証方法を使用できます。組み込み ID プロバイダを構成するときに、このプロバイダで使用する認証方法を関連付けます。
- **サードパーティ ID プロバイダの接続の構成**
vRealize Automation にはデフォルトの ID プロバイダ接続インスタンスが付属しています。ユーザーは、ジャストインタイム ユーザー プロビジョニングまたは他のカスタム構成をサポートするために追加の ID プロバイダ接続を作成することがあります。
- **追加の Workspace ID プロバイダの構成**
ディレクトリ管理コネクタを構成してユーザー認証を行う場合は、Workspace IDP を作成し、パスワード認証を有効にします。
- **組み込み ID プロバイダの接続の構成**
複数の組み込み ID プロバイダを構成し、これらに認証方法を関連付けることができます。

サードパーティ ID プロバイダの接続の構成

vRealize Automation にはデフォルトの ID プロバイダ接続インスタンスが付属しています。ユーザーは、ジャストインタイム ユーザー プロビジョニングまたは他のカスタム構成をサポートするために追加の ID プロバイダ接続を作成することがあります。

vRealize Automation にはデフォルトの ID プロバイダが付属しています。多くの場合、デフォルトのプロバイダでお客様のニーズを十分に満たすことができます。企業の既存の ID 管理ソリューションを使用している場合、カスタムの ID プロバイダを設定し、ユーザーを既存の ID ソリューションにリダイレクトすることができます。

カスタムの ID プロバイダを使用すると、ディレクトリ管理は、プロバイダとの信頼関係を確立するためにそのプロバイダからの SAML メタデータを使用します。この関係が確立されると、ディレクトリ管理は、サブジェクト名の ID に基づいて内部の vRealize Automation ユーザーのリストに SAML アサーションからユーザーをマッピングします。

前提条件

- この ID プロバイダ インスタンスで認証を行うネットワーク範囲を設定します。[ネットワーク範囲の追加または編集](#)を参照してください。
- サードパーティのメタデータ ドキュメントにアクセスします。これは、メタデータへの URL または実際のメタデータのいずれかです。
- テナント管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [ディレクトリ管理] - [ID プロバイダ] の順に選択します。

このページには、構成済み ID プロバイダがすべて表示されます。

- 2 [ID プロバイダを追加] をクリックします。

ID プロバイダのオプション メニューが表示されます。

- 3 [サード パーティ IDP を作成] を選択します。

- 4 適切な情報を入力して、ID プロバイダを構成します。

オプション	説明
ID プロバイダ名	この ID プロバイダ インスタンスの名前を入力します。
SAML メタデータ	<p>サードパーティの XML ベースの IdP メタデータ ドキュメントを追加して、ID プロバイダとの信頼を確立します。</p> <ol style="list-style-type: none"> 1 SAML メタデータ URL または xml コンテンツをテキスト ボックスに入力します。 2 [プロセス IdP メタデータ] をクリックします。IdP でサポートされている NameID の形式は、メタデータから抽出され、名前 ID 形式テーブルに追加されます。 3 名前 ID 値の列で、表示される ID 形式にマッピングするサービスのユーザー属性を選択します。独自のサードパーティ名の ID 形式を追加して、サービスのユーザー属性値にマッピングできます。 4 (オプション) NameIDPolicy 応答識別子の文字列形式を選択します。
ユーザー	この ID プロバイダを使用して認証できるユーザーの Directories Management ディレクトリを選択します。
ジャストインタイムのユーザー プロビジョニング	<p>適切なサード パーティ ID プロバイダを使用してジャストインタイムのプロビジョニングをサポートするには適切なオプションを選択します。</p> <p>ジャストインタイムのプロビジョニングに使用する [ディレクトリ名] を入力します。</p> <p>ジャストインタイムのプロビジョニングに使用する外部の ID プロバイダ内にある 1 つまたは複数の [ドメイン] を入力します。</p>
ネットワーク	<p>サービス内で構成されている既存のネットワーク範囲が表示されます。</p> <p>この ID プロバイダ インスタンスで認証を行うユーザーのネットワーク範囲を、IP アドレスで指定します。</p>
認証方法	サードパーティ ID プロバイダがサポートする認証方法を追加します。認証方法をサポートする SAML 認証コンテキスト クラスを選択します。

オプション	説明
SAML 署名証明書	[サービス プロバイダ (SP) メタデータ] をクリックして、Directories Management の SAML サービス プロバイダのメタデータ URL を確認します。URL をコピーして保存します。この URL は、サードパーティ ID プロバイダで SAML アサーションを編集して Directories Management ユーザーをマッピングするときに構成されます。
ホスト名	[ホスト名] のフィールドが表示される場合は、認証用に ID プロバイダにリダイレクトするホスト名を入力します。443 以外の非標準ポートを使用している場合、「ホスト名:ポート」の形式で設定します。たとえば、myco.example.com:8443 のように入力します。

5 [追加] をクリックします。

次のステップ

- サードパーティの ID プロバイダ インスタンスを設定するために必要な Directories Management サービス プロバイダのメタデータをコピーして保存します。このメタデータは、ID プロバイダ ページの SAML 署名証明書のセクションで入手できます。
- サービスのデフォルト ポリシーに ID プロバイダの認証方法を追加します。

カタログに追加するリソースの追加とカスタマイズに関する情報については、Directories Management ガイドを参照してください。

追加の Workspace ID プロバイダの構成

ディレクトリ管理コネクタを構成してユーザー認証を行う場合は、Workspace IDP を作成し、パスワード認証を有効にします。

複数のロード バランサの背後で動作する追加のコネクタを構成することができます。展開に複数のロード バランサが含まれている場合は、ロード バランシングされた各構成の認証用に、追加の Workspace ID プロバイダ (IDP) を構成できます。

手順

- 1 [管理] - [ディレクトリ管理] - [ID プロバイダ] の順に選択します。

このページには、構成済み ID プロバイダがすべて表示されます。

- 2 [ID プロバイダを追加] をクリックします。

ID プロバイダのオプション メニューが表示されます。

- 3 [Workspace IDP を作成] を選択します。

- 4 適切な情報を入力して、ID プロバイダを構成します。

オプション	説明
ID プロバイダ名	この組み込み ID プロバイダ インスタンスの名前を入力します。
ユーザー	認証するユーザーを選択します。構成されたディレクトリが一覧表示されます。
ユーザー	この Workspace ID プロバイダを使用して認証できるユーザーのグループを選択します。

オプション	説明
ネットワーク	サービス内で構成されている既存のネットワーク範囲が表示されます。この ID プロバイダ インスタンスで認証を行うユーザーのネットワーク範囲を、IP アドレスで指定します。
認証方法	サービスで構成されている認証方法が表示されます。この ID プロバイダに関連付ける認証方法のチェック ボックスを選択します。 AirWatch および AirWatch Connector に関するデバイスの準拠状態とパスワードについては、[AirWatch の設定] ページでオプションが有効であることを確認します。

5 [追加] をクリックします。

組み込み ID プロバイダの接続の構成

複数の組み込み ID プロバイダを構成し、これらに認証方法を関連付けることができます。

前提条件

組み込みの Kerberos 認証を使用している場合は、iOS デバイス管理プロファイルの AirWatch 構成で使用する KDC 発行者証明書をダウンロードします。

手順

1 [管理] - [ディレクトリ管理] - [ID プロバイダ] の順に選択します。

このページには、構成済み ID プロバイダがすべて表示されます。

2 [ID プロバイダを追加] をクリックします。

ID プロバイダのオプション メニューが表示されます。

3 [組み込み IDP を作成] を選択します。

4 適切な情報を入力して、ID プロバイダを構成します。

オプション	説明
ID プロバイダ名	この組み込み ID プロバイダ インスタンスの名前を入力します。
ユーザー	認証するユーザーを選択します。構成されたディレクトリが一覧表示されます。
ネットワーク	サービス内で構成されている既存のネットワーク範囲が表示されます。この ID プロバイダ インスタンスで認証を行うユーザーのネットワーク範囲を、IP アドレスで指定します。
認証方法	サービスで構成されている認証方法が表示されます。この ID プロバイダに関連付ける認証方法のチェック ボックスを選択します。 AirWatch および AirWatch Connector に関するデバイスの準拠状態とパスワードについては、[AirWatch の構成] ページで適切なオプションが有効であることを確認します。

5 [追加] をクリックします。

代替ユーザー認証製品とディレクトリ管理との統合

一般的に、ディレクトリ管理を最初に構成する場合、既存の vRealize Automation インフラストラクチャに付属するコネクタを使用し、ユーザー ID とパスワードをベースとした認証および管理用の Active Directory 接続を作

成します。また、ディレクトリ管理と、Kerberos や RSA SecurID など、他の認証ソリューションを統合することができます。

ID プロバイダのインスタンスとして、Directories Management コネクタ インスタンス、サードパーティの ID プロバイダ インスタンス、または両方の組み合わせを利用できます。

Directories Management サービスで使用する ID プロバイダ インスタンスは、SAML 2.0 アサーションを使用してサービスと通信するネットワーク内のフェデレーション機関を作成します。

Directories Management サービスを初めて展開する場合、コネクタがサービスの最初の ID プロバイダになります。ユーザー認証と管理には既存の Active Directory インフラストラクチャが使用されます。

次の認証方法がサポートされます。これらの認証方法は、管理コンソールで構成します。

表 2-8. ディレクトリ管理でサポートされるユーザー認証タイプ

認証タイプ	説明
パスワード（オンプレミス展開）	Active Directory 以外何も構成しない場合、Directories Management は Active Directory によるパスワード認証をサポートします。この方法では、Active Directory に対して直接、ユーザーを認証します。
Kerberos（デスクトップ向け）	Kerberos 認証は、ドメイン ユーザーにアプリケーション ポータルへのシングル サインオン アクセスを提供します。ユーザーは、一度ネットワークにサインインすれば再度サインインする必要はありません。
証明書（オンプレミス展開）	証明書による認証を構成すると、クライアントはデスクトップやモバイル デバイス上の証明書、およびスマート カード アダプタを使用した認証を行うことができます。 証明書による認証では、ユーザーが認証に必要な物を用意し、知識を持つ必要があります。X.509 証明書は、公開鍵基盤の規格を使用して、証明書に含まれる公開鍵がユーザーに属するものであることを確認します。
RSA SecurID（オンプレミス展開）	RSA SecurID 認証が構成されている場合、Directories Management は RSA SecurID サーバの認証エージェントとして構成されます。RSA SecurID 認証では、ユーザーがトークン ベースの認証システムを使用する必要があります。RSA SecurID は、企業ネットワークの外部から Directories Management にアクセスするユーザーのための認証方法です。
RADIUS（オンプレミス展開）	RADIUS 認証は、二要素認証オプションを提供します。Directories Management サービスにアクセスできる RADIUS サーバをセットアップします。ユーザーがユーザー名とパスワードでログインすると、認証のためのアクセス要求が RADIUS サーバに送信されます。
RSA Adaptive Authentication（オンプレミス展開）	RSA 認証は、Active Directory によるユーザー名とパスワードのみの認証よりも強固な多要素認証を実現します。RSA Adaptive Authentication が有効の場合、リスク ポリシーで指定されたリスク インジケータが RSA ポリシー管理アプリケーションで設定されます。必要な認証プロンプトを決定するために、アダプティブ認証の Directories Management サービス構成が使用されます。
モバイル SSO（iOS 版）	iOS 版のモバイル SSO 認証は AirWatch により管理された iOS デバイスのシングル サインオン認証に使用されます。モバイル SSO（iOS 版）認証は、Directories Management サービスの一部であるキー配布センター（KDC）を使用します。KDC サービスは、この認証方法を有効にする前に VMware Identity Manager サービスで開始する必要があります。
モバイル SSO（Android 版）	Android 版のモバイル SSO 認証は AirWatch により管理された Android デバイスのシングル サインオン認証に使用されます。認証用の証明書を AirWatch から取得するため、Directories Management サービスと AirWatch の間でプロキシ サービスが設定されます。
パスワード（AirWatch コネクタ）	AirWatch Cloud Connector は、ユーザー パスワード認証のために Directories Management サービスに統合することができます。Directories Management サービスを構成して AirWatch ディレクトリからのユーザーを同期します。

ユーザーは、認証方法、デフォルトのアクセス ポリシー ルール、ネットワーク範囲、および構成する ID プロバイダ インスタンスに基づいて認証されます。認証方法が構成された後、使用される認証方法をデバイス タイプに応じて指定するアクセス ポリシー ルールを作成します。

■ Directories Management のための SecurID の構成

RSA SecurID サーバを構成する場合は、RSA SecurID サーバの認証エージェントとして Directories Management サービスの情報を追加し、Directories Management サービスで RSA SecurID サーバの情報を構成する必要があります。

■ Directories Management の RADIUS の構成

RADIUS (リモート認証ダイヤルイン ユーザー サービス) 認証の使用をユーザーに要求するように Directories Management を構成できます。RADIUS サーバ情報は Directories Management サービス上で構成します。

■ ディレクトリ管理で証明書またはスマート カード アダプタを使用するための構成

X.509 証明書認証を構成すると、クライアントはデスクトップやモバイル デバイス上の証明書や、スマート カード アダプタを使用して認証できます。証明書による認証は、ユーザーの認証方法 (プライベート キーまたはスマート カード) と、ユーザーが入力する情報 (プライベート キーのパスワードまたはスマート カードの PIN) に基づいて行われます。X.509 証明書は、公開鍵基盤 (PKI) の規格を使用して、証明書に含まれるパブリック キーがユーザーに属するものであることを確認します。スマート カード認証では、ユーザーはコンピュータにスマート カードを接続して、PIN を入力します。

■ ユーザー認証のためのサードパーティ ID プロバイダ インスタンスの構成

Directories Management サービスでユーザー認証に使用するサードパーティ ID プロバイダを構成できます。

■ ユーザーに適用する認証方法の管理

Directories Management サービスでは、構成する認証方法、デフォルトのアクセス ポリシー、ネットワーク範囲、および ID プロバイダ インスタンスに基づいて、ユーザーを認証します。

■ Directories Management 用 Kerberos の構成

Kerberos 認証によって、Active Directory ドメインに正常にサインインしたユーザーは、追加の認証情報を指定せずにアプリ ポータルにアクセスできます。Windows 認証を有効にすると、Kerberos プロトコルによってユーザーのブラウザと Directories Management サービス間の通信が安全になります。Kerberos がユーザーの展開環境で機能するようにするために、Active Directory を直接構成する必要はありません。

Directories Management のための SecurID の構成

RSA SecurID サーバを構成する場合は、RSA SecurID サーバの認証エージェントとして Directories Management サービスの情報を追加し、Directories Management サービスで RSA SecurID サーバの情報を構成する必要があります。

SecurID を構成してセキュリティを強化する場合は、お使いの Directories Management 展開環境向けにネットワークが適切に構成されていることを確認する必要があります。SecurID については特に、正しいポートが開いている、SecurID がネットワーク外部のユーザーを認証できることを確認する必要があります。

Directories Management セットアップ ウィザードを実行し、Active Directory との接続を構成したら、RSA SecurID サーバを準備するために必要な情報を取得できます。Directories Management 用に RSA SecurID サーバを準備してから、管理コンソールの SecurID を有効化します。

■ RSA SecurID サーバを準備する

RSA SecurID サーバは Directories Management アプライアンスを認証エージェントとした情報で構成される必要があります。必須の情報は、ネットワーク インターフェイスのホスト名と IP アドレスです。

■ RSA SecurID 認証の構成

ディレクトリ管理を RSA SecurID サーバの認証エージェントとして構成したら、コネクタに RSA SecurID 構成情報を追加する必要があります。

RSA SecurID サーバを準備する

RSA SecurID サーバは Directories Management アプライアンスを認証エージェントとした情報で構成される必要があります。必須の情報は、ネットワーク インターフェイスのホスト名と IP アドレスです。

前提条件

- RSA Authentication Manager のバージョン 6.1.2、7.1 SP2 以降、または 8.0 以降がエンタープライズ ネットワークにインストールされて動作していることを確認します。Directories Management サーバは、AuthSDK_Java_v8.1.1.312.06_03_11_03_16_51 (Agent API 8.1 SP1) を使用しますが、このバージョンは、RSA Authentication Manager (RSA SecurID サーバ) の以前のバージョンのみをサポートしています。RSA Authentication Manager (RSA SecurID サーバ) のインストールと構成の詳細については、RSA のドキュメントを参照してください。

手順

- 1 RSA SecurID サーバのサポート対象バージョンで、Directories Management Connector を認証エージェントとして追加します。以下の情報を入力します。

オプション	説明
ホスト名	Directories Management のホスト名。
IP アドレス	Directories Management の IP アドレス。
代替 IP アドレス	RSA SecurID サーバに到達するために、トラフィックがコネクタからネットワーク アドレス変換 (NAT) デバイスにパススルーする場合は、アプライアンスのプライベート IP アドレスを入力します。

- 2 圧縮された構成ファイルをダウンロードし、sdconf.rec ファイルを解凍します。

Directories Management で RSA SecurID を構成するときにこのファイルを後でアップロードできるようにしておきます。

次のステップ

管理コンソールに移動し、[ID とアクセス管理] タブの [セットアップ] ページで、コネクタを選択し、[認証アダプタ] ページで、SecurID を構成します。

RSA SecurID 認証の構成

ディレクトリ管理を RSA SecurID サーバの認証エージェントとして構成したら、コネクタに RSA SecurID 構成情報を追加する必要があります。

前提条件

- RSA Authentication Manager (RSA SecurID サーバ) がインストールされ、正しく構成されていることを確認します。
- 圧縮ファイルを RSA SecurID サーバからダウンロードし、サーバ構成ファイルを展開します。

手順

- 1 テナント管理者として、[管理] - [ディレクトリ管理] - [コネクタ] の順に移動します。
- 2 [コネクタ] ページで、RSA SecurID で構成されているコネクタのワーカー リンクを選択します。
- 3 [認証アダプタ] をクリックしてから、[SecurIDdpAdapter] をクリックします。
ID マネージャーのサインイン ページにリダイレクトされます。
- 4 [認証アダプタ] ページの [SecurIDdpAdapter] 行で、[編集] をクリックします。
- 5 [SecurID 認証アダプタ] ページで構成します。

RSA SecurID サーバで使用される情報と生成されるファイルは、[SecurID] ページを構成する際に必要です。

オプション	アクション
名前	名前は必須です。デフォルトの名前は、SecurIDdpAdapter です。このタイプは変更できません。
SecurID を有効化	このボックスをオンにして SecurID 認証を有効化します。
許可される認証の試行回数	RSA SecurID トークンを使用する場合のログイン失敗が許可される最大回数を入力します。デフォルトは、5 回です。
コネクタのアドレス	コネクタ インスタンスの IP アドレスを入力します。入力する値は、認証エージェントとしてコネクタ アプライアンスを RSA SecurID サーバに追加するときに使用した値と一致する必要があります。代替 IP アドレス プロンプトに割り当てられた値が RSA SecurID サーバにある場合は、その値をコネクタの IP アドレスとして入力します。別の IP アドレスが割り当てられていない場合は、認証エージェントとして Workspace アプライアンスを RSA SecurID サーバに追加するときに使用した値を IP アドレスのプロンプトに入力します。
エージェント IP アドレス	RSA SecurID サーバの [IP アドレス] プロンプトに割り当てられている値を入力します。
サーバ構成	RSA SecurID サーバ構成ファイルをアップロードします。最初に、RSA SecurID サーバから圧縮ファイルをダウンロードしてサーバ構成ファイル（デフォルトの名前は <code>sdconf.rec</code> ）を解凍する必要があります。
ノード シークレット	[ノード シークレット] フィールドを空白のままにしておくと、ノード シークレットを自動生成できます。RSA SecurID サーバのノード シークレット ファイルをクリアすることをお勧めします。このファイルを意図的にアップロードしないでください。RSA SecurID サーバとサーバ コネクタ インスタンスのノード シークレット ファイルが常に一致するようにしてください。どちらかでノード シークレットを変更する場合は、もう一方でも同じように変更します。

- 6 [保存] をクリックします。

次のステップ

デフォルトのアクセス ポリシーに認証方法を追加します。[管理] - [ディレクトリ管理] - [ポリシー] の順に移動し、[デフォルト ポリシーの編集] をクリックしてデフォルト ポリシー ルールを編集し、適切な認証順序で SecurID 認証方法をルールに追加します。

Directories Management の RADIUS の構成

RADIUS（リモート認証ダイヤルイン ユーザー サービス）認証の使用をユーザーに要求するように Directories Management を構成できます。RADIUS サーバ情報は Directories Management サービス上で構成します。

RADIUS のサポートにより、トークンベースの二要素認証を使用する代替オプションが幅広く提供されます。RADIUS などの二要素認証ソリューションは、別のサーバでインストールされている認証マネージャと連携動作するため、ID マネージャ サービスにアクセスできる構成済みの RADIUS サーバが必要となります。

ユーザーがマイ アプリ ポータルにサインインするときに RADIUS 認証が有効になっていると、特別なログイン ダイアログ ボックスがブラウザに表示されます。ユーザーは RADIUS 認証のユーザー名とパスワードをログイン ダイアログ ボックスに入力します。RADIUS サーバがアクセス チャレンジを発行する場合は、ID マネージャ サービスによって、2 つ目のパスワードの入力を求めるダイアログ ボックスが表示されます。現時点で、RADIUS チャレンジのサポートは、テキスト入力の要求に限定されています。

ユーザーがダイアログ ボックスに認証情報を入力したら、ユーザーの携帯電話に対し、コードとともに、RADIUS サーバから SMS テキスト メッセージやメールを送信したり、他の何らかのアウトオブバンド メカニズムを使用してテキストを送信したりできます。ユーザーはこのテキストとコードをログイン ダイアログ ボックスに入力して、認証を完了できます。

Active Directory からユーザーをインポートできる RADIUS サーバの場合、エンド ユーザーは、RADIUS 認証のユーザー名とパスワードの入力を求められる前に、まず Active Directory 認証情報の入力を求められることがあります。

RADIUS サーバを準備する

RADIUS サーバをセットアップしてから、Directories Management サービスからの RADIUS 要求を受け入れるように RADIUS サーバを構成します。

RADIUS サーバの設定に関する詳細については、RADIUS ベンダーのセットアップ ガイドを参照してください。RADIUS 構成情報は、サービスで RADIUS を構成する際に使用するので、書き留めておきます。Directories Management を構成するために必要な RADIUS 情報のタイプを表示するには、[ディレクトリ管理の RADIUS 認証の構成](#)を参照してください。

セカンダリ RADIUS 認証サーバをセットアップすると、これを使用して高可用性を実現できます。RADIUS 認証に構成されたサーバ タイムアウトが経過してもプライマリ RADIUS サーバが応答しない場合は、セカンダリ サーバに要求がルーティングされます。プライマリ サーバが応答しなくなると、セカンダリ サーバがその後のすべての認証要求を受け取ります。

ディレクトリ管理の RADIUS 認証の構成

認証マネージャ サーバで RADIUS ソフトウェアを有効にします。RADIUS 認証については、ベンダーの構成ドキュメントに従ってください。

前提条件

認証マネージャ サーバで RADIUS ソフトウェアをインストールして構成します。RADIUS 認証については、ベンダーの構成ドキュメントに従ってください。

サービス上で RADIUS を構成するには、次の RADIUS サーバ情報を把握する必要があります。

- RADIUS サーバの IP アドレスまたは DNS 名。
- 認証ポート番号。認証ポートは、通常 1812 です。
- 認証タイプ。認証タイプには、PAP（パスワード認証プロトコル）、CHAP（チャレンジ ハンドシェイク認証プロトコル）、MSCHAP1 および MSCHAP2（Microsoft チャレンジ ハンドシェイク認証プロトコル、バージョン 1 および 2）があります。
- RADIUS プロトコル メッセージで暗号化および復号化に使用される RADIUS 共有シークレット。
- RADIUS 認証に必要な特定のタイムアウトおよび再試行の値。
- テナント管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [ディレクトリ管理] - [コネクタ] の順に選択します。
- 2 [コネクタ] ページで、RADIUS 認証用に構成されているコネクタのワーカー リンクを選択します。
- 3 [認証アダプタ] をクリックしてから、[RadiusAuthAdapter] をクリックします。
ID マネージャーのログイン ページにリダイレクトされます。
- 4 [認証アダプタ] ページで [編集] をクリックして、次のフィールドを構成します。

オプション	アクション
名前	名前は必須です。デフォルトの名前は、RadiusAuthAdapter です。このタイプは変更できます。
Radius アダプタを有効にする	RADIUS 認証を有効にするには、このボックスをオンにします。
許可される認証の試行回数	RADIUS を使用してログインする場合のログイン失敗が許可される最大回数を入力します。デフォルトは、5 回です。
Radius サーバの試行回数	再試行の合計回数を指定します。プライマリ サーバが反応しない場合、サービスは決められた時間が経つまで待機してからもう一度再試行します。
Radius サーバのホスト名/アドレス	RADIUS サーバのホスト名または IP アドレスを入力します。
認証ポート	Radius 認証のポート番号を入力します。これは通常 1812 になります。
アカウント ポート	ポート番号に 0 を入力します。アカウント ポートは、現時点で使用されていません。
認証タイプ	RADIUS サーバでサポートされている認証プロトコルを入力します。PAP、CHAP、MSCHAP1、MSCHAP2 のいずれかを入力します。
共有シークレット	RADIUS サーバと VMware Identity Manager サービス間で使用される共有シークレットを入力します。
サーバ タイムアウト（秒）	RADIUS サーバのタイムアウトを秒単位で入力します。この時間が経過しても RADIUS サーバが応答しない場合には、再試行が送信されます。

オプション	アクション
レルムのプリフィックス	(オプション) ユーザー アカウントの場所はレルムと呼ばれます。 レルムのプリフィックス文字列を指定すると、ユーザー名が RADIUS サーバに送信されるときに、その文字列が名前の先頭に置かれます。たとえば、jdoe というユーザー名が入力され、レルムのプリフィックスとして DOMAIN-A\ が指定された場合は、DOMAIN-A\jdoe というユーザー名が RADIUS サーバに送信されます。これらのフィールドを構成しない場合は、入力したユーザー名だけが送信されます。
レルムのサフィックス	(オプション) レルムのサフィックスを指定すると、その文字列はユーザー名の末尾に置かれます。たとえば、サフィックスが @myco.com の場合は、jdoe@myco.com というユーザー名が RADIUS サーバに送信されます。
ログイン ページのパスフレーズのヒント	正しい RADIUS パスコードの入力をユーザーに促すために、ユーザー ログイン ページに表示するテキスト文字列を入力します。たとえば、[Active Directory パスワード、それから SMS パスコード] でこのフィールドを構成すると、ログイン ページのメッセージでは [Active Directory パスワード、それから SMS パスコードを入力してください] のように表示されます。デフォルトのテキスト文字列は、[RADIUS Passcode] です。

5 セカンダリ RADIUS サーバを有効にして、高可用性を実現できます。

セカンダリ サーバは、手順 4 の説明に従って構成します。

6 [保存] をクリックします。

次のステップ

デフォルトのアクセス ポリシーに RADIUS 認証方法を追加します。[管理] - [ディレクトリ管理] - [ポリシー] の順に選択し、[デフォルト ポリシーの編集] をクリックしてデフォルト ポリシー ルールを編集し、適切な認証順序で RADIUS 認証方法をルールに追加します。

ディレクトリ管理で証明書またはスマート カード アダプタを使用するための構成

X.509 証明書認証を構成すると、クライアントはデスクトップやモバイル デバイス上の証明書や、スマート カード アダプタを使用して認証できます。証明書による認証は、ユーザーの認証方法（プライベート キーまたはスマート カード）と、ユーザーが入力する情報（プライベート キーのパスワードまたはスマート カードの PIN）に基づいて行われます。X.509 証明書は、公開鍵基盤 (PKI) の規格を使用して、証明書に含まれるパブリック キーがユーザーに属するものであることを確認します。スマート カード認証では、ユーザーはコンピュータにスマート カードを接続して、PIN を入力します。

スマート カードの証明書は、ユーザーのコンピュータのローカル証明書ストアにコピーされます。ローカル証明書ストア内の証明書は、このユーザーのコンピュータで実行されているすべてのブラウザで使用できますが、いくつかの例外があります。

注： 証明書認証を構成し、ロード バランサの背後でサービス アプライアンスがセットアップされている場合、コネクタにロード バランサでの SSL パススルーが構成されていて、ロード バランサで SSL を終了するように構成されていないことを確認します。この構成では、コネクタとクライアント間で SSL ハンドシェイクを確実に実行し、コネクタに証明書を渡すことができます。SSL パススルーが設定された別のロード バランサの背後に追加のコネクタを構成し、これらのコネクタで証明書ベースの認証を有効にして、構成することができます。

証明書による認証でのユーザー プリンシパル名の使用

Active Directory では認証マッピングを使用できます。証明書およびスマート カードによるログインでは、Active Directory のユーザー プリンシパル名 (UPN) を使用して、ユーザー アカウントが検証されます。Directories Management サービスでの認証を試行するユーザーの Active Directory アカウントには、証明書の UPN と一致する有効な UPN が関連付けられている必要があります。

証明書に UPN が存在しない場合、メール アドレスを使用してユーザー アカウントを検証するように、Directories Management を構成できます。

また、別の UPN タイプを有効にして使用することもできます。

認証に必要な証明機関

証明書認証によるログインを有効化するには、ルート証明書と中間証明書を Directories Management にアップロードする必要があります。

証明書は、ユーザーのコンピュータのローカル証明書ストアにコピーされます。ローカル証明書ストアの証明書は、いくつかの例外がありますが、ユーザーのコンピュータで実行されているすべてのブラウザで利用できるため、ブラウザの Directories Management インスタンスでも利用できます。

スマート カード認証の場合、ユーザーが Directories Management インスタンスへの接続を開始すると、Directories Management サービスが信頼された証明機関 (CA) のリストをブラウザに送信します。ブラウザは、信頼された CA のリストを利用可能なユーザー証明書に対してチェックし、適切な証明書を選択してから、スマートカードの PIN の入力をユーザーに要求します。有効なユーザー証明書が複数ある場合には、ブラウザで証明書を選択するようにユーザーは求められます。

ユーザーが認証できない場合、ルート CA と中間 CA が正常にセットアップされていないか、ルートおよび中間 CA がサーバにアップロードされた後にサービスが再起動されていない可能性があります。これらの場合には、ブラウザはインストールされている証明書を表示できず、ユーザーは正しい証明書を選択できないため、証明書による認証が失敗します。

証明書失効チェックの使用

証明書失効チェックを構成すると、ユーザー証明書が失効したユーザーは認証されなくなります。ユーザーが組織を退職した場合、スマート カードを紛失した場合、または別の部門に異動した場合に、証明書が失効されることは多くあります。

証明書失効リスト (CRL) とオンライン証明書ステータス プロトコル (OCSP) 証明書の失効チェックがサポートされます。CRL は、証明書を発行した CA が公開する失効された証明書のリストです。OCSP は、証明書の失効ステータスを取得するために使用される証明書検証プロトコルです。

証明書失効チェックは、証明書認証を構成するときに、管理コンソールの [コネクタ] > [認証アダプタ] > [CertificateAuthAdapter] ページで構成できます。

同じ証明書認証アダプタの構成で CRL と OCSP の両方を構成できます。両方のタイプの証明書失効チェックを構成し、[OCSP の障害時に CRL を使用する] チェックボックスを有効にしている場合、OCSP が最初にチェックされ、OCSP で障害が発生した場合には、CRL に戻って失効チェックが実行されます。CRL で障害が発生した場合、OCSP に戻って失効チェックが実行されることはありません。

ログインでの CRL チェック

証明書の失効を有効にすると、Directories Management サーバは CRL を読み取って、ユーザーの証明書の失効ステータスを判断します。

証明書が失効していると、証明書による認証は失敗します。

ログインでの OCSP 証明書チェック

証明書ステータス プロトコル (OCSP) による失効チェックを構成すると、Directories Management は OCSP レスポンダに要求を送信し、特定のユーザー証明書の失効ステータスを判別します。Directories Management サーバは、OCSP 署名証明書を使用して、OCSP レスポンダから受信した応答が正規であるか検証します。

証明書が失効していれば、認証は失敗します。

OSCP レスポンドから応答を受信しない場合や、応答が無効である場合に、CRL に戻ってチェックするように、認証を構成できます。

ディレクトリ管理のための証明書認証の構成

証明書による認証は、vRealize Automation 管理コンソールのディレクトリ管理機能で有効にし、構成します。

注： Kerberos やスマート カード認証などのサードパーティ ID プロバイダを使用している場合、システム管理者は vRealize Automation 展開で外部コネクタを構成する必要があります。

前提条件

- ユーザーから提示された証明書に署名した CA からルート証明書と中間証明書を入手します。
- (オプション) 証明書認証のための有効な証明書ポリシーのオブジェクト識別子 (OID) のリスト。
- 失効チェックのための、CRL のファイルの場所、OCSP サーバーの URL。
- (オプション) OCSP 応答署名証明書ファイルの場所。
- 認証の前に同意書の表示を有効化している場合には、同意書の内容。

手順

- 1 テナント管理者として、[管理] - [ディレクトリ管理] - [コネクタ] の順に移動します。
- 2 [コネクタ] ページで、構成されているコネクタのワーカー リンクを選択します。
- 3 [認証アダプタ] をクリックしてから、[CertificateAuthAdapter] をクリックします。
ID マネージャーのサインイン ページにリダイレクトされます。
- 4 [CertificateAuthAdapter] 行で、[編集] をクリックします。
- 5 証明書認証アダプタのページで構成します。

注： アスタリスクは、必須フィールドを示します。その他のすべてのフィールドはオプションです。

オプション	説明
*名前	名前は必須です。デフォルトの名前は、CertificateAuthAdapter です。この名前は変更できます。
証明書アダプタを有効にする	証明書認証を有効化するには、このチェック ボックスをオンにします。
*ルートおよび中間 CA 証明書	アップロードする証明書ファイルを選択します。DER または PEM としてエンコードされた複数のルート CA および中間 CA 証明書を選択できます。
アップロードされた CA 証明書	<p>アップロードされた証明書ファイルは、フォームの [アップロードされた CA 証明書] セクションに表示されます。</p> <p>サービスを再起動しないと、新しい証明書は利用可能になりません。</p> <p>[Web サービスを再起動する] をクリックしてサービスを再起動し、信頼されるサービスに証明書を追加します。</p>
<p>注： サービスを再起動しても、証明書認証は有効にはなりません。サービスが再起動したら、このページの構成を続けます。ページの最後に [保存] をクリックすると、サービスで証明書認証が有効になります。</p>	

オプション	説明
証明書に UPN が含まれていない場合はメールを使用する	ユーザー プリンシパル名 (UPN) が証明書に存在しない場合に、サブジェクトの別名の拡張として emailAddress 属性を使用してユーザー アカウントを検証するには、このチェック ボックスをオンにします。
承認された証明書ポリシー	証明書ポリシー拡張で承認されたオブジェクト識別子のリストを作成します。 証明書発行ポリシーのオブジェクト ID 番号 (OID) を入力します。[別の値を追加] をクリックして、OID を追加します。
証明書の失効を有効にする	証明書の失効チェックを有効にするには、このチェック ボックスをオンにします。これにより、ユーザー 証明書が失効したユーザーは認証されなくなります。
証明書から CRL を使用する	証明書を発行した CA が公開する証明書失効リスト (CRL) を使用して証明書のステータス (失効しているかどうか) を確認するには、このチェック ボックスをオンにします。
CRL の場所	CRL を取得するサーバのファイル パスまたはローカル ファイル パスを入力します。
OCSP の失効を有効にする	証明書検証プロトコルとしてオンライン証明書ステータス プロトコル (OCSP) を使用して、証明書の失効ステータスを取得するには、このチェック ボックスをオンにします。
OCSP の障害時に CRL を使用する	CRL と OCSP の両方を構成し、OCSP チェックが利用できない場合に CRL の使用に戻るには、このチェック ボックスをオンにします。
OCSP Nonce を送信する	OCSP 要求の一意の ID を応答で送信する場合には、このチェック ボックスをオンにします。
OCSP の URL	OCSP による失効を有効にした場合は、失効チェック用の OCSP サーバ アドレスを入力します。
OCSP レスポンドの署名証明書	レスポンドの OCSP 証明書のパスを入力します。たとえば、/path/to/file.cer のようになります。
認証前に同意書を有効にする	ユーザーが証明書認証を使用してマイ アプリ ポータルにログインする前に同意書ページを表示するには、このチェック ボックスをオンにします。
同意書の内容	同意書に表示するテキストをこのテキスト ボックスに入力します。

6 [保存] をクリックします。

次のステップ

- デフォルトのアクセス ポリシーに証明書認証方法を追加します。[管理] - [ディレクトリ管理] - [ポリシー] の順に移動して、[デフォルト ポリシーの編集] をクリックし、デフォルト ポリシーを編集して証明書を追加して、デフォルト ポリシーの初期認証方法になるようにします。証明書は、ポリシー ルールに表示される認証方法の一番上に配置する必要があります。そうしないと、証明書による認証は失敗します。
- 証明書認証を構成し、ロード バランサの背後でサービス アプライアンスがセットアップされている場合、ロード バランサで Directories Management コネクタ が SSL パススルーで構成されており、ロード バランサで SSL を終了するように構成されていないことを確認します。この構成では、コネクタとクライアント間で SSL ハンドシェイクを確実に実行し、コネクタに証明書を渡すことができます。

ユーザー認証のためのサードパーティ ID プロバイダ インスタンスの構成

Directories Management サービスでユーザー認証に使用するサードパーティ ID プロバイダを構成できます。

管理コンソールを使用してサードパーティ ID プロバイダ インスタンスを追加する前に、次の作業を完了します。

- サードパーティ インスタンスが SAML 2.0 互換であり、サービスがサードパーティ インスタンスに到達できることを確認します。

- 管理コンソールで ID プロバイダを構成するときに、追加する適切なサードパーティ メタデータ情報を取得します。サードパーティのインスタンスから取得するメタデータ情報は、メタデータへの URL または実際のメタデータのいずれかです。

サードパーティ ID プロバイダの接続の構成

vRealize Automation にはデフォルトの ID プロバイダ接続インスタンスが付属しています。ユーザーは、ジャストインタイム ユーザー プロビジョニングまたは他のカスタム構成をサポートするために追加の ID プロバイダ接続を作成することがあります。

vRealize Automation にはデフォルトの ID プロバイダが付属しています。多くの場合、デフォルトのプロバイダでお客様のニーズを十分に満たすことができます。企業の既存の ID 管理ソリューションを使用している場合、カスタムの ID プロバイダを設定し、ユーザーを既存の ID ソリューションにリダイレクトすることができます。

カスタムの ID プロバイダを使用すると、ディレクトリ管理は、プロバイダとの信頼関係を確立するためにそのプロバイダからの SAML メタデータを使用します。この関係が確立されると、ディレクトリ管理は、サブジェクト名の ID に基づいて内部の vRealize Automation ユーザーのリストに SAML アサーションからユーザーをマッピングします。

前提条件

- この ID プロバイダ インスタンスで認証を行うネットワーク範囲を設定します。[ネットワーク範囲の追加または編集](#)を参照してください。
- サードパーティのメタデータ ドキュメントにアクセスします。これは、メタデータへの URL または実際のメタデータのいずれかです。
- テナント管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [ディレクトリ管理] - [ID プロバイダ] の順に選択します。

このページには、構成済み ID プロバイダがすべて表示されます。

- 2 [ID プロバイダを追加] をクリックします。

ID プロバイダのオプション メニューが表示されます。

- 3 [サードパーティ IDP を作成] を選択します。

- 4 適切な情報を入力して、ID プロバイダを構成します。

オプション	説明
ID プロバイダ名	この ID プロバイダ インスタンスの名前を入力します。
SAML メタデータ	<p>サードパーティの XML ベースの IdP メタデータ ドキュメントを追加して、ID プロバイダとの信頼を確立します。</p> <ol style="list-style-type: none"> 1 SAML メタデータ URL または xml コンテンツをテキスト ボックスに入力します。 2 [プロセス IdP メタデータ] をクリックします。IdP でサポートされている NameID の形式は、メタデータから抽出され、名前 ID 形式テーブルに追加されます。 3 名前 ID 値の列で、表示される ID 形式にマッピングするサービスのユーザー属性を選択します。独自のサードパーティ名の ID 形式を追加して、サービスのユーザー属性値にマッピングできます。 4 (オプション) NameIDPolicy 応答識別子の文字列形式を選択します。

オプション	説明
ユーザー	この ID プロバイダを使用して認証できるユーザーの Directories Management ディレクトリを選択します。
ジャストインタイムのユーザー プロビジョニング	適切なサード パーティ ID プロバイダを使用してジャストインタイムのプロビジョニングをサポートするには適切なオプションを選択します。 ジャストインタイムのプロビジョニングに使用する [ディレクトリ名] を入力します。 ジャストインタイムのプロビジョニングに使用する外部の ID プロバイダ内にある 1 つまたは複数の [ドメイン] を入力します。
ネットワーク	サービス内で構成されている既存のネットワーク範囲が表示されます。 この ID プロバイダ インスタンスで認証を行うユーザーのネットワーク範囲を、IP アドレスで指定します。
認証方法	サードパーティ ID プロバイダがサポートする認証方法を追加します。認証方法をサポートする SAML 認証コンテキスト クラスを選択します。
SAML 署名証明書	[サービス プロバイダ (SP) メタデータ] をクリックして、Directories Management の SAML サービス プロバイダのメタデータ URL を確認します。URL をコピーして保存します。この URL は、サードパーティ ID プロバイダで SAML アサーションを編集して Directories Management ユーザーをマッピングするときに構成されます。
ホスト名	[ホスト名] のフィールドが表示される場合は、認証用に ID プロバイダにリダイレクトするホスト名を入力します。443 以外の非標準ポートを使用している場合、「ホスト名:ポート」の形式で設定します。たとえば、myco.example.com:8443 のように入力します。

5 [追加] をクリックします。

次のステップ

- サードパーティの ID プロバイダ インスタンスを設定するために必要な Directories Management サービス プロバイダのメタデータをコピーして保存します。このメタデータは、ID プロバイダ ページの SAML 署名証明書のセクションで入手できます。
- サービスのデフォルト ポリシーに ID プロバイダの認証方法を追加します。

カタログに追加するリソースの追加とカスタマイズに関する情報については、Directories Management ガイドを参照してください。

ユーザーに適用する認証方法の管理

Directories Management サービスでは、構成する認証方法、デフォルトのアクセス ポリシー、ネットワーク範囲、および ID プロバイダ インスタンスに基づいて、ユーザーを認証します。

ユーザーがログインを試行するときに、サービスはデフォルトのアクセス ポリシーを評価して、適用するポリシー内のルールを選択します。認証方法は、ルールに表示されている順序で適用されます。ルールの認証方法とネットワーク範囲の要件と一致する最初の ID プロバイダ インスタンスが選択され、ユーザー認証要求は、その ID プロバイダ インスタンスに転送され認証が行われます。認証が失敗すると、ルールで構成されている次の認証方法が適用されます。

デバイス タイプ、またはデバイス タイプとネットワーク範囲に基づいて認証方法が使用されるように指定するルールを追加できます。たとえば、特定のネットワークから iOS デバイスを使用してログインするユーザーに RSA SecurID を使用して認証するよう求めるルールを構成できます。または、社内ネットワークの IP アドレスからログインするすべてのデバイス タイプにパスワードを使用して認証するよう指定するルールを構成できます。

ネットワーク範囲の追加または編集

ネットワーク範囲を管理し、Active Directory リンクを経由してユーザーがログインできる IP アドレスを定義できます。作成したネットワーク範囲は、特定の ID プロバイダ インスタンスやアクセス ポリシー ルールに追加します。

使用するネットワーク トポロジを基準として、Directories Management 環境のネットワーク範囲を定義します。

ALL RANGES と呼ばれるネットワーク範囲は、デフォルトとして作成されます。このネットワーク範囲には、インターネットで利用可能なすべての IP アドレス、つまり 0.0.0.0 から 255.255.255.255 が含まれます。展開環境の ID プロバイダ インスタンスが 1 つの場合でも、デフォルトのネットワーク範囲に対して IP アドレス範囲を変更したり、他の範囲を加えたりして、特定の IP アドレスの除外や追加を行えます。特定の目的に合わせて適用できる特定の IP アドレスでネットワーク範囲を作成できます。

注： デフォルトのネットワーク範囲 ALL RANGES とその説明「全範囲用のネットワーク」は、編集可能です。
[ネットワーク範囲] ページでネットワーク範囲名をクリックすると、名前と説明を編集できます。また、ほかの言語にテキストを変更することも可能です。

前提条件

- Active Directory の基本的なユーザー ID とパスワード認証をサポートする、適切な Active Directory リンクが設定された vRealize Automation 環境でテナントを構成します。
- 使用するネットワークに Active Directory をインストールおよび構成します。
- テナント管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [ディレクトリ管理] - [ネットワーク範囲] の順に選択します。
- 2 既存のネットワーク範囲を編集するか、新しいネットワーク範囲を追加します。

オプション	説明
既存の範囲の編集	編集するネットワーク範囲の名前をクリックします。
範囲の追加	新しい範囲を追加するには、[ネットワーク範囲を追加] をクリックします。

- 3 フォームを完成させます。

フォーム アイテム	説明
名前	ネットワーク範囲の名前を入力します。
説明	ネットワーク範囲の説明を入力します。
View ボッド	View ボッド オプションは、View モジュールが有効の場合のみ表示されます。 クライアント アクセス用 URL ホスト。ネットワーク範囲に対して、正しい Horizon Client アクセス用の URL を入力します。 クライアント アクセス用ポート。ネットワーク範囲に対して、正しい Horizon Client アクセス用のポートを入力します。
IP アドレス範囲	IP アドレス範囲を編集または追加し、必要なすべての IP アドレスを含め、不必要な IP アドレスを排除します。

次のステップ

- 各ネットワーク範囲を ID プロバイダ インスタンスに関連付けます。
- ネットワーク範囲をアクセス ポリシー ルールに適宜関連付けます。[アクセス ポリシー設定の構成](#)を参照してください。

ディレクトリと同期する属性の選択

Active Directory と同期するように Directories Management ディレクトリをセットアップするときに、ディレクトリと同期するユーザー属性を指定します。ディレクトリをセットアップする前に、[ユーザー属性] ページで、必要となるデフォルト属性を指定し、Active Directory 属性にマッピングするその他の属性を適宜追加できます。

ディレクトリが作成される前に [ユーザー属性] ページを構成するときに、必須にするデフォルト属性を変更したり、属性を必須としてマークしたり、カスタム属性を追加したりできます。

デフォルトでマッピングされている属性のリストについては、[Active Directory で同期されるユーザー属性の管理](#)を参照してください。

ディレクトリが作成された後で、必須の属性を変更したり、カスタム属性を削除したりできます。ある属性を必須属性に変更することはできません。

ディレクトリと同期する別の属性を追加するときには、ディレクトリが作成された後に、ディレクトリの [マップされた属性] ページに移動して、これらの属性を Active Directory の属性にマッピングします。

手順

- 1 vRealize Automation にシステムまたはテナント管理者としてログインします。
- 2 [管理] タブをクリックします。
- 3 [ディレクトリ管理] - [ユーザー属性] を選択します。
- 4 [デフォルト属性] セクションで、必須属性のリストを確認して、必須にする必要がある属性が反映されるように必要な変更を加えます。
- 5 [属性] セクションで、Directories Management ディレクトリの属性名をリストに追加します。
- 6 [保存] をクリックします。
デフォルト属性のステータスがアップデートされ、追加した属性が、ディレクトリの [マップされた属性] リストに追加されます。
- 7 ディレクトリが作成された後に、[ID ストア] ページに移動して、ディレクトリを選択します。
- 8 [同期設定] - [マップされた属性] をクリックします。
- 9 追加した属性のドロップダウン メニューで、マップ先の Active Directory 属性を選択します。
- 10 [保存] をクリックします。

結果

ディレクトリは、Active Directory と次回同期されるときにアップデートされます。

デフォルトのアクセス ポリシーの適用

Directories Management サービスには、アプリ ポータルへのユーザー アクセスを制御するデフォルトのアクセス ポリシーが含まれています。必要に応じてポリシーを編集してポリシーを変更できます。

パスワード認証以外の認証方法を有効にする場合、デフォルトのポリシーを編集して、ポリシー ルールに有効化した認証方法を追加する必要があります。

デフォルトのアクセス ポリシー内の各ルールでは、アプリケーション ポータルへのユーザー アクセスを許可するための一連の基準が満たされている必要があります。ネットワーク範囲を適用して、コンテンツにアクセスできるユーザーのタイプを選択し、使用する認証方法を選択します。[アクセス ポリシーの管理](#)を参照してください。

サービスがログインを試行する回数は、認証方法によって異なります。Kerberos や証明書による認証では、サービスは 1 度だけ認証を試行します。ユーザーのログイン試行が失敗すると、ルールの次の認証方法が試みられます。Active Directory パスワードおよび RSA SecurID 認証によるログインの最大失敗試行回数はデフォルトで 5 回に設定されています。ユーザーがログインに 5 回失敗すると、サービスはリストの次の認証方法を使用してログインを試みます。すべての認証方法で失敗すると、サービスはエラーメッセージを表示します。

認証方法をポリシー ルールに適用する

パスワード認証の方法だけが、デフォルトのポリシー ルールに構成されています。構成済みのその他の認証方法に変更したり、認証に使用する認証方法の順序を設定するには、ポリシー ルールを編集する必要があります。

前提条件

組織がサポートしている認証方法を有効にして構成します。[代替ユーザー認証製品とディレクトリ管理との統合](#)を参照してください。

手順

- 1 [管理] - [ディレクトリ管理] - [ポリシー] の順に選択します。
- 2 編集するデフォルトのアクセス ポリシーをクリックします。
- 3 ポリシー ルールを編集するには、[ポリシー ルール] の [認証方法] 列で、編集する認証方法をクリックします。
新しいポリシー ルールを追加するには、[+] アイコンをクリックします。
- 4 [保存] をクリックし、ポリシー ページで再び [保存] をクリックします。

ポリシー ルールの編集

ユーザーのネットワーク範囲が次の場合...

すべての範囲

およびユーザーのコンテンツアクセス元が次の場合...

Web ブラウザ

次に、以下の方法を使用して認証する必要があります...

Password

および

前の認証方式に失敗した場合は:

認証方法の選択-

専用

+

フォールバック方法

再認証までの待機時間: 時間

- 5 [保存] をクリックし、ポリシー ページで再び [保存] をクリックします。

Directories Management 用 Kerberos の構成

Kerberos 認証によって、Active Directory ドメインに正常にサインインしたユーザーは、追加の認証情報を指定せずにアプリ ポータルにアクセスできます。Windows 認証を有効にすると、Kerberos プロトコルによってユーザーのブラウザと Directories Management サービス間の通信が安全になります。Kerberos がユーザーの展開環境で機能するようにするために、Active Directory を直接構成する必要はありません。

現在、ユーザーのブラウザとサービスの間のやり取りは、Windows オペレーティング システムでのみ、Kerberos によって認証されます。それ以外のオペレーティング システムからのサービスへのアクセスでは、Kerberos 認証を利用できません。

■ Kerberos 認証の構成

Directories Management サービスを構成して Kerberos 認証を使用するには、ドメインに参加して Directories Management コネクタで Kerberos 認証を有効にする必要があります。

■ Web インターフェイスにアクセスするための Internet Explorer の構成

ユーザーの展開環境に Kerberos が構成されていたり、Internet Explorer ブラウザを使用してユーザーが Web インターフェイスにアクセスできるようにしたりするには、Internet Explorer ブラウザを構成する必要があります。

■ Web インターフェイスにアクセスするための Firefox の構成

展開環境に Kerberos が構成されている場合に、Firefox ブラウザを使用してユーザーが Web インターフェイスにアクセスできるようにするには、Firefox ブラウザを構成する必要があります。

■ Web インターフェイスにアクセスするための Chrome ブラウザの構成

ユーザーの展開環境に Kerberos が構成されていたり、Chrome ブラウザを使用してユーザーが Web インターフェイスにアクセスできるようにしたりするには、Chrome ブラウザを構成する必要があります。

Kerberos 認証の構成

Directories Management サービスを構成して Kerberos 認証を使用するには、ドメインに参加して Directories Management コネクタで Kerberos 認証を有効にする必要があります。

前提条件

- vCenter Server に NSX Edge を展開して、NSX ロード バランサを構成します。ロード バランサのセットアップの詳細については、『vRealize Automation のロード バランシング』を参照してください。
- ドメインをマスター テナントに参加させます。別のテナントにディレクトリを接続する前に、この操作を行う必要があります。
 - a デフォルトのテナントに、administrator@vsphere.local としてログインします。
 - b ローカル ユーザー TestUser を作成し、テナント管理者に TestUser と入力します。
 - c [管理] - [ディレクトリ管理] - [コネクタ] の順に選択します。
 - d 各アプライアンス コネクタで、[ドメインへの参加] を選択します。
 - e [ドメインへの参加] で、[カスタム ドメイン] を選択し、テナントを接続するドメインと認証情報、および接続先 OU を入力します。

- デフォルトのテナントとデフォルト以外のテナントのディレクトリの接続を設定します。Kerberos 認証は、統合 Windows 認証と LDAP 経由の Active Directory で使用できます。[Active Directory over LDAP/IWA リンクの構成](#) および [OpenLDAP ディレクトリ接続の設定](#) を参照してください。
- vRealize Automation ノードのホスト名が、参加している Active Directory ドメインと一致していることを確認します。たとえば、vRealize Automation が COMPANY.COM という Active Directory レalmに参加している場合、ホスト名は node.company.com である必要があります。
- ワークスペースの ID プロバイダを設定します。展開内のすべてのノードがワークスペース ID プロバイダに登録されており、ロード バランサ名が定義されていることを確認します。
 - a [管理] - [ディレクトリ管理] - [ID プロバイダ] の順に選択します。
 - b 適切な ID プロバイダのリンクを選択します。
たとえば、WorkspaceIDP__1 を選択します。
 - c ID プロバイダのリンクをクリックして、構成された IdP のホスト名を見つけます。Web ブラウザを設定する場合は、必要に応じてホスト名を記録します。
 - d ワークスペース IdP のすべての適用可能なノードを登録し、ホスト名のロード バランサ FQDN を入力します。
 - e [保存] をクリックします。
- デフォルト テナントのテナント ディレクトリを設定します。『vRealize Automation のインストール』で、「デフォルト テナントへのアクセスの構成」を参照してください。

手順

- 1 テナント管理者として、[管理] - [ディレクトリ管理] - [コネクタ] の順に移動します。
- 2 [コネクタ] ページで、Kerberos 認証を構成しているコネクタについて、[ドメインに参加] をクリックします。
- 3 [ドメインに参加] ページで、Active Directory ドメインの情報を入力します。

オプション	説明
ドメイン	Active Directory の完全修飾ドメイン名を入力します。入力するドメイン名は、コネクタ サーバが存在するのと同じ Windows ドメインである必要があります。
ドメイン ユーザー	システムを Active Directory ドメインに参加させる権限を持つ、Active Directory 内のアカウントのユーザー名を入力します。
ドメイン パスワード	AD ユーザー名と関連付けられているパスワードを入力します。このパスワードが Directories Management によって保存されることはありません。

[保存] をクリックします。

[ドメインに参加] ページを更新すると、現在ドメインに参加していることを示すメッセージが表示されます。

- 4 コネクタの [ワーカー] 列で [認証アダプタ] をクリックします。
- 5 [KerberosIdpAdapter] をクリックします。

ID マネージャーのサインイン ページにリダイレクトされます。

6 [KerberosIpdAdapter] の行で [編集] をクリックして、Kerberos 認証ページを構成します。

オプション	説明
名前	名前は必須です。デフォルトの名前は、KerberosIpdAdapter です。このタイプは変更できます。
ディレクトリ UID 属性	ユーザー名を含むアカウント属性を入力します。
Windows 認 証を有効にする	ユーザーのブラウザと Directories Management との間の認証を拡張する場合に選択します。
NTLM を有効 にする	Active Directory インフラストラクチャが NTLM 認証に依存している場合にのみ、NT LAN Manager (NTLM) プロトコルベースの認証を有効にするときに選択します。
リダイレクトを 有効にする	ラウンド ロビン DNS やロード バランサが Kerberos でサポートされない場合に選択します。認証要求は、リダイレクト ホスト名にリダイレクトされます。選択した場合、[ホスト名をリダイレクト] テキスト ボックスにリダイレクト ホスト名を入力します。これは、通常はサービスのホスト名になります。

7 [保存] をクリックします。

8 適用可能なすべてのノードで Kerberos 認証を設定します。

a [管理] - [ディレクトリ管理] - [コネクタ] の順に選択します。

このページには、現在設定されているコネクタが表示されます。デフォルトでは、パスワード認証のみが設定されています。

b 最初の vRealize Automation アプライアンス に関連付けられているワーカー ハイパーリンクをクリックします。

c KerberosIpdAdapter リンクをクリックして [認証] ページを開きます。

パスワードを入力して、KerberosIpdAdapter リンクを再起動することが必要な場合もあります。

d ディレクトリ UID 属性を指定し、デフォルト値の sAMAccountName を入力します。

e [Windows 認証を有効にする] および、[リダイレクトを有効にする] チェック ボックスを選択します。

f [NTLM] は、古いドメイン コントローラにのみ必要であるため、選択を解除しておきます。

g リダイレクト ホスト名の VA1 アプライアンスの名前を入力します。

h [保存] をクリックします。

9 デフォルトのアクセス ポリシーを設定します。Kerberos を設定するには、3 つのアクセス ポリシー (Kerberos、パスワード、ローカル パスワード) が必要です。

a [管理] - [ディレクトリ管理] - [ポリシー] の順に選択します。

b default_access_policy_set を選択します。

c Web ブラウザ行の [認証方法] 見出しにあるハイパーリンク値 [パスワード] をクリックします。

d 緑色の + アイコンをクリックして、Kerberos、パスワード、およびパスワード (ローカル ディレクトリ) という新しい認証方法を作成します。

e 各認証方法で、ユーザーのネットワーク範囲として [全範囲] を選択し、ユーザーのコンテンツ アクセス方法として [Web ブラウザ] を選択します。

f 第 1 認証方法を Kerberos に変更し、フェイルバック方法を [パスワード] に設定します。

g [保存]、[OK] の順にクリックします。

Web インターフェイスにアクセスするための Internet Explorer の構成

ユーザーの展開環境に Kerberos が構成されていたり、Internet Explorer ブラウザを使用してユーザーが Web インターフェイスにアクセスできるようにしたりするには、Internet Explorer ブラウザを構成する必要があります。

Kerberos 認証は、Windows オペレーティング システム上の Directories Management と連携して動作します。

注： ここに記載する Kerberos 関連の手順を、他のオペレーティング システムに適用しないでください。

前提条件

Kerberos を構成した後に、Internet Explorer ブラウザをユーザーごとに構成するか、ユーザーに手順を指示します。

手順

- 1 Windows にドメイン内のユーザーとしてログインしていることを確認します。
- 2 Internet Explorer で、自動ログインを有効にします。
 - a [ツール] - [インターネット オプション] - [セキュリティ] を選択します。
 - b [レベルのカスタマイズ] を選択します。
 - c [イントラネットゾーンでのみ自動的にログオンする] を選択します。
 - d [OK] をクリックします。
- 3 コネクタ仮想アプライアンスのこのインスタンスがローカル イントラネット ゾーンの一部であることを確認します。
 - a Internet Explorer を使用して、Directories Management サインインのための URL `https://myconnectorhost.domain/authenticate/` にアクセスします。
 - b ブラウザ ウィンドウのステータス バーの右下に表示されているゾーンを確認します。
ゾーンがローカル イントラネットであれば、Internet Explorer の構成は完了です。
- 4 ゾーンがローカル イントラネットでない場合は、Directories Management サインインのための URL をイントラネット ゾーンに追加します。
 - a [ツール] - [インターネット オプション] - [セキュリティ] - [ローカル イントラネット] - [サイト] を選択します。
 - b [イントラネットのネットワークを自動的に検出する] を選択します。
このオプションが選択されていなかった場合は、選択するだけで、 をイントラネット ゾーンに追加できる場合があります。
 - c (オプション) [イントラネットのネットワークを自動的に検出する] を選択した場合は、[OK] をクリックして、すべてのダイアログ ボックスを閉じます。

- d [ローカル イン트라ネット] ダイアログ ボックスで、[詳細設定] をクリックします。
2 つ目の [ローカル イン트라ネット] という名前のダイアログ ボックスが表示されます。
 - e Directories Management の URL を [次の Web サイトをゾーンに追加する] テキスト ボックスに入力します。

https://myconnectorhost.domain/authenticate/
 - f [追加 > 閉じる > OK] をクリックします。
- 5** Internet Explorer が信頼済みサイトとして Windows 認証をパスするよう許可されていることを確認します。
- a [インターネット オプション] ダイアログ ボックスで、[詳細設定] タブをクリックします。
 - b [統合 Windows 認証を使用する] を選択します。

このオプションは、Internet Explorer の再起動後に初めて有効になります。
 - c [OK] をクリックします。
- 6** Web インターフェイスにログインして、アクセスをチェックします。

Kerberos 認証が成功すると、テストの URL が Web インターフェイスに接続されます。

結果

Kerberos プロトコルによって、この Internet Explorer ブラウザ インスタンスと Directories Management の間のすべてのやり取りのセキュリティが保証されます。これで、ユーザーはシングル サインオンでマイ アプリ ポータルにアクセスできます。

Web インターフェイスにアクセスするための Firefox の構成

展開環境に Kerberos が構成されている場合に、Firefox ブラウザを使用してユーザーが Web インターフェイスにアクセスできるようにするには、Firefox ブラウザを構成する必要があります。

Kerberos 認証は、Windows オペレーティング システム上の Directories Management と連携して動作します。

前提条件

Kerberos を構成した後に、Firefox ブラウザをユーザーごとに構成するか、ユーザーに手順を指示します。

手順

- 1** Firefox ブラウザの [URL] テキスト ボックスに about:config と入力して、詳細設定にアクセスします。
- 2** [細心の注意を払って使用する] をクリックします。
- 3** [設定名] 列の [network.negotiate-auth.trusted-uris] をダブルクリックします。
- 4** Directories Management の URL をテキスト ボックスに入力します。

https://myconnectorhost.domain.com
- 5** [OK] をクリックします。
- 6** [設定名] 列の [network.negotiate-auth.delegation-uris] をダブルクリックします。

- 7 Directories Management の URL をテキスト ボックスに入力します。

`https://myconnectorhost.domain.com/authenticate/`

- 8 [OK] をクリックします。

- 9 Firefox ブラウザを使用して、のログイン URL にログインして、Kerberos の機能をテストします。たとえば、`https://myconnectorhost.domain.com/authenticate/` にログインします。

Kerberos 認証が成功すると、テスト URL が Web インターフェイスに接続されます。

結果

Kerberos プロトコルによって、この Firefox ブラウザ インスタンスと Directories Management の間のすべてのやり取りのセキュリティが保証されます。これで、シングル サインオンでマイ アプリ ポータルにアクセスできます。

Web インターフェイスにアクセスするための Chrome ブラウザの構成

ユーザーの展開環境に Kerberos が構成されていたり、Chrome ブラウザを使用してユーザーが Web インターフェイスにアクセスできるようにしたりするには、Chrome ブラウザを構成する必要があります。

Kerberos 認証は、Windows オペレーティング システム上の Directories Management と連携して動作します。

注： ここに記載する Kerberos 関連の手順を、他のオペレーティング システムに適用しないでください。

前提条件

- Kerberos を構成します。
- Chrome は Internet Explorer の構成を使用して Kerberos 認証を有効にするため、Internet Explorer を構成して、Chrome が Internet Explorer の構成を使用できるようにする必要があります。Chrome の Kerberos 認証の構成方法については、Google のドキュメントを参照してください。

手順

- 1 Chrome ブラウザを使用して、Kerberos の機能をテストします。
- 2 `https://myconnectorhost.domain.com/authenticate/` にある Directories Management にログインします。

Kerberos 認証が成功すると、テストの URL が Web インターフェイスに接続されます。

結果

関連するすべての Kerberos 構成が正しければ、関連プロトコル (Kerberos) によって、この Chrome ブラウザ インスタンスと Directories Management の間のすべてのやり取りのセキュリティが確保されます。ユーザーは、シングル サインオンでマイ アプリ ポータルにアクセスできます。

ディレクトリ管理の外部コネクタのアップグレード

vRealize Automation ディレクトリ管理の構成で外部コネクタを使用している場合、このコネクタを時々アップグレードする必要があります。

vRealize Automation の展開のバージョンをアップグレードするとき、または新しいコネクタのビルドに必要な機能を提供される場合、外部コネクタをアップグレードする必要があります。

このドキュメントは、スタンドアロンの追加外部コネクタを展開したユーザーのみを対象としています。vRealize Automation では、外部コネクタ アプライアンスは、たとえばスマート カード認証により使用できます。

デフォルトでコネクタは、VMware の Web サイトを使用してアップグレード手順を実行します。そのため、コネクタ アプライアンスにはインターネット接続が必要です。また、コネクタ アプライアンスのプロキシ サーバ設定を構成する必要があります (該当する場合)。

コネクタ インスタンスにインターネット接続がセットアップされていない場合は、オフラインでアップグレードを実行できます。オフラインでアップグレードするには、アップグレード パッケージをダウンロードして、アップグレード ファイルをホストするようにローカル Web サーバをセットアップします。

対象者

この情報は、ディレクトリ管理をインストール、アップグレード、および構成するユーザーを対象としています。また、仮想マシン技術に精通した経験のある Windows または Linux システム管理者を想定しています。

外部コネクタのアップグレードの準備

コネクタのアップグレードを準備するには、利用可能なアップグレードを確認し、該当する場合は、アプライアンスのプロキシ サーバ設定を構成する必要があります。

■ 外部コネクタをアップグレードできるかどうかをオンラインでチェックする

コネクタ アプライアンスにインターネット接続がセットアップされている場合は、アプライアンスからオンラインでアップグレードを実行できることを確認します。

■ 外部コネクタ アプライアンスのプロキシ サーバ設定を構成する

コネクタ アプライアンスは、VMware のアップデート サーバにインターネットでアクセスします。HTTP プロキシを使用するインターネット アクセスをネットワーク構成で指定している場合は、アプライアンスのプロキシ設定を調整する必要があります。

外部コネクタをアップグレードできるかどうかをオンラインでチェックする

コネクタ アプライアンスにインターネット接続がセットアップされている場合は、アプライアンスからオンラインでアップグレードを実行できることを確認します。

手順

- 1 コネクタ アプライアンスに root ユーザーとしてログインします。
- 2 次のコマンドを実行します。

```
/usr/local/horizon/update/updatemgr.hznupdateinstaller
```

- 3 次のコマンドを実行して、オンラインのアップグレードを確認します。

```
/usr/local/horizon/update/updatemgr.hzncheck
```

外部コネクタ アプライアンスのプロキシ サーバ設定を構成する

コネクタ アプライアンスは、VMware のアップデート サーバにインターネットでアクセスします。HTTP プロキシを使用するインターネット アクセスをネットワーク構成で指定している場合は、アプライアンスのプロキシ設定を調整する必要があります。

インターネット トラフィックのみを処理するプロキシを有効にします。プロキシが正しく設定されていることを確認するために、ドメイン内の内部トラフィック用のパラメータを no-proxy に設定します。

注： 認証が必要なプロキシ サーバはサポートされません。

前提条件

- コネクタ アプライアンスの root パスワードがあることを確認します。
- プロキシ サーバ情報があることを確認します。

手順

- 1 コネクタ アプライアンスに root ユーザーとしてログインします。
- 2 コマンド ラインに YaST と入力して YaST ユーティリティを実行します。
- 3 左ペインで [ネットワーク サービス] を選択してから、[プロキシ] を選択します。
- 4 [HTTP プロキシ URL] フィールドと [HTTPS プロキシ URL] フィールドにプロキシ サーバの URL を入力します。
- 5 [終了] を選択して YaST ユーティリティを終了します。
- 6 コネクタ仮想アプライアンスで Tomcat サーバを再起動して新しいプロキシ設定を使用します。

```
service horizon-workspace restart
```

結果

コネクタ アプライアンスで VMware のアップデート サーバを利用できるようになりました。

オンラインでの外部コネクタのアップグレード

適切な接続がある場合、ディレクトリ管理の外部コネクタをオンラインでアップグレードできます。

前提条件

- コネクタ アプライアンスが、HTTP を介してポート 80 で vapp-updates.vmware.com を解決してアクセスできることを確認します。
- コネクタのアップグレードが存在することを確認します。適切なコマンドを実行して、アップグレードを確認します。「Directories Management コネクタをオンラインでアップグレードできるかどうかをチェックする」を参照してください。
- アプライアンスのプライマリ ルート パーティションで利用可能なディスク容量が 2 GB 以上あることを確認します。
- コネクタが適切に構成されていることを確認します。

- バックアップのためにコネクタ アプライアンスのスナップショットを取得します。スナップショットの取得方法の詳細については、vSphere のドキュメントを参照してください。
- アウトバウンドの HTTP アクセスのために HTTP プロキシ サーバが必要な場合は、コネクタ アプライアンスのプロキシ サーバ設定を構成します。「Directories Management コネクタ アプライアンスのプロキシ サーバ設定を構成する」を参照してください。

手順

- 1 コネクタ アプライアンスに root ユーザーとしてログインします。
- 2 次のコマンドを実行します。

```
/usr/local/horizon/update/updatemgr.hznupdateinstaller
```

- 3 次のコマンドを実行して、オンラインのアップグレードが存在することを確認します。

```
/usr/local/horizon/update/updatemgr.hzncheck
```

- 4 次のコマンドを実行して、アプライアンスを更新します。

```
/usr/local/horizon/update/updatemgr.hznupdate
```

アップグレード中に発生したメッセージは、update.log ファイル (/opt/vmware/var/log/update.log) に保存されます。

- 5 もう一度 updatemgr.hzn check コマンドを実行して、より新しいアップデートがないことを確認します。

```
/usr/local/horizon/update/updatemgr.hzncheck
```

- 6 アップグレードしたアプライアンスのバージョンを確認します。

```
vamicli version --appliance
```

新しいバージョンが表示されます。

- 7 コネクタ アプライアンスを再起動します。

```
reboot
```

オフラインでの外部コネクタのアップグレード

既存の vRealize Automation ディレクトリ管理コネクタ アプライアンスのアップグレード時にインターネットに接続できない場合は、オフライン アップグレードを実行できます。ローカル Web サーバにアップグレード リポジトリをセットアップして、コネクタ アプライアンスがローカル Web サーバを使用してアップグレードするように構成する必要があります。

前提条件

- コネクタのアップグレードが存在することを確認します。My VMware Downloads サイト (my.vmware.com) でアップグレードを確認します。

- アプライアンスのプライマリ ルート パーティションで利用可能なディスク容量が 2 GB 以上あることを確認します。
- コネクタが適切に構成されていることを確認します。
- バックアップのためにコネクタ アプライアンスのスナップショットを取得します。スナップショットの取得方法の詳細については、vSphere のドキュメントを参照してください。
- ローカル Web サーバでアップグレード ファイルをホストするようにコネクタ アプライアンスを構成します。「オフライン アップグレード向けにローカル Web サーバを準備する」を参照してください。

手順

1 オフライン アップグレード向けにローカル Web サーバを準備する

オフラインでのコネクタのアップグレードを開始する前に、コネクタ アプライアンスのサブディレクトリを含むディレクトリ構造を作成して、ローカルの Web サーバを準備します。

2 コネクタを構成してオフライン アップグレードを実行する

オフライン アップグレードを実行するには、ローカルの Web サーバを参照するようにコネクタ アプライアンスを構成します。その後にアプライアンスをアップグレードします。

オフライン アップグレード向けにローカル Web サーバを準備する

オフラインでのコネクタのアップグレードを開始する前に、コネクタ アプライアンスのサブディレクトリを含むディレクトリ構造を作成して、ローカルの Web サーバを準備します。

前提条件

- My VMware から `identity-manager-connector-versionNumber-buildNumber-updaterepo.zip` ファイルをダウンロードします。my.vmware.com にアクセスして、[VMware Identity Manager Download] ページに移動し、[VMware Identity Manager コネクト オフライン アップグレード パッケージ] に表示されているファイルをダウンロードします。
- IIS Web サーバを使用する場合は、ファイル名に特殊文字を利用できるよう Web サーバを構成します。これを構成するには、[フィルタリングを要求] セクションで [ダブル エスケープを許可] オプションを選択します。

手順

- 1 Web サーバの `http://YourWebServer/VM/` にディレクトリを作成して、ダウンロードした zip ファイルをコピーします。
- 2 Web サーバに `.sig` (text/plain) および `.sha256` (text/plain) の MIME タイプが含まれていることを確認します。
これらの MIME タイプが含まれない場合、Web サーバの更新確認は失敗します。
- 3 zip ファイルを展開します。
zip ファイルから抽出された内容は、`http://YourWebServer/VM/` に配置されます。
ファイルから抽出された内容には、サブディレクトリの `/manifest` と `/package-pool` が含まれます。

- 4 次の `updatelocal.hzn` コマンドを実行して、URL に有効なアップデート コンテンツが含まれていることを確認します。

```
/usr/local/horizon/update/updatelocal.hzn checkurl http://YourWebServer/VM/
```

コネクタを構成してオフライン アップグレードを実行する

オフライン アップグレードを実行するには、ローカルの Web サーバを参照するようにコネクタ アプライアンスを構成します。その後にアプライアンスをアップグレードします。

前提条件

オフライン アップグレード向けにローカル Web サーバを準備します。

手順

- 1 コネクタ アプライアンスに root ユーザーとしてログインします。
- 2 次のコマンドを実行して、ローカルの Web サーバを使用するアップグレード リポジトリを構成します。

```
/usr/local/horizon/update/updatelocal.hzn seturl http://YourWebServer/VM/
```

注： 構成を元に戻してオンライン アップグレードの機能を回復するには、次のコマンドを実行します。

```
/usr/local/horizon/update/updatelocal.hzn setdefault
```

- 3 アップグレードを実行します。

- a 次のコマンドを実行します。

```
/usr/local/horizon/update/updatemgr.hznupdateinstaller
```

- b 次のコマンドを実行して、利用可能なアップグレードのバージョンを確認します。

```
/usr/local/horizon/update/updatemgr.hzncheck
```

- c 次のコマンドを実行して、コネクタを更新します。

```
/usr/local/horizon/update/updatemgr.hznupdate
```

アップグレード中に発生したメッセージは、`update.log` ファイル（`/opt/vmware/var/log/update.log`）に保存されます。

- d `updatemgr.hzn check` コマンドを再実行します。

```
/usr/local/horizon/update/updatemgr.hzncheck
```

- e アップグレードしたアプライアンスのバージョンを確認します。

```
vamicli version --appliance
```

このコマンドは新しいバージョンを表示します。

- f コネクタ アプライアンスを再起動します。

たとえば、コマンド ラインで次のコマンドを実行します。

```
reboot
```

結果

コネクタのアップグレードは完了です。

外部コネクタをアップグレードした後の設定の構成

コネクタ 2016.3.1.0 以降にアップグレードした場合、いくつかの設定が必要になる場合があります。

Kerberos 認証でのドメインへの再参加

Kerberos 認証または Active Directory（統合 Windows 認証）ディレクトリを使用する場合は、ドメインへの参加を解除して、再びドメインに参加させる必要があります。この操作は、環境内のすべてのコネクタ仮想アプライアンスに必要です。

- 1 [管理] - [ディレクトリ管理] - [コネクタ] を選択します
- 2 [コネクタ] ページで、Kerberos 認証、または Active Directory（統合 Windows 認証）ディレクトリに使用されている各コネクタに対し、[ドメイン参加を解除] をクリックします。
- 3 ドメインに参加させるには、ドメインへの参加権限を含む Active Directory 証明書が必要です。詳細については、[コネクタ マシンをドメインに参加させる](#) を参照してください。
- 4 Kerberos 認証を使用している場合、Kerberos 認証アダプタを再度有効にします。[認証アダプタ] ページにアクセスするには、[コネクタ] ページの [ワーカー] 列で適切なリンクをクリックし、[認証アダプタ] タブを選択します。
- 5 使用している他の認証アダプタが有効になっていることを確認します。

[ドメイン] ページの更新

Active Directory（統合 Windows 認証）を使用している場合、または LDAP 経由の Active Directory で [このディレクトリ は DNS サービス ロケーションをサポートします] オプションを有効にしている場合は、ディレクトリの [ドメイン] ページを更新します。

- 1 [管理] - [ディレクトリ管理] - [ディレクトリ] を選択します。
- 2 適切なディレクトリを選択して編集します。
- 3 バインド DN ユーザーのパスワードを入力して、[保存] をクリックします。
- 4 ページの左側で [同期設定] をクリックして、[ドメイン] タブを選択します。

5 [保存] をクリックします。

DNS サービス ロケーションとドメイン コントローラ

注： コネクタ 2016.3.1.0 以降では、DNS サービス ロケーションを有効にしたディレクトリを作成するときに、`domain_krb.properties` ファイルが自動的に作成され、ドメイン コントローラが自動的に入力されます。元の環境に `domain_krb.properties` ファイルが含まれていた場合、アップグレード後に [ドメイン] ページを保存し直すと、このファイルが更新され、後から追加したドメインがファイルに追加されます。元の環境に `domain_krb.properties` ファイルが含まれていない場合は、ファイルが作成され、ドメイン コントローラが自動的に入力されます。`domain_krb.properties` ファイルの詳細については、[ドメイン コントローラの選択](#)を参照してください。

外部コネクタのアップグレード エラーのトラブルシューティング

エラー ログを確認することで、vRA ディレクトリ管理の外部コネクタのアップグレードに関する問題のトラブルシューティングを行うことができます。コネクタが起動しない場合は、スナップショットにロールバックして前のインスタンスに戻ることができます。

■ アップグレード エラー ログの確認

アップグレード時に発生したエラーを解決するには、エラー ログを確認します。アップグレード ログ ファイルは、`/opt/vmware/var/log` ディレクトリ内にあります。

■ コネクタのスナップショットへのロールバック

アップグレード後にコネクタが正常に起動せず、アップグレード エラー ログを確認してアップグレード コマンドを再実行しても問題を解決できない場合、以前のコネクタ インスタンスにロールバックすることができます。

■ ログ ファイル バンドルの収集

VMware サポートに送信するログ ファイルのバンドルを収集できます。バンドルはコネクタの構成ページから取得します。

アップグレード エラー ログの確認

アップグレード時に発生したエラーを解決するには、エラー ログを確認します。アップグレード ログ ファイルは、`/opt/vmware/var/log` ディレクトリ内にあります。

エラーが発生した場合、アップグレード後にコネクタが起動しない可能性があります。

手順

- 1 コネクタ アプライアンスにログインします。
- 2 `/opt/vmware/var/log` ディレクトリに移動します。
- 3 `update.log` ファイルを開いてエラー メッセージを調べます。
- 4 エラーを解決して、もう一度アップグレード コマンドを実行します。アップグレード コマンドは、停止した場所から再開します。

注： または、スナップショットにロールバックしてもう一度アップデートを実行します。

コネクタのスナップショットへのロールバック

アップグレード後にコネクタが正常に起動せず、アップグレード エラー ログを確認してアップグレード コマンドを再実行しても問題を解決できない場合、以前のコネクタ インスタンスにロールバックすることができます。

手順

- ◆ 元のコネクタ インスタンスのバックアップとして取得したスナップショットのいずれかにロールバックします。詳細については、vSphere のドキュメントを参照してください。

ログ ファイル バンドルの収集

VMware サポートに送信するログ ファイルのバンドルを収集できます。バンドルはコネクタの構成ページから取得します。

次のログ ファイルがバンドルに収集されます。

表 2-9. ログ ファイル

コンポーネント	ログ ファイルの場所	説明
Apache Tomcat ログ (catalina.log)	/opt/vmware/horizon/workspace/logs/ catalina.log	Apache Tomcat は他のログ ファイルに記録されないメッセージを記録します。
Configurator ログ (configurator.log)	/opt/vmware/horizon/workspace/logs/ configurator.log	Configurator が REST クライアントと Web インターフェイスから受け取る要求。
コネクタ ログ (connector.log)	/opt/vmware/horizon/workspace/logs/ connector.log	Web インターフェイスから受信された各要求の記録。各ログ エントリには要求 URL、タイムスタンプ、例外が含まれています。同期アクションは記録されません。

手順

- 1 コネクタの構成ページ (<https://connectorURL:8443/cfg/logs>) にログインします。
- 2 [ログ バンドルの準備] をクリックします。
- 3 バンドルをダウンロードして、これを VMware サポートに送信します。

シナリオ：高可用性 vRealize Automation に対する Active Directory リンクを構成する

テナント管理者として、LDAP ディレクトリ接続による Active Directory を構成して、高可用性 vRealize Automation の導入環境に対するユーザー認証をサポートしようと思います。

各 vRealize Automation アプライアンスにはユーザー認証をサポートするコネクタが含まれていますが、通常、ディレクトリの同期用にコネクタを 1 つ構成します。同期用に、どのコネクタを選択してもかまいません。ディレクトリ管理の高可用性をサポートするには、セカンダリ vRealize Automation アプライアンスに対応する別のコネクタを構成する必要があります。このコネクタは、ID プロバイダに接続して同一の Active Directory を指定します。このように構成すると、1 台目の vRealize Automation Appliance が故障しても、もう一方がユーザー認証の管理を引き継ぎます。

高可用性環境では、すべてのノードで、同一の Active Directory、ユーザー、認証方法などの設定を使用する必要があります。最も直接的な実現方法は、ID プロバイダ ホストとしてロード バランサ ホストを設定し、ID プロバイダをクラスタに昇格させることです。このように構成すると、すべての認証要求はロード バランサに送られ、必要に応じていずれかのコネクタにこの要求が転送されます。


前提条件


- 適切なロード バランサを使用して分散 vRealize Automation 導入環境をインストールします。『vRealize Automation のインストール』を参照してください。
- テナント管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [ディレクトリ管理] - [ディレクトリ] を選択します。
- 2 [ディレクトリの追加] をクリックします。
- 3 Active Directory アカウントの詳細な設定を入力し、デフォルトのオプションを受け入れます。

オプション	入力例
ディレクトリ名	Active Directory ドメイン名の IP アドレスを追加します。
同期コネクタ	すべての vRealize Automation アプライアンスにはコネクタが含まれています。利用可能なコネクタのいずれかを使用します。
ベース DN	ディレクトリ サーバ 検索の先頭に識別名(DN)を入力します。たとえば、[cn=users,dc=corp,dc=local] と入力します。
バインド DN	共通名 (CN) など、ユーザーを検索する権限がある Active Directory ユーザー アカウントの完全識別名 (DN) を入力します。たとえば、[cn=config_admin infra,cn=users,dc=corp,dc=local] と入力します。
バインド DN パスワード	ユーザーを検索できるアカウントの Active Directory パスワードを入力します。

- 4 [接続をテスト] をクリックし、構成したディレクトリへの接続をテストします。
接続が失敗した場合は、すべてのフィールドのエントリを確認し、必要に応じてシステム管理者に問い合わせてください。
- 5 [保存して次へ] をクリックします。
[ドメインの選択] ページにドメインのリストが表示されます。
- 6 デフォルトのドメインが選択された状態のままで [次へ] をクリックします。
- 7 属性名が適切な Active Directory 属性にマップされていることを確認します。適切にマッピングされていない場合は、ドロップダウン メニューから正しい Active Directory 属性を選択します。[次へ] をクリックします。
- 8 同期させたいグループやユーザーを選択します。
 - a [追加] アイコン () をクリックします。
 - b ユーザー ドメインを入力し、[グループの検索] をクリックします。
たとえば、**cn=users,dc=corp,dc=local** と入力します。

- c [すべて選択] チェック ボックスをオンにします。
 - d [選択] をクリックします。
 - e [次へ] をクリックします。
 - f  をクリックしてさらにユーザーを追加します。たとえば、
CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com のように入力します。

ユーザーを除外するには、[+] をクリックしていくつかのタイプのユーザーを除外するフィルタを作成します。フィルタリングの基準となるユーザー属性、クエリ ルールおよび値を選択します。
 - g [次へ] をクリックします。
- 9** このページで、ディレクトリと同期しているユーザーやグループの数を確認し、[ディレクトリの同期] をクリックします。
- ディレクトリの同期処理は少し時間がかかりますが、バックグラウンドで実行されるので、作業を続けることができます。
- 10** 高可用性をサポートする 2 番目のコネクタを構成します。
- a テナント管理者として、vRealize Automation の展開のロード バランサにログインします。
ロード バランサの URL は *load balancer address/vcac/org/tenant_name* です。
 - b [管理] - [ディレクトリ管理] - [ID プロバイダ] の順に選択します。
 - c システムで現在使用している ID プロバイダをクリックします。
システムに基本的な ID 管理を提供する既存のディレクトリとコネクタが表示されます。
 - d [コネクタの追加] ドロップダウン リストをクリックし、2 番目の vRealize Automation アプライアンスに対応するコネクタを選択します。
 - e コネクタを選択すると表示される [バインド DN パスワード] テキスト ボックスに適切なパスワードを入力します。
 - f [コネクタの追加] をクリックします。
 - g ロード バランサをポイントするようにホスト名を編集します。

結果

コーポレート Active Directory が vRealize Automation に接続され、ディレクトリ管理が高可用性に対応するように設定されました。

次のステップ

セキュリティを強化するために、ID プロバイダと Active Directory の双方向の信頼を構成することができます。
[vRealize Automation と Active Directory 間で双方向の信頼関係を構築を参照してください。](#)

vRealize Automation でのスマート カードおよびサードパーティ ID プロバイダの認証用外部コネクタの構成

証明書認証やスマート カード認証を行うサードパーティ ID プロバイダを使用している場合、システム管理者はディレクトリ管理を使用して、vRealize Automation 展開で外部コネクタを構成する必要があります。また、ここに示されている手順は、すべてのタイプの証明書認証に幅広く適用されます。

ディレクトリ管理は、構成された各 Active Directory に対して複数の ID プロバイダおよびコネクタ クラスタをサポートします。サードパーティ ID プロバイダまたはスマート カードの認証を使用するには、単一の外部コネクタをセットアップするか、SSL パススルーを許可するロード バランサの背後に適切な ID プロバイダを備えたコネクタ クラスタをセットアップすることができます。詳細については、[コネクタとコネクタ クラスタの管理](#) を参照してください。

外部コネクタの更新の詳細については、[ディレクトリ管理の外部コネクタのアップグレード](#) を参照してください。

スマート カード認証にはさまざまな証明書構成オプションを使用できます。[ディレクトリ管理で証明書またはスマート カード アダプタを使用するための構成](#) を参照してください。

前提条件

- vRealize Automation 展開で使用する適切な Active Directory 接続を構成します。
- コネクタを構成するのに必要な OVA ファイルを [VMware vRealize Automation Tools and SDK](#) からダウンロードします。
- テナント管理者として vRealize Automation にログインします。

手順

1 [コネクタ アクティベーション トークンの生成](#)

スマート カード認証に使用するコネクタ仮想アプライアンスを展開する前に、vRealize Automation コンソールから新しいコネクタのアクティベーション コードを生成します。アクティベーション コードは、ディレクトリ管理とコネクタ間の通信を確立するために使用されます。

2 [コネクタ OVA ファイルを展開する](#)

コネクタ OVA ファイルをダウンロードしたら、VMware vSphere Client または vSphere Web Client を使用して展開できます。

3 [コネクタ設定を構成する](#)

コネクタ OVA を展開したら、セットアップ ウィザードを実行してアプライアンスのアクティベーションを行い、管理者パスワードを構成する必要があります。

4 [パブリック証明機関の適用](#)

ディレクトリ管理のインストール時に、デフォルトの SSL 証明書が生成されます。デフォルトの証明書はテストに使用できますが、本番環境には商用の SSL 証明書を生成してインストールする必要があります。

5 [ワークスペース ID プロバイダの作成](#)

外部コネクタで使用するワークスペース ID プロバイダを作成する必要があります。

6 証明書認証の構成とデフォルトのアクセス ポリシー ルールの構成

vRealize Automation の Active Directory およびドメインで使用する外部コネクタを構成する必要があります。

コネクタ アクティベーション トークンの生成

スマート カード認証に使用するコネクタ仮想アプライアンスを展開する前に、vRealize Automation コンソールから新しいコネクタのアクティベーション コードを生成します。アクティベーション コードは、ディレクトリ管理とコネクタ間の通信を確立するために使用されます。

単一のコネクタまたはコネクタ クラスタを構成することができます。コネクタ クラスタを使用する場合は、必要な各コネクタに対してこの手順を繰り返します。

前提条件

- テナント管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [ディレクトリ管理] - [コネクタ] を選択します。
- 2 [コネクタの追加] をクリックします。
- 3 [コネクタ ID 名] テキスト ボックスに新しいコネクタの名前を入力します。
- 4 [アクティベーション コードを生成] をクリックします。

コネクタのアクティベーション コードが [コネクタ アクティベーション コード] ボックスに表示されます。

- 5 OVA ファイルを使用して、コネクタの構成に使用するアクティベーション コードをコピーします。
- 6 [OK] をクリックします。

コネクタ OVA ファイルを展開する

コネクタ OVA ファイルをダウンロードしたら、VMware vSphere Client または vSphere Web Client を使用して展開できます。

vSphere Client または vSphere Web Client を使用して OVA ファイルを展開します。

前提条件

- コネクタ OVA の展開に使用する DNS レコードとホスト名を特定します。
- vSphere Web Client を使用する場合は、Firefox ブラウザまたは Chrome ブラウザを使用します。Internet Explorer を使用して OVA ファイルを展開しないでください。
- コネクタを構成するのに必要な OVA ファイルを [VMware vRealize Automation Tools and SDK](#) からダウンロードします。

手順

- 1 vSphere Client または vSphere Web Client で、[ファイル] - [OVF テンプレートを展開] を選択します。

2 [OVF テンプレートの展開] ページで、使用環境のコネクタの展開に固有の情報を入力します。

ページ	説明
vCenter Server の IP アドレス	OVA パッケージの場所を参照するか、または特定の URL を入力します。
OVA テンプレートの詳細	正しいバージョンを選択していることを確認します。
ライセンス	エンド ユーザー使用許諾契約を読み、[同意する] をクリックします。
名前と場所	仮想アプライアンスの名前を入力します。名前はインベントリ フォルダ内で一意である必要があり、最大で 80 文字指定できます。名前の大文字と小文字は区別されます。 仮想アプライアンスの場所を選択します。
ホスト/クラスタ	ホストまたはクラスタを選択して展開したテンプレートを実行します。
リソース プール	リソース プールを選択します。
ストレージ	仮想マシン ファイルを格納する場所を選択します。
ディスク形式	ファイルのディスク形式を選択します。本番環境の場合は、[シック プロビジョニング] 形式を選択します。評価やテストには [シン プロビジョニング] 形式を使用します。
ネットワークのマッピング	ユーザーの環境のネットワークを OVF テンプレートのネットワークにマッピングします。
プロパティ	<p>a [タイムゾーンの設定] フィールドで、正しいタイム ゾーンを選択します。</p> <p>b デフォルトでは、[カスタム エクスペリエンス改善プログラム] チェック ボックスはオンになっています。VMware はお客様のご要望への対応を向上させるために、お客様の展開環境に関する匿名データを収集します。データを収集されたくない場合は、チェック ボックスをオフにします。</p> <p>c [ホスト名] テキスト ボックスに、使用するホスト名を入力します。空白にすると、逆引き DNS を使用してホスト名が参照されます。</p> <p>d コネクタに固定 IP アドレスを構成するには、デフォルト ゲートウェイ、DNS、IP アドレス、およびネットマスクのそれぞれにアドレスを入力します。</p> <p>重要： ホスト名を含む 4 つのアドレス フィールドのいずれかが空白の場合は、DHCP が使用されます。</p> <p>DHCP を構成する場合は、アドレス フィールドを空白のままにしておきます。</p>
終了準備の完了	選択内容を確認し、[終了] をクリックします。

ネットワークの速度によっては、展開に数分かかることがあります。進捗のダイアログ ボックスで進捗状況を表示できます。

3 展開が完了したら、アプライアンスを選択して右クリックし、[パワー] - [パワーオン] を選択します。

アプライアンスは初期化されます。[コンソール] タブで詳細を確認できます。仮想アプライアンスの初期化が完了すると、コンソール画面に のバージョンと、 セットアップ ウィザードにログインしてセットアップを完了するための URL が表示されます。

次のステップ

セットアップ ウィザードを使用して、アクティブ化コードと管理者パスワードを追加します。

コネクタ設定を構成する

コネクタ OVA を展開したら、セットアップ ウィザードを実行してアプライアンスのアクティベーションを行い、管理者パスワードを構成する必要があります。

前提条件

- コネクタのアクティベーション コードが生成されました。
- コネクタ アプライアンスがパワーオンされていること、そしてコネクタの URL を把握していることを確認します。
- コネクタ管理者、root アカウントおよび sshuser アカウントに使用するパスワードのリストを収集します。

手順

- 1 セットアップ ウィザードを実行するには、OVA が展開された後に [コンソール] タブに表示されたコネクタの URL を入力します。
- 2 [ようこそ] ページで、[続行] をクリックします。
- 3 次のコネクタ仮想アプライアンスの管理者アカウントでは強力なパスワードを作成します。

強度の高いパスワードの長さは、少なくとも 8 文字であり、大文字と小文字が含まれ、少なくとも 1 つ数字および特殊文字が含まれる必要があります。

オプション	説明
アプライアンス管理者	アプライアンス管理者のパスワードを作成します。ユーザー名は [admin] です。変更することはできません。このアカウントとパスワードを使用してコネクタ サービスにログインし、証明書、アプライアンスのパスワード、および syslog の構成を管理します。 重要： [admin] ユーザーは、6 文字以上のパスワードを使用する必要があります。
root アカウント	デフォルトの VMware root パスワードが、コネクタ アプライアンスのインストールに使用されました。新しい root パスワードを作成します。
sshuser アカウント	コネクタ アプライアンスへのリモート アクセスに使用するパスワードを作成します。

- 4 [続行] をクリックします。
- 5 [コネクタをアクティブ化] ページで、アクティブ化コードを貼り付けて、[続行] をクリックします。
- 6 vRealize Automation 内部コネクタで自己署名証明書を使用している場合は、vRealize Automation アプライアンスで `cat /etc/apache2/server-cert.pem` コマンドを実行することで適切な証明書を取得できます。

[ロード バランサで SSL を終了する] タブを選択し、/horizon_workspace_rootca.pem のリンクをクリックします。

アクティベーション コードが検証され、サービスとコネクタ インスタンス間の通信が確立されてコネクタ構成が完了します。

次のステップ

サービスでは、ニーズに基づいて環境をセットアップします。たとえば、2 つの統合 Windows 認証ディレクトリを同期させるためにコネクタを追加した場合は、ディレクトリを作成し、それを新しいコネクタと関連付けます。

パブリック証明機関の適用

ディレクトリ管理のインストール時に、デフォルトの SSL 証明書が生成されます。デフォルトの証明書はテストに使用できますが、本番環境には商用の SSL 証明書を生成してインストールする必要があります。

ディレクトリ管理がロード バランサを参照している場合、SSL 証明書はロード バランサに適用されます。

証明書をインポートするときに、[このキーをエクスポート可能にする]を選択する必要があります。

カスタム証明書の CSR を生成する場合は、CN または認証局のサイト ドメイン名を指定するだけです。

前提条件

証明書署名リクエスト (CSR) を生成し、認証局 (CA) から有効な署名証明書を取得します。組織が CA によって署名された SSL 証明書を提供している場合には、これらの証明書を使用できます。証明書は PEM 形式である必要があります。

手順

- 1 管理者ユーザーとして、次の URL にあるコネクタ アプライアンス管理ページにログインします。
`https://myconnector.mycompany:8443/cfg`
- 2 管理者コンソールで、[アプライアンス設定] をクリックします。
デフォルトで仮想アプライアンス構成が選択されます。
- 3 [構成の管理] をクリックします。
- 4 VMware Identify Manager のサーバ管理者ユーザー パスワードを入力します。
- 5 [証明書のインストール] を選択します。
- 6 [Identity Manager Appliance (Identity Manager アプライアンス)] タブの [Terminate SSL (SSL を終了)] で、[Custom Certificate (カスタム証明書)] を選択します。
- 7 [SSL 証明書チェーン] テキストボックスに、ホスト、中間、ルート証明書の順に貼り付けます。
SSL 証明書は、証明書チェーン全体が正しい順序で含まれている場合にのみ機能します。各証明書について、-----BEGIN CERTIFICATE----- と -----END CERTIFICATE----- の行を含めて、これらの行の間にあるすべての行をコピーします。
証明書に FQDN ホスト名が含まれていることを確認します。
- 8 プライベート キーを [プライベート キー] テキストボックスに貼り付けます。----BEGIN RSA PRIVATE KEY と ---END RSA PRIVATE KEY の行の間にあるすべての行をコピーします。
- 9 [保存] をクリックします。

例：証明書の例**証明書チェーンの例**

-----BEGIN CERTIFICATE-----

jIQvt9WdR9Vpg3WQT5+C3HU17bUOwvhp/r0+

...

...

...

W53+O05j5xsxzDJfWr1lqBIFf/OkIYCPcyK1

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

WdR9Vpg3WQT5+C3HU17bUOwvhp/rjIQvt90+

...

...

...

O05j5xsxzDJfWr1lqBIFf/OkIYCPW53+cyK1

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

dR9Vpg3WQTjIQvt9W5+C3HU17bUOwvhp/r0+

...

...

...

5j5xsxzDJfWr1lqW53+O0BIFf/OkIYCPcyK1

-----END CERTIFICATE-----

プライベート キーの例

-----BEGIN RSA PRIVATE KEY-----

jIQvtg3WQT5+C3HU17bU9WdR9VpOwvhp/r0+

...

...

...

1lqBIFFW53+O05j5xsxzDJfWr/OkIYCPcyK1

-----END RSA PRIVATE KEY-----

ワークスペース ID プロバイダの作成

外部コネクタで使用するワークスペース ID プロバイダを作成する必要があります。

前提条件

- テナント管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [ディレクトリ管理] - [ID プロバイダ] の順に選択します。

- 2 [ID プロバイダを追加] を選択します。
- 3 [Workspace IDP を作成] を選択します。
- 4 [ID プロバイダ名] フィールドに ID プロバイダの名前を入力します。
- 5 ID プロバイダを使用するユーザーに対応するディレクトリを選択します。
選択したディレクトリによって、ID プロバイダで使用できるコネクタが決まります。
- 6 外部コネクタまたはスマート カード認証用に構成したコネクタを選択してください。

注： 展開がロード バランサの背後に配置される場合は、ロード バランサの URL を入力します。

- 7 ID プロバイダにアクセスするネットワークを選択します。
- 8 [追加] をクリックします。

証明書認証の構成とデフォルトのアクセス ポリシー ルールの構成

vRealize Automation の Active Directory およびドメインで使用する外部コネクタを構成する必要があります。

前提条件

テナント管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [ディレクトリ管理] - [コネクタ] の順に選択します。
- 2 [ワーカー] 列で必要なコネクタを選択します。
選択されたワーカーがコネクタの [詳細] タブの [ワーカー名] テキスト ボックスに表示され、コネクタ タイプ 情報が [コネクタ タイプ] テキスト ボックスに表示されます。
- 3 [関連付けられたディレクトリ] テキスト ボックスで必要な Active Directory を指定することにより、コネクタがその Active Directory にリンクすることを確認します。
- 4 [関連付けられたドメイン] テキスト ボックスに適切なドメイン名を入力します。
- 5 [AuthAdapters] タブを選択し、CertificateAuthAdapter を有効にします。
- 6 展開に合わせて証明書認証を適切に構成してください。
[ディレクトリ管理のための証明書認証の構成](#)を参照してください。
- 7 [管理] - [ディレクトリ管理] - [ポリシー] の順に選択します。
- 8 [デフォルトのポリシーを編集] をクリックします。
- 9 ポリシー ルールに証明書を追加し、それを最初の認証方法にします。

証明書は、ポリシー ルールに表示される認証方法の一番上に配置する必要があります。そうしないと、証明書による認証は失敗します。

マルチ ドメインまたはマルチ フォレストの Active Directory リンクの作成

システム管理者として、マルチ ドメインまたはマルチ フォレストの Active Directory リンクを構成する必要があります。

マルチ ドメインまたはマルチ フォレストの Active Directory リンクの構成手順は基本的に同じです。マルチ フォレストのリンクの場合、すべての適用可能なドメイン間で双方向の信頼が必要です。

前提条件

- 適切なロード バランサを使用して分散 vRealize Automation 導入環境をインストールします。『vRealize Automation のインストール』を参照してください。
- テナント管理者として vRealize Automation にログインします。
- 展開に適切なドメインと Active Directory フォレストを構成します。

手順

- 1 [管理] - [ディレクトリ管理] - [ディレクトリ] を選択します。
- 2 [ディレクトリの追加] をクリックします。
- 3 [ディレクトリの追加] ページの [ディレクトリ名] テキスト ボックスで Active Directory サーバの名前を指定します。
- 4 [ディレクトリ名] 見出しにある [Active Directory (統合 Windows 認証)] を選択します。
- 5 [ディレクトリの同期と認証] セクションで、Active Directory から VMware Directories Management ディレクトリにユーザーを同期するコネクタを構成します。

オプション	説明
同期コネクタ	お使いのシステムに適したコネクタを選択します。各 vRealize Automation アプライアンスにはデフォルトのコネクタが含まれています。適切なコネクタの選択について不明な点がある場合は、システム管理者に問い合わせてください。
認証	適切なラジオ ボタンをクリックして、選択したコネクタで認証も行うかどうかを指定します。
ディレクトリ検索属性	ユーザー名を含む適切なアカウント属性を選択します。

展開の構成に応じて、使用可能な 1 つ以上のコネクタを選択します。

- 6 [ドメイン名]、[ドメイン管理者ユーザー名]、および [ドメイン管理者パスワード] の各テキスト ボックスに適切な参加ドメイン認証情報を入力します。

一例として、次のように入力できます。[ドメイン名]: `hs.trcint.com`、[ドメイン管理者ユーザー名]: `devadmin`、[ドメイン管理者パスワード]: `xxxx`。

- 7 [バインド ユーザーの詳細] セクションで、ディレクトリ同期を促進するための適切な Active Directory（統合 Windows 認証）を入力します。

オプション	説明
バインド ユーザー UPN	そのドメインで認証できるユーザーのユーザー プリンシパル名を入力します。たとえば、UserName@example.com のように入力します。
バインド DN パスワード	バインド ユーザーのパスワードを入力します。

- 8 [保存して次へ] をクリックします。

[ドメインの選択] ページにドメインのリストが表示されます。


- 9 適切なチェック ボックスをクリックし、システム展開に必要なドメインを選択します。

- 10 [次へ] をクリックします。

- 11 Directories Management のディレクトリ属性名が、正しい Active Directory 属性にマッピングされていることを確認します。

適切にマッピングされていない場合は、ドロップダウン メニューから正しい Active Directory 属性を選択します。


- 12 [次へ] をクリックします。


- 13  をクリックして、Active Directory とこのディレクトリを同期するグループを選択します。

Active Directory グループを追加するときに、そのグループのメンバーがユーザー リストに含まれていない場合、これらのメンバーが追加されます。

注： Directories Management のユーザー認証システムでは、グループやユーザーを追加する場合 Active Directory からデータをインポートするため、その処理速度は Active Directory の機能によって制限されます。その結果、追加するグループとユーザーの数に応じて、インポート処理にかなりの時間がかかる場合があります。遅延または問題の発生を最小限に抑えるには、グループとユーザーを vRealize Automation の運用上必要な数に制限します。システム パフォーマンスの低下またはエラーが発生した場合は、不要なアプリケーションをすべて閉じて、Active Directory に十分なメモリが割り当てられるようにしてください。問題が解決されない場合は、必要に応じて Active Directory に割り当てるメモリを増やしてください。多数のユーザーおよびグループを持つシステムでは、場合によっては Active Directory に割り当てるメモリを最大 24 GB まで増やす必要があります。

- 14 [次へ] をクリックします。

- 15  をクリックしてさらにユーザーを追加します。たとえば、**CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com** のように入力します。

ユーザーを除外するには、 をクリックして特定のタイプのユーザーを除外するフィルタを作成します。フィルタリングの基準となるユーザー属性、クエリ ルールおよび値を選択します。

- 16 [次へ] をクリックします。

- 17 このページで、ディレクトリと同期しているユーザー数とグループ数を確認します。

ユーザー数とグループ数を変更する場合には、[編集] リンクをクリックします。

18 [Workspace にプッシュ] をクリックして、ディレクトリとの同期を開始します。

次のステップ

グループとユーザーのロールの構成

テナント管理者はビジネス グループとカスタム グループを作成し、vRealize Automation コンソールへのユーザー アクセス権を付与します。

ディレクトリ ユーザーまたはグループへのロールの割り当て

テナント管理者は、ユーザーまたはグループにロールを割り当てることで、ユーザーにアクセス権を付与します。

ユーザーまたはグループがパイプラインを変更およびトリガできるようにするには、それらのユーザーまたはグループに権限を割り当てる必要があります。ユーザーまたはグループにリリース マネージャのロールを割り当てると、パイプラインを変更およびトリガできます。ユーザーまたはグループにリリース エンジニアのロールを割り当てると、パイプラインをトリガできます。詳細については、『Using vRealize Code Stream』を参照してください。

前提条件

テナント管理者として vRealize Automation にログインします。

手順

- 1** [管理] - [ユーザーおよびグループ] - [ディレクトリ ユーザーとディレクトリ グループ] を選択します。
- 2** [検索] ボックスにユーザー名またはグループ名を入力して Enter キーを押します。
 アットマーク (@)、バックスラッシュ (\)、またはスラッシュ (/) を名前に使用することはできません。
 user@domain という形式でユーザー名またはグループ名を入力することで、検索を最適化できます。
- 3** ロールを割り当てるユーザーまたはグループの名前をクリックします。
- 4** [このユーザーにロールを追加します] リストから 1 つ以上のロールを選択します。
 [選択されたロールで付与される権限] リストには、付与する特定の権限が示されています。
- 5** (オプション) [次へ] をクリックすると、ユーザーまたはグループに関する詳細情報が表示されます。
- 6** [ユーザー詳細] ページの [全般] タブで、ユーザーを追加するロールのリストをスクロールします。
 - a パイプラインを変更およびトリガーする権限をユーザーに付与するには、[リリース マネージャ] チェックボックスを選択します。
 - b パイプラインをトリガする権限をユーザーに付与するには、[リリース エンジニア] チェックボックスを選択します。
- 7** [アップデート] をクリックします。

結果

現在、vRealize Automation にログインしているユーザーは、アクセス権が付与されているページに移動する前に、ログアウトして vRealize Automation にログインし直す必要があります。

次のステップ

必要に応じて、Active Directory 接続のユーザーおよびグループから独自のカスタム グループを作成できます。[カスタム グループの作成](#)を参照してください。

カスタム グループの作成

テナント管理者は、他のカスタム グループ、ID ストア グループ、および個々の ID ストア ユーザーを組み合わせることによってカスタム グループを作成できます。カスタム グループを使用すると、事業部門や部署などの組織単位に対応するビジネス グループに比べて、vRealize Automation 内のアクセスをより細かく制御できます。

カスタム グループを使用すると、標準の vRealize Automation グループ割り当てよりも細かい単位で、タスクのアクセス権を付与することができます。たとえば、カスタム グループを作成して、テナント管理者がテナント内の特定の権限を持つユーザーを制御できるようにすることが可能です。

カスタム グループにはロールを割り当てることができますが、ロールを割り当てる必要がない場合もあります。たとえば、マシン仕様の承認者という名前のカスタム グループを作成し、すべての事前のマシン承認に使用することができます。また、すべてのグループを一箇所で管理できるようにするために、ビジネス グループにマップするカスタム グループを作成する場合があります。これらの場合、ロールを割り当てる必要はありません。

前提条件

テナント管理者として vRealize Automation にログインします。

手順

1 [管理] - [ユーザーおよびグループ] - [カスタム グループ] を選択します。

2 [新規] をクリックします。

3 [名前] テキスト ボックスにグループ名を入力します。

カスタム グループ名には、セミコロン (;) の後に等号 (=) が続く組み合わせを含めることはできません。

4 (オプション) [説明] テキスト ボックスに説明を入力します。

5 [このグループにロールを追加する] リストから 1 つ以上のロールを選択します。

[選択されたロールで付与される権限] リストには、付与する特定の権限が示されています。

6 [次へ] をクリックします。

7 ユーザーとグループを追加してカスタム グループを作成します。

a [検索] ボックスにユーザー名またはグループ名を入力して Enter キーを押します。

アットマーク (@)、バックスラッシュ (\)、またはスラッシュ (/) を名前に使用することはできません。
user@domain という形式でユーザー名またはグループ名を入力することで、検索を最適化できます。

b ユーザーまたはグループを選択してカスタム グループに追加します。

8 [完了] をクリックします。

結果

現在、vRealize Automation にログインしているユーザーは、アクセス権が付与されているページに移動する前に、ログアウトして vRealize Automation にログインし直す必要があります。

カスタム グループとルールを使用したジャストインタイム ユーザーの追加

vRealize Automation ユーザーは、ジャストインタイム ユーザー プロビジョニングを使用すると、Active Directory にアクセスすることなく展開に追加できます。新しいユーザーに対してジャストインタイム プロビジョニングを呼び出すには、該当するカスタム グループにポピュレートするルールを作成する必要があります。

初回ログイン時、ジャストインタイム ユーザーには、[上級グループ メンバーシップ] ウィザード ページで作成したルールに基づいて動的にグループ メンバーシップが割り当てられます。初回ログイン後、通常の方法でグループ メンバーシップを割り当てることができます。このウィザードのこの 2 番目のページには、4 つの選択ボックスが含まれています。これらは、ジャストインタイム ユーザーを定義するさまざまな条件に基づくルールを作成するためのものです。

たとえば、最初のルールの選択ボックスで、条件として [ドメイン] を選択し、2 つ目のボックスで [一致] を選択できます。次に、3 つ目のルールのボックスで、ドメインを入力できます。これらの選択により、ジャストインタイム メンバーシップに基づいた、指定したドメインに関連付けられているユーザーを確立するルールを作成します。3 番目のボックスの選択は、自由入力形式のボックスです。最初の 2 つの選択ボックスで選択した内容に論理的に関連する情報を入力することができます。

注： ジャストインタイム ユーザーを構成する場合、NameId 形式のマッピングは、ユーザーを一意に識別する属性を指定します。NameId として使用されるこの属性は、ユーザーに対して一意である必要があります。また、属性自体は SAML 要求の一部として指定する必要があります。NameId 属性または NameId の値を変更すると、ログインの試行時にエラーが発生します。たとえば、NameId が `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` NameId 形式を使用してユーザーの SAMAccountName にマッピングされている場合は、SAMAccountName も個別に指定する必要があります。userName と SAMAccountName の値は変更しないでください。

vRealize Automation は、ジャストインタイム ユーザーを構成するためのワイルドカード一致をサポートしています。ワイルドカード一致を有効にして使用方法の詳細については、[ジャストインタイム ユーザーに対するワイルドカードによる一致の使用](#) を参照してください。

注： さまざまな条件に基づいてジャストインタイム ユーザーを追加する複数のルールを作成できます。複数のルールを作成する場合は、メインのルール ボックスの上にある [一致] ルール選択ボックスを使用し、vRealize Automation でのジャストインタイム ユーザーの追加時にルールの一部または全部に一致する必要があるかどうかを指定できます。

手順

- 1 [管理] - [ユーザーおよびグループ] - [カスタム グループ] の順に選択し、ジャストイン タイムのユーザーにとって適切なグループなど、既存のグループを特定します。

詳細については、[カスタム グループの作成](#) を参照してください。

グループの名前ではなく、グループの行をクリックします。

- 2 [上級メンバーシップ] をクリックします。

必要に応じて、[グループへのユーザーの追加] ページでユーザーを個別に追加できます。

- 3 [次へ] をクリックして [グループ ルール] ページを表示します。

- 4 ユーザーの構成に適切な 1 つ以上のルールを作成するには、一致ルール選択ボックスを使用します。

[一致] ルール選択ボックスの下にある 3 つのメインのルール選択ボックスで、下矢印をクリックして情報を入力すると、ドロップ ダウン メニューが有効になり、目的のルールを作成できます。上記のように、* および \ 文字を使用できることに注意してください。

- 5 [次へ] をクリックします。

- 6 グループからユーザーを除外する場合は、ユーザーを検索し、[ユーザーをグループから除外] ページにこれらのユーザーを追加します。

- 7 [次へ] をクリックします。

- 8 [確認] ページでグループの設定を確認し、[保存] をクリックしてルールと設定を保存および実装します。

結果

作成したルールに基づいてジャストインタイム ユーザーが追加されます。

ジャストインタイム ユーザーに対するワイルドカードによる一致の使用

vRealize Automation は、ジャストインタイム ユーザーを構成するために、ワイルドカードによる一致ルールをサポートしています。

ワイルドカードによる一致の有効化

デフォルトでは、ワイルドカードによる一致は有効になっていません。ワイルドカードによる一致を有効にするには、次のように、適切な REST API コマンドを実行する必要があります。

```
PUT:- https://{VRA_HOSTNAME}/SAAS/t/VSPHERE.LOCAL/jersey/manager/api/system/config/
isDynamicGroupWildcardEnabled
Content-Type: application/vnd.vmware.horizon.manager.systemconfigparameter+json
Accept: application/vnd.vmware.horizon.manager.systemconfigparameter+json
Authorization: HZN <token> (edited)
{
  "name": "isDynamicGroupWildcardEnabled",
  "values": {
    "values": [
      "true"
    ]
  }
}
```

ワイルドカード構成を有効にする API に使用される HZN トークンは、vsphere.local tenant の管理者ユーザー用である必要があります。

SAML アサーション属性の vRealize Automation ユーザー属性へのマッピング

SAML アサーション内の属性名は、vRealize Automation ユーザー属性ページで定義されている属性名と完全に一致する必要があります。ユーザーの名を含む SAML 属性には「firstName」、姓には「lastName」のように名前を付ける必要があります。ID プロバイダが [ユーザー属性] ページで定義されていない追加のユーザー属性を送信する場合、管理者はそれらの属性をページに追加する必要があります。たとえば、ID プロバイダが「groups」または「memberof」という SAML 属性でユーザー グループのメンバーシップ情報を送信する場合は、vRealize Automation ユーザー属性「groups」または「memberof」を追加する必要があります。属性名では、大文字と小文字を正確に使用します。

注： ユーザー グループ メンバーシップを定義する複数値属性内の Group_Name などの文字列を確実に識別するには、ワイルドカードを *Group_Name* として指定します。

[一致する] および [一致しない] 条件では、* をワイルドカードとして使用し、文字パターンの一致をルールに含めることができます。たとえば、<userinput>*Smi*</userinput> と入力すると、Smith、Smiley、Smirnoff など名前に smi が含まれる文字列が、途中に含む場合も含めて選択されます。パターンとの完全一致をすべて検索する場合は、パターンを入力するときに * の前にバックスラッシュ (\) を追加します。たとえば、<userinput>*Adam* </userinput> と入力すると、パターン「Adam*」と完全に一致するすべての名前が検索されます。* はフレーズ内のどこにでも使用することができ、* & * を含む任意の文字を前後に配置することができます。

ビジネス グループの作成

ビジネス グループは、サービスとリソースのセットをユーザーのセットに関連付けるために使用されます。これらのグループは、多くの場合、事業部門、部署、またはその他の組織単位に対応しています。予約を構成したり、ビジネス グループ メンバーのサービス カタログ アイテムをプロビジョニングする資格をユーザーに与えたりできるように、ビジネス グループを作成します。

ビジネス グループ ロールに複数のユーザーを追加するには、複数の個別ユーザーを追加するか、または ID ストアグループまたはカスタム グループをロールに追加することで複数のユーザーを同時に追加することができます。たとえば、カスタム グループ Sales Support Team を作成し、そのグループをサポート ロールに追加することができます。また、既存の ID ストア ユーザー グループを使用できます。選択したユーザーおよびグループは、ID ストアで有効でなければなりません。

vCloud Director の統合をサポートするには、vRealize Automation ビジネス グループの同一ビジネス グループ メンバーが、vCloud Director 組織のメンバーでもある必要があります。

テナント管理者がビジネス グループを作成すると、ビジネス グループ マネージャには、マネージャの電子メールアドレスとメンバーを修正できる権限が付与されます。テナント管理者はすべてのオプションを修正できます。


この手順では、IaaS がインストールされて構成されていることを想定しています。

前提条件

- テナント管理者として vRealize Automation にログインします。
- ビジネス グループのメンバーによって作成されたマシンを特定の Active Directory 組織単位に追加する場合は、Active Directory ポリシーを構成します。[Active Directory ポリシーの作成](#)を参照してください。ポリシーは、ビジネス グループの作成時に適用することも、後で追加することもできます。

- プロビジョニングされたマシン名の前に付加されるグループのデフォルトのマシン プリフィックスを指定する場合は、ファブリック管理者からプリフィックスをリクエストします。 [マシン プリフィックスの構成](#)を参照してください。マシン プリフィックスは XaaS では申請できません。

手順

- 1 [管理] - [ユーザーおよびグループ] - [ビジネス グループ] を選択します。
- 2 [新規] アイコン () をクリックします。
- 3 ビジネス グループの詳細を構成します。

オプション	説明
Name	ビジネス グループの名前を入力します。
説明	説明を入力します。
キャパシティ アラート メール送信先	容量アラート通知を受信する必要があるユーザーの 1 つまたは複数のメール アドレスを入力します。エイリアスのメール アドレスはサポートされません。各メール アドレスが特定のユーザー用である必要があります。 エントリが複数ある場合はコンマで区切ります。たとえば、 JoeAdmin@mycompany.com, WeiMgr@mycompany.com と入力します。
Active Directory のポリシー	ビジネス グループのデフォルトの Active Directory ポリシーを選択します。

- 4 カスタム プロパティを追加します。
- 5 [次へ] をクリックして [メンバー] ページに移動します。
- 6 ユーザー名とカスタム ユーザー グループ名を入力し、Enter キーを押します。

1 つ以上の個別ユーザーまたはカスタム ユーザー グループをビジネス グループに追加できます。これでユーザーを指定できます。または後で入力するための空のビジネス グループを作成できます。

オプション	説明
グループ マネージャ ロール	資格を作成したり、グループの承認ポリシーを割り当てることができます。
サポート ロール	ビジネス グループの他のメンバーの代理として、サービス カタログ アイテムの申請と管理を行うことができます。
共有アクセス ロール	他のビジネス グループのメンバーによって展開されたリソースを使用できるほか、これらのリソースに対してアクションを実行できます。
ユーザー ロール	資格付与の対象となるサービス カタログ アイテムを申請できます。

- 7 [次へ] をクリックして [インフラストラクチャ] ページに移動します。

8 デフォルトのインフラストラクチャ オプションを構成します。

オプション	説明
デフォルトのマシン プリフィックス	<p>ビジネス グループに事前構成されたマシン プリフィックスを選択します。</p> <p>このプリフィックスはマシン ブループリントで使用されます。ブループリントがデフォルトのプリフィックスを使用していて、ここでプリフィックスを指定しない場合は、ビジネス グループ名に基づいてマシン プリフィックスが作成されます。ベスト プラクティスでは、デフォルトのプリフィックスを使用します。しかし、特定のプリフィックスでブループリントを構成したり、サービス カタログ ユーザーがブループリントを申請するときにサービス カタログ ユーザーによるプリフィックスの上書きを許可したりできます。</p> <p>XaaS ブループリントは、デフォルトのマシン プリフィックスは使用しません。ここでプリフィックスを構成し、XaaS ブループリントを使用する資格をこのビジネス グループに付与しても、XaaS マシンのプロビジョニングには影響を与えません。</p>
Active Directory コンテナ	<p>Active Directory コンテナを入力します。このオプションは、WIM プロビジョニングにのみ適用されます。</p> <p>他のプロビジョニング方法では、プロビジョニングされたマシンを Active Directory コンテナに参加させるために追加の構成が必要です。</p>

9 [完了] をクリックします。

結果

テナント管理者は、予約を作成してビジネス グループにリソースを割り当てるできるようになります。ビジネス グループ マネージャは、ビジネス グループのメンバーの資格を作成できます。

次のステップ

- ビジネス グループがプロビジョニングするマシンの場所に基づいて、ビジネス グループの予約を作成します。
[予約シナリオの選択](#)を参照してください。
- カタログ アイテムが公開され、サービスが存在する場合は、ビジネス グループ メンバーの資格を作成できます。
[ユーザーにサービス、カタログ アイテム、アクションの使用資格を付与](#)を参照してください。

グループ メンバー表示時のパフォーマンス低下のトラブルシューティング

ビジネス グループまたはカスタム グループのメンバーがグループの詳細を表示すると、表示に時間がかかります。

問題

多数のユーザーが使用する環境でユーザー情報を表示すると、ユーザー インターフェイスに名前が表示されるまでに時間がかかります。

原因

大規模な Active Directory 環境では、名前のロードにより多くの時間が必要です。

解決方法

- ◆ データの取得時間を短縮するには、大量の個別メンバーを名前を追加するのではなく、可能な限り Active Directory グループまたはカスタム グループを使用します。

フィルタリングの予期しないエントリのトラブルシューティング

フィルタ選択の作成に使用されるビジネス グループ リストに、予期しないまたは重複したエントリが表示されます。

問題

この問題は、[管理] - [ユーザーおよびグループ] - [ビジネス グループ] でビジネス グループに変更を加えた際に発生します。[展開] ページでは、ビジネス グループを基準にして展開をフィルタリングする際に、フィルタ基準として使用可能なビジネス グループのリストに変更内容が反映されなかったり、ビジネス グループの重複などの予期しない結果が表示されたりします。

原因

システムは、30 分ごとに 1 回のみ変更をポーリングします。

解決方法

最大 30 分間待ってからブラウザを更新して、ビジネス グループ フィルタ選択リストを更新します。

追加テナントの作成

システム管理者として、ユーザーが割り当てられた作業を完了するのに必要な適切なアプリケーションおよびリソースにアクセスできるように、追加の vRealize Automation テナントを作成できます。

テナントは、ソフトウェア インスタンス内で作業する特定の権限を持ったユーザーのグループです。一般的に、デフォルトの vRealize Automation テナントは、システムのインストールおよび初期構成時に作成されます。その後、管理者は、ユーザーがログインして割り当てられた作業を完了できるように、追加テナントを作成できます。管理者は、システム運用に必要なだけのテナントを作成できます。テナント作成時、管理者は、名前、ログイン URL、ローカル ユーザー、管理者などの基本構成を指定する必要があります。基本テナント情報の構成後、テナント管理者は、vRealize Automation コンソールの [管理] タブにある [ディレクトリ管理] 機能を使用して、適切な Active Directory 接続にログインして設定する必要があります。さらに、テナント管理者はテナントにカスタム ブランディングを適用できます。

前提条件

システム管理者 として vRealize Automation コンソールにログインします。

手順

1 (オプション) テナント情報の指定

テナントを構成する最初の手順は、新しいテナントに名前を付けて vRealize Automation に追加し、テナント固有のアクセス URL を作成します。

2 (オプション) ローカル ユーザーの構成

vRealize Automation のシステム管理者は、各アプライアンス テナントのローカル ユーザーを構成する必要があります。

3 (オプション) 管理者の指定

1 人以上のテナント管理者および IaaS 管理者を、テナント用に構成した ID ストアから指定できます。


テナント情報の指定

テナントを構成する最初の手順は、新しいテナントに名前を付けて vRealize Automation に追加し、テナント固有のアクセス URL を作成します。

前提条件

システム管理者 として vRealize Automation コンソールにログインします。

手順

- 1 [管理] - [テナント] を選択します。
- 2 [新規] アイコン () をクリックします。
- 3 [名前] テキスト ボックスに名前を入力します。
- 4 (オプション) [説明] テキスト ボックスに説明を入力します。
- 5 テナントの一意の識別子を [URL 名] テキスト ボックスに入力します。

この URL トークンは、vRealize Automation コンソール URL の末尾にテナント固有の識別子を追加するときに使用します。

たとえば、**mytenant** と入力すると、`https://vrealize-appliance-hostname.domain.name/vcac/org/mytenant` という URL が作成されます。

注： vRealize Automation 7.0 と 7.1 では、テナントの URL を必ず小文字にしてください。

- 6 (オプション) 電子メール アドレスを [連絡先電子メール] テキスト ボックスに入力します。
- 7 [送信して次へ] をクリックします。

ローカル ユーザーの構成

vRealize Automation のシステム管理者は、各アプライアンス テナントのローカル ユーザーを構成する必要があります。

管理者がテナントの一般情報を作成すると、[ローカル ユーザー] タブが有効になり、管理者はテナントにアクセスするユーザーを指定できます。テナントの構成が完了すると、ローカル テナント ユーザーは各テナントにログインし、割り当てられた作業を行うことができます。

注： ユーザーを追加した後は、その構成を変更できません。ユーザー構成に関する何らかの要素の変更が必要な場合は、そのユーザーを削除したうえで作成し直す必要があります。

手順

- 1 [ローカル ユーザー] タブの [追加] ボタンをクリックします。
- 2 [ユーザー詳細] ダイアログの [名] フィールドおよび [姓] フィールドに名と姓を入力します。
- 3 [電子メール] フィールドにユーザーの電子メール アドレスを入力します。
- 4 [ユーザー名] フィールドおよび [パスワード] フィールドにユーザーのユーザー ID とパスワードを入力します。
- 5 [追加] ボタンをクリックします。

6 この手順は、テナントのすべてのローカル ユーザーに対し、必要に応じて繰り返します。

結果

指定したローカル ユーザーがテナントに作成されます。

管理者の指定

1 人以上のテナント管理者および IaaS 管理者を、テナント用に構成した ID ストアから指定できます。

テナント管理者は、ID ストア、ユーザー、グループ、資格、およびテナントのコンテンツ内の共有ブループリントの管理だけでなく、テナント特有のブランディングの構成も担当します。IaaS 管理者は、IaaS 内のインフラストラクチャ ソース エンドポイントの構成、ファブリック管理者の指定、および IaaS ログの監視を担当します。

前提条件

- IaaS 管理者を指定する前に、IaaS をインストールする必要があります。IaaS のインストールの詳細については、vRealize Automation のインストールを参照してください。

手順

- 1 ユーザー名またはグループ名を [テナント管理者] 検索ボックスに入力し、Enter を押します。
より短時間で結果を得るには、ユーザー名またはグループ名全体（例：myAdmins@mycompany.domain）を入力します。この手順を繰り返し、その他のテナント管理者を指定します。
- 2 IaaS がインストールされている場合は、ユーザー名またはグループ名を [IaaS 管理者] 検索ボックスに入力し、Enter を押します。
より短時間で結果を得るには、ユーザー名またはグループ名全体（例：IaaSAdmins@mycompany.domain）を入力します。この手順を繰り返し、その他のインフラストラクチャ管理者を指定します。
- 3 [追加] をクリックします。

テナントを削除する

システム管理者は、不要なテナントを vRealize Automation から削除できます。

テナントを削除すると、このテナントは vRealize Automation インターフェイスから直ちに削除されますが、このテナントが環境から完全に削除されるには、数時間かかる場合があります。テナントを削除してから、同じ URL を使用して別のテナントを作成する場合は、削除が完了するまで数時間待ってから、新規テナントを作成してください。

前提条件

システム管理者として vRealize Automation コンソールにログインします。

手順

- 1 [管理] - [テナント] を選択します。

2 削除するテナントを選択します。

テナントを選択する際には、実際の名前をクリックしないでください。実際の名前をクリックすると、テナントが編集用に開かれます。

3 [削除] をクリックします。

結果

これで、vRealize Automation 導入環境からテナントが削除されます。

マルチ テナントのセキュリティ設定

マルチ テナント環境のテナント間で共有される NSX セキュリティ オブジェクトの可用性を制御できます。

vRealize Automation で NSX セキュリティ オブジェクトを作成する際に、デフォルトの可用性をグローバル (関連付けられているエンドポイントが予約を持つすべてのテナントで使用可能)、または管理者以外のすべてのユーザーに非表示のいずれかにすることができます。

テナントで共有されるセキュリティ オブジェクトの可用性は、関連付けられているエンドポイントがテナントに予約または予約ポリシーを持つかどうかによって異なります。

テナント間で共有される新しいセキュリティ オブジェクトの可用性を制御する方法と、既存のセキュリティ オブジェクトの動作、クロステナント関連の動作、この vRealize Automation リリースへのアップグレード後の動作については、関連トピック [vRealize Automation でのセキュリティ オブジェクトへのテナント アクセスの制御](#)で説明しています。

カスタム ブランディングの構成

vRealize Automation では、テナントのログインページとアプリケーション ページにカスタム ブランディングを適用できます。

カスタム ブランディングには、テキストと背景の色、会社ロゴ、会社名、プライバシー ポリシー、著作権情報、テナントのログイン ページやアプリケーション ページに表示するその他の関連情報などを含めることができます。

テナント ログイン ページのカスタム ブランディング

[ログイン画面のブランディング] ページを使用して、カスタム ブランディングを vRealize Automation テナントのログイン ページに適用します。

テナント ログイン ページでデフォルトの vRealize Automation ブランディングを使用するか、[ログイン画面のブランディング] ページでカスタム ブランディングを構成することができます。カスタム ブランディングはすべてのテナント アプリケーションに同じように適用されることに注意してください。

このページでは、すべてのテナント ログイン ページのブランディングを構成できます。

[ログイン画面のブランディング] ページの [プレビュー] ペインには、現在実装されているテナントのログイン ブランディングが表示されます。

注： テナント ログイン ページの新しいブランディングを保存してからすべてのログイン ページに表示されるようになるまでに最大で 5 分の遅延が生じることがあります。

前提条件

カスタム ロゴまたはその他のイメージをブランディングで使用するには、該当する画像ファイルを用意しておく必要があります。

手順

- 1 vRealize Automation にシステムまたはテナント管理者としてログインします。
- 2 [管理] タブをクリックします。
- 3 [ブランディング] - [ログイン画面のブランディング] を選択します。
- 4 ロゴ イメージを追加するには、[ロゴ] フィールドの下にある [アップロード] ボタンをクリックして、該当するフォルダに移動し、ロゴのイメージ ファイルを選択します。
- 5 イメージを追加する場合は、[イメージ] (オプション) フィールドの [アップロード] をクリックし、該当するフォルダに移動して追加のイメージ ファイルを選択します。
- 6 背景の色をカスタマイズするには、[背景色]、[題字の色]、[ログイン ボタンの背景色]、[ログイン ボタンの前景色] フィールドに 16 進数コードを入力します。

必要に応じて、16 進数の色コードのリストをインターネットで検索します。
- 7 [保存] をクリックして、設定を適用します。

結果

テナント ユーザーのログイン ページにカスタム ブランディングが表示されます。

テナント アプリケーションのカスタム ブランディング

[アプリケーションのブランディング] ページを使用して、カスタム ブランディングを vRealize Automation テナント アプリケーションに適用します。

ユーザー アプリケーションでデフォルトの vRealize Automation ブランディングを使用するか、[アプリケーションのブランディング] ページでカスタム ブランディングを構成することができます。このページでは、アプリケーション ページのヘッダとフッタでブランディングを構成できます。カスタム ブランディングはすべてのユーザー アプリケーションに同じように適用されることに注意してください。

[アプリケーションのブランディング] ページの一番下には、ヘッダまたはフッタに現在実装されているブランディングが表示されます。

前提条件

ブランディングでカスタム ロゴを使用する場合、ロゴの画像ファイルを用意しておく必要があります。

手順

- 1 vRealize Automation にシステムまたはテナント管理者としてログインします。
- 2 [管理] タブをクリックします。
- 3 [ブランディング] - [アプリケーションのブランディング] を選択します。
- 4 [ヘッダー] タブがアクティブになっていない場合は、クリックします。

- 5 デフォルトの vRealize Automation ブランディングを使用する場合は、[デフォルトの使用] チェック ボックスをクリックします。
- 6 カスタム ブランディングを実装するには、[ヘッダー] タブと [フッター] タブのフィールドを適宜選択します。
 - a [ヘッダー ロゴ] フィールドの [参照] ボタンをクリックして、該当するフォルダに移動し、ロゴのイメージ ファイルを選択します。
 - b [会社名] フィールドに会社名を入力します。

マウス カーソルをロゴの上に移動すると、指定した名前が表示されます。
 - c [製品名] フィールドに製品名を入力します。

ここに入力した名前はロゴの隣にあるアプリケーション ヘッドに表示されます。
 - d [16 進数の背景色] フィールドにアプリケーションの外周の背景色にする 16 進数の色コードを入力します。

必要に応じて、16 進数の色コードのリストをインターネットで検索します。
 - e [16 進数のテキスト色] フィールドにテキストの色にする 16 進数のコードを入力します。

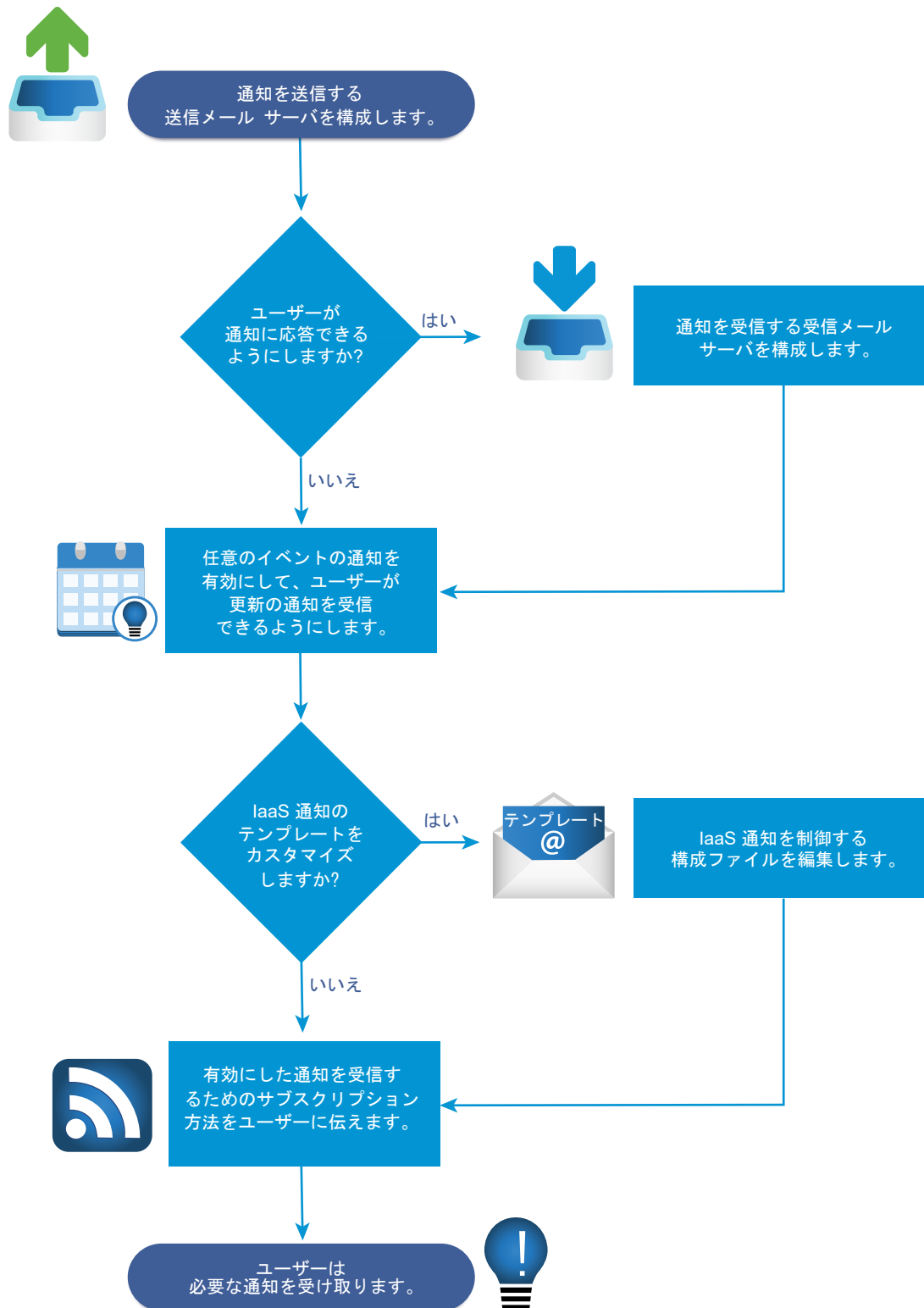
必要に応じて、16 進数のテキスト色コードのリストをインターネットで検索します。
 - f [次へ] をクリックして、[フッター] タブをアクティブにします。
 - g [著作権情報] フィールドに情報を入力します。
 - h [プライバシー ポリシー リンク] フィールドに会社のプライバシー ポリシー声明へのリンクを入力します。
 - i [お問い合わせリンク] フィールドに会社の連絡先情報を入力します。
- 7 [アップデート] をクリックして、ブランディング構成を実装します。

結果

テナント ユーザーのアプリケーション ページにカスタム ブランディングが表示されます。

通知構成のチェックリスト

特定のイベントの発生時にユーザー通知を送信するように vRealize Automation を構成できます。登録する通知を選択できますが、通知トリガーとして有効にするイベントからのみ選択できます。



通知構成のチェックリストには、通知を構成するために必要な一連の手順の概要と、各手順の判断ポイントまたは詳細な指示へのリンクがあります。

表 2-10. 通知構成のチェックリスト

タスク	必要なロール	詳細
<input type="checkbox"/> 通知を送信する送信メール サーバを構成します。	<ul style="list-style-type: none"> ■ システム管理者はデフォルトのグローバル サーバを構成します。 ■ テナント管理者は管理するテナント用のサーバを構成します。 	テナント用に初めてサーバを構成する場合は、 テナント固有の送信電子メール サーバの追加 を参照してください。デフォルトのグローバル サーバをオーバーライドする必要がある場合は、 システムのデフォルト送信電子メール サーバのオーバーライド を参照してください。すべてのテナントにグローバル デフォルト サーバを構成する場合は、 グローバル送信電子メール サーバの作成 を参照してください。
<input type="checkbox"/> (オプション) 受信メール サーバを構成して、タスクの実行に関する通知をユーザーが受信し、適切に対応できるようにします。	<ul style="list-style-type: none"> ■ システム管理者はデフォルトのグローバル サーバを構成します。 ■ テナント管理者は管理するテナント用のサーバを構成します。 	テナント用に初めてサーバを構成する場合は、 テナント固有の受信電子メール サーバの追加 を参照してください。 デフォルトのグローバル サーバをオーバーライドする必要がある場合は、 システムのデフォルト受信電子メール サーバのオーバーライド を参照してください。 すべてのテナントに対してグローバル デフォルト サーバを構成する場合は、 グローバル受信電子メール サーバの作成 を参照してください。
<input type="checkbox"/> (オプション) マシンの有効期限日の前に E メール通知をいつ送信するかを指定します。	システム管理者	マシン有効期限の E メール通知日付のカスタマイズ を参照してください。
<input type="checkbox"/> ユーザー通知をトリガーする vRealize Automation のイベントを選択します。通知トリガーとして有効にするイベントの通知のみを登録できます。	テナント管理者	通知の構成 を参照してください。
<input type="checkbox"/> (オプション) リースの有効期限など、マシンの所有者に送信されるマシン関連のイベント通知のテンプレートを構成します。	vRealize Automation サーバのインストール ディレクトリ (通常は %SystemDrive%\Program Files x86\VMware\VCAC\Server) 下のディレクトリ \Templates へのアクセス権を持つユーザーは、これらのメール通知のテンプレートを構成できます。	自動 IaaS 電子メールのテンプレートの構成 を参照してください。
<input type="checkbox"/> ユーザーは構成された通知に自動的に登録されます。 必要に応じて、有効にした通知の登録方法についての指示をユーザーに提供できます。自分のロールに関連する通知のみを登録することもできます。	すべてのユーザー	通知の登録 を参照してください。

通知用のグローバル電子メール サーバの構成

テナント管理者は、自身のテナントの通知構成の一部として電子メール サーバを追加できます。システム管理者として、すべてのテナントに対してシステム デフォルトとして表示される、グローバルな受信および送信電子メール サーバ

サーバを設定できます。通知を有効にする前に、テナント管理者がこれらの設定をオーバーライドしない場合、vRealize Automation はグローバルに構成された電子メール サーバを使用します。


グローバル受信電子メール サーバの作成

システム管理者は、承認応答などの受信電子メール通知を処理するために、グローバル受信電子メール サーバを作成できます。作成できる受信サーバは 1 台のみで、これはすべてのテナントにデフォルトとして表示されます。通知を有効にする前に、テナント管理者がこれらの設定をオーバーライドしない場合、vRealize Automation はグローバルに構成された電子メール サーバを使用します。

前提条件

システム管理者 として vRealize Automation コンソールにログインします。

手順

- 1 [管理] - [電子メール サーバ] を選択します。
- 2 [追加] アイコン () をクリックします。
- 3 [電子メール – 受信] を選択します。
- 4 [OK] をクリックします。
- 5 [名前] テキスト ボックスに名前を入力します。
- 6 (オプション) [説明] テキスト ボックスに説明を入力します。
- 7 (オプション) セキュリティに SSL を使用するには、[SSL] チェック ボックスを選択します。
- 8 サーバのプロトコルを選択します。
- 9 [サーバ名] テキスト ボックスにサーバの名前を入力します。
- 10 [サーバのポート] テキスト ボックスにサーバのポート番号を入力します。
- 11 [フォルダ名] テキスト ボックスに電子メールのフォルダ名を入力します。
このオプションは、IMAP サーバ プロトコルを選択した場合のみ必須です。
- 12 [ユーザー名] テキスト ボックスにユーザー名を入力します。
- 13 [パスワード] テキスト ボックスにパスワードを入力します。
- 14 vRealize Automation ユーザーが返信可能な電子メール アドレスを [電子メール アドレス] テキスト ボックスに入力します。
- 15 (オプション) [サーバから削除] を選択すると、通知サービスから取得した処理済みの電子メールがすべてサーバから削除されます。
- 16 vRealize Automation が電子メール サーバからの自己署名証明書を受け入れられるかどうかを選択します。
- 17 [テスト接続] をクリックします。
- 18 [追加] をクリックします。


グローバル送信電子メール サーバの作成

システム管理者は、送信電子メール通知を処理するために、グローバル送信電子メール サーバを作成できます。作成できる送信サーバは 1 台のみで、これはすべてのテナントにデフォルトとして表示されます。通知を有効にする前に、テナント管理者がこれらの設定をオーバーライドしない場合、vRealize Automation はグローバルに構成された電子メール サーバを使用します。

前提条件

システム管理者 として vRealize Automation コンソールにログインします。

手順

- 1 [管理] - [電子メール サーバ] を選択します。
- 2 [追加] アイコン () をクリックします。
- 3 [電子メール – 送信] を選択します。
- 4 [OK] をクリックします。
- 5 [名前] テキスト ボックスに名前を入力します。
- 6 (オプション) [説明] テキスト ボックスに説明を入力します。
- 7 [サーバ名] テキスト ボックスにサーバの名前を入力します。
- 8 暗号化方式を選択します。
 - [SSL の使用] をクリックします。
 - [TLS の使用] をクリックします。
 - [なし] をクリックすると、通信が暗号化されずに送信されます。
- 9 [サーバのポート] テキスト ボックスにサーバのポート番号を入力します。
- 10 (オプション) サーバで認証が必要な場合は、[必須] チェック ボックスを選択します。
 - a [ユーザー名] テキスト ボックスにユーザー名を入力します。
 - b [パスワード] テキスト ボックスにパスワードを入力します。
- 11 vRealize Automation の電子メールの発信元として表示する必要がある電子メール アドレスを [送信者アドレス] テキスト ボックスに入力します。
この電子メール アドレスは、指定したユーザー名とパスワードに対応します。
- 12 vRealize Automation が電子メール サーバからの自己署名証明書を受け入れられるかどうかを選択します。
- 13 [テスト接続] をクリックします。
- 14 [追加] をクリックします。

テナント固有の送信電子メール サーバの追加


テナント管理者は、送信電子メール サーバを追加して、承認などの作業アイテムの完了通知を送信できます。

各テナントに設定できる送信電子メール サーバは 1 つのみです。システム管理者がすでにグローバル送信電子メール サーバを構成している場合は、[システムのデフォルト送信電子メール サーバのオーバーライド](#)を参照してください。

前提条件

- テナント管理者として vRealize Automation にログインします。
- 電子メール サーバで認証が要求される場合、指定したユーザーは ID ストアおよびビジネス グループに存在している必要があります。

手順

- 1 [管理] - [通知] - [電子メール サーバ] を選択します。
- 2 [追加] アイコン () をクリックします。
- 3 [電子メール – 送信] を選択します。
- 4 [OK] をクリックします。
- 5 [名前] テキスト ボックスに名前を入力します。
- 6 (オプション) [説明] テキスト ボックスに説明を入力します。
- 7 [サーバ名] テキスト ボックスにサーバの名前を入力します。
- 8 暗号化方式を選択します。
 - [SSL の使用] をクリックします。
 - [TLS の使用] をクリックします。
 - [なし] をクリックすると、通信が暗号化されずに送信されます。
- 9 [サーバのポート] テキスト ボックスにサーバのポート番号を入力します。
- 10 (オプション) サーバで認証が必要な場合は、[必須] チェック ボックスを選択します。
 - a [ユーザー名] テキスト ボックスにユーザー名を入力します。
 - b [パスワード] テキスト ボックスにパスワードを入力します。
- 11 vRealize Automation の電子メールの発信元として表示する必要がある電子メール アドレスを [送信者アドレス] テキスト ボックスに入力します。
この電子メール アドレスは、指定したユーザー名とパスワードに対応します。
- 12 vRealize Automation が電子メール サーバからの自己署名証明書を受け入れられるかどうかを選択します。
このオプションは、暗号化を有効にした場合にのみ使用可能です。
 - 自己署名証明書を受け入れるには、[はい] をクリックします。
 - 自己署名証明書を拒否するには、[いいえ] をクリックします。
- 13 [テスト接続] をクリックします。
- 14 [追加] をクリックします。

テナント固有の受信電子メール サーバの追加


テナント管理者は、ユーザーが承認などの作業アイテムの完了通知に応答できるように、受信電子メール サーバを追加できます。

各テナントに設定できる受信電子メール サーバは 1 つのみです。システム管理者がすでにグローバル受信電子メール サーバを構成している場合は、[システムのデフォルト受信電子メール サーバのオーバーライド](#)を参照してください。

前提条件

- テナント管理者として vRealize Automation にログインします。
- 指定したユーザーが ID ストアおよびビジネス グループに存在していることを確認します。

手順

- 1 [管理] - [通知] - [電子メール サーバ] を選択します。
- 2 [追加] アイコン () をクリックします。
- 3 [電子メール - 受信] を選択し、[OK] をクリックします。
- 4 次の受信電子メール サーバ オプションを構成します。

オプション	アクション
[名前]	受信電子メール サーバの名前を入力します。
[説明]	受信電子メール サーバの説明を入力します。
[セキュリティ]	[SSL の使用] チェック ボックスを選択します。
[プロトコル]	サーバのプロトコルを選択します。
[サーバ名]	サーバ名を入力します。
[サーバのポート]	サーバのポート番号を入力します。

- 5 [フォルダ名] テキスト ボックスに電子メールのフォルダ名を入力します。
このオプションは、IMAP サーバ プロトコルを選択した場合のみ必須です。
- 6 [ユーザー名] テキスト ボックスにユーザー名を入力します。
- 7 [パスワード] テキスト ボックスにパスワードを入力します。
- 8 vRealize Automation ユーザーが返信可能な電子メール アドレスを [電子メール アドレス] テキスト ボックスに入力します。
- 9 (オプション) [サーバから削除] を選択すると、通知サービスから取得した処理済みの電子メールがすべてサーバから削除されます。
- 10 vRealize Automation が電子メール サーバからの自己署名証明書を受け入れられるかどうかを選択します。
このオプションは、暗号化を有効にした場合にのみ使用可能です。
 - 自己署名証明書を受け入れるには、[はい] をクリックします。
 - 自己署名証明書を拒否するには、[いいえ] をクリックします。

11 [テスト接続] をクリックします。

12 [追加] をクリックします。

システムのデフォルト送信電子メール サーバのオーバーライド

システム管理者がシステムのデフォルト送信電子メール サーバを構成している場合、テナント管理者はこのグローバル設定をオーバーライドすることができます。

前提条件

テナント管理者として vRealize Automation にログインします。

手順

1 [管理] - [通知] - [電子メール サーバ] を選択します。

2 送信電子メール サーバを選択します。

3 [グローバルをオーバーライド] をクリックします。

4 [名前] テキスト ボックスに名前を入力します。

5 (オプション) [説明] テキスト ボックスに説明を入力します。

6 [サーバ名] テキスト ボックスにサーバの名前を入力します。

7 暗号化方式を選択します。

- [SSL の使用] をクリックします。
- [TLS の使用] をクリックします。
- [なし] をクリックすると、通信が暗号化されずに送信されます。

8 [サーバのポート] テキスト ボックスにサーバのポート番号を入力します。

9 (オプション) サーバで認証が必要な場合は、[必須] チェック ボックスを選択します。

- a [ユーザー名] テキスト ボックスにユーザー名を入力します。
- b [パスワード] テキスト ボックスにパスワードを入力します。

10 vRealize Automation の電子メールの発信元として表示する必要がある電子メール アドレスを [送信者アドレス] テキスト ボックスに入力します。

この電子メール アドレスは、指定したユーザー名とパスワードに対応します。

11 vRealize Automation が電子メール サーバからの自己署名証明書を受け入れられるかどうかを選択します。

このオプションは、暗号化を有効にした場合にのみ使用可能です。

- 自己署名証明書を受け入れるには、[はい] をクリックします。
- 自己署名証明書を拒否するには、[いいえ] をクリックします。

12 [テスト接続] をクリックします。

13 [追加] をクリックします。

システムのデフォルト受信電子メール サーバのオーバーライド

システム管理者がシステムのデフォルト受信電子メール サーバを構成している場合、テナント管理者はこのグローバル設定をオーバーライドすることができます。

前提条件

テナント管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [通知] - [電子メール サーバ] を選択します。
- 2 [電子メール サーバ] テーブルで受信電子メール サーバを選択します。
- 3 [グローバルをオーバーライド] をクリックします。
- 4 次の受信電子メール サーバのオプションを入力します。

オプション	アクション
[名前]	受信電子メール サーバの名前を入力します。
[説明]	受信電子メール サーバの説明を入力します。
[セキュリティ]	セキュリティに SSL を使用するには、[SSL] チェック ボックスを選択します。
[プロトコル]	サーバのプロトコルを選択します。
[サーバ名]	サーバ名を入力します。
[サーバのポート]	サーバのポート番号を入力します。

- 5 [フォルダ名] テキスト ボックスに電子メールのフォルダ名を入力します。
このオプションは、IMAP サーバ プロトコルを選択した場合のみ必須です。
- 6 [ユーザー名] テキスト ボックスにユーザー名を入力します。
- 7 [パスワード] テキスト ボックスにパスワードを入力します。
- 8 vRealize Automation ユーザーが返信可能な電子メール アドレスを [電子メール アドレス] テキスト ボックスに入力します。
- 9 (オプション) [サーバから削除] を選択すると、通知サービスから取得した処理済みの電子メールがすべてサーバから削除されます。
- 10 vRealize Automation が電子メール サーバからの自己署名証明書を受け入れられるかどうかを選択します。
このオプションは、暗号化を有効にした場合にのみ使用可能です。
 - 自己署名証明書を受け入れるには、[はい] をクリックします。
 - 自己署名証明書を拒否するには、[いいえ] をクリックします。
- 11 [テスト接続] をクリックします。
- 12 [追加] をクリックします。

システム デフォルトの電子メール サーバに戻す

システムのデフォルト サーバをオーバーライドするテナント管理者が設定をグローバル設定に戻すことができます。

前提条件

テナント管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [通知] - [電子メール サーバ] を選択します。
- 2 デフォルトの設定に戻す電子メール サーバを選択します。
- 3 [グローバルに戻す] をクリックします。
- 4 [可] をクリックします。

通知の構成

通知を受信するかどうかは、各ユーザーが決定します。ただし、通知をトリガーするイベントは、テナント管理者が決定します。

前提条件

- テナント管理者として vRealize Automation にログインします。
- テナント管理者またはシステム管理者が送信電子メール サーバを構成していることを確認します。[テナント固有の送信電子メール サーバの追加](#)を参照してください。

手順

- 1 [管理] - [通知] - [シナリオ] を選択します。
- 2 1 つ以上の通知を選択します。
- 3 [有効化] をクリックします。

結果

これで、環境設定で通知を登録しているユーザーが、通知を受信するようになりました。

マシン有効期限の E メール通知日付のカスタマイズ

マシンの有効期限日の前に E メール通知をいつ送信するかを指定できます。

vRealize Automation が有効期限通知 E メールをマシンの有効期限日の何日前に送信するかを定義する設定を変更できます。この E メールは、マシンの有効期限日をユーザーに通知します。デフォルトの設定は、マシンの有効期限の 7 日前です。

手順

- 1 管理アクセス権が付与されている認証情報を使用して vRealize Automation サーバにログインします。
- 2 `/etc/vcac/setenv-user` ファイルを開きます。

- 3 次の行をファイルに追加して、マシンの有効期限の何日前に通知するかを指定します。ここで、この例の 3 は、マシンの有効期限の 3 日前を指定します。

```
VCAC_OPTS="$VCAC_OPTS -Dlease.enforcement.prearchive.notification.days=3"
```

- 4 次のコマンドを実行して、仮想アプライアンス上の vCAC サービスを再起動します。

```
service vcac-server restart
```

次のステップ

高可用性ロード バランサ環境で作業している場合は、HA 環境内のすべての仮想アプライアンスに対してこの手順を繰り返します。

自動 IaaS 電子メールのテンプレートの構成

マシンの所有者に、そのマシンに関連するさまざまな vRealize Automation イベントについて通知メールを送信するように構成できます。

通知をトリガするイベントには、アーカイブ期間や仮想マシン リースの有効期限切れまたは有効期限日の接近などがあります。

vRealize Automation E メール通知の構成、有効化、無効化の詳細については、次のブログ記事およびナレッジベース記事を参照してください。

- [vRealize Automation での E メールのカスタマイズ](#)
- [Customizing email templates in vRealize Automation \(2088805\)](#)
- [Examples for customizing email templates in vRealize Automation \(2102019\)](#)

通知の登録

管理者が通知を構成している場合は、自動的に登録されます。通知イベントには、カタログ申請または必要な承認の正常終了を含めることができます。

手動で登録する必要がある場合は、通知を有効にできます。

前提条件

vRealize Automation にログインします。

手順

- 1 [環境設定] をクリックします。
- 2 通知テーブルの電子メール プロトコルに対して [有効] チェック ボックスを選択します。
- 3 [適用] をクリックします。
- 4 [閉じる] をクリックします。

プロビジョニングされたマシンで RDP 接続をサポートするためのカスタム RDP ファイルの作成

システム管理者は、RDP 設定を構成するために IaaS アーキテクトがブループリントで使用するカスタム リモート デスクトップ プロトコル ファイルを作成します。RDP ファイルを作成し、ファイルのフル パス名をアーキテクト に提供して、アーキテクトがファイルをブループリントに含められるようにします。カタログ管理者はその後、RDP アクションの権限をユーザーに付与します。

注： セキュリティ強化の構成が有効にされた Internet Explorer を使用している場合、.rdp ファイルはダウンロードできません。

前提条件

IaaS Manager Service に管理者としてログインします。

手順

- 1 現在のディレクトリを `<vRA_installation_dir>\Rdp` に設定します。
- 2 ファイル `Default.rdp` をコピーし、同じディレクトリで `Console.rdp` という名前に変更します。
- 3 エディタで `Console.rdp` ファイルを開きます。
- 4 RDP 設定をファイルに追加します。

例： **connect to console:i:1**

- 5 分散環境で作業している場合は、Model Manager Web サイト コンポーネントがインストールされている IaaS ホスト マシンに管理者権限を持つユーザーとしてログインします。
- 6 `Console.rdp` ファイルをディレクトリ `vRA_installation_dir\Server\Website\Rdp` にコピーします。
- 7 ブループリントに `VirtualMachine.Rdp.File` カスタム プロパティを追加します。

IaaS アーキテクトは RDP カスタム プロパティを Windows マシン ブループリントに追加することができます。カタログ管理者はその後、[RDP を使用して接続] アクションの使用資格をユーザーに付与できます。

[Windows マシン ブループリントへの RDP 接続サポートの追加](#)を参照してください。

シナリオ：複数の拠点にまたがる導入環境向けにデータセンターの場所を追加する

システム管理者がボストンとロンドンのデータセンターの場所を定義したい場合、ファブリック管理者が各データセンターのコンピュー ト リソースに対して、それぞれ場所を定義できます。ブループリント アーキテクトがブループリントを作成する際、場所の機能を有効にできるため、ユーザーがカタログ アイテム申請フォームを入力した場合、プロビジョニング対象として、ボストンまたはロンドンのマシンを選択できるようになります。

データセンターはロンドンとボストンにあります。また、ボストンにいるユーザーにはロンドンのインフラストラクチャでマシンをプロビジョニングできないようにし、一方でロンドンにいるユーザーにはボストンのインフラストラクチャでマシンをプロビジョニングできないようにします。必ず、ボストンのユーザーはボストンのインフラストラクチャでプロビジョニングを行い、ロンドンのユーザーはロンドンのインフラストラクチャでプロビジョニングを行うようにすることで、ユーザーがマシンを申請するときにプロビジョニングに適切な場所を選択できるようにします。



xml ファイル内のデータセンターの場所を、テナントまたはビジネス グループに基づいてフィルタすることはできません。マルチテナント環境の場合、プロパティ定義を使用すると、テナントまたはビジネス グループに基づいてフィルタすることができます。プロパティ定義の使用の詳細については、ブログ記事「[How to use dynamic property definitions](#)」を参照してください。

手順

- 1 管理者の認証情報を使用して IaaS Web サーバ ホストにログインします。
これは、IaaS Web サイト コンポーネントをインストールしたマシンです。
- 2 Windows サーバのインストール ディレクトリ（通常は %SystemDrive%\Program Files x86\VMware \vCAC\Server）にあるファイル WebSite\XmlData\DataCenterLocations.xml を編集します。
- 3 ファイルの CustomDataType セクションを編集して、場所ごとに Data Name エントリを作成します。

```
<CustomDataType>
  <Data Name="London" Description="London datacenter" />
  <Data Name="Boston" Description="Boston datacenter" />
</CustomDataType>
```

- 4 ファイルを保存して閉じます。
- 5 Manager Service を再起動します。
- 6 1 台以上の IaaS Web サーバ ホストがある場合は、冗長構成の各インスタンスに対してこの手順を繰り返します。

結果

ファブリック管理者は、各データセンターに配置されたコンピュート リソースに対して、適切な場所を適用できるようになります。[シナリオ：地域間展開のためにコンピュート リソースに場所を適用する](#) を参照してください。

次のステップ

Vrm.DataCenter.Location プロパティをブループリントに追加するか、またはブループリントの [申請時の場所を表示] オプションを有効にすることで、ユーザーからマシンのプロビジョニングが申請されたときにデータセンターの場所を指定するようユーザーに求めることができます。

vRealize Orchestrator の設定

vRealize Orchestrator は自動化と管理エンジンであり、vRealize Automation を拡張して XaaS と他の拡張性をサポートします。vRealize Automation アプライアンスで事前構成された vRealize Orchestrator サーバを

構成して使用することも、外部サーバインスタンスとして vRealize Orchestrator を展開して、その外部インスタンスと vRealize Automation を関連付けることもできます。

vRealize Orchestrator により、管理者およびアーキテクトは、ワークフロー デザイナを使用して複雑な自動化タスクを作成し、vRealize Automation からワークフローにアクセスして実行できます。

vRealize Orchestrator は、vRealize Orchestrator プラグインを使用することで、外部のテクノロジーおよびアプリケーションにアクセスして制御することができます。

vRealize Orchestrator を使用するように vRealize Automation を構成すると、XaaS ブループリント管理の一環として、vRealize Orchestrator ワークフローを vRealize Orchestrator サービス カタログに公開できます。

IaaS マシンの管理を拡張するためにワークフローを実行する場合は、vRealize Orchestrator をエンドポイントとして構成する必要があります。

構成権限

システム管理者およびテナント管理者は、外部サーバまたは組み込みの vRealize Orchestrator サーバを使用するように vRealize Automation を構成できます。

さらに、システム管理者は各テナントに使用可能なワークフロー フォルダを決定することもできます。

テナント管理者は vRealize Orchestrator プラグインをエンドポイントとして構成できます。

ロール	vRealize Orchestrator 関連の構成権限
システム管理者	<ul style="list-style-type: none"> ■ すべてのテナントに対し vRealize Orchestrator サーバを構成します。 ■ テナントごとにデフォルトの vRealize Orchestrator ワークフロー フォルダを定義します。
テナント管理者	<ul style="list-style-type: none"> ■ 固有のテナントに対し vRealize Orchestrator サーバを構成します。 ■ vRealize Orchestrator プラグインをエンドポイントとして追加します。

組み込み vRealize Orchestrator サーバの構成

vRealize Automation アプライアンスには事前構成された vRealize Orchestrator のインスタンスが含まれています。

前提条件

vRealize Automation アプライアンスを展開します。詳細については、『vRealize Automation のインストール』の「vRealize Automation アプライアンスの展開」を参照してください。

手順

- 1 システム管理者またはテナント管理者として vRealize Automation コンソールにログインします。
- 2 [管理] - [VRO 構成] - [サーバ構成] を選択します。
- 3 [デフォルトの Orchestrator サーバを使用します] をクリックします。

結果

組み込みの vRealize Orchestrator サーバへの接続が構成されました。[vCAC] ワークフロー フォルダおよび関連するユーティリティ アクションが自動的にインポートされます。[vCAC] - [ASD] ワークフロー フォルダには、エンドポイントを構成し、リソース マッピングを作成するためのワークフローが含まれます。

vRealize Orchestrator コントロール センターへのログイン

vRealize Automation に組み込みのデフォルトの vRealize Orchestrator インスタンスの構成を編集するには、vRealize Orchestrator コントロール センターにログインする必要があります。

組み込みの vRealize Orchestrator インスタンスの構成サービスが自動的に開始されます。

注: vRealize Orchestrator Appliance コマンドライン コンソールから `chkconfig vco-configurator` コマンドを実行して、構成が自動的に開始することを確認できます。サービスから `off` が報告される場合は、`chkconfig vco-configurator on` コマンドを実行し、アプライアンスを再起動します。

手順

- 1 Web ブラウザで vRealize Automation の URL に接続します。
- 2 [vRealize Orchestrator コントロール センター] をクリックします。
`https://vra-vr-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter` にリダイレクトされます。
- 3 vRealize Automation 環境のルート認証情報を入力します。

vRealize Orchestrator クライアントへのログイン

デフォルトの vRealize Orchestrator インスタンスで一般的な管理タスクの実行またはワークフローの編集と作成を行うには、vRealize Orchestrator クライアントにログインする必要があります。

vRealize Orchestrator クライアント インターフェイスは、ワークフロー、アクション、および他のカスタム要素を開発するための管理権限を持つ開発者向けに設計されています。

手順

- 1 Web ブラウザで vRealize Automation の URL に接続します。
- 2 [vRealize Orchestrator クライアント] をクリックします。
クライアント ファイルがダウンロードされます。
- 3 ダウンロードをクリックし、プロンプトの指示に従います。
- 4 [セキュリティ警告]ウィンドウで、証明書の警告を処理するためのオプションを選択します。

vRealize Orchestrator クライアントは、SSL 証明書を使用して vRealize Orchestrator サーバと通信します。信頼性のある CA が、インストール中に証明書に署名することはありません。vRealize Orchestrator サーバに接続するたびに、セキュリティ警告を受け取ります。

オプション	説明
続行	現在の SSL 証明書を使用して続行します。 同一の vRealize Orchestrator サーバに再接続した場合またはリモート vRealize Orchestrator サーバを使用してワークフローを同期しようとした場合、警告メッセージがもう一度表示されます。
キャンセル	ウィンドウを閉じて、ログイン プロセスを停止します。

デフォルトの SSL 証明書を CA により署名された証明書に変更できます。SSL 証明書の変更に関する詳細については、『VMware vRealize Orchestrator のインストールおよび構成』を参照してください。

5 [実行] をクリックします。

6 vRealize Orchestrator ログイン ページで、[ホスト名] テキスト ボックスに vRealize Automation アプライアンスの IP アドレスまたはドメイン名、さらにデフォルトのポート番号に **443** を入力します。

たとえば、`vrealize_automation_appliance_ip:443` を入力します。

7 vRealize Orchestrator クライアントのユーザー名とパスワードを入力し、[ログイン] をクリックします。

認証情報は、デフォルト テナント管理者のユーザー名およびパスワードです。

次のステップ

システム上でのパッケージのインポート、ワークフローの作成、または root アクセス権限の設定を行うことができます。『VMware vRealize Orchestrator クライアントの使用』 および 『VMware vRealize Orchestrator を使用した開発』を参照してください。

外部 vRealize Orchestrator サーバの構成

外部 vRealize Orchestrator サーバを使用するように vRealize Automation を設定できます。

システム管理者は、すべてのテナントに対してデフォルトの vRealize Orchestrator サーバをグローバルに構成できます。テナント管理者は、自分のテナントに対してのみ vRealize Orchestrator サーバを構成できます。

外部 vRealize Orchestrator サーバ インスタンスに接続するには、vRealize Orchestrator でユーザー アカウントに表示権限と実行権限を付与する必要があります。

- Single Sign-On 認証。ユーザー情報は XaaS 申請と共に vRealize Orchestrator に送られ、申請対象のワークフローの表示権限と実行権限がユーザーに付与されます。
- 基本認証。指定するユーザー アカウントは、表示権限と実行権限を持つ vRealize Orchestrator グループのメンバーまたは vcoadmins グループのメンバーである必要があります。

前提条件

- 外部の vRealize Orchestrator アプライアンスをインストールして構成します。[vRealize Orchestrator 製品のドキュメント](#)の「vRealize Orchestrator のインストールおよび構成」を参照してください。
- システム管理者またはテナント管理者として vRealize Automation コンソールにログインします。

手順

- 1 [管理] - [vRO 構成] - [サーバ構成] を選択します。
- 2 [外部 Orchestrator サーバを使用します] をクリックします。
- 3 名前と説明（説明は任意）を入力します。

- 4 [ホスト] テキスト ボックスに、vRealize Orchestrator サーバが実行されているマシンの IP アドレスまたは DNS 名を入力します。

注： 外部 vRealize Orchestrator がクラスタ モードで動作するように設定されている場合は、クラスタ内の vRealize Orchestrator サーバにクライアント要求を分散するロード バランサ仮想サーバの IP アドレスまたはホスト名を入力します。

- 5 [ポート] テキスト ボックスに、外部 vRealize Orchestrator サーバと通信するポート番号を入力します。
vRealize Orchestrator のデフォルト ポートは 8281 です。
- 6 認証タイプを選択します。

オプション	説明
Single Sign On	vCenter Single Sign-On を使用して、vRealize Orchestrator サーバに接続します。 このオプションは、共通の vRealize Orchestrator インスタンスを使用するように vRealize Automation と vCenter Single Sign-On を設定した場合にのみ適用されます。
基本	[ユーザー名] および [パスワード] テキスト ボックスに入力したユーザー名とパスワードで、vRealize Orchestrator サーバに接続します。 使用するユーザー アカウントは、vRealize Orchestrator vcoadmins グループのメンバー、または表示権限と実行権限を持つグループのメンバーである必要があります。

- 7 [テスト接続] をクリックします。
- 8 [OK] をクリックします。
- 9 `xaas.package` パッケージをインポートします。
 - a vRealize Automation アプライアンスに root としてログインします。
 - b `/usr/lib/vcac/content/o11n/` フォルダ内で `xaas.package` パッケージを見つけます。
 - c `xaas.package` パッケージを外部クライアントにインポートします。

結果

外部 vRealize Orchestrator サーバへの接続が構成され、[vCAC] ワークフロー フォルダおよび関連するユーティリティ アクションがインポートされました。[vCAC] - [ASD] ワークフロー フォルダには、エンドポイントを構成し、リソース マッピングを作成するためのワークフローが含まれます。

次のステップ

[vRealize Orchestrator クライアントへのログイン](#)。

リソースの構成

エンドポイント、予約、ネットワーク プロファイルなどのリソースを、vRealize Automation のブループリント定義およびマシン プロビジョニングをサポートするように構成できます。

laaS リソース設定のチェックリスト

laaS 管理者とファブリック管理者は、laaS リソースを設定して既存のインフラストラクチャを vRealize Automation と統合し、インフラストラクチャ リソースを vRealize Automation ビジネス リソースに割り当てます。

laaS リソースの設定チェックリストを使用すると、laaS リソースの設定に必要な手順の概要を表示できます。



表 2-11. laaS リソース設定のチェックリスト

タスク	vRealize Automation ロール	詳細
<input type="checkbox"/> インフラストラクチャのエンドポイントを作成し、vRealize Automation の管理下にリソースを置きます。	laaS 管理者	エンドポイント シナリオの選択.
<input type="checkbox"/> ファブリック グループを作成してインフラストラクチャ リソースをグループに編成し、リソース管理のために 1 人以上の vRealize Automation ファブリック管理者を指定します。	laaS 管理者	ファブリック グループの作成.
<input type="checkbox"/> vRealize Automation を介してプロビジョニングされたマシン名の作成に使用するマシン プリフィックスを設定します。	ファブリック管理者	マシン プリフィックスの構成.
<input type="checkbox"/> (オプション) ネットワーク プロファイルを作成し、プロビジョニングされたマシンのネットワーク設定を行います。	ファブリック管理者	ネットワーク プロファイルの作成.
<input type="checkbox"/> 予約を作成、または必要に応じて予約およびストレージ予約のプロファイルを作成し、インフラストラクチャ リソースをビジネス グループに割り当てます。	■ ファブリック管理者としても設定されている場合は、laaS 管理者 ■ ファブリック管理者	予約と予約ポリシーの設定.

エンドポイントの設定

vRealize Automation とインフラストラクチャ間の通信を可能にするエンドポイントを作成して設定します。

エンドポイントはタイプに応じたカテゴリに分けられます。

- クラウド

クラウド カテゴリには、vCloud Air、vCloud Director、Amazon EC2、および OpenStack の各エンドポイント タイプが含まれます

■ IP アドレス管理

このカテゴリは、vRealize Orchestrator ワークフローで、Infoblox IP アドレス管理などのサードパーティの IP アドレス管理エンドポイント タイプを登録した場合にのみ表示されます。

■ 管理

このカテゴリには、vRealize Operations Manager エンドポイントのみが含まれます。

■ ネットワークおよびセキュリティ

このカテゴリには、プロキシおよび NSX の各エンドポイント タイプが含まれます。

プロキシ エンドポイントは、Amazon、vCloud Air、または vCloud Director のエンドポイントに関連付けることができます。

NSX エンドポイントは、vSphere エンドポイントに関連付けることができます。

■ オーケストレーション

このカテゴリには、vRealize Orchestrator エンドポイントのみが含まれます。

■ ストレージ

このカテゴリには、NetApp ONTAP エンドポイントが含まれます。

■ 仮想

仮想カテゴリには、vSphere、Hyper-V (SCVMM)、および KVM (RHEV) の各エンドポイント タイプが含まれます。

vRealize Orchestrator で追加のエンドポイント タイプを構成し、vRealize Automation でサポートされているエンドポイント タイプとともに使用できます。プログラムによってエンドポイントをインポートおよびエクスポートすることもできます。

アップグレード後または移行後のエンドポイントの使用については、[アップグレードまたは移行されたエンドポイントを使用する場合の考慮事項](#)を参照してください。

エンドポイント シナリオの選択

ターゲットのエンドポイント タイプに基づいてエンドポイント シナリオを選択します。

使用可能なエンドポイントの設定については、[エンドポイント設定リファレンス](#)を参照してください。

表 2-12. エンドポイント シナリオの選択

エンドポイント	詳細情報
vSphere	vSphere エンドポイントの作成 を参照してください。
NSX	NSX for vSphere エンドポイントの作成と vSphere エンドポイントへの関連付け または NSX-T エンドポイントの作成と vSphere エンドポイントへの関連付け を参照してください。
vCloud Air (サブスクリプションまたはオンデマンド)	vCloud Air エンドポイントの作成 を参照してください。

表 2-12. エンドポイント シナリオの選択 (続き)

エンドポイント	詳細情報
vCloud Director	vCloud Director エンドポイントの作成 を参照してください。
vRealize Orchestrator	vRealize Orchestrator エンドポイントの作成 を参照してください。
vRealize Operations	vRealize Operations Manager エンドポイントの作成 を参照してください。
サードパーティの IP アドレス管理プロバイダ	サードパーティの IP アドレス管理プロバイダ エンドポイントの作成 を参照してください。
Microsoft Azure	Microsoft Azure エンドポイントの作成 を参照してください。
Puppet	Puppet エンドポイントの作成 を参照してください。
Amazon	Amazon エンドポイントの作成 および Amazon インスタンス タイプの追加 を参照してください。
OpenStack	OpenStack エンドポイントの作成 を参照してください。
プロキシ	プロキシ エンドポイントの作成とクラウド エンドポイントへの関連付け
Hyper-V (SCVMM)	Hyper-V (SCVMM) エンドポイントの作成 を参照してください。
KVM (RHEV)	エンドポイント設定リファレンス を参照してください。
NetApp ONTAP	仮想プロビジョニング用として容量を効率的に利用したストレージおよびエンドポイント設定リファレンス を参照してください。
Hyper-v (スタンドアロン)、XenServer、または Xen プール マスター	Hyper-V、XenServer、または Xen プール エンドポイントの作成 を参照してください。
エンドポイントのインポート	プログラムによるエンドポイントのインポートまたはエクスポート を参照してください。

エンドポイント設定リファレンス

エンドポイント設定を使用して、データ収集およびサービス カタログ展開の場所とアクセス認証情報を定義します。

[全般] タブ

ほとんどの vRealize Automation エンドポイントには、次のオプションが含まれています。特定のエンドポイント タイプに固有の設定も、併せて記載しています。

表 2-13. [全般] タブの設定

設定	説明
[名前]	エンドポイント名を入力します。
[説明]	エンドポイントの説明を入力します。

表 2-13. [全般] タブの設定（続き）

設定	説明
[アドレス]	<p>エンドポイント固有のアドレス形式を使用して、エンドポイント アドレスを入力します。</p> <ul style="list-style-type: none"> ■ KVM (RHEV) または NetApp ONTAP エンドポイントの場合、アドレスは次のいずれかの形式である必要があります。 <ul style="list-style-type: none"> ■ <code>https://FQDN</code> ■ <code>https://IP_address</code> <p>例: <code>https://mycompany-kvmrhev1.mycompany.local</code> または <code>netapp-1.mycompany.local</code>。</p> ■ OpenStack エンドポイントの場合、アドレスは <code>https:// FQDN/powervc/ openstack/ service</code> という形式にする必要があります。たとえば、<code>https://openstack.mycompany.com/powervc/openstack/admin</code> のように指定します。 ■ OpenStack エンドポイントの場合、アドレスは次のいずれかの形式である必要があります。 <ul style="list-style-type: none"> ■ <code>https://FQDN:500</code> ■ <code>https://IP_address:500</code> ■ vSphere エンドポイントの場合、アドレスは <code>https://host/sdk</code> という形式である必要があります。 ■ NSX エンドポイントの場合、アドレスは <code>https://host</code> という形式である必要があります。 ■ vRealize Orchestrator エンドポイントの場合、アドレスは https プロトコルで、vRealize Orchestrator サーバの完全修飾名または IP アドレス、および vRealize Orchestrator ポート番号が含まれている必要があります (例: <code>https://vrealize-automation-appliance-hostname:443/vco</code>)。 ■ vRealize Operations エンドポイントの場合、アドレスは <code>https://host/suite-api</code> という形式である必要があります。
[組み込みの認証情報]	<p>vSphere の組み込みの認証情報を使用する場合は、ユーザー名とパスワードを入力する必要はありません。</p> <p>この設定は、vSphere エンドポイントのみに適用されます。</p>
[ユーザー名]	<p>ユーザー インターフェイスで提案されているとおりに、エンドポイント固有の形式でエンドポイント用に保存した管理者レベルのユーザー名を入力します。</p>
[パスワード]	<p>エンドポイントの認証情報として保存した、管理者権限を持つユーザーのパスワードを入力します。</p>
[OpenStack プロジェクト]	<p>OpenStack テナント名を入力します。</p> <p>この設定は、OpenStack エンドポイントのみに適用されます。</p>
[組織]	<p>組織の管理者である場合は、vCloud Director 組織名を入力できます。</p> <p>この設定は、vCloud Director のみに適用されます。</p>
[アクセス キーの ID]	<p>Amazon AWS キー ID を入力します。</p> <p>この設定は、Amazon AWS のエンドポイントのみに適用されます。</p>
[プライベート アクセス キー]	<p>Amazon AWS プライベート アクセス キーを入力します。</p> <p>この設定は、Amazon のエンドポイントのみに適用されます。</p>

表 2-13. [全般] タブの設定（続き）

設定	説明
[ポート]	プロキシ エンドポイント アドレスに接続するためのポート値を入力します。 この設定は、プロキシ エンドポイントのみに適用されます。
[優先度]	優先度の値を、1 以上の整数値で入力します。値が小さいほど、優先度が高くなります。 優先度の値は、組み込みの VMware.VCenterOrchestrator.Priority カスタム プロパティに関連付けられます。 この設定は、vRealize Orchestrator エンドポイントのみに適用されます。

[プロパティ] タブ

すべてのエンドポイント タイプで、[プロパティ] タブを使用して、カスタム プロパティまたはプロパティ グループ、および設定をキャプチャします。特定のエンドポイント タイプのカスタム プロパティの例については、『カスタム プロパティのリファレンス』を参照してください。

[関連付け] タブ

関連付け元のエンドポイントに応じて、NSX エンドポイントまたはプロキシ エンドポイントへの関連付けを作成できます。vSphere エンドポイントを NSX エンドポイントに関連付け、NSX 設定を vSphere エンドポイントに割り当てることができます。また、vCloud Air、vCloud Director、または Amazon のエンドポイントをプロキシ エンドポイントに関連付け、プロキシ設定を vCloud Air、vCloud Director、または Amazon のエンドポイントに割り当てることができます。

接続をテスト

テスト接続アクションを使用すると、証明書、ホスト エンドポイント アドレス、vSphere、NSX、または vRealize Operations Manager エンドポイントの証明書を検証できます。[テスト接続を使用する場合の考慮事項](#)を参照してください。

vSphere エンドポイントの作成

エンドポイントを作成して、vRealize Automation が vSphere 環境と通信し、コンピュート リソースの検出、データの収集、およびマシンのプロビジョニングを実行できるようにします。NSX for vSphere または NSX-T エンドポイントに関連付けることで、必要に応じて、NSX 設定を vSphere エンドポイントに関連付けることができます。

NSX マネージャを使用していた vSphere エンドポイントをアップグレードまたは移行した場合、ソース vSphere エンドポイントと新しい NSX エンドポイントとの間の関連付けを含む新しい NSX エンドポイントが作成されません。

vSphere 環境が NSX for vSphere または NSX-T と統合されている場合は、[NSX for vSphere エンドポイントの作成と vSphere エンドポイントへの関連付け](#)または [NSX-T エンドポイントの作成と vSphere エンドポイントへの関連付け](#)を参照してください。

NSX-T エンドポイントは、vRealize Automation 内の複数の vSphere エンドポイントに関連付けることができます。ただし、vSphere エンドポイントは、NSX for vSphere エンドポイントと NSX-T エンドポイントのどちらか 1 つの NSX にのみ関連付けることができます。

エンドポイント接続および証明書の信頼性を検証する方法の詳細については、[テスト接続を使用する場合の考慮事項](#)を参照してください。

前提条件

- IaaS 管理者として vRealize Automation にログインします。
- vSphere プロキシ エージェントをインストールして、vSphere エンドポイントを管理する必要があり、エンドポイントとエージェントにはまったく同じ名前を使用します。エージェントのインストールについての詳細は、vRealize Automation のインストールを参照してください。
- vSphere エンドポイントを使用して OVF テンプレートから仮想マシンを展開する場合、エンドポイントに関連付けられている vCenter Server で、認証情報に vSphere 権限 VApp.Import が含まれていることを確認します。

VApp.Import 権限では、OVF からインポートした設定を使用して vSphere マシンを展開することができます。vSphere 権限の詳細は、[vSphere SDK のドキュメント](#)に記載されています。

OVF が Web サイトでホストされている場合は、[OVF ホスト Web サイトへのプロキシ エンドポイントの作成](#)を参照してください。

- vSphere エンドポイントに対して追加の NSX ネットワークおよびセキュリティを設定する場合は、NSX アプリケーションの種類に応じて、NSX for vSphere または NSX-T エンドポイントを作成します。vSphere エンドポイントを作成するときに、NSX エンドポイントに関連付けることができます。

手順

- 1 [インフラストラクチャ] - [エンドポイント] - [エンドポイント] を選択します。

- 2 [新規] - [仮想] - [vSphere] を選択します。

- 3 [名前] テキスト ボックスに名前を入力します。

名前は、インストールまたはデータ収集が失敗した場合に vSphere プロキシ エージェントに提供されるエンドポイント名と一致する必要があります。

- 4 (オプション) [説明] テキスト ボックスに説明を入力します。

- 5 [アドレス] テキスト ボックスに vCenter Server インスタンスの URL を入力します。

URL は次のように入力する必要があります。 **https://hostname/sdk** または **https://IP_address/sdk**

たとえば、**https://vsphereA/sdk** と入力します。

- 6 vSphere 管理者レベルのユーザー名とパスワードを入力するか、代わりに、vSphere の組み込みの認証情報を使用します。

カスタム属性の変更権限を持つ認証情報を入力します。

ユーザー名の形式は、*domain \username* です。

[統合認証情報を使用] を選択して、vSphere プロキシ エージェントのサービス アカウントを使用して vCenter Server に接続します。

vSphere の組み込みの認証情報を使用する場合は、ユーザー名とパスワードを入力する必要はありません。

- 7 (オプション) [プロパティ] をクリックし、提供されたカスタム プロパティ、プロパティ グループ、またはエンドポイント用の独自のプロパティ定義を追加します。

- 8 (オプション) エンドポイントの NSX ネットワークおよびセキュリティを設定するには、[関連付け] をクリックして既存の NSX for vSphere または NSX-T エンドポイントに関連付けます。

関連付けを作成するには、少なくとも 1 つの NSX エンドポイントが必要です。

- 9 (オプション) [接続をテスト] をクリックして、認証情報、ホスト エンドポイント アドレス、証明書の信頼性を検証します。このアクションは、エンドポイントをデータ収集できるように、マネージャ サービスとエージェントが実行されていることもチェックします。[OK] アクションは、これらと同一の条件をテストします。

[接続をテスト] アクションは、次のいずれかの条件に関する情報を返します。

- 証明書エラー

証明書が見つからない場合、信頼済みの場合、または期限が切れている場合は、証明書のサムプリントを受け入れるよう求められます。サムプリントを受け入れない場合でも、エンドポイントを保存することはできますが、マシンのプロビジョニングが失敗する場合があります。

- エージェント エラー

関連付けられた vSphere エージェントが見つかりませんでした。テストを成功させるには、エージェントが実行されている必要があります。

- ホスト エラー

指定されたエンドポイント アドレスにアクセスできないか、関連付けられているマネージャ サービスが実行されていません。テストを成功させるには、マネージャ サービスが実行されている必要があります。

- 認証情報エラー

指定されたアドレスにあるエンドポイントでは、指定されたユーザー名とパスワードの組み合わせが正しくありません。

- Timeout

許容時間の 2 分以内にテスト アクションを完了できませんでした。

[接続をテスト] アクションが失敗した場合でも、エンドポイントを保存することはできますが、マシンのプロビジョニングが失敗する場合があります。

信頼された証明書に、証明書の期限が切れているなどの問題がある場合は、証明書のサムプリントを受け入れるよう求められます。

- 10 [OK] をクリックしてエンドポイントを保存します。

[OK] アクションは、[接続のテスト] アクションと同じ条件でテストします。上記の条件のいずれかが見つかり、メッセージを返します。保存できた場合は、確認のためにエラーが画面に表示されたままになります。

結果

vRealize Automation では、エンドポイントからデータを収集して、コンピューティング リソースを検出します。

注： 初回のデータ収集後に vSphere データセンターの名前を変更すると、プロビジョニングに失敗する場合があります。

初期データ収集後に既存エンドポイントのデータ収集を実行する方法については、[エンドポイントのソースおよび実行中のデータ収集の確認](#)を参照してください。

次のステップ

エンドポイントからファブリック グループにコンピュート リソースを追加します。[ファブリック グループの作成](#)を参照してください。

NSX for vSphere エンドポイントの作成と vSphere エンドポイントへの関連付け

NSX for vSphere エンドポイントを作成して既存の vSphere エンドポイントに関連付けることができます。

NSX マネージャを使用していた vSphere エンドポイントをアップグレードまたは移行した場合、ソース vSphere エンドポイントと新しい NSX エンドポイントとの間の関連付けを含む新しい NSX エンドポイントが作成されます。

NSX-T エンドポイントは、vRealize Automation 内の複数の vSphere エンドポイントに関連付けることができます。ただし、vSphere エンドポイントは、NSX for vSphere エンドポイントと NSX-T エンドポイントのどちらか 1 つの NSX にのみ関連付けることができます。

エンドポイントの作成時に NSX 接続および証明書の信頼性を検証する方法については、[テスト接続を使用する場合の考慮事項](#)を参照してください。

前提条件

- IaaS 管理者として vRealize Automation にログインします。
- vSphere プロキシ エージェントをインストールして、vSphere エンドポイントを管理する必要があり、エンドポイントとエージェントにはまったく同じ名前を使用します。エージェントのインストールについての詳細は、vRealize Automation のインストールを参照してください。
- NSX for vSphere ネットワークを設定します。[ネットワークおよびセキュリティ コンポーネントの設定](#)を参照してください。
- [vSphere エンドポイントの作成](#)。

vRealize Automation で NSX のネットワーク、セキュリティ、およびロード バランシング機能を使用するには、NSX Manager の認証情報を使用する場合、NSX Manager 管理者アカウントを使用する必要があります。

手順

- 1 [インフラストラクチャ] - [エンドポイント] - [エンドポイント] を選択します。
- 2 [新規] - [ネットワークおよびセキュリティ] - [NSX] の順に選択します。
- 3 [名前] テキスト ボックスに名前を入力します。
- 4 (オプション) [説明] テキスト ボックスに説明を入力します。
- 5 [アドレス] テキスト ボックスに NSX for vSphere インスタンスの URL を入力します。
URL は次のように指定する必要があります。**https://hostname** または **https://IP_address**
たとえば、**https://abx.nsx-manager.local/** と指定します。
- 6 NSX for vSphere エンドポイント用に保存されている、NSX の管理者権限を持つユーザー名とパスワードを入力します。
- 7 (オプション) [プロパティ] をクリックし、提供されたカスタム プロパティ、プロパティ グループ、またはエンドポイント用の独自のプロパティ定義を追加します。

- 8 NSX for vSphere ネットワークおよびセキュリティ設定を既存の vSphere エンドポイントに関連付けるには、[関連付け] をクリックし、既存の vSphere エンドポイントを選択します。

関連付けを作成する前に、vSphere エンドポイントを作成する必要があります。

vSphere エンドポイントは、NSX for vSphere または NSX-T のいずれか 1 種類のネットワークおよびセキュリティ プラットフォームとのみ関連付けることができます。

NSX for vSphere エンドポイントは 1 台の vSphere エンドポイントにのみ関連付けることができます。この関連付けの制約は、ユニバーサル オンデマンド ネットワークをプロビジョニングして、別の vCenter Server でプロビジョニングされている vSphere マシンに、これを接続できないことを意味します。

関連付けが完了すると、ページの [説明] 列には NSX for vSphere の関連付けタイプが表示されます。

- 9 (オプション) [接続をテスト] をクリックして、認証情報、ホスト エンドポイント アドレス、証明書の信頼性を検証します。このアクションは、エンドポイントをデータ収集できるように、マネージャ サービスとエージェントが実行されていることもチェックします。[OK] アクションは、これらと同一の条件をテストします。

[接続をテスト] アクションは、次のいずれかの条件に関する情報を返します。

- 証明書エラー

証明書が見つからない場合、信頼済みの場合、または期限が切れている場合は、証明書のサムプリントを受け入れるよう求められます。サムプリントを受け入れない場合でも、エンドポイントを保存することはできますが、マシンのプロビジョニングが失敗する場合があります。

- エージェント エラー

関連付けられた vSphere エージェントが見つかりませんでした。テストを成功させるには、エージェントが実行されている必要があります。

- ホスト エラー

指定されたエンドポイント アドレスにアクセスできないか、関連付けられているマネージャ サービスが実行されていません。テストを成功させるには、マネージャ サービスが実行されている必要があります。

- 認証情報エラー

指定されたアドレスにあるエンドポイントでは、指定されたユーザー名とパスワードの組み合わせが正しくありません。

- Timeout

許容時間の 2 分以内にテスト アクションを完了できませんでした。

[接続をテスト] アクションが失敗した場合でも、エンドポイントを保存することはできますが、マシンのプロビジョニングが失敗する場合があります。

信頼された証明書に、証明書の期限が切れているなどの問題がある場合は、証明書のサムプリントを受け入れるよう求められます。

- 10 [OK] をクリックしてエンドポイントを保存します。

[OK] アクションは、[接続のテスト] アクションと同じ条件でテストします。上記の条件のいずれかが見つかり、メッセージを返します。保存できた場合は、確認のためにエラーが画面に表示されたままになります。

結果

vRealize Automation では、エンドポイントからデータを収集して、コンピューティング リソースを検出します。初期データ収集後に既存エンドポイントのデータ収集を実行する方法については、[エンドポイントのソースおよび実行中のデータ収集の確認](#)を参照してください。

次のステップ

エンドポイントからファブリック グループにコンピュート リソースを追加します。[ファブリック グループの作成](#)を参照してください。

NSX-T エンドポイントの作成と vSphere エンドポイントへの関連付け

NSX-T エンドポイントを作成して既存の vSphere エンドポイントに関連付けることができます。

NSX-T エンドポイントが含まれているブループリントを展開すると、NSX-T ネットワーク、セキュリティ、およびロード バランサのコンポーネントや、NSX-T エンドポイントの関連付けられている vSphere マシン コンポーネントなど、展開に含まれるすべての NSX-T コンポーネントにタグが割り当てられます。タグは展開に一意で、初期導入およびそれ以降に展開で実行した後続のアクションのコンポーネントに関連付けられます。タグの名前は、展開の名前と同じです。

NSX-T エンドポイントは、vRealize Automation 内の複数の vSphere エンドポイントに関連付けることができます。ただし、vSphere エンドポイントは、NSX for vSphere エンドポイントと NSX-T エンドポイントのどちらか 1 つの NSX にのみ関連付けることができます。

エンドポイントの作成時に NSX 接続および証明書の信頼性を検証する方法については、[テスト接続を使用する場合の考慮事項](#)を参照してください。

前提条件

- IaaS 管理者として vRealize Automation にログインします。
- vSphere プロキシ エージェントをインストールして、vSphere エンドポイントを管理する必要があり、エンドポイントとエージェントにはまったく同じ名前を使用します。エージェントのインストールについての詳細は、vRealize Automation のインストールを参照してください。
- NSX-T ネットワークを設定します。[ネットワークおよびセキュリティ コンポーネントの設定](#)を参照してください。
- [vSphere エンドポイントの作成](#)。

vRealize Automation で NSX のネットワーク、セキュリティ、およびロード バランシング機能を使用するには、NSX Manager の認証情報を使用する場合、NSX Manager 管理者アカウントを使用する必要があります。

vRealize Automation は NSX-T エンドポイントへの接続に基本認証を使用します。

手順

- 1 [インフラストラクチャ] - [エンドポイント] - [エンドポイント] を選択します。
- 2 [新規] - [ネットワークおよびセキュリティ] - [NSX-T] の順に選択します。
- 3 [名前] テキスト ボックスに名前を入力します。
- 4 (オプション) [説明] テキスト ボックスに説明を入力します。

- 5 [アドレス] テキスト ボックスに NSX-T インスタンスの URL を入力します。

URL は次のように指定する必要があります。**https://hostname** または **https://IP_address**

たとえば、**https://abx-nsxt3-manager.local** と指定します。

- 6 NSX-T エンドポイント用に保存されている、NSX の管理者権限を持つユーザー名とパスワードを入力します。
- 7 (オプション) [プロパティ] をクリックし、提供されたカスタム プロパティ、プロパティ グループ、またはエンドポイント用の独自のプロパティ定義を追加します。
- 8 NSX-T ネットワークおよびセキュリティ設定を既存の vSphere エンドポイントに関連付けるには、[関連付け] をクリックし、既存の vSphere エンドポイントを選択します。

関連付けを作成する前に、vSphere エンドポイントを作成する必要があります。

vSphere エンドポイントは、NSX for vSphere または NSX-T のいずれか 1 種類のネットワークおよびセキュリティ プラットフォームとのみ関連付けることができます。

1 つ以上の vSphere エンドポイントに NSX-T エンドポイントに関連付けることができます。これにより、異なる vCenter Server にある複数の ESX クラスタを 1 つの NSX-T インスタンスで管理できます。

関連付けが完了すると、ページの [説明] 列には NSX-T の関連付けタイプが表示されます。

- 9 (オプション) [接続をテスト] をクリックして、認証情報、ホスト エンドポイント アドレス、証明書の信頼性を検証します。このアクションは、エンドポイントをデータ収集できるように、マネージャ サービスとエージェントが実行されていることもチェックします。[OK] アクションは、これらと同一の条件をテストします。

[接続をテスト] アクションは、次のいずれかの条件に関する情報を返します。

- 証明書エラー

証明書が見つからない場合、信頼済みの場合、または期限が切れている場合は、証明書のサムプリントを受け入れるよう求められます。サムプリントを受け入れない場合でも、エンドポイントを保存することはできますが、マシンのプロビジョニングが失敗する場合があります。

- エージェント エラー

関連付けられた vSphere エージェントが見つかりませんでした。テストを成功させるには、エージェントが実行されている必要があります。

- ホスト エラー

指定されたエンドポイント アドレスにアクセスできないか、関連付けられているマネージャ サービスが実行されていません。テストを成功させるには、マネージャ サービスが実行されている必要があります。

- 認証情報エラー

指定されたアドレスにあるエンドポイントでは、指定されたユーザー名とパスワードの組み合わせが正しくありません。

- Timeout

許容時間の 2 分以内にテスト アクションを完了できませんでした。

[接続をテスト] アクションが失敗した場合でも、エンドポイントを保存することはできますが、マシンのプロビジョニングが失敗する場合があります。

信頼された証明書に、証明書の期限が切れているなどの問題がある場合は、証明書のサムプリントを受け入れるよう求められます。

10 [OK] をクリックしてエンドポイントを保存します。

[OK] アクションは、[接続のテスト] アクションと同じ条件でテストします。上記の条件のいずれかが見つかったら、メッセージを返します。保存できた場合は、確認のためにエラーが画面に表示されたままになります。

結果

vRealize Automation では、エンドポイントからデータを収集して、コンピューティング リソースを検出します。

初期データ収集後に既存エンドポイントのデータ収集を実行する方法については、[エンドポイントのソースおよび実行中のデータ収集の確認](#)を参照してください。

次のステップ

エンドポイントからファブリック グループにコンピュート リソースを追加します。[ファブリック グループの作成](#)を参照してください。

vCloud Air エンドポイントの作成

OnDemand またはサブスクリプション サービス用の vCloud Air エンドポイントを作成できます。プロキシ エンドポイントに関連付けることにより、プロキシ設定を vCloud Director エンドポイントに関連付けることもできます。

vCloud Air 管理コンソールの詳細については、vCloud Air のドキュメントを参照してください。

注： vCloud Air エンドポイントと vCloud Director エンドポイント用に定義された予約では、マシンのプロビジョニングにネットワーク プロファイルを使用できません。

vCloud Air エンドポイントの場合、vCloud Air サブスクリプション インスタンスの組織名と仮想データセンター名は同一である必要があります。

エンドポイントにプロキシ設定を関連付ける方法については、[プロキシ エンドポイントの作成とクラウド エンドポイントへの関連付け](#)を参照してください。

前提条件

- IaaS 管理者として vRealize Automation にログインします。
- vCloud Air のサブスクリプション サービスまたは OnDemand アカウントに対して、仮想インフラストラクチャ管理者の権限があることを確認します。
- 追加のセキュリティを構成し、接続がプロキシ サーバを通過するようにする場合は、プロキシ エンドポイントを作成します。vCloud Director エンドポイントを作成する際に、プロキシ エンドポイントに関連付けることができます。[プロキシ エンドポイントの作成とクラウド エンドポイントへの関連付け](#)を参照してください。

手順

- 1 [インフラストラクチャ] - [エンドポイント] - [エンドポイント] を選択します。
- 2 [新規] - [クラウド] - [vCloud Air] を選択します。
- 3 名前と説明（説明は任意）を入力します。

- 4 [アドレス] テキスト ボックスで、vCloud Air のデフォルト エンドポイント アドレスを受け入れるか、新しいアドレスを入力します。

vCloud Air のデフォルト エンドポイント アドレスは、Default URL for vCloud Air endpoint グローバル プロパティで指定されているとおり、<https://vca.vmware.com> です。

- 5 管理者レベルのユーザー名とパスワードを入力します。

認証情報は、vCloud Air サブスクリプション サービスまたは OnDemand のアカウント管理者のものでなければなりません。

ユーザー名の形式は、*domain \username* です。

VMware Remote Console を使用して、接続権限を持つ組織管理者の認証情報を入力します。

- 6 (オプション) [プロパティ] をクリックし、提供されたカスタム プロパティ、プロパティ グループ、またはエンドポイント用の独自のプロパティ定義を追加します。
- 7 (オプション) 追加のセキュリティを構成し、接続がプロキシ サーバを通過するように強制するには、[関連付け] をクリックして既存のプロキシ エンドポイントに関連付けます。

関連付けを作成するには、少なくとも 1 つのプロキシ エンドポイントが必要です。

- 8 [OK] をクリックします。

次のステップ

[ファブリック グループの作成](#)。

vCloud Director エンドポイントの作成

1 つの vCloud Director エンドポイントを作成して、環境内のすべての vCloud Director 仮想データ センター (vDC) を管理できます。あるいは個別のエンドポイントを作成して、各 vCloud Director 組織を管理できます。プロキシ エンドポイントに関連付けることにより、プロキシ設定を vCloud Director エンドポイントに関連付けることもできます。

組織 vDC の詳細については、vCloud Director のドキュメントを参照してください。

同一の vCloud Director インスタンスに対して、単一のエンドポイントと個別の組織エンドポイントを作成しないでください。

vRealize Automation では、プロキシ エージェントを使用して vSphere リソースを管理します。

注： vCloud Air エンドポイントと vCloud Director エンドポイント用に定義された予約では、マシンのプロビジョニングにネットワーク プロファイルを使用できません。

vCloud Director マシンのリース情報は、vCloud Director ではなく vRealize Automation で指定する必要があります。vCloud Director でリース情報を指定した場合は、このリース情報は vRealize Automation で認識されないか、使用されません。vCloud Director マシンのリース情報は、vCloud Director ではなく、vRealize Automation ブループリントに入力します。

エンドポイントにプロキシ設定を関連付ける方法については、[プロキシ エンドポイントの作成とクラウド エンドポイントへの関連付け](#)を参照してください。

前提条件

- IaaS 管理者として vRealize Automation にログインします。
- 追加のセキュリティを構成し、接続がプロキシ サーバを通過するようにする場合は、プロキシ エンドポイントを作成します。vCloud Director エンドポイントを作成する際に、プロキシ エンドポイントに関連付けることができます。[プロキシ エンドポイントの作成とクラウド エンドポイントへの関連付け](#)を参照してください。

手順

- 1 [インフラストラクチャ] - [エンドポイント] - [エンドポイント] を選択します。
- 2 [新規] - [クラウド] - [vCloud Director] を選択します。
- 3 名前と説明（説明は任意）を入力します。
- 4 [アドレス] テキスト ボックスに vCloud Director サーバの URL を入力します。
URL は、FQDN または IP_address のいずれかのタイプにする必要があります。
たとえば https://mycompany.com のように入力します。
- 5 管理者レベルのユーザー名とパスワードを入力します。
 - vCloud Director サーバに接続して、ユーザーが管理者ロールを持つ組織を指定するには、組織管理者の認証情報を使用します。このような認証情報を使用すると、エンドポイントは関連付けられた組織 vDC にのみアクセスできます。vCloud Director インスタンス内の追加組織ごとにエンドポイントを追加すると、vRealize Automation と統合できます。
 - vCloud Director インスタンス内のすべての組織 vDC にアクセスできるようにするには、vCloud Director のシステム管理者認証情報を使用し、[組織] テキスト ボックスは空白にしておきます。
- 6 組織の管理者である場合は、[組織] テキスト ボックスに vCloud Director の組織名を入力できます。

オプション	説明
すべての組織 vCD の検出	vCloud Director をプライベート クラウドに実装した場合は、[組織] テキスト ボックスを空白のままにすると、アプリケーションは使用可能なすべての組織 vDC を検出できます。
各組織 vCD の個別のエンドポイント	[組織] テキスト ボックスに vCloud Director の組織名を入力します。

[組織] の名前は、仮想データセンター (vDC) 名としても表示される vCloud Director の組織名と一致します。Virtual Private Cloud を使用している場合、この名前は M123456789-12345 形式の一意の ID になります。Dedicated Cloud では、この名前はターゲット vDC の名前になります。

システム レベルで vCloud Director に直接接続している場合、たとえば [組織] フィールドを空欄にする場合は、システム管理者の認証情報が必要になります。エンドポイントに組織を入力する場合は、その組織で組織管理者の認証情報を持つユーザーが必要になります。

VMware Remote Console を使用して、接続権限を持つ認証情報を入力します。

- 単一のエンドポイントですべての組織を管理する場合は、システム管理者の認証情報を入力します。
- 組織の複数の仮想データセンターをそれぞれ異なるエンドポイントで管理するには、仮想データセンターの組織管理認証情報を個別に作成します。

同じ vCloud Director インスタンスに、単一システムレベルのエンドポイントと個別の組織エンドポイントを作成しないでください。

- 7 (オプション) [プロパティ] をクリックし、提供されたカスタム プロパティ、プロパティ グループ、またはエンドポイント用の独自のプロパティ定義を追加します。
- 8 (オプション) 追加のセキュリティを構成し、接続がプロキシ サーバを通過するように強制するには、[関連付け] をクリックして既存のプロキシ エンドポイントに関連付けます。

関連付けを作成するには、少なくとも 1 つのプロキシ エンドポイントが必要です。

- 9 [OK] をクリックします。

次のステップ

[ファブリック グループの作成](#)。

Amazon エンドポイントの作成

エンドポイントを作成して、Amazon インスタンスに接続できます。必要に応じて、プロキシ エンドポイントに関連付けることで、プロキシ設定を Amazon エンドポイントに関連付けることができます。

vRealize Automation は、ブループリント作成時に使用する複数の Amazon インスタンス タイプを提供しますが、独自のインスタンス タイプをインポートする場合は、[Amazon インスタンス タイプの追加](#)を参照してください。

エンドポイントにプロキシ設定を関連付ける方法については、[プロキシ エンドポイントの作成とクラウド エンドポイントへの関連付け](#)を参照してください。

前提条件

- IaaS 管理者として vRealize Automation にログインします。
- 追加のセキュリティを構成し、接続がプロキシ サーバを通過するようにする場合は、プロキシ エンドポイントを作成します。Amazon エンドポイントを作成するときに、プロキシ エンドポイントに関連付けることができます。[プロキシ エンドポイントの作成とクラウド エンドポイントへの関連付け](#)を参照してください。

手順

- 1 [インフラストラクチャ] - [エンドポイント] - [エンドポイント] を選択します。

- 2 [新規] - [クラウド] - [Amazon EC2] を選択します。

- 3 名前と説明（説明は任意）を入力します。

通常この名前は、このエンドポイントに対応する Amazon アカウントを示します。

- 4 Amazon エンドポイントの管理者権限を持つアクセス キー ID を入力します。

Amazon アクセス キー ID に関連付けることができるエンドポイントは 1 つのみです。

Amazon エンドポイントを作成するために必要なアクセス キーを取得するには、AWS フル アクセス管理者認証情報を持つユーザーからキーを申請するか、AWS フル アクセス管理者ポリシーで追加構成される必要があります。詳細については、Amazon のドキュメントを参照してください。

- 5 Amazon エンドポイントのプライベート アクセス キーを入力します。

- 6 (オプション) [プロパティ] をクリックし、提供されたカスタム プロパティ、プロパティ グループ、またはエンドポイント用の独自のプロパティ定義を追加します。
- 7 (オプション) 追加のセキュリティを構成し、接続がプロキシ サーバを通過するように強制するには、[関連付け] をクリックして既存のプロキシ エンドポイントに関連付けます。

関連付けを作成するには、少なくとも 1 つのプロキシ エンドポイントが必要です。

- 8 [OK] をクリックします。

結果

エンドポイントを作成すると、vRealize Automation は Amazon Web Services リージョンからのデータ収集を開始します。

次のステップ

エンドポイントからファブリック グループにコンピュート リソースを追加します。[ファブリック グループの作成](#)を参照してください。

Amazon インスタンス タイプの追加

vRealize Automation には、Amazon ブループリントとともに使用するための複数のインスタンス タイプが用意されています。管理者は、インスタンス タイプを追加および削除できます。

IaaS 管理者によって管理されるマシン インスタンス タイプは、ブループリント アーキテクトが Amazon ブループリントを作成または編集するときにブループリント アーキテクトに対して利用可能になります。Amazon マシン イメージおよびインスタンス タイプは、Amazon Web Services 製品を介して利用可能になります。

前提条件

IaaS 管理者として vRealize Automation にログインします。

手順

- 1 [インフラストラクチャ] - [管理] - [インスタンス タイプ] をクリックします。
- 2 [新規] をクリックします。
- 3 新規インスタンス タイプを追加し、次のパラメータを指定します。

これらのパラメータに指定できる、利用可能な Amazon インスタンス タイプおよび設定値の詳細については、aws.amazon.com/ec2 の EC2 Instance Types - Amazon Web Services (AWS) および docs.aws.amazon.com の Instance Types にある Amazon Web Services のドキュメントから入手できます。

- 名前
- API 名
- タイプ名
- IO パフォーマンス名
- CPU
- メモリ (GB)

- ストレージ (GB)
- 計算単位

4 [保存] アイコン (👍) をクリックします。

結果

IaaS アーキテクトは、Amazon Web Services ブループリントを作成するとき、カスタムのインスタンス タイプを使用できます。

次のステップ

エンドポイントからファブリック グループにコンピュート リソースを追加します。[ファブリック グループの作成](#)を参照してください。

プロキシ エンドポイントの作成とクラウド エンドポイントへの関連付け

プロキシ エンドポイントを作成し、そのプロキシ設定を vCloud Air、vCloud Director、または Amazon のエンドポイントに関連付けることができます。

プロキシ マネージャを使用していた vCloud Air、vCloud Director、または Amazon エンドポイントをアップグレードまたは移行した場合、vCloud Air、vCloud Director、または Amazon エンドポイントと新しいプロキシ エンドポイントとの間の関連付けを含む新しい vCloud Air、vCloud Director、または Amazon エンドポイントが作成されます。

前提条件

- IaaS 管理者として vRealize Automation にログインします。
- 次のエンドポイント タイプのいずれかを作成します。
 - [vCloud Air エンドポイントの作成](#)
 - [Amazon エンドポイントの作成](#)
 - [vCloud Director エンドポイントの作成](#)

プロキシ エンドポイントとの関連付けを作成するには、vCloud Air、vCloud Director、または Amazon のエンドポイントが少なくとも 1 つ必要です。

手順

- 1 [インフラストラクチャ] - [エンドポイント] - [エンドポイント] を選択します。
- 2 [新規] - [ネットワークおよびセキュリティ] - [プロキシ] の順に選択します。
- 3 [名前] テキスト ボックスに名前を入力します。
- 4 (オプション) [説明] テキスト ボックスに説明を入力します。
- 5 [アドレス] テキスト ボックスに、インストール済みプロキシ エージェントの URL を入力します。
- 6 [ポート] テキスト ボックスに、プロキシ サーバへの接続に使用するポート番号を入力します。
- 7 管理者レベルのユーザー名とパスワードを入力します。

- 8 (オプション) [プロパティ] をクリックし、提供されたカスタム プロパティ、プロパティ グループ、またはエンドポイント用の独自のプロパティ定義を追加します。
- 9 vCloud Air、vCloud Director、または Amazon エンドポイントにプロキシ設定を関連付けるには、[関連付け] をクリックし、1 つ以上のエンドポイントを選択します。

関連付けを作成するには、少なくとも 1 つの vCloud Air、vCloud Director、または Amazon エンドポイントが必要です。

1 つ以上のエンドポイントにプロキシ エンドポイントを関連付けることができます。

- 10 [OK] をクリックします。

結果

vRealize Automation では、エンドポイントからデータを収集して、コンピューティング リソースを検出します。

次のステップ

エンドポイントからファブリック グループにコンピュート リソースを追加します。[ファブリック グループの作成](#)を参照してください。

OVF ホスト Web サイトへのプロキシ エンドポイントの作成

プロキシ エンドポイントを作成すると、ブループリントの vSphere マシン コンポーネントに OVF をインポートする際に使用したり、OVF が Web サイトにホストされている際にはイメージ コンポーネント プロファイルの値セットとして使用したりすることが可能です。

OVF 展開環境の構成については、[vSphere エンドポイントの作成](#)および [OVF からプロビジョニングするブループリントの構成](#)を参照してください。

前提条件

- IaaS 管理者として vRealize Automation にログインします。

手順

- 1 [インフラストラクチャ] - [エンドポイント] - [エンドポイント] を選択します。
- 2 [新規] - [ネットワークおよびセキュリティ] - [プロキシ] の順に選択します。
- 3 [名前] テキスト ボックスに名前を入力します。
- 4 (オプション) [説明] テキスト ボックスに説明を入力します。
- 5 [アドレス] テキスト ボックスに、OVF をホストする Web サイトの URL を入力します。
- 6 [ポート] テキスト ボックスに、Web サイトのプロキシ サーバへの接続に使用するポート番号を入力します。
- 7 管理者レベルのユーザー名とパスワードを入力します。
- 8 (オプション) [プロパティ] をクリックし、提供されたカスタム プロパティ、プロパティ グループ、またはエンドポイント用の独自のプロパティ定義を追加します。
- 9 [OK] をクリックします。

結果

これで、エンドポイントを使用して OVF を取得する Web サイトを定義できるようになります。詳細については、[OVF を使用した、vSphere コンポーネントのブループリント設定の定義](#)および [OVF を使用したコンポーネントプロファイルへのイメージの値セットの定義](#)を参照してください。

vRealize Orchestrator エンドポイントの作成

vRealize Orchestrator サーバに接続する vRealize Orchestrator エンドポイントを作成できます。

複数のエンドポイントを設定して、別々の vRealize Orchestrator サーバに接続できますが、各エンドポイントに優先度を設定する必要があります。

vRealize Orchestrator ワークフローを実行するとき、vRealize Automation は、最初に最も優先度の高い vRealize Orchestrator エンドポイントの使用を試みます。そのエンドポイントにアクセスできない場合は、vRealize Orchestrator サーバがワークフローを実行できるようになるまで、次に優先度の高いエンドポイントの使用を試みます。

前提条件

- IaaS 管理者として vRealize Automation にログインします。

手順

- 1 [インフラストラクチャ] - [エンドポイント] - [エンドポイント] を選択します。
- 2 [新規] - [オーケストレーション] - [vRealize Orchestrator] の順に選択します。
- 3 名前と説明（説明は任意）を入力します。
- 4 vRealize Orchestrator サーバの完全修飾名または IP アドレスおよび vRealize Orchestrator ポート番号を含む URL を入力します。

転送プロトコルは HTTPS にする必要があります。ポートが指定されない場合は、デフォルト ポート 443 が使用されます。

vRealize Automation アプライアンスに組み込まれたデフォルトの vRealize Orchestrator インスタンスを使用するには、**`https://vrealize-automation-appliance-hostname:443/vco`** と入力します。

- 5 vRealize Orchestrator の認証情報を [ユーザー名] と [パスワード] テキスト ボックスに入力し、vRealize Orchestrator エンドポイントに接続します。

使用する認証情報には、IaaS から呼び出す vRealize Orchestrator ワークフローに対する実行権限が必要です。

vRealize Automation アプライアンスに組み込まれたデフォルトの vRealize Orchestrator インスタンスを使用する場合、ユーザー名は **`administrator@vsphere.local`**、パスワードは、SSO の構成時に指定した管理者パスワードになります。

- 6 [優先度] テキスト ボックスに 1 以上の整数を入力します。
値が小さいほど、優先度が高くなります。
- 7 (オプション) [プロパティ] をクリックし、提供されたカスタム プロパティ、プロパティ グループ、またはエンドポイント用の独自のプロパティ定義を追加します。
- 8 [OK] をクリックします。

ネットワークの vRealize Orchestrator エンドポイントの設定

vRealize Automation ワークフローを使用して vRealize Orchestrator ワークフローを呼び出す場合は、vRealize Orchestrator インスタンスまたはサーバをエンドポイントとして設定する必要があります。

vRealize Orchestrator エンドポイントの追加の詳細については、[vRealize Orchestrator エンドポイントの作成](#)を参照してください。

vRealize Orchestrator エンドポイントをマシン ブループリントに関連付けて、そのブループリントからプロビジョニングされたマシンの vRealize Orchestrator ワークフローのすべてが、そのエンドポイントを使用して実行されるようにすることができます。

vRealize Automation には、デフォルトで、組み込みの vRealize Orchestrator インスタンスが含まれています。本番環境またはテスト環境で vRealize Automation ワークフローを実行するときや、事前検証（POC）を作成するときに、vRealize Orchestrator エンドポイントとしてこの組み込みのインスタンスを使用することをお勧めします。

また、この vRealize Orchestrator エンドポイントは、本番環境で vRealize Automation ワークフローを実行する場合に使用することをお勧めします。

vRealize Orchestrator プラグインは、vRealize Orchestrator 7.1 以降では自動的にインストールされます。個別にインストールする vRealize Orchestrator プラグインは提供されていません。

vRealize Operations Manager エンドポイントの作成

vRealize Operations Manager ホスト スイート API に接続する vRealize Operations Manager エンドポイントを作成できます。

vRealize Operations Manager 接続と証明書の信頼性を検証する方法については、[テスト接続を使用する場合の考慮事項](#)を参照してください。

前提条件

- IaaS 管理者として vRealize Automation にログインします。

手順

- 1 [インフラストラクチャ] - [エンドポイント] - [エンドポイント] を選択します。
- 2 [新規] - [管理] - [vRealize Operations Manager] を選択します。
- 3 名前と説明（説明は任意）を入力します。
- 4 [アドレス] テキスト ボックスに vRealize Operations Manager サーバの URL を入力します。
URL の形式は、**https://hostname/suite-api**。である必要があります。
- 5 vRealize Operations Manager ユーザー名とパスワードの認証情報を入力します。
- 6 （オプション）[プロパティ] をクリックし、提供されたカスタム プロパティ、プロパティ グループ、またはエンドポイント用の独自のプロパティ定義を追加します。

- 7 (オプション) [接続をテスト] をクリックして、認証情報、ホスト エンドポイント アドレス、証明書の信頼性を検証します。このアクションは、エンドポイントをデータ収集できるように、マネージャ サービスとエージェントが実行されていることもチェックします。[OK] アクションは、これらと同一の条件をテストします。

[接続をテスト] アクションは、次のいずれかの条件に関する情報を返します。

■ 証明書エラー

証明書が見つからない場合、信頼済みの場合、または期限が切れている場合は、証明書のサムプリントを受け入れるよう求められます。サムプリントを受け入れない場合でも、エンドポイントを保存することはできますが、マシンのプロビジョニングが失敗する場合があります。

■ エージェント エラー

関連付けられた vSphere エージェントが見つかりませんでした。テストを成功させるには、エージェントが実行されている必要があります。

■ ホスト エラー

指定されたエンドポイント アドレスにアクセスできないか、関連付けられているマネージャ サービスが実行されていません。テストを成功させるには、マネージャ サービスが実行されている必要があります。

■ 認証情報エラー

指定されたアドレスにあるエンドポイントでは、指定されたユーザー名とパスワードの組み合わせが正しくありません。

■ Timeout

許容時間の 2 分以内にテスト アクションを完了できませんでした。

[接続をテスト] アクションが失敗した場合でも、エンドポイントを保存することはできますが、マシンのプロビジョニングが失敗する場合があります。

信頼された証明書に、証明書の期限が切れているなどの問題がある場合は、証明書のサムプリントを受け入れるよう求められます。

8 [OK] をクリックします。

サードパーティの IP アドレス管理プロバイダ エンドポイントの作成

サードパーティの IP アドレス管理プロバイダ エンドポイントの種類を vRealize Orchestrator で登録して設定した場合、その IPAM ソリューション プロバイダのエンドポイントを vRealize Automation で作成できます。

外部 IP アドレス管理ソリューションの提供を目的として vRealize Orchestrator パッケージをインポートし、IP アドレス管理エンドポイント タイプを vRealize Orchestrator で登録した場合、そのエンドポイント タイプを vRealize Automation エンドポイントの作成時に選択できます。

注： この例は、Infoblox IP アドレス管理プラグイン (VMware Solution Exchange からダウンロード可能) の使用を前提としています。VMware から提供されている IP アドレス管理ソリューション SDK を使用して独自に IP アドレス管理プロバイダ パッケージを作成した場合も、この手順を使用できます。「前提条件」に書かれている手順で、独自のサード パーティ製 IP アドレス管理ソリューション パッケージをインポートし、設定することができます。

vRealize Automation の最初の IP アドレス管理エンドポイントは、vRealize Orchestrator の IP アドレス管理ソリューション プロバイダ プラグインに対してエンドポイント タイプを登録したときに作成されます。

前提条件

- サードパーティ製 IP アドレス管理プロバイダ パッケージの入手、および vRealize Orchestrator へのインポート。
- vRealize Orchestrator でサードパーティ製 IP アドレス管理エンドポイント タイプを登録するワークフローの実行。
- IaaS 管理者として vRealize Automation にログインします。

この例では、お使いのサードパーティの IP アドレス管理プロバイダのプラグインまたはパッケージのために vRealize Orchestrator に登録したエンドポイント タイプを使用して、Infoblox IP アドレス管理エンドポイントを作成します。

手順

- 1 [インフラストラクチャ] - [エンドポイント] - [エンドポイント] を選択します。

- 2 [新規] - [IP アドレス管理] - [*IP アドレス管理エンドポイント タイプ*]を選択します。

Infoblox などの登録済みの外部 IP アドレス管理プロバイダ エンドポイント タイプを選択します。外部 IP アドレス管理プロバイダ エンドポイントは、サードパーティの vRealize Orchestrator パッケージをインポート済みで、パッケージ ワークフローを実行してそのエンドポイント タイプを登録している場合にのみ使用できます。

Infoblox IP アドレス管理の場合は、プライマリ IP アドレス管理エンドポイント タイプのみが一覧表示されます。カスタム プロパティを使用して、セカンダリ IP アドレス管理エンドポイント タイプを指定できます。

この例では、登録済みの外部 IP アドレス管理エンドポイント タイプ（たとえば、[Infoblox NIOS]）を選択します。

- 3 名前と説明（説明は任意）を入力します。

- 4 プロバイダに固有の URL 形式（たとえば、https://host_name/name）を使用して、[アドレス] テキスト ボックスに登録済み IP アドレス管理エンドポイントの場所を入力します。

たとえば、vRealize Orchestrator で IP アドレス管理エンドポイント タイプを登録している場合は、複数の IP アドレス管理エンドポイントを作成できます（https://nsx62-scale-infoblox、https://nsx62-scale-infoblox2 など）。登録済みのプライマリ エンドポイント タイプを入力します。さらに 1 つまたは複数のセカンダリ IP アドレス管理エンドポイントを指定するには、カスタム プロパティを使用して、IP アドレス管理ソリューション プロバイダに固有の拡張可能属性をエミュレートします。

- 5 IP アドレス管理ソリューション プロバイダ アカウントにアクセスするために必要なユーザー名とパスワードを入力します。

IP アドレス管理ソリューション プロバイダ アカウントの認証情報は、vRealize Automation でエンドポイントを作成、設定、および編集するために必要です。vRealize Automation は、IP アドレス管理エンドポイント認証情報を使用して、指定されたエンドポイント タイプ（たとえば、Infoblox）と通信し、IP アドレスの割り当てや他の操作を実行します。この動作は、vRealize Automation での vSphere エンドポイント認証情報の使用方法と似ています。

- 6 (オプション) [プロパティ] をクリックし、特定の IP アドレス管理ソリューション プロバイダにとって有意なエンドポイント プロパティを追加します。

それぞれの IP アドレス管理ソリューション プロバイダ (Infoblox、Bluecat など) は、一意の拡張可能属性を使用します。これらの拡張可能属性は、vRealize Automation カスタム プロパティを使用してエミュレートできます。たとえば、Infoblox では、拡張可能属性を使用してプライマリ エンドポイントとセカンダリ エンドポイントを区別します。

- 7 [OK] をクリックします。

次のステップ

エンドポイントからファブリック グループにコンピュート リソースを追加します。[ファブリック グループの作成](#)を参照してください。

Microsoft Azure エンドポイントの作成

Microsoft Azure エンドポイントを作成すると、vRealize Automation と Azure 展開との間の認証情報による接続を容易にすることができます。

エンドポイントは、仮想マシン ブループリントの作成に使用できるリソース (ここでは Azure インスタンス) への接続を確立します。Azure エンドポイントは、Azure 仮想マシンのプロビジョニングを行うためのブループリントの基盤として使用するために必要です。複数の Azure サブスクリプションを使用する場合は、それぞれのサブスクリプション ID に対してエンドポイントが必要です。

代わりに、vRealize Orchestrator ワークフロー ツリーで、[ライブラリ] - [Azure] - [構成] の下にある Azure 接続の追加コマンドを使用して、vRealize Orchestrator から直接 Azure の接続を作成できます。ほとんどの場合、ここに記載されたエンドポイント構成を介した接続の作成方法が、推奨されるオプションになります。

Azure エンドポイントは、vRealize Orchestrator および XaaS 機能でサポートされます。Azure エンドポイントを作成、削除、または編集できます。既存のエンドポイントを変更した後、Azure ポータルで、更新された接続を通じた更新を数時間にわたって実行しないと、問題が発生する可能性があります。service vco-service restart コマンドを使用して vRealize Orchestrator サービスを再起動する必要があります。サービスを再起動しないと、エラーになります。

前提条件

- Microsoft Azure インスタンスを構成し、有効な Microsoft Azure サブスクリプションを取得します (サブスクリプション ID が必要となります)。Azure の設定とサブスクリプション ID の取得に関する詳細については、[Microsoft Azure エンドポイントの構成](#)を参照してください。
- vRealize Automation 環境に 1 つ以上のテナントと 1 つのビジネス グループがあることを確認します。
- Active Directory アプリケーションを <https://azure.microsoft.com/ja-jp/documentation/articles/resource-group-create-service-principal-portal> での説明どおりに作成します。
- エンドポイントとブループリントの構成時に必要になるため、次の Azure 関連情報を書き留めておきます。
 - サブスクリプション ID
 - テナント ID
 - ストレージ アカウント名
 - リソース グループ名

- 場所
 - 仮想ネットワーク名
 - クライアント アプリケーションの ID
 - クライアント アプリケーションのプライベート キー
 - 仮想マシン イメージの URN
- vRealize Automation Azure 実装では、Microsoft Azure のサポート対象地域のサブセットがサポートされています。[Azure のサポート対象地域](#)を参照してください。
 - テナント管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [vRO 構成] - [エンドポイント] を選択します。
- 2 [新規] アイコン (+) をクリックします。
- 3 [プラグイン] タブの [プラグイン] ドロップダウン メニューをクリックし、[Azure] を選択します。
- 4 [次へ] をクリックします。
- 5 名前と説明（説明は任意）を入力します。
- 6 [次へ] をクリックします。
- 7 [詳細] タブで、エンドポイントに関する情報をテキスト ボックスに入力します。

パラメータ	説明
接続設定	
[接続名]	新しいエンドポイント接続の一意の名前。この名前は、特定の接続を識別しやすくするために vRealize Orchestrator インターフェイスに表示されます。
[Azure サブスクリプション ID]	Azure サブスクリプションの ID。ストレージ アカウントや仮想マシンなど、ユーザーが利用できる Azure のリソースは、この ID によって定義されます。
[Azure 環境]	展開する Azure リソースの地理的リージョン。vRealize Automation は、サブスクリプション ID に基づいて最新の Azure リージョンをすべてサポートしています。
リソース マネージャの設定	
[Azure サービス URI]	Azure インスタンスにアクセスするための URI。デフォルト値の https://management.azure.com/ は、多くの標準的な実装に適しています。このボックスは、環境を選択すると自動的に入力されます。
[テナント ID]	エンドポイントで使用する Azure のテナント ID。
[クライアント ID]	エンドポイントで使用する Azure のクライアント ID。これは、Active Directory アプリケーションを作成すると割り当てられます。

パラメータ	説明
[クライアント シークレット]	Azure クライアント ID で使用するキー。このキーは、Active Directory アプリケーションを作成すると割り当てられます。
[Azure ストレージ URI]	Azure ストレージ インスタンスにアクセスするための URI。このボックスは、環境を選択すると自動的に入力されます。
プロキシ設定	
[プロキシ ホスト]	社内でプロキシ Web サーバを使用している場合は、そのサーバのホスト名を入力します。
[プロキシ ポート]	社内でプロキシ Web サーバを使用している場合は、そのサーバのポート番号を入力します。

- 8 (オプション) [プロパティ] をクリックし、提供されたカスタム プロパティ、プロパティ グループ、または独自のカスタム プロパティ定義を追加します。

- 9 [完了] をクリックします。

次のステップ

適切なリソース グループ、ストレージ アカウント、およびネットワーク セキュリティ グループを Azure に作成します。また、実装に適したロード バランサも作成する必要があります。

アクション	オプション
Azure リソース グループの作成	<ul style="list-style-type: none"> ■ Azure ポータルを使用してリソース グループを作成します。具体的な手順については、Azure ドキュメントを参照してください。 ■ Library/Azure/Resource/Create resource group にある適切な vRealize Orchestrator ワークフローを使用します。 ■ vRealize Automation で、vRealize Orchestrator ワークフローを含んだ XaaS ブループリントを作成して公開します。リソース グループは、それをサービスと資格に接続した後で申請できます。 <p>注： リソース グループ リソース タイプのサポートや管理は vRealize Automation では行われません。</p>
Azure ストレージ アカウントの作成	<ul style="list-style-type: none"> ■ Azure を使用してストレージ アカウントを作成します。具体的な手順については、Azure ドキュメントを参照してください。 ■ Library/Azure/Storage/Create storage account にある適切な vRealize Orchestrator ワークフローを使用します。 ■ vRealize Automation で、vRealize Orchestrator ワークフローを含んだ XaaS ブループリントを作成して公開します。ストレージ アカウントは、サービスと資格に接続した後で申請できます。
Azure のネットワーク セキュリティ グループの作成	<ul style="list-style-type: none"> ■ Azure を使用してセキュリティ グループを作成します。具体的な手順については、Azure ドキュメントを参照してください。 ■ Library/Azure/Network/Create Network security group にある適切な vRealize Orchestrator ワークフローを使用します。 ■ vRealize Automation で、vRealize Orchestrator ワークフローを含んだ XaaS ブループリントを作成して公開します。セキュリティ グループは、それをサービスと資格に接続した後で申請できます。

Microsoft Azure エンドポイントの構成

vRealize Automation で Microsoft Azure エンドポイントを作成するには、情報を収集して構成を実行する必要があります。

手順

1 Microsoft Azure サブスクリプションおよびテナント ID を検索して記録します。

- サブスクリプション ID - Azure ポータルの左側のツールバーにある [サブスクリプション] アイコンをクリックして、サブスクリプション ID を表示します。
- テナント ID - [ヘルプ] アイコンをクリックし、Azure ポータルで [診断を表示] を選択します。テナントを検索して特定したら、ID を記録します。

- 2** 新しいストレージ アカウントとリソース グループを作成して、開始することができます。または、これらを後からブループリントで作成できます。

■ ストレージ アカウント - アカウントを構成するには、次の手順を使用します。

- 1 Azure ポータルで、サイドバーのストレージ アカウントのアイコンを見つけます。正しいサブスクリプションが選択されていることを確認し、[追加] をクリックします。また、Azure 検索フィールドでストレージ アカウントを検索することもできます。
- 2 ストレージ アカウントに必要な情報を入力します。サブスクリプション ID が必要になります。
- 3 既存のリソース グループを使用するか、新たに作成するかを選択します。リソース グループの名前は後で必要になるため、メモしておきます。

注： 後で必要になるため、ストレージ アカウントの場所を保存します。

- 3** 仮想ネットワークを作成します。または、適切な既存のネットワークがある場合は、そのネットワークを選択できます。

ネットワークを作成する場合は、[既存のリソース グループの使用] を選択し、前の手順で作成したグループを指定する必要があります。また、以前に指定したのと同じ場所を選択します。オブジェクトの使用対象となるすべてのコンポーネント間で場所が一致しない場合、Microsoft Azure は、仮想マシンまたはその他のオブジェクトを展開しません。

- a 左側のパネルで仮想ネットワーク アイコンを見つけてクリックするか、仮想ネットワークを検索します。正しいサブスクリプションを選択して、[追加] をクリックします。
- b 新しい仮想ネットワークの一意の名前を入力し、後で使用するために記録します。
- c [アドレス空間] フィールドに、仮想ネットワークの適切な IP アドレスを入力します。
- d 正しいサブスクリプションが選択されていることを確認して、[追加] をクリックします。
- e 残りの基礎構成情報を入力します。
- f 必要に応じて他のオプションを変更できますが、多くの構成では、デフォルトのままにしておくことができます。
- g [作成] をクリックします。

- 4** vRealize Automation が認証できるように、Azure Active Directory アプリケーションを設定します。

- a Azure の左側のメニューで Active Directory アイコンを見つけ、クリックします。
- b [アプリの登録] をクリックし、[追加] を選択します。
- c Azure 名の検証に準拠するアプリケーションの名前を入力します。
- d アプリケーション タイプを [Web アプリ/API] のままにします。
- e サインオン URL には、使用状況に適した任意のものを指定できます。
- f [作成] をクリックします。

- 5 vRealize Automation でプライベート キーを作成して、アプリケーションを認証します。
 - a Azure でアプリケーションの名前をクリックします。
アプリケーション ID を後で使用するためにメモしておきます。
 - b 次のペインで [すべての設定] をクリックし、設定リストからキーを選択します。
 - c 新しいキーの説明を入力し、期間を選択します。
 - d [保存] をクリックします。キー値は後で取得できないため、安全な場所にコピーしておきます。
 - e 左側のメニューで、アプリケーションの [API のアクセス許可] を選択し、[権限の追加] をクリックして新しい権限を作成します。
 - f [API の選択] ページで、[Azure サービス管理] を選択します。
 - g [権限の委任] をクリックします。
 - h [権限の選択] で user_impersonation を選択し、[権限の追加] をクリックします。
- 6 仮想マシンを展開および管理できるように、Active Directory アプリケーションを認証して Azure サブスクリプションに接続します。
 - a 左側のメニューで [サブスクリプション] アイコンをクリックし、新しいサブスクリプションを選択します。
パネルをスライドさせるには、名前のテキストのクリックが必要になる場合があります。
 - b アクセス コントロール (IAM) オプションを選択すると、サブスクリプションに対する権限が表示されます。
 - c [ロールの割り当ての追加] 見出しの下にある [追加] をクリックします。
 - d [ロール] ドロップダウンから [共同作成者] を選択します。
 - e [アクセスの割り当て] ドロップダウンで、デフォルトの選択をそのままにします。
 - f [選択] ボックスにアプリケーションの名前を入力します。
 - g [保存] をクリックします。
 - h ロールを追加して、新しいアプリケーションに所有者、共同作成者、およびリーダーのロールが割り当てられるようにします。
 - i [保存] をクリックします。

次のステップ

Microsoft Azure コマンド ライン インターフェイス ツールをインストールする必要があります。これらのツールは、Windows および Mac オペレーティング システムの両方で無償で利用できます。これらのツールのダウンロードとインストールの詳細については、Microsoft のドキュメントを参照してください。

コマンド ライン インターフェイスがインストールされている場合は、新しいサブスクリプションに認証する必要があります。

- 1 ターミナル ウィンドウを開き、Microsoft Azure のログイン情報を入力します。認証を行うための URL と短いコードが表示されます。
- 2 ブラウザで、デバイス上のアプリケーションから受信したコードを入力します。

3 認証コードを入力し、[続行] をクリックします。

4 Azure アカウントを選択してログインします。

複数のサブスクリプションがある場合は、`azure account set <subscription-name>` コマンドを使用して正しいものが選択されていることを確認します。

5 続行する前に、`azure provider register microsoft.compute` コマンドを使用して新しい Azure サブスクリプションに Microsoft.Compute プロバイダを登録する必要があります。

コマンドがタイムアウトになり、初回の実行でエラーが発生した場合は、コマンドを再度実行します。

構成が完了したら、`azure vm image list` コマンドを使用して、使用可能な仮想マシン イメージ名を取得できます。必要なイメージを選択して、そのイメージに指定された URN を記録し、後でブループリントで使用できます。

Puppet エンドポイントの作成

Puppet エンドポイントを作成して、vSphere 仮想マシンへの Puppet 構成管理コンポーネントの追加をサポートできます。これらのコンポーネントを使用すると、Puppet マスターを使用して仮想マシンに構成管理を実施できるようになります。


エンドポイントで外部リソース（この場合は Puppet マスター インスタンス）への接続が確立されます。エンドポイントにより、Puppet 構成管理コンポーネントを vSphere 仮想マシンのブループリントに配置できます。これらのブループリントに基づいてプロビジョニングされた仮想マシンには、関連付けられた Puppet マスターによる制御を容易にする Puppet エージェントが含まれています。

Puppet プラグインとその設定のデモの詳細については、<https://www.youtube.com/watch?v=P-VglzE9o-o> を参照してください。

前提条件

- Puppet Enterprise をインストールして、お使いの環境用に構成します。
- Puppet プラグインのバージョン 3.0 をダウンロードして、vRealize Orchestrator 環境にインストールします。このプラグインは <https://marketplace.vmware.com/vsx/solutions/puppet-plugin-for-vrealize-automation?ref=search> からダウンロードできます。このプラグインのインストールと使用については、https://docs.puppet.com/pe/latest/vro_intro.html を参照してください。

手順

- 1 [管理] - [vRO 構成] - [エンドポイント] を選択します。
- 2 [新規] アイコン () をクリックします。
- 3 [プラグイン] タブの [プラグイン] ドロップダウン メニューをクリックし、[Puppet プラグイン] を選択します。
- 4 [次へ] をクリックします。
- 5 名前と説明（説明は任意）を入力します。
- 6 [次へ] をクリックします。

7 [詳細] タブで、エンドポイントに関する情報をテキスト ボックスに入力します。

パラメータ	説明
[この Puppet マスターの表示名]	エンドポイントの接続に関連付けられている Puppet マスターの名前。この名前は、特定の接続を識別しやすくするために vRealize Orchestrator インターフェイスに表示されます。
[ホスト名または IP アドレス]	このエンドポイントで使用されている Puppet マスターの FQDN または IP アドレス。
[SSH ポート]	この Puppet マスターの安全な通信に使用するために定義されているポート。
[SSH RBAC とユーザー名]	Puppet マスターとの接続に必要なロール ベースのアクセス コントロールのユーザー名。
[SSH と RBAC パスワード]	Puppet マスターを使用したセキュリティの構成に必要なロール ベースのアクセス コントロールのユーザー名。
[このマスターでシェル コマンドの sudo を使用する]	管理者が、このエンドポイントに基づいた仮想マシンでのセキュリティ オプションのため、Linux サーバで Sudo コマンドを使用できるようにする場合は、このオプションを選択します。

8 [OK] をクリックします。

結果

これで、Puppet エージェントを含む vSphere 仮想マシンを展開できるように、Puppet 構成管理コンポーネントを vSphere ブループリントに追加できるようになりました。

Ansible エンドポイントの作成

Ansible エンドポイントを作成して、vSphere 仮想マシンへの Ansible 構成管理コンポーネントの追加をサポートできます。これらのコンポーネントを使用すると、Ansible Tower を使用して仮想マシンに構成管理を実施できるようになります。

前提条件

- 環境に合わせて Ansible Tower をインストールし、構成します。
- Ansible プラグインをダウンロードし、vRealize Orchestrator 環境にインストールします。プラグインは <https://marketplace.vmware.com/vsx/solutions/sovlabs-ansible-tower-plugin-for-vra-cm-framework-1?ref=search> から入手できます。

手順

- 1 [管理] - [vRO 構成] - [エンドポイント] を選択します。
- 2 [新規] アイコンをクリックします。
- 3 [プラグイン] タブの [プラグイン] ドロップダウン メニューをクリックし、Ansible プラグインを選択します。
- 4 [次へ] をクリックします。
- 5 [エンドポイント] タブで、名前と、必要に応じて説明を入力します。
- 6 [次へ] をクリックします。

7 [詳細] タブで ページで、エンドポイントに関する情報をテキスト ボックスに入力します。

[詳細] タブ ページ	説明
Ansible Tower エンドポイント構成	<p>エンドポイント構成の情報を追加します。</p> <ul style="list-style-type: none"> ■ Ansible Tower エンドポイント構成：名前と IP アドレスまたはホスト名を、それぞれのテキスト ボックスに入力します。 ■ Ansible Tower の認証情報の設定：このエンドポイントに関連付けられている Ansible Tower のログイン認証情報を入力します。 ■ SSL 証明書のインポート：Ansible Tower の証明書を vRealize Orchestrator がサイレントに受け入れるかどうかを選択します。
Ansible Tower ホスト アクセス	<p>該当する場合は、展開されたマシンが Ansible Tower マシンに接続できるように、Ansible Tower マシンの SSH 認証情報を入力して、カスタムの動的インベントリ スクリプトを設定します。</p>
組織とインベントリのセットアップ	<p>組織名とインベントリを設定します。動的インベントリの設定値を追加します。</p>
フィルタとグループ	<p>キー値ペアのプロパティ フィルタと、Ansible 動的グループを設定します。</p>
起動時プロンプトのオーバーライド (オプション)	<p>Ansible Job のオプションのほか、マシン、テンプレート、インベントリのオプションを設定します。</p>
vRA プロパティの変換	<p>該当する場合、プロビジョニング後に Ansible がカスタム プロパティの処理の際に使用する置換文字列を入力します。</p>

8 [完了] をクリックします。

Hyper-V (SCVMM) エンドポイントの作成

エンドポイントを作成して、vRealize Automation がご使用の SCVMM 環境と通信し、コンピュート リソースの検出、データの収集、およびマシンのプロビジョニングを実行できるようにします。

前提条件

- IaaS 管理者として vRealize Automation にログインします。
- Hyper-V (SCVMM) エンドポイントを管理するには、DEM エージェントをインストールして構成する必要があります。詳細については、『vRealize Automation のインストール』の SCVMM の要件に関する情報を参照してください。

詳細については、[SCVMM 環境の準備](#)を参照してください。

手順

- 1 [インフラストラクチャ] - [エンドポイント] - [エンドポイント] を選択します。
- 2 [新規] - [仮想] - [Hyper-V (SCVMM)] を選択します。
- 3 [名前] テキスト ボックスに名前を入力します。
- 4 (オプション) [説明] テキスト ボックスに説明を入力します。

- 5 [アドレス] テキスト ボックスにエンドポイントの URL を入力します。

URL は、*FQDN* または *IP_address* のいずれかのタイプにする必要があります。

例: **mycompany-scvmm1.mycompany.local**

- 6 管理者レベルのユーザー名と、このエンドポイント用に保存したパスワードを入力します。

認証情報をまだ保存してない場合は、ここで保存できます。

- 7 (オプション) [プロパティ] をクリックし、提供されたカスタム プロパティ、プロパティ グループ、またはエンドポイント用の独自のプロパティ定義を追加します。

- 8 [OK] をクリックします。

結果

vRealize Automation では、エンドポイントからデータを収集して、コンピューティング リソースを検出します。

次のステップ

エンドポイントからファブリック グループにコンピュート リソースを追加します。[ファブリック グループの作成](#)を参照してください。

OpenStack エンドポイントの作成

vRealize Automation が OpenStack インスタンスと通信を行うためには、エンドポイントを作成する必要があります。

前提条件

- IaaS 管理者として vRealize Automation にログインします。
- OpenStack または PowerVC の要件を満たしたマシンに vRealize Automation DEM がインストールされていることを確認します。『vRealize Automation のインストール』を参照してください。
- OpenStack のフレーバーが現在サポートされていることを確認します。『vRealize Automation のサポートマトリックス』を参照してください。

以前の vRealize Automation インストール環境からアップグレードまたは移行した後で、OpenStack エンドポイントのデータ収集が失敗した場合は、各 Keystone V3 OpenStack エンドポイントに `VMware.Endpoint.Openstack.IdentityProvider.Domain.Name` カスタム プロパティを追加して、有効なドメイン名を指定し、データ収集を有効にできます。

手順

- 1 [インフラストラクチャ] - [エンドポイント] - [エンドポイント] を選択します。
- 2 [新規] - [クラウド] - [OpenStack] を選択します。
- 3 名前と説明（説明は任意）を入力します。

- 4 [アドレス] テキスト ボックスにエンドポイントの URL を入力します。

オプション	説明
PowerVC	URL は <code>http://myPowerVC.com:5000</code> または <code>http://FQDN:5000</code> の形式にする必要があります。
Openstack	URL は <code>FQDN:5000</code> または <code>IP_address:5000</code> の形式にする必要があります。エンドポイント アドレスには <code>/v2.0</code> サフィックスを含めないでください。

- 5 管理者レベルのユーザー名とパスワードを入力します。

指定する認証情報には、エンドポイントに関連付けられた OpenStack テナント内の管理者ロールが必要です。

- 6 [OpenStack プロジェクト] テキスト ボックスに OpenStack テナント名を入力します。

OpenStack テナントが異なる複数のエンドポイントを設定した場合は、テナントごとに予約ポリシーを作成します。これにより、マシンは適切なテナント リソースにプロビジョニングされるようになります。

- 7 [プロパティ] をクリックし、提供されたカスタム プロパティ、プロパティ グループ、またはエンドポイント用の独自のプロパティ定義を追加します。

Keystone V3 が有効になっている場合は、特定のドメインを指定する

VMware.Endpoint.Openstack.IdentityProvider.Domain.Name カスタム プロパティを追加します。

- 8 [OK] をクリックします。

結果

vRealize Automation では、エンドポイントからデータを収集して、コンピューティング リソースを検出します。

次のステップ

エンドポイントからファブリック グループにコンピュート リソースを追加します。[ファブリック グループの作成](#)を参照してください。

Hyper-V、XenServer、または Xen プール エンドポイントの作成

エンドポイントを作成して、vRealize Automation が Hyper-V、XenServer、または Xen プール メイン環境と通信し、コンピューティング リソースの検出、データの収集、およびマシンのプロビジョニングを実行できるようにします。

前提条件

- IaaS 管理者として vRealize Automation にログインします。
- システム管理者は、エンドポイントに対応する保存された認証情報を使用してプロキシ エージェントをインストールする必要があります。『vRealize Automation のインストール』を参照してください。

手順

- 1 [インフラストラクチャ] - [エンドポイント] - [エージェント] を選択します。

- 2 [コンピューティング リソース] テキスト ボックスに、ご使用の Hyper-V サーバ、Xen サーバ、または Xen メイン プールの完全修飾 DNS 名を入力します。

注： Xen プール エンドポイントの場合、メイン プールの名前を入力する必要があります。vRealize Automation のコンピューティング リソース テーブルでエントリが重複しないようにするために、構成済みの Xen プール メイン アドレスと一致するアドレスを指定します。たとえば、Xen プール メイン アドレスがホスト名を使用している場合、完全修飾ドメイン名 (FQDN) ではなく、ホスト名を入力します。Xen プール メイン アドレスが FQDN を使用する場合は、FQDN を入力します。

- 3 システム管理者がこのエンドポイントのためにインストールしたプロキシ エージェントを、[プロキシ エージェント名] ドロップダウン メニューから選択します。
- 4 (オプション) [説明] テキスト ボックスに説明を入力します。
- 5 [OK] をクリックします。

結果

vRealize Automation では、エンドポイントからデータを収集して、コンピューティング リソースを検出します。

次のステップ

エンドポイントからファブリック グループにコンピュート リソースを追加します。[ファブリック グループの作成](#)を参照してください。

テスト接続を使用する場合の考慮事項

テスト接続アクションを使用すると、証明書、ホスト エンドポイント アドレスに加え、vSphere、NSX for vSphere、NSX-T、および vRealize Operations Manager エンドポイントの証明書を検証できます。

このアクションは、エンドポイントからデータ収集できるように、マネージャ サービスとエージェントが実行されていることもチェックします。

[接続をテスト] アクションは、次のいずれかの条件に関する情報を返します。

■ 証明書エラー

証明書が見つからない場合、信頼済みの場合、または期限が切れている場合は、証明書のサムプリントを受け入れるよう求められます。サムプリントを受け入れない場合でも、エンドポイントを保存することはできますが、マシンのプロビジョニングが失敗する場合があります。

■ エージェント エラー

関連付けられた vSphere エージェントが見つかりませんでした。テストを成功させるには、エージェントが実行されている必要があります。

■ ホスト エラー

指定されたエンドポイント アドレスにアクセスできないか、関連付けられているマネージャ サービスが実行されていません。テストを成功させるには、マネージャ サービスが実行されている必要があります。

■ 認証情報エラー

指定されたアドレスにあるエンドポイントでは、指定されたユーザー名とパスワードの組み合わせが正しくありません。

■ Timeout

許容時間の 2 分以内にテスト アクションを完了できませんでした。

アップグレードまたは移行後のエンドポイントで [接続をテスト] を実行するとエラーが発生する場合は、[アップグレードまたは移行されたエンドポイントを使用する場合の考慮事項](#)を参照して、証明書の信頼を確立する手順をご確認ください。

プログラムによるエンドポイントのインポートまたはエクスポート

vRealize Automation 7.3 以降でプログラムによってエンドポイントをインポートおよびエクスポートするには、新しい vRealize Automation エンドポイント構成サービス REST API または vRealize CloudClient を使用する必要があります。

vRealize CloudClient のドキュメントには、適用可能なすべてのコマンドライン フォーマット、サンプル、および使用方法が記載されています。

vRealize CloudClient のアプリケーションとドキュメントは、<https://developercenter.vmware.com/tool/cloudclient> の vRealize CloudClient 製品ページからダウンロードできます。

エンドポイントのソースおよび実行中のデータ収集の確認

特定のエンドポイントに関連付けられているマシンおよびコンピュート リソースを確認できます。データ収集を手動で開始することもできます。

前提条件

- IaaS 管理者として vRealize Automation にログインします。
- 少なくとも 1 つのエンドポイントが存在することを確認します。

手順

- 1 [インフラストラクチャ] - [エンドポイント] - [エンドポイント] を選択します。
- 2 既存のエンドポイントの行を選択し、[アクション] をクリックします。

次の使用可能なアクションのいずれかを選択します。

- [コンピュート リソースの表示] をクリックして、[インフラストラクチャ] - [コンピュート リソース] ページを開きます。このページを使用して、コンピュート リソースの設定を確認および編集できます。
- [マシンの表示] をクリックして、[インフラストラクチャ] - [管理対象マシン] ページを開きます。
- [データ収集] をクリックして [データ収集] ページを開き、エンドポイントのデータ収集を開始します。ページを更新して、データ収集の現在のステータスを表示できます。

アップグレードまたは移行されたエンドポイントを使用する場合の考慮事項

vRealize Automation 7.3 以前のリリースからアップグレードまたは移行した後は、次の考慮事項を理解して対応することが重要です。

この情報は、この vRealize Automation リリースにアップグレードまたは移行されたエンドポイントに適用されます。

- vRealize Automation 7.3 より前のリリースからアップグレードまたは移行すると、プロキシ設定が含まれている vCloud Air、vCloud Director、および Amazon の各エンドポイントは、そのプロキシ設定が含まれている新しいプロキシ エンドポイントに関連付けられます。

アップグレード後または移行後、新しいプロキシ エンドポイント名は Proxy_YYYYYY となります。YYYYYY はプロキシの URL、ポート、および認証情報のハッシュです。別のエンドポイント（たとえば、vCloud Air や Amazon のエンドポイント）に対して同一のプロキシ設定（たとえば、同一の URL、ポート、および認証情報）を使用していた場合、アップグレード後または移行後は、1 台のプロキシ エンドポイントのみが、vCloud Air および Amazon のエンドポイントと新しいプロキシ エンドポイントに関連付けられます。プロキシ エンドポイントは、複数の Amazon、vCloud Air、または vCloud Director のエンドポイントに関連付けることができます。

- NSX マネージャ設定が含まれている vSphere エンドポイントをアップグレードすると、各 vSphere エンドポイントは NSX マネージャ設定が含まれている新しい NSX エンドポイントに関連付けられます。

アップグレード後または移行後、NSX エンドポイント名は NSX_XXXXXX となります。XXXXXX は、vRealize Automation 7.3 より前のリリースにおける、親 vSphere エンドポイントの名前です。

- vRealize Automation のアップグレードまたは移行が完了したら、インフラストラクチャ管理者は新しい NSX およびプロキシのエンドポイント名を変更できます。
- アップグレードまたは移行されたエンドポイントのデフォルトのセキュリティ設定では、信頼されていない証明書を受け入れません。
- 信頼されていない証明書を使用していた場合、以前の vRealize Automation インストール環境からアップグレードまたは移行した後、vSphere と NSX のすべてのエンドポイントに対して、次の手順を実行して証明書の検証を有効にする必要があります。そうしないと、エンドポイントの操作が証明書のエラーで失敗します。詳細については、VMware ナレッジベースの記事「Endpoint communication is broken after upgrade to vRA 7.3 (KB2150230)」(<http://kb.vmware.com/kb/2150230>) および「How to download and install vCenter Server root certificates to avoid Web Browser certificate warnings (KB2108294)」(<http://kb.vmware.com/kb/2108294>) を参照してください。
 - アップグレード後または移行後に、vRealize Automation vSphere エージェント マシンにログインし、[サービス] タブを使用して vSphere エージェントを再起動します。
移行ではすべてのエージェントが再起動されない場合があるため、必要に応じて手動で再起動します。
 - 少なくとも 1 つの ping レポートが終了するのを待ちます。ping レポートの完了には 1、2 分かかります。
 - vSphere エージェントがデータ収集を開始したら、IaaS 管理者として vRealize Automation にログインします。
 - [インフラストラクチャ] - [エンドポイント] - [エンドポイント] の順にクリックします。
 - vSphere エンドポイントを編集し、[接続をテスト] をクリックします。
 - 証明書のプロンプトが表示されたら、[OK] をクリックして証明書を受け入れます。

証明書のプロンプトが表示されない場合、証明書が現在、プロキシ エージェント マシンや DEM マシンなどのエンドポイントのサービスをホストする Windows マシンの信頼されたルート認証局に正しく保存されていない可能性があります。

- g [OK] をクリックして、証明書の承認を適用し、エンドポイントを保存します。
- h vSphere エンドポイントごとにこの手順を繰り返します。
- i NSX エンドポイントごとにこの手順を繰り返します。
- j [[インフラストラクチャ] > [コンピュート リソース]] に移動し、[vCenter Server コンピュート] リソースを右クリックして [データ収集] を実行します。

[接続をテスト] 操作は成功したものの、一部のデータ収集やプロビジョニング操作が失敗した場合、エンドポイントとして機能するすべてのエージェント マシンとすべての DEM マシンに同じ証明書をインストールできません。または、既存のマシンから証明書をアンインストールして、問題のあるエンドポイントに対して上記の手順を繰り返します。

- vRealize Automation 7.2 以前のリリースで、プログラムによってエンドポイントを作成、編集、および削除するために使用した vRealize Automation REST API は、vRealize Automation 7.3 以降のリリースではサポートされません。vRealize Automation 7.3 以降のリリースでプログラムによってエンドポイントを作成、編集、および削除するには、新しい vRealize Automation endpoint-configuration-service REST API または vRealize CloudClient のいずれかを使用する必要があります。
- 以前の vRealize Automation インストール環境からアップグレードまたは移行した後で、OpenStack エンドポイントのデータ収集が失敗した場合は、各 Keystone V3 OpenStack エンドポイントに `VMware.Endpoint.Openstack.IdentityProvider.Domain.Name` カスタム プロパティを追加して、有効なドメイン名を指定し、データ収集を有効にできます。
- サードパーティの IP アドレス管理エンドポイントをアップグレードすると、RegisterIPAMEndpoint ワークフローが含まれている vRealize Orchestrator パッケージがアップグレードされます。vRealize Automation のアップグレードが終了したら、vRealize Orchestrator でワークフローの再実行が必要となる場合があります。
- 複数のエンドポイントの認証情報を変更するには、個別にエンドポイントを編集するか、または vRealize CloudClient を使用してバルク更新を実行します。
- vCloud Air や vCloud Director などの一部のエンドポイント タイプは、vRealize Automation 6.2.x から vRealize Automation 7.3 以降に直接アップグレードまたは移行することはできません。
- vRealize Automation 7.3 へのアップグレードまたは移行が正常に完了した後、[インフラストラクチャ] - [エンドポイント] ページにエンドポイントがまったく表示されないか、または特定のエンドポイント タイプおよびエンドポイントのみが表示される場合は、[ナレッジベースの記事 KB2150252](#) の推奨される解決策を参照してください。

エンドポイントの削除時の考慮事項

特定の状況で特定のエンドポイント タイプを削除できます。

- データ収集されていないエンドポイントは削除できます。
- OpenStack、Amazon、VRO の各エンドポイントは、データ収集されていても予約がなければ削除できます。他のエンドポイント タイプは、データ収集されている場合は削除できません。

- サードパーティの IP アドレス管理エンドポイントは、ネットワーク プロファイルへの関連付けがない場合は削除できます。
- vSphere エンドポイントを削除すると、確認のプロンプトに次の依存関係が示されます。
 - データ収集されているエンドポイント。
 - コンピュート リソースにマッピングされる予約内で参照されているエンドポイント。予約で参照されているエンドポイントは削除できません。予約にはコンピュー ト リソースが必要です。
 - 既存のブループリントで参照されているテンプレートが含まれているエンドポイント。
エンドポイントを削除しても、ブループリントは削除されません。
 - 使用中の仮想マシンによって使用されているエンドポイント。
- プログラムによってエンドポイントを削除するには、vRealize Automation 7.3 で導入された、新しい vRealize Automation エンドポイント構成サービス REST API である CREATE、EDIT、DELETE を使用するか、vRealize CloudClient を使用します。vRealize Automation 7.3 よりも前のエンドポイント構成サービス REST API を使用してエンドポイントを削除することはできません。

接続された vSphere エンドポイントが見つからない場合のトラブルシューティング

vSphere エンドポイントのデータ収集に失敗する場合、プロキシ名とエンドポイント名の不一致が原因の可能性あります。

問題

vSphere エンドポイントでのデータ収集に失敗します。 ログ メッセージに、次のようなエラーが出力されます。

```
This exception was caught: The attached endpoint 'vCenter' cannot be found.
```

原因

vRealize Automation で構成するエンドポイント名は、インストール時に vSphere プロキシ エージェントに提供されるエンドポイント名と一致する必要があります。vSphere エンドポイントに対するデータ収集は、エンドポイント名とプロキシ エージェント名が一致しないと失敗します。一致する名前でもエンドポイントが構成されるまで、ログ メッセージに次のようなエラーが出力されます。

```
This exception was caught: The attached endpoint 'expected endpoint name' cannot be found.
```

解決方法

- 1 [インフラストラクチャ] - [監視] - [ログ] を選択します。
- 2 「Attached Endpoint Cannot be Found」というエラー メッセージを検索します。

たとえば、

```
This exception was caught: The attached endpoint 'expected endpoint name' cannot be found.
```


- 3 ログ メッセージに出力されるエンドポイント名に一致するように vSphere エンドポイントを編集します。
 - a [インフラストラクチャ] - [エンドポイント] - [エンドポイント] を選択します。
 - b 編集するエンドポイントの名前をクリックします。
 - c [名前] テキスト ボックスに目的のエンドポイント名を入力します。
 - d [OK] をクリックします。

解決方法

プロキシ エージェントがエンドポイントと通信できるようになり、データ収集に成功します。

ファブリック グループの作成

インフラストラクチャ リソースをファブリック グループに編成してファブリック グループのリソースを管理するために、1 人以上のファブリック管理者を指定できます。

ファブリック グループは仮想およびクラウドのエンドポイントに必要です。複数ユーザーへのファブリック管理者 ロールの付与は、一度に 1 人ずつ追加する方法で行うことも、ID ストア グループまたはカスタム グループをファブリック管理者として選択することによって行うこともできます。

前提条件

- IaaS 管理者として vRealize Automation にログインします。
- 1 つ以上のエンドポイントを作成する。[エンドポイント シナリオの選択](#)を参照してください。

手順

- 1 [インフラストラクチャ] - [エンドポイント] - [ファブリック グループ] を選択します。
- 2 [新規] アイコン (+) をクリックします。
- 3 [名前] テキスト ボックスに名前を入力します。
- 4 (オプション) [説明] テキスト ボックスに説明を入力します。
- 5 [ファブリック管理者] テキスト ボックスにユーザーの名前またはメール アドレスを入力し、検索アイコンをクリックして、表示されたユーザーのメール アドレスから選択します。

複数のユーザーを追加するには、この手順を繰り返します。

- 6 1 つ以上の [コンピュート リソース] を選択して、ファブリック グループに含めます。

データ収集中に検出されるのは、クラスタに存在するリソースで、ファブリック グループに選択したリソースのみです。たとえば、クラスタに存在するテンプレートで、選択したテンプレートのみが検出されて、ビジネス グループに作成した予約でのクローン作成に利用できます。

- 7 [OK] をクリックします。

結果

これで、ファブリック管理者がマシン プリフィックスを構成できるようになります。[マシン プリフィックスの構成](#)を参照してください。

現在、vRealize Automation にログインしているユーザーは、アクセス権が付与されているページに移動する前に、ログアウトして vRealize Automation にログインし直す必要があります。

マシン プリフィックスの構成

vRealize Automation でプロビジョニングされるマシンの名前の作成に使用されるマシン プリフィックスを作成できます。マシン プリフィックスは、ブループリントのデザイン キャンバスでマシン コンポーネントを定義するときが必要です。

プリフィックスはベース名で、その後に指定された桁数のカウンタが続きます。桁がすべて使用された時点で、vRealize Automation は最初の数字にロールバックします。

マシン プリフィックスは次の制限に従う必要があります。

- 大文字と小文字を区別しない ASCII 英字 a ~ z、数字 0 ~ 9、およびハイフン (-) のみが含まれる。
- ハイフンから始まらない。
- 他の記号、句読文字、空白文字は使用できない。
- 数字も数えて 15 文字を超えていないこと（ホスト名における Windows 制限（15 文字）に従うため）。



長さが制限を超えているホスト名は、マシンがプロビジョニングされるときに切り詰められ、次にデータ収集が実行されるときにアップデートされます。ただし、WIM プロビジョニング名は切り詰められません。指定された名前が 15 文字を超えていると、プロビジョニングが失敗します。

- vRealize Automation は、単一インスタンスにおける同一名を持つ複数の仮想マシンの使用をサポートしません。マシン名の重複を引き起こす命名規則を選択した場合、名前が重複しているマシンは vRealize Automation でプロビジョニングされません。可能な場合、vRealize Automation はすでに使用されているその名前をスキップし、指定されているマシン プリフィックスを使用して新しいマシン名を生成します。一意の名前を生成できない場合、プロビジョニングは失敗します。

前提条件

ファブリック管理者として vRealize Automation にログインします。

手順

- 1 [インフラストラクチャ] - [管理] - [マシン プリフィックス] をクリックします。
- 2 [新規] アイコン () をクリックします。
- 3 [名前] テキスト ボックスに、マシン プリフィックスを入力します。
- 4 マシン プリフィックスをすべてのテナントで表示するか、現在のテナントでのみ表示するかを [対象] 列で指定します。
- 5 [桁数] テキスト ボックスに、マシン プリフィックスの桁数を入力します。
- 6 [次の番号] テキスト ボックスに、カウンタの開始番号を入力します。
- 7 [保存] アイコン () をクリックします。

結果

テナント管理者は、ユーザーが vRealize Automation にアクセスしてマシンを申請できるように、ビジネス グループを作成できます。

ネットワーク プロファイルの作成

ネットワーク プロファイルには、ゲートウェイ、サブネット、アドレス範囲などの IP アドレス情報が格納されています。vRealize Automation は、vSphere の DHCP または指定された IP アドレス管理プロバイダを使用して、プロビジョニング対象のマシンに IP アドレスを割り当てます。

ネットワーク プロファイルを作成し、利用可能なネットワークの種類を定義できます。このプロファイルは、オンデマンドのネットワーク アドレス変換 (NAT) およびルーティング ネットワーク プロファイルの外部ネットワーク プロファイルおよびテンプレートなどで、新しいネットワーク パスの NSX 論理スイッチと適切なルーティング設定を構築します。ネットワーク プロファイルは、ネットワーク コンポーネントをブループリントに追加するときに必要となります。

ネットワーク プロファイルは、マシンをプロビジョニングするときのネットワーク設定に使用されます。マシンをプロビジョニングするときに作成される NSX Edge デバイスの設定もネットワーク プロファイルで指定します。予約およびブループリントを作成するときに、ネットワーク プロファイルを指定します。予約では、1つのネットワーク パスに1つのネットワーク プロファイルを割り当て、ブループリント内のマシン コンポーネントにこれらのパスのいずれかを指定できます。

ブループリントの作成者は、ブループリントの中でネットワーク コンポーネントを定義するときに適切なネットワーク プロファイルを指定します。プロビジョニングするマシンのネットワーク アダプタやロード バランサを定義するときには、既存のネットワーク プロファイルのほか、オンデマンド NAT やオンデマンド ルーティング ネットワーク プロファイルを使用できます。

ネットワーク プロファイルは、Infoblox などサード パーティの IP アドレス管理 (IPAM) プロバイダにも対応しています。IP アドレス管理用のネットワーク プロファイルが設定されている場合、プロビジョニングしたマシンは、その IP アドレス データや関連情報 (DNS、ゲートウェイなど) を、設定済みの IP アドレス管理ソリューションから取得できます。ネットワーク プロファイルで使用する IP アドレス管理エンドポイントは、Infoblox などサード パーティ プロバイダの IP アドレス管理パッケージを使用して定義できます。

注： サードパーティの IP アドレス管理プロバイダを使用していて、マシンを展開するネットワークを指定する場合は、[ナレッジベースの記事 KB2148656](#) で説明されている既知の問題を回避するために、VLAN ごとに別個のネットワーク プロファイルを使用します。

サードパーティの IP アドレス管理プロバイダを使用しない代わりに vRealize Automation で提供される IP アドレス管理エンドポイントを使用する場合は、ネットワーク プロファイルで使用する IP アドレスの範囲を指定できます。マシンに割り当てられた指定範囲内の各 IP アドレスは、マシンの破棄時に、再割り当てのために解放されます。マシンに割り当てられる固定 IP アドレスの範囲は、ネットワーク プロファイルを作成して定義できます。クローン作成するか、キックスタート/AutoYaST プロビジョニングを使用して仮想マシンをプロビジョニングするとき、申請しているマシンの所有者は所定の IP アドレス範囲から固定 IP アドレスを割り当てることができます。

ネットワーク プロファイルは、予約の特定のネットワーク パスに割り当てることができます。vSphere などマシンのコンポーネント タイプによっては、ブループリントの作成時や編集時にネットワーク プロファイルを割り当てることができます。

注： 展開された仮想マシンのネットワーク プロファイルを変更することはできませんが、仮想マシンの接続先ネットワークを変更することはできます。そのネットワークが別のネットワーク プロファイルに関連付けられている場合、vRealize Automation はそのネットワーク プロファイルの IP アドレスを仮想マシンに割り当てます。ただし、ユーザーがゲスト OS の IP アドレスを更新するまでは、仮想マシンは継続して元の IP アドレスを使用します。または、展開された仮想マシンに対して再構成アクションを使用できます。この場合も、ゲスト OS の IP アドレスの更新が必要です。

予約およびブループリントのネットワーク プロファイルを指定した場合は、ブループリントの値が優先されます。たとえば、ネットワーク プロファイルがブループリントに指定されており (VirtualMachine.NetworkN.ProfileName カスタム プロパティを使用)、なおかつブループリントで使用されている予約でも指定されている場合は、ブループリントに指定されているネットワーク プロファイルが優先されます。ただし、ブループリントでカスタム プロパティが使用されておらず、また、マシン NIC のネットワーク プロファイルを選択した場合、vRealize Automation では、ネットワーク プロファイルが指定されているマシン NIC に対して予約ネットワーク パスが使用されます。

これらのネットワーク タイプの詳細については、NSX 情報センター (https://www.vmware.com/support/pubs/nsx_pubs.html) で『NSX 管理ガイド』を参照してください。

表 2-14. vRealize Automation ネットワーク プロファイルで利用可能なネットワーク タイプ

ネットワーク タイプ	説明
外部	<p>vSphere サーバ上で構成されている既存のネットワーク。NAT およびルーティング ネットワーク タイプの外部部分です。 外部ネットワーク プロファイルでは、外部ネットワークで利用できる固定 IP アドレスの範囲を定義できます。</p> <p>指定された VMware IP アドレス管理エンドポイント、または vRealize Orchestrator で登録および構成したサードパーティの IP アドレス管理サービス プロバイダのエンドポイント (Infoblox IP アドレス管理など) から取得した IP アドレス範囲を使用することができます。IP アドレス範囲は、割り当て時に IP アドレス ブロックから作成されます。</p> <p>固定 IP アドレス範囲が含まれる外部ネットワーク プロファイルは、NAT およびルーティング ネットワークに必須です。</p> <p>既存のネットワークの外部ネットワーク プロファイルの作成を参照してください。</p>
NAT	<p>プロビジョニング中に作成されたオンデマンド ネットワーク。外部通信に IP アドレスを 1 セット使用し、内部通信に別のセットを使用する NAT ネットワークです。</p> <p>1 対 1 の NAT ネットワークの場合は、すべての仮想マシンに、外部ネットワーク プロファイルの外部 IP アドレスと、NAT ネットワーク プロファイルの内部 IP アドレスが割り当てられます。 1 対多の NAT ネットワークの場合は、すべてのマシンが外部ネットワーク プロファイルの単一の IP アドレスを共有して、外部通信を行います。</p> <p>指定された VMware IP アドレス管理エンドポイント、または vRealize Orchestrator で登録および構成したサードパーティの IP アドレス管理サービス プロバイダのエンドポイント (Infoblox IP アドレス管理など) から取得した IP アドレス範囲を使用することができます。IP アドレス範囲は、割り当て時に IP アドレス ブロックから作成されます。</p> <p>NAT ネットワーク プロファイルでは、双方向通信用の変換テーブルを使用するローカルおよび外部ネットワークを定義します。</p> <p>オンデマンド ネットワークの NAT ネットワーク プロファイルの作成を参照してください。</p>
経路指定済み	<p>プロビジョニング中に作成されたオンデマンド ネットワーク。ルーティング ネットワークには、分散論理ルーター (DLR) を使用して一緒にリンクされたサブネット全体に分配されるルーティング可能な IP アドレス空間が含まれます。</p> <p>すべての新しいルーティング ネットワークには、次回利用可能なサブネットが割り当てられており、同一のネットワーク プロファイルを使用する他のルーティング ネットワークと関連付けられています。同じルーティング ネットワーク プロファイルを持つルーティング ネットワークを使用してプロビジョニングされる仮想マシンは、互いに通信できるほか、外部ネットワークとも通信できます。</p> <p>指定された VMware IP アドレス管理エンドポイント、または vRealize Orchestrator で登録および構成したサードパーティの IP アドレス管理サービス プロバイダのエンドポイント (Infoblox IP アドレス管理など) から取得した IP アドレス範囲を使用することができます。IP アドレス範囲は、割り当て時に IP アドレス ブロックから作成されます。</p> <p>ルーティング ネットワーク プロファイルでは、ルーティング可能な空間と利用可能なサブネットを定義します。</p> <p>オンデマンド ネットワークのルーティング ネットワーク プロファイルの作成を参照してください。</p>

ネットワーク プロファイルを使用した IP アドレス範囲の制御

ネットワーク プロファイルを使用することにより、Linux キックスタートまたは autoYaST を使用し、クローン作成によってプロビジョニングされた仮想マシンや、キックスタートを使用して OpenStack でプロビジョニングされたクラウド マシンでは、事前定義された範囲から固定 IP アドレスを割り当てることができます。

デフォルトの場合、vRealize Automation は、プロビジョニングされたマシンに、Dynamic Host Configuration Protocol (DHCP) を使用して IP アドレスを割り当てます。

ネットワーク プロファイルを作成することにより、マシンに割り当てられる固定 IP アドレスの範囲を定義できます。ネットワーク プロファイルは、予約されている特定のネットワーク パスに割り当てることができます。 クローン作成、キックスタート、または autoYaST によってプロビジョニングされ、関連するネットワーク プロファイルでネットワーク パスに追加されたマシンは、割り当てられた固定 IP アドレスでプロビジョニングされます。固定 IP アドレス割り当てでプロビジョニングする場合は、カスタム仕様を使用する必要があります。

既存のオンデマンド NAT またはオンデマンド ルーティング ネットワーク コンポーネントをデザイン キャンバスに追加し、vSphere マシン コンポーネントを接続するネットワーク プロファイルを選択することによって、ネットワーク プロファイルをブループリントの vSphere マシン コンポーネントに割り当てることができます。カスタム プロパティ `VirtualMachine.NetworkN.ProfileName` (N はネットワーク ID) を使用して、ブループリントにネットワーク プロファイルを割り当てすることもできます。

必要に応じて、指定された vRealize Automation IP アドレス管理、または登録済みおよび構成済みのサードパーティの IP アドレス管理サービス プロバイダのエンドポイントをネットワーク プロファイルで使用して、IP アドレスを取得および構成できます。外部 IP アドレス管理の要件については、[サードパーティ製 IP アドレス管理プロバイダ サポートを提供するためのチェックリスト](#)を参照してください。

ネットワーク プロファイルでサードパーティの IP アドレス管理サービス プロバイダのエンドポイントを選択すると、vRealize Automation は、登録済みの外部 IP アドレス管理プロバイダのエンドポイント (Infoblox など) から IP アドレス範囲を取得します。次に、そのエンドポイントから IP アドレスの値を割り当てます。指定されている範囲のサブネット マスクを使用し、該当する IP アドレス ブロックからサブネットが割り当てられます。

予約およびブループリントのネットワーク プロファイルを指定した場合は、ブループリントの値が優先されます。たとえば、ネットワーク プロファイルがブループリントに指定されており (VirtualMachine.NetworkN.ProfileName カスタム プロパティを使用)、なおかつブループリントで使用されている予約でも指定されている場合は、ブループリントに指定されているネットワーク プロファイルが優先されます。ただし、ブループリントでカスタム プロパティが使用されておらず、また、マシン NIC のネットワーク プロファイルを選択した場合、vRealize Automation では、ネットワーク プロファイルが指定されているマシン NIC に対して予約ネットワーク パスが使用されます。

ネットワーク プロファイルの IP アドレスをインポートするための CSV ファイル形式について

vRealize Automation ネットワーク プロファイルに IP アドレス ネットワーク範囲をインポートするには、正しく形式設定された CSV ファイルを使用します。

CSV ファイルのエントリは、次の形式に従う必要があります。

CSV フィールド	説明
ip_address	IPv4 形式の IP アドレス。
machine_name	vRealize Automation 内の管理対象マシンの名前。このフィールドが空の場合、デフォルト値は名前なしになります。また、このフィールドが空の場合、status フィールドの値を Allocated にはできません。
status	割り当て済みまたは未割り当て、大文字と小文字が区別されます。このフィールドが空の場合、デフォルト値は Unallocated です。status が Allocated の場合、machine_name フィールドを空にすることはできません。
NIC_offset	負ではない整数。 NIC オフセットは、IP アドレスが割り当てられている仮想マシンの NIC を示します。仮想マシンのさまざまな NIC に複数の IP アドレスが割り当てられている場合は、NIC ごとに、対応する NIC オフセットが含まれている IP アドレス エントリが 1 つあります。0 に設定すると、オフセットなしが指定されます。

次のエントリ例は、マシンの IP アドレスが 100.10.100.1、名前が mymachine01、ステータスが割り当て済み、NIC オフセットなしであることを示しています。

```
100.10.100.1,mymachine01,Unallocated,0
```

シナリオ：CSV ファイルからネットワーク プロファイルに IP アドレスをインポートする

適切にフォーマットされた CSV ファイルをインポートすることにより、IP アドレスをネットワーク プロファイル 範囲に追加できます。また、vRealize Automation の範囲を編集したり、変更を加えた CSV ファイルや別の CSV ファイルをインポートしたりすることによって、ネットワーク プロファイル範囲のアドレスを変更することもできます。

ネットワーク プロファイル範囲の IP アドレスを追加または変更するには、CSV ファイルをインポートするか、または手動で値を入力します。また、サードパーティの IP アドレス管理プロバイダが提供する IP アドレスも使用できます。

- IP アドレス範囲の初期設定を vRealize Automation ネットワーク プロファイルにインポートします。
- ネットワーク プロファイルで、インポートした値を適用して、最初の名前付きネットワーク範囲を作成します。
- 1 つまたは複数の IP アドレスを vRealize Automation のネットワーク範囲から削除します。
- 変更を加えた CSV ファイルや別の CSV ファイルをインポートして、ネットワーク範囲の値がどのように変更されるかを確認します。

サードパーティの IP アドレス管理エンドポイントを使用するネットワーク プロファイルの場合、IP アドレスは vRealize Automation ではなくサードパーティの IP アドレス管理プロバイダによって管理されるため、[CSV からインポート] オプションを使用できません。

前提条件

- ファブリック管理者として vRealize Automation にログインします。
- ネットワーク範囲に追加するためにインポートする IP アドレスを含む CSV ファイルを作成します。[サードパーティの IP アドレス管理プロバイダを使用した外部ネットワーク プロファイルの作成およびネットワーク プロファイルの IP アドレスをインポートするための CSV ファイル形式について](#)を参照してください。

手順

- 1 [インフラストラクチャ] - [予約] - [ネットワーク プロファイル] を選択します。
- 2 [新規] をクリックし、ドロップダウン メニューからネットワーク プロファイル タイプを選択します。
この例では、*External* を選択します。
- 3 [名前] テキスト ボックスに **My Network Profile with CSV** と入力します。
- 4 [説明] テキスト ボックスに **Testing network range IP addresses with CSV** と入力します。
CSV ファイルのインポート オプションは、[ネットワーク範囲] および [IP アドレス] のタブ ページの設定に適用されます。
- 5 (オプション) 設定済みの IP アドレス管理エンドポイントがあればこれを選択します。ない場合は、この手順をスキップします。
- 6 [サブネット マスク] と [ゲートウェイ] のテキスト ボックスに適切な IP アドレス値を入力します。
- 7 [DNS] タブをクリックします。
- 8 DNS サフィックスなどの該当する情報を入力し、[ネットワーク範囲] タブをクリックします。
[ネットワーク範囲] タブをクリックすると、[CSV からインポート] オプションが使用可能になります。

- 9 新しいネットワーク範囲名と IP アドレス範囲を手動で入力する場合は、[新規] をクリックします。適切なフォーマットの CSV ファイルから IP アドレス情報をインポートする場合は、[CSV からインポート] をクリックします。

■ [新規] をクリックします。

- a ネットワーク範囲の名前を入力します。
- b ネットワーク範囲の説明を入力します。
- c 範囲の開始 IP アドレスを入力します。
- d 範囲の終了 IP アドレスを入力します。

■ [CSV からインポート] をクリックします。

- a CSV ファイルを参照して選択するか、または CSV ファイルを [CSV からインポート] ダイアログボックスにドラッグします。

CSV ファイルの行は、*ip_address*, *machine_name*, *status*, *NIC offset* という形式になります。

例：

```
100.10.100.1,mymachine01,Unallocated,0
```

CSV フィールド	説明
ip_address	IPv4 形式の IP アドレス。
machine_name	vRealize Automation 内の管理対象マシンの名前。このフィールドが空の場合、デフォルト値は名前なしになります。また、このフィールドが空の場合、status フィールドの値を Allocated にはできません。
status	割り当て済みまたは未割り当て、大文字と小文字が区別されます。このフィールドが空の場合、デフォルト値は Unallocated です。status が Allocated の場合、machine_name フィールドを空にすることはできません。
NIC_offset	負ではない整数。 NIC オフセットは、IP アドレスが割り当てられている仮想マシンの NIC を示します。仮想マシンのさまざまな NIC に複数の IP アドレスが割り当てられている場合は、NIC ごとに、対応する NIC オフセットが含まれている IP アドレス エントリが 1 つあります。0 に設定すると、オフセットなしが指定されます。

- b [適用] をクリックします。

10 [OK] をクリックします。

IP アドレス範囲の名前が [定義された範囲] リストに表示されます。範囲内の IP アドレスが [定義された IP アドレス] リストに表示されます。

[適用] をクリックするか、ネットワーク プロファイルを保存してから編集すると、アップロードされる IP アドレスが [IP アドレス] ページに表示されます。

11 [IP アドレス] タブをクリックし、指定されたアドレス空間範囲の IP アドレス データを表示します。

IP アドレス情報を CSV ファイルからインポートした場合、範囲の名前は CSV からインポート済み として生成されます。

- 12 (オプション) [ネットワーク範囲] ドロップダウン メニューから IP アドレス情報を選択して、IP アドレス エントリをフィルタリングします。**

定義済みのすべてのネットワーク範囲、CSV ファイルからインポートしたネットワーク範囲、または名前付きのネットワーク範囲に関する情報を表示できます。詳細には、開始 IP アドレス、マシン名、最終変更日、タイムスタンプ、IP ステータスなどが含まれます。

次のステップ

もう一度 CSV ファイルから IP アドレスをインポートすると、以前の IP アドレスはインポートした CSV ファイルの情報で置き換えられます。

既存のネットワークの外部ネットワーク プロファイルの作成

外部ネットワーク プロファイルを作成して、マシンのプロビジョニング用に既存のネットワークを構成するようにネットワーク設定を指定できます (プロビジョニング中に使用する NSX Edge デバイスの構成も含まれます)。

提供されている vRealize Automation IP アドレス管理プロバイダ エンドポイント、または vRealize Orchestrator に登録したサードパーティの IP アドレス管理プロバイダ エンドポイント (Infoblox など) を使用できます。

提供されている IP アドレス管理エンドポイントを使用した外部ネットワーク プロファイルの作成

外部ネットワーク プロファイルを作成して、既存のネットワークでマシンをプロビジョニングするときに使用するネットワーク プロパティと固定 IP アドレスの範囲を定義できます。

マシンのプロビジョニングで使用するため、ネットワーク プロファイルで固定 IP アドレスのネットワーク範囲を 1 つ以上定義できます。範囲を指定しない場合、ネットワーク予約ポリシーとしてネットワーク プロファイルを使用し、仮想マシン ネットワーク カード (vNIC) の予約ネットワーク パスを選択できます。

外部ネットワーク プロファイルの作成と外部 IP アドレス管理プロバイダ エンドポイントの使用については、[サードパーティの IP アドレス管理プロバイダを使用した外部ネットワーク プロファイルの作成](#)を参照してください。

手順

- 1 指定された IP アドレス管理エンドポイントを使用して外部ネットワーク プロファイルの情報を指定する**

外部ネットワーク プロファイルは、既存のネットワークのプロパティと設定を識別します。外部ネットワーク プロファイルは、NAT およびルーティング ネットワーク プロファイルに必要です。

- 2 指定された IP アドレス管理エンドポイントを使用して外部ネットワーク プロファイルの IP アドレス範囲を設定する**

マシンのプロビジョニングで使用するため、ネットワーク プロファイルで固定 IP アドレスのネットワーク範囲を 1 つ以上定義できます。範囲を指定しない場合、ネットワーク予約ポリシーとしてネットワーク プロファイルを使用し、仮想マシン ネットワーク カード (vNIC) の予約ネットワーク パスを選択できます。

次のステップ

ネットワーク プロファイルを予約内のネットワーク パスに割り当てるか、ブループリント アーキテクトがブループリント内のネットワーク プロファイルを指定できます。外部ネットワーク プロファイルは、オンデマンド NAT またはルーティング ネットワーク プロファイルを作成するときに使用できます。

指定された IP アドレス管理エンドポイントを使用して外部ネットワーク プロファイルの情報を指定する

外部ネットワーク プロファイルは、既存のネットワークのプロパティと設定を識別します。外部ネットワーク プロファイルは、NAT およびルーティング ネットワーク プロファイルに必要です。

登録されているサード パーティの IP アドレス管理エンドポイント (Infoblox など) から IP アドレス管理のアドレス情報を取得することによって外部ネットワーク プロファイルを作成する方法については、[サードパーティ製 IP アドレス管理プロバイダ サポートを提供するためのチェックリスト](#)と[サードパーティの IP アドレス管理プロバイダを使用した外部ネットワーク プロファイルの作成](#)を参照してください。以下の手順に従い、VMware 内部 IP アドレス管理エンドポイントを使用して、ネットワーク プロファイルを作成します。

前提条件

- ファブリック管理者として vRealize Automation にログインします。

手順

- 1 [インフラストラクチャ] - [予約] - [ネットワーク プロファイル] を選択します。

- 2 [新規] をクリックし、ドロップダウン メニューから [External] を選択します。

- 3 名前と説明 (説明は任意) を入力します。

- 4 指定された [vRealize Automation IP アドレス管理] エンドポイントに対するデフォルトの [IP アドレス管理エンドポイント] の値を受け入れます。

- 5 [サブネット マスク] テキスト ボックスに IP サブネット マスクを入力します。

ネットワーク プロファイルで定義するルーティング可能なアドレス空間全体のサイズは、サブネット マスクで指定します。

たとえば、255.255.0.0 のように入力します。

- 6 [ゲートウェイ] テキスト ボックスにルーティング ゲートウェイの IP アドレスを IPv4 形式 (例: 10.10.110.1) で入力します。

ネットワーク プロファイルで定義されたゲートウェイの IP アドレスは、割り当て時に NIC に割り当てられます。ゲートウェイ エントリは、NAT ネットワーク プロファイルで常に必要とされます。

NSX-T を使用している場合、DHCP サーバのデフォルト ゲートウェイは、NSX-T の NAT が 1 対多に設定されたデフォルト ゲートウェイにする必要があります。IP アドレス プールのデフォルト ゲートウェイは、vRealize Automation の NAT が 1 対多に設定されたデフォルト ゲートウェイと一致する必要があります。

ネットワーク プロファイルの [ゲートウェイ] テキスト ボックスに値が割り当てられない場合は、VirtualMachine.Network0.Gateway カスタム プロパティを使用してゲートウェイを割り当てる必要があります。

- 7 [DNS] タブをクリックします。

- 8 DNS と WINS の値を必要に応じて入力します。

DNS の値は、DNS 名の登録と解決に使用されます。内部 IP アドレス管理エンドポイントを使用している場合、DNS と WINS のフィールドは、オプションになります。外部 IP アドレス管理エンドポイントを使用している場合、DNS と WINS の値は、サード パーティの IP アドレス管理プロバイダによって提供されます。

a (オプション) [プライマリ DNS] サーバの値を入力します。

b (オプション) [セカンダリ DNS] サーバの値を入力します。

- c (オプション) [DNS サフィックス] の値を入力します。
- d (オプション) [DNS 検索サフィックス] の値を入力します。
- e (オプション) [優先 WINS] サーバの値を入力します。
- f (オプション) [代替 WINS] サーバの値を入力します。

次のステップ

固定 IP アドレスの IP アドレス範囲を設定できます。 [指定された IP アドレス管理エンドポイントを使用して外部ネットワーク プロファイルの IP アドレス範囲を設定する](#) を参照してください。

指定された IP アドレス管理エンドポイントを使用して外部ネットワーク プロファイルの IP アドレス範囲を設定する

マシンのプロビジョニングで使用するため、ネットワーク プロファイルで固定 IP アドレスのネットワーク範囲を 1 つ以上定義できます。範囲を指定しない場合、ネットワーク予約ポリシーとしてネットワーク プロファイルを使用し、仮想マシン ネットワーク カード (vNIC) の予約ネットワーク パスを選択できます。

IP アドレス範囲の値は、インポートした CSV ファイルまたは外部 IP アドレス管理プロバイダから取得した IP アドレスを使用して手動で定義できます。手動で定義する IP アドレス範囲は、CSV を介してインポートする IP アドレスと併用できます。たとえば、ユーザー インターフェイスを使用して一部の範囲を定義し、その他の範囲は CSV ファイルからインポートして定義することが可能です。

CSV ファイルからのインポートを再度行くと、その CSV ファイルの名前に関係なく、前回の CSV ファイルのインポート時にインポートされた IP アドレス範囲が消去されて新しい IP アドレス範囲情報が追加されます。つまり、インポートを 2 回以上行くと、その前にインポートしたデータが上書きされます。CSV ファイルを更新し、その CSV ファイルをネットワーク プロファイルに再インポートするプロセスは、無制限に繰り返すことができます。

外部ネットワーク プロファイルに IP アドレス範囲が定義されていない場合は、このプロファイルを使用して、仮想ネットワーク カード (vNIC) 用のネットワークを指定できます。ルーティング ネットワーク プロファイルや NAT ネットワーク プロファイルに既存のネットワーク プロファイルを使用する場合は、少なくとも 1 つの固定 IP アドレス範囲が必要です。

前提条件

[指定された IP アドレス管理エンドポイントを使用して外部ネットワーク プロファイルの情報を指定する](#)。

手順

- 1 [ネットワーク範囲] タブをクリックします。
- 2 新しいネットワーク範囲名と IP アドレス範囲を手動で入力する場合は、[新規] をクリックします。適切なフォーマットの CSV ファイルから IP アドレス情報をインポートする場合は、[CSV からインポート] をクリックします。
 - [新規] をクリックします。
 - a ネットワーク範囲の名前を入力します。
 - b ネットワーク範囲の説明を入力します。
 - c 範囲の開始 IP アドレスを入力します。
 - d 範囲の終了 IP アドレスを入力します。

■ [CSV からインポート] をクリックします。

- a CSV ファイルを参照して選択するか、または CSV ファイルを [CSV からインポート] ダイアログ ボックスにドラッグします。

CSV ファイルの行は、*ip_address*, *machine_name*, *status*, *NIC offset* という形式になります。

例：

```
100.10.100.1,mymachine01,Unallocated,0
```

CSV フィールド	説明
ip_address	IPv4 形式の IP アドレス。
machine_name	vRealize Automation 内の管理対象マシンの名前。このフィールドが空の場合、デフォルト値は名前なしになります。また、このフィールドが空の場合、status フィールドの値を Allocated にはできません。
status	割り当て済みまたは未割り当て、大文字と小文字が区別されます。このフィールドが空の場合、デフォルト値は Unallocated です。status が Allocated の場合、machine_name フィールドを空にすることはできません。
NIC_offset	負ではない整数。 NIC オフセットは、IP アドレスが割り当てられている仮想マシンの NIC を示します。仮想マシンのさまざまな NIC に複数の IP アドレスが割り当てられている場合は、NIC ごとに、対応する NIC オフセットが含まれている IP アドレス エントリが 1 つあります。0 に設定すると、オフセットなしが指定されます。

- b [適用] をクリックします。

3 [OK] をクリックします。

IP アドレス範囲の名前が [定義された範囲] リストに表示されます。範囲内の IP アドレスが [定義された IP アドレス] リストに表示されます。

[適用] をクリックするか、ネットワーク プロファイルを保存してから編集すると、アップロードされる IP アドレスが [IP アドレス] ページに表示されます。

4 [IP アドレス] タブをクリックし、指定されたアドレス空間範囲の IP アドレス データを表示します。

IP アドレス情報を CSV ファイルからインポートした場合、範囲の名前は CSV からインポート済み として生成されます。

5 (オプション) [ネットワーク範囲] ドロップダウン メニューから IP アドレス情報を選択して、IP アドレス エントリをフィルタリングします。

定義済みのすべてのネットワーク範囲、CSV ファイルからインポートしたネットワーク範囲、または名前付きのネットワーク範囲に関する情報を表示できます。詳細には、開始 IP アドレス、マシン名、最終変更日、タイムスタンプ、IP ステータスなどが含まれます。

- 6 (オプション) [IP ステータス] ドロップダウン メニューからステータス タイプを選択して、IP アドレス エントリをフィルタリングすると、選択した IP ステータスに一致する IP アドレス エントリのみが表示されます。ステータスの設定は、[割り当て済み]、[未割当て]、[削除済み]、[期限切れ] です。

[期限切れ] または [削除済み] 状態の IP アドレスに対して、[再要求] をクリックすると、それらの IP アドレス 範囲が割り当て可能になります。再利用を有効にするには、プロファイルを保存する必要があります。アドレスは直ちには再利用されません。したがって、[ステータス] 列も [期限切れ] または [削除済み] から [割り当て済み] へと直ちには変更されません。

- 7 [OK] をクリックして、ネットワーク プロファイルを完了します。

結果

ネットワーク プロファイルを予約内のネットワーク パスに割り当てるか、ブループリント アーキテクトがブループリント内のネットワーク プロファイルを指定できます。外部ネットワーク プロファイルを作成した場合は、NAT ネットワーク プロファイルやルーティング ネットワーク プロファイルの作成時にその外部ネットワーク プロファイルを使用できます。

サードパーティの IP アドレス管理プロバイダを使用した外部ネットワーク プロファイルの作成

vRealize Orchestrator でインポート、構成、および登録したサードパーティの IP アドレス管理プロバイダ ソリューションを使用して、そのサードパーティ プロバイダから IP アドレスを取得できます。

登録されているサードパーティの IP アドレス管理ソリューション プロバイダ エンドポイントを使用してゲートウェイ、サブネット マスク、DHCP/WINS 設定を取得する外部ネットワーク プロファイルを作成できます。

マシンのプロビジョニングで使用するため、ネットワーク プロファイルで固定 IP アドレスのネットワーク範囲を 1 つ以上定義できます。範囲を指定しない場合、ネットワーク予約ポリシーとしてネットワーク プロファイルを使用し、仮想マシン ネットワーク カード (vNIC) の予約ネットワーク パスを選択できます。

IP アドレス管理プロバイダを使わずに外部ネットワーク プロファイルを作成する方法と、提供されている内部 IP アドレス管理プロバイダ エンドポイントを使用して外部ネットワーク プロファイルを作成する方法については、[提供されている IP アドレス管理エンドポイントを使用した外部ネットワーク プロファイルの作成](#)を参照してください。

手順

1 サードパーティの IP アドレス管理エンドポイントを使用した外部ネットワーク プロファイル情報の指定

外部ネットワーク プロファイルは、既存のネットワークのプロパティと設定を識別します。外部ネットワーク プロファイルは、NAT およびルーティング ネットワーク プロファイルに必要です。vRealize Orchestrator で IP アドレス管理エンドポイントを登録および設定した場合は、IP アドレス情報を IP アドレス管理プロバイダで提供することを指定できます。

2 サードパーティの IP アドレス管理エンドポイントを使用して外部ネットワーク プロファイルの IP アドレス範囲を設定する

マシンのプロビジョニングで使用するため、ネットワーク プロファイルで固定 IP アドレスのネットワーク範囲を 1 つ以上定義できます。範囲を指定しない場合、ネットワーク予約ポリシーとしてネットワーク プロファイルを使用し、仮想マシン ネットワーク カード (vNIC) の予約ネットワーク パスを選択できます。

次のステップ

ネットワーク プロファイルを予約内のネットワーク パスに割り当てるか、ブループリント アーキテクトがブループリント内のネットワーク プロファイルを指定できます。外部ネットワーク プロファイルは、オンデマンド NAT またはルーティング ネットワーク プロファイルを作成するときに使用できます。

サードパーティの IP アドレス管理エンドポイントを使用した外部ネットワーク プロファイル情報の指定
外部ネットワーク プロファイルは、既存のネットワークのプロパティと設定を識別します。外部ネットワーク プロファイルは、NAT およびルーティング ネットワーク プロファイルに必要です。vRealize Orchestrator で IP アドレス管理エンドポイントを登録および設定した場合は、IP アドレス情報を IP アドレス管理プロバイダで提供することを指定できます。

前提条件

- vRealize Orchestrator で外部 IP アドレス管理プロバイダ プラグインがインポートおよび設定されていること、および vRealize Orchestrator で IP アドレス管理プロバイダ エンドポイント タイプが登録されていることを確認します。この例の場合、サポートされる外部 IP アドレス管理ソリューション プロバイダは Infoblox です。[サードパーティ製 IP アドレス管理プロバイダ サポートを提供するためのチェックリスト](#)を参照してください。
- [サードパーティの IP アドレス管理プロバイダ エンドポイントの作成](#)。
- 登録済みの IP アドレス管理エンドポイント ワークフローを使用して、vRealize Orchestrator Appliance をグローバル テナントのスタンドアロン Orchestrator として設定します (administrator@vsphere.local)。
- ファブリック管理者として vRealize Automation にログインします。

手順

- 1 [インフラストラクチャ] - [予約] - [ネットワーク プロファイル] を選択します。
- 2 [新規] をクリックし、ドロップダウン メニューから [External] を選択します。
- 3 名前と説明（説明は任意）を入力します。
- 4 サード パーティの IP アドレス管理プロバイダ エンドポイントを構成した場合、[IP アドレス管理エンドポイント] ドロップダウン メニューからサード パーティの IP アドレス管理エンドポイントを選択します。

vRealize Orchestrator で登録したサードパーティの IP アドレス管理プロバイダのエンドポイントを選択する場合、IP アドレスは、指定された IP アドレス管理サービス プロバイダから取得されます。サブネット マスクや DNS/WINS オプションなどの IP アドレス仕様は使用できません。これらの機能は、選択したサードパーティの IP アドレス管理エンドポイントで制御されるためです。

次のステップ

IP アドレスのネットワーク範囲を定義して、ネットワーク プロファイル定義を完了できます。

サードパーティの IP アドレス管理エンドポイントを使用して外部ネットワーク プロファイルの IP アドレス範囲を設定する

マシンのプロビジョニングで使用するため、ネットワーク プロファイルで固定 IP アドレスのネットワーク範囲を 1 つ以上定義できます。範囲を指定しない場合、ネットワーク予約ポリシーとしてネットワーク プロファイルを使用し、仮想マシン ネットワーク カード (vNIC) の予約ネットワーク パスを選択できます。

サードパーティ製 IP アドレス管理プロバイダによって提供されている IP アドレスを使用して、IP アドレス範囲を定義できます。

vRealize Automation では、データベース内の外部 IP アドレス管理の範囲 ID のみが保存され、範囲詳細は保存されません。このページまたはブループリントでネットワーク プロファイルを編集する場合、vRealize Automation では IP アドレス管理サービスを呼び出し、選択した範囲 ID に基づいて範囲詳細を取得します。

注：一部のサードパーティ製 IP アドレス管理プロバイダには既知の問題があり、ネットワーク範囲を返すときにクエリがタイムアウトし、その結果リストが空になることがあります。この問題を回避するには、タイムアウトにならないように検索条件を指定し、ネットワーク範囲の情報を取得します。

たとえば、IP アドレス管理プロバイダによっては、IP アドレス管理プロバイダ アプリケーションで各ネットワークに VLAN という名前のプロパティを追加し、そのプロパティに 4 などの値を割り当てることができます。その上で、vRealize Automation の [ネットワーク プロファイル] ページにある [ネットワーク範囲の選択] テキスト ボックスで、VLAN=4 のようにプロパティと値でフィルタリングできます。

または、次の手順を使用して、タイムアウト設定を増やすことができます。

- 1 vRealize Automation アプライアンスの各ノードで、`/etc/vcac/webapps/o11n-gateway-service/WEB-INF/classes/META-INF/spring/root/o11n-gateway-service-context.xml` ファイルを開きます。
- 2 30 秒のタイムアウト値を、より大きい値に変更します。
- 3 `service vcac-server restart` と入力して、vcac サーバを再起動します。

前提条件

サードパーティの IP アドレス管理エンドポイントを使用した外部ネットワーク プロファイル情報の指定。

手順

- 1 [ネットワーク範囲] タブをクリックして、新しいネットワーク範囲を作成するか、既存のネットワーク範囲を選択します。

選択した範囲の詳細（それぞれの名前、説明、開始 IP アドレス、終了 IP アドレスなど）が表示されます。ステータスに関する情報も表示されます。
- 2 [アドレス空間] ドロップダウン メニューで、エンドポイントに利用可能なすべてのアドレス空間のリストからアドレス空間を選択します。
- 3 [追加] をクリックして、指定したアドレス空間で利用できるネットワーク範囲を 1 つ以上選択します。

ネットワーク範囲を選択する場合、サードパーティの IP アドレス管理プロバイダを使用すると、空のリストが表示されます。詳細については、ナレッジベースの記事 KB2148656 (<http://kb.vmware.com/kb/2148656>) を参照してください。
- 4 [OK] をクリックします。

IP アドレス範囲の名前が [定義された範囲] リストに表示されます。範囲内の IP アドレスが [定義された IP アドレス] リストに表示されます。

[適用] をクリックするか、ネットワーク プロファイルを保存してから編集すると、アップロードされる IP アドレスが [IP アドレス] ページに表示されます。

5 [OK] をクリックして、ネットワーク プロファイルを完了します。

次のステップ

ネットワーク プロファイルを予約内のネットワーク パスに割り当てるか、ブループリント アーキテクトがブループリント内のネットワーク プロファイルを指定できます。

オンデマンド ネットワークのルーティング ネットワーク プロファイルの作成

提供された vRealize Automation IP アドレス管理エンドポイント、または適切に構成および登録されたサードパーティの IP アドレス管理エンドポイントのいずれかを使用する、オンデマンド ルーティング ネットワーク プロファイルを作成することができます。

ルーティング ネットワーク プロファイルは、複数のネットワークにわたって分割されているルーティング可能な IP アドレス空間を表します。それぞれの新しいルーティング ネットワークは、ルーティング可能な IP アドレス空間から次に利用可能なサブネットを割り当てます。ルーティング ネットワークは、同じネットワーク プロファイルを使用する他のすべてのルーティング ネットワークにアクセスできます。それぞれのルーティング サブネットは、同じネットワーク プロファイルによって作成された他のすべてのサブネットにアクセスできます。

サードパーティの IP アドレス管理プロバイダの場合、そのプロバイダによってルーティング可能な IP アドレス空間の作成と管理が行われます。ネットワーク管理者は、サードパーティの IP アドレス管理プロバイダを使用して、ルーティング可能な IP アドレス空間を定義し、専用の IP アドレス ブロックを作成します。ルーティング ネットワーク プロファイルを作成または編集するときは、サードパーティの IP アドレス管理プロバイダから取得した IP アドレス ブロックを 1 つ以上を選択できます。

ルーティング ネットワーク プロファイルの新しいインスタンスがサードパーティの IP アドレス管理プロバイダから割り当てられると、vRealize Automation は、ルーティング ネットワーク プロファイルとサブネット サイズによって決定される IP アドレス ブロックを使用してプロバイダを呼び出して、次に使用可能なサブネットを予約し、範囲を作成します。結果の範囲は、同じ展開内のルーティング ネットワークに割り当てられるマシンの IP アドレスを割り当てるために使用されます。

提供されている IP アドレス管理エンドポイントを使用したルーティング ネットワーク プロファイルの作成

ルーティング ネットワーク プロファイルで提供されている IP アドレス管理エンドポイントを使用すると、オンデマンド ルーティング ネットワーク用に、ルーティング可能な IP アドレス空間と使用可能なサブネットを定義できます。

提供されている vRealize Automation IP アドレス管理エンドポイントを使用すると、静的 IP アドレスの範囲と基本 IP アドレスをルーティング ネットワーク プロファイルに割り当てることができます。

指定された VMware IP アドレス管理エンドポイント、または vRealize Orchestrator で登録および構成したサードパーティの IP アドレス管理サービス プロバイダのエンドポイント（Infoblox IP アドレス管理など）から取得した IP アドレス範囲を使用することができます。IP アドレス範囲は、割り当て時に IP アドレス ブロックから作成されます。

手順

1 vRealize Automation IP アドレス管理エンドポイントを使用したルーティング ネットワーク プロファイル情報の指定

提供されている IP アドレス管理エンドポイントを使用する場合、ネットワーク プロファイル情報は、ネットワークのプロビジョニングで使用するルーティング ネットワーク プロパティ、基になる外部ネットワーク プロファイル、およびその他の値を指定します。

2 vRealize Automation IP アドレス管理エンドポイントを使用したルーティング ネットワーク プロファイル IP アドレス範囲の構成

ネットワークのプロビジョニングでできるように、固定 IP アドレスの範囲を 1 つ以上定義できます。

vRealize Automation IP アドレス管理エンドポイントを使用したルーティング ネットワーク プロファイル情報の指定

提供されている IP アドレス管理エンドポイントを使用する場合、ネットワーク プロファイル情報は、ネットワークのプロビジョニングで使用するルーティング ネットワーク プロパティ、基になる外部ネットワーク プロファイル、およびその他の値を指定します。

サードパーティの IP アドレス管理エンドポイントを使用してルーティング ネットワーク プロファイルを作成する場合は、[サードパーティの IP アドレス管理エンドポイントを使用したルーティング ネットワーク プロファイル情報の指定](#)を参照してください。

前提条件

- ファブリック管理者として vRealize Automation にログインします。
- 外部ネットワーク プロファイルを作成します。[提供されている IP アドレス管理エンドポイントを使用した外部ネットワーク プロファイルの作成](#)を参照してください。

手順

- 1 [インフラストラクチャ] - [予約] - [ネットワーク プロファイル] を選択します。
- 2 [新規] をクリックし、ドロップダウン メニューから [ルーティング] を選択します。
- 3 名前と説明（説明は任意）を入力します。
- 4 指定された [vRealize Automation IP アドレス管理] エンドポイントに対するデフォルトの [IP アドレス管理エンドポイント] の値を受け入れます。
- 5 [外部ネットワーク プロファイル] ドロップダウン メニューから既存の外部ネットワーク プロファイルを選択します。

- 6 外部ネットワーク プロファイルに関連付けられたサブネット マスクを [サブネット マスク] テキスト ボックスに入力します。

ネットワーク プロファイルで定義するルーティング可能なアドレス空間全体のサイズは、サブネット マスクで指定します。

たとえば、255.255.0.0 のように入力します。

- 7 [サブネット マスク範囲] テキスト ボックスのドロップダウン メニューから値を選択し、[IP アドレス範囲] ページの [範囲の生成] オプションでどのように範囲が生成されるのかを決定します。

たとえば、255.255.255.0 のように入力します。

サブネット マスクで指定されたアドレス空間から、ネットワーク プロファイルの各展開インスタンスに割り当てられる個々のアドレス ブロックをどのように切り出すかを定義するのがサブネット マスク範囲です。サブネット マスク範囲の値を選択する際は、ルーティング ネットワークの使用を検討している展開の数を考慮してください。

ルーティング ネットワーク プロファイルを使用する展開ごとに 1 つの範囲が使用されます。利用できるルーティング対象範囲の数は、サブネット マスクをサブネット マスク範囲で除した値と等しくなります（例： $255.255.0.0/255.255.255.0 = 256$ ）。

- 8 最初の使用可能な IP アドレスを [ベース IP アドレス] テキスト ボックスに入力します。

サード パーティのエンドポイントを選択した場合、このオプションは利用できません。

たとえば、120.120.0.1 のように入力します。

- 9 [DNS] タブをクリックします。

- 10 DNS と WINS の値を必要に応じて入力します。

DNS の値は、DNS 名の登録と解決に使用されます。内部 IP アドレス管理エンドポイントを使用している場合、DNS と WINS のフィールドは、オプションになります。外部 IP アドレス管理エンドポイントを使用している場合、DNS と WINS の値は、サード パーティの IP アドレス管理プロバイダによって提供されます。

- a （オプション） [プライマリ DNS] サーバの値を入力します。
- b （オプション） [セカンダリ DNS] サーバの値を入力します。
- c （オプション） [DNS サフィックス] の値を入力します。
- d （オプション） [DNS 検索サフィックス] の値を入力します。
- e （オプション） [優先 WINS] サーバの値を入力します。
- f （オプション） [代替 WINS] サーバの値を入力します。

次のステップ

[vRealize Automation IP アドレス管理エンドポイントを使用したルーティング ネットワーク プロファイル IP アドレス範囲の構成。](#)

vRealize Automation IP アドレス管理エンドポイントを使用したルーティング ネットワーク プロファイル IP アドレス範囲の構成

ネットワークのプロビジョニングで使用できるように、固定 IP アドレスの範囲を 1 つ以上定義できます。

プロビジョニング中、すべての新しいルーティング ネットワークは次に利用可能な範囲を割り当て、それを IP アドレス空間として使用します。

前提条件

[vRealize Automation IP アドレス管理エンドポイントを使用したルーティング ネットワーク プロファイル情報の指定](#)。

手順

- 1 [ネットワーク範囲] タブをクリックして、新しいネットワーク範囲を作成するか、既存のネットワーク範囲を選択します。

選択した範囲の詳細（それぞれの名前、説明、開始 IP アドレス、終了 IP アドレスなど）が表示されます。ステータスに関する情報も表示されます。

- 2 [範囲の生成] をクリックして、[全般] タブに入力したサブネット マスク、サブネット マスクの範囲、および基本 IP アドレス情報に基づいてネットワーク範囲を生成します。

vRealize Automation は、範囲サブネット マスクに基づいて、基本 IP アドレスから始まる範囲を生成します。

たとえば、サブネット マスクが 255.255.0.0 でサブネット マスク範囲が 255.255.255.0 の場合、vRealize Automation は、Range1 ~ Rangen という名前を使用して 255 個の IP アドレス範囲を生成します。

- 3 [OK] をクリックします。

サードパーティの IP アドレス管理エンドポイントを使用したルーティング ネットワーク プロファイルの作成

ルーティング ネットワーク プロファイルでサードパーティの IP アドレス管理エンドポイントを使用すると、ルーティング可能な IP アドレス空間がサードパーティの IP アドレス管理プロバイダによって作成および管理されます。

ルーティング ネットワーク プロファイルでサードパーティの IP アドレス管理エンドポイントを使用すると、プロバイダは、オンデマンド ネットワークのそれぞれのインスタンスに対して新しい IP アドレス範囲を作成します。

指定された VMware IP アドレス管理エンドポイント、または vRealize Orchestrator で登録および構成したサードパーティの IP アドレス管理サービス プロバイダのエンドポイント（Infoblox IP アドレス管理など）から取得した IP アドレス範囲を使用することができます。IP アドレス範囲は、割り当て時に IP アドレス ブロックから作成されます。

手順

- 1 [サードパーティの IP アドレス管理エンドポイントを使用したルーティング ネットワーク プロファイル情報の指定](#)

サードパーティの IP アドレス管理エンドポイントを使用する場合、ネットワーク プロファイル情報は、ネットワークのプロビジョニングで使用するルーティング ネットワーク プロパティ、基になる外部ネットワーク プロファイル、およびその他の値を指定します。

- 2 [サードパーティの IP アドレス管理エンドポイントを使用したルーティング ネットワーク プロファイル IP アドレス範囲の構成](#)

ネットワークのプロビジョニングでできるように、名前付きの固定 IPv4 ネットワーク アドレスの範囲を 1 つ以上定義できます。

サードパーティの IP アドレス管理エンドポイントを使用したルーティング ネットワーク プロファイル情報の指定
サードパーティの IP アドレス管理エンドポイントを使用する場合、ネットワーク プロファイル情報は、ネットワークのプロビジョニングで使用されるルーティング ネットワーク プロパティ、基になる外部ネットワーク プロファイル、およびその他の値を指定します。

前提条件

- ファブリック管理者として vRealize Automation にログインします。
- 外部ネットワーク プロファイルを作成します。提供されている [IP アドレス管理エンドポイントを使用した外部ネットワーク プロファイルの作成](#)または[サードパーティの IP アドレス管理プロバイダを使用した外部ネットワーク プロファイルの作成](#)を参照してください。
- サードパーティの IP アドレス管理エンドポイントを作成および構成します。[サードパーティの IP アドレス管理プロバイダ エンドポイントの作成](#)を参照してください。

手順

- 1 [インフラストラクチャ] - [予約] - [ネットワーク プロファイル] を選択します。
- 2 [新規] をクリックし、ドロップダウン メニューから [ルーティング] を選択します。
- 3 名前と説明（説明は任意）を入力します。
- 4 サードパーティの IP アドレス管理プロバイダ エンドポイントを構成した場合、[IP アドレス管理エンドポイント] ドロップダウン メニューからサードパーティの IP アドレス管理エンドポイントを選択します。

vRealize Orchestrator で登録したサードパーティの IP アドレス管理プロバイダのエンドポイントを選択する場合、IP アドレスは、指定された IP アドレス管理サービス プロバイダから取得されます。サブネット マスクや DNS/WINS オプションなどの IP アドレス仕様は使用できません。これらの機能は、選択したサードパーティの IP アドレス管理エンドポイントで制御されるためです。

- 5 [外部ネットワーク プロファイル] ドロップダウン メニューから既存の外部ネットワーク プロファイルを選択します。

指定された IP アドレス管理エンドポイントを使用するように構成された外部ネットワーク プロファイルのみが、選択の候補として一覧表示されます。

- 6 [サブネット マスク範囲] テキスト ボックスのドロップダウン メニューから値を選択し、プロビジョニング用に作成されるネットワーク サブネットの数を決めます。

たとえば、255.255.255.0 のように入力します。

サブネット マスクで指定されたアドレス空間から、ネットワーク プロファイルの各展開インスタンスに割り当てられる個々のアドレス ブロックをどのように切り出すかを定義するのがサブネット マスク範囲です。サブネット マスク範囲の値を選択する際は、ルーティング ネットワークの使用を検討している展開の数を考慮してください。

ルーティング ネットワーク プロファイルを使用する展開ごとに 1 つの範囲が使用されます。利用できるルーティング対象範囲の数は、サブネット マスクをサブネット マスク範囲で除した値と等しくなります（例：255.255.0.0/255.255.255.0 = 256）。

- 7 [IP アドレス ブロック] タブをクリックしてアドレス空間を定義し、固定 IPv4 ネットワーク アドレスの名前付き範囲を管理します。

オンデマンド ルーティング用に作成（または割り当てられる）IP 範囲は、空いている IP アドレス ブロックから確保されます。

次のステップ

サードパーティの IP アドレス管理エンドポイントを使用したルーティング ネットワーク プロファイル IP アドレス範囲の構成。

サードパーティの IP アドレス管理エンドポイントを使用したルーティング ネットワーク プロファイル IP アドレス範囲の構成

ネットワークのプロビジョニングで使用できるように、名前付きの固定 IPv4 ネットワーク アドレスの範囲を 1 つ以上定義できます。

プロビジョニング中、それぞれの新しいルーティング ネットワークは次に利用可能な範囲を割り当て、その割り当てた範囲を IP アドレス空間として使用します。IP アドレス ブロックは、サードパーティの IP アドレス管理プロバイダから取得されます。プロビジョニング中、ルーティング ネットワークは、提供されている範囲サブネット マスクと一致するサブネット マスクを使用してブロックから割り当てられます。

前提条件

サードパーティの IP アドレス管理エンドポイントを使用したルーティング ネットワーク プロファイル情報の指定。

手順

- 1 アドレス空間ドロップダウン メニューから、プロビジョニングに利用できる IP アドレス ブロックを制限するための [アドレス空間] を選択します。

アドレス空間テキスト ボックスの下に IP アドレス ブロックを追加した後は、[アドレス空間] の値を選択できなくなります。1 つのルーティング ネットワーク プロファイルで複数のアドレス空間をカバーすることはできません。

- 2 IP アドレス ブロック（IP アドレス管理プロバイダの範囲）をプロバイダ固有の検索構文を使用するか、検索ドロップダウン メニューから選択して追加します。複数追加することもできます。

該当する IP アドレス ブロックがサード パーティの IP アドレス管理プロバイダから取得されます。

ネットワーク範囲を選択する場合、サードパーティの IP アドレス管理プロバイダを使用すると、空のリストが表示されます。詳細については、ナレッジベースの記事 KB2148656 (<http://kb.vmware.com/kb/2148656>) を参照してください。

- a [追加] をクリックします。
- b [検索] をクリックします。
- c 検索構文を入力するか、またはドロップダウン メニューから IP アドレス ブロック（複数可）を選択します。
- d [OK] をクリックします。

- 3 [適用] をクリックします。

- 4 [OK] をクリックします。

オンデマンド ネットワークの NAT ネットワーク プロファイルの作成

提供された vRealize Automation IP アドレス管理エンドポイント、または適切に構成および登録されたサードパーティの IP アドレス管理エンドポイントのいずれかを使用する、オンデマンド NAT ネットワーク プロファイルを作成することができます。

提供されている IP アドレス管理エンドポイントを使用した NAT ネットワーク プロファイルの作成

外部のネットワーク プロファイルを基準として、オンデマンドの NSX NAT ネットワーク プロファイルを作成することができます。提供されている vRealize Automation IP アドレス管理エンドポイントを使用すると、静的 IP アドレスと DHCP アドレスの範囲を NAT ネットワーク プロファイルに割り当てることができます。

NAT ネットワークでは、外部通信に IP アドレスを 1 セット使用し、内部通信に別のセットを使用します。外部 IP アドレスは外部ネットワーク プロファイルから割り当てられ、内部 IP アドレスは NAT ネットワーク プロファイルによって定義されます。新しい NAT ネットワークをプロビジョニングすると、NAT ネットワーク プロファイルの新しいインスタンスが作成され、マシン IP アドレスを割り当てるために使用されます。

指定された VMware IP アドレス管理エンドポイント、または vRealize Orchestrator で登録および構成したサードパーティの IP アドレス管理サービス プロバイダのエンドポイント（Infoblox IP アドレス管理など）から取得した IP アドレス範囲を使用することができます。IP アドレス範囲は、割り当て時に IP アドレス ブロックから作成されます。

1 対多の NAT ネットワークでは、NAT ルールを定義しておき、NAT ネットワーク コンポーネントをブループリントに追加するときそのルールを構成できます。また、展開の中で NAT ネットワークを編集するときに NAT ルールを変更することができます。

手順

1 vRealize Automation IP アドレス管理エンドポイントを使用した NAT ネットワーク プロファイル情報の指定

ネットワーク プロファイルでは、組み込みの vRealize Automation IP アドレス管理機能によって、オンデマンド NAT ネットワークのプロパティ、その基盤となる外部ネットワーク プロファイル、NAT タイプ、およびネットワークのプロビジョニングで使用されるその他の値が指定されます。

2 vRealize Automation IP アドレス管理エンドポイントを使用した NAT ネットワーク プロファイル IP アドレス範囲の設定

ネットワークのプロビジョニングで使用できるように、固定 IP アドレスの範囲を 1 つ以上定義できます。

vRealize Automation IP アドレス管理エンドポイントを使用した NAT ネットワーク プロファイル情報の指定
ネットワーク プロファイルでは、組み込みの vRealize Automation IP アドレス管理機能によって、オンデマンド NAT ネットワークのプロパティ、その基盤となる外部ネットワーク プロファイル、NAT タイプ、およびネットワークのプロビジョニングで使用されるその他の値が指定されます。

サードパーティの IP アドレス管理エンドポイントを使用する NAT ネットワーク プロファイルを作成する場合は、[サードパーティの IP アドレス管理エンドポイントを使用した NAT ネットワーク プロファイル情報の指定](#)を参照してください。

前提条件

- ファブリック管理者として vRealize Automation にログインします。

- 外部ネットワーク プロファイルを作成します。提供されている [IP アドレス管理エンドポイントを使用した外部ネットワーク プロファイルの作成](#) を参照してください。

手順

- 1 [インフラストラクチャ] - [予約] - [ネットワーク プロファイル] を選択します。
- 2 [新規] をクリックし、ドロップダウン メニューから [NAT] を選択します。
- 3 名前と説明（説明は任意）を入力します。
- 4 指定された [vRealize Automation IP アドレス管理] エンドポイントに対するデフォルトの [IP アドレス管理エンドポイント] の値を受け入れます。
- 5 [外部ネットワーク プロファイル] ドロップダウン メニューから既存の外部ネットワーク プロファイルを選択します。
- 6 [NAT タイプ] ドロップダウン メニューから 1 対 1 または 1 対多のネットワーク アドレス変換タイプを選択します。

オプション	説明
1 対 1	<p>各ネットワーク アダプタに外部固定 IP アドレスを割り当てます。すべてのマシンが外部ネットワークにアクセスでき、外部ネットワークからもアクセスできます。</p> <p>NSX Edge アップリンクに割り当てる外部 IP アドレスは、すべてが同じサブネットに属している必要があります。vRealize Automation で 1 対 1 の NAT を使用する場合、対応する外部ネットワーク プロファイルに含まれる IP アドレス範囲は、単一のサブネットに属している必要があります。</p>
1 対多	<p>ネットワーク上のすべてのマシンで 1 つの外部 IP アドレスを共有します。内部マシンには、DHCP または固定 IP アドレスのいずれかを設置できます。すべてのマシンが外部ネットワークにアクセスできますが、外部ネットワークからアクセスできるマシンはありません。このオプションを選択すると、DHCP グループの [有効化] チェック ボックスが有効になります。</p> <p>NSX for vSphere の場合、1 対多の NAT 変換タイプでは、NAT ネットワーク コンポーネントをブループリントに追加するときに NAT ルールを定義できます。</p> <p>NSX for vSphere では 1 対 1 の NAT と 1 対多の NAT ネットワークをサポートしていますが、NSX-T では 1 対多の NAT のみをサポートしています。</p>

- 7 [サブネット マスク] テキスト ボックスに IP サブネット マスクを入力します。

ネットワーク プロファイルで定義するルーティング可能なアドレス空間全体のサイズは、サブネット マスクで指定します。

たとえば、255.255.0.0 のように入力します。
- 8 [ゲートウェイ] テキスト ボックスにルーティング ゲートウェイの IP アドレスを IPv4 形式（例：10.10.110.1）で入力します。

ネットワーク プロファイルで定義されたゲートウェイの IP アドレスは、割り当て時に NIC に割り当てられます。ゲートウェイ エントリは、NAT ネットワーク プロファイルで常必要とされます。

NSX-T を使用している場合、DHCP サーバのデフォルト ゲートウェイは、NSX-T の NAT が 1 対多に設定されたデフォルト ゲートウェイにする必要があります。IP アドレス プールのデフォルト ゲートウェイは、vRealize Automation の NAT が 1 対多に設定されたデフォルト ゲートウェイと一致する必要があります。

ネットワーク プロファイルの [ゲートウェイ] テキスト ボックスに値が割り当てられない場合は、VirtualMachine.Network0.Gateway カスタム プロパティを使用してゲートウェイを割り当てる必要があります。

- 9 (オプション) [DHCP] グループで [有効] チェック ボックスを選択し、[IP アドレス範囲開始] と [IP アドレス範囲終了] の値を入力します。

NAT タイプを 1 対多に設定した場合のみ、チェック ボックスを選択できます。

NSX-T では、IP アドレス プール範囲の最初の IP アドレスが、NSX-T で <FirstIpInPool>/<subnetMaskOfNat> と定義されているとおりに DHCP サーバの IP アドレスと一致する必要があります。NSX-T の IP アドレス プールは 2 番目の IP アドレスで開始する必要があります。

- 10 (オプション) DHCP リース時間を設定して、マシンが 1 つの IP アドレスを使用できる時間を定義します。

- 11 [DNS] タブをクリックします。

- 12 DNS と WINS の値を必要に応じて入力します。

DNS の値は、DNS 名の登録と解決に使用されます。内部 IP アドレス管理エンドポイントを使用している場合、DNS と WINS のフィールドは、オプションになります。外部 IP アドレス管理エンドポイントを使用している場合、DNS と WINS の値は、サード パーティの IP アドレス管理プロバイダによって提供されます。

- a (オプション) [プライマリ DNS] サーバの値を入力します。
- b (オプション) [セカンダリ DNS] サーバの値を入力します。
- c (オプション) [DNS サフィックス] の値を入力します。
- d (オプション) [DNS 検索サフィックス] の値を入力します。
- e (オプション) [優先 WINS] サーバの値を入力します。
- f (オプション) [代替 WINS] サーバの値を入力します。

次のステップ

[vRealize Automation IP アドレス管理エンドポイントを使用した NAT ネットワーク プロファイル IP アドレス範囲の設定。](#)

vRealize Automation IP アドレス管理エンドポイントを使用した NAT ネットワーク プロファイル IP アドレス範囲の設定

ネットワークのプロビジョニングでできるように、固定 IP アドレスの範囲を 1 つ以上定義できます。

ネットワーク範囲の開始 IP アドレスと終了 IP アドレスは、DHCP のアドレスと重ならないようにしてください。重複するアドレス範囲を含んだプロファイルを保存しようとすると、vRealize Automation によって検証エラーが表示されます。

前提条件

[vRealize Automation IP アドレス管理エンドポイントを使用した NAT ネットワーク プロファイル情報の指定。](#)

手順

- 1 [ネットワーク範囲] タブをクリックして、新しいネットワーク範囲を作成するか、既存のネットワーク範囲を選択します。

選択した範囲の詳細（それぞれの名前、説明、開始 IP アドレス、終了 IP アドレスなど）が表示されます。ステータスに関する情報も表示されます。

- 2 新しいネットワーク範囲名と IP アドレス範囲を手動で入力する場合は、[新規] をクリックします。適切なフォーマットの CSV ファイルから IP アドレス情報をインポートする場合は、[CSV からインポート] をクリックします。

- [新規] をクリックします。

- a ネットワーク範囲の名前を入力します。
- b ネットワーク範囲の説明を入力します。
- c 範囲の開始 IP アドレスを入力します。
- d 範囲の終了 IP アドレスを入力します。

- [CSV からインポート] をクリックします。

- a CSV ファイルを参照して選択するか、または CSV ファイルを [CSV からインポート] ダイアログ ボックスにドラッグします。

CSV ファイルの行は、*ip_address, machine_name, status, NIC offset* という形式になります。

例：

```
100.10.100.1,mymachine01,Unallocated,0
```

CSV フィールド	説明
ip_address	IPv4 形式の IP アドレス。
machine_name	vRealize Automation 内の管理対象マシンの名前。このフィールドが空の場合、デフォルト値は名前なしになります。また、このフィールドが空の場合、status フィールドの値を Allocated にはできません。
status	割り当て済みまたは未割り当て、大文字と小文字が区別されます。このフィールドが空の場合、デフォルト値は Unallocated です。status が Allocated の場合、machine_name フィールドを空にすることはできません。
NIC_offset	負ではない整数。 NIC オフセットは、IP アドレスが割り当てられている仮想マシンの NIC を示します。仮想マシンのさまざまな NIC に複数の IP アドレスが割り当てられている場合は、NIC ごとに、対応する NIC オフセットが含まれている IP アドレス エントリが 1 つあります。0 に設定すると、オフセットなしが指定されます。

- b [適用] をクリックします。

- 3 [OK] をクリックします。

IP アドレス範囲の名前が [定義された範囲] リストに表示されます。範囲内の IP アドレスが [定義された IP アドレス] リストに表示されます。

[適用] をクリックするか、ネットワーク プロファイルを保存してから編集すると、アップロードされる IP アドレスが [IP アドレス] ページに表示されます。

4 [IP アドレス] タブをクリックし、名前付きのネットワーク範囲の IP アドレスを表示します。

5 (オプション) [ネットワーク範囲] ドロップダウン メニューから IP アドレス情報を選択して、IP アドレス エントリをフィルタリングします。

定義済みのすべてのネットワーク範囲、CSV ファイルからインポートしたネットワーク範囲、または名前付きのネットワーク範囲に関する情報を表示できます。詳細には、開始 IP アドレス、マシン名、最終変更日、タイムスタンプ、IP ステータスなどが含まれます。

6 (オプション) [IP ステータス] ドロップダウン メニューからステータス タイプを選択して、IP アドレス エントリをフィルタリングすると、選択した IP ステータスに一致する IP アドレス エントリのみが表示されます。ステータスの設定は、[割り当て済み]、[未割当て]、[削除済み]、[期限切れ] です。

[期限切れ] または [削除済み] 状態の IP アドレスに対して、[再要求] をクリックすると、それらの IP アドレス範囲が割り当て可能になります。再利用を有効にするには、プロファイルを保存する必要があります。アドレスは直ちには再利用されません。したがって、[ステータス] 列も [期限切れ] または [削除済み] から [割り当て済み] へと直ちには変更されません。

7 [OK] をクリックします。

サードパーティの IP アドレス管理エンドポイントを使用した NAT ネットワーク プロファイルの作成

外部のネットワーク プロファイルを基準として、オンデマンドの NSX NAT ネットワーク プロファイルを作成することができます。NSX NAT ネットワーク プロファイルで、サードパーティの IP アドレス管理エンドポイントを使用すると、サードパーティの IP アドレス管理プロバイダによって IP アドレス空間が作成および管理されます。

NAT ネットワーク プロファイルでサードパーティの IP アドレス管理エンドポイントを使用すると、プロバイダは、オンデマンド ネットワークのそれぞれのインスタンスに対して新しい IP アドレス範囲を作成します。1 つ以上の範囲で定義された一連の内部 IP アドレスは、サードパーティの IP アドレス管理プロバイダのエンドポイントで、NAT ネットワークのすべてのインスタンスに対して作成されます。これらの IP アドレス範囲は、同じ展開内の NAT ネットワークに割り当てられるマシンの IP アドレスを割り当てるために使用されます。単一のアドレス空間内に重複する IP アドレスを定義することはできないため、NAT ネットワークのそれぞれのインスタンスに対して新しいアドレス空間がプロバイダによって作成されます。NAT ネットワークを破棄すると、IP アドレス管理プロバイダ エンドポイントと新しいアドレス空間の NAT ネットワーク範囲が破棄されます。

指定された VMware IP アドレス管理エンドポイント、または vRealize Orchestrator で登録および構成したサードパーティの IP アドレス管理サービス プロバイダのエンドポイント (Infoblox IP アドレス管理など) から取得した IP アドレス範囲を使用することができます。IP アドレス範囲は、割り当て時に IP アドレス ブロックから作成されます。

1 対多の NAT ネットワークでは、NAT ルールを定義しておき、NAT ネットワーク コンポーネントをブループリントに追加するときにそのルールを構成できます。また、展開の中で NAT ネットワークを編集するときに NAT ルールを変更することができます。

手順

1 サードパーティの IP アドレス管理エンドポイントを使用した NAT ネットワーク プロファイル情報の指定

サードパーティの IP アドレス管理エンドポイントを使用する場合、ネットワーク プロファイル情報は、ネットワークのプロビジョニングで使用される NAT ネットワーク プロパティ、基になる外部ネットワーク プロファイル、およびその他の値を指定します。

2 サードパーティの IP アドレス管理エンドポイントを使用した NAT ネットワーク プロファイル IP アドレス範囲の設定

NAT を使用して、ネットワークのプロビジョニングに使用する 1 つ以上の IP アドレス範囲を定義できます。

サードパーティの IP アドレス管理エンドポイントを使用した NAT ネットワーク プロファイル情報の指定

サードパーティの IP アドレス管理エンドポイントを使用する場合、ネットワーク プロファイル情報は、ネットワークのプロビジョニングで使用される NAT ネットワーク プロパティ、基になる外部ネットワーク プロファイル、およびその他の値を指定します。

前提条件

- ファブリック管理者として vRealize Automation にログインします。
- 外部ネットワーク プロファイルを作成します。提供されている [IP アドレス管理エンドポイントを使用した外部ネットワーク プロファイルの作成](#)または[サードパーティの IP アドレス管理プロバイダを使用した外部ネットワーク プロファイルの作成](#)を参照してください。
- サードパーティの IP アドレス管理エンドポイントを作成および構成します。[サードパーティの IP アドレス管理プロバイダ エンドポイントの作成](#)を参照してください。

手順

- 1 [インフラストラクチャ] - [予約] - [ネットワーク プロファイル] を選択します。
- 2 [新規] をクリックし、ドロップダウン メニューから [NAT] を選択します。
- 3 名前と説明（説明は任意）を入力します。
- 4 サードパーティの IP アドレス管理プロバイダ エンドポイントを構成した場合、[IP アドレス管理エンドポイント] ドロップダウン メニューからサードパーティの IP アドレス管理エンドポイントを選択します。

vRealize Orchestrator で登録したサードパーティの IP アドレス管理プロバイダのエンドポイントを選択する場合、IP アドレスは、指定された IP アドレス管理サービス プロバイダから取得されます。サブネット マスクや DNS/WINS オプションなどの IP アドレス仕様は使用できません。これらの機能は、選択したサードパーティの IP アドレス管理エンドポイントで制御されるためです。

- 5 [外部ネットワーク プロファイル] ドロップダウン メニューから既存の外部ネットワーク プロファイルを選択します。

指定された IP アドレス管理エンドポイントを使用するように構成された外部ネットワーク プロファイルのみが、選択の候補として一覧表示されます。

- 6 [NAT タイプ] ドロップダウン メニューから 1 対 1 または 1 対多のネットワーク アドレス変換タイプを選択します。

オプション	説明
1 対 1	<p>各ネットワーク アダプタに外部固定 IP アドレスを割り当てます。すべてのマシンが外部ネットワークにアクセスでき、外部ネットワークからもアクセスできます。</p> <p>NSX Edge アップリンクに割り当てる外部 IP アドレスは、すべてが同じサブネットに属している必要があります。vRealize Automation で 1 対 1 の NAT を使用する場合、対応する外部ネットワーク プロファイルに含まれる IP アドレス範囲は、単一のサブネットに属している必要があります。</p>
1 対多	<p>ネットワーク上のすべてのマシンで 1 つの外部 IP アドレスを共有します。内部マシンには、固定 IP アドレスのみを使用できます。すべてのマシンが外部ネットワークにアクセスできますが、外部ネットワークからアクセスできるマシンはありません。</p> <p>サードパーティの IP アドレス管理プロバイダを利用して NAT を使用する場合、DHCP はサポートされません。</p> <p>NSX for vSphere の場合、1 対多の NAT 変換タイプでは、NAT ネットワーク コンポーネントをブループリントに追加するときに NAT ルールを定義できます。</p> <p>NSX for vSphere では 1 対 1 の NAT と 1 対多の NAT ネットワークをサポートしていますが、NSX-T では 1 対多の NAT のみをサポートしています。</p>

- 7 [サブネット マスク] テキスト ボックスに IP サブネット マスクを入力します。

ネットワーク プロファイルで定義するルーティング可能なアドレス空間全体のサイズは、サブネット マスクで指定します。

たとえば、255.255.0.0 のように入力します。

- 8 [ゲートウェイ] テキスト ボックスにルーティング ゲートウェイの IP アドレスを IPv4 形式（例：10.10.110.1）で入力します。

ネットワーク プロファイルで定義されたゲートウェイの IP アドレスは、割り当て時に NIC に割り当てられます。ゲートウェイ エントリは、NAT ネットワーク プロファイルで常に必要とされます。

NSX-T を使用している場合、DHCP サーバのデフォルト ゲートウェイは、NSX-T の NAT が 1 対多に設定されたデフォルト ゲートウェイにする必要があります。IP アドレス プールのデフォルト ゲートウェイは、vRealize Automation の NAT が 1 対多に設定されたデフォルト ゲートウェイと一致する必要があります。

ネットワーク プロファイルの [ゲートウェイ] テキスト ボックスに値が割り当てられない場合は、VirtualMachine.Network0.Gateway カスタム プロパティを使用してゲートウェイを割り当てる必要があります。

- 9 [DNS] タブをクリックします。

- 10 DNS と WINS の値を必要に応じて入力します。

DNS の値は、DNS 名の登録と解決に使用されます。内部 IP アドレス管理エンドポイントを使用している場合、DNS と WINS のフィールドは、オプションになります。外部 IP アドレス管理エンドポイントを使用している場合、DNS と WINS の値は、サードパーティの IP アドレス管理プロバイダによって提供されます。

a （オプション） [プライマリ DNS] サーバの値を入力します。

b （オプション） [セカンダリ DNS] サーバの値を入力します。

- c (オプション) [DNS サフィックス] の値を入力します。
- d (オプション) [DNS 検索サフィックス] の値を入力します。
- e (オプション) [優先 WINS] サーバの値を入力します。
- f (オプション) [代替 WINS] サーバの値を入力します。

次のステップ

サードパーティの IP アドレス管理エンドポイントを使用した NAT ネットワーク プロファイル IP アドレス範囲の設定。

サードパーティの IP アドレス管理エンドポイントを使用した NAT ネットワーク プロファイル IP アドレス範囲の設定

NAT を使用して、ネットワークのプロビジョニングに使用する 1 つ以上の IP アドレス範囲を定義できます。

前提条件

サードパーティの IP アドレス管理エンドポイントを使用した NAT ネットワーク プロファイル情報の指定。

手順

- 1 [ネットワーク範囲] タブをクリックして、新しいネットワーク範囲を作成するか、既存のネットワーク範囲を選択します。

選択した範囲の詳細（それぞれの名前、説明、開始 IP アドレス、終了 IP アドレスなど）が表示されます。ステータスに関する情報も表示されます。

- 2 [新規] をクリックし、ネットワーク範囲を定義します。

- a ネットワーク範囲名と説明を入力します。
- b 開始 IP アドレスと終了 IP アドレスを入力して、範囲を定義します。
- c [適用] をクリックします。

- 3 [OK] をクリックします。

IP アドレス範囲の名前が [定義された範囲] リストに表示されます。範囲内の IP アドレスが [定義された IP アドレス] リストに表示されます。

[適用] をクリックするか、ネットワーク プロファイルを保存してから編集すると、アップロードされる IP アドレスが [IP アドレス] ページに表示されます。

- 4 [IP アドレス] タブをクリックし、名前付きのネットワーク範囲の IP アドレスを表示します。

- 5 (オプション) [ネットワーク範囲] ドロップダウン メニューから IP アドレス情報を選択して、IP アドレス エントリをフィルタリングします。

定義済みのすべてのネットワーク範囲、CSV ファイルからインポートしたネットワーク範囲、または名前付きのネットワーク範囲に関する情報を表示できます。詳細には、開始 IP アドレス、マシン名、最終変更日、タイムスタンプ、IP ステータスなどが含まれます。

- 6 (オプション) [IP ステータス] ドロップダウン メニューからステータス タイプを選択して、IP アドレス エントリをフィルタリングすると、選択した IP ステータスに一致する IP アドレス エントリのみが表示されます。ステータスの設定は、[割り当て済み]、[未割り当て]、[削除済み]、[期限切れ] です。

[期限切れ] または [削除済み] 状態の IP アドレスに対して、[再要求] をクリックすると、それらの IP アドレス 範囲が割り当て可能になります。再利用を有効にするには、プロファイルを保存する必要があります。アドレスは直ちには再利用されません。したがって、[ステータス] 列も [期限切れ] または [削除済み] から [割り当て済み] へと直ちには変更されません。

- 7 [OK] をクリックします。

プロビジョニングされたマシンの破棄による IP アドレスの解放

展開したマシンを破棄すると、IP アドレスが削除されます。割り当てられている IP アドレス（たとえば、ネットワーク プロファイル範囲内の IP アドレス）は、解放されてその後のプロビジョニングで使用できるようになります。

固定 IP アドレスを持つマシンを削除すると、その IP アドレスは他のマシンで使用できるようになります。固定 IP アドレスを再要求するプロセスは 30 分ごとに実行されるため、使用されていないアドレスが即座に有効になるとは限りません。

サードパーティの IP アドレス管理プロバイダを使用している場合、vRealize Automation は、サードパーティの IP アドレス管理プロバイダ プラグインまたはパッケージの vRealize Orchestrator ワークフローを使用して、関連付けられている IP アドレスを削除します。

予約と予約ポリシーの設定

vRealize Automation 予約では、プロビジョニング要求でマシンの配置を決定するポリシー、優先順位、および割り当てを定義できます。

予約ポリシーにより、マシンのプロビジョニングが使用可能な予約のサブセットに限定されます。ストレージ予約ポリシーの使用により、ブループリント アーキテクトはマシンのポリュームを異なるデータストアに割り当てることができます。

正常にプロビジョニングするには、十分な使用可能ストレージが予約に含まれていることが必要です。予約のストレージの可用性は以下の要素によって異なります。

- データストア/クラスタで使用可能なストレージ容量。
- そのデータストア/クラスタで予約されているストレージ容量。
- vRealize Automation ですでに割り当てられているストレージ容量。

たとえば、データストア/クラスタで利用可能なストレージが vCenter Server にあっても、十分なストレージが予約されていない場合、プロビジョニングは「割り当てることができる予約はありません」というエラーと共に失敗します。予約に割り当てられるストレージは、その特定の予約に含まれる仮想マシンの数によって異なり、仮想マシンの状態には関連しません。VMware ナレッジベースの記事「Machine XXX: No reservation is available to allocate within the group XXX.Total XX GB of storage was requested (KB2151030)」を参照してください。この記事は、<http://kb.vmware.com/kb/2151030> から参照できます。

予約

vRealize Automation の予約を作成して、ファブリック グループのプロビジョニング リソースを特定のビジネス グループに割り当てることができます。

たとえば、単一コンピュート リソースの共有のメモリ、CPU、ネットワーク、およびストレージ リソースが特定のビジネス グループに属していること、または特定のマシンが特定のビジネス グループに割り当てられていることを指定するために、予約を使用できます。

ブループリント展開でのネットワーク通信の管理には、ネットワーク予約ポリシーを使用します。マシン プロビジョニングを申請する場合は、予約ポリシーを使用して、展開用に検討可能な予約をグループ化します。

複数のビジネス グループで予約を共有することはできません。

注： プロビジョニング済みのマシンに予約によって割り当てられたストレージとメモリは、割り当てられたマシンが破棄アクションによって vRealize Automation で削除されると、割り当て解除されます。vCenter Server でマシンが削除される場合は、ストレージとメモリの割り当ては解除されません。

次のマシン タイプの予約を作成できます。

- vSphere
- vCloud Air
- vCloud Director
- Amazon EC2
- Microsoft Azure
- Hyper V (SCVMM)
- Hyper-V スタンドアロン
- KVM (RHEV)
- OpenStack
- XenServer

セキュリティ設定を指定するには、予約、ブループリント、またはゲスト エージェント スクリプトで情報を指定します。プロビジョニングするマシンにゲスト エージェントが必要な場合は、その要件を含んだセキュリティ ルールを予約またはブループリントに追加する必要があります。たとえば、すべてのマシン間の通信を拒否するデフォルトのセキュリティ ポリシーを使用したうえで、特定のマシン間の通信を許可するためのセキュリティ ポリシーを別途設けた場合、カスタマイズ段階でゲスト エージェントが vRealize Automation と通信できなくなる可能性があります。このような問題がマシンのプロビジョニング中に発生しないようにするためには、カスタマイズ段階で通信を許可するデフォルトのセキュリティ ポリシーを使用します。

予約シナリオの選択

予約を作成してリソースをビジネス グループに割り当てることができます。予約の作成手順は、シナリオに応じて異なります。

ターゲットのエンドポイント タイプに基づいて予約シナリオを選択します。

特定のタイプのマシンをプロビジョニングできるように、各ビジネス グループには、そのメンバー用の予約を 1 つ以上作成する必要があります。たとえば、OpenStack の予約が設定され、Amazon の予約が設定されていないビジネス グループは、Amazon から仮想マシンを申請できません。この例ではビジネス グループに、Amazon のリソース専用の予約を 1 つ割り当てする必要があります。

表 2-15. 予約シナリオの選択

シナリオ	手順
vSphere の予約を作成する。	Hyper-V、KVM、SCVMM、vSphere、XenServer の予約の作成
vCloud Air エンドポイントのリソースを割り当てる予約を作成する。	vCloud Air の予約の作成
vCloud Director エンドポイントのリソースを割り当てる予約を作成する。	vCloud Director の予約の作成
Amazon リソースにリソースを割り当てる予約を作成する (Amazon Virtual Private Cloud の有無は問わない)。	Amazon EC2 の予約の作成
OpenStack リソースにリソースを割り当てる予約を作成する。	OpenStack 予約の作成
Hyper-V のリソースを割り当てる予約を作成する。	Hyper-V、KVM、SCVMM、vSphere、XenServer の予約の作成
KVM のリソースを割り当てる予約を作成する。	Hyper-V、KVM、SCVMM、vSphere、XenServer の予約の作成
OpenStack のリソースにリソースを割り当てる予約を作成 する。	OpenStack 予約の作成
SCVMM のリソースを割り当てる予約を作成する。	Hyper-V、KVM、SCVMM、vSphere、XenServer の予約の作成
XenServer のリソースを割り当てる予約を作成する。	Hyper-V、KVM、SCVMM、vSphere、XenServer の予約の作成
Microsoft Azure のリソースを割り当てる予約を作成する。	Microsoft Azure の予約の作成

クラウド カテゴリ予約の作成

クラウド カテゴリ タイプ予約により、特定の vRealize Automation ビジネス グループのクラウド サービス アカウントのプロビジョニング サービスにアクセスできます。使用可能なクラウド予約タイプには、Amazon、OpenStack、vCloud Air、vCloud Director が含まれます。

予約とは、特定の vRealize Automation ビジネス グループに割り当てられるコンピューティング リソースの、共有されているメモリ、CPU、ネットワーク、およびストレージ リソースの一部のことです。

ビジネス グループは、1 つのエンドポイントで複数の予約を使用するか、複数のエンドポイントで複数の予約を使用することができます。

予約の割り当てモデルは、関連付けられたデータセンターの割り当てモデルに応じて決まります。使用可能な割り当てモデルは、割り当てプール、従量課金、予約プールです。これらの割り当てモデルの詳細については、vCloud Director または vCloud Air のドキュメントを参照してください。

ビジネス グループに割り当てられたファブリック リソースの共有を定義することに加えて、予約では、マシンの配置を決定するポリシー、優先度、および割り当てを定義できます。

正常にプロビジョニングするには、十分な使用可能ストレージが予約に含まれている必要があります。予約のストレージの可用性は以下の要素によって異なります。

- データストア/クラスタで使用可能なストレージ容量。
- そのデータストア/クラスタで予約されているストレージ容量。
- vRealize Automation ですでに割り当てられているストレージ容量。

たとえば、データストア/クラスタで利用可能なストレージが vCenter Server にあっても、十分なストレージが予約されていない場合、プロビジョニングは「割り当てることができる予約はありません」というエラーと共に失敗します。予約に割り当てられるストレージは、その特定の予約に含まれる仮想マシンの数によって異なり、仮想マシンの状態には関連しません。VMware ナレッジベースの記事「Machine XXX: No reservation is available to allocate within the group XXX.Total XX GB of storage was requested (KB2151030)」を参照してください。この記事は、<http://kb.vmware.com/kb/2151030> から参照できます。

クラウド予約の選択ロジックについて

ビジネス グループのメンバーがクラウド マシンのプロビジョニング申請を作成するとき、vRealize Automation は、そのビジネス グループが利用できる予約の 1 つからマシンを選択します。クラウド予約には、Amazon、OpenStack、vCloud Air、および vCloud Director が含まれます。

マシンをプロビジョニングする予約は、次の基準を満たす必要があります。

- 予約のプラットフォーム タイプは、マシンの申請元であるブループリントと同じでなければならない。
- 予約は有効状態である必要がある。
- 予約は、そのマシン割り当てに容量が残っている状態か、または無制限の割り当てが指定された状態でなければならない。

割り当てられたマシン割り当てには、パワーオン状態のマシンだけが含まれます。たとえば、予約の割り当てが 50 で、40 台のマシンがすでにプロビジョニングされているが、そのうちの 20 台だけがパワーオン状態の場合、予約の割り当ては（80 パーセントではなく）40 パーセントが割り当てられていることになります。

- 予約には、マシン申請で指定されたセキュリティ グループが含まれていなければならない。
- 予約は、ブループリントで指定されたマシン イメージを持つ領域と関連付けられていなければならない。
- 予約には、マシンをプロビジョニングするのに十分な未割り当てメモリ リソースと未割り当てストレージ リソースがなければならない。

従量課金予約では、リソースの制限はありません。

- Amazon マシンの場合、申請では、可用性ゾーンと、マシンにプロビジョニングされるサブネットが Virtual Private Cloud (VPC) 内のものか VPC 以外の場所かを指定する。予約は、ネットワーク タイプ（VPC または VPC 以外）に一致していなければならない。
- vCloud Air または vCloud Director の場合、申請で割り当てモデルを指定する場合は、予約に関連付けられた仮想データセンターに同じ割り当てモデルがなければならない。
- vCloud Director または vCloud Air の場合、指定された組織が有効でなければならない。
- ブループリント テンプレートが予約で利用できなければならない。予約ポリシーが複数のリソースとマップする場合、テンプレートはパブリックでなければならない。
- クラウド プロバイダがネットワーク選択をサポートし、ブループリントに具体的なネットワーク設定値が構成されている場合、それらの同じネットワークが予約に指定されている必要がある。

ブループリントまたは予約に固定 IP アドレス割り当てのネットワーク プロファイルが指定されている場合、新しいマシンに割り当てる IP アドレスを使用する必要があります。

- 申請で割り当てモデルを指定する場合、予約内の割り当てモデルと申請内の割り当てモデルが一致していなければならない。

- ブループリントで予約ポリシーが指定される場合、予約はその予約ポリシーに属している必要がある。

予約ポリシーは、特定のブループリントからのマシンのプロビジョニングに対する付加的な要件のすべてを、選択された予約が満たしていることを保証する方法の 1 つです。たとえば、ブループリントで特定のマシン イメージを使用する場合、予約ポリシーを使用して、必要なイメージを持つ領域と関連付けられた予約にプロビジョニングを制限できます。

選択基準のすべてを満たす予約が存在しないと、プロビジョニングは失敗します。

すべての基準を満たす予約が複数存在する場合、申請されたマシンのプロビジョニングに使用される予約は、次のロジックで決定されます。

- 優先度の値が高い予約が選択される前に、優先度の値が低い予約が選択される。
- 複数の予約に同じ優先度が指定されている場合、マシン割り当ての割り当て率が最も低い予約が選択される。
- 複数の予約の優先度と割り当ての使用状況が同じである場合、ラウンド ロビン方式でマシンが複数の予約にわたって分散される。

注： ネットワーク プロファイルでラウンド ロビンを選択することはできませんが、ネットワーク（存在する場合）でラウンド ロビンを選択し、さまざまなネットワーク プロファイルに関連付けることができます。

予約に利用できるストレージ パスとして、マシン ボリュームをプロビジョニングするうえで十分な容量を持つものが複数存在する場合は、次のロジックに従ってストレージ パスが選択されます。

- 優先度の値が高いストレージ パスが選択される前に、優先度の値が低いストレージ パスが選択される。
- ブループリントまたは申請でストレージ予約ポリシーが指定されている場合、ストレージ パスはそのストレージ予約ポリシーに属している必要がある。

カスタム プロパティ `VirtualMachine.DiskN.StorageReservationPolicyMode` が `NotExact` に設定され、十分な容量のストレージ パスがストレージ予約ポリシー内に存在しない場合、指定されたストレージ予約ポリシーに属していないストレージ パスを使用してプロビジョニングが進められます。

`VirtualMachine.DiskN.StorageReservationPolicyMode` のデフォルト値は `Exact` です。

- 複数のストレージ パスの優先度が同じである場合、ラウンド ロビン方式のスケジュールでマシンが複数のストレージ パスにわたって分散されます。

Amazon EC2 の予約の作成

ビジネス グループのメンバーがマシン プロビジョニングを申請できるようにするには、事前に予約を作成して、マシンにリソースを割り当てておく必要があります。

Amazon Virtual Private Cloud または Amazon VPC 以外に対応する Amazon の予約を操作できます。

Amazon Web Services ユーザーは Amazon Virtual Private Cloud を作成し、仕様に従って仮想ネットワーク トポロジを設計できます。Amazon VPC の使用を計画している場合は、Amazon VPC を vRealize Automation の予約に割り当てする必要があります。

Amazon の予約を作成したり、ブループリントのマシン コンポーネントを構成するときは、指定された Amazon リージョンで使用可能なセキュリティ グループのリストから選択できます。セキュリティ グループは、データ収集時にインポートされます。

注： 予約を作成した後、ビジネス グループまたはコンピュート リソースの関連付けを変更することはできません。

AWS Management Console を使用して Amazon VPC を作成する方法については、Amazon Web Services のドキュメントを参照してください。

手順

1 Amazon の予約情報の指定

各予約は特定のビジネス グループ用に構成されており、特定のコンピュート リソース上のマシンを申請できるようにアクセスが許可されています。

2 Amazon の予約用のリソースおよびネットワーク設定の指定

この vRealize Automation の予約からマシンをプロビジョニングするためのリソースおよびネットワークの設定を指定します。

3 Amazon の予約用のカスタム プロパティとアラートの指定

カスタム プロパティを vRealize Automation の予約に関連付けることができます。また予約リソースが低下すると電子メール通知を送信するように、アラートを構成することもできます。

Amazon の予約情報の指定

各予約は特定のビジネス グループ用に構成されており、特定のコンピュート リソース上のマシンを申請できるようにアクセスが許可されています。


注： 予約を作成した後、ビジネス グループまたはコンピュート リソースの関連付けを変更することはできません。

追加、編集、または削除時に予約の表示を制御するには、[予約] ページの [カテゴリ別にフィルタ] オプションを使用します。カテゴリ別のフィルタを行うと、予約リストにテスト エージェントの予約は表示されないことに注意してください。

前提条件

- ファブリック管理者として vRealize Automation にログインします。
- テナント管理者によって少なくとも 1 つのビジネス グループが作成されていることを確認します。
- コンピュート リソースが存在することを確認します。
- ネットワーク設定を構成します。
- (オプション) ネットワーク プロファイル情報を構成します。
- 目的の Amazon ネットワークにアクセスできることを確認してください。たとえば VPC を使用する場合は、Amazon Virtual Private Cloud (VPC) ネットワークにアクセスできることを確認します。
- 必要なキー ペアが存在することを確認します。 [キー ペアの管理](#)を参照してください。

手順

- 1 [インフラストラクチャ] - [予約] - [予約] を選択します。
- 2 [新規] アイコン () をクリックして、作成する予約のタイプを選択します。
[Amazon EC2] を選択します。
- 3 [名前] テキスト ボックスに名前を入力します。

4 [テナント] ドロップダウン メニューから、テナントを選択します。

5 [ビジネス グループ] ドロップダウン メニューから、ビジネス グループを選択します。

この予約を使用してマシンをプロビジョニングできるのは、このビジネス グループ内のユーザーだけです。

6 (オプション) [予約ポリシー] ドロップダウン メニューから、予約ポリシーを選択します。

このオプションを選択するには、1つ以上の予約ポリシーが存在している必要があります。後で予約を編集して予約ポリシーを指定できます。

予約ポリシーを使用すると、プロビジョニングを特定の予約に制限することができます。

7 [優先度] テキスト ボックスに数値を入力し、予約の優先度を設定します。

優先度は、ビジネス グループに複数の予約が存在する場合に使用されます。優先度 1 の予約は、優先 2 の予約よりも優先的にプロビジョニングに使用されます。

8 (オプション) この予約をアクティブにしない場合は、[この予約を有効にする] チェック ボックスの選択を解除します。

結果

このページから移動しないでください。予約は完了していません。

Amazon の予約用のリソースおよびネットワーク設定の指定

この vRealize Automation の予約からマシンをプロビジョニングするためのリソースおよびネットワークの設定を指定します。

Amazon の予約を作成したり、ブループリントのマシン コンポーネントを構成するときは、指定された Amazon アカウントのリージョンで使用可能なセキュリティ グループのリストから選択できます。セキュリティ グループは、データ収集時にインポートされます。セキュリティ グループは、マシンへのアクセスを制御するファイアウォールとして機能します。各リージョンには、最低 1 つのデフォルトのセキュリティ グループが用意されています。管理者は Amazon Web Services Management Console を使用して、追加のセキュリティ グループの作成、Microsoft Remote Desktop Protocol または SSH のポートの構成、Amazon VPN の仮想プライベート ネットワークの設定を行うことができます。Amazon Web Services でのセキュリティ グループの作成と使用に関する詳細については、Amazon のドキュメントを参照してください。

ロード バランサの詳細については、vRealize Automation の構成を参照してください。

前提条件

[Amazon の予約情報の指定。](#)

手順

1 [リソース] タブをクリックします。

2 [コンピュート リソース] ドロップダウン メニューから、マシンをプロビジョニングするコンピュート リソースを選択します。

利用可能な Amazon のリージョンがリストに表示されます。

- 3 (オプション) [マシン割り当て] テキスト ボックスに数値を入力し、この予約でプロビジョニングできるマシンの最大数を設定します。

割り当てに加えられるのは、パワーオン状態のマシンだけです。予約を無制限にするには空白にします。

- 4 [キー ペア] ドロップダウン メニューから、コンピュー ト インスタンスにキー ペアを割り当てる方法を選択します。

オプション	説明
未指定	予約レベルではなく、ブループリント レベルでキー ペアの動作を制御します。
ビジネス グループ毎に自動生成	同じコンピュー ト リソースとビジネス グループが存在する場合に他の予約でプロビジョニングされるマシンを含め、同じビジネス グループでプロビジョニングされるマシンはすべて、キー ペアが同じです。この方法で生成されるキー ペアはビジネス グループに関連付けられるため、ビジネス グループが削除されるときにはキー ペアも削除されます。
マシン毎に自動生成	各マシンには一意のキー ペアがあります。どのキー ペアも複数のマシンで共有されることはないため、これは最も安全な方法です。
特定のキー ペア	この予約でプロビジョニングされるマシンはすべて、同じキー ペアを持ちます。この予約に使用するキー ペアを参照します。

- 5 [キー ペア] ドロップダウン メニューで [特定のキー ペア] を選択した場合は、[特定のキー ペア] ドロップダウン メニューからキー ペア値を選択します。

- 6 Amazon Virtual Private Cloud が構成されている場合は、[VPC のサブネットに割り当て] チェック マーク ボックスをオンにします。 それ以外の場合は、ボックスをオフにします。

[VPC のサブネットに割り当て] をオンにした場合は、この同じページではなくポップアップ メニューに、次の場所またはサブネット、セキュリティ グループ、ロード バランサのオプションが表示されます。

VPC 予約の場合、予約で許可されるそれぞれの VPC に対してセキュリティ グループとサブネットを指定します。

- 7 [場所] または [サブネット] リストから、1 つ以上の利用可能な場所 (VPC 以外) またはサブネット (VPC) を選択します。

プロビジョニングで使用する利用可能な各場所またはサブネットを選択します。

- 8 [セキュリティ グループ] リストから、プロビジョニング時にマシンに割り当てることができる 1 つ以上のセキュリティ グループを選択します。

プロビジョニング中にマシンに割り当てることができる各セキュリティ グループを選択します。使用可能な各リージョンには、少なくとも 1 つのセキュリティ グループが指定されている必要があります。

- 9 [ロード バランサ] リストから 1 つ以上の使用可能なロード バランサを選択します。

Elastic ロード バランサ機能を使用する場合は、選択した場所またはサブネットに適用される 1 つ以上の利用可能なロード バランサを選択します。

結果

今すぐ予約を保存するには、[保存] をクリックします。 カスタム プロパティを追加して予約仕様をさらに詳細に制御することもできます。 また、この予約に割り当てられたリソースが残り少なくなったときにメール通知を送信するように、アラートを構成することもできます。

Amazon の予約用のカスタム プロパティとアラートの指定

カスタム プロパティを vRealize Automation の予約に関連付けることができます。また予約リソースが低下すると電子メール通知を送信するように、アラートを構成することもできます。

カスタム プロパティと電子メール アラートは、予約のオプション構成です。カスタム プロパティの関連付けやアラートの設定を行う必要がない場合は、[保存] をクリックして予約の作成を終了します。

カスタム プロパティは必要なだけいくつでも追加できます。

アラートを構成すると、指定されたしきい値に達した時点ではなく、毎日アラートが生成されます。

重要： 通知は、メール アラートが構成され、かつ通知が有効になっている場合のみ、送信されます。

前提条件

Amazon の予約用のリソースおよびネットワーク設定の指定。

手順

- 1 [プロパティ] タブをクリックします。
- 2 [新規] をクリックします。
- 3 有効なカスタム プロパティ名を入力します。
- 4 必要に応じて、プロパティ値を入力します。
- 5 [保存] をクリックします。
- 6 (オプション) その他のカスタム プロパティを追加します。
- 7 [アラート] タブをクリックします。
- 8 アラートが送信されるように構成するには、[容量アラート] チェック ボックスを選択します。
- 9 スライダを使用して、使用可能なリソース割り当てのしきい値を設定します。
- 10 アラート通知を受信するには、[受信者] テキスト ボックスに Active Directory ユーザーまたはグループの名前 (E メール アドレスではない) を入力します。
各行に名前を入力します。複数のエントリを区切るには、Enter を押します。
- 11 メール アラートにグループ マネージャを含めるには、[グループ マネージャにアラートを送信] を選択します。
E メール アラートは、ビジネス グループの [マネージャの Eメールの送信先] リストに含まれるユーザーに送信されます。
- 12 リマインダーの頻度 (日数) を指定します。
- 13 [保存] をクリックします。

結果

予約が保存され、[予約] リストに表示されます。

次のステップ

必要に応じて予約ポリシーを構成するか、プロビジョニングの予約を開始します。

ブループリントを作成する権限を持つユーザーは、すぐにブループリントを作成できます。

OpenStack 予約の作成

ビジネス グループのメンバーがマシン プロビジョニングを申請できるようにするには、事前に予約を作成して、マシンにリソースを割り当てておく必要があります。

OpenStack 予約を作成します。

手順

1 OpenStack 予約情報の指定

各予約は特定のビジネス グループ用に構成されており、特定のコンピュート リソース上のマシンを申請できるようにアクセスが許可されています。

2 OpenStack 予約用のリソースおよびネットワーク設定の指定

この vRealize Automation 予約からプロビジョニングされるマシンで利用できるリソースおよびネットワークの設定を指定します。

3 OpenStack 予約用のカスタム プロパティとアラートの指定

カスタム プロパティを vRealize Automation の予約に関連付けることができます。また予約リソースが低下すると電子メール通知を送信するように、アラートを構成することもできます。

OpenStack 予約情報の指定

各予約は特定のビジネス グループ用に構成されており、特定のコンピュート リソース上のマシンを申請できるようにアクセスが許可されています。

注： 予約を作成した後、ビジネス グループまたはコンピュート リソースの関連付けを変更することはできません。


追加、編集、または削除時に予約の表示を制御するには、[予約] ページの [カテゴリ別にフィルタ] オプションを使用します。カテゴリ別のフィルタを行うと、予約リストにテスト エージェントの予約は表示されないことに注意してください。

前提条件

- ファブリック管理者として vRealize Automation にログインします。
- テナント管理者によって少なくとも 1 つのビジネス グループが作成されていることを確認します。
- コンピュート リソースが存在することを確認します。
- 任意のセキュリティ グループまたは浮動 IP アドレスが構成されていることを確認します。
- 必要なキー ペアが存在することを確認します。 [キー ペアの管理](#)を参照してください。
- コンピュート リソースが存在することを確認します。
- ネットワーク設定を構成します。

手順

- 1 [インフラストラクチャ] - [予約] - [予約] を選択します。

- 2 [新規] アイコン () をクリックして、作成する予約のタイプを選択します。

[OpenStack] を選択します。

- 3 [名前] テキスト ボックスに名前を入力します。

- 4 [テナント] ドロップダウン メニューから、テナントを選択します。

- 5 [ビジネス グループ] ドロップダウン メニューから、ビジネス グループを選択します。

この予約を使用してマシンをプロビジョニングできるのは、このビジネス グループ内のユーザーだけです。

- 6 (オプション) [予約ポリシー] ドロップダウン メニューから、予約ポリシーを選択します。

このオプションを選択するには、1 つ以上の予約ポリシーが存在している必要があります。 後で予約を編集して予約ポリシーを指定できます。

予約ポリシーを使用すると、プロビジョニングを特定の予約に制限することができます。

- 7 [優先度] テキスト ボックスに数値を入力し、予約の優先度を設定します。

優先度は、ビジネス グループに複数の予約が存在する場合に使用されます。優先度 1 の予約は、優先 2 の予約よりも優先的にプロビジョニングに使用されます。

- 8 (オプション) この予約をアクティブにしない場合は、[この予約を有効にする] チェック ボックスの選択を解除します。

結果

このページから移動しないでください。予約は完了していません。

OpenStack 予約用のリソースおよびネットワーク設定の指定

この vRealize Automation 予約からプロビジョニングされるマシンで利用できるリソースおよびネットワークの設定を指定します。

前提条件

[OpenStack 予約情報の指定。](#)

手順

- 1 [リソース] タブをクリックします。

- 2 [コンピュート リソース] ドロップダウン メニューから、マシンをプロビジョニングするコンピュート リソースを選択します。

この予約でクローンの作成に使用できるのは、選択したクラスタ上に存在するテンプレートのみです。

プロビジョニングの際に、ローカル ストレージに接続されたホストにマシンが配置されます。予約でローカル ストレージが使用されている場合は、予約によってプロビジョニングされるすべてのマシンが、このローカル ストレージを格納しているホストに作成されます。ただし、VirtualMachine.Admin.ForceHost カスタム プロパティを使用する場合は、マシンが強制的に別のホストにプロビジョニングされるため、プロビジョニングが失敗します。また、マシンのクローン作成に使用したテンプレートがローカル ストレージに存在するものの、別のクラスタ上のマシンに接続されている場合にも、プロビジョニングが失敗します。この場合は、テンプレートにアクセスできないことが原因でプロビジョニングが失敗します。

- 3 (オプション) [マシン割り当て] テキスト ボックスに数値を入力し、この予約でプロビジョニングできるマシンの最大数を設定します。

割り当てに加えられるのは、パワーオン状態のマシンだけです。予約を無制限にするには空白にします。

- 4 [キー ペア] ドロップダウン メニューから、コンピュート インスタンスにキー ペアを割り当てる方法を選択します。

オプション	説明
未指定	予約レベルではなく、ブループリント レベルでキー ペアの動作を制御します。
ビジネス グループ毎に自動生成	同じコンピュート リソースとビジネス グループが存在する場合に他の予約でプロビジョニングされるマシンを含め、同じビジネス グループでプロビジョニングされるマシンはすべて、キー ペアが同じです。この方法で生成されるキー ペアはビジネス グループに関連付けられるため、ビジネス グループが削除されるときにはキー ペアも削除されます。
マシン毎に自動生成	各マシンには一意のキー ペアがあります。どのキー ペアも複数のマシンで共有されることはないため、これは最も安全な方法です。
特定のキー ペア	この予約でプロビジョニングされるマシンはすべて、同じキー ペアを持ちます。この予約に使用するキー ペアを参照します。

- 5 [キー ペア] ドロップダウン メニューで [特定のキー ペア] を選択した場合は、[特定のキー ペア] ドロップダウン メニューからキー ペア値を選択します。
- 6 [セキュリティ グループ] リストから、プロビジョニング時にマシンに割り当てることができる 1 つ以上のセキュリティ グループを選択します。
- 7 [ネットワーク] タブをクリックします。
- 8 この予約を使用してプロビジョニングされるマシンのネットワーク パスを構成します。

- a (オプション) オプションが使用できる場合、[エンドポイント] ドロップダウン メニューからストレージ エンドポイントを選択します。

NetApp ONTAP エンドポイントが存在しており、なおかつホストが仮想である場合は、FlexClone オプションがエンドポイント列に表示されます。 NetApp ONTAP エンドポイントが存在する場合は、ストレージ パスに割り当てられたエンドポイントが [予約] ページに表示されます。 ストレージ パスのエンドポイントを追加、アップデート、または削除すると、すべての該当する予約に変更内容が表示されます。

ストレージ パスのエンドポイントを追加、アップデート、または削除すると、[予約] ページに変更内容が表示されます。

- b この予約でプロビジョニングするマシンに対して [ネットワーク アダプタ] を 1 つ以上選択します。
- c (オプション) 選択した各ネットワーク アダプタに対して利用可能な [ネットワーク プロファイル] を選択します。
- d (オプション) 詳細設定が選択可能な場合は、[トランスポート ゾーン] と、ロード バランサを含むブループリントを展開する際に使用する [Tier 0 分散論理ルーター] を選択します。

トランスポート ゾーンは、ネットワーク アダプタの転送範囲にどのクラスタを含めるかを定義します。トランスポート ゾーンが予約とブループリントの両方に指定されている場合は、トランスポート ゾーンの各値が一致している必要があります。

1つの予約に複数のネットワーク アダプタを選択できますが、マシンをプロビジョニングするときに使用されるのは1つのネットワークだけです。

結果

今すぐ予約を保存するには、[保存] をクリックします。 カスタム プロパティを追加して予約仕様をさらに詳細に制御することもできます。 また、この予約に割り当てられたリソースが残り少なくなったときにメール通知を送信するように、アラートを構成することもできます。

OpenStack 予約用のカスタム プロパティとアラートの指定

カスタム プロパティを vRealize Automation の予約に関連付けることができます。また予約リソースが低下すると電子メール通知を送信するように、アラートを構成することもできます。

カスタム プロパティと電子メール アラートは、予約のオプション構成です。 カスタム プロパティの関連付けやアラートの設定を行う必要がない場合は、[保存] をクリックして予約の作成を終了します。

カスタム プロパティは必要なだけいくつでも追加できます。

重要： 通知は、メール アラートが構成され、かつ通知が有効になっている場合のみ、送信されます。

アラートを構成すると、指定されたしきい値に達した時点ではなく、毎日アラートが生成されます。

前提条件

[OpenStack 予約用のリソースおよびネットワーク設定の指定。](#)

手順

- 1 [プロパティ] タブをクリックします。
- 2 [新規] をクリックします。
- 3 有効なカスタム プロパティ名を入力します。
- 4 必要に応じて、プロパティ値を入力します。
- 5 [保存] をクリックします。
- 6 (オプション) その他のカスタム プロパティを追加します。
- 7 [アラート] タブをクリックします。
- 8 アラートが送信されるように構成するには、[容量アラート] チェック ボックスを選択します。
- 9 スライダを使用して、使用可能なリソース割り当てのしきい値を設定します。
- 10 アラート通知を受信するには、[受信者] テキスト ボックスに Active Directory ユーザーまたはグループの名前 (E メール アドレスではない) を入力します。

各行に名前を入力します。複数のエントリを区切るには、Enter を押します。

- 11 メール アラートにグループ マネージャを含めるには、[グループ マネージャにアラートを送信] を選択します。
E メール アラートは、ビジネス グループの [マネージャの Eメールの送信先] リストに含まれるユーザーに送信されます。

- 12 リマインダーの頻度 (日数) を指定します。

13 [保存] をクリックします。

結果

予約が保存され、[予約] リストに表示されます。

次のステップ

必要に応じて予約ポリシーを構成するか、プロビジョニングの予約を開始します。

ブループリントを作成する権限を持つユーザーは、すぐにブループリントを作成できます。

vCloud Air の予約の作成

ビジネス グループのメンバーがマシン プロビジョニングを申請する前に、vRealize Automation の予約を作成して、マシンにリソースを割り当てる必要があります。

各ビジネス グループには、そのメンバー用の予約を 1 つ以上作成し、そのタイプのマシンをプロビジョニングできるようにする必要があります。

手順

1 vCloud Air 予約情報の指定

vCloud Air マシンのサブスクリプションまたは OnDemand リソースごとに予約を作成できます。各予約は特定のビジネス グループ用に構成されており、マシンを申請できるようにアクセスが許可されています。

2 vCloud Air の予約用のリソースおよびネットワーク設定の指定

この vRealize Automation の予約からプロビジョニングされる vCloud Air マシンで利用できるリソースおよびネットワークの設定を指定します。

3 vCloud Air 予約用のカスタム プロパティとアラートの指定

カスタム プロパティを vRealize Automation の予約に関連付けることができます。また予約リソースが低下すると電子メール通知を送信するように、アラートを構成することもできます。

vCloud Air 予約情報の指定

vCloud Air マシンのサブスクリプションまたは OnDemand リソースごとに予約を作成できます。各予約は特定のビジネス グループ用に構成されており、マシンを申請できるようにアクセスが許可されています。

追加、編集、または削除時に予約の表示を制御するには、[予約] ページの [カテゴリ別にフィルタ] オプションを使用します。カテゴリ別のフィルタを行うと、予約リストにテスト エージェントの予約は表示されないことに注意してください。

注： 予約を作成した後、ビジネス グループまたはコンピュート リソースの関連付けを変更することはできません。


前提条件

- ファブリック管理者として vRealize Automation にログインします。
- テナント管理者によって少なくとも 1 つのビジネス グループが作成されていることを確認します。
- コンピュート リソースが存在することを確認します。
- ネットワーク設定を構成します。

- (オプション) ネットワーク プロファイル情報を構成します。

手順

- 1 [インフラストラクチャ] - [予約] - [予約] を選択します。

- 2 [新規] アイコン () をクリックして、作成する予約のタイプを選択します。

選択可能なクラウド予約のタイプとして、Amazon、OpenStack、vCloud Air、および vCloud Director があります。

[vCloud Air] を選択します。

- 3 [名前] テキスト ボックスに名前を入力します。

- 4 [テナント] ドロップダウン メニューから、テナントを選択します。

- 5 [ビジネス グループ] ドロップダウン メニューから、ビジネス グループを選択します。

この予約を使用してマシンをプロビジョニングできるのは、このビジネス グループ内のユーザーだけです。

- 6 (オプション) [予約ポリシー] ドロップダウン メニューから、予約ポリシーを選択します。

このオプションを選択するには、1 つ以上の予約ポリシーが存在している必要があります。後で予約を編集して予約ポリシーを指定できます。

予約ポリシーを使用すると、プロビジョニングを特定の予約に制限することができます。

- 7 [優先度] テキスト ボックスに数値を入力し、予約の優先度を設定します。

優先度は、ビジネス グループに複数の予約が存在する場合に使用されます。優先度 1 の予約は、優先 2 の予約よりも優先的にプロビジョニングに使用されます。

- 8 (オプション) この予約をアクティブにしない場合は、[この予約を有効にする] チェック ボックスの選択を解除します。

結果

このページから移動しないでください。予約は完了していません。

vCloud Air の予約用のリソースおよびネットワーク設定の指定

この vRealize Automation の予約からプロビジョニングされる vCloud Air マシンで使用できるリソースおよびネットワークの設定を指定します。

vCloud Director の予約からプロビジョニングされるマシンで使用できるリソース割り当てモデルは、割り当てプール、従量課金、および予約プールです。従量課金の場合、ストレージまたはメモリの容量を指定する必要はありませんが、ストレージ パスの優先度を指定する必要があります。これらの割り当てモデルの詳細については、vCloud Air のドキュメントを参照してください。

標準またはディスクレベルのストレージ プロファイルを指定できます。マルチレベル ディスク ストレージは vCloud Air エンドポイントで利用可能です。

Storage Distributed Resource Scheduler (SDRS) ストレージを使用する統合の場合、ストレージ クラスタを選択することで、この予約からプロビジョニングされるマシンのストレージの配置やロード バランシングを、SDRS によって自動的に処理することができます。 SDRS 自動化モードは [自動] に設定しておく必要があります。 そうしない場合は、クラスタ内でスタンドアロン データストアとして動作させるデータストアを選択してください。 FlexClone ストレージ デバイスでは、SDRS はサポートされていません。

注： vCloud Air エンドポイントと vCloud Director エンドポイント用に定義された予約では、マシンのプロビジョニングにネットワーク プロファイルを使用できません。

前提条件

[vCloud Director 予約情報の指定](#).

手順

1 [リソース] タブをクリックします。

2 [コンピュート リソース] ドロップダウン メニューから、マシンをプロビジョニングするコンピュート リソースを選択します。

この予約でクローンの作成に使用できるのは、選択したクラスタ上に存在するテンプレートのみです。

3 割り当てモデルを選択します。

4 (オプション) [マシン割り当て] テキスト ボックスに数値を入力し、この予約でプロビジョニングできるマシンの最大数を設定します。

割り当てに加えられるのは、パワーオン状態のマシンだけです。予約を無制限にするには空白にします。

5 [メモリ] テーブルから、この予約に割り当てるメモリの量を GB 単位で指定します。

予約に必要な全体のメモリ値は、選択したコンピュート リソースから計算されます。

6 1 つ以上のリストされたストレージ パスを選択します。

使用可能なストレージ パスのオプションは、選択したコンピュート リソースから導出されます。

a [この予約が予約されました] テキスト ボックスに値を入力し、この予約に割り当てるストレージ容量を指定します。

b [優先度] テキスト ボックスに数値を入力し、ストレージ パスの優先度を、この予約に属する他のストレージ パスに対する相対優先度として指定します。

優先度は、複数のストレージ パスに対して使用します。優先度 0 のストレージ パスは、優先度 1 のパスよりも先に使用されます。

c この予約でストレージ パスを使用しないようにするには、[無効] オプションをクリックします。

d この手順を繰り返して、クラスタおよびデータストアを必要に応じて構成します。

7 [ネットワーク] タブをクリックします。

8 この予約を使用してプロビジョニングされるマシンのネットワーク パスを構成します。

- a (オプション) オプションが使用できる場合、[エンドポイント] ドロップダウン メニューからストレージ エンドポイントを選択します。

NetApp ONTAP エンドポイントが存在しており、なおかつホストが仮想である場合は、FlexClone オプションがエンドポイント列に表示されます。 NetApp ONTAP エンドポイントが存在する場合は、ストレージ パスに割り当てられたエンドポイントが [予約] ページに表示されます。 ストレージ パスのエンドポイントを追加、アップデート、または削除すると、すべての該当する予約に変更内容が表示されます。

ストレージ パスのエンドポイントを追加、アップデート、または削除すると、[予約] ページに変更内容が表示されます。

- b この予約でプロビジョニングするマシンに対して [ネットワーク アダプタ] を 1 つ以上選択します。
- c (オプション) 選択した各ネットワーク アダプタに対して利用可能な [ネットワーク プロファイル] を選択します。
- d (オプション) 詳細設定が選択可能な場合は、[トランスポート ゾーン] と、ロード バランサを含むブループリントを展開する際に使用する [Tier 0 分散論理ルーター] を選択します。

トランスポート ゾーンは、ネットワーク アダプタの転送範囲にどのクラスタを含めるかを定義します。トランスポート ゾーンが予約とブループリントの両方に指定されている場合は、トランスポート ゾーンの各値が一致している必要があります。

1 つの予約に複数のネットワーク アダプタを選択できますが、マシンをプロビジョニングするときに使用されるのは 1 つのネットワークだけです。

結果

今すぐ予約を保存するには、[保存] をクリックします。 カスタム プロパティを追加して予約仕様をさらに詳細に制御することもできます。 また、この予約に割り当てられたリソースが残り少なくなったときにメール通知を送信するように、アラートを構成することもできます。

vCloud Air 予約用のカスタム プロパティとアラートの指定

カスタム プロパティを vRealize Automation の予約に関連付けることができます。また予約リソースが低下すると電子メール通知を送信するように、アラートを構成することもできます。

カスタム プロパティと電子メール アラートは、予約のオプション構成です。 カスタム プロパティの関連付けやアラートの設定を行う必要がない場合は、[保存] をクリックして予約の作成を終了します。

カスタム プロパティは必要なだけいくつでも追加できます。

アラートを構成すると、指定されたしきい値に達した時点ではなく、毎日アラートが生成されます。

重要： 通知は、メール アラートが構成され、かつ通知が有効になっている場合のみ、送信されます。

アラートは、制限の指定なしで作成された従量課金の予約には使用できません。

前提条件

[vCloud Air の予約用のリソースおよびネットワーク設定の指定](#)

手順

- 1 [プロパティ] タブをクリックします。
- 2 [新規] をクリックします。
- 3 有効なカスタム プロパティ名を入力します。
- 4 必要に応じて、プロパティ値を入力します。
- 5 (オプション) プロパティ値を暗号化するには、[暗号化済み] チェック ボックスを選択します。
- 6 (オプション) ユーザーに値の入力を求めるには、[プロンプト表示] チェック ボックスを選択します。
このオプションは、プロビジョニングのときにオーバーライドされることはありません。
- 7 [保存] をクリックします。
- 8 (オプション) その他のカスタム プロパティを追加します。
- 9 [アラート] タブをクリックします。
- 10 アラートが送信されるように構成するには、[容量アラート] チェック ボックスを選択します。
- 11 スライダを使用して、使用可能なリソース割り当てのしきい値を設定します。
- 12 アラート通知を受信するには、[受信者] テキスト ボックスに Active Directory ユーザーまたはグループの名前 (E メール アドレスではない) を入力します。
各行に名前を入力します。複数のエントリを区切るには、Enter を押します。
- 13 メール アラートにグループ マネージャを含めるには、[グループ マネージャにアラートを送信] を選択します。
E メール アラートは、ビジネス グループの [マネージャの Eメールの送信先] リストに含まれるユーザーに送信されます。
- 14 リマインダーの頻度 (日数) を指定します。
- 15 [保存] をクリックします。

結果

予約が保存され、[予約] リストに表示されます。

vCloud Director の予約の作成

ビジネス グループのメンバーがマシン プロビジョニングを申請する前に、vRealize Automation の予約を作成して、マシンにリソースを割り当てる必要があります。

各ビジネス グループには、そのメンバー用の予約を 1 つ以上作成し、そのタイプのマシンをプロビジョニングできるようにする必要があります。

手順**1 vCloud Director 予約情報の指定**

vCloud Director の組織の仮想データセンター (VDC) ごとに予約を作成できます。各予約は特定のビジネス グループ用に構成されており、特定のコンピュート リソース上のマシンを申請できるようにアクセスが許可されています。

2 vCloud Director の予約用のリソースおよびネットワーク設定の指定

この vRealize Automation の予約からプロビジョニングされる vCloud Director マシンで使用できるリソースおよびネットワークの設定を指定します。

3 vCloud Director の予約用のカスタム プロパティとアラートの指定

カスタム プロパティを vRealize Automation の予約に関連付けることができます。また予約リソースが低下すると電子メール通知を送信するように、アラートを構成することもできます。

次のステップ

必要に応じて予約ポリシーを構成するか、プロビジョニングの予約を開始します。

ブループリントを作成する権限を持つユーザーは、すぐにブループリントを作成できます。

vCloud Director 予約情報の指定

vCloud Director の組織の仮想データセンター (VDC) ごとに予約を作成できます。各予約は特定のビジネスグループ用に構成されており、特定のコンピュート リソース上のマシンを申請できるようにアクセスが許可されています。


追加、編集、または削除時に予約の表示を制御するには、[予約] ページの [カテゴリ別にフィルタ] オプションを使用します。カテゴリ別のフィルタを行うと、予約リストにテスト エージェントの予約は表示されないことに注意してください。

注： 予約を作成した後、ビジネス グループまたはコンピュート リソースの関連付けを変更することはできません。

前提条件

- ファブリック管理者として vRealize Automation にログインします。
- テナント管理者によって少なくとも 1 つのビジネス グループが作成されていることを確認します。
- コンピュート リソースが存在することを確認します。
- ネットワーク設定を構成します。
- (オプション) ネットワーク プロファイル情報を構成します。

手順

- 1 [インフラストラクチャ] - [予約] - [予約] を選択します。
- 2 [新規] アイコン () をクリックして、作成する予約のタイプを選択します。
 選択可能なクラウド予約のタイプとして、Amazon、OpenStack、vCloud Air、および vCloud Director があります。
 [vCloud Director] を選択します。
- 3 [名前] テキスト ボックスに名前を入力します。
- 4 [テナント] ドロップダウン メニューから、テナントを選択します。
- 5 [ビジネス グループ] ドロップダウン メニューから、ビジネス グループを選択します。
 この予約を使用してマシンをプロビジョニングできるのは、このビジネス グループ内のユーザーだけです。

6 (オプション) [予約ポリシー] ドロップダウン メニューから、予約ポリシーを選択します。

このオプションを選択するには、1 つ以上の予約ポリシーが存在している必要があります。後で予約を編集して予約ポリシーを指定できます。

予約ポリシーを使用すると、プロビジョニングを特定の予約に制限することができます。

7 [優先度] テキスト ボックスに数値を入力し、予約の優先度を設定します。

優先度は、ビジネス グループに複数の予約が存在する場合に使用されます。優先度 1 の予約は、優先 2 の予約よりも優先的にプロビジョニングに使用されます。

8 (オプション) この予約をアクティブにしない場合は、[この予約を有効にする] チェック ボックスの選択を解除します。**結果**

このページから移動しないでください。予約は完了していません。

vCloud Director の予約用のリソースおよびネットワーク設定の指定

この vRealize Automation の予約からプロビジョニングされる vCloud Director マシンで使用できるリソースおよびネットワークの設定を指定します。

vCloud Director の予約からプロビジョニングされるマシンで使用できるリソース割り当てモデルは、割り当てプール、従量課金、および予約プールです。従量課金の場合、ストレージまたはメモリの容量を指定する必要はありませんが、ストレージ パスの優先度を指定する必要があります。これらの割り当てモデルの詳細については、vCloud Director のドキュメントを参照してください。

標準またはディスクレベルのストレージ プロファイルを指定できます。マルチレベル ディスク ストレージは、vCloud Director 5.6 以降のエンドポイントで利用可能です。マルチレベル ディスク ストレージは、vCloud Director 5.5 エンドポイントではサポートされていません。

Storage Distributed Resource Scheduler (SDRS) ストレージを使用する統合の場合、ストレージ クラスタを選択することで、この予約からプロビジョニングされるマシンのストレージの配置やロード バランシングを、SDRS によって自動的に処理することができます。SDRS 自動化モードは [自動] に設定しておく必要があります。そうしない場合は、クラスタ内でスタンドアロン データストアとして動作させるデータストアを選択してください。FlexClone ストレージ デバイスでは、SDRS はサポートされていません。

注： vCloud Air エンドポイントと vCloud Director エンドポイント用に定義された予約では、マシンのプロビジョニングにネットワーク プロファイルを使用できません。

前提条件

[vCloud Director 予約情報の指定](#).

手順**1** [リソース] タブをクリックします。**2** [コンピュート リソース] ドロップダウン メニューから、マシンをプロビジョニングするコンピュート リソースを選択します。

この予約でクローンの作成に使用できるのは、選択したクラスタ上に存在するテンプレートのみです。

3 割り当てモデルを選択します。**4** (オプション) [マシン割り当て] テキスト ボックスに数値を入力し、この予約でプロビジョニングできるマシンの最大数を設定します。

割り当てに加えられるのは、パワーオン状態のマシンだけです。予約を無制限にするには空白にします。

5 [メモリ] テーブルから、この予約に割り当てるメモリの量を GB 単位で指定します。

予約に必要な全体のメモリ値は、選択したコンピュート リソースから計算されます。

6 1 つ以上のリストされたストレージ パスを選択します。

使用可能なストレージ パスのオプションは、選択したコンピュート リソースから導出されます。

a [この予約が予約されました] テキスト ボックスに値を入力し、この予約に割り当てるストレージ容量を指定します。**b** [優先度] テキスト ボックスに数値を入力し、ストレージ パスの優先度を、この予約に属する他のストレージ パスに対する相対優先度として指定します。

優先度は、複数のストレージ パスに対して使用します。優先度 0 のストレージ パスは、優先度 1 のパスよりも先に使用されます。

c この予約でストレージ パスを使用しないようにするには、[無効] オプションをクリックします。**d** この手順を繰り返して、クラスタおよびデータストアを必要に応じて構成します。**7** [ネットワーク] タブをクリックします。**8** この予約を使用してプロビジョニングされるマシンのネットワーク パスを構成します。**a** (オプション) オプションが使用できる場合、[エンドポイント] ドロップダウン メニューからストレージ エンドポイントを選択します。

NetApp ONTAP エンドポイントが存在しており、なおかつホストが仮想である場合は、FlexClone オプションがエンドポイント列に表示されます。NetApp ONTAP エンドポイントが存在する場合は、ストレージ パスに割り当てられたエンドポイントが [予約] ページに表示されます。ストレージ パスのエンドポイントを追加、アップデート、または削除すると、すべての該当する予約に変更内容が表示されます。

ストレージ パスのエンドポイントを追加、アップデート、または削除すると、[予約] ページに変更内容が表示されます。

b この予約でプロビジョニングするマシンに対して [ネットワーク アダプタ] を 1 つ以上選択します。**c** (オプション) 選択した各ネットワーク アダプタに対して利用可能な [ネットワーク プロファイル] を選択します。**d** (オプション) 詳細設定が選択可能な場合は、[トランスポート ゾーン] と、ロード バランサを含むブループリントを展開する際に使用する [Tier 0 分散論理ルーター] を選択します。

トランスポート ゾーンは、ネットワーク アダプタの転送範囲にどのクラスタを含めるかを定義します。トランスポート ゾーンが予約とブループリントの両方に指定されている場合は、トランスポート ゾーンの各値が一致している必要があります。

1 つの予約に複数のネットワーク アダプタを選択できますが、マシンをプロビジョニングするときに使用されるのは 1 つのネットワークだけです。

結果

今すぐ予約を保存するには、[保存] をクリックします。 カスタム プロパティを追加して予約仕様をさらに詳細に制御することもできます。 また、この予約に割り当てられたリソースが残り少なくなったときにメール通知を送信するように、アラートを構成することもできます。

vCloud Director の予約用のカスタム プロパティとアラートの指定

カスタム プロパティを vRealize Automation の予約に関連付けることができます。 また予約リソースが低下すると電子メール通知を送信するように、アラートを構成することもできます。

カスタム プロパティと電子メール アラートは、予約のオプション構成です。 カスタム プロパティの関連付けやアラートの設定を行う必要がない場合は、[保存] をクリックして予約の作成を終了します。

カスタム プロパティは必要なだけいくつでも追加できます。

アラートを構成すると、指定されたしきい値に達した時点ではなく、毎日アラートが生成されます。

重要： 通知は、メール アラートが構成され、かつ通知が有効になっている場合のみ、送信されます。

アラートは、制限の指定なしで作成された従量課金の予約には使用できません。

前提条件

[vCloud Director の予約用のリソースおよびネットワーク設定の指定。](#)

手順

- 1 [プロパティ] タブをクリックします。
- 2 [新規] をクリックします。
- 3 有効なカスタム プロパティ名を入力します。
- 4 必要に応じて、プロパティ値を入力します。
- 5 (オプション) プロパティ値を暗号化するには、[暗号化済み] チェック ボックスを選択します。
- 6 (オプション) ユーザーに値の入力を求めるには、[プロンプト表示] チェック ボックスを選択します。
このオプションは、プロビジョニングのときにオーバーライドされることはありません。
- 7 [保存] をクリックします。
- 8 (オプション) その他のカスタム プロパティを追加します。
- 9 [アラート] タブをクリックします。
- 10 アラートが送信されるように構成するには、[容量アラート] チェック ボックスを選択します。
- 11 スライダを使用して、使用可能なリソース割り当てのしきい値を設定します。
- 12 アラート通知を受信するには、[受信者] テキスト ボックスに Active Directory ユーザーまたはグループの名前 (E メール アドレスではない) を入力します。

各行に名前を入力します。複数のエントリを区切るには、Enter を押します。

- 13 メールアラートにグループ マネージャを含めるには、[グループ マネージャにアラートを送信] を選択します。
E メール アラートは、ビジネス グループの [マネージャの E メールを送信先] リストに含まれるユーザーに送信されます。
- 14 リマインダーの頻度（日数）を指定します。
- 15 [保存] をクリックします。

結果

予約が保存され、[予約] リストに表示されます。

Microsoft Azure の予約の作成

特定のビジネス グループに対する Azure 予約を作成し、そのグループ内のユーザーが、指定されたコンピューティング リソース上の Azure 仮想マシンを申請できるようにします。

お使いの環境で VPN トンネルを介したシングル サインオンをサポートしている場合は、[プロパティ] タブの設定を使用して、Azure 仮想マシンでこの機能のサポートを構成できます。

注： Azure 予約を作成するときは、[アラート] タブを無視してください。このタブは関係ありません。予約を作成した後、ビジネス グループの関連付けを変更することはできません。また、他のマシンタイプとは異なり、Azure 予約とブループリントの間に直接的なリンクはありません。

追加、編集、または削除時に予約の表示を制御するには、[予約] ページの [カテゴリ別にフィルタ] オプションを使用します。カテゴリ別のフィルタを行うと、予約リストにテスト エージェントの予約は表示されないことに注意してください。

前提条件

- ファブリック管理者として vRealize Automation にログインします。
- テナント管理者によって少なくとも 1 つのビジネス グループが作成されていることを確認します。
- (オプション) ネットワーク プロファイル情報を構成します。
- 必要なすべての Azure リソースへのアクセス権があることを確認します。
- 必要なキー ペアが存在することを確認します。キー ペアについては、vRealize Automation の構成を参照してください。
- 該当する Azure エンドポイントで使用されるものと一致する有効な Azure サブスクリプション ID を取得します。複数の Azure サブスクリプションを使用する場合は、それぞれのサブスクリプションに対して予約を作成する必要があります。
- お使いの環境で VPN トンネルを介したシングル サインオンをサポートしている場合は、予約を作成する前に、適切な VPC 接続を構成する必要があります。[ネットワークと Azure 間の VPC 接続の設定](#)を参照してください。

手順

1 Microsoft Azure 予約の基本的情報の構成

Microsoft Azure 予約のための基本的情報を指定します。

2 Azure 予約リソース情報の設定

Azure 予約を設定する際に、使用している Azure インスタンスに基づいて、リソース グループとストレージ アカウントの情報を割り当てることができます。予約を設定すると、vRealize Automation のプロビジョニング ロジックで仮想マシンをプロビジョニングする際に、その予約に指定されたリソース情報に従ってリソース（リソース グループやストレージ アカウントなど）の割り当てが試行されます。

3 Azure プロパティの設定

Azure 予約にカスタム プロパティを追加して、VPN トンネルなどのオプションをサポートし、複数のネットワーク間の通信をサポートすることができます。この機能によって、ブループリントへのソフトウェア コンポーネントの追加も容易になります。

4 Azure 予約ネットワーク情報の設定


Azure 仮想マシンの仮想ネットワークとロード バランサーの情報を、予約に設定できます。

Microsoft Azure 予約の基本的情報の構成

Microsoft Azure 予約のための基本的情報を指定します。

[予約情報] ページの情報は、[予約ポリシー] を除き、すべて必須です。それに続く Azure 予約ページの情報は、すべてオプションです。

手順

- 1 [インフラストラクチャ] - [管理] - [予約] を選択します。
- 2 [新規] アイコン () をクリックして、作成する予約のタイプを選択します。
[Azure] を選択します。
- 3 [名前] テキスト ボックスに名前を入力します。
- 4 [ビジネス グループ] ドロップダウン メニューから、ビジネス グループを選択します。
この予約を使用してマシンをプロビジョニングできるのは、このビジネス グループ内のユーザーだけです。
- 5 [予約ポリシー] テキスト ボックスは、Azure 予約には適用されないため無視します。
- 6 [優先度] テキスト ボックスに数値を入力し、予約の優先度を設定します。
優先度は、ビジネス グループに複数の予約が存在する場合に使用されます。優先度 1 の予約は、優先 2 の予約よりも優先的にプロビジョニングに使用されます。
- 7 (オプション) この予約をアクティブにしない場合は、[この予約を有効にする] チェック ボックスの選択を解除します。
- 8 [OK] をクリックします。

Azure 予約リソース情報の設定

Azure 予約を設定する際に、使用している Azure インスタンスに基づいて、リソース グループとストレージ アカウントの情報を割り当てることができます。予約を設定すると、vRealize Automation のプロビジョニング ロジックで仮想マシンをプロビジョニングする際に、その予約に指定されたリソース情報に従ってリソース（リソース グループやストレージ アカウントなど）の割り当てが試行されます。

Azure 仮想マシンのリソース グループとストレージ アカウントの情報は予約の中で設定できます。ただし予約の中では、それらのフィールドを空欄にしておいてもかまいません。これらのフィールドを空欄にした場合、リソース グループとストレージ アカウントに関して、指定された Azure サブスクリプション ID に結び付けられているデフォルトの情報が、関連するすべてのブループリントで使用されます。この情報は、ブループリントを作成するときや、仮想マシンをプロビジョニングするときに更新することもできます。

前提条件

Azure インスタンスのサブスクリプション ID が必要となります。

手順

1 [サブスクリプション ID] テキスト ボックスに、ご使用の Azure サブスクリプション ID を入力します。

2 [場所] ドロップダウンをクリックして予約の場所を選択します。

このフィールドを空欄にすると、場所に依存しない予約を作成することができます。ただしその場合は、ブループリントを作成するときか Azure 仮想マシンをプロビジョニングするときに場所の情報を指定する必要があります。

3 [リソース グループ] テーブルの [新規] をクリックします。

a Azure インスタンスに基づいて、[名前] テキスト ボックスに適切なリソース グループ名の情報を入力します。

注： [名前] ボックスを空白にすることはできません。

b 優先順位を表す数値を [優先順位] テキスト ボックスに割り当てます。

この割り当てによって、リソース グループに複数のリソース グループが存在した場合の優先順位が決まります。数値の低い方が優先順位は高くなります。

c [保存] をクリックしてリソース グループを予約に追加します。

4 [ストレージ アカウント] テーブルの [新規] をクリックします。

a Azure インスタンスに基づいて、[名前] テキスト ボックスに適切なストレージ アカウント名の情報を入力します。

注： [名前] ボックスを空白にすることはできません。

b 優先順位を表す数値を [優先順位] テキスト ボックスに割り当てます。

c [保存] をクリックしてストレージ アカウントを予約に追加します。

この割り当てによって、予約に複数のストレージ アカウントが存在した場合の優先順位が決まります。数値の低い方が優先順位は高くなります。

5 [OK] をクリックして次のタブに進みます。

Azure プロパティの設定

Azure 予約にカスタム プロパティを追加して、VPN トンネルなどのオプションをサポートし、複数のネットワーク間の通信をサポートすることができます。この機能によって、ブループリントへのソフトウェア コンポーネントの追加も容易になります。

ネットワークの VPN トンネルをサポートするのに適切な URL を定義するカスタム プロパティを作成する必要があります。さらに、以前ダウンロードした Azure トンネルの設定スクリプトにパスを定義するプロパティを作成する必要があります。

SSH トンネルを呼び出したときに `vRealize_automation_appliance_fqdn` に割り当てた Azure トンネルの物理マシンのプライベート IP アドレスとポート 1443 を使用します。

次の表は、VPN トンネルをサポートするのに必要なプロパティの名前と値です。

名前	Value
Azure.Windows.ScriptPath	Windows ベース システムにトンネリングを構成するダウンロードしたスクリプトへのパスを指定します。展開環境に合わせてパスを更新します。
Azure.Linux.ScriptPath	Linux ベース システムにトンネリングを構成するダウンロードしたスクリプトへのパスを指定します。展開環境に合わせてパスを更新します。
agent.download.url	展開環境で VPN エージェントの URL を指定します。URL フォーマットは <code>https:// Private_IP:1443/software-service/resources/noble-agent.jar</code> です。
software.agent.service.url	展開の VPN ソフトウェア エージェント サービスの URL を入力します。URL 形式は <code>https:// Private_IP:1443/software-service/api</code> です。
software.ebs.url	展開のイベント ブローカ サービスの URL を入力します。URL 形式は <code>https:// Private_IP:1443/event-broker-service/api</code> です。

前提条件

- VMware 提供の Azure スクリプトを vRealize Automation アプライアンスの [ゲストおよびソフトウェアのエージェント インストーラ] ページからダウンロードします。
これらのスクリプトは、VPN トンネルをサポートするために必要な Azure 拡張機能をインストールします。2 つのスクリプト、`script.ps1` および `script.sh` があります。`.ps1` ファイルは Windows システム用、`.sh` ファイルは Linux システム用です。
 - a `https://vrealize-automation-appliance-fqdn/software` を実行して [VMware vRealize Automation アプライアンス] ページを開きます。
 - b [vRealize Automation コンポーネント (IaaS、ゲストおよびソフトウェア エージェント、ツール)] をインストールする という見出しの下 の [ゲストおよびソフトウェア エージェント] リンクをクリックします。
 - c [Azure マシン] という見出しの下 の Azure スクリプト ファイルをダウンロードします。スクリプト ファイルを適切な場所に保存します。Azure 予約カスタム プロパティを設定するときに、この場所を指定する必要があります。

手順

- 1 [プロパティ] タブをクリックします。

- 2 [新規] をクリックします。
- 3 [プロパティ] ダイアログ ボックスにカスタム プロパティの適切な名前と値を入力します。
- 4 各プロパティを作成するときに、ダイアログ ボックスで [OK] をクリックしてそのプロパティを追加します。
- 5 必要なプロパティをすべて追加したら、[OK] をクリックして設定を保存します。

次のステップ

VPN トンネルをサポートするカスタム プロパティを作成したら、Azure ブループリントのソフトウェア コンポーネントを作成できます。詳細については、vRealize Automation の構成 を参照してください。

Azure のソフトウェア コンポーネントを設定する場合は、[新しいソフトウェア] ページの [コンテナ] ドロップダウンで [Azure 仮想マシン] を選択します。

Azure 予約ネットワーク情報の設定

Azure 仮想マシンの仮想ネットワークとロード バランサーの情報を、予約に設定できます。

このページの一部または全部を空欄にしておき、仮想マシンをプロビジョニングするときに仮想ネットワークとロード バランサーの情報を設定することもできます。

ネットワーク プロファイルを指定し、サブネットを指定しなかった場合は、指定されたネットワーク プロファイルの最初にあるネットワーク範囲の名前がサブネット名として使用されます。ネットワーク プロファイルが指定されている場合は、vNet テキスト ボックスを空欄にしてもかまいません。この場合、その指定されたネットワーク プロファイルの最初のネットワーク範囲の名前がサブネット名として使用され、vNet 名は、該当するサブネットを含んだ最初の Azure vNet に解決されます。

前提条件

ご利用の Azure インスタンスから適切な仮想ネットワークとロード バランサー情報を取得します。

手順

- 1 [ネットワーク] テーブルの [新規] をクリックして、仮想マシンで使用する適切な Azure 仮想ネットワークの情報を設定します。
 - a Azure インスタンスから [vNet] テキスト ボックスに適切な vNet 名の情報を貼り付けます。
 - b Azure インスタンスから [サブネット] テキスト ボックスに適切なサブネット名の情報を貼り付けます。
サブネットの指定はオプションです。このボックスを空欄にした場合、指定した vNet のサブネットがデフォルトで使用されます。
 - c [ネットワーク プロファイル] テキスト ボックスに適切な名前を入力または貼り付けます。ブループリントのネットワーク プロファイルを使用して、ネットワーク インターフェイス カードをネットワークに関連付けることができます。

ネットワーク プロファイルの指定はオプションです。Azure ネットワークの構造と連動させるのではなく、vRealize Automation に定義されているネットワーク プロファイルに基づいてブループリントを作成したい場合は、ネットワーク プロファイルを使用してください。

- d 優先順位を表す数値を [優先順位] テキスト ボックスに割り当てます (該当する場合)。

この割り当てによって、仮想ネットワークに複数の予約が存在した場合の優先順位が決まります。数値の低い方が優先順位は高くなります。

- e [保存] をクリックしてリソース グループを予約に追加します。

- 2 複数のマシンを展開したうえでロード バランサーを使用する場合は、ロード バランサー テーブルの [新規] をクリックします。

- a Azure インスタンスから [名前] テキスト ボックスに適切なロード バランサーの名前を貼り付けます。

- b Azure インスタンスから [バックエンド アドレス プール] テキスト ボックスに適切な名前を貼り付けます。

- c 優先順位を表す数値を [優先順位] テキスト ボックスに割り当てます (該当する場合)。

この割り当てによって、仮想ネットワークに複数のロード バランサが存在した場合の優先順位が決まります。数値の低い方が優先順位は高くなります。

- d [保存] をクリックしてロード バランサを予約に追加します。

- 3 ファイアウォール越しにやり取りする必要がある複数のマシンを展開する場合は、[セキュリティ グループ] テーブルの [新規] をクリックします。

- a Azure インスタンスから [名前] テキスト ボックスにセキュリティ グループの名前を貼り付けます。

- b 優先順位を表す数値を [優先順位] テキスト ボックスに割り当てます (該当する場合)。

この割り当てによって、仮想ネットワークに複数のセキュリティ グループが存在した場合の優先順位が決まります。数値の低い方が優先順位は高くなります。

- c [保存] をクリックしてセキュリティ グループを予約に追加します。

- 4 [OK] をクリックします。

シナリオ：概念実証の環境用の Amazon 予約の作成

概念実証の環境用に、SSH トンネルを使用して一時的にネットワークと Amazon との間の VPC 接続を確立したため、ソフトウェア ブートストラップ エージェントおよびゲスト エージェントがトンネルを経由して通信を実行するように、Amazon の予約にカスタム プロパティを追加する必要があります。

ネットワークと Amazon との間の VPC 接続が必要になるのは、ゲスト エージェントを使用してプロビジョニングするマシンをカスタマイズする場合、またはブループリントに ソフトウェア コンポーネントを含める場合のみです。本番環境では Amazon Web Services を経由して正式にこの接続を構成します。ここでは概念実証の環境で作業しているため、代わりに一時 SSH トンネルを構成しました。

ファブリック管理者権限を使用して、予約を作成し、Amazon Web Services リソースを割り当てます。そして、SSH トンネリングをサポートするいくつかのカスタム プロパティを含めます。また、トンネル マシンと同一の地域および VPC にある予約も構成します。

前提条件

- ファブリック管理者として vRealize Automation にログインします。

- SSH トンネルを構成してネットワークと Amazon との間の VPC 接続を確立します。Amazon AWS トンネル マシンのサブネット、セキュリティ グループ、プライベート IP アドレスをメモします。[事前検証 \(POC\) 環境でネットワークと Amazon との間に VPC 接続を構成](#)を参照してください。
- 概念実証の環境でブループリントを設計する必要がある IT 組織のメンバーのビジネス グループを作成します。[ビジネス グループの作成](#)を参照してください。
- テナント管理者によって少なくとも 1 つのビジネス グループが作成されていることを確認します。

手順

1 シナリオ：概念実証の環境用の Amazon AWS 予約情報の指定

概念実証の環境で機能をテストできるように、ブループリント アーキテクトのチームのリソースを予約します。この予約を構成して、アーキテクト ビジネス グループにリソースを割り当てます。

2 シナリオ：概念実証の環境用の Amazon AWS ネットワーク設定の指定

トンネル マシンが使用しているものと同じの地域とネットワーク設定を使用するための予約を構成します。パワーオンできるマシンの数をこの予約で制限して、リソース使用量を管理します。

3 シナリオ：トンネルを介したエージェント通信を実行するためのカスタム プロパティの指定


ネットワークと Amazon との間の VPC 接続を構成するときに、Amazon AWS トンネル マシンを vRealize Automation リソースにアクセスできるようにポート転送を構成しました。

シナリオ：概念実証の環境用の Amazon AWS 予約情報の指定

概念実証の環境で機能をテストできるように、ブループリント アーキテクトのチームのリソースを予約します。この予約を構成して、アーキテクト ビジネス グループにリソースを割り当てます。

注： 予約を作成した後、ビジネス グループまたはコンピュート リソースの関連付けを変更することはできません。

手順

- 1 [インフラストラクチャ] - [予約] - [予約] を選択します。
- 2 [新規] アイコン（）をクリックして、作成する予約のタイプを選択します。
[Amazon] を選択します。
- 3 [名前] テキスト ボックスに **Amazon Tunnel POC** と入力します。
- 4 [ビジネス グループ] ドロップダウン メニューから、ブループリント アーキテクト用に作成したビジネス グループを選択します。
- 5 [優先度] テキスト ボックスに **1** と入力し、この予約に最も高い優先順位を設定します。

結果

ビジネス グループと予約の優先度が構成されました。しかし、まだリソースを割り当て、SSH トンネルのためのカスタム プロパティを構成する必要があります。

シナリオ：概念実証の環境用の Amazon AWS ネットワーク設定の指定

トンネル マシンが使用しているものと同じの地域とネットワーク設定を使用するための予約を構成します。パワーオンできるマシンの数をこの予約で制限して、リソース使用量を管理します。

手順

- 1 [リソース] タブをクリックします。
- 2 [コンピュート リソース] ドロップダウン メニューから、マシンをプロビジョニングするコンピュート リソースを選択します。

トンネル マシンがある Amazon AWS 地域を選択します。
- 3 (オプション) [マシン割り当て] テキスト ボックスに数値を入力し、この予約でプロビジョニングできるマシンの最大数を設定します。

割り当てに加えられるのは、パワーオン状態のマシンだけです。予約を無制限にするには空白にします。
- 4 [キー ペア] ドロップダウン メニューから [キー ペアの指定] を選択します。

これは概念実証の環境であるため、この予約を使用してプロビジョニングされているすべてのマシンで単一のキー ペアを共有するために選択します。
- 5 [キー ペア] ドロップダウン メニューからアーキテクト ユーザーと共有するキー ペアを選択します。
- 6 [VPC のサブネットに割り当て] チェックボックスを有効にします。
- 7 トンネル マシンが使用しているものと同一のサブネットとセキュリティ グループを選択します。

結果

トンネル マシンと同一の地域とネットワーク設定を使用するために予約を構成しましたが、ソフトウェア ブートストラップ エージェントとゲスト エージェントがトンネルを介して通信を実行できるようにするカスタム プロパティを追加する必要があります。

シナリオ：トンネルを介したエージェント通信を実行するためのカスタム プロパティの指定

ネットワークと Amazon との間の VPC 接続を構成するときに、Amazon AWS トンネル マシンを vRealize Automation リソースにアクセスできるようにポート転送を構成しました。

エージェントを構成するには、予約にトンネルのカスタム プロパティを追加して、それらのポートにアクセスする必要があります。

注： 組織のネットワークと vRealize Automation ネットワークの間で PAT または NAT システム ネットワークを使用している場合は、これらのプロパティを使用してプライベート IP アドレスおよびポートにアクセスすることができます。

手順

- 1 [プロパティ] タブをクリックします。
- 2 [新規] をクリックします。

3 トンネル カスタム プロパティを構成します。

SSH トンネルを呼び出したときに `vRealize_automation_appliance_fqdn` に割り当てた Amazon AWS トンネル マシンのプライベート IP アドレスとポート 1443 を使用します。

オプション	値
<code>software.ebs.url</code>	<code>https://Private_IP:1443/event-broker-service/api</code>
<code>software.agent.service.url</code>	<code>https://Private_IP:1443/software-service/api</code>
<code>agent.download.url</code>	<code>https://Private_IP:1443/software-service/resources/nobel-agent.jar</code>

4 [保存] をクリックします。

結果

予約を作成して Amazon AWS リソースをアーキテクト ビジネス グループに割り当てました。ゲスト エージェントとソフトウェア ブートストラップ エージェントをサポートするための予約を構成しました。アーキテクトは、ゲスト エージェントを活用するブループリントを作成して、展開されたマシンをカスタマイズするか ソフトウェア コンポーネントを含めることができます。

仮想カテゴリ予約の作成

仮想カテゴリ タイプ予約により、特定の vRealize Automation ビジネス グループの仮想マシン デプロイのプロビジョニング サービスにアクセスできます。使用できる仮想予約タイプには、vSphere、Hyper-V、KVM、SCVMM、XenServer などがあります。

予約とは、特定の vRealize Automation ビジネス グループに割り当てられるコンピューティング リソースの、共有されているメモリ、CPU、ネットワーク、およびストレージ リソースの一部のことです。

ビジネス グループは、1つのエンドポイントで複数の予約を使用するか、複数のエンドポイントで複数の予約を使用することができます。

仮想マシンをプロビジョニングするには、ビジネス グループが仮想コンピュート リソースに対して1つ以上の予約を行う必要があります。各予約が示すのは1つのビジネス グループのみですが、ビジネス グループは、単一のコンピュート リソースに対して複数の予約を行ったり、異なるタイプのコンピュート リソースに対して複数の予約を行うことができます。

ビジネス グループに割り当てられたファブリック リソースの共有を定義することに加えて、予約では、マシンの配置を決定するポリシー、優先度、および割り当てを定義できます。

正常にプロビジョニングするには、十分な使用可能ストレージが予約に含まれていることが必要です。予約のストレージの可用性は以下の要素によって異なります。

- データストア/クラスタで使用可能なストレージ容量。
- そのデータストア/クラスタで予約されているストレージ容量。
- vRealize Automation ですでに割り当てられているストレージ容量。

たとえば、データストア/クラスタで利用可能なストレージが vCenter Server にあっても、十分なストレージが予約されていない場合、プロビジョニングは「割り当てることができる予約はありません」というエラーと共に失敗します。予約に割り当てられるストレージは、その特定の予約に含まれる仮想マシンの数によって異なり、仮想マシンの状態には関連しません。VMware ナレッジベースの記事「Machine XXX: No reservation is available to allocate within the group XXX.Total XX GB of storage was requested (KB2151030)」を参照してください。この記事は、<http://kb.vmware.com/kb/2151030> から参照できます。

予約の選択ロジックについて

ビジネス グループのメンバーが仮想マシンに対するプロビジョニング申請を作成すると、vRealize Automation は、そのビジネス グループで使用可能な予約の 1 つからマシンを選択します。

マシンをプロビジョニングする予約は、次の基準を満たす必要があります。

- 予約のプラットフォーム タイプは、マシンの申請元であるブループリントと同じでなければならない。
一般的な仮想ブループリントは、任意のタイプの仮想予約でプロビジョニングできます。
- 予約は有効状態である必要がある。
- コンピュート リソースは、アクセス可能でなければならない、メンテナンス モードであってはならない。
- 予約は、そのマシン割り当てに容量が残っている状態か、または無制限の割り当てが指定された状態でなければならない。

割り当てられたマシン割り当てには、パワーオン状態のマシンだけが含まれます。たとえば、予約の割り当てが 50 で、40 台のマシンがすでにプロビジョニングされているが、そのうちの 20 台だけがパワーオン状態の場合、予約の割り当ては（80 パーセントではなく）40 パーセントが割り当てられていることになります。

- 予約には、マシンをプロビジョニングするのに十分な未割り当てメモリ リソースと未割り当てストレージ リソースがなければならない。

仮想予約のマシン割り当て、メモリ、またはストレージがすべて割り当てられている場合、その予約からはそれ以上仮想マシンをプロビジョニングすることはできません。リソースの予約は仮想コンピュート リソースの物理容量を超えて行うことができます（オーバーコミット状態）、コンピュート リソースの物理容量が 100 パーセント 割り当てられている場合、そのコンピュート リソースの予約では、それらのリソースが解放されるまで、それ以上マシンをプロビジョニングすることができません。

- ブループリントに具体的なネットワーク設定値が構成されている場合、それらの同じネットワークが予約に指定されている必要がある。

ブループリントまたは予約に固定 IP アドレス割り当てのネットワーク プロファイルが指定されている場合、新しいマシンに割り当てる IP アドレスを使用できる必要があります。

- ブループリントまたは申請で場所が指定される場合、コンピュート リソースがその場所に関連付けられている必要がある。

カスタム プロパティ `Vrm.DataCenter.Policy` の値が **Exact** で、その場所に関連付けられたコンピュート リソースの予約の中に他の基準をすべて満たすものが存在しない場合、プロビジョニングは失敗します。

`Vrm.DataCenter.Policy` の値が **NotExact** で、その場所に関連付けられたコンピュート リソースの予約の中に他の基準をすべて満たすものが存在しない場合、場所に関係なく、他の予約でプロビジョニングを進めることができます。このオプションがデフォルトになります。

- ブループリントまたは申請でカスタム プロパティ `VirtualMachine.Host.TpmEnabled` が指定される場合、信頼されるハードウェアが予約のコンピュータ リソースに設置されている必要がある。
- ブループリントで予約ポリシーが指定される場合、予約はその予約ポリシーに属している必要がある。

予約ポリシーは、特定のブループリントからのマシンのプロビジョニングに対する付加的な要件のすべてを、選択された予約が満たしていることを保証する方法の 1 つです。たとえば、予約ポリシーを使用して、プロビジョニングをクローン作成のための特定のテンプレートを持つコンピュータ リソースだけに制限できます。

選択基準のすべてを満たす予約が存在しないと、プロビジョニングは失敗します。

すべての基準を満たす予約が複数存在する場合、申請されたマシンのプロビジョニングに使用される予約は、次のロジックで決定されます。

- 優先度の値が高い予約が選択される前に、優先度の値が低い予約が選択される。
- 複数の予約に同じ優先度が指定されている場合、マシン割り当ての割り当て率が最も低い予約が選択される。
- 複数の予約の優先度と割り当ての使用状況が同じである場合、ラウンド ロビン方式でマシンが複数の予約にわたって分散される。

注： ネットワーク プロファイルでラウンド ロビンを選択することはできませんが、ネットワーク（存在する場合）でラウンド ロビンを選択し、さまざまなネットワーク プロファイルに関連付けることができます。

予約に利用できるストレージ パスとして、マシン ボリュームをプロビジョニングするうえで十分な容量を持つものが複数存在する場合は、次のロジックに従ってストレージ パスが選択されます。

- ブループリントまたは申請でストレージ予約ポリシーが指定されている場合、ストレージ パスはそのストレージ予約ポリシーに属している必要がある。

カスタム プロパティ `VirtualMachine.DiskN.StorageReservationPolicyMode` の値が **NotExact** で、十分な容量のストレージ パスがストレージ予約ポリシー内に存在しない場合、指定されたストレージ予約ポリシーに属していないストレージ パスを使用してプロビジョニングが進められます。

`VirtualMachine.DiskN.StorageReservationPolicyMode` のデフォルト値は **Exact** です。

- 優先度の値が高いストレージ パスが選択される前に、優先度の値が低いストレージ パスが選択される。
- 複数のストレージ パスの優先度が同じである場合、ラウンド ロビン方式でマシンが複数のストレージ パスにわたって分散される。

NSX ネットワークおよびセキュリティのための vSphere 予約の作成

vSphere 予約を作成して、関連付けられた NSX-T または NSX for vSphere エンドポイントと連携させることができます。

NSX に関する全般的な考慮事項

NSX が設定されている場合は、ブループリントを作成または編集するときに、NSX のトランスポート ゾーン、ネットワークの予約ポリシー、アプリケーションの分離設定を指定できます。これらは、[ブループリント] および [ブループリントのプロパティ] ページの [NSX 設定] タブで設定できます。

ブループリントに追加するネットワークおよびセキュリティ コンポーネントの設定は、NSX for vSphere と NSX-T の構成に基づいており、vSphere クラスタの NSX インベントリのためにデータ収集を実行済みである必要があります。ネットワークおよびセキュリティ コンポーネントは、NSX 固有のもので、vSphere マシン コンポーネントとのみ使用できます。NSX の設定の詳細については、使用しているアプリケーションに応じて、[NSX for vSphere 製品のドキュメント](#)または [NSX-T 製品のドキュメント](#)にある『管理ガイド』を参照してください。

プロビジョニングを正常に行うためには、ブループリントでマシン ネットワークを定義するときに、予約のトランスポート ゾーンをマシン ブループリントのトランスポート ゾーンと一致させる必要があります。同様に、マシンのルーティング ゲートウェイをプロビジョニングする場合は、予約に定義されているトランスポート ゾーンがブループリントに定義されているトランスポート ゾーンに一致する必要があります。

それぞれの展開における NSX-T 固有のトポロジに関する考慮事項については、[ネットワーク、セキュリティ、ロード バランサの構成に応じた NSX-T の展開トポロジについて](#)を参照してください。

NSX for vSphere の考慮事項

vRealize Automation が NAT またはルーティング ネットワークによってマシンをプロビジョニングする場合、ルーティング ゲートウェイをネットワーク ルータとしてプロビジョニングします。Edge またはルーティング ゲートウェイは、コンピュート リソースを使用する管理マシンです。またプロビジョニングされたマシン コンポーネントのネットワーク通信も管理します。Edge またはルーティング ゲートウェイのプロビジョニングに使用される予約では、NAT およびルーティング ネットワーク プロファイルで使用される外部ネットワークを決定します。さらに、ルーティング ネットワーク設定に使用される予約 Edge またはルーティング ゲートウェイも決定します。予約のルーティング ゲートウェイは、ルーティング ネットワークをルーティング テーブル内のエントリとリンクします。

ルーティング ネットワークを設定する際に予約で Edge またはルーティング ゲートウェイとネットワーク プロファイルを選択する場合は、ルーティング ネットワーク同士をリンクするために使用するネットワーク パスを選択し、そのパスをルーティング ネットワーク プロファイルの設定に使用する外部ネットワーク プロファイルに割り当てます。ネットワーク パスに割り当て可能なネットワーク プロファイルのリストは、ネットワーク インターフェイス用に選択されたサブネット マスクとプライマリ IP アドレスに基づいて、そのネットワーク パスのサブネットに一致するようにフィルタリングされます。

Edge またはルーティング ゲートウェイの予約ポリシーを指定すると、Edge またはルーティング ゲートウェイを使用してマシンをプロビジョニングするときに使用する予約を特定できます。デフォルトでは、vRealize Automation はルーティング ゲートウェイとマシン コンポーネントに同じ予約を使用します。

vRealize Automation 予約で Edge またはルーティング ゲートウェイを使用する場合は、外部の NSX 環境でルーティング ゲートウェイを構成してから、インベントリ データ収集を実行します。NSX の場合は、NSX Edge インスタンスが動作していることを確認してから、静的ルートの場合はデフォルト ゲートウェイを、Edge Services Gateway または Distributed Router の場合は動的なルーティングの詳細を構成する必要があります。『NSX 管理ガイド』を参照してください。

予約内の 1 つ以上のセキュリティ グループを選択し、vRealize Automation でその予約を使用してプロビジョニングされるすべてのコンポーネント マシンに、基本のセキュリティ ポリシーを適用します。プロビジョニングされたすべてのマシンが、これらの指定されたセキュリティ グループに追加されます。

NSX-T の考慮事項

NSX-T エンドポイントに関連付けられている vSphere エンドポイントの予約を作成するときは、予約に関する以下の情報を設定する必要があります。

- ブループリントのトランスポート ゾーンを定義します。

- プロビジョニングされた展開の接続先となる Tier-0 論理ルーターを選択します。
- 外部ネットワーク プロファイルを Tier-0 論理ルーターにマッピングします。

予約では、NSX-T NS グループはサポートされません。

NSX-T に固有の展開およびトポロジの考慮事項の詳細については、[ネットワーク、セキュリティ、ロード バランサの構成に応じた NSX-T の展開トポロジについて](#)を参照してください。

Hyper-V、KVM、SCVMM、vSphere、XenServer の予約の作成

ビジネス グループのメンバーがマシン プロビジョニングを申請できるようにするには、事前に予約を作成して、マシンにリソースを割り当てておく必要があります。

特定のタイプのマシンをプロビジョニングできるように、各ビジネス グループには、そのメンバー用の予約を 1 つ以上作成する必要があります。たとえば、vSphere 予約は作成されているが KVM (RHEV) 予約は作成されていないというビジネス グループは、KVM (RHEV) 仮想マシンを申請できません。この例では、ビジネス グループに KVM (RHEV) リソース専用の予約を割り当てる必要があります。

手順

1 仮想予約情報の指定

各予約は特定のビジネス グループ用に構成されており、特定のコンピュート リソース上のマシンを申請できるようにユーザーにアクセス権が付与されています。

2 仮想予約用のリソースおよびネットワーク設定の指定

この vRealize Automation の予約からマシンをプロビジョニングするためのリソースおよびネットワークの設定を指定します。

3 仮想予約用のカスタム プロパティとアラートの指定

カスタム プロパティを vRealize Automation の予約に関連付けることができます。また予約リソースが低下すると電子メール通知を送信するように、アラートを構成することもできます。

仮想予約情報の指定

各予約は特定のビジネス グループ用に構成されており、特定のコンピュート リソース上のマシンを申請できるようにユーザーにアクセス権が付与されています。

追加、編集、または削除時に予約の表示を制御するには、[予約] ページの [カテゴリ別にフィルタ] オプションを使用します。カテゴリ別のフィルタを行うと、予約リストにテスト エージェントの予約は表示されないことに注意してください。


注： 予約を作成した後、ビジネス グループまたはコンピュート リソースの関連付けを変更することはできません。

前提条件

- ファブリック管理者として vRealize Automation にログインします。
- テナント管理者によって少なくとも 1 つのビジネス グループが作成されていることを確認します。
- コンピュート リソースが存在することを確認します。
- ネットワーク設定を構成します。
- (オプション) ネットワーク プロファイル情報を構成します。

手順

1 [インフラストラクチャ] - [予約] - [予約] を選択します。

2 [新規] アイコン () をクリックして、作成する予約のタイプを選択します。

選択可能な仮想予約のタイプとして、Hyper-V、KVM、SCVMM、vSphere、および XenServer があります。

たとえば [vSphere] を選択します。

3 [名前] テキスト ボックスに名前を入力します。

4 [テナント] ドロップダウン メニューから、テナントを選択します。

5 [ビジネス グループ] ドロップダウン メニューから、ビジネス グループを選択します。

この予約を使用してマシンをプロビジョニングできるのは、このビジネス グループ内のユーザーだけです。

6 (オプション) [予約ポリシー] ドロップダウン メニューから、予約ポリシーを選択します。

このオプションを選択するには、1 つ以上の予約ポリシーが存在している必要があります。後で予約を編集して予約ポリシーを指定できます。

予約ポリシーを使用すると、プロビジョニングを特定の予約に制限することができます。

7 [優先度] テキスト ボックスに数値を入力し、予約の優先度を設定します。

優先度は、ビジネス グループに複数の予約が存在する場合に使用されます。優先度 1 の予約は、優先 2 の予約よりも優先的にプロビジョニングに使用されます。

8 (オプション) この予約をアクティブにしない場合は、[この予約を有効にする] チェック ボックスの選択を解除します。

結果

このページから移動しないでください。予約は完了していません。

仮想予約用のリソースおよびネットワーク設定の指定

この vRealize Automation の予約からマシンをプロビジョニングするためのリソースおよびネットワークの設定を指定します。

vSphere 環境で作業しており、Net App FlexClone テクノロジーを使用したストレージ デバイスがある場合は、予約で FlexClone データストアを選択できます。FlexClone ストレージ デバイスでは、SDRS はサポートされていません。

正常にプロビジョニングするには、十分な使用可能ストレージが予約に含まれていることが必要です。予約のストレージの可用性は以下の要素によって異なります。

- データストア/クラスタで使用可能なストレージ容量。
- そのデータストア/クラスタで予約されているストレージ容量。
- vRealize Automation ですでに割り当てられているストレージ容量。

たとえば、データストア/クラスタで利用可能なストレージが vCenter Server にあっても、十分なストレージが予約されていない場合、プロビジョニングは「割り当てることができる予約はありません」というエラーと共に失敗します。予約に割り当てられるストレージは、その特定の予約に含まれる仮想マシンの数によって異なり、仮想マシンの状態には関連しません。VMware ナレッジベースの記事「Machine XXX: No reservation is available to allocate within the group XXX.Total XX GB of storage was requested (KB2151030)」を参照してください。この記事は、<http://kb.vmware.com/kb/2151030> から参照できます。

NSX for vSphere または NSX-T で使用するために vSphere (vCenter Server) 予約を作成または編集している場合は、選択したネットワーク向けの詳細なオプションを使用してトランスポート ゾーンと Tier 1 分散論理ルーターの情報を指定することができます。

前提条件

仮想予約情報の指定。

手順

- 1 [リソース] タブをクリックします。
- 2 [コンピュート リソース] ドロップダウン メニューから、マシンをプロビジョニングするコンピュート リソースを選択します。

この予約でクローンの作成に使用できるのは、選択したクラスタ上に存在するテンプレートのみです。

プロビジョニングの際に、ローカル ストレージに接続されたホストにマシンが配置されます。予約でローカル ストレージが使用されている場合は、予約によってプロビジョニングされるすべてのマシンが、このローカル ストレージを格納しているホストに作成されます。ただし、VirtualMachine.Admin.ForceHost カスタム プロパティを使用する場合は、マシンが強制的に別のホストにプロビジョニングされるため、プロビジョニングが失敗します。また、マシンのクローン作成に使用したテンプレートがローカル ストレージに存在するものの、別のクラスタ上のマシンに接続されている場合にも、プロビジョニングが失敗します。この場合は、テンプレートにアクセスできないことが原因でプロビジョニングが失敗します。

- 3 (オプション) [マシン割り当て] テキスト ボックスに数値を入力し、この予約でプロビジョニングできるマシンの最大数を設定します。

割り当てに加えられるのは、パワーオン状態のマシンだけです。予約を無制限にするには空白にします。

- 4 [メモリ] テーブルから、この予約に割り当てるメモリの量を GB 単位で指定します。

予約に必要な全体のメモリ値は、選択したコンピュート リソースから計算されます。

- 5 [メモリ] テーブルから、この予約に割り当てるメモリの量を GB 単位で指定します。

予約に必要な全体のメモリ値は、選択したコンピュート リソースから計算されます。

- 6 1 つ以上のリストされたストレージ パスを選択します。

使用可能なストレージ パスのオプションは、選択したコンピュート リソースから導出されます。

Storage Distributed Resource Scheduler (SDRS) ストレージを使用する統合の場合、ストレージ クラスタを選択することで、この予約からプロビジョニングされるマシンのストレージの配置やロード バランシングを、SDRS によって自動的に処理することができます。SDRS 自動化モードは [自動] に設定しておく必要があります。そうしない場合は、クラスタ内でスタンドアロン データストアとして動作させるデータストアを選択してください。FlexClone ストレージ デバイスでは、SDRS はサポートされていません。

クラスタ内の個々のディスクカストレージ クラスタを選択できますが、両方を選択することはできません。ストレージ クラスタを選択した場合、この予約からプロビジョニングされるマシンのストレージの配置やロード バランシングを Storage DRS が制御します。

- 7 コンピュート リソースで利用できる場合は、[リソース プール] ドロップダウン メニューからリソース プールを選択します。
- 8 [ネットワーク] タブをクリックします。
- 9 この予約を使用してプロビジョニングされるマシンのネットワーク パスを構成します。

- a (オプション) オプションが使用できる場合、[エンドポイント] ドロップダウン メニューからストレージ エンドポイントを選択します。

NetApp ONTAP エンドポイントが存在しており、なおかつホストが仮想である場合は、FlexClone オプションがエンドポイント列に表示されます。 NetApp ONTAP エンドポイントが存在する場合は、ストレージ パスに割り当てられたエンドポイントが [予約] ページに表示されます。 ストレージ パスのエンドポイントを追加、アップデート、または削除すると、すべての該当する予約に変更内容が表示されます。

ストレージ パスのエンドポイントを追加、アップデート、または削除すると、[予約] ページに変更内容が表示されます。

- b この予約でプロビジョニングするマシンに対して [ネットワーク アダプタ] を 1 つ以上選択します。
- c (オプション) 選択した各ネットワーク アダプタに対して利用可能な [ネットワーク プロファイル] を選択します。
- d (オプション) 詳細設定が選択可能な場合は、[トランスポート ゾーン] と、ロード バランサを含むブループリントを展開する際に使用する [Tier 0 分散論理ルーター] を選択します。

トランスポート ゾーンは、ネットワーク アダプタの転送範囲にどのクラスタを含めるかを定義します。トランスポート ゾーンが予約とブループリントの両方に指定されている場合は、トランスポート ゾーンの各値が一致している必要があります。

1 つの予約に複数のネットワーク アダプタを選択できますが、マシンをプロビジョニングするときに使用されるのは 1 つのネットワークだけです。

結果

今すぐ予約を保存するには、[保存] をクリックします。 カスタム プロパティを追加して予約仕様をさらに詳細に制御することもできます。 また、この予約に割り当てられたリソースが残り少なくなったときにメール通知を送信するように、アラートを構成することもできます。

仮想予約用のカスタム プロパティとアラートの指定

カスタム プロパティを vRealize Automation の予約に関連付けることができます。また予約リソースが低下すると電子メール通知を送信するように、アラートを構成することもできます。

カスタム プロパティと電子メール アラートは、予約のオプション構成です。 カスタム プロパティの関連付けやアラートの設定を行う必要がない場合は、[保存] をクリックして予約の作成を終了します。

カスタム プロパティは必要なだけいくつでも追加できます。

重要： 通知は、メール アラートが構成され、かつ通知が有効になっている場合のみ、送信されます。

アラートを構成すると、指定されたしきい値に達した時点ではなく、毎日アラートが生成されます。

前提条件

仮想予約用のリソースおよびネットワーク設定の指定。

手順

- 1 [プロパティ] タブをクリックします。
- 2 [新規] をクリックします。
- 3 有効なカスタム プロパティ名を入力します。
- 4 必要に応じて、プロパティ値を入力します。
- 5 (オプション) プロパティ値を暗号化するには、[暗号化済み] チェック ボックスを選択します。
- 6 (オプション) ユーザーに値の入力を求めるには、[プロンプト表示] チェック ボックスを選択します。
このオプションは、プロビジョニングのときにオーバーライドされることはありません。
- 7 (オプション) その他のカスタム プロパティを追加します。
- 8 [アラート] タブをクリックします。
- 9 アラートが送信されるように構成するには、[容量アラート] チェック ボックスを選択します。
- 10 スライダを使用して、使用可能なリソース割り当てのしきい値を設定します。
- 11 アラート通知を受信するには、[受信者] テキスト ボックスに Active Directory ユーザーまたはグループの名前 (E メール アドレスではない) を入力します。
各行に名前を入力します。複数のエントリを区切るには、Enter を押します。
- 12 メール アラートにグループ マネージャを含めるには、[グループ マネージャにアラートを送信] を選択します。
E メール アラートは、ビジネス グループの [マネージャの Eメールの送信先] リストに含まれるユーザーに送信されます。
- 13 リマインダーの頻度 (日数) を指定します。
- 14 [保存] をクリックします。

結果

予約が保存され、[予約] リストに表示されます。

次のステップ

必要に応じて予約ポリシーを構成するか、プロビジョニングの予約を開始します。

ブループリントを作成する権限を持つユーザーは、すぐにブループリントを作成できます。

予約の編集によるネットワーク プロファイルの割り当て

予約にネットワーク プロファイルを割り当てることで、予約を使用してプロビジョニングするマシンに、固定 IP アドレスなどを割り当てることができます。

[新規ブループリント] または [ブループリントのプロパティ] ページの [プロパティ] タブのカスタム プロパティ `VirtualMachine.NetworkN.ProfileName` を使用して、ネットワーク プロファイルをブループリントに割り当てることもできます。

予約およびブループリントのネットワーク プロファイルを指定した場合は、ブループリントの値が優先されます。たとえば、ネットワーク プロファイルがブループリントに指定されており (`VirtualMachine.NetworkN.ProfileName` カスタム プロパティを使用)、なおかつブループリントで使用されている予約でも指定されている場合は、ブループリントに指定されているネットワーク プロファイルが優先されます。ただし、ブループリントでカスタム プロパティが使用されておらず、また、マシン NIC のネットワーク プロファイルを選択した場合、vRealize Automation では、ネットワーク プロファイルが指定されているマシン NIC に対して予約ネットワーク パスが使用されます。

注： この情報は Amazon Web Services には適用されません。

前提条件

- ファブリック管理者として vRealize Automation にログインします。
- ネットワーク プロファイルを作成します。 [ネットワーク プロファイルの作成](#)を参照してください。

手順

- 1 [インフラストラクチャ] - [予約] - [予約] を選択します。
- 2 予約をポイントして [編集] をクリックします。
- 3 [ネットワーク] タブをクリックします。
- 4 ネットワーク パスにネットワーク プロファイルを割り当てます。
 - a 固定 IP アドレスを有効にするネットワーク パスを選択します。
ネットワーク パスのオプションは [リソース] タブの設定によって変わります。
 - b [ネットワーク プロファイル] ドロップダウン メニューからプロファイルを選択し、利用可能なネットワーク プロファイルをパスにマッピングします。
 - c (オプション) この手順を繰り返して、この予約の他のネットワーク パスにネットワーク プロファイルを割り当てます。
- 5 [OK] をクリックします。

予約ポリシー

予約ポリシーを使用して、予約申請の処理方法を管理できます。ブループリントからマシンをプロビジョニングするとき、プロビジョニングは、予約ポリシーで指定されたリソースに制限されます。

予約ポリシーは、予約申請の処理を制御するための任意指定の手段を提供します。予約ポリシーをブループリントに適用すると、そのブループリントからプロビジョニングされたマシンを使用可能な予約のサブセットのみに制限することができます。

予約ポリシーを使用すると、リソースを収集してサービス レベルごとにグループ化することや、特定のタイプのリソースを特定の目的のために簡単に利用できるようになります。ユーザーがマシンを申請する場合は、マシンに対して十分な容量がある適切なタイプの任意の予約に対してプロビジョニングできます。次のシナリオでは、予約ポリシーの考えられる使用例をいくつか示します。

- プロビジョニングされたマシンが、NetApp FlexClone をサポートする特定のデバイスを含む予約に確実に配置されるようにする場合
- クラウド マシンのプロビジョニングを、特定のブループリントに必要なマシン イメージを含む特定の領域に制限する場合
- 重量課金割り当てモデルをサポートするマシン タイプで、それに代わる手段として使用する場合

1 つの予約ポリシーに複数の予約を追加できますが、予約は 1 つのポリシーにのみ属することができます。1 つの予約ポリシーを複数のブループリントに割り当てることができます。1 つのブループリントには 1 つの予約ポリシーのみを含めることができます。

注： vCloud Air エンドポイントと vCloud Director エンドポイント用に定義された予約では、マシンのプロビジョニングにネットワーク プロファイルを使用できません。

注： プラットフォームで SDRS が有効になっている場合は、SDRS によって個々の仮想マシン ディスクのストレージまたは仮想マシンのすべてのストレージのロード バランシングを行うことができます。SDRS データストア クラスタを使用している場合は、予約ポリシーとストレージ予約ポリシーを使用する際に競合が発生することがあります。たとえば、ポリシーまたはストレージ ポリシーのいずれかの予約でスタンドアロン データストアまたは SDRS クラスタ内のデータストアが選択されている場合、仮想マシンのストレージは SDRS によって起動されずに停止することがあります。SDRS クラスタへのストレージ配置を使用してマシンの再プロビジョニングを申請する場合、SDRS の自動化レベルが無効になっているとマシンが削除されます。プロビジョニングおよび SDRS の関連情報については、`VirtualMachine.Admin.Datastore.Cluster.ResourceLeaseDurationSec` カスタム プロパティを参照してください。

予約ポリシーの構成

予約ポリシーを作成すると、リソースを収集してさまざまなサービス レベルでグループ化できます。また、特定のタイプのリソースを特定の目的に使用することが容易になります。予約ポリシーを作成した後、そのポリシーを予約に割り当てる必要があります。これにより、テナント管理者とビジネス グループ マネージャは、ブループリントでポリシーを効率的に使用できるようになります。

予約ポリシーには、異なるタイプの予約を含めることができますが、特定の申請の予約を選択する際には、ブループリントのタイプに一致する予約のみが考慮されます。

手順

1 予約ポリシーの作成

予約ポリシーを使用して類似の予約をグループ化できます。

2 予約への予約ポリシーの割り当て

予約の作成時に、予約ポリシーを割り当てることができます。また、既存の予約を編集して、予約ポリシーの割り当てや、割り当ての変更ができます。

予約ポリシーの作成

予約ポリシーを使用して類似の予約をグループ化できます。

最初に予約ポリシーを作成し、次にポリシーを予約に追加して、ブループリントの作成者がブループリントで予約ポリシーを使用できるようにすることができます。


ポリシーは空のコンテナとして作成されます。

追加、編集、または削除時に予約ポリシーの表示を制御するには、[予約ポリシー] ページの [タイプ別にフィルタ] オプションを使用します。

前提条件

ファブリック管理者として vRealize Automation にログインします。

手順

- 1 [インフラストラクチャ] - [予約] - [予約ポリシー] を選択します。
- 2 [新規] アイコン () をクリックします。
- 3 [名前] テキスト ボックスに名前を入力します。
- 4 [タイプ] ドロップダウン メニューから [予約ポリシー] を選択します。
- 5 [説明] テキスト ボックスに説明を入力します。
- 6 [OK] をクリックします。

予約への予約ポリシーの割り当て

予約の作成時に、予約ポリシーを割り当てることができます。また、既存の予約を編集して、予約ポリシーの割り当てや、割り当ての変更ができます。

前提条件

[予約ポリシーの作成](#)。

手順

- 1 [インフラストラクチャ] - [予約] - [予約] を選択します。
- 2 予約をポイントして [編集] をクリックします。
- 3 [予約ポリシー] ドロップダウン メニューから、予約ポリシーを選択します。
- 4 [保存] をクリックします。

ストレージ予約ポリシー

ストレージ予約ポリシーを作成して、ブループリント アーキテクトが vSphere、KVM (RHEV)、および SCVMM プラットフォーム タイプ用の別のデータストアか、または vCloud Air や vCloud Director のリソースなど、他のリソース用の別のストレージ プロファイルに仮想マシンのボリュームを割り当てられるようにします。

仮想マシンのボリュームを別のデータストアまたは別のストレージ プロファイルに割り当てると、ブループリント アーキテクトは、より効果的にストレージ容量を制御および使用できるようになります。たとえば、オペレーティング システム ボリュームを比較的低速で安価なデータストアまたはストレージ プロファイルにデプロイし、データベース ボリュームを高速のデータストアまたはストレージ プロファイルにデプロイできます。

一部のマシン エンドポイントはストレージ プロファイルを 1 つしかサポートしていませんが、それ以外はマルチレベル ディスク ストレージをサポートしています。マルチレベル ディスク ストレージは、vCloud Director 5.6 以上のエンドポイントおよび vCloud Air エンドポイントで使用できます。マルチレベル ディスク ストレージは、vCloud Director 5.5 エンドポイントではサポートされていません。

ブループリントを作成すると、単一のデータストア、または複数のデータストアを表すストレージ予約ポリシーを、ボリュームに割り当てることができます。ボリュームに単一のデータストアまたはストレージ プロファイルを割り当てると、可能な場合、vRealize Automation はそのデータストアまたはストレージ プロファイルをプロビジョニング時に使用します。ストレージ予約ポリシーをボリュームに割り当てると、プロビジョニング時に vCloud Air や vCloud Director などの他のリソースと連携している場合、vRealize Automation はデータストアの 1 つまたはストレージ プロファイルを使用します。

ストレージ予約ポリシーは、基本的にはファブリック管理者によって 1 つ以上のデータストアまたはストレージ プロファイルに適用されるタグです。ファブリック管理者は、速度や価格といった類似する特性を持つデータストアまたはストレージ プロファイルのグループ化にストレージ予約ポリシーを適用します。データストアまたはストレージ プロファイルは、一度に 1 つのストレージ予約ポリシーにしか割り当てることができませんが、ストレージ予約ポリシーは多数の異なるデータストアまたはストレージ プロファイルに適用できます。

ストレージ予約ポリシーを作成し、1 つ以上のデータストアまたはストレージ プロファイルに割り当てることができます。ブループリント作成者は、ストレージ予約ポリシーを仮想ブループリントのボリュームに割り当てることができます。そのブループリントを使用するマシンをユーザーが申請すると、vRealize Automation はブループリントに指定されているストレージ予約ポリシーを使用して、マシンのボリュームに適したデータストアまたはストレージ プロファイルを選択します。

注： プラットフォームで SDRS が有効になっている場合は、SDRS によって個々の仮想マシン ディスクのストレージまたは仮想マシンのすべてのストレージのロード バランシングを行うことができます。SDRS データストア クラスタを使用している場合は、予約ポリシーとストレージ予約ポリシーを使用する際に競合が発生することがあります。たとえば、ポリシーまたはストレージ ポリシーのいずれかの予約でスタンドアロン データストアまたは SDRS クラスタ内のデータストアが選択されている場合、仮想マシンのストレージは SDRS によって起動されずに停止することがあります。SDRS クラスタへのストレージ配置を使用してマシンの再プロビジョニングを申請する場合、SDRS の自動化レベルが無効になっているとマシンが削除されます。プロビジョニングおよび SDRS の関連情報については、`VirtualMachine.Admin.Datastore.Cluster.ResourceLeaseDurationSec` カスタム プロパティを参照してください。

プロビジョニング済みのマシンに予約によって割り当てられたストレージとメモリは、割り当てられたマシンが破棄アクションによって vRealize Automation で削除されると、割り当て解除されます。vCenter Server でマシンが削除される場合は、ストレージとメモリの割り当ては解除されません。

たとえば、既存の展開でマシンに関連付けられている予約を削除することはできません。vCenter Server で展開済みのマシンを手動で移動または削除する場合、vRealize Automation では引き続き、展開済みのマシンをライブとして認識するため、関連付けられた予約を削除することはできません。

ストレージ予約ポリシーの構成

ストレージ予約ポリシーを作成して、速度や価格などの特性が類似しているデータストアをグループ化することができます。ストレージ予約ポリシーの作成後は、ブループリントでそのポリシーを使用する前に、そのポリシーにデータストアを取り込む必要があります。

手順

1 ストレージ予約ポリシーの作成

ストレージ予約ポリシーを使用して、速度や価格などの特性が類似しているデータストアをグループ化することができます。

2 データストアへのストレージ予約ポリシーの割り当て

コンピュート リソースにストレージ予約ポリシーを関連付けできます。ストレージ予約ポリシーが作成された後、そのポリシーにデータストアを割り当てる必要があります。データストアは、1つのストレージ予約ポリシーにしか属することができません。ブループリントで使用するためデータストアのグループを作成するには、複数のデータストアを追加します。

ストレージ予約ポリシーの作成

ストレージ予約ポリシーを使用して、速度や価格などの特性が類似しているデータストアをグループ化することができます。


ポリシーは空のコンテナとして作成されます。

追加、編集、または削除時に予約ポリシーの表示を制御するには、[予約ポリシー] ページの [タイプ別にフィルタ] オプションを使用します。

前提条件

ファブリック管理者として vRealize Automation にログインします。

手順

- 1 [インフラストラクチャ] - [予約] - [予約ポリシー] を選択します。
- 2 [新規] アイコン () をクリックします。
- 3 [名前] テキスト ボックスに名前を入力します。
- 4 [タイプ] ドロップダウン メニューから [ストレージ予約ポリシー] を選択します。
- 5 [説明] テキスト ボックスに説明を入力します。
- 6 [OK] をクリックします。

データストアへのストレージ予約ポリシーの割り当て

コンピュート リソースにストレージ予約ポリシーを関連付けできます。ストレージ予約ポリシーが作成された後、そのポリシーにデータストアを割り当てる必要があります。データストアは、1つのストレージ予約ポリシーにしか属することができません。ブループリントで使用するためデータストアのグループを作成するには、複数のデータストアを追加します。

前提条件

[ストレージ予約ポリシーの作成。](#)

手順

- 1 [インフラストラクチャ] - [コンピュート リソース] - [コンピュート リソース] を選択します。
- 2 コンピュート リソースを指定して [編集] をクリックします。
- 3 [構成] タブをクリックします。
- 4 [ストレージ] テーブル内の、ストレージ予約ポリシーに追加するデータストアを見つけます。
- 5 目的の [ストレージ パス] オブジェクトの横にある [編集] アイコン (✎) をクリックします。
- 6 [ストレージ予約ポリシー] 列ドロップダウン メニューから、ストレージ予約ポリシーを選択します。
マシンのプロビジョニング後は、ストレージ予約ポリシーの変更により、ディスク上のストレージ プロファイルが変更された場合でも、ポリシーは変更できません。
- 7 [OK] をクリックします。
- 8 (オプション) ストレージ予約ポリシーに追加のデータストアを割り当てます。
- 9 [OK] をクリックします。

ワークロードの配置

ブループリントを展開する際に、ワークロード配置は収集されたデータを使用して、使用可能なリソースに基づくブループリントの展開先を推奨します。vRealize Automation と vRealize Operations Manager は連携して、新規ブループリントを展開する際のワークロードの推奨される配置先を示します。

vRealize Automation は、ビジネス グループ、予約、割り当てなどの組織ポリシーを管理する一方で、vRealize Operations Manager のキャパシティ分析と連携してマシンを配置します。ワークロード配置は、vSphere エンドポイントでのみ使用可能です。

ワークロード配置で使用される用語

ワークロード配置では、いくつかの用語が使用されます。

- vSphere 内のクラスタは、vRealize Automation のコンピューティング リソースにマッピングされます。
- 予約にはコンピューティングとストレージが含まれ、ストレージは個々のデータストアまたはデータストア クラスタで構成できます。予約には、複数のデータストア、データストア クラスタ、またはその両方を含めることができます。
- 複数の予約が同じクラスタを参照できます。
- 仮想マシンは、複数のクラスタに移動できます。
- ワークロード配置が有効な場合、プロビジョニング ワークフローで配置ポリシーが使用され、ブループリントの展開先が推奨されます。

ワークロード配置によるブループリントのプロビジョニング

ワークロード配置を使用してブループリントをプロビジョニングする場合、プロビジョニング ワークフローでは、vRealize Automation での予約と、vRealize Operations Manager からの配置の最適化を使用します。

- 1 vRealize Automation は、プロビジョニング先への配置を許可するガバナンス ルールを提供します。

- 2 vRealize Operations Manager は、分析データをベースに、最適な配置先を推奨します。
- 3 vRealize Automation は、vRealize Operations Manager が推奨する配置に基づいて、プロビジョニングプロセスを続行します。

vRealize Operations Manager が推奨を提供できない場合、または推奨を使用できない場合、vRealize Automation はデフォルトの配置ロジックにフォールバックします。

開発者がカタログ アイテムを選択し、カタログ アイテムの申請フォームを記入すると、vRealize Automation は次の事項を考慮して仮想マシンをプロビジョニングします。

表 2-16. 仮想マシンのプロビジョニングに関する考慮事項

考慮事項	効果
ポリシー	vRealize Automation の予約ポリシーに複数の予約が含まれることがあります。
予約	<p>vRealize Automation は、申請を評価し、どの予約が申請内容に適しているかを判断します。</p> <ul style="list-style-type: none"> ■ vRealize Operations Manager の分析に基づく配置が有効な場合、vRealize Automation は予約のリストを vRealize Operations Manager に渡し、運用メトリックに則って、配置に最適な予約を決定します。 ■ 配置が vRealize Operations Manager の推奨に基づいていない場合、vRealize Automation は優先順位と可用性に基づいて配置を決定します。 <p>予約は、リソースの使用状況を追跡するように更新されます。</p> <p>vRealize Operations Manager が、vRealize Automation では容量不足または該当しなくなったと見なされるクラスタやデータストアを推奨した場合、vRealize Automation は例外をログに記録します。vRealize Automation では、そのデフォルトの配置メカニズムに基づいてプロビジョニングを続行できます。</p>

仮想マシン用のリソースを特定するため、vRealize Automation は候補の予約のリストを示します。リスト内の各候補には、クラスタと、1つ以上のデータストアまたはデータストア クラスタを含めることができます。vRealize Operations Manager では、候補の予約を使用して、配置先候補のリストを作成し、最適な配置先を特定します。

vRealize Operations Manager のポリシーで、クラスタの分散レベル、使用率、およびバッファ容量を設定します。1つのクラスタまたはデータストア クラスタが含まれる単一の予約について、vRealize Automation は推奨された配置先が適しているかどうかを検証します。

- 配置先に問題がない場合、vRealize Automation は推奨に基づいてブループリントを展開します。
- 配置先に問題がある場合、vRealize Automation はデフォルトの配置動作で仮想マシンを配置します。

配置を検討する際には、健全性と使用率の問題も考慮する必要があります。クラウド管理者と仮想インフラストラクチャ管理者はインフラストラクチャを管理しますが、開発者はアプリケーションの健全性を重視しています。開発者をサポートするため、ワークロード配置戦略では健全性と使用率の問題も考慮しなければなりません。

表 2-17. 健全性および使用率の問題に関する考慮事項

ワークロードの問題	配置ソリューション
開発者が環境内の健全性の問題を報告。	vRealize Automation が、問題があるクラスタ、または大規模なワークロードが原因で過剰に使用されているクラスタに、ブループリントをプロビジョニングしています。vRealize Automation は、vRealize Operations Manager でのキャパシティ分析と連携して、十分なキャパシティを持つクラスタにブループリントをプロビジョニングする必要があります。
開発者が使用率の問題を報告。	環境内のクラスタは使用率が低下しています。vRealize Automation は、vRealize Operations Manager が提供するキャパシティ分析と連携して、使用率が最大化されているクラスタにブループリントをプロビジョニングする必要があります。

ブループリントをプロビジョニングするユーザー

次の表は、ブループリントをプロビジョニングするユーザーとアクションについて説明しています。

表 2-18. ブループリントをプロビジョニングするユーザーおよびロール

ステップ	ユーザー	アクション	必要なロール
1	クラウド管理者または仮想インフラストラクチャ (VI) 管理者	仮想マシンの初期配置が組織のポリシーを満たしており、運用分析データに基づいて最適化されていることを確認します。	IaaS 管理者ロール
1	ファブリック管理者	vRealize Automation で予約、予約ポリシー、および配置ポリシーを定義します。	ファブリック管理者ロール、インフラストラクチャ アーキテクト
1	IaaS 管理者	ワークロード配置のために必要な、vSphere および vRealize Operations Manager のエンドポイントを定義します。	IaaS 管理者ロール
2	インフラストラクチャ アーキテクト	仮想マシン コンポーネント タイプを直接操作するブループリント アーキテクトとして、ブループリントを作成するときに、予約ポリシーを仮想マシンに割り当てます。予約ポリシーは、ブループリントのマシン コンポーネントのプロパティとして指定します。	インフラストラクチャ アーキテクト
3	インフラストラクチャ アーキテクト、アプリケーション アーキテクト、ソフトウェア アーキテクト、XaaS アーキテクト	仮想マシンをプロビジョニングするためのブループリントを作成し、公開します。マシン コンポーネントを直接操作するのは、インフラストラクチャ アーキテクトのみです。その他のアーキテクト ロールは、ネストでインフラストラクチャのブループリントを再利用できますが、マシン コンポーネントの設定を編集することはできません。 ブループリントには、コンポーネントを 1 つのみ含めることも、ネストされたブループリント、XaaS コンポーネント、多階層アプリケーション用の複数の仮想マシンなどを含めることもできます。 vRealize Automation は、予約の構成に基づいて仮想マシンを配置し、必要に応じて、ブループリントのマシン コンポーネント レベルで予約ポリシーを含めます。たとえば、ブループリントに 2 台のマシンを含め、マシンごとに異なるポリシーを適用できます。 vRealize Automation はまた、vRealize Operations Manager が提供する運用分析データに基づいて仮想マシンを最適化します。	インフラストラクチャ アーキテクト
4	クラウド管理者または仮想インフラストラクチャ管理者	vRealize Automation がプロビジョニングする仮想マシンの初期配置を制御するポリシーを選択します。 管理者は次の処理を実行できます。 <ul style="list-style-type: none">■ API を使用してポリシーを選択します。■ デフォルトの配置ポリシーを使用して、vRealize Automation で各サーバを順番に使用し、ワークロードを分散させます。この方法では、vRealize Operations Manager との連携は不要です。	IaaS 管理者ロール、インフラストラクチャ アーキテクト
5	仮想インフラストラクチャ管理者	vRealize Operations Manager で、カスタム データセンターとカスタム グループを作成します。次に仮想インフラストラクチャ管理者は、それらのカスタム データセンターに、ワークロードの統合と分散に使用するポリシーを適用します。	IaaS 管理者ロール、インフラストラクチャ アーキテクト
6	ファブリック管理者	vRealize Automation で配置ポリシーを選択します。 ワークロード配置ポリシーを使用すると、新しいブループリントを展開するときにマシンを配置する場所を vRealize Automation に決定させることができます。配置ポリシーには、vRealize Operations Manager からの情報が必要です。	ファブリック管理者ロール

表 2-18. ブループリントをプロビジョニングするユーザーおよびロール（続き）

ステップ	ユーザー	アクション	必要なロール
7	開発者	仮想マシンをプロビジョニングするブループリントを要求します。 3 階層アプリケーションを実行する場合、ブループリントを複数のマシンで構成できます。	
8	開発者	開発者がブループリントを展開する際は、vRealize Operations Manager が、申請内容に関連するクラスタに適した配置ポリシーを検索します。	

配置ポリシーの詳細については、[配置ポリシー](#)を参照してください。

ワークロード配置を設定するには、[ワークロード配置の構成](#)を参照してください。

仮想マシンの配置に必要な Distributed Resource Scheduler (DRS)

vSphere DRS は、vRealize Automation と vRealize Operations Manager で仮想マシンのプロビジョニングおよび配置に使用される配置エンジンです。

vRealize Automation が仮想マシンの最適な配置を提案するためには、クラスタで DRS を有効にして、それを全自動に設定する必要があります。設定すると、vRealize Automation は vSphere DRS API を使用して、仮想マシンの正しい配置を決定します。

vRealize Automation は vRealize Operations Manager 配置サービスと連携します。vRealize Operations Manager は、DRS が有効で完全に自動化されているクラスタについてのみ、推奨する配置先を示します。

vRealize Automation ストレージ予約ポリシーの影響

vRealize Automation ストレージ予約ポリシーは、vRealize Operations Manager によるワークロード配置に影響します。

vRealize Operations Manager によるワークロード配置が有効な場合、vRealize Automation は、使用可能な予約のリストを vRealize Operations Manager に渡します。vRealize Operations Manager は、そのリストを評価して運用分析に基づくストレージ配置を行います。

注： vRealize Operations Manager によるワークロード配置では、ストレージ予約ポリシーが 1 つだけある、1 台以上のディスクを含む仮想マシンのみがサポートされます。個別のディスク配置はサポートされていないため、ディスク配置では複数のポリシーの組み合わせはサポートされていません。

ブループリントにストレージ予約ポリシーが含まれている場合、vRealize Operations Manager からのワークロード配置の推奨事項は、次のように変更されます。

構成	配置
仮想マシンに 1 台以上のディスクが含まれ、そのいずれにもストレージ予約ポリシーが指定されていない場合	配置は通常どおりに行われます。vRealize Operations Manager は、候補の予約の、フィルタリングされていない完全なリストを評価します。
仮想マシンに 1 台以上のディスクが含まれ、そのすべてに同じストレージ予約ポリシーが指定されている場合	候補の予約はストレージ レベルでフィルタリングされ、vRealize Operations Manager は、そのストレージ予約ポリシーに一致するデータストアのみを評価します。

構成	配置
仮想マシンに複数のディスクが含まれ、その一部に同じストレージ ポリシーが指定され、それ以外にはストレージ予約ポリシーが指定されていない場合	<ul style="list-style-type: none"> ■ ストレージ割り当てタイプがデフォルトの [収集] である場合、すべてのディスクが同じポリシーを共有するものとして扱われます。vRealize Operations Manager は、そのストレージ予約ポリシーに一致するデータストアを評価します。 ■ ストレージ割り当てタイプが [分散] の場合、個別のディスク配置はサポートされていないため、vRealize Operations Manager の推奨事項に沿って仮想マシンを配置することはできません。その代わりに、デフォルトで vRealize Automation 配置アルゴリズムによる配置が行われます。 <p>ストレージ割り当てタイプを設定するには、カスタム プロパティを使用します。</p>
仮想マシンに複数台のディスクが含まれ、それぞれのディスクに異なるストレージ予約ポリシーが指定されている場合	競合しているストレージ予約ポリシー要件があるため、vRealize Operations Manager の推奨事項に沿ってこれらの仮想マシンを配置することはできません。その代わりに、デフォルトで vRealize Automation 配置アルゴリズムによる配置が行われます。
仮想マシンに特定のストレージ パスが必要な場合	<p>ストレージ パスをすでに指定しているため、vRealize Operations Manager の推奨事項に沿ってこれらの仮想マシンを配置することはできません。配置は、vRealize Operations Manager によって推奨される配置と一致する場合もあれば一致しない場合もあります。</p> <p>ストレージ パスを設定するには、カスタム プロパティを使用します。</p>

配置エラー - vRealize Operations Manager ベースの配置を実行できない場合、エラーにその理由が示されます。理由として、上記のリストに示されているサポートされない条件や、vRealize Operations Manager と vRealize Automation の間の通信エラーなどの環境要因が示される場合があります。

エラーを確認するには、[要求] - [実行] の順に移動します。右上にある [配置エラーを表示] をクリックします。

ワークロード配置の制限事項

新しいブループリントを展開するときに、ワークロード配置の配置ポリシーを使用してマシンを配置する際には、制限事項に注意してください。

- vRealize Operations Manager では、vRealize Automation ソリューションは、vRealize Automation が管理するクラスターと仮想マシンを識別します。
- vRealize Automation がデータセンターまたはカスタム データセンター コンテナの子オブジェクトを vRealize Operations Manager で管理している場合、これらのオブジェクトをリバランスまたは移動する機能は使用できません。vRealize Automation[] 管理対象オブジェクトでアクションの除外をオンまたはオフにすることはできません。
- vRealize Automation を管理するオブジェクトでは、ワークロード配置の動作は次のとおりです。
 - カスタム データセンターまたはデータセンターに vRealize Automation を管理するクラスターが含まれていると、ワークロード配置でクラスターのリバランスを実行できません。
 - クラスターに vRealize Automation が管理する仮想マシンが含まれていると、ワークロード配置でこれらの仮想マシンを移動できません。
- vRealize Operations Manager は、vCenter Server でリソース プールへのワークロード配置をサポートしていません。
- vRealize Operations Manager 7.5 以降では、ワークロード配置のために vSAN データストアをサポートしています。関連情報については、vRealize Operations Manager 7.5 の [リリースノート](#) を参照してください。

ワークロード配置を設定する権限

ワークロード配置および配置ポリシーを設定するには、vRealize Automation および vRealize Operations Manager における権限が必要です。

vRealize Automation では、ワークロード配置を設定するためにファブリック管理者ロールが必要です。

vRealize Automation 情報センターでユーザー ロールの概要を参照してください。

vRealize Operations Manager で、ワークロード配置のためのユーザー ロールを作成し、そのロールに権限を付与する必要があります。

- ユーザー アカウントで、オブジェクト階層に含まれる vSphere ホストとクラスタおよび vSphere ストレージに読み取り専用権限を割り当てます。
- このユーザー ロールがワークロード配置で API 呼び出しを実行できるように、API に対する読み取りと書き込みの権限を割り当てます。[管理] - [アクセス コントロール] - [権限] を選択し、[REST API] - [他のすべての読み取り/書き込み API] を選択します。

エンドポイントを登録する際に、vRealize Automation は vRealize Operations Manager ロールを使用します。また、プロビジョニング中に、カタログ アイテムを要求したユーザーの代わりに配置の推奨を要求する際にもこのロールを使用します。

詳細については、vRealize Operations Manager 情報センターでアクセス コントロールに関する情報を参照してください。

配置ポリシー

配置ポリシーを使用すると、新しいブループリントを展開するときにマシンを配置する場所を vRealize Automation に決定させることができます。配置ポリシーでは、vRealize Operations Manager の分析を使用してクラスタに対するワークロードを特定することで、配置先を提案できます。

配置ポリシーを使用する前に、いくつかの手順を実行する必要があります。vRealize Automation で、vRealize Operations Manager および vCenter Server インスタンスのエンドポイントを作成します。次に、ファブリック グループを作成し、vCenter Server エンドポイントへの予約を追加します。

vRealize Operations Manager から vRealize Automation にワークロード配置分析が確実に提供されるようにするために、以下が必要です。

- ワークロード配置に使用される vRealize Operations Manager インスタンスに vRealize Automation ソリューションをインストールします。
- vCenter Server を監視するように vRealize Operations Manager を設定します。

ワークロード配置用に vRealize Automation および vRealize Operations Manager を設定するには、[ワークロード配置の構成](#)を参照してください。

配置ポリシーの特定

vRealize Automation インスタンスで、[インフラストラクチャ] - [予約] - [配置ポリシー] の順に選択します。

vRealize Operations Manager から提供されるワークロード配置分析を使用するには、[配置の推奨に vRealize Operations Manager を使用する] を選択します。

ワークロード配置ポリシーを使用しない場合、vRealize Automation はデフォルトの配置方法を使用します。

ワークロード配置の構成

新しいブループリントを展開する際に、配置ポリシーを使用してマシンを配置するには、vRealize Operations Manager が提供する分析を使用するように vRealize Automation を構成します。また、ワークロードを統合して、クラスタのコンピューティング リソースに分散するためのポリシーを適用するように vRealize Operations Manager を構成します。

vRealize Automation で、エンドポイントを構成し、ファブリック グループを作成し、予約を追加します。vRealize Operations Manager で、ワークロードのバランス調整をサポートするようにポリシーを構成し、そのポリシーをカスタムのコンピューティング リソースが含まれているカスタム グループに適用します。

前提条件

配置ポリシーがブループリントの配置先を提案できるようになるには、いくつかの手順を実行する必要があります。

- 配置ポリシーを理解します。[配置ポリシー](#)を参照してください。
- ワークロード配置に使用される vRealize Operations Manager インスタンスの vRealize Automation にエンドポイントが存在していることを確認します。[vRealize Operations Manager エンドポイントの作成](#)を参照してください。
- vCenter Server インスタンスの vRealize Automation にエンドポイントが存在していることを確認します。[vSphere エンドポイントの作成](#)を参照してください。
- vCenter Server エンドポイントに予約を追加します。[予約](#)を参照してください。
- ファブリック グループを追加し、ユーザーがファブリック グループ管理者であることを確認します。[ファブリック グループの作成](#)を参照してください。
- vRealize Operations Manager が vRealize Automation が監視しているのと同じインフラストラクチャを監視していることを確認し、同じ vCenter Server インスタンスが含まれていることを確認します。vRealize Operations Manager 情報センターで、[VMware vSphere Solution in vRealize Operations Manager](#) を参照してください。
- 予約、ストレージ予約、ブループリント、委任プロバイダを理解します。vRealize Automation 情報センターを参照してください。
- ワークロード配置に使用される vRealize Operations Manager ポリシーでフィルとバランスの設定を理解して定義します。vRealize Operations Manager 情報センターで [Workload Automation Details](#) を参照してください。

手順

1 ワークロード配置のための vRealize Automation の構成

新しいブループリントを展開するときに、ワークロード配置分析を使用してマシンを配置するには、vRealize Automation インスタンスを準備する必要があります。

2 vRealize Automation でのワークロード配置のための vRealize Operations Manager の構成

新しいブループリントを展開するときに、vRealize Automation にワークロード配置の分析を提供してマシンを配置するには、vRealize Operations Manager インスタンスを準備する必要があります。

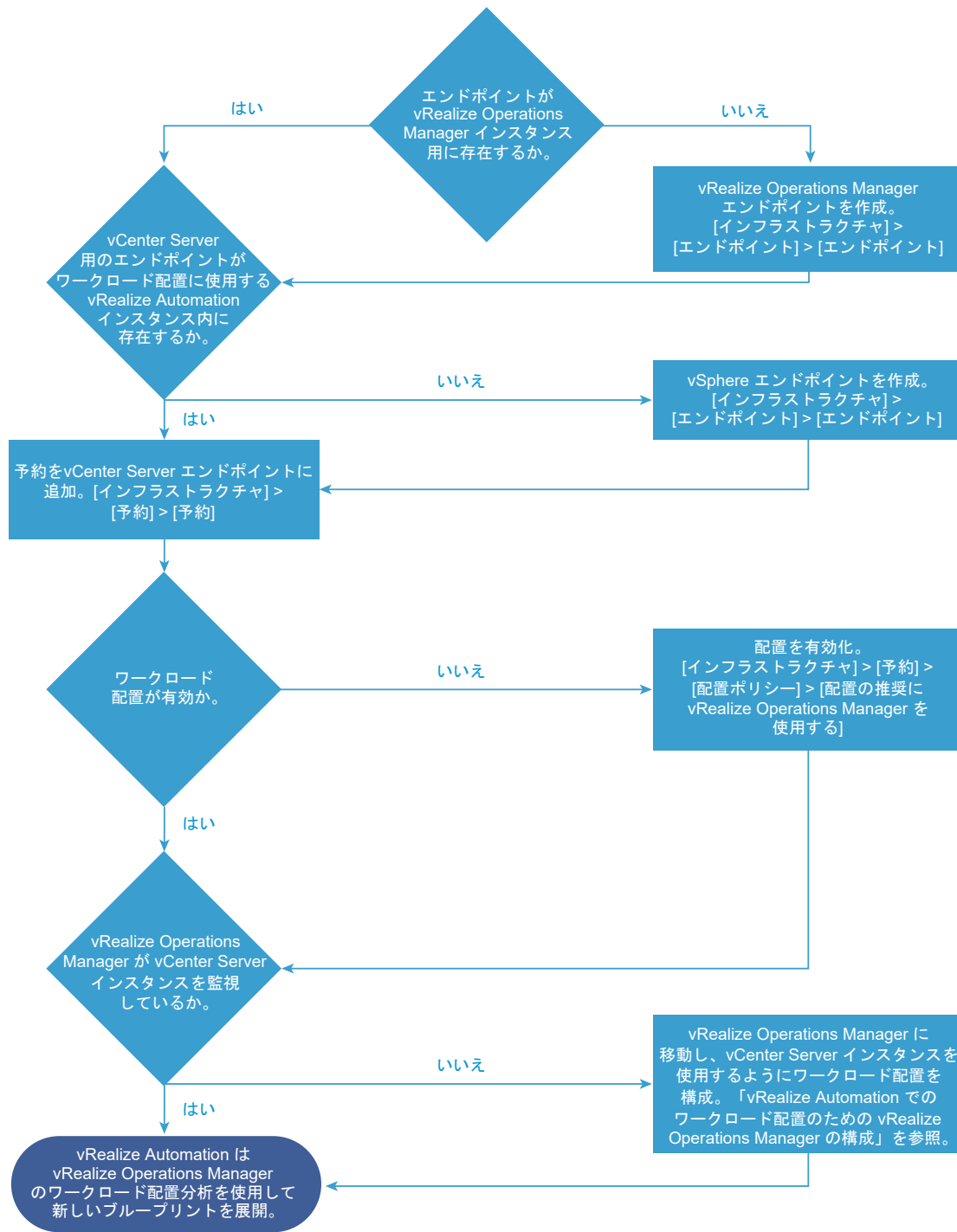
結果

ワークロード配置の分析を使用して新しいブループリントの配置先を提案するように vRealize Automation と vRealize Operations Manager を構成しました。

ワークロード配置のための vRealize Automation の構成

新しいブループリントを展開するときに、ワークロード配置分析を使用してマシンを配置するには、vRealize Automation インスタンスを準備する必要があります。

配置ポリシーを使用するために vRealize Automation インスタンスを準備するには、エンドポイントの構成、アプリケーション グループの作成、および予約の追加を行います。



前提条件

- ワークロード配置を使用するには、要件を理解しておく必要があります。[ワークロード配置の構成](#)を参照してください。
- vRealize Automation で、特定のユーザー ロールと vRealize Operations Manager 権限を追加して認証情報を検証します。vRealize Automation 情報センターでユーザー ロールの概要を参照してください。

手順

- 1 vRealize Automation インスタンスで、vRealize Operations Manager インスタンスのエンドポイントを追加し、[OK] をクリックします。
 - a [インフラストラクチャ] - [エンドポイント] - [エンドポイント] を選択します。
 - b [新規] - [管理] - [vRealize Operations Manager] を選択します。
 - c [vRealize Operations Manager] エンドポイントの全般情報を入力します。

エンドポイントのプロパティを指定する必要はありません。

- 2 vRealize Automation インスタンスで、vCenter Server インスタンスのエンドポイントを追加し、[OK] をクリックします。
 - a [インフラストラクチャ] - [エンドポイント] - [エンドポイント] を選択します。
 - b [新規] - [仮想] - [vSphere (vCenter)] の順に選択します。
 - c 一般情報、プロパティ、および vCenter Server エンドポイントの関連付けを入力します。

エンドポイントを追加して、vRealize Automation がそこからデータを収集した後、それらのエンドポイントのコンピューティング リソースを利用できます。その後、作成するファブリック グループにそれらのコンピューティング リソースを追加できます。

- 3 その他のユーザーが予約を作成して、配置ポリシーを有効にできるように、ファブリック グループを作成します。
 - a [インフラストラクチャ] - [エンドポイント] - [ファブリック グループ] の順に選択します。
 - b [新規] をクリックし、ファブリック グループの情報を入力します。

オプション	説明
Name	ファブリック グループの有意な名前を入力します。
説明	有用な説明を入力します。
ファブリック管理者	ファブリック管理者として指定する各ユーザーのメール アドレスを入力します。
コンピュート リソース	管理者が管理できるコンピュート リソース クラスタを選択します。

ファブリック グループにコンピューティング リソースを追加して、vRealize Automation がそこからデータを収集した後、ファブリック管理者はコンピューティング リソースの予約を作成できます。

4 vCenter Server インスタンス内のコンピューティング リソースの予約を作成します。

- a [インフラストラクチャ] - [予約] - [予約] を選択します。
- b [新規] - [vSphere (vCenter)] を選択します。
- c 各タブで、予約の情報を入力します。

オプション	アクション
一般	予約ポリシー、ポリシーの優先順位を選択し、[この予約を有効にする] をクリックします。
リソース	マシン割り当て、メモリ、およびストレージを選択します。リソース プールを選択する必要はありません。
ネットワーク	ネットワーク アダプタを選択します。ネットワーク プロファイルを選択する必要はありません。
プロパティ	必要に応じて、予約にカスタム プロパティを追加します。
アラート	必要に応じて、キャパシティが予約のしきい値を超えたときに受信者に通知するように [キャパシティ アラート] を選択します。

5 配置ポリシーを有効にします。

- a [インフラストラクチャ] - [予約] - [配置ポリシー] の順に選択します。
- b [配置の vRealize Operations Manager の使用に関する推奨事項] という名前のチェック ボックスを選択します。

結果

ユーザーがブループリントを展開するときに、vRealize Operations Manager の分析を使用してマシンを配置するための vRealize Automation を構成しました。

次のステップ

vRealize Operations Manager を構成して、vCenter Server インスタンスを監視し、クラスタ コンピューティング リソースにワークロード配置ポリシーを適用します。[vRealize Automation でのワークロード配置のための vRealize Operations Manager の構成](#)を参照してください。

vRealize Automation でのワークロード配置のための vRealize Operations Manager の構成

新しいブループリントを展開するときに、vRealize Automation にワークロード配置の分析を提供してマシンを配置するには、vRealize Operations Manager インスタンスを準備する必要があります。

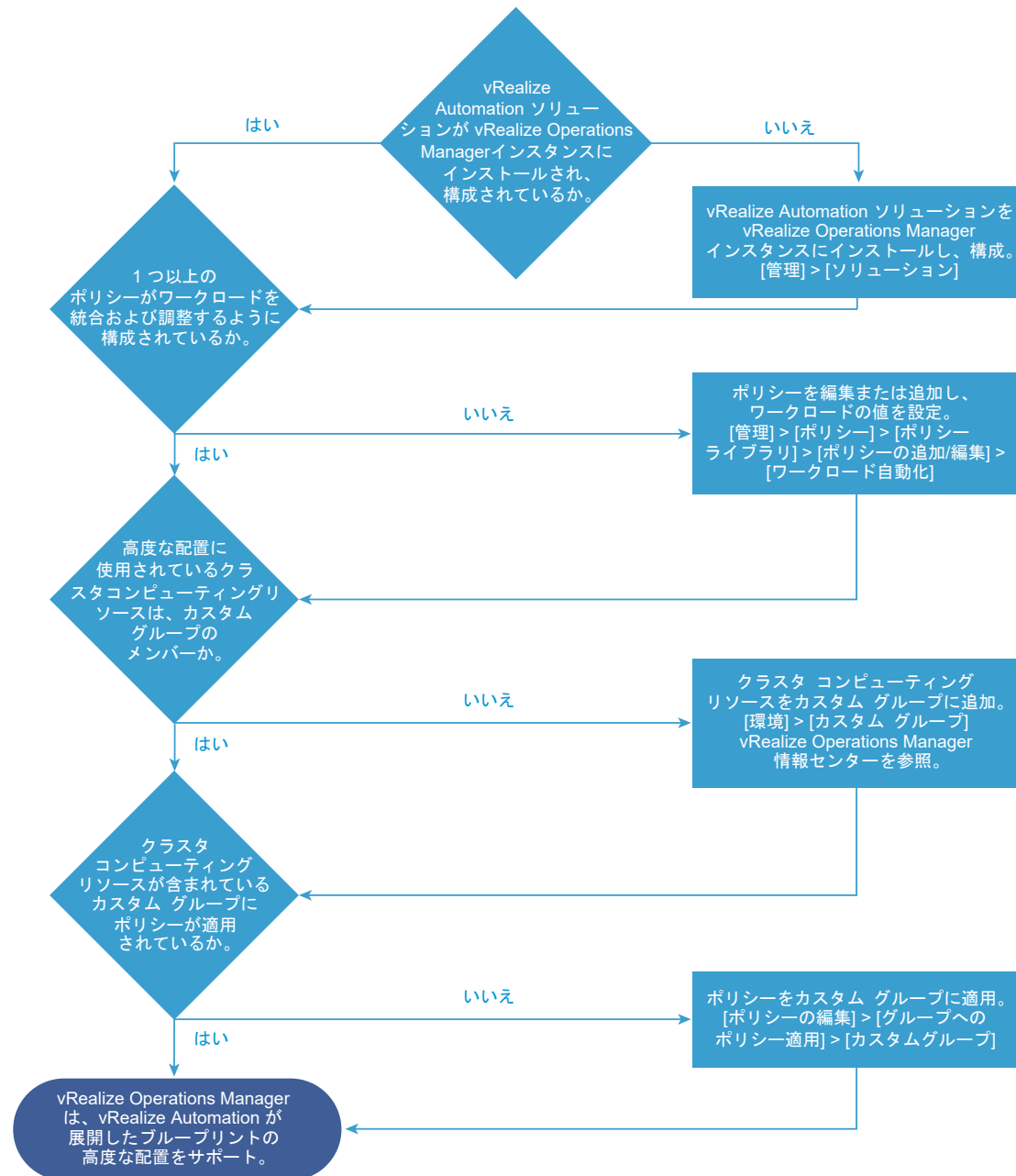
注意： 1 つの vRealize Operations Manager インスタンスにのみ、管理パックが含まれた vRealize Automation ソリューションをインストールする必要があります。

分析を vRealize Automation に提供するために vRealize Operations Manager インスタンスを準備するには、vRealize Automation ソリューションをインストールして構成します。また、ポリシーを設定して、そのポリシーをクラスタのコンピューティング リソースに適用する必要もあります。

vRealize Automation ソリューションを構成すると、vRealize Automation が管理する仮想マシンを移動したりリバランスしたりできなくなります。

vRealize Operations Manager インスタンスに vRealize Automation ソリューションがインストールされていない場合でも、ワークロード配置では、vRealize Automation が管理する仮想マシンを移動またはリバランスできます。

ワークロード配置で仮想マシンを移動できるようにするには、それらの仮想マシンがデータセンターまたはカスタムデータセンター内に置かれている必要があります。



前提条件

- vRealize Automation をワークロード配置の分析を使用するように構成します。ワークロード配置のための vRealize Automation の構成を参照してください。

- ワークロード配置に使用されている vRealize Operations Manager インスタンスで、vRealize Automation ソリューションがインストールされ構成されていることを確認します。このソリューションの詳細については、[Management Pack for vRealize Automation on Solution Exchange](#) を参照してください。vRealize Operations Manager でワークロード配置がどのように機能するかの詳細については、[Workload Automation Details](#) と vRealize Operations Manager ドキュメントで関連するトピックを参照してください。

手順

- 1 ワークロード配置を管理する vRealize Operations Manager のインスタンスで、vRealize Automation ソリューションをインストールして構成します。
 ソリューションがすでにインストールされている場合があります。
 - a vRealize Operations Manager にインストールされているソリューションを表示するには、[管理] - [ソリューション] をクリックします。
 - b vRealize Automation ソリューションがすでにインストールされているかどうかを確認します。
 vRealize Automation ソリューションがリストに表示されない場合は、ソリューションをダウンロードしてインストールします。[Management Pack for vRealize Automation on Solution Exchange](#) を参照してください。
 - c ソリューションがリストに表示される場合は、[VMware vRealize Automation ソリューション] を選択して、[構成] をクリックします。
 - d vRealize Automation ソリューションを構成し、設定を保存します。
 ソリューションを構成する詳細については、vRealize Operations Manager 情報センターで [Solutions in vRealize Operations Manager](#) を参照してください。
- 2 vRealize Operations Manager のデフォルト ポリシーを使用しない場合は、カスタム グループを作成する必要があります。その後で、カスタム グループにクラスタ コンピューティング リソースを追加します。
 デフォルト ポリシー以外のポリシーをクラスタに適用するには、カスタム グループを追加します。その後、そのポリシーをカスタム グループに適用します。デフォルト ポリシーを使用する場合は、デフォルト ポリシーがすべてのオブジェクトに適用されるため、カスタム グループを作成する必要はありません。
 - a [環境] - [カスタム グループ] をクリックします。
 - b クラスタにカスタム グループが存在しない場合は、カスタム グループを作成します。
 詳細については、vRealize Operations Manager 情報センターで、[ユーザー シナリオ：カスタム オブジェクト グループの作成](#) を参照してください。
 - c カスタム グループにクラスタを追加し、カスタム グループを保存します。

3 ワークロードを統合してバランスを調整するポリシーをクラスタで設定し、そのポリシーをカスタム グループに適用します。

統合率、バランス、フィル、CPU、メモリ、およびディスク容量の設定を確立するためのポリシーを vRealize Operations Manager で設定します。たとえば、クラスタのステータスおよび容量に基づいて新しい管理対象のワークロードの最適な配置を決定するため、[ワークロードの統合] という名前の設定を変更します。また、[ワークロードのバランス調整] のしきい値を、ワークロードを配置するために必要なレベルに変更します。1 つ以上のポリシーを設定して、クラスタのコンピューティング リソースに適用できます。

- a ポリシーを見つけるには、[管理] - [ポリシー] - [ポリシー ライブラリ] の順にクリックします。
- b ワークロード値を設定するには、[ポリシーの追加/編集] をクリックし、[ワークロード自動化] をクリックします。

[ワークロードを統合] および [クラスタ ヘッドルーム] という名前の設定は、仮想マシンの初期配置に適用されます。

- [ワークロードを統合] を [なし] に設定すると、ワークロード配置は、ポリシーを適用するすべてのクラスタ間でワークロードを分散します。[ワークロードを統合] を [なし] 以外の値に設定すると、ワークロード配置は、最も使用率の高いクラスタを最初に設定します。
- [クラスタ ヘッドルーム] は、クラスタで予約されているバッファ容量で、総キャパシティに占めるパーセンテージで示されます。たとえば、クラスタ ヘッドルームを 20% に設定すると、そのバッファのため、ワークロード配置でそのクラスタ上に仮想マシンが配置されない可能性があります。理由は、そのクラスタの CPU やメモリ用の空き容量、またはディスク容量が 20% より少なくなるためです。

- c ポリシー ワークスペースで、[グループへのポリシー適用] をクリックします。
- d カスタム グループを選択します。
- e ポリシーを保存します。

結果

ユーザーがブループリントを展開する際に、vRealize Automation がワークロード配置の分析を使用してマシンの配置先を提案するように vRealize Operations Manager を構成しました。

次のステップ

vRealize Automation と vRealize Operations Manager が環境内のエンドポイントとオブジェクトからデータを収集するのを待ちます。その後、新しいブループリントを展開するときに、vRealize Automation でワークロード配置の推奨、配置先の候補、および確認のために選択した配置が表示されるようになります。

ワークロード配置のトラブルシューティング

ワークロード配置で問題が発生した場合は、このトラブルシューティング情報を使用して問題を解決します。

ワークロード配置が正常に動作するためには vRealize Automation ソリューションが必要

ワークロード配置が個々のマシンに基づいており、マシン レベルで配置が完了しました。vRealize Automation と vRealize Operations Manager が同時にインストールされている場合は、vRealize Automation ソリューションもインストールする必要があります。

管理バックとアダプタを含むソリューションでは、コンテナのリバランス アクションまたは 仮想マシンの移動 アクションが無効になっているクラスタが識別されます。リバランス アクションは、クラスタが所属するカスタム データセンターでは無効になります。

- 管理対象の vRealize Automation クラスタを含まないカスタム データセンターに所属する非管理対象の vRealize Automation クラスタでは、仮想マシンの移動 アクションおよび コンテナのリバランス アクションが有効になります。管理対象の vRealize Automation クラスタでは、これらのアクションが無効になります。
- vRealize Operations Manager では、vRealize Automation Adapter は、予約をマッピングするクラスタ上の仮想マシンを移動またはリバランスできないようにします。

注意： vRealize Automation ソリューションは、単一の vRealize Operations Manager インスタンスにのみインストールする必要があります。

高可用性が有効だが、無効にする必要がある

HA が有効なときに vRealize Operations Manager がダウンすると、vRealize Operations Manager を呼び出すワークロード配置で使用されるタイムアウトが失敗する場合があります。

vRealize Automation は、`catalina.out` ログ ファイルにワークロード配置エラーを記録します。

vRealize Automation の vSphere エンドポイントは監視されない

vRealize Operations Manager は予約クラスタを含む vSphere vCenter Server インスタンスを監視しません。

vRealize Operations Manager でクラスタ、データストア、またはデータストア クラスタに対して vRealize Automation の候補の予約を配置しようとするときに識別できなかった予約は無視されます。配置に対する応答で、vRealize Operations Manager は予約を識別できないことを vRealize Automation に通知します。

その結果、vRealize Automation では、識別できない候補の予約を示す警告アイコンが要求の実行に関する配置の詳細に表示されます。

不一致が発生すると、vRealize Automation がリストの一番上に表示される

vRealize Automation と vRealize Operations Manager は、インフラストラクチャについて異なるビューを管理します。ただし、両方とも、同じインフラストラクチャ内の同じ vCenter Server インスタンスを管理する必要があります。

切断と不一致を識別し、詳細を表示する必要があります。

vRealize Automation Adapter がダウンしている場合の対処

初期配置は、vRealize Operations Manager から受信した宛先候補のリストに常に基づきます（インストール直後にユーザーがクラスタを追加する場合など）。

管理バックとアダプタを含む vRealize Automation ソリューションを vRealize Operations Manager で使用できない場合は、仮想マシンの移動アクションおよびコンテナのリバランス アクションを使用できます。

vRealize Operations Manager を使用した継続的な最適化

継続的な最適化を行うと、vRealize Operations Manager による vRealize Automation ワークロードの自律的な管理を行うことができます。

継続的な最適化では、ワークロードのリバランスおよび再配置を活用し、初期状態のワークロード配置に縛られることなく、vRealize Automation を vRealize Operations Manager と組み合わせて使用できます。仮想化リソースはさまざまな大きさの負荷で利用されるため、vRealize Automation でプロビジョニングされるワークロードは必要に応じて移動します。

- 継続的な最適化では、vRealize Operations Manager 内に新しいデータセンターが自動的に作成されます。各 vRealize Automation の vCenter Server エンドポイントごとに 1 つ、新しいデータセンターがあります。
- 新しく作成されたデータセンターでは、管理対象の各 vRealize Automation クラスタがエンドポイントに関連付けられています。

注： vRealize Automation と非 vRealize Automation のクラスタが混在するデータセンターを手動で作成しないでください。

- 継続的な最適化は、新しく作成した vRealize Automation ベースのデータセンターからのみ実行できます。
- 最適化では、ビジネス グループが異なる場合に発生する可能性のある vCenter Server のクラスタ間での異なる予約要件はサポートされません。

最適化は vRealize Automation に基づくデータセンター レベルで行われ、クラスタ間で予約要件が異なると正常な処理が妨げられる可能性があります。その場合、一部のターゲット クラスタまたはストレージが要件を満たさず、最適化の処理が妨げられたことを示すエラーが表示されます。

- 最適化によって vRealize Automation または vRealize Operations Manager ポリシー違反が新しく発生することはありません。
 - 既存のポリシー違反がある場合、最適化によって vRealize Operations Manager の運用インテントの問題を修正できます。
 - 既存のポリシー違反がある場合、最適化によって vRealize Operations Manager のビジネス インテントの問題は修正できません。

たとえば、仮想マシンをその予約ポリシーに含まれていないクラスタに手動で移動した場合、vRealize Operations Manager は違反を検出せず、解決も試みません。ビジネス インテントの問題を修正するには、vRealize Automation を使用してワークロードを移動する必要があります。

- このリリースは、データセンター レベルで運用インテントに従います。すべてのメンバー vRealize Automation クラスタが同じ設定で最適化されます。

クラスタごとに異なる運用インテントを設定するには、別の vCenter Server エンドポイントに関連付けられている別の vRealize Automation データセンター内にクラスタを構成する必要があります。テスト用と本番環境用のクラスタを分けることは、1 つの例です。

- vRealize Operations Manager は vRealize Automation に、vRealize Automation ポリシーおよび予約に基づいて許可される配置を問い合わせます。
- vRealize Operations Manager の配置タグは、vRealize Automation でプロビジョニングされるワークロードには適用できません。

また、複数のマシンに関わる最適化をスケジュール設定によって実行できます。定期的なスケジュールが設定された最適化は、ゼロか全体かというプロセスではありません。状況によってマシンの移動が中断された場合は、再配置が成功したマシンはその再配置が維持され、vRealize Operations Manager の通常の動作として、次の vRealize Operations Manager サイクルで残りの再配置が試みられます。このように、最適化が部分的に完了した場合に vRealize Automation に対して悪影響を及ぼすことはありません。

vRealize Automation での負荷が分散されていないワークロードの特定

vRealize Automation は、1つのクラスタにワークロードが過度にプロビジョニングされていることを検出できます。

手順

- 1 ワークロードのプロビジョニング先を確認するには、[インフラストラクチャ] - [コンピュート リソース] - [コンピュート リソース] の順にクリックします。

負荷が分散されていないマシン配置があれば、メモします。

- 2 予約によって1つのクラスタへのプロビジョニングが過度になることがあります。予約を確認するには、[インフラストラクチャ] - [予約] - [予約] の順にクリックします。

優先順位と、それがマシンの配置に影響する可能性に注意してください。

継続的な最適化の有効化

vRealize Operations Manager で vRealize Automation アダプタを追加すると、vRealize Operations Manager は自動的に vRealize Automation ベースのワークロード専用の新しいデータセンターを作成します。

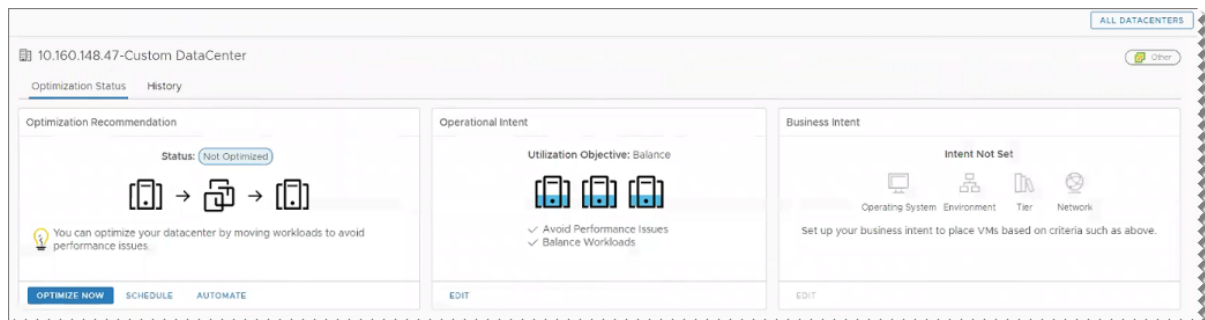
アダプタの追加以外には、継続的な最適化のための独立したインストール手順はありません。新しいデータセンター内で、ワークロードの再配置のために vRealize Operations Manager の設定と使用を開始できます。[継続的な最適化の例](#)を参照してください。

継続的な最適化の例

次の例は、vRealize Operations Manager による vRealize Automation の継続的な最適化でリバランスを行うワークフローを示します。

- 1 vRealize Operations Manager で、自動的に作成された vRealize Automation データセンターを選択します。
- 2 [運用インテント] の下で [編集] をクリックし、[負荷分散] を選択します。

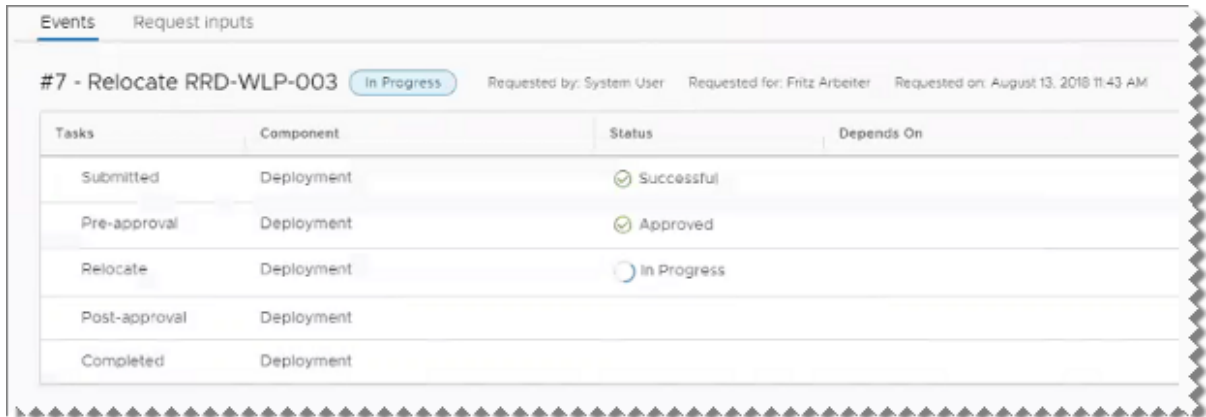
データセンターが vRealize Automation の最適化のためのものである場合、ビジネス インテントは無効なため、選択も編集もできません。



- 3 [最適化の推奨] の下で、[今すぐ最適化] をクリックします。

提案された処理の前と後を示す図が vRealize Operations Manager によって表示されます。

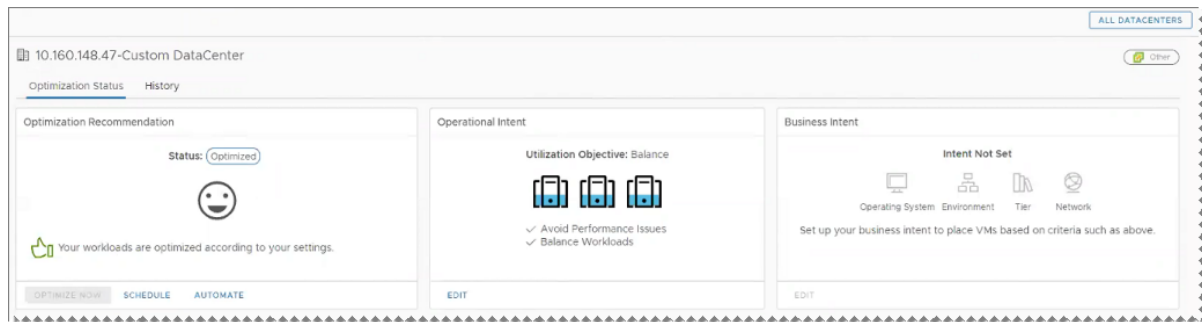
- 4 [次へ] をクリックします。
- 5 [アクションの開始] をクリックします。
- 6 vRealize Automation で、[展開] をクリックし、イベントのステータスを観察することにより、進行中の処理を監視します。



Events		Request inputs	
#7 - Relocate RRD-WLP-003 In Progress Requested by: System User Requested for: Fritz Arbeiter Requested on: August 13, 2018 11:43 AM			
Tasks	Component	Status	Depends On
Submitted	Deployment	Successful	
Pre-approval	Deployment	Approved	
Relocate	Deployment	In Progress	
Post-approval	Deployment		
Completed	Deployment		

リバランスが完了すると、vRealize Automation の表示が更新されます。[コンピュート リソース] ページに、マシンが移動したことが示されます。

vRealize Operations Manager では、次のデータ収集によって表示が更新され、最適化が完了したことが示されます。



vRealize Operations Manager で処理を確認するには、[管理] - [履歴] - [最近のタスク] の順にクリックします。

vRealize Operations Manager での vRealize Automation データセンターの特定

vRealize Operations Manager を使用して、管理対象の vRealize Automation データセンターだけを表示できます。

手順

- 1 vRealize Operations Manager で、[すべてのデータセンター] をクリックします。
- 2 右側の上部にある [表示] ドロップダウンをクリックします。

3 管理対象の vRealize Automation データセンターのみを選択します。



キー ペアの管理

キー ペアは、クラウド インスタンスのプロビジョニングと接続に使用されます。キー ペアを使用して、Windows のパスワードを復号化したり、Linux マシンにログインしたりします。

キー ペアは、Amazon AWS でのプロビジョニングに必要です。Red Hat OpenStack の場合、キー ペアの使用は任意です。

既存のキー ペアは、クラウド エンドポイントを追加するときに、データ収集の一部としてインポートされます。ファブリック管理者は、vRealize Automation コンソールを使用してキー ペアを作成および管理することもできます。vRealize Automation コンソールからキー ペアを削除すると、そのキー ペアはクラウド サービス アカウントからも削除されます。

キー ペアを手動で管理する他に、vRealize Automation を構成して、マシンまたはビジネス グループごとにキー ペアを自動生成することもできます。

- ファブリック管理者は、キー ペアの自動生成を予約レベルで構成できます。
- キー ペアをブループリント レベルで管理することになる場合、ファブリック管理者は、予約で [未指定] を選択する必要があります。
- テナント管理者またはビジネス グループ マネージャは、キー ペアの自動生成をブループリント レベルで構成できます。
- キー ペアの生成が予約とブループリントの両方のレベルで構成されている場合は、予約設定がブループリント設定をオーバーライドします。

キー ペアの作成

vRealize Automation を使用して、エンドポイントで使用するキー ペアを作成できます。

前提条件

- ファブリック管理者として vRealize Automation にログインします。
- クラウド エンドポイントを作成して、クラウド コンピュート リソースをファブリック グループに追加します。[エンドポイント シナリオの選択](#)および[ファブリック グループの作成](#)を参照してください。

手順

- 1 [インフラストラクチャ] - [予約] - [キー ペア] を選択します。
- 2 [新規] をクリックします。

- 3 [名前] テキスト ボックスに名前を入力します。
- 4 [コンピュー ト リソース] ドロップダウン メニューからクラウド リージョンを選択します。
- 5 [OK] をクリックします。

結果

[秘密鍵] 列の値が ***** である場合に、キー ペアを使用できます。

キー ペアのプライベート キーのアップロード

PEM 形式のキー ペアのプライベート キーをアップロードできます。

前提条件

- ファブリック管理者として vRealize Automation にログインします。
- キー ペアを持っている必要があります。 [キー ペアの作成](#)を参照してください。

手順

- 1 [インフラストラクチャ] - [予約] - [キー ペア] を選択します。
- 2 プライベート キーをアップロードするキー ペアを見つけます。
- 3 [編集] アイコン (✎) をクリックします。
- 4 次のいずれかの方法で、キーをアップロードします。
 - PEM でエンコードされたファイルを参照して、[アップロード] をクリックします。
 - -----BEGIN RSA PRIVATE KEY----- で始まり -----END RSA PRIVATE KEY----- で終わるプライベート キーのテキストを貼り付けます。
- 5 [保存] アイコン (✓) をクリックします。

キー ペアからのプライベート キーのエクスポート

キー ペアから PEM エンコード ファイルにプライベート キーをエクスポートします。

前提条件

- ファブリック管理者として vRealize Automation にログインします。
- プライベート キーのキー ペアが存在する必要があります。 [キー ペアのプライベート キーのアップロード](#)を参照してください。

手順

- 1 [インフラストラクチャ] - [予約] - [キー ペア] を選択します。
- 2 プライベート キーのエクスポート元のキー ペアを見つけます。
- 3 [エクスポート] アイコン (📄) をクリックします。
- 4 ファイルを保存する場所を参照し、[保存] をクリックします。

シナリオ：地域間展開のためにコンピュート リソースに場所を適用する

ファブリック管理者として、コンピュート リソースにボストンまたはロンドンのデータセンターに属するというラベルを付け、地域間の展開をサポートしたいと考えています。ブループリント アーキテクトがブループリントで場所の機能を有効化すると、ユーザーは、ボストンまたはロンドンのどちらのデータセンターにマシンをプロビジョニングするかを選択できます。



データセンターはロンドンとボストンにあります。また、ボストンにいるユーザーにはロンドンのインフラストラクチャでマシンをプロビジョニングできないようにし、一方でロンドンにいるユーザーにはボストンのインフラストラクチャでマシンをプロビジョニングできないようにします。必ず、ボストンのユーザーはボストンのインフラストラクチャでプロビジョニングを行い、ロンドンのユーザーはロンドンのインフラストラクチャでプロビジョニングを行うようにすることで、ユーザーがマシンを申請するときにプロビジョニングに適切な場所を選択できるようにします。

前提条件

- ファブリック管理者として vRealize Automation にログインします。
- システム管理者として、データセンターの場所を定義します。 [シナリオ：複数の拠点にまたがる導入環境向けにデータセンターの場所を追加する](#) を参照してください。

手順

- 1 [インフラストラクチャ] - [コンピュート リソース] - [コンピュート リソース] を選択します。
- 2 ボストンのデータセンターに配置されたコンピュート リソースをポイントし、[編集] をクリックします。
- 3 [場所] ドロップダウン メニューからボストンを選択します。
- 4 [OK] をクリックします。
- 5 必要に応じてこの手順を繰り返し、コンピュート リソースおよびボストンとロンドンの場所を関連付けます。

結果

IaaS アーキテクトがブループリントを作成すると、場所の機能を有効化でき、ユーザーがカタログ アイテム申請フォームを入力した場合にボストンまたはロンドンのマシンのプロビジョニングを選択できるようになります。 [ユーザーが地域間展開でデータセンターの場所を選択できるようにする](#) を参照してください。

サードパーティ製 IP アドレス管理プロバイダを使用した vRealize Automation 環境のプロビジョニング

vRealize Automation ネットワーク プロファイルで使用される IP アドレスおよび範囲は、サポートされているサードパーティ製 IP アドレス管理ソリューション プロバイダ (Infoblox など) から取得できます。

ネットワーク プロファイル内の IP アドレス範囲は、関連付けられている予約（ブループリントで指定）の中で使用されます。資格のあるユーザーがブループリント カタログ アイテムを使用してマシンのプロビジョニングを申請すると、サードパーティ製の IP アドレス管理によって指定された IP アドレス範囲から IP アドレスが取得されます。マシンの展開後、対応する vRealize Automation アイテムの詳細ページを照会することによって、使用されている IP アドレスを検出できます。

表 2-19. Infoblox の IP アドレス管理チェックリストを使用した vRealize Automation 環境のプロビジョニングの準備

タスク	説明	詳細
サードパーティ製 IP アドレス管理ソリューション プロバイダ プラグインまたはパッケージを取得、インポート、設定する。	vRealize Orchestrator プラグインを取得、インポートして、vRealize Orchestrator 設定ワークフローを実行し、vRealize Orchestrator で IP アドレス管理プロバイダのエンドポイント タイプを登録します。 必要な IP アドレス管理プロバイダ パッケージが VMware Solution Exchange (https://marketplace.vmware.com/vsx) に含まれていない場合は、IPAM Solution Provider SDK と関連ドキュメントを使用して独自に作成できます。 code.vmware.com/web/sdk の vRealize Automation のサードパーティ IP アドレス管理パッケージの例を参照してください。	サードパーティ製 IP アドレス管理プロバイダ サポートを提供するためのチェックリスト を参照してください。
サードパーティの IP アドレス管理ソリューション プロバイダのエンドポイントを作成する。	vRealize Automation で新しい IP アドレス管理エンドポイントを作成します。	サードパーティの IP アドレス管理プロバイダ エンドポイントの作成 を参照してください。
外部ネットワーク プロファイルでサードパーティ製 IP アドレス管理ソリューション プロバイダのエンドポイント設定を指定する。	外部ネットワーク プロファイルを作成し、定義済みの IP アドレス管理エンドポイントを vRealize Automation で指定します。	サードパーティの IP アドレス管理プロバイダを使用した外部ネットワーク プロファイルの作成 を参照してください。
必要に応じて、ルーティング ネットワーク プロファイルでサードパーティ製 IP アドレス管理ソリューション プロバイダのエンドポイント設定を指定する。	オンデマンド ネットワーク プロファイルを作成し、定義済みの IP アドレス管理エンドポイントを vRealize Automation で指定します。	サードパーティの IP アドレス管理エンドポイントを使用したルーティング ネットワーク プロファイルの作成 または サードパーティの IP アドレス管理エンドポイントを使用した NAT ネットワーク プロファイルの作成 を参照してください。
ネットワーク プロファイルを使用して予約を定義する。	ネットワーク プロファイルを呼び出す予約を vRealize Automation で作成します。	Hyper-V、KVM、SCVMM、vSphere、XenServer の予約の作成 を参照してください。
ネットワーク プロファイルを使用したブループリントを定義する。	予約を使用するブループリントを vRealize Automation で作成します。	3 章 サービス ブループリントのユーザーへの提供 を参照してください。
ブループリントを使用できるようにカタログに公開する。	vRealize Automation でカタログにブループリントを公開します。必要なすべての資格を追加します。	ブループリントの公開 を参照してください。
ブループリント カタログ アイテムを使用してマシンのプロビジョニングを申請する。	vRealize Automation からブループリント カタログ アイテムを使用してマシンのプロビジョニングを申請します。	サービス カタログの管理 を参照してください。

XaaS リソースの構成

XaaS エンドポイントを構成することにより、使用している環境に vRealize Automation を接続できます。vRealize Orchestrator プラグインをエンドポイントとして構成する場合、vRealize Orchestrator 構成インターフェイスを使用するのではなく、vRealize Automation ユーザー インターフェイスを使用してプラグインを構成します。

vRealize Orchestrator の機能と、VMware およびサードパーティの技術を vRealize Automation に公開する vRealize Orchestrator プラグインを使用するために、プラグインをエンドポイントとして追加することにより、vRealize Orchestrator プラグインを構成できます。この方法では、vCenter Server インスタンス、Microsoft Active Directory ホストなどの、さまざまなホストおよびサーバへの接続を作成します。

vRealize Automation UI を使用することにより vRealize Orchestrator プラグインをエンドポイントとして追加する場合は、デフォルトの vRealize Orchestrator サーバで構成ワークフローを実行します。構成ワークフローは、[vRealize Automation] - [XaaS] - [エンドポイント構成] ワークフロー フォルダにあります。

重要： vRealize Orchestrator および vRealize Automation コンソールでの単一プラグインの構成はサポートされず、エラーが発生します。

エンドポイントとしての Active Directory プラグインの構成


エンドポイントを追加して Active Directory プラグインを構成し、実行中の Active Directory インスタンスに接続して、ユーザーやユーザー グループ、Active Directory コンピュータ、組織単位などを管理します。

Active Directory エンドポイントを追加した後、いつでもアップデートできます。

前提条件

- Microsoft Active Directory インスタンスへのアクセス権があることを確認します。Microsoft Active Directory のドキュメントを参照してください。
- テナント管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [vRO 構成] - [エンドポイント] を選択します。
- 2 [新規] アイコン（）をクリックします。
- 3 [プラグイン] ドロップダウン メニューで [Active Directory] を選択します。
- 4 [次へ] をクリックします。
- 5 名前と説明（説明は任意）を入力します。
- 6 [次へ] をクリックします。

7 Active Directory サーバの詳細を構成します。

- a [Active Directory ホスト IP/URL] テキスト ボックスに、Active Directory が実行されているホストの IP アドレスまたは DNS 名を入力します。

- b [ポート] テキスト ボックスに、Active Directory サーバのルックアップ ポートを入力します。

vRealize Orchestrator は、Active Directory 階層ドメイン構造をサポートしています。ドメイン コントローラがグローバル カタログを使用するように構成されている場合は、ポート 3268 を使用する必要があります。デフォルト ポート 389 を使用してグローバル カタログ サーバに接続することはできません。ポート 389 および 3268 に加えて、LDAPS 用にポート 636 を使用できます。

- c [ルート] テキスト ボックスに、Active Directory サービスのルート要素を入力します。

たとえば、ドメイン名が *mycompany.com* の場合、ルート Active Directory は **dc=mycompany,dc=com** です。

このノードは、適切な認証情報を入力後にサービス ディレクトリを参照するために使用されます。サービス ディレクトリが大きい場合、ノードをツリーで指定することで、検索を絞り込んでパフォーマンスを向上させることができます。たとえば、ディレクトリ全体を検索するのではなく、

ou=employees,dc=mycompany,dc=com を指定できます。このルート要素は、従業員グループのすべてのユーザーを表示します。

- d (オプション) vRealize Orchestrator と Active Directory 間の接続用の暗号化された証明書を有効にするには、[SSL の使用] ドロップダウン メニューから [はい] を選択します。

証明書が自己署名であっても、確認を求められることなく、SSL 証明書が自動的にインポートされます。

- e (オプション) [デフォルト ドメイン] テキスト ボックスにドメインを入力します。

たとえば、ドメイン名が *mycompany.com* の場合、**@mycompany.com** と入力します。

8 共有セッション設定を構成します。

認証情報は、すべての Active Directory ワークフローおよびアクションを実行するために vRealize Orchestrator によって使用されます。

- a [共有セッションのユーザー名] テキスト ボックスに共有セッション用のユーザー名を入力します。

- a [共有セッションのパスワード] テキスト ボックスに共有セッション用のパスワードを入力します。

9 [完了] をクリックします。

結果

Active Directory インスタンスをエンドポイントとして追加しました。XaaS アーキテクトは XaaS を使用して Active Directory プラグイン ワークフローをカタログ アイテムおよびリソース アクションとして公開できます。

次のステップ

- vRealize Automation ブループリントを使用して環境内の Active Directory ユーザーを管理するには、Active Directory に基づいた XaaS ブループリントを作成します。例については、[ユーザーを作成および変更するための XaaS ブループリントとアクションの作成](#) を参照してください。

- マシンの展開時に vRealize Automation を使用して Active Directory レコードを作成する場合は、異なる Active Directory ポリシーを作成して各種ビジネス グループやブループリントに適用することができます。
[Active Directory ポリシーの作成と適用](#)を参照してください。


エンドポイントとしての HTTP-REST プラグインの構成

エンドポイントを追加し、REST ホストへ接続する HTTP-REST プラグインを構成します。

前提条件

- テナント管理者として vRealize Automation にログインします。
- REST ホストへのアクセス権があることを確認します。

手順

- 1 [管理] - [vRO 構成] - [エンドポイント] を選択します。
- 2 [新規] アイコン () をクリックします。
- 3 [プラグイン] ドロップダウン メニューから [HTTP-REST] を選択します。
- 4 [次へ] をクリックします。
- 5 名前と説明 (説明は任意) を入力します。
- 6 [次へ] をクリックします。
- 7 REST ホストの情報を指定します。
 - a [名前] テキスト ボックスにホストの名前を入力します。
 - b [URL] テキスト ボックスにホストのアドレスを入力します。

注： Kerberos アクセス認証を使用する場合、ホスト アドレスは FDQN 形式で指定する必要があります。

 - c (オプション) [接続タイムアウト (秒)] テキスト ボックスに接続のタイムアウトまでの秒数を入力します。
デフォルト値は 30 秒です。
 - d (オプション) [操作タイムアウト (秒)] テキスト ボックスに操作のタイムアウトまでの秒数を入力します。
デフォルト値は 60 秒です。
- 8 (オプション) プロキシ設定を構成します。
 - a プロキシを使用するには、[プロキシを使用する] ドロップダウン メニューから [はい] を選択します。
 - b [プロキシ アドレス] テキスト ボックスにプロキシ サーバの IP を入力します。
 - c [プロキシ ポート] テキスト ボックスにプロキシ サーバと通信するポート番号を入力します。
- 9 [次へ] をクリックします。

10 認証タイプを選択します。

オプション	アクション
なし	認証は要求されません。
OAuth 1.0	<p>OAuth 1.0 プロトコルを使用します。OAuth 1.0 の下で必須認証パラメータを指定する必要があります。</p> <ul style="list-style-type: none"> a [ユーザーキー] テキスト ボックスに、サービス プロバイダとしてユーザーを識別するのに使用するキーを入力します。 b [ユーザーシークレット] テキスト ボックスに、ユーザーキーの所有権を確立するシークレットを入力します。 c (オプション) [アクセス トークン] テキスト ボックスに、保護されたリソースへのアクセス権を取得するのにユーザーが使用するアクセス トークンを入力します。 d (オプション) [アクセス トークン シークレット] テキスト ボックスに、トークンの所有権を確立するのにユーザーが使用するシークレットを入力します。
OAuth 2.0	<p>OAuth 2.0 プロトコルを使用します。</p> <p>[トークン] テキスト ボックスに認証トークンを入力します。</p>
基本	<p>基本アクセス認証を指定します。ホストとの通信は共有セッション モードです。</p> <ul style="list-style-type: none"> a [認証ユーザー名] テキスト ボックスに共有セッション用のユーザー名を入力します。 b [認証パスワード] テキスト ボックスに共有セッション用のパスワードを入力します。
ダイジェスト	<p>暗号化を使用するダイジェスト アクセス認証を指定します。ホストとの通信は共有セッション モードです。</p> <ul style="list-style-type: none"> a [認証ユーザー名] テキスト ボックスに共有セッション用のユーザー名を入力します。 b [認証パスワード] テキスト ボックスに共有セッション用のパスワードを入力します。
NTLM	<p>Window セキュリティ サポート プロバイダ (SSP) フレームワーク内の NT LAN Manager (NTLM) アクセス認証を指定します。ホストとの通信は共有セッション モードです。</p> <ul style="list-style-type: none"> a 共有セッション用のユーザー認証情報を指定します。 <ul style="list-style-type: none"> ■ [認証ユーザー名] テキスト ボックスに共有セッション用のユーザー名を入力します。 ■ [認証パスワード] テキスト ボックスに共有セッション用のパスワードを入力します。 b NTLM 詳細の構成 <ul style="list-style-type: none"> ■ (オプション) [NTLM 認証のワークステーション] テキスト ボックスにワークステーション名を入力します。 ■ [NTLM 認証のドメイン] テキスト ボックスにドメイン名を入力します。
Kerberos	<p>Kerberos アクセス認証を指定します。ホストとの通信は共有セッション モードです。</p> <ul style="list-style-type: none"> a [認証ユーザー名] テキスト ボックスに共有セッション用のユーザー名を入力します。 b [認証パスワード] テキスト ボックスに共有セッション用のパスワードを入力します。

11 [完了] をクリックします。

結果

エンドポイントを構成し、REST ホストを追加しました。XaaS アーキテクトは XaaS を使用して、HTTP-REST プラグイン ワークフローをカタログ アイテムおよびリソース アクションとして公開できます。


エンドポイントとしての PowerShell プラグインの構成

エンドポイントを追加し、実行中の PowerShell ホストに接続する PowerShell プラグインを構成して、vRealize Orchestrator アクションおよびワークフローから PowerShell スクリプトおよびコマンドレットを呼び出してその結果と連携することができます。

前提条件

- Windows PowerShell ホストへのアクセス権があることを確認します。Microsoft Windows PowerShell の詳細については、Windows PowerShell のドキュメントを参照してください。
- テナント管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [vRO 構成] - [エンドポイント] を選択します。
- 2 [新規] アイコン（) をクリックします。
- 3 [プラグイン] ドロップダウン メニューから [PowerShell] を選択します。
- 4 [次へ] をクリックします。
- 5 名前と説明（説明は任意）を入力します。
- 6 [次へ] をクリックします。
- 7 PowerShell ホストの詳細を指定します。
 - a [名前] テキスト ボックスにホストの名前を入力します。
 - b [ホスト/IP] テキスト ボックスにホストの IP アドレスまたは FQDN を入力します。
- 8 プラグインが接続する PowerShell ホスト タイプを選択します。

オプション	アクション
WinRM	<ol style="list-style-type: none"> a PowerShell ホストの詳細の下に [ポート] テキスト ボックスに、ホストとの通信に使用するポート番号を入力します。 b [転送プロトコル] ドロップダウン メニューから転送プロトコルを選択します。 <p>注： HTTPS 転送プロトコルを使用する場合、リモート PowerShell ホストの証明書が vRealize Orchestrator キーストアにインポートされます。</p> <ol style="list-style-type: none"> c [認証] ドロップダウン メニューから認証タイプを選択します。 <p>注： Kerberos 認証を使用するには、WinRM サービスで有効化します。Kerberos 認証の構成の詳細については、『PowerShell プラグインの使用』を参照してください。</p>
SSH	なし。

- 9 [ユーザー名] および [パスワード] テキスト ボックスに、PowerShell ホストとの共有セッション通信用の認証情報を入力します。
- 10 [完了] をクリックします。

結果

Windows PowerShell ホストがエンドポイントとして追加されました。XaaS アーキテクトは XaaS を使用して、PowerShell プラグイン ワークフローをカタログ アイテムおよびリソース アクションとして公開できます。


エンドポイントとしての SOAP プラグインの構成

エンドポイントを追加し、SOAP サービスをインベントリ オブジェクトとして定義する SOAP プラグインを構成して、その定義されたオブジェクトで SOAP 操作を実行できます。

前提条件

- SOAP ホストへのアクセス権があることを確認します。このプラグインは SOAP バージョン 1.1 および 1.2、WSDL 1.1 および 2.0 をサポートします。
- テナント管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [vRO 構成] - [エンドポイント] を選択します。
- 2 [新規] アイコン () をクリックします。
- 3 [プラグイン] ドロップダウン メニューから [SOAP] を選択します。
- 4 [次へ] をクリックします。
- 5 名前と説明 (説明は任意) を入力します。
- 6 [次へ] をクリックします。
- 7 SOAP ホストの詳細を指定します。
 - a [名前] テキスト ボックスにホストの名前を入力します。
 - b [WSDL コンテンツの指定] ドロップダウン メニューから、テキストとして WSDL コンテンツを指定するかどうかを選択します。

オプション	アクション
はい	[WSDL コンテンツ] テキスト ボックスに WSDL テキストを入力します。
いいえ	[WSDL URL] テキスト ボックスに正しいパスを入力します。
 - c (オプション) [接続タイムアウト (秒)] テキスト ボックスに接続のタイムアウトまでの秒数を入力します。
デフォルト値は 30 秒です。
 - d (オプション) [要求タイムアウト (秒)] テキスト ボックスに操作のタイムアウトまでの秒数を入力します。
デフォルト値は 60 秒です。

8 (オプション) プロキシ設定を指定します。

- a プロキシを使用するには、[プロキシ] ドロップダウン メニューから [はい] を選択します。
- b [アドレス] テキスト ボックスにプロキシ サーバの IP を入力します。
- c [ポート] テキスト ボックスにプロキシ サーバと通信するポート番号を入力します。

9 [次へ] をクリックします。**10** 認証タイプを選択します。

オプション	アクション
なし	認証は要求されません。
基本	<p>基本アクセス認証を指定します。ホストとの通信は共有セッション モードです。</p> <ul style="list-style-type: none"> a [ユーザー名] テキスト ボックスに共有セッション用のユーザー名を入力します。 b [パスワード] テキスト ボックスに共有セッション用のパスワードを入力します。
ダイジェスト	<p>暗号化を使用するダイジェスト アクセス認証を指定します。ホストとの通信は共有セッション モードです。</p> <ul style="list-style-type: none"> a [ユーザー名] テキスト ボックスに共有セッション用のユーザー名を入力します。 b [パスワード] テキスト ボックスに共有セッション用のパスワードを入力します。
NTLM	<p>Windows セキュリティ サポート プロバイダ (SSP) フレームワークの NT LAN Manager (NTLM) アクセス認証を指定します。ホストとの通信は共有セッション モードです。</p> <ul style="list-style-type: none"> a ユーザー認証情報を指定します。 <ul style="list-style-type: none"> ■ [ユーザー名] テキスト ボックスに共有セッション用のユーザー名を入力します。 ■ [パスワード] テキスト ボックスに共有セッション用のパスワードを入力します。 b NTLM 設定を指定します。 <ul style="list-style-type: none"> ■ [NTLM ドメイン] テキスト ボックスにドメイン名を入力します。 ■ (オプション) [NTLM ワークステーション] テキスト ボックスにワークステーション名を入力します。
ネゴシエーション	<p>Kerberos アクセス認証を指定します。ホストとの通信は共有セッション モードです。</p> <ul style="list-style-type: none"> a ユーザー認証情報を指定します。 <ul style="list-style-type: none"> 1 [ユーザー名] テキスト ボックスに共有セッション用のユーザー名を入力します。 2 [パスワード] テキスト ボックスに共有セッション用のパスワードを入力します。 b [Kerberos サービスの SPN] テキスト ボックスに Kerberos サービスの SPN を入力します。

11 [完了] をクリックします。**結果**

SOAP サービスを追加しました。XaaS アーキテクトは XaaS を使用して、SOAP プラグイン ワークフローをカタログ アイテムおよびリソース アクションとして公開できます。


エンドポイントとしての vCenter Server プラグインの構成

エンドポイントを追加し、実行中の vCenter Server インスタンスに接続する vCenter Server プラグインを構成して、vSphere インベントリ オブジェクトを管理する XaaS ブループリントを作成できます。

前提条件

- vCenter Server をインストールして構成します。『vSphere のインストールとセットアップ』を参照してください。
- テナント管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [vRO 構成] - [エンドポイント] を選択します。
- 2 [新規] アイコン () をクリックします。
- 3 [プラグイン] ドロップダウン メニューから [vCenter Server] を選択します。
- 4 [次へ] をクリックします。
- 5 名前と説明 (説明は任意) を入力します。
- 6 [次へ] をクリックします。
- 7 vCenter Server インスタンスの情報を指定します。
 - a [追加する vCenter Server インスタンスの IP またはホスト名] テキスト ボックスにマシンの IP アドレスまたは DNS 名を入力します。

これは、追加する vCenter Server インスタンスがインストールされたマシンの IP アドレスまたは DNS 名です。
 - b [vCenter Server インスタンスのポート] テキスト ボックスに vCenter Server インスタンスと通信するポートを入力します。

デフォルト ポートは 443 です。
 - c [vCenter Server インスタンスへの接続に使用する SDK の場所] テキスト ボックスに vCenter Server インスタンスへの接続に使用する SDK の場所を入力します。

たとえば、`/sdk` です。
- 8 [次へ] をクリックします。
- 9 接続パラメータを定義します。
 - a [vCenter Server インスタンスの HTTP ポート - VC プラグイン バージョン 5.5.2 以前に該当] テキスト ボックスに vCenter Server インスタンスの HTTP ポートを入力します。
 - b [Orchestrator が vCenter Server インスタンスへの接続に使用するユーザーのユーザー名] および [Orchestrator が vCenter Server インスタンスへの接続に使用するユーザーのパスワード] テキスト ボックスに vCenter Server インスタンスへの接続を確立するために使用する vRealize Orchestrator の認証情報を入力します。

選択するユーザーは、vCenter Server エクステンションを管理する権限およびカスタム定義された権限のセットを持つ、有効なユーザーである必要があります。
- 10 [完了] をクリックします。

結果

vCenter Server インスタンスをエンドポイントとして追加しました。XaaS アーキテクトは XaaS を使用して、vCenter Server プラグイン ワークフローをカタログ アイテムおよびリソース アクションとして公開できます。

Microsoft Azure エンドポイントの作成

Microsoft Azure エンドポイントを作成すると、vRealize Automation と Azure 展開との間の認証情報による接続を容易にすることができます。

エンドポイントは、仮想マシン ブループリントの作成に使用できるリソース（ここでは Azure インスタンス）への接続を確立します。Azure エンドポイントは、Azure 仮想マシンのプロビジョニングを行うためのブループリントの基盤として使用するために必要です。複数の Azure サブスクリプションを使用する場合は、それぞれのサブスクリプション ID に対してエンドポイントが必要です。

代わりに、vRealize Orchestrator ワークフロー ツリーで、[ライブラリ] - [Azure] - [構成] の下にある Azure 接続の追加コマンドを使用して、vRealize Orchestrator から直接 Azure の接続を作成できます。ほとんどの場合、ここに記載されたエンドポイント構成を介した接続の作成方法が、推奨されるオプションになります。


Azure エンドポイントは、vRealize Orchestrator および XaaS 機能でサポートされます。Azure エンドポイントを作成、削除、または編集できます。既存のエンドポイントを変更した後、Azure ポータルで、更新された接続を通じた更新を数時間にわたって実行しないと、問題が発生する可能性があります。service vco-service restart コマンドを使用して vRealize Orchestrator サービスを再起動する必要があります。サービスを再起動しないと、エラーになります。

前提条件

- Microsoft Azure インスタンスを構成し、有効な Microsoft Azure サブスクリプションを取得します（サブスクリプション ID が必要となります）。Azure の設定とサブスクリプション ID の取得に関する詳細については、[Microsoft Azure エンドポイントの構成](#)を参照してください。
- vRealize Automation 環境に 1 つ以上のテナントと 1 つのビジネス グループがあることを確認します。
- Active Directory アプリケーションを <https://azure.microsoft.com/ja-jp/documentation/articles/resource-group-create-service-principal-portal> での説明どおりに作成します。
- エンドポイントとブループリントの構成時に必要になるため、次の Azure 関連情報を書き留めておきます。
 - サブスクリプション ID
 - テナント ID
 - ストレージ アカウント名
 - リソース グループ名
 - 場所
 - 仮想ネットワーク名
 - クライアント アプリケーションの ID
 - クライアント アプリケーションのプライベート キー
 - 仮想マシン イメージの URN

- vRealize Automation Azure 実装では、Microsoft Azure のサポート対象地域のサブセットがサポートされています。[Azure のサポート対象地域](#)を参照してください。
- テナント管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [vRO 構成] - [エンドポイント] を選択します。
- 2 [新規] アイコン（) をクリックします。
- 3 [プラグイン] タブの [プラグイン] ドロップダウン メニューをクリックし、[Azure] を選択します。
- 4 [次へ] をクリックします。
- 5 名前と説明（説明は任意）を入力します。
- 6 [次へ] をクリックします。
- 7 [詳細] タブで、エンドポイントに関する情報をテキスト ボックスに入力します。

パラメータ	説明
接続設定	
[接続名]	新しいエンドポイント接続の一意の名前。この名前は、特定の接続を識別しやすくするために vRealize Orchestrator インターフェイスに表示されます。
[Azure サブスクリプション ID]	Azure サブスクリプションの ID。ストレージ アカウントや仮想マシンなど、ユーザーが利用できる Azure のリソースは、この ID によって定義されます。
[Azure 環境]	展開する Azure リソースの地理的リージョン。vRealize Automation は、サブスクリプション ID に基づいて最新の Azure リージョンをすべてサポートしています。
リソース マネージャの設定	
[Azure サービス URI]	Azure インスタンスにアクセスするための URI。デフォルト値の <code>https://management.azure.com/</code> は、多くの標準的な実装に適しています。このボックスは、環境を選択すると自動的に入力されます。
[テナント ID]	エンドポイントで使用する Azure のテナント ID。
[クライアント ID]	エンドポイントで使用する Azure のクライアント ID。これは、Active Directory アプリケーションを作成すると割り当てられます。
[クライアント シークレット]	Azure クライアント ID で使用するキー。このキーは、Active Directory アプリケーションを作成すると割り当てられます。
[Azure ストレージ URI]	Azure ストレージ インスタンスにアクセスするための URI。このボックスは、環境を選択すると自動的に入力されます。
プロキシ設定	

パラメータ	説明
[プロキシ ホスト]	社内でプロキシ Web サーバを使用している場合は、そのサーバのホスト名を入力します。
[プロキシ ポート]	社内でプロキシ Web サーバを使用している場合は、そのサーバのポート番号を入力します。

8 (オプション) [プロパティ] をクリックし、提供されたカスタム プロパティ、プロパティ グループ、または独自のカスタム プロパティ定義を追加します。

9 [完了] をクリックします。

次のステップ

適切なリソース グループ、ストレージ アカウント、およびネットワーク セキュリティ グループを Azure に作成します。また、実装に適したロード バランサも作成する必要があります。

アクション	オプション
Azure リソース グループの作成	<ul style="list-style-type: none"> ■ Azure ポータルを使用してリソース グループを作成します。具体的な手順については、Azure ドキュメントを参照してください。 ■ Library/Azure/Resource/Create resource group にある適切な vRealize Orchestrator ワークフローを使用します。 ■ vRealize Automation で、vRealize Orchestrator ワークフローを含んだ XaaS ブループリントを作成して公開します。リソース グループは、それをサービスと資格に接続した後で申請できます。 <p>注： リソース グループ リソース タイプのサポートや管理は vRealize Automation では行われません。</p>
Azure ストレージ アカウントの作成	<ul style="list-style-type: none"> ■ Azure を使用してストレージ アカウントを作成します。具体的な手順については、Azure ドキュメントを参照してください。 ■ Library/Azure/Storage/Create storage account にある適切な vRealize Orchestrator ワークフローを使用します。 ■ vRealize Automation で、vRealize Orchestrator ワークフローを含んだ XaaS ブループリントを作成して公開します。ストレージ アカウントは、サービスを資格に接続した後で申請できます。
Azure のネットワーク セキュリティ グループの作成	<ul style="list-style-type: none"> ■ Azure を使用してセキュリティ グループを作成します。具体的な手順については、Azure ドキュメントを参照してください。 ■ Library/Azure/Network/Create Network security group にある適切な vRealize Orchestrator ワークフローを使用します。 ■ vRealize Automation で、vRealize Orchestrator ワークフローを含んだ XaaS ブループリントを作成して公開します。セキュリティ グループは、それをサービスと資格に接続した後で申請できます。

Azure のサポート対象地域

vRealize Automation Azure 実装では、Microsoft Azure のサポート対象地域のサブセットがサポートされています。

次の Azure 地域が vRealize Automation 内の Azure 実装でサポートされます。

■ 東アジア	■ オーストラリア東部
■ 東南アジア	■ オーストラリア南東部
■ 米国中部	■ インド南部
■ 米国東部	■ インド中央部
■ 米国東部 2	■ インド西部
■ 米国西部	■ カナダ中央部
■ 米国西部 2	■ カナダ東部
■ 米国北中部	■ 米国中西部
■ 米国中南部	■ 韓国中央部
■ 北ヨーロッパ	■ 韓国南部
■ 西ヨーロッパ	■ イギリス西部
■ 西日本	■ イギリス南部
■ 東日本	■ 中国東部
■ ブラジル南部	■ 中国北部

コンテナの作成と構成

vRealize Automation の コンテナ タブを使用すると、vRealize Automation のコンテナ 統合アプリケーションを開き、コンテナとコンテナ ネットワーク設定を作成および構成して、vRealize Automation ブループリントアーキテクトが利用できるようにすることができます。

統合 コンテナ アプリケーションの新規および既存のテンプレートとイメージを使用してコンテナを定義できます。次に、コンテナ コンポーネントとその関連ネットワーク設定を vRealize Automation ブループリントに追加できます。

コンテナのホストおよびクラスタの管理

追加したホストは、[クラスタ] ページから表示および管理することができます。コンテナ のコンテキストにおけるホストとは、コンテナを実行する仮想マシンまたはインフラストラクチャです。

[インフラストラクチャ] タブの [クラスタ] ページには、新しいクラスタおよびホストを追加するためのコントロールが含まれています。コンテナ環境にホストを追加するには、ホストをクラスタに追加する必要があります。既存のホストのプロビジョニング申請の状態を監視し、ライブラリと [展開] タブの任意のページから、コンテナのイベントログを表示できます。ページの右側に [申請] および [イベント ログ] パネルがあります。

コンテナ ホスト クラスタの作成

コンテナを展開するには、クラスタにホストを追加する必要があります。

前提条件

[コンテナ] タブの左上からビジネス グループを選択します。

手順

- 1 コンテナ管理者として vRealize Automation コンソールにログインします。
- 2 [コンテナ] タブをクリックします。
- 3 [インフラストラクチャ] - [コンテナ ホスト クラスタ] の順にクリックします。
- 4 [クラスタ] をクリックします。
- 5 クラスタの名前と説明を入力します。
- 6 [タイプ] ドロップダウン メニューで、いずれかの Docker 仮想コンテナ ホスト (VCH) を選択します。
- 7 ホストの IP アドレスまたはホスト名を **http(s)://<hostname>:<port>** という URL 形式で入力します。
- 8 ログイン認証情報をリストから選択します。

コンテナ は、認証情報による認証とパブリック キー/プライベート キーによる認証に対応しています。[ID 管理] ページから、認証情報を追加できます。

- 9 [保存] をクリックします。

結果

コンテナ ホスト クラスタが作成されました。

コンテナの展開ポリシーの使用

展開ポリシーは、ホストとコンテナ定義にリンクさせることができます。vRealize Automation のコンテナ の展開ポリシーは、特定のホストの環境設定とコンテナ展開時用の割り当てを設定するために使用します。

コンテナに適用される展開ポリシーには、コンテナ ホストに適用される配置よりも高い優先度が与えられます。

注： 以降の vRealize Automation リリースでは、展開ポリシーは廃止されます。

ホストの展開ポリシーの設定

特定のホストの環境設定とコンテナ展開時の割り当てを設定します。

注： 以降の vRealize Automation リリースでは、展開ポリシーは廃止されます。

前提条件

ホストをクラスタに追加します。

手順

- 1 コンテナ管理者として vRealize Automation コンソールにログインします。
- 2 [コンテナ] タブをクリックします。
- 3 [インフラストラクチャ] - [コンテナ ホスト クラスタ] の順に選択します。
- 4 編集するホストを含むクラスタをクリックします。
- 5 [リソース] をクリックします。

- 6 構成が必要なホスト上のオプション アイコンをクリックし、[編集] をクリックします。
- 7 展開ポリシーを選択し、[更新] をクリックします。

コンテナ定義用の展開ポリシーの設定

コンテナ定義用に展開ポリシーを設定します。

注： 今後の vRealize Automation リリースでは、展開ポリシーは廃止されます。

手順

- 1 [コンテナ] タブをクリックします。
- 2 [コンテナ ホスト クラスタ] をクリックして、コンテナのプロビジョニングを開始します。
- 3 リストから既存のコンテナを選択します。
- 4 プロビジョニングのオプションでは、[ポリシー] をクリックします。
- 5 [展開ポリシー] ドロップダウン リストで既存のポリシーを選択します。
- 6 コンテナをプロビジョニングするか、またはテンプレートとして保存します。

コンテナ設定の構成

新しいまたは既にあるコンテナ構成プロパティとコンテナ構成設定を使用してシングル コンテナ アプリケーションまたはマルチコンテナ アプリケーションを定義することができます。

コンテナ コンポーネントを使用した展開には、vRealize Automation のコンテナ の主要な設定に加えて、次の vRealize Automation 設定が利用できます。

- 健全性の構成
- リンク
- 公開サービス
- クラスタ サイズ、スケール イン パラメータ、スケール アウト パラメータ

コンテナ の健全性チェックの構成

健全性チェックは、独自の条件に基づいてコンテナのステータスを更新するようにその方法を構成できます。

コンテナでコマンドを実行するときは、HTTP プロトコルまたは TCP プロトコルを使用できます。健全性チェックのモードを指定することもできます。

前提条件

- サポートされている vRealize Automation 環境で vRealize Automation のコンテナ が有効になっていることを確認します。
- コンテナ管理者またはコンテナ アーキテクトのロールの権限があることを確認します。

手順

- 1 vRealize Automation にログインします。

- 2 [コンテナ] タブをクリックします。
- 3 左側のペインで [ライブラリ] - [テンプレート] の順に選択します。
- 4 テンプレートまたはイメージを編集します。

オプション	説明
テンプレートを編集するには次の手順に従います。	<ol style="list-style-type: none"> a 開きたいテンプレートの右上のセクションの [編集] をクリックします。 b 開きたいコンテナの右上のセクションの [編集] をクリックします。
イメージを編集するには次の手順に従います。	イメージの [プロビジョニング] ボタンの横にある矢印をクリックし、[追加情報の入力] をクリックします。

- 5 [健全性の構成] タブをクリックします。
- 6 健全性のモードを選択します。

表 2-20. 健全性構成モード

モード	説明
[なし]	デフォルト。健全性チェックは構成されません。
[HTTP]	<p>[HTTP] を選択する場合は、アクセスする API と使用する HTTP メソッドおよびバージョンを指定する必要があります。API は相対指定です。コンテナのアドレスを入力する必要はありません。また、操作のタイムアウト期間を指定し、健全性のしきい値を設定する必要があります。</p> <p>たとえば健全性のしきい値が 2 である場合、呼び出しが連続して 2 回以上成功すると、コンテナが健全かつ RUNNING ステータスと見なされます。非健全性のしきい値が 2 である場合、呼び出しが 2 回以上失敗すると、コンテナが非健全かつ ERROR ステータスと見なされます。健全性のしきい値と非健全性のしきい値の間に該当するコンテナの状態はすべて、DEGRADED ステータスとなります。</p>
[TCP 接続]	[TCP 接続] を選択した場合、入力するのはコンテナのポートだけにかまいません。健全性チェック時には、指定されたポートでコンテナとの TCP 接続が確立できるかどうかを試されます。また、HTTP の場合と同様、操作のタイムアウト値を指定し、健全性のしきい値または非健全性のしきい値を設定する必要があります。
[コマンド]	[コマンド] を選択する場合は、コンテナに対して実行するコマンドを入力する必要があります。健全性チェックが成功するかどうかは、コマンドの終了ステータスによって決まります。
[プロビジョニング時に健全性チェックを無視]	プロビジョニング時に健全性チェックを強制的に実行するには、このオプションを選択解除します。健全性チェックを強制的に実行することで、コンテナは、1 回の健全性チェックが成功するまで、プロビジョニングされていると見なされません。
[Autodeploy]	コンテナがエラー状態の場合にコンテナを自動的に再展開します。

- 7 [保存] をクリックします。

コンテナ のリンクの構成

コンテナ サービス間の通信とホスト間の負荷分散に伴う課題は、リンクと公開サービスによって解決されます。コンテナに使用するリンクの設定は、コンテナ で構成します。

アプリケーションでは、リンクを使用して複数のサービス間の通信を実現できます。コンテナ におけるリンクは Docker リンクに似ていますが、その接続の対象はホスト間のコンテナです。リンクは、サービス名とエイリアスという 2 つの要素から成ります。サービス名は、呼び出しの対象となるサービスまたはテンプレートの名前です。エイリアスは、サービスと通信を行うときに使用するホスト名です。

たとえば、Web サービスとデータベース サービスを含んだアプリケーションがあり、Web サービスからデータベース サービスへのリンクを **my-db** というエイリアスを使って定義する場合、その Web サービス アプリケーションは、`my-db:{PORT_OF_DB}` への TCP 接続を開くことになります。`PORT_OF_DB` は、コンテナの設定でホストに割り当てられたパブリック ポートに関係なく、データベースが待機するポートです。MySQL がそのデフォルト ポートである 3306 でアップデートの有無をチェックし、コンテナ ホストの公開ポートが 32799 である場合、この Web アプリケーションは、`my-db:3306` でデータベースにアクセスすることになります。

注： リンクの代わりにネットワークを使用することをお勧めします。現在リンクは、Docker のレガシー機能となっており、コンテナ クラスタをリンクするうえで、かなりの制限が存在します。次に示したのは、その制限の例です。

- Docker では、同じエイリアスを持つ複数のリンクがサポートされません。vRealize Automation のコンテナ によるリンク エイリアスの自動生成を有効にすることをお勧めします。
 - コンテナ ランタイムのリンクは更新できません。リンクされたクラスタをスケール アップまたはスケール ダウンしたとき、それに依存するコンテナのリンクは更新されません。
-

前提条件

- サポートされている vRealize Automation 環境で vRealize Automation のコンテナ が有効になっていることを確認します。
- コンテナ管理者またはコンテナ アーキテクトのロールの権限があることを確認します。
- サービスをリンクするためのブリッジ ネットワークが利用できることを確認します。
- 対象サービスの内部ポートが公開されていることを確認します。サービス間で通信を行えるよう、サービスは他の任意のポートにマッピングできますが、そのホストの外部からアクセスできることが必要です。
- サービスのホスト同士が相互にアクセスできることを確認します。

手順

- 1 vRealize Automation にログインします。
- 2 [コンテナ] タブをクリックします。
- 3 左側のペインで [ライブラリ] - [テンプレート] の順に選択します。

4 テンプレートまたはイメージを編集します。

オプション	説明
テンプレートを編集するには次の手順に従います。	a 開きたいテンプレートの右上のセクションの [編集] をクリックします。 b 開きたいコンテナの右上のセクションの [編集] をクリックします。
イメージを編集するには次の手順に従います。	イメージの [プロビジョニング] ボタンの横にある矢印をクリックし、[追加情報の入力] をクリックします。

5 [基本] タブをクリックします。

6 [サービス] テキスト ボックスに、コンテナが依存しているサービスをカンマ区切りで入力します。

7 そのサービスの記述名を [エイリアス] テキスト ボックスに入力します。サービスが複数ある場合はカンマ区切りで入力してください。

8 [保存] をクリックします。

コンテナ の公開サービスの構成

ロード バランサーには、アドレスとプレースホルダをコンテナの設定で指定することにより、一意のホスト名を使用できます。

URL の中で自動的に生成される部分の位置は、プレースホルダによって決まります。この値は、ホスト名ごとに一意となります。このアドレスでは、%s 形式の文字を使用して、プレースホルダの位置を指定することができます。

注： プレースホルダを使用しない場合は、システム構成に応じてホスト名のプリフィックスまたはサフィックスとして配置されます。

構築するアプリケーションに含まれているサービスをパブリックに公開する必要がある、なおかつそのサービスでスケール インとスケール アウトをサポートする必要がある場合、個々のノードに要求を振り分けることのできるロード バランサーの使用をお勧めします。そのアプリケーションをプロビジョニングした後は、サービスのスケール イン時とスケール アウト時にロード バランサーの構成が更新されます。vRealize Automation

前提条件

- サポートされている vRealize Automation 環境で vRealize Automation のコンテナ が有効になっていることを確認します。
- コンテナ管理者またはコンテナ アーキテクトのロールの権限があることを確認します。

手順

1 vRealize Automation にログインします。

2 [コンテナ] タブをクリックします。

3 左側のペインで [ライブラリ] - [テンプレート] の順に選択します。

4 テンプレートまたはイメージを編集します。

オプション	説明
テンプレートを編集するには次の手順に従います。	a 開きたいテンプレートの右上のセクションの [編集] をクリックします。 b 開きたいコンテナの右上のセクションの [編集] をクリックします。
イメージを編集するには次の手順に従います。	イメージの [プロビジョニング] ボタンの横にある矢印をクリックし、[追加情報の入力] をクリックします。

5 [ネットワーク] タブをクリックします。

6 [アドレス] テキスト ボックスに、プレースホルダの場所を入力します。

host というアドレスは、仮想ホストとして機能します。アドレス host にアクセスするには、etc/hosts ファイルにマッピング情報を追加するか、または DNS を使用してコンテナのアドレスをホスト名に対応付けます。

7 [コンテナ ポート] テキスト ボックスに、サービスを公開するためのポート番号を入力します。

フォームに記載されているサンプルの形式で入力してください。コンテナ アプリケーションで複数のポートを公開している場合は、どの内部ポートでサービスを公開できるかを指定します。

8 [保存] をクリックします。

コンテナ のクラスタ サイズとスケールの構成

コンテナ クラスタは、コンテナ の配置設定でクラスタ サイズを指定することによって作成できます。

クラスタを構成すると、指定した数のコンテナが コンテナ によってプロビジョニングされます。要求の負荷は、クラスタに存在するすべてのコンテナに分散されます。

クラスタのサイズは、プロビジョニングされるコンテナ（またはアプリケーション）のクラスタ サイズを変更することで1つずつ増減させることができます。クラスタ サイズを実行時に変更した場合、すべてのアフィニティ フィルタと配置ルールが考慮されます。

前提条件

- サポートされている vRealize Automation 環境で vRealize Automation のコンテナ が有効になっていることを確認します。
- コンテナ管理者またはコンテナ アーキテクトのロールの権限があることを確認します。

手順

- 1 vRealize Automation にログインします。
- 2 [コンテナ] タブをクリックします。
- 3 左側のペインで [ライブラリ] - [テンプレート] の順に選択します。

4 テンプレートまたはイメージを編集します。

オプション	説明
テンプレートを編集するには次の手順に従います。	a 開きたいテンプレートの右上のセクションの [編集] をクリックします。 b 開きたいコンテナの右上のセクションの [編集] をクリックします。
イメージを編集するには次の手順に従います。	イメージの [プロビジョニング] ボタンの横にある矢印をクリックし、[追加情報の入力] をクリックします。

5 [ポリシー] タブをクリックします。

6 コンテナのクラスター サイズを設定します。

7 [保存] をクリックします。

コンテナ でのテンプレートとイメージの構成および使用

コンテナ では、テンプレートを使用してコンテナをプロビジョニングします。

テンプレートは、コンテナまたは一連のコンテナのプロビジョニングに使用する、再利用可能な構成です。テンプレートでは、リンクされたサービスで構成される多層アプリケーションを定義できます。

サービスは、1 つ以上の同種のコンテナまたはイメージとして定義されます。

[テンプレート] ページで既存のテンプレートを基にしてカスタム コンテナ テンプレートを作成できます。または、適切なフォーマットの YAML ファイルをインポートすることもできます。コンテナ テンプレートやイメージをプロビジョニングすることもできます。

カスタム コンテナ テンプレートの作成

カスタム テンプレートを作成し、それを使用してコンテナを定義できます。

テンプレートは、コンテナまたはコンテナのスイートをプロビジョニングするために使用できる、再利用可能な構成です。

[テンプレート] ページには、定義したレジストリに基づいて使用できるテンプレート イメージが表示されます。カスタム テンプレートは、既存のテンプレート イメージに基づいて作成するか、またはテンプレートまたは Docker Compose ファイルをインポートして作成できます。[コンテナ テンプレートまたは Docker Compose ファイルのインポート](#)を参照してください。

カスタム テンプレートまたはイメージは、[テンプレートまたはイメージからのコンテナのプロビジョニング](#)に説明されている [プロビジョニング] - [追加情報の入力] オプションを使用して作成することもできます。

前提条件

- コンテナ管理者のロールの権限があることを確認します。

手順

1 コンテナ管理者として vRealize Automation コンソールにログインします。

2 [コンテナ] タブをクリックします。

3 左側のペインで [ライブラリ] - [テンプレート] の順に選択します。

プロビジョニングに利用できるテンプレートとイメージが一覧表示されます。

- 構成済みのテンプレート ([イメージ] ビュー)。
- 既存のテンプレートまたはカスタムのテンプレート ([テンプレート] ビュー)。
- 指定したレジストリに基づいて利用可能なすべてのテンプレートとイメージ ([すべて] ビュー)。

[インポート] オプションと[エクスポート] オプションを使用してテンプレートやイメージをインポートしたりエクスポートしたりすることもできます。

4 テンプレートに含めるイメージの [プロビジョニング] ボタンの横にある矢印をクリックします。

5 [追加情報の入力] をクリックします。

6 [テンプレートとして保存] をクリックし、変更内容を新しいコンテナ テンプレートとして Containers for vRealize Automation に保存します。

次のステップ

テンプレートは、将来のプロビジョニングのために編集できます。テンプレートからプロビジョニングされた既存のアプリケーションは、プロビジョニング後にテンプレートに加えた変更の影響を受けません。

コンテナ テンプレートまたは Docker Compose ファイルのインポート

vRealize Automation のコンテナ では、インポートした Docker コンテナ テンプレートまたは Docker Compose YAML ファイルをカスタム テンプレートとして使用できます。

YAML ファイルを使用する場合は、YAML ファイルの内容をテキストとして入力するか、YAML ファイルを参照してアップロードします。YAML ファイルは、テンプレート、異なるコンテナの構成、およびその接続を表します。サポートされている形式タイプは、Docker Compose YAML と vRealize Automation のコンテナ YAML です。

vRealize Automation のコンテナ YAML は Docker Compose に似ていますが、vRealize Automation REST API または vRealize CloudClient で表示できる vRealize Automation ブループリント YAML 形式を使用しています。vRealize Automation のコンテナ YAML では、既存の Docker Compose アプリケーションをインポートし、コンテナ を使用してそれらを変更、プロビジョニング、および管理できます。

前提条件

- サポートされている vRealize Automation 環境で vRealize Automation のコンテナ が有効になっていることを確認します。
- コンテナ管理者として vRealize Automation にログインします。

vRealize Automation サービスの REST API で使用される YAML の形式については、『vRealize Automation API リファレンス』を参照してください。

手順

1 [コンテナ] タブをクリックします。

2 左側のペインで [ライブラリ] - [テンプレート] の順に選択します。

プロビジョニングに利用できるテンプレートとイメージが一覧表示されます。

- 構成済みのテンプレート ([イメージ] ビュー)。
- 既存のテンプレートまたはカスタムのテンプレート ([テンプレート] ビュー)。
- 指定したレジストリに基づいて利用可能なすべてのテンプレートとイメージ ([すべて] ビュー)。

[インポート] オプションと[エクスポート] オプションを使用してテンプレートやイメージをインポートしたりエクスポートしたりすることもできます。

3 [テンプレートまたは Docker Compose のインポート] アイコンをクリックします。

[テンプレートのインポート] ページが表示されます。

4 YAML ファイルの内容を設定します。

オプション	説明
ファイルからロード	特定のディレクトリの YAML ファイルを参照して選択するには、[ファイルからロード] をクリックします。
テンプレートまたは Docker Compose の入力	[テンプレートまたは Docker Compose の入力] テキスト ボックスに、適切な形式の YAML ファイルの内容を貼り付けます。

5 [インポート] をクリックします。

[テンプレート] ビューに新しいテンプレートが表示されます。

テンプレートまたはイメージからのコンテナのプロビジョニング

テンプレートまたはイメージからコンテナをプロビジョニングするには、[テンプレート] ビューを使用します。

プロビジョニング プロセスでは、プロビジョニング元のテンプレートまたはイメージにある構成設定に基づいてコンテナが作成されます。

テンプレートもしくはイメージからコンテナをプロビジョニングするには、既存の構成設定を使用するか、または構成設定を編集してから、プロビジョニングを実行します。

構成設定を編集および保存して、カスタマイズされたコンテナ テンプレートまたはイメージを新規に作成することもできます。

前提条件

- サポートされている vRealize Automation 環境で vRealize Automation のコンテナ が有効になっていることを確認します。
- コンテナ管理者として vRealize Automation にログインします。

手順

1 [コンテナ] タブをクリックします。

2 左側のペインで [ライブラリ] - [テンプレート] の順に選択します。

プロビジョニングに利用できるテンプレートとイメージが一覧表示されます。

- 構成済みのテンプレート ([イメージ] ビュー)。
- 既存のテンプレートまたはカスタムのテンプレート ([テンプレート] ビュー)。
- 指定したレジストリに基づいて利用可能なすべてのテンプレートとイメージ ([すべて] ビュー)。

[インポート] オプションと[エクスポート] オプションを使用してテンプレートやイメージをインポートしたりエクスポートしたりすることもできます。

3 [すべて] ビュー、[イメージ] ビュー、または [テンプレート] ビューのオプションを使用して、プロビジョニングするイメージまたはテンプレートを表示します。

4 テンプレートまたはイメージをプロビジョニングします。

オプション	説明
既存の設定を使用してプロビジョニング。	<p>a [プロビジョニング] をクリックします。</p> <p>[プロビジョニング要求] ビューにプロビジョニングの成否に関する情報が表示されます。</p>
設定を編集してプロビジョニング。	<p>a [プロビジョニング] ボタンの隣にある矢印をクリックします。</p> <p>b [追加情報の入力] をクリックします。</p> <p>c コンテナの追加情報を [コンテナのプロビジョニング フォーム] に入力します。</p> <p>d フォームの更新が終了したら、[プロビジョニング] をクリックし、変更された設定を使用してプロビジョニングを実行します。</p> <p>e [テンプレートとして保存] をクリックし、変更内容を新しいコンテナ テンプレートとして vRealize Automation のコンテナ に保存します。</p> <p>[プロビジョニング要求] ビューにプロビジョニングの成否に関する情報が表示されます。</p>

コンテナ テンプレートまたは Docker Compose ファイルのエクスポート

コンテナ テンプレートを Docker Compose YAML ファイルまたは vRealize Automation のコンテナ YAML ファイルとしてエクスポートできます。

テンプレートをインポートし、それを vRealize Automation REST API または vRealize CloudClient を使用してプログラムで、または コンテナ でグラフィカルに変更できます。その後、変更したファイルをエクスポートできます。たとえば、Docker Compose 形式をインポートした後、vRealize Automation 複合サービス API で使用されるブループリント YAML 形式でエクスポートできます。ただし、テンプレートを Docker Compose 形式でエクスポートした場合は、コンテナ に固有の一部の構成（健全性構成、アフィニティ制約など）は含まれません。

前提条件

- サポートされている vRealize Automation 環境で vRealize Automation のコンテナ が有効になっていることを確認します。
- コンテナ管理者として vRealize Automation にログインします。

vRealize Automation サービスの REST API で使用される YAML の形式については、『vRealize Automation API リファレンス』を参照してください。

手順

1 [コンテナ] タブをクリックします。

2 左側のペインで [ライブラリ] - [テンプレート] の順に選択します。

プロビジョニングに利用できるテンプレートとイメージが一覧表示されます。

- 構成済みのテンプレート ([イメージ] ビュー)。
- 既存のテンプレートまたはカスタムのテンプレート ([テンプレート] ビュー)。
- 指定したレジストリに基づいて利用可能なすべてのテンプレートとイメージ ([すべて] ビュー)。

[インポート] オプションと[エクスポート] オプションを使用してテンプレートやイメージをインポートしたりエクスポートしたりすることもできます。

3 テンプレートを選択し、[エクスポート] アイコンをクリックします。

4 プロンプトが表示されたら、出力形式タイプを選択します。

- [YAML ブループリント]

この形式は、vRealize Automation 複合サービス API で使用されるブループリント YAML 形式に従っています。

- [Docker Compose]

この形式は、Docker Compose アプリケーションで使用される YAML 形式に従っています。

5 [エクスポート] をクリックします。

6 プロンプトが表示されたら、ファイルを保存するか、または適切なアプリケーションでファイルを開きます。

コンテナ レジストリの使用

Docker レジストリは、ステートレスなサーバサイド アプリケーションです。vRealize Automation のコンテナのレジストリを使用して Docker イメージを格納および配布できます。

レジストリを構成するには、レジストリのアドレス、カスタム レジストリ名、およびオプションで認証情報を指定する必要があります。アドレスの先頭には HTTP か HTTPS を付け、レジストリがセキュアであるか非セキュアであるか指定する必要があります。接続の種類を指定しなかった場合、デフォルトで HTTPS が使用されます。

注： HTTP の場合はポート 80 を、HTTPS の場合はポート 443 を宣言する必要があります。ポートを指定しなかった場合、Docker エンジンがポート 5000 を要求します。これにより接続が切断されることがあります。

注： HTTP は安全でないと考えられているため、HTTP レジストリを使用することは推奨されません。HTTP を使用する場合、各ホストの DOCKER_OPTS プロパティを

DOCKER_OPTS="--insecure-registry myregistrydomain.com:5000".

詳細については、Docker のドキュメント (<https://docs.docker.com/registry/insecure/>) を参照してください。

コンテナ では、次の方法で Docker Registry HTTP API V1 と V2 の両方と通信できます。

HTTP 経由の V1（非セキュアで簡素な HTTP レジストリ）

このタイプのレジストリは自由に検索できますが、`--insecure-registry` フラグを使用して各 Docker ホストを手動で構成し、非セキュアなレジストリのイメージを基にコンテナをプロビジョニングする必要があります。プロパティの設定後、Docker デーモンを再起動する必要があります。

HTTPS 経由の V1

NGINX など、リバース プロキシの背後で使います。https://github.com/docker/docker-registry から標準の実装をオープン ソースで利用できます。

HTTPS 経由の V2

https://github.com/docker/distribution で標準の実装がオープン ソース公開されています。

HTTPS 経由の V2（基本認証あり）

https://github.com/docker/distribution で標準の実装がオープン ソース公開されています。

HTTPS 経由の V2（中央サービスによる認証あり）

Docker レジストリはスタンドアロン モードで実行できます。このモードでは、認証検査はありません。サポートされるサードパーティのレジストリは、JFrog Artifactory と Harbor です。Docker Hub は、すべてのテナントでデフォルトで有効になっており、レジストリ リストには表示されませんが、システム プロパティで無効にすることができます。

注： Docker は通常、不明な認証局が署名した証明書により構成されているセキュアなレジストリとは通信を行いません。このような場合は、コンテナ サービスにより信頼されていない証明書がすべての Docker ホストに自動的にアップロードされ、ホストがこれらのレジストリに接続できるようになります。特定のホストに証明書をアップロードできない場合、そのホストは自動的に無効になります。

コンテナ レジストリの作成と管理

複数のレジストリを構成すると、パブリック イメージとプライベート イメージの両方にアクセスできます。

レジストリは、イメージをアップロードまたはダウンロードできるパブリック ストアまたはプライベート ストアです。作成したレジストリは無効にすることも、編集または削除することもできます。[テンプレート] タブに表示されるイメージは、定義するレジストリに基づきます。

レジストリを作成または管理するときに、[認証情報] または [証明書] ボタンをクリックして、認証情報と証明書を追加または管理できます。

前提条件

- コンテナ管理者として vRealize Automation にログインします。
- 少なくとも 1 台のホストが構成され、コンテナのネットワーク構成に利用できることを確認します。

手順

- 1 [コンテナ] タブをクリックします。

- 2 [ライブラリ] - [グローバル レジストリ] の順に選択します。
- 3 [レジストリ] をクリックして新しいレジストリを作成します。
- 4 レジストリのアドレスを入力します。
- 5 レジストリの名前を入力します。
- 6 ドロップダウン リストからログイン認証情報を選択します。
- 7 (オプション) [確認] をクリックして、構成されたパラメータが有効であることを確認します。
- 8 レジストリを追加するには、[保存] をクリックします。

イメージをお気に入りに追加

よく使用するイメージまたは好みのイメージにすばやくアクセスできるように、お気に入りとして追加できます。

お気に入りに追加されたイメージは、検索しなくても [リポジトリ] ホーム画面に表示されます。お気に入りにイメージを追加、削除できるのはコンテナ管理者ですが、すべてのユーザーがリポジトリごとにお気に入りのイメージを表示できます。お気に入りとしてマークされたイメージは、名前の横に星が表示されます。

手順

- 1 [リポジトリ] ページで、ドロップダウン メニューからレジストリを選択し、目的のイメージを検索します。
- 2 [プロビジョニング] の横にある矢印をクリックし、[イメージをお気に入りに追加] を選択します。

イメージが正常にお気に入りに追加されたという通知が表示され、イメージの名前の横に星が追加されます。

結果

このイメージは、検索しなくても [リポジトリ] ページに表示されます。お気に入りからイメージを削除するには、[リポジトリ] ページで [プロビジョニング] の横にある矢印をクリックし、[イメージをお気に入りから削除] を選択します。

コンテナのネットワーク リソースの構成

vRealize Automation のコンテナ アプリケーションでは、コンテナおよびコンテナ テンプレートのネットワーク構成の作成、修正、および添付が可能です。

コンテナをプロビジョニングすると、ネットワーク構成が組み込まれ、利用可能になります。vRealize Automation ブループリントに追加したコンテナ コンポーネントのネットワーク設定は、カスタマイズが可能です。

コンテナ用の新しいネットワークの作成

適切なネットワーク構成を利用できない場合は、vRealize Automation で新しいネットワーク構成を作成できます。

前提条件

- コンテナ管理者、コンテナ アーキテクト、IaaS 管理者のいずれかのロールの権限があることを確認します。
- 少なくとも 1 台のホストが構成され、コンテナのネットワーク構成に利用できることを確認します。

手順

- 1 vRealize Automation にログインします。
- 2 [コンテナ] タブをクリックします。
- 3 左側のペインで [展開] - [ネットワーク] の順に選択します。

メイン パネルには、コンテナの展開の一環としてプロビジョニングできる既存のネットワーク構成が表示されます。このネットワーク構成には、追加した Docker ホストから収集された構成と、vRealize Automation で作成された構成とが含まれています。ネットワーク構成を表す各アイコンに、ネットワークと IP アドレス管理ドライバのほか、サブネット、ゲートウェイ、IP アドレス範囲の情報、そのネットワーク構成を使用するコンテナの数、ホストの数が表示されます。

- 4 [+ネットワーク] をクリックします。
- 5 ネットワークの名前を入力します。

新しい構成の作成が完了すると、名前値に一意の識別子が付加されます。

- 6 (オプション) より詳細な設定を追加するには、[詳細設定] チェック ボックスをオンにします。

新しいネットワーク構成設定が [ネットワークの追加] パネルに表示されます。

7 高度なネットワーク構成を行います。

オプション	説明
IP アドレス管理構成	<p>サブネット</p> <p>このネットワーク構成に使用する一意のサブネットとゲートウェイのアドレスを入力します。同じコンテナ ホスト上の他のネットワークと重複しないように注意してください。</p>
カスタム プロパティ	<p>新しいネットワーク構成のカスタム プロパティを必要に応じて指定します。</p> <p>containers.ipam.driver</p> <p>コンテナ専用です。コンテナ ネットワーク コンポーネントをブループリントに追加するときに使用する IP アドレス管理ドライバを指定します。サポートされる値は、使用するコンテナ ホスト環境にインストールされているドライバによって異なります。たとえば、サポートされる値は、コンテナ ホストにインストールされている IP アドレス管理プラグインに応じて infoblox または calico になる場合があります。</p> <p>このプロパティ名と値では大文字と小文字が区別されます。プロパティ値は、追加するときに検証されません。指定したドライバがプロビジョニング時にコンテナ ホストにない場合、エラー メッセージが返され、プロビジョニングが失敗します。</p> <p>containers.network.driver</p> <p>コンテナ専用です。コンテナ ネットワーク コンポーネントをブループリントに追加するときに使用するネットワーク ドライバを指定します。サポートされる値は、使用するコンテナ ホスト環境にインストールされているドライバによって異なります。デフォルトでは、Docker によって提供されるネットワーク ドライバには bridge、overlay、および macvlan が含まれ、Virtual Container Host (VCH) によって提供されるネットワーク ドライバには bridge ドライバが含まれています。コンテナ ホストにインストールされているネットワーク プラグインに応じて、weave や calico などのサードパーティのネットワーク ドライバも使用できます。</p> <p>このプロパティ名と値では大文字と小文字が区別されます。プロパティ値は、追加するときに検証されません。指定したドライバがプロビジョニング時にコンテナ ホストにない場合、エラー メッセージが返され、プロビジョニングが失敗します。</p>

注： 詳細設定を指定せずにネットワークを作成した場合、vRealize Automation によって設定が自動的に適用されます。

8 ドロップダウン メニューから、ネットワークに接続するホストを選択します。

9 [作成] をクリックします。

コンテナ テンプレートへのネットワークの追加

コンテナ テンプレートにネットワーク構成を追加して、コンテナを互いに接続することができます。そのテンプレートを使用するすべてのアプリケーションには、このネットワーク構成が自動的に実装されます。必要に応じて既存のネットワークを追加することも、新しいネットワークを構成して追加することもできます。

前提条件

- 利用可能なテンプレートがあることを確認します。テンプレートがない場合は先に作成してください。
- コンテナ管理者、コンテナ アーキテクト、IaaS 管理者のいずれかのロールの権限があることを確認します。

- 少なくとも 1 台のホストが構成され、コンテナのネットワーク構成に利用できることを確認します。

手順

- 1 vRealize Automation にログインします。
- 2 [コンテナ] タブをクリックします。
- 3 左側のペインで [ライブラリ] - [テンプレート] の順に選択します。
プロビジョニングに利用できるテンプレートとイメージが一連のアイコンで表示されます。
- 4 (オプション) テンプレートだけが表示されるようにビューを変更する場合は、アイコンの右上のヘッダにある [ビュー: テンプレート] をクリックしてください。
- 5 カスタマイズしたいテンプレートの右上のセクションの [編集] をクリックします。
[テンプレートの編集] ページが表示され、コンテナ アイコンとプラス記号付きのブランク アイコンが表示されます。
- 6 ブランク アイコンをポイントします。
[ネットワークの追加] アイコンが表示されます。
- 7 [ネットワークの追加] アイコンをクリックします。
[ネットワークの追加] パネルが表示されます。
- 8 既存のネットワークを追加するか、新しいネットワークを作成して追加します。

オプション	説明
既存のネットワークを追加します。	a [既存] チェック ボックスをクリックします。 b [名前] フィールド内をクリックして、既存のネットワークのリストを表示します。 c 使用するネットワークを選択して、[保存] をクリックします。
新しいネットワークを構成して追加します。	a ネットワークの名前を入力します。 b より詳細な構成設定を追加するには、[詳細設定] チェック ボックスをクリックします。 c [保存] をクリックします。

- 9 ネットワークを表す水平アイコンの任意の場所にコンテナからネットワーク接続アイコンをドラッグして、コンテナにネットワークを接続します。

コンテナのボリュームの構成

vRealize Automation のコンテナ アプリケーションでは、コンテナおよびコンテナ テンプレートのボリュームの作成、修正、および添付が可能です。

vRealize Automation のコンテナ では、パーシステント データ管理に Docker ボリュームを使用します。ボリュームを使用して、次のタスクを実行できます。

- 同じホスト内のコンテナ間でボリュームを共有します。
- データを即座に更新します。
- コンテナの削除後に、ボリュームのデータを保存します。

コンテナ用の新しいボリュームの作成

コンテナ ストレージを拡張するには、まずデータ ボリュームを作成する必要があります。

前提条件

- コンテナ管理者、コンテナ アーキテクト、IaaS 管理者のいずれかのロールの権限があることを確認します。
- 少なくとも 1 台のホストが構成され、コンテナのボリューム構成に利用できることを確認します。

手順

- 1 vRealize Automation にログインします。
- 2 [コンテナ] タブをクリックします。
- 3 左側のペインで [展開] - [ボリューム] の順に選択します。

メイン パネルには、展開済みのコンテナに接続可能な既存のボリュームの構成が表示されます。このボリューム構成には、追加した Docker ホストから収集された構成と、vRealize Automation で作成された構成とが含まれています。ボリュームのインスタンスには、ドライバ、範囲、およびドライバのオプションが表示されます。

- 4 [+ボリューム] をクリックします。
- 5 ボリュームの名前を入力します。
構成の作成が完了すると、名前の値に一意的識別子が付加されます。
- 6 [ドライバ] テキスト ボックスに、使用するボリューム プラグインのドライバを入力します。何も入力しない場合は、ローカルがデフォルト値として使用されます。
- 7 (オプション) より詳細な構成設定を追加するには、[詳細設定] チェック ボックスをクリックします。
追加の設定が表示されます。
- 8 (オプション) 詳細なボリュームを設定します。

オプション	説明
ドライバのオプション	使用するドライバのオプションを指定します。このオプションは、使用しているボリュームのプラグインによって異なります。
カスタム プロパティ	新しい構成のカスタム プロパティを指定します。

- 9 ドロップダウン メニューから、ボリュームを接続するホストを選択します。
- 10 [作成] をクリックします。
[ボリュームの作成] パネルが非表示になり、追加したボリュームが [ボリューム] タブに表示されます。

次のステップ

コンテナ テンプレートへのボリュームの追加

コンテナ テンプレートへのボリュームの追加

ボリュームをテンプレートに追加して、コンテナにボリュームを接続します。

前提条件

- 利用可能なテンプレートがあることを確認します。テンプレートがない場合は先に作成してください。
- コンテナ管理者、コンテナ アーキテクト、IaaS 管理者のいずれかのロールの権限があることを確認します。
- 少なくとも 1 台のホストが構成され、コンテナのボリューム構成に利用できることを確認します。

手順

- 1 vRealize Automation にログインします。
- 2 [コンテナ] タブをクリックします。
- 3 左側のペインで [ライブラリ] - [テンプレート] の順に選択します。
プロビジョニングに利用できるテンプレートとイメージが一連のアイコンで表示されます。
- 4 (オプション) テンプレートだけが表示されるようにビューを変更する場合は、アイコンの右上のヘッダにある [ビュー: テンプレート] をクリックしてください。
- 5 カスタマイズしたいテンプレートの右上のセクションの [編集] をクリックします。
テンプレートの編集ページが表示され、コンテナ アイコン (プラス記号付きのブランク アイコンを含む) が表示されます。
- 6 プラス記号が付いたブランク アイコンの上にカーソルを置くと、[ボリュームの追加] アイコンが表示されます。
- 7 [ボリュームの追加] アイコンをクリックします。
- 8 既存のボリュームを追加するか、新しいボリュームを作成して追加します。

オプション	説明
既存のボリュームを追加します。	a [既存] チェック ボックスをクリックします。 b [名前] フィールド内をクリックして、既存のボリュームのリストを表示します。 c 使用するボリュームを選択して、[保存] をクリックします。
新しいボリュームを構成して追加します。	a ボリュームの名前を入力します。 b [ドライバ] テキスト ボックスに、使用するボリューム プラグインのドライバを入力します。外部ストレージ システムを使用していない場合は、 local と入力します。 c より詳細な構成設定を追加するには、[詳細設定] チェック ボックスをクリックします。 d [保存] をクリックします。

[ボリュームの追加] パネルが消え、テンプレートの編集ページのコンテナ アイコンの下の水平アイコンとして、追加したボリュームが表示されます。ボリューム アイコンはコンテナ アイコンの最下部にも表示されます。

- 9 ボリュームを表す水平アイコンの任意の場所にコンテナからボリューム接続アイコンをドラッグして、コンテナにボリュームを接続します。
- 10 (オプション) ボリュームがマウントされる場所を変更するには、コンテナのパスをクリックします。

次のステップ

[テンプレートまたはイメージからのコンテナのプロビジョニング](#)

PKS コンテナの作成と構成

Pivotal コンテナ サービス (PKS) により、企業およびサービス プロバイダは Kubernetes ベースのコンテナ サービスの展開と運用を簡素化できます。

PKS コンテナの主な機能は次のとおりです。

- 高可用性
 - PKS には、Kubernetes クラスタ向けに、定期的な健全性チェックと自己修正機能を備えたフォルト トレランスが組み込まれています。
- 高度なネットワークおよびセキュリティ
 - PKS は、NSX-T との深い統合により、マイクロセグメンテーション、ロード バランシング、セキュリティ ポリシーなどの高度なコンテナ ネットワークを実現しています。
- 運用の合理化
 - PKS は、Kubernetes のクラスタ展開およびライフ サイクル管理を実現します。
- マルチテナント
 - PKS は、マルチテナントをサポートしており、エンタープライズ内およびクラウド サービス内でワークロードの分離とプライバシーを実現します。

PKS エンドポイントの追加

PKS コンテナを作成する前に、PKS エンドポイントを追加する必要があります。

PKS コンテナを作成するには、まず PKS エンドポイントを追加します。PKS エンドポイントを使用すると、プラン、既存の Kubernetes クラスタ、ビジネス グループをリンクできます。

前提条件

- コンテナ管理者権限
- PKS 認証情報
- UAA アドレス
- PKS のエンドポイント アドレス

手順

- 1 [ID 管理] - [認証情報] という順で認証情報に移動し、PKS 認証情報を作成して保存します。
- 2 [PKS エンドポイント] - [エンドポイントの作成] の順に選択します。
- 3 保存する前に、PKS エンドポイントとテスト接続の詳細を入力します。

テストが失敗した場合は、PKS 認証情報、UAA アドレス、PKS エンドポイント アドレスが正しいことを確認します。アドレスがアクティブであるかどうかを確認するために、ping の実行が必要になることもあります。接続を再試行します。

4 [作成] をクリックして PKS エンドポイントを保存します。

注： [証明書の確認] ウィンドウが表示されます。ここで [証明書の表示] を選択すると、証明書の詳細が表示されます。[はい] をクリックして進み、エンドポイントを保存します。

結果

PKS エンドポイントが保存されます。PKS エンドポイントを保存した後、そのエンドポイントをクリックすると、それに関連付けられている使用可能な Kubernetes クラスタが表示されます。vRealize Automation 内でクラスタが登録されていない場合、[申請] 列の値は [いいえ] になります。登録するには、[クラスタを追加](#) する必要があります。エンドポイントを編集するには、PKS エンドポイント名をクリックし、その詳細を変更します。エンドポイントを削除するには、エンドポイントを選択し、[削除] をクリックします。

PKS エンドポイントをビジネス グループに割り当て

PKS エンドポイントを作成した後、特定のビジネス グループに割り当ててアクセス権を付与できます。

PKS エンドポイントを作成した後、特定のビジネス グループにプランを割り当てることにより、このエンドポイントへのアクセス権を付与できます。これは、特定のグループによる特定の機能へのアクセスを禁止、制限するために使用されます。

注： プランは、PKS 内で個別に作成できます。プランを vRealize Automation 内で追加、変更することはできません。

前提条件

- コンテナ管理者権限
- 既存の PKS エンドポイント

手順

- 1 PKS エンドポイントを開き、[プラン割り当て] をクリックします。
- 2 グループのリストから目的のグループ、プランのリストから目的のプランをそれぞれ選択します。

注： [+] ボタンと [-] ボタンを使用して、各ビジネス グループに複数のプランを割り当てたり、同じプランを複数のビジネス グループに割り当てたりすることができます。

- 3 [保存] をクリックしてプラン割り当てを保存します。

新しい PKS クラスタの要求

必要なクラスタ構成がない場合は、既存のエンドポイントに PKS の新しいクラスタを要求できます。

コンテナ開発者またはコンテナ管理者は、PKS エンドポイントに新しいクラスタを要求できます。各 PKS エンドポイントに複数のクラスタを含めることができます。新しいクラスタが作成されたら、[クラスタの追加] を使用して環境に追加し、必要に応じてプロビジョニングできます。

前提条件

- 既存の PKS エンドポイント

- コンテナ開発者またはコンテナ管理者の権限

手順

- 1 [PKS クラスタ] - [新規クラスタ] の順に選択します。

- 2 PKS エンドポイントを選択します。

PKS エンドポイントを選択すると、ビジネス グループで使用可能なプランに基づいてプランが自動的に入力されます。

- 3 クラスタの詳細を入力します。

注： ワーカー ノードの数はプランで定義されますが、この数はニーズに合わせて変更できます。

- 4 このクラスタに接続する方法を選択します。

- マスター ホスト名 - クラスタのホスト名を使用して接続します。DNS レコードがあることが前提です。
- マスター ノードの IP アドレス - クラスタの IP アドレスを使用して接続します。

- 5 [作成] をクリックします。

結果

新しいクラスタが作成されて、[PKS クラスタ] ホームページに表示されます。

PKS クラスタの追加

PKS エンドポイントの作成後、使用可能な関連付けられたクラスタを vRealize Automation に登録できます。

PKS エンドポイントを作成した後、vRealize Automation でクラスタを追加することにより、関連付けられたクラスタを登録できます。登録されたクラスタには、単独のイメージをプロビジョニングできます。

前提条件

- コンテナ管理者権限
- 使用可能なクラスタを持つ PKS エンドポイント

手順

- 1 クラスタの追加先が正しいビジネス グループであることを確認します。ビジネス グループの名前は、左上のペインに表示されます。ビジネス グループを切り替えるには、[グループ] をクリックします。

- 2 [PKS クラスタ] - [クラスタの追加] の順に選択します。

- 3 使用可能なクラスタにポピュレートする PKS エンドポイントを選択します。

- 4 このクラスタに接続する方法を選択します。

- マスター ホスト名 - クラスタのホスト名を使用して接続します。DNS レコードがあることが前提です。
- マスター ノードの IP アドレス - クラスタの IP アドレスを使用して接続します。

- 5 [追加] をクリックします。

結果

クラスタが [PKS クラスタ] ページに表示されます。

PKS クラスタの詳細

クラスタの詳細では、クラスタの編集と操作に必要な情報とツールが提供されています。

[PKS クラスタ] ページでクラスタ名をクリックすると、既存の PKS クラスタの確認と変更ができます。また、クラスタの詳細には、より複雑な構成でのクラスタの操作に使用できるインタラクティブなツールも含まれています。

注： クラスタのワーカー ノード数のみが編集可能です。

[ダッシュボード]

ダッシュボードのフィールド ステータスには、Kubernetes ダッシュボードがインストールされていることが示されています。ダッシュボードがインストールされている場合は、[インストール済み] をクリックしてログインすると、アクセスが可能になります。

注： ダッシュボードは、基本認証のクラスタで構成する必要があります。基本認証がない場合にはログインできません。

[KubeConfig]

kubeconfig リンクはダウンロード可能なクラスタ用の構成ファイルです。コンテナ開発者は、この構成ファイルを使用して、Kubernetes クラスタに接続したり、コマンドライン プロンプト ウィンドウ内で Kubernetes を構成したりすることが可能になります。これには、たとえば **kubect1** コマンドを使用します。

Kubernetes クラスタに対する 1 つのイメージのプロビジョニング

vRealize Automation に含まれるコンテナ機能により、PKS クラスタに 1 つのイメージをプロビジョニングすることができます。

PKS クラスタが追加された後、1 つのイメージを Kubernetes ポッドと展開の組み合わせとして、そのクラスタにプロビジョニングできます。

前提条件

- コンテナ開発者権限
- PKS クラスタ

手順

- 1 [ライブラリ] - [リポジトリ] の順に移動します。
- 2 ドロップダウン メニューから目的のレジストリを選択します。
- 3 リポジトリ テキスト ボックスを使用して、そのレジストリ内で既存のイメージを検索します。
- 4 目的のイメージのタイルで、[プロビジョニング] をクリックします。
- 5 プロビジョニングの詳細を入力し、[プロビジョニング] をクリックします。

結果

選択したイメージが Kubernetes クラスタにプロビジョニングされ、サイドバーの [申請] ウィンドウに表示されます。また、[Kubernetes] - [展開] および [Kubernetes] - [ポッド] でも確認のために表示されます。

注： クラスタをプロビジョニングするには、kubeconfig ファイルをダウンロードして **kubect1** コマンドを使用する方法もあります。詳細については、[PKS クラスタの詳細](#)を参照してください。

デフォルトの vRealize Orchestrator サーバでの追加プラグインのインストール

vRealize Orchestrator 構成インターフェイスを使用して、デフォルトの vRealize Orchestrator サーバに追加パッケージおよびプラグインをインストールすることができます。

デフォルトの vRealize Orchestrator サーバに追加プラグインをインストールし、XaaS でワークフローを使用することができます。

また、デフォルトの vRealize Orchestrator サーバに追加パッケージをインポートし、vRealize Automation 外部 IP アドレス管理プロバイダ エンドポイント タイプとして設定することもできます。Infoblox IP アドレス管理パッケージの取得、インポート、および設定については、[サードパーティ製 IP アドレス管理プロバイダ サポートを提供するためのチェックリスト](#)を参照してください。

パッケージ ファイル (.package) およびプラグイン インストール ファイル (.vmoapp または .dar) は、VMware Solution Exchange (https://solutionexchange.vmware.com/store/category_groups/cloud-management) で入手できます。プラグイン ファイルの詳細については、vRealize Orchestrator のプラグインのドキュメント (https://www.vmware.com/support/pubs/vco_plugins_pubs.html) を参照してください。

新しいプラグインのインストールに関する詳細については、『Installing and Configuring VMware vCenter Orchestrator』を参照してください。

Active Directory ポリシーの操作

Active Directory ポリシーでは、マシン レコードのプロパティ（ドメインや、vRealize Automation ブループリントを使用してレコードが作成されている組織単位など）を定義しています。

ポリシーをビジネス グループに適用している場合は、そのビジネス グループ メンバーからのすべてのマシン要求が、指定された組織単位に追加されます。複数の種類の組織単位について異なるポリシーを作成したうえで、ビジネス グループごとに異なるポリシーを適用することができます。

カスタム プロパティを使用した Active Directory ポリシーのオーバーライド

提供されている Active Directory カスタム プロパティを使用して、特定のブループリント上の Active Directory ポリシー、ドメイン、組織単位、その他の値をそのブループリントの展開時にオーバーライドすることができます。

提供されている Active Directory カスタム プロパティのリストについては、カスタム プロパティのリファレンスを参照してください。カスタム プロパティのプリフィックスは `ext.policy.activedirectory` です。

用意されているプロパティに加えて、独自のカスタム プロパティを作成できます。独自のカスタム プロパティには `ext.policy.activedirectory` をプリフィックスとして追加する必要があります。たとえば、`ext.policy.activedirectory.domain.extension` または `ext.policy.activedirectory.yourproperty` のようになります。プロパティは、カスタムの vRealize Orchestrator Active Directory ワークフローに渡されます。

カスタム プロパティの詳細については、『カスタム プロパティのリファレンス』を参照してください。オーバーライドする値によっては、プロパティ定義の作成が必要になる場合があります。たとえば、使用可能な Active Directory ポリシーを vRealize Automation から取得するプロパティ定義を作成することがあります。また、要求側ユーザーが 2 つ以上の代替組織単位からの選択を行うことができる定義を作成することもあります。『カスタム プロパティのリファレンス』を参照してください。

Active Directory ポリシーの作成と適用

ビジネス グループごとに割り当てるポリシーを変えられるように、1 つ以上の Active Directory ポリシーを作成します。複数の種類のポリシーを使用すると、ビジネス グループのメンバーシップに基づいて異なる組織単位にマシンレコードを追加できます。

必要に応じて、割り当てられている Active Directory ポリシーをオーバーライドできます。

手順

1 Active Directory ポリシーの作成

Active Directory ポリシーを作成して、ユーザーによるマシンの展開時にレコードが追加される Active Directory インスタンス内の場所を定義します。ポリシーをビジネス グループに割り当てることで、そのビジネス グループのメンバーによって展開されるすべてのマシンで、指定した組織単位内にレコードが作成されるようにすることができます。

2 シナリオ : Active Directory ポリシーをオーバーライドするためのカスタム プロパティのブループリントへの追加

開発ビジネス グループのブループリント アーキテクトとして、アプリケーション マシンとデータベース マシンが 1 台ずつ含まれているブループリントを用意しています。適用されている Active Directory ポリシーとは異なる組織単位にデータベース マシンのレコードを追加したいと考えています。

Active Directory ポリシーの作成

Active Directory ポリシーを作成して、ユーザーによるマシンの展開時にレコードが追加される Active Directory インスタンス内の場所を定義します。ポリシーをビジネス グループに割り当てることで、そのビジネス グループのメンバーによって展開されるすべてのマシンで、指定した組織単位内にレコードが作成されるようにすることができます。


展開を実行するビジネス グループごとにマシンのドメインや追加先の Active Directory インスタンスを変える必要がある場合は、Active Directory ポリシーを個別に作成します。

前提条件

- Active Directory エンドポイントが作成済みであることを確認します。[エンドポイントとしての Active Directory プラグインの構成](#)を参照してください。

- 外部の vRealize Orchestrator サーバを使用している場合は、正しく設定されていることを確認してください。[外部 vRealize Orchestrator サーバの構成](#)を参照してください。
- テナント管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [Active Directory ポリシー] の順に選択します。
- 2 [新規] アイコン（) をクリックします。
- 3 Active Directory ポリシーの詳細を設定します。

オプション	説明
ID	永続的な値を入力します。 この値に空白や特殊文字を含めることはできません。 この値は後で変更することができません。ただし、同じポリシーを異なる ID を使用して作成し直すことはできます。
説明	ポリシーの説明です。
Active Directory エンドポイント	作成するポリシーが適用される Active Directory エンドポイントを選択します。
ドメイン	ルート ドメインを入力します。 <i>mycompany.com</i> という形式にします。
組織単位	このポリシーの組織単位の識別名を入力します。 階層はカンマ区切りのリストとして入力する必要があります。たとえば、 <i>ou=development,dc=corp,dc=domain,dc=com</i> のようにします。

- 4 [OK] をクリックします。

結果

vRealize Orchestrator Active Directory エンドポイントがリストに追加されます。このポリシーは、ビジネス グループに適用したり、ブループリントまたはビジネス グループで使用したりできます。

次のステップ

- 複数のポリシー オプションを用意する場合は、さらにポリシーを作成します。
- ブループリントの展開時にビジネス グループのメンバーシップに基づいて Active Directory にレコードを追加するには、適切な Active Directory ポリシーをビジネス グループに追加します。[ビジネス グループの作成](#)を参照してください。ポリシーは、ビジネス グループの作成時に適用することも、後で追加することもできます。
- 特定のブループリントのビジネス グループについて Active Directory ポリシーをオーバーライドするには、ブループリントに Active Directory カスタム プロパティを追加します。[シナリオ：Active Directory ポリシーをオーバーライドするためのカスタム プロパティのブループリントへの追加](#)を参照してください。

シナリオ: Active Directory ポリシーをオーバーライドするためのカスタム プロパティのブループリントへの追加
開発ビジネス グループのブループリント アーキテクトとして、アプリケーション マシンとデータベース マシンが 1 台ずつ含まれているブループリントを用意しています。適用されている Active Directory ポリシーとは異なる組織単位にデータベース マシンのレコードを追加したいと考えています。

開発ビジネス グループに適用されている既存のポリシーがあります。このポリシーは ou=development, dc=corp, dc=domain, dc=com にマシン レコードを追加します。すべてのデータベース マシンを ou=databases, dc=corp, dc=domain, dc=com に追加しようとしています。データベース サーバが含まれているブループリントで、Active Directory 組織単位をオーバーライドして、データベース マシン レコードを ou=databases, dc=corp, dc=domain, dc=com に追加します。

このシナリオでは、以下の点を想定しています。


- Active Directory に開発およびデータベース用の組織単位が含まれている。
- サービスに含まれているテスト用ブループリントがあり、そのサービスに資格が付与されている。

この簡単な例で示したポリシーのオーバーライド方法のほかに、カスタム プロパティと Active Directory ポリシーを使用して、ブループリントの展開時に Active Directory にその他の変更を加えることもできます。[Active Directory ポリシーの操作](#)を参照してください。

前提条件

- Active Directory ポリシーが少なくとも 1 つあることを確認します。[Active Directory ポリシーの作成](#)を参照してください。たとえば、ou=development, dc=corp, dc=domain, dc=com にレコードを追加する開発ポリシーを作成します。
- Active Directory ポリシーの適用先としたビジネス グループがあることを確認します。[ビジネス グループの作成](#)を参照してください。たとえば、開発ビジネス グループでは開発ポリシーを使用しています。

手順

- 1 テスト用ブループリントで、キャンバス内のデータベース マシンを選択します。
- 2 [プロパティ] タブをクリックします。
- 3 [カスタム プロパティ] タブをクリックします。
- 4 [新規] アイコン () をクリックします。
- 5 デフォルトの組織単位を変更するためのカスタム プロパティを追加します。
 - a [名前] テキスト ボックスに **ext.policy.activedirectory.orgunit** と入力します。
 - b [値] テキスト ボックスに **ou=databases,dc=corp,dc=domain,dc=com** と入力します。
 - c [オーバーライド可能] を選択解除します。
 - d [OK] をクリックします。
- 6 [終了] をクリックします。

結果

このテスト用ブループリントにはカスタム プロパティが含まれていますが、ユーザーの申請フォームにこのカスタム プロパティは表示されません。

次のステップ

テスト用ブループリントを要求します。データベース マシンのレコードがデータベースの組織単位に追加されていたこと、またアプリケーション マシンのレコードが開発の組織単位に追加されていることを確認します。結果に問題がなければ、このカスタム プロパティを本番環境のブループリントに追加できます。

通知と代理人のユーザー環境設定

システム承認者通知や通知言語設定のデフォルト構成をオーバーライドするには、ユーザー環境設定を使用します。

ユーザー環境設定にアクセスするには、vRealize Automation ヘッダーでユーザー名をクリックし、[環境設定] を選択します。

次のオプションはログインしているユーザーに固有です。

表 2-21. ユーザー環境設定のオプション

オプション	説明
代理人の割り当て	承認申請を他のユーザーに再割り当てできます。たとえば、カタログ申請の承認者が、休暇で不在の場合を考えます。この場合、すべての承認通知は 1 人以上の承認者に委任されます。この割り当てにより、申請はただちに代理人に転送されます。代理人は、リストから削除されるまで有効です。
通知	E メール メッセージがデフォルト言語ではなく選択した言語で送信されるように通知言語を変更できます。言語を選択して、言語設定をサポートする通知サブスクリプションを追加します。

サービス ブループリントのユーザーへの提供

3

カタログ アイテムとアクションを作成してユーザーにオン デマンド サービスを提供し、次に資格および承認を使用して、サービス申請権限を与えるユーザーを慎重に管理します。

この章には、次のトピックが含まれています。

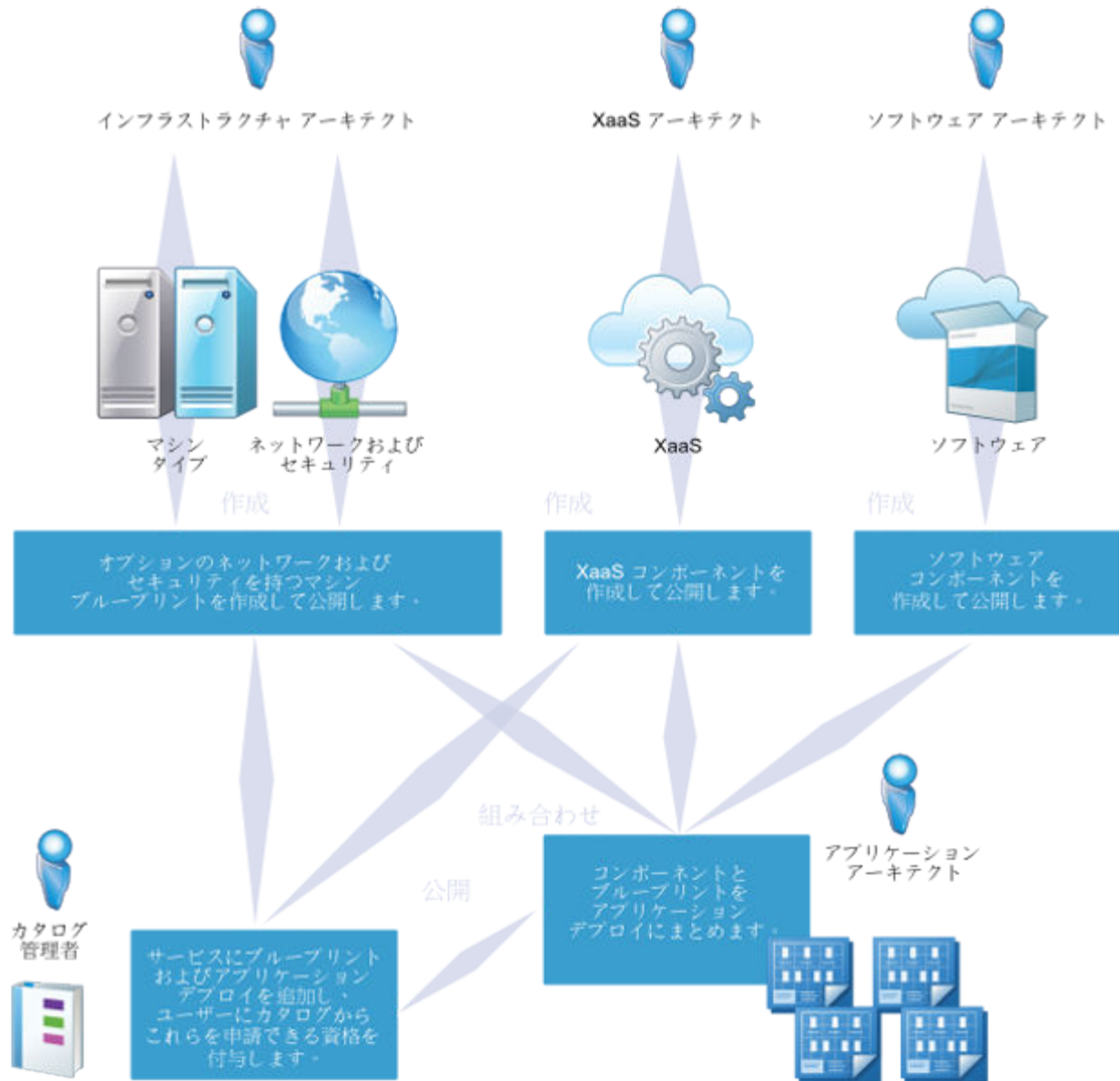
- [ブループリントの設計](#)
- [デザイン ライブラリの作成](#)
- [開発者によるブループリントの連携](#)
- [複合ブループリントの組み合わせ](#)
- [ブループリント申請フォームのカスタマイズ](#)
- [失敗したプロビジョニング要求のテストおよびトラブルシューティング](#)
- [サービス カatalogの管理](#)

ブループリントの設計

ブループリント アーキテクトは、ソフトウェア コンポーネント、マシン ブループリント、カスタム XaaS ブループリントを作成し、ユーザーがカタログから申請するアイテムを定義するブループリントにそれらのコンポーネントを組み合わせます。カタログは、デフォルトの申請フォームを表示したり、各公開されたブループリントのカスタム フォームを作成することができます。

単一のマシンや単一のカスタム XaaS ブループリント用にブループリントを作成または公開できますが、他の構成要素を使用したマシン コンポーネントと XaaS ブループリントを統合して、複数マシン、ネットワークおよびセキュリティ、ライフ サイクルが完全にサポートされているソフトウェア、およびカスタム XaaS 機能を含む高度なカタログ アイテム ブループリントを設計することもできます。

定義するカタログ アイテムに応じて、1 人のインフラストラクチャ アーキテクトが 1 つのマシン コンポーネントをブループリントとして公開するようにプロセスをシンプルにしたり、多くの異なるタイプのコンポーネントを作成する複数のアーキテクトをプロセスに追加して、申請するユーザー向けに完全なアプリケーション スタックを設計したりすることができます。



ソフトウェア コンポーネント

ソフトウェア コンポーネントを作成および公開し、マシンのプロビジョニング中にソフトウェアをインストールして、ソフトウェアのライフ サイクルをサポートできます。たとえば、開発者用のブループリントを作成し、開発環境がすでにインストールされ構成されたマシンを申請することができます。ソフトウェア コンポーネント自身はカタログ アイテムではありません。ソフトウェア コンポーネントとマシン コンポーネントを統合して、カタログ アイテム ブループリントを作成する必要があります。 [ソフトウェア コンポーネントの設計](#)を参照してください。

マシンのブループリント

シンプルなブループリントを作成および公開して単一のマシンをプロビジョニングすることも、追加のマシン コンポーネントとオプションで以下のコンポーネント タイプの任意の組み合わせを含むさらに複雑なブループリントを作成することもできます。

- ソフトウェア コンポーネント
- 既存のブループリント
- NSX ネットワークおよびセキュリティ コンポーネント
- XaaS コンポーネント
- コンテナ コンポーネント
- カスタムまたはその他のコンポーネント

[マシン ブループリントの設計](#)を参照してください。

XaaS ブループリント

vRealize Orchestrator ワークフローを XaaS ブループリントとして公開できます。たとえば、Active Directory ユーザー用のカスタム リソースを作成し、マネージャが Active Directory グループに新しいユーザーをプロビジョニングできるように XaaS ブループリントを設計できます。設計タブ以外の XaaS コンポーネントを作成および管理します。公開済みの XaaS ブループリントを再使用して、アプリケーション ブループリントを作成できますが、少なくとも 1 つ以上のマシン コンポーネントを統合した場合のみです。 [XaaS ブループリントおよびリソース アクションの設計](#)を参照してください。

複数マシン、XaaS、ソフトウェア コンポーネントを組み合わせたアプリケーション ブループリント

任意の数のマシン コンポーネント、ソフトウェア コンポーネント、XaaS ブループリントをマシン ブループリントに追加し、ユーザーに高度な機能を提供できます。

たとえば、マネージャ用のブループリントを作成し、新規雇用の設定をプロビジョニングすることができます。複数のマシン コンポーネント、ソフトウェア コンポーネント、および XaaS ブループリントを統合して、Active Directory の新しいユーザーをプロビジョニングできます。品質管理マネージャは新規雇用カタログ アイテムを申請し、新しい品質管理担当者が Active Directory にプロビジョニングされます。担当者には、この環境でテストケースを実行するために必要なすべてのソフトウェアが備わっている作業用仮想マシン 2 台（Windows と Linux の各 1 台）が支給されます。

デザイン ライブラリの作成

再利用可能なブループリント コンポーネントのライブラリを作成できます。アーキテクトは、このライブラリをアプリケーション ブループリントに組み合わせて、高度なオンデマンド サービスをユーザーに提供することができます。

最小のブループリント デザイン コンポーネント（1 つのマシン ブループリント、ソフトウェア コンポーネント、および XaaS ブループリント）のライブラリを作成してから、これらの基本構成要素を新しいさまざまな方法で組み合わせ、ユーザーに高レベルの機能を提供する高度なカタログ アイテムを作成します。

サンプルのブループリントは、VMware Solution Exchange (<https://solutionexchange.vmware.com>) および <https://code.vmware.com> から入手できます。

表 3-1. デザイン ライブラリの作成

カタログ アイテム	ロール	コンポーネント	説明	詳細
マシン	インフラストラクチャ アーキテクト	[ブループリント] タブでマシン ブループリントを作成します。	<p>マシン ブループリントを作成して、仮想、プライベート、パブリック、ハイブリッドのクラウド マシンを迅速に配信できます。</p> <p>カタログ管理者は公開されたマシン ブループリントをスタンドアロン ブループリントとしてカタログに追加できますが、他のコンポーネントとマシン ブループリントを組み合わせ、複数のマシン ブループリント、ソフトウェア、または XaaS ブループリントを含むさらに高度なカタログ アイテムを作成することもできます。</p>	マシンのブループリントの設定
マシンにおける NSX ネットワークおよびセキュリティ	インフラストラクチャ アーキテクト	[ブループリント] タブで vSphere マシン ブループリントに NSX ネットワークとセキュリティのコンポーネントを追加できます。	<p>仮想マシンが物理ネットワークと仮想ネットワークを介して安全かつ効率的に他の仮想マシンと相互に通信できるように、ネットワーク プロファイルやセキュリティ グループなど、ネットワークとセキュリティのコンポーネントを設定できます。</p> <p>カタログ管理者がカタログに追加する前に、ネットワークとセキュリティのコンポーネントを 1 つ以上の vSphere マシン コンポーネントと組み合わせる必要があります。NSX のネットワークとセキュリティのコンポーネントは vSphere マシン ブループリントにのみ適用できます。</p>	NSX 設定によるブループリントの設計
マシン上のソフトウェア	ソフトウェア アーキテクト ソフトウェア コンポーネントをデザインキャンバスに正常に追加するには、ビジネス グループ メンバー、ビジネス グループ管理者、またはテナント管理者ロールにターゲット カタログへのアクセス権があることも必要です。	[ソフトウェア] タブでソフトウェア コンポーネントを作成して公開し、[ブループリント] タブでマシン ブループリントと組み合わせます。	<p>ソフトウェア コンポーネントをマシン ブループリントに追加し、クラウド環境内で複合型アプリケーションの標準化、展開、構成、アップデート、スケール調整をします。このようなアプリケーションは、単純な Web アプリケーションから高度にカスタマイズされたアプリケーションやパッケージ化されたアプリケーションまで、多岐にわたります。</p> <p>ソフトウェア コンポーネントだけがカタログに表示されることはありません。ソフトウェア コンポーネントを作成して公開し、1 台以上のマシンを含むアプリケーション ブループリントを組み合わせる必要があります。</p>	ソフトウェア コンポーネントの作成

表 3-1. デザイン ライブラリの作成（続き）

カタログ アイテム	ロール	コンポーネント	説明	詳細
カスタム IT サービス	XaaS アーキテクト	[XaaS] タブで XaaS ブループリントを作成して公開します。	vRealize Automation の機能をマシン、ネットワーク、セキュリティ、ソフトウェア プロビジョニングの全体に対して拡張する XaaS カタログ アイテムを作成できます。既存の vRealize Orchestrator ワークフローとプラグインを使用したり、vRealize Orchestrator で開発したカスタム スクリプトを使用することで、さまざまな IT サービスの配信を自動化できます。 カタログ 管理者は公開された XaaS ブループリントをスタンドアロン ブループリントとしてカタログに追加できますが、[ブループリント] タブで他のコンポーネントと組み合わせ、さらに高度なカタログ アイテムを作成することもできます。	XaaS ブループリントおよびリソース アクションの設計
公開されたブループリント構成要素を組み立て、新しいカタログ アイテムを作成する	<ul style="list-style-type: none"> ■ アプリケーション アーキテクト ■ インフラストラクチャ アーキテクト ■ ソフトウェア アーキテクト 	[[ブループリント]] タブで、1 つ以上のマシン コンポーネントまたはマシン ブループリントに、追加のマシン ブループリント、XaaS ブループリント、ソフトウェア コンポーネントを組み合わせます。	公開したコンポーネントおよびブループリントを新しい方法で組み合わせ、高度な機能を提供する IT サービス パッケージを作成できます。	複合ブループリントの組み合わせ

マシン ブループリントの設計

マシン ブループリントは、マシンの完全な仕様であり、マシンの属性、プロビジョニング方法、およびポリシーと管理の設定を決定します。作成するカタログ アイテムの複雑さによっては、ブループリント内の 1 つ以上のマシン コンポーネントをデザイン キャンバス内の他のコンポーネントと組み合わせ、ネットワークとセキュリティ、ソフトウェア コンポーネント、XaaS コンポーネント、および他のブループリント コンポーネントを含む、より精巧なカタログ アイテムを作成できます。

仮想プロビジョニング用として容量を効率的に利用したストレージ

容量を効率的に利用するストレージ テクノロジーは、マシンの操作で実際に必要になるストレージのみを使用することで、従来のストレージ方法の非効率的な部分を排除しています。通常、これはマシンに実際に割り当てられるストレージの一部のみです。vRealize Automation は、容量を効率的に利用するテクノロジーを使用した 2 種類のプロビジョニング（シン プロビジョニングと FlexClone プロビジョニング）をサポートしています。

標準ストレージを使用すると、パワーオフでも、プロビジョニングされたマシンに割り当てられるストレージは、マシンに正常にコミットされます。これにより、ストレージ リソースが著しく消費される場合があります。それは、いくつかの物理マシンが 100% のフル ディスクを使用して動作するように、いくつかの仮想マシンがマシンに割り当てられたストレージを実際にすべて使用するためです。容量を効率的に利用するストレージ テクノロジーを使用すると、割り当てられたストレージおよび使用するストレージは個別に追跡され、使用するストレージのみがプロビジョニングされたマシンに正常にコミットされます。

シン プロビジョニング

シン プロビジョニングでは、すべての仮想プロビジョニング方法がサポートされています。仮想プラットフォーム、ストレージ タイプ、およびデフォルト ストレージ構成に応じて、シン プロビジョニングがマシン プロビジョニング時に常に使用される可能性があります。たとえば、NFS を使用して vSphere ESX Server を統合する場合は、シン プロビジョニングが常に採用されます。しかし、ローカルまたは iSCSI ストレージを使用して vSphere ESX Server を統合する場合は、カスタム プロパティ `VirtualMachine.Admin.ThinProvision` がブループリントで指定された場合のみ、マシンのプロビジョニングにシン プロビジョニングが使用されます。シン プロビジョニングの詳細については、仮想プラットフォームで提供されるドキュメントを参照してください。

Net App FlexClone プロビジョニング

Network File System (NFS) ストレージおよび FlexClone テクノロジーを使用する vSphere 環境の場合、Net App FlexClone プロビジョニングのブループリントを作成できます。

NFS ストレージのみを使用できます。それ以外の場合、マシンのプロビジョニングは失敗します。他のタイプのマシン プロビジョニングの FlexClone ストレージ パスを指定できますが、FlexClone ストレージ パスは標準ストレージのように動作します。

FlexClone テクノロジーを使用するマシンのプロビジョニングに必要な手順の概要は次のとおりです。

- 1 laaS 管理者は NetApp ONTAP エンドポイントを作成します。[エンドポイント設定リファレンス](#)を参照してください。
- 2 laaS 管理者は、エンドポイントでデータ収集を実行し、エンドポイントがコンピュー ト リソースおよび予約ページに表示されるようにします。

NetApp ONTAP エンドポイントが存在しており、なおかつホストが仮想である場合は、FlexClone オプションがエンドポイント列の予約ページに表示されます。NetApp ONTAP エンドポイントが存在する場合は、ストレージ パスに割り当てられたエンドポイントが [予約] ページに表示されます。

- 3 ファブリック管理者は、vSphere の予約の作成、Flexclone ストレージの有効化、および FlexClone テクノロジーを使用する NFS ストレージ パスの指定を行います。[Hyper-V](#)、[KVM](#)、[SCVMM](#)、[vSphere](#)、[XenServer](#) の[予約の作成](#)を参照してください。
- 4 インフラストラクチャ アーキテクトまたはその他の権限を持つユーザーは、FlexClone のプロビジョニング用のブループリントを作成します。

ブループリントのパラメータ化について

コンポーネント プロファイルを使用して、ブループリントをパラメータ化できます。特定の展開タイプに応じて、大規模、中規模、小規模のブループリントを別々に作成する代わりに、仮想マシンのサイズを小規模、中規模、大規模から選択できる単一のブループリントを作成することができます。ユーザーはカタログ アイテムを展開するときに、サイズを 1 つ選択できます。

コンポーネント プロファイルにより、作成するブループリントの数を最小に抑制し、カタログを簡素化します。コンポーネント プロファイルを使用すると、ブループリントに vSphere マシン コンポーネントを定義できます。使用可能なコンポーネント プロファイルのタイプは、Size と Image です。コンポーネント プロファイルをマシン コンポーネントに追加すると、CPU 数やストレージ量など、マシン コンポーネントの他の設定よりも、そのコンポーネント プロファイル設定が優先されます。

コンポーネント プロファイルは、vSphere マシン コンポーネントでのみ使用可能です。

Size および Image コンポーネント プロファイルの値セットの定義に関する関連情報については、『カスタム プロパティのリファレンス』の「」を参照してください。

ブループリントで vSphere マシン コンポーネントのコンポーネント プロファイルおよび選択された値セットを追加する方法については、[vSphere マシン コンポーネントの設定](#)を参照してください。

OVF からインポートされた設定を使用してコンポーネント プロファイルの情報を追加する方法については、[OVF からプロビジョニングするブループリントの構成](#)を参照してください。

マシンのプロビジョニングを申請するときにコンポーネント プロファイルを使用する方法については、[パラメータ化されたブループリントを使用したマシン プロビジョニングの申請](#)を参照してください。

承認ポリシーを作成することで、Size および Image コンポーネント プロファイルの値セット条件に基づいて、ブループリントによるマシンのプロビジョニングを申請するときに、事前承認を要求できます。詳細については、[仮想マシン ポリシー タイプに基づく承認ポリシーの例](#)を参照してください。

注：

カタログからマシンのプロビジョニングを申請するときに、ブループリントのパラメータ化を使用する方法については、[パラメータ化されたブループリントを使用したマシン プロビジョニングの申請](#)を参照してください。

マシンのブループリントの設定

他のアーキテクトがアプリケーション ブループリントのコンポーネントとして再使用することができ、カタログ管理者がカタログ サービスに含めることができるスタンドアロン ブループリントとして、マシン コンポーネントを設定および公開します。


この手順では、ブループリントの作成プロセスの簡単な概要を説明します。追加の詳細は、以下を参照してください。

- [NSX 設定によるブループリントの設計](#)
- [ブループリントのパラメータ化について](#)
- [\[ブループリントのプロパティ\] 設定](#)
- [OVF からプロビジョニングするブループリントの構成](#)
- [ブループリントとコンテンツのエクスポートおよびインポート](#)
- [Microsoft Azure ブループリントの作成とリソース アクションの組み込み](#)
- [vSphere ブループリントへの構成管理機能の追加](#)

前提条件

- インフラストラクチャ アーキテクトとして vRealize Automation にログインします。
- テンプレート、WinPE、および ISO の作成などのプロビジョニングのための外部準備を完了するか、または管理者から外部準備に関する情報を収集します。
- テナントを構成します。[テナント設定の構成](#)を参照してください。
- IaaS リソースを構成します。[IaaS リソース設定のチェックリスト](#)を参照してください。
- 『vRealize Automation の構成』を参照してください。

手順

- 1 [設計] - [ブループリント] を選択します。
- 2 [新規] アイコン () をクリックします。
- 3 [新規ブループリント] ダイアログ ボックスでのプロンプトの指示に従って全般設定を行います。
- 4 [OK] をクリックします。
- 5 [カテゴリ] エリアで [マシン タイプ] をクリックして、使用可能なマシン タイプのリストを表示します。
- 6 プロビジョニングするマシンのタイプをデザイン キャンバスにドラッグします。
- 7 各タブに情報を入力し、[\[ブループリントのプロパティ\] 設定](#)の説明に沿ってマシン プロビジョニングの詳細を設定します。
- 8 [完了] をクリックします。
- 9 ブループリントを選択して、[公開] をクリックします。

結果

これで、マシン コンポーネントがスタンドアロン ブループリントとして設定および公開されました。 カタログ管理者は、このマシン ブループリントをカタログ サービスに含め、このブループリントを申請する資格をユーザーに付与することができます。 他のアーキテクトは、このマシン ブループリントを再使用して、ソフトウェア コンポーネント、XaaS ブループリント、または追加のマシン ブループリントが取り込まれたより高度なアプリケーションを作成できます。

次のステップ

マシン ブループリントを、ソフトウェア コンポーネント、XaaS ブループリント、または追加のマシン ブループリントと組み合わせて、より高度なアプリケーション ブループリントを作成できます。 [複合ブループリントの組み合わせおよびネストされたブループリントの動作について](#)を参照してください。

マシンのブループリント設定

ブルー プリント全体の設定およびカスタム プロパティを定義することができます。

[ブループリントのプロパティ] 設定

ブループリントを作成するときに [ブループリントのプロパティ] ページを使用すると、ブループリント全体に適用される設定を指定できます。ブループリントを作成後、これらの設定を [ブループリントのプロパティ] ページで編集できます。

[全般] タブ

[全般] タブの設定は、ブループリント全体に適用されます。

表 3-2. [全般] タブの設定

設定	説明
[名前]	ブループリントの名前を入力します。
[ID]	[ID] フィールドには、入力した名前に基づいて、自動的に値が割り当てられます。このフィールドはこの段階では編集できますが、ブループリントの保存後は変更できません。ID は永続的かつテナント内で一意であるため、プログラムでブループリントとやり取りしたり、プロパティ バインドを作成するときに使用できます。
[説明]	ほかのアーキテクトが利用できるように、ブループリントのサマリを記載します。この説明は、申請フォーム上でユーザーにも表示されます。
[展開の上限数]	このブループリントを使用してマシンをプロビジョニングするときに作成できる展開の最大数を指定します。
リース日数：[最小値] および [最大値]	<p>最小値および最大値を入力するとユーザーは、その範囲内でリース期間を選択できます。リースが終了すると、展開は破棄されるか、アーカイブされます。最小値も最大値も指定しなかった場合、リースは無期限に設定されます。</p> <p>マシンのリース情報は、ソース エンドポイントのアプリケーションではなく vRealize Automation ブループリントに入力します。外部アプリケーションにリース情報を指定した場合は、このリース情報は vRealize Automation で認識されないか、使用されません。</p>
[アーカイブ (日)]	リースの有効期限が切れた後すぐに展開を破棄する代わりに、一時的に展開を保持するアーカイブ期間を指定できます。リースの有効期限が切れたときに展開を破棄するには、0 を指定します。アーカイブ期間は、リースの有効期限が切れた日に始まります。アーカイブの有効期限が切れると、展開は破棄されます。デフォルトは 0 です。
[既存の環境へ更新を伝達]	CPU、メモリ、またはストレージの拡大された最小と最大の範囲は、ブループリントからプロビジョニングされたアクティブ展開にプッシュされます。新しい範囲は、古い範囲をすべて含んでいる必要があります。たとえば、元の値の最小値が 32 で最大値が 128 (32, 128) の場合、(16, 128)、(32, 256)、(2, 1000) などへの変更は再構成時またはスケールアウト時に有効になりますが、(33, 512) や (4, 64) への変更は有効になりません。

[NSX 設定] タブ

NSX が設定されている場合は、ブループリントを作成または編集するときに、NSX のトランスポート ゾーン、ネットワークの予約ポリシー、アプリケーションの分離設定を指定できます。これらは、[ブループリント] および [ブループリントのプロパティ] ページの [NSX 設定] タブで設定できます。

NSX の設定の詳細については、[NSX における \[新規ブループリント\] および \[ブループリントのプロパティ\] ページの設定](#)を参照してください。

[プロパティ] タブ

ブループリント レベルで追加したカスタム プロパティは、すべてのコンポーネントを含むブループリント全体に適用されます。優先順位の詳細については、「カスタム プロパティのリファレンス」を参照してください。

表 3-3. [プロパティ] タブの設定

タブ	設定	説明
[プロパティ グループ]		プロパティ グループは、再利用可能なプロパティのグループです。これにより、カスタム プロパティをブループリントへ追加するプロセスを簡素化できます。テナント管理者とファブリック管理者は、一緒に使用することが多いプロパティをグループ化できるため、カスタム プロパティを個別に挿入することなくプロパティ グループをブループリントに追加できます。
	[追加]	1 つまたは複数の既存のプロパティ グループを追加し、ブループリント全体に適用します。 コンテナに関連する次のプロパティ グループが用意されています。 ■ コンテナ ホストのプロパティと証明書認証 ■ コンテナ ホストのプロパティとユーザー/パスワード認証
	[上へ移動]/[下へ移動]	グループ間の優先順位を指定することで、各プロパティ グループに与えられる相対的な優先順位を制御します。リストの先頭のグループが最も優先度が高く、そのグループに属するカスタム プロパティに最高の優先度が割り当てられます。優先順位はドラッグ アンド ドロップ操作で並べ替えることができます。
	[プロパティの表示]	選択したプロパティ グループに属するカスタム プロパティを表示します。
	[マージされたプロパティの表示]	1 つのカスタム プロパティが 2 つ以上のプロパティ グループに属している場合は、最も優先度の高いプロパティ グループに属する値が優先的に使用されます。
[カスタム プロパティ]		プロパティ グループの代わりに個々のカスタム プロパティを追加できます。
	[新規]	個々のカスタム プロパティを追加し、ブループリント全体に適用します。
	[名前]	プロパティ名を入力します。カスタム プロパティとその定義の一覧については、『カスタム プロパティのリファレンス』を参照してください。
	[値]	カスタム プロパティの値を入力します。
	[暗号化済み]	たとえば、値がパスワードの場合に、プロパティ値を暗号化するように選択できます。
	[オーバーライド可能]	次回以降にプロパティを使用する人がプロパティ値をオーバーライドできるように指定できます。 [申請に表示] を選択すると、ユーザーはカタログアイテムを申請するときにプロパティ値を表示して、編集することができます。
	[申請に表示]	プロビジョニング申請フォームにプロパティの名前および値が表示されるように指定できます。ユーザーが値を指定できるようにする場合は、[オーバーライド可能] を選択します。

vSphere マシン コンポーネントの設定

vRealize Automation のブループリント デザイン キャンバスで、vSphere マシン コンポーネントに構成可能な設定とオプションについて理解します。vSphere は、デザイン キャンバスで NSX のネットワークおよびセキュリティ設定を使用できる唯一のマシン コンポーネント タイプです。

[全般] タブ

vSphere マシン コンポーネントの全般設定を行います。

表 3-4. [全般] タブの設定

設定	説明
[ID]	マシン コンポーネントの名前を入力するか、デフォルト値を受け入れます。
[説明]	その他のアーキテクトで利用できるよう、マシン コンポーネントのサマ리를記載します。
[申請時の場所を表示]	<p>vCloud Air などのクラウド環境では、ユーザーがプロビジョニングしたマシンに対して地域を選択できるようになります。</p> <p>vSphere などの仮想環境の場合、場所の機能を構成することにより、ユーザーは申請されたマシンをプロビジョニングする特定のデータセンターの場所を選択できるようになります。このオプションを完全に設定するには、システム管理者がデータセンターの場所に関する情報を場所ファイルに追加し、ファブリック管理者がコンピュータ リソースを編集して、そのリソースを場所に関連付けます。</p>
[予約ポリシー]	<p>予約ポリシーをブループリントに適用すると、そのブループリントからプロビジョニングされるマシンを使用可能な予約のサブセットに制限することができます。ファブリック管理者は、予約ポリシーを作成することで、予約申請の処理方法の管理に役立つオプションを提供できます。たとえば、リソースを収集してサービス レベルごとにグループ化したり、目的にあわせて特定のタイプのリソースを容易に利用できるようになります。ファブリック管理者が予約ポリシーを設定していない場合は、このドロップダウン メニューにオプションは一切表示されません。現在のテナントに適用できる予約ポリシーのみを利用できます。</p>
[マシン プリフィックス]	<p>マシン プリフィックスはファブリック管理者によって作成され、プロビジョニングされるマシンの名前を作成するために使用されます。[グループのデフォルトを使用] を選択すると、ユーザーのビジネス グループのデフォルトとして設定されたマシン プリフィックスに従って、ブループリントからプロビジョニングされるマシンに名前が付けられます。設定されているマシン プリフィックスがない場合は、ビジネス グループの名前に基づいて生成されます。現在のテナントに適用できるマシン プリフィックスのみを利用できます。</p> <p>ファブリック管理者がほかにマシン プリフィックス オプションを提供しており、選択が可能な場合は、申請者が誰であっても、ブループリントからプロビジョニングされるすべてのマシンに 1 つのプリフィックスが適用されるよう設定できます。</p>
インスタンス数 : [最小値] および [最大値]	<p>展開やスケール イン アクション、スケールアウト アクションの対象としてユーザーが申請できる最大数および最小数のインスタンスを構成します。ユーザーに選択肢を与えないようにするには、[最小値] フィールドと [最大値] フィールドに同じ値を入力します。この場合、プロビジョニングの対象となるインスタンス数が指定した数に限定され、そのマシン コンポーネントを拡張するアクションが無効となります。</p> <p>XaaS コンポーネントは拡張可能でなく、拡張処理中には更新されません。ブループリントで XaaS コンポーネントを使用する場合は、拡張処理の後にユーザーが実行できるリソース アクションを作成し、必要に応じて XaaS コンポーネントを拡張または更新することができます。または、マシン コンポーネントごとに許可する具体的なインスタンス数を設定して、拡張を無効にすることもできます。</p>

[ビルド情報] タブ

vSphere マシン コンポーネントのビルド情報を設定します。

表 3-5. [ビルド情報] タブ

設定	説明
[ブループリントのタイプ]	このブループリントからプロビジョニングされるマシンがデスクトップまたはサーバのどちらに分類されるかを選択します。これは、記録保持のため、またライセンス管理に使用します。
[アクション]	<p>[アクション] ドロップダウン メニューに表示されるオプションは、選択したマシンのタイプによって異なります。</p> <p>次のアクションを使用できます。</p> <ul style="list-style-type: none"> ■ [作成] <p>クローン作成オプションを使用せずにマシン コンポーネント仕様を作成します。</p> ■ [クローン作成] <p>テンプレートおよびカスタマイズ オブジェクトから仮想マシンのコピーを作成します。</p> ■ [リンク クローン] <p>リンク クローンと呼ばれる仮想マシンの容量を効率的に利用したコピーをプロビジョニングします。リンク クローンは、仮想マシンのスナップショットに基づいており、差分ディスクのチェーンを使用して親のマシンとの差異を記録します。</p> <p>ブループリントで識別された仮想マシン スナップショットは、リンク クローン仮想マシンのプロビジョニング前にパワーオフされている必要があります。</p> ■ [NetApp FlexClone] <p>ファブリック管理者が NetApp FlexClone ストレージを使用するよう予約を設定している場合は、NetApp FlexClone テクノロジーを使用して容量を効率的に利用したマシンのクローンを作成できます。</p>

表 3-5. [ビルド情報] タブ （続き）

設定	説明
[プロビジョニング ワークフロー]	<p>[プロビジョニング ワークフロー] ドロップダウン メニューに表示されるオプションは、選択したマシンのタイプとアクションによって異なります。</p> <ul style="list-style-type: none"> ■ [BasicVmWorkflow] <p>ゲスト OS を使用せずにマシンをプロビジョニングします。</p> ■ [ExternalProvisioningWorkflow] <p>仮想マシン インスタンスまたはクラウドベースのイメージから起動することによってマシンを作成します。</p> ■ [ImportOvfWorkflow] <p>仮想マシン テンプレートから vSphere 仮想マシンを展開する CloneWorkflow と同様の方法で、OVF テンプレートから vSphere 仮想マシンを展開できます。マシン ブループリントの vSphere コンポーネントへのインポート、またはパラメータ化されたブループリントの Image コンポーネント プロファイルへのインポートが可能になります。</p> ■ [LinuxKickstartWorkflow] <p>マシンへのオペレーティング システムのインストールのために、キックスタートまたは autoYaST 構成ファイルおよび Linux 配布イメージを使用し、ISO イメージから起動することでマシンをプロビジョニングします。</p> ■ [VirtualSccmProvisioningWorkflow] <p>マシンをプロビジョニングし、ISO イメージからの起動のために SCCM タスク シーケンスへ制御を渡して、Windows オペレーティング システムを展開し、vRealize Automation ゲスト エージェントをインストールします。</p> ■ [WIMImageWorkflow] <p>既存の Windows リファレンス マシンの Windows Imaging File Format (WIM) イメージを使用して、WinPE 環境で起動したり、オペレーティング システムをインストールすることでマシンをプロビジョニングします。</p> <p>ブループリントで WIM プロビジョニング ワークフローを使用する場合は、マシンで使用される各ディスクのサイズを示すストレージ値を指定します。マシン コンポーネントの最小ストレージ値としてすべてのディスクの合計値を使用します。また、各ディスクのサイズには、オペレーティング システムに対応する十分な容量を指定します。</p>
[クローン作成元]	<p>クローンの作成元となるマシン テンプレートを選択します。各列のドロップダウン メニューの [フィルタ] オプションを使用することで、使用可能なテンプレートのリストに制限を加えることができます。</p> <p>リンク クローンの場合、クローン作成元として利用可能なスナップショットがあり、テナント管理者またはビジネス グループ マネージャとして管理するマシンのみが表示されます。</p> <p>テンプレートからクローンを作成するには、テンプレートが配置されたマシンのビジネス グループ マネージャまたはテナント管理者である必要があります。</p>

表 3-5. [ビルド情報] タブ （続き）

設定	説明
[スナップショットからクローン作成]	<p>リンク クローンの場合、選択したマシン テンプレートを基盤とし、クローンの作成元となる既存のスナップショットを選択します。マシンは、既存のスナップショットがすでにあり、そのマシンをテナント管理者またはビジネス グループ マネージャとして管理する場合にのみリストに表示されます。</p> <p>[現在のスナップショットの使用] を選択する場合、仮想マシンの最新の状態と同じ特性でクローンが定義されます。実際のスナップショットに対応するクローンを作成する場合は、ドロップダウン メニュー オプションをクリックして、リストから特定のスナップショットを選択します。</p> <p>注： スナップショットという言葉は紛らわしいかもしれません。既存のスナップショットを選択した場合、スナップショットによって生成された新しいディスクが作成されます。[現在のスナップショットの使用] オプションには、親として使用するベース ディスクが存在せず、フル クローン アクションがサイレントに実行されます。回避策として、ベース ディスク上にスナップショットを作成するか、vRealize Orchestrator ワークフローを使用してスナップショットを作成したうえで、そのスナップショットから直接クローンを作成してください。</p> <p>このオプションは、リンク クローン アクションでのみ使用できます。</p>
[カスタム仕様]	<p>利用可能なカスタム仕様を指定します。カスタム仕様 は、固定 IP アドレスを使用してクローンを作成する場合にのみ必要になります。</p> <p>カスタム仕様 を使用せずに Windows マシンをカスタマイズすることはできません。Linux クローン マシンの場合、カスタム仕様、外部スクリプト、またはその両方を使用してカスタマイズができます。</p>

[マシン リソース] タブ

vSphere マシン コンポーネントの CPU、メモリおよびストレージ設定を指定します。

表 3-6. [マシン リソース] タブ

設定	説明
[CPU : 最小値] および [最大値]	プロビジョニングされたマシンで使用可能な CPU 数の最小値と最大値を入力します。
[メモリ (MB) : 最小値] および [最大値]	プロビジョニングされたマシンで使用可能なメモリの最小容量と最大容量を入力します。
[ストレージ (GB) : 最小値] および [最大値]	<p>プロビジョニングされたマシンで使用可能なストレージの最小容量と最大容量を入力します。</p> <p>ブループリントで WIM プロビジョニング ワークフローを使用する場合は、マシンで使用される各ディスクのサイズを示すストレージ値を指定します。マシン コンポーネントの最小ストレージ値としてすべてのディスクの合計値を使用します。また、各ディスクのサイズには、オペレーティング システムに対応する十分な容量を指定します。</p>

[ストレージ] タブ

1 つ以上のストレージ予約ポリシーを含むストレージ ポリ्यूーム設定をマシン コンポーネントに追加することで、ストレージ容量を管理できます。

表 3-7. [ストレージ] タブの設定

設定	説明
[ID]	ストレージ ポリュームの ID または名前を入力します。
[容量 (GB)]	ストレージ ポリュームのストレージ容量を入力します。
[ドライブ文字/マウント パス]	ストレージ ポリュームのドライブ文字またはマウント パスを入力します。 このオプションは、ゲスト エージェントに関連するプロビジョニング中に使用されます。マシンのプロビジョニング後に変更することはできません。ゲスト エージェントを使用していない場合、このオプションは無視されます。
[ラベル]	ストレージ ポリュームのドライブ文字とマウント パスのラベルを入力します。 このオプションは、ゲスト エージェントに関連するプロビジョニング中に使用されます。マシンのプロビジョニング後に変更することはできません。ゲスト エージェントを使用していない場合、このオプションは無視されます。
[ストレージ予約ポリシー]	このストレージ ポリュームで使用する既存のストレージ予約ポリシーを入力します。現在のテナントに適用できるストレージ予約ポリシーのみを利用できます。
[カスタム プロパティ]	このストレージ ポリュームで使用するすべてのカスタム プロパティを入力します。
[最大ポリューム]	マシン コンポーネントからプロビジョニングされるときに利用可能な許容ストレージ ポリュームの最大数を入力します。ストレージ ポリュームの追加を無効にするには 0 を入力します。デフォルト値は 60 です。
[ストレージ予約ポリシーの表示と変更をユーザーに許可]	プロビジョニング時に、関連付けられている予約ポリシーの削除や、別の予約ポリシーの指定をユーザーに許可するには、このチェック ボックスを選択します。

[ネットワーク] タブ

vRealize Automation の外部で設定された NSX のネットワークおよびロード バランサに基づいて、vSphere マシン コンポーネントのネットワーク設定を設定できます。デザイン キャンバスに定義された、1 つ以上の既存またはオンデマンドの NSX ネットワーク コンポーネントの設定を使用できます。

vSphere マシン コンポーネントで [ネットワーク] タブの設定を使用する前に、NSX のネットワークおよびセキュリティ コンポーネントを追加および構成する方法については、[ネットワークおよびセキュリティ コンポーネントの設定](#)を参照してください。

vSphere マシン コンポーネントに適用するブループリントレベルの NSX 設定については、[NSX における \[新規ブループリント\] および \[ブループリントのプロパティ\] ページの設定](#)を参照してください。

表 3-8. [ネットワーク] タブの設定

設定	説明
[ネットワーク]	ドロップダウン メニューからネットワーク コンポーネントを選択します。デザイン キャンバスに設定されたネットワーク コンポーネントのみが一覧表示されます。現在のテナントに適用できるネットワーク プロファイルのみを利用できます。
[割り当てタイプ]	ネットワーク コンポーネントから取得されたデフォルトの割り当てを適用するか、ドロップダウン メニューから割り当てタイプを選択します。[DHCP] および [固定] オプションの値はネットワーク コンポーネントの設定から取得されます。
[アドレス]	ネットワークの IP アドレスを指定します。このオプションは固定アドレス タイプでのみ使用できます。
[ロード バランシング]	ロード バランシングに使用するサービスを入力します。
[カスタム プロパティ]	選択したネットワーク コンポーネントまたはネットワーク プロファイルに設定済みのカスタム プロパティを表示します。
[最大ネットワーク アダプタ]	このマシン コンポーネントに許可するネットワーク アダプタまたは NIC の最大数を指定します。デフォルトは無制限です。マシン コンポーネントの NIC 追加を無効にする場合は、0 に設定します。

[セキュリティ] タブ

vRealize Automation の外部で構成された NSX に基づいて、vSphere マシン コンポーネントのセキュリティを構成できます。必要に応じて、デザイン キャンバスの既存またはオンデマンドの NSX セキュリティ コンポーネントの設定を使用できます。

デザイン キャンバスの既存またはオンデマンドのセキュリティ グループとセキュリティ タグ コンポーネントのセキュリティ設定は、自動的に利用可能になります。

vSphere マシン コンポーネントで [セキュリティ] タブの設定を使用する前に、NSX のネットワークおよびセキュリティ コンポーネントを追加および構成する方法については、[ネットワークおよびセキュリティ コンポーネントの設定](#)を参照してください。

vSphere マシン コンポーネントに適用するブループリントレベルの NSX 情報については、[NSX における \[新規ブループリント\] および \[ブループリントのプロパティ\] ページの設定](#)を参照してください。

表 3-9. [セキュリティ] タブの設定

設定	説明
[名前]	NSX セキュリティ グループまたはタグの名前を表示します。名前はデザイン キャンバスのセキュリティ コンポーネントから取得されます。 リストのセキュリティ グループまたはタグの隣にあるチェック ボックスを選択すると、マシン コンポーネントからプロビジョニングする際に、そのセキュリティ グループまたはタグが使用されます。
[タイプ]	セキュリティ要素が、オンデマンド セキュリティ グループ、既存セキュリティ グループ、セキュリティ タグのうち、どのタイプであるかを示します。

表 3-9. [セキュリティ] タブの設定（続き）

設定	説明
[説明]	セキュリティ グループまたはタグに定義されている説明を表示します。
[エンドポイント]	NSX セキュリティ グループまたはタグによって使用されるエンドポイントを表示します。

[プロパティ] タブ

vSphere マシン コンポーネントのカスタム プロパティおよびプロパティ グループの情報を必要に応じて指定します。

[プロパティ] タブを利用することで、個別またはグループのカスタム プロパティをマシン コンポーネントに追加できます。ブループリントを作成または編集するときに、[プロパティ] タブを使用して、カスタム プロパティとプロパティ グループをブループリント全体に追加することもできます。作成または編集時には [ブループリントのプロパティ] ページを使用します。

[カスタム プロパティ] タブでは、既存のカスタム プロパティのオプションを追加または設定することができます。カスタム プロパティは vRealize Automation で提供され、プロパティ定義を作成することも可能です。

表 3-10. [プロパティ] - [カスタム プロパティ] タブの設定

設定	説明
[名前]	カスタム プロパティの名前を入力するか、ドロップダウン メニューから使用可能なカスタム プロパティを選択します。プロパティは、テナント管理者またはファブリック管理者がプロパティ定義を作成した場合にのみドロップダウン メニューに表示されます。
[値]	カスタム プロパティ名に関連する値を入力するか、編集します。たとえば、値を <code>true</code> と設定し、資格のあるユーザーが SSH を使用して仮想マシンに接続することを許可します。
[暗号化済み]	たとえば、値がパスワードの場合に、プロパティ値を暗号化するように選択できます。
[オーバーライド可能]	次回以降にプロパティを使用する人がプロパティ値をオーバーライドできるように指定できます。[申請に表示] を選択した場合、ビジネス ユーザー（通常はアーキテクト）がカタログ アイテムを申請するときにプロパティ値を確認して編集することが可能になります。
[申請に表示]	プロパティ名とその値をエンド ユーザーに公開する場合は、マシン プロビジョニングの申請時に申請フォームでプロパティを表示するように選択できます。ユーザーが値を指定できるようにするには、[オーバーライド可能] も選択する必要があります。

[プロパティ グループ] タブを使用すると、既存のカスタム プロパティ グループの設定や追加やができます。独自のプロパティ グループの作成や、作成したプロパティ グループを使用することができます。

表 3-11. [プロパティ] - [プロパティ グループ]タブの設定

設定	説明
[名前]	ドロップダウン メニューから使用可能なプロパティ グループを選択します。
[上へ移動]/[下へ移動]	リスト上のプロパティ グループの優先順位レベルを降順で制御します。先に表示されているプロパティ グループは次に表示されているプロパティ グループより優先順位が上になります。
[プロパティの表示]	選択したプロパティ グループに属するカスタム プロパティを表示します。
[マージされたプロパティの表示]	リスト上のプロパティ グループのすべてのカスタム プロパティが、プロパティ グループのリストに表示されている順序で表示されます。同じプロパティが複数のプロパティ グループに表示される場合、リスト上には、リスト内で最初に検出されたプロパティ名が 1 つだけ表示されます。

[プロファイル] タブ

コンポーネント プロファイルを使用すると、ブループリントをパラメータ化できます。たとえば、小規模、中規模、大規模のブループリントを個別に作成するのではなく、小規模、中規模、大規模の機能を持つ 1 つのブループリントを作成し、展開時にこれらのサイズから 1 つを選択することができます。コンポーネント プロファイルは、ブループリントの数を最小に抑制し、カタログを簡素化することを目的に設計されています。

提供された vRealize Automation コンポーネント プロファイルの Size と Image の値セットを作成してある場合は、ブループリントのマシン コンポーネントにそれらの設定を追加して構成することができます。カタログ アイテムを展開するときに、別の値セットを選択することもできます。

コンポーネント プロファイルは、vSphere マシン コンポーネントでのみ使用可能です。

コンポーネント プロファイルをブループリント内の vSphere マシン コンポーネントに追加すると、プロファイルの選択された値セットで定義された設定によって、CPU 数やストレージなどのマシン コンポーネントの設定がオーバーライドされます。

コンポーネント プロファイルの値セットは、クラスタ内のすべての vSphere マシンに適用されます。

Size または Image コンポーネント プロファイルを使用してマシンを再構成することはできませんが、プロファイルに基づいて計算される CPU、メモリ、およびストレージの範囲は、引き続き再構成することができます。たとえば、小 (1 個の CPU、1,024 MB のメモリ、10 GB のストレージ)、中 (3 個の CPU、2,048 MB のメモリ、12 GB のストレージ)、大 (5 個の CPU、3,072 MB のメモリ、15 GB のストレージ) という Size 値セットを使用した場合、マシンの再構成時に使用可能な範囲は、1 個 ~ 5 個の CPU、1,024 MB ~ 3,072 MB のメモリ、および 1 GB ~ 15 GB のストレージです。

詳細については、『カスタム プロパティのリファレンス』を参照してください。

表 3-12. [プロファイル] タブの設定

設定	説明
[追加]	Size または Image コンポーネント プロファイルを追加します。
[値セットの編集]	定義済みの値セットのリストから選択することにより、選択したコンポーネント プロファイルに対して 1 つまたは複数の値セットを割り当てます。1 つの値セットをデフォルトとして選択できます。
[削除]	Size または Image コンポーネント プロファイルを削除します。

vCloud Air マシン コンポーネントの設定

vRealize Automation のブループリント デザイン キャンバスで、vCloud Air マシン コンポーネントに構成可能な設定とオプションについて理解します。

[全般] タブ

vCloud Air マシン コンポーネントの全般設定を行います。

表 3-13. [全般] タブの設定

設定	説明
[ID]	マシン コンポーネントの名前を入力するか、デフォルト値を受け入れます。
[説明]	その他のアーキテクトで利用できるよう、マシン コンポーネントのサマリを記載します。
[申請時の場所を表示]	vCloud Air などのクラウド環境では、ユーザーがプロビジョニングしたマシンに対して地域を選択できるようになります。 vSphere などの仮想環境の場合、場所の機能を構成することにより、ユーザーは申請されたマシンをプロビジョニングする特定のデータセンターの場所を選択できるようになります。このオプションを完全に設定するには、システム管理者がデータセンターの場所に関する情報を場所ファイルに追加し、ファブリック管理者がコンピューティング リソースを編集して、そのリソースを場所に関連付けます。
[予約ポリシー]	予約ポリシーをブループリントに適用すると、そのブループリントからプロビジョニングされるマシンを使用可能な予約のサブセットに制限することができます。ファブリック管理者は、予約ポリシーを作成することで、予約申請の処理方法の管理に役立つオプションを提供できます。たとえば、リソースを収集してサービス レベルごとにグループ化したり、目的にあわせて特定のタイプのリソースを容易に利用できるようになります。ファブリック管理者が予約ポリシーを設定していない場合は、このドロップダウン メニューにオプションは一切表示されません。現在のテナントに適用できる予約ポリシーのみを利用できます。

表 3-13. [全般] タブの設定（続き）

設定	説明
[マシン プリフィックス]	<p>マシン プリフィックスはファブリック管理者によって作成され、プロビジョニングされるマシンの名前を作成するために使用されます。[グループのデフォルトを使用]を選択すると、ユーザーのビジネス グループのデフォルトとして設定されたマシン プリフィックスに従って、ブループリントからプロビジョニングされるマシンに名前が付けられます。設定されているマシン プリフィックスがない場合は、ビジネス グループの名前に基づいて生成されます。現在のテナントに適用できるマシン プリフィックスのみを利用できます。</p> <p>ファブリック管理者がほかにマシン プリフィックス オプションを提供しており、選択が可能な場合は、申請者が誰であっても、ブループリントからプロビジョニングされるすべてのマシンに 1 つのプリフィックスが適用されるよう設定できます。</p>
インスタンス数 : [最小値] および [最大値]	<p>展開やスケール イン アクション、スケールアウト アクションの対象としてユーザーが申請できる最大数および最小数のインスタンスを構成します。ユーザーに選択肢を与えないようにするには、[最小値] フィールドと [最大値] フィールドに同じ値を入力します。この場合、プロビジョニングの対象となるインスタンス数が指定した数に限定され、そのマシン コンポーネントを拡張するアクションが無効となります。</p> <p>XaaS コンポーネントは拡張可能でなく、拡張処理中には更新されません。ブループリントで XaaS コンポーネントを使用する場合は、拡張処理の後にユーザーが実行できるリソース アクションを作成し、必要に応じて XaaS コンポーネントを拡張または更新することができます。または、マシン コンポーネントごとに許可する具体的なインスタンス数を設定して、拡張を無効にすることもできます。</p>

[ビルド情報] タブ

vCloud Air マシン コンポーネントのビルド情報を設定します。

表 3-14. [ビルド情報] タブ

設定	説明
[ブループリントのタイプ]	このブループリントからプロビジョニングされるマシンがデスクトップまたはサーバのどちらに分類されるかを選択します。これは、記録保持のため、またライセンス管理に使用します。
[アクション]	<p>[アクション] ドロップダウン メニューに表示されるオプションは、選択したマシンのタイプによって異なります。</p> <p>vCloud Air マシン コンポーネントで利用可能なプロビジョニング アクションは、クローン作成のみです。</p> <ul style="list-style-type: none"> ■ [クローン作成] <p>テンプレートおよびカスタマイズ オブジェクトから仮想マシンのコピーを作成します。</p>

表 3-14. [ビルド情報] タブ （続き）

設定	説明
[プロビジョニング ワークフロー]	<p>[プロビジョニング ワークフロー] ドロップダウン メニューに表示されるオプションは、選択したマシンのタイプとアクションによって異なります。</p> <p>vCloud Air マシン コンポーネントで利用可能なプロビジョニングアクションは、CloneWorkflow のみです。</p> <p>■ [CloneWorkflow]</p> <p>クローン、リンク クローン、または NetApp Flexclone のいずれかの方法で仮想マシンのコピーを作成します。</p>
[クローン作成元]	<p>クローンの作成元となるマシン テンプレートを選択します。各列のドロップダウン メニューの [フィルタ] オプションを使用することで、使用可能なテンプレートのリストに制限を加えることができます。</p> <p>リンク クローンの場合、クローン作成元として利用可能なスナップショットがあり、テナント管理者またはビジネス グループ マネージャとして管理するマシンのみが表示されます。</p> <p>テンプレートからクローンを作成するには、テンプレートが配置されたマシンのビジネス グループ マネージャまたはテナント管理者である必要があります。</p>

[マシン リソース] タブ

vCloud Air マシン コンポーネントの CPU、メモリおよびストレージ設定を指定します。

表 3-15. [マシン リソース] タブ

設定	説明
[CPU : 最小値] および [最大値]	プロビジョニングされたマシンで使用可能な CPU 数の最小値と最大値を入力します。
[メモリ (MB) : 最小値] および [最大値]	プロビジョニングされたマシンで使用可能なメモリの最小容量と最大容量を入力します。
[ストレージ (GB) : 最小値] および [最大値]	プロビジョニングされたマシンで使用可能なストレージの最小容量と最大容量を入力します。

[ストレージ] タブ

1 つ以上のストレージ予約ポリシーを含むストレージ ポリリューム設定をマシン コンポーネントに追加することで、ストレージ容量を管理できます。

表 3-16. [ストレージ] タブの設定

設定	説明
[ID]	ストレージ ポリリュームの ID または名前を入力します。
[容量 (GB)]	ストレージ ポリリュームのストレージ容量を入力します。
[ドライブ文字/マウント パス]	<p>ストレージ ポリリュームのドライブ文字またはマウント パスを入力します。</p> <p>このオプションは、ゲスト エージェントに関連するプロビジョニング中に使用されます。マシンのプロビジョニング後に変更することはできません。ゲスト エージェントを使用していない場合、このオプションは無視されます。</p>

表 3-16. [ストレージ] タブの設定（続き）

設定	説明
[ラベル]	ストレージ ボリュームのドライブ文字とマウント パスのラベルを入力します。 このオプションは、ゲスト エージェントに関連するプロビジョニング中に使用されます。マシンのプロビジョニング後に変更することはできません。ゲスト エージェントを使用していない場合、このオプションは無視されます。
[ストレージ予約ポリシー]	このストレージ ボリュームで使用する既存のストレージ予約ポリシーを入力します。現在のテナントに適用できるストレージ予約ポリシーのみを利用できます。
[カスタム プロパティ]	このストレージ ボリュームで使用するすべてのカスタム プロパティを入力します。
[最大ボリューム]	マシン コンポーネントからプロビジョニングされるときに利用可能な許容ストレージ ボリュームの最大数を入力します。ストレージ ボリュームの追加を無効にするには 0 を入力します。デフォルト値は 60 です。
[ストレージ予約ポリシーの表示と変更をユーザーに許可]	プロビジョニング時に、関連付けられている予約ポリシーの削除や、別の予約ポリシーの指定をユーザーに許可するには、このチェック ボックスを選択します。

[プロパティ] タブ

vCloud Air マシン コンポーネントのカスタム プロパティおよびプロパティ グループの情報を必要に応じて指定します。

[プロパティ] タブを利用することで、個別またはグループのカスタム プロパティをマシン コンポーネントに追加できます。ブループリントを作成または編集するときに、[プロパティ] タブを使用して、カスタム プロパティとプロパティ グループをブループリント全体に追加することもできます。作成または編集時には [ブループリントのプロパティ] ページを使用します。

[カスタム プロパティ] タブでは、既存のカスタム プロパティのオプションを追加または設定することができます。カスタム プロパティは vRealize Automation で提供され、プロパティ定義を作成することも可能です。

表 3-17. [プロパティ] - [カスタム プロパティ] タブの設定

設定	説明
[名前]	カスタム プロパティの名前を入力するか、ドロップダウン メニューから使用可能なカスタム プロパティを選択します。プロパティは、テナント管理者またはファブリック管理者がプロパティ定義を作成した場合にのみドロップダウン メニューに表示されます。
[値]	カスタム プロパティ名に関連する値を入力するか、編集します。たとえば、値を true と設定し、資格のあるユーザーが SSH を使用して仮想マシンに接続することを許可します。
[暗号化済み]	たとえば、値がパスワードの場合に、プロパティ値を暗号化するように選択できます。

表 3-17. [プロパティ] - [カスタム プロパティ]タブの設定（続き）

設定	説明
[オーバーライド可能]	次回以降にプロパティを使用する人がプロパティ値をオーバーライドできるように指定できます。[申請に表示] を選択した場合、ビジネス ユーザー（通常はアーキテクト）がカタログ アイテムを申請するときにプロパティ値を確認して編集することが可能になります。
[申請に表示]	プロパティ名とその値をエンド ユーザーに公開する場合は、マシン プロビジョニングの申請時に申請フォームでプロパティを表示するように選択できます。ユーザーが値を指定できるようにするには、[オーバーライド可能] も選択する必要があります。

[プロパティ グループ] タブを使用すると、既存のカスタム プロパティ グループの設定や追加やができます。独自のプロパティ グループの作成や、作成したプロパティ グループを使用することができます。

表 3-18. [プロパティ] - [プロパティ グループ]タブの設定

設定	説明
[名前]	ドロップダウン メニューから使用可能なプロパティ グループを選択します。
[上へ移動]/[下へ移動]	リスト上のプロパティ グループの優先順位レベルを降順で制御します。先に表示されているプロパティ グループは次に表示されているプロパティ グループより優先順位が上になります。
[プロパティの表示]	選択したプロパティ グループに属するカスタム プロパティを表示します。
[マージされたプロパティの表示]	リスト上のプロパティ グループのすべてのカスタム プロパティが、プロパティ グループのリストに表示されている順序で表示されます。同じプロパティが複数のプロパティ グループに表示される場合、リスト上には、リスト内で最初に検出されたプロパティ名が 1 つだけ表示されます。

Amazon マシン コンポーネント設定

vRealize Automation ブループリント デザイン キャンバスで Amazon マシン コンポーネントに構成可能な設定とオプションについて理解します。

[全般] タブ

Amazon マシン コンポーネントの全般設定を構成します。

表 3-19. [全般] タブの設定

設定	説明
[ID]	マシン コンポーネントの名前を入力するか、デフォルト値を受け入れます。
[説明]	その他のアーキテクトで利用できるよう、マシン コンポーネントのサマ리를記載します。

表 3-19. [全般] タブの設定（続き）

設定	説明
[申請時の場所を表示]	<p>vCloud Air などのクラウド環境では、ユーザーがプロビジョニングしたマシンに対して地域を選択できるようになります。</p> <p>vSphere などの仮想環境の場合、場所の機能を構成することにより、ユーザーは申請されたマシンをプロビジョニングする特定のデータセンターの場所を選択できるようになります。このオプションを完全に設定するには、システム管理者がデータセンターの場所に関する情報を場所ファイルに追加し、ファブリック管理者がコンピュータ リソースを編集して、そのリソースを場所に関連付けます。</p>
[予約ポリシー]	<p>予約ポリシーをブループリントに適用すると、そのブループリントからプロビジョニングされるマシンを使用可能な予約のサブセットに制限することができます。ファブリック管理者は、予約ポリシーを作成することで、予約申請の処理方法の管理に役立つオプションを提供できます。たとえば、リソースを収集してサービス レベルごとにグループ化したり、目的にあわせて特定のタイプのリソースを容易に利用できるようになります。ファブリック管理者が予約ポリシーを設定していない場合は、このドロップダウン メニューにオプションは一切表示されません。現在のテナントに適用できる予約ポリシーのみを利用できます。</p>
[マシン プリフィックス]	<p>マシン プリフィックスはファブリック管理者によって作成され、プロビジョニングされるマシンの名前を作成するために使用されます。[グループのデフォルトを使用]を選択すると、ユーザーのビジネス グループのデフォルトとして設定されたマシン プリフィックスに従って、ブループリントからプロビジョニングされるマシンに名前が付けられます。設定されているマシン プリフィックスがない場合は、ビジネス グループの名前に基づいて生成されます。現在のテナントに適用できるマシン プリフィックスのみを利用できます。</p> <p>ファブリック管理者がほかにマシン プリフィックス オプションを提供しており、選択が可能な場合は、申請者が誰であっても、ブループリントからプロビジョニングされるすべてのマシンに 1 つのプリフィックスが適用されるよう設定できます。</p>
インスタンス数 : [最小値] および [最大値]	<p>展開やスケール イン アクション、スケール アウト アクションの対象としてユーザーが申請できる最大数および最小数のインスタンスを構成します。ユーザーに選択肢を与えないようにするには、[最小値] フィールドと [最大値] フィールドに同じ値を入力します。この場合、プロビジョニングの対象となるインスタンス数が指定した数に限定され、そのマシン コンポーネントを拡張するアクションが無効となります。</p> <p>XaaS コンポーネントは拡張可能でなく、拡張処理中には更新されません。ブループリントで XaaS コンポーネントを使用する場合は、拡張処理の後にユーザーが実行できるリソース アクションを作成し、必要に応じて XaaS コンポーネントを拡張または更新することができます。または、マシン コンポーネントごとに許可する具体的なインスタンス数を設定して、拡張を無効にすることもできます。</p>

[ビルド情報] タブ

Amazon マシン コンポーネントのビルド情報設定を構成します。

表 3-20. [ビルド情報] タブ

設定	説明
[ブループリントのタイプ]	このブループリントからプロビジョニングされるマシンがデスクトップまたはサーバのどちらに分類されるかを選択します。これは、記録保持のため、またライセンス管理に使用します。
[プロビジョニング ワークフロー]	<p>Amazon マシン コンポーネントで利用可能なプロビジョニング ワークフローは CloudProvisioningWorkflow のみです。</p> <ul style="list-style-type: none"> ■ [CloudProvisioningWorkflow] <p>仮想マシン インスタンスまたはクラウドベースのイメージから起動することによってマシンを作成します。</p>
[Amazon マシン イメージ]	利用可能な Amazon マシン イメージを選択します。Amazon マシン イメージは、オペレーティング システムなどのソフトウェア構成を含むテンプレートです。マシン イメージは Amazon Web Services アカウントにより管理されます。[AMI ID] 列のドロップダウン メニューにある [フィルタ] オプションを使用して、表示される Amazon マシン イメージ名のリストに制限を加えることができます。
[キー ペア]	<p>キー ペアは、Amazon Web Services のプロビジョニングに必要です。</p> <p>キー ペアは、クラウド インスタンスのプロビジョニングと接続に使用されます。Windows のパスワードの復号化や Linux マシンへのログインにも使用されます。</p> <p>次のキー ペア オプションを使用できます。</p> <ul style="list-style-type: none"> ■ 未指定 <p>予約レベルではなく、ブループリント レベルでキー ペアの動作を制御します。</p> ■ ビジネス グループ毎に自動生成 <p>同じビジネス グループ内にプロビジョニングされている各マシンが同じキー ペアを持つことのように指定します。同じコンピュータリソースを利用し、同じビジネス グループに存在するマシンであれば、他の予約にプロビジョニングされていても適用されます。キー ペアはビジネス グループに関連付けられるため、ビジネス グループが削除されるときにはキー ペアも削除されます。</p> ■ マシン毎に自動生成 <p>各マシンが一意のキー ペアを持つように指定します。複数のマシンでキー ペアを共有することはないため、[マシン毎に自動生成] オプションが最も安全な方法となります。</p>
[マシンの Amazon ネットワーク オプションを有効にします]	申請の送信時に、マシンのプロビジョニング先を Virtual Private Cloud またはそれ以外の場所のどちらにするかを選択できます。
[インスタンス タイプ]	<p>Amazon インスタンス タイプを 1 つ以上選択します。Amazon インスタンスは、Amazon Web Services でアプリケーションを実行可能な仮想サーバです。インスタンスは、適切なインスタンス タイプを選択することで、Amazon マシン イメージから作成されます。</p> <p>vRealize Automation は、プロビジョニングに対応しているマシン イメージのインスタンス タイプを管理します。</p> <p>vRealize Automation で Amazon インスタンス タイプを使用する際の詳細については、Amazon インスタンス タイプについてと Amazon インスタンス タイプの追加を参照してください。</p>

[マシン リソース] タブ

Amazon マシン コンポーネントの CPU、メモリ、ストレージ、および EBS ボリューム設定を指定します。

root ボリュームを除く、展開のすべての Amazon マシンのストレージ ボリュームも再構成できます。

表 3-21. [マシン リソース] タブ

設定	説明
[CPU : 最小値] および [最大値]	プロビジョニングされたマシンで使用可能な CPU 数の最小値と最大値を入力します。
[メモリ (MB) : 最小値] および [最大値]	プロビジョニングされたマシンで使用可能なメモリの最小容量と最大容量を入力します。
[ストレージ (GB) : 最小値] および [最大値]	プロビジョニングされたマシンで使用可能なストレージの最小容量と最大容量を入力します。
[EBS ストレージ (GB) : 最小値] および [最大値]	プロビジョニングされたマシンで使用可能な Amazon Elastic Block Store (EBS) ストレージの最小容量と最大容量を入力します。 Amazon マシン コンポーネントを含む展開環境を破棄すると、そのマシンのライフサイクルで追加されたすべての EBS ボリュームは、破棄されずに切り離されます。vRealize Automation には、EBS ボリュームを破棄するオプションは用意されていません。
ボリュームの削除	Amazon 展開を破棄するときに、EC2 ボリュームを個別に削除できるようにするか、一括で削除できるようにするかを指定します。 [はい] と [いいえ] のどちらかを指定しても、展開内のすべてのボリュームの一括破棄アクションを実行できます。デフォルト値は null または空白です。 <ul style="list-style-type: none"> ■ はい - Amazon 展開を破棄し、ボリュームを削除します。 ■ いいえ - Amazon 展開を破棄し、ボリュームを保持します。 ■ null または空白 - Amazon 展開を破棄するときに、[はい] または [いいえ] の値を指定するようユーザーに要求します。

[プロパティ] タブ

Amazon マシン コンポーネントのカスタム プロパティとプロパティ グループの情報を必要に応じて指定します。

[プロパティ] タブを利用することで、個別またはグループのカスタム プロパティをマシン コンポーネントに追加できます。ブループリントを作成または編集するときに、[プロパティ] タブを使用して、カスタム プロパティとプロパティ グループをブループリント全体に追加することもできます。作成または編集時には [ブループリントのプロパティ] ページを使用します。

[カスタム プロパティ] タブでは、既存のカスタム プロパティのオプションを追加または設定することができます。カスタム プロパティは vRealize Automation で提供され、プロパティ定義を作成することも可能です。

表 3-22. [プロパティ] - [カスタム プロパティ]タブの設定

設定	説明
[名前]	カスタム プロパティの名前を入力するか、ドロップダウン メニューから使用可能なカスタム プロパティを選択します。プロパティは、テナント管理者またはファブリック管理者がプロパティ定義を作成した場合にのみドロップダウン メニューに表示されます。
[値]	カスタム プロパティ名に関連する値を入力するか、編集します。たとえば、値を <code>true</code> と設定し、資格のあるユーザーが SSH を使用して仮想マシンに接続することを許可します。
[暗号化済み]	たとえば、値がパスワードの場合に、プロパティ値を暗号化するように選択できます。
[オーバーライド可能]	次回以降にプロパティを使用する人がプロパティ値をオーバーライドできるように指定できます。[申請に表示] を選択した場合、ビジネス ユーザー（通常はアーキテクト）がカタログ アイテムを申請するときにプロパティ値を確認して編集することが可能になります。
[申請に表示]	プロパティ名とその値をエンド ユーザーに公開する場合は、マシン プロビジョニングの申請時に申請フォームでプロパティを表示するように選択できます。ユーザーが値を指定できるようにするには、[オーバーライド可能] も選択する必要があります。

[プロパティ グループ] タブを使用すると、既存のカスタム プロパティ グループの設定や追加やができます。独自のプロパティ グループの作成や、作成したプロパティ グループを使用することができます。

表 3-23. [プロパティ] - [プロパティ グループ]タブの設定

設定	説明
[名前]	ドロップダウン メニューから使用可能なプロパティ グループを選択します。
[上へ移動]/[下へ移動]	リスト上のプロパティ グループの優先順位レベルを降順で制御します。先に表示されているプロパティ グループは次に表示されているプロパティ グループより優先順位が上になります。
[プロパティの表示]	選択したプロパティ グループに属するカスタム プロパティを表示します。
[マージされたプロパティの表示]	リスト上のプロパティ グループのすべてのカスタム プロパティが、プロパティ グループのリストに表示されている順序で表示されます。同じプロパティが複数のプロパティ グループに表示される場合、リスト上には、リスト内で最初に検出されたプロパティ名が 1 つだけ表示されます。

OpenStack マシン コンポーネント設定

vRealize Automation のブループリント デザイン キャンバスで、OpenStack マシン コンポーネント用に構成可能な設定とオプションについて理解します。

[全般] タブ

OpenStack マシン コンポーネントの全般設定を構成します。

表 3-24. [全般] タブの設定

設定	説明
[ID]	マシン コンポーネントの名前を入力するか、デフォルト値を受け入れます。
[説明]	その他のアーキテクトで利用できるよう、マシン コンポーネントのサマリを記載します。
[申請時の場所を表示]	<p>vCloud Air などのクラウド環境では、ユーザーがプロビジョニングしたマシンに対して地域を選択できるようになります。</p> <p>vSphere などの仮想環境の場合、場所の機能を構成することにより、ユーザーは申請されたマシンをプロビジョニングする特定のデータセンターの場所を選択できるようになります。このオプションを完全に設定するには、システム管理者がデータセンターの場所に関する情報を場所ファイルに追加し、ファブリック管理者がコンピュータ リソースを編集して、そのリソースを場所に関連付けます。</p>
[予約ポリシー]	<p>予約ポリシーをブループリントに適用すると、そのブループリントからプロビジョニングされるマシンを使用可能な予約のサブセットに制限することができます。ファブリック管理者は、予約ポリシーを作成することで、予約申請の処理方法の管理に役立つオプションを提供できます。たとえば、リソースを収集してサービス レベルごとにグループ化したり、目的にあわせて特定のタイプのリソースを容易に利用できるようになります。ファブリック管理者が予約ポリシーを設定していない場合は、このドロップダウン メニューにオプションは一切表示されません。現在のテナントに適用できる予約ポリシーのみを利用できます。</p>
[マシン プリフィックス]	<p>マシン プリフィックスはファブリック管理者によって作成され、プロビジョニングされるマシンの名前を作成するために使用されます。[グループのデフォルトを使用]を選択すると、ユーザーのビジネス グループのデフォルトとして設定されたマシン プリフィックスに従って、ブループリントからプロビジョニングされるマシンに名前が付けられます。設定されているマシン プリフィックスがない場合は、ビジネス グループの名前に基づいて生成されます。現在のテナントに適用できるマシン プリフィックスのみを利用できます。</p> <p>ファブリック管理者がほかにマシン プリフィックス オプションを提供しており、選択が可能な場合は、申請者が誰であっても、ブループリントからプロビジョニングされるすべてのマシンに 1 つのプリフィックスが適用されるよう設定できます。</p>
インスタンス数 : [最小値] および [最大値]	<p>展開やスケール イン アクション、スケールアウト アクションの対象としてユーザーが申請できる最大数および最小数のインスタンスを構成します。ユーザーに選択肢を与えないようにするには、[最小値] フィールドと [最大値] フィールドに同じ値を入力します。この場合、プロビジョニングの対象となるインスタンス数が指定した数に限定され、そのマシン コンポーネントを拡張するアクションが無効となります。</p> <p>XaaS コンポーネントは拡張可能でなく、拡張処理中には更新されません。ブループリントで XaaS コンポーネントを使用する場合は、拡張処理の後にユーザーが実行できるリソース アクションを作成し、必要に応じて XaaS コンポーネントを拡張または更新することができます。または、マシン コンポーネントごとに許可する具体的なインスタンス数を設定して、拡張を無効にすることもできます。</p>

[ビルド情報] タブ

OpenStack マシン コンポーネントのビルド情報設定を構成します。

表 3-25. [ビルド情報] タブ

設定	説明
[ブループリントのタイプ]	このブループリントからプロビジョニングされるマシンがデスクトップまたはサーバのどちらに分類されるかを選択します。これは、記録保持のため、またライセンス管理に使用します。
[プロビジョニング ワークフロー]	<p>次のプロビジョニング ワークフローは OpenStack マシン コンポーネントに使用できます。</p> <ul style="list-style-type: none"> ■ [CloudLinuxKickstartWorkflow] <p>マシンへのオペレーティング システムのインストールのために、キックスタートまたは autoYaST 構成ファイルおよび Linux 配布イメージを使用し、ISO イメージから起動することでマシンをプロビジョニングします。</p> ■ [CloudProvisioningWorkflow] <p>仮想マシン インスタンスまたはクラウドベースのイメージから起動することによってマシンを作成します。</p> ■ [CloudWIMImageWorkflow] <p>既存の Windows リファレンス マシンの Windows Imaging File Format (WIM) イメージを使用して、WinPE 環境で起動したり、オペレーティング システムをインストールすることでマシンをプロビジョニングします。</p> <p>ブループリントで WIM プロビジョニング ワークフローを使用する場合は、マシンで使用される各ディスクのサイズを示すストレージ値を指定します。マシン コンポーネントの最小ストレージ値としてすべてのディスクの合計値を使用します。また、各ディスクのサイズには、オペレーティング システムに対応する十分な容量を指定します。</p>
[OpenStack イメージ]	使用可能な OpenStack イメージを選択します。OpenStack イメージは、オペレーティング システムなどのソフトウェア構成を含むテンプレートです。イメージは OpenStack アカウントによって管理されます。[名前] 列のドロップダウン メニューにある [フィルタ] オプションを使用して、表示される OpenStack イメージ名のリストに制限を加えることができます。

表 3-25. [ビルド情報] タブ （続き）

設定	説明
[キー ペア]	<p>OpenStack のプロビジョニングの場合、キー ペアはオプションです。キー ペアは、クラウド インスタンスのプロビジョニングと接続に使用されます。Windows のパスワードの復号化や Linux マシンへのログインにも使用されます。</p> <p>次のキー ペア オプションを使用できます。</p> <ul style="list-style-type: none"> ■ 未指定 <p>予約レベルではなく、ブループリント レベルでキー ペアの動作を制御します。</p> ■ ビジネス グループ毎に自動生成 <p>同じビジネス グループ内にプロビジョニングされている各マシンが同じキー ペアを持つことのように指定します。同じコンピュータリソースを利用し、同じビジネス グループに存在するマシンであれば、他の予約にプロビジョニングされていても適用されます。キー ペアはビジネス グループに関連付けられるため、ビジネス グループが削除されるときにはキー ペアも削除されます。</p> ■ マシン毎に自動生成 <p>各マシンが一意的キー ペアを持つように指定します。複数のマシンでキー ペアを共有することはないため、[マシン毎に自動生成] オプションが最も安全な方法となります。</p>
[フレーバー]	<p>OpenStack フレーバーを 1 つ以上選択します。OpenStack フレーバーは、OpenStack でプロビジョニングされたインスタンスのマシンリソース仕様を定義する仮想ハードウェア テンプレートです。フレーバーは、OpenStack プロバイダ内で管理され、データ収集中にインポートされます。</p>

[マシン リソース] タブ

OpenStack マシン コンポーネントの CPU、メモリ、およびストレージ設定を指定します。

表 3-26. [マシン リソース] タブ

設定	説明
[CPU : 最小値] および [最大値]	<p>プロビジョニングされたマシンで使用可能な CPU 数の最小値と最大値を入力します。</p>
[メモリ (MB) : 最小値] および [最大値]	<p>プロビジョニングされたマシンで使用可能なメモリの最小容量と最大容量を入力します。</p>
[ストレージ (GB) : 最小値] および [最大値]	<p>プロビジョニングされたマシンで使用可能なストレージの最小容量と最大容量を入力します。</p> <p>ブループリントで WIM プロビジョニング ワークフローを使用する場合は、マシンで使用される各ディスクのサイズを示すストレージ値を指定します。マシン コンポーネントの最小ストレージ値としてすべてのディスクの合計値を使用します。また、各ディスクのサイズには、オペレーティング システムに対応する十分な容量を指定します。</p>

[プロパティ] タブ

OpenStack マシン コンポーネントのカスタム プロパティおよびプロパティ グループの情報を必要に応じて指定します。

[プロパティ] タブを利用することで、個別またはグループのカスタム プロパティをマシン コンポーネントに追加できます。ブループリントを作成または編集するときに、[プロパティ] タブを使用して、カスタム プロパティとプロパティ グループをブループリント全体に追加することもできます。作成または編集時には [ブループリントのプロパティ] ページを使用します。

[カスタム プロパティ] タブでは、既存のカスタム プロパティのオプションを追加または設定することができます。カスタム プロパティは vRealize Automation で提供され、プロパティ定義を作成することも可能です。

表 3-27. [プロパティ] - [カスタム プロパティ] タブの設定

設定	説明
[名前]	カスタム プロパティの名前を入力するか、ドロップダウン メニューから使用可能なカスタム プロパティを選択します。プロパティは、テナント管理者またはファブリック管理者がプロパティ定義を作成した場合にのみドロップダウン メニューに表示されます。
[値]	カスタム プロパティ名に関連する値を入力するか、編集します。たとえば、値を <code>true</code> と設定し、資格のあるユーザーが SSH を使用して仮想マシンに接続することを許可します。
[暗号化済み]	たとえば、値がパスワードの場合に、プロパティ値を暗号化するように選択できます。
[オーバーライド可能]	次回以降にプロパティを使用する人がプロパティ値をオーバーライドできるように指定できます。[申請に表示] を選択した場合、ビジネス ユーザー（通常はアーキテクト）がカタログ アイテムを申請するときにプロパティ値を確認して編集することが可能になります。
[申請に表示]	プロパティ名とその値をエンド ユーザーに公開する場合は、マシン プロビジョニングの申請時に申請フォームでプロパティを表示するように選択できます。ユーザーが値を指定できるようにするには、[オーバーライド可能] も選択する必要があります。

[プロパティ グループ] タブを使用すると、既存のカスタム プロパティ グループの設定や追加やができます。独自のプロパティ グループの作成や、作成したプロパティ グループを使用することができます。

表 3-28. [プロパティ] - [プロパティ グループ] タブの設定

設定	説明
[名前]	ドロップダウン メニューから使用可能なプロパティ グループを選択します。
[上へ移動]/[下へ移動]	リスト上のプロパティ グループの優先順位レベルを降順で制御します。先に表示されているプロパティ グループは次に表示されているプロパティ グループより優先順位が上になります。

表 3-28. [プロパティ] - [プロパティ グループ]タブの設定 (続き)

設定	説明
[プロパティの表示]	選択したプロパティ グループに属するカスタム プロパティを表示します。
[マージされたプロパティの表示]	リスト上のプロパティ グループのすべてのカスタム プロパティが、プロパティ グループのリストに表示されている順序で表示されます。同じプロパティが複数のプロパティ グループに表示される場合、リスト上には、リスト内で最初に検出されたプロパティ名が 1 つだけ表示されます。

ネットワーク カスタム プロパティの使用

ブループリントまたはマシン コンポーネント レベルでネットワーク カスタム プロパティを使用して、vSphere および NSX を含まないブループリント以外のマシン コンポーネントのネットワークおよびセキュリティの情報を指定できます。

[ネットワークとセキュリティ] コンポーネントは、vSphere マシン コンポーネントで使用する場合にのみ利用可能です。vSphere 以外のマシン コンポーネントには、[ネットワーク] タブまたは [セキュリティ] タブが含まれていません。

vSphere マシン コンポーネントと NSX が関連付けられている場合、ユーザー インターフェイスでネットワーク、セキュリティ、およびロード バランシングの設定を使用します。[ネットワーク] または [セキュリティ] タブのないマシン コンポーネントの場合、デザイン キャンパスの [プロパティ] タブに、VirtualMachine.Network0.Name などのネットワークおよびセキュリティのカスタム プロパティを追加することができます。NSX ネットワーク、セキュリティ、ロード バランサのプロパティを適用できるのは vSphere マシンだけです。

デザイン キャンパスにマシン コンポーネントを構成する際に、[プロパティ] タブを使用して、個別に、または既存のプロパティ グループの一部として、カスタム プロパティを定義できます。あるマシン コンポーネントに定義したカスタム プロパティは、ブループリントからプロビジョニングされるそのタイプのマシンに属します。

使用可能なカスタム プロパティの詳細については、「カスタム プロパティのリファレンス」を参照してください。

クローン ブループリントおよびリンク クローン ブループリントのトラブルシューティング

リンク クローン ブループリントまたはクローン ブループリントを作成する際にマシンまたはテンプレートが見つかりません。共有クローン ブループリントを使用してマシンを申請すると、マシンのプロビジョニングに失敗します。

問題

クローン ブループリントまたはリンク クローン ブループリントを使用する際に、次のいずれかの問題が発生することがあります。

- リンク クローン ブループリントを作成する際に、リストにクローン作成の対象となるマシンが 1 台も表示されないか、クローン作成する必要があるマシンが表示されません。
- クローン ブループリントを作成する際に、クローン作成の対象となるテンプレートのリストにテンプレートが 1 つも表示されないか、必要なテンプレートが表示されません。
- 共有クローン ブループリントを使用してマシンを申請すると、プロビジョニングが失敗します。

- データ収集のタイミングによっては、リンク クローン ブループリントの作成または編集時に、既に削除されたテンプレートが依然として表示される場合があります。

SDRS のプロビジョニング中は、リンク クローンはサポートされないことに注意してください。リンク クローンは親と同じデータストアに作成されますが、クラスタのデータストア間で再分散されません。これにより、最終的に親データストアがいっぱいになることがあります。

原因

クローン ブループリントおよびリンク クローン ブループリントでよくある問題には複数の原因が考えられます。

ブループリントの作成時に使用できる [現在のスナップショットの使用] オプションと、[クローン作成元] および [スナップショットからクローン作成] に関する関連情報については、[vSphere マシン コンポーネントの設定](#)を参照してください。

表 3-29. クローン ブループリントおよびリンク クローン ブループリントでよくある問題の原因

問題	原因	ソリューション
マシンがない	ユーザーがリンク クローン ブループリントを作成できるのは、自身がテナント管理者またはビジネス グループ マネージャとして管理しているマシンを使用した場合のみです。	テナントまたはビジネス グループに属するユーザーが、vSphere マシンを申請する必要があります。該当するロールを割り当てられているユーザーは、自分でマシンを申請できます。 このダイアログには非管理対象マシンも表示されます。 管理対象のマシンがインポートされている場合があります。このダイアログに表示されるマシンは、vRealize Automation からプロビジョニングされている必要はありません。
テンプレートがない	特定のエンドポイントでデータ収集に失敗したか、コンポーネントのプラットフォームでエンドポイントを利用できません。	<ul style="list-style-type: none"> ■ エンドポイントがクラスタ化されており、複数のコンピュート リソースが含まれている場合は、IaaS 管理者が当該テンプレートを含むクラスタをファブリック グループに追加していることを確認します。 ■ 新規テンプレートの場合は、IT 部門が、ファブリック グループに含まれている同一クラスタ上にテンプレートを配置していることを確認します。
共有ブループリントを使用したプロビジョニングが失敗する	ブループリントの場合、共有クローン ブループリントからのマシンのプロビジョニングに使用される予約に、選択したテンプレートが存在するかどうかの検証を行うことができません。	資格を使用して、テンプレートが存在するコンピュート リソースを予約しているユーザーのみにブループリントの使用を制限することを確認します。

表 3-29. クローン ブループリントおよびリンク クローン ブループリントでよくある問題の原因（続き）

問題	原因	ソリューション
ゲスト エージェントによるプロビジョニングが失敗する	仮想マシンが、ゲスト OS のカスタマイズの完了直後、ゲスト エージェントの作業アイテムが完了する前に再起動されている可能性があるため、プロビジョニングに失敗します。 カスタム プロパティ <code>VirtualMachine.Admin.CustomizeGuestOSDelay</code> を使用して遅延時間を増やすことができます。	カスタム プロパティ <code>VirtualMachine.Admin.CustomizeGuestOSDelay</code> が追加されていることを確認します。値は HH:MM:SS 形式にする必要があります。値が設定されていない場合、デフォルト値は 1 分 (00:01:00) になります。
クローン作成のベースとして使用されたテンプレートが見つからないため、クローンまたはリンク クローン ブループリントのプロビジョニングが失敗する	既に存在しないテンプレートからクローン作成されたブループリントを使用して、マシンをプロビジョニングすることはできません。 vRealize Automation ではデータ収集を定期的に行い、デフォルトでは 24 時間ごとに実行します。テンプレートが削除されると、次のデータ収集が行われるまで、この変更は反映されないため、存在しなくなったテンプレートに基づいてブループリントが作成される可能性があります。	既存のテンプレートを使用してブループリントを再定義してから、プロビジョニングを申請してください。 予防措置として、クローンまたはリンク クローン ブループリントを定義する前に、データ収集を適宜実行できます。

NSX 設定によるブループリントの設計

vRealize Automation と NSX for vSphere または NSX-T を統合するように構成した場合、デザイン キャンパスのネットワーク、セキュリティ、およびロード バランサのコンポーネントを使用して、マシン プロビジョニングのブループリントを構成できます。

以下の NSX のネットワークおよびセキュリティ設定をブループリント全体に追加することもできます。

- トランSPORT ゾーン - プロビジョニングされたマシンの展開で使用するネットワークを含みます。
- ネットワーク予約ポリシー - プロビジョニングされたマシン展開のネットワーク通信を管理します。
- アプリケーションの隔離 - プロビジョニングされたマシン展開で使用するマシン間の内部トラフィックのみが許可されます。

vRealize Automation と NSX の統合については、[vRA and NSX - Intro to Network and Security Automation](#) のブログ記事と、[Networking and Security with vRealize Automation and NSX](#) コースの内容を参照してください。

NSX 設定は、vSphere マシン コンポーネント タイプにのみ適用できます。

NSX における [新規ブループリント] および [ブループリントのプロパティ] ページの設定

ブループリントを作成するときに [新規ブループリント] ページを使用すると、NSX の一部の設定を含む、ブループリント全体に適用される設定を指定できます。ブループリントを作成後、これらの設定を [ブループリントのプロパティ] ページで編集できます。

[全般] タブ

[全般] タブの設定は、ブループリント全体に適用されます。

表 3-30. [全般] タブの設定

設定	説明
[名前]	ブループリントの名前を入力します。
[ID]	[ID] フィールドには、入力した名前に基づいて、自動的に値が割り当てられます。このフィールドはこの段階では編集できますが、ブループリントの保存後は変更できません。ID は永続的かつテナント内で一意であるため、プログラムでブループリントとやり取りしたり、プロパティ バインドを作成するときに使用できます。
[説明]	ほかのアーキテクトが利用できるように、ブループリントのサマリを記載します。この説明は、申請フォーム上でユーザーにも表示されます。
[展開の上限数]	このブループリントを使用してマシンをプロビジョニングするときに作成できる展開の最大数を指定します。
リース日数：[最小値] および [最大値]	<p>最小値および最大値を入力するとユーザーは、その範囲内でリース期間を選択できます。リースが終了すると、展開は破棄されるか、アーカイブされます。最小値も最大値も指定しなかった場合、リースは無期限に設定されます。</p> <p>マシンのリース情報は、ソース エンドポイントのアプリケーションではなく vRealize Automation ブループリントに入力します。外部アプリケーションにリース情報を指定した場合は、このリース情報は vRealize Automation で認識されないか、使用されません。</p>
[アーカイブ (日)]	リースの有効期限が切れた後すぐに展開を破棄する代わりに、一時的に展開を保持するアーカイブ期間を指定できます。リースの有効期限が切れたときに展開を破棄するには、0 を指定します。アーカイブ期間は、リースの有効期限が切れた日に始まり、アーカイブの有効期限が切れると、展開は破棄されます。デフォルトは 0 です。
[既存の環境へ更新を伝達]	CPU、メモリ、またはストレージの拡大された最小と最大の範囲は、ブループリントからプロビジョニングされたアクティブ展開にプッシュされます。新しい範囲は、古い範囲をすべて含んでいる必要があります。たとえば、元の値の最小値が 32 で最大値が 128 (32、128) の場合、(16、128)、(32、256)、(2、1000) などへの変更は再構成時またはスケールアウト時に有効になりますが、(33、512) や (4、64) への変更は有効になりません。

[NSX 設定] タブ

NSX が設定されている場合は、ブループリントを作成または編集するときに、NSX のトランスポート ゾーン、ネットワークの予約ポリシー、アプリケーションの分離設定を指定できます。これらは、[ブループリント] および [ブループリントのプロパティ] ページの [NSX 設定] タブで設定できます。

NSX の設定に関する詳細については、『NSX 管理ガイド』を参照してください。

表 3-31. [NSX 設定] タブの設定

設定	説明
[トランスポート ゾーン (トランスポート ゾーン)]	<p>プロビジョニングしたマシン環境で使用可能な 1 つ以上のネットワークを含む、既存の NSX トランスポート ゾーン (トランスポート ゾーン) を選択します。</p> <p>トランスポート ゾーンは、ネットワークの転送範囲にどのクラスタを含めるかを定義します。マシンをプロビジョニングする際に、トランスポート ゾーンが予約とブループリントの両方に指定されている場合は、トランスポート ゾーンの各値が一致している必要があります。現在のテナントに適用できるトランスポート ゾーンのみを利用できます。</p> <p>ブループリントに NSX for vSphere または NSX-T オンデマンド ネットワークや、ブループリントを展開するときに作成されるセキュリティ オブジェクトが含まれる場合、そのブループリントにはトランスポート ゾーンが必要です。</p> <p>詳細については、ブループリントへの NSX トランスポート ゾーンの適用を参照してください。</p>
[ネットワーク予約ポリシー]	<p>NSX for vSphere では、ネットワーク予約ポリシーを選択すると、ブループリント展開でエッジまたは DLR の配置場所を決定しやすくなります。</p> <p>vRealize Automation が NAT またはルーティング ネットワーク用のマシンをプロビジョニングする際、ネットワーク ルータとしてルーティング ゲートウェイをプロビジョニングします。Edge またはルーティング ゲートウェイは管理マシンであり、他の仮想マシンと同様にコンピュート リソースを使用します。そして環境内のすべてのマシンのネットワーク通信を管理します。NAT で使用される外部ネットワークと、ロード バランサの仮想 IP アドレスは、Edge またはルーティング ゲートウェイのプロビジョニングに使用する予約によって決まります。ベスト プラクティスとして、NSX Edge などの管理マシンには別の管理クラスタを使用します。</p> <p>NSX-T では、ネットワーク予約ポリシーを選択すると、ブループリント展開で tier-0 論理ルーターの配置場所を決定しやすくなります。</p> <p>詳細については、ブループリントへの NSX ネットワーク予約ポリシーの適用を参照してください。</p>
[アプリケーションの隔離]	<p>NSX for vSphere で設定したアプリケーションの隔離セキュリティ ポリシーを使用するには、[App の隔離] チェック ボックスを選択します。アプリケーションの隔離ポリシーは、ブループリントのすべての vSphere マシン コンポーネントに適用されます。必要に応じてセキュリティ グループとタグを追加して、vRealize Orchestrator が隔離されたネットワーク設定を開いてアプリケーションの隔離環境と通信する追加のネットワーク パスを使用できるようにします。</p> <p>詳細については、ブループリントへの NSX アプリケーションの隔離の適用を参照してください。</p>

[プロパティ] タブ

ブループリント レベルで追加したカスタム プロパティは、すべてのコンポーネントを含むブループリント全体に適用されます。優先順位の詳細については、「カスタム プロパティのリファレンス」を参照してください。

表 3-32. [プロパティ] タブの設定

タブ	設定	説明
[プロパティ グループ]		プロパティ グループは、再利用可能なプロパティのグループです。これにより、カスタム プロパティをブループリントへ追加するプロセスを簡素化できます。テナント管理者とファブリック管理者は、一緒に使用することが多いプロパティをグループ化できるため、カスタム プロパティを個別に挿入することなくプロパティ グループをブループリントに追加できます。
	[追加]	1 つまたは複数の既存のプロパティ グループを追加し、ブループリント全体に適用します。 コンテナに関連する次のプロパティ グループが用意されています。 ■ コンテナ ホストのプロパティと証明書認証 ■ コンテナ ホストのプロパティとユーザー/パスワード認証
	[上へ移動]/[下へ移動]	グループ間の優先順位を指定することで、各プロパティ グループに与えられる相対的な優先順位を制御します。リストの先頭のグループが最も優先度が高く、そのグループに属するカスタム プロパティに最高の優先度が割り当てられます。優先順位はドラッグ アンド ドロップ操作で並べ替えることができます。
	[プロパティの表示]	選択したプロパティ グループに属するカスタム プロパティを表示します。
	[マージされたプロパティの表示]	1 つのカスタム プロパティが 2 つ以上のプロパティ グループに属している場合は、最も優先度の高いプロパティ グループに属する値が優先的に使用されます。
[カスタム プロパティ]		プロパティ グループの代わりに個々のカスタム プロパティを追加できます。
	[新規]	個々のカスタム プロパティを追加し、ブループリント全体に適用します。
	[名前]	プロパティ名を入力します。カスタム プロパティとその定義の一覧については、『カスタム プロパティのリファレンス』を参照してください。
	[値]	カスタム プロパティの値を入力します。
	[暗号化済み]	たとえば、値がパスワードの場合に、プロパティ値を暗号化するように選択できます。
	[オーバーライド可能]	次回以降にプロパティを使用する人がプロパティ値をオーバーライドできるように指定できます。 [申請に表示] を選択すると、ユーザーはカタログアイテムを申請するときにプロパティ値を表示して、編集することができます。
	[申請に表示]	プロビジョニング申請フォームにプロパティの名前および値が表示されるように指定できます。ユーザーが値を指定できるようにする場合は、[オーバーライド可能] を選択します。

ブループリントへの NSX トランスポート ゾーンの適用

NSX 管理者は、トランスポート ゾーンを作成してクラスタでのネットワーク使用状況を管理することができます。

トランスポート ゾーンは、論理スイッチでアクセスできるホストを制御します。複数の vCenter Server にまたがってホストを含む、1 つ以上のホスト クラスタを範囲とします。

オンデマンド NAT またはオンデマンド ルーティング ネットワークを含むブループリントの場合、プロビジョニング済みのマシン展開環境で使用されるネットワークを含むトランスポート ゾーンを指定します。

NSX-T エンドポイントを含むブループリントでは、トランスポート ゾーンを指定する必要があります。

ブループリントに指定したトランスポート ゾーンは、ブループリントで使用する予約に指定したトランスポート ゾーンと一致する必要があります。[ブループリントへの NSX ネットワーク予約ポリシーの適用](#)を参照してください。

- ブループリントで NSX-T オンデマンド コンポーネントを使用しない場合は、トランスポート ゾーンの値は無視されます。
- NSX-T では、複数のオーバーレイ トランスポート ゾーンおよび複数の VLAN トランスポート ゾーンがサポートされます。
- トランスポート ゾーンは論理スイッチの作成に必要です。論理スイッチはトランスポート ゾーン内に作成されます。
- ブループリントの作成時には、現在のテナントのトランスポート ゾーンのみが公開されます。トランスポート ゾーンは、現在のテナントの予約によって使用されている場合に使用可能になります。

ブループリントへの NSX ネットワーク予約ポリシーの適用

ブループリントをプロビジョニングする場合は、予約ポリシーを使用して、展開用に検討可能な予約をグループ化します。ネットワーク情報は、各予約に含まれています。

この予約ポリシーにトランスポート ゾーンがある場合、ブループリントで指定されているトランスポート ゾーンと一致している必要があります。[ブループリントへの NSX トランスポート ゾーンの適用](#)を参照してください。

[新規ブループリント] または [ブループリントのプロパティ] ページを使用して、ブループリント レベルのネットワーク予約ポリシーを適用できます。

NSX for vSphere の考慮事項

NSX for vSphere では、この予約ポリシーは NSX Edge の配置や、オンデマンド ネットワークに関連付けられた分散論理ルーター (DLR) の選択の決定に役立ちます。これはルーティング ゲートウェイ予約ポリシーまたは Edge 予約ポリシーとも呼ばれます。

たとえば、NSX for vSphere では、NAT ネットワーク プロファイルおよびロード バランサにより、vRealize Automation で NSX Edge サービス ゲートウェイを展開できます。ルーティング ネットワーク プロファイルでは、NSX for vSphere 論理 Distributed Router (DLR) を使用します。DLR を vRealize Automation で使用するには、事前に NSX で作成する必要があります。vRealize Automation では DLR を作成できません。データ収集後に、vRealize Automation では DLR を使用して、仮想マシンのプロビジョニングを実行できます。

NSX Edge は、ルーティング サービスと NSX 環境の外部のネットワークへの接続を提供します。NSX Edge Gateway は NAT、ダイナミック ルーティングなどの一般的なゲートウェイ サービスを提供して、分離されたサブネット共有（アップリンク）ネットワークへ接続します。一般的な NSX Edge の展開には、NSX Edge が各テナントに仮想境界を作成したマルチテナントが含まれています。

vRealize Automation は、NAT ネットワークやロード バランサに対して、Edge サービス ゲートウェイなどのルーティング ゲートウェイをプロビジョニングします。ルーティング ネットワークの場合、vRealize Automation は既存の分散ルータを使用します。

Edge またはルーティング ゲートウェイのプロビジョニングに使用する予約により、NAT およびルーティング ネットワークのプロファイルで使用される外部ネットワークと、ロード バランサの仮想 IP アドレスが決まります。

NSX-T の考慮事項

NSX-T では、この予約ポリシーは展開に使用する Tier-0 論理ルーターの選択に役立ちます。

Tier-0 分散論理ルーターには、Tier-1 分散論理ルーターに接続するダウンリンク ポート、および外部ネットワークに接続するアップリンク ポートがあります。vRA は、出力方向の物理ルーター アクセスのために Tier-1 論理ルーターを Tier-0 論理ルーターに接続し、NAT およびロード バランサ サービスを実行するために Edge クラスタを論理ルーターに割り当てます。

ブループリントへの NSX アプリケーションの隔離の適用

アプリケーションの隔離を有効にして、ブループリントでプロビジョニングしたコンポーネント間の内部トラフィックのみを許可することができます。

NSX のアプリケーションの隔離ポリシーはファイアウォールとして動作し、展開内のプロビジョニングされたマシンとの間の送受信トラフィックすべてをブロックします。定義済みの NSX のアプリケーションの隔離ポリシーを指定する場合、ブループリントによってプロビジョニングされたマシンは相互に通信することができますが、ファイアウォールの外部に接続することはできなくなります。

アプリケーションの隔離ルールが指定され、セキュリティ ルールもブループリントのセキュリティ グループを使用して指定されている場合、アプリケーションの隔離設定はブループリントの展開時に最後に処理されるルールになります。

[新規ブループリント] または [ブループリントのプロパティ] ページを使用して、ブループリント レベルのアプリケーションの隔離を適用できます。

NSX for vSphere の考慮事項

プロビジョニングされたコンポーネントはセキュリティ グループに配置され、ファイアウォール ルールを使用して隔離されます。アプリケーションの隔離を有効にするには、NSX のこの機能をサポートするように vSphere のエンドポイントが構成されている必要があります。

NSX for vSphere のアプリケーションの隔離ポリシーを使用すると、ブループリントによってプロビジョニングされたマシン間の内部トラフィックのみが許可されます。プロビジョニングを申請すると、プロビジョニングされるマシンのセキュリティ グループが作成されます。アプリケーションの隔離ポリシーが NSX for vSphere で作成され、そのセキュリティ グループに適用されます。展開内のコンポーネント間で内部トラフィックのみを許可するように、ファイアウォール ルールがセキュリティ ポリシーで定義されています。

NSX for vSphere Edge ロード バランサと NSX for vSphere のアプリケーションの隔離セキュリティ ポリシーの両方を使用するブループリントによるプロビジョニングの場合、動的にプロビジョニングされたロード バランサはセキュリティ グループに追加されません。これにより、ロード バランサが、接続を処理することになっているマシンと通信することのないようにしています。Edge は、NSX for vSphere Distributed Firewall から除外されるため、セキュリティ グループに追加できません。ロード バランシングが正常に機能するようにするため、別のセキュリティ グループまたはセキュリティ ポリシーを使用して、ロード バランシングのために必要なトラフィックがコンポーネント仮想マシンに送られるようにしてください。

アプリケーションの隔離ポリシーは、NSX for vSphere での他のセキュリティ ポリシーと比較して優先順位が低くなります。たとえば、プロビジョニングされた展開に Web コンポーネント マシンとアプリケーション コンポーネント マシンが含まれており、Web コンポーネント マシンが Web サービスをホストしている場合、サービスでポート 80 と 443 で受信トラフィックを許可する必要があります。この場合、ユーザーはファイアウォール ルールを定義して、NSX for vSphere で Web セキュリティ ポリシーを作成し、これらのポートへの受信トラフィックを許可する必要があります。vRealize Automation では、プロビジョニングされたマシン デプロイの Web コンポーネントで、ユーザーが Web セキュリティ ポリシーを適用する必要があります。

注： ブループリントに 1 つ以上のロード バランサが含まれており、ブループリントでアプリケーション隔離が有効である場合、ロード バランサ VIP が IP アドレス セットとしてアプリケーション隔離セキュリティ グループに追加されます。ブループリントに、マシン階層に関連付けられているオンデマンド セキュリティ グループが含まれており、このマシン階層がロード バランサにも関連付けられている場合、オンデマンド セキュリティ グループには、マシン層と、ロード バランサ VIP の IP アドレス セットが含まれます。

Web コンポーネント マシンが、ロード バランサを使用してポート 8080 および 8443 でアプリケーション コンポーネント マシンにアクセスする必要がある場合、Web セキュリティ ポリシーには、ポート 80 および 443 への受信トラフィックを許可する既存のファイアウォール ルールに加えて、ポート 8080 および 8443 への送信トラフィックを許可するファイアウォール ルールも含める必要があります。

NSX-T の考慮事項

プロビジョニングされたコンポーネントは NSGroup に配置され、ファイアウォール ルールを使用して隔離されます。アプリケーションの隔離を有効にするには、NSX のこの機能をサポートするように vSphere のエンドポイントが構成されている必要があります。

NSX-T は、2 階層の論理ルーター トポロジをサポートしています。上部層の論理ルーターが Tier-0 で、下部層の論理ルーターが Tier-1 です。この構成では、プロバイダ管理者とテナント管理者の両者が、それぞれのサービスとポリシーを完全に制御できます。NSX-T 管理者が Tier-0 のルーティングとサービスを制御および設定し、テナント管理者が Tier-1 を制御および設定します。

ネットワークおよびセキュリティ コンポーネントの設定

vRealize Automation は、NSX プラットフォームに基づく仮想ネットワークに対応しています。また、Integrated vRealize Automation のコンテナ ネットワークにも対応します。

NSX ネットワークおよびセキュリティと vRealize Automation を統合するには、IaaS 管理者が vSphere と NSX のエンドポイントを設定する必要があります。vRealize Automation では、NSX for vSphere と NSX-T がサポートされています。

外部準備の詳細については、vRealize Automation の構成を参照してください。

予約およびブループリントでネットワーク設定を指定するネットワーク プロファイルを作成することができます。外部ネットワーク プロファイルにより、既存の物理ネットワークを定義します。オンデマンド NAT とルーティング ネットワーク プロファイルにより、NSX 論理スイッチと、新しいネットワーク パスに適したルーティング設定を構築できます。

ブループリントに追加するネットワークおよびセキュリティ コンポーネントの設定は、NSX for vSphere と NSX-T の構成に基づいており、vSphere クラスタの NSX インベントリのためにデータ収集を実行済みである必要があります。ネットワークおよびセキュリティ コンポーネントは、NSX 固有のもので、vSphere マシン コンポーネントとのみ使用できます。NSX の設定の詳細については、使用しているアプリケーションに応じて、[NSX for vSphere 製品のドキュメント](#)または [NSX-T 製品のドキュメント](#)にある『管理ガイド』を参照してください。

vSphere マシン コンポーネントと NSX が関連付けられている場合、ユーザー インターフェイスでネットワーク、セキュリティ、およびロード バランシングの設定を使用します。[ネットワーク] または [セキュリティ] タブのない マシン コンポーネントの場合、デザイン キャンパスの [プロパティ] タブに、VirtualMachine.Network0.Name などのネットワークおよびセキュリティのカスタム プロパティを追加することができます。NSX ネットワーク、セキュリティ、ロード バランサのプロパティを適用できるのは vSphere マシンだけです。

予約およびブループリントのネットワーク プロファイルを指定した場合は、ブループリントの値が優先されます。たとえば、ネットワーク プロファイルがブループリントに指定されており (VirtualMachine.NetworkN.ProfileName カスタム プロパティを使用)、なおかつブループリントで使用されている予約でも指定されている場合は、ブループリントに指定されているネットワーク プロファイルが優先されます。ただし、ブループリントでカスタム プロパティが使用されておらず、また、マシン NIC のネットワーク プロファイルを選択した場合、vRealize Automation では、ネットワーク プロファイルが指定されているマシン NIC に対して予約ネットワーク パスが使用されます。

コンピュータ リソースに応じて、vSphere エンドポイントを識別するトランスポート ゾーンを選択できます。トランスポート ゾーンにより、そのゾーン内で作成された論理スイッチに関連付けることができるホストおよびクラスタを指定します。トランスポート ゾーンの範囲には、複数の vSphere クラスタを含めることができます。プロビジョニングで使用するブループリントおよび予約のトランスポート ゾーンの設定は同じにする必要があります。トランスポート ゾーンは、NSX の環境で定義されます。

セキュリティ設定を指定するには、予約、ブループリント、またはゲスト エージェント スクリプトで情報を指定します。プロビジョニングするマシンにゲスト エージェントが必要な場合は、その要件を含んだセキュリティ ルールを予約またはブループリントに追加する必要があります。たとえば、すべてのマシン間の通信を拒否するデフォルトのセキュリティ ポリシーを使用したうえで、特定のマシン間の通信を許可するためのセキュリティ ポリシーを別途設けた場合、カスタマイズ段階でゲスト エージェントが vRealize Automation と通信できなくなる可能性があります。このような問題がマシンのプロビジョニング中に発生しないようにするためには、カスタマイズ段階で通信を許可するデフォルトのセキュリティ ポリシーを使用します。

コンテナ ネットワーク コンポーネントをブループリントに追加することもできます。

vRealize Automation でのセキュリティ オブジェクトへのテナント アクセスの制御

vRealize Automation の NSX セキュリティ オブジェクトのクロス テナント可用性を制御できます。

vRealize Automation で NSX セキュリティ オブジェクトを作成する際に、デフォルトの可用性をグローバル (関連付けられているエンドポイントが予約を持つすべてのテナントで使用可能)、または管理者以外のすべてのユーザーに非表示のいずれかにすることができます。

テナントで共有されるセキュリティ オブジェクトの可用性は、関連付けられているエンドポイントがテナントに予約または予約ポリシーを持つかどうかによって異なります。

NSX はセキュリティ グループをテナントしません。ただし、vRealize Automation のセキュリティ グループの可用性は、VMware.Endpoint.NSX.HideDiscoveredSecurityObjects カスタム プロパティを使用することで制御できます。

デフォルトでは、新しいセキュリティ オブジェクトは、関連付けられている NSX エンドポイントに予約がある場合に、すべてのテナントで使用可能になります。アクティブなテナントの予約がエンドポイントにない場合、セキュリティ オブジェクトはアクティブなテナントで使用できません。

NSX エンドポイントに `VMware.Endpoint.NSX.HideDiscoveredSecurityObjects` カスタム プロパティを設定していない場合、デフォルトでは新しいセキュリティ オブジェクトがグローバルに設定されます。この vRealize Automation リリースへのアップグレード前からあるセキュリティ オブジェクトは、カスタム プロパティとは無関係にグローバルに設定されます。

注： この vRealize Automation リリースにアップグレードすると、以前のリリースからのセキュリティ グループは、デフォルトでグローバルに設定されます。既存のセキュリティ グループとセキュリティ タグは、関連付けられているエンドポイントの予約があるすべてのテナントで使用できます。

新しいセキュリティ グループは、関連付けられている NSX エンドポイントに

`VMware.Endpoint.NSX.HideDiscoveredSecurityObjects` カスタム プロパティを追加することでデフォルトで非表示にできます。この設定は、次に NSX エンドポイントがデータ収集され、新しいセキュリティ オブジェクトのみに適用された際に有効になります。

既存のセキュリティ オブジェクトのテナント設定をプログラムで変更することもできます。たとえば、セキュリティ グループがグローバルに設定されている場合、vRealize Automation REST API または vRealize CloudClient で、関連付けられている NSX エンドポイントのテナント ID 設定を使用してセキュリティ オブジェクトのテナント可用性を変更できます。NSX エンドポイントに対して使用可能なテナント ID 設定は、次のとおりです。

- "`<global>`" - セキュリティ オブジェクトはすべてのテナントで使用できます。これは、本リリースにアップグレードした後の既存のセキュリティ オブジェクトと、新規で作成したすべてのセキュリティ オブジェクトの場合のデフォルト設定です。
- "`<unscoped>`" - セキュリティ オブジェクトはすべてのテナントで使用できません。システム管理者のみがセキュリティ オブジェクトにアクセスできます。これは、特定のテナントに最終的に割り当てるセキュリティ オブジェクトを定義する際に最適な設定です。
- "`tenant_id_name`" - セキュリティ オブジェクトは単一の、名前付きのテナントでのみ使用できます。

vRealize Automation REST API または vRealize CloudClient ツールを使用して、特定のエンドポイントに関連付けられているセキュリティ オブジェクトのテナント ID パラメータ (`tenantId`) を、名前付きのテナントに割り当てることができます。

vRealize Automation REST API コマンドの詳細については、vRealize Automation 7.x リリースの [vRealize Automation API ドキュメント](#) セクションにある『vRealize Automation API リファレンス』を参照してください。詳細については、vRealize Automation 7.x リリースの [vRealize Automation API ドキュメント](#) セクションにある『vRealize Automation プログラミング ガイド』を参照してください。

vRealize CloudClient の詳細については、<https://code.vmware.com/web/dp/tool/cloudclient> を参照してください。

ネットワーク、セキュリティ、ロード バランサの構成に応じた NSX-T の展開トポロジについて

vRealize Automation プループリント内で NSX-T のネットワークおよびセキュリティとロード バランサ コンポーネントをどのように構成するかによって、さまざまな展開トポロジを使用できます。

ネットワークおよびセキュリティ

- ルーティング ネットワーク

ブループリント内の vSphere マシン コンポーネントに NSX-T ルーティング ネットワーク コンポーネントを適用すると、次のトポロジが NSX-T にプロビジョニングされます。

- Tier-1 ルーターが作成されます。
- 論理スイッチが作成されます。
- Tier-1 ルーターは論理スイッチにダウンリンクされます。
- 個別に経路指定されたルートは、Tier-1 ルーター上でアドバタイズされます。
- NAT ネットワーク (固定 IP アドレス)

ブループリント内の vSphere マシン コンポーネントに NSX-T NAT ネットワークを適用すると、次のトポロジが NSX-T にプロビジョニングされます。

 - Tier-1 ルーターが作成されます。
 - 論理スイッチが作成されます。
 - Tier-1 ルーターは Edge クラスタに接続されます。
 - Tier-1 ルーターは Tier-0 ルーターにアップリンクされ、Tier-0 ルーターは予約から選択されます。
 - Tier-1 ルーターは論理スイッチにダウンリンクされます。
 - すべての NAT ルートは、Tier-1 ルーターでアドバタイズされます。
 - オンデマンド NAT ネットワーク プロファイルをサポートする外部ネットワーク プロファイルから、各 NAT ネットワークに 1 つの外部 IP アドレスが割り当てられます。この IP アドレスは、SNAT ルールと DNAT ルールに使用されます。
- NAT ネットワーク (DHCP)

ブループリント内の vSphere マシン コンポーネントに、DHCP 機能を持つ NSX-T NAT ネットワークを適用すると、次のトポロジが NSX-T にプロビジョニングされます。

 - Tier-1 ルーターが作成されます。
 - 論理スイッチが作成されます。
 - Tier-1 ルーターは Edge クラスタに接続されます。
 - Tier-1 ルーターは Tier-0 ルーターにアップリンクされ、Tier-0 ルーターは予約から選択されます。
 - Tier-1 ルーターは論理スイッチにダウンリンクされます。
 - IP アドレス プールを持つ DHCP サーバがプロビジョニングされます。
 - すべての NAT ルートは、Tier-1 ルーターでアドバタイズされます。
- アプリケーションの隔離

NSX-T コンポーネントを含むブループリントでアプリケーションの隔離が必要な場合は、NSX-T で次のトポロジがプロビジョニングされます。

注： ブループリントを作成または編集するときに、[ブループリントのプロパティ] ページでブループリントにアプリケーションの隔離を設定します。

- NS グループが作成されます。
- ファイアウォールの隔離ルールを含むファイアウォール セクションが作成されます。
- タグを使用して、アプリケーション隔離 NS グループにブループリント内のマシンが追加されます。
- ロード バランサ VIP と、IP セットでの NAT ネットワーク用の外部 IP アドレスが、アプリケーション隔離 NS グループに追加されます。

アプリケーション隔離 NS グループをサポートするには、マシンを不透明ネットワークに接続する必要があります。

■ 既存 NS グループ

ブループリント内の vSphere マシン コンポーネントに既存 NS グループのコンポーネントを適用すると、NSX-T で次のトポロジがプロビジョニングされます。

- NS グループに関連付けられているマシンが、タグをメンバーシップ基準として使用して、NSX-T 内の NS グループに追加されます。

既存 NS グループをサポートするには、マシンを不透明ネットワークに接続する必要があります。

ロード バランサ

NSX-T ブループリントの展開におけるロード バランサでは、次のトポロジがサポートされます。

- NAT オンデマンド ネットワークへのワンアーム。
- ルーティング オンデマンド ネットワークへのワンアーム。
- (既存の) 外部ネットワークへのワンアーム。
- NAT に 1 つ、外部に 1 つの 2 アーム。
- ルーティングに 1 つ、外部に 1 つの 2 アーム。

NSX-T ロード バランサがブループリントに追加されると、ネットワーク トポロジに加えて次のトポロジが展開にプロビジョニングされます。

- ロード バランサが外部ネットワークに対してワンアーム接続されている場合を除くすべてのトポロジには、以下が適用されます。
 - ブループリントに複数のロード バランサ コンポーネントが指定されている場合でも、1 つのロード バランサ サービスが作成されます。
 - ロード バランサ サービスは、展開の Tier-1 ルーターに接続されます。Tier-1 ルーターはオンデマンドで作成されます。

- ロード バランサが外部ネットワークに対してワンアーム接続されているトポロジには、以下が適用されます。
 - 予約で指定される外部ネットワークは、vCenter Server の不透明ネットワーク（NSX-T 論理スイッチ）である必要があります。
 - Tier-1 ルーターが配置され、外部ネットワーク（NSX-T 論理スイッチ）に接続されている必要があります。
 - Tier-1 ルーターがまだ配置されていない場合は、ロード バランサ サーバがオンデマンドで作成され、Tier-1 ルーターに接続されます。配置されている場合は、既存のロード バランサが使用されます。
- VIP がプライベート NAT ネットワークに配置されていない限り、VIP ルートがアダプタイズされます。
- 1 台または複数の仮想サーバがロード バランサ サービスで作成されます。
ロード バランサ サービスあたりの仮想サーバの数には、ロード バランサのサイズに基づく制限があります。
- 仮想サーバごとに、仮想サーバのアプリケーション プロファイルが作成されます。
- パーシステンス オプションが設定されている仮想サーバごとに、仮想サーバのパーシステンス プロファイルが作成されます。
- メンバーシップ プール内の各マシンの固定 IP アドレスを含むメンバーシップ プールが設定されます。
- ブループリントに指定されているロード バランサ コンポーネントの数に関係なく、1 つのロード バランサ サービスが作成されます。
- 各メンバー プールに対して健全性モニターが作成、設定されます。

HTTPS をサポートする仮想サーバの場合、NSX for vSphere のロード バランサとは異なり、NSX-T ロード バランサでは SSL パススルーはサポートされません。vRealize Automation では、ロード バランサの仮想サーバが SSL をロード バランサで終了し、ロード バランサからプール メンバーまではプレーンな HTTP を使用するよう設定されます。証明書名と SSL クライアントのプロファイル名は、どちらも NSX-T 内で指定されている必要があります。仮想サーバに HTTPS を設定するときに指定する必要があります。NSX-T トラスト マネージャに証明書をインポートできます。

ブループリントに複数の NSX-T コンポーネントが指定されている場合、Tier-1 論理ルーターはすべてのコンポーネント間で共有され、適宜設定されます。外部 Tier-1 の論理ルーター ID が、vRealize Automation の [展開] ページで各コンポーネントの [詳細] ビューに表示されます。

ブループリントでの NSX for vSphere ネットワーク コンポーネントの使用

1 つ以上の NSX for vSphere ネットワーク コンポーネントをデザイン キャンバスに追加して、ブループリントの vSphere マシン コンポーネント用に設定できます。

ブループリントに追加するネットワークおよびセキュリティ コンポーネントの設定は、NSX for vSphere の構成に基づいており、vSphere クラスターの NSX for vSphere インベントリのためにデータ収集を実行済みである必要があります。ネットワークおよびセキュリティ コンポーネントは、NSX for vSphere 固有のもので、vSphere マシン コンポーネントとのみ使用できます。NSX for vSphere の設定の詳細については、[NSX for vSphere 製品のドキュメント](#)にある『NSX 管理ガイド』を参照してください。

NSX for vSphere の既存のネットワーク コンポーネントの追加

既存の NSX for vSphere ネットワーク コンポーネントをデザイン キャンバスに追加すると、その設定をブループリント内の 1 つ以上の vSphere マシン コンポーネントに関連付けることができます。

既存のネットワーク コンポーネントを使用して NSX for vSphere ネットワークをデザイン キャンバスに追加し、その設定を vSphere マシン コンポーネント、および vSphere に属する ソフトウェア または XaaS コンポーネントで使用するよう構成できます。

既存のネットワーク コンポーネントまたはオンデマンド ネットワーク コンポーネントをマシン コンポーネントと関連付けると、NIC 情報がマシン コンポーネントと一緒に保存されます。指定するネットワーク プロファイル情報は、ネットワーク コンポーネントと一緒に保存されます。

複数のネットワークおよびセキュリティ コンポーネントをデザイン キャンバスに追加できます。

vSphere マシン コンポーネントと NSX が関連付けられている場合、ユーザー インターフェイスでネットワーク、セキュリティ、およびロード バランシングの設定を使用します。[ネットワーク] または [セキュリティ] タブのないマシン コンポーネントの場合、デザイン キャンバスの [プロパティ] タブに、`VirtualMachine.Network0.Name` などのネットワークおよびセキュリティのカスタム プロパティを追加することができます。NSX ネットワーク、セキュリティ、ロード バランサのプロパティを適用できるのは vSphere マシンだけです。

ブループリントの作成時には、現在のテナントに適用可能なネットワーク プロファイルのみが公開されます。具体的には、ネットワーク プロファイルは、プロファイルに 1 つ以上のネットワークが割り当てられている現在のテナントに 1 つ以上の予約がある場合に利用可能になります。

前提条件

- NSX のネットワーク設定を作成および構成します。vRealize Automation の構成 の NSX 構成チェックリストおよび [NSX for vSphere 製品のドキュメント](#) にある『NSX for vSphere 管理ガイド』を参照してください。
- クラスタの NSX インベントリが正常に実行されたことを確認します。
vRealize Automation の NSX 構成を使用するには、データ収集を実行する必要があります。
- ネットワーク プロファイルを作成します。
- インフラストラクチャ アーキテクトとして vRealize Automation にログインします。
- デザイン キャンバスで新規または既存のブループリントを開くには、[設計] タブを使用します。

手順

- 1 使用可能なネットワークおよびセキュリティ コンポーネントのリストを表示するには、[カテゴリ] セクションの [ネットワークとセキュリティ] をクリックします。
- 2 [既存のネットワーク] コンポーネントをデザイン キャンバス上にドラッグします。
- 3 [既存のネットワーク] テキスト ボックス内をクリックし、既存のネットワーク プロファイルを選択します。
説明、サブネット マスク、ゲートウェイの値は、選択したネットワーク プロファイルに基づいて入力されます。
- 4 (オプション) [DNS/WINS] タブをクリックします。
- 5 (オプション) ネットワーク プロファイルの DNS と WINS の設定を指定します。
 - プライマリ DNS
 - セカンダリ DNS
 - DNS サフィックス

- 優先 WINS
- 代替 WINS

既存のネットワークの DNS または WINS の設定を変更することはできません。

6 (オプション) [IP アドレス範囲] タブをクリックします。

ネットワーク プロファイルに指定されている IP アドレス範囲が表示されます。ソート順序や列の表示を変更できます。NAT ネットワークの場合、IP アドレス範囲値を変更することもできます。

7 ブループリントをドラフトとして保存するには [保存] を、ブループリントの設定を継続するには [完了] をクリックします。

次のステップ

vSphere マシン コンポーネントの [ネットワーク] タブでネットワーク設定を追加できます。

NSX for vSphere の NAT ルールの作成と使用

NAT ネットワーク コンポーネントが、クラスタ化されていない vSphere マシン コンポーネントまたはオンデマンド NSX for vSphere ロード バランサ コンポーネントに関連付けられている場合、ブループリント内の 1 対多 NAT ネットワーク コンポーネントに NAT ルールを追加できます。

NSX for vSphere でサポートされる任意のプロトコルに対して NAT ルールを定義できます。Edge の外部 IP アドレスから NAT ネットワーク コンポーネント内のプライベート IP アドレスに対して、ポートまたはポート範囲をマッピングできます。

■ vSphere マシン コンポーネント

クラスタ化されていない vSphere マシン コンポーネントに関連付けられている 1 対多 NAT ネットワーク コンポーネントに対して NAT ルールを作成できます。

たとえば、2 台のマシンがブループリントの 1 対多 NAT ネットワーク コンポーネントに関連付けられている場合、外部 IP アドレスのポート 443 が NAT ネットワークのポート 80 と TCP プロトコルを使用してそれらのマシンに接続できるようにする NAT ルールを定義できます。

■ NSX for vSphere ロード バランサ コンポーネント

NSX for vSphere ロード バランサ コンポーネントの VIP ネットワークに関連付けられている 1 対多 NAT ネットワーク コンポーネントに対して NAT ルールを作成できます。

たとえば、NAT ネットワーク コンポーネントが 3 台のマシンのロード バランシングを行っているロード バランサ コンポーネントに関連付けられている場合、外部 IP アドレスのポート 90 が NAT ネットワークのポート 80 と UDP プロトコルを使用してロード バランサ VIP に接続できるようにする NAT ルールを定義できます。

任意の数の NAT ルールを作成でき、ルールの処理順序を制御できます。

NAT ルールでは、次の要素はサポートされていません。

- 現在のネットワーク内に存在しない NIC
- DHCP を使用して IP アドレスを取得するように構成されている NIC
- マシンのクラスタ

ブループリント内の NAT ネットワーク コンポーネントに NAT ルールを追加するには、[オンデマンド NAT または オンデマンド ルーティング ネットワーク コンポーネントの追加](#) を参照してください。

NAT ルールの使用方法については、この [vmwarelab ブログの投稿](#)などの公開記事を参照してください。

オンデマンド NAT またはオンデマンド ルーティング ネットワーク コンポーネントの追加

NSX for vSphere オンデマンド NAT ネットワーク コンポーネントまたは NSX for vSphere オンデマンド ルーティング ネットワーク コンポーネントをデザイン キャンバスに追加すると、その設定をブループリント内の 1 つ以上の vSphere マシン コンポーネントに関連付けることができますようになります。

既存のネットワーク コンポーネントまたはオンデマンド ネットワーク コンポーネントをマシン コンポーネントと関連付けると、NIC 情報がマシン コンポーネントと一緒に保存されます。指定するネットワーク プロファイル情報は、ネットワーク コンポーネントと一緒に保存されます。

複数のネットワークおよびセキュリティ コンポーネントをデザイン キャンバスに追加できます。

単一のブループリントに複数のオンデマンド ネットワーク コンポーネントを持つことができます。ただし、ブループリントで使用されるすべてのオンデマンド ネットワーク プロファイルが、同一の外部ネットワーク プロファイルを参照する必要があります。

vSphere マシン コンポーネントと NSX が関連付けられている場合、ユーザー インターフェイスでネットワーク、セキュリティ、およびロード バランシングの設定を使用します。[ネットワーク] または [セキュリティ] タブのないマシン コンポーネントの場合、デザイン キャンバスの [プロパティ] タブに、VirtualMachine.Network0.Name などのネットワークおよびセキュリティのカスタム プロパティを追加することができます。NSX ネットワーク、セキュリティ、ロード バランサのプロパティを適用できるのは vSphere マシンだけです。

ブループリントの作成時には、現在のテナントに適用可能なネットワーク プロファイルのみが公開されます。具体的には、ネットワーク プロファイルは、プロファイルに 1 つ以上のネットワークが割り当てられている現在のテナントに 1 つ以上の予約がある場合に利用可能になります。

前提条件

- NSX for vSphere のネットワーク設定を作成および構成します。「vRealize Automation の構成」および [NSX for vSphere 製品のドキュメント](#) にある『NSX 管理ガイド』を参照してください。

- クラスタの NSX インベントリが正常に実行されたことを確認します。

vRealize Automation の NSX 構成を使用するには、データ収集を実行する必要があります。

- オンデマンドのネットワーク プロファイルを作成します。[ネットワーク プロファイルの作成](#)を参照してください。

たとえば、オンデマンドの NAT ネットワーク コンポーネントを追加する場合は、[オンデマンド ネットワークの NAT ネットワーク プロファイルの作成](#)を参照してください。

- インフラストラクチャ アーキテクトとして vRealize Automation にログインします。
- デザイン キャンバスで新規または既存のブループリントを開くには、[設計] タブを使用します。
- NAT ネットワーク コンポーネントの NAT ルールを指定する場合は、1 対多の NAT ネットワーク プロファイルを使用する必要があります。[提供されている IP アドレス管理エンドポイントを使用した NAT ネットワーク プロファイルの作成](#)または[サードパーティの IP アドレス管理エンドポイントを使用した NAT ネットワーク プロファイルの作成](#)を参照してください。NAT ルールの詳細については、[NSX for vSphere の NAT ルールの作成と使用](#)を参照してください。

手順

- 1 使用可能なネットワークおよびセキュリティ コンポーネントのリストを表示するには、[カテゴリ] セクションの [ネットワークとセキュリティ] をクリックします。
- 2 オンデマンド NAT またはオンデマンド ルーティング ネットワーク コンポーネントをデザイン キャンバスにドラッグします。
- 3 デザイン キャンバスでコンポーネントに一意のラベルを付けるには、[ID] テキスト ボックスにコンポーネント名を入力します。
- 4 [親ネットワーク プロファイル] ドロップダウン メニューから適切なネットワーク プロファイルを選択します。たとえば、NAT ネットワーク コンポーネントを追加する場合は、目的のネットワーク設定をサポートするように構成された NAT ネットワーク プロファイルを選択します。

NAT ネットワーク コンポーネントの NAT ルールを指定する場合は、1 対多の NAT に構成されている親ネットワーク プロファイルを使用する必要があります。

選択するプロファイルの種類に応じて、次のネットワーク設定の値が、ネットワーク プロファイルの選択に基づいてポピュレートされます。値の変更はネットワーク プロファイル側で行う必要があります。

- 外部ネットワーク プロファイル名
 - NAT タイプ (オンデマンド NAT)
 - サブネット マスク
 - サブネット マスク範囲 (オンデマンド ルーティング)
 - サブネット マスク範囲 (オンデマンド ルーティング)
 - 基本 IP アドレス (オンデマンド ルーティング)
- 5 (オプション) [説明] テキスト ボックスにコンポーネントの説明を入力します。
 - 6 (オプション) [DNS/WINS] タブをクリックします。
 - 7 (オプション) ネットワーク プロファイルの DNS と WINS の設定を指定します。
 - プライマリ DNS
 - セカンダリ DNS
 - DNS サフィックス
 - 優先 WINS
 - 代替 WINS

既存のネットワークの DNS または WINS の設定を変更することはできません。

- 8 [IP アドレス範囲] タブをクリックします。

ネットワーク プロファイルに指定されている IP アドレス範囲が表示されます。ソート順序や列の表示を変更できます。NAT ネットワークの場合、IP アドレス範囲値を変更することもできます。

- a [IP アドレス範囲の開始] テキスト ボックスに開始 IP アドレスの値を入力します。
- b [IP アドレス範囲の終了] テキスト ボックスに終了 IP アドレスの値を入力します。

- 9 固定の IP アドレス範囲を使用する 1 対多の NAT ネットワーク プロファイルに基づいている NAT ネットワークを使用している場合は、[NAT ルール] タブを使用して、外部 IP アドレスを有効にするルールを追加し、内部 NAT ネットワークのコンポーネントにアクセスすることができます。

1 対多の NAT ネットワークでは、NAT ルールを定義しておき、NAT ネットワーク コンポーネントをブループリントに追加するときにそのルールを構成できます。また、展開の中で NAT ネットワークを編集するときに NAT ルールを変更することができます。

選択可能なオプションは、NAT ネットワーク コンポーネントに関連付けられている vSphere マシンまたは NSX for vSphere ロード バランサ コンポーネントに基づいています。

- [名前]: 固有のルールの名前を入力します。
- [コンポーネント]: 関連付けられている vSphere マシンまたは NAT ネットワークと関連付けられているロード バランサ コンポーネントのリストから選択します。

NAT ルールは、クラスタ化されていないマシンでのみサポートされます。1 より大きなクラスタ サイズを指定した場合、構成はサポートされないためコンポーネントはリストされません。

- [ソース ポート]: 任意のオプションを選択して、有効なポートまたはポート範囲を入力するか、有効なプロパティ バインドを指定します。
- [ターゲット ポート]: 任意のオプションを選択して、有効なポートまたはポート範囲を入力するか、有効なプロパティ バインドを指定します。
- [プロトコル]: 任意の有効な NSX for vSphere サポート対象のプロトコルを入力するか、TCP、UDP、または任意のオプションを選択します。
- [説明]: NAT ルールの設定の簡単な説明を入力します。

- 10 ブループリントをドラフトとして保存するには [保存] を、ブループリントの設定を継続するには [完了] をクリックします。

次のステップ

vSphere マシン コンポーネントの [ネットワーク] タブでネットワーク設定を追加できます。

ブループリントでの NSX-T ネットワーク コンポーネントの使用

1 つ以上の NSX-T ネットワーク コンポーネントをデザイン キャンバスに追加して、ブループリントの vSphere マシン コンポーネント用に設定できます。

ブループリントに追加するネットワークおよびセキュリティ コンポーネントの設定は、NSX-T の構成に基づいており、vSphere クラスタの NSX-T インベントリのためにデータ収集を実行済みである必要があります。ネットワークおよびセキュリティ コンポーネントは、NSX-T 固有のもので、vSphere マシン コンポーネントとのみ使用できます。NSX-T の設定の詳細については、[NSX-T 製品のドキュメント](#)にある『NSX-T 管理ガイド』を参照してください。

NSX-T エンドポイントが含まれているブループリントを展開すると、NSX-T ネットワーク、セキュリティ、およびロード バランサのコンポーネントや、NSX-T エンドポイントの関連付けられている vSphere マシン コンポーネントなど、展開に含まれるすべての NSX-T コンポーネントにタグが割り当てられます。タグは展開に一意で、初期導入およびそれ以降に展開で実行した後続のアクションのコンポーネントに関連付けられます。タグの名前は、展開の名前と同じです。

NSX-T に固有の展開およびトポロジの考慮事項の詳細については、[ネットワーク、セキュリティ、ロード バランサの構成に応じた NSX-T の展開トポロジについて](#)を参照してください。

NSX-T の既存のネットワーク コンポーネントの追加

既存の NSX-T ネットワーク コンポーネントをデザイン キャンバスに追加すると、その設定をブループリント内の 1 つ以上の vSphere マシン コンポーネントに関連付けることができます。

既存のネットワーク コンポーネントを使用して NSX-T ネットワークをデザイン キャンバスに追加し、その設定を vSphere マシン コンポーネント、および vSphere に属する ソフトウェア または XaaS コンポーネントで使用するよう構成できます。

既存のネットワーク コンポーネントまたはオンデマンド ネットワーク コンポーネントをマシン コンポーネントと関連付けると、NIC 情報がマシン コンポーネントと一緒に保存されます。指定するネットワーク プロファイル情報は、ネットワーク コンポーネントと一緒に保存されます。

複数のネットワークおよびセキュリティ コンポーネントをデザイン キャンバスに追加できます。

vSphere マシン コンポーネントと NSX が関連付けられている場合、ユーザー インターフェイスでネットワーク、セキュリティ、およびロード バランシングの設定を使用します。[ネットワーク] または [セキュリティ] タブのないマシン コンポーネントの場合、デザイン キャンバスの [プロパティ] タブに、VirtualMachine.Network0.Name などのネットワークおよびセキュリティのカスタム プロパティを追加することができます。NSX ネットワーク、セキュリティ、ロード バランサのプロパティを適用できるのは vSphere マシンだけです。

ブループリントの作成時には、現在のテナントに適用可能なネットワーク プロファイルのみが公開されます。具体的には、ネットワーク プロファイルは、プロファイルに 1 つ以上のネットワークが割り当てられている現在のテナントに 1 つ以上の予約がある場合に利用可能になります。

前提条件

- NSX-T のネットワーク設定を作成および構成します。vRealize Automation の構成および [NSX-T 製品のドキュメント](#)にある『NSX-T 管理ガイド』を参照してください。
- クラスタの NSX インベントリが正常に実行されたことを確認します。
vRealize Automation の NSX 構成を使用するには、データ収集を実行する必要があります。
- ネットワーク プロファイルを作成します。
- インフラストラクチャ アーキテクトとして vRealize Automation にログインします。
- デザイン キャンバスで新規または既存のブループリントを開くには、[設計] タブを使用します。

手順

- 1 使用可能なネットワークおよびセキュリティ コンポーネントのリストを表示するには、[カテゴリ] セクションの [ネットワークとセキュリティ] をクリックします。
- 2 [既存のネットワーク] コンポーネントをデザイン キャンバス上にドラッグします。
- 3 [既存のネットワーク] テキスト ボックス内をクリックし、既存のネットワーク プロファイルを選択します。
説明、サブネット マスク、ゲートウェイの値は、選択したネットワーク プロファイルに基づいて入力されます。
- 4 (オプション) [DNS/WINS] タブをクリックします。

5 (オプション) ネットワーク プロファイルの DNS と WINS の設定を指定します。

- プライマリ DNS
- セカンダリ DNS
- DNS サフィックス
- 優先 WINS
- 代替 WINS

既存のネットワークの DNS または WINS の設定を変更することはできません。

6 (オプション) [IP アドレス範囲] タブをクリックします。

ネットワーク プロファイルに指定されている IP アドレス範囲が表示されます。ソート順序や列の表示を変更できます。NAT ネットワークの場合、IP アドレス範囲値を変更することもできます。

7 ブループリントをドラフトとして保存するには [保存] を、ブループリントの設定を継続するには [完了] をクリックします。

次のステップ

vSphere マシン コンポーネントの [ネットワーク] タブでネットワーク設定を追加できます。

NSX-T の NAT ルールの作成と使用

NAT ネットワーク コンポーネントが、クラスタ化されていない vSphere マシン コンポーネントに関連付けられている場合、ブループリント内の 1 対多 NAT ネットワーク コンポーネントに NAT ルールを追加できます。

NSX-T でサポートされる任意のプロトコルに対して NAT ルールを定義できます。Edge の外部 IP アドレスから NAT ネットワーク コンポーネント内のプライベート IP アドレスに対して、ポートまたはポート範囲をマッピングできます。

クラスタ化されていない vSphere マシン コンポーネントに関連付けられている 1 対多 NAT ネットワーク コンポーネントに対して NAT ルールを作成できます。たとえば、2 台のマシンがブループリントの 1 対多 NAT ネットワーク コンポーネントに関連付けられている場合、外部 IP アドレスのポート 443 が NAT ネットワークのポート 80 と TCP プロトコルを使用してそれらのマシンに接続できるようにする NAT ルールを定義できます。

NSX-T ロード バランサまたは NSX-T バージョン 2.2 では、NAT ルールはサポートされません。

任意の数の NAT ルールを作成でき、ルールの処理順序を制御できます。

NAT ルールでは、次の要素はサポートされていません。

- 現在のネットワーク内に存在しない NIC
- DHCP を使用して IP アドレスを取得するように構成されている NIC
- マシンのクラスタ

ブループリント内の NAT ネットワーク コンポーネントに NAT ルールを追加するには、[NSX-T オンデマンド NAT または NSX-T オンデマンド ルーティング ネットワーク コンポーネントの追加](#) を参照してください。

NSX-T オンデマンド NAT または NSX-T オンデマンド ルーティング ネットワーク コンポーネントの追加

NSX-T オンデマンド NAT ネットワーク コンポーネントまたは NSX-T オンデマンド ルーティング ネットワーク コンポーネントをデザイン キャンバスに追加すると、その設定をブループリント内の 1 つ以上の vSphere マシン コンポーネントに関連付けることができますようになります。

既存のネットワーク コンポーネントまたはオンデマンド ネットワーク コンポーネントをマシン コンポーネントと関連付けると、NIC 情報がマシン コンポーネントと一緒に保存されます。指定するネットワーク プロファイル情報は、ネットワーク コンポーネントと一緒に保存されます。

複数のネットワークおよびセキュリティ コンポーネントをデザイン キャンバスに追加できます。

単一のブループリントに複数のオンデマンド ネットワーク コンポーネントを持つことができます。ただし、ブループリントで使用されるすべてのオンデマンド ネットワーク プロファイルが、同一の外部ネットワーク プロファイルを参照する必要があります。

NSX-T の場合、各種のネットワークで使用されるネットワーク範囲は、ブループリント内で重複することはできません。この制限は、NSX-T Tier-1 ルーター ネットワークを設定する場合に適用されます。

vSphere マシン コンポーネントと NSX が関連付けられている場合、ユーザー インターフェイスでネットワーク、セキュリティ、およびロード バランシングの設定を使用します。[ネットワーク] または [セキュリティ] タブのないマシン コンポーネントの場合、デザイン キャンバスの [プロパティ] タブに、VirtualMachine.Network0.Name などのネットワークおよびセキュリティのカスタム プロパティを追加することができます。NSX ネットワーク、セキュリティ、ロード バランサのプロパティを適用できるのは vSphere マシンだけです。

ブループリントの作成時には、現在のテナントに適用可能なネットワーク プロファイルのみが公開されます。具体的には、ネットワーク プロファイルは、プロファイルに 1 つ以上のネットワークが割り当てられている現在のテナントに 1 つ以上の予約がある場合に利用可能になります。

前提条件

- NSX for vSphere のネットワーク設定を作成および構成します。vRealize Automation の構成および [NSX-T 製品のドキュメント](#)にある『NSX for vSphere 管理ガイド』を参照してください。
- クラスタの NSX インベントリが正常に実行されたことを確認します。
vRealize Automation の NSX 構成を使用するには、データ収集を実行する必要があります。
- オンデマンドのネットワーク プロファイルを作成します。 [ネットワーク プロファイルの作成](#)を参照してください。
たとえば、オンデマンドの NAT ネットワーク コンポーネントを追加する場合は、 [オンデマンド ネットワークの NAT ネットワーク プロファイルの作成](#)を参照してください。
- インフラストラクチャ アーキテクトとして vRealize Automation にログインします。
- デザイン キャンバスで新規または既存のブループリントを開くには、[設計] タブを使用します。
- NAT ネットワーク コンポーネントの NAT ルールを指定する場合は、1 対多の NAT ネットワーク プロファイルを使用する必要があります。 [提供されている IP アドレス管理エンドポイントを使用した NAT ネットワーク プロファイルの作成](#)または [サードパーティの IP アドレス管理エンドポイントを使用した NAT ネットワーク プロファイルの作成](#)を参照してください。 NAT ルールの詳細については、 [NSX for vSphere の NAT ルールの作成と使用](#)を参照してください。

手順

- 1 使用可能なネットワークおよびセキュリティ コンポーネントのリストを表示するには、[カテゴリ] セクションの [ネットワークとセキュリティ] をクリックします。
- 2 NSX-T オンデマンド NAT または NSX-T オンデマンド ルーティング ネットワーク コンポーネントをデザイン キャンバスにドラッグします。
- 3 デザイン キャンバスでコンポーネントに一意のラベルを付けるには、[ID] テキスト ボックスにコンポーネント名を入力します。
- 4 [親ネットワーク プロファイル] ドロップダウン メニューから適切なネットワーク プロファイルを選択します。たとえば、NAT ネットワーク コンポーネントを追加する場合は、目的のネットワーク設定をサポートするように構成された NAT ネットワーク プロファイルを選択します。

NAT ネットワーク コンポーネントの NAT ルールを指定する場合は、1 対多の NAT に構成されている親ネットワーク プロファイルを使用する必要があります。

選択するプロファイルの種類に応じて、次のネットワーク設定の値が、ネットワーク プロファイルの選択に基づいてポピュレートされます。値の変更はネットワーク プロファイル側で行う必要があります。

- 外部ネットワーク プロファイル名
 - NAT タイプ (NSX-T オンデマンド NAT)
 - サブネット マスク
 - サブネット マスク範囲 (NSX-T オンデマンド ルーティング)
 - サブネット マスク範囲 (NSX-T オンデマンド ルーティング)
 - 基本 IP アドレス (NSX-T オンデマンド ルーティング)
- 5 (オプション) [説明] テキスト ボックスにコンポーネントの説明を入力します。
 - 6 (オプション) [DNS/WINS] タブをクリックします。
 - 7 (オプション) ネットワーク プロファイルの DNS と WINS の設定を指定します。
 - プライマリ DNS
 - セカンダリ DNS
 - DNS サフィックス
 - 優先 WINS
 - 代替 WINS

既存のネットワークの DNS または WINS の設定を変更することはできません。

- 8 [IP アドレス範囲] タブをクリックします。

ネットワーク プロファイルに指定されている IP アドレス範囲が表示されます。ソート順序や列の表示を変更できます。NAT ネットワークの場合、IP アドレス範囲値を変更することもできます。

- a [IP アドレス範囲の開始] テキスト ボックスに開始 IP アドレスの値を入力します。
- b [IP アドレス範囲の終了] テキスト ボックスに終了 IP アドレスの値を入力します。

- 9 固定の IP アドレス範囲を使用する 1 対多の NAT ネットワーク プロファイルに基づいている NAT ネットワークを使用している場合は、[NAT ルール] タブを使用して、外部 IP アドレスを有効にするルールを追加し、内部 NAT ネットワークのコンポーネントにアクセスすることができます。

1 対多の NAT ネットワークでは、NAT ルールを定義しておき、NAT ネットワーク コンポーネントをブループリントに追加するときにそのルールを構成できます。また、展開の中で NAT ネットワークを編集するときに NAT ルールを変更することができます。

選択可能なオプションは、NAT ネットワーク コンポーネントに関連付けられている vSphere マシン コンポーネントに基づいています。

- [名前]：固有のルールの名前を入力します。
- [コンポーネント]：関連付けられている vSphere マシンまたは NAT ネットワークと関連付けられているロード バランサ コンポーネントのリストから選択します。

NAT ルールは、クラスタ化されていないマシンでのみサポートされます。1 より大きなクラスタ サイズを指定した場合、構成はサポートされないためコンポーネントはリストされません。

- [ソース ポート]：任意のオプションを選択して、有効なポートまたはポート範囲を入力するか、有効なプロパティ バインドを指定します。
- [ターゲット ポート]：任意のオプションを選択して、有効なポートまたはポート範囲を入力するか、有効なプロパティ バインドを指定します。
- [プロトコル]：任意の有効な NSX-T サポート対象のプロトコルを入力するか、TCP、UDP、または任意のオプションを選択します。
- [説明]：NAT ルールの設定の簡単な説明を入力します。

- 10 ブループリントをドラフトとして保存するには [保存] を、ブループリントの設定を継続するには [完了] をクリックします。

次のステップ

vSphere マシン コンポーネントの [ネットワーク] タブでネットワーク設定を追加できます。

ブループリントでの NSX for vSphere ロード バランサ コンポーネントの使用

1 つ以上のオンデマンド NSX for vSphere ロード バランサ コンポーネントをデザイン キャンバスに追加して、ブループリントの vSphere マシン コンポーネント設定を構成できます。

ブループリントに追加するネットワークおよびセキュリティ コンポーネントの設定は、NSX for vSphere と NSX-T の構成に基づいており、vSphere クラスタの NSX インベントリのためにデータ収集を実行済みである必要があります。ネットワークおよびセキュリティ コンポーネントは、NSX 固有のもので、vSphere マシン コンポーネントとのみ使用できます。NSX の設定の詳細については、使用しているアプリケーションに応じて、[NSX for vSphere 製品のドキュメント](#)または [NSX-T 製品のドキュメント](#)にある『管理ガイド』を参照してください。

次のルールをブループリントのロード バランサ プールおよび VIP ネットワーク設定に適用します。

- プール ネットワーク プロファイルが NAT の場合、VIP ネットワーク プロファイルを NAT ネットワーク プロファイルに含めることができます。
- プール ネットワーク プロファイルがルーティングされている場合、VIP ネットワーク プロファイルには、同一のルーティング ネットワークのみを利用できます。

- プール ネットワーク プロファイルが外部の場合、VIP ネットワーク プロファイルには、同じ外部ネットワーク プロファイルのみを利用できます。

各ロード バランサ コンポーネントには、ロード バランサ サービスとも呼ばれる複数の仮想サーバを含めることができます。ロード バランサ コンポーネントの各仮想サーバには、1つのポートとプロトコルがあります。たとえば、HTTP サービスまたは HTTPS サービスのロード バランシングが可能です。ロード バランサには、ロード バランシングしている複数のサービスを含めることができます。

NSX Edge は、ロード バランサ仮想サーバを含むネットワーク デバイスです。ブルー プリントで複数のロード バランサ コンポーネントを保持できますが、展開をプロビジョニングする場合、各ロード バランサ コンポーネントに定義されている仮想サーバは単一の NSX Edge に含まれています。

ブループリントに 1つ以上のロード バランサが含まれており、ブループリントでアプリケーション隔離が有効である場合、ロード バランサ VIP が IP アドレス セットとしてアプリケーション隔離セキュリティ グループに追加されます。ブループリントに、マシン階層に関連付けられているオンデマンド セキュリティ グループが含まれており、このマシン階層がロード バランサにも関連付けられている場合、オンデマンド セキュリティ グループには、マシン層と、ロード バランサ VIP の IP アドレス セットが含まれます。

既存の展開に含まれるロード バランサ設定を再構成して、仮想サーバを追加、編集または削除できます。

アップグレードまたは移行後のロード バランサ コンポーネントを使用する場合の考慮事項

ターゲット vRealize Automation リリースの NSX ロード バランサ コンポーネントについて操作する際は、次の考慮事項を理解することが重要です。

この情報は、この vRealize Automation リリースにアップグレードまたは移行された NSX for vSphere ロード バランサ コンポーネントに適用されます。

- ロード バランサの再構成アクションを実行する際の問題を回避するために、このリリースへのアップグレードまたは移行の前および後で、NSX のネットワークおよびセキュリティ インベントリ データ収集を実行する必要があります。新しい展開でのロード バランサの再構成アクションには影響しません。

詳細は、『vRealize Automation 7.1 以降からのアップデート』および『vRealize Automation の移行』を参照してください。

- ロード バランサを再設定できます。必要なカタログ資格は再構成（ロード バランサ）です。
- vRealize Automation 7.x からこの vRealize Automation リリースにアップグレードまたは移行した展開の場合、ロード バランサの再構成はロード バランサが 1つのみの環境でのみ可能です。
- ロード バランサの再構成の操作は、vRealize Automation 6.2.x からこの vRealize Automation のリリースにアップグレードまたは移行された環境ではサポートされません。

オンデマンド ロード バランサ コンポーネントの追加

NSX オンデマンド ロード バランサ コンポーネントをデザイン キャンバスにドラッグし、ブループリントの vSphere マシン コンポーネントおよびコンテナ コンポーネントで使用するための設定を作成できます。

特定の種類のネットワーク トラフィックの動作を定義する NSX for vSphere アプリケーション プロファイルの作成に関連する情報については、[NSX for vSphere 製品のドキュメント](#)にある『NSX 管理ガイド』を参照してください。

手順

1 ロード バランサ メンバーの設定の定義

オンデマンド NSX ロード バランサ コンポーネントを定義することにより、ネットワーク内のプロビジョニングされた vSphere メンバー マシンまたはコンテナ マシンの間でタスク処理を分散できます。

2 仮想サーバの全般設定の定義

ロード バランサに単一の仮想サーバ プロトコルとポートを定義することも、追加の NSX ロード バランサ オプションをカスタマイズするために仮想サーバを追加することもできます。

3 仮想サーバの配布設定の定義

[全般] タブで [カスタマイズ] オプションを選択すると、メンバーがトラフィックを受信するポート、NSX ロード バランサがそのポートにアクセスするために使用できるプロトコル タイプ、ロード バランシングに使用するアルゴリズム、パーシステンス設定など、プール メンバーに関する情報を指定できます。

4 仮想サーバの健全性チェック設定の定義

[全般] タブで [カスタマイズ] オプションを選択すると、NSX ロード バランサが仮想サーバ内のプールに対して健全性チェックを実行する方法または実行するかどうかを指定できます。

5 仮想サーバの詳細設定の定義

[全般] タブで [カスタマイズ] オプションを選択することで、NSX ロード バランサ コンポーネントをカスタマイズして、単一のプール メンバーが認識できる同時接続数や、仮想サーバが処理できる同時接続の最大数などの設定を指定できます。

6 ロード バランサのログ オプションの定義

ロード バランサのログ アクションのタイプを定義できます。これにより、ロード バランサのログに記録される対象が決まります。

ロード バランサ メンバーの設定の定義

オンデマンド NSX ロード バランサ コンポーネントを定義することにより、ネットワーク内のプロビジョニングされた vSphere メンバー マシンまたはコンテナ マシンの間でタスク処理を分散できます。

デザイン キャンバスのブループリントにロード バランサ コンポーネントを追加するときは、ロード バランサ コンポーネントで仮想サーバ定義を作成または編集するときに、デフォルトまたはカスタムのオプションを選択できます。デフォルト オプションでは、仮想サーバのプロトコル、ポート、説明を指定し、他のすべての設定にデフォルトを使用できます。カスタム オプションでは、さらに詳細なレベルで定義できます。

ロード バランサが外部ネットワークを使用してプロビジョニングされている場合、VIP (VIP ネットワーク) とメンバー プール (メンバー ネットワーク) は、同一の既存ネットワーク上に配置されている必要があります。VIP とメンバープールが同一の外部ネットワーク上にない場合は、プロビジョニングに失敗します。

前提条件

- NSX のロード バランサを作成し、設定します。vRealize Automation の構成および『NSX 管理ガイド』を参照してください。

- クラスタの NSX インベントリが正常に実行されたことを確認します。
- vRealize Automation の NSX 構成を使用するには、データ収集を実行する必要があります。
- ネットワーク プロファイルを作成します。
 - インフラストラクチャ アーキテクトとして vRealize Automation にログインします。
 - デザイン キャンバスで新規または既存のブループリントを開くには、[設計] タブを使用します。
 - 少なくとも 1 つの vSphere マシン コンポーネントまたはコンテナ コンポーネントがブループリントに存在することを確認します。

手順

- 1 使用可能なネットワークおよびセキュリティ コンポーネントのリストを表示するには、[カテゴリ] セクションの [ネットワークとセキュリティ] をクリックします。

- 2 [オンデマンド ロード バランサ] コンポーネントをデザイン キャンバス上にドラッグします。

- 3 デザイン キャンバスでコンポーネントに一意のラベルを付けるには、[ID] テキスト ボックスにコンポーネント名を入力します。

- 4 [メンバー] ドロップダウン メニューから vSphere マシン コンポーネント名またはコンテナ コンポーネント名を選択します。

リストには、アクティブなブループリントの vSphere マシン コンポーネントとコンテナ コンポーネントのみが含まれています。

- 5 [メンバー ネットワーク] ドロップダウン メニューからロード バランシング対象の NIC を選択します。

このリストには、選択した vSphere マシン メンバーに対して定義されている NIC が含まれます。

- 6 [VIP ネットワーク] ドロップダウン メニューから使用可能な仮想 IP アドレス ネットワークを選択します。たとえば、使用可能な外部ネットワークまたは NAT ネットワークを選択します。

ブループリントに複数の NSX ロード バランサおよび NSX オンデマンド ネットワーク コンポーネントを保持できますが、すべてが同じ VIP ネットワークに関連付けられている必要があります。

- 7 (オプション) [IP アドレス] テキスト ボックスに、NIC の有効な IP アドレスを入力します。

デフォルトの設定は、VIP ネットワークに関連付けられている固定 IP アドレスです。別の IP アドレスや IP アドレス範囲を指定できます。デフォルトでは、関連付けられている VIP ネットワークから次の使用可能 IP アドレスが割り当てられます。

IP アドレスのフィールドを空のままにしておくと、プロビジョニング時に関連付けられた VIP ネットワークから IP アドレスを割り当てることができます。

指定する IP アドレスが他のタイプのネットワークである場合、プロビジョニングできる展開は 1 つだけです。それ以降の展開では、IP アドレスが既に最初の展開によって使用されているため、IP アドレスの割り当てが失敗します。

- 8 仮想サーバの定義を作成するには、[新規] をクリックします。[仮想サーバの全般設定の定義](#)を参照してください。

各ロード バランサ コンポーネントには、少なくとも 1 台の仮想サーバが必要です。

ログ オプションを指定するには、[ロード バランサのログ オプションの定義](#)を参照してください。

仮想サーバの全般設定の定義

ロード バランサに単一の仮想サーバ プロトコルとポートを定義することも、追加の NSX ロード バランサ オプションをカスタマイズするために仮想サーバを追加することもできます。

たとえば、ロード バランサ コンポーネントをカスタマイズして、健全性チェック プロトコルおよびポート、アルゴリズム、パシステンス、透過性などの設定を定義することができます。

前提条件

[ロード バランサ メンバーの設定の定義](#)。

手順

- 1 [新規仮想サーバ] ページで[全般] タブをクリックします。
- 2 仮想サーバのロード バランシングに使用するために、[プロトコル] ドロップダウン メニューでネットワーク トラフィック プロトコルを選択します。

プロトコル オプションは、HTTP、HTTPS、TCP、UDP です。

- 3 [ポート] テキスト ボックスにポート値を入力します。

選択したプロトコルによって、デフォルト ポート設定が決まります。

プロトコル	デフォルト ポート
HTTP	80
HTTPS	443
TCP	8080
UDP	デフォルトなし

HTTP、HTTPS、TCP プロトコルは、UDP とポートを共有できます。たとえば、サービス 1 がポート 80 で TCP、HTTP、または HTTPS を使用する場合、サービス 2 はポート 80 で UDP を使用できます。ただし、サービス 1 がポート 80 で UDP を使用する場合、サービス 2 はポート 80 で UDP を使用することはできません。

- 4 (オプション) 仮想サーバ コンポーネントの説明を入力します。
- 5 いずれかの [設定] オプションを選択します。

- [その他すべての設定にデフォルト値を使用]

その他すべてのデフォルト設定を受け入れます。[OK] をクリックしてロード バランサ コンポーネント定義を終了し、ブループリントでの作業を続行します。

[カスタマイズ] をクリックして、追加のタブ オプションを調べることによって、デフォルト値を表示できます。デフォルト設定が許容可能な場合は、[全般] タブで [その他すべての設定にデフォルト値を使用] をクリックします。

- [カスタマイズ]

たとえば、健全性の監視に異なるプロトコルを定義する場合や、メンバー トラフィックを監視するために別のポートを定義する場合などに、追加設定を使用してロード バランサ コンポーネントを構成します。

カスタマイズした設定を追加できる追加のタブが表示されます。

[その他すべての設定にデフォルト値を使用] を選択して [OK] をクリックすると、デザイン キャンバスでブループリントの定義または編集を続行することができます。[カスタマイズ] を選択した場合は、手順を続行します。

- 6 [配布] タブをクリックし、[仮想サーバの配布設定の定義](#) トピックの手順に従って、NSX ロード バランサ コンポーネントでの仮想サーバの定義を続行します。

仮想サーバの配布設定の定義

[全般] タブで [カスタマイズ] オプションを選択すると、メンバーがトラフィックを受信するポート、NSX ロード バランサがそのポートにアクセスするために使用できるプロトコル タイプ、ロード バランシングに使用するアルゴリズム、パーシステンス設定など、プール メンバーに関する情報を指定できます。

プールは、ロード バランシングされているマシンのクラスタを表します。プール メンバーは、そのクラスタ内の 1 つのマシンを表します。

デフォルトのメンバー プロトコルとメンバー ポートの設定は、[全般] ページのプロトコルとポートの設定と一致します。

メンバー マシンのプールは、ブループリント ロード バランサ コンポーネント ユーザー インターフェイスの [メンバー] オプション値に表示されます。[メンバー] エントリは、プールまたはマシンのクラスタに設定されます。

前提条件

[仮想サーバの全般設定の定義](#)。

手順

- 1 (オプション) [メンバー プロトコル] 設定は、[全般] タブで指定しているプロトコルと一致します。この設定では、プール メンバーがネットワーク トラフィックを受信する方法を定義します。
- 2 (オプション) [メンバー ポート] テキスト ボックスにポート番号を入力して、プール メンバーがネットワーク トラフィックを受信するポートを指定します。

たとえば、ロード バランサの仮想 IP アドレス (VIP) の受信要求がポート 80 で受信される場合に、その要求をプール メンバーの別のポート (ポート 8080 など) にルーティングする場合があります。

3 (オプション) このプールのアルゴリズム バランシング メソッドを選択します。

アルゴリズム オプションとオプションで必要となるアルゴリズム パラメータについては、次の表で説明します。

オプション	説明とアルゴリズム パラメータ
ROUND_ROBIN	<p>各サーバは、割り当てられている重みに従って順番に使用されます。</p> <p>ロード バランサが vRealize Automation で作成されている場合、重みはすべてのメンバーで同じです。</p> <p>これは、サーバの処理時間が等分されたままになる場合に、最も円滑で公平なアルゴリズムです。</p> <p>このオプションでは、アルゴリズムのパラメータは無効になります。</p>
IP-HASH	<p>ソース IP アドレスのハッシュ、および実行されているすべてのサーバの重みの合計に基づいて、サーバを選択します。</p> <p>このオプションでは、アルゴリズムのパラメータは無効になります。</p>
LEASTCONN	<p>サーバの既存の接続数に基づいて、クライアント要求を複数のサーバに配信します。</p> <p>新しい接続は、接続数が最も少ないサーバに送信されます。</p> <p>このオプションでは、アルゴリズムのパラメータは無効になります。</p>
URI	<p>URI の左側の部分（疑問符の前の部分）がハッシュされ、実行中のサーバの合計重みによって除算されます。</p> <p>結果により、要求を受信するサーバが指定されます。これにより、サーバが起動したり停止したりしない限り、URI がいつも同一のサーバに送信されるようにします。</p> <p>URI アルゴリズム パラメータには 2 つのオプション (<code>uriLength=<len></code>、<code>uriDepth=<dep></code>) があります。[アルゴリズムのパラメータ] テキスト ボックスの個別の行に、長さ と 深さ のパラメータを入力します。</p> <p>長さ と 深さ のパラメータには、正の整数が続きます。これらのオプションでは、URI の最初の部分のみに基づいてサーバのバランシングを行うことができます。</p> <p>長さのパラメータは、アルゴリズムが URI の最初の部分に定義された文字だけを対象としてハッシュを計算することを示します。長さのパラメータの範囲は $1 \leq len < 256$ です。</p> <p>深さのパラメータは、ハッシュの計算に使用されるディレクトリの最大の深さを示します。要求に含まれる各スラッシュが 1 つのレベルとして数えられます。深さのパラメータの範囲は $1 \leq dep < 10$ です。</p> <p>両方のパラメータが指定されている場合は、いずれかのパラメータに達したときに評価が停止します。</p>
HTTPHEADER	<p>各 HTTP 要求で HTTP ヘッダー名の検索が行われます。</p> <p>カッコで囲まれたヘッダー名は、ACL の「hdr()」関数と同様に大文字と小文字が区別されません。</p> <p>HTTPHEADER アルゴリズム パラメータのオプションは 1 つ (<code>headerName=<name></code>) です。たとえば、host を HTTPHEADER アルゴリズム パラメータとして使用できます。</p> <p>ヘッダーがない、または値を含んでいない場合は、ラウンド ロビン アルゴリズムが適用されます。</p>
URL	<p>引数に指定される URL パラメータは、各 HTTP GET 要求のクエリ文字列内で検索されます。</p> <p>URL アルゴリズム パラメータのオプションは 1 つ (<code>urlParam=<url></code>) です。</p> <p>パラメータの後ろに等号の = と値が続く場合、その値がハッシュされ、実行されるサーバの重みの合計で割られます。結果により、要求を受信するサーバが指定されます。このプロセスを使用して要求に含まれるユーザー ID が追跡され、サーバの起動または停止が起こらない限り、常に同一のユーザー ID が同一のサーバに送信されます。</p> <p>値またはパラメータが検出されない場合は、ラウンド ロビン アルゴリズムが適用されます。</p>

4 (オプション) このプールのパーシステンス メソッドを選択します。

パーシステンス設定により、クライアント要求を処理した特定のプール メンバーなど、セッション データが追跡されて保存されます。また、同一のセッションまたは後続のセッションでは、クライアント要求が同一のプール メンバーに転送されます。

プロトコル	サポートされるパーシステンス メソッド
HTTP	なし、Cookie、ソース IP アドレス
HTTPS	なし、ソース IP アドレスと SSL セッション ID
TCP	なし、ソース IP アドレス、MSRDP
UDP	なし、ソース IP アドレス

- クライアントで特定のサイトに初めてアクセスする際に、一意の Cookie を挿入してセッションを識別するには、[Cookie] を選択します。その後の要求で Cookie が参照され、適切なサーバへの接続が維持されます。
- ソース IP アドレスに基づいてセッションを追跡するには、[ソース IP] を選択します。クライアントが、接続元アドレスのアフィニティ パーシステンスをサポートする仮想サーバへの接続を要求すると、ロード バランサは、そのクライアントが以前接続したかどうかを確認し、接続したことがあれば、クライアントを同一のプール メンバーに返します。
- [SSL セッション ID] を選択し、SSL パススルーの HTTPS トラフィック パターンを選択します。
 - SSL パススルー - クライアント -> HTTPS -> LB (SSL を終了) -> HTTPS -> サーバ
 - クライアント - HTTP -> LB -> HTTP -> サーバ

注： vRealize Automation は現在、SSL パススルーのみをサポートしています。いずれのオプションを選択しても、SSL パススルーの方式が使用されます。

- [MSRDP] を選択して、Microsoft Remote Desktop Protocol (RDP) サービスを実行している Windows のクライアントおよびサーバの間でパーシステントなセッションを維持するように設定します。MSRDP パーシステンスを有効にするための推奨シナリオは、サポートされている Windows Server を実行しているメンバーで構成されるロード バランシング プールを作成し、そこですべてのメンバーが Windows クラスタに属し、Windows セッション ディレクトリに参加するようにすることです。
- [なし] を選択すると、後続のリコールのためにセッション アクションが保存されなくなります。

5 Cookie パーシステンス設定を使用している場合は、Cookie 名を入力します。

- 6 (オプション) [モード] ドロップダウン メニューから、Cookie が挿入されるモードを選択します。

オプション	説明
挿入	NSX Edge が Cookie を送信します。 サーバが 1 つ以上の Cookie を送信すると、クライアントは もう 1 つ Cookie (サーバの Cookie + NSX Edge の Cookie) を受信します。サーバが Cookie を送信しない場合は、クライアントは NSX Edge の Cookie を受信します。
プリフィックス	サーバが Cookie を送信します。クライアントが複数の Cookie をサポートしていない場合は、このオプションを使用します。 1 つの Cookie のみをサポートする独自のクライアントを使用する独自のアプリケーションを使用している場合、Web サーバは Cookie を送信しますが、NSX Edge がその Cookie 情報をサーバ Cookie 値に (プリフィックスとして) 挿入します
アプリケーション セッション	サーバは Cookie を送信しません。その代わりに、ユーザー セッション情報を URL として送信します。 たとえば、 <code>http://mysite.com/admin/UpdateUserServlet;jsessionid=X000X0XXX0XXXX</code> が送信される場合、 <code>jsessionid</code> がユーザー セッション情報であり、パーシステンスのために使用されます。

- 7 (オプション) Cookie のパーシステンスの有効期間を秒単位で入力します。

たとえば、TCP ソース IP アドレスを使用した L7 ロード バランシングでは、既存の接続がまだ存続していても、指定された有効期間内に新しい TCP 接続が作成されないと、パーシステンス エントリがタイムアウトになります。

- 8 (オプション) [健全性チェック] タブをクリックし、[仮想サーバの健全性チェック設定の定義](#)トピックの手順に従って、NSX ロード バランサ コンポーネントでの仮想サーバの定義を続行します。

仮想サーバの健全性チェック設定の定義

[全般] タブで [カスタマイズ] オプションを選択すると、NSX ロード バランサが仮想サーバ内のプールに対して健全性チェックを実行する方法または実行するかどうかを指定できます。

デフォルトの健全性チェック プロトコルと健全性チェック ポートの設定は、[全般] タブのプロトコルとポートの設定と一致します。

関連情報については、https://www.vmware.com/support/pubs/nsx_pubs.html にある NSX 製品ドキュメントの「Create a Service Monitor」を参照してください。NSX ドキュメントでは、仮想サーバのメンバーをプール メンバーとして言及していることに注意してください。

前提条件

[仮想サーバの全般設定の定義](#)。

手順

- 1 (オプション) [健全性チェック プロトコル] ドロップダウン メニューで健全性チェック プロトコルを選択して、ロード バランサがプール メンバーの健全性を判断するためにリッスンするときの、プール メンバーへのアクセス方法を指定します。

プロトコル オプションは、[HTTP]、[HTTPS]、[TCP]、[ICMP]、[UDP]、[なし] です。

[全般] タブで指定されているデフォルト プロトコルを使用することもできます。

- 2 (オプション) [健全性チェック ポート] ボックスに値を入力して、ロード バランサが仮想サーバ メンバーまたはプール メンバーの健全性を監視するためにリッスンするポートを指定します。

NSX ドキュメントでは、仮想サーバのメンバーをプール メンバーとして言及していることに注意してください。

HTTP、HTTPS、TCP プロトコルは、UDP とポートを共有できます。たとえば、サービス 1 がポート 80 で TCP、HTTP、または HTTPS を使用する場合、サービス 2 はポート 80 で UDP を使用できます。ただし、サービス 1 がポート 80 で UDP を使用する場合、サービス 2 はポート 80 で UDP を使用することはできません。

- 3 サーバが ping される [間隔] の値を秒単位で入力します。
- 4 [タイムアウト] にサーバからの応答に受信するまでの最長時間を秒単位で入力します。
- 5 [最大試行回数] にサーバが切断していると判断するまでにサーバに ping する回数を入力します。
- 6 選択した [健全性チェック プロトコル] に基づいて追加の健全性チェック設定を指定します。
 - a サーバのステータスを検出するために使用する [メソッド] を入力します。オプションは、GET、OPTIONS、POST です。
 - b サーバのステータスを検出するためのリクエストで使用する [URL] を入力します。これが GET および POST (デフォルトで [/]) メソッド オプションに使用される URL です。
 - c [送信] テキスト ボックスで、接続の確立後にサーバに送信される文字列を入力します。
[送信] テキスト ボックスで、接続の確立後にサーバに送信される文字列を入力します。
 - d [受信] テキスト ボックスで、サーバから受信する文字列を入力します。

受信した文字列がこの定義と一致する場合にのみ、サーバが稼動状態と見なされます。

この文字列は、応答のヘッダであるか、または本文内にあります。

- 7 [詳細] タブをクリックし、[仮想サーバの詳細設定の定義](#)トピックの手順に従って、NSX ロード バランサ コンポーネントでの仮想サーバの定義を続行します。

ログ オプションを指定するには、[ロード バランサのログ オプションの定義](#)を参照してください。

仮想サーバの詳細設定の定義

[全般] タブで [カスタマイズ] オプションを選択することで、NSX ロード バランサ コンポーネントをカスタマイズして、単一のプール メンバーが認識できる同時接続数や、仮想サーバが処理できる同時接続の最大数などの設定を指定できます。

前提条件

[仮想サーバの全般設定の定義](#)。

手順

- 1 [接続制限] テキスト ボックスに値を入力して、仮想サーバが処理できる NSX の最大同時接続数を指定します。

この設定は、すべてのメンバーの接続数を考慮します。

制限を指定しない場合は、0 を入力します。

- 2 [接続速度制限] テキスト ボックスに値を入力して、1 秒間に許容できる NSX の受信接続要求の最大数を指定します。

この設定は、すべてのメンバーの接続数を考慮します。

制限を指定しない場合は、0 を入力します。

- 3 (オプション) 各仮想 IP (VIP) アドレスが、L7 ロード バランサではなく、より高速な L4 ロード バランサを使用するように指定するには、[アクセラレーションを有効化] チェック ボックスを選択します。
- 4 (オプション) [透過性] チェック ボックスを選択すると、ロード バランサ プールのメンバーは、ロード バランサを呼び出すマシンの IP アドレスを表示できるようになります。

選択しない場合、ロード バランサ プールのメンバーには、トラフィックのソース IP アドレスがロード バランサの内部 IP アドレスとして表示されます。

- 5 [最大接続数] テキスト ボックスに値を入力して、単一のプール メンバーが認識できる同時接続の最大数を指定します。

受信する接続要求数がこの値よりも大きい場合はキューに入れられ、接続が可能になると受信した順番で処理されます。

最大値を指定しない場合は値 0 を入力します。

- 6 [最小接続数] テキスト ボックスに値を入力して、単一のプール メンバーが常に許容する必要がある同時接続の最小数を指定します。

最小値を指定しない場合は値 0 を入力します。

- 7 仮想サーバの定義を終了するには、[OK] をクリックします。

- 8 ログ作成オプションを指定するには、[ロード バランサのログ オプションの定義](#)を参照してください。それ以外の場合は、[保存] または [完了] をクリックします。

ロード バランサのログ オプションの定義

ロード バランサのログ アクションのタイプを定義できます。これにより、ロード バランサのログに記録される対象が決まります。

ロード バランサ コンポーネントを定義した後、またはロード バランサ コンポーネントを定義するときに、ロード バランサのトラフィック ログを収集するためのログ レベルを指定できます。ブループリントでロード バランサ コンポーネントに定義したログ レベルは、ブループリントで定義されているすべてのロード バランサに適用されます。

ログ レベルには、デバッグ、情報、警告、エラー、重大があります。デバッグおよび情報レベルを選択した場合、ユーザーの要求がログに記録されます。一方、警告、エラー、重大レベルを選択した場合、ユーザーの要求はログに記録されません。

NSX ロード バランサのログの追加情報については、『NSX 管理ガイド』を参照してください。

前提条件

[ロード バランサ メンバーの設定の定義](#)。

手順

- 1 デザイン キャンバスで、ロード バランサ コンポーネントの [全般] タブを選択します。

2 [ログ レベル] ドロップダウン メニューから、1つ以上のログ オプションを選択します。

ロード バランサのトラフィック ログを収集するためのログ レベルを選択します。この設定は、ブループリント内のすべての NSX ロード バランサ コンポーネントに適用されます。

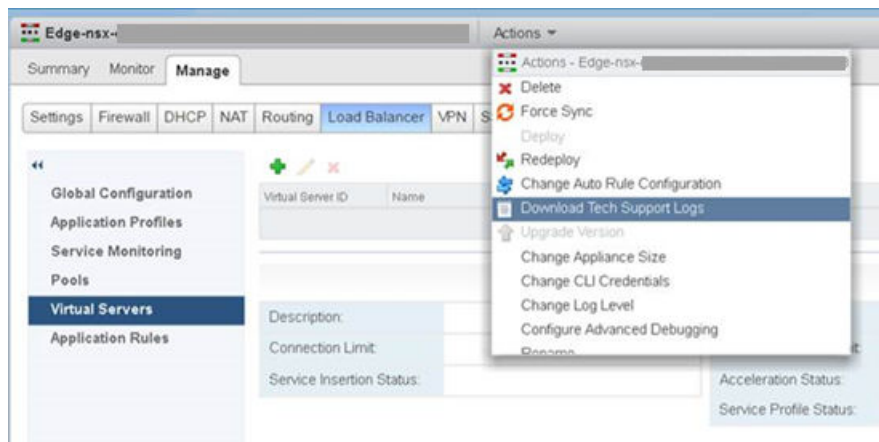
vSphere Web Client でログ設定が定義されます。

- なし
- 情報
- 緊急
- アラート
- 重大
- エラー
- 警告
- 通知
- デバッグ

3 [保存] をクリックします。

結果

vSphere Web クライアントでログの表示およびダウンロードができます。これには、https://www.vmware.com/support/pubs/nsx_pubs.htmlにある NSX 製品ドキュメントの「Download Tech Support Logs for NSX Edge」で説明されているとおり、NSX Edge の [アクション] メニューを使用します。



ブループリントでの NSX-T ロード バランサ コンポーネントの使用

1つ以上のオンデマンド NSX-T ロード バランサ コンポーネントをデザイン キャンバスに追加して、ブループリントの vSphere マシン コンポーネント設定を構成できます。

ブループリントに追加するネットワークおよびセキュリティ コンポーネントの設定は、NSX for vSphere と NSX-T の構成に基づいており、vSphere クラスターの NSX インベントリのためにデータ収集を実行済みである必要があります。ネットワークおよびセキュリティ コンポーネントは、NSX 固有のもので、vSphere マシン コンポーネントとのみ使用できます。NSX の設定の詳細については、使用しているアプリケーションに応じて、[NSX for vSphere 製品のドキュメント](#)または [NSX-T 製品のドキュメント](#)にある『管理ガイド』を参照してください。

ブループリントに追加するネットワークおよびセキュリティ コンポーネントの設定は、NSX-T の構成に基づいており、vSphere クラスターの NSX-T インベントリのためにデータ収集を実行済みである必要があります。ネットワークおよびセキュリティ コンポーネントは、NSX-T 固有のもので、vSphere マシン コンポーネントとのみ使用できます。NSX-T の設定の詳細については、[NSX-T 製品のドキュメント](#)にある『NSX-T 管理ガイド』を参照してください。

次のルールをブループリントのロード バランサ プールおよび VIP ネットワーク設定に適用します。

- プール ネットワーク プロファイルが NAT の場合、VIP ネットワーク プロファイルを NAT ネットワーク プロファイルに含めることができます。
- プール ネットワーク プロファイルがルーティングされている場合、VIP ネットワーク プロファイルには、同一のルーティング ネットワークまたは同一の外部ネットワークのみを利用できます。
- プール ネットワーク プロファイルが外部の場合、VIP ネットワーク プロファイルには、同じ外部ネットワーク プロファイルのみを利用できます。

各ロード バランサ コンポーネントには、ロード バランサ サービスとも呼ばれる複数の仮想サーバを含めることができます。ロード バランサ コンポーネントの各仮想サーバには、1つのポートとプロトコルがあります。たとえば、HTTP サービスまたは HTTPS サービスのロード バランシングが可能です。ロード バランサには、ロード バランシングしている複数のサービスを含めることができます。

NSX ロード バランサは、ロード バランサ仮想サーバを含むサービスです。

ブループリントに1つ以上のロード バランサが含まれており、ブループリントでアプリケーション隔離が有効である場合、ロード バランサ VIP が IP アドレス セットとしてアプリケーション隔離セキュリティ グループに追加されます。ブループリントに、マシン階層に関連付けられているオンデマンド セキュリティ グループが含まれており、このマシン階層がロード バランサにも関連付けられている場合、オンデマンド セキュリティ グループには、マシン層と、ロード バランサ VIP の IP アドレス セットが含まれます。

NSX-T に固有の展開およびトポロジの考慮事項の詳細については、[ネットワーク、セキュリティ、ロード バランサの構成に応じた NSX-T の展開トポロジについて](#)を参照してください。

NSX-T オンデマンド ロード バランサの追加

NSX-T オンデマンド ロード バランサ コンポーネントをデザイン キャンバスにドラッグし、ブループリントの vSphere マシン コンポーネントおよびコンテナ コンポーネントで使用するための設定を作成できます。

NSX-T ロード バランサは、負荷の配分がユーザーにとって透過的になるように、受信サービス リクエストを複数のサーバ間で均等に配分します。ロード バランシングは、最適なりソース使用率の実現、スループットの最大化、応答時間の最小化、過負荷の回避に役立ちます。

仮想 IP アドレスをプール サーバのセットにマッピングして、ロード バランシングを利用することができます。ロード バランサは仮想 IP アドレスによる TCP、UDP、HTTP、または HTTPS リクエストを受け入れ、どのプール メンバーを使用するか決定します。ロード バランサは Tier-1 論理ルーターに接続されます。

環境のニーズに応じて、既存の仮想サーバおよびプール メンバーを増やすことでネットワーク トラフィックの大きな負荷を処理できるようにロード バランサのパフォーマンスを拡大することができます。

NSX-T ロード バランサを作成してネットワーク トラフィックの動作を定義する方法については、[NSX-T 製品のドキュメント](#)にある NSX-T 管理ガイドの 論理ロード バランサ および ロード バランサ コンポーネントの構成を参照してください。

手順

1 NSX-T ロード バランサ メンバーの設定の定義

NSX-T オンデマンド ロード バランサ コンポーネントを定義することにより、ネットワーク内のプロビジョニングされた vSphere メンバー マシンまたはコンテナ マシンの間でタスク処理を分散できます。

2 NSX-T の仮想サーバの全般設定の定義

ロード バランサに単一の仮想サーバ プロトコルとポートを定義することも、追加の NSX-T ロード バランサ オプションをカスタマイズするために仮想サーバを追加することもできます。

3 NSX-T の仮想サーバの配布設定の定義

仮想サーバを定義するときに [カスタマイズ] オプションを選択すると、メンバーがトラフィックを受信するポート、NSX-T ロード バランサがそのポートにアクセスするためのプロトコル タイプ、ロード バランシングに使用するアルゴリズム、パーシステンス設定など、プール メンバーに関する情報を指定できます。

4 NSX-T の仮想サーバの健全性チェック設定の定義

[全般] タブで [カスタマイズ] オプションを選択すると、NSX-T ロード バランサが仮想サーバ内のプールに対して健全性チェックを実行する方法または実行するかどうかを指定できます。

5 NSX-T の仮想サーバの詳細設定の定義

[全般] タブで [カスタマイズ] オプションを選択することで、NSX-T ロード バランサ コンポーネントをカスタマイズして、単一のプール メンバーが認識できる同時接続数や、仮想サーバが処理できる同時接続の最大数などの設定を指定できます。

6 NSX-T ロード バランサのログ オプションの定義

ロード バランサのログ アクションのタイプを定義できます。これにより、ロード バランサのログに記録される対象が決まります。

NSX-T ロード バランサ メンバーの設定の定義

NSX-T オンデマンド ロード バランサ コンポーネントを定義することにより、ネットワーク内のプロビジョニングされた vSphere メンバー マシンまたはコンテナ マシンの間でタスク処理を分散できます。

デザイン キャンバスのブループリントにロード バランサ コンポーネントを追加するときは、ロード バランサ コンポーネントで仮想サーバ定義を作成または編集するときに、デフォルトまたはカスタムのオプションを選択できます。デフォルト オプションでは、仮想サーバのプロトコル、ポート、説明を指定し、他のすべての設定にデフォルトを使用できます。カスタム オプションでは、さらに詳細なレベルで定義できます。

ロード バランサが外部ネットワークを使用してプロビジョニングされている場合、VIP (VIP ネットワーク) とメンバー プール (メンバー ネットワーク) は、同一の既存ネットワーク上に配置されている必要があります。VIP とメンバープールが同一の外部ネットワーク上にない場合は、プロビジョニングに失敗します。

前提条件

- NSX のロード バランサを作成し、設定します。 [NSX ネットワークおよびセキュリティ構成の準備のためのチェックリスト](#)を参照してください。

- クラスタの NSX インベントリが正常に実行されたことを確認します。
vRealize Automation の NSX 構成を使用するには、データ収集を実行する必要があります。
- ネットワーク プロファイルを作成します。 [ネットワーク プロファイルの作成](#)を参照してください。
- インフラストラクチャ アーキテクトとして vRealize Automation にログインします。
- デザイン キャンバスで新規または既存のブループリントを開くには、[設計] タブを使用します。
- 少なくとも 1 つの vSphere マシン コンポーネントまたはコンテナ コンポーネントがブループリントに存在することを確認します。

手順

- 1 使用可能なネットワークおよびセキュリティ コンポーネントのリストを表示するには、[カテゴリ] セクションの [ネットワークとセキュリティ] をクリックします。

- 2 [NSX-T オンデマンド ロード バランサ] コンポーネントをデザイン キャンバス上にドラッグします。

- 3 デザイン キャンバスでコンポーネントに一意のラベルを付けるには、[ID] テキスト ボックスにコンポーネント名を入力します。

- 4 [メンバー] ドロップダウン メニューから vSphere マシン コンポーネント名またはコンテナ コンポーネント名を選択します。

リストには、アクティブなブループリントの vSphere マシン コンポーネントとコンテナ コンポーネントのみが含まれています。

- 5 [メンバー ネットワーク] ドロップダウン メニューからロード バランシング対象の NIC を選択します。

このリストには、選択した vSphere マシン メンバーに対して定義されている NIC が含まれます。

- 6 [VIP ネットワーク] ドロップダウン メニューから使用可能な仮想 IP アドレス ネットワークを選択します。たとえば、使用可能な外部ネットワークまたは NAT ネットワークを選択します。

ブループリントに複数の NSX ロード バランサおよび NSX オンデマンド ネットワーク コンポーネントを保持できますが、すべてが同じ VIP ネットワークに関連付けられている必要があります。

- 7 (オプション) [IP アドレス] テキスト ボックスに、NIC の有効な IP アドレスを入力します。

デフォルトの設定は、VIP ネットワークに関連付けられている固定 IP アドレスです。別の IP アドレスや IP アドレス範囲を指定できます。デフォルトでは、関連付けられている VIP ネットワークから次の使用可能 IP アドレスが割り当てられます。

IP アドレスのフィールドを空のままにしておくと、プロビジョニング時に関連付けられた VIP ネットワークから IP アドレスを割り当てることができます。

指定する IP アドレスが他のタイプのネットワークである場合、プロビジョニングできる展開は 1 つだけです。それ以降の展開では、IP アドレスが既に最初の展開によって使用されているため、IP アドレスの割り当てが失敗します。

- 8 仮想サーバの定義を作成するには、[新規] をクリックします。 [NSX-T の仮想サーバの全般設定の定義](#)を参照してください。

各ロード バランサ コンポーネントには、少なくとも 1 台の仮想サーバが必要です。

ログ オプションを指定するには、[NSX-T ロード バランサのログ オプションの定義](#)を参照してください。

NSX-T の仮想サーバの全般設定の定義

ロード バランサに単一の仮想サーバ プロトコルとポートを定義することも、追加の NSX-T ロード バランサ オプションをカスタマイズするために仮想サーバを追加することもできます。

たとえば、ロード バランサ コンポーネントをカスタマイズして、健全性チェック プロトコルおよびポート、アルゴリズム、パシステンス、透過性などの設定を定義することができます。

前提条件

[NSX-T ロード バランサ メンバーの設定の定義](#)。

手順

1 [仮想サーバ] ページで [全般] タブをクリックします。

2 仮想サーバのロード バランシングに使用するために、[プロトコル] ドロップダウン メニューでネットワーク トラフィック プロトコルを選択します。

プロトコル オプションは、HTTP、HTTPS、TCP、UDP です。

NSX-T ロード バランシングでは、SSL パススルー モードはサポートされませんが、代わりに SSL 終了モードが使用されます。HTTPS を指定する場合は、以下の追加情報を指定する必要があります。これらの情報は、あらかじめ NSX-T マネージャ内になければなりません。

- NSX-T 証明書インベントリ内の証明書の名前。ロード バランサは、この証明書をクライアントに提示します。
- クライアント SSL プロファイルの名前。

3 [ポート] テキスト ボックスにポート値を入力します。

選択したプロトコルによって、デフォルト ポート設定が決まります。

プロトコル	デフォルト ポート
HTTP	80
HTTPS	443
TCP	8080
UDP	デフォルトなし

HTTP、HTTPS、TCP プロトコルは、UDP とポートを共有できます。たとえば、サービス 1 がポート 80 で TCP、HTTP、または HTTPS を使用する場合、サービス 2 はポート 80 で UDP を使用できます。ただし、サービス 1 がポート 80 で UDP を使用する場合、サービス 2 はポート 80 で UDP を使用することはできません。

4 (オプション) 仮想サーバ コンポーネントの説明を入力します。

5 [配布] タブをクリックし、[NSX-T の仮想サーバの配布設定の定義](#)トピックの手順に従って、NSX-T ロード バランサ コンポーネントでの仮想サーバの定義を続行します。

NSX-T の仮想サーバの配布設定の定義

仮想サーバを定義するときに [カスタマイズ] オプションを選択すると、メンバーがトラフィックを受信するポート、NSX-T ロード バランサがそのポートにアクセスするためのプロトコル タイプ、ロード バランシングに使用するアルゴリズム、パーシステンス設定など、プール メンバーに関する情報を指定できます。

プールは、ロード バランシングされているマシンのクラスタを表します。プール メンバーは、そのクラスタ内の 1 つのマシンを表します。

デフォルトのメンバー プロトコルとメンバー ポートの設定は、[全般] ページのプロトコルとポートの設定と一致します。

メンバー マシンのプールは、ブループリント ロード バランサ コンポーネント ユーザー インターフェイスの [メンバー] オプション値に表示されます。[メンバー] エントリは、プールまたはマシンのクラスタに設定されます。

前提条件

NSX-T ロード バランサ メンバーの設定の定義。

手順

- 1 (オプション) [メンバー プロトコル] 設定は、[全般] タブで指定しているプロトコルと一致します。この設定では、プール メンバーがネットワーク トラフィックを受信する方法を定義します。
- 2 (オプション) [メンバー ポート] テキスト ボックスにポート番号を入力して、プール メンバーがネットワーク トラフィックを受信するポートを指定します。

たとえば、ロード バランサの仮想 IP アドレス (VIP) の受信要求がポート 80 で受信される場合に、その要求をプール メンバーの別のポート (ポート 8080 など) にルーティングする場合があります。

- 3 (オプション) このプールのアルゴリズム バランシング メソッドを選択します。

アルゴリズム オプションとオプションで必要となるアルゴリズム パラメータについては、次の表で説明します。

詳細については、[VMware NSX-T 製品のドキュメント](#)で、「ロード バランシング用サーバ プールの追加」を参照してください。

オプション	説明とアルゴリズム パラメータ
ROUND_ROBIN	受信したクライアント要求を、要求処理能力がある利用可能なサーバのリストに基づいて持ち回りで処理します。サーバ プール メンバーの重みは設定されていた場合でも無視されます。
WEIGHTED ROUND ROBIN	各サーバに、プール内の他のサーバに対するパフォーマンスを表す重みの値が割り当てられます。この値により、サーバに送信されるクライアント要求の数が、プール内の他のサーバと比較して決定されます。このロード バランシング アルゴリズムは、利用可能なサーバ リソース間で負荷の分散を公平にすることを重視しています。
IP-HASH	ソース IP アドレスのハッシュ、および実行されているすべてのサーバの重みの合計に基づいて、サーバを選択します。

オプション	説明とアルゴリズム パラメータ
LEASTCONN	サーバ上の既存の接続数に基づいてクライアント リクエストを複数のサーバに分散します。接続数が最も少ないサーバに新しい接続が送信されます。サーバ プール メンバーの重みは設定されていた場合でも無視されます。
WEIGHTED LEASTCONN	各サーバに、プール内の他のサーバに対するパフォーマンスを表す重みの値が割り当てられます。この値により、サーバに送信されるクライアント要求の数が、プール内の他のサーバと比較して決定されます。このロード バランシング アルゴリズムは、重みの値を使用して利用可能なサーバ リソース間で負荷の分散を公平にすることを重視しています。重みの値を設定せず、スロー スタートを有効にしている場合、値はデフォルトで 1 になります。

4 (オプション) このプールのパーシステンス メソッドを選択します。

パーシステンス設定により、クライアント要求を処理した特定のプール メンバーなど、セッション データが追跡されて保存されます。また、同一のセッションまたは後続のセッションでは、クライアント要求が同一のプール メンバーに転送されます。パーシステンス方法の詳細については、[NSX-T 製品のドキュメント](#)にある「パーシステンス プロファイルの設定」を参照してください。

- [なし] を選択すると、後続のリコールのためにセッション アクションが保存されなくなります。
- クライアントで特定のサイトに初めてアクセスする際に、一意の Cookie を挿入してセッションを識別するには、[Cookie] を選択します。その後の要求で Cookie が参照され、適切なサーバへの接続が維持されます。
- ソース IP アドレスに基づいてセッションを追跡するには、[ソース IP] を選択します。クライアントが、接続元アドレスのアフィニティ パーシステンスをサポートする仮想サーバへの接続を要求すると、ロード バランサは、そのクライアントが以前接続したかどうかを確認し、接続したことがあれば、クライアントを同一のプール メンバーに返します。

5 Cookie パーシステンスを使用している場合は、Cookie 名を入力します。

6 (オプション) [モード] ドロップダウン メニューから、Cookie が挿入されるモードを選択します。

オプション	説明
挿入	セッションを識別する一意の Cookie を作成します。
プリフィックス	既存の Cookie を追加します。
書き換え	既存の Cookie を上書きします。

7 (オプション) Cookie のパーシステンスの有効期間を秒単位で入力します。

たとえば、TCP ソース IP アドレスを使用した L7 ロード バランシングでは、既存の接続がまだ存続していても、指定された有効期間内に新しい TCP 接続が作成されないと、パーシステンス エントリがタイムアウトになります。

8 (オプション) [健全性チェック] タブをクリックし、[NSX-T の仮想サーバの健全性チェック設定の定義](#)トピックの手順に従って、NSX-T ロード バランサ コンポーネントでの仮想サーバの定義を続行します。

NSX-T の仮想サーバの健全性チェック設定の定義

[全般] タブで [カスタマイズ] オプションを選択すると、NSX-T ロード バランサが仮想サーバ内のプールに対して健全性チェックを実行する方法または実行するかどうかを指定できます。

デフォルトの健全性チェック プロトコルと健全性チェック ポートの設定は、[全般] タブのプロトコルとポートの設定と一致します。

関連情報については、[NSX-T 製品のドキュメント](#)を参照してください。NSX-T ドキュメントでは、仮想サーバのメンバーをプール メンバーとして言及していることに注意してください。

前提条件

NSX-T の仮想サーバの配布設定の定義。

手順

- 1 (オプション) [健全性チェック プロトコル] ドロップダウン メニューで健全性チェック プロトコルを選択して、ロード バランサがプール メンバーの健全性を判断するためにリッスンするときの、プール メンバーへのアクセス方法を指定します。

プロトコル オプションは、[なし]、[HTTP]、[HTTPS]、[TCP]、[ICMP]、[UDP] です。

[全般] タブで指定されているデフォルト プロトコルを使用することもできます。

- 2 (オプション) [健全性チェック ポート] ボックスに値を入力して、ロード バランサが仮想サーバ メンバーまたはプール メンバーの健全性を監視するためにリッスンするポートを指定します。

NSX ドキュメントでは、仮想サーバのメンバーをプール メンバーとして言及していることに注意してください。

HTTP、HTTPS、TCP プロトコルは、UDP とポートを共有できます。たとえば、サービス 1 がポート 80 で TCP、HTTP、または HTTPS を使用する場合、サービス 2 はポート 80 で UDP を使用できます。ただし、サービス 1 がポート 80 で UDP を使用する場合、サービス 2 はポート 80 で UDP を使用することはできません。

- 3 サーバが ping される [間隔] の値を秒単位で入力します。
- 4 [タイムアウト] にサーバからの応答に受信するまでの最長時間を秒単位で入力します。
- 5 [最大試行回数] にサーバが切断していると判断するまでにサーバに ping する回数を入力します。
- 6 HTTP プロトコルまたは HTTPS プロトコルを指定した場合は、サーバのステータスを検出するために使用する [メソッド] を入力します。
- 7 サーバのステータスを検出するためのリクエストで使用する [URL] がわかっている場合、入力します。これが GET および POST (デフォルトで [/]) メソッド オプションに使用される URL です。
- 8 送信文字列および受信文字列がわかっている場合、[送信] と [受信] テキスト ボックスにそれぞれ入力します。

[送信] テキスト ボックスで、接続の確立後にサーバに送信される文字列を入力します。

[受信] テキスト ボックスで、サーバから受信する文字列を入力します。受信した文字列がこの定義と一致する場合にのみ、サーバが稼動状態と見なされます。

- 9 [詳細] タブをクリックし、[NSX-T の仮想サーバの詳細設定の定義](#)トピックの手順に従って、NSX-T ロード バランサ コンポーネントでの仮想サーバの定義を続行します。

ログ オプションを指定するには、[NSX-T ロード バランサのログ オプションの定義](#)を参照してください。

NSX-T の仮想サーバの詳細設定の定義

[全般] タブで [カスタマイズ] オプションを選択することで、NSX-T ロード バランサ コンポーネントをカスタマイズして、単一のプール メンバーが認識できる同時接続数や、仮想サーバが処理できる同時接続の最大数などの設定を指定できます。

前提条件

[NSX-T の仮想サーバの全般設定の定義](#)。

手順

- 1 [接続制限] テキスト ボックスに値を入力して、仮想サーバが処理できる NSX-T の最大同時接続数を指定します。

この設定は、すべてのメンバーの接続数を考慮します。

制限を指定しない場合は、0 を入力します。
- 2 [接続速度制限] テキスト ボックスに値を入力して、1 秒間に許容できる NSX-T の受信接続要求の最大数を指定します。

この設定は、すべてのメンバーの接続数を考慮します。

制限を指定しない場合は、0 を入力します。
- 3 (オプション) [透過性] チェック ボックスを選択すると、ロード バランサ プールのメンバーは、ロード バランサを呼び出すマシンの IP アドレスを表示できるようになります。

選択しない場合、ロード バランサ プールのメンバーには、トラフィックのソース IP アドレスがロード バランサの内部 IP アドレスとして表示されます。
- 4 [最大接続数] テキスト ボックスに値を入力して、単一のプール メンバーが認識できる同時接続の最大数を指定します。

受信する接続要求数がこの値よりも大きい場合はキューに入れられ、接続が可能になると受信した順番で処理されます。

最大値を指定しない場合は値 0 を入力します。
- 5 仮想サーバの定義を終了するには、[OK] をクリックします。
- 6 ログ作成オプションを指定するには、[NSX-T ロード バランサのログ オプションの定義](#)を参照してください。それ以外の場合は、[保存] または [完了] をクリックします。

NSX-T ロード バランサのログ オプションの定義

ロード バランサのログ アクションのタイプを定義できます。これにより、ロード バランサのログに記録される対象が決まります。

ロード バランサのトラフィック ログを収集するためのログ レベルを指定できます。ブループリントで NSX-T ロード バランサ コンポーネントに定義したログ レベルは、ブループリントのすべてのロード バランサに適用されます。

ログ レベルには、デバッグ、情報、警告、エラー、重大があります。デバッグおよび情報レベルを選択した場合、ユーザーの要求がログに記録されます。一方、警告、エラー、重大レベルを選択した場合、ユーザーの要求はログに記録されません。

NSX-T ロード バランサのログの詳細については、[NSX-T 製品のドキュメント](#)にある『NSX-T 管理ガイド』を参照してください。

前提条件

NSX-T ロード バランサ メンバーの設定の定義

手順

- 1 デザイン キャンバスで、ロード バランサ コンポーネントの [全般] タブを選択します。
- 2 [ログ レベル] ドロップダウン メニューから、1つ以上のログ オプションを選択します。

vSphere Web Client でログ設定が定義されます。

- なし
- 緊急
- アラート
- 重大
- エラー
- 警告
- 情報
- デバッグ

- 3 ロード バランサのサイズを小規模、中規模、大規模から選択します。
- 4 [保存] をクリックし、[終了] をクリックします。

ブループリントでの NSX for vSphere セキュリティ コンポーネントの使用

NSX for vSphere セキュリティ コンポーネントをデザイン キャンバスに追加することで、構成済みの設定をブループリントの1つ以上の vSphere マシン コンポーネントで利用できるようになります。

セキュリティ グループ、タグ、およびポリシーは、NSX アプリケーションにおいて vRealize Automation の外部で構成されます。

ブループリントに追加するネットワークおよびセキュリティ コンポーネントの設定は、NSX for vSphere と NSX-T の構成に基づいており、vSphere クラスタの NSX インベントリのためにデータ収集を実行済みである必要があります。ネットワークおよびセキュリティ コンポーネントは、NSX 固有のもので、vSphere マシン コンポーネントとのみ使用できます。NSX の設定の詳細については、使用しているアプリケーションに応じて、[NSX for vSphere 製品のドキュメント](#)または [NSX-T 製品のドキュメント](#)にある『管理ガイド』を参照してください。

NSX で vSphere のコンピュート リソースのセキュリティ グループ、タグ、およびポリシーを構成して、ブループリントにセキュリティ制御機能を追加できます。データ収集の実行後に、vRealize Automation でセキュリティ構成を選択できるようになります。

NSX for vSphere セキュリティ戦略の例については、[vRealize and NSX](#) ブログの投稿を参照してください。

NSX for vSphere の既存およびオンデマンドのセキュリティ グループ

セキュリティ グループとは、たとえば、Distributed Firewall ルール、サード パーティのセキュリティ サービスの統合（ウイルス対策や侵入検知）など、一連のセキュリティ ポリシーにマップされた vSphere インベントリのアセットまたはグループ オブジェクトのコレクションです。グループ化機能を使用すると、Distributed Firewall を保護するために、仮想マシンやネットワーク アダプタなどのリソースを割り当てるカスタム コンテナを作成できます。グループの定義後に、ファイアウォール ルールにそのグループをソースまたはターゲットとして追加して保護することが可能です。

予約で指定したセキュリティ グループに加えて、ブループリントにも既存またはオンデマンドの vSphere セキュリティ グループを追加できます。

オンデマンド セキュリティ グループは 1 つ以上作成できます。1 つ以上のセキュリティ ポリシーを選択して、セキュリティ グループを構成することができます。

セキュリティ ポリシーは、セキュリティ グループに適用可能な一連のエンドポイント、ファイアウォール、およびネットワーク イントロスペクション サービスです。オンデマンド セキュリティ グループをブループリントで使用すると、セキュリティ ポリシーを vSphere 仮想マシンに追加できます。セキュリティ ポリシーを予約に直接追加することはできません。データ収集後に、コンピュート リソースに対して NSX for vSphere で定義されたセキュリティ ポリシーをブループリントで選択できるようになります。

セキュリティ グループはソース リソースで管理します。各種リソース タイプのセキュリティ グループの管理方法の詳細については、NSX for vSphere のドキュメントを参照してください。

注： アプリケーションの隔離を有効にすると、分離セキュリティ ポリシーが作成されます。アプリケーションの隔離では、論理ファイアウォールを使用して、ブループリントのアプリケーションに対するすべての受信トラフィックおよび送信トラフィックをブロックできます。App の隔離ポリシーを含むブループリントによりプロビジョニングされたコンポーネント マシンは相互に通信できますが、他のセキュリティ グループが、アクセスを許可するセキュリティ ポリシーを備えたブループリントに追加されない限り、ファイアウォール外部には接続できません。

ブループリントに 1 つ以上のロード バランサが含まれており、ブループリントでアプリケーション隔離が有効である場合、ロード バランサ VIP が IP アドレス セットとしてアプリケーション隔離セキュリティ グループに追加されます。ブループリントに、マシン階層に関連付けられているオンデマンド セキュリティ グループが含まれており、このマシン階層がロード バランサにも関連付けられている場合、オンデマンド セキュリティ グループには、マシン層と、ロード バランサ VIP の IP アドレス セットが含まれます。

NSX for vSphere の既存のセキュリティ タグ

NSX for vSphere の既存のセキュリティ タグ コンポーネントを追加できます。セキュリティ タグは、グループ化メカニズムとして使用できる修飾子オブジェクトまたは分類エントリです。作成するセキュリティ グループにオブジェクトを追加するときに、オブジェクトが満たす必要のある基準を定義します。これにより、サポートされている多くのパラメータを使用してフィルタ基準を定義し、検索条件に一致するマシンを追加できるようになります。たとえば、指定されたセキュリティ タグを使用してタグ化されているすべてのマシンを、セキュリティ グループに追加できます。

NSX for vSphere の既存のセキュリティ グループ コンポーネントの追加

既存の NSX for vSphere セキュリティ グループ コンポーネントをデザイン キャンバスに追加すると、その設定をブループリント内の 1 つ以上の vSphere マシン コンポーネントに関連付けることができるようになります。

既存のセキュリティ グループ コンポーネントを使用して NSX セキュリティ グループをデザイン キャンバスに追加し、その設定を vSphere マシン コンポーネント、および vSphere に属する ソフトウェア または XaaS コンポーネントで使用するよう構成できます。

デフォルトでは、ブループリントの作成時に、現在のテナントに適用可能なセキュリティ グループが公開されます。具体的には、セキュリティ グループは、関連付けられたエンドポイントの予約が現在のテナントにある場合に使用可能になります。テナント アクセスの制御方法の詳細については、[vRealize Automation でのセキュリティ オブジェクトへのテナント アクセスの制御](#)を参照してください。

前提条件

- NSX のセキュリティ グループを作成および構成します。vRealize Automation の構成 の NSX 構成チェックリストおよび [NSX for vSphere 製品のドキュメント](#) にある『NSX for vSphere 管理ガイド』を参照してください。
- クラスタの NSX インベントリが正常に実行されたことを確認します。
vRealize Automation の NSX 構成を使用するには、データ収集を実行する必要があります。
- セキュリティ コンポーネントの概念を確認します。[ブループリントでの NSX for vSphere セキュリティ コンポーネントの使用](#)を参照してください。
- インフラストラクチャ アーキテクトとして vRealize Automation にログインします。
- デザイン キャンバスで新規または既存のブループリントを開くには、[設計] タブを使用します。

手順

- 1 使用可能なネットワークおよびセキュリティ コンポーネントのリストを表示するには、[カテゴリ] セクションの [ネットワークとセキュリティ] をクリックします。
- 2 [既存のセキュリティ グループ] コンポーネントをデザイン キャンバス上にドラッグします。
- 3 [セキュリティ グループ] ドロップダウン メニューから既存のセキュリティ グループを選択します。
- 4 [OK] をクリックします。
- 5 ブループリントをドラフトとして保存するには [保存] を、ブループリントの設定を継続するには [完了] をクリックします。

結果

vSphere マシン コンポーネントの [セキュリティ] タブでセキュリティ設定を追加できます。

NSX for vSphere の既存のセキュリティ タグ コンポーネントの追加

NSX for vSphere の既存のセキュリティ タグ コンポーネントをブループリントのデザイン キャンバスに追加すると、その設定をブループリント内の 1 つ以上の vSphere コンポーネントに関連付けられるようになります。

セキュリティ タグ コンポーネントを使用して vSphere の既存のセキュリティ タグをデザイン キャンバスに追加し、その構成を vSphere マシン コンポーネント、および vSphere に属する ソフトウェア コンポーネントで使用するよう構成できます。

デフォルトでは、ブループリントの作成時に、現在のテナントに適用可能なセキュリティ タグが公開されます。具体的には、セキュリティ タグは、関連付けられたエンドポイントの予約が現在のテナントにある場合に使用可能になります。テナント アクセスの制御方法の詳細については、[vRealize Automation でのセキュリティ オブジェクトへのテナント アクセスの制御](#)を参照してください。

複数のネットワークおよびセキュリティ コンポーネントをデザイン キャンバスに追加できます。

詳細については、[ブループリントでの NSX for vSphere セキュリティ コンポーネントの使用](#)を参照してください。

前提条件

- NSX のセキュリティ タグを作成および構成します。vRealize Automation の構成 の NSX 構成チェックリストおよび [NSX for vSphere 製品のドキュメント](#) にある『NSX for vSphere 管理ガイド』を参照してください。
- クラスタの NSX インベントリが正常に実行されたことを確認します。
vRealize Automation の NSX 構成を使用するには、データ収集を実行する必要があります。
- インフラストラクチャ アーキテクトとして vRealize Automation にログインします。
- デザイン キャンバスで新規または既存のブループリントを開くには、[設計] タブを使用します。

手順

- 1 使用可能なネットワークおよびセキュリティ コンポーネントのリストを表示するには、[カテゴリ] セクションの [ネットワークとセキュリティ] をクリックします。
- 2 [既存のセキュリティ タグ] コンポーネントをデザイン キャンバス上にドラッグします。
- 3 [セキュリティ タグ] テキスト ボックスをクリックし、既存のセキュリティ タグを選択します。
- 4 [OK] をクリックします。
- 5 ブループリントをドラフトとして保存するには [保存] を、ブループリントの設定を継続するには [完了] をクリックします。

結果

vSphere マシン コンポーネントの [セキュリティ] タブでセキュリティ設定を追加できます。

オンデマンド セキュリティ グループ コンポーネントの追加

オンデマンド NSX セキュリティ グループ コンポーネントをデザイン キャンバスに追加して、その設定をブループリント内の 1 つ以上の vSphere マシン コンポーネント、または使用可能なその他のコンポーネント タイプに関連付けることができます。

オンデマンド セキュリティ グループを作成する場合は、セキュリティ ポリシーを追加してグループを作成します。セキュリティ ポリシーはグローバルに公開することも、デフォルトで非表示にすることもできます。ポリシーは、関連付けられている NSX エンドポイントがテナントに予約を持っている場合に、そのテナントにのみ公開されます。

デフォルトでは、ブループリントの作成時に、現在のテナントに適用可能なセキュリティ グループが公開されます。具体的には、セキュリティ グループは、関連付けられたエンドポイントの予約が現在のテナントにある場合に使用可能になります。テナント アクセスの制御方法の詳細については、[vRealize Automation でのセキュリティ オブジェクトへのテナント アクセスの制御](#)を参照してください。

前提条件

- NSX のセキュリティ ポリシーを作成および構成します。『NSX 管理ガイド』を参照してください。
- クラスタの NSX インベントリが正常に実行されたことを確認します。
vRealize Automation の NSX 構成を使用するには、データ収集を実行する必要があります。
- インフラストラクチャ アーキテクトとして vRealize Automation にログインします。

- セキュリティ コンポーネントの概念を確認します。 [ブループリントでの NSX for vSphere セキュリティ コンポーネントの使用](#) を参照してください。
- デザイン キャンバスで新規または既存のブループリントを開くには、[設計] タブを使用します。

手順

- 1 使用可能なネットワークおよびセキュリティ コンポーネントのリストを表示するには、[カテゴリ] セクションの [ネットワークとセキュリティ] をクリックします。
- 2 [オンデマンド セキュリティ グループ] コンポーネントをデザイン キャンバス上にドラッグします。
- 3 名前と説明（説明は任意）を入力します。
- 4 [セキュリティ ポリシー] 領域の [追加] アイコンをクリックして使用可能なセキュリティ ポリシーを選択することにより、1 つ以上のセキュリティ ポリシーを追加します。
- 5 [OK] をクリックします。
- 6 ブループリントをドラフトとして保存するには [保存] を、ブループリントの設定を継続するには [完了] をクリックします。

結果

vSphere マシン コンポーネントの [セキュリティ] タブでセキュリティ設定を追加できます。

ブループリントでの NSX-T セキュリティ コンポーネントの使用

NSX-T ネットワーク セキュリティ コンポーネントをデザイン キャンバスに追加することで、構成済みの設定をブループリントの 1 つ以上の関連付けられている vSphere マシン コンポーネントで利用できるようになります。

NSX-T の既存の NS グループを使用すると、Distributed Firewall を保護するために、仮想マシンやネットワーク アダプタなどのリソースを割り当てることができます。

NSX-T で vSphere のコンピュート リソースの NS グループを構成して、ブループリントにセキュリティ制御機能を追加できます。データ収集の実行後に、vRealize Automation でセキュリティ構成を選択できるようになります。ファイアウォール ルールのソースまたはターゲットとして、NSX-T の既存の NS グループ コンポーネントをブループリントに追加できます。

NSX-T NS セキュリティ グループは、vRealize Automation の外部の NSX-T アプリケーションで管理されます。NS グループの管理の詳細については、NSX-T 製品ドキュメントを参照してください。

ブループリントに追加するネットワークおよびセキュリティ コンポーネントの設定は、NSX for vSphere と NSX-T の構成に基づいており、vSphere クラスタの NSX インベントリのためにデータ収集を実行済みである必要があります。ネットワークおよびセキュリティ コンポーネントは、NSX 固有のもので、vSphere マシン コンポーネントとのみ使用できます。NSX の設定の詳細については、使用しているアプリケーションに応じて、[NSX for vSphere 製品のドキュメント](#)または [NSX-T 製品のドキュメント](#)にある『管理ガイド』を参照してください。

NSX-T エンドポイントが含まれているブループリントを展開すると、NSX-T ネットワーク、セキュリティ、およびロード バランサのコンポーネントや、NSX-T エンドポイントの関連付けられている vSphere マシン コンポーネントなど、展開に含まれるすべての NSX-T コンポーネントにタグが割り当てられます。タグは展開に一意で、初期導入およびそれ以降に展開で実行した後続のアクションのコンポーネントに関連付けられます。タグの名前は、展開の名前と同じです。

アプリケーションの隔離が有効の場合、ルールを持つ新しいファイアウォール セクションが展開用に作成されます。アプリケーションの隔離では、論理ファイアウォールを使用して、ブループリントのアプリケーションに対するすべての受信トラフィックおよび送信トラフィックをブロックできます。アプリケーションの隔離ポリシーを含むブループリントによりプロビジョニングされたコンポーネント マシンは相互に通信できますが、他の NS グループが、アクセスを許可するセキュリティ ルールを備えたブループリントに追加されない限り、ファイアウォール外部には接続できません。

ブループリントに 1 つ以上のロード バランサが含まれており、ブループリントでアプリケーション隔離が有効である場合、ロード バランサ VIP が IP アドレス セットとしてアプリケーション隔離セキュリティ グループに追加されます。ブループリントに、マシン階層に関連付けられているオンデマンド セキュリティ グループが含まれており、このマシン階層がロード バランサにも関連付けられている場合、オンデマンド セキュリティ グループには、マシン層と、ロード バランサ VIP の IP アドレス セットが含まれます。

NSX-T の場合、アプリケーションの隔離は、作成される唯一のオンデマンド NS グループです。ロード バランサの VIP と NAT の一対多ネットワークの外部 IP アドレスを含む IP アドレス セットが含まれています。

NSX-T に固有の展開およびトポロジの考慮事項の詳細については、[ネットワーク、セキュリティ、ロード バランサの構成に応じた NSX-T の展開トポロジについて](#)を参照してください。

NSX-T NSGroup コンポーネントの追加

NSX-T の既存の NS グループ コンポーネントをデザイン キャンバスに追加し、その設定を vSphere マシン コンポーネントや、ソフトウェアおよびネットワーク コンポーネントなどの他の関連したコンポーネントで使用するよう設定できます。

NSX-T NS グループには、IP セット、MAC セット、論理ポート、論理スイッチおよび他の NS グループの組み合わせを含めることができます。NSGroup はファイアウォール ルールでソースおよびターゲットとして指定できます。NSGroup の特徴については、[NSX-T 製品のドキュメント](#)にある NSX-T 管理ガイドの NSGroup の作成を参照してください。

注： NSGroup セキュリティは、NSX-T で管理する不透明なネットワークに接続された仮想マシンに適用されません。仮想マシンが vSphere dvPortGroup に接続されている場合、そのネットワークに対してマイクロセグメンテーションは使用できません。

デフォルトでは、ブループリントの作成時または編集時に、現在のテナントに適用される NSGroup が公開されます。セキュリティ グループは、関連付けられたエンドポイントの予約が現在のテナントにある場合に使用可能になります。テナント アクセスの制御方法の詳細については、[vRealize Automation でのセキュリティ オブジェクトへのテナント アクセスの制御](#)を参照してください。

前提条件

- NSX-T で NS グループを作成し、設定します。 [NSX ネットワークおよびセキュリティ構成の準備のためのチェックリスト](#)を参照してください。
- クラスタの NSX インベントリが正常に実行されたことを確認します。
vRealize Automation の NSX 構成を使用するには、データ収集を実行する必要があります。
- セキュリティ コンポーネントの概念を確認します。 [ブループリントでの NSX-T セキュリティ コンポーネントの使用](#)を参照してください。
- インフラストラクチャ アーキテクトとして vRealize Automation にログインします。

- デザイン キャンバスで新規または既存のブループリントを開くには、[設計] タブを使用します。

手順

- 1 使用可能なネットワークおよびセキュリティ コンポーネントのリストを表示するには、[カテゴリ] セクションの [ネットワークとセキュリティ] をクリックします。
- 2 [NSX-T NSGroup] コンポーネントをデザイン キャンバス上にドラッグします。
- 3 ドロップダウン メニューから NSGroup を選択します。
- 4 要求された場合は、関連付けられたエンドポイントを入力します。
- 5 ブループリントをドラフトとして保存するには [保存] を、ブループリントの設定を継続するには [完了] をクリックします。

結果

vSphere マシン コンポーネントの [セキュリティ] タブでセキュリティ設定を追加できます。

ネットワークおよびセキュリティ コンポーネントの関連付け

ネットワークおよびセキュリティ コンポーネントをデザイン キャンバス上にドラッグすると、それらの設定がブループリントのマシン コンポーネント構成で使用可能になります。マシンのネットワークおよびセキュリティ設定を定義したら、必要に応じてロード バランサ コンポーネントの設定を関連付けることができます。

NSX ネットワークまたはセキュリティ コンポーネントをデザイン キャンバスに追加して、使用可能な設定を定義した後、キャンバスで vSphere マシン コンポーネントの [ネットワーク] および [セキュリティ] タブを開き、その設定を構成できます。

オンデマンド NAT ネットワーク コンポーネントをデザイン キャンバス上にドラッグして、ブループリントで vSphere マシン コンポーネントまたは NSX ロード バランサ コンポーネントに関連付けることができます。

ブループリントに追加するネットワークおよびセキュリティ コンポーネントの設定は、NSX for vSphere と NSX-T の構成に基づいており、vSphere クラスタの NSX インベントリのためにデータ収集を実行済みである必要があります。ネットワークおよびセキュリティ コンポーネントは、NSX 固有のもので、vSphere マシン コンポーネントとのみ使用できます。NSX の設定の詳細については、使用しているアプリケーションに応じて、[NSX for vSphere 製品のドキュメント](#)または [NSX-T 製品のドキュメント](#)にある『管理ガイド』を参照してください。

注： ブループリントに1つ以上のロード バランサが含まれており、ブループリントでアプリケーション隔離が有効である場合、ロード バランサ VIP が IP アドレス セットとしてアプリケーション隔離セキュリティ グループに追加されます。ブループリントに、マシン階層に関連付けられているオンデマンド セキュリティ グループが含まれており、このマシン階層がロード バランサにも関連付けられている場合、オンデマンド セキュリティ グループには、マシン層と、ロード バランサ VIP の IP アドレス セットが含まれます。

Edge (ソース ポート) の外部 IP アドレスから NAT ネットワーク コンポーネント (ターゲット ポート) のプライベート IP アドレスへのマッピングを、NAT ルールを使用して TCP または UDP ポートで許可する方法については、[NSX for vSphere の NAT ルールの作成と使用](#)または [NSX-T の NAT ルールの作成と使用](#)を参照してください。

NSX-T に固有の展開およびトポロジの考慮事項の詳細については、[ネットワーク、セキュリティ、ロード バランサの構成に応じた NSX-T の展開トポロジについて](#)を参照してください。

OVF からプロビジョニングするブループリントの構成

OVF を使用して、vSphere マシンのプロパティとハードウェア設定を定義できます。これは、通常は vRealize Automation のブループリント構成ページで定義するか、vRealize Automation REST API または vRealize CloudClient を使用してプログラムで定義されます。

OVF から設定をインポートして、イメージ コンポーネント プロファイルに値セットを定義することもできます。パラメータ化されたブループリントは、イメージおよびサイズ コンポーネント プロファイル タイプを使用します。

OVF は、仮想マシン向けのソフトウェア アプリケーションをパッケージおよび配布するためのオープンソース規格です。

OVF のプロビジョニングは、ソース マシンが vCenter Server でホストされている仮想マシン テンプレートではなく、サーバまたは Web サイトでホストされている OVF テンプレートであるという点を除けば、クローン作成と同様です。

OVF ファイルは通常、単一の仮想マシンまたは仮想アプライアンスの記述に使用されます。ここには、仮想ディスク イメージ ファイルと仮想ハードウェアの記述の形式についての情報が含まれていることもあります。これらは、ディスク イメージに含まれる OS またはアプリケーションの実行をエミュレートする際に必要になります。OVA ファイルは、OVF 記述子ファイル、オプションの生成および証明書ファイルなどの関連ファイルも含め、仮想マシンの記述に使用されるファイルを含んだ仮想アプライアンス パッケージです。

ImportOvfWorkflow プロビジョニング オプションは、ブループリントの定義時に vSphere マシン コンポーネントで使用できます。プロパティ ディクショナリにイメージ コンポーネント プロファイルの値セットを定義する際にも使用できます。

次のタイプの情報を記述する OVF には、ブループリントの設定を追加できます。

- 最小 CPU、メモリ、およびストレージ割り当て。
- ユーザーが設定可能なカスタム プロパティ。
- ブループリントのパラメータ化のためのコンポーネント プロファイル設定。

複数マシンの OVF および OVA はサポートされていません。

重要な考慮事項には、次のものがあります。

- OVF ファイルと OVA パッケージがサポートされます。
- ホストされる OVF または OVA が配備された HTTP サーバに対するユーザー名およびパスワードによる基本認証がサポートされます。ブループリントで指定されている URL は検証されます。
- OVF および OVA ファイルは、vCenter Server からデータ収集されません。
- EBS サブスクリプションがサポートされます。
- ブループリントにユーザー設定可能な OVF 設定をインポートする際は、カスタム プロパティを定義できます。
- vSphere マシン プロビジョニングの申請時に OVF インポートから取得した設定は、追加、変更、削除が可能です。
- マシンの再構成中に、設定を追加、変更、または削除することができます。

OVF を使用した、vSphere コンポーネントのブループリント設定の定義

OVF から設定をインポートして、vRealize Automation ブループリントで vSphere マシン コンポーネントを設定するプロセスを簡素化できます。

この手順は、vRealize Automation ブループリントの作成プロセスについて基本的な知識があることを前提としています。

前提条件

- インフラストラクチャ アーキテクトとして vRealize Automation にログインします。
- [マシンのブループリントの設定](#)で指定されている残りの前提条件を満たしている。

手順

- 1 [設計] - [ブループリント] を選択します。
- 2 [新規] アイコン (+) をクリックします。
- 3 ブループリントの名前と説明を入力し、[OK] をクリックします。
- 4 [カテゴリ] 領域で[マシン タイプ]をクリックし、[vSphere (vCenter) マシン] コンポーネントをデザイン キャンバスにドラッグします。
- 5 [ビルド情報] タブをクリックし、次のオプションを指定します。
 - [ブループリントのタイプ]: サーバ
 - [アクション]: 作成
 - [プロビジョニング ワークフロー]: ImportOvfWorkflow

ImportOvfWorkflow 設定を使用すると、[URL] オプションが利用可能になります。

The screenshot shows the 'Design Canvas' interface. A 'vSphere (vCenter) Machine' component is placed on the canvas. Below the canvas, the configuration panel for 'vSphere__vCenter__Machine_1' is displayed. The 'Build Information' tab is selected, showing the following settings:

- Blueprint type: Server
- Action: Create
- Provisioning workflow: ImportOvfWorkflow
- * URL: (highlighted with an orange box)
- CONF... button (highlighted with a blue box)
- Authentication needed: ☐
- Use proxy: ☐

- 6 OVF の場所を指定します。
 - OVF URL へのパスを `https://server/folder/name.ovf` または `name.ova` の形式で入力します。

OVF をホストしているサーバで認証を有効にする場合は、ユーザーの認証に使用する認証情報を入力します。

- OVF が Web サイトにホストされていて、Web サイトへのアクセスに使用するプロキシ エンドポイントを作成している場合は、[プロキシを使用] を選択し、使用可能なプロキシ エンドポイントを選択します。

7 [構成] をクリックします。

注： 認証エラー メッセージが表示される場合は、OVF がホストされているサーバに対する認証情報が必要です。この場合、[認証が必要] チェック ボックスを選択し、OVF が含まれている HTTP サーバでの認証に必要な [ユーザー名] と [パスワード] の認証情報を入力し、[構成] を再度クリックします。

[構成] オプションのウィザードが開き、カスタム プロパティとして OVF からインポートされる、ユーザー設定が可能なすべてのプロパティと値が表示されます。インポートする設定可能プロパティがない場合は、空で表示されます。

- a ウィザードを使用して、インポートされるデフォルト値を受け入れるか、インポートの前にブループリントに対してこれらの値を変更します。
- b [OK] をクリックしてプロパティと値をインポートします。

OVF テンプレートのユーザー設定が可能なすべてのプロパティは、VMware.Ovf で始まる編集可能な vRealize Automation カスタム プロパティとしてブループリントにインポートされます。その他のプロパティは、インポート後に編集されることはない非表示のプロパティとしてインポートされます。

8 [マシン リソース] タブをクリックして [CPU]、[メモリ (MB)]、および [ストレージ (GB)] オプションの最小値エントリに反映される、OVF インポートの結果を表示します。

インポート後、これらの値は任意に変更できます。

9 [ストレージ] タブをクリックして、OVF のインポートの結果を表示します。

10 [プロパティ] - [カスタム プロパティ] タブの順にクリックして、OVF のインポート結果を表示します。

11 [保存] をクリックします。

次のステップ

ブループリント設定の定義を続行するか、[完了] をクリックします。

OVF を使用したコンポーネント プロファイルへのイメージの値セットの定義

OVF から設定をインポートして、パラメータ化された vRealize Automation ブループリントで使用するイメージ コンポーネント プロファイルに 1 つ以上の値セットを作成できます。

Image コンポーネント プロファイルに値セットの定義をインポートすると、ブループリント内の vSphere マシン コンポーネントのコンポーネント プロファイルに 1 つまたは複数の値セットを追加できるようになります。ユーザーがカタログ アイテムを申請すると、使用可能な Image を選択して、イメージの値セットで定義されているパラメータを使用した展開が可能になります。

OVF をインポートすると、ユーザーが設定可能なプロパティおよび OVF の値は、値セットのカスタム プロパティとしてインポートされません。イメージの値セットに関連してインポートされた OVF からの新しいカスタム プロパティを使用する場合は、vSphere マシン コンポーネントまたはブループリント全体で新しいカスタム プロパティを手動で定義する必要があります。パラメータ化されたブループリントで作成されたカスタム プロパティは、各コンポーネント プロファイルのイメージの値セットに適用できる必要があります。

注： vRealize Automation の OVF のカスタム プロパティは、vSphere の OVF カスタム プロパティには適用されません。vRealize Automation にイメージの値セットを 1 つ、vSphere にイメージの値セット 1 つを作成することを検討してください。

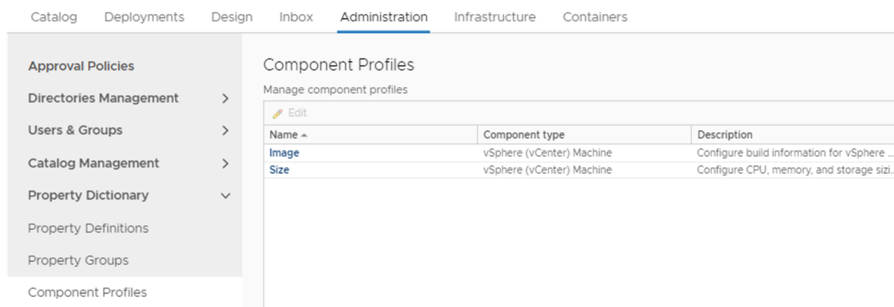
ブループリントのパラメータ化のコンポーネント プロファイルの使用に関する詳細については、[ブループリントのパラメータ化について](#)を参照してください。

前提条件

- テナント管理者および IaaS 管理者のアクセス権を持つ管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [プロパティ ディクショナリ] - [コンポーネント プロファイル] の順に選択します。



- 2 [名前] 列で [イメージ] をクリックします。

指定されたイメージ コンポーネントのプロパティに関する情報が表示されます。

- 3 [値セット] タブをクリックします。

- 4 新しい値を定義するには、[新規] をクリックし、Image を設定します。

a [表示名] フィールドでは、ValueSet 区切り記号に付加する値、たとえば **ProdOVF** を入力します。

b [名前] テキスト ボックスでは、表示されるデフォルト値を受け入れるか、カスタム名を入力します。

c [説明] テキスト ボックスには、**シナリオ A のクローンを作成するためのビルド設定**などの説明を入力します。

d [ステータス] ドロップダウン メニューでは、[有効] または [無効] を選択します。

カタログ プロビジョニングの申請フォームで値が表示されるように設定する場合は、[有効] を選択します。

e [作成] ビルド アクションを選択します。

f ブループリントのタイプとして、[サーバ] または [デスクトップ] を選択します。

g [ImportOvfWorkflow] プロビジョニング ワークフローを選択します。

- h OVF URL へのパスを `https://server/folder/name.ovf` または `name.ova` の形式で入力します。
- i OVF をホストしているサーバで認証を有効にする場合は、ユーザーの認証に使用する認証情報を入力します。
- j OVF が Web サイトにホストされていて、Web サイトへのアクセスに使用するプロキシ エンドポイントを作成している場合は、[プロキシを使用] を選択し、使用可能なプロキシ エンドポイントを選択します。

5 [保存] をクリックします。

6 設定が完了したら、[完了] をクリックします。

次のステップ

イメージを作成し、イメージの値セットを定義する OVF をインポートした後は、イメージをブループリントの vSphere マシン コンポーネントに追加できます。

ブループリントでのコンテナ コンポーネントの使用

ブループリントでコンテナ コンポーネントを構成して使用することができます。

コンテナ管理者が vRealize Automation のコンテナ でコンテナの定義を作成した後、コンテナ アーキテクトは、デザイン キャンバスで vRealize Automation ブループリントのコンテナ コンポーネントを追加したり構成したりすることができます。

コンテナ コンポーネントの設定

vRealize Automation のコンテナ コンテナ コンポーネントに関するブループリントの設定とオプションは、vRealize Automation デザイン キャンバスで構成できます。

[全般] タブ

ブループリントのコンテナ コンポーネントに関する一般的な設定は、デザイン キャンバスで構成します。

表 3-33. [全般] タブの設定

設定	説明
[名前]	ブループリントのコンテナ コンポーネントの名前を入力します。
[説明]	他のアーキテクトが利用できるよう、コンテナ コンポーネントのサマリを記載します。
[イメージ]	プライベート レジストリや Docker Hub レジストリなど、管理対象のレジストリにおけるイメージのフル ネームを入力します（例：registry.hub.docker.com/library/python）。
[コマンド]	特定のイメージに適用するコマンドを入力します（python app.py など）。このコマンドは、コンテナのプロビジョニング プロセスの開始時に実行されます。
[リンク]	単一のホスト上または複数のホスト間でコンテナ同士を接続するもう一つの方法としてリンクがあります。このコンテナのリンク先となるサービスを入力してください（redis、datadog など）。

[ネットワーク] タブ

ブループリントのコンテナ コンポーネントに関するネットワーク設定は、デザイン キャンバスで設定します。

コンテナはネットワークに接続することができます。デザイン キャンバスでは、このネットワークが、コンテナのネットワーク コンポーネントとして表されます。利用可能なネットワークに関する情報は、コンテナ コンポーネント フォームの [ネットワーク] ページで指定します。

表 3-34. [ネットワーク] タブの設定

設定	説明
[ネットワーク]	<p>選択したイメージに対して定義する既存のネットワークを指定します。新しいネットワークを作成することもできます。</p> <p>ネットワーク コンテナ コンポーネントをデザイン フォームに追加するとき、ここに指定したネットワークが、選択できる有効なオプションとして一覧表示されます。</p>
[ポート バインディング]	<p>選択ネットワークのポート バインディングを指定します。ポート バインディングは、プロトコル ホスト、ホスト ポート、コンテナ ポートから成ります。</p>
[すべてのポートを公開]	<p>コンテナ イメージに使用されているポートをすべてのユーザーに公開する場合は、このチェック ボックスを選択します。</p>
[ホスト名]	<p>コンテナのホスト名を指定します。名前を指定しなかった場合、ブループリントのコンテナ コンポーネントの名前がデフォルト値として使用されます。</p>
[ネットワーク モード]	<p>コンテナのネットワーク スタックを指定します。値を指定しなかった場合、ブリッジ ネットワーク モードでコンテナが構成されます。</p>

[ストレージ] タブ

ブループリントのコンテナ コンポーネントに関するストレージ設定はデザイン キャンバスで構成します。

表 3-35. [ストレージ] タブの設定

設定	説明
[ボリューム]	<p>コンテナで使用するためにホストからマッピングするストレージ ボリュームを指定します。</p>
[継承元ボリューム]	<p>別のコンテナから継承するストレージ ボリュームを指定します。</p>
[作業ディレクトリ]	<p>コマンド実行の起点となるディレクトリを指定します。</p>

[ポリシー] タブ

ブループリントのコンテナ コンポーネントに関するポリシー設定（展開ポリシー、アフィニティ制約など）は、デザイン キャンバスで設定します。

表 3-36. [ポリシー] タブの設定

設定	説明
[展開ポリシー]	このコンテナの展開に使用する一連のホストに関してのプリファレンスを設定する展開ポリシーを指定します。ホスト、ポリシー、コンテナの定義に展開ポリシーを関連付けることで、コンテナを展開するときのホスト、ポリシー、割り当てのプリファレンスを設定することができます。展開ポリシーは、vRealize Automation の [コンテナ] タブを使用して追加できます。
[クラスタのサイズ]	このコンテナからクラスタとして生成するインスタンスの数を指定します。
[再起動ポリシー]	終了時にコンテナを再起動する方法について、再起動ポリシーを指定します。
[最大再起動]	失敗時に再起動するポリシーを選択した場合は、再起動の最大数を指定できます。
[CPU 共有]	プロビジョニングしたリソースに割り当てられる CPU 共有の数を指定します。
[メモリ リミット]	0 から配置ゾーンで使用可能なメモリまでの範囲で数値を指定します。これは、この配置に含まれるリソースで利用できるメモリの合計になります。0 は無制限を意味します。
[メモリ スワップ]	合計メモリの制限。
[アフィニティ制約]	<p>同じホストまたは異なるホストに複数のコンテナをプロビジョニングした場合のルールを定義します。</p> <ul style="list-style-type: none"> ■ アフィニティ タイプ <p>アンチアフィニティの場合、複数のコンテナがそれぞれ異なるホストに配置されます。それ以外の場合は、同じホストにコンテナが配置されます。</p> ■ サービス <p>ドロップダウン メニューから選択できるサービス名は、[全般] タブの [名前] フィールドに指定されたコンテナ コンポーネントの名前と一致します。</p> ■ 制約 <p>制約が満たされなかったときにプロビジョニングを失敗させる場合は、強い制約を指定します。制約が満たされなかったときでもプロビジョニングを続行する場合は、弱い制約を指定します。</p>

[環境]タブ

ブループリントのコンテナ コンポーネントに関する環境設定（プロパティ バインドなど）は、デザイン キャンバスで設定します。

表 3-37. [環境] タブの設定

設定	説明
[名前]	変数の名前。
[バインド]	テンプレートの一部になっている別のプロパティに変数をバインドします。バインドを選択する際には、値を <code>_resource~TemplateComponent~TemplateComponentProperty</code> 構文で入力する必要があります。
[値]	環境変数の値です。バインドを選択した場合は、バインドするプロパティの値になります。

[プロパティ] タブ

ブループリントのコンテナ コンポーネントに関する個々のカスタム プロパティとそのグループは、デザイン キャンバスで設定します。

[プロパティ] グループ タブを選択し、[追加] をクリックすると、次のオプションが利用できます。

- コンテナ ホストのプロパティと証明書認証
- コンテナ ホストのプロパティとユーザー/パスワード認証

その他のプロパティ グループが定義されている場合、それらも一覧表示されます。

[カスタム プロパティ] タブを選択し、[追加] をクリックすれば、個々のカスタム プロパティをコンテナ コンポーネントに追加できます。

表 3-38. カスタム プロパティの [プロパティ] タブの設定

設定	説明
[名前]	カスタム プロパティの名前を入力するか、ドロップダウン メニューから使用可能なカスタム プロパティを選択します。
[値]	カスタム プロパティ名に関連する値を入力するか、編集します。
[暗号化済み]	たとえば、値がパスワードの場合に、プロパティ値を暗号化するように選択できます。
[オーバーライド可能]	次回以降にプロパティを使用する人がプロパティ値をオーバーライドできるように指定できます。[申請に表示] を選択した場合、ビジネス ユーザー（通常はアーキテクト）がカタログ アイテムを申請するときにプロパティ値を確認して編集することが可能になります。
[申請に表示]	プロパティ名とその値をエンド ユーザーに公開する場合は、マシン プロビジョニングの申請時に申請フォームでプロパティを表示するように選択できます。ユーザーが値を指定できるようにするには、[オーバーライド可能] も選択する必要があります。

[健全性の構成] タブ

ブループリントのコンテナ コンポーネントに関する健全性構成モードはデザイン キャンバスで指定します。

表 3-39. [健全性の構成] タブの設定

モード設定	説明
[なし]	デフォルト。健全性チェックは構成されません。
[HTTP]	[HTTP] を選択する場合は、アクセスする API と使用する HTTP メソッドおよびバージョンを指定する必要があります。API は相対指定です。コンテナのアドレスを入力する必要はありません。また、操作のタイムアウト期間を指定し、健全性のしきい値を設定する必要があります。たとえば健全性のしきい値が 2 である場合、呼び出しが連続して 2 回以上成功すると、コンテナが健全かつ RUNNING ステータスと見なされます。非健全性のしきい値が 2 である場合、呼び出しが 2 回以上失敗すると、コンテナが非健全かつ ERROR ステータスと見なされます。健全性のしきい値と非健全性のしきい値の間に該当するコンテナの状態はすべて、DEGRADED ステータスとなります。
[TCP 接続]	[TCP 接続] を選択した場合、入力するのはコンテナのポートだけでかまいません。健全性チェック時には、指定されたポートでコンテナとの TCP 接続が確立できるかどうかを試されます。また、HTTP の場合と同様、操作のタイムアウト値を指定し、健全性のしきい値または非健全性のしきい値を設定する必要があります。
[コマンド]	[コマンド] を選択する場合は、コンテナに対して実行するコマンドを入力する必要があります。健全性チェックが成功するかどうかは、コマンドの終了ステータスによって決まります。
[プロビジョニング時に健全性チェックを無視]	プロビジョニング時に健全性チェックを強制的に実行するには、このオプションを選択解除します。健全性チェックを強制的に実行することで、コンテナは、1 回の健全性チェックが成功するまで、プロビジョニングされていると見なされません。
[Autodeploy]	コンテナがエラー状態の場合にコンテナを自動的に再展開します。

[ログ構成] タブ

ブループリントのコンテナ コンポーネントに関するログ モードはデザイン キャンバスで指定します。必要に応じてログ オプションを指定することもできます。

表 3-40. [ログ構成] タブの設定

設定	説明
[ドライバ]	ドロップダウン メニューからログの形式を選択します。
[オプション]	ログ形式に基づく名前と値の形式を使用してドライバ オプションを入力します。

ブループリントでのコンテナ プロパティとプロパティ グループの使用

定義済みのプロパティ グループを vRealize Automation ブループリント内のコンテナ コンポーネントに追加することができます。これらのプロパティを含むブループリントを使用してマシンをプロビジョニングすると、プロビジョニングしたマシンが、Docker コンテナのホスト マシンとして登録されます。

vRealize Automation のコンテナ では、次の 2 つのプロパティ グループのコンテナ固有のカスタム プロパティを提供しています。コンテナ コンポーネントをブループリントに追加すると、これらのプロパティ グループをコンテナに追加して、プロビジョニングしたマシンをコンテナ ホストとして登録できます。

- コンテナ ホストのプロパティと証明書認証
- コンテナ ホストのプロパティとユーザー/パスワード認証

これらのプロパティ グループは、[管理] - [プロパティ ディクショナリ] - [プロパティ グループ] を選択すると vRealize Automation で表示されます。

プロパティ グループはすべてのテナントが共有するものであるため、マルチテナント環境で作業している場合は、プロパティのクローン作成とカスタマイズを検討してください。プロパティ グループとグループ内のプロパティに一意の名前を付けることで、それらを編集して特定のテナント用にカスタムの値を定義することができます。

最もよく使用されているプロパティは `Container.Auth.PublicKey` と `Container.Auth.PrivateKey` です。これらを使用して、コンテナ管理者はコンテナ ホストでの認証用のクライアント証明書を提供します。

表 3-41. コンテナ カスタム プロパティ

プロパティ	説明
<code>containers.ipam.driver</code>	コンテナ専用です。コンテナ ネットワーク コンポーネントをブループリントに追加するときに使用する IP アドレス管理ドライバを指定します。サポートされる値は、使用するコンテナ ホスト環境にインストールされているドライバによって異なります。たとえば、サポートされる値は、コンテナ ホストにインストールされている IP アドレス管理プラグインに応じて <code>infoblox</code> または <code>calico</code> になる場合があります。
<code>containers.network.driver</code>	コンテナ専用です。コンテナ ネットワーク コンポーネントをブループリントに追加するときに使用するネットワーク ドライバを指定します。サポートされる値は、使用するコンテナ ホスト環境にインストールされているドライバによって異なります。デフォルトでは、Docker によって提供されるネットワーク ドライバには <code>bridge</code> 、 <code>overlay</code> 、および <code>macvlan</code> が含まれ、Virtual Container Host (VCH) によって提供されるネットワーク ドライバには <code>bridge</code> ドライバが含まれています。コンテナ ホストにインストールされているネットワーク プラグインに応じて、 <code>weave</code> や <code>calico</code> などのサードパーティのネットワーク ドライバも使用できます。
<code>Container</code>	コンテナ専用です。デフォルト値は <code>App.Docker</code> であり、必須です。このプロパティは変更しないでください。
<code>Container.Auth.User</code>	コンテナ専用です。コンテナ ホストに接続するためのユーザー名を指定します。
<code>Container.Auth.Password</code>	コンテナ専用です。ユーザー名のパスワード、または使用するパブリック キーまたはプライベート キーのいずれかのパスワードを指定します。暗号化されたプロパティ値がサポートされています。
<code>Container.Auth.PublicKey</code>	コンテナ専用です。コンテナ ホストに接続するためのパブリック キーを指定します。
<code>Container.Auth.PrivateKey</code>	コンテナ専用です。コンテナ ホストに接続するためのプライベート キーを指定します。暗号化されたプロパティ値がサポートされています。
<code>Container.Connection.Protocol</code>	コンテナ専用です。通信プロトコルを指定します。デフォルト値は <code>API</code> であり、必須です。このプロパティは変更しないでください。

表 3-41. コンテナ カスタム プロパティ (続き)

プロパティ	説明
Container.Connection.Scheme	コンテナ専用です。通信方法を指定します。デフォルトは https です。
Container.Connection.Port	コンテナ専用です。コンテナ 接続ポートを指定します。デフォルトは 2376 です。
Extensibility.Lifecycle.Properties.VMPSMasterWorkflow32.MachineActivated	コンテナ専用です。すべての コンテナ プロパティを公開し、プロビジョニングされたホストを登録するために使用するイベント ブローカ プロパティを指定します。デフォルト値は Container* であり、必須です。このプロパティは変更しないでください。
Extensibility.Lifecycle.Properties.VMPSMasterWorkflow32.Disposing	コンテナ専用です。上記のすべての コンテナ プロパティを公開し、プロビジョニングされたホストを登録解除するために使用するイベント ブローカ プロパティを指定します。デフォルト値は Container* であり、必須です。このプロパティは変更しないでください。

デザイン キャンバスでの コンテナ ネットワーク コンポーネントの使用

1 つ以上の コンテナ ネットワーク コンポーネントをデザイン キャンバスに追加して、ブループリントの vSphere マシン コンポーネント用に設定できます。

containers.ipam.driver および containers.network.driver は、ブループリントに追加するとコンポーネントに追加できます。

コンテナ ネットワーク コンポーネントの追加

コンテナ コンポーネントを含んだ vRealize Automation ブループリントにコンテナ ネットワーク情報を追加することができます。

vRealize Automation のコンテナ のコンテナは、vRealize Automation の [コンテナ] タブで構成できます。vRealize Automation の [設計] タブのオプションを使用して、これらのコンテナとそのネットワーク設定をコンポーネントとしてブループリントに追加することができます。

前提条件

- コンテナ アーキテクトとして vRealize Automation にログインします。
- デザイン キャンバスで新規または既存のブループリントを開くには、[設計] タブを使用します。

手順

- 1 使用可能なネットワークおよびセキュリティ コンポーネントのリストを表示するには、[カテゴリ] セクションの [ネットワークとセキュリティ] をクリックします。
- 2 [コンテナ ネットワーク] コンポーネントをデザイン キャンバス上にドラッグします。
- 3 デザイン キャンバスでコンポーネントに一意のラベルを付けるには、[名前] テキスト ボックスに名前を入力します。
- 4 (オプション) [説明] テキスト ボックスにコンポーネントの説明を入力します。

- 5 (オプション) 外部の IP アドレス管理設定を指定したくない場合は、[外部] チェック ボックスを選択してください。

[外部]チェック ボックスを選択した場合、[IP アドレス管理構成]タブが削除されます。

- 6 [IP アドレス管理構成]タブをクリックし、ブループリントのコンテナ コンポーネントに指定されたネットワークのサブネット、IP アドレス範囲、ゲートウェイの情報を新たに指定するか、または既存の情報を編集します。

IP アドレス管理構成は、Docker などサポート対象のコンテナ アプリケーションで過去に作成されたネットワークではなく、vRealize Automation によって作成された新しいネットワークに適用されます。これらの設定は検証されません。したがって設定が他のネットワークと重複している場合、プロビジョニングは失敗します。たとえば、サブネットとゲートウェイはコンテナ ホスト内で一意である必要があります。

- 7 [プロパティ] タブをクリックして、コンポーネントのカスタム プロパティを指定します。

[プロパティ] グループ タブを選択し、[追加] をクリックすると、次のオプションが利用できます。

- コンテナ ホストのプロパティと証明書認証
- コンテナ ホストのプロパティとユーザー/パスワード認証

その他のプロパティ グループが定義されている場合、それらも一覧表示されます。

[カスタム プロパティ] タブを選択し、[追加] をクリックすれば、個々のカスタム プロパティをコンテナ コンポーネントに追加できます。

表 3-42. カスタム プロパティの [プロパティ] タブの設定

設定	説明
[名前]	カスタム プロパティの名前を入力するか、ドロップダウン メニューから使用可能なカスタム プロパティを選択します。
[値]	カスタム プロパティ名に関連する値を入力するか、編集します。
[暗号化済み]	たとえば、値がパスワードの場合に、プロパティ値を暗号化するように選択できます。
[オーバーライド可能]	次回以降にプロパティを使用する人がプロパティ値をオーバーライドできるように指定できます。[申請に表示] を選択した場合、ビジネス ユーザー（通常はアーキテクト）がカタログ アイテムを申請するときにプロパティ値を確認して編集することが可能になります。
[申請に表示]	プロパティ名とその値をエンド ユーザーに公開する場合は、マシン プロビジョニングの申請時に申請フォームでプロパティを表示するように選択できます。ユーザーが値を指定できるようにするには、[オーバーライド可能] も選択する必要があります。

- 8 ブループリントをドラフトとして保存するには [保存] を、ブループリントの設定を継続するには [完了] をクリックします。

次のステップ

コンテナ コンポーネントの [ネットワーク] タブでコンテナ ネットワーク設定を追加できます。

ブループリントで使用するコンテナ テンプレートのプッシュ

コンテナ テンプレートを vRealize Automation ブループリントで使用可能にできます。

コンテナ テンプレートには、複数のコンテナを含めることができます。vRealize Automation にマルチコンテナ テンプレートをプッシュすると、vRealize Automation のマルチコンポーネント ブループリントとしてテンプレートが作成されます。

コンテナ テンプレートに追加したコンテナ固有のプロパティは、vRealize Automation ブループリントで認識されます。[ブループリントでのコンテナ プロパティとプロパティ グループの使用](#)を参照してください。

vRealize Automation カタログで公開されたブループリントのプロビジョニングを要求するときは、そのブループリントのソース コンテナ アプリケーションをプロビジョニングします。

vRealize Automation ブループリントに追加できる他のコンポーネントとして、次のコンポーネント タイプがあります。

- マシン タイプ
- ソフトウェア コンポーネント
- 他のブループリント
- NSX ネットワークおよびセキュリティ コンポーネント
- XaaS コンポーネント
- カスタム コンポーネント

テンプレートは、コンテナ から vRealize Automation にプッシュできます。vRealize Automation ブループリントを変更しても、コンテナ テンプレートには影響ありません。

コンテナ テンプレートを後で変更し、変更したテンプレートを再度プッシュして、vRealize Automation のブループリントを上書きすることが可能です。テンプレートを vRealize Automation にプッシュすると、ブループリントが上書きされ、各プッシュ間に行われた vRealize Automation のブループリントの変更がすべて失われます。ブループリントの変更が失われないようにするには、vRealize CloudClient を使用して新しいブループリントのクローンを作成するか、ブループリントをエクスポートします。

ブループリントからの Docker コンテナまたはホストのプロビジョニング

vRealize Automation ブループリントを作成し、これを使用して、マシンを登録済み Docker コンテナ ホストとしてプロビジョニングできます。

プロビジョニングしたマシンをコンテナ ホストとして登録するには、次の要件を満たす必要があります。

- マシンをプロビジョニングするときに使用したブループリントに、コンテナ 固有のカスタム プロパティが含まれている。

必要なコンテナ固有のカスタム プロパティが 2 つのプロパティ グループで提供されている。[ブループリントでのコンテナ プロパティとプロパティ グループの使用](#)を参照してください。

vRealize Automation でカスタム プロパティおよびプロパティ グループを使用する方法については、『カスタム プロパティのリファレンス』を参照してください。

- マシンにネットワーク経由でアクセスできる。

たとえば、マシンは、有効な IP アドレスを備えており、パワーオン状態である必要があります。

特定のカスタム プロパティを含む vRealize Automation ブループリントを定義することにより、このブループリントでプロビジョニングを実行するときにマシンをコンテナ ホストとして指定できます。

必要なブループリント プロパティを含むマシンが正常にプロビジョニングされると、そのマシンは、コンテナ に登録され、vRealize Automation からイベントとアクションを受信します。

Microsoft Azure ブループリントの作成とリソース アクションの組み込み

クラウドまたはファブリック管理者は、ビジネス グループ管理者がビルディング ブロックとして導入する Microsoft Azure 仮想マシンのブループリントを作成して、利用者向けにカスタマイズおよびプロビジョニングされたマシンを作成できます。また、DevOps 管理者は、複合ブループリントを作成するときに、Azure マシンのブループリントを作成することも、既存の Azure マシンのブループリントを使用することもできます。

■ Microsoft Azure 用のブループリントの作成

Azure 仮想マシン リソースへのアクセスが可能な Microsoft Azure 仮想マシン ブループリントを作成できます。

■ Azure カスタム リソース アクションの作成

カスタム リソース アクションを作成および使用して、Azure 仮想マシンを制御することができます。

Microsoft Azure 用のブループリントの作成

Azure 仮想マシン リソースへのアクセスが可能な Microsoft Azure 仮想マシン ブループリントを作成できます。

vRealize Automation の [ブループリントの編集] ページの [マシン タイプ] カテゴリにデフォルトの Azure Machine テンプレートが表示されます。この仮想マシン テンプレートは、次の手順で説明する Azure ブループリントの基礎として使用できます。Azure ブループリントを作成したら、そのブループリントを設計に従って公開および展開したり、カスタム Azure リソースやその他のブループリントとともに使用して複合ブループリントを作成したりできます。

ブループリントを作成して公開した後、適切な権限を持つユーザーは、vRealize Automation サービス カタログにより、Azure インスタンスを要求しプロビジョニングすることができます。

Azure ブループリントでは、仮想マシンの要件を定義します。vRealize Automation は、これらの要件を使用して展開に最も適切な予約を選択します。

[新規ブループリント] ダイアログ ボックスの [NSX 設定] タブと [プロパティ] タブについては、『vRealize Automation の構成』を参照してください。

1 つの展開から 2 台の仮想マシンを同時に作成する場合、2 つのネットワーク インターフェイス名と 2 つの仮想マシン名を作成する必要があります。

注： 同じ名前のプリフィックスを使用して Azure と vSphere の両方に展開をプロビジョニングすることは避けてください。Azure と vSphere の名前が重複し、一部のユーザーに問題を引き起こす可能性があります。

前提条件

- 有効な Azure サブスクリプション ID と、リソース グループ、ストレージ アカウント、および仮想ネットワークなどに関連する情報を取得します。これらの情報は、ブループリントを作成する際に必要になる場合があります。
- vRealize Automation の環境で使用する Azure への接続を作成するため、Azure エンドポイントを構成します。

- ビジネス グループに合わせて Azure 予約を適切に設定してください。

手順

- 1 [設計] - [ブループリント] を選択します。

- 2 [新規] アイコン（）をクリックします。

- 3 [名前] テキスト ボックスにブループリント名を入力します。

入力した名前は [ID] テキスト ボックスにも入力されます。ほとんどの場合、[NSX 設定] タブと [プロパティ] タブは無視して構いません。

- 4 [OK] をクリックします。

- 5 [カテゴリ] メニューの [マシン タイプ] をクリックします。

- 6 [Azure Machine] 仮想マシン テンプレートをデザイン キャンバスにドラッグします。

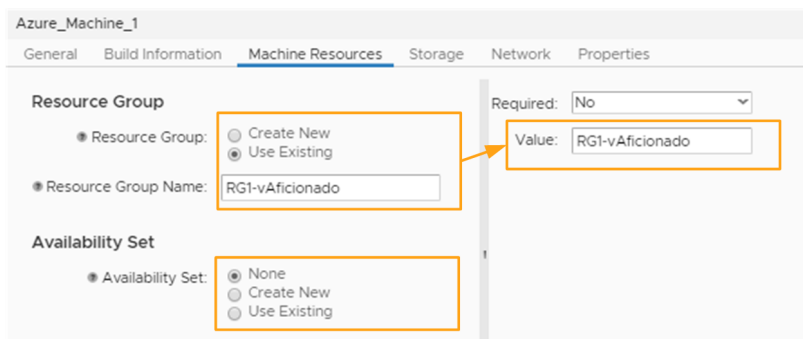
ブループリントの基礎として使用するカスタム Azure リソースを作成した場合は、[カテゴリ] リスト内の割り当て済みカテゴリからそのリソースを選択できます。

- 7 デザイン キャンバスの下半分のタブ付きページにあるテキスト ボックスに、Azure 仮想マシンの必須情報を入力します。タブ付きページは、Azure Machine テンプレートをデザイン キャンバスにドラッグすると表示されます。

これらのタブのすべてに、テキスト ボックスなどのパラメータが用意されています。ブループリントの基準として構成された Azure エンドポイントが主となって、これらのタブで利用可能な選択肢が決定されます。

ほとんどのパラメータでは、パラメータ名の隣にあるテキスト ボックスをクリックすると、ページの右側に新しいペインが開きます。このペインでは、[値] テキスト ボックスにパラメータ値を入力できるほか、それが [必須] であるかどうかを指定できます。場合によっては、[最小値] と [最大値] を入力できることもあります。右ペイン内の [適用] をクリックすると、最初のテキスト ボックスが入力されます。

図 3-1. Azure ブループリント右側のメニュー



The screenshot shows the 'Machine Resources' tab for 'Azure_Machine_1'. It includes sections for 'Resource Group' and 'Availability Set'. The 'Resource Group' section has radio buttons for 'Create New' and 'Use Existing' (selected), and a text field for 'Resource Group Name' containing 'RG1-vAficionado'. The 'Availability Set' section has radio buttons for 'None' (selected), 'Create New', and 'Use Existing'. On the right, there is a 'Required' dropdown set to 'No' and a 'Value' text field containing 'RG1-vAficionado'.

ほとんどのパラメータには、[詳細オプション] ボタンも用意されています。これらのオプションによって、パラメータの長さの指定だけでなく、エンド ユーザーに対してパラメータを非表示にすることもできます。

注： ブループリント構成を続行するには、各タブの必須パラメータを入力する必要があります。フィールドを空のままにする場合は、前に戻ってエントリを削除してから、保存を行ってください。

タブ	説明	重要なパラメータ
一般	使用されるエンドポイントなど、Azure 仮想マシンの基本的な接続情報を選択します。	<p>[ID]: 作成する Azure 仮想マシンを識別します。この名前を変更した場合は、デザイン キャンパス上の Azure 仮想マシン イメージも自動的に更新されます。</p> <p>[説明]: 作成する仮想マシンと、その仮想マシンが必須であるかを指定します。</p> <p>[インスタンス]: これを選択すると、拡張性のある仮想マシンを作成できます。[最小値] フィールドと [最大値] フィールドを使用して、このマシンから作成できる Azure インスタンスの数を指定します。</p> <p>[パスワード認証の使用]: パスワード認証を使用する場合は [はい] を選択し、SSH を使用する場合は [いいえ] を選択します。</p> <p>[管理ユーザー名]: このパラメータを空のままにすると、マシンをプロビジョニングするユーザーによって割り当てられます。</p> <p>[管理者パスワード]: このパラメータを空のままにすると、マシンをプロビジョニングする個別のユーザーが適切なパスワードを指定できます。</p>
ビルド情報	作成する仮想マシンについての情報を設定できます。	<p>[場所]: この仮想マシンを展開する地理的位置を選択します。</p> <p>[マシン プリフィックス]: 該当するラジオ ボタンを選択し、関連するビジネス グループからのマシン プリフィックスを使用するのか、それともカスタムプリフィックスを作成するのかを指定します。カスタム プリフィックスを使用する場合は、[カスタム マシン プリフィックス] テキスト ボックスに、使用するプリフィックスを入力します。</p> <p>[仮想マシン イメージ タイプ]: ラジオ ボタンを使用して、[カスタム]仮想マシン イメージまたは[標準]仮想マシン イメージを選択します。カスタム仮想マシンは、Azure の従来の展開から作成され、クラウド サービス、ストレージ アカウント、および可用性セットに関して、より多くの構成オプションが使用可能です。</p> <p>[仮想マシン イメージ]: ブループリントの基盤となる Azure 仮想マシン イメージを指定します。</p> <ul style="list-style-type: none"> ■ 標準仮想マシン イメージの場合、マシン イメージ URN は、(publisher):(offer):(sku): (version) という形式に一致している必要があります。 ■ 管理対象ディスクの場合、マシン イメージ URN は次の形式に一致する必要があります: (ResourceGroupName):(CustomImageName) ■ カスタム仮想マシン イメージの場合、マシン イメージ URN は、次の形式に一致している必要があります。 <p><code>https://storageaccount.blob.core.windows.net/container/image.vhd</code></p> <p>また、カスタム イメージの場合、[OS イメージ タイプ (Windows または Linux)] テキスト ボックスを入力する必要があります。</p> <p>[管理者ユーザー]: このブループリント ベースの仮想マシンに設定する、特定の管理者ユーザー名を入力します。ここでは空白のままにし、申請フォームに入力することもできます。</p> <p>[認証]: 該当するラジオ ボタンを選択し、このブループリントに基づく仮想マシンでパスワード認証と SSH 認証のどちらが必要になるかを指定します。</p> <p>[管理者パスワード]: 仮想マシン インスタンスの管理者パスワード。</p> <p>[シリーズ]: 仮想マシン インスタンスの一般的なサイズを定義します。シリーズについては、Azure のドキュメント (https://azure.microsoft.com/ja-jp/documentation/articles/virtual-machines-windows-sizes/) を参照してください。</p>

タブ	説明	重要なパラメータ
		<p>[サイズ] : シリーズ内の特定の仮想マシン インスタンスのサイズを定義します。サイズは選択したシリーズに関連付けられます。Azure インスタンスとの有効な接続を確立している場合、利用可能なサイズは、サブスクリプションと、選択した場所およびシリーズに基づいて動的に統合されます。サイズについては、Azure のドキュメントを参照してください。</p> <p>[インスタンス サイズの詳細] : 仮想マシン インスタンスのシリーズとサイズに関するオプションの情報。</p>
マシン リソース	<p>仮想マシン リソースをバケットに編成します。リソース グループは、Web サイト、アカウント、データベース、ネットワークなどの仮想マシン リソースをグループ化する組織構成です。</p> <p>[可用性セット] は、冗長性に対応するために 2 台以上の仮想マシンを管理するメカニズムです。Azure 可用性セットの詳細については、https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-manage-availability/を参照してください。</p> <p>注： Azure インスタンスの最大数が 1 より大きいブループリントを設定する場合は、新しいリソースグループと可用性セットを作成するのではなく、既存のリソースグループと可用性セットを使用する必要があります。同じ展開の複数のインスタンスで新しいリソースグループまたは新しい可用性セットを使用する場合、ロード バランサへの関連付けがあると、エラーやその他の問題が発生します。</p>	<p>[リソース グループの作成または再利用] : 該当するラジオ ボタンを選択し、既存の Azure リソース グループを使用するのか、それとも新しい Azure リソース グループを作成するのかを指定します。既存のリソース グループの名前は、Azure ポータルの [リソース グループ] ページで確認できます。リソース グループの新規作成を選択した場合は、新しいグループの適切な名前が [リソース グループ] テキスト ボックスに自動的に表示されます。</p> <p>[可用性セットの作成または再利用] : 作業内容に応じて適切なラジオ ボタンを選択します。[新規作成] を選択した場合は、新しい可用性セットの情報がテキスト ボックスに表示されます。</p>

タブ	説明	重要なパラメータ
ストレージ	<p>Azure 管理対象ディスク、またははこのブループリントのストレージ アカウントを選択できます。管理対象ディスクの場合、Azure は構成とメンテナンスに関連するストレージの大半を処理します。ストレージ アカウントは、Azure Blob、Queue Table、File Storage など、さまざまな Azure ストレージへのアクセスを提供します。ほとんどのブループリントの場合、デフォルトを受け入れることができます。</p>	<p>[ストレージ タイプ] - 管理対象のディスクと、手動で管理するストレージ アカウントのどちらを提供するかを選択します。</p> <ul style="list-style-type: none"> ■ 管理対象ディスクを選択した場合は、プレミアム ディスクと標準ディスクのどちらを使用するかを [仮想マシンのディスク タイプ] で選択します。それ以外の選択ボックスは無視して構いません。 ■ ストレージ アカウントを選択した場合は、仮想マシンのストレージ アカウント名を [OS ディスクのストレージ アカウント] ボックスに入力します。このストレージ アカウントには、Azure 仮想マシンのオペレーティング システム ディスクが展開されます。ストレージ グループの情報は Azure ポータルにあります。ストレージ アカウントは、1 つ以上所有できます。 <p>注： ストレージ アカウント名にアンダースコアなどの特殊文字を使用するとエラーが発生する可能性があります。</p> <p>[起動時診断を有効にする]：このチェック ボックスは、Azure インスタンスで診断データを使用する場合に選択します。</p> <p>[データ ディスクの数]：仮想マシンで使用されるデータ ストレージ ディスクの数を選択します。最大 4 つのディスクを指定できます。これらのディスクは、[ストレージ アカウント] テキスト ボックスに指定されたオペレーティング システム ディスクに追加して使用されます。</p> <p>ストレージ ディスクの番号</p> <ul style="list-style-type: none"> ■ [ディスク名]：ディスクに割り当てる名前を指定します。 ■ [ディスク タイプ]：ストレージ デバイスのタイプ。 ■ [ディスク サイズ]：ストレージのサイズ。 ■ [レプリケーション]：ディスクのバックアップに使用される冗長性方式。 ■ [ホスト キャッシュ]：パフォーマンスを高めるために読み取り/書き込みをキャッシュするかどうかを指定します。

タブ	説明	重要なパラメータ
ネットワーク	<p>仮想マシン ブループリント用のネットワークを選択できます。ほとんどのブループリントでは、デフォルトを受け入れることができ、利用者は、展開時に該当するネットワーク情報を入力します。</p> <p>注： 作成できる仮想マシンはインターフェイスあたり 1 台のみですが、各仮想マシンは、最大 4 つのインターフェイスを持つことができます。</p>	<p>表をクリックして右側にダイアログを開くと、次のフィールドを含む編集可能な別の表が表示されます。</p> <ul style="list-style-type: none"> ■ [ロード バランサー名]: Azure インスタンスで使用するロード バランサー。 ■ [ネットワーク インターフェイスの数]: Azure インスタンスで使用するネットワーク インターフェイスの数を選択します。ネットワーク インターフェイスの数は、[ストレージ] タブで選択した仮想マシン サイズでサポートされる必要があります。 ■ [ネットワーク インターフェイス]: 仮想マシン ブループリントの適切なネットワーク インターフェイスを選択します。既存のネットワークを入力する場合、他のすべてのネットワーク タブは無視して構いません。存在しないネットワーク インターフェイス名を入力した場合、その名前の新しいインターフェイスが作成され、その他の [ネットワーク] タブを使用してインターフェイスを構成できます。 ■ [NIC 名のプリフィックス]: ネットワーク インターフェイス カードのプリフィックス。 ■ [IP アドレス タイプ]: 仮想マシンで使用する IP アドレスが静的 IP アドレスと動的 IP アドレスのいずれであるかを指定します。 ■ [ネットワーク構成]: 該当するネットワーク構成を入力します。ネットワーク プロファイルがサポートされます。オプションには、[Azure ネットワークの指定] と [ネットワーク プロファイルの使用] の 2 つがあり、選択したオプションに応じて、後続のフィールドが変化します。 ■ [Azure ネットワークの指定] を選択した場合は、次のオプションを使用できます。これらのテキスト ボックスを空のままにした場合は、該当する予約で指定された情報に基づいて、デフォルトのネットワーク構成が使用されます。 <ul style="list-style-type: none"> ■ [vNet 名]: 仮想ネットワークの名前 ■ [subNet 名]: Azure サブネットのドメイン名。 <p>注： インストール後の作業で、Azure のパブリック IP アドレスを設定できます。</p> <ul style="list-style-type: none"> ■ [ネットワーク プロファイルの使用] を選択した場合、ネットワーク構成は、基盤となる Azure 構成から分離され、代わりに vRealize Automation ネットワーク プロファイルに結合されます。 <ul style="list-style-type: none"> ■ [ネットワーク プロファイル] テキスト ボックスを空のままにした場合は、ネットワーク プロファイルが指定された該当する予約に基づいて、デフォルトの Azure vNet およびサブネットのペアが解決されます。 ■ ネットワーク プロファイルを入力した場合は、一致する予約に基づいて、Azure vNet およびサブネットが解決されます。
プロパティ	<p>カスタム プロパティをブループリントに追加できます。ここで適用されるカスタム プロパティは、のちに優先して割り当てられるカスタム プロパティによってオーバーライドされる場合があります。カスタム プロパティの優先順位の詳細については、「カスタム プロパティのリファレンス」を参照してください。</p>	<p>カスタム プロパティを追加するオプションは 2 つあり、[プロパティ] ダイアログには対応する 2 つのタブがあります。</p> <ul style="list-style-type: none"> ■ プロパティ グループ: これらは、カスタム プロパティを追加するプロセスを簡素化する再利用可能なグループです。プロパティ グループを選択するオプションは 4 つあります。 <ul style="list-style-type: none"> ■ [追加] - 使用可能なプロパティ グループをブループリントに追加することができます。 ■ [上へ移動/下へ移動] - プロパティ グループの優先順位をコントロールできます。最初のグループが最も優先度が高く、そのグループに属するカスタム プロパティに最高の優先度が割り当てられます。

タブ	説明	重要なパラメータ
		<ul style="list-style-type: none"> ■ [プロパティの表示] - 選択したグループ内にカスタム プロパティを表示できます。 ■ [マージされたプロパティの表示] - 1つのカスタム プロパティが2つ以上のプロパティ グループに属している場合は、最も優先度の高いプロパティ グループに属する値が優先的に使用されます。これらのマージされたプロパティを表示することで、プロパティ グループの優先順位付けが容易になります。 ■ カスタム プロパティ: このタブを使用して、カスタム プロパティを個別に追加します。 <ul style="list-style-type: none"> ■ [新規] - カスタム プロパティをブループリントに個別に追加することができます。 ■ [名前] - プロパティを識別する名前を入力します。カスタム プロパティとその定義の一覧については、『カスタム プロパティのリファレンス』を参照してください。 ■ [値] - カスタム プロパティの値を入力します。 ■ [暗号化済み] - プロパティを暗号化できます。 ■ [オーバーライド可能] - 次のユーザーまたは後続のユーザーがオーバーライドできるプロパティ値を指定することができます。[申請に表示]を選択した場合、ビジネス ユーザー（通常はアーキテクト）がカタログ アイテムを申請するときにプロパティ値を確認して編集することが可能になります。 ■ 申請に表示 - プロパティ名とその値をエンド ユーザーに公開する場合は、マシン プロビジョニングの申請時に申請フォームでプロパティを表示するように選択できます。ユーザーが値を指定できるようにするには、[オーバーライド可能] も選択する必要があります。

8 [完了] をクリックすると、ブループリント構成が保存され、ブループリントのメイン ページに戻ります。

次のステップ

VPN トンネルをサポートするように Azure 予約のカスタム プロパティを設定してある場合は、Azure ブループリントにソフトウェア コンポーネントを追加できます。

- 1 [カテゴリ] メニューで、[ソフトウェア コンポーネント] を選択します。Azure ブループリントを構成したソフトウェア コンポーネントが下のペインに表示されます。
- 2 コンテナのドロップダウン値から Azure 仮想マシンを選択します。
- 3 目的のソフトウェア コンポーネントを選択し、デザイン キャンバス上の Azure 仮想マシンにドラッグします。
- 4 ソフトウェア コンポーネントにとって必須のプロパティがある場合は、デザイン キャンバスの下の該当するパラメータのテキスト ボックスに入力します。
- 5 [保存] をクリックします。

ブループリントを公開する場合は、ブループリントのメイン ページで該当するブループリントを選択し、[公開] をクリックします。公開したブループリントは、[カタログ アイテム] ページで使用可能になります。ビジネス グループ マネージャまたは同等のユーザーは、この公開されたブループリントを複合ブループリントの基礎として使用することもできます。

Azure カスタム リソース アクションの作成

カスタム リソース アクションを作成および使用して、Azure 仮想マシンを制御することができます。

vRealize Automation の Azure 実装には、デフォルトの状態では次の 2 つのカスタム リソース アクションが用意されています。

- 仮想マシンの起動
- 仮想マシンの停止

また、vRealize Automation インターフェイスで使用できる vRealize Orchestrator ライブラリからアクセス可能なワークフローを使用して、カスタム リソース アクションを作成できます。

Azure リソース アクションは、vRealize Automation におけるその他のあらゆる XaaS リソース アクションと同じように操作できます。XaaS リソース アクションの詳細については、「ブループリントおよびリソース アクションの作成」および vRealize Automation の構成にある「vRealize Automation での vRealize Orchestrator 統合」を参照してください。

前提条件

vRealize Automation 展開用の有効な Azure エンドポイントを構成します。

手順

- 1 [設計] - [XaaS] - [リソース アクション] の順に選択します
- 2 [新規] をクリックします。
- 3 vRealize Orchestrator ワークフロー ライブラリで [Orchestrator] - [ライブラリ] - [Azure] の順に移動します。
- 4 適切なフォルダとワークフローを選択します。
- 5 その他の XaaS リソース アクションと同じように、必要なアクションを設定します。

vSphere ブループリントへの構成管理機能の追加

vSphere ブループリントに構成管理コンポーネントを追加して、vSphere 仮想マシンの構成管理をサポートすることができます。

vRealize Automation では、Puppet および Ansible の構成管理機能を vSphere ブループリントに追加できます。

Puppet ベースの構成管理は、通常、Puppet Enterprise アプリケーションに基づいて、ロールと環境を使用してソフトウェアの構成を定義して管理します。Puppet でのロールと環境の意味は、IT の一般的な意味とは異なることに注意してください。

Ansible ベースの構成管理は、Ansible Tower 実装で定義されるジョブ テンプレートに基づいて行います。複数のテンプレートを選択して、順序を指定できます。マシンが展開された後、vRealize Automation から破棄されるまでの間は、これらのテンプレートを実行できます。

エンドポイントは、既存の Puppet または Ansible エンタープライズ展開との接続を確立します。エンドポイントが作成されるとき、vRealize Automation は、指定した展開から必要な情報を取得します。Puppet または Ansible が有効な仮想マシン ブループリントを構成するとき、事前バインドと遅延バインドのいずれかのシナリオを指定できます。

注： Ansible および Puppet コンポーネントは現在、vSphere ブループリントと仮想マシンでのみサポートされています。

Puppet コンポーネントの vSphere ブループリントへの追加

Puppet 設定の管理コンポーネントを vSphere ブループリントに追加して、Puppet マスターを使用する vSphere 仮想マシン設定に適用されている管理を容易にすることができます。

Puppet コンポーネントを vSphere ブループリントに追加すると、Puppet エージェントがそのブループリントから作成された仮想マシンに追加されます。

Puppet が有効になっている vSphere ブループリントを作成するときに、事前バインドまたは遅延バインドの構成を作成するかどうかを選択する必要があります。

事前バインドで、ユーザーは、Puppet コンポーネントがブループリントに追加されるときに、特定のブループリントに基づくすべての仮想マシンの Puppet ロールと環境設定を定義します。これらの設定は、ブループリントが存在している間は変化しません。遅延バインドにはいくつかのオプションがあります。

- ブループリントで [Puppet 環境] と [Puppet ロール] のテキスト ボックスを空のままにし、ユーザーが申請時にこれらの設定を指定します。
- [Puppet 環境] を指定し、[Puppet ロール] のボックスは空のままにします。ユーザーは、申請時にロールを指定する必要があります。

前提条件

適切な vSphere ブループリントを作成します。詳細については、[vSphere マシン コンポーネントの設定](#) を参照してください。

手順

- 1 [設計] - [ブループリント] を選択します。
- 2 ブループリントの [デザイン] ページで、[カテゴリ] メニューから、[構成管理] を選択します。
- 3 Puppet コンポーネントを選択し、デザイン キャンバス上の vSphere コンポーネントにドラッグします。
- 4 ページの下部にある [全般] タブに Puppet コンポーネントの [ID] および [説明] を入力します。
ID と説明は任意です。
- 5 [サーバ] タブをクリックします。
- 6 ドロップダウンをクリックし、ブループリントの適切な Puppet マスターを選択します。

- 7 このコンポーネントに対して事前バインドを使用する場合は、適切な [Puppet 環境] と [Puppet ロール] を選択します。

事前バインドを構成するには、Puppet 環境とロールを選択します。遅延バインドでコンポーネントを作成する場合は、[Puppet 環境] を選択するか、[Puppet 環境] と [Puppet ロール] のテキスト ボックスを空のままにし、[申請フォームで設定] チェック ボックスを選択します。

注： [申請フォームで設定] チェック ボックスは関連付けられています。1つを選択すると、もう一方も自動的に選択されます。

- 8 [完了] をクリックすると、Puppet コンポーネント構成が保存され、メインのルーブリントの [設計] ページに戻ります。

vSphere ブループリントへの Ansible コンポーネントの追加

Ansible 設定の管理コンポーネントを vSphere ブループリントに追加して、Ansible Tower を使用する vSphere 仮想マシン設定に適用されている管理を容易にすることができます。

Ansible コンポーネントを vSphere ブループリントに追加すると、Ansible Tower は展開済みのリソースと通信してコマンドを実行できるようになります。

前提条件

適切な vSphere ブループリントを作成します。詳細については、[vSphere マシン コンポーネントの設定](#) を参照してください。

手順

- 1 [設計] - [ブループリント] を選択します。
- 2 ブループリントの [デザイン] ページで、[カテゴリ] メニューから、[構成管理] を選択します。
- 3 Ansible コンポーネントを選択し、デザイン キャンバス上の vSphere コンポーネントにドラッグします。
- 4 ページの下部にある [全般] タブに Ansible コンポーネントの [ID] および [説明] を入力します。

ID と説明は任意です。

5 [詳細] タブをクリックし、Ansible Tower、プロジェクト、テンプレートの適切な情報を入力します。

- a 適切な [Ansible Tower] と、このコンポーネントを使用する [組織] を選択します。
- b Ansible コンポーネントに対して事前バインドまたは遅延バインドを設定します。
 - このコンポーネントに対して事前バインドを使用する場合は、適切な [プロジェクト] と [ジョブ テンプレート] を選択します。[ジョブ テンプレートのプロビジョニング解除] テキスト ボックスで、マシンを破棄するときに実行する適切なテンプレートを選択します。[申請フォームで設定] チェック ボックスは空のままにします。また、適切な Ansible 環境とロールを選択します。
 - 遅延バインドでコンポーネントを作成する場合は、[プロジェクト]、[ジョブ テンプレート]、および[ジョブ テンプレートのプロビジョニング解除] ボックスで値を設定する代わりに、[申請フォームで設定] チェック ボックスを選択できます。

注： [申請フォームで設定] チェック ボックスは関連付けられています。1つを選択すると、その下のチェック ボックスも自動的に選択されます。この機能は、[プロジェクト] フィールドがジョブ テンプレートのフィルタとして動作するために働きます。プロジェクトを指定すると、ジョブ テンプレートのリストが自動的にプロジェクトによってフィルタリングされます。そのため、プロジェクトで [申請フォームで設定] を選択すると、次の 2 つのフィールドが自動的に選択されます。

6 [完了] をクリックすると、Ansible コンポーネント構成が保存され、メインのブループリントの [設計] ページに戻ります。

Windows マシン ブループリントへの RDP 接続サポートの追加

カタログ管理者が Windows ブループリントの [RDP を使用して接続] アクションの使用資格ユーザーに付与するには、RDP カスタム プロパティをブループリントに追加し、システム管理者が準備した RDP ファイルを参照します。

注： ファブリック管理者によって必要なカスタム プロパティを含むプロパティ グループが作成されており、そのプロパティ グループをブループリントに追加した場合は、ブループリントにカスタム プロパティを個別に追加する必要はありません。

前提条件

- テナント管理者またはビジネス グループ マネージャとして vRealize Automation にログインします。
- システム管理者が作成したカスタム RDP ファイルの名前を取得します。[プロビジョニングされたマシンで RDP 接続をサポートするためのカスタム RDP ファイルの作成](#) を参照してください。
- 1 つ以上の Windows マシン ブループリントを作成します。

手順

- 1 [設計] - [ブループリント] を選択します。
- 2 アップデートするブループリントを指定して、[編集] をクリックします。
- 3 キャンバスでマシン コンポーネントを選択し、詳細を編集します。
- 4 [プロパティ] タブをクリックします。

5 [カスタム プロパティ] タブをクリックします。

6 RDP 設定を構成します。

a [新規プロパティ] をクリックします。

b [名前] テキスト ボックスに RDP カスタム プロパティ名を入力し、[値] テキスト ボックスに対応する値を入力します。

オプション	説明と値
VirtualMachine.Rdp.File	設定の取得元である RDP ファイルを指定します。たとえば My_RDP_Settings.rdp。このファイルは、vRealize Automation インストール ディレクトリの Website\Rdp サブディレクトリに存在する必要があります。
VirtualMachine.Rdp.SettingN	マシンへの RDP リンクを開くときに使用される RDP 設定を指定します。N は、各 RDP 設定を区別するために使用される一意の番号です。たとえば、認証要件が指定されないように RDP 認証レベルを指定するには、カスタム プロパティ VirtualMachine.Rdp.Setting1 を定義し、値を authentication level:i:3 に設定します。使用可能な RDP 設定とその正しい構文については、 Windows Server でのリモート デスクトップ サービス向けの RDP 設定 などの Microsoft Windows RDP ドキュメントを参照してください。
VirtualMachine.Admin.NameCompletion	ユーザー インターフェイス オプションの [RDP を使用して接続] または [SSH を使用して接続] の場合に、RDP または SSH ファイルで生成されるマシンの完全修飾ドメイン名に含めるドメイン名を指定します。たとえば、値を myCompany.com に設定すると、RDP または SSH ファイルに <i>my-machine-name.myCompany.com</i> という完全修飾ドメイン名が生成されます。

c [保存] をクリックします。

7 ブループリントの行を選択して、[公開] をクリックします。

結果

カタログ管理者は、ブループリントからプロビジョニングされたマシンの [RDP を使用して接続] アクションの使用資格をユーザーに付与することができます。ユーザーがアクションの使用資格を持っていない場合、RDP を使用して接続できません。

CentOS ブループリントへの Active Directory クリーンアップの追加

IaaS アーキテクトとして、プロビジョニングされたマシンがハイパーバイザーから削除されるたびに、Active Directory 環境がクリーンアップされるように vRealize Automation を構成したいと考えています。そのため、ブループリントを編集し、Active Directory クリーンアップ プラグインを構成します。

Active Directory クリーンアップ プラグインを使用して、マシンをハイパーバイザーから削除する場合に発生する Active Directory アカウント アクションを指定します。

- AD アカウントの削除
- AD アカウントの無効化
- AD アカウントの名前の変更
- 別の AD 組織単位 (OU) への AD アカウントの移動

前提条件

注： この情報は Amazon Web Services には適用されません。

- インフラストラクチャ アーキテクトとして vRealize Automation にログインします。
- Active Directory 環境について次の情報を収集します。
 - Active Directory アカウントの削除、無効化、名前変更、または移動に必要な十分な権限を持つユーザー名およびパスワード。ユーザー名は domain\username の形式で指定します。
 - (オプション) 破棄されたマシンの移動先の OU 名。
 - (オプション) 破棄されたマシンに添付するプリフィックス。
- マシン ブループリントを作成します。『[マシンのブループリントの設定](#)』を参照してください。

手順

- 1 [設計] - [ブループリント] を選択します。
- 2 ブループリントをポイントし、[編集] をクリックします。
- 3 キャンバス上のマシン コンポーネントを選択して [詳細] タブを表示します。
- 4 [プロパティ] タブをクリックします。
- 5 [カスタム プロパティ] タブをクリックし、Active Directory クリーンアップ プラグインを構成します。
 - a [新規プロパティ] をクリックします。
 - b [名前] テキスト ボックスに、Plugin.AdMachineCleanup.Execute と入力します。
 - c [値] テキスト ボックスに **true** と入力します。
 - d [保存] アイコン (🟢) をクリックします。
- 6 カスタム プロパティを追加して、Active Directory クリーンアップ プラグインを構成します。

オプション	説明と値
Plugin.AdMachineCleanup.UserName	[値] テキスト ボックスに Active Directory アカウントのユーザー名を入力します。このユーザーには、Active Directory アカウントの削除、無効化、移動、名前変更を行うための十分な権限が必要です。ユーザー名は domain\username の形式で指定します。
Plugin.AdMachineCleanup.Password	[値] テキスト ボックスに、Active Directory アカウントのユーザー名のパスワードを入力します。
Plugin.AdMachineCleanup.Delete	破棄されたマシンのアカウントを無効にする代わりに削除するには、True に設定します。
Plugin.AdMachineCleanup.MoveToOu	破棄するマシンのアカウントを新しい Active Directory の組織単位に移動します。値はアカウントの移動先の組織単位です。この値の形式は ou=OU, dc=dc です (例: ou=trash,cn=computers,dc=lab,dc=local)。
Plugin.AdMachineCleanup.RenamePrefix	プリフィックスを追加して、破棄するマシンのアカウント名を変更します。プリフィックス文字列を値の先頭に追加します (例: destroyed_)。

- 7 [OK] をクリックします。

結果

ブループリントによってプロビジョニングされたマシンがハイパーバイザーから削除されるたびに、Active Directory 環境がアップデートされるようになりました。

申請者によるマシン ホスト名指定の許可

ブループリント アーキテクトとして、ユーザーがブループリントを申請する場合に独自のマシン名を選択できるようにします。そのため、ブループリントを編集し、ホスト名カスタム プロパティを追加し、申請時にユーザーに値の入力を求めるプロンプトを表示するよう構成します。

注： ファブリック管理者によって必要なカスタム プロパティを含むプロパティ グループが作成されており、そのプロパティ グループをブループリントに追加した場合は、ブループリントにカスタム プロパティを個別に追加する必要はありません。

前提条件

- インフラストラクチャ アーキテクトとして vRealize Automation にログインします。
- マシン ブループリントを作成します。『[マシンのブループリントの設定](#)』を参照してください。

手順

- 1 [設計] - [ブループリント] を選択します。
- 2 ブループリントをポイントし、[編集] をクリックします。
- 3 キャンバス上のマシン コンポーネントを選択し、詳細タブを表示します。
- 4 [プロパティ] タブをクリックします。
- 5 [新規プロパティ] をクリックします。
- 6 [名前] テキスト ボックスに **ホスト名** を入力します。
- 7 [値] テキスト ボックスを空欄にします。
- 8 申請時にユーザーにホスト名の入力を求めるプロンプトを表示するよう vRealize Automation を構成します。

a [オーバーライド可能] を選択します。

b [申請に表示] を選択します。

ホスト名を一意のものにする必要があるため、ユーザーがこのブループリントから申請できるのは、1 度に 1 つのマシンのみです。

- 9 [保存] アイコン (🟢) をクリックします。
- 10 [OK] をクリックします。

結果

ユーザーがブループリントからマシンを申請するには、マシンのホスト名を指定する必要があります。vRealize Automation は、指定されたホスト名が一意のものかどうかを検証します。

ユーザーが地域間展開でデータセンターの場所を選択できるようにする

ブループリント アーキテクトとして、ボストンまたはロンドンのインフラストラクチャ上にマシンをプロビジョニングするかどうかをユーザーが選択できるようにするため、ブループリントを編集して場所の機能を有効にします。



データセンターはロンドンとボストンにあります。また、ボストンにいるユーザーにはロンドンのインフラストラクチャでマシンをプロビジョニングできないようにし、一方でロンドンにいるユーザーにはボストンのインフラストラクチャでマシンをプロビジョニングできないようにします。必ず、ボストンのユーザーはボストンのインフラストラクチャでプロビジョニングを行い、ロンドンのユーザーはロンドンのインフラストラクチャでプロビジョニングを行うようにすることで、ユーザーがマシンを申請するときにプロビジョニングに適切な場所を選択できるようにします。

前提条件

- インフラストラクチャ アーキテクトとして vRealize Automation にログインします。
- システム管理者として、データセンターの場所を定義します。シナリオ：複数の拠点にまたがる導入環境向けに [データセンターの場所を追加する](#) を参照してください。
- ファブリック管理者として、コンピュータ リソースに適した場所を適用します。シナリオ：地域間展開のために [コンピュータ リソースに場所を適用する](#) を参照してください。
- マシン ブループリントを作成します。『[マシンのブループリントの設定](#)』を参照してください。

手順

- 1 [設計] - [ブループリント] を選択します。
- 2 ブループリントをポイントし、[編集] をクリックします。
- 3 キャンバス上のマシン コンポーネントを選択し、[全般] タブを表示します。
- 4 [申請時の場所を表示] チェック ボックスを選択します。
- 5 [完了] をクリックします。
- 6 ブループリントをポイントし、[公開] をクリックします。

結果

以上で、ビジネス グループ ユーザーは、ブループリントからプロビジョニングされるマシンを申請するときにデータセンターの場所を選択するように求められるようになります。

ソフトウェア コンポーネントの設計

ソフトウェア アーキテクトは、再利用可能なソフトウェア コンポーネントを作成して、構成プロパティを標準化し、アクション スクリプトを使用して、展開の拡張処理中にコンポーネントをインストール、構成、アンインストール、更新する方法を具体的に指定します。これらのアクション スクリプトはいつでも記述し直して、同時に公開し、プロビジョニングされたソフトウェア コンポーネントに変更を反映させることができます。

汎用かつ再利用可能なアクション スクリプトを設計するには、ソフトウェア プロパティと呼ばれる名前と値のペアを定義して使用し、これをパラメータとしてアクション スクリプトに渡します。ソフトウェア プロパティに未知の値や、将来定義する必要のある値が含まれる場合は、他のブループリント アーキテクトまたはエンド ユーザーに値を入力するように要求または許可することができます。マシンの IP アドレスなど、ブループリント内の別のコンポーネントからの値を使用する必要がある場合は、そのマシンの IP アドレス プロパティにソフトウェア プロパティをバインドできます。ソフトウェア プロパティを使用してアクション スクリプトをパラメータ化すると、汎用かつ再利用可能になるため、スクリプトを変更することなく、さまざまな環境にソフトウェア コンポーネントを展開できます。

表 3-43. ライフ サイクル アクション

ライフ サイクル アクション	説明
インストール	ソフトウェアをインストールします。たとえば、Tomcat サーバ インストーラをダウンロードして、Tomcat サービスをインストールできます。インストール ライフ サイクル アクション用に記述するスクリプトは、初期導入申請中またはスケール アウトの一環として、ソフトウェアが最初にプロビジョニングされる際に実行されます。
構成	ソフトウェアを構成します。Tomcat の例の場合は、JAVA_OPTS と CATALINA_OPTS を設定できます。インストール アクションの完了後に構成スクリプトが実行されます。
開始	ソフトウェアを開始します。たとえば、Tomcat サーバで start コマンドを使用して、Tomcat サービスを開始できます。構成アクションの完了後に開始スクリプトが実行されます。
アップデート	拡張可能なブループリントをサポートするようにソフトウェア コンポーネントを設計する場合は、スケール インまたはスケール アウトの処理の後に必要なアップデートを処理します。たとえば、拡張された展開のクラスタのサイズを変更し、ロード バランサを使用してクラスタ化されたノードを管理できます。複数回実行 (idempotent) し、スケール インとスケール アウトの両方に対応できるようにアップデート スクリプトを設計します。拡張処理を実施するには、すべての従属ソフトウェア コンポーネントでアップデート スクリプトが実行されます。
アンインストール	ソフトウェアをアンインストールします。たとえば、展開を破棄する前にアプリケーションで特定のアクションを実行することができます。アンインストール スクリプトは、ソフトウェア コンポーネントが破棄されるたびに実行されます。

VMware Solution Exchange では、さまざまなミドルウェア サービスやアプリケーション用の事前定義されたソフトウェア コンポーネントをダウンロードできます。vRealize CloudClient または vRealize Automation の REST API を使用することで、事前定義された ソフトウェア コンポーネントを vRealize Automation インスタンスにプログラムでインポートできます。

- VMware Solution Exchange にアクセスするには、『https://solutionexchange.vmware.com/store/category_groups/cloud-management』を参照してください。
- vRealize Automation REST API の詳細については、プログラミング ガイド、および <https://code.vmware.com> で [vRealize Automation コンテンツ サービス API](#) を参照してください。
- vRealize CloudClient の詳細については、『<https://developercenter.vmware.com/tool/cloudclient>』を参照してください。

プロパティ タイプと設定オプション

汎用かつ再利用可能なアクション スクリプトを設計するには、ソフトウェア プロパティと呼ばれる名前と値のペアを定義して使用し、これをパラメータとしてアクション スクリプトに渡します。文字列、アレイ、コンテンツ、ブール値、整数値を使用するソフトウェア プロパティを作成できます。各自で値を指定したり、別のユーザーに値の入力を要求したり、バインドを作成して別のブループリント コンポーネントから値を取得したりすることができます。

プロパティ オプション

[計算済み] チェック ボックスを選択して、文字列プロパティの値を計算し、ソフトウェア プロパティを構成するときに適切なチェック ボックスを選択して、プロパティを暗号化したり、オーバーライドしたり、必須化したりできます。これらのオプションを値と組み合わせて、さまざまな目的を達成します。たとえば、ブループリントでソフトウェア コンポーネントを使用する際にパスワードの値を指定し、その値を暗号化するようにブループリント アーキテクトに要求することができます。パスワード プロパティを作成し、値のテキスト ボックスを空白のままにします。[オーバーライド可能]、[必須]、[暗号化済み] を選択します。エンド ユーザーのパスワードを要求する場合、ブループリント アーキテクトは [申請に表示] を選択して、申請フォームに入力する際にパスワードを入力するようにユーザーに要求できます。

オプション	説明
[暗号化済み]	プロパティを暗号化済みとしてマークすることで、vRealize Automation で値がマスクされ、アスタリスクとして表示されるようにします。 プロパティを暗号化済みから暗号化なしに変更すると、vRealize Automation はプロパティ値をリセットします。 安全性を維持するため、プロパティに新しい値を設定する必要があります。
[オーバーライド可能]	アプリケーション ブループリントを組み合わせる場合は、アーキテクトによるこのプロパティの値の編集を許可します。 値を入力すると、デフォルトとして表示されます。
[必須項目]	アーキテクトはこのプロパティに値を指定するか、入力されたデフォルト値を受け入れる必要があります。
[計算値]	計算されたプロパティ値は、INSTALL、CONFIGURE、START、UPDATE ライフ サイクル スクリプトによって割り当てられます。割り当てられた値は、以降の使用可能なライフ サイクル ステージとブループリント内でこれらのプロパティにバインドされたコンポーネントに伝播されます。文字列プロパティ以外のプロパティに [計算値] を選択すると、プロパティ タイプが文字列に変更されます。

計算値プロパティのオプションを選択する場合は、カスタム プロパティの値を空白の状態にします。計算値のスクリプトを作成します。

表 3-44. 計算値プロパティ オプションのスクリプト例

文字列プロパティの例	スクリプト構文	使用例
my_unique_id = ""	Bash - \$my_unique_id	export my_unique_id="0123456789"
	Windows CMD - %my_unique_id%	set my_unique_id=0123456789
	Windows PowerShell - \$my_unique_id	\$my_unique_id = "0123456789"

文字列プロパティ

文字列プロパティには文字列の値を入力します。各自で文字列を指定したり、別のユーザーに値の入力を要求したり、別の文字列プロパティへのバインドを作成して別のブループリント コンポーネントから値を取得したりすることができます。文字列の値には、任意の ASCII 文字を使用できます。プロパティ バインドを作成するには、デザイン キャンパスの [プロパティ] タブを使用して、バインドする適切なプロパティを選択します。これにより、プロパティ値が Raw 文字列データとしてアクション スクリプトに渡されます。ブループリントの文字列プロパティにバインドする際には、クラスタ化できないブループリント コンポーネントをバインドするようにしてください。コンポーネントがクラスタ化される場合、文字列の値はアレイになり、希望する値が取得されなくなります。

文字列プロパティの例	スクリプト構文	使用例
admin_email = "admin@email987.com"	Bash - \$admin_email	echo \$admin_email
	Windows CMD - %admin_email%	echo %admin_email%
	Windows PowerShell - \$admin_email	write-output \$admin_email

アレイ プロパティ

アレイ プロパティには、文字列、整数値、10 進数、ブール値の配列を使用し、["値 1", "値 2", "値 3"...] というように定義します。各自で値を指定したり、別のユーザーに値の入力を要求したり、プロパティ バインドを作成して別のブループリント コンポーネントから値を取得したりすることができます。

アレイ タイプのソフトウェア プロパティを作成する場合（データ型は整数または 10 進数）は、ロケールに関わらず、配列要素の区切り文字としてセミコロンを使用する必要があります。コンマ (,) またはドット (.) を使用しないでください。一部のロケールでは、10 進数の区切り文字としてコンマ (,) を使用できます。例：

- フランス語の有効な配列は、[1,11;2,22;3,33] のようになります。
- 英語の有効な配列は、[1.11,2.22,3.33] のようになります。

配列に大きい数を渡す場合は、グループ化の形式を使用しないでください。たとえば、**4444 444.000**（フランス語）、**4.444.444,000**（イタリア語）、または **4,444,444.000**（英語）を使用しないでください。ロケールに固有の形式を含むデータ ファイルは、異なるロケールのマシンに転送されるときに誤って解釈される可能性があるためです。グループ化の形式は使用できません。**4,444,444.000** などの数は 3 つの独立した番号としてとみなされるためです。代わりに、**4444444.000** と入力します。

アレイ プロパティの値を定義する場合は、アレイを角括弧で囲む必要があります。文字列のアレイの場合、アレイ要素の値には、任意の ASCII 文字を含めることができます。アレイ プロパティ値に含まれるバックスラッシュ文字を正しくエンコードするには、1 つ余分にバックスラッシュを追加します（例：["c:\\test1\\test2"]）。バインド プロパティの場合は、デザイン キャンバスの [プロパティ] タブを使用して、バインドする適切なプロパティを選択します。アレイにバインドする場合は、特定の順番で値アレイが生成されないように、ソフトウェア コンポーネントを設計する必要があります。

たとえば、アプリケーション サーバ仮想マシンのクラスタの負荷を分散しているロード バランサ仮想マシンについて考えます。このような場合、ロード バランサ サービスのアレイ プロパティを定義して、そのアレイ プロパティに各アプリケーション サーバ仮想マシンの IP アドレスのアレイを設定します。

次のロード バランサ サービス構成スクリプトでは、アレイ プロパティを使用して、Red Hat、Windows、および Ubuntu の各オペレーティング システム間で適切なロード バランシング機能を構成しています。

アレイ プロパティの例	スクリプト構文	使用例
operating_systems = ["Red Hat","Windows","Ubuntu"]	Bash - \${operating_systems[@]} (文字列のアレイ全体の場合) \${operating_systems[N]} (個々のアレイ要素の場合)	<pre>for ((i = 0 ; i < \$ {#operating_systems[@]} ; i++)); do echo \${operating_systems[i]} done</pre>
	Windows CMD - %operating_systems_% ここで、N はアレイ内の要素の位置	<pre>for /F "delims== tokens=2" %%A in ('set operating_systems_') do (echo %%A)</pre>
	Windows PowerShell - \$operating_systems (文字列のアレイ全体の場合) \$operating_systems[N] (個々のアレイ要素の場合)	<pre>foreach (\$os in \$operating_systems) { write-output \$os }</pre>

コンテンツ プロパティ

コンテンツ プロパティの値は、コンテンツをダウンロードするためのファイルへの URL です。ソフトウェア エージェントは、URL から仮想マシンにコンテンツをダウンロードして、仮想マシン内のローカル ファイルの場所をスクリプトに渡します。

コンテンツ プロパティは、HTTP または HTTPS プロトコルを使用した有効な URL として定義する必要があります。たとえば、Dukes Bank サンプル アプリケーションの JBOSS アプリケーション サーバ ソフトウェア コンポーネントでコンテンツ プロパティに cheetah_tgz_url を指定するとします。さらに、製品が ソフトウェア アプライアンスでホストされていて、URL がアプライアンスのその場所を参照しているとします。ソフトウェア エージェントは、この製品を指定された場所から展開先の仮想マシンにダウンロードします。

コンテンツ プロパティで利用できる software.http.proxy 設定については、カスタム プロパティのリファレンスを参照してください。

文字列プロパティの例	スクリプト構文	使用例
cheetah_tgz_url = "http:// app_content_server_ip:port/artifacts/ software/jboss/cheetah-2.4.4.tar.gz"	Bash - \$cheetah_tgz_url	tar -zxvf \$cheetah_tgz_url
	Windows CMD - %cheetah_tgz_url%	start /wait c:\unzip.exe %cheetah_tgz_url%
	Windows PowerShell - \$cheetah_tgz_url	& c:\unzip.exe \$cheetah_tgz_url

ブール値のプロパティ

ブール値のプロパティ タイプを使用すると、[値] ドロップダウン メニューに True と False のオプションが表示されます。

整数値のプロパティ

ゼロ、正または負の整数値には整数値のプロパティ タイプを使用します。

10 進数のプロパティ

非循環小数を表す値には、10 進数のプロパティ タイプを使用します。

ソフトウェア コンポーネントに別のコンポーネントからの情報が必要である場合

いくつかの展開シナリオでは、コンポーネントは、自身をカスタマイズするために、別のコンポーネントのプロパティ値を必要とします。vRealize Automation では、プロパティ バインドを作成することで、これが可能です。プロパティ バインド用にソフトウェア アクション スクリプトを設計できますが、実際のバインドはブループリントを組み合わせるアーキテクトが構成します。

ソフトウェア アーキテクト、IaaS アーキテクト、またはアプリケーション アーキテクトは、プロパティをハードコードされた値に設定する以外に、ソフトウェア コンポーネント プロパティをブループリント内の他のプロパティにバインドできます (IP アドレスやインストールの場所など)。ソフトウェア プロパティを別のプロパティにバインドする場合、別のコンポーネントのプロパティ値や仮想マシンのプロパティ値に基づいてスクリプトをカスタマイズできます。たとえば WAR コンポーネントの場合、Apache Tomcat サーバのインストール場所を必要とすることがあります。スクリプトでは、server_home プロパティ値を Apache Tomcat サーバの install_path プロパティ値に設定するよう WAR コンポーネントを構成できます。ブループリントを組み合わせるアーキテクトが server_home プロパティを Apache Tomcat サーバの install_path プロパティにバインドする限り、server_home プロパティ値は正しく設定されます。

作成したアクション スクリプトでは、スクリプトに定義されるプロパティのみを使用でき、文字列とアレイの値でのみプロパティ バインドを作成できます。ブループリントのプロパティ アレイは特定の順番で返されることはないため、クラスタ可能または拡張可能なコンポーネントにバインドしても、期待する値が生成されない可能性があります。たとえば、ソフトウェア コンポーネントにはマシンのクラスタの各マシン ID が必要であり、ユーザーが 1 ～ 10 台のマシンからクラスタを申請し、展開を拡張できるように許可します。ソフトウェア プロパティを文字列タイプとして構成する場合は、ランダムに選択された単一のマシン ID をクラスタから取得します。ソフトウェア プロパティを

アレイ タイプとして構成する場合は、クラスタ内のすべてのマシン ID のアレイが順不同に取得されます。ユーザーが展開を拡張する場合は、その処理ごとに値の順序が異なる可能性があります。クラスタ化されたコンポーネントの値を失わないようにするには、ソフトウェア プロパティでアレイ タイプを使用できます。ただし、特定の順番で値アレイが生成されないように、ソフトウェア コンポーネントを設計する必要があります。

異なるタイプのプロパティをバインドする場合の文字列プロパティ値の例については、「文字列プロパティ バインドの例」の表を参照してください。

表 3-45. 文字列プロパティ バインドの例

プロパティ タイプの例	バインドするプロパティ タイプ	バインド結果 (A が B にバインド)
文字列 (プロパティ A)	文字列 (プロパティ B="Hi")	A="Hi"
文字列 (プロパティ A)	コンテンツ (プロパティ B="http://my.com/content")	A="http://my.com/content"
文字列 (プロパティ A)	アレイ (プロパティ B=["1","2"])	A=["1","2"]
文字列 (プロパティ A)	計算値 (プロパティ B="Hello")	A="Hello"

異なるタイプのプロパティをバインドする場合のアレイ プロパティ値の例については、「アレイ プロパティ バインドの例」の表を参照してください。

表 3-46. アレイ プロパティ バインドの例

プロパティ タイプの例	バインドするプロパティ タイプ	バインド結果 (A が B にバインド)
アレイ (プロパティ A)	文字列 (プロパティ B="Hi")	A="Hi"
アレイ (プロパティ A)	コンテンツ (プロパティ B="http://my.com/content")	A="http://my.com/content"
アレイ (プロパティ A)	計算値 (プロパティ B="Hello")	A="Hello"

サポートされるプロパティ タイプの詳細については、[プロパティ タイプと設定オプション](#)を参照してください。

ライフ サイクル ステージ間のプロパティ値の受け渡し

アクション スクリプトを使用してライフ サイクル ステージ間のプロパティ値を変更して受け渡すことができます。

算出されたプロパティの場合、プロパティの値を変更し、その値をアクション スクリプトの次のライフ サイクル ステージに渡すことができます。たとえば、コンポーネント A にステージング済みと定義された progress_status 値がある場合、INSTALL および CONFIGURE ライフ サイクル ステージでは、それぞれのアクション スクリプトでその値を progress_status=installed に変更します。コンポーネント B がコンポーネント A にバインドされている場合、アクション スクリプトのライフ サイクル ステージにおける progress_status のプロパティ値は、コンポーネント A と同じになります。

ソフトウェア コンポーネントで、コンポーネント B が A に依存するように定義します。この依存関係によって、コンポーネントが同じノード内にあっても異なるノード間にあっても、コンポーネント間の正しいプロパティ値の受け渡しが定義されます。

たとえば、サポートされているスクリプトを使用して、アクション スクリプト内のプロパティ値をアップデートできます。

- Bash `progress_status="completed"`
- Windows CMD `set progress_status=completed`
- Windows PowerShell `$progress_status="completed"`

注： アレイおよびコンテンツのプロパティでは、ライフ サイクル ステージのアクション スクリプト間での、変更されたプロパティ値の受け渡しはサポートされていません。

コンポーネントの開発のベスト プラクティス

プロパティとアクション スクリプトを定義するベスト プラクティスについて理解するには、ソフトウェア コンポーネントとアプリケーション ブループリントを VMware Solution Exchange からダウンロードしてインポートします。

ソフトウェア コンポーネントを開発するときは、これらのベスト プラクティスに従います。

- スクリプトを中断することなく実行するには、戻り値をゼロ (0) に設定する必要があります。この設定により、エージェントはすべてのプロパティをキャプチャし、それらを ソフトウェア サーバに送信できます。
- 一部のインストーラでは、tty コンソールへのアクセスが必要になります。/dev/console からの入力をリダイレクトします。たとえば、RabbitMQ ソフトウェア コンポーネントでは、インストール スクリプトで `./rabbitmq_rhel.py --setup-rabbitmq < /dev/console` コマンドを使用することがあります。
- コンポーネントが複数のライフ サイクル ステージを使用する場合は、INSTALL ライフ サイクル ステージでプロパティ値を変更できます。新しい値は、次のライフ サイクル ステージに送られます。アクション スクリプトは展開中にプロパティの値を計算し、依存しているその他のスクリプトにその値を提供できます。たとえば、Clustered Dukes Bank サンプル アプリケーションでは、インストール ライフ サイクル ステージ中に JBossAppServer サービスが JVM_ROUTE プロパティを計算します。このプロパティは、JBossAppServer サービスがライフ サイクルを構成するために使用します。次に、Apache ロード バランサ サービスは、その JVM_ROUTE プロパティを `all(appserver:JbossAppServer:JVM_ROUTE)` プロパティにバインドし、node0 と node1 の最終計算値を取得します。アプリケーションの展開を正常に完了するために、コンポーネントが別のコンポーネントからのプロパティ値を必要とする場合、アプリケーションブループリントに依存関係を明示的に記述する必要があります。

注： 複数のライフ サイクル ステージを使用するコンポーネントのコンテンツ プロパティの値は変更できません。

ソフトウェア コンポーネントの作成

その他のソフトウェア アーキテクト、IaaS アーキテクト、アプリケーション アーキテクトがアプリケーション ブループリントを組み合わせるのに使用できるソフトウェア コンポーネントを設定および公開します。

前提条件

ソフトウェア アーキテクトとして vRealize Automation にログインします。

手順

1 [設計] - [ソフトウェア コンポーネント] を選択します。

2 [追加] アイコン () をクリックします。

3 名前と説明 (説明は任意) を入力します。

ソフトウェア コンポーネントに指定した名前を使用して、vRealize Automation によりテナント内で一意のソフトウェア コンポーネントの ID が作成されます。このフィールドはこの段階では編集できますが、ブループリントの保存後は変更できません。ID は永続的かつテナント内で一意であるため、プログラムによるブループリントとの通信や、プロパティ バインドの作成などに使用されます。

4 (オプション) ソフトウェア コンポーネントをブループリントに含める方法を制御する場合、[コンテナ] ドロップダウン メニューからコンテナ タイプを選択します。

オプション	説明
[マシン]	ソフトウェア コンポーネントは、マシン上に直接配置する必要があります。
公開済みのソフトウェア コンポーネントのいずれか	作成した別のソフトウェア コンポーネント上に特別にインストールできるようにソフトウェア コンポーネントを設計する場合、リストからこのソフトウェア コンポーネントを選択します。たとえば、以前作成した JBOSS コンポーネント上にインストールできるように EAR コンポーネントを設計する場合、リストから JBOSS コンポーネントを選択します。
[ソフトウェア コンポーネント]	マシン上に直接インストールできないが、複数の異なるソフトウェア コンポーネント上にはインストールできるソフトウェア コンポーネントを設計する場合、[ソフトウェア コンポーネント] オプションを選択します。たとえば、WAR コンポーネントを設計して、Tomcat サーバ ソフトウェア コンポーネントと Tcserver ソフトウェア コンポーネント上にインストールする場合、ソフトウェア コンポーネントのコンテナ タイプを選択します。

5 [次へ] をクリックします。

6 アクション スクリプトで使用するプロパティを定義します。

a [追加] アイコン () をクリックします。

b プロパティの名前を入力します。

c プロパティの説明を入力します。

この説明は、ブループリントでソフトウェア コンポーネントを使用するアーキテクトに表示されます。

- d プロパティの値として希望するタイプを選択します。
- e プロパティの値を定義します。

オプション	説明
入力値をここで使用する	<ul style="list-style-type: none"> ■ 値を入力します。 ■ [オーバーライド可能] を選択解除します。 ■ [必須] を選択します。
アーキテクトに値の入力を要求する	<ul style="list-style-type: none"> ■ デフォルト値を指定するには、値を入力します。 ■ [オーバーライド可能] を選択します。 ■ [必須] を選択します。
アーキテクトが希望する場合は値の入力を許可する	<ul style="list-style-type: none"> ■ デフォルト値を指定するには、値を入力します。 ■ [オーバーライド可能] を選択します。 ■ [必須] を選択解除します。

アーキテクトは、申請フォームでユーザーに表示するように ソフトウェア プロパティを設定できます。アーキテクトは [申請に表示] オプションを使用すると、オーバーライド可能としてマークしたプロパティの値をユーザーが入力するように要求または要請できます。

- 7 プロンプトに従って、少なくとも 1 つ以上のソフトウェア ライフ サイクル アクションのスクリプトを入力します。

表 3-47. ライフ サイクル アクション

ライフ サイクル アクション	説明
インストール	ソフトウェアをインストールします。たとえば、Tomcat サーバ インストーラをダウンロードして、Tomcat サービスをインストールできます。インストール ライフ サイクル アクション用に記述するスクリプトは、初期導入申請中またはスケール アウトの一環として、ソフトウェアが最初にプロビジョニングされる際に実行されます。
構成	ソフトウェアを構成します。Tomcat の例の場合は、JAVA_OPTS と CATALINA_OPTS を設定できます。インストール アクションの完了後に構成スクリプトが実行されます。
開始	ソフトウェアを開始します。たとえば、Tomcat サーバで start コマンドを使用して、Tomcat サービスを開始できます。構成アクションの完了後に開始スクリプトが実行されます。
アップデート	拡張可能なブループリントをサポートするようにソフトウェア コンポーネントを設計する場合は、スケール インまたはスケール アウトの処理の後に必要なアップデートを処理します。たとえば、拡張された展開のクラスタのサイズを変更し、ロード バランサを使用してクラスタ化されたノードを管理できます。複数回実行 (idempotent) し、スケール インとスケール アウトの両方に対応できるようにアップデート スクリプトを設計します。拡張処理を実施する際には、すべての従属ソフトウェア コンポーネントでアップデート スクリプトが実行されます。
アンインストール	ソフトウェアをアンインストールします。たとえば、展開を破棄する前にアプリケーションで特定のアクションを実行することができます。アンインストール スクリプトは、ソフトウェア コンポーネントが破棄されるたびに実行されます。

アクション スクリプトに終了コードと状態コードを含めます。サポート対象の各スクリプト タイプには、終了コードと状態コードの固有の要件があります。

スクリプト タイプ	成功状態	エラー状態	サポート対象外のコマンド
Bash	<ul style="list-style-type: none"> ■ return 0 ■ exit 0 	<ul style="list-style-type: none"> ■ return non-zero ■ exit non-zero 	なし
Windows CMD	exit /b 0	exit /b non-zero	exit 0 または exit non-zero コードは使用しないでください。
PowerShell	exit 0	exit non-zero;	warning、verbose、debug、host コールは使用しないでください。

8 マシンの再起動を求めるスクリプトの場合は、[再起動] チェックボックスを選択します。

スクリプトの実行後、マシンは、次のライフ サイクル スクリプトを開始する前に再起動されます。

9 [完了] をクリックします。

10 ソフトウェア コンポーネントを選択して、[公開] をクリックします。

結果

ソフトウェア コンポーネントの構成および公開しました。他のソフトウェア アーキテクト、IaaS アーキテクト、およびアプリケーション アーキテクトはこのソフトウェア コンポーネントを使用して、アプリケーション ブループリントにソフトウェアを追加できます。

次のステップ

公開済みのソフトウェア コンポーネントをアプリケーション ブループリントに追加します。[複合ブループリントの組み合わせ](#)を参照してください。

ソフトウェア コンポーネントの設定

プロビジョニングされたマシン上の ソフトウェア コンポーネントをインストール、構成、アップデート、またはアンインストールするため、全般設定、プロパティの作成、カスタム アクション スクリプトの記述を行います。

ソフトウェア アーキテクトとして、[設計] - [ソフトウェア コンポーネント] をクリックし、[追加] アイコンをクリックして、新規 ソフトウェア コンポーネントを作成します。

新規 ソフトウェア の全般設定

全般設定を ソフトウェア コンポーネントに適用します。

表 3-48. 新規 ソフトウェア の全般設定

設定	説明
[名前]	ソフトウェア コンポーネント名を入力します。
[ID]	ソフトウェア コンポーネントに指定した名前を使用して、vRealize Automation によりテナント内で一意の ソフトウェア コンポーネントの ID が作成されます。このフィールドはこの段階では編集できませんが、ブループリントの保存後は変更できません。ID は永続的かつテナント内で一意であるため、プログラムによるブループリントとの通信や、プロパティ バインドの作成などに使用されます。

表 3-48. 新規 ソフトウェア の全般設定 （続き）

設定	説明
[説明]	他のアーキテクトで活用するために ソフトウェア コンポーネントについて概要を示します。
[コンテナ]	<p>デザイン キャンバスでは、ブループリント アーキテクトは選択したコンテナ タイプの内部にのみ ソフトウェア コンポーネントを配置できます。</p> <ul style="list-style-type: none"> ■ デザイン キャンバスでマシン コンポーネントに直接、ソフトウェア コンポーネントを配置するようにアーキテクトに要求するには、[マシン] を選択します。 ■ マシン コンポーネントには直接配置せず、複数の異なる ソフトウェア コンポーネントのいずれかの内部にネストできる ソフトウェア コンポーネントを設計する場合は、[ソフトウェア コンポーネント] を選択します。 ■ 作成済みの別の ソフトウェア コンポーネントの内部にネストするために ソフトウェア コンポーネントを設計する場合は、公開済みの特定の ソフトウェア コンポーネントを選択します。 ■ Azure ブループリント用として ソフトウェア コンポーネントを設計する場合は、[Azure 仮想マシン] を選択します。

新規 ソフトウェア プロパティ

ソフトウェア コンポーネント プロパティを使用して、スクリプトをパラメータ化できます。これにより、定義されたプロパティを環境変数として、マシン上で実行中のスクリプトに渡すことができます。プロビジョニングされたマシンのソフトウェア エージェントは、スクリプトを実行する前に vRealize Automation とやり取りして、プロパティを解決します。次に、プロパティからスクリプト固有の変数を作成し、スクリプトに渡します。

表 3-49. 新規 ソフトウェア プロパティ

設定	説明
[名前]	ソフトウェア プロパティ名を入力します。プロパティの名前には、英数字、ハイフン (-)、またはアンダースコア (_) のみを使用できます。大文字と小文字は区別されます。
[説明]	他のユーザーが活用できるように、プロパティやその値の要件についての概要を提示します。
[タイプ]	ソフトウェア では、文字列、アレイ、コンテンツ、ブール値、整数値のタイプをサポートします。サポートされるプロパティ タイプの詳細については、 プロパティ タイプと設定オプション を参照してください。プロパティ バインドの詳細については、 ソフトウェア コンポーネントに別のコンポーネントからの情報が必要である場合とブループリント コンポーネント間でのプロパティ バインドの作成 を参照してください。

表 3-49. 新規 ソフトウェア プロパティ （続き）

設定	説明
[値]	<ul style="list-style-type: none"> ■ 入力値を使用するには、次の手順に従います。 <ul style="list-style-type: none"> ■ [値] を入力します。 ■ [必須] を選択します。 ■ [オーバーライド可能] を選択解除します。 ■ アーキテクトに値の入力を要求するには、次の手順に従います。 <ul style="list-style-type: none"> ■ （オプション）[値] を入力して、デフォルトを指定します。 ■ [オーバーライド可能] を選択します。 ■ [必須] を選択します。 ■ アーキテクトが値を入力するか、空白にすることを許可するには、次の手順に従います。 <ul style="list-style-type: none"> ■ （オプション）[値] を入力して、デフォルトを指定します。 ■ [オーバーライド可能] を選択します。 ■ [必須] を選択解除します。
[暗号化済み]	<p>プロパティを暗号化済みとしてマークすることで、vRealize Automation で値がマスクされ、アスタリスクとして表示されるようになります。 プロパティを暗号化済みから暗号化なしに変更すると、vRealize Automation はプロパティ値をリセットします。 安全性を維持するため、プロパティに新しい値を設定する必要があります。</p> <p>重要： セキュアなプロパティが echo コマンドまたはその他の同様のコマンドを使用してスクリプトに出力されると、これらの値はログ ファイルにプレーン テキストで表示されます。ログ ファイルの値はマスクされません。</p>
[オーバーライド可能]	<p>アプリケーション ブループリントを組み合わせる場合は、アーキテクトによるこのプロパティの値の編集を許可します。 値を入力すると、デフォルトとして表示されます。</p>
[必須項目]	<p>アーキテクトはこのプロパティに値を指定するか、入力されたデフォルト値を受け入れる必要があります。</p>
[計算値]	<p>計算されたプロパティ値は、INSTALL、CONFIGURE、START、UPDATE ライフ サイクル スクリプトによって割り当てられます。割り当てられた値は、以降の使用可能なライフ サイクル ステージとブループリント内でこれらのプロパティにバインドされたコンポーネントに伝播されます。文字列プロパティ以外のプロパティに [計算値] を選択すると、プロパティ タイプが文字列に変更されます。</p>

新規 ソフトウェア アクション

Bash、Windows CMD、PowerShell のいずれかのアクション スクリプトを作成して、展開の拡張処理中にコンポーネントをインストール、構成、アンインストール、更新する方法を具体的に指定します。

表 3-50. ライフ サイクル アクション

ライフ サイクル アクション	説明
インストール	ソフトウェアをインストールします。たとえば、Tomcat サーバ インストーラをダウンロードして、Tomcat サービスをインストールできます。インストール ライフ サイクル アクション用に記述するスクリプトは、初期導入申請中またはスケール アウトの一環として、ソフトウェアが最初にプロビジョニングされる際に実行されます。
構成	ソフトウェアを構成します。Tomcat の例の場合は、JAVA_OPTS と CATALINA_OPTS を設定できます。インストール アクションの完了後に構成スクリプトが実行されます。
開始	ソフトウェアを開始します。たとえば、Tomcat サーバで start コマンドを使用して、Tomcat サービスを開始できます。構成アクションの完了後に開始スクリプトが実行されます。
アップデート	拡張可能なブループリントをサポートするようにソフトウェア コンポーネントを設計する場合は、スケール インまたはスケール アウトの処理の後に必要なアップデートを処理します。たとえば、拡張された展開のクラスタのサイズを変更し、ロード バランサを使用してクラスタ化されたノードを管理できます。複数回実行 (idempotent) し、スケール インとスケール アウトの両方に対応できるようにアップデート スクリプトを設計します。拡張処理を実施する際には、すべての従属ソフトウェア コンポーネントでアップデート スクリプトが実行されます。
アンインストール	ソフトウェアをアンインストールします。たとえば、展開を破棄する前にアプリケーションで特定のアクションを実行することができます。アンインストール スクリプトは、ソフトウェア コンポーネントが破棄されるたびに実行されます。

マシンの再起動を求めるスクリプトの場合は、[再起動] チェックボックスを選択します。スクリプトの実行後、マシンは、次のライフ サイクル スクリプトを開始する前に再起動されます。アクション スクリプトを実行する際に、ユーザーの操作を求めるメッセージを表示するプロセスがないことを確認します。中断によってスクリプトが一時停止し、無期限にアイドル状態になる原因になり、最終的に失敗します。さらに、アプリケーションの展開に適用できる適切な終了コードをスクリプトに含める必要があります。スクリプトに終了コードや戻りコードがない場合、スクリプトで実行される最後のコマンドが終了ステータスになります。サポートされるスクリプト タイプ (Bash、Windows CMD、PowerShell) によって、終了コードや戻りコードは異なります。

スクリプト タイプ	成功状態	エラー状態	サポート対象外のコマンド
Bash	<ul style="list-style-type: none"> return 0 exit 0 	<ul style="list-style-type: none"> return non-zero exit non-zero 	なし
Windows CMD	exit /b 0	exit /b non-zero	exit 0 または exit non-zero コードは使用しないでください。
PowerShell	exit 0	exit non-zero;	warning、verbose、debug、host コールは使用しないでください。

XaaS ブループリントおよびリソース アクションの設計

XaaS ブループリントは、カタログ アイテムとして公開するか、ブループリント デザイン キャンバスで使用できます。リソース アクションは、展開されたアイテム上で実行するアクションです。

XaaS は vRealize Orchestrator を使用して、アイテムをプロビジョニングまたはアクションを実行するワークフローを実行します。たとえば、ワークフローを構成して、vSphere 仮想マシンやグループに属する Active Directory ユーザーの作成や、PowerShell スクリプトの実行を行うことができます。カスタムの vRealize Orchestrator ワークフローを作成した場合、サービス カatalogのアイテムとしてこのワークフローを提供することで、資格のあるユーザーはこのワークフローを実行することができます。

XaaS ブループリントは、デザイン キャンバスに作成するブループリントのコンポーネントとして使用することも、サービス カatalogに直接公開することもできます。

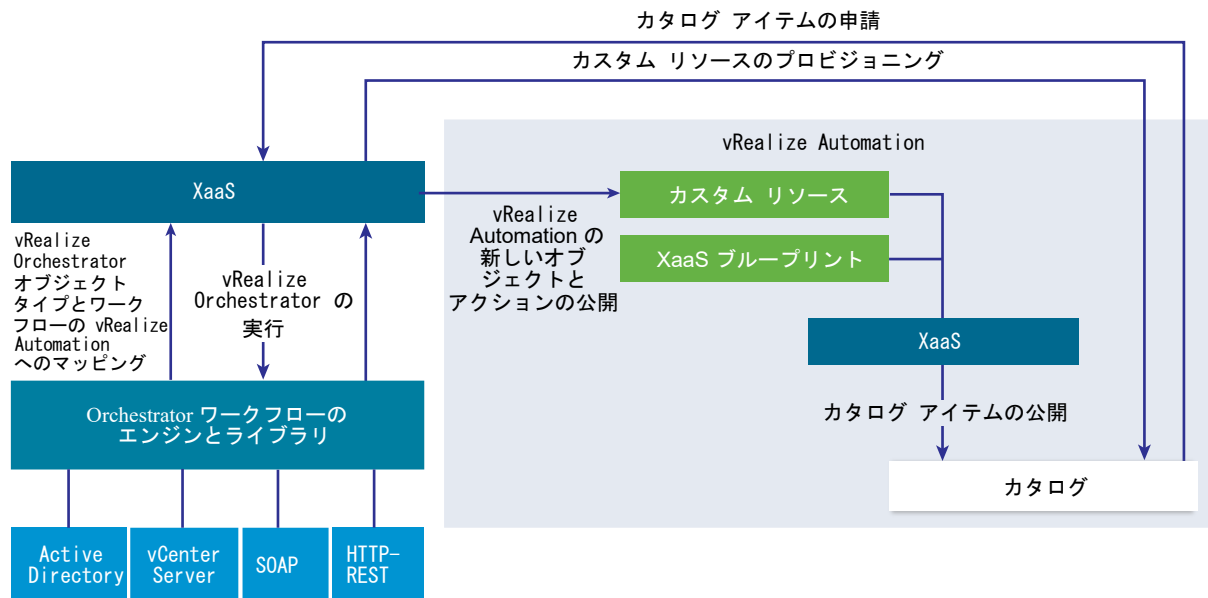
ブループリントを別のブループリントのコンポーネントとして使用する場合、展開されたブループリントをスケールインまたはスケールアウトするときにそのブループリントがスケーリングされるように構成できます。

vRealize Automation 内での vRealize Orchestrator の統合

vRealize Orchestrator は、vRealize Automation 内に統合されたワークフロー エンジンです。

vRealize Automation とともに配布された vRealize Orchestrator サーバは事前構成されているため、システム管理者が vRealize Automation Appliance を展開するときには、vRealize Orchestrator サーバは起動されて実行されています。

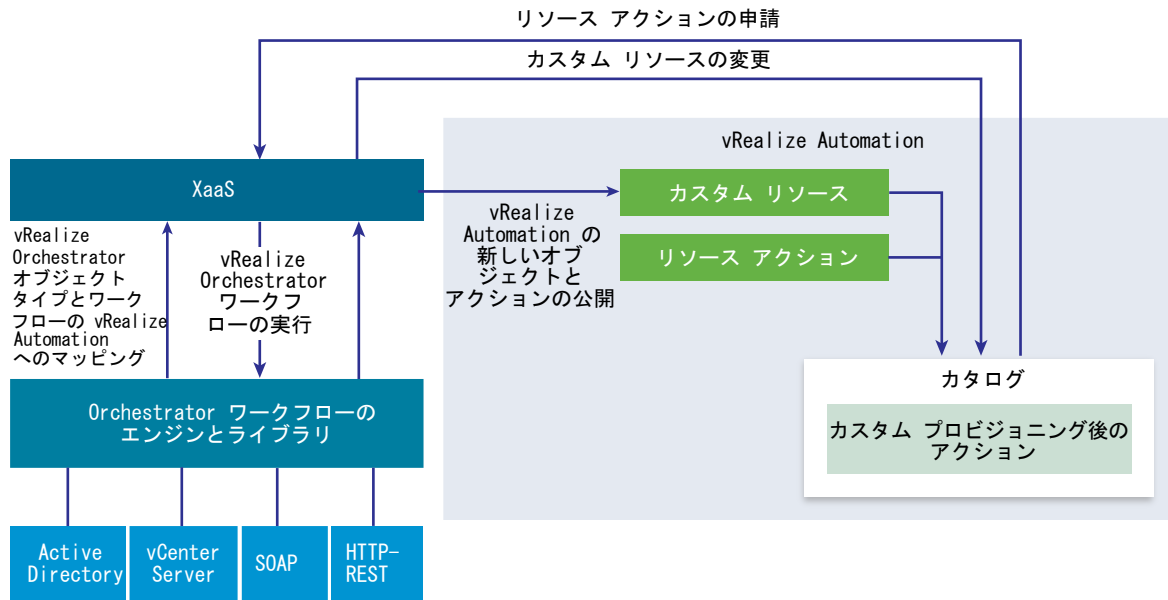
図 3-2. XaaS に含まれているカタログ アイテムを作成および申請して、カスタム リソースをプロビジョニングする



XaaS アーキテクトは、サポートされているエンドポイントと提供されているワークフローに関連するカスタム リソースを追加し、それらのリソースに基づいて XaaS のブループリントとアクションを作成します。テナント管理者とビジネス グループ マネージャは、XaaS のブループリントとアクションをサービス カタログに追加できます。XaaS ブループリントは、ブループリント デザイナでも使用できます。

サービス カタログ ユーザーがアイテムを申請すると、vRealize Automation は vRealize Orchestrator ワークフローを実行して、カスタム リソースをプロビジョニングします。

図 3-3. カスタム リソースを変更するためのカスタム リソース アクションの作成と申請



また、XaaS アーキテクトは、vRealize Orchestrator ワークフローをリソース アクションとして追加することで、vRealize Automation の機能を拡張することもできます。サービス カタログ ユーザーは、カスタム リソースをプロビジョニングした後、プロビジョニング後のアクションを実行できます。ユーザーはこのように vRealize Orchestrator ワークフローを実行して、プロビジョニング済みカスタム リソースを変更します。

サービス カタログ ユーザーがカタログ アイテムとして XaaS ブループリントまたはリソース アクションを申請すると、XaaS サービスは対応する vRealize Orchestrator ワークフローを実行して、次のデータをグローバル パラメータとしてワークフローに渡します。

表 3-51. XaaS グローバル パラメータ

パラメータ	説明
__asd_tenantRef	ワークフローを申請するユーザーのテナント
__asd_subtenantRef	ワークフローを申請するユーザーのビジネス グループ
__asd_catalogRequestId	このワークフロー実行に対する、カタログからの申請 ID
__asd_requestedFor	申請のターゲット ユーザー。申請がユーザーの代わりに行われる場合は、ターゲット ユーザーは、ワークフローの申請対象の代わりのユーザーであり、それ以外の場合は、ワークフローを申請しているユーザーになります。
__asd_requestedBy	ワークフローを申請するユーザー

XaaS ブループリントまたはリソース アクションで、ユーザー操作スキーマ要素を含む vRealize Orchestrator ワークフローが使用される場合、ユーザーがサービスを申請すると、ワークフローは自身の実行をサスペンドして、ユーザーによって必須データが指定されるまで待機します。待機中のユーザー操作に対応するには、[受信箱] - [手動ユーザー アクション] に移動する必要があります。

デフォルトの vRealize Orchestrator サーバ インベントリはすべてのテナントで共有されており、テナントごとに使用することはできません。たとえば、サービス アーキテクトが、クラスタ コンピュート リソースを作成するためのサービス ブループリントを作成する場合、各種テナントのユーザーは、別々のテナントに属していても、すべての vCenter Server インスタンスのインベントリ アイテムを検索する必要があります。

システム管理者は別個に vRealize Orchestrator をインストールするか vRealize Orchestrator Appliance を展開することで、外部 vRealize Orchestrator インスタンスを設定して、外部 vRealize Orchestrator インスタンスと連携するように vRealize Automation を構成することができます。

また、システム管理者は、テナントごとに vRealize Orchestrator ワークフロー カテゴリを構成して、各テナントが利用できるワークフローを定義することができます。

さらに、テナント管理者は外部 vRealize Orchestrator インスタンスを構成することもできますが、自身のテナントの分だけしか構成できません。

外部 vRealize Orchestrator インスタンスと vRealize Orchestrator ワークフロー カテゴリを構成する方法については、『vCenter Orchestrator とプラグインの構成』を参照してください。

vRealize Orchestrator プラグインのリスト

プラグインを利用すると、vRealize Orchestrator を使用して、外部のテクノロジーおよびアプリケーションにアクセスし、制御することができます。vRealize Orchestrator プラグインで外部テクノロジーを公開することで、外部テクノロジーのオブジェクトと関数にアクセスするワークフローにオブジェクトおよび関数を組み込むことができます。

プラグインを使用してアクセスできる外部テクノロジーには、仮想化管理ツール、電子メール システム、データベース、ディレクトリ サービス、リモート制御インターフェイスなどがあります。

標準セットの vRealize Orchestrator プラグインを使用して、vCenter Server API および電子メール機能などの外部テクノロジーをワークフローに組み込むことができます。また、vRealize Orchestrator オープン プラグイン アーキテクチャを使用し、他のアプリケーションにアクセスするためのプラグインを開発できます。

表 3-52. vRealize Orchestrator にデフォルトで含まれるプラグイン

プラグイン	目的
vCenter Server	vRealize Orchestrator を使用して自動化する管理プロセスに vCenter Server のすべてのオブジェクトおよび関数を組み込むことができるように、vCenter Server API へのアクセスを提供します。
構成	vRealize Orchestrator の認証、データベース接続、SSL 証明書などを構成するためのワークフローを提供します。
vCO ライブラリ	クライアント プロセスのカスタマイズおよび自動化の基本的な構成要素として機能するワークフローを提供します。ワークフロー ライブラリには、ライフ サイクル管理、プロビジョニング、ディザスタ リカバリ、ホット バックアップ、および他の標準プロセスのテンプレートが含まれます。テンプレートのコピーおよび編集を行い、ニーズに応じてテンプレートを変更できます。
SQL	Java Database Connectivity (JDBC) API を提供します。これは、Java プログラミング言語とさまざまなデータベースの間で利用されるデータベースに依存しない接続方法であり、業界標準です。このようなデータベースには、スプレッドシートまたはフラットファイルなど、SQL データベースおよび他の表形式データ ソースがあります。JDBC API は、ワークフローから SQL ベースのデータベースにアクセスするためのコール レベル API を提供します。

表 3-52. vRealize Orchestrator にデフォルトで含まれるプラグイン（続き）

プラグイン	目的
SSH	Secure Shell v2 (SSH-2) プロトコルの実装を提供します。ワークフローでパスワードと公開鍵ベースの認証を使用して、リモート コマンドおよびファイル転送セッションを実行できます。キーボード操作による認証をサポートしています。必要に応じて、SSH プラグインにより、vRealize Orchestrator クライアント インベントリ内を直接参照するリモート ファイル システムを提供できます。
XML	ワークフローに実装できる Document Object Model (DOM) XML パーサーです。また、vRealize Orchestrator JavaScript API で ECMAScript for XML (E4X) 実装を使用できます。
メール	簡易メール転送プロトコル (SMTP) を使用してワークフローから電子メールを送信します。
ネットワーク	Jakarta Apache Commons Net Library をラップします。Telnet、FTP、POP3、および IMAP の実装を提供します。POP3 および IMAP 部分は、電子メールを読み取るために使用します。Mail プラグインと Net プラグインを組み合わせ、ワークフローに電子メールの包括的な送信機能と受信機能を提供します。
列挙	他のプラグインがワークフローで使用できる一般的な列挙値を提供します。
ワークフロー ドキュメント	ワークフローまたはワークフロー カテゴリに関して PDF 形式で情報を生成できるワークフローを提供します。
HTTP-REST	vCenter Orchestrator と REST のホスト間の通信を確立することで、REST Web サービスを管理できます。
SOAP	vCenter Orchestrator と SOAP のホスト間の通信を確立することで、SOAP Web サービスを管理できます。
AMQP	ブローカーとも呼ばれる Advanced Message Queuing Protocol (AMQP) サーバと通信できます。
SNMP	SNMP 対応システムおよびデバイスに接続して情報を受信できるように vCenter Orchestrator を有効にします。
Active Directory	vCenter Orchestrator と Microsoft Active Directory 間の通信を確立します。
vCO WebOperator	vRealize Orchestrator ライブラリのワークフローにアクセスし、Web ブラウザを使用してネットワーク全体でワークフローと通信できるようにする Web ビューです。
動的タイプ	動的タイプを定義し、この動的タイプのオブジェクトを作成して使用できます。
PowerShell	PowerShell ホストを管理し、カスタム PowerShell 操作を実行できます。
マルチノード	階層オーケストレーション、Orchestrator インスタンスの管理、および Orchestrator アクティビティのスケールアウトのワークフローが含まれています。
vRealize Automation	vRealize Orchestrator と vRealize Automation 間の通信用ワークフローを作成して実行できます。

VMware が開発して配布する vRealize Orchestrator プラグインに関する詳細については、VMware vRealize Orchestrator のドキュメントのランディング ページを参照してください。

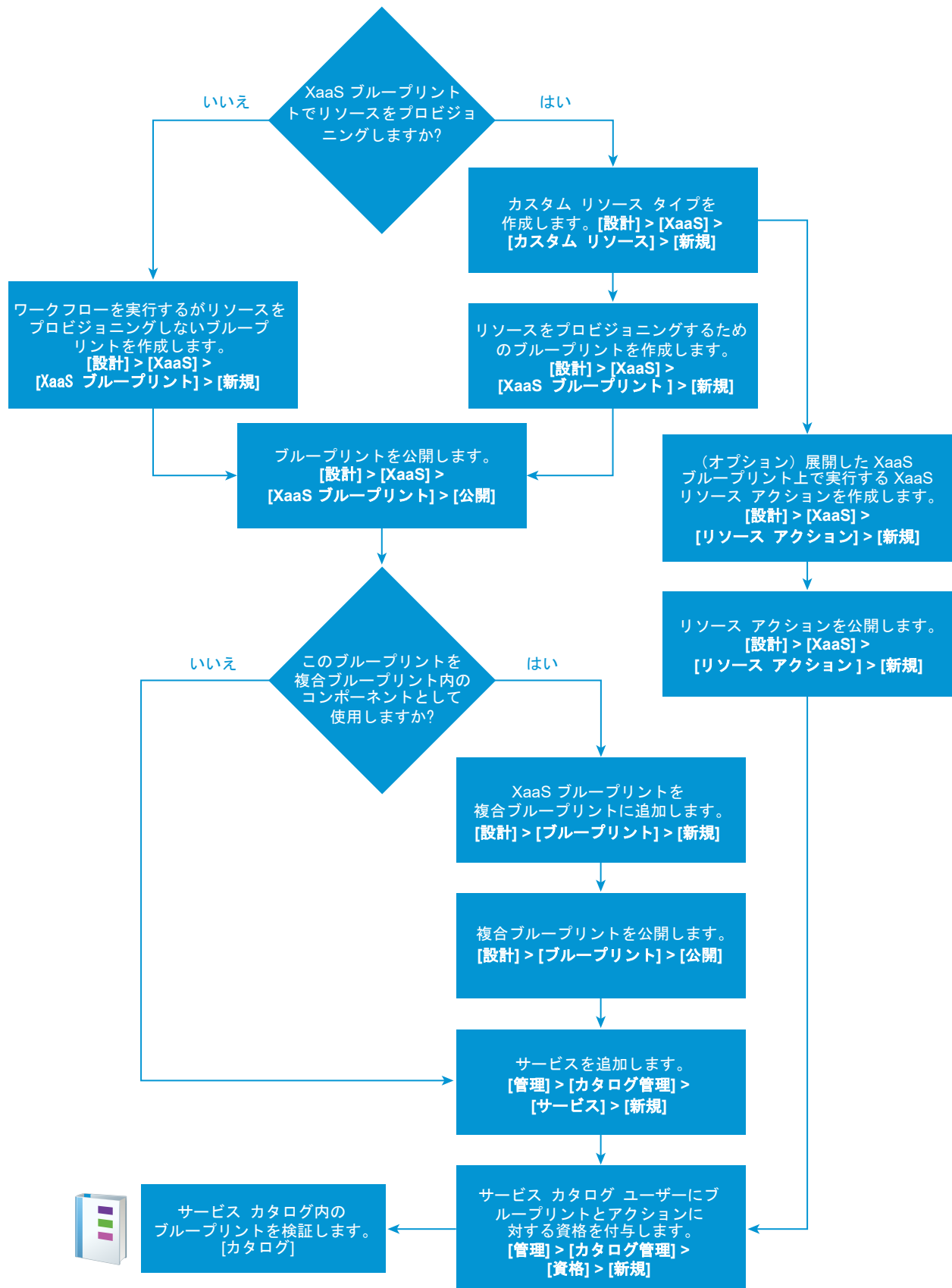
XaaS ブループリントおよびリソース アクションの作成

XaaS ブループリントは、カタログ アイテムとしてユーザーが使用でき、デザイン キャンバスを使用して 1 つの複合ブループリントにまとめることができます。リソース アクションは、プロビジョニングされたアイテム上で実行され、プロビジョニング後のアイテムを管理します。

たとえば、XaaS ブループリントを使用し、グループ内に Active Directory ユーザーを作成できます。その後、リソース アクションを使用し、ユーザーによるパスワードの変更を要求することができます。

XaaS ブループリント ワークフロー

XaaS ブループリントおよびオプションのリソース アクションを作成するために従うワークフローは、ブループリントをどのように使用するかに応じて異なります。次のワークフローは、基本的なプロセスを提供します。



XaaS ブループリントの用語

XaaS ブループリントは、リソースをプロビジョニングしたり、プロビジョニングされたリソースを変更したり、お使用の環境でタスクを実行するサービスとして動作させることができる、vRealize Orchestrator のワークフローです。ブループリントとリソース アクションには、微妙な違いのある用語がいくつかあります。サービス カタログ ユーザー用のブループリントを設計するときには、これらを理解しておく必要があります。

以下の定義は、XaaS ブループリントを操作するときに使われる用語を理解するのに役立ちます。

カスタム リソース

vRealize Orchestrator プラグインの API を介してリソースとして公開される vRealize Orchestrator のオブジェクト タイプ。カスタム リソースを作成して、XaaS プロビジョニング ブループリントの出力パラメータを定義し、リソース アクションの入力パラメータを定義します。

XaaS ブループリント コンポーネント

ブループリント デザイン キャンバスで利用できるプロビジョニングまたは非プロビジョニング ブループリント。このタイプのブループリントは、スタンドアロン XaaS ブループリントの場合もあります。

スタンドアロン XaaS ブループリント

サービス カタログで直接使用可能な、公開されているプロビジョニングまたは非プロビジョニング ブループリント。

プロビジョニング ブループリント

vRealize Orchestrator のワークフローを実行し、エンドポイント用の vRealize Orchestrator プラグイン API を使用してターゲットのエンドポイントにリソースをプロビジョニングするプロビジョニング ブループリント。たとえば、仮想 NIC を vSphere のネットワーク デバイスに追加するブループリントです。プロビジョニング ブループリントを作成するには、vRealize Orchestrator のリソース タイプを定義したカスタム リソースが必要です。

サービス カタログのユーザーがこのタイプのカatalog アイテムをリクエストすると、ワークフローがアイテムをプロビジョニングします。展開したアイテムは [展開] タブに保存されます。このタイプのプロビジョニングされるリソースに対しては、プロビジョニング後の操作を定義できます。必要な場合は、インスタンスを追加または削除することで、ブループリントを拡張可能なものにすることもできます。

非プロビジョニング ブループリント

非プロビジョニング ブループリントは、エンドポイント変更用の API が不要なタスクを行う vRealize Orchestrator ワークフローを実行します。たとえば、レポートを作成し、ターゲットの通信システムにレポートを E メール送信または投稿するワークフローです。

サービス カタログのユーザーがこのタイプのカatalog アイテムをリクエストすると、ワークフローがスクリプト化されたタスクを実行します。ただし、展開したアイテムは [展開] タブに保存されません。このタイプのブループリントでは、プロビジョニング後の操作を実行できません。非プロビジョニング ブループリントは、拡張可能なブループリントのサポート ワークフローとして使用できます。たとえば、ブループリントを作成して高可用性ロードバランサを更新することが可能です。

複合ブループリント

デザイン キャンバスを使用して作成したブループリント。複合ブループリントは 1 つ以上のコンポーネントを使用します。たとえば、マシン コンポーネント、ソフトウェア コンポーネント、XaaS コンポーネントなどです。コンポーネントをサービスに追加すると、展開として表示されます。コンポーネントを資格に追加してサービス カタログのユーザーが利用できるようにすると、複合ブループリントとして表示されます。複合ブループリントは、1 つのブループリント コンポーネントから成るものも可能です。また、複数のマシン、ソフトウェア、およびネットワークを備えたアプリケーション全体を含めることもできます。

リソース アクション

展開したプロビジョニング ブループリントで実行できるワークフロー。展開したブループリントは、XaaS ブループリントでもブループリント コンポーネントでも、vRealize Orchestrator のリソース タイプにマップしたマシン タイプでも構いません。

XaaS ブループリントの設計上の考慮事項

XaaS ブループリントを作成する前に、リソースを正しくプロビジョニングするブループリントを作成できるように、ブループリントの目的を理解する必要があります。

XaaS ブループリントは、デザイン キャンバス内のブループリント コンポーネントとして、またはスタンドアロンのブループリントとして作成および使用できます。ブループリントは、プロビジョニング ブループリントと非プロビジョニング ブループリントのどちらにもすることが可能です。

表 3-53. XaaS ブループリントのタイプと結果

XaaS ブループリントのタイプ	カスタム リソースが必須	ブループリントを展開時に拡張可能	展開済みのブループリントに対してリソース アクションを実行可能
リソースをプロビジョニングするブループリント コンポーネント	はい	はい。 拡張するように構成されている場合は、展開を拡張するとブループリントも拡張します。	はい。 展開が拡張されるとブループリントも拡張します。また、展開済みのコンポーネントに対して他のリソース アクションを実行できます。 ブループリント コンポーネントは [展開] タブに表示されます。
ワークフローは実行するが、リソースはプロビジョニングしないブループリント コンポーネント	いいえ。 ブループリントは vRealize Orchestrator のサーバ構成を使用しますが、XaaS のカスタム リソースは必要としません。	いいえ。 リソースはプロビジョニングしませんが、拡張処理の一部として実行することは可能です。 たとえば、拡張処理を基にした新しい構成を使用してロード バランサを更新できます。	いいえ。 非プロビジョニング コンポーネントに対してリソース アクションを実行することはできません。

表 3-53. XaaS ブループリントのタイプと結果（続き）

XaaS ブループリントのタイプ	カスタム リソースが必須	ブループリントを展開時に拡張可能	展開済みのブループリントに対してリソース アクションを実行可能
リソースをプロビジョニングする スタンドアロンのブループリント	はい	いいえ。 インスタンスを追加または削除するには、リソース アクションを作成する必要があります。	はい。 拡張に対応するために作成したアクションなど、リソース アクションを展開済みのリソースに対して実行できます。 ブループリントは [展開] タブに表示されます。
ワークフローは実行するが、リソースはプロビジョニングしない スタンドアロン ブループリント	いいえ。 ブループリントは vRealize Orchestrator のサーバ構成を使用しますが、XaaS のカスタム リソースは必要としません。	いいえ。 リソースはプロビジョニングしませんが、リソース アクションの一部として実行することは可能です。	いいえ。 非プロビジョニング コンポーネントに対してリソース アクションを実行することはできません。

XaaS カスタム リソースの追加

カスタム リソースを作成し、プロビジョニング用に XaaS アイテムを定義します。XaaS ブループリントまたはアクションを作成するには、ブループリントまたはアクション ワークフローのオブジェクト タイプと互換性のあるカスタム リソースが必要です。

カスタム リソースを作成することで、vRealize Orchestrator プラグインの API を介して公開されるオブジェクト タイプをリソースとしてマップします。カスタム リソースを使用して、プロビジョニング用の XaaS ブループリントの出力パラメータを定義し、リソース アクションの入力パラメータを定義します。


ブループリントまたはリソース アクション ワークフローがリソースをプロビジョニングしない場合や展開されたブループリントで実行されない場合は、カスタム リソースを作成する必要はありません。たとえば、ワークフローがプロビジョニング操作後にデータベース値を更新する場合や E メール メッセージを送信する場合は、カスタム リソースは必要ありません。

カスタムリソースを作成するとき、プロビジョニングされたアイテムの詳細に関する読み取り専用フォームのフィールドを指定できます。[カスタム リソース フォームの設計](#)を参照してください。

前提条件

- XaaS アーキテクトとして vRealize Automation にログインします。
- 詳細オプション情報を使用して、カスタム リソースを構成します。[XaaS カスタム リソース ウィザード オプション](#)を参照してください。

手順

- 1 [設計] - [XaaS] - [カスタム リソース] を選択します。
- 2 [新規] アイコン（）をクリックします。

3 [リソース タイプ] タブの値を構成します。

- a [Orchestrator タイプ] テキスト ボックスで vRealize Orchestrator オブジェクト タイプを入力するか選択します。

たとえば、文字 v を含むタイプを表示するには、**v** と入力します。すべてのタイプを表示するには、スペースを入力します。

- b 名前と説明（説明は任意）を入力します。

- c バージョンを入力します。

<メジャー>.<マイナー>.<マイクロ>-<リビジョン>の形式がサポートされています。

- d [次へ] をクリックします。

4 必要に応じて [詳細フォーム] タブを編集します。

要素を削除、編集、再配置することでカスタム リソース フォームを編集できます。フォームおよびフォーム ページを追加し、要素を新規フォームおよびフォーム ページにドラッグすることもできます。

5 [完了] をクリックします。

結果

カスタム リソースが作成され、[カスタム リソース] ページに表示されます。このカスタム リソースに基づいて XaaS ブループリントまたはアクションを作成できます。

次のステップ

- XaaS ブループリントを作成します。 [XaaS ブループリントの追加](#)を参照してください。
- XaaS リソース アクションを作成します。 [XaaS リソース アクションの作成](#)を参照してください。

XaaS カスタム リソース ウィザード オプション

これらのカスタム リソース オプションは、カスタム リソースを作成または変更するために使用します。これにより、リソースのプロビジョニングや、プロビジョニングされたリソースの変更を行う XaaS ブループリントとリソース アクション ワークフローを実行することができます。

1つのオブジェクト タイプにつき、カスタム リソースを1つのみ作成できます。このカスタム リソースは、複数のブループリントおよびリソース アクションに使用することができます。

カスタム リソース アクションを作成するには、[設計] - [XaaS] - [カスタム リソース] を選択します。

[リソース タイプ]

構成された vRealize Orchestrator インスタンスにインストールされたプラグインに基づいて [リソース タイプ] タブに表示される、使用可能なオブジェクト タイプの一覧です。vRealize Automation は、構成された vRealize Orchestrator インスタンスから値を収集します。

表 3-54. [リソース タイプ] のオプション

オプション	説明
[Orchestrator タイプ]	<p>プロビジョニングに使用するワークフローをサポートするタイプを入力または選択します。</p> <p>このタイプは、スクリプティング API で表示されるプラグイン名（たとえば、VC for vCenter など）およびオブジェクト タイプ（たとえば、VirtualMachine など）で構成されます。この例では、API は VC:VirtualMachine という値を使用しています。</p> <p>このタイプは、ブループリント ワークフローの出力パラメータまたはリソース アクション ワークフローの入力パラメータとして使用することができます。</p>
[名前]	XaaS ブループリントまたはリソース アクションの作成時に区別できるように、わかりやすいカスタム リソース名を入力します。
[説明]	詳細な説明を入力します。
[バージョン]	<メジャー>.<マイナー>.<マイクロ>-<リビジョン>のフォームがサポートされています。

[詳細フォーム]

これらのフォーム フィールドは、サービス カタログ ユーザーがこのカスタム リソースを使用するアイテムをプロビジョニングする際に、読み取り専用の値として表示されます。既存のフィールドを変更したり、外部で定義された新しいフィールドを追加したりすることもできます。

フォームの構成に関する詳細については、[カスタム リソース フォームの設計](#)を参照してください。

[使用場所]

1 つのオブジェクト タイプにつき、作成できるカスタム リソースは 1 つのみであるため、このウィザードのページでカスタム リソースがどのように使用されているかを確認することができます。

このタブは保存されたカスタム リソースで使用可能であり、リソースの作成時には使用できません。

表 3-55. [使用場所] のオプション

オプション	説明
[XaaS ブループリント]	<p>このカスタム リソースを使用するために構成されるブループリントの一覧です。</p> <p>このページから、次のアクションを実行することができます。</p> <ul style="list-style-type: none"> ■ [編集]。ブループリントを開きます。構成情報の表示または変更ができます。 ■ [公開/公開解除]。複合ブループリントでの使用またはサービスへの追加を可能にすることで、ブループリントの状態を変更します。ブループリントを公開解除した場合、複合ブループリントでの使用およびサービスへの追加ができなくなる可能性があるほか、サービス カタログ内でも使用不能になる可能性があります。 ■ [削除]。システムからこのブループリントを削除します。
[リソース アクション]	<p>このカスタム リソースを使用するために構成されるリソース アクションの一覧です。</p> <p>このページから、次のアクションを実行することができます。</p> <ul style="list-style-type: none"> ■ [編集]。リソース アクションを開きます。構成情報の表示または変更ができます。 ■ [公開/公開解除]。資格内で使用可能にすることで、リソース アクションの状態を変更します。リソース アクションを公開解除した場合、サービスへの追加ができなくなる可能性があるほか、展開されたブループリント上で実行できなくなる可能性があります。 ■ [削除]。システムからこのリソース アクションを削除します。

XaaS ブループリントの作成

XaaS ブループリントには、プロビジョニング用のブループリントと、それ以外のブループリントとがあります。提供されている vRealize Orchestrator プロビジョニング ワークフローの一部には、仮想マシンの作成、Active Directory へのユーザーの追加、または仮想マシン スナップショットの作成が含まれます。プロビジョニング用ではないワークフローは、たとえばロード バランサーを更新したり、レポートを作成して受信者に送信したりする場合に作成します。

XaaS ブループリントの作成には、vRealize Orchestrator に用意されているワークフローをベースとして使用できるほか、ご利用の環境に固有の目的を果たすために独自のワークフローを作成して使用することもできます。

手順

1 XaaS ブループリントの追加

XaaS ブループリントとは、ご利用の環境内のターゲット システムに変更を加える vRealize Orchestrator ワークフローの実行に関する仕様です。ブループリントには、このワークフローが含まれているほか、入力パラメータ、送信フォーム、読み取り専用フォーム、アクションの順序、プロビジョニング操作、非プロビジョニング操作を追加することができます。

2 複合ブループリントへの XaaS ブループリントの追加

XaaS ブループリントを複合ブループリントのコンポーネントとして追加する方法は、デザイン キャンバスで他のブループリント コンポーネントを追加するときと似ています。

XaaS ブループリントの追加

XaaS ブループリントとは、ご利用の環境内のターゲット システムに変更を加える vRealize Orchestrator ワークフローの実行に関する仕様です。ブループリントには、このワークフローが含まれているほか、入力パラメータ、送信フォーム、読み取り専用フォーム、アクションの順序、プロビジョニング操作、非プロビジョニング操作を追加することができます。

使用する XaaS ブループリントは、次のような方法で作成できます。

- XaaS ブループリント コンポーネントを作成する。コンポーネント ブループリントは、ブループリントのデザイン キャンバスで複合ブループリントの構成要素として使用できるプロビジョニング ブループリントまたは非プロビジョニング ブループリントです。ブループリントをコンポーネントとして使用する場合は、展開済みの複合ブループリントのスケールイン操作とスケールアウト操作をサポートするコンポーネントのライフサイクル オプションを構成する必要があります。

また、このタイプのブループリントは、スタンドアロン ブループリントとして公開することもできます。


- スタンドアロン XaaS ブループリントを作成する。スタンドアロン ブループリントは、サービス カタログに公開されて直接資格が付与されるプロビジョニング ブループリントまたは非プロビジョニング ブループリントです。

XaaS ブループリントを使用して Active Directory ユーザーを作成する方法の例については、[ユーザーを作成および変更するための XaaS ブループリントとアクションの作成](#) を参照してください。

前提条件

- XaaS アーキテクトとして vRealize Automation にログインします。
- ブループリントでリソースをプロビジョニングする必要がある場合、サービス ブループリントの出力パラメータに対応するカスタム リソースを作成します。[XaaS カスタム リソースの追加](#)を参照してください。vRealize Orchestrator プラグイン API を使用していない場合、カスタム リソースを構成する必要はありません。
- XaaS ブループリントを作成するということは、コンポーネント ブループリントまたはカタログ アイテムとして vRealize Orchestrator ワークフローを公開することになります。ブループリントには、編集可能なフォームが含まれています。[XaaS ブループリント フォームの設計](#)を参照してください。
- ブループリントの構成は、詳細オプションの情報を使用して行います。[XaaS ブループリントの新規作成または編集ウィザードのオプション](#)を参照してください。

手順

- 1 [設計] - [XaaS] - [XaaS ブループリント] を選択します。
- 2 [新規] アイコン () をクリックします。

- 3 ブループリントでリソースをプロビジョニングするときに実行されるワークフローを [ワークフロー] タブで選択します。

ブループリントの編集では、このタブを利用できません。

- a vRealize Orchestrator ワークフロー ライブラリを参照して、カスタム リソースに関連するワークフローを選択します。
 - b 後から正しく値を指定できるように入力パラメータと出力パラメータを確認しておきます。
 - c [次へ] をクリックします。
- 4 [全般] タブでオプションを構成し、[次へ] をクリックします。
 - a 同様のブループリントと区別するために、[名前] テキスト ボックスにこのブループリントの名前を入力します。
 - b このブループリントを複合ブループリントのコンポーネントとして使用しない場合は、[デザイン キャンバスのコンポーネントとして利用可能にする] チェック ボックスを選択解除します。
 - 5 [ブループリント フォーム] タブで、必要に応じてフォームを編集し、[次へ] をクリックします。
 - 6 [プロビジョニングされたリソース] ページで値を選択し、[次へ] をクリックします。

オプション	説明
プロビジョニングなし	このワークフローでリソースをプロビジョニングしない場合は、このオプションを選択するか、またはフィールドを空にしてください。
<以前に作成したカスタム リソース>	このプロビジョニング ワークフローをサポートするカスタム リソースを選択します。

- 7 スケールイン、スケールアウト、破棄の各操作時のこのブループリントの動作を [コンポーネント ライフサイクル] タブで定義します。

これらのワークフローは、このブループリントを構成要素として含む、展開済みの複合ブループリントで実行されます。各種オプションの利用の可否は、ブループリントによって異なります。ブループリントのワークフローによっては一部のオプションがサポートされていない場合や、省略できない場合があります。

- 8 [完了] をクリックします。
- 9 目的のブループリントの行を選択し、[公開] をクリックします。

結果

XaaS ブループリントの作成と公開は以上です。

次のステップ

- このブループリントをスタンドアロン ブループリントとして直接サービス カタログに追加するには、サービスを追加したうえで、目的のブループリントをサービスに追加します。[サービスの追加](#)を参照してください。
- このブループリントを複合ブループリントのコンポーネントとして使用する場合は、[複合ブループリントへの XaaS ブループリントの追加](#)を参照してください。

XaaS ブループリントの新規作成または編集ウィザードのオプション

これらのオプションは、展開される際に vRealize Orchestrator ワークフローを実行する XaaS ブループリントの作成に使用します。このワークフローは環境内でターゲット システムを変更します。

ブループリントの作成の手順については、[XaaS ブループリントの追加](#)を参照してください。

このウィザードを使用するには、[設計] - [XaaS] - [XaaS ブループリント] を選択します。

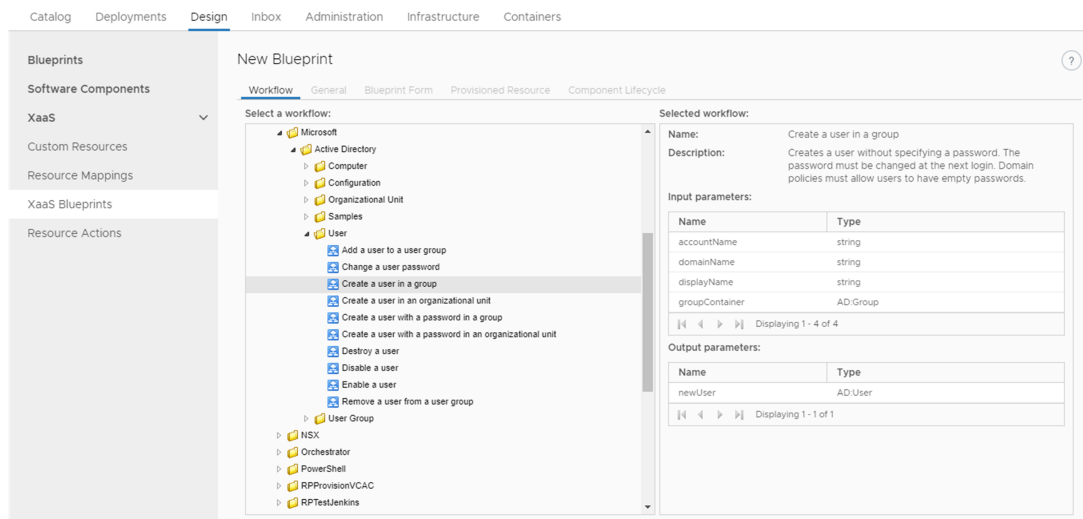
[ワークフロー] タブ

ブループリントがリソースをプロビジョニングする際に実行されるワークフローを選択します。

ブループリントの編集では、このタブを利用できません。

次の図では、ワークフロー ツリーが左側に表示されており、パラメータが右側に表示されています。

図 3-4. XaaS ブループリント ウィザード内の [ワークフロー] タブ



入力および出力パラメータを確認し、自分またはサービス カタログ ユーザーが次の状況下で正しい値を入力できることを確認します。

- このウィザードまたはブループリント デザイン キャンバスでブループリント フォームをカスタマイズしたとき。
- 入力パラメータをすべて空白のままにして、サービス カタログ ユーザーが値を設定できるかどうか。

[全般] タブ

ブループリントとその動作のメタデータを設定します。

表 3-56. [全般] タブのオプション

オプション	説明
[名前]	次の場所に表示させることのできるブループリントの名前です。 <ul style="list-style-type: none"> ■ デザイン キャンバス。[デザイン キャンバスのコンポーネントとして利用可能にする] を選択した場合、この値がカテゴリのリストに名前として表示されます。 ■ サービス。ブループリントをスタンドアロン ブループリントとして使用した場合、この値がカタログ アイテムをサービスに追加する際の名前として表示されます。 ■ 資格。ブループリントに個々のアイテムとしての資格を付与した場合、この値が [アイテムの追加] リストに名前として表示されます。
[説明]	詳細な説明を入力し、類似のアイテムと区別できるようにします。
[カタログ申請情報ページを非表示にする]	チェック ボックスを選択すると、サービス カatalog ユーザーがアイテムを要求する際、説明と理由の入力が不要になります。デフォルトではこのチェック ボックスは選択されています。
[バージョン]	<メジャー>.<マイナー>.<マイクロ>-<リビジョン>の形式がサポートされています。
[デザイン キャンバスのコンポーネントとして利用可能にする]	ブループリントをデザイン キャンバス ブループリントのコンポーネントとして使用する場合、このオプションを選択します。 公開されたブループリントは、カスタム リソースを設定したときに選択したカテゴリ内で使用できるようになります。 このオプションを選択しなかった場合、ブループリントはデザイン キャンバスに表示されません。ただしその場合でも、ブループリントをサービスに追加し、ユーザーにスタンドアロン ブループリントとして展開する資格を付与することが可能です。

[ブループリント フォーム] タブ

このウィザードのページに表示されるフィールドは、ワークフロー入力パラメータです。次の変更のうち、1 つ以上を実施することができます。

- フォームへのフィールドの追加。
- フィールドの削除や編集などによる既存のフィールドの変更。
- 入力パラメータとしてのデフォルト値の入力。

このような変更は、次のユーザーに表示されるフォームに影響します。

- XaaS ブループリントがブループリント コンポーネントとして使用される場合、デザイン キャンバスで作業しているアプリケーション アーキテクト。
- ブループリントがスタンドアロン ブループリントとして公開される場合、サービス カatalog ユーザー。

フォームの構成に関する詳細については、[XaaS ブループリント フォームの設計](#)を参照してください。

[プロビジョニングされたリソース]

プロビジョニングされたリソースは、関連する XaaS カスタム リソースにブループリントをリンクさせます。このカスタム リソースは、[設計] - [XaaS] - [カスタム リソース] の [カスタム リソース] ページで設定したものです。

表 3-57. [プロビジョニングされたリソース] のオプション

オプション	説明
[以前に作成したカスタム リソース]	<p>プロビジョニング ブループリントの実行に必要な vRealize Orchestrator リソース タイプを定義するカスタム リソースを選択します。</p> <p>プロビジョニング ブループリントは、vRealize Orchestrator ワークフローを実行してターゲット エンドポイントにリソースをプロビジョニングします。このとき、エンドポイントには vRealize Orchestrator プラグイン API を使用します。たとえば、仮想 NIC を vSphere のネットワーク デバイスに追加するブループリントです。</p> <p>このタイプのプロビジョニングされるリソースに対しては、プロビジョニング後の操作を定義できます。必要に応じてインスタンスを追加または削除することで、ブループリントを拡張可能にすることもできます。</p> <p>結果</p> <ul style="list-style-type: none"> ■ ブループリントは拡張することが可能です。 ■ ブループリントは、選択されたカスタム リソース向けに指定された、デザイン キャンパスのカテゴリ内に表示されます。 ■ アイテムを含むブループリントを展開した場合、ブループリントは [展開] タブに表示されます。展開後はそのアイテム上で任意のアクションを実行することができます。
[プロビジョニングなし]	<p>非プロビジョニング ブループリントは、エンドポイント変更用の API が不要なタスクを行う vRealize Orchestrator ワークフローを実行します。たとえば、レポートと E メールを作成したり、それをターゲット通信システムへ投稿したりすることが該当します。</p> <p>結果</p> <ul style="list-style-type: none"> ■ ブループリントは拡張することができません。非プロビジョニング ブループリントは、拡張可能なブループリントのサポート ワークフローとして使用できます。たとえば、ブループリントを作成して高可用性ロードバランサを更新することが可能です。 ■ ブループリントは、デザイン キャンパスの XaaS カテゴリに表示されます。 ■ アイテムを含むブループリントを展開した場合でも、ブループリントは [展開] タブに表示されません。展開後もそのアイテム上ではいかなるアクションも実行することができません。

[コンポーネントのライフサイクル] タブ

[コンポーネントのライフサイクル] タブは、[デザイン キャンパスのコンポーネントとして利用可能にする] を [全般] タブで選択したときに使用可能になります。

これらのオプションは、ブループリントが複合ブループリント内のコンポーネントとして使用されているとき、展開後のスケール インとスケールアウトの操作時におけるブループリントの動作を定義するために使用します。

各オプションは、ブループリントによっては使用できない場合があります。ブループリントのワークフローによっては一部のオプションがサポートされていない場合や、省略できない場合があります。XaaS が複合ブループリントで使用されている可能性があるため、ブループリントを正しく拡張するための更新および削除オプションがブループリントで使用可能な場合は、割り当ておよび割り当て解除オプションと同様に、更新および削除オプションも設定する必要があります。

表 3-58. [コンポーネントのライフサイクル] オプション

オプション	説明
[拡張可能]	<p>このオプションを選択すると、サービス カタログ ユーザーが、スケール インまたはスケール アウトの操作の一環として、このブループリント コンポーネントのインスタンス数を展開後に変更することが可能になります。</p> <p>このオプションは、[プロビジョニングされたリソース] タブでカスタム リソースを選択した場合に使用できます。[プロビジョニングなし] のオプションを選択した場合、このオプションは使用できません。</p> <p>ブループリントを拡張可能にする場合、デザイン キャンバスの [全般] タブに [インスタンス] オプションが追加されます。次の例を参照してください。[拡張可能] を選択しない場合、[インスタンス] オプションはデザイン キャンバスでは使用できません。</p>
	
[プロビジョニング ワークフロー]	<p>プロビジョニングまたはスケール アウト操作中に実行されるワークフローです。このワークフローはブループリントの作成時に選択されたものであり、値を編集することはできません。</p>
[割り当てワークフロー]	<p>初回のすべてのプロビジョニングまたはスケール アウト操作の前に実行されるワークフローを選択します。</p> <p>このライフ サイクル ワークフロー タイプは Azure の割り当てにも対応しています。拡張操作のための割り当てワークフローを作成する場合、次の値を含める必要があります。</p> <ul style="list-style-type: none"> ■ 入力パラメータ <ul style="list-style-type: none"> ■ パラメータ名が requestData、パラメータのタイプが Properties であるもの。 ■ パラメータ名が subtenant、パラメータのタイプが Properties であるもの。 ■ reservations、かつパラメータのタイプが Arrays/ Properties であるもの。 ■ 出力パラメータ <ul style="list-style-type: none"> ■ パラメータ タイプが Properties であるパラメータを含める必要があります。

表 3-58. [コンポーネントのライフサイクル] オプション（続き）

オプション	説明
[更新ワークフロー]	<p>コンポーネントが拡張可能ではないが更新は可能な場合に、スケール インまたはスケール アウトを含む更新操作中に実行されるワークフローを選択します。</p> <p>たとえば、複合ブループリント内のいずれかのコンポーネントに対するスケール インまたはスケール アウト操作で作成された新しい構成で、ロード バランサが更新されます。</p> <p>更新ワークフローは、拡張されたコンポーネントに付随するコンポーネントに適用される可能性があります、それ自体が拡張可能であるわけではありません。更新ワークフローは、更新操作に基づき、拡張可能でないコンポーネントを変更することができます。</p> <p>拡張操作のための更新ワークフローを作成する場合、次の値を含める必要があります。</p> <ul style="list-style-type: none"> ■ 入力パラメータ。 <ul style="list-style-type: none"> ■ パラメータ名にかかわらず、プロビジョニング ワークフローの出力パラメータ タイプに一致するパラメータを含める必要があります。 ■ パラメータ名が data、パラメータのタイプが Properties であるもの。
[削除ワークフロー]	<p>スケール インまたは削除操作中に実行されるワークフローを選択します。</p> <p>拡張操作のための削除ワークフローを作成する場合、次の値を含める必要があります。</p> <ul style="list-style-type: none"> ■ 入力パラメータ。 <ul style="list-style-type: none"> ■ パラメータ名にかかわらず、プロビジョニング ワークフローの出力パラメータ タイプに一致するパラメータを含める必要があります。 <p>たとえば、単一の仮想マシン プロビジョニングの作成ワークフローに VC:VirtualMachine という出力パラメータが含まれている場合、削除ワークフローにはタイプが VC:VirtualMachine である入力パラメータを含める必要があります。</p>

表 3-58. [コンポーネントのライフサイクル] オプション（続き）

オプション	説明
[割り当て解除ワークフロー]	<p>すべての削除またはスケール イン操作の後に実行されるワークフローを選択します。操作中に割り当て解除が失敗した場合でも、削除ワークフローは正常に実行されます。</p> <p>割り当て解除は、複合ブループリントのスケール インまたは削除を行うときの最終処理です。削除操作の後に実行され、リソースを開放します。</p> <p>このライフ サイクル ワークフロー タイプは Azure の割り当てにも対応しています。拡張操作のための割り当て解除ワークフローを作成する場合、次の値を含める必要があります。</p> <ul style="list-style-type: none"> ■ 入力パラメータ。 <ul style="list-style-type: none"> ■ パラメータ名が <code>data</code>、パラメータのタイプが <code>Properties</code> であるもの。
[カテゴリ]	<p>XaaS ブループリントが表示されるデザイン キャンパスの場所を指定するため、[デザイン キャンパス カテゴリ] ドロップダウン メニューで値を選択します。</p> <p>カテゴリを選択しない場合、ブループリントは公開の際に XaaS カテゴリに追加されます。</p>

複合ブループリントへの XaaS ブループリントの追加

XaaS ブループリントを複合ブループリントのコンポーネントとして追加する方法は、デザイン キャンパスで他のブループリント コンポーネントを追加するときと似ています。

同じ方法を使用して XaaS を複合ブループリントに追加します。アプリケーション ブループリントを構成する複数のコンポーネントの 1 つとして、または唯一のブループリント コンポーネントとして、このブループリントを使用することができます。

XaaS ブループリントのみをユーザーに提供する場合、XaaS ブループリントを複合ブループリントに追加せずに、サービスに追加してユーザーに資格を付与することができます。

展開したアプリケーション ブループリントでスケールイン操作またはスケールアウト操作を実行した場合、ブループリントのライフサイクル オプションの構成内容に応じて XaaS ブループリントがスケール調整されます。

前提条件

- インフラストラクチャ アーキテクトとして vRealize Automation にログインします。
- XaaS ブループリントを作成して公開します。 [XaaS ブループリントの作成](#)を参照してください。ブループリントを作成する際、デザイン キャンパスにおけるブループリントの配置先となるカテゴリを指定しておく必要があります。
- 複合ブループリントの XaaS ブループリント フォームをカスタマイズする方法について確認します。 [XaaS ブループリントとアクション用のフォーム設計](#)を参照してください。

手順

1 [設計] - [ブループリント] を選択します。

2 XaaS を追加するブループリントの名前を選択します。

デザイン キャンパスが表示されます。デザイン キャンパスには、現在のアプリケーション コンポーネント ブループリントと他のコンポーネントが含まれています。

- 3 [カテゴリ] リストで目的のブループリントを探します。
- 4 ブループリントをキャンバスにドラッグします。
- 5 [全般] タブと [作成] タブでデフォルト値を構成します。

これらのデフォルト値は、ユーザーがアイテムを申請したときにサービス カタログ フォームに表示されます。

- 6 [終了] をクリックします。
- 7 ブループリントを選択して、[公開] をクリックします。

結果

これで、XaaS ブループリントが複合ブループリントに追加されます。

次のステップ

複合ブループリントをサービスに追加します。[サービス カタログの管理](#)を参照してください。

XaaS リソース アクションの作成

vRealize Orchestrator ワークフローを使用して、プロビジョニングされたアイテムを管理できるようにリソース アクションを作成します。

前提条件

- XaaS アーキテクトとして vRealize Automation にログインします。
- アクションをサポートするカスタム リソースがあることを確認します。[XaaS カスタム リソースの追加](#)を参照してください。
- XaaS カタログ アイテムとしてプロビジョニングされていないアイテムで実行されるアクションを作成する場合は、ターゲット リソースをマップしていることを確認します。[XaaS リソース アクションと連動するその他のリソースのマッピング](#)を参照してください。

手順

1 リソース アクションの作成

リソース アクションは、サービス カタログ ユーザーがプロビジョニングされたカタログ アイテム上で実行できる XaaS ワークフローです。XaaS アーキテクトとして、リソース アクションを作成し、ユーザーがプロビジョニングされたアイテムで実行できる操作を定義することができます。

2 リソース アクションの公開

新たに作成されたリソース アクションはドラフト状態になっており、公開する必要があります。

3 XaaS リソース アクションへのアイコンの割り当て

リソース アクションを作成して公開した後、編集してアクションにアイコンを割り当てることができます。

リソース アクションの作成


リソース アクションは、サービス カタログ ユーザーがプロビジョニングされたカタログ アイテム上で実行できる XaaS ワークフローです。XaaS アーキテクトとして、リソース アクションを作成し、ユーザーがプロビジョニングされたアイテムで実行できる操作を定義することができます。

リソース アクションを作成することで、vRealize Orchestrator ワークフローをプロビジョニング後の操作として関連付けます。このプロセス中に、デフォルトの送信および読み取り専用フォームを編集できます。[リソース アクション フォームの設計](#)を参照してください。

前提条件

- XaaS アーキテクトとして vRealize Automation にログインします。
- リソース アクションの入力パラメータに対応するカスタム リソースを作成します。

手順

- 1 [設計] - [XaaS] - [リソース アクション] を選択します
- 2 [新規] アイコン () をクリックします。
- 3 vRealize Orchestrator ワークフロー ライブラリを参照して、カスタム リソースに関連するワークフローを選択します。

選択したワークフローの名前、説明、および入力パラメータと出力パラメータが、vRealize Orchestrator の定義に従って表示されます。

- 4 [次へ] をクリックします。
- 5 [リソース タイプ] ドロップダウン メニューから、以前に作成したカスタム リソースを選択します。
- 6 [入力パラメータ] ドロップダウン メニューから、リソース アクションの入力パラメータを選択します。
- 7 [次へ] をクリックします。
- 8 名前と説明（説明は任意）を入力します。

vRealize Orchestrator での定義に従って、[名前] および [説明] テキスト ボックスに、ワークフローの名前と説明が入力されます。

- 9 (オプション) このリソース アクションの説明と申請理由の入力をユーザーに求めない場合は、[カタログ申請情報ページを非表示にする] チェック ボックスを選択します。
- 10 バージョンを入力します。

<メジャー>.<マイナー>.<マイクロ>-<リビジョン>の形式がサポートされています。

- 11 (オプション) アクションのタイプを選択します。

オプション	説明
削除	リソース アクション ワークフローの入力パラメータが破棄され、[展開] タブからアイテムが削除されます。たとえば、このリソース アクションで、プロビジョニングされたマシンを削除します。
プロビジョニング	<p>プロビジョニングを行うためのリソース アクションです。たとえば、カタログ アイテムをコピーする際に、このリソース アクションを使用します。</p> <p>ドロップダウン メニューから、出力パラメータを選択します。以前に作成したカスタム リソースを選択して、ユーザーがこのリソース アクションを申請したときに、プロビジョニングされたアイテムが [展開] タブに追加されるようにできます。[プロビジョニングなし] オプションしかない場合は、リソース アクションはプロビジョニングするためのものでないか、出力パラメータの正しいカスタム リソースが作成されていないため、続行できません。</p>

アクション ワークフローに応じて、オプションのいずれか、または両方を選択することも、選択しないことも可能です。

12 ユーザーがリソース アクションを使用できる条件を選択し、[次へ] をクリックします。

13 (オプション) [フォーム] タブでリソース アクションのフォームを編集します。

リソース アクションのフォームは、vRealize Orchestrator ワークフローのプレゼンテーションにマッピングされます。要素を削除、編集、再配置するなど、フォームを変更することができます。また、新しいフォームおよびフォーム ページを追加して、必要な要素を新しいフォームとフォーム ページにドラッグすることができます。

オプション	アクション
フォームの追加	フォーム名の隣にある [新規フォーム] アイコン () をクリックして、必要な情報を指定し、[送信] をクリックします。
フォームの編集	フォーム名の隣にある [編集] アイコン () をクリックして、必要な変更を行い、[送信] をクリックします。
ワークフローのプレゼンテーションの再生成	フォーム名の隣にある [再構築] アイコン () をクリックして、[OK] をクリックします。
フォームの削除	フォーム名の横にある [削除] アイコン () をクリックし、確認ダイアログ ボックスの [OK] をクリックします。
フォーム ページの追加	フォーム ページ名の隣にある [新規ページ] アイコン () をクリックして、必要な情報を指定し、[送信] をクリックします。
フォーム ページの編集	フォーム ページ名の隣にある [編集] アイコン () をクリックして、必要な変更を行い、[送信] をクリックします。
フォーム ページの削除	フォーム名の横にある [削除] アイコン () をクリックし、確認ダイアログ ボックスの [OK] をクリックします。
フォーム ページへの要素の追加	左の [新しいフィールド] ペインから右のペインに要素をドラッグします。必要な情報を指定して、[送信] をクリックします。
要素の編集	編集する要素の隣にある [編集] アイコン () をクリックして、必要な変更を行い、[送信] をクリックします。
要素の削除	削除する要素の横にある [削除] アイコン () をクリックし、確認ダイアログ ボックスの [OK] をクリックします。

14 [完了] をクリックします。

結果

リソース アクションが作成され、[リソース アクション] ページのリストに表示されます。

次のステップ

リソース アクションを公開します。 [リソース アクションの公開](#) を参照してください。

リソース アクションの公開

新たに作成されたリソース アクションはドラフト状態になっており、公開する必要があります。

前提条件

XaaS アーキテクトとして vRealize Automation にログインします。

手順

- 1 [設計] - [XaaS] - [リソース アクション] を選択します
- 2 公開するリソース アクションの行を選択して、[公開] をクリックします。

結果

リソース アクションのステータスが公開済みに変わります。

次のステップ

アイコンをリソース アクションに割り当てます。 [XaaS リソース アクションへのアイコンの割り当て](#)を参照してください。ビジネス グループ マネージャとテナント管理者は、資格の作成時にこのアクションを使用することができます。

XaaS リソース アクションへのアイコンの割り当て

リソース アクションを作成して公開した後、編集してアクションにアイコンを割り当てることができます。

前提条件

XaaS アーキテクトとして vRealize Automation にログインします。

手順

- 1 [管理] - [カタログ管理] - [アクション] を選択します。
- 2 作成したリソース アクションを選択します。
- 3 [構成] をクリックします。
- 4 [参照] をクリックして、追加するアイコンを選択します。
- 5 [開く] をクリックします。
- 6 [アップデート] をクリックします。

結果

リソース アクションにアイコンが割り当てられました。ビジネス グループ マネージャとテナント管理者は、資格でリソース アクションを使用できます。

XaaS リソース アクションと連動するその他のリソースのマッピング

XaaS を使用してプロビジョニングされなかったアイテムをマップして、これらのアイテムでリソース アクションを実行できるようにします。

リソース マッピング スクリプトのアクションとワークフロー

vSphere、vCloud Director、または vCloud Air 仮想マシンのために提供されているリソース マッピングを使用できます。また、カスタムの vRealize Orchestrator スクリプト アクションまたはワークフローを作成して、他の

vRealize Automation カタログ リソース タイプを vRealize Orchestrator インベントリ タイプにマップできます。

vRealize Automation で提供されているリソース マッピング

vRealize Automation には、IaaS vSphere 仮想マシン、IaaS vCloud Director、および展開のリソース マッピングが含まれています。

vRealize Automation には、提供されている XaaS リソース マッピングそれぞれの vRealize Orchestrator リソース マッピングのスクリプト アクションが含まれています。提供されているリソース マッピングのスクリプト アクションは、組み込みの vRealize Orchestrator サーバの `com.vmware.vcac.asd.mappings` パッケージに配置されています。

vRealize Orchestrator ワークフローを `vCACAFE:CatalogResource` とともに入力パラメータとして使用する展開済み複合ブループリントがあり、そのブループリントで実行されるリソース アクションを作成すると、[展開] マッピングが入力リソース タイプとして適用されます。[展開] マッピングが適用されるのは、選択したワークフローに `vCACAFE:CatalogResource` が入力パラメータとして含まれる場合のみです。たとえば、ユーザーの代わりにリソース アクションを要求するアクションを作成した場合、このワークフローが `vCACAFE:CatalogResource` を使用するため、[リソースの入力] タブのリソース タイプは「展開」になります。

IaaS vCD 仮想マシンおよび IaaS VC VirtualMachine リソース マッピングは、IaaS リソースと一致する仮想マシンを vRealize Orchestrator、vSphere または vCloud Director 仮想マシンにマップするアクションで使用されます。

リソース マッピングの作成

vRealize Orchestrator のバージョンにより、vRealize Orchestrator ワークフローまたはスクリプト アクションのいずれかを作成して vRealize Orchestrator と vRealize Automation の間でリソースをマップできます。

リソース マッピングを作成するには、プロビジョニングしたリソースを定義するキーと値のペアを含んだ Properties、対応する vRealize Orchestrator プラグインによって予期される vRealize Orchestrator インベントリ タイプの出力パラメータを使用します。マッピングに利用可能なプロパティはリソースのタイプによります。たとえば、EXTERNAL_REFERENCE_ID プロパティは個々の仮想マシンを定義する共通キー パラメータであり、ユーザーはこのプロパティを使用してカタログ リソースを照会できます。EXTERNAL_REFERENCE_ID を使用しないリソースのマッピングを作成する場合、個々の仮想マシンに渡された他のプロパティの 1 つを使用することができます。たとえば、名前や説明などです。

ワークフローおよびスクリプト アクションの開発の詳細については、『VMware vCenter Orchestrator における開発』を参照してください。

リソース マッピングの作成

vRealize Automation は、vSphere、vCloud Director、および vCloud Air の各マシンのリソース マッピングを提供します。別のタイプのカタログ リソース用の追加のリソース マッピングを作成できます。

前提条件

- XaaS アーキテクトとして vRealize Automation にログインします。
- マッピング スクリプトまたはワークフローが vRealize Orchestrator で利用できることを確認します。[リソース マッピング スクリプトのアクションとワークフロー](#)を参照してください。

手順

1 [設計] - [XaaS] - [リソース マッピング] を選択します

2 [新規] アイコン（）をクリックします。

3 名前と説明（説明は任意）を入力します。

4 バージョンを入力します。

<メジャー>.<マイナー>.<マイクロ>-<リビジョン>の形式がサポートされています。

5 [カタログ リソースのタイプ] テキスト ボックスにカタログ リソースのタイプを入力して Enter を押します。
プロビジョニングされたアイテムの詳細ビューにカタログ リソースのタイプが表示されます。

6 [Orchestrator タイプ] テキスト ボックスに vRealize Orchestrator オブジェクト タイプを入力して Enter を押します。

これはリソース マッピング ワークフローの出力パラメータです。

7 （オプション）ターゲット基準を追加し、このリソース マッピングを使用して作成されたリソース アクションの可用性を制限します。

また、リソース アクションは、承認と資格に基づいた制限の対象にもなります。

a [条件に基づいて使用可能] を選択します。

b 条件のタイプを選択します。

オプション	説明
[次のすべて]	定義した条件節がすべて満たされると、このリソース マッピングを使用して作成されたリソース アクションを、ユーザーが利用できるようになります。
[次のいずれか]	定義した条件節のいずれかが満たされると、このリソース マッピングを使用して作成されたリソース アクションを、ユーザーが利用できるようになります。
[次を含まない]	定義した条件節が存在する場合、このリソース マッピングを使用して作成されたリソース アクションは利用できません。

c プロンプトに従って、条件節を作成し、条件を入力します。

8 vRealize Orchestrator ライブラリからリソース マッピングのスクリプト アクションまたはワークフローを選択します。

9 [OK] をクリックします。

XaaS ブループリントとアクション用のフォーム設計

XaaS には、ブループリントおよびリソース アクションの送信フォームと詳細フォームの設計に使用できるフォーム デザイナがあります。フォーム デザイナはワークフローのプレゼンテーションを基に、デフォルト フォームの変更 に使用できるデフォルトのフォームとフィールドを動的に生成します。

ユーザーがカタログ アイテムやリソース アクションを送信する場合に入力できる、インタラクティブ フォームを作成できます。カタログ アイテムまたはプロビジョニング済みリソースの詳細ビューで表示可能な情報を定義する、読み取り専用フォームも作成できます。

XaaS カスタム リソース、XaaS ブループリント、リソース アクションを作成すると、汎用のフォームが生成されます。

表 3-59. XaaS オブジェクト タイプと関連フォーム

オブジェクト タイプ	デフォルトのフォーム	その他のフォーム
カスタム リソース	vRealize Orchestrator プラグイン インベントリ タイプの属性に基づく、リソース詳細フォーム（読み取り専用）。	■ なし
XaaS ブループリント	選択したワークフローのプレゼンテーションに基づく、申請の送信フォーム。	■ カタログ アイテムの詳細（読み取り専用） ■ 送信された申請の詳細（読み取り専用）
リソース アクション	選択したワークフローのプレゼンテーションに基づく、アクションの送信フォーム。	■ 送信されたアクションの詳細（読み取り専用）

デフォルト フォームの変更や新しいフォームの設計を行うことができます。フィールドをドラッグしてフォームに追加したり、並べ替えたりすることができます。特定のフィールドの値に制約を設定したり、デフォルト値を指定したり、フォームに入力するエンド ユーザーに指示書を提供したりすることができます。

目的が多様なため、読み取り専用フォームの設計で実行できる操作は、送信フォームを設計するための操作に比べて限定的です。

フォーム デザイナのフィールド

リソース アクションおよび XaaS ブループリントのデフォルトの生成フォームに新しい事前定義フィールドを追加することにより、ワークフローのプレゼンテーションおよび機能を拡張することができます。

入力パラメータが vRealize Orchestrator ワークフローで定義されている場合は、vRealize Automation でデフォルトで生成されたフォーム上に表示されます。フォームのデフォルトで生成されたフィールドを使用しない場合は、そのフィールドを削除して、パレットから新しいフィールドをドラッグ アンド ドロップできます。交換しようとするフィールドと同じ ID を使用する場合は、ワークフロー マッピングを解除することなく、デフォルトの生成フィールドを置き換えることができます。

また、次の場合にワークフローのプレゼンテーションおよび機能を拡張できるようにするため、vRealize Orchestrator ワークフローの入力値に基づいて生成されたフィールドを除く新しいフィールドを追加することもできます。

■ 既存のフィールドへの制約の追加

たとえば、新しいドロップダウン メニューを作成して、**dd** という名前を付けることができます。また、ゴールド、シルバー、ブロンズ、およびカスタムの事前定義済みオプションも作成できます。CPU などの事前定義済みフィールドがある場合、このフィールドに次の制約を追加できます。

- dd がゴールドの場合、CPU は 2,000 MHz になります。
- dd がシルバーの場合、CPU は 1,000 MHz になります。
- dd がブロンズの場合、CPU は 500 MHz になります。
- dd がカスタムの場合、CPU フィールドは編集可能で、ユーザーはカスタム値を指定できます。

■ フィールドへの外部値定義の追加

vRealize Orchestrator スクリプト アクションを実行し、設計するフォームのユーザーに追加情報を提供することができるよう、外部値の定義をフィールドに追加することができます。たとえば、仮想マシンのファイアウォール設定を変更するワークフローを作成するとします。リソース アクションの申請ページでは、開いているポートの設定をユーザーが変更できるようにするだけでなく、オプションが開いているポートに制限されるようにもします。この場合は、外部値の定義をデュアル リスト フィールドに追加し、開いているポートを問い合わせるカスタムの vRealize Orchestrator スクリプト アクションを選択できます。申請フォームがロードされると、スクリプト アクションが実行され、開いているポートがオプションとしてユーザーに表示されます。

- vRealize Orchestrator ワークフローでグローバル パラメータとして扱われる新規フィールドを追加します。

たとえば、ワークフローにより、サードパーティ システムとの統合が実現すると、ワークフローの開発者は、通常時に処理される入力パラメータを定義しますが、カスタム フィールドを追加する方法も指定します。さらに、スクリプト処理ボックスでは、**my3rdparty** で始まるすべてのグローバル パラメータが処理されるとします。その後、XaaS アーキテクトがユーザーに提供する特定の値を指定する場合、XaaS アーキテクトは **my3rdparty_CPU** という名前の新しいフィールドを追加できます。

表 3-60. リソース アクションまたは XaaS ブループリント フォームの新しいフィールド

フィールド	説明
[テキスト フィールド]	1 行のテキスト ボックス
[テキスト エリア]	複数行のテキスト ボックス
[リンク]	ユーザーが URL を入力するフィールド。http、https、ftp、mailto、または / を使用できます。「file:///」は使用しないでください。
[電子メール]	ユーザーが電子メール アドレスを入力するフィールド
[パスワード フィールド]	ユーザーがパスワードを入力するフィールド
[整数フィールド]	ユーザーが整数を入力するテキスト ボックス 最小値、最大値、増分を追加して、このフィールドをスライダにできます。
[小数フィールド]	ユーザーが小数を入力するテキスト ボックス 最小値、最大値、増分を追加して、このフィールドをスライダにできます。
[日時]	ユーザーが日付を指定（カレンダー メニューから日付を選択）し、時間も選択（上下矢印を使用）できるテキスト ボックス
[デュアル リスト]	ユーザーが 2 つのリストの間で事前定義の値セットを移動させるリスト ビルダです。1 つ目のリストにはすべての未選択のオプションが含まれ、2 つ目のリストにはユーザーの選択オプションが含まれています。
[チェック ボックス]	チェック ボックス
[はい/いいえ]	[はい] または [いいえ] を選択するためのドロップダウン メニュー
[ドロップダウン]	ドロップダウン メニュー
[リスト]	リスト
[チェック ボックス リスト]	チェック ボックス リスト
[ラジオ ボタン グループ]	ラジオ ボタンのグループ

表 3-60. リソース アクションまたは XaaS ブループリント フォームの新しいフィールド（続き）

フィールド	説明
[検索]	クエリがオートコンプリートで入力され、ユーザーがオブジェクトを選択する検索テキスト ボックス
[ツリー]	ユーザーが利用可能なオブジェクトを参照して選択するために使用するツリー
[マップ]	ユーザーがプロパティのキーと値のペアを定義するために使用するマップ テーブル

また、[セクション ヘッダー] フォーム フィールドを使用して、セクション内のフォームページを、個別の見出しと、読み取り専用情報テキストを追加するための [テキスト] フォーム フィールドに分けることもできます。

フォーム デザインでの制約と値

ブループリントまたはリソース アクション フォームの要素を編集する場合、さまざまな制約および値を要素に適用できます。

制約

要素に適用できる制約は、編集またはフォームに追加する要素のタイプにより異なります。制約値の中には、vRealize Orchestrator ワークフローで構成されるものもあります。それらの値は、ワークフローの実行時に評価される条件に依存することが多いため、[制約] タブには表示されません。ブループリント フォームに対して構成する制約値は、vRealize Orchestrator ワークフローに含まれる制約より優先されます。

フィールドの計算後に最小値と最大値のバインドが再計算されるのは、ブループリントが申請された場合のみです。

要素に適用する制約ごとに、以下のいずれかのオプションを選択して制約を定義することができます。

未設定

vRealize Orchestrator ワークフローのプレゼンテーションからプロパティを取得します。

定数

編集している要素を必須または任意に設定します。

フィールド

要素をフォームからの別の要素にバインドします。たとえば、チェック ボックスなどの別の要素が選択された場合にのみ、要素を必須に設定することができます。

条件付き

条件を適用します。条件を使用して、さまざまな句や式を作成し、それらを要素の状態または制約に適用できます。

外部

値を定義する vRealize Orchestrator スクリプト アクションを選択します。

表 3-61. フォーム デザイナでの制約

制約	説明
必須	要素が必須かどうかを示します。
読み取り専用	フィールドが読み取り専用かどうかを示します。
値	要素の値を設定します。
表示	<p>ユーザーが要素を表示できるかどうかを示します。</p> <p>vRealize Orchestrator ワークフローの表示グループに可視性制約を適用すると、XaaS の送信された申請の詳細フォームではこの制約は無視され、非表示にしたいフィールドがフォームに表示されます。</p> <p>送信された申請の詳細フォームに表示せず、申請ユーザーには不要なフィールドを非表示にするには、XaaS ブループリント デザイナの [ブループリント フォーム] タブで、送信された申請の詳細フォームからそのフィールドを削除します。このタブを見つけるには、新規 XaaS ブループリント フォームの追加を参照してください。</p>
最小長	文字列入力要素の文字の最小数を設定します。
最大長	文字列入力要素の文字数の上限を設定します。
最小値	数値入力要素の最小値を設定します。
最大値	数値入力要素の最大値を設定します。
増分	[10 進数] または [整数] フィールドなどの要素の増分を設定します。たとえば、[整数] フィールドを [スライド] として表示する場合、この手順の値を使用できます。
最小数	<p>選択できる要素の最小アイテム数を設定します。</p> <p>たとえば、[チェック ボックス リスト] を追加または編集する場合、ユーザーが続行するために選択する必要がある、チェック ボックスの最小数を設定できます。</p>
最大数	<p>選択できる要素の最大アイテム数を設定します。</p> <p>たとえば、[チェック ボックス リスト] を追加または編集する場合、ユーザーが続行するために選択する必要がある、チェック ボックスの最大数を設定できます。</p>

値

要素に値を適用したり、フィールドに対しユーザーへの表示内容を定義することができます。選択可能なオプションは、編集またはフォームに追加する要素のタイプにより異なります。

表 3-62. フォーム デザイナの値

値	説明
未設定	vRealize Orchestrator ワークフローのプレゼンテーションから、編集している要素の値を取得します。
定義済みの値	vRealize Orchestrator インベントリの関連オブジェクトのリストから値を選択します。
値	ラベル付きの固定カスタム値を定義します。
外部値	vRealize Orchestrator スクリプト アクションを選択すると、ワークフローによって直接公開されない情報を使用して値が定義されます。

フォーム デザイナの外部値の定義

フォーム デザイナの一部の要素を編集する場合には、カスタムの vRealize Orchestrator スクリプト アクションを使用する外部値定義を割り当て、ワークフローによって直接公開されない情報を入力することができます。

たとえば、リソース アクションを公開して、プロビジョニングされたマシンにソフトウェアをインストールすることができます。ダウンロード可能なすべてのソフトウェアの静的リストをユーザーに提供する代わりに、マシンのオペレーティング システムに関連するソフトウェア、ユーザーがマシンにインストールしていなかったソフトウェア、またはマシンで有効期限が切れておりアップデートが必要なソフトウェアを、そのリストに動的に取り込むことができます。

カスタムの動的コンテンツをユーザーに提供するには、vRealize Orchestrator スクリプト アクションを作成して、ユーザーに対して表示する情報を取得します。作成したスクリプト アクションは、外部値の定義としてフォーム デザイナのフィールドに割り当てます。リソースまたはサービスのブループリント フォームがユーザーに対して表示されると、スクリプト アクションにより、カスタム情報が取得されてユーザーに表示されます。

外部値定義を使用して、デフォルトまたは読み取り専用値の入力、ブール式の作成、制約の定義、リストやチェックボックスなどから選択する消費者向けオプションが可能になります。

必須フィールドを含むワークフローを使用してブループリントを作成する場合は、ブループリントを必須ではないものとして設定した場合でも申請フォームでは必須になります。

フォーム デザイナの操作

XaaS ブループリント、カスタム リソース アクション、カスタム リソースを作成するときに、フォーム デザイナを使用して、ブループリント、アクション、リソースのフォームを編集することができます。アイテムまたはアクションのユーザーがカタログ アイテムを申請したり、プロビジョニング後の操作を実行したりするときに表示される内容を編集し、定義することができます。

デフォルトの場合、XaaS ブループリント、リソース アクション、またはカスタム リソース フォームは、vRealize Orchestrator のワークフローのプレゼンテーションに基づいて生成されます。

vRealize Orchestrator プレゼンテーションのステップは、フォーム ページとして表示され、vRealize Orchestrator プレゼンテーション グループは個別のセクションとして表示されます。選択されたワークフローの入力タイプは、フォーム内のさまざまなフィールドとして表示されます。たとえば、vRealize Orchestrator のタイプ string はテキスト ボックスで表示されます。VC:VirtualMachine などの複合タイプは検索ボックスやツリーで表示されるため、ユーザーは英数字の値を入力して、仮想マシンを検索したり、参照して選択したりすることができます。

フォーム デザイナで、オブジェクトの表示方法を編集できます。たとえば、デフォルトの VC:VirtualMachine の表示を編集して、検索ボックスの代わりにツリーにすることができます。また、チェック ボックス、ドロップダウン メニューなどの新しいフィールドを追加して、各種制約を適用することもできます。追加する新しいフィールドが無効か、vRealize Orchestrator ワークフロー入力に正しくマッピングされていない場合、ユーザーがワークフローを実行すると、vRealize Orchestrator は無効なフィールドまたはマッピングされていないフィールドをスキップします。

カスタム リソース フォームの設計

リソース詳細フォームのすべてのフィールドは、ユーザーがカスタム リソースをプロビジョニングするとき、ユーザーのアイテム詳細ページに読取り専用として表示されます。 フィールドの削除、変更、または再配置などの基本的な編集操作をこのフォームに対して行ったり、vRealize Orchestrator のスクリプト アクションを使用する外部で定義された新しいフィールドを追加して追加の読取り専用情報をユーザーに提供したりすることができます。

■ カスタム リソース要素の編集

カスタム リソースの [詳細フォーム] ページにある要素のいくつかの特性を編集できます。ページの各デフォルト フィールドは、カスタム リソースのプロパティを表しています。 プロパティのタイプやデフォルト値を変更することはできませんが、名前、サイズ、および説明を編集することはできます。

■ 新規カスタム リソース フォーム ページの追加

新規ページを追加して、フォームを複数のタブに再編成できます。

■ カスタム リソース フォームへのセクション ヘッダーの挿入

フォームを複数のセクションに分けるためにセクション ヘッダーを挿入することができます。

■ カスタム リソース フォームへのテキスト要素の挿入

テキスト ボックスを挿入して、フォームに説明テキストを追加できます。

■ カスタム リソース フォームへの外部定義フィールドの挿入

新しいフィールドを挿入し、そのフィールドに外部値の定義を割り当てて、ユーザーがカスタム リソースをプロビジョニングするときにアイテムの詳細ページで見ることができる読取り専用情報を動的に提供することができます。

カスタム リソース要素の編集

カスタム リソースの [詳細フォーム] ページにある要素のいくつかの特性を編集できます。ページの各デフォルト フィールドは、カスタム リソースのプロパティを表しています。 プロパティのタイプやデフォルト値を変更することはできませんが、名前、サイズ、および説明を編集することはできます。

前提条件

- テナント管理者または XaaS アーキテクトとして vRealize Automation にログインします。
- [XaaS カスタム リソースの追加](#)。

手順

- 1 [設計] - [XaaS] - [カスタム リソース] を選択します。
- 2 編集するカスタム リソースをクリックします。
- 3 [詳細フォーム] タブをクリックします。
- 4 編集する要素を指定して、[編集] をクリックします。

- 5 [ラベル] テキスト ボックスにフィールドの新しい名前を入力してラベルを変更します。
- 6 [説明] テキスト ボックスの説明を編集します。
- 7 [サイズ] ドロップダウン メニューからオプションを選択して、要素のサイズを変更します。
- 8 [ラベル サイズ] ドロップダウン メニューからオプションを選択し、ラベルのサイズを変更します。
- 9 [送信] をクリックします。
- 10 [完了] をクリックします。

新規カスタム リソース フォーム ページの追加

新規ページを追加して、フォームを複数のタブに再編成できます。

前提条件

- テナント管理者または XaaS アーキテクトとして vRealize Automation にログインします。
- [XaaS カスタム リソースの追加](#)。

手順

- 1 [設計] - [XaaS] - [カスタム リソース] を選択します。
- 2 編集するカスタム リソースをクリックします。
- 3 [詳細フォーム] タブをクリックします。
- 4 [フォーム ページ] 名の隣にある [新規ページ] アイコン (+) をクリックします。
- 5 未使用の画面タイプを選択し、[送信] をクリックします。

リソース詳細またはリソース リスト ビューをすでに選択している場合は、同一タイプを作成することはできません。

- 6 [送信] をクリックします。
- 7 フォームを構成します。
- 8 [完了] をクリックします。

結果

元のフォーム ページからいくつかの要素を削除して新規フォーム ページに挿入できます。また、外部値の定義を使用した新しいフィールドを追加して、vRealize Orchestrator ワークフローで直接公開されない情報をユーザーに提供できます。

カスタム リソース フォームへのセクション ヘッダーの挿入

フォームを複数のセクションに分けるためにセクション ヘッダーを挿入することができます。

前提条件

- テナント管理者または XaaS アーキテクトとして vRealize Automation にログインします。
- [XaaS カスタム リソースの追加](#)。

手順

- 1 [設計] - [XaaS] - [カスタム リソース] を選択します。
- 2 編集するカスタム リソースをクリックします。
- 3 [詳細フォーム] タブをクリックします。
- 4 [セクション ヘッダー] 要素を [フォーム] ペインから [フォーム ページ] ペインにドラッグします。
- 5 セクションの名前を入力します。
- 6 要素の外をクリックして、変更内容を保存します。
- 7 [完了] をクリックします。

カスタム リソース フォームへのテキスト要素の挿入

テキスト ボックスを挿入して、フォームに説明テキストを追加できます。

前提条件

- テナント管理者または XaaS アーキテクトとして vRealize Automation にログインします。
- [XaaS カスタム リソースの追加](#)。

手順

- 1 [設計] - [XaaS] - [カスタム リソース] を選択します。
- 2 編集するカスタム リソースをクリックします。
- 3 [詳細フォーム] タブをクリックします。
- 4 [テキスト] 要素を [フォーム] ペインから [フォーム ページ] ペインにドラッグします。
- 5 追加するテキストを入力します。
- 6 要素の外をクリックして、変更内容を保存します。
- 7 [完了] をクリックします。

カスタム リソース フォームへの外部定義フィールドの挿入

新しいフィールドを挿入し、そのフィールドに外部値の定義を割り当てて、ユーザーがカスタム リソースをプロビジョニングするときにアイテムの詳細ページで見ることができる読み取り専用情報を動的に提供することができます。

前提条件

- テナント管理者または XaaS アーキテクトとして vRealize Automation にログインします。
- [XaaS カスタム リソースの追加](#)。
- vRealize Orchestrator スクリプト アクションを作成またはインポートして、ユーザーに提供する情報を取得します。

手順

- 1 [設計] - [XaaS] - [カスタム リソース] を選択します。
- 2 編集するカスタム リソースをクリックします。

- 3 [詳細フォーム] タブをクリックします。
- 4 要素を [新しいフィールド] ペインからドラッグして [フォーム ページ] ペインにドロップします。
- 5 [ID] テキスト ボックスに、要素の ID を入力します。
- 6 [ラベル] テキスト ボックスにラベルを入力します。
フォーム上のユーザーにラベルが表示されます。
- 7 (オプション) [タイプ] ドロップダウン メニューからフィールドのタイプを選択します。
- 8 [エンティティ タイプ] 検索ボックスに vRealize Orchestrator スクリプト アクションの結果タイプを入力し、Enter を押します。
たとえば、スクリプト アクションを使用して現在のユーザーを表示し、スクリプトによって vRealize Orchestrator の結果タイプ LdapUser が返されるようにするには、[エンティティ タイプ] 検索ボックスに **LdapUser** と入力して Enter を押します。
- 9 [外部値の追加] をクリックします。
- 10 カスタムの vRealize Orchestrator スクリプト アクションを選択します。
- 11 [送信] をクリックします。
- 12 [送信] を再度クリックします。
- 13 [完了] をクリックします。

結果

フォームがユーザーに対して表示されると、スクリプト アクションにより、カスタム情報が取得されてユーザーに表示されます。

XaaS ブループリント フォームの設計

XaaS ブループリントを作成する場合、フォームへの新規フィールドの追加、既存フィールドの変更、フィールドの削除、またはフィールドの再配置を行うことで、ブループリントのフォームを編集できます。また、新規フォームおよびフォーム ページを作成して、新規フィールドをドラッグ アンド ドロップすることもできます。

■ 新規 XaaS ブループリント フォームの追加

XaaS として公開するワークフローのデフォルトで生成されたフォームを編集する場合、新規 XaaS ブループリント フォームを追加できます。

■ XaaS ブループリント要素の編集

XaaS ブループリントの [ブループリント フォーム] ページにある要素のいくつかの特性を編集できます。要素のタイプとそのデフォルト値を変更し、さまざまな制約および値を適用できます。

■ 新しい要素の追加

XaaS ブループリントのデフォルトで生成されたフォームを編集する場合、定義済みの新しい要素をフォームに追加できます。たとえば、デフォルトで生成されたフィールドを使用しない場合は、それらを削除して新しいフィールドに置き換えることができます。

■ XaaS ブループリント フォームへのセクション ヘッダの挿入

フォームを複数のセクションに分けるためにセクション ヘッダーを挿入することができます。

■ XaaS ブループリント フォームへのテキスト要素の追加

テキスト ボックスを挿入して、フォームに説明テキストを追加できます。

新規 XaaS ブループリント フォームの追加


XaaS として公開するワークフローのデフォルトで生成されたフォームを編集する場合、新規 XaaS ブループリント フォームを追加できます。

新規 XaaS ブループリント フォームを追加することで、カタログ アイテムの詳細ページおよび送信された申請の詳細ページの操作環境を定義します。カタログ アイテムの詳細および送信された申請の詳細フォームを追加しない場合、ユーザーには申請フォームで定義されたものが表示されます。

前提条件

- テナント管理者または XaaS アーキテクトとして vRealize Automation にログインします。
- [XaaS ブループリントの追加](#)。

手順

- 1 [設計] - [XaaS] - [XaaS ブループリント] を選択します。
- 2 編集する XaaS ブループリントをクリックします。
- 3 [ブループリント フォーム] タブをクリックします。
- 4 [新規フォーム] アイコン () をクリックします。
- 5 名前と説明 (説明は任意) を入力します。
- 6 [画面タイプ] メニューから画面タイプを選択します。

オプション	説明
カタログ アイテムの詳細	ユーザーがカタログ アイテムをクリックしたときに表示されるカタログ アイテムの詳細ページ。
申請フォーム	デフォルトの XaaS ブループリント フォーム。ユーザーがカタログ アイテムを申請すると、申請フォームが表示されます。
送信された申請の詳細	ユーザーがアイテムを申請した後、[展開] タブで申請の詳細を表示するときに示される申請の詳細ページ。

- 7 [送信] をクリックします。

次のステップ

必要なフィールドを [新しいフィールド] ペインから [フォーム ページ] ペインにドラッグして追加します。

XaaS ブループリント要素の編集

XaaS ブループリントの [ブループリント フォーム] ページにある要素のいくつかの特性を編集できます。要素のタイプとそのデフォルト値を変更し、さまざまな制約および値を適用できます。

前提条件

- テナント管理者または XaaS アーキテクトとして vRealize Automation にログインします。

■ XaaS ブループリントの追加。

手順

- 1 [設計] - [XaaS] - [XaaS ブループリント] を選択します。
- 2 編集する XaaS ブループリントをクリックします。
- 3 [ブループリント フォーム] タブをクリックします。
- 4 編集する要素を特定します。
- 5 [編集] アイコン (✎) をクリックします。
- 6 [ラベル] テキスト ボックスにフィールドの新しい名前を入力して、ユーザーに表示するラベルを変更します。
- 7 [説明] テキスト ボックスの説明を編集します。
- 8 [タイプ] ドロップダウン メニューからオプションを選択して、要素の表示タイプを変更します。
オプションは、編集する要素のタイプによって異なります。
- 9 [サイズ] ドロップダウン メニューからオプションを選択して、要素のサイズを変更します。
- 10 [ラベル サイズ] ドロップダウン メニューからオプションを選択し、ラベルのサイズを変更します。
- 11 要素のデフォルト値を編集します。

オプション	説明
未設定	vRealize Orchestrator ワークフローのプレゼンテーションから、編集している要素の値を取得します。
定数	編集している要素のデフォルト値を指定した定数値に設定します。
フィールド	要素のデフォルト値を、この表示からの別の要素のパラメータにバインドします。
条件付き	条件を適用します。条件を使用することで、さまざまな条件節や式を作成し、それらを要素に適用できます。
外部	vRealize Orchestrator スクリプト アクションを選択して値を定義します。

- 12 [制約] タブで、制約を要素に適用します。

オプション	説明
未設定	vRealize Orchestrator ワークフローのプレゼンテーションから、編集している要素の値を取得します。
定数	編集している要素のデフォルト値を指定した定数値に設定します。
フィールド	要素のデフォルト値を、この表示からの別の要素のパラメータにバインドします。
条件付き	条件を適用します。条件を使用することで、さまざまな条件節や式を作成し、それらを要素に適用できます。
外部	vRealize Orchestrator スクリプト アクションを選択して値を定義します。

13 [値] タブで、要素の 1 つ以上の値を追加します。

使用可能なオプションは、編集する要素のタイプによって異なります。

オプション	説明
未設定	vRealize Orchestrator ワークフローのプレゼンテーションから、編集している要素の値を取得します。
定義済みの値	<p>vRealize Orchestrator インベントリの関連オブジェクトのリストから値を選択します。</p> <p>a [定義済みの値] 検索ボックスに値を入力して、vRealize Orchestrator インベントリを検索します。</p> <p>b 検索結果から値を選択して Enter を押します。</p>
値	<p>ラベル付きのカスタム値を定義します。</p> <p>a [値] テキスト ボックスに値を入力します。</p> <p>b [ラベル] テキスト ボックスに値のラベルを入力します。</p> <p>c [追加] アイコン () をクリックします。</p>
外部値	<p>vRealize Orchestrator スクリプト アクションを選択し、ワークフローで直接公開されない情報を使用して値を定義します。</p> <ul style="list-style-type: none"> ■ [外部値の追加] を選択します。 ■ vRealize Orchestrator スクリプト アクションを選択します。 ■ [送信] をクリックします。

14 [送信] をクリックします。**15** [完了] をクリックします。

新しい要素の追加

XaaS ブループリントのデフォルトで生成されたフォームを編集する場合、定義済みの新しい要素をフォームに追加できます。たとえば、デフォルトで生成されたフィールドを使用しない場合は、それらを削除して新しいフィールドに置き換えることができます。

前提条件

- テナント管理者または XaaS アーキテクトとして vRealize Automation にログインします。
- [XaaS ブループリントの追加](#)。

手順

- 1 [設計] - [XaaS] - [XaaS ブループリント] を選択します。
- 2 編集する XaaS ブループリントをクリックします。
- 3 [ブループリント フォーム] タブをクリックします。
- 4 要素を [新しいフィールド] ペインからドラッグして [フォーム ページ] ペインにドロップします。
- 5 [ID] テキスト ボックスにワークフロー入力パラメータの ID を入力します。
- 6 [ラベル] テキスト ボックスにラベルを入力します。
フォーム上のユーザーにラベルが表示されます。
- 7 (オプション) [タイプ] ドロップダウン メニューからフィールドのタイプを選択します。

- 8 [エンティティ タイプ] テキスト ボックスに vRealize Orchestrator オブジェクトを入力して Enter を押します。

この手順は、一部のフィールド タイプでは不要です。

オプション	説明
結果のタイプ	スクリプト アクションを使用してフィールドの外部値を定義する場合は、vRealize Orchestrator スクリプト アクションの結果のタイプを入力します。
入力パラメータ	ユーザーのフィールド入力を受け入れ、パラメータを vRealize Orchestrator に戻す場合は、vRealize Orchestrator ワークフローが受け入れる入力パラメータのタイプを入力します。
出力パラメータ	フィールドを使用してユーザーに情報を表示する場合は、vRealize Orchestrator ワークフローの出力パラメータのタイプを入力します。

- 9 (オプション) [複数の値] チェック ボックスを選択して、ユーザーが複数のオブジェクトを選択できるようにします。

このオプションは、一部のフィールド タイプでは利用できません。

- 10 [送信] をクリックします。

- 11 [アップデート] をクリックします。

次のステップ

要素を編集してデフォルト設定を変更し、さまざまな制約や値を適用できます。

XaaS ブループリント フォームへのセクション ヘッダの挿入

フォームを複数のセクションに分けるためにセクション ヘッダーを挿入することができます。

前提条件

- テナント管理者または XaaS アーキテクトとして vRealize Automation にログインします。
- [XaaS ブループリントの追加](#)。

手順

- 1 [設計] - [XaaS] - [XaaS ブループリント] を選択します。
- 2 編集する XaaS ブループリントをクリックします。
- 3 [ブループリント フォーム] タブをクリックします。
- 4 [セクション ヘッダー] 要素を [フォーム] ペインから [フォーム ページ] ペインにドラッグします。
- 5 セクションの名前を入力します。
- 6 要素の外をクリックして、変更内容を保存します。
- 7 [アップデート] をクリックします。

XaaS ブループリント フォームへのテキスト要素の追加

テキスト ボックスを挿入して、フォームに説明テキストを追加できます。

前提条件

- テナント管理者または XaaS アーキテクトとして vRealize Automation にログインします。
- [XaaS ブループリントの追加](#)。

手順

- 1 [設計] - [XaaS] - [XaaS ブループリント] を選択します。
- 2 編集する XaaS ブループリントをクリックします。
- 3 [ブループリント フォーム] タブをクリックします。
- 4 [テキスト] 要素を [新しいフィールド] ペインから [フォーム ページ] ペインにドラッグします。
- 5 追加するテキストを入力します。
- 6 要素の外をクリックして、変更内容を保存します。
- 7 [アップデート] をクリックします。

リソース アクション フォームの設計

リソース アクションを作成する場合、フォームへの新規フィールドの追加、既存フィールドの変更、フィールドの削除、またはフィールドの再配置を行うことで、アクションのフォームを編集できます。また、新規フォームおよびフォーム ページを作成して、新規フィールドをドラッグ アンド ドロップすることもできます。

新規リソース アクション フォームの追加


リソース アクションとして公開するワークフローのデフォルトで生成されたフォームを編集する場合、新規リソース アクション フォームを追加できます。

新規リソース アクション フォームを追加することで、送信されたアクションの詳細ページの外観を定義します。送信されたアクションの詳細フォームを追加しない場合、ユーザーにはアクション フォームで定義されたものが表示されます。

前提条件

- テナント管理者または XaaS アーキテクトとして vRealize Automation にログインします。
- [リソース アクションの作成](#)。

手順

- 1 [設計] - [XaaS] - [リソース アクション] を選択します
- 2 編集するリソース アクションをクリックします。
- 3 [フォーム] タブをクリックします。
- 4 [新規フォーム] アイコン () をクリックします。
- 5 名前と説明 (説明は任意) を入力します。

6 [画面タイプ] メニューから画面タイプを選択します。

オプション	説明
アクション フォーム	プロビジョニング後のアクションを実行するときに、ユーザーに表示されるデフォルトのリソース アクション フォーム。
送信されたアクションの詳細	ユーザーがアクションを申請し、[展開] タブで申請の詳細を表示するときに示される申請の詳細ページ。

7 [送信] をクリックします。

次のステップ

必要なフィールドを [新しいフィールド] ペインから [フォーム ページ] ペインにドラッグして追加します。

リソース アクション フォームへの新しい要素の追加

リソース アクションのデフォルトで生成されたフォームを編集する場合、定義済みの新しい要素をフォームに追加できます。たとえば、デフォルトで生成されたフィールドを使用しない場合は、それらを削除して新しいフィールドに置き換えることができます。

前提条件

- テナント管理者または XaaS アーキテクトとして vRealize Automation にログインします。
- [リソース アクションの作成](#)。

手順

- 1 [設計] - [XaaS] - [リソース アクション] を選択します
- 2 編集するリソース アクションをクリックします。
- 3 [フォーム] タブをクリックします。
- 4 要素を [新しいフィールド] ペインからドラッグして [フォーム ページ] ペインにドロップします。
- 5 [ID] テキスト ボックスにワークフロー入力パラメータの ID を入力します。
- 6 [ラベル] テキスト ボックスにラベルを入力します。
フォーム上のユーザーにラベルが表示されます。
- 7 (オプション) [タイプ] ドロップダウン メニューからフィールドのタイプを選択します。

- 8 [エンティティ タイプ] テキスト ボックスに vRealize Orchestrator オブジェクトを入力して Enter を押します。

この手順は、一部のフィールド タイプでは不要です。

オプション	説明
結果のタイプ	スクリプト アクションを使用してフィールドの外部値を定義する場合は、vRealize Orchestrator スクリプト アクションの結果のタイプを入力します。
入力パラメータ	ユーザーのフィールド入力を受け入れ、パラメータを vRealize Orchestrator に戻す場合は、vRealize Orchestrator ワークフローが受け入れる入力パラメータのタイプを入力します。
出力パラメータ	フィールドを使用してユーザーに情報を表示する場合は、vRealize Orchestrator ワークフローの出力パラメータのタイプを入力します。

- 9 (オプション) [複数の値] チェック ボックスを選択して、ユーザーが複数のオブジェクトを選択できるようにします。

このオプションは、一部のフィールド タイプでは利用できません。

- 10 [送信] をクリックします。

- 11 [完了] をクリックします。

次のステップ

要素を編集してデフォルト設定を変更し、さまざまな制約や値を適用できます。

リソース アクション要素の編集

リソース アクションの [フォーム] ページにある要素のいくつかの特性を編集できます。要素のタイプとそのデフォルト値を変更し、さまざまな制約および値を適用できます。

前提条件

- テナント管理者または XaaS アーキテクトとして vRealize Automation にログインします。
- [リソース アクションの作成](#)。

手順

- 1 [設計] - [XaaS] - [リソース アクション] を選択します
- 2 編集するリソース アクションをクリックします。
- 3 [フォーム] タブをクリックします。
- 4 編集する要素を特定します。
- 5 [編集] アイコン (✎) をクリックします。
- 6 [ラベル] テキスト ボックスにフィールドの新しい名前を入力して、ユーザーに表示するラベルを変更します。
- 7 [説明] テキスト ボックスの説明を編集します。

- 8 [タイプ] ドロップダウン メニューからオプションを選択して、要素の表示タイプを変更します。
- オプションは、編集する要素のタイプによって異なります。
- 9 [サイズ] ドロップダウン メニューからオプションを選択して、要素のサイズを変更します。
- 10 [ラベル サイズ] ドロップダウン メニューからオプションを選択し、ラベルのサイズを変更します。
- 11 要素のデフォルト値を編集します。

オプション	説明
未設定	vRealize Orchestrator ワークフローのプレゼンテーションから、編集している要素の値を取得します。
定数	編集している要素のデフォルト値を指定した定数値に設定します。
フィールド	要素のデフォルト値を、この表示からの別の要素のパラメータにバインドします。
条件付き	条件を適用します。条件を使用することで、さまざまな条件節や式を作成し、それらを要素に適用できます。
外部	vRealize Orchestrator スクリプト アクションを選択して値を定義します。


- 12 [制約] タブで、制約を要素に適用します。

オプション	説明
未設定	vRealize Orchestrator ワークフローのプレゼンテーションから、編集している要素の値を取得します。
定数	編集している要素のデフォルト値を指定した定数値に設定します。
フィールド	要素のデフォルト値を、この表示からの別の要素のパラメータにバインドします。
条件付き	条件を適用します。条件を使用することで、さまざまな条件節や式を作成し、それらを要素に適用できます。
外部	vRealize Orchestrator スクリプト アクションを選択して値を定義します。

- 13 [値] タブで、要素の 1 つ以上の値を追加します。

使用可能なオプションは、編集する要素のタイプによって異なります。

オプション	説明
未設定	vRealize Orchestrator ワークフローのプレゼンテーションから、編集している要素の値を取得します。
定義済みの値	vRealize Orchestrator インベントリに関連オブジェクトのリストから値を選択します。 a [定義済みの値] 検索ボックスに値を入力して、vRealize Orchestrator インベントリを検索します。 b 検索結果から値を選択して Enter を押します。

オプション	説明
値	ラベル付きのカスタム値を定義します。 a [値] テキスト ボックスに値を入力します。 b [ラベル] テキスト ボックスに値のラベルを入力します。 c [追加] アイコン () をクリックします。
外部値	vRealize Orchestrator スクリプト アクションを選択し、ワークフローで直接公開されない情報を使用して値を定義します。 ■ [外部値の追加] を選択します。 ■ vRealize Orchestrator スクリプト アクションを選択します。 ■ [送信] をクリックします。

14 [送信] をクリックします。

15 [アップデート] をクリックします。

リソース アクション フォームへのセクション ヘッダーの挿入

フォームを複数のセクションに分けるためにセクション ヘッダーを挿入することができます。

前提条件

- テナント管理者または XaaS アーキテクトとして vRealize Automation にログインします。
- [リソース アクションの作成](#)。

手順

- 1 [設計] - [XaaS] - [リソース アクション] を選択します
- 2 編集するリソース アクションをクリックします。
- 3 [フォーム] タブをクリックします。
- 4 [セクション ヘッダー] 要素を [フォーム] ペインから [フォーム ページ] ペインにドラッグします。
- 5 セクションの名前を入力します。
- 6 要素の外をクリックして、変更内容を保存します。
- 7 [完了] をクリックします。

リソース アクション フォームへのテキスト要素の追加

テキスト ボックスを挿入して、フォームに説明テキストを追加できます。

前提条件

- テナント管理者または XaaS アーキテクトとして vRealize Automation にログインします。
- [リソース アクションの作成](#)。

手順

- 1 [設計] - [XaaS] - [リソース アクション] を選択します
- 2 編集するリソース アクションをクリックします。

- 3 [フォーム] タブをクリックします。
- 4 [テキスト] 要素を [新しいフィールド] ペインから [フォーム ページ] ペインにドラッグします。
- 5 追加するテキストを入力します。
- 6 要素の外をクリックして、変更内容を保存します。
- 7 [完了] をクリックします。

XaaS の例とシナリオ

この例とシナリオでは、vRealize Automation で XaaS のブループリントとリソース アクションを使用する一般的なタスクを実施する方法を提案しています。

ユーザーを作成および変更するための XaaS ブループリントとアクションの作成

XaaS を使用して、グループ内のユーザーをプロビジョニングするためのカタログ アイテムを作成および公開できます。新しいプロビジョニング後の操作をプロビジョニングされたユーザーに関連付けることもできます。たとえば、サービス カatalog ユーザーがユーザー パスワードを変更できるようにする操作が該当します。

XaaS アーキテクトとして、カスタム リソース、XaaS ブループリントを作成し、ユーザー作成用のカタログ アイテムを公開します。ユーザーのパスワードを変更するためのリソース アクションも作成します。

カタログ管理者として、サービスを作成し、このサービスにブループリント カatalog アイテムを含めることができます。さらに、フォーム デザイナを使用することでカタログ アイテムのワークフロー プレゼンテーションを編集し、申請フォームのユーザーへの表示方法を変更します。

ビジネス グループ マネージャまたはテナント管理者として、新しく作成したサービス、カタログ アイテム、およびリソース アクションの使用資格をユーザーに付与します。

前提条件

Active Directory プラグインが適切に構成され、Active Directory のユーザーを作成する権限があることを確認します。

手順

1 カスタム リソースとしてのテスト ユーザーの作成

カスタム リソースを作成し、それを vRealize Orchestrator オブジェクト タイプ AD:User にマップできます。

2 ユーザーを作成するための XaaS ブループリントの作成

Create a user in a group XaaS ブループリントを作成して、Active Directory ユーザーを追加してそのユーザーを Active Directory グループに割り当てるワークフローを実行できます。ブループリントは、スタンドアロン XaaS ブループリントまたはブループリント コンポーネントとして作成できます。このシナリオでは、スタンドアロン ブループリントを作成します。

3 ユーザー パスワードを変更するリソース アクションの作成

リソース アクションを作成して、XaaS のユーザーが、ユーザーをプロビジョニングした後に、ユーザー ブループリントを作成し、ユーザーのパスワードを変更することができます。

4 サービスの作成とサービスへの Create a test user ブループリントの追加

サービスを作成して、Create a user カタログ アイテムをサービス カタログに表示できます。

5 ユーザーへのサービスとリソース アクションの使用資格の付与

ビジネス グループ マネージャとテナント管理者は、サービスおよびリソース アクションの使用資格をユーザーまたはユーザー グループに付与できます。使用資格が付与されたユーザーには、カタログにサービスが表示され、サービスに含まれる Create a test user カタログ アイテムを要求できるようになります。ユーザーはアイテムをプロビジョニングした後、ユーザー パスワードの変更を要求できます。


カスタム リソースとしてのテスト ユーザーの作成

カスタム リソースを作成し、それを vRealize Orchestrator オブジェクト タイプ AD:User にマップできます。

前提条件

XaaS アーキテクトとして vRealize Automation にログインします。

手順

- 1 [設計] - [XaaS] - [カスタム リソース] を選択します。
- 2 [新規] アイコン () をクリックします。
- 3 [Orchestrator タイプ] テキスト ボックスに、**AD:User** と入力し、Enter キーを押します。
- 4 リストにある [AD:User] を選択します。
- 5 リソースの名前を入力します。
たとえば、**Test User** です。
- 6 リソースの説明を入力します。
たとえば、
This is a test custom resource that I will use for my catalog item to create a user in a group. です。
- 7 [次へ] をクリックします。
- 8 フォームのデフォルト値はそのままにします。
- 9 [終了] をクリックします。

結果

テスト ユーザーのカスタム リソースが作成され、[カスタム リソース] ページに表示されます。

次のステップ

XaaS ブループリントを作成します。


ユーザーを作成するための XaaS ブループリントの作成

Create a user in a group XaaS ブループリントを作成して、Active Directory ユーザーを追加してそのユーザーを Active Directory グループに割り当てるワークフローを実行できます。ブループリントは、スタンドアロン XaaS ブループリントまたはブループリント コンポーネントとして作成できます。このシナリオでは、スタンドアロン ブループリントを作成します。

前提条件

- Active Directory ユーザーのプロビジョニングをサポートするカスタム リソース アクションを作成することを確認します。[カスタム リソースとしてのテスト ユーザーの作成](#)を参照してください。
- XaaS アーキテクトとして vRealize Automation にログインします。

手順

- 1 [設計] - [XaaS] - [XaaS ブループリント] を選択します。
- 2 [新規] アイコン () をクリックします。
- 3 [ワークフローの選択] ペインで、[Orchestrator] - [ライブラリ] - [Microsoft] - [Active Directory] - [ユーザー] を選択し、[Create a user in a group] ワークフローを選択します。
- 4 [次へ] をクリックします。
- 5 [全般] タブのオプションを構成します。
 - a ブループリントの名前を **Create a test user** に変更し、説明はそのままにします。
 - b [デザイン キャンバスのコンポーネントとして利用可能にする] チェック ボックスを選択解除します。
 これは、このブループリントをデザイン キャンバスでブループリント コンポーネントとして使用できるようにするのではなく、サービス カタログに直接公開するための設定です。スケールインまたはスケールアウト ワークフローを構成する必要はありません。
 [コンポーネントのライフサイクル] タブはユーザー インターフェイスから削除されました。
- 6 [次へ] をクリックします。
- 7 ブループリント フォームを編集します。
 - a [Win2000 形式のドメイン名] をクリックします。
 - b [制約] タブをクリックします。
 - c [値] ドロップダウンの矢印をクリックし、ドロップダウン メニューで [定数] を選択して、**test.domain** と入力します。
 - d [表示] ドロップダウンの矢印をクリックし、ドロップダウン メニューで [定数] を選択して、ドロップダウン メニューで [いいえ] を選択します。
 ドメイン名をカタログ アイテムのユーザーに非表示にしました。
 - e [適用] をクリックして、変更内容を保存します。
- 8 [次へ] をクリックします。
- 9 プロビジョニングする出力パラメータとして [newUser [テスト ユーザー]] を選択します。
- 10 [次へ] をクリックします。
- 11 [終了] をクリックします。
- 12 [XaaS ブループリント] ページで、[Create a test user] 行を選択し、[公開] をクリックします。

結果

テスト ユーザーを作成するためのブループリントを作成し、このブループリントをサービスに追加できるようにしました。

次のステップ

プロビジョニングされたユーザー アカウントで実行するアクションを作成します。[ユーザー パスワードを変更するリソース アクションの作成](#)を参照してください。


ユーザー パスワードを変更するリソース アクションの作成

リソース アクションを作成して、XaaS のユーザーが、ユーザーをプロビジョニングした後に、ユーザー ブループリントを作成し、ユーザーのパスワードを変更することができます。

前提条件

- XaaS アーキテクトとして vRealize Automation にログインします。
- Active Directory ユーザーのプロビジョニングをサポートするカスタム リソース アクションを作成することを確認します。[カスタム リソースとしてのテスト ユーザーの作成](#)を参照してください。

手順

- 1 [設計] - [XaaS] - [リソース アクション] を選択します
- 2 [新規] アイコン () をクリックします。
- 3 vRealize Orchestrator ワークフロー ライブラリで[Orchestrator] - [ライブラリ] - [Microsoft] - [Active Directory] - [ユーザー]に移動し、[ユーザー パスワードの変更] ワークフローを選択します。
- 4 [次へ] をクリックします。
- 5 [リソース タイプ] ドロップダウン メニューから [テスト ユーザー] を選択します。
これは、以前に作成したカスタム リソースです。
- 6 [入力パラメータ] ドロップダウン メニューから [ユーザー]を選択します。
- 7 [次へ] をクリックします。
- 8 リソース アクションの名前を **Change the password of the Test User** に変更し、[詳細] タブに表示される説明をそのままにします。
- 9 [次へ] をクリックします。
- 10 (オプション) フォームはそのままにしておきます。
- 11 [終了] をクリックします。
- 12 [リソース アクション] ページで、[Change the password of the Test User] 行を選択し、[公開] をクリックします。

結果

ユーザーのパスワードを変更するためのリソース アクションを作成し、資格を追加するために使用できるようにしました。

次のステップ

Create a test user ブループリントをサービスに追加します。[サービスの作成とサービスへの Create a test user ブループリントの追加](#)を参照してください。

サービスの作成とサービスへの Create a test user ブループリントの追加



サービスを作成して、Create a user カタログ アイテムをサービス カタログに表示できます。

前提条件

- テナント管理者またはカタログ管理者として vRealize Automation にログインします。
- XaaS ブループリントが作成済みであることを確認します。[ユーザーを作成するための XaaS ブループリントの作成](#)を参照してください。

テナント管理者またはカタログ管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [カタログ管理] - [サービス] を選択します。
 - 2 [新規] アイコン () をクリックします。
 - 3 サービスの名前として **Active Directory Test User** と入力します。
 - 4 [ステータス] ドロップダウン メニューから [有効] を選択します。
 - 5 その他のテキスト ボックスは空白にしておきます。
 - 6 [OK] をクリックします。
 - 7 [サービス] リストで、[Active Directory Test User] 行を選択し、[カタログ アイテムの管理] をクリックします。
 - 8 [新規] アイコン () をクリックします。
 - 9 [Create a test user] を選択し、[OK] をクリックします。
- Create a test user XaaS ブループリントがカタログ アイテムのリストに追加されます。
- 10 [閉じる] をクリックします。

結果

Active Directory Test User サービスに Create a test user ブループリントが含まれます。サービスにアクションを追加する必要はありません。

次のステップ

ブループリントを要求してアクションを実行する資格をユーザーに割り当てることができます。[ユーザーへのサービスとリソース アクションの使用資格の付与](#)を参照してください。

ユーザーへのサービスとリソース アクションの使用資格の付与


ビジネス グループ マネージャとテナント管理者は、サービスおよびリソース アクションの使用資格をユーザーまたはユーザー グループに付与できます。使用資格が付与されたユーザーには、カタログにサービスが表示され、サービ

スに含まれる Create a test user カタログ アイテムを要求できるようになります。ユーザーはアイテムをプロビジョニングした後、ユーザー パスワードの変更を要求できます。

前提条件

- テナント管理者またはビジネス グループ マネージャとして vRealize Automation にログインします。
- Create a user ブループリントがサービスに追加されていることを確認します。[サービスの作成とサービスへの Create a test user ブループリントの追加](#)を参照してください。
- [ユーザー パスワードの変更] リソース アクションがあることを確認します。[ユーザー パスワードを変更する リソース アクションの作成](#)を参照してください。

手順

- 1 [管理] - [カタログ管理] - [資格] を選択します。
- 2 [新規] アイコン () をクリックします。
- 3 [名前] テキスト ボックスに **Create an Active Directory user** と入力します。
- 4 [説明] および [有効期限日] テキスト ボックスを空のままにします。
- 5 [ステータス] ドロップダウン メニューから [有効] を選択します。
- 6 [ビジネス グループ] ドロップダウン メニューからターゲットのビジネス グループを選択します。
たとえば、IT アカウント マネージャ ビジネス グループを選択します。
- 7 [すべてのユーザーおよびグループ] を選択して、このビジネス グループ (たとえば、IT アカウント マネージャ) のすべてのメンバーに対してユーザー アカウントを作成する資格を付与します。

選択したユーザーには、サービス、およびカタログのサービスに含まれるカタログ アイテムが表示されます。これらのユーザーは、作成されたユーザー アカウントでパスワードの変更アクションを実行できます。
- 8 [次へ] をクリックします。
- 9 [使用可能なサービス] テキスト ボックスに **Active Directory Test User** と入力し、Enter キーを押します。
- 10 [使用可能なアクション] テキスト ボックスに **Change the password of the Test User** と入力し、Enter キーを押します。
- 11 [完了] をクリックします。

結果

アクティブな資格を作成して、IT アカウント マネージャ ビジネス グループのメンバー ユーザーがユーザーを作成できるようにしました。ユーザーは、プロビジョニングされた後、プロビジョニングされたユーザー アカウントでパスワード変更リソース アクションを実行できます。

次のステップ

Active Directory ユーザーを作成する資格が付与されたユーザーとしてログインします。[カタログ] タブで、XaaS ブループリントによってユーザーが正常に作成されることを確認します。ユーザーが作成された後、[展開] タブでパスワード変更アクションを実行します。

仮想マシンを移行する XaaS アクションの作成および公開

IaaS でプロビジョニングされた vSphere 仮想マシンでユーザーが実行できる操作を拡張するための XaaS リソース アクションを作成および公開できます。

このシナリオでは、vSphere 仮想マシンの即時に移行するためのリソース アクションを作成します。

前提条件

XaaS アーキテクトとして vRealize Automation にログインします。

手順

1 vSphere 仮想マシンを移行するリソース アクションの作成

カスタム リソース アクションを作成して、ユーザーが vSphere 仮想マシンを IaaS でプロビジョニングした後に、vSphere 仮想マシンを移行することができます。

2 vSphere 仮想マシンを移行するためのアクションの公開

[仮想マシンのクイック移行] リソース アクションをプロビジョニング後の操作として使用するには、この操作を公開する必要があります。

vSphere 仮想マシンを移行するリソース アクションの作成

カスタム リソース アクションを作成して、ユーザーが vSphere 仮想マシンを IaaS でプロビジョニングした後に、vSphere 仮想マシンを移行することができます。

手順

- 1 [設計] - [XaaS] - [リソース アクション] を選択します
- 2 [追加] (+) をクリックします。
- 3 vRealize Orchestrator ワークフロー ライブラリで[Orchestrator] - [ライブラリ] - [vCenter] - [仮想マシンの管理] - [移動と移行]に移動し、[仮想マシンのクイック移行] ワークフローを選択します。
- 4 [次へ] をクリックします。
- 5 [リソース タイプ] ドロップダウン メニューから [IaaS VC VirtualMachine] を選択します。
- 6 [入力パラメータ] ドロップダウン メニューから [仮想マシン] を選択します。
- 7 [次へ] をクリックします。
- 8 [詳細] タブに表示されるリソース アクション名および説明をそのままにします。
- 9 [次へ] をクリックします。
- 10 フォームはそのままにしておきます。
- 11 [終了] をクリックします。

結果

仮想マシンを移行するリソース アクションが作成され、[リソース アクション] ページのリストに表示されます。

次のステップ

vSphere 仮想マシンを移行するためのアクションの公開

vSphere 仮想マシンを移行するためのアクションの公開

[仮想マシンのクイック移行] リソース アクションをプロビジョニング後の操作として使用するには、この操作を公開する必要があります。

手順

- 1 [設計] - [XaaS] - [リソース アクション] を選択します
- 2 [仮想マシンのクイック移行] リソース アクションの行を選択して、[公開] ボタンをクリックします。

結果

これで、vRealize Orchestrator ワークフローがリソース アクションとして作成され、公開されます。「仮想マシンのクイック移行」 リソース アクションがアクション リストに入っていることを確認するには、[管理] - [カタログ 管理] - [アクション] の順に移動します。リソース アクションにアイコンを割り当てることができます。 [XaaS リソース アクションへのアイコンの割り当て](#)を参照してください。

次のステップ

IaaS によってプロビジョニングされた vSphere 仮想マシンを含む資格にアクションを追加します。 [ユーザーにサービス、カタログ アイテム、アクションの使用資格を付与](#)を参照してください。

vMotion で仮想マシンを移行する XaaS アクションの作成

XaaS を使用して、IaaS でプロビジョニングされた仮想マシンを vMotion を使用して移行するためのリソース アクションを作成および公開できます。

このシナリオでは、vMotion を使用して vSphere 仮想マシンを移行するためのリソース アクションを作成します。また、フォーム デザイナを使用してワークフロー プレゼンテーションを編集し、申請の際にユーザーがアクションを確認する方法を変更します。

前提条件

XaaS アーキテクトとして vRealize Automation にログインします。

手順

1 vMotion で vSphere 仮想マシンを移行するアクションの作成

カスタム リソース アクションを作成して、サービス カタログ ユーザーが、IaaS で vSphere 仮想マシンをプロビジョニングした後に、vMotion で vSphere 仮想マシンを移行することができます。

2 リソース アクション フォームの編集

リソース アクション フォームは、vRealize Orchestrator ワークフローのプレゼンテーションをマッピングします。フォームを編集して、リソース アクションのユーザーがプロビジョニング後に操作を実行する場合に表示される内容を定義します。

3 送信されたアクションの詳細フォームの追加およびアクションの保存

「vMotion で仮想マシンを移行」するリソース アクションに新規フォームを追加して、プロビジョニング後の操作を申請した後、ユーザーに提示する内容を定義できます。


4 vMotion で仮想マシンを移行するアクションの公開

[vMotion で仮想マシンを移行する] リソース アクションをプロビジョニング後の操作として使用するには、この操作を公開する必要があります。

vMotion で vSphere 仮想マシンを移行するアクションの作成

カスタム リソース アクションを作成して、サービス カタログ ユーザーが、IaaS で vSphere 仮想マシンをプロビジョニングした後に、vMotion で vSphere 仮想マシンを移行することができます。

手順

- 1 [設計] - [XaaS] - [リソース アクション] を選択します
- 2 [追加] () をクリックします。
- 3 vRealize Orchestrator ワークフロー ライブラリで [Orchestrator] - [ライブラリ] - [vCenter] - [仮想マシンの管理] - [移動と移行] に移動し、[vMotion による仮想マシンの移行] ワークフローを選択します。
- 4 [次へ] をクリックします。
- 5 [リソース タイプ] ドロップダウン メニューから [IaaS VC VirtualMachine] を選択します。
- 6 [入力パラメータ] ドロップダウン メニューから [仮想マシン] を選択します。
- 7 [次へ] をクリックします。
- 8 [詳細] タブに表示されるリソース アクション名および説明をそのままにします。
- 9 [次へ] をクリックします。



次のステップ

リソース アクション フォームの編集。

リソース アクション フォームの編集

リソース アクション フォームは、vRealize Orchestrator ワークフローのプレゼンテーションをマッピングします。フォームを編集して、リソース アクションのユーザーがプロビジョニング後に操作を実行する場合に表示される内容を定義します。

手順

- 1 [削除] アイコン () をクリックして、[プール] 要素を削除します。
- 2 [ホスト] 要素を編集します。
 - a [編集] アイコン () をクリックします。[ホスト] フィールドの横にあります。
 - b [ラベル] テキスト ボックスで **Target host** と入力します。
 - c [タイプ] ドロップダウン メニューから [検索] を選択します。
 - d [制約] タブをクリックします。
 - e [必須] ドロップダウン メニューから [定数] を選択し、[はい] を選択します。
ホスト フィールドが常に必須になりました。
 - f [送信] をクリックします。

3 [優先度] 要素を編集します。

- a [優先度] フィールドの横にある [編集] アイコン (✎) をクリックします。
- b [ラベル] テキスト ボックスで **Priority of the task** と入力します。
- c [タイプ] ドロップダウン メニューから [ラジオ ボタン グループ] を選択します。
- d [値] タブをクリックして、[未設定] チェック ボックスを選択解除します。
- e [定義済みの値] 検索テキスト ボックスで **lowPriority** と入力し、Enter を押します。
- f [定義済みの値] 検索テキスト ボックスで **defaultPriority** と入力し、Enter を押します。
- g [定義済みの値] 検索テキスト ボックスで **highPriority** と入力し、Enter を押します。
- h [送信] をクリックします。

ユーザーがリソース アクションを申請すると、[lowPriority]、[defaultPriority]、および [highPriority] の 3 つのラジオ ボタンで構成されるラジオ ボタン グループが表示されます。

4 [状態] 要素を編集します。

- a [状態] フィールドの横にある [編集] アイコン (✎) をクリックします。
- b [ラベル] テキスト ボックスで **Virtual machine state** と入力します。
- c [タイプ] ドロップダウン メニューから [ドロップダウン] を選択します。
- d [値] タブをクリックして、[未設定] チェック ボックスを選択解除します。
- e [定義済みの値] 検索テキスト ボックスで **poweredOff** と入力し、Enter を押します。
- f [定義済みの値] 検索テキスト ボックスで **poweredOn** と入力し、Enter を押します。
- g [定義済みの値] 検索テキスト ボックスで **suspended** と入力し、Enter を押します。
- h [送信] をクリックします。

ユーザーがリソース アクションを申請すると、[poweredOff]、[poweredOn]、および [サスペンド中] の 3 つのオプションで構成されるドロップダウン メニューが表示されます。

結果

[vMotion で仮想マシンを移行する] ワークフローのワークフロー プレゼンテーションが編集されました。

次のステップ

[送信されたアクションの詳細フォームの追加およびアクションの保存。](#)

送信されたアクションの詳細フォームの追加およびアクションの保存

「vMotion で仮想マシンを移行」するリソース アクションに新規フォームを追加して、プロビジョニング後の操作を申請した後、ユーザーに提示する内容を定義できます。

手順

- 1 [フォーム] ドロップダウン メニューの横にある 新規フォーム[] のアイコン (✚ フォーム) をクリックします。

- 2 [名前] テキスト ボックスに **Submitted action** と入力します。
- 3 [説明] フィールドは空白のままにします。
- 4 [画面タイプ] メニューから [送信されたアクションの詳細] を選択します。
- 5 [送信] をクリックします。
- 6 [フォーム ページ] ドロップダウン メニューの横にある [編集] アイコン (✎) をクリックします。
- 7 [見出し] テキスト ボックスに **Details** と入力します。
- 8 [送信] をクリックします。
- 9 [フォーム] ペインから [テキスト] 要素をドラッグし、[フォーム] ページにドロップします。
- 10 **You submitted a request to migrate your machine with vMotion. Wait until the process completes successfully.** と入力します。
- 11 テキスト ボックスの外をクリックして、変更内容を保存します。
- 12 [送信] をクリックします。
- 13 [追加] をクリックします。

結果

vMotion で仮想マシンを移行するリソース アクションが作成され、[リソース アクション] ページのリストに表示されます。

次のステップ

[vMotion で仮想マシンを移行するアクションの公開。](#)

vMotion で仮想マシンを移行するアクションの公開

[vMotion で仮想マシンを移行する] リソース アクションをプロビジョニング後の操作として使用するには、この操作を公開する必要があります。

手順

- 1 [設計] - [XaaS] - [リソース アクション] を選択します
- 2 [vMotion で仮想マシンを移行する] リソース アクションの行を選択して、[公開] ボタンをクリックします。

結果

これで、vRealize Orchestrator ワークフローがリソース アクションとして作成され、公開されます。「vMotion による仮想マシンの移行」 リソース アクションがアクションのリストに入っていることを確認するには、[管理] - [カタログ管理] - [アクション]の順に移動します。リソース アクションにアイコンを割り当てることができます。

[XaaS リソース アクションへのアイコンの割り当て](#)を参照してください。

ワークフローのプレゼンテーションを編集することで、アクションの操作性を定義できます。

次のステップ

ビジネス グループ マネージャおよびテナント管理者は、「vMotion での仮想マシンの移行」リソース アクションを資格に含めることができます。仮想プラットフォームの IaaS ブループリントを作成、公開する方法については、[マシン ブループリントの設計](#)を参照してください。

スナップショットを作成する XaaS アクションの作成および公開

XaaS を使用して、IaaS でプロビジョニングされた vSphere 仮想マシンのスナップショットを作成するリソース アクションを作成および公開できます。

このシナリオでは、IaaS を使用してプロビジョニングされた vSphere 仮想マシンのスナップショットを作成するリソース アクションを作成します。また、フォーム デザイナを使用してワークフロー プレゼンテーションを編集し、申請の際にユーザーがアクションを確認する方法を変更します。

前提条件

XaaS アーキテクトとして vRealize Automation にログインします。

手順

1 vSphere 仮想マシンのスナップショットを作成するアクションの作成

カスタム リソース アクションを作成して、ユーザーが、IaaS で vSphere 仮想マシンをプロビジョニングした後に、vSphere 仮想マシンのスナップショットを作成することができます。

2 スナップショット取得のアクションを公開する

[スナップショットを作成する] リソース アクションをプロビジョニング後の操作として使用するには、この操作を公開する必要があります。

vSphere 仮想マシンのスナップショットを作成するアクションの作成

カスタム リソース アクションを作成して、ユーザーが、IaaS で vSphere 仮想マシンをプロビジョニングした後に、vSphere 仮想マシンのスナップショットを作成することができます。

手順

- 1 [設計] - [XaaS] - [リソース アクション] を選択します
- 2 [追加] (+) をクリックします。
- 3 vRealize Orchestrator ワークフロー ライブラリで [Orchestrator] - [ライブラリ] - [vCenter] - [仮想マシンの管理] - [スナップショット]に移動し、[スナップショットの作成] ワークフローを選択します。
- 4 [次へ] をクリックします。
- 5 [リソース タイプ] ドロップダウン メニューから [IaaS VC VirtualMachine] を選択します。
- 6 [入力パラメータ] ドロップダウン メニューから [仮想マシン] を選択します。
- 7 [次へ] をクリックします。
- 8 [詳細] タブに表示されるリソース アクション名および説明をそのままにします。
- 9 [次へ] をクリックします。
- 10 フォームはそのままにしておきます。

11 [追加] をクリックします。

結果

仮想マシンのスナップショット作成のリソース アクションを作成しました。これは [リソース アクション] ページのリストに表示されます。

次のステップ

[スナップショット取得のアクションを公開する。](#)

スナップショット取得のアクションを公開する

[スナップショットを作成する] リソース アクションをプロビジョニング後の操作として使用するには、この操作を公開する必要があります。

手順

- 1 [設計] - [XaaS] - [リソース アクション] を選択します
- 2 [スナップショットを作成する] リソース アクションの行を選択して、[公開] ボタンをクリックします。

結果

これで、vRealize Orchestrator ワークフローがリソース アクションとして作成され、公開されます。「スナップショットの作成」 リソース アクションがアクション リストに入っていることを確認するには、[管理] - [カタログ管理] - [アクション] の順に移動します。リソース アクションにアイコンを割り当てることができます。 [XaaS リソース アクションへのアイコンの割り当て](#)を参照してください。

次のステップ

ビジネス グループ マネージャとテナント管理者は、「スナップショットの作成」 リソース アクションを資格に含めることができます。仮想プラットフォームの IaaS ブループリントを作成、公開する方法については、[マシン ブループリントの設計](#)を参照してください。

Amazon 仮想マシンを開始する XaaS アクションの作成および公開

XaaS を使用して、サードパーティによってプロビジョニングされたリソースでユーザーが実行できる操作を拡張するためのアクションを作成および公開できます。

このシナリオでは、Amazon 仮想マシンを即時開始するためのリソース アクションを作成し、公開します。

前提条件

- Amazon Web Services 用の vRealize Orchestrator プラグインをデフォルトの vRealize Orchestrator サーバにインストールします。

- Amazon インスタンスのリソース マッピング用の vRealize Orchestrator ワークフローを作成またはインポートします。

手順

1 Amazon インスタンス用のリソース マッピングの作成

リソース マッピングを作成し、IaaS を使用してプロビジョニングされる Amazon インスタンスと Amazon Web Services プラグインで公開される vRealize Orchestrator タイプの AWS:EC2Instance を関連付けることができます。

2 Amazon 仮想マシンを開始するリソース アクションの作成

リソース アクションを作成して、ユーザーがプロビジョニングされた Amazon 仮想マシンを開始することができます。

3 Amazon インスタンス開始のアクションの公開

新たに作成した [インスタンスを開始する] リソース アクションをプロビジョニング後の操作として Amazon 仮想マシンで使用するには、この操作を公開する必要があります。

Amazon インスタンス用のリソース マッピングの作成

リソース マッピングを作成し、IaaS を使用してプロビジョニングされる Amazon インスタンスと Amazon Web Services プラグインで公開される vRealize Orchestrator タイプの AWS:EC2Instance を関連付けることができます。

前提条件

- XaaS アーキテクトとして vRealize Automation にログインします。
- vRealize Orchestrator リソース マッピング ワークフローまたはスクリプト アクションを作成またはインポートします。

手順

- 1 [設計] - [XaaS] - [リソース マッピング] を選択します
- 2 [追加] (+) をクリックします。
- 3 [名前] テキスト ボックスに **EC2 インスタンス** と入力します。
- 4 [カタログ リソースのタイプ] テキスト ボックスに **クラウド マシン** と入力します。
- 5 [Orchestrator タイプ] テキスト ボックスに **AWS:EC2Instance** と入力します。
- 6 [常時使用可能] を選択します。
- 7 使用するリソース マッピングのタイプを選択します。
- 8 vRealize Orchestrator ライブラリからカスタム リソース マッピングのスクリプト アクションまたはワークフローを選択します。
- 9 [追加] をクリックします。

結果

Amazon リソース マッピングを使用すると、IaaS を使用してプロビジョニングされる Amazon マシンのリソース アクションを作成できます。

次のステップ

[Amazon 仮想マシンを開始するリソース アクションの作成。](#)

Amazon 仮想マシンを開始するリソース アクションの作成

リソース アクションを作成して、ユーザーがプロビジョニングされた Amazon 仮想マシンを開始することができます。

前提条件

XaaS アーキテクトとして vRealize Automation にログインします。

手順

- 1 [設計] - [XaaS] - [リソース アクション] を選択します
- 2 [追加] (+) をクリックします。
- 3 [Orchestrator] - [ライブラリ] - [Amazon Web Services] - [Elastic Cloud] - [インスタンス]を選択し、ワークフロー フォルダの [インスタンスの開始] ワークフローを選択します。
- 4 [次へ] をクリックします。
- 5 [リソース タイプ] ドロップダウン メニューから [EC2 インスタンス] を選択します。
これは以前に作成したリソース マッピングの名前です。
- 6 [入力パラメータ] ドロップダウン メニューから [インスタンス] を選択します。
これはリソース マッピングと一致するリソース アクション ワークフローの入力パラメータです。
- 7 [次へ] をクリックします。
- 8 名前と説明はそのままにします。
リソース アクションのデフォルト名は [インスタンスの開始] です。
- 9 [次へ] をクリックします。
- 10 [フォーム] タブのフィールドはそのままにします。
- 11 [追加] をクリックします。

結果

Amazon 仮想マシンを開始するリソース アクションが作成され、[リソース アクション] ページに表示されます。

次のステップ

[Amazon インスタンス開始のアクションの公開。](#)

Amazon インスタンス開始のアクションの公開

新たに作成した [インスタンスを開始する] リソース アクションをプロビジョニング後の操作として Amazon 仮想マシンで使用するには、この操作を公開する必要があります。

前提条件

XaaS アーキテクトとして vRealize Automation にログインします。

手順

- 1 [設計] - [XaaS] - [リソース アクション] を選択します
- 2 [インスタンスを開始する] リソース アクションの行を選択して、[公開] をクリックします。

結果

[インスタンスを開始する] リソース アクションのステータスが公開済みに変わります。

次のステップ

Amazon のカタログ アイテムを含む資格に [インスタンスを開始する] アクションを追加します。 [ユーザーにサービス、カタログ アイテム、アクションの使用資格を付与](#) を参照してください。

XaaS ブループリントでの不正確なアクセントと特殊文字のトラブルシューティング

ASCII 以外の文字列を使用する言語の XaaS ブループリントを作成する場合、アクセントおよび特殊文字が使用できない文字として表示されます。

原因

デフォルト設定以外の vRealize Orchestrator 構成プロパティが有効化されている場合があります。

解決方法

- 1 Orchestrator サーバ システムで、`/etc/vco/app-server/` に移動します。
- 2 `Vmo.properties` 構成ファイルをテキスト エディタで開きます。
- 3 次のプロパティが無効になっていることを確認します。

```
com.vmware.o11n.webview.htmlescaping.disabled
```

- 4 `vmo.properties` ファイルを保存します。
- 5 vRealize Orchestrator サーバを再起動します。

ブループリントの公開

ブループリントはドラフト状態で保存されるため、カタログ アイテムとして構成したり、デザイン キャンバスでブループリント コンポーネントとして使用したりするには、手動で公開する必要があります。

ブループリントを公開したら、サービス カatalogでのプロビジョニングの申請に対応できる資格を、ブループリントに付与することができます。

ブループリントの公開は、1 度だけ行う必要があります。公開されたブループリントを変更すると、カタログおよびネストされたブループリント コンポーネントに自動的に反映されます。

ブループリントの公開

ブループリントを公開すると、マシンのプロビジョニングに使用できるほか、必要に応じて別のブループリントで再使用できます。マシン プロビジョニングを申請するためにブループリントを使用するには、公開後そのブループリントに資格を付与する必要があります。他のブループリントでコンポーネントとして利用されるブループリントの場合、資格は不要です。

前提条件

- インフラストラクチャ アーキテクトとして vRealize Automation にログインします。
- ブループリントを作成します。『vRealize Automation ブループリント作成のチェックリスト』を参照してください。

手順

- 1 [設計] タブをクリックします。
- 2 [ブループリント] をクリックします。
- 3 公開するブループリントを指定して、[公開] をクリックします。
- 4 [OK] をクリックします。

結果

ブループリントはカタログ アイテムとして公開されますが、まずそのブループリントに資格を付与し、サービス カタログでユーザーが使用できるようにする必要があります。

次のステップ

ブループリントをカタログ サービスに追加し、ブループリントでの定義に従ってマシン プロビジョニング時にカタログ アイテムを申請できるようユーザーに資格を付与してください。

開発者によるブループリントの連携

vRealize Automation ブループリントは、ユーザー インターフェイスを使用して作成できるだけでなく、スタンドアローンやその他のソースから提供されたブループリントを vRealize CloudClient などのツールを使用してプログラムで操作することもできます。このとき、vRealize Suite アプリケーション、ワークフロー、およびサードパーティ製のツールを使用して他の開発者と連携できます。

これらの方法については、次のトピックを参照してください。

- [ブループリントとコンテンツのエクスポートおよびインポート](#)
- [提供されているスタンドアローン ブループリントのダウンロードと構成](#)
- [複数開発者環境でのブループリントおよびその他の IaaS コンテンツの作成](#)

ブループリントとコンテンツのエクスポートおよびインポート

vRealize Automation REST API を使用するか、または vRealize CloudClient を使用することで、プログラムにより、ある vRealize Automation 環境から別の環境へとブループリントとコンテンツをエクスポートできます。

たとえば、ブループリントを開発環境で作成およびテストした後、本番環境にインポートできます。また、コミュニティ フォーラムで入手したプロパティ定義をアクティブな vRealize Automation テナント インスタンスにインポートすることもできます。

次の vRealize Automation のコンテンツ アイテムは、いずれもプログラムでインポートおよびエクスポートできます。

- アプリケーションのブループリントおよびそれらのすべてのコンポーネント
- IaaS マシンのブループリント
- ソフトウェア コンポーネント
- XaaS ブループリント
- コンポーネント プロファイル
- プロパティ グループ

プロパティ グループ情報はテナントに固有であり、ターゲットの vRealize Automation インスタンスにプロパティ グループが既に存在する場合にのみブループリントとともにインポートされます。

ある vRealize Automation インスタンス テナントから別のテナントにブループリントをエクスポートするとき、そのブループリントに定義されているプロパティ グループ情報は、ターゲットのテナント インスタンスにプロパティ グループが既に存在している場合を除き、インポートされたブループリントに対して認識されません。たとえば、mica1 という名前のプロパティ グループを含むブループリントをインポートする場合、ブループリントをインポートする vRealize Automation インスタンスに mica1 プロパティ グループが存在していなければ、インポートされたブループリントに mica1 プロパティ グループは存在しません。ある vRealize Automation インスタンスから別のインスタンスにブループリントをエクスポートするときにプロパティ グループ情報が失われないようにするには、ブループリントをインポートする前に、vRealize CloudClient を使用してプロパティ グループを含むエクスポート パッケージ zip ファイルを作成し、このパッケージ zip ファイルをターゲット テナントにインポートします。vRealize CloudClient を使用してプロパティ グループおよびその他の vRealize Automation アイテムを一覧表示、パッケージ、エクスポート、およびインポートする方法については、VMware Developer Center (<https://developercenter.vmware.com/tool/cloudclient>) を参照してください。

表 3-63. インポートおよびエクスポート ツールの選択

ツール	詳細情報
vRealize CloudClient	https://developercenter.vmware.com/tool/cloudclient の VMware code.vmware.com サイトの vRealize CloudClient のページを参照してください。
vRealize Automation REST API	https://code.vmware.com/apis/vrealize-automation の VMware API Explorer で vRealize Automation 用の API ドキュメントを参照してください。

注： vRealize Automation 展開間で、ブループリントをプログラムでエクスポートおよびインポートする場合（たとえば、テスト環境から本番環境へ、またはある組織から別の組織へ）、テンプレートのクローン作成のデータがパッケージに含まれているかを確認することが重要です。ブループリント パッケージをインポートすると、デフォルトの設定はパッケージ内の情報に基づいて割り当てられます。たとえば、クローン形式のワークフローを使用して作成したブループリントをエクスポートしてからインポートする場合に、クローン データがベースにしているテンプレートが、ブループリントをインポートする vRealize Automation の展開内のエンドポイントにない場合、インポートされたブループリント設定の一部がその展開に適用されません。

シナリオ：Dukes Bank for vSphere サンプル アプリケーションをインポートし、環境に合わせて構成する

IT プロフェッショナルとして vRealize Automation の評価または学習を行っており、vRealize Automation インスタンスに堅牢なサンプル アプリケーションをインポートして、利用できる機能を短時間で調査し、組織のニーズに適した vRealize Automation ブループリントをビルドする可能性について判断できるようにします。

前提条件

- CentOS 6.x Linux リファレンス マシンを準備して、マシンをテンプレートに変換し、カスタマイズ仕様を作成します。[シナリオ：Dukes Bank for vSphere サンプル アプリケーション ブループリントをインポートするための準備](#)を参照してください。
- 外部ネットワーク プロファイルを作成して、ゲートウェイと IP アドレスの範囲を指定します。[サードパーティの IP アドレス管理プロバイダを使用した外部ネットワーク プロファイルの作成](#)を参照してください。
- 外部ネットワーク プロファイルを vSphere 予約にマップします。[Hyper-V、KVM、SCVMM、vSphere、XenServer の予約の作成](#)を参照してください。サンプル アプリケーションは、外部ネットワーク プロファイルがないとプロビジョニングを正常に行うことができません。
- インフラストラクチャ アーキテクトとソフトウェア アーキテクトの両方の権限があることを確認します。Dukes Bank サンプル アプリケーションをインポートし、Dukes Bank ブループリントとソフトウェア コンポーネントを操作するには、両方のロールが必要です。

手順

1 [シナリオ：Dukes Bank for vSphere サンプル アプリケーションをインポートする](#)

vRealize Automation アプライアンスから Dukes Bank for vSphere アプリケーションをダウンロードします。vRealize Automation テナントにサンプル アプリケーションをインポートし、ネットワークとソフトウェア コンポーネントを備えた複数のマシン コンポーネントを含むマルチティア vRealize Automation ブループリントの処理サンプルを表示します。

2 シナリオ : Dukes Bank vSphere サンプル コンポーネントを環境に合わせて構成する

インフラストラクチャ アーキテクト権限を使用して、Dukes Bank の各マシン コンポーネントを構成し、環境用に作成したカスタマイズ仕様、テンプレート、およびマシン プリフィックスを使用するようにします。

結果

お客様の環境用の Dukes Bank for vSphere サンプル アプリケーションが構成されました。ブループリント開発を初めて行う場合、vRealize Automation の評価ツール、または vRealize Automation の機能やコンポーネントの理解を支援する学習リソースとしてご利用ください。

シナリオ : Dukes Bank for vSphere サンプル アプリケーションをインポートする

vRealize Automation アプライアンスから Dukes Bank for vSphere アプリケーションをダウンロードします。vRealize Automation テナントにサンプル アプリケーションをインポートし、ネットワークとソフトウェア コンポーネントを備えた複数のマシン コンポーネントを含むマルチティア vRealize Automation ブループリントの処理サンプルを表示します。

手順

- 1 SSH を使用して vRealize Automation アプライアンスに root としてログインします。
- 2 vRealize Automation アプライアンスから Dukes Bank for vSphere サンプル アプリケーションを /tmp にダウンロードします。

```
wget --no-check-certificate https://vRealize_VA_Hostname_fqdn:5480/blueprints/
DukesBankAppForvSphere.zip
```

パッケージを解凍しないでください。

- 3 <http://developercenter.vmware.com/tool/cloudclient> から /tmp に vRealize CloudClient をダウンロードします。
- 4 cloudclient-4x-dist.zip パッケージを解凍します。
- 5 /bin ディレクトリの vRealize CloudClient を実行します。

```
$>./bin/cloudclient.sh
```

- 6 プロンプトが表示されたら、使用許諾契約に同意してください。
- 7 vRealize CloudClient を使用し、ソフトウェア アーキテクトおよびインフラストラクチャ アーキテクトの権限を持つユーザーとして vRealize Automation アプライアンスにログインします。

```
CloudClient>vra login userpass --server https://vRealize_VA_Hostname_fqdn --user
<user@domain.com> --tenant <TenantName>
```

- 8 プロンプトが表示されたら、ログイン パスワードを入力します。
- 9 DukesBankAppForvSphere.zip コンテンツが利用できることを確認します。

```
vra content import --path /<Path>/DukesBankAppForvSphere.zip --dry-run true --resolution OVERWRITE
```

OVERWRITE エントリはすべて大文字で入力する必要があります。

skip の代わりに上書きする解決を構成することで、可能な場合には vRealize Automation が競合を修正するようにすることができます。

10 Dukes Bank サンプル アプリケーションをインポートします。

```
vra content import --path /<Path>/DukesBankAppForvSphere.zip --dry-run false --resolution OVERWRITE
```

OVERWRITE エントリはすべて大文字で入力する必要があります。

結果

vRealize Automation コンソールにソフトウェア アーキテクトおよびインフラストラクチャ アーキテクトの権限を持つユーザーとしてログインすると、Dukes Bank のブループリントとソフトウェア コンポーネントが [設計] - [ブループリント] タブと [設計] - [ソフトウェア コンポーネント] タブに表示されます。

シナリオ : Dukes Bank vSphere サンプル コンポーネントを環境に合わせて構成する

インフラストラクチャ アーキテクト権限を使用して、Dukes Bank の各マシン コンポーネントを構成し、環境用に作成したカスタマイズ仕様、テンプレート、およびマシン プリフィックスを使用するようにします。

このシナリオでは、マシン コンポーネントを構成し、vSphere Web Client で作成したテンプレートからマシンのクローンを作成します。スナップショットに基づいた仮想マシンの領域を効率的に利用したコピーを作成する場合、サンプル アプリケーションはリンク クローンもサポートします。リンク クローンは、差分ディスクのチェーンを使用して親マシンとの差異を追跡します。短時間でプロビジョニングが行われてストレージ コストを削減できるため、パフォーマンスが最優先でない場合に適しています。

手順

1 インフラストラクチャ アーキテクトとして vRealize Automation コンソールにログインします。

Dukes Bank サンプル アプリケーションを環境内で動作するように構成できるのは、インフラストラクチャ アーキテクト ロールを使用した場合のみですが、サンプル ソフトウェア コンポーネントの表示または編集を行う場合には、ソフトウェア アーキテクト ロールも必要になります。

2 [設計] - [ブループリント] を選択します。

3 [DukesBankApplication] ブループリントを選択し、[編集] アイコンをクリックします。

4 [appserver-node] を編集して、環境内で vRealize Automation がこのマシン コンポーネントをプロビジョニングできるようにします。

ブループリントを構成してこのマシン コンポーネントの複数のインスタンスをプロビジョニングし、ロード バランサ ノード機能を確認できるようにします。

a デザイン キャンパスの [appserver-node] コンポーネントをクリックします。

構成の詳細が下のパネルに表示されます。

b [マシン プリフィックス] ドロップダウン メニューからマシン プリフィックスを選択します。

- c ブループリントを構成して、最小で 2 個から最大で 10 個のインスタンスを選択し、このノードのインスタンスを 2 個から 10 個プロビジョニングします。

申請フォームで、ユーザーは 2 個から 10 個の appserver ノードをプロビジョニングできます。スケールインおよびスケールアウトのアクションを使用できるユーザーは、ニーズの変化に合わせて展開を拡張できます。

- d [ビルド情報] タブをクリックします。
- e [プロビジョニング ワークフロー] ドロップダウン メニューから [Cloneworkflow] を選択します。
- f [クローン作成元] ダイアログから [dukes_bank_template] を選択します。
- g [カスタマイズ仕様] テキスト ボックスに **Customspecs_sample** と入力します。

このフィールドでは大文字と小文字が区別されます。

- h [マシン リソース] タブをクリックします。
- i メモリ設定が少なくとも 2048 MB であることを確認します。

5 [loadbalancer-node] を編集して、環境内で vRealize Automation がこのマシン コンポーネントをプロビジョニングできるようにします。

- a デザイン キャンパスの [loadbalancer-node] コンポーネントをクリックします。
- b [マシン プリフィックス] ドロップダウン メニューからマシン プリフィックスを選択します。
- c [ビルド情報] タブをクリックします。
- d [プロビジョニング ワークフロー] ドロップダウン メニューから [Cloneworkflow] を選択します。
- e [クローン作成元] ダイアログから [dukes_bank_template] を選択します。
- f [カスタマイズ仕様] テキスト ボックスに **Customspecs_sample** と入力します。

このフィールドでは大文字と小文字が区別されます。

- g [マシン リソース] タブをクリックします。
- h メモリ設定が少なくとも 2048 MB であることを確認します。

6 [database-node] マシン コンポーネントに対して繰り返します。

7 [保存と終了] をクリックします。

変更を保存して、[ブループリント] タブに戻ります。

8 [DukesBankApplication] ブループリントを選択して、[公開] をクリックします。

結果

環境用の Dukes Bank サンプル アプリケーション ブループリントが構成され、完成したブループリントが公開されます。

次のステップ

公開されたブループリントは、カタログ サービスを構成し、ブループリントをサービスに追加し、ユーザーにブループリントを申請する資格を付与するまで、カタログ内のユーザーに表示されません。 [サービス カatalog構成用のチェックリスト](#)を参照してください。

Dukes Bank ブループリントを構成してカタログに表示された後は、サンプル アプリケーションのプロビジョニングを申請できます。 [シナリオ： Dukes Bank サンプル アプリケーションをテストする](#)を参照してください。

シナリオ： Dukes Bank サンプル アプリケーションをテストする

Dukes Bank カatalog アイテムを申請し、サンプル アプリケーションにログインして動作を確認し、vRealize Automation ブループリント機能を表示します。

前提条件

- Dukes Bank サンプル アプリケーションをインポートし、環境で機能するようにブループリント コンポーネントを構成します。 [シナリオ： Dukes Bank for vSphere サンプル アプリケーションをインポートし、環境に合わせて構成する](#)を参照してください。
- サービス カatalogを構成し、公開済みの Dukes Bank ブループリントをユーザーが申請できるようにします。 [サービス カatalog構成用のチェックリスト](#)を参照してください。
- プロビジョニングする仮想マシンが yum リポジトリに到達していることを確認します。

手順

- 1 Dukes Bank カatalog アイテムの使用資格を持つユーザーとして、vRealize Automation コンソールにログインします。
- 2 [カatalog] タブをクリックします。
- 3 Dukes Bank サンプル アプリケーションのカatalog アイテムを特定し、[申請] をクリックします。
- 4 赤色のアスタリスクの付いた各コンポーネントに必要な申請情報を入力します。
 - a JBossAppServer コンポーネントに移動し、必要な申請情報を入力します。
 - b vRealize Automation アプライアンスの完全修飾ドメイン名を [app_content_server_ip] テキストボックスに入力します。
 - c Dukes_Bank_App ソフトウェア コンポーネントに移動し、必要な申請情報を入力します。
 - d vRealize Automation アプライアンスの完全修飾ドメイン名を [app_content_server_ip] テキストボックスに入力します。
- 5 [送信] をクリックします。

使用するネットワークと vCenter Server インスタンスによって異なりますが、Dukes Bank サンプル アプリケーションが完全にプロビジョニングされるまで約 15 ～ 20 分かかります。[展開] タブでステータスを監視することができます。アプリケーションのプロビジョニング後、[展開] タブでカatalog アイテムの詳細を表示できます。

- 6 アプリケーションのプロビジョニング後、ロード バランサ サーバの IP アドレスを特定し、Dukes Bank サンプル アプリケーションにアクセスできます。
 - a [展開] をクリックします。
 - b Dukes Bank のサンプル アプリケーションの展開を見つけ、展開名をクリックします。
 - c [コンポーネント] タブで、Apache ロード バランサ サーバを選択します。
 - d [ネットワーク] タブを選択します。
 - e IP アドレスをメモします。
- 7 Dukes Bank サンプル アプリケーションにログインします。
 - a `http://IP_Apache_Load_Balancer:8081/bank/main.faces` でロード バランサ サーバに移動します。
 アプリケーション サーバに直接アクセスする場合には、`http://IP_AppServer:8080/bank/main.faces` に移動します。
 - b [ユーザー名] テキスト ボックスに **200** を入力します。
 - c [パスワード] テキスト ボックスに **foobar** を入力します。

結果

有効な Dukes Bank サンプル アプリケーションが完成しました。独自のブループリント開発を初めて行う場合、vRealize Automation の評価ツール、または vRealize Automation の機能やコンポーネントの理解を支援する学習リソースとしてご利用ください。

提供されているスタンドアローン ブループリントのダウンロードと構成

vRealize Automation アプライアンスから、提供されているスタンドアローン ブループリントと関連するソフトウェア コンポーネントをダウンロードできます。

[Download and Configure vRealize Automation Standalone Blueprint](#) では、vRealize Automation アプライアンスからスタンドアローンの vRealize Automation ブループリントをダウンロードし、vRealize Automation でブループリントをインポートおよび構成して、複数の vRealize Orchestrator ワークフローと組み合わせて使用するプロセスについて説明しています。

複数開発者環境でのブループリントおよびその他の IaaS コンテンツの作成

vRealize Orchestrator ワークフローを vRealize Suite およびサード パーティ製の開発者ツールと組み合わせることで、vRealize Automation ブループリントが同一の場合でも、異なる場合でも、複数の開発者が複数の vRealize Automation ブループリント アーティファクトに対して同時に作業することができます。

vRealize Suite Lifecycle Manager などのツールを使用して、vRealize Automation やその他の vRealize Suite ツールおよび OVA と、GitLab、GitHub、Houdini などのサード パーティ製のツール、および [VMware Solution Exchange](#) のその他のアプリケーション アーティファクトの複数開発者環境を簡素化することができます。

vRealize Automation ブループリントと、プロパティ、イベント ブローカ サブスクリプション、ソフトウェア コンポーネント、複数開発者環境の vRealize Orchestrator ワークフローなどのその他の IaaS コンテンツの作成については、次のリソースを参照してください。

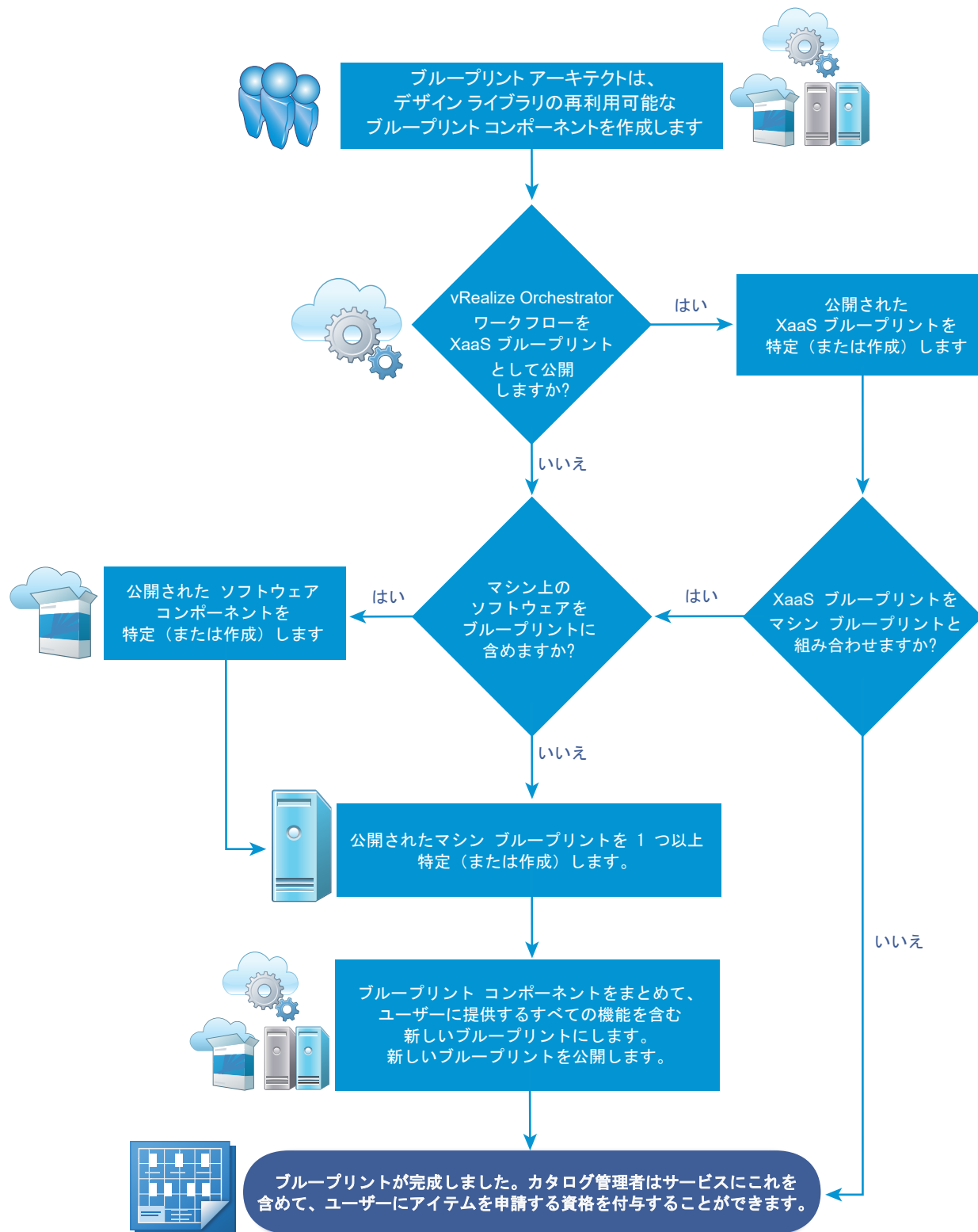
- [ビデオ - What's New in Lifecycle Manager](#)
- [ブログの記事 - vRealize Automation with Infrastructure Blueprint - Configuring Multi-developer Environment](#)
- [ドキュメント - 提供されているスタンドアローン ブループリントのダウンロードと構成](#)
- [ブログの記事 - Lifecycle Manager with GitLab Integration](#)
- [ブログの記事 - LifeCycle Manager overview](#)

複合ブループリントの組み合わせ

公開したブループリントとブループリント コンポーネントを新しい方法で組み合わせて再利用し、高度な機能を提供する IT サービス パッケージを作成できます。

コンポーネント ブループリントにカスタム フォームがある場合、カスタム申請フォームは新しいブループリントに適用されません。新しいブループリントの新規フォームを作成する必要があります。カスタム申請フォームの詳細については、[ブループリント申請フォームのカスタマイズ](#)を参照してください。

図 3-5. 複合ブループリントを組み合わせるためのワークフロー



■ ネストされたブループリントの動作について

ブループリントは、1つのコンポーネントとして別のブループリントにネストすることで再利用できます。ブループリントのネストは再利用と、マシンのプロビジョニングにおけるモジュラー性制御を目的として実施できますが、ネストされたブループリントを操作する際には特定のルールと考慮事項があります。

■ **ブループリントを組み合わせる際のマシン コンポーネントと ソフトウェア コンポーネントの使用**

ブループリントを組み合わせる際に、サポートされるマシン コンポーネントの上部に ソフトウェア コンポーネントを配置して、提供します。

■ **ブループリント コンポーネント間でのプロパティ バインドの作成**

いくつかの展開シナリオでは、コンポーネントは、自身をカスタマイズするために、別のコンポーネントのプロパティ値を必要とします。XaaS、マシン、ソフトウェア、およびカスタム プロパティをブループリント内の他のプロパティにバインドできます。

■ **依存関係の作成とプロビジョニングの順序の制御**

あるブループリント コンポーネントの情報が、別のコンポーネントのプロビジョニングの完了に必要な場合、依存関係にあるコンポーネントが先にプロビジョニングされないように、デザイン キャンバスで明示的な依存関係を描画してプロビジョニングに順序付けをすることができます。明示的な依存関係によって、展開のビルド順が制御され、スケール インやスケール アウトの処理中に従属する更新がトリガされます。ソフトウェア コンポーネントは、ブループリント内で順序付けされている必要があります。

ネストされたブループリントの動作について

ブループリントは、1つのコンポーネントとして別のブループリントにネストすることで再利用できます。ブループリントのネストは再利用と、マシンのプロビジョニングにおけるモジュラー性制御を目的として実施できますが、ネストされたブループリントを操作する際には特定のルールと考慮事項があります。

1つ以上のネストされたブループリントを含むブループリントは外部ブループリントと呼ばれます。あるブループリントを作成または編集しながら、別のブループリント コンポーネントをデザイン キャンバスに追加する場合、このブループリント コンポーネントはネストされたブループリントと呼ばれ、ネストされたブループリントが追加されたコンテナ ブループリントは外部ブループリントと呼ばれます。

ネストされたブループリントを使用するには、必ずしも分かりやすいとはいえない考慮事項が存在します。マシンのプロビジョニング機能を最大限活用するには、ルールおよび考慮事項を理解することが重要です。

ブループリントのネストに関する一般的なルールと考慮事項

- ブループリントの複雑性を最小限に抑えるためのベスト プラクティスとして、ブループリントのレベルを 3 つに制限します。最上位レベルのブループリントは 3 つのレベルの 1 つです。
- ユーザーが外部ブループリントを使用できる場合、そのユーザーはそれにネストされたブループリントも使用できます。
- 承認ポリシーをブループリントに適用することができます。承認されると、ブループリント カタログ アイテムおよびそのコンポーネント（ネストされたブループリントなど）すべてがプロビジョニングされます。また、異なる承認ポリシーを別のコンポーネントに適用することもできます。承認ポリシーはすべて、申請されたブループリントがプロビジョニングされるまでに承認する必要があります。

- 公開済みのブループリントを編集する際には、このブループリントを使用してすでにプロビジョニングされている展開は変更しません。プロビジョニング時、作成される展開では、自身にネストされたブループリントを含むブループリントから現在の値を読み取ります。プロビジョニング済みの展開に転送できる変更は、スクリプトの更新やアンインストールを行うための編集のような、ソフトウェア コンポーネントへの編集のみです。
- 以下の場合を除き、外部ブループリントで定義された設定によって、ネストされたブループリントで構成された設定がオーバーライドされます。
 - ネストされたブループリントの名前は変更できますが、ネストされたブループリント内のマシン コンポーネントや他のコンポーネントの名前を変更することはできません。
 - ネストされたブループリント内のマシン コンポーネントのカスタム プロパティを追加または削除することはできません。ただし、それらのカスタム プロパティは編集できます。ネストされたブループリント内のマシン コンポーネントのプロパティ グループを追加、編集、または削除することはできません。

- ネストされたブループリントの設定に対する変更（他のアーキテクトによる変更も含む）は、外部ブループリントに表示されます。ただし、外部ブループリントでこれらの設定をオーバーライドした場合を除きます。

- 外部ブループリントの最大リース時間は、コンポーネント ブループリントの最大リースの値に制限されます。

ネストされたブループリントおよび外部ブループリントで指定されたリース時間には、任意の値を設定できます。ただし、外部ブループリントの最大リース時間は、ネストされたブループリントの最大リース時間のうち最も小さい値に制限する必要があります。これにより、アプリケーション アーキテクトは、不変および可変のリース値を含む複合ブループリントを設計できますが、設計した複合ブループリントは、インフラストラクチャ アーキテクトが指定した制約内に収まります。ネストされたブループリントで定義された最大リース値が、外部ブループリントで定義された最大リース値よりも小さい場合は、プロビジョニング申請が失敗します。

- 外部ブループリントでの作業中は、ネストされたブループリント内のマシン コンポーネントに対して構成されたマシン リソース設定をオーバーライドできます。
- 外部ブループリントでの作業中は、ネストされたブループリント内のマシン コンポーネントにソフトウェア コンポーネントをドラッグできます。
- ネストされたブループリント内のマシン コンポーネントが削除されたブループリント、またはマシン コンポーネントの ID が変更されたブループリントを開いたときに、マシン コンポーネントが現在のブループリントのコンポーネントに関連付けられている場合、関連付けられているコンポーネントが削除され、次のようなメッセージが表示されます。

現在のブループリント内のコンポーネントが参照しているネストされたブループリント内のマシン コンポーネントが削除されたか、またはそのマシン コンポーネントの ID が変更されています。存在しないか変更されたマシン コンポーネント ID に関連付けられている現在のブループリント内のコンポーネントは、すべて削除されました。ネストされたブループリント内の存在しないか変更されたマシン コンポーネント ID と現在のブループリント内のコンポーネントとの関連付けの履歴を維持して、ネストされたブループリントの問題を修正するには、[キャンセル] をクリックします。ネストされたブループリントを開き、存在しない元の ID のマシン コンポーネントを再び追加するか、またはマシン コンポーネントの ID を元の ID に戻してください。ネストされたブループリント内の存在しないか変更されたマシン コンポーネント ID と現在のブループリント内のコンポーネントとの関連付けの履歴をすべて削除するには、[保存] をクリックします。

- ブループリントを公開すると、ソフトウェア コンポーネントのデータはスナップショットのように扱われます。ソフトウェア コンポーネントのプロパティに後で変更を加えても、ソフトウェア コンポーネントが含まれるブループリントは新しいプロパティのみを認識します。ブループリントを公開した時点でソフトウェア コンポー

メントにあったプロパティを更新しても、ブループリントでは更新されません。ブループリントの公開後に追加したプロパティのみが、ブループリントに継承されます。ただし、ソフトウェア コンポーネントが含まれるブループリントでソフトウェア コンポーネントのインスタンスを変更して、そのブループリントを変更することができます。

ブループリントのネストに関するネットワークおよびセキュリティのルールおよび考慮事項

- 外部ブループリントのネットワークおよびセキュリティ コンポーネントは、ネストされたブループリントで定義したマシンに関連付けることができます。
- NSX ネットワーク、セキュリティ、およびロード バランサ コンポーネント、およびそれらの設定は、ネストされたブループリントではサポートされていません。
- アプリケーションの隔離が外部ブループリントに適用されると、ネストされたブループリントで指定したアプリケーションの隔離設定がオーバーライドされます。
- 外部ブループリントで定義されるトランスポート ゾーン設定は、ネストされたブループリントで指定したトランスポート ゾーン設定をオーバーライドします。
- 外部ブループリントでの作業中は、内部またはネストされたブループリントで構成したネットワーク コンポーネント設定およびマシン コンポーネント設定に関連するロード バランサ設定を構成できます。
- オンデマンド NAT ネットワーク コンポーネントを含むネストされたブループリントの場合、外部ブループリントでは、このオンデマンド NAT ネットワーク コンポーネントで指定した IP アドレス範囲を編集できません。
- 外部ブループリントには、オンデマンドのネットワーク設定またはロード バランサ設定を含む内部ブループリントを含めることはできません。NSX のオンデマンドのネットワーク コンポーネントまたは NSX のロード バランサ コンポーネントを含む内部ブループリントの使用は、サポートされていません。
- NSX のネットワークまたはセキュリティ コンポーネントを含むネストされたブループリントの場合、ネストされたブループリントで指定したネットワーク プロファイルまたはセキュリティ ポリシーの情報を変更できません。ただし、外部ブループリントに追加した他の vSphere マシン コンポーネントのそれらの設定を再利用することはできます。
- ネストされたブループリント内の NSX のネットワークとセキュリティ コンポーネントに複合ブループリント内で一意の名前が付けられるようにするには、vRealize Automation が、まだ一意の名前が付いていないネットワークとセキュリティ コンポーネントに、ネストされたブループリント ID のプリフィックスを付けます。たとえば、ID 名 xbp_1 の付いたブループリントを外部ブループリントに追加し、両方のブループリントに OD_Security_Group_1 という名前のオンデマンド セキュリティ グループ コンポーネントが含まれる場合、ネストされたブループリント内のコンポーネントは、ブループリント デザイン キャンバスで xbp_1_OD_Security_Group_1 という名前に変更されます。外部ブループリントのネットワークとセキュリティ コンポーネントの名前にプリフィックスはありません。
- コンポーネント設定は、コンポーネントがどのブループリントにあるかによって異なります。たとえば、内部と外部の両方のブループリント レベルでセキュリティ グループ、セキュリティ タグまたはオンデマンド ネットワークを含める場合、外部ブループリントの設定が内部ブループリントの設定をオーバーライドします。内部ブループリント レベルで動作する既存のネットワークを除き、ネットワークおよびセキュリティ コンポーネントは外部ブループリント レベルでのみサポートされます。問題を回避するため、セキュリティ グループ、セキュリティ タグ、およびオンデマンド ネットワークは、すべて外部ブループリントのみに追加します。

ブループリントのネストに関するソフトウェア コンポーネントの考慮事項

拡張可能なブループリントの場合は、ベスト プラクティスとして、他のブループリントを再利用しない単一レイヤのブループリントを作成することが推奨されます。通常、拡張処理中の更新プロセスは、ソフトウェア プロパティをマシン プロパティにバインドする際に作成する依存関係などの、暗黙的な依存関係によってトリガされます。しかし、ネストされたブループリントにおける暗黙的な依存関係によって更新プロセスがトリガされない場合もあります。拡張可能なブループリントでネストされたブループリントを使用する必要がある場合は、ネストされたブループリントのコンポーネント間で手動で依存関係を描画して、常に更新をトリガする明示的な依存関係を作成することができます。

ブループリントを組み合わせる際のマシン コンポーネントと ソフトウェア コンポーネントの使用

ブループリントを組み合わせる際に、サポートされるマシン コンポーネントの上部に ソフトウェア コンポーネントを配置して、提供します。

ソフトウェア コンポーネントをサポートするには、ゲスト エージェントとソフトウェア ブートストラップ エージェントが含まれるテンプレート、スナップショット、または Amazon マシン イメージに基づいて、選択するマシンブループリントにマシン コンポーネントを含める必要があります。また、サポートされているプロビジョニング方法を使用する必要もあります。

ソフトウェア エージェントはインターネット プロトコル バージョン 6 (IPv6) をサポートしていないため、IPv4 設定を使用します。

注： ソフトウェア コンポーネントは、ブループリントにおいて順序付けされた依存関係が必要です。順序付けされていないソフトウェア コンポーネントが原因でブループリントのプロビジョニングが失敗することがあります。ソフトウェア コンポーネントに関して実際の順序の依存関係がない場合は、ソフトウェア コンポーネント間の擬似依存関係を追加することで、ブループリントの順序付け要件を満たすことができます。

拡張可能なブループリントを設計する場合は、ベスト プラクティスとして、他のブループリントを再利用しない単一レイヤーのブループリントを作成することが推奨されます。通常、拡張処理中に使用される更新プロセスは、プロパティ バインドなどの暗黙的な依存関係によってトリガされます。しかし、ネストされたブループリントにおける暗黙的な依存関係によって更新プロセスがトリガされない場合もあります。

IaaS アーキテクト、アプリケーション アーキテクト、ソフトウェア アーキテクトはすべて、ブループリントを組み合わせたことができますが、マシン コンポーネントを構成できるのは IaaS アーキテクトだけです。IaaS アーキテクトでない場合、独自のマシン コンポーネントを構成することはできませんが、IaaS アーキテクトが作成して公開したマシン ブループリントを再利用することは可能です。

ソフトウェア コンポーネントをデザイン キャンバスに正常に追加するには、ビジネス グループ メンバー、ビジネス グループ管理者、またはテナント管理者ロールにターゲット カタログへのアクセス権があることも必要です。

拡張可能なブループリントでネストされたブループリントを使用する必要がある場合は、ネストされたブループリントのコンポーネント間で手動で依存関係を描画して、常に更新をトリガする明示的な依存関係を作成することができます。

注： ブループリントを公開すると、ソフトウェア コンポーネントのデータはスナップショットのように扱われます。ソフトウェア コンポーネントのプロパティに後で変更を加えても、ソフトウェア コンポーネントが含まれるブループリントは新しいプロパティのみを認識します。ブループリントを公開した時点でソフトウェア コンポーネントにあったプロパティを更新しても、ブループリントでは更新されません。ブループリントの公開後に追加したプロパティのみが、ブループリントに継承されます。ただし、ソフトウェア コンポーネントが含まれるブループリントでソフトウェア コンポーネントのインスタンスを変更して、そのブループリントを変更することができます。

表 3-64. ソフトウェアをサポートするプロビジョニングの方法

マシン タイプ	プロビジョニング方法
vSphere	クローン作成
vSphere	リンク クローン
vCloud Director	クローン作成
vCloud Air	クローン作成
Amazon AWS	Amazon マシン イメージ

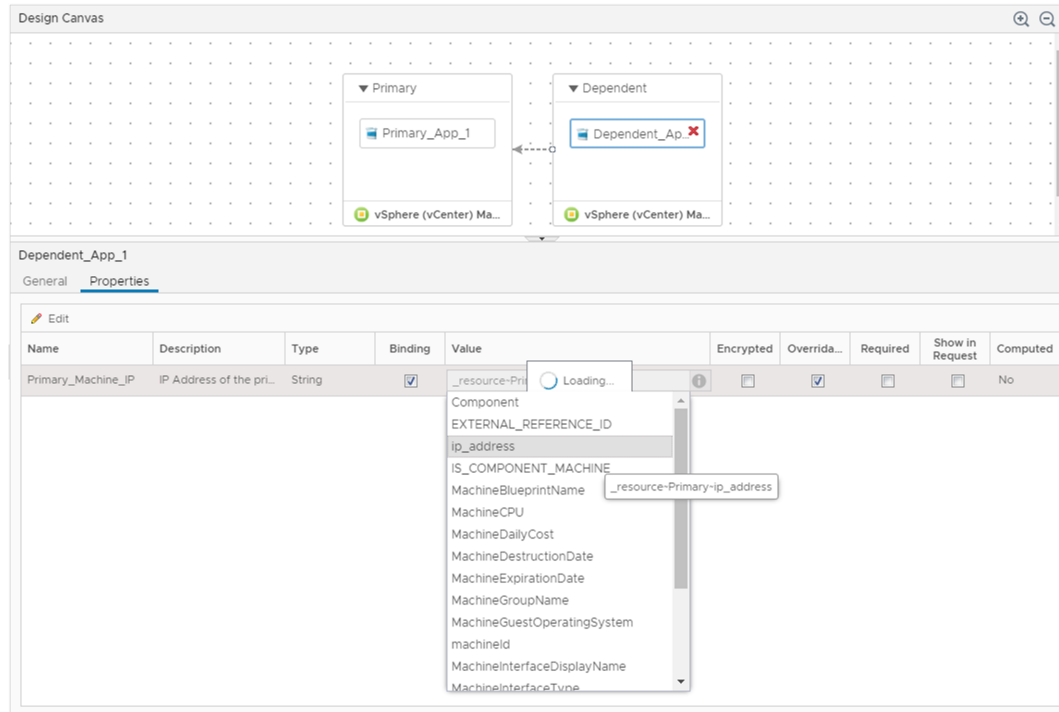
ブループリント コンポーネント間でのプロパティ バイン드의作成

いくつかの展開シナリオでは、コンポーネントは、自身をカスタマイズするために、別のコンポーネントのプロパティ値を必要とします。XaaS、マシン、ソフトウェア、およびカスタム プロパティをブループリント内の他のプロパティにバインドできます。

たとえば、ソフトウェア アーキテクトが、WAR コンポーネントのライフ サイクル スクリプトでプロパティ定義を変更できるとします。WAR コンポーネントには、Apache Tomcat サーバ コンポーネントのインストール場所が必要になるため、ソフトウェア アーキテクトは WAR コンポーネントを構成し、server_home プロパティ値を Apache Tomcat サーバの install_path プロパティ値に設定します。アーキテクトがブループリントを組み合わせるため、ソフトウェア コンポーネントが正常にプロビジョニングされるように、Apache Tomcat サーバの install_path プロパティに server_home プロパティをバインドする必要があります。

ブループリントのコンポーネントを構成する場合は、プロパティ バインドを設定します。[ブループリント] ページで、キャンバスにコンポーネントをドラッグし、[プロパティ] タブをクリックします。プロパティをブループリント内の別のプロパティにバインドするには、[バインド] チェックボックスを選択します。値テキスト ボックスの *ComponentName~PropertyName* を入力するか、下矢印を使用して利用可能なバインド オプションのリストを生成することができます。コンポーネントとプロパティとの間の区切り文字としてチルダ文字 (~) を使用します。たとえば、property dp_port にバインドするには、MySQL ソフトウェア コンポーネントで mysql-db_port と入力できます。マシンの IP アドレスまたは ソフトウェア コンポーネントのホスト名など、プロビジョニング中に構成されるプロパティをバインドするには、_resource~ComponentName~PropertyName と入力します。たとえば、マシンの予約名をバインドするには、_resource~vSphere_Machine_1~MachineReservationName と入力できます。

図 3-6. マシンの IP アドレスにソフトウェア プロパティをバインドする



依存関係の作成とプロビジョニングの順序の制御

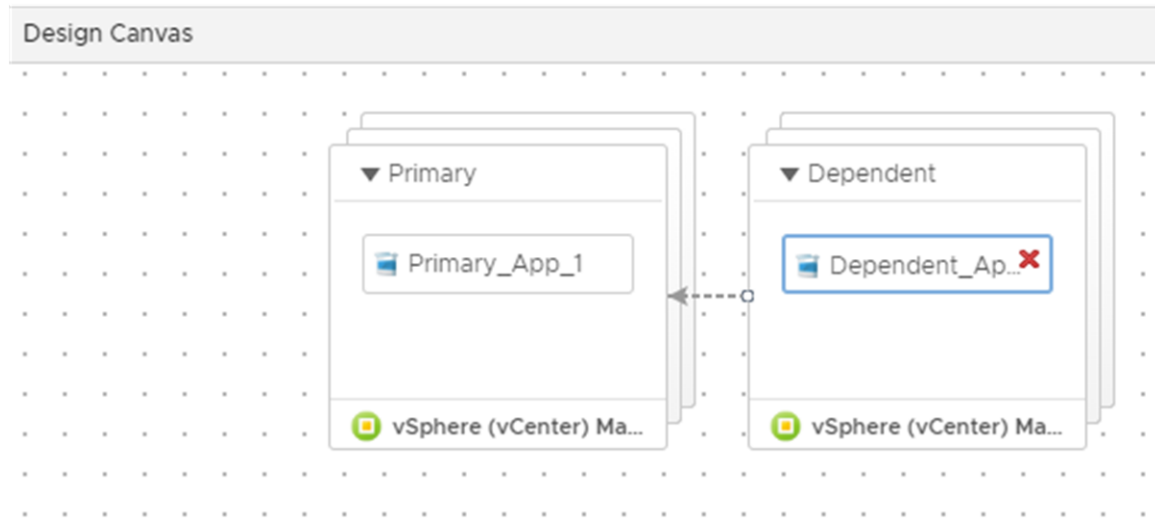
あるブループリント コンポーネントの情報が、別のコンポーネントのプロビジョニングの完了に必要な場合、依存関係にあるコンポーネントが先にプロビジョニングされないように、デザイン キャンバスで明示的な依存関係を描画してプロビジョニングに順序付けをすることができます。明示的な依存関係によって、展開のビルド順が制御され、スケール インやスケール アウトの処理中に従属する更新がトリガされます。ソフトウェア コンポーネントは、ブループリント内で順序付けされている必要があります。

複数のマシンとアプリケーションを含んだブループリントを設計する際には、別のマシンのプロパティがないと、目的とするマシンへのアプリケーションのインストールが完了できない場合があります。たとえば Web サーバを構築する場合、アプリケーションをインストールしてデータベース テーブルをインスタンス化するためには、事前にデータベース サーバのホスト名が必要です。明示的な依存関係をマップすると、Web サーバのプロビジョニングが完了してから、データベース サーバのプロビジョニングが開始されます。

注： ソフトウェア コンポーネントは、ブループリントにおいて順序付けされた依存関係が必要です。順序付けされていないソフトウェア コンポーネントが原因でブループリントのプロビジョニングが失敗することがあります。ソフトウェア コンポーネントに関して実際の順序の依存関係がない場合は、ソフトウェア コンポーネント間の擬似依存関係を追加することで、ブループリントの順序付け要件を満たすことができます。

デザイン キャンバスで依存関係をマッピングするには、依存する側のコンポーネントから依存される側のコンポーネントに線を描画します。描画が完了すると、2 番目にビルドするコンポーネントから 1 番目にビルドするコンポーネントに向かう矢印が表示されます。たとえば「依存関係のマッピングによるビルド順の制御」の図で、依存するマシンのプロビジョニングは、プライマリ マシンが構築されるまで実行されません。また両方のマシンを同時にプロビジョニングするように構成する一方で、ソフトウェア コンポーネント間に依存関係を描画することもできます。

図 3-7. 依存関係のマッピングによるビルド順の制御



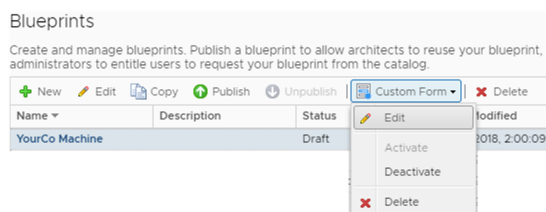
拡張可能なブループリントを設計する場合は、ベスト プラクティスとして、他のブループリントを再利用しない単一レイヤーのブループリントを作成することが推奨されます。通常、拡張処理中の更新プロセスは、ソフトウェア プロパティをマシン プロパティにバインドする際に作成する依存関係などの、暗黙的な依存関係によってトリガされます。しかし、ネストされたブループリントにおける暗黙的な依存関係によって更新プロセスがトリガされない場合もあります。拡張可能なブループリントでネストされたブループリントを使用する必要がある場合は、ネストされたブループリントのコンポーネント間で手動で依存関係を描画して、常に更新をトリガする明示的な依存関係を作成することができます。

ブループリント申請フォームのカスタマイズ

作成および公開されたカタログのブループリントをユーザーが申請すると、ブループリントにフォームが表示されます。ブループリントの作成または編集時には、デフォルト フォームを使用することも、ブループリント申請フォームをカスタマイズすることもできます。デフォルト フォームで指定された情報や必要な情報が、ユーザーに表示したい内容と異なる場合には、フォームをカスタマイズします。

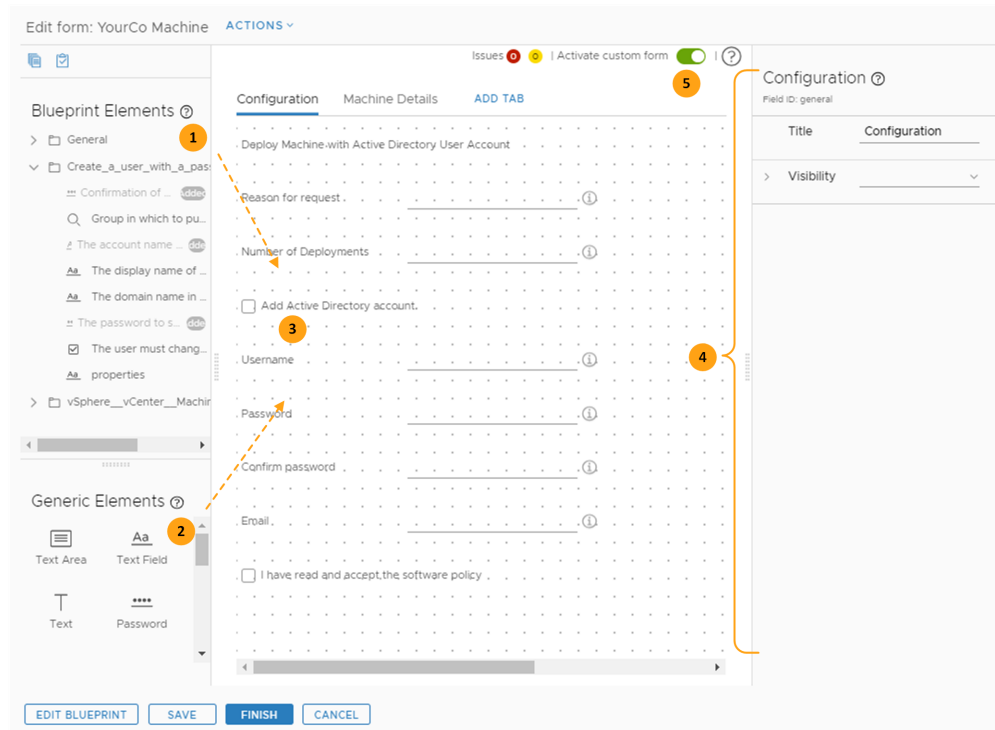
申請フォームのカスタマイズ

カスタム申請フォーム デザイナには、ブループリント データ グリッドまたはブループリント キャンバスからアクセスします。



カスタム申請フォーム デザイナ

カスタム フォームを作成するにはフォーム デザイナを使用します。



カスタム フォームは以下の手順で作成します。

- 1 デザイン キャンバス (3) に要素 (1 および 2) をドラッグします。
- 2 プロパティ ペイン (4) を使用して各要素を構成します。
- 3 フォーム (5) を有効にします。

上書きを禁止するようにプロパティが構成されていなければ、ブループリント要素のリストにはカスタム プロパティが含まれます。プロパティのオーバーライド可能オプションが [いいえ] に設定されている場合、フィールドはカスタマイズ対象になりません。

検証と制約

カスタム フォーム デザイナは、フィールドに制約を追加するデータ検証と、外部検証ソースを使用したデータ検証をサポートしています。フォームを作成する際に適用される制約オプションについては、[カスタム フォーム デザイナのフィールド プロパティ](#)を参照してください。

- 制約の例については、[Active Directory オプションを使用したカスタム申請フォームの作成](#)を参照してください。
- 外部検証については、[カスタム フォーム デザイナでの外部検証の使用](#)を参照してください。

検証と依存関係をフォームに追加するときは、申請ユーザーがフィールドに入力するか、システムがフィールドを検証する必要があります。これを行わないと、依存フィールドがフォームに表示されない場合があります。

たとえば、最初のタブのフィールドに後続のフィールドが依存している場合、前のタブで依存値が指定されるまで、後続のタブに依存フィールドが表示されない場合があります。

カスタム申請フォームのアクション

アクション メニュー項目を使用すると、フォームへの入力や、他のシステムとのフォームの共有が可能になります。

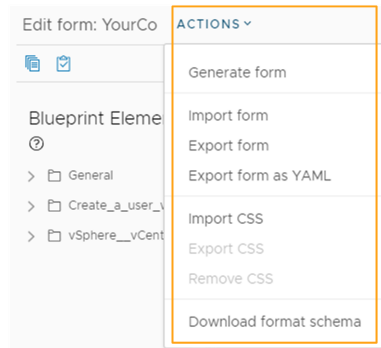


表 3-65. カスタム申請フォームのアクション メニュー項目

アクション メニュー項目	説明
[フォームの生成]	<p>各ブループリント コンポーネントに関連付けられているすべてのフィールドをフォーム デザイナに追加します。各コンポーネントはタブに追加されます。フォームの作成または変更後にこのメニュー項目を使用すると、現在のフォームは生成されたフォームで上書きされます。</p> <p>このメニュー項目を使用すると、カタログでユーザーに表示しないフィールドの非表示または削除ができます。フォームを生成しない場合でも、ユーザーに表示するテキスト ボックスを追加したり構成したりすることができます。</p>
[フォームのインポート]	JSON または YAML ファイルからカスタム フォームをインポートします。
[フォームのエクスポート]	<p>現在のカスタム フォームを JSON ファイルとしてエクスポートします。</p> <p>別のブループリントで使用するコンポーネントに一致する部分を使用するときは、ファイルをエクスポートします。</p>
[フォームを YAML 形式でエクスポート]	<p>現在のカスタム フォームを YAML 形式でエクスポートします。</p> <p>カスタム フォームを vRealize Automation インスタンスから別のインスタンスに移動するときは、ファイルを YAML 形式でエクスポートします。たとえば、テスト環境から本番環境への移動の場合です。フォームを YAML 形式で編集する場合には、フォームをエクスポートして編集し、ブループリントにインポートして戻します。</p>

表 3-65. カスタム申請フォームのアクション メニュー項目 （続き）

アクション メニュー項目	説明
[CSS のインポート]	<p>カタログ申請フォームを拡張する CSS ファイルをインポートします。ファイルは以下の例のようになります。この例では、フォント サイズを変更してテキストを太字にしています。参照されるフィールドは、上記のカスタム申請フォーム デザイナのセクションにある画像に表示されている [Active Directory ユーザー アカウントによるマシンの展開] テキスト フィールドです。</p> <pre>#<field-ID> .grid-item { font-size: 16px; font-weight: bold; width: 600px; }</pre> <p>この例の <field-ID> は、キャンバスのフィールドの ID です。値を確認するには、キャンバスでフィールドを選択します。値は、右側のペインの名前の下にあります。上記の画像では、値は text_d947bc97 です。</p> <p>ファイルをインポートするには、これを <filename>.css として保存します。</p>
[CSS のエクスポート]	インポートした CSS をエクスポートします。
[CSS の削除]	<p>カスタム CSS を破棄します。</p> <p>破棄した CSS は復元できません。</p>
[フォーマット スキーマのダウンロード]	<p>カスタム フォームで使用されるコントロールとステートメントの構造と説明を含む JSON ファイルをダウンロードします。</p> <p>このスキーマを使用すると、フォームの作成や既存のフォームの変更ができます。変更した JSON ファイルは、カスタム フォームとしてインポートできます。</p>

Active Directory オプションを使用したカスタム申請フォームの作成

デフォルト フォームで申請ユーザーに情報が過不足なく提供されていない場合には、カスタム フォームを作成します。フォームへのフィールドの追加、フォーム上でのフィールドの非表示、フィールドへの事前入力と、その表示/非表示が可能です。

この使用事例は、vSphere 仮想マシンのタイプを含むブループリントと、その仮想マシンに Active Directory 管理者アカウントを構成する XaaS ブループリントに基づいています。XaaS ブループリントは、「パスワードを使用したグループのユーザーの作成」ワークフローに基づいています。

この使用事例の目的は次の通りです。

- ユーザーに管理者パスワードを設定するオプションを提供する。
- CPU とメモリの値の両方に GB 単位が使用されるように、マシンの詳細を事前設定する。

この使用事例の利点について説明します。この使用事例には、以下のフォーム カスタマイズの例が含まれています。

- 特定のフィールドを空のフォームに追加する。
- 表示/非表示のチェック ボックスを設定する。

- 申請ユーザーがチェック ボックスを選択するまで、フィールドを非表示にする。
- 検証をフィールドに追加する。
- ブループリント フィールドが MB 単位で計算されていても、メモリ フィールドを GB 単位で表示する。
- 正規表現を使用する。

前提条件

- アプリケーション アーキテクト、ソフトウェア アーキテクト、またはインフラストラクチャ アーキテクト として、vRealize Automation にログインします。
- vSphere ブループリントと XaaS ブループリントを含む YourCo マシンとユーザーのブループリントを作成し、グループにパスワード付きの Active Directory ユーザー アカウントを作成します。例については、[ユーザーを作成するための XaaS ブループリントの作成](#)を参照してください。

手順

- 1 [設計] - [ブループリント] を選択します。
- 2 YourCo マシンとユーザーのブループリントを含む行を強調表示して、[カスタム フォーム] - [編集] の順にクリックします。
- 3 [全般] タブの名前を変更します。
 - a タブをクリックします。
 - b 右側の [プロパティ] ペインの [タイトル] プロパティに「**Configuration**」と入力します。
- 4 新しい [Configuration] タブに、以下のフィールドを、値を指定して追加および設定します。

提供されている表示、値、制約の値を使用します。

フォームをビルドする際にエラーがあれば解決します。

スクリーンショット内のフィールド	ブループリントの要素のソース	表示	値	制約
Active Directory ユーザー アカウントを使用してマシンを展開する	汎用要素 > テキスト	ラベルとタイプ <ul style="list-style-type: none"> ■ 表示タイプ = テキスト 可視性 <ul style="list-style-type: none"> ■ 値のソース = 定数 ■ 表示 = はい 	デフォルト値 <ul style="list-style-type: none"> ■ デフォルト値 = Active Directory ユーザー アカウントを使用してマシンを展開する ■ 値のソース = 定数 	
申請の理由	ブループリントの要素 > vSphere_vCenter_Machine > 説明	ラベルとタイプ <ul style="list-style-type: none"> ■ ラベル = 申請の理由 ■ 表示タイプ = テキスト フィールド 可視性 <ul style="list-style-type: none"> ■ 値のソース = 定数 ■ 表示 = はい 読み取り専用 <ul style="list-style-type: none"> ■ 値のソース = 定数 ■ 読み取り専用 = いいえ カスタム ヘルプ <ul style="list-style-type: none"> ■ Signpost のヘルプ = 申請の理由を入力します。 		必須 <ul style="list-style-type: none"> ■ 値のソース = 定数 ■ 必須 = はい
展開の数	ブループリントの要素 > 全般 > 展開の数	ラベルとタイプ <ul style="list-style-type: none"> ■ ラベル = 展開の数 ■ 表示タイプ = 整数 可視性 <ul style="list-style-type: none"> ■ 値のソース = 定数 ■ 表示 = はい 読み取り専用 <ul style="list-style-type: none"> ■ 値のソース = 定数 ■ 読み取り専用 = いいえ カスタム ヘルプ <ul style="list-style-type: none"> ■ Signpost のヘルプ = 展開するブループリントのインスタンス数を選択します。 	デフォルト値 <ul style="list-style-type: none"> ■ 値のソース = 定数 ■ デフォルト値 = 1 	必須 <ul style="list-style-type: none"> ■ 値のソース = 定数 ■ 必須 = はい 最小値 <ul style="list-style-type: none"> ■ 値のソース = 定数 ■ 最小値 = 1
Active Directory アカウントの追加チェックボックス	汎用要素 > チェック ボックス	ラベルとタイプ <ul style="list-style-type: none"> ■ ラベル = Active Directory アカウントを追加する ■ 表示タイプ = チェック ボックス 可視性 <ul style="list-style-type: none"> ■ 値のソース = 定数 ■ 表示 = はい 		

スクリーンショット内のフィールド				
	ブループリントの要素のソース	表示	値	制約
ユーザー名	ブループリントの要素 > グループにユーザーとパスワードを作成する > ユーザーのアカウント名	ラベルとタイプ <ul style="list-style-type: none"> ■ ラベル = ユーザー名 ■ 表示タイプ = テキスト フィールド 可視性 <p>注： この可視性プロパティは、後続のフィールドで同じように構成され、[Active Directory アカウントを追加する] チェック ボックスが選択されない場合、フィールドは非表示になります。</p> <ul style="list-style-type: none"> ■ 値のソース = 条件値 ■ 式 = 値の設定 = はい [Active Directory アカウントを追加する] が [はい] と等しい場合 <p>カスタム ヘルプ</p> <ul style="list-style-type: none"> ■ Signpost のヘルプ = 管理者ユーザー名を入力します。 	デフォルト値 <ul style="list-style-type: none"> ■ 値のソース = 定数 ■ デフォルト値 = 管理者 	必須 <ul style="list-style-type: none"> ■ 値のソース = 定数 ■ 必須 = はい 正規表現 <p>注： 正規表現は、JavaScript 構文に従います。</p> <ul style="list-style-type: none"> ■ 値のソース = 定数 ■ 正規表現 = "[a-z]*\$" ■ 検証エラー メッセージ = ユーザー名に特殊文字や数字を含めることはできません。
パスワード	ブループリントの要素 > グループにユーザーとパスワードを作成する > 新しく作成されたアカウントのパスワードの設定	ラベルとタイプ <ul style="list-style-type: none"> ■ ラベル = パスワード ■ 表示タイプ = パスワード 可視性 <ul style="list-style-type: none"> ■ 値のソース = 条件値 ■ 式 = 値の設定 = はい [Active Directory アカウントを追加する] が [はい] と等しい場合 <p>カスタム ヘルプ</p> <ul style="list-style-type: none"> ■ Signpost のヘルプ = 管理者アカウントのパスワードを指定します。 		必須 <ul style="list-style-type: none"> ■ 値のソース = 定数 ■ 必須 = はい 正規表現 <ul style="list-style-type: none"> ■ 値のソース = 定数 ■ 正規表現 = "^(?=.*[A-Z])(?=.*[O-9])(?=.*[a-z]).{8,}\$" ■ メッセージ = 管理者パスワードは 8 文字以上で指定する必要があります。英数字と特殊文字を含めることができます。

スクリーンショット内のフィールド				
フィールド	ブループリントの要素のソース	表示	値	制約
パスワードの確認	ブループリントの要素 > グループにユーザーとパスワードを作成する > パスワードの確認	ラベルとタイプ ■ ラベル = パスワードの確認 表示タイプ = パスワード 可視性 ■ 値のソース = 条件値 ■ 式 = 値を [はい] に設定します [Active Directory アカウントを追加する] が [はい] と等しい場合 カスタム ヘルプ ■ Signpost のヘルプ = 管理者アカウントのパスワードを再入力します。		必須 ■ 値のソース = 定数 ■ 必須 = はい フィールドに一致 ■ フィールドに一致 = パスワード
メール	汎用要素 > テキスト フィールド	ラベルとタイプ ■ ラベル = E メール ■ 表示タイプ = テキスト フィールド 可視性 ■ 値のソース = 条件値 ■ 式 = 値の設定 = はい [Active Directory アカウントを追加する] が [はい] と等しい場合 カスタム ヘルプ ■ Signpost のヘルプ = 管理者の E メールを指定します。	デフォルト値 ■ 値のソース = 計算値 ■ 演算子 = 連結 ■ 追加値 = フィールド。ユーザー名を選択します。 ■ 追加値 = 定数。 @yourco.com を入力します。	正規表現 ■ 値のソース = 定数 ■ 正規表現 = "^[A-Za-zO-9._%+~]"+@[A-Za-zO-9.-]+\.[A-Za-z]{2,}\$" ■ 検証エラー メッセージ = 有効な E メールを指定します。
「ソフトウェアポリシーを読んで同意しました」チェック ボックス。	汎用要素 > チェック ボックス	ラベルとタイプ ■ 要素のラベル = ソフトウェアポリシーを読んで同意しました ■ 表示タイプ = チェック ボックス 可視性 ■ 値のソース = 条件値 ■ 式 = 値の設定 = はい [Active Directory アカウントを追加する] が [はい] と等しい場合		

5 [タブの追加] をクリックして、右の [タイトル] プロパティに **マシンの詳細** を入力します。

6 [マシンの詳細] タブに次のフィールドを構成します。

提供されている表示、値、制約の値を使用します。

スクリーンショット内のフィールド	ブループリントの要素のソース	表示	値	制約
ストレージ (GB)	ブループリントの要素 > vSphere_vCenter_Machine > ストレージ (GB)	ラベルとタイプ <ul style="list-style-type: none"> ■ ラベル = ストレージ (GB) ■ 表示タイプ = 整数 可視性 <ul style="list-style-type: none"> ■ 値のソース = 定数 ■ 可視性 = はい 読み取り専用 <ul style="list-style-type: none"> ■ 値のソース = 定数 ■ 読み取り専用 = いいえ 	デフォルト値 <ul style="list-style-type: none"> ■ 値のソース = 定数 ■ デフォルト値 = 4 	最小値 <ul style="list-style-type: none"> ■ 値のソース = 定数 ■ 最小値 = 2
CPU の数	ブループリントの要素 > vSphere_vCenter_Machine > CPU	ラベルとタイプ <ul style="list-style-type: none"> ■ ラベル = CPU の数 ■ 表示タイプ = 整数 可視性 <ul style="list-style-type: none"> ■ 値のソース = 定数 ■ 可視性 = はい 	デフォルト値 <ul style="list-style-type: none"> ■ 値のソース = 定数 ■ デフォルト値 = 1 	最小値 <ul style="list-style-type: none"> ■ 値のソース = 定数 ■ 最小値 = 1

スクリーンショット内のフィールド				
	ブループリントの要素のソース	表示	値	制約
メモリ (GB)	汎用要素 > 整数	ラベルとタイプ ■ ラベル = メモリ (GB) ■ 表示タイプ = 整数 可視性 ■ 値のソース = 定数 ■ 可視性 = はい	デフォルト値 ■ 値のソース = 定数 ■ デフォルト値 = 1	最小値 ■ 値のソース = 定数 ■ 最小値 = 1
メモリ (MB)	ブループリントの要素 > vSphere_vCenter_Machine > メモリ (MB)	ラベルとタイプ ■ ラベル = メモリ (MB) ■ 表示タイプ = 整数 可視性 ■ 値のソース = 定数 ■ 可視性 = いいえ	デフォルト値 ■ 値のソース = 計算値 ■ 演算子 = 乗算 ■ 追加値 = フィールド。メモリ (GB) を選択します ■ 追加値 = 定数。1024 を入力します	

- 7 すべてのエラーを解決します。フォームは保存できますが、フォームにエラーがなくなるまで有効にすることはできません。
- 8 フォームを保存してフォーム デザイナを閉じ、[完了] をクリックします。
- 9 ブループリントを選択して、[公開] をクリックします。
- 10 ユーザーがサービス カタログでアイテムを申請する時にカスタム フォームを利用できるようにするには、[ブループリント] ページのツールバーで、[カスタム フォーム] - [有効化] の順に選択します。

次のステップ

- ブループリントをサービス カタログで利用できるようにします。[サービス カタログの管理](#)を参照してください。
- カタログで、申請フォームが次の例のようになっていることを確認します。

カスタム フォーム デザイナのフィールド プロパティ

フィールド プロパティは、選択したフィールドの外観や、ユーザーに提示されるデフォルト値を決定します。また、ユーザーが vRealize Automation のカタログ申請フォームに有効なエントリを確実に指定できるように、フィールドに適用するルールを決定します。

各フィールドは個別に構成します。フィールドを選択してフィールド プロパティを編集します。

値のソース

プロパティの多くは、さまざまな値のソースのオプションから選択できます。すべてのソース オプションが、すべてのフィールド タイプまたはプロパティで利用できるわけではありません。

- [定数。]値は常に一定になります。プロパティに応じて、値は文字列、整数、正規表現の場合や、[はい] または [いいえ] などの限定されたリストから選択する場合があります。たとえば、デフォルト値の整数として 1 を指定したり、読み取り専用プロパティに [いいえ] を選択したりできます。また、フィールドのエントリを検証する正規表現を指定することもできます。
- [条件値。]値は 1 つ以上の条件に基づきます。条件は記述された順に処理されます。複数の条件が真の場合、値が真の最後の条件によってプロパティに対するフィールドの動作が決定されます。たとえば、別のフィールドの値に基づいてフィールドが表示されるかどうかを決定する条件を作成することができます。
- [外部ソース。]値は vRealize Orchestrator のアクションの結果に基づきます。たとえば、スクリプトによる vRealize Orchestrator アクションに基づいてコストを計算します。例については、[カスタム フォーム デザイナでの vRealize Orchestrator アクションの使用](#)を参照してください。

- [バインド フィールド。]値はバインドされるフィールドと同じになります。使用可能なフィールドは、同じフィールド タイプに限定されます。たとえば、認証に必要なチェック ボックス フィールドのデフォルト値を別のチェック ボックス フィールドにバインドします。申請フォームの 1 つのターゲット フィールドのチェック ボックスを選択すると、現在のフィールドのチェック ボックスが選択されます。
- [計算値。]値は、選択したフィールドと値に対する演算に基づいて決定されます。テキスト フィールドは連結演算子を使用します。整数フィールドは、選択した加算、減算、乗算、除算処理を使用します。たとえば、乗算処理を使用することでメガバイトをギガバイトに変換する整数フィールドを設定することができます。

フィールドの表示

表示プロパティを使用すると、フィールドをフォームに表示するかどうかや、カタログ ユーザーに提供するラベルやカスタム ヘルプを決定することができます。

一部のブループリントには、固定値を持つフィールドが含まれていることがあります。このタイプのフィールドをカスタム フォームに追加するときは、[表示] オプションのみが使用可能で、フィールドは常に読み取り専用です。

表 3-66. [表示] タブのオプション

オプション	説明
[ラベルとタイプ]	<p>ラベルを指定して表示タイプを選択します。</p> <p>使用可能な表示タイプはフィールドに依存します。複数のテキスト タイプをサポートするフィールドと、整数のみをサポートするフィールドがあります。利用可能な値:</p> <ul style="list-style-type: none"> ■ 10 進数 ■ ドロップダウン ■ イメージ ■ Integer ■ 複数選択 ■ パスワード ■ ラジオ グループ ■ テキスト ■ テキスト エリア ■ テキスト フィールド <p>ドロップダウンやデータ グリッドのフィールドには、[ブレースホルダ] 設定が含まれます。入力された値は、ドロップダウン メニューに内部ラベルまたは指示、あるいはデータ グリッドの一般的なラベルまたは指示として表示されます。</p> <p>値ピッカー フィールドとツリー ピッカー フィールドには、[リファレンス タイプ] の設定が含まれます。リファレンス タイプは、値またはツリー ピッカーの検索を、そのタイプをサポートする vRealize Orchestrator サーバ インベントリに限定するために使用される vRealize Orchestrator リソース タイプです。リファレンス タイプをサポートするアクションを選択して、検索をさらに制限することができます。2 つのピッカーに関する詳細については、カスタム フォーム デザインでの値ピッカーまたはツリー ピッカー要素の使用を参照してください。</p>
[可視性]	<p>申請フォームのフィールドを表示または非表示にします。</p> <ul style="list-style-type: none"> ■ [定数。][はい] を選択すると、フォームにフィールドが表示されます。フィールドを非表示にするには [いいえ] を選択します。 ■ [条件値。]可視性は真の値になる最初の式によって決定されます。たとえば、フィールドは、フォームでチェック ボックスが選択されている場合に表示されます。 ■ [外部ソース。]可視性は、選択した vRealize Orchestrator アクションの結果によって決定されます。
[読み取り専用]	<p>ユーザーがフィールドの値を変更できないようにします。</p> <ul style="list-style-type: none"> ■ [定数。]値を表示して変更を許可しない場合は [はい] を選択します。変更を許可するには [いいえ] を選択します。 ■ [条件値。]ステータスは真の値になる最初の式によって決定されます。たとえば、ストレージ フィールドが 2 GB より大きい場合、フィールドは読み取り専用になります。 ■ [外部ソース。]ステータスは、選択した vRealize Orchestrator アクションの結果によって決定されます。

表 3-66. [表示] タブのオプション（続き）

オプション	説明
[ページの行数]	データ グリッド要素の場合のみです。 行数を入力します。
[カスタム ヘルプ]	ユーザーにフィールドに関する情報を提供します。この情報は、フィールドの Signpost のヘルプに表示されます。 単純なテキストまたは href リンクを含む HTML を使用することができます。たとえば、 <code>vRealize Automation documentation</code> のように指定します。

フィールド値

デフォルト値を指定するには、値プロパティを使用します。

表 3-67. [値] タブのオプション

オプション	説明
[列]	データ グリッド要素の場合のみです。 テーブルの各列のラベル、ID、値のタイプを指定します。 データ グリッドのデフォルト値には、定義されている列と一致するヘッダー データを含める必要があります。たとえば、user_name ID 列と、user_role ID 列がある場合に、最初の行は user_name,user_role になります。 構成の例については、 カスタム フォーム デザイナでのデータ グリッド要素の使用 を参照してください。
[デフォルト値]	値のソースに基づいて、フィールドにデフォルト値を入力します。 可能なソース値はフィールドに依存します。 <ul style="list-style-type: none"> ■ [定数。]入力した文字列です。 ■ [条件値。]デフォルト値は、真の値になる最初の式によって決定されます。たとえば、[メモリ] フィールドが 512 MB 未満の場合、[ストレージ] フィールドのデフォルト値は 1 GB になります。 contains 演算子は、選択されたフィールドに指定された値が含まれていることを確認します。within 演算子は、選択されたフィールドに指定された文字列があることを確認します。たとえば、式が Field A within development で、Field A = dev、lop または ment の場合、式は true になりますが、Field A = prod または test の場合は false と評価されます。 ■ [外部ソース。]値は、選択した vRealize Orchestrator アクションの結果に基づきます。 ■ [バインド フィールド。]値は選択したフィールドと同じです。 ■ [計算値。]値は指定したフィールドの値と選択した演算子の結果に基づきます。たとえば、MB 単位のメモリのデフォルト値は、GB 単位のメモリに 1024 を掛けた値に基づきます。

表 3-67. [値] タブのオプション（続き）

オプション	説明
[値のオプション]	<p>ドロップダウン、複数選択、ラジオ グループ、値ピッカー フィールドの値を入力します。</p> <ul style="list-style-type: none"> ■ [定数。]リストの形式は「[値 ラベル,値 ラベル,値 ラベル]」になります。たとえば、2 Small,4 Medium,8 Large のように指定します。 ■ [外部ソース。]値は、選択した vRealize Orchestrator アクションの結果に基づきます。
[ステップ]	<p>整数または 10 進数フィールドの増分値または減少値を定義します。たとえば、デフォルト値が 1 でステップの値を 3 に設定すると、許容される値は 4、7、10 になります。</p>

フィールドの制約

制約プロパティを使用することで、申請ユーザーが申請フォームで有効な値を指定するようにします。

値の有効性は、外部検証を使用することでも確保できる場合があります。[カスタム フォーム デザイナでの外部検証の使用](#)を参照してください。

表 3-68. [制約] タブのオプション

オプション	説明
[必須項目]	<p>申請ユーザーは、このフィールドの値を指定する必要があります。</p> <ul style="list-style-type: none"> ■ [定数。]申請ユーザーによる値の指定を必須にするには、[はい] を選択します。フィールドをオプションにする場合は[いいえ]を選択します。 ■ [条件値。]フィールドが必須かどうかは、真の値になる最初の式によって決定されます。たとえば、別のフィールドでオペレーティングシステム ファミリが Darwin で始まっている場合に、該当フィールドを必須にします。 ■ [外部ソース。]ステータスは、選択した vRealize Orchestrator アクションの結果に基づきます。
[正規表現]	<p>値を検証する正規表現と、検証が失敗したときに表示されるメッセージを指定します。</p> <p>正規表現は、JavaScript 構文に従います。概要については、正規表現の作成を参照してください。詳細なガイダンスについては、構文を参照してください。</p> <ul style="list-style-type: none"> ■ [定数。]正規表現を指定します。たとえば、メールアドレスの場合に、正規表現を <code>^[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,}\$</code> にして、検証エラー メッセージを「メールアドレスの形式が無効です。もう一度やり直してください。」にします。 ■ [条件値。]使用される正規表現は、真の値になる最初の式によって決定されます。

表 3-68. [制約] タブのオプション（続き）

オプション	説明
[最小値]	<p>最小の数値を指定します。たとえば、パスワードは 8 文字以上で指定する必要があります。</p> <p>エラー メッセージを指定します。たとえば、「パスワードは 8 文字以上にする必要があります」とします。</p> <ul style="list-style-type: none"> ■ [定数。]整数を入力します。 ■ [条件値。]最小値は、真の値になる最初の式で決定されます。たとえば、オペレーティング システムが Linux と等しくない場合、CPU の最小値を 4 とします。 ■ [外部ソース。]値は、選択した vRealize Orchestrator アクションの結果に基づきます。
[最大値]	<p>最大の数値です。たとえば、フィールドを 50 文字に制限します。</p> <p>エラー メッセージを指定します。たとえば、「この説明は 50 文字を超えることはできません」とします。</p> <ul style="list-style-type: none"> ■ [定数。]整数を入力します。 ■ [条件値。]最大値は、真の値になる最初の式で決定されます。たとえば、展開場所が AMEA と等しい場合、ストレージの最大値を 2 GB とします。 ■ [外部ソース。]値は、選択した vRealize Orchestrator アクションの結果に基づきます。
[フィールドに一致]	<p>このフィールドの値は、選択したフィールドの値と一致する必要があります。</p> <p>たとえば、[パスワード確認] フィールドは [パスワード] フィールドと一致する必要があります。</p>

カスタム フォーム デザイナでの vRealize Orchestrator アクションの使用

vRealize Automation ブループリントの申請フォームをカスタマイズするときに、vRealize Orchestrator アクションの結果に基づいていくつかのフィールドの動作を設定することができます。

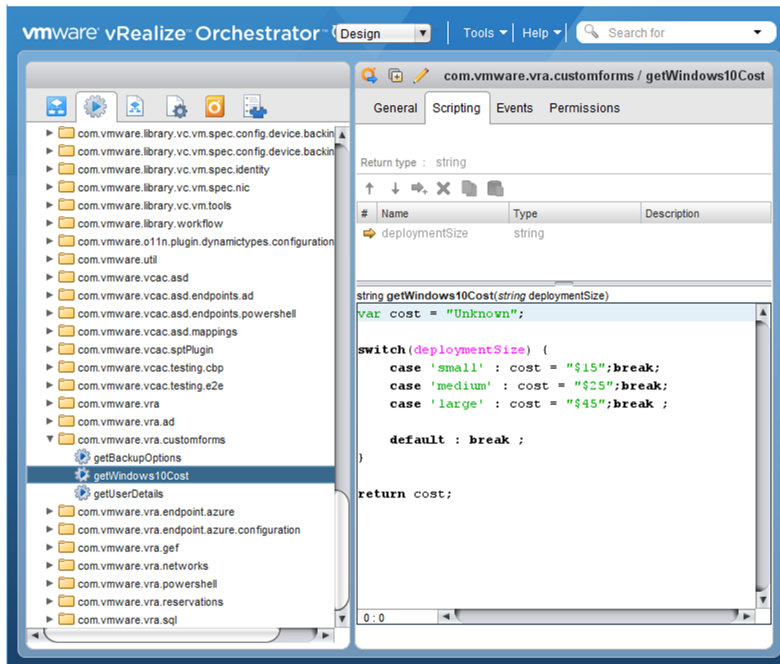
vRealize Orchestrator アクションを使用する方法はいくつかあります。3 番目のソースからデータを取得するアクションや、サイズとコストを定義するスクリプトを使用できます。この例では、スクリプトを使用します。

アクションを使用してフィールドに入力するスクリプトを作成する場合は、Array [Any] タイプを使用しないでください。

例：サイズとコストのフィールドの例

このユース ケースでは、カタログ ユーザーが仮想マシンのサイズを選択したらそのマシンの 1 日あたりのコストを表示できるようにします。この例では、vRealize Orchestrator を使用してサイズとコストを関連付け、ブループリントのカスタム フォームにサイズ フィールドとコスト フィールドを追加します。コスト フィールドに表示される値は、サイズ フィールドによって決まります。

- 1 vRealize Orchestrator で、次の例のような deploymentSize スクリプトを使用して getWindows10Cost アクションを設定します。



スクリプトの例として以下を使用します。

```
var cost = "Unknown";

switch(deploymentSize) {
  case 'small' : cost = "$15";break;
  case 'medium' : cost = "$25";break;
  case 'large' : cost = "$45";break ;

  default : break ;
}

return cost;
```

- 2 vRealize Automation で、サイズ フィールドとコスト フィールドをブループリントのカスタム フォームに追加し、設定します。

サイズ フィールドは、Small、Medium、および Large の値を含む複数選択形式にします。

vRealize Automation で、サイズ フィールドとコスト フィールドをブループリントのカスタム フォームに追加し、設定します。

[値] タブで、次のプロパティ値を設定します。

- デフォルト値 = **Large**
- 値のオプション
 - 値のソース = **Constant**
 - 値の定義 = **small|Small,medium|Medium,large|Large**

- 3 サイズ フィールドで選択された値に基づいて vRealize Orchestrator アクションに定義されているコストを表示するようにコスト フィールドを設定します。

Cost ②
Field ID: cost

Appearance **Values** Constraints

▼ Default value External source

Value source External source ▼

Select action com.vmware.vra.customforms/getWindows10Cost

Action inputs

deploymentSize Field ▼ Size ▼

[値] タブで、次のプロパティ値を設定します。

- デフォルト値 = 外部ソース
- アクションの選択 = <vRealize Orchestrator アクション フォルダ>/getWindows10Cost
- アクションの入力
 - deploymentSize。この値はアクションに設定されています。
 - フィールド
 - サイズ

カスタム フォーム デザイナーでの値ピッカーまたはツリー ピッカー要素の使用

申請フォームをカスタマイズするときは、リストの検索結果からユーザーが選択できる要素を指定するか、ツリーを参照して一致する値を見つけることができます。

値ピッカーとツリー ピッカーは、カスタム フォームの [表示] タブで定義されているリファレンス タイプで動作します。リファレンス タイプは、vRealize Orchestrator リソースです。たとえば、AD:UserGroup または VC:Datastore です。リファレンス タイプを定義することで、ユーザーが検索文字列を入力すると、結果またはツリー オプションは一致するパラメータを持つリソースに制限されます。

値ピッカーの場合、外部ソースを構成することによって可能な値をさらに制限することができます。ツリー ピッカーの場合、外部ソースを構成することによってデフォルト値を指定できます。

値ピッカーの操作

値ピッカーは、検索オプションとしてカタログ形式で表示されます。ユーザーが文字列を入力し、ピッカーが構成された方法に基づいてオプションを提供します。次のユースケースに基づいてピッカーを使用できます。値ピッカーの最も価値のある用途は、外部ソース値とペアリングすることです。

- 定数値のソースを持つ値ピッカー。この方法は、要求しているユーザーが、事前定義された値の静的リストから選択するようにしたい場合に使用します。コンボボックス、ドロップダウン、複数選択、ラジオグループの要素と同様、この方法は定義された定数値およびラベルに基づいて検索結果をリストに表示します。
- 定義された値ソースを持たない値ピッカー。この方法は、要求しているユーザーが、構成されたリファレンスタイプを持つ特定のオブジェクトを vRealize Orchestrator インベントリから検索するようにしたい場合に使用します。たとえば、リファレンスタイプが VC:Datastore で、ユーザーが取得されたリストからデータストアを選択する場合などです。
- 外部の値のソースを持つ値ピッカー。この方法は、要求しているユーザーが vRealize Orchestrator アクションに基づく結果から選択するようにしたい場合に使用します。たとえば、統合データベースから 2 つ以上の値を取得するアクションがあり、ユーザーが取得されたリストから値を選択する場合などです。アクションは、フィルタ `var filter = System.getContext().getParameter("__filter");` を含む必要があります。

ツリー ピッカーの操作

ツリー ピッカーは、検索オプションとしてカタログ形式で表示されます。ユーザーが文字列を入力すると、ツリーピッカーが表示されます。ツリーでは、ユーザーはリファレンスタイプに一致する値を選択できます。たとえば、リファレンスタイプが VC:Datastore の場合、要求しているユーザーはデータストアオブジェクトを選択できます。リファレンスタイプが VC:VirtualMachine の場合、ユーザーは仮想マシンを選択できます。

- 定義された値ソースを持たないツリーピッカー。この方法は、要求しているユーザーが、構成されたリファレンスタイプを持つ特定のオブジェクトを階層ツリーで参照するようにしたい場合に使用します。たとえば、リファレンスタイプが VC:Datastore で、ユーザーが取得されたツリーからデータストアを選択する場合などです。
- 外部の値のソースを持つツリーピッカー。この方法は、ツリー内でデフォルトの選択肢を提供する場合に使用します。要求しているユーザーは、プリセット値を選択するか、異なる値を参照することができます。たとえば、リファレンスタイプ VC:Datastore の場合、ネットワークを指定するアクションの入力値の結果に基づいて、ツリー内のデータストアを特定のデータストアにプリセットすることができます。

カスタム フォーム デザイナーでのデータ グリッド要素の使用

ブループリントの申請フォームをカスタマイズするときは、テーブル形式で情報を追加します。テーブルに含めるデータは、手動で入力することも、外部ソースを使用して入力することもできます。

例：CSV データを入力する例

このユースケースでは、カスタム申請フォームに入力する値のテーブルを用意します。テーブル内の情報を、定数値のソースとして入力します。ソースは CSV データ構造に基づき、最初の行がヘッダーになります。ヘッダーは、列 ID をカンマで区切ります。それ以降の各行は、テーブルの各行に表示されるデータです。

- 1 データグリッドの汎用要素をデザインキャンバスに追加します。
- 2 データグリッドを選択し、プロパティペインで値を定義します。

Data Grid ☺
Field ID: datagrid_0a3999da

Appearance Values

Columns

ADD COLUMN

Label	Username	
Id	username	
Type	String	▼

Label	Employee ID	
Id	employeeId	
Type	Integer	▼

Label	Manager	
Id	manager	
Type	String	▼

Default value Constant

Value source Constant ▼

CSV

```
username,employeeId,manager
leonardo,95621,Farah
vindhya,15496,Farah
martina,52648,Nikolai
```

ラベル	ID	タイプ
ユーザー名	username	文字列
Employee ID	employeeId	Integer
Manager	manager	文字列

CSV 値を定義します。

```
username,employeeId,manager
leonardo,95621,Farah
vindhya,15496,Farah
martina,52648,Nikolai
```

- 3 データ グリッドにブループrintの申請フォームで想定されるデータが表示されていることを確認します。

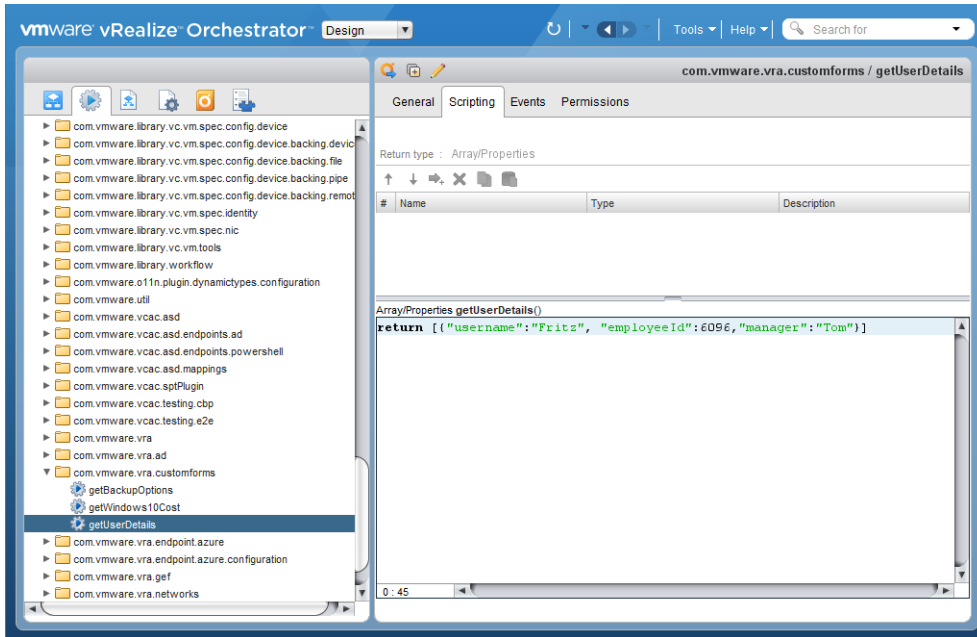
<input type="checkbox"/>	Username ▼	Employee ID ▼	Manager ▼
<input checked="" type="checkbox"/>	leonardo	95621	Farah
<input type="checkbox"/>	vindhya	15496	Farah
<input type="checkbox"/>	martina	52648	Nikolai
<input checked="" type="checkbox"/> 1 1 - 3 / 3			

例：外部ソースの例

この例は前の例を使用していますが、値は vRealize Orchestrator アクションに基づいています。これは単純なアクションの例ですが、ローカル データベースまたはシステムからこの情報を取得する、より複雑なアクションを使用することができます。

検証に使用するアクションには、Array/Properties の入力パラメータが必要です。

- 1 vRealize Orchestrator で、次の例のような配列で `getUserDetails` アクションを設定します。



次のスクリプト例を使用します。

```
return [{\"username\": \"Fritz\", \"employeeId\": 6096, \"manager\": \"Tom\"}]
```

- 2 vRealize Automation で、データ グリッドを追加し、次の値を含むデータ グリッド列を設定します。

ラベル	ID	タイプ
ユーザー名	username	文字列
Employee ID	employeeid	Integer
Manager	manager	文字列

- 3 [値のソース] リストで、[外部ソース] を選択します。
- 4 [アクションの選択] で、「getUserDetails」と入力し、vRealize Orchestrator で作成したアクションを選択します。
- 5 保存して、申請フォームのテーブルを確認します。

<input checked="" type="checkbox"/>	Username	Employee ID	Manager
<input checked="" type="checkbox"/>	Fritz	6096	Tom

カスタム フォーム デザイナでの外部検証の使用

申請時にユーザーが有効な値を指定できるようにするため、フィールドに制約を追加したり、外部検証ソースを使用したりすることで、申請フォームをカスタマイズできます。

最小値、最大値、正規表現、「フィールドに一致」、「空ではない」などのフィールド プロパティは、値の有効性を確保するために制約を使用して設定することができます。[カスタム フォーム デザイナのフィールド プロパティ](#)を参照してください。

外部検証では、vRealize Orchestrator アクションを使用して、外部ソースの有効な値を確認します。

データ グリッド値を検証する場合、検証に使用するアクションには、Array/Properties の入力パラメータが必要です。

外部検証を使用するのは、以下のような場合です。

- 有効な値が外部ソースで定義されている。たとえば、vRealize Orchestrator のように指定します。
- 検証が複数のフィールドに影響する。たとえば、vRealize Orchestrator アクションは、ディスク サイズとストレージ プール容量を収集し、使用可能容量に基づいて指定されたサイズの値を検証します。

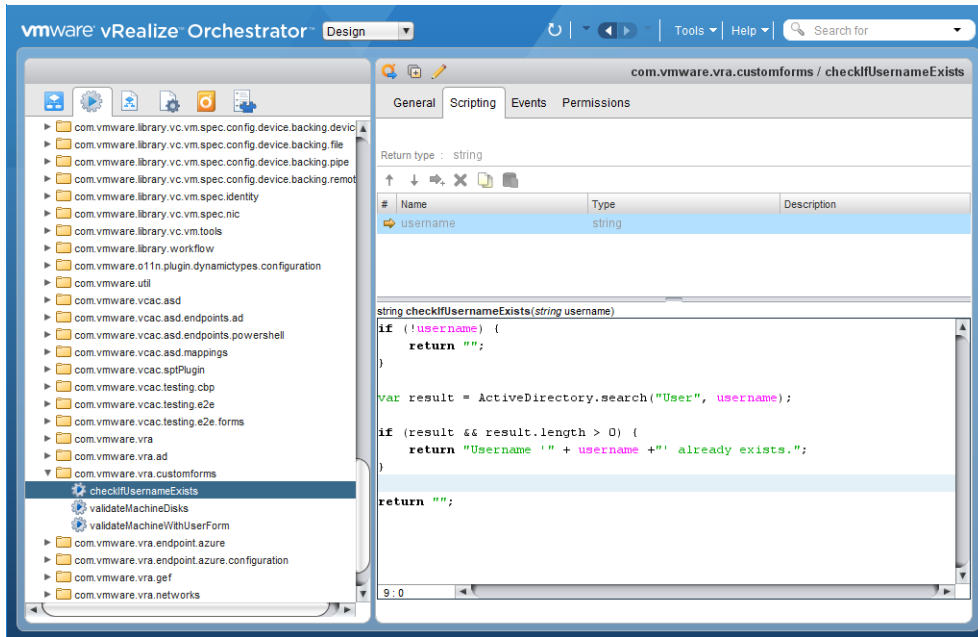
1 つのブループリント内での複数の外部検証の順序が問題になります。検証は、外部検証キャンバスに表示される順序で処理されます。同じフィールドに対する検証が 2 つある場合は、後の検証結果が先の検証結果を上書きします。検証を並べ替えるには、キャンバス上でカードをクリックしてドラッグします。

例：vRealize Orchestrator ユーザーの例

この使用事例では、カタログ ユーザーに新しいユーザー名のみを入力させます。この例を実行するには、フォームで入力されたユーザー名が Active Directory データベースにあるかどうかを確認するアクションを vRealize Orchestrator に設定します。名前があった場合には、申請フォームにエラー メッセージが表示されます。

この使用事例は、[Active Directory オプションを使用したカスタム申請フォームの作成](#)の例に適用されます。

- 1 vRealize Orchestrator で、以下の例のようなスクリプトを使用してアクション `checkIfUsernameExists` を設定します。



スクリプトの例として以下を使用します。この例では、`return` は、検証が失敗した場合に表示されるメッセージです。

```

if (!username) {
    return "";
}

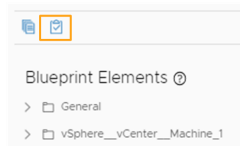
var result = ActiveDirectory.search("User", username);

if (result && result.length > 0) {
    return "Username '" + username + "' already exists.";
}

return "";

```

- 2 vRealize Automation で、ブループリントのカスタム フォーム デザイナを開いて、[外部検証] をクリックして [Orchestrator 検証] タイプをキャンバスにドラッグします。



- 3 外部検証オプションを構成します。

- 検証ラベル = ユーザー名があるかどうかを確認します
- アクションの選択 = <vRealize Orchestrator アクション フォルダ>/checkIfUsernameExists
- アクションの入力
 - ユーザー名 = フィールドとユーザー名
- 強調表示されているフィールド
 - [フィールドの追加] をクリックして、ユーザー名を選択します。

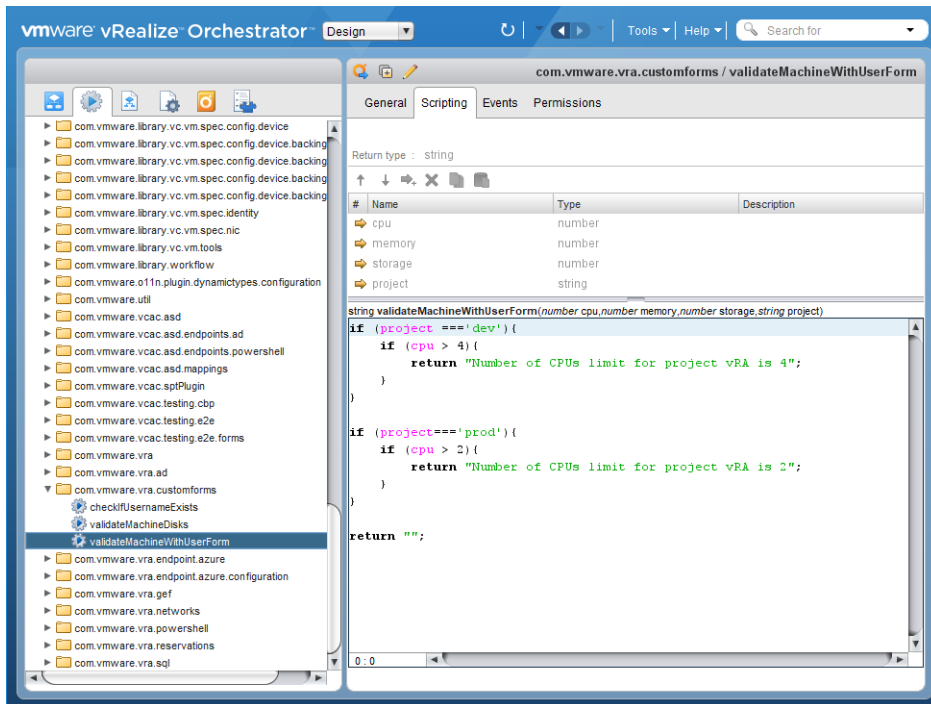
入力した値が検証に失敗した場合、カタログ申請フォームにフィールド レベルの検証エラーが表示されます。グローバル エラーが発生する場合は、強調表示されたフィールドを設定しないでください。

例： vRealize Orchestrator の複数フィールドの例

この使用事例では、CPU、メモリ、ストレージの値を検証をプロジェクトの値に基づいたものにします。たとえば、ユーザーが Dev プロジェクトを選択する場合、CPU の最大数は 4 になります。Prod を選択する場合、最大値は 2 です。

この使用事例では、[Active Directory オプションを使用したカスタム申請フォームの作成](#)の例にプロジェクト フィールドを追加します。プロジェクトを Dev と Prod を値とするドロップダウンとして構成します。

- 1 vRealize Orchestrator で、以下の例のようなスクリプトを使用してアクション `validateMachineWithUserForm` を設定します。



CPUを確認するスクリプトの例としては、以下を使用してください。必要に応じて、スクリプトへのメモリとストレージの値の追加を続行します。この例では、「return」は、検証が失敗した場合に表示されるメッセージです。

```

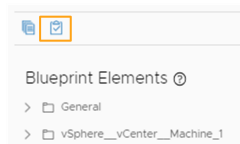
if (project === 'dev'){
    if (cpu > 4){
        return "Number of CPUs limit for project vRA is 4";
    }
}

if (project==='prod'){
    if (cpu > 2){
        return "Number of CPUs limit for project vRA is 2";
    }
}

return "";

```

- 2 vRealize Automation で、ブループリントのカスタム フォーム デザイナを開いて、[外部検証] をクリックして [Orchestrator 検証] タイプをキャンバスにドラッグします。



- 3 外部検証オプションを構成します。

- 検証ラベル = 検証マシンの詳細
- アクションの選択 = <vRealize Orchestrator アクション フォルダ> / validateMachineWithUserForm
- アクションの入力
 - cpu = フィールドと CPU の数
 - メモリ = フィールドとメモリ (GB)
 - ストレージ = フィールドとストレージ (GB)
 - プロジェクト = フィールドとプロジェクト
- 強調表示されているフィールド
 - [フィールドの追加] をクリックして、**プロジェクト** を選択します。

カタログに、次の例のような検証エラーが表示される可能性があります。

失敗したプロビジョニング要求のテストおよびトラブルシューティング

ブループリントのアーキテクトまたは管理者は、作業用のブループリントを確実にユーザーに提供する必要があります。

カタログ申請はさまざまな理由で失敗することがあります。失敗の原因には、ネットワーク トラフィック、エンドポイント リソースの不足、または欠陥のあるブループリントの仕様などが考えられます。または、プロビジョニングの要求は成功しても、展開が機能していないように見えることもあります。ブループリント アーキテクトは、ユーザーが正常に展開できないブループリントを提供しないようにする必要があります。

テスト用のサービスと資格を作成して、ブループリントをカタログから展開することができます。[サービス カatalog 構成用のチェックリスト](#)を参照してください。

リソースが正常にプロビジョニングされない場合は、vRealize Automation を使用して失敗した展開のトラブルシューティングを行うことができます。

失敗の状態

プロビジョニング要求が失敗すると、次のいずれかの状態が表示されます。

- [失敗しました。]要求はいくつかの理由で失敗する可能性があります。1 つは、ターゲットのエンドポイントでリソースが不足している、ブループリントをサポートするための十分なリソースがない、ブループリントが不適切に設計されたために修正が必要である、などが原因でプロビジョニング プロセスが機能しなかった場合です。もう 1 つは、要求が組織内の誰かの承認を必要とし、承認者が要求を拒否した場合です。展開で実行したアクションが失敗した可能性もあります。失敗は、上で述べた環境または承認の理由によって引き起こされる可能性があります。

問題の原因を調査するには、次のトラブルシューティングのワークフローを使用します。問題を解決できる場合は、[破棄] および [再送信] に関するアクションのオプションを確認します。[プロビジョニングされたリソースのアクション メニュー コマンド](#)を参照してください。

- [部分的に成功。]要求は部分的に成功します。つまり、一部のコンポーネントは展開されますが、プロビジョニング手順の一部が正常に完了していません。

次のトラブルシューティングのワークフローを使用して、部分的に成功したコンポーネントを特定し、問題の原因を調査します。問題を解決できる場合は、[破棄] に関するアクションのオプション、および [再開] を使用できるかについて確認します。[プロビジョニングされたリソースのアクション メニュー コマンド](#)および[再開アクションの動作](#)を参照してください。


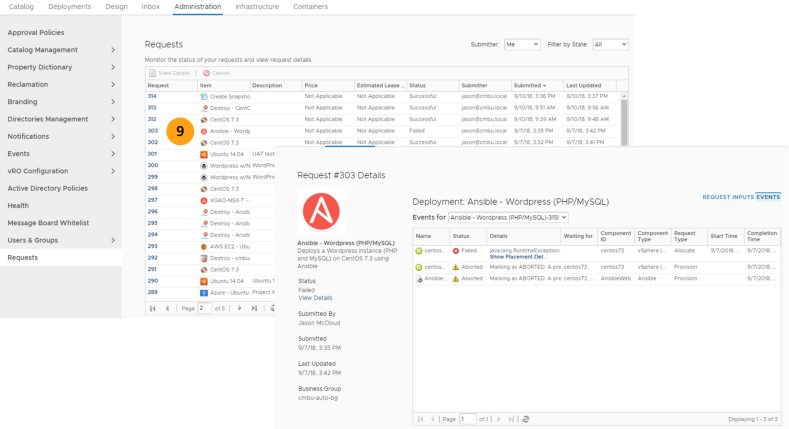
トラブルシューティングのワークフロー

このワークフローを使用して、失敗した展開の調査を開始できます。調査によって失敗の原因が一時的な環境の問題であることが判明した場合は、エラーを解決して要求を再送信することができます。問題が要求の仕様にある場合は、ブループリントを更新して新しい要求を送信できます。

表 3-69. エラーのトラブルシューティングを開始する方法

ワークフロー	トラブルシューティングの手順	例
1	[展開] タブでは、失敗した展開がステータス バーに表示されます。カードには最後の失敗メッセージが含まれています。詳細については、展開名または進行状況バーをクリックしてください。	
2	展開の詳細の [履歴] タブでは、イベント ワークフローを使用してプロビジョニング プロセスが失敗した場所を確認できます。このワークフローは、展開でアクションを実行し、変更が失敗した場合にも役に立ちます。	
3	失敗ステータスはワークフローが失敗した場所を示します。	
4	この情報は、エラー メッセージのより詳細なバージョンを提供します。 signpost のヘルプにあるこの情報では問題を特定して解決するのに不十分な場合は、イベント ログでさらに調査を行うことができます。	
5	次の手順には管理者ロールが必要です。 その他のエラーおよび警告のコンテキストでエラーを見つけるには、[管理] - [イベント] - [イベント ログの表示] を選択します。	
6	詳細検索を使用して、展開の詳細のメッセージに基づいてエラーを見つけることができます。	
7	イベントの詳細を表示するには、[ターゲット ID] リンクをクリックします。	

表 3-69. エラーのトラブルシューティングを開始する方法（続き）

ワークフロー	トラブルシューティングの手順	例
8	イベントの詳細には、トラブルシューティングの作業に役立つ追加のプロビジョニング情報が含まれています。	 <p>The screenshot shows the 'Event Details' page for a failed request. The 'Event description' field contains the error message: 'Exception thrown for last endpoint: https://vmc-iaas01.cmbu.local/WAPV/ - [Error code: 42000] - [Error Msg: Infrastructure service provider error: The list of unallocated IP addresses for the network profile Production Network has been exhausted.]'.</p>
9	管理者は、ユーザーによる他の要求のコンテキストで要求を表示することもできます。 [管理] - [要求] を選択し、要求番号をクリックして、要求の入力とイベントを調べます。	 <p>The screenshot shows the 'Requests' page in the vRealize Automation console. A list of requests is displayed, with request #303 highlighted. The 'Request #303 Details' panel is open, showing the deployment configuration for 'Ansible - Wordpress (PHP/MySQL)' and a table of events. The events table shows a 'Failed' status for the 'Deploy' action.</p>

再開アクションの動作

失敗した展開に対して再開を使用して、特定の状況下で失敗した時点からプロビジョニングプロセスを再開できます。再開アクションは、有効な場合、プロビジョニング申請または該当する操作が失敗したときに使用できます。

プロビジョニング申請に対して再開を使用するには、`_debug_deployment = true` カスタム プロパティをブループリントに追加する必要があります。デフォルトでは、失敗した展開はロールバックされ、クリーンアップされて、リソースが解放されます。`_debug_deployment = true` プロパティを指定すると、失敗した時点の展開が保持され、再開アクションがサポートされている場合は、その動作に基づいて、再開アクションを実行できます。サポートされている操作に対してのみ再開を使用する場合は、`_debug_deployment` プロパティを有効にする必要はありません。

`_debug_deployment` の詳細については、「カスタム プロパティのリファレンス」を参照してください。

プロビジョニング申請またはサポートされているアクションに対して再開を使用するには、ユーザーに再開アクションを実行する資格を付与します。[ユーザーにサービス、カタログ アイテム、アクションの使用資格を付与](#)を参照してください。

次のプロビジョニング アクティビティの再開アクションを実行する資格をユーザーに付与できます。

- プロビジョニング申請
- 再開アクション
- スケール イン アクション
- スケール アウト アクション

■ 破棄アクション

再開アクションの制約

ブループリントの新しいインスタンスを申請せずに再開を使用できるかどうかを判断する際は、制約を考慮してください。

- ブループリントは申請した時点で変更できなくなります。

申請時に、ブループリントの変更不可能なバージョンがカタログ申請に関連付けられます。この固定バージョンには、属性、カスタム プロパティ、設定など、プロビジョニングの開始時点の仕様がすべて含まれています。失敗の原因となるエラーがブループリントにある場合に、そのエラーを修正し、再開を使用しても失敗します。申請に関連付けられているバージョンが参照されるためです。この場合は、新しいインスタンスをプロビジョニングする必要があります。

例

- ブループリント A で 5 GB の RAM を要求したが、3 GB しか予約されていないため、申請が失敗しました。3 GB のみを要求するようにブループリントを更新してから再開を実行しても、再開アクションは失敗します。再開を実行すると、元の申請がチェックされ、以前と同様に 5 GB を要求します。ただし、ビジネス グループのシステム予約を 5 GB に増やしてから再開を実行すると、再開アクションは成功します。
- ゲスト カスタム仕様が含まれているブループリント B を申請したら、失敗しました。調査したところ、vCenter Server インスタンスでゲスト カスタム仕様の名前が変更されていたことがわかりました。新しい名前でブループリントを更新してから再開を実行しても、失敗します。ブループリントを更新しても、再開アクションでは元のバージョンが使用されるためです。新しい名前を今後使用する場合は、再開を使用せずに、ブループリントの新しいインスタンスを展開します。または、vCenter Server インスタンスでゲスト カスタム仕様の名前を元のバージョンで想定されている名前に変更してから、再開を実行する必要があります。次のプロビジョニング申請が失敗しないようにするには、忘れずに正しいゲスト カスタム仕様を使用してブループリントを更新してください。

申請時のブループリントの仕様をサポートするようにターゲットの展開環境を更新できる場合、再開は機能します。

- 失敗した時点からのみ再試行されます。

再開アクションでは、失敗した時点からコンポーネントのタスクを再試行します。プロビジョニング申請全体を再送信することはありません。

例

- ブループリント C では、アプリケーション仮想マシンとデータベース仮想マシンを作成します。データベース仮想マシンは正常に展開されましたが、アプリケーション仮想マシンのプロビジョニングが失敗しました。再開アクションを実行した場合、アプリケーション仮想マシンのプロビジョニングのみが再試行されます。

失敗とマークされたコンポーネントは、実行されなかったものとして処理されます。スクリプト エラーなどが原因で、データベース仮想マシンの構成段階でインストールが失敗したが、データベースは影響を受けていない場合、再開アクションでスクリプトが実行されても、そのデータベースは保持されます。構成スクリプトが含まれているインストール スクリプトは再度実行されず、再開は成功しません。スクリプトを修正し、新しいインスタンスをプロビジョニングする必要があります。

- 他に考慮が必要なのは、手順の割り当てが成功したものの、プロビジョニングに失敗した場合です。この例では、再開すると、プロビジョニングに失敗した時点から再試行され、再開された申請では古い割り当て情報を処理するため、再開が失敗します。

破棄要求が失敗した後の展開環境の強制破棄

破棄要求の失敗により、本来の状況とは異なる展開環境を強制破棄できます。

展開の破棄操作中に vRealize Automation が展開リソースの破棄に失敗すると、残りの展開リソースが破棄されずに、破棄操作が即座に停止します。この失敗により、本来の状況とは異なる展開環境が残り、展開を破棄する明確な方法がなく、リソースを使い続けます。ビジネス グループ管理者は、このような状態で残っている展開を強制破棄できます。

前提条件

- [ビジネス グループ管理者] として vRealize Automation にログインしていることを確認します。
- 強制破棄アクションを実行する前に、[プロビジョニングされたリソースのアクション メニュー コマンド](#)で破棄アクションの詳細を確認します。

手順

- 1 [展開] タブで、破棄する展開を見つけます。
- 2 [アクション] をクリックし、[破棄] をクリックします。
- 3 説明を入力し、申請の理由を入力します。
- 4 [強制破棄] を選択し、[送信] をクリックします。

結果

vRealize Automation が、展開環境内のすべてのリソースを含む完全な破棄を試行します。vRealize Automation が展開リソースを破棄できない場合は、そのリソースをスキップして、展開内の残りのリソースの破棄を続行します。

次のステップ

展開内のすべてのリソースが正常に破棄されたことを確認します。強制破棄の操作中に破棄されなかったすべてのリソースを、手動で破棄する必要があります。次回のプロビジョニング処理時に vRealize Automation がホスト名や IP アドレスなどの設定の詳細を再利用する可能性があるため、プロビジョニングしたすべての仮想マシン オブジェクトが破棄されていることを確認します。

vRealize Orchestrator ワークフローが含まれている、失敗した展開のトラブルシューティング

失敗したブループリント展開に vRealize Orchestrator ワークフローが含まれている場合、トークン ID を使用してワークフローでの問題をトラブルシューティングできます。vRealize Orchestrator 内でログを検索するには、トークン ID を使用します。

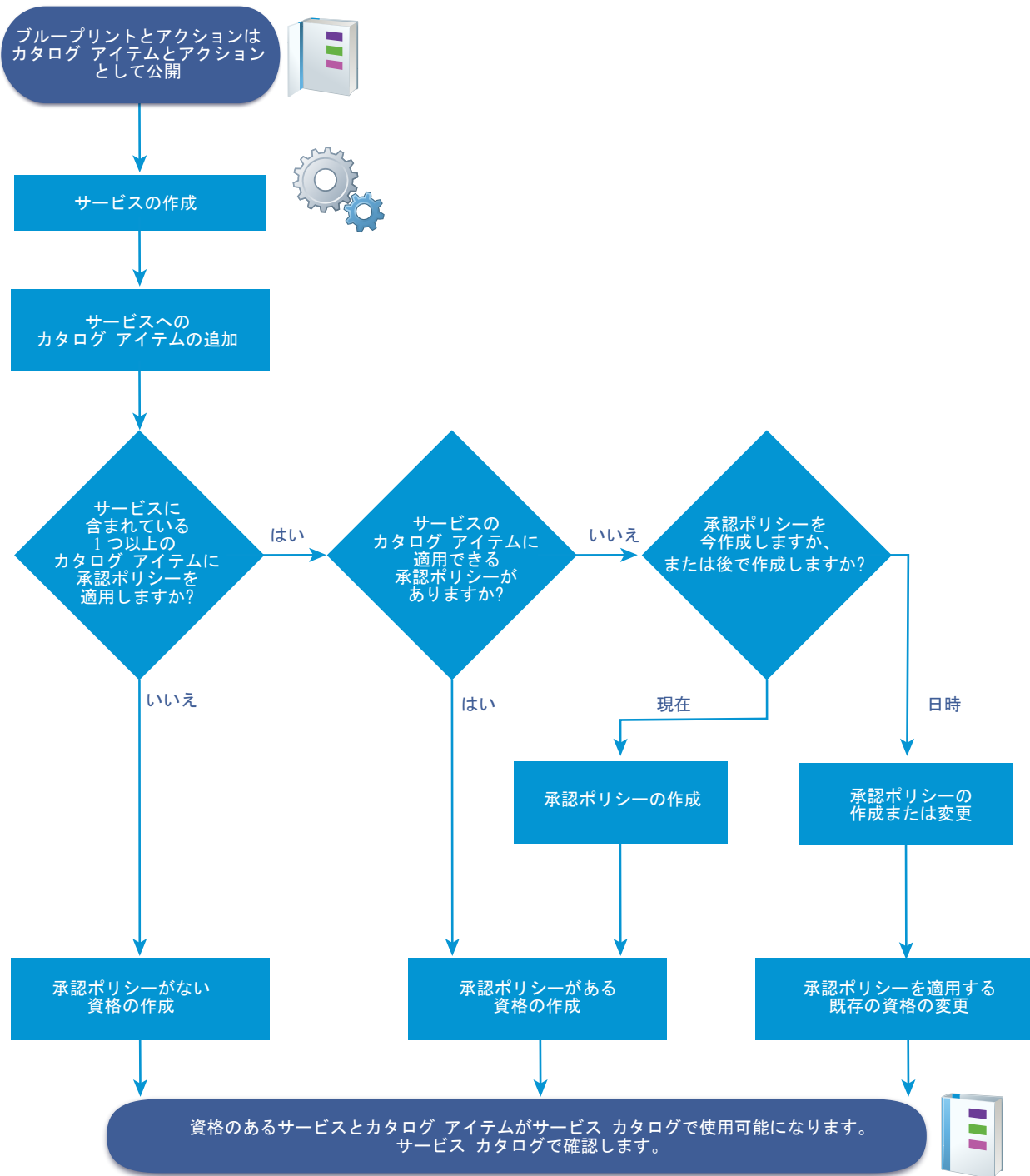
解決方法

- 1 失敗したワークフローのトークン ID を見つけます。
 - a vRealize Automation で、[展開] タブをクリックし、展開またはアクションを見つけてます。
 - b 展開名をクリックします。
申請は、展開またはアクションです。
 - c [履歴] タブ、[要求の入力] タブの順にクリックします。
ブループリントが vRealize Orchestrator ワークフローに基づいている場合、ページのタイトルは [vRealize Orchestrator ワークフロー実行の詳細] です。
 - d トークン ID を見つけて、テキスト ファイルまたはクリップボードにコピーします。
たとえば、ff8080815a685352015a6c8d450801ee です。
- 2 コントロール センターを使用して、vRealize Orchestrator 内のワークフロー ログを見つけてます
 - a ブラウザの検索ボックスに vRealize Automation のベース URL を入力します。
[VMwarevRealize Automation Appliance] ページが表示されます。
 - b [vRealize Orchestrator コントロール センター] をクリックします。
 - c root 権限を持つユーザーとしてログインします。
 - d [ワークフローの確認] をクリックします。
 - e [終了したワークフロー] をクリックします。
 - f [トークン ID] テキスト ボックスにワークフロー トークンを貼り付けます。
トークン ID に一致するワークフローにリストが表示されます。
 - g 行をクリックし、ログで障害の原因を確認します。

サービス カタログの管理

顧客は、サービス カタログにおいて、自分で使用するためにプロビジョニングするマシンとその他のアイテムを申請します。サービスの構築方法、1 つ以上のアイテムに対するユーザーへの資格付与の方法、およびガバナンスの適用方法に基づいて、サービス カタログ アイテムへのユーザー アクセスを管理します。

サービス カタログに対してアイテムを追加するために従うワークフローは、承認ポリシーを作成および適用するかどうかにによって異なります。



サービス カatalog構成用のチェックリスト

ブループリントとアクションを作成して公開したら、vRealize Automation サービスの作成、カタログ アイテムの構成、および資格と承認の割り当てを行うことができます。

サービス カatalog構成のチェックリストには、カatalogを構成するために必要な手順の概要と、各手順の判断ポイントまたは詳細な指示へのリンクがあります。

表 3-70. サービス カタログ チェックリストの構成

タスク	必要なロール	詳細
<input type="checkbox"/> サービスを追加する。	テナント管理者または カタログ管理者	サービスの追加 を参照してください。
<input type="checkbox"/> サービスにカタログ アイテムを追加する。	テナント管理者または カタログ管理者	サービスへのカタログ アイテムの追加 を参照してください。
<input type="checkbox"/> サービスのカタログ アイテムを構成する。	テナント管理者または カタログ管理者	カタログ アイテムの設定 を参照してください。
<input type="checkbox"/> 資格を作成し、カタログ アイテムに適用する。	テナント管理者または ビジネス グループ マネージャ	ユーザーにサービス、カタログ アイテム、アクションの使用資格を付与 を参照してください。
<input type="checkbox"/> 承認ポリシーを作成し、カタログ アイテムに適用する。	テナント管理者または承認管理者は、承認ポリシーを作成できません。 テナント管理者またはビジネス グループ管理者は、承認ポリシーを適用できます。	承認ポリシーの作成 を参照してください。

サービスの作成

サービスは、サービス カタログに含まれるカタログ アイテムのグループです。関連するすべてのカタログ アイテムの使用資格をビジネス グループ ユーザーに付与してサービスを使用可能にしたり、承認ポリシーをサービスに適用したりできます。

サービスは、カタログ アイテムの動的グループとして機能します。サービスを使用可能にすると、サービスに関連付けられたすべてのカタログ アイテムは、サービス カタログ内で指定ユーザーが利用できるようになります。またサービスに追加した、あるいはサービスから削除したカタログ アイテムはサービス カタログに反映されます。

サービスを作成すると、そのサービスをサービス カテゴリとして使用できるため、サービス カタログ ユーザーに応じて提供するサービスをまとめることができます。たとえば、Windows 7、8、10 オペレーティング システムのカタログ アイテムを含む Windows デスクトップ サービスや、CentOS および RHEL オペレーティング システムのアイテムを含む Linux サービスなどです。

サービスの追加

サービス カタログ ユーザーがカタログ アイテムを使用できるようにするためにサービスを追加します。ユーザーにアイテムの使用資格を付与するには、カタログ アイテムをサービスに関連付ける必要があります。

ユーザーにサービスの使用資格が付与されると、カタログ アイテムがサービス カタログ内に一緒に表示されます。個々のカタログ アイテムについてユーザーに使用資格を付与することもできます。

前提条件

テナント管理者またはカタログ管理者として vRealize Automation にログインします。

手順

1 [管理] - [カタログ管理] - [サービス] を選択します。

2 [新規] アイコン（）をクリックします。

3 名前と説明を入力します。

これらの値は、カタログ ユーザーのサービス カタログに表示されます。

4 サービス固有のアイコンをサービス カタログ内に追加するには、[参照] をクリックして画像を選択します。

サポートされている画像ファイルの種類は、GIF、JPG、および PNG です。表示される画像のサイズは 40 x 40 ピクセルです。カスタムの画像を選択しない場合、サービス カタログにはデフォルトのアイコンが表示されます。

5 [ステータス] ドロップダウン メニューからステータスを選択します。

オプション	説明
無効	サービス カタログでサービスを利用できません。サービスがこの状態の場合、サービスにカタログ アイテムを関連付けることはできませんが、ユーザーにサービスの使用資格を付与することはできません。有効かつ使用資格のあるサービスに対して [無効] を選択すると、そのサービスは、再アクティブ化するまでサービス カタログから削除されます。
有効	(デフォルト) サービスおよび関連付けられたカタログ アイテムの使用資格をユーザーに付与することができ、資格が付与されると、ユーザーはそれらをサービス カタログで使用できます。
削除済み	vRealize Automation からサービスを削除します。サービスに関連付けられたカタログ アイテムはすべて存在したままですが、カタログ ユーザーはサービス カタログ内のサービスに関連付けられたアイテムはいずれも使用できません。

6 サービス設定を構成します。

次の設定により、サービス カタログ ユーザーに情報が提供されます。この設定によって、サービスの可用性が影響を受けることはありません。

オプション	説明
時間	サポート チームが対応可能な時刻を構成します。時間はユーザーの現地時刻に基づきます。サービス時間を複数の日付にまたがって指定することはできません。たとえば、サービス時間を午後 4:00 から午前 4:00 のように設定することはできません。深夜 0 時をまたぐ場合は、2 つの資格を作成します。1 つの資格は 午後 4:00 から午前 12:00 までとし、もう 1 つは午前 12:00 から午前 4:00 とします。
所有者	サービスおよび関連付けられたカタログ アイテムのプライマリ所有者であるユーザーまたはユーザー グループを指定します。
サポート チーム	サービス カタログ ユーザーがサービスを使用してアイテムをプロビジョニングするときに発生した問題のサポートを担当するカスタムのユーザー グループまたはユーザーを指定します。
処理時間帯の変更	サービスを変更する日付と時間を選択します。指定した日付と時間は情報として提供されるもので、サービスの可用性に影響を与えることはありません。

7 [追加] をクリックします。

次のステップ

カタログ アイテムをサービスに関連付けて、ユーザーにアイテムの資格を付与できるようにします。 [サービスへのカタログ アイテムの追加](#)を参照してください。


サービスへのカタログ アイテムの追加

カタログ アイテムをサービスに追加して、ユーザーにサービス カatalog内のアイテムを申請する資格を付与できるようにします。1つのカタログ アイテムには、1のサービスのみ関連付けることができます。

前提条件

- テナント管理者またはカタログ管理者として vRealize Automation にログインします。
- サービスが存在していることを確認します。 [サービスの追加](#)を参照してください。
- 1つ以上のカタログ アイテムが公開されていることを確認します。 [カタログ アイテムの設定](#)を参照してください。

手順

- 1 [管理] - [カタログ管理] - [サービス] を選択します。
- 2 カatalog アイテムの追加先のサービスを選択して、[カタログ アイテムの管理] をクリックします。
- 3 [カタログ アイテム] アイコン () をクリックします。
 - a サービスに含めるカタログ アイテムを選択します。

[カタログ アイテムの選択] ダイアログ ボックスに、サービスにまだ関連付けられていないアイテムのみが表示されます。
 - b [追加] をクリックします。
- 4 [閉じる] をクリックします。

次のステップ

- カatalog アイテムにカスタムのアイコンを追加できます。追加したアイコンは、サービス カatalogでアイテムといっしょに表示されます。 [カタログ アイテムの設定](#)を参照してください。
- サービスまたはカタログ アイテムの使用資格をユーザーに付与して、ユーザーが、サービス カatalog内のサービスまたはカタログ アイテムを申請できるようにします。 [資格の作成](#)を参照してください。

カタログ アイテムとアクションでの作業

カタログ アイテムは、マシン、ソフトウェア コンポーネント、およびその他のオブジェクトの公開済みのブループリントです。カタログ管理領域内のアクションは公開済みのアクションであり、プロビジョニングされたカタログ アイテムで実行できます。リストを使用して、公開されるブループリントとアクションを決定し、サービス カatalog ユーザーがそのブループリントとアクションを使用できるようにすることができます。

公開済みカタログ アイテム

カタログ アイテムは公開済みブループリントです。公開済みブループリントは、他のブループリントでも使用できます。他のブループリントで再利用されたブループリントは、カタログ アイテム リストに表示されません。

公開済みのカタログ アイテムには、ブループリントのコンポーネントのみのアイテムも含めることができます。たとえば、公開済みのソフトウェア コンポーネントはカタログ アイテムとしてリストされますが、展開の一部としてのみ使用できます。

使用資格が付与されたユーザーがサービス カタログでカタログ アイテムを使用できるようにするためには、展開カタログ アイテムをサービスに関連付ける必要があります。アクティブなアイテムだけが、サービス カタログに表示されます。別のサービス向けのカタログ アイテムを構成したり、サービスをサービス カタログから一時的に削除する場合に無効にしたり、カタログに表示されるカスタム アイコンを追加したりできます。

公開済みアクション

アクションは、プロビジョニングされたカタログ アイテムに加えることができる変更です。たとえば、仮想マシンを再起動できます。

アクションには、組み込みアクション、または XaaS を使用して作成されたアクションを含めることができます。マシンまたは他の指定されたブループリントを追加するときに、組み込みアクションが追加されます。XaaS アクションは、作成して公開する必要があります。

アクションはサービスと関連付けられません。アクションは、アクションが実行されるカタログ アイテムを含む使用資格に含める必要があります。ユーザーが使用資格を持つアクションは、サービス カタログに表示されません。アクションがアイテムとアイテムの現在の状態に適用可能かどうかに基づいて、サービス カタログ ユーザーの [展開] タブにあるプロビジョニングされたアイテムでアクションが使用できるようになります。

[展開] タブに表示されるアクションに、カスタム アイコンを追加できます。

カタログ アイテムの設定

カタログ アイテムは、ユーザーに使用資格を付与できる公開済みのブループリントです。ステータスや関連付けられているサービスを変更するには、カタログ アイテム オプションを使用します。選択したカタログ アイテムを含む使用資格を表示することもできます。

サービス カタログには、サービスに関連付けられ、ユーザーに使用資格が付与されているカタログ アイテムだけが表示されます。カタログ アイテムに関連付けることができるサービスは 1 つだけです。

資格や公開済みカタログ アイテム リストから特定のカタログ アイテムを削除せずに、サービス カタログに表示しないようにするには、そのアイテムを無効化してください。無効な状態のカタログ アイテムは、グリッドでの使用が中止され、設定の詳細情報でも無効となります。これは後から有効にできます。

前提条件

- テナント管理者またはカタログ管理者として vRealize Automation にログインします。
- カatalog アイテムとして公開された 1 つ以上のブループリントがあることを確認します。[ブループリントの公開](#)を参照してください。

手順

- 1 [管理] - [カタログ管理] - [カタログ アイテム] を選択します。
- 2 カatalog アイテムを選択し、[構成] をクリックします。

3 カタログ アイテムを設定します。

オプション	説明
アイコン	画像を参照します。サポートされている画像ファイルの種類は、GIF、JPG、および PNG です。表示される画像のサイズは 40 x 40 ピクセルです。カスタムの画像を選択しない場合、サービス カタログにはデフォルトのカタログ アイコンが表示されます。
ステータス	<p>[有効]、[無効]、[ステージング] の値があります。</p> <ul style="list-style-type: none"> ■ [有効]。カタログ アイテムはサービス カタログに表示されており、使用資格を付与されたユーザーはこれを使用してリソースをプロビジョニングできます。アイテムは公開済みとしてカタログ アイテム リストに表示されます。 ■ [無効]。カタログ アイテムはサービス カタログで利用できません。アイテムは使用中としてカタログ アイテム リストに表示されます。 ■ [ステージング]。カタログ アイテムはサービス カタログで利用できません。ステージング メニューは、無効になっているアイテムを再度有効にする可能性がある場合、これを使用するために使用します。ステージングとしてカタログ アイテム リストに表示されます。
割り当て	<p>このカタログ アイテムのインスタンスをユーザーが展開できる数を設定します。</p> <p>この数を超えると、カタログ申請に通知が表示され、申請は送信されません。</p>
サービス	サービスを選択します。使用資格が付与されたユーザーのサービス カタログに表示させる場合は、すべてのカタログ アイテムをサービスに関連付ける必要があります。リストには、有効と無効のサービスが含まれます。

4 ユーザーがカタログ アイテムを使用できるようになる資格を表示するには、[資格] タブをクリックします。

5 [アップデート] をクリックします。

次のステップ

- カatalog アイテムをサービス カタログで使えるようにするには、アイテムに関連付けられたサービスまたは個々のアイテムに対する資格をユーザーに付与する必要があります。[資格の作成](#)を参照してください。
- 個々のユーザーの承認ポリシーが正しく適用されるように資格処理の順序を指定するには、同一ビジネス グループの複数の資格に対して優先順位を設定します。[資格の優先順位付け](#)を参照してください。

サービス カタログのアクションの構成

アクションとは、プロビジョニングされたアイテムで実行可能な変更またはワークフローのことです。アイコンを追加したり、選択したアクションを含む資格を表示したりできます。

アクションは、プロビジョニングされたマシン、ネットワーク、およびその他のブループリント コンポーネントに対する組み込みのアクションか、公開済みの XaaS アクションのいずれかです。

アイコンに使用できる画像ファイルの種類は、GIF、JPG、PNG です。表示される画像のサイズは 40 x 40 ピクセルです。カスタムの画像を選択しない場合、[展開] タブにはデフォルトのアクション アイコンが表示されます。

前提条件

- テナント管理者またはカタログ管理者として vRealize Automation にログインします。
- 公開された 1 つ以上のアクションがあることを確認します。[ブループリントの公開](#)および[リソース アクションの公開](#)を参照してください。

手順

- 1 [管理] - [カタログ管理] - [アクション] を選択します。
- 2 共有アクションを選択し、[詳細の表示] をクリックするか、XaaS アクションの場合は [構成] をクリックします。
- 3 画像を参照します。
- 4 ユーザーによるアクションが使用可能となる資格を表示するには、[資格] タブをクリックします。
- 5 [完了] をクリックします。

次のステップ

[ユーザーにサービス、カタログ アイテム、アクションの使用資格を付与。](#)

資格の作成

資格では、選択されたビジネス グループのメンバー用のサービス カatalogで利用できるアイテムとアクションを管理します。アイテムをサービス カatalogに表示するには、資格が有効でなければなりません。ガバナンスを必要とするアイテムがある場合は、資格を使用して、さまざまなアイテムに承認ポリシーを適用できます。

資格を設定するには、カタログ アイテムがサービスに含まれている必要があります。資格には、複数のサービス、他の資格に含まれるサービスのカタログ アイテム、展開したカタログ アイテムに対して実行するアクションを含めることができます。

資格オプションの相互作用について

資格の設定方法によって、サービス カatalogに表示されるアイテムが決まります。サービス カatalog ユーザーが申請できる内容や承認ポリシーの適用方法は、サービス、カタログ アイテムおよびコンポーネント、アクション、および承認ポリシーの相互作用の影響を受けます。

資格を作成するときは、サービス、カタログ アイテム、アクション、および承認の相互作用を考慮する必要があります。

■ 資格におけるサービス

使用可能なサービスは、カタログ アイテムの動的グループとして機能します。サービスの使用資格が付与された後、そのサービスにカタログ アイテムが追加された場合、新たに設定を行わなくても、指定されたユーザーはその新しいカタログ アイテムを使用できます。

■ 資格におけるカタログ アイテムとコンポーネント

資格が付与されたカタログ アイテムは、サービス カatalog内で申請できるブループリントです。資格が付与されたコンポーネントはブループリントの一部ですが、サービス カatalog内で明確に申請することはできません。

■ 資格におけるアクション

アクションは、展開されたカタログ アイテムで実行されます。プロビジョニングされたカタログ アイテム、およびそれらのアイテムで実行する資格が与えられたアクションは、[展開] タブに表示されます。展開されたアイテムでアクションを実行するには、サービス カatalogからアイテムをプロビジョニングしたカタログ アイテムと同一の資格に、そのアクションが含まれている必要があります。

■ 資格における承認ポリシー

承認ポリシーは、環境内のリソースを管理できるように、資格内で適用されます。

資格におけるサービス

使用可能なサービスは、カタログ アイテムの動的グループとして機能します。サービスの使用資格が付与された後、そのサービスにカタログ アイテムが追加された場合、新たに設定を行わなくても、指定されたユーザーはその新しいカタログ アイテムを使用できます。

サービスに承認ポリシーを適用すると、すべてのアイテムが申請時に同じ承認ポリシーの対象になります。

資格におけるカタログ アイテムとコンポーネント

資格が付与されたカタログ アイテムは、サービス カatalog内で申請できるブループリントです。資格が付与されたコンポーネントはブループリントの一部ですが、サービス カatalog内で明確に申請することはできません。

資格が付与されたカタログ アイテムおよびコンポーネントには、次のようなアイテムを含めることができます。

カタログ アイテム

- 資格のあるユーザーに提供するサービスのアイテム（現在の資格に含まれていないサービスでも可能）。

たとえばカタログ管理者は、さまざまな異なるバージョンの Red Hat Enterprise Linux (RHEL) を Red Hat サービスと関連付けて、製品 A の品質管理技術者にそのサービスの使用資格を付与したとします。その後カタログ管理者は、トレーニング チーム用に、Linux ベースのオペレーティング システムの最新バージョンのみが含まれるサービス カatalog アイテムの作成申請を受け取りました。カタログ管理者は、サービスに他のオペレーティング システムの最新バージョンを含んだトレーニング チーム用の資格を作成します。カタログ管理者は、最新バージョンの RHEL を既に別のサービスに関連付けているため、Red Hat サービス全体を追加するのではなく、RHEL をカタログ アイテムとして追加します。

- 現在の資格に含まれるサービス内のアイテム。ただし、サービスに適用したポリシーとは異なる承認ポリシーを個々のカタログ アイテムに適用できます。

たとえばビジネス グループ マネージャは、開発チームに、3 つの仮想マシン カatalog アイテムを含むサービスの使用資格を付与したとします。ビジネス グループ マネージャは、5 つ以上の CPU を含むマシンに対して、仮想インフラストラクチャ管理者の承認が必要な承認ポリシーを適用します。仮想マシンの 1 台はパフォーマンス テストに使用されるため、それをカタログ アイテムとして追加し、同じユーザー グループに対して制約の少ない承認ポリシーを適用します。

コンポーネント

- コンポーネントはカタログ アイテムの一部であるため、サービス カatalog内では名前で利用できません。これらのコンポーネントに個別に資格を付与して、コンポーネントが含まれるカタログ アイテムとは異なる特定の承認ポリシーを適用できます。

たとえば、アイテムにマシンとソフトウェアが含まれているとします。マシンはプロビジョニング可能なアイテムとして利用でき、サイト マネージャの承認を必要とする承認ポリシーが適用されています。ソフトウェアは、スタンドアロンのプロビジョニング可能なアイテムとして利用できず、マシン申請の一部としてのみ利用できます。しかしソフトウェアの承認ポリシーでは、組織のソフトウェア ライセンス管理者の承認が必要です。マシンがサービス カatalogで申請されると、マシンは、サイト管理者とソフトウェア ライセンス管理者から承認されなければ、プロビジョニングされません。プロビジョニングされたマシンは、ソフトウェア エントリとともに、マシンの一部として、申請者の [展開] タブに表示されます。

資格におけるアクション

アクションは、展開されたカタログ アイテムで実行されます。プロビジョニングされたカタログ アイテム、およびそれらのアイテムで実行する資格が与えられたアクションは、[展開] タブに表示されます。展開されたアイテムでアクションを実行するには、サービス カタログからアイテムをプロビジョニングしたカタログ アイテムと同一の資格に、そのアクションが含まれている必要があります。

たとえば、資格 1 には vSphere 仮想マシンとスナップショット作成アクションが含まれ、資格 2 には vSphere 仮想マシンのみが含まれているとします。資格 1 から vSphere マシンを展開するとき、スナップショット作成アクションを利用できます。資格 2 から vSphere マシンを展開するときは、アクションはありません。資格 2 ユーザーがアクションを利用できるようにするには、スナップショット作成アクションを資格 2 に追加します。

資格内のカタログ アイテムに適用できないアクションを選択した場合、そのアクションは [展開] タブにアクションとして表示されません。たとえば、資格に vSphere マシンが含まれ、クラウド マシンで破棄アクションを使用可能にした場合、破棄アクションは、プロビジョニングされたマシンで実行できません。

資格内のカタログ アイテムに適用されたポリシーと異なる承認ポリシーを、アクションに適用できます。

サービス カタログ ユーザーが複数のビジネス グループのメンバーであり、パワーオンとパワーオフを実行できるのが 1 つのグループのみで、他のグループは破棄のみを実行できる場合、このユーザーは、該当するプロビジョニングされたマシンでこれらのビジネス グループに対して 3 つすべてのアクションを使用可能にできます。

ユーザーへのアクションの使用資格付与時のベスト プラクティス

ブループリントは複雑であり、プロビジョニングされたブループリント上でアクションを実行すると、予期しない動作を招く場合があります。サービス カタログ ユーザーがプロビジョニングされたアイテム上でアクションを実行する場合は、次のベスト プラクティスを使用します。

- ユーザーに [マシンの破棄] アクションの使用資格を付与する場合は、[展開の破棄] の使用資格をユーザーに付与します。プロビジョニングされたブループリントとは展開のことです。

展開にはマシンを含めることができます。サービス カタログ ユーザーに [マシンの破棄] アクションを実行する資格が付与されているが、[展開の破棄] を実行する資格が付与されていない場合、サービス カタログ ユーザーが展開内の最後または唯一のマシン上で [マシンの破棄] アクションを実行すると、このアクションを実行する権限がないことを知らせるメッセージが表示されます。両方のアクションの使用資格を付与するには、展開が使用環境から削除されていることを確認します。[展開の破棄] アクションのガバナンスを管理するには、事前承認ポリシーを作成し、アクションにこのポリシーを割り当てます。このポリシーにより、指定された承認者は、申請を実行する前に、展開の破棄申請を検証できるようになります。

- [リースの変更]、[所有者を変更]、[有効期限]、[再構成]、およびマシンや展開に適用できるその他のアクションの使用資格をサービス カタログ ユーザーに付与する場合、ユーザーに両方のアクションの使用資格を付与します。

資格における承認ポリシー

承認ポリシーは、環境内のリソースを管理できるように、資格内で適用されます。

資格を作成するときに承認ポリシーを適用するには、ポリシーが既に存在している必要があります。存在しない場合は、資格を作成して、この資格内のカタログ アイテムとアクションで必要となる承認ポリシーを作成するまで、資格をドラフトまたは無効状態にしておき、後からポリシーを適用します。

アイテムまたはアクションに、承認ポリシーを適用する必要はありません。承認ポリシーが適用されていない場合は、承認申請をトリガしなくても、申請があればアイテムとアクションが展開されます。

ユーザーにサービス、カタログ アイテム、アクションの使用資格を付与

サービス、カタログ アイテム、またはアクションを資格に追加すると、その資格で識別されるユーザーは、サービス カatalogのプロビジョニング可能なアイテムを申請できます。アクションはアイテムに関連付けられ、申請元ユーザーの [展開] タブに表示されます。

次に示すユーザー ロールには、ビジネス グループの資格作成許可が与えられています。

- テナント管理者は、自身のテナント内のどのビジネス グループの資格も作成することができます。
- ビジネス グループ マネージャは、自身が管理するグループの資格を作成できます。
- カatalog管理者は、自身のテナント内のすべてのビジネス グループの資格を作成できます。


資格を作成する場合は、資格を付与する対象のビジネス グループとビジネス グループ内のメンバーを選択する必要があります。

資格を作成してサービス、カタログ アイテム、および承認を含むアクションの相互作用を使用できるようにする方法については、[資格の作成](#)を参照してください。

前提条件

- テナント管理者またはカatalog管理者として vRealize Automation にログインします。
- ユーザーに資格が付与されるカatalog アイテムがサービスに関連付けられていることを確認します。 [サービスへのカatalog アイテムの追加](#)を参照してください。
- 資格を定義しているビジネス グループが存在しており、メンバー ユーザーとユーザー グループが定義されていることを確認します。 [ビジネス グループの作成](#)を参照してください。
- この資格の作成時に承認を追加する場合、承認ポリシーが存在していることを確認します。 [承認ポリシーの作成](#)を参照してください。承認を含めずにサービス カatalogのアイテムに対する資格をユーザーに付与した場合、後で資格を変更して承認を追加できます。

手順


- 1 [管理] - [カatalog管理] - [資格] を選択します。
- 2 [新規] アイコン () をクリックします。
- 3 [詳細] オプションを構成します。

[詳細] では、資格リストに資格を表示する方法、およびサービス カatalog内のアイテムに対するアクセス権を所有するユーザーを指定します。

オプション	説明
名前と説明	資格リストに表示される資格に関する情報です。
有効期限日	特定の日付に資格を無効にする場合に、その日付と時刻を設定します。

オプション	説明
ステータス	<p>使用できる値は、[有効]、[無効]、および [削除済み] です。</p> <ul style="list-style-type: none"> ■ 有効。アイテムは、サービス カタログ内で使用可能です。このオプションは、資格の追加または編集を行うときに使用できます。 ■ [無効]。アイテムはサービス カタログ内で使用可能ではありません。その資格は、有効期限日が過ぎたか、ユーザーの操作によって、無効にされました。 ■ [削除済み]。資格が削除されます。
ビジネス グループ	<p>ビジネス グループを選択します。1つのビジネス グループについてのみ資格を作成できます。資格を付与されるユーザーはビジネス グループのメンバーである必要があります。</p> <p>資格をすべてのユーザーに付与するには、「すべてのユーザー」ビジネス グループを作成するか、またはそれぞれのビジネス グループに対して資格を作成する必要があります。</p> <p>ビジネス グループ マネージャとしてログインしている場合は、自身のビジネス グループについてのみ資格を作成できます。</p>
ユーザーおよびグループ	<p>カタログ アイテムとアクションに対する資格をビジネス グループのすべてのメンバーに付与するには、[すべてのユーザーおよびグループ] を選択します。または、ユーザーまたはグループに個別に資格を付与することができます。資格を有効化するには、ビジネス グループ ユーザーまたはグループを1つ以上選択する必要があります。</p>

4 [次へ] をクリックします。

5 [新規] アイコン () をクリックして、この資格で利用可能なサービス、カタログ アイテム、アクションをユーザーが利用できるようにします。

資格は、サービス、アイテム、アクションをさまざまな方法で組み合わせることによって作成できます。

オプション	説明
使用可能なサービス	<p>資格のあるユーザーに、サービスに関連付けられたすべての公開済みカタログ アイテムへのアクセスを許可する場合は、そのサービスを追加します。</p> <p>使用可能なサービスは動的な資格です。後でアイテムをサービスに追加すると、そのアイテムは資格のあるユーザーのサービス カタログに追加されます。資格には、サービスと個々のカタログ アイテムを含めることができます。</p>
使用可能なカタログ アイテムおよびコンポーネント	<p>資格のあるユーザーが使用可能な個々のアイテムを追加します。</p> <p>資格には、サービスと個々のカタログ アイテムを含めることができます。サービスに含まれるアイテムに別の承認ポリシーを適用するには、ポリシーをカタログ アイテムとして追加します。アイテムの承認ポリシーとこのポリシーが属するサービスの承認ポリシーが同一の資格内にある場合、アイテムの承認ポリシーは、サービスの承認ポリシーよりも優先されます。これらのポリシーが異なる資格内にある場合、順序は設定した優先順位に基づきます。</p> <p>カタログ アイテムは、サービス カタログで使用可能となるサービスに関連付ける必要があります。カタログ アイテムには、現在の資格に属するサービスだけでなく、任意のサービスを関連付けることができます。</p> <p>コンポーネントはカタログ アイテムの一部ですが、サービス カタログ内では名前では利用できません。たとえば、MySQL ソフトウェアは、CentOS 仮想マシン カatalog アイテムのコンポーネントです。コンポーネントは、カタログ アイテムを使用する資格を持ちます。ソフトウェアに固有の承認ポリシーを適用する場合は、アイテムに個別に資格を付与します。それ以外の場合は、親アイテムとともに展開されるコンポーネントに資格を付与する必要はありません。</p>

オプション	説明
使用可能なアクション	<p>プロビジョニングされたアイテムのアクションの実行をユーザーに許可する場合にアクションを追加します。</p> <p>この資格からプロビジョニングされたアイテムに対して実行する必要があるアクションは、その同じ資格に含まれている必要があります。</p> <p>使用可能なアクションは、サービス カタログには表示されません。それらは、プロビジョニングされたアイテムの [展開] タブに表示されます。</p>
アクションをこの資格に定義されているアイテムにのみ適用する	<p>登録されたアクションがすべての該当するサービス カタログ アイテムを使用可能なのか、この資格のアイテムにだけ使用可能なのか決定します。</p> <p>これを選択した場合、この資格内の該当するアイテムに対してビジネス グループ メンバーがアクションを使用できます。このアクションの資格付与方法では、特定のアイテムのアクションを指定できます。</p> <p>このオプションが選択されていない場合、すべての該当するカタログ アイテムの資格内で指定されたユーザーがアクションを使用できます。アイテムがこの資格に含まれているかどうかは関係ありません。これらのアクションに適用されたすべての承認ポリシーも有効です。</p>

- 各セクションのドロップダウン メニューを使用して、使用可能なアイテムをフィルタリングします。
- チェック ボックスを選択して、資格にアイテムを含めます。
- 選択したサービス、アイテム、またはアクションに承認ポリシーを追加するには、[選択したアイテムにこのポリシーを適用] ドロップダウン メニューから承認ポリシーを選択します。

サービスに承認ポリシーを適用すると、そのサービス内のすべてのアイテムが同じ承認ポリシーを持つようになります。アイテムごとに異なるポリシーを適用するには、アイテムをカタログ アイテムとして追加し、適切なポリシーを適用します。

- [OK] をクリックします。

サービス、アイテム、またはアクションが資格に追加されます。

- [完了] をクリックして資格を保存します。

結果

資格のステータスが [有効] の場合は、サービスとアイテムがサービス カタログに追加されます。

次のステップ

使用可能なサービスとカタログ アイテムが資格のあるユーザーのサービス カタログに表示されていること、および申請したアイテムが期待どおりにターゲット オブジェクトをプロビジョニングしていることを確認します。選択したユーザーの代わりにアイテムを申請することができます。

資格の優先順位付け

同じビジネス グループに複数の資格が存在する場合は、資格に優先順位を付けることにより、サービス カタログ ユーザーが申請するときに、その資格および関連付けられた承認ポリシーが指定の順序で処理されるようにすることができます。

ユーザー グループの承認ポリシーを構成するときに、1 つ以上のサービス、カタログ アイテム、またはアクションについて、グループ メンバーが固有のポリシーを持つようにする場合は、メンバー資格の優先順位をグループ資格より上位にします。メンバーがサービス カatalog 内のアイテムを申請するとき、適用される承認ポリシーは、そのビジネス グループの資格の優先順位に基づいて決まります。メンバーの名前が初めて検出されるとき、カスタム ユーザー グループの一部としての承認ポリシー、または個別のユーザーとしての承認ポリシーのいずれかが適用されます。

たとえば、同じカタログ アイテムに対して 2 つの資格を作成し、会計ユーザー グループに 1 つの承認ポリシーが適用され、そのグループのメンバーである Chris には別の承認ポリシーが適用されるようにすることができます。

表 3-71. 資格例

資格 1	資格 2
ビジネス グループ：財務	ビジネス グループ：財務
ユーザーおよびグループ：会計グループ	ユーザーおよびグループ：Chris
カタログ アイテム 1：ポリシー A	カタログ アイテム 1：ポリシー C

Chris がサービス カatalog のカタログ アイテム 1 を申請します。財務ビジネス グループの資格の優先順位に基づいて、別のポリシーが Chris の申請に適用されます。


表 3-72. 結果例

構成と結果	優先順位	優先順位
優先順位	1：資格 1 2：資格 2	1：資格 2 2：資格 1
適用ポリシー	ポリシー A が適用されます。 Chris は会計ユーザー グループのメンバーです。資格を付与されたユーザーとして Chris を検索すると、資格 1 で停止し、承認ポリシーが適用されます。	ポリシー C が適用されます。 資格を付与されたユーザーとして Chris を検索すると、資格 2 で停止し、承認ポリシーが適用されます。

前提条件

テナント管理者またはカタログ管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [カタログ管理] - [資格] を選択します。
- 2 [優先順位付け] アイコン () をクリックします。
- 3 [ビジネス グループ] ドロップダウン リストからビジネス グループを選択します。
- 4 資格をリスト内の新しい場所にドラッグすると、その優先度を変更されます。
- 5 アップデート方法を選択します。

オプション	説明
アップデート	変更内容を保存します。
アップデートして閉じる	変更内容を保存してから、[資格の優先順位付け] ウィンドウを閉じます。

承認ポリシーの操作

承認ポリシーは、環境内のリソースを管理できるようにサービス カタログ申請に追加するガバナンスです。各ポリシーは、サービス、カタログ アイテム、およびこれらのアイテムの使用資格をユーザーに付与するときのアクションに対して適用できる、定義された一連の条件です。

承認ポリシーの処理

まず、ガバナンスのプロビジョニングが必要な承認ポリシーをテナント管理者または承認管理者が作成します。

承認ポリシーは、承認ポリシー タイプまたは特定のアイテムに対して作成されます。ポリシーがポリシー タイプに基づく場合、一致するカタログ アイテム タイプに適用できます。たとえば、ポリシーがソフトウェア ポリシー タイプに基づく場合、資格内の任意のソフトウェア アイテムに対してポリシーを定義し、適用することができます。ポリシーが特定のアイテムに対するものである場合は、そのアイテムのみに適用する必要があります。たとえば、アイテムが特定のソフトウェア アイテムである場合、資格内のその特定のデータベース ソフトウェア アイテムのみに適用する必要があります。

ポリシーには、事前承認および事後承認の要件を含めることができます。事前承認では、申請されたアイテムがプロビジョニングされる前に申請が承認される必要があります。事後承認ポリシーでは、プロビジョニングされたアイテムを申請元ユーザーが利用できるようにする前に承認者が申請を受け入れる必要があります。

事前承認および事後承認の構成は、承認ポリシーがいつトリガされるのか、誰がどのように申請を受け入れるのかを決定する 1 つ以上のレベルで構成されます。複数のレベルを含めることができます。たとえば、承認ポリシーでは、マネージャ承認に 1 つのレベル、その後の財務承認にもう 1 つのレベルを割り当てることができます。

次に、テナント管理者またはビジネス グループ マネージャは必要に応じてサービス、カタログ アイテム、およびアクションに対して承認ポリシーを適用します。

最後に、承認ポリシーが適用されるアイテムをサービス カタログ ユーザーが申請したときに、承認者が [受信箱] タブでその申請を承認または却下します。申請元ユーザーは、[展開] タブである申請の承認ステータスを追跡できます。

仮想マシン ポリシー タイプに基づく承認ポリシーの例

同一のカタログ アイテム タイプに適用できる承認ポリシーを作成できますが、サービス カタログでアイテムが申請された場合、その承認ポリシーによって異なる結果が生じます。承認ポリシーがどのように定義および適用されているかにより、サービス カタログ ユーザーおよび承認者に対する影響は異なります。

次の表に、すべて同一の承認ポリシーのタイプに基づく異なる承認ポリシーの例を示します。これらの例は、承認ポリシーを設定して、異なるタイプの管理を実現する方法を示したものです。

表 3-73. 承認ポリシーおよび結果の例

管理の目的	選択するポリシー タイプ	事前承認または事 後承認	承認が必要なとき	承認者	資格にポリシー が適用される方 法	サービス カタロ グでアイテムが申 請されたときの結 果
ビジネス グループ マネージャはすべての仮想マシンの申請を承認する必要があります。 承認ポリシーは複数の資格の複数のビジネス グループに適用可能であることが必要です。	サービス カタログ - カタログ アイテム申請 - 仮想マシン	[事前承認] タブへの追加	[常に必要] を選択	[申請から承認者を判断する] を選択します。 条件 [ビジネス グループ] - [マネージャ] - [ユーザー] - [マネージャ] を選択します。 [誰でも承認できる] を選択します。	資格は、ビジネス グループに基づいています。この承認は、仮想マシンにマネージャの承認を必要とするすべての資格で使用できます。	この承認が適用された仮想マシンが、サービス カタログ ユーザーから申請された場合、ビジネス グループ マネージャはマシンがプロビジョニングされる前にその申請を承認する必要があります。
仮想インフラストラクチャ管理者は、仮想マシンの正しいプロビジョニングを確認し、申請しているユーザーに仮想マシンがリリースされる前にその申請を承認する必要があります。	サービス カタログ - カタログ アイテム申請 - 仮想マシン	[事後承認] タブへの追加	[常に必要] を選択	[特定のユーザーおよびグループ] を選択します。 仮想インフラストラクチャ管理者のカスタム ユーザーグループを選択します。 [誰でも承認できる] を選択します。	この承認は、vCenter Server に仮想マシンがプロビジョニングされた後で仮想インフラストラクチャ管理者による仮想マシンのチェックを必要とするすべての資格で使用できます。	この承認が適用された仮想マシンが、サービス カタログ ユーザーから申請された場合、仮想マシンはプロビジョニングされます。仮想インフラ管理者グループの各メンバーが申請を承認すると、マシンはそのユーザーにリリースされます。
仮想インフラストラクチャ リソースを管理し、価格を制御するには、2 つの事前承認レベルを追加し、1 つの承認をマシンリソースの承認に、もう 1 つを 1 日あたりのマシンの価格の承認に設定します。	サービス カタログ - カタログ アイテム申請 - 仮想マシン	[事前承認] タブへの追加	レベル 1 [条件に応じて必要] を選択します。 [CPU] > [6]、[メモリ] > [8]、または [ストレージ] > [100 GB] の条件を構成します。	[申請から承認者を判断する] を選択します。 条件 [申請者] > [マネージャ] を選択します。 [システム プロパティ] をクリックして、[CPU] を選択します。承認者が受け入れ可能なレベルに値を変更できるように、[メモリ]、および [ストレージ] を選択します。	この承認ポリシーは、申請しているユーザーのマネージャや経理部のメンバーが申請を承認する資格で使用できます。	サービス カタログ ユーザーが仮想マシンを申請すると、申請された CPU、メモリ、またはストレージの量がレベル 1 で指定されている量を超えているかどうかを判定するため、申請が評価されます。超えているものがない場合、レベル 2 の条件が評価されます。申請が 1 つ以上のレベル 1 の条件を超えている場合、マネージャによる申請の承認が必要になります。マネージャには、

表 3-73. 承認ポリシーおよび結果の例（続き）

管理の目的	選択するポリシー タイプ	事前承認または事 後承認	承認が必要なとき	承認者	資格にポリシー が適用される方 法	サービス カタロ グでアイテムが申 請されたときの結 果
			レベル 2 [条件に応じて必 要] を選択しま す。 [価格] > [1 日あ たり 15.00] の条 件を構成します。	[特定のユーザーお よびグループ] を 選択します。 経理のカスタム ユ ーザー グループを 選択します。 [誰でも承認でき る] を選択します。		申請された構成量 を少なくして承認 するオプションが あります。また、 マネージャは申請 を拒否できます。
パラメータ化され たブループリント カタログ アイテ ムの場合、クラウ ド管理者は size の vSphere マ シン コンポーネ ント プロファイ ルが large に設 定されている展開 要求を承認する必 要があります。	サービス カタロ グ - カタログ ア イテム申請 - 仮 想マシン	[事前承認] タブ への追加	レベル 1 [条件に応じて必 要] を選択しま す。 レベル 2 [単一条件] を選 択します。 [コンポーネント プロファイル] - [vSphere マシ ンのサイズ] を選 択します。 [サイズ] = [大] の条件を構成しま す。	[特定のユーザーお よびグループ] を 選択します。 申請の承認を許可 されているユーザ ーとグループを選 択します。 [誰でも承認でき る] を選択します。	この承認ポリシ ーは、クラウド管 理者によるプロ ビジョニング申 請の承認を必要 とする資格で使 用できます。	この承認が適用さ れた仮想マシン が、サービス カタ ログ ユーザーか ら申請された場 合、クラウド管理 者はマシンがプロ ビジョニングされ る前にその申請を 承認する必要があります。

承認ポリシーが複合展開に適用されるアクションの例

複合ブループリントのさまざまなコンポーネント上で実行できるアクションに承認ポリシーを適用する場合、承認プロセスは、資格の構成方法と承認ポリシーの適用方法により異なります。

この例では、具体的な詳細を使用してブループリントを作成し、異なる資格内でプロビジョニングされたブループリント上でサービス カタログから実行できるアクションに承認ポリシーを適用します。このブループリントは、別のブループリントを含む複合ブループリントです。使用するアクションには、プロビジョニングされたアイテムの削除、ブループリントの展開の削除、マシンに対する仮想マシンの削除があります。このアクションの結果、削除する内容と、適用する承認ポリシーが承認申請をトリガするタイミングが決まります。

ブループリント例

この例では、仮想マシンでネストしたブループリントを含むブループリントを構成します。

- ブループリント 1 - 連続統合のブループリント
 - ブループリント 2 - 本番環境適用前のブループリント
 - 仮想マシン 1 - TestAsAService vSphere 仮想マシン

削除アクションの承認ポリシー

プロビジョニングされたアイテムを削除するには、2 つの承認ポリシーを構成します。削除 - この例のブループリント 1 と ブループリント 2 上で展開アクションを実行できます。削除 - 仮想マシン 1 上で仮想マシン アクションを実行できます。承認ポリシーを資格内のアクションに適用できるように、承認ポリシーを作成します。

承認ポリシー名	承認ポリシー タイプ
承認ポリシー A	サービス カタログ - リソース アクション申請 - 削除 - 展開
承認ポリシー B	サービス カタログ - リソース アクション申請 - 削除 - 仮想マシン

アクションに適用する資格と承認ポリシー

3 つの資格を構成します。各資格には複合ブループリントが含まれます。各資格で、削除アクションを追加し、承認ポリシーを適用します。

資格名	プロビジョニングされたマシン上で使用可能なアクション	適用される承認ポリシー
資格 1	削除 - 展開	承認ポリシー A
資格 2	削除 - 仮想マシン	承認ポリシー B
資格 3	削除 - 展開 削除 - 仮想マシン	承認ポリシー A 承認ポリシー B

サービス カタログのユーザー アクション

サービス カタログ ユーザーがアクションを実行すると、ブループリントまたはマシンが、ユーザーが実行するアクションに応じて削除されます。

サービス カタログの ユーザー アクション	選択したアクション	削除されたブループリントまたは マシン
アクション 1	削除 - 展開アクションがブループリント 1 - 連続統合のブループリント上で実行されます	ブループリント 1、ブループリント 2、および仮想マシン 1
アクション 2	削除 - 展開アクションがネストされたブループリント 2 - 本番環境適用前ブループリント上で実行されます	ブループリント 2 および仮想マシン 1
アクション 3	削除 - 仮想マシン アクションが展開内のマシン（仮想マシン 1 - TestAsAService vSphere 仮想マシン）上で実行されます	仮想マシン 1

資格内のアクションに適用される承認ポリシー

承認ポリシーを適用すると、承認者は、サービス カタログ ユーザーがアクションを実行するブループリントまたはマシンに応じて承認申請を受信します。

資格名	アクションの承認ポリシー	ユーザー アクション	トリガされる承認申請	承認されると、ブループリントまたはマシンが削除されます
資格 1 - 展開の削除承認ポリシー	ポリシー A (展開の削除承認ポリシー) 削除 - 展開アクションのみ対象	アクション 1 (ブループリント 1 上で削除 - 展開アクションを実行)	承認申請はブループリント 1 に対してのみトリガされます	ブループリント 1、ブループリント 2、および仮想マシン 1
		アクション 2 (ブループリント 2 上で削除 - 展開アクションを実行)	承認申請はブループリント 2 に対してのみトリガされます	ブループリント 2 および仮想マシン 1
		アクション 3 (仮想マシン 1 上で削除 - 仮想マシン アクションを実行)	トリガされる承認申請はありません	仮想マシン 1
資格 2	ポリシー B (削除 - 仮想マシン ポリシー) 削除 - 仮想マシン アクションのみ対象	アクション 1 (ブループリント 1 上で削除 - 展開アクションを実行)	トリガされる承認申請はありません	ブループリント 1、ブループリント 2、および仮想マシン 1
		アクション 2 (ブループリント 2 上で削除 - 展開アクションを実行)	トリガされる承認申請はありません	ブループリント 2 および仮想マシン 1
		アクション 3 (仮想マシン 1 上で削除 - 仮想マシン アクションを実行)	承認申請は仮想マシン 1 に対してのみトリガされます	仮想マシン 1
資格 3	ポリシー A (展開の削除承認ポリシー) 削除 - 展開アクションのみ対象およびポリシー B (削除 - 仮想マシン ポリシー) 削除 - 仮想マシン アクションのみ対象	アクション 1 (ブループリント 1 上で削除 - 展開アクションを実行)	承認申請はブループリント 1 に対してのみトリガされます	ブループリント 1、ブループリント 2、および仮想マシン 1
		アクション 2 (ブループリント 2 上で削除 - 展開アクションを実行)	承認申請はブループリント 2 に対してのみトリガされます	ブループリント 2 および仮想マシン 1
		アクション 3 (仮想マシン 1 上で削除 - 仮想マシン アクションを実行)	承認申請は仮想マシン 1 に対してのみトリガされます	仮想マシン 1

複数の資格での承認ポリシーの例

複数の資格で使用されているアイテムに承認ポリシーを適用し、その資格がビジネス グループ内の同一のユーザーに付与されている場合、承認ポリシーが資格内で明示的に適用されていないサービスでも、そのアイテムで承認ポリシーはトリガされます。

たとえば、次のブループリント、サービス、承認ポリシー、および資格を作成します。

ブループリント

- RHEL vSphere 仮想マシン
- QE テストには RHEL vSphere 仮想マシンが含まれます。
- QE トレーニングには RHEL vSphere 仮想マシンが含まれます。

サービス

- QE テスト ブループリントはテスト サービスと関連付けられます。
- QE トレーニング ブループリントはトレーニング サービスと関連付けられます。

資格

- 資格 1
- 資格 2

表 3-74. 資格の構成

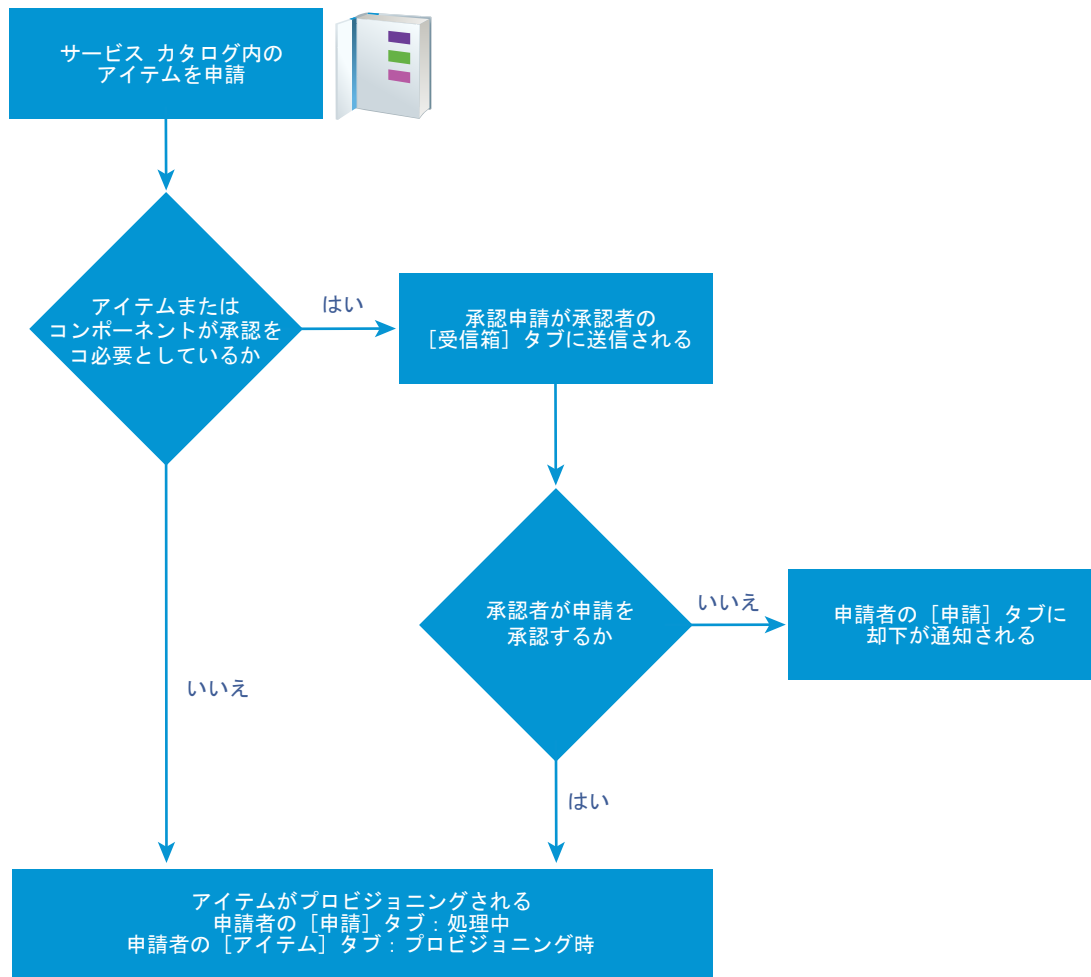
資格名	ビジネス グループ	使用可能なサービス	使用可能なアイテム
資格 1	QE	テスト	カタログ アイテム申請 - 仮想マシン コンポーネントに適用される仮想マシン
資格 2	QE	トレーニング	

結果

ユーザーがサービス カタログで QE トレーニングを選択すると、RHEL vSphere 仮想マシンは QE トレーニング ブループリントで使用される仮想マシン コンポーネントに基づくブループリントであるため、RHEL vSphere 仮想マシンに対する承認ポリシーがトリガされます。

サービス カタログでの承認ポリシーの処理

承認ポリシーが適用されたサービス カタログのアイテムをユーザーが申請した場合、申請は、承認者および申請元ユーザーによって、次のワークフローと同様に処理されます。



承認ポリシーの作成

テナント管理者と承認管理者は、承認ポリシーを定義して資格で使用できます。事前承認および事後承認のイベントに対して、複数のレベルを持つ承認ポリシーを設定できます。

ソフトウェア コンポーネント ブループリントの設定を変更し、承認ポリシーでこの設定を使用して承認申請をトリガする場合、承認申請が予測どおりに機能しない場合があります。コンポーネントの設定を変更する必要がある場合、変更によって1つ以上の承認ポリシーが影響を受けないことを確認します。

前提条件

テナント管理者または承認管理者として vRealize Automation にログインします。

手順

1 承認ポリシー情報の指定

承認ポリシーを作成するときは、承認ポリシー タイプ、名前、説明、およびステータスを定義します。

2 承認レベルの作成

承認ポリシーを作成するときに、事前承認レベルと事後承認レベルを追加できます。

3 システム プロパティとカスタム プロパティを含めるための承認フォームの構成

承認フォームに表示されるシステム プロパティとカスタム プロパティを追加できます。承認者が承認申請を入力する前に、CPU またはメモリなどのマシン リソース設定のシステム プロパティと、カスタム プロパティの値を変更できるように、これらのプロパティを追加します。

4 承認ポリシー設定

承認ポリシーを作成する場合、サービス カタログ ユーザーによって申請されたアイテムの承認のタイミングを決定するさまざまなオプションを構成します。申請のプロビジョニング開始前、またはアイテムのプロビジョニング後で申請元ユーザーにアイテムがリリースされる前に、承認が必要になります。

承認ポリシー情報の指定

承認ポリシーを作成するときは、承認ポリシー タイプ、名前、説明、およびステータスを定義します。

前提条件

テナント管理者または承認管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [承認ポリシー] を選択します。
- 2 [新規] アイコン (+) をクリックします。
- 3 ポリシー タイプまたはソフトウェア コンポーネントを選択します。

オプション	説明
[承認ポリシーのタイプを選択]	<p>ポリシー申請タイプに基づいて承認ポリシーを作成します。</p> <p>このオプションを選択すると、このタイプのすべてのカタログ アイテムに適用可能な承認ポリシーを定義できます。申請タイプには、一般申請、カタログ アイテム申請、またはリソース アクション申請があります。</p> <p>利用可能な条件構成オプションは、タイプに応じて異なります。タイプがより具体的になるほど、構成フィールドもより詳細になります。たとえば、[サービス カタログ - カatalog アイテム申請] には、すべてのカタログ アイテム申請に共通するフィールドしかありませんが、[サービス カタログ - カatalog アイテム申請 - 仮想マシン] には、共通するオプションと仮想マシン固有のオプションも含まれます。</p> <p>申請タイプにより、承認ポリシーを適用できるカタログ アイテムまたはアクションが制限されます。</p>
[アイテムを選択]	<p>固有のアイテムに基づいて承認ポリシーを作成します。</p> <p>このオプションを選択すると、サービス カタログの個別アイテムとしてではなく、マシンや他の展開の一部としてのみ利用可能な固有のアイテムに適用可能な承認ポリシーを定義できます。たとえば、ソフトウェア コンポーネントなどです。</p> <p>利用可能な条件構成フィールドはアイテムに固有で、ポリシー タイプ アイテムに提供される条件よりも詳細に設定できます。</p>
[リスト]	<p>利用可能なポリシー タイプまたはカタログ アイテムを一覧表示します。</p> <p>特定のアイテムまたはタイプを見つけるには、検索したり、列をソートしたりします。</p>

- 4 [OK] をクリックします。
- 5 名前と説明（説明は任意）を入力します。

6 [ステータス] ドロップダウン メニューで、ポリシーの状態を選択します。

オプション	説明
ドラフト	承認ポリシーを編集可能な状態で保存します。
有効	承認ポリシーを読み取り専用状態で保存します。この状態のポリシーは資格で使用できます。
無効	承認ポリシーを読み取り専用状態で保存します。この状態のポリシーは、有効化されるまで資格で使用できません。

次のステップ

事前承認レベルおよび事後承認レベルを作成します。

承認レベルの作成

承認ポリシーを作成するときに、事前承認レベルと事後承認レベルを追加できます。


1 つの承認ポリシーに対して複数の承認レベルを作成できます。サービス カタログ ユーザーが、複数のレベルを持つ承認ポリシーが適用されたアイテムを申請すると、承認申請が次の承認者に送信される前に、最初のレベルをそれぞれ受け入れる必要があります。[承認ポリシーの操作](#)を参照してください。

リース期間要求によってトリガーされる承認ポリシーを構成する場合は、承認要件として「常に必要」を選択する必要があります。

前提条件

[承認ポリシー情報の指定](#)。

手順

- 1 [事前承認] または [事後承認] タブで、[新規] アイコン（）をクリックします。
- 2 名前と説明（説明は任意）を入力します。
- 3 承認要件を選択します。

オプション	説明
常に必要	承認ポリシーがすべての申請でトリガされます。
条件に応じて必要	<p>この承認ポリシーは 1 つ以上の条件節に基づいています。</p> <p>このオプションを選択すると、条件を作成する必要があります。資格内の使用可能なサービス、カタログ アイテム、またはアクションにこの承認ポリシーを適用すると、条件が評価されます。条件を満たす場合は、申請のプロビジョニング前に、指定した承認者方法で申請を承認する必要があります。条件が満たされない場合は、承認を求めずに申請をプロビジョニングします。たとえば、4 個以上の CPU を搭載した仮想マシンの申請は、仮想インフラストラクチャ管理者によって承認される必要があります。</p> <p>条件のベースとなるフィールドを利用できるかどうかは、選択した承認ポリシー タイプまたはカタログ アイテムに応じて決まります。</p> <p>条件に値を入力する場合、値の大文字と小文字は区別されます。</p> <p>複数の条件節を構成するには、条件節にブール演算子を選択します。</p>

4 承認者を選択します。

オプション	アクション
特定のユーザーおよびグループ	承認申請を選択したユーザーに送信します。
申請から承認者を判断する	<p>定義した条件に基づいて、承認申請をユーザーに送信します。</p> <p>注： 申請によって動的に決定されるすべてのユーザーおよび申請者が vRealize Automation 内にいること、これらが Active Directory で同期されていていること、そして [管理] - [ユーザーおよびグループ] - [ディレクトリ ユーザーとディレクトリ グループ] から参照できることを確認します。</p> <p>ディレクトリ管理 ID プロバイダで同期されていないユーザーがカタログ申請中に何らかの方法で参照されると、「アイテムの承認が申請されました」ランタイム エラーが発生して申請は失敗します。</p>
イベント サブスクリプションを使用する	<p>定義したイベント サブスクリプションに基づいて承認申請を処理します。</p> <p>ワークフロー サブスクリプションは、[管理] - [イベント] - [サブスクリプション] で定義する必要があります。適用可能なワークフロー サブスクリプションは事前承認と事後承認です。</p>

5 申請またはアクションの承認者を指定します。

オプション	説明
誰でも承認できる	<p>承認者のうち 1 人のみが申請の処理前に承認する必要があります。</p> <p>サービス カatalogでアイテムが申請されると、承認の申請がすべての承認者に送信されます。1 人の承認者が申請を承認すると、この申請は承認され、承認の申請が他の承認者の受信箱から削除されます。</p>
全員の承認が必要	申請の処理前に、指定された承認者全員が承認する必要があります。

6 承認フォームにプロパティを追加し、レベルを保存します。

- 承認フォームにプロパティを追加するには、[システム プロパティ] または [カスタム プロパティ] をクリックします。
- レベルを保存するには、[OK] をクリックします。

次のステップ

承認フォームにプロパティを追加するには、[システム プロパティとカスタム プロパティを含めるための承認フォームの構成](#)を参照してください。

システム プロパティとカスタム プロパティを含めるための承認フォームの構成

承認フォームに表示されるシステム プロパティとカスタム プロパティを追加できます。承認者が承認申請を入力する前に、CPU またはメモリなどのマシン リソース設定のシステム プロパティと、カスタム プロパティの値を変更できるように、これらのプロパティを追加します。

利用可能なシステム プロパティは、承認ポリシー タイプとブループリントの構成方法に応じて異なります。一部のプロパティでは、プロパティがシステム プロパティ リストに表示される前に、ブループリント内で構成したフィールドに最大値と最小値を含める必要があります。


承認レベルを追加すると、カスタム プロパティを追加することができます。カスタム プロパティを構成し、ブループリントに含めると、承認フォームに追加したカスタム プロパティによって、ブループリント、プロパティ グループ、またはエンドポイントなどにあるこのカスタム プロパティの他のインスタンスがすべて上書きされます。

承認者は、承認フォームで選択または構成したプロパティを変更できます。


前提条件

- テナント管理者または承認管理者として vRealize Automation にログインします。
- [承認レベルの作成](#)。

手順

- 1 [事前承認] または [事後承認] タブで、[新規] アイコン（）をクリックします。
- 2 [システム プロパティ] タブをクリックします。
- 3 承認プロセス中に承認者が構成する各システム プロパティのチェック ボックスを選択します。
- 4 カスタム プロパティを構成します。

承認プロセス中に承認者が構成する 1 つ以上のカスタム プロパティを追加します。

- a [カスタム プロパティ] タブをクリックします。
- b [新規] アイコン（）をクリックします。
- c カスタム プロパティの値を入力します。

オプション	説明
Name	プロパティ名を入力します。
ラベル	承認フォームで承認者に表示されるラベルを入力します。
説明	承認者の詳細情報を入力します。 この情報は、フォームにフィールドのヒントとして表示されます。

- d [保存] をクリックします。
- e 複数のカスタム プロパティを削除するには、行を選択して [削除] をクリックします。

- 5 [OK] をクリックします。

次のステップ

- 他の事前承認または事後承認レベルを追加します。
- 承認ポリシーを保存します。[資格] にサービス、アイテム、またはアクションを適用するには、ポリシーを有効にする必要があります。

承認ポリシー設定

承認ポリシーを作成する場合、サービス カタログ ユーザーによって申請されたアイテムの承認のタイミングを決定するさまざまなオプションを構成します。申請のプロビジョニング開始前、またはアイテムのプロビジョニング後で申請元ユーザーにアイテムがリリースされる前に、承認が必要になります。

[管理] - [承認ポリシー] を選択します。[新規] をクリックします。

■ 承認ポリシー タイプ設定

承認ポリシー タイプでは、承認ポリシーの構成方法と資格内でポリシーを適用するアイテムやアクションを指定します。承認レベルを追加すると、ポリシー タイプまたはアイテムが、承認レベルの条件を作成できるフィールドに影響を与えます。

■ 承認ポリシー設定の追加

ポリシーの状態などの承認ポリシーに関する基本情報を構成して、ポリシーを管理できるようにします。

■ 承認ポリシー設定へのレベル情報の追加

承認レベルには、サービス カタログ ユーザーが、追加するアイテム、システム プロパティ、およびカスタム プロパティを申請する場合に承認プロセスをトリガする条件が含まれます。トリガされると、承認申請は指定された承認者に送信されます。

■ 承認ポリシー設定へのシステム プロパティの追加

承認者が値を変更できるように、承認フォームに追加するシステム プロパティを選択しました。

■ 承認ポリシー設定へのカスタム プロパティの追加

承認者が値を変更できるように、承認フォームに追加するカスタム プロパティを構成します。

承認ポリシー タイプ設定

承認ポリシー タイプでは、承認ポリシーの構成方法と資格内でポリシーを適用するアイテムやアクションを指定します。承認レベルを追加すると、ポリシー タイプまたはアイテムが、承認レベルの条件を作成できるフィールドに影響を与えます。

[管理] - [承認ポリシー] を選択します。[新規] をクリックします。

表 3-75. 承認ポリシー タイプ オプション

オプション	説明
[承認ポリシーのタイプを選択]	<p>ポリシー申請タイプに基づいて承認ポリシーを作成します。</p> <p>このオプションを選択すると、このタイプのすべてのカタログ アイテムに適用可能な承認ポリシーを定義できます。申請タイプには、一般申請、カタログ アイテム申請、またはリソース アクション申請があります。</p> <p>利用可能な条件構成オプションは、タイプに応じて異なります。タイプがより具体的になるほど、構成フィールドもより詳細になります。たとえば、[サービス カatalog - カatalog アイテム申請] には、すべてのカタログ アイテム申請に共通するフィールドしかありませんが、[サービス カatalog - カatalog アイテム申請 - 仮想マシン] には、共通するオプションと仮想マシン固有のオプションも含まれます。</p> <p>申請タイプにより、承認ポリシーを適用できるカタログ アイテムまたはアクションが制限されます。</p>
[アイテムを選択]	<p>固有のアイテムに基づいて承認ポリシーを作成します。</p> <p>このオプションを選択すると、サービス カatalog の個別アイテムとしてではなく、マシンや他の展開の一部としてのみ利用可能な固有のアイテムに適用可能な承認ポリシーを定義できます。たとえば、ソフトウェアコンポーネントなどです。</p> <p>利用可能な条件構成フィールドはアイテムに固有で、ポリシー タイプアイテムに提供される条件よりも詳細に設定できます。</p>
[リスト]	<p>利用可能なポリシー タイプまたはカタログ アイテムを一覧表示します。</p> <p>特定のアイテムまたはタイプを見つけるには、検索したり、列をソートしたりします。</p>

承認ポリシー設定の追加

ポリシーの状態などの承認ポリシーに関する基本情報を構成して、ポリシーを管理できるようにします。

承認ポリシーの基本情報を定義するには、[管理] - [承認ポリシー] を選択します。[新規] をクリックします。ポリシー タイプを選択して [OK] をクリックします。

表 3-76. 承認ポリシー オプション

オプション	説明
名前	資格で承認ポリシーを適用する場合に表示される名前。
説明	承認ポリシーの作成方法に関する詳細説明を入力します。この情報は承認ポリシーの管理に役立ちます。
ステータス	<p>指定可能な値は次のとおりです。</p> <ul style="list-style-type: none"> ■ ドラフト。資格で承認ポリシーを適用できません。ポリシーを有効にしたら、ドラフトに戻すことはできません。 ■ 有効。資格で承認ポリシーを適用できます。 ■ 無効。資格で承認ポリシーを適用できません。ポリシーを資格に適用せず、無効にした場合は、このポリシーを削除できますが、再アクティブ化することはできません。ポリシーを適用してから、無効にした場合は、ポリシーが適用されたアイテムを別のポリシーにリンクするか、アイテムのリンクを解除する必要があります。ユーザーはリンク解除されたアイテムおよびアクションを使用できませんが、承認ポリシーは適用されません。

表 3-76. 承認ポリシー オプション（続き）

オプション	説明
ポリシー タイプ	承認ポリシーの申請タイプを表示します。 承認ポリシーのベースとなるカタログ アイテムを選択すると、関連する申請タイプが表示されます。
アイテム	選択したカタログ アイテムが表示されます。 承認ポリシーのベースとなる申請タイプを選択すると、このフィールドは空白になります。
最終アップデート者	承認ポリシーを変更したユーザーの名前。
最終アップデート日	承認ポリシーを最後に更新した日付。
事前承認レベル	申請アイテムのプロビジョニング前またはアクションの実行前に承認を求めるには、サービス カatalog ユーザーがアイテムを申請する際に承認プロセスをトリガする条件を 1 つ以上構成します。
事後承認レベル	アイテムをプロビジョニングした後で、プロビジョニングしたまたは変更したアイテムを申請元のサービス カatalog ユーザーにリリースする場合に承認を求めるには、承認プロセスをトリガする条件を 1 つ以上構成します。 たとえば、仮想インフラストラクチャ管理者が、仮想マシンがサービス カatalog ユーザーにリリースされる前に、機能する状態にあることを検証するなどです。
リンクされた資格の表示	承認ポリシーがサービス、カタログ アイテム、またはアクションに適用される場合にすべての資格を表示します。ある資格内のアイテムを別のポリシーにリンクすることができます。 このオプションは、有効な承認ポリシーを表示している場合にのみ利用可能です。

承認ポリシー設定へのレベル情報の追加

承認レベルには、サービス カatalog ユーザーが、追加するアイテム、システム プロパティ、およびカスタム プロパティを申請する場合に承認プロセスをトリガする条件が含まれます。トリガされると、承認申請は指定された承認者に送信されます。

承認ポリシーの基本情報を定義するには、[管理] - [承認ポリシー] を選択します。[新規] をクリックします。ポリシー タイプを選択して [OK] をクリックします。[事前承認] タブまたは [事後承認] タブで、[新規] アイコン (+) をクリックします。

処理する順番に基づいてレベルに優先順位を付けます。承認ポリシーがトリガされ、承認の最初のレベルが却下されると、申請は却下されます。

表 3-77. レベル情報のオプション

オプション	説明
[名前]	名前を入力します。 承認ポリシーが指定された申請を確認しているときにレベル名が表示されます。
[説明]	レベルの説明を入力します。 たとえば、CPU 4 個未満や仮想インフラ管理者などです。

表 3-77. レベル情報のオプション（続き）

オプション	説明
[いつ承認が必要ですか?]	承認ポリシーがトリガされるタイミングを選択します。
[常に必要]	<p>承認ポリシーがすべての申請でトリガされます。</p> <p>このオプションを選択し、資格内の使用可能なサービス、カタログ アイテム、またはアクションにこの承認ポリシーを適用する場合、申請のプロビジョニング前に、指定した承認者方法で申請を承認する必要があります。たとえば、申請するユーザーのマネージャがすべての申請を承認する必要がある場合です。</p>
[条件に応じて必要]	<p>この承認ポリシーは 1 つ以上の条件節に基づいています。</p> <p>このオプションを選択すると、条件を作成する必要があります。資格内の使用可能なサービス、カタログ アイテム、またはアクションにこの承認ポリシーを適用すると、条件が評価されます。条件を満たす場合は、申請のプロビジョニング前に、指定した承認者方法で申請を承認する必要があります。条件が満たされない場合は、承認を求めずに申請をプロビジョニングします。たとえば、4 個以上の CPU を搭載した仮想マシンの申請は、仮想インフラストラクチャ管理者によって承認される必要があります。</p> <p>条件のベースとなるフィールドを利用できるかどうかは、選択した承認ポリシー タイプまたはカタログ アイテムに応じて決まります。</p> <p>条件に値を入力する場合、値の大文字と小文字は区別されます。</p> <p>複数の条件節を構成するには、条件節にブール演算子を選択します。</p> <ul style="list-style-type: none"> ■ 次のすべて。すべての条件節が満たされる場合、承認がトリガされます。これは、各条件節の間にブール演算子 AND があるためです。 ■ 次のいずれか。条件節のいずれかが満たされる場合、承認レベルがトリガされます。これは、各条件節の間にブール演算子 OR があるためです。 ■ 次を含まない。いずれの条件節も満たされない場合、承認レベルがトリガされます。これは、各条件節の間にブール演算子 NOT があるためです。
[承認者]	承認者方法を選択します。
[特定のユーザーおよびグループ]	<p>承認申請を選択したユーザーに送信します。</p> <p>申請のプロビジョニング前またはアクションの実行前に、サービス カタログ申請を承認する必要のあるユーザーまたはユーザー グループを選択します。たとえば、[誰でも承認できる]を選択すると、申請は仮想インフラストラクチャ管理者グループに送られます。</p>
[申請からユーザーを判断する]	<p>定義した条件に基づいて、承認申請をユーザーに送信します。</p> <p>たとえば、この承認ポリシーをビジネス グループ全体に適用し、ビジネス グループ マネージャが申請を承認できるようにするには、[ビジネス グループ] - [ユーザー] - [ユーザー] - [マネージャ] を選択します。</p>
[イベント サブスクリプションを使用する]	<p>定義したイベント サブスクリプションに基づいて承認申請を処理します。</p> <p>ワークフロー サブスクリプションは、[管理] - [イベント] - [サブスクリプション] で定義する必要があります。適用可能なワークフロー サブスクリプションは事前承認と事後承認です。</p>

表 3-77. レベル情報のオプション（続き）

オプション	説明
[誰でも承認できる]	承認者のうち 1 人のみが申請の処理前に承認する必要があります。 サービス カタログでアイテムが申請されると、承認の申請がすべての承認者に送信されます。1 人の承認者が申請を承認すると、この申請は承認され、承認の申請が他の承認者の受信箱から削除されます。 最初の承認者が申請を却下すると、申請元ユーザーに却下の通知が送られ、承認申請が承認者の受信箱から削除されます。 最初の承認者が申請を承認した後で、この承認申請を 2 人目の承認者のコンソールで開いても、2 人目の承認者は承認申請を送信できません。最初の承認者の対応で完了したと見なされました。 [特定のユーザーおよびグループ] または [申請から承認者を判断する] を選択し、複数の承認者が存在する場合、これは追加オプションの 1 つです。承認者が 1 人のみの場合は、このオプションは適用されません。
[全員の承認が必要]	申請の処理前に、指定された承認者全員が承認する必要があります。 [特定のユーザーおよびグループ] または [申請から承認者を判断する] を選択し、複数の承認者が存在する場合、これは追加オプションの 1 つです。承認者が 1 人のみの場合は、このオプションは適用されません。

承認ポリシー設定へのシステム プロパティの追加

承認者が値を変更できるように、承認フォームに追加するシステム プロパティを選択しました。

たとえば、仮想マシン申請の場合、承認者が CPU を 6 個から 4 個に申請を変更できるようにする場合は CPU を選択します。

システム プロパティを選択するには、[管理] - [承認ポリシー] を選択します。[新規] をクリックします。ポリシータイプを選択して [OK] をクリックします。[事前承認] タブまたは [事後承認] タブで、[新規] アイコン (+) をクリックして、[システム プロパティ] タブをクリックします。

表 3-78. システム プロパティ オプション

オプション	説明
[プロパティ]	利用可能なシステム プロパティのリストは、選択した申請タイプやカタログ アイテム、システム プロパティが選択したアイテムに存在するかどうかによって異なります。 一部のプロパティは、ブループリントが特定の方法で構成された場合にのみ利用可能となります。たとえば、CPU などです。CPU システム プロパティを使用して承認ポリシーを適用するブループリントは、範囲で構成する必要があります。たとえば、CPU の最小値が 2 で、最大値が 8 などです。

承認ポリシー設定へのカスタム プロパティの追加

承認者が値を変更できるように、承認フォームに追加するカスタム プロパティを構成します。

たとえば、仮想マシン承認の場合、承認者が vCenter Server でマシンを追加するフォルダを指定できるようにするには、**VMware.VirtualCenter.Folder** を追加します。

また、この承認ポリシー フォームに固有のカスタム プロパティを追加することもできます。


システム プロパティを選択するには、[管理] - [承認ポリシー] を選択します。[新規] をクリックします。ポリシー タイプを選択して [OK] をクリックします。[事前承認] タブまたは [事後承認] タブで、[新規] アイコン（）をクリックして、[カスタム プロパティ] タブをクリックします。

表 3-79. カスタム プロパティ

オプション	説明
[名前]	プロパティ名を入力します。
[ラベル]	承認フォームで承認者に表示されるラベルを入力します。
[説明]	承認者の詳細情報を入力します。 この情報は、フォームにフィールドのヒントとして表示されます。

承認ポリシーの変更

有効または無効な承認ポリシーを変更することはできません。元のポリシーのコピーを作成し、期待する結果が得られないポリシーと置き換える必要があります。有効および無効な承認ポリシーは読み取り専用です。ドラフト状態の承認ポリシーは変更することができます。


承認ポリシーのコピーを作成する場合、新しいポリシーは元のポリシー タイプをベースにします。このポリシー タイプ以外の属性はすべて編集できます。レベルの変更、追加、または削除、あるいはフォームへのシステムやカスタム プロパティの追加において、承認ポリシーを変更する場合はこの操作を行います。

事前承認レベルおよび事後承認レベルを作成できます。承認レベルの作成については、[承認レベルの作成](#)を参照してください。

前提条件

テナント管理者または承認管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [承認ポリシー] を選択します。
- 2 コピーする承認ポリシーの行を選択します。
- 3 [コピー] アイコン（）をクリックします。
承認ポリシーのコピーが作成されます。
- 4 編集する新しい承認ポリシーを選択します。
- 5 [名前] テキスト ボックスに名前を入力します。
- 6 （オプション） [説明] テキスト ボックスに説明を入力します。

- 7 [ステータス] ドロップダウン メニューで、ポリシーの状態を選択します。

オプション	説明
ドラフト	承認ポリシーを編集可能な状態で保存します。
有効	承認ポリシーを読み取り専用状態で保存します。この状態のポリシーは資格で使用できます。
無効	承認ポリシーを読み取り専用状態で保存します。この状態のポリシーは、有効化されるまで資格で使用できません。

- 8 事前承認レベルおよび事後承認レベルを編集します。

- 9 [OK] をクリックします。

結果

既存の承認ポリシーに基づいて新しい承認ポリシーを作成しました。

次のステップ

新しい承認ポリシーを資格に適用します。[ユーザーにサービス、カタログ アイテム、アクションの使用資格を付与](#)を参照してください。

承認ポリシーの無効化

承認ポリシーが古くなったと判断した場合は、プロビジョニング中に利用できないようにこのポリシーを無効にすることができます。

承認ポリシーを無効にするには、承認ポリシーが現在適用されている各資格に新しいポリシーを割り当てる必要があります。

無効化した承認ポリシーを後で再アクティブ化したり、無効化したポリシーを削除したりできます。

前提条件

テナント管理者または承認管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [承認ポリシー] を選択します。
- 2 承認ポリシー名をクリックします。
- 3 [リンクされた資格の表示] をクリックします。
 - a [すべて次に置換] ドロップダウン メニューで、新しい承認ポリシーを選択します。
リストに複数の資格が含まれている場合、新しい承認ポリシーはすべての一覧表示された資格に適用されません。
 - b [OK] をクリックします。
- 4 承認ポリシーにリンクされた資格がないことを確認したら、[ステータス] ドロップダウン メニューから [無効] を選択します。
- 5 [OK] をクリックします。

6 承認ポリシーを削除するには、無効化したポリシーを含む行を選択します。

- a [削除] をクリックします。
- b [OK] をクリックします。

結果

承認ポリシーを使用し、このポリシーを無効にした資格から、承認ポリシーのリンクが解除されます。後で再アクティブ化して、資格内のアイテムに再度適用することができます。

次のステップ

この承認ポリシーがもう必要ない場合は、削除することができます。[承認ポリシーの削除](#)を参照してください。

承認ポリシーの削除

無効化した不要な承認ポリシーがある場合は、vRealize Automation から削除することができます。

前提条件

- 承認ポリシーをリンク解除および無効します。[承認ポリシーの無効化](#)を参照してください。
- テナント管理者または承認管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [承認ポリシー] を選択します。
- 2 無効なポリシーを含む行を選択します。
- 3 [削除] をクリックします。
- 4 [OK] をクリックします。

結果

承認ポリシーを削除します。

シナリオ：MySQL を搭載した CentOS の承認ポリシーを作成および適用する

開発と品質管理のビジネス グループのテナント管理者として、カタログ アイテム申請を厳しく制御したいと考えています。ユーザーが、MySQL を搭載した CentOS カタログ アイテムをプロビジョニングする前に、vSphere 仮想インフラストラクチャの管理者がマシン申請を承認し、ソフトウェア マネージャがソフトウェア申請を承認できるようにします。

vSphere MySQL 搭載 CentOS サービス カタログ申請の承認ポリシー（vSphere 仮想インフラストラクチャ管理者が詳細な条件に基づいてマシンを承認するのに必要）と、MySQL ソフトウェア コンポーネントの承認ポリシー（ソフトウェア管理者が申請ごとに承認するのに必要）を作成して適用します。

承認管理者は承認を作成することだけができ、承認を資格に適用できるのはビジネス グループ マネージャです。テナント管理者として、承認の作成と資格への適用の両方を行うことができます。

前提条件


- テナント管理者として vRealize Automation コンソールにログインします。承認ポリシーの作成と適用の両方を行えるのは、テナント管理者のみです。
- MySQL 搭載 CentOS カタログ アイテムがサービスに含まれていることを確認します。[シナリオ：MySQL を搭載した CentOS アプリケーション ブループリントをサービス カタログで利用できるようにする](#)を参照してください。

シナリオ：MySQL 搭載 CentOS 仮想マシン承認ポリシーを作成する


テナント管理者として、環境内に適切にプロビジョニングした仮想マシンを確実に開発と品質管理グループに渡したいと考えています。そのために特定の種類の申請の事前承認を必要とする承認ポリシーを作成します。


MySQL 搭載 CentOS 仮想マシンは vCenter Server リソースを消費するので、2048 MB を超えるメモリまたは 3 つ以上の CPU が申請されたときにリソースが適切に消費されるように、vSphere 仮想インフラストラクチャの管理者が申請を承認するようにします。また、申請の承認前に、申請された CPU とメモリの値を変更する機能も承認者に付与します。

手順

- 1 [管理] - [承認ポリシー] を選択します。
- 2 仮想マシン プロビジョニングの承認ポリシーを作成します。
 - a [新規] アイコン () をクリックします。
 - b [承認ポリシーのタイプを選択] を選択します。
 - c リストで、[サービス カタログ - カatalog アイテム申請 - 仮想マシン] を選択します。
 - d [OK] をクリックします。
 - e 次のオプションを構成します。

オプション	構成
名前	CentOS on vSphere CPU or Memory VM と入力します。
説明	Requires VI Admin approval for CPU>2 or Memory>2048 と入力します。
ステータス	[有効] を選択します。

- 3 [事前承認] タブで [追加] アイコン () をクリックします。
- 4 トリガ基準と承認アクションを使用して [レベル情報] を構成します。
 - a [名前] テキスト ボックスに **CPU>2 or Memory>2048 – VI Admin** と入力します。
 - b [説明] テキスト ボックスに **VI Admin approval for CPU and Memory** と入力します。
 - c [条件に応じて必要] を選択します。
 - d [条件節] ドロップダウン リストで、[次のいずれか] を選択します。
 - e 新しい [条件節] ドロップダウン リストで、[CPU] を選択し、条件節の値を [CPU > 2] と構成します。

- f [式の追加] をクリックし、条件節の値を **Memory (MB) > 2048** と構成します。
- g [特定のユーザーおよびグループ] を選択します。
- h 検索テキスト ボックスに、vSphere 仮想インフラストラクチャの管理者または管理者グループの名前を入力し、検索アイコン () をクリックします。
- i ユーザーまたはグループを選択します。
- j [誰でも承認できる] を選択します。

申請に必要なのは 1 人の仮想インフラストラクチャの管理者のみで、リソースを確認して申請を承認します。

- 5 [システム プロパティ] タブをクリックし、承認者が申請を承認する前に、申請された CPU とメモリの値を変更できるようにプロパティを選択します。
 - a [CPU] および [メモリ (MB)] のチェック ボックスを選択します。
 - b [OK] をクリックします。
- 6 [OK] をクリックします。

結果


仮想マシン申請の承認ポリシーを作成しましたが、MySQL コンポーネントの承認も作成したいと考えています。ポリシーを資格に適用するまで、トリガされる承認はありません。

シナリオ： CentOS 用の MySQL ソフトウェア コンポーネントの承認ポリシーを作成する

テナント管理者として、ライセンス使用量を追跡できるように MySQL インストールに対する承認ポリシーの作成と適用を、ソフトウェア マネージャから依頼されました。Linux 仮想マシン 用 MySQL ソフトウェア コンポーネントが申請されるたびに、ソフトウェア ライセンス マネージャに通知するポリシーを作成します。


一部の環境では、ソフトウェア マネージャがライセンス キーをプロビジョニングする必要があるため、このタイプの承認が必要になる場合があります。このシナリオで、ソフトウェア マネージャは申請の追跡と承認のみを実行する必要があります。承認ポリシーの作成後、Linux 仮想マシン用 MySQL カタログ アイテムにこのポリシーを適用します。この承認ポリシーは限定的であるため、資格内の Linux 仮想マシン用 MySQL ソフトウェア コンポーネントにのみ適用できます。

手順


- 1 [管理] - [承認ポリシー] を選択します。
- 2 MySQL ソフトウェア コンポーネントの承認ポリシーを作成します。
 - a [新規] アイコン () をクリックします。
 - b [アイテムを選択] を選択します。
 - c [Linux 仮想マシン用 MySQL] を選択します。

- d [OK] をクリックします。
- e 次のオプションを構成します。

オプション	構成
名前	MySQL tracking approval と入力します。
説明	Approval request sent to software manager と入力します。
ステータス	[有効] を選択します。

3 [事前承認] タブで [追加] アイコン () をクリックします。

4 トリガ基準と承認アクションを使用して [レベル情報] を構成します。

- a [名前] テキスト ボックスに **MySQL software deployment notice** と入力します。
- b [説明] テキスト ボックスに **Software mgr approval of software installation** と入力します。
- c [常に必要] を選択します。
- d [特定のユーザーおよびグループ] を選択します。
- e 検索テキスト ボックスでソフトウェア マネージャの名前を入力し、検索アイコン () をクリックしてユーザーを選択します。
- f [誰でも承認できる] を選択します。

申請の承認に必要なソフトウェア マネージャは 1 人のみです。

[OK] をクリックします。

5 [OK] をクリックします。

結果

仮想マシンの承認ポリシーと Linux 仮想マシン用 MySQL ソフトウェア コンポーネントの承認ポリシーが作成されました。承認ポリシーを資格に適用するまで、トリガされる承認はありません。

シナリオ：MySQL を搭載した CentOS コンポーネントに承認ポリシーを適用する

テナント管理者として、承認ポリシーおよび資格を作成できます。開発および品質の資格を変更すると、サービス カタログ ユーザーが承認を要求する際にトリガされるように作成した承認ポリシーを適用することができます。

ビジネス グループにカタログ サービス全体の使用資格を付与することは難しくありませんが、カタログ アイテムの個別の資格を作成する場合と同様の制御およびガバナンスは提供されません。たとえば、ユーザーにサービスの使用資格を付与した場合、ユーザーはサービス内のあらゆるカタログ アイテムとこのサービスに今後追加されるすべてのアイテムを申請できます。つまり、マネージャの承認を常に必要とするなど、サービス内のカタログ アイテムごとに適用される非常に高レベルの承認ポリシーのみを使用することもできます。カタログ アイテムの使用資格を個別に付与した場合は、各アイテムに固有の承認ポリシーを作成して適用し、サービス内でどのアイテムを誰が申請できるかを厳密に管理できます。各カタログ アイテムに個別のコンポーネントの使用資格を付与した場合は、さらに細かく管理できます。


資格に含まれるアイテムに適用する承認ポリシーが不明な場合は、後でこの手順に戻って適用することができます。このシナリオでは、発行済みの 1 つのアプリケーション ブループリントの 2 つのコンポーネントに、異なる承認ポリシーを適用します。

手順

- 1 [管理] - [カタログ管理] - [資格] を選択します。
- 2 [Dev and QE Entitlement (開発および品質管理の資格)] をクリックします。
- 3 [アイテムと承認] タブをクリックします。
- 4 MySQL を搭載した CentOS マシンを追加して、承認ポリシーを適用します。
 - a [使用可能なアイテム] 見出しの横にある [アイテムの追加] アイコン (✚) をクリックします。
 - b [MySQL を搭載した CentOS] チェック ボックスを選択します。
 - c [選択したアイテムにこのポリシーを適用] ドロップダウンの矢印をクリックします。
vSphere 上の CentOS の CPU とメモリはリストに表示されません。
 - d [すべて表示] をクリックして下矢印をクリックして、すべての承認ポリシーを表示します。
 - e [vSphere 上の CentOS の CPU] と[メモリ [サービス カタログ - カタログ アイテム申請 - 仮想マシン]] を選択します。
vSphere CentOS マシンはアプリケーション ブループリント内のマシン ブループリントです。カタログ アイテム タイプに最適なポリシーを選択できるように、ポリシー名を確認します。ポリシーを誤って適用した場合は、この承認ポリシーが失敗するか、不正な条件に基づく承認申請がトリガされます。
 - f [OK] をクリックします。
- 5 MySQL for Linux Virtual Machine ソフトウェア コンポーネントをアイテムとして追加し、MySQL アイテムに承認ポリシーを適用します。
 - a [使用可能なカタログ アイテムおよびコンポーネント] 見出しの横にある [カタログ アイテムおよびコンポーネントの追加] アイコン (✚) をクリックします。
 - b [カタログ アイテムおよびコンポーネント] ドロップダウン メニューで [いいえ] を選択します。
ソフトウェア コンポーネントは常にマシンと関連付けられます。サービス カタログでの個別の要求に対しては使用できるようになりません。
 - c [MySQL for Linux Virtual Machines] チェック ボックスを選択します。
 - d [選択したアイテムにこのポリシーを適用] ドロップダウンの矢印をクリックします。
 - e [MySQL トラッキング承認 [サービス カタログ - カタログ アイテム申請 - ソフトウェア コンポーネント]] を選択します。
承認ポリシーはこの特定のソフトウェア コンポーネントに対して作成されており、仮想マシンに追加されるため、詳細なオプションは必要ありません。
 - f [OK] をクリックします。

6 プロビジョニング済みのマシンでユーザーが実行できるアクションを追加します。

このシナリオでは、承認ポリシーをアクションに適用しません。

- a [使用可能なアクション] 見出しの横にある [アクションの追加] アイコン () をクリックします。
- b 次のアクションを選択します。

名前/タイプ	説明
スナップショットの作成/仮想マシン	仮想マシンのスナップショットを作成します。その際、インストール済みのソフトウェアも含められます。開発者はスナップショットを作成し、開発中にその状態に戻すことができます。
破棄/展開	マシンだけでなく、プロビジョニングされたブループリント全体を破棄します。このアクションは、孤立したコンポーネントが発生するのを避けるために使用します。
パワーオフ/マシン	仮想マシンをオフにします。
パワーオン/マシン	仮想マシンをオンにします。
スナップショットまで戻る/仮想マシン	以前に作成したスナップショットに戻ります。

- c [OK] をクリックします。

7 [完了] をクリックします。

結果

この資格により、異なるブループリント コンポーネントに別の承認を求めることが可能になります。

次のステップ

ビジネス グループのメンバーとして、サービス カタログ内の MySQL を搭載した CentOS アイテムを要求して、資格と承認が期待通りに機能していることを確認します。

パラメータ化されたブループリントを使用したマシン プロビジョニングの申請

サイズまたはイメージ コンポーネントのプロファイルを含むように設計された vSphere マシン ブループリントのマシン プロビジョニングを申請する際には、使用可能な値セットを選択してプロビジョニング設定を指定します。

プロビジョニングの申請時に、使用可能な Size および Image オプションの中から選択することができます。1つの値セットを選択すると、対応するプロパティ値がその申請にバインドされます。

コンポーネント プロファイルの値セットは、クラスタ内のすべての vSphere マシンに適用されます。

コンポーネント プロファイルの構成については、[ブループリントのパラメータ化について](#)を参照してください。

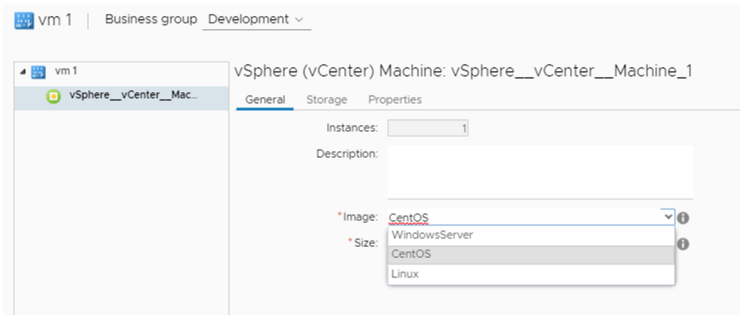
前提条件

- Size または Image コンポーネント プロファイル用の値セットを定義します。『カスタム プロパティのリファレンス』の「[およびを参照してください](#)」。
- Image または Size コンポーネント プロファイルを持つ vSphere マシン コンポーネントを含むブループリントを作成します。[マシンのブループリントの設定](#)および [vSphere マシン コンポーネントの設定](#)を参照してください。

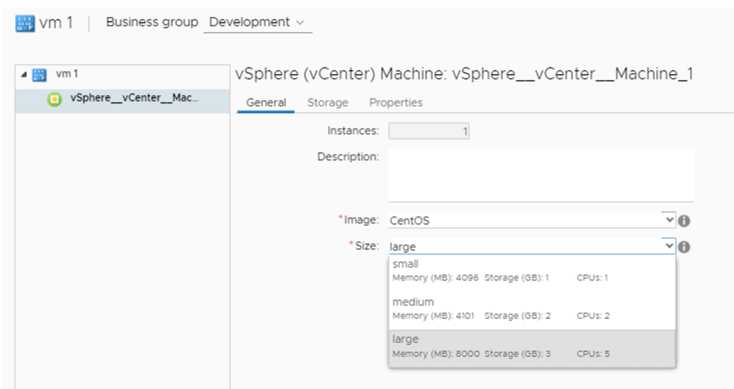
- カタログにブループリントを公開します。[ブループリントの公開](#)を参照してください。
- カatalog内のブループリントを構成します。[サービス カatalog構成用のチェックリスト](#)および[仮想マシン ポリシー タイプに基づく承認ポリシーの例](#)を参照してください。

手順

- 1 [カタログ] をクリックします。
- 2 申請するカタログ サービスを選択し、[申請] をクリックします。
- 3 プロビジョニングする vSphere マシン コンポーネントを選択し、プロビジョニングするインスタンスの数を指定します。
- 4 [イメージ] ドロップダウン メニューからイメージの値セット オプションを選択します。



- 5 [サイズ] ドロップダウン メニューからサイズの値セット オプションを選択します。



- 6 [送信] をクリックします。

次のステップ

Size および Image コンポーネント プロファイル用に定義した値セットは、カタログ プロビジョニング申請フォームの [カタログ] タブにある [イメージ] および [サイズ] ドロップダウン メニューで使用できます。

シナリオ：MySQL を搭載した CentOS アプリケーション ブループリントをサービス カatalogで利用できるようにする

開発と品質管理グループがテスト ケースを実行できるように、テナント管理者として、ブループリント アーキテクトが CentOS に MySQL 用のカタログ アイテムを作成するように申請しました。ソフトウェア アーキテクトは、ユーザー用のカタログ アイテムの準備が整ったことを通知していました。ビジネス ユーザーがアイテムを利用でき

ようにするには、ブループリントと ソフトウェア コンポーネントをカタログ サービスと関連付け、カタログ アイテムの申請資格をビジネス グループ メンバーに付与する必要があります。

前提条件

- テナント管理者またはカタログ管理者として vRealize Automation にログインします。
- MySQL のブループリントを vSphere CentOS 仮想マシンに公開します。[デザイン ライブラリの作成](#) でマシンおよびソフトウェア コンポーネントのブループリントを作成するプロセスを参照してください。
- ブループリントを開発環境で作成する場合は、ブループリントを本番環境にインポートします。[ブループリントとコンテンツのエクスポートおよびインポート](#)を参照してください。
- 予約を作成し、vSphere リソースを開発と品質管理ビジネス グループに割り当てます。[Hyper-V、KVM、SCVMM、vSphere、XenServer の予約の作成](#)を参照してください。

手順

1 シナリオ：開発と品質管理カタログ サービスを作成する

テナント管理者として、開発と品質管理グループのカタログ サービスを個別に作成することで、専用のカタログ アイテムが財務や人事などの他のグループに表示されないようにしたいと考えています。Dev and QE Service というカタログ サービスを作成し、開発と品質管理が必要とするすべてのカタログ アイテムを公開して、テスト ケースを実行します。

2 シナリオ：開発と品質管理サービスに MySQL を搭載した CentOS を追加する

テナント管理者として、開発と品質管理サービスに MySQL カatalog アイテムを搭載した CentOS を追加したいと考えています。


3 シナリオ：ユーザーに開発および品質管理サービス アイテムをカタログ アイテムとして申請する資格を付与する

テナント管理者として、開発および品質管理の資格を作成し、カタログ アイテムといくつかの関連アクションを追加して、開発と品質管理のユーザーが、MySQL を搭載した CentOS カatalog アイテムを申請し、マシンと展開に対してアクションを実行できるようにします。

シナリオ：開発と品質管理カタログ サービスを作成する

テナント管理者として、開発と品質管理グループのカタログ サービスを個別に作成することで、専用のカタログ アイテムが財務や人事などの他のグループに表示されないようにしたいと考えています。Dev and QE Service というカタログ サービスを作成し、開発と品質管理が必要とするすべてのカタログ アイテムを公開して、テスト ケースを実行します。

手順

- 1 [管理] - [カタログ管理] - [サービス] を選択します。
- 2 [新規] アイコン () をクリックします。
- 3 [名前] テキスト ボックスに **Dev and QE Service** と入力します。
- 4 [説明] テキスト ボックスに **Dev and QE application catalog items for test cases** という説明を入力します。

- 5 [ステータス] ドロップダウン メニューから [有効] を選択します。
- 6 サービスを作成するカタログ管理者として、検索オプションを使用し、[所有者] に名前を追加します。
- 7 サポート チームというカスタム ユーザー グループを追加します。

たとえば、カタログ アイテムのプロビジョニング時に問題が発生した場合、ユーザーやサービス カatalog ユーザーが問い合わせできるように、IaaS アーキテクトとソフトウェア アーキテクトを含むカスタム ユーザー グループを追加します。

- 8 [OK] をクリックします。

結果

開発と品質管理カタログ サービスの作成と有効化が完了しました。カタログ アイテムはまだ含まれていません。

シナリオ：開発と品質管理サービスに MySQL を搭載した CentOS を追加する

テナント管理者として、開発と品質管理サービスに MySQL カatalog アイテムを搭載した CentOS を追加したいと考えています。

手順

- 1 [管理] - [Catalog管理] - [サービス] を選択します。
- 2 [サービス] リストで開発と品質管理サービス行を選択し、[Catalog アイテムの管理] をクリックします。
- 3 [新規] アイコン (+) をクリックします。
- 4 [MySQL を搭載した CentOS] を選択します。

サービスとはまだ関連付けられていない公開済みのブループリントおよびコンポーネントのみがリストに表示されます。ブループリントが表示されない場合は、ブループリントが公開されているか、または別のサービスに含まれていないかを確認します。

- 5 [OK] をクリックします。
- 6 [閉じる] をクリックします。

結果

開発と品質管理サービスに MySQL カatalog アイテムを搭載した CentOS を公開しました。ユーザーにアイテムまたはサービスの使用資格を付与するまでは、誰もアイテムを表示または申請できません。

シナリオ：ユーザーに開発および品質管理サービス アイテムをCatalog アイテムとして申請する資格を付与する

テナント管理者として、開発および品質管理の資格を作成し、Catalog アイテムといくつかの関連アクションを追加して、開発と品質管理のユーザーが、MySQL を搭載した CentOS カatalog アイテムを申請し、マシンと展開に対してアクションを実行できるようにします。

このシナリオでは、このサービスに今後追加されるCatalog アイテムを使用できるように、ユーザーにサービスの使用資格を付与します。また、ユーザーがプロビジョニングされた展開を管理できるようにするため、パワーオンとパワーオフ、スナップショット、資格に対する展開の破棄などのアクションを追加します。

手順

1 [管理] - [カタログ管理] - [資格] を選択します。

2 [新規] アイコン（）をクリックします。

3 詳細を構成します。


- a [名前] テキスト ボックスの **Dev and QE Entitlement** という名前を入力します。
- b [ステータス] ドロップダウン メニューで [有効] を選択します。
- c [ビジネス グループ] ドロップダウン メニューで [開発と品質管理] グループを選択します。
- d [ユーザーおよびグループ] 領域で、1 人以上のユーザーを追加します。

ブループリントが予測どおり機能していることを確認できない場合には、自分自身のみを追加します。正常に機能している場合は、個別のユーザーを追加できるため、カスタム ユーザー グループも追加できます。

e [次へ] をクリックします。


4 サービスを追加します。

CentOS と MySQL のカタログ アイテムを個別に追加しても、サービスを追加することで、サービス カタログ内のビジネス グループ メンバーが、サービスに後日追加される追加アイテムを利用できるようになります。

- a [使用可能なサービス] 見出しの横にある [サービスの追加] アイコン（）をクリックします。
- b [開発と品質管理サービス] を選択します。
- c [OK] をクリックします。

開発と品質管理サービスが [使用可能なサービス] リストに追加されます。

5 アクションを追加します。

- a [使用可能なアクション] 見出しの横にある [アクションの追加] アイコン（）をクリックします。
- b [タイプ] 列ヘッダをクリックしてリストをソートします。

タイプに基づいて次のアクションを選択します。これらのアクションは、開発と品質管理のユーザーがテスト ケース マシンを使用する場合に役立ち、これらのビジネス グループ メンバーが使用できる唯一のアクションです。

ファイルタイプ	アクション名
マシン	パワーオン
マシン	パワーオフ
仮想マシン	スナップショットの作成
仮想マシン	スナップショットまで戻る
展開	削除
展開の破棄アクションは、仮想マシンだけでなく、展開全体を破棄します。	

c [OK] をクリックします。

5 つのアクションが [使用可能なアクション] リストに追加されます。

6 [終了] をクリックします。

結果

MySQL を搭載した CentOS カタログ アイテムが新しい開発と品質管理カタログ サービスに追加され、ビジネスグループ メンバーにアイテムの申請と管理の使用資格が付与されました。

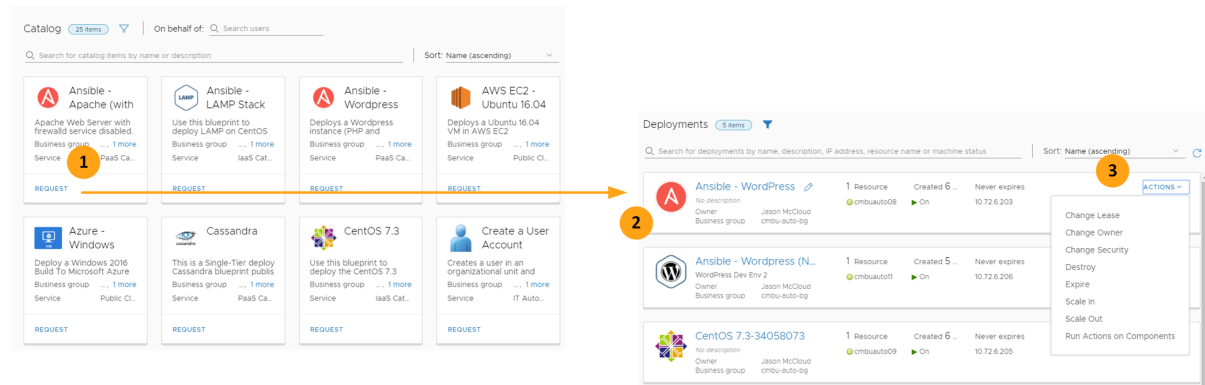
次のステップ

MySQL を搭載した CentOS カタログ アイテムをプロビジョニングして動作を確認したら、資格にユーザーを追加し、開発と品質管理のユーザーにカタログ アイテムを一般公開することができます。資格内のリソースのプロビジョニングを細かく制御する場合は、MySQL ソフトウェア コンポーネントおよびソフトウェア テスト用 CentOS マシン向けの承認ポリシーを作成できます。[シナリオ：MySQL を搭載した CentOS の承認ポリシーを作成および適用する](#)を参照してください。

カタログの使用と導入環境の管理

4

カタログは利用可能なブループリントで、導入環境はプロビジョニングされたブループリントです。管理者はカタログ アイテムを提供します。ユーザーはリソースを展開として要求および管理できます。導入環境の管理の一環として、変更のためのアクションを実行することができます。



次のワークフローはカタログから開始します。

- 1 カタログ内のアイテムを要求します。カタログには、自分がメンバーであるビジネス グループが使用資格を持つ公開されたブループリントが含まれています。
- 2 プロビジョニングしたリソースを導入環境として管理します。プロビジョニング プロセスを監視し、導入環境を管理し、導入環境上でアクションを実行できます。
- 3 アクションを使用して、展開後の導入環境を変更します。たとえば、メモリを増やしたり、CPU を減らしたり、不要になった導入環境を破棄したりするなどのアクションがあります。

この章には、次のトピックが含まれています。

- [カタログの操作](#)
- [展開の操作](#)
- [受信箱の操作](#)

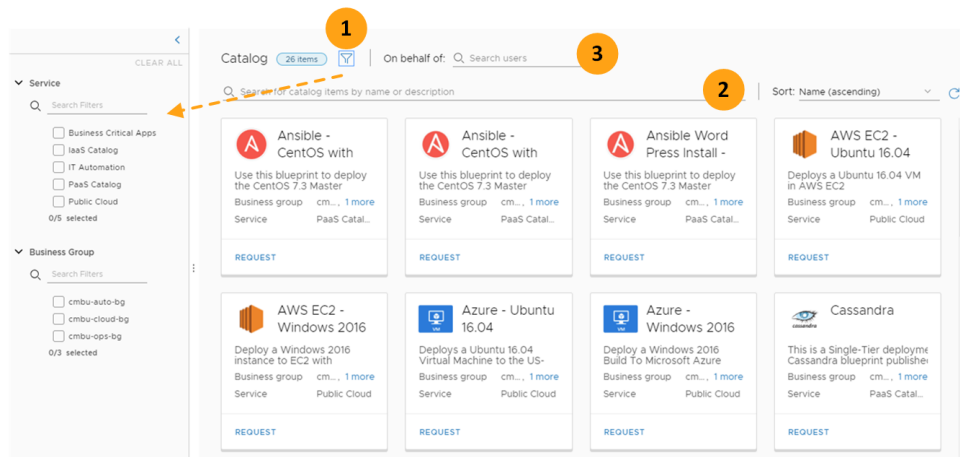
カタログの操作

カタログとは、展開可能なブループリントのリストです。ブループリント アーキテクトは、コンポーネントの設計、アイテムを申請するときに選択できるカスタム オプション、ブループリントが組織の vRealize Automation エンドポイントに基づいて展開される場所を決定します。

使用可能なカタログ アイテムは、1 つまたは複数のビジネス グループでのメンバーシップと、そのビジネス グループに、ブループリントをプロビジョニングする資格がどのように与えられているかに基づいて決まります。

カタログ アイテムの検索

この例では、小さいカタログを使用します。大規模なエンタープライズ環境では、1 ページを超えるカタログになることもあります。

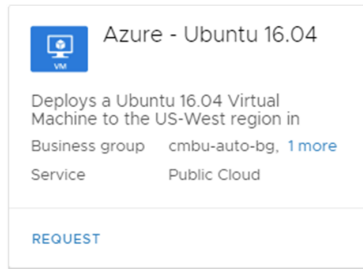


次のオプションを使用して、展開するブループリントを見つけます。

- 1 サービスとビジネス グループに基づいて、リストに [フィルタ] を適用します。
- 2 [検索] および [ソート] を使用してカタログ アイテムを検索し、編成します。
- 3 [代理] でユーザーを選択してカタログ アイテムの数を制限し、そのユーザーの代わりにアイテムを申請します。展開できるブループリントは、ユーザーがメンバーになっているビジネス グループが資格を付与されているものに限定されます。ユーザー名を選択すると、使用可能なカタログ アイテムのリストに、そのユーザーのメンバーシップが反映されます。権限の代わりに管理者、ビジネス グループ管理者が使用でき、ビジネス グループを構成するときに 1 つ以上のビジネス グループ メンバーに割り当てることができます。 [ビジネス グループの作成](#) を参照してください。

カタログ カード

カタログ カードは、単一のマシンまたはアプリケーション全体を展開するブループリントを表します。また、別の方法でプロビジョニングする XaaS ワークフローを表す場合もあります。たとえば、ユーザーを Active Directory に追加します。



カードに含まれる情報は、カタログ アイテムを要求する資格が付与されているビジネス グループ、アイテムが関連付けられているサービスなどです。

カタログ申請を送信する方法

カタログ申請を送信する際、申請フォームはブループリントによって異なる可能性があります。フォーム間の相違は、ブループリント デザインで設定されます。

フォームのバリエーションは、申請をカスタマイズできる程度によって異なります。申請をカスタマイズするために選択できるオプションが複数与えられる場合も、まったくオプションが与えられない場合もあります。

たとえば、ブループリント アーキテクトはブループリントを設計し、CPU の具体的な数を選択できたり、あらかじめ決められている CPU の数を大、中、小から選択できる場合があります。または、制限の多いブループリントにして、送信する前にブループリントに変更を加えることを一切許可しない場合も考えられます。

申請が正常にプロビジョニングされると、展開されたワークロードやサービスを管理できるようになります。

前提条件

- 1 つまたは複数のカタログ アイテムに対する資格が付与されているビジネス グループのメンバーである必要があります。[資格の作成](#)を参照してください。
- 別のユーザーに代わって展開する場合は、そのビジネス グループ内でサポート ロールが割り当てられている必要があります。[ビジネス グループの作成](#)を参照してください。

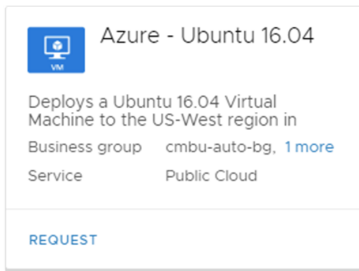
手順

- 1 [カタログ] をクリックします。
- 2 1 つまたは複数のビジネス グループでサポート ロールが割り当てられ、他のグループ メンバーの代わりに展開する場合は、[代理] 検索領域にユーザーまたはカスタム グループの名前を入力します。

カタログ アイテムのリストは、ここで選択したユーザーまたはグループがメンバーになっているビジネス グループに資格を与えられているアイテムに限定されます。

ユーザーを選択しないと、申請は本人のものとして送信されます。

- 3 検索とソートのオプションを使用して、展開するアイテムを特定し、[申請] をクリックします。



Azure - Ubuntu 16.04

Deploys a Ubuntu 16.04 Virtual Machine to the US-West region in

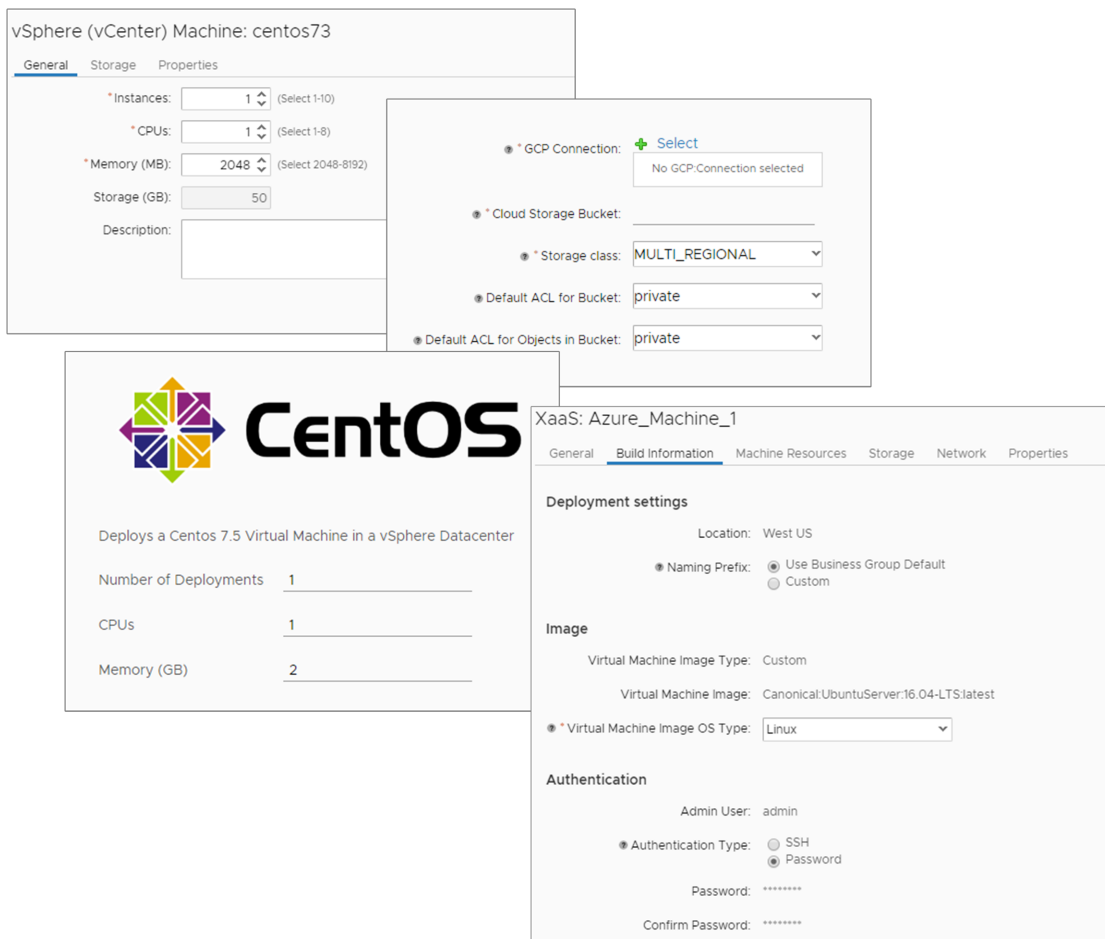
Business group cmbu-auto-bg, [1 more](#)

Service Public Cloud

[REQUEST](#)

- 4 ブループリントに対する資格が付与されている複数のビジネス グループのメンバーである場合は、展開に関連付けるビジネス グループを選択します。
- 5 申請フォームで、必須のオプションと使用可能なオプションを設定します。

ブループリントの設定方法に応じてフォームが異なる場合があります。単純なものから複数のタブを持つ複雑なものまで、いくつかの例を示します。



vSphere (vCenter) Machine: centos73

General Storage Properties

* Instances: 1 (Select 1-10)

* CPUs: 1 (Select 1-8)

* Memory (MB): 2048 (Select 2048-8192)

Storage (GB): 50

Description:

* GCP Connection: [Select](#)
No GCP Connection selected

* Cloud Storage Bucket:

* Storage class: MULTI_REGIONAL

* Default ACL for Bucket: private

* Default ACL for Objects in Bucket: private

XaaS: Azure_Machine_1

General Build Information Machine Resources Storage Network Properties

Deployment settings

Location: West US

* Naming Prefix: ☒ Use Business Group Default ☐ Custom

Image

Virtual Machine Image Type: Custom

Virtual Machine Image: Canonical:UbuntuServer:16.04-LTS:latest

* Virtual Machine Image OS Type: Linux

Authentication

Admin User: admin

* Authentication Type: ☐ SSH ☒ Password

Password: *****

Confirm Password: *****

- 6 [送信] をクリックします。

結果

プロビジョニングのために申請が送信され、[展開] タブが開いて、申請の進行状況を追跡できるようになります。

次のステップ

申請が展開されることを確認します。[プロビジョニング要求の監視](#)を参照してください。

展開の操作

展開は、カタログから要求したプロビジョニングされたブループリントです。プロビジョニング プロセスを通じて送信された要求のステータスを監視し、展開されたリソースを追跡し、アクションを使用してそれらの展開されたリソースを管理できます。

要求のステータスの監視

進行中の要求は [展開] タブに表示されます。カードを使用して、完了までのプロビジョニング プロセスを完了します。

プロビジョニング プロセスが失敗した場合は、エラー メッセージとイベントを確認し、要求が失敗した場所を特定して問題を解決できます。[失敗したプロビジョニング要求のテストおよびトラブルシューティング](#)を参照してください。

The screenshot shows the 'Deployments' tab with 1 item. A search bar is present with the text 'Search for deployments by name, description, IP address, resource name or machine status'. The sort option is 'Created Date (descending)'. The deployment card shows:

- Icon:** Red circle with a white 'A'.
- Title:** Ansible Word Press Install - PHP, MyS...
- Description:** No description
- Owner:** Jason McCloud
- Business group:** cmbu-auto-bg
- ID:** #287 - Provision Ansible Word Press Install - PHP, MySql all in one - In Progress
- Progress:** 14% (represented by a blue bar)
- Actions:** CANCEL
- Time:** 3 minutes since submitted

展開済みリソースの管理

要求は [展開] タブで管理します。

管理には、展開がオンになっていることの確認も含まれます。また、展開をスケール インまたはスケール アウトし、ニーズに合わせて変更する場合があります。または、展開の詳細を確認することもできます。詳細については、[展開されたカタログ アイテムの管理](#)を参照してください。

プロビジョニング要求の監視

展開を使用して、カタログで行った要求の進行状況を監視します。リソースが正常にプロビジョニングされている場合は、展開されたリソースも管理できます。

進行中の要求が表示されない場合は、要求が送信されなかったか、すでに完了しています。

要求の監視

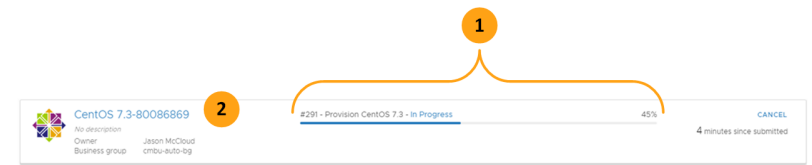
カタログ要求を監視するには、[展開] を選択します。

展開リストで要求のステータスを追跡します。

- 1 展開カード (1) で要求のステータスを追跡します。始めてカタログアイテムが要求された場合は、ステータスバーの進行状況にはパーセントが表示されません。最初の展開後は、後続の要求によって計算された進行状況がパーセントで表示されます。

展開されたリソースに対してアクションを実行すると、ステータスバーには選択した変更のステータスが示されます。

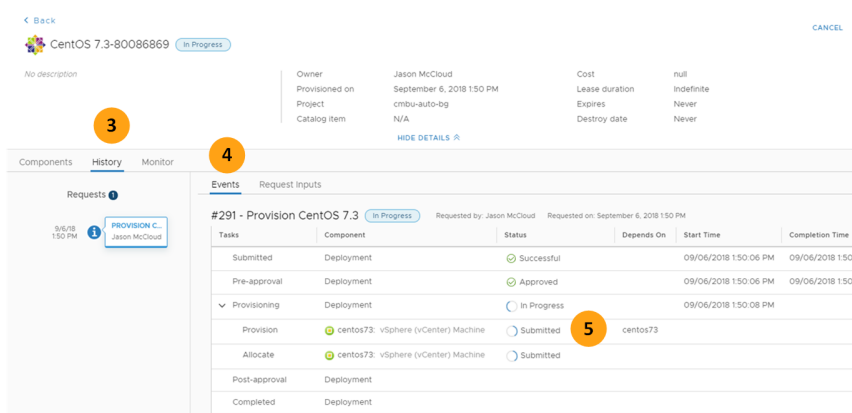
- 2 進行中の詳細を表示するには、展開のステータスバー (1) または展開名 (2) をクリックします。



展開中のプロビジョニングの詳細を確認します。

- 1 [履歴] タブ (3) には展開イベントと入力値が表示されます。
- 2 [イベント] タブ (4) にはプロビジョニング要求の詳細が表示されます。
- 3 プロビジョニングワークフロー (5) を確認して、現在どのコンポーネントが展開されているかを確認できます。

要求がプロビジョニングプロセスを完了しない場合は、[失敗したプロビジョニング要求のテストおよびトラブルシューティング](#)を参照してください。



処理中の要求のキャンセル

要求を送信し、その後でキャンセルすることを決定した場合、プロビジョニングプロセスは停止し、展開されたリソースはすべてロールバックされ、クリーンアップされます。

キャンセル処理に時間がかかる場合は、管理者に依頼して強制的にキャンセルすることができます。管理者は、キャンセル中の状態の要求をキャンセルすることができます。キャンセルを強制すると、ロールバックが完了しない場合があります。ターゲットシステムでリソースを手動でクリーンアップする必要があります。

失敗したカタログ申請のトラブルシューティング

カタログアイテムの要求はいくつかの理由で失敗することがあります。失敗の原因には、ネットワークトラフィック、エンドポイントリソースの不足、または欠陥のあるブループリントの仕様などが考えられます。または、プロビジョニングの要求は成功しても、展開が機能していないように見えることもあります。vRealize Automation を使用して展開を検証し、エラーメッセージを確認して、問題が解決可能な環境にあるかを判断できます。

vRealize Automation でのロールがカタログユーザーで、管理者権限を持っていない場合、このワークフローを使用して最初のトラブルシューティングを行うことができます。さらに詳細な調査を行うために、組織内の誰かの支援を必要とする場合があります。

失敗の状態

プロビジョニング要求が失敗すると、次のいずれかの状態が表示されます。

- [失敗しました。]要求はいくつかの理由で失敗する可能性があります。1つは、ターゲットのエンドポイントでリソースが不足している、ブループリントをサポートするための十分なリソースがない、ブループリントが不適切に設計されたために修正が必要である、などが原因でプロビジョニング プロセスが機能しなかった場合です。もう1つは、要求が組織内の誰かの承認を必要とし、承認者が要求を拒否した場合です。展開で実行したアクションが失敗した可能性もあります。失敗は、上で述べた環境または承認の理由によって引き起こされる可能性があります。

問題の原因を調査するには、次のトラブルシューティングのワークフローを使用します。問題を解決できる場合は、[破棄] および [再送信] に関するアクションのオプションを確認します。[プロビジョニングされたリソースのアクション メニュー コマンド](#)を参照してください。

- [部分的に成功。]要求は部分的に成功します。つまり、一部のコンポーネントは展開されますが、プロビジョニング手順の一部が正常に完了していません。

次のトラブルシューティングのワークフローを使用して、部分的に成功したコンポーネントを特定し、問題の原因を調査します。問題を解決できる場合は、[破棄] に関するアクションのオプション、および [再開] を使用できるかについて確認します。[プロビジョニングされたリソースのアクション メニュー コマンド](#)および[再開アクションの動作](#)を参照してください。

カタログ ユーザーのワークフローのトラブルシューティング

このワークフローを使用して、失敗した展開の調査を開始できます。調査によって失敗の原因が一時的な環境の問題であることが判明した場合は、エラーを解決して要求を再送信することができます。問題が要求の仕様にある場合は、ブループリント アーキテクトに連絡する必要があります。

表 4-1. エラーのトラブルシューティングを開始する方法

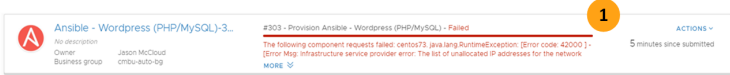
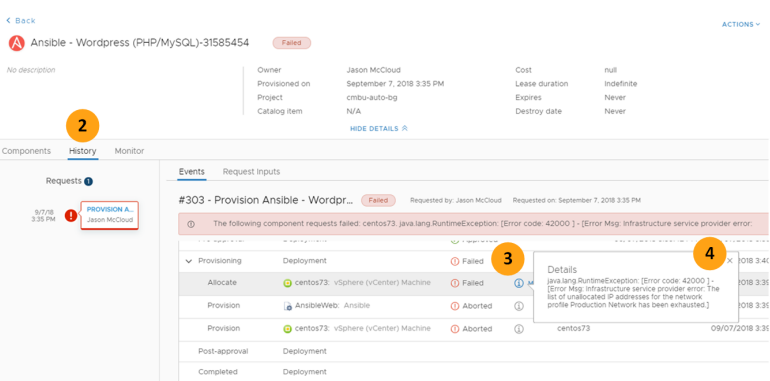
ワークフロー	トラブルシューティングの手順	例
1	[展開] タブでは、失敗した展開がステータス バーに表示されます。カードには最後の失敗メッセージが含まれています。詳細については、展開名または進行状況バーをクリックしてください。	
2	展開の詳細の [履歴] タブでは、イベント ワークフローを使用してプロビジョニング プロセスが失敗した場所を確認できます。このワークフローは、展開でアクションを実行し、変更が失敗した場合にも役に立ちます。	

表 4-1. エラーのトラブルシューティングを開始する方法（続き）

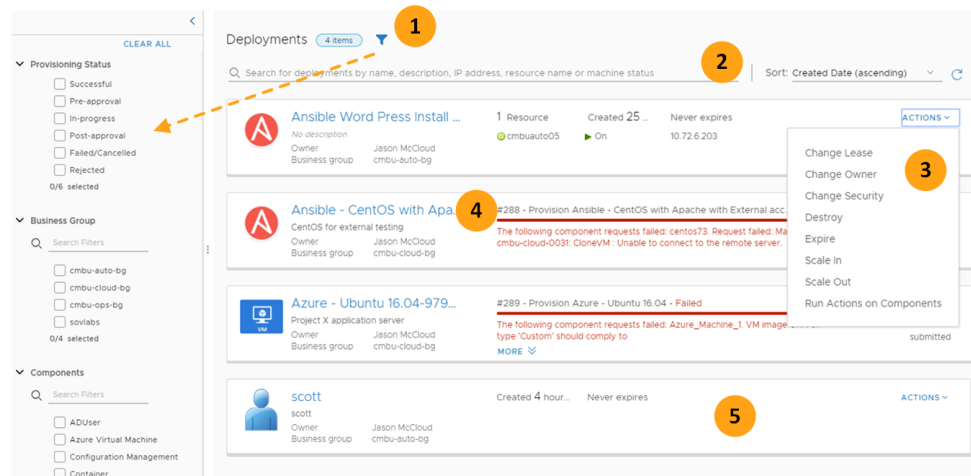
ワークフロー	トラブルシューティングの手順	例
3	失敗ステータスはワークフローが失敗した場所を示します。	
4	この情報は、エラー メッセージのより詳細なバージョンを提供します。 signpost のヘルプにあるこの情報では問題を特定して解決するのに不十分な場合は、イベント ログでさらに調査を行うことができます。 イベント ログを表示するには、ユーザー ロールが必要です。ブループリント アーキテクトまたは管理者は、追加のトラブルシューティングを行うことができます。 失敗したプロビジョニング要求のテストおよびトラブルシューティング を参照してください。	

展開されたカタログ アイテムの管理

展開の所有者または他のユーザーを支援する管理者は、展開の詳細を使用して展開されたアイテムのライフサイクルを管理できます。展開の詳細は、各コンポーネントに関する現在の情報を提供し、履歴を使用して時間の経過に伴う変化を追跡します。展開を操作する場合、アクションを使用して展開されたアイテムを変更できます。一部の変更はアクションを使用せずに実行することができます。

カードからの展開の管理

デプロイ カード リストは展開の概要を提供します。成功しましたか?実行していますか?



展開されたリソースを vRealize Automation から検索および管理するには、次のオプションを使用します。

- 1 要求の現在のステータス、展開先のビジネス グループ、含まれるサブコンポーネント、所有者ユーザー、およびプロビジョニングまたは有効期限の範囲に基づいて、リストを[フィルタ]します。[プロビジョニング ステータス]と[要求番号]フィルタは最初のプロビジョニング プロセスにのみ適用され、実行する可能性のある後続のアクションには適用されません。その他のフィルタは展開全般に適用されます。
- 2 [検索] および [並べ替え] を使用して展開を見つけ、編成します。
- 3 展開を管理するには、[アクション] をクリックして、使用資格のある展開レベルのアクションを実行します。個々のコンポーネントでアクションを実行するには、展開の詳細を開く必要があります。このアクションには、設計ブループリントが対象の標準的なアクション、または XaaS ブループリントを対象に作成されたカスタムの XaaS リソース アクションがあります。標準アクションの詳細については、[展開されたリソースに対するアクションの実行](#)を参照してください。
- 4 プロビジョニング イベント、履歴、およびコンポーネントレベルのアクションを含む展開の詳細を表示および管理するには、展開名をクリックします。上位 3 つは、標準のブループリントの初期プロビジョニング要求を表します。
- 5 また、ワークフローを実行する XaaS 展開要求を管理することもできます。ワークフローによって、リソースまたはワークフローが外部システムで実行されることがあります。この例では、XaaS はユーザーを Active Directory ドメインに追加しました。

展開の詳細を使用した環境の管理

展開の詳細を使用して、次の管理情報を実行します。

- [詳細。]カードで見つかった基本情報。展開名と説明を変更し、展開レベルのアクションを実行することもできます。
- [[コンポーネント] タブ。]各コンポーネントの完全な構成。コンポーネント レベルのアクションを実行することもできます。
- [履歴] タブ。展開に対する変更の完全な履歴。配置についての詳細情報と、変更ごとに提供された入力値についても確認できます。

- [監視 タブ。] vRealize Operations Manager と統合すると、展開およびコンポーネントの監視メトリック データとアラートが表示されます。
- [アクション。] 詳細を使用して、展開レベルのアクションまたはコンポーネントレベルのアクションを実行することもできます。

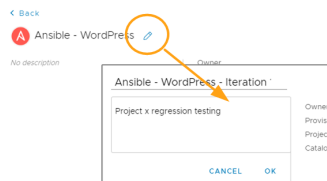
展開の詳細の使用

展開の詳細では、カード上で見つかった基本情報以外の情報を提供します。展開の名前と説明を変更し、展開とコンポーネントレベルのアクションを実行することもできます。

展開元のブループリントやコストなど、展開に関する基本情報を確認します。

展開名を変更します。

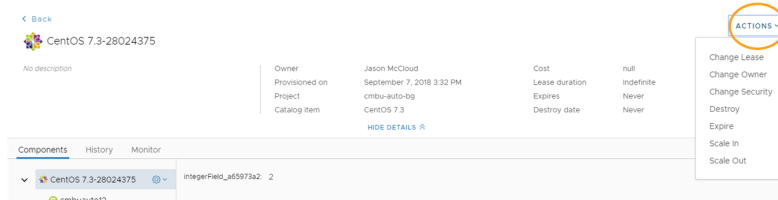
展開名にはブループリントの名前が使用されています。この名前は、対象の展開にとって意味をなさない場合があります。ニーズに合わせて名前と説明を更新できます。



- 1 名前をポイントし、鉛筆アイコンをクリックします。
- 2 名前と説明を意味のある内容に更新します。

展開レベルのアクションを実行する

展開レベルのアクションは、展開全体に影響を与える変更に限定されています。利用可能なアクションのリストは、ビジネス グループにアクションの使用資格がどのように付与されているかによって異なります。



展開コンポーネント

展開の詳細の [コンポーネント] タブには、すべての展開されたコンポーネントの完全な構成が表示されます。ここでは、マシンとネットワークがどのように構成されているかを確認できます。また、コンポーネントレベルのアクションを実行して構成を変更することもできます。

提供された展開を理解する必要がある場合、またはインスタンスの問題をトラブルシューティングする場合は、コンポーネントの詳細を確認してください。

アクションを使用して行った変更はすべて詳細に反映されます。

CentOS 7.3-28024375 In Progress

No description

Owner: Jason McCloud
Provisioned on: September 7, 2018 3:32 PM
Project: cmbu-auto-bg
Catalog item: CentOS 7.3

Cost: null
Lease duration: Indefinite
Expires: Never
Destroy date: Never

Components History Monitor

General Storage Network Security Properties

Name: cmbuauto12
Component: centos73
Status: On (CreateSnapshot)
CPU: 1
Memory (MB): 2048
Storage (GB): 50
Description: Provisioned by VMware vRA
Owner: jason@cmbu.local
Blueprint: CentOS 7.3
Compute resource: Cluster-1

Change Backup Jobs (Veeam)
Change Protection Jobs (Coh...
Change SLA Domain (Rubrik)
Execute Ansible Tower Job Te...
Instant Backup (Rubrik)
Instant Backup (VeeamZIP)
Manage Properties (SovLabs P...
Recover Files and Folders (Co...
Recover Files and Folders (Ru...
Recover Files and Folders (Ve...

コンポーネントレベルのアクションを実行する

コンポーネントレベルのアクションはコンポーネント固有です。利用可能なアクションは、ビジネス グループにアクションの使用資格がどのように付与されているかによって異なります。管理者がアクションを実行する権限を与えていない場合、歯車アイコンやアクション リストは表示されません。

展開の履歴

展開の詳細の [履歴] タブには、初期プロビジョニングから、1つ以上のアクションを使用して行った変更まで、展開の完全な履歴が含まれています。完全なプロビジョニング履歴を使用して、いつ変更が発生したか、どの値が提供されたかを知ることができます。

いつ変更が発生したか、またはいつインスタンスの問題を調査したかを確認する必要がある場合は、履歴の詳細を参照します。また、失敗した展開のトラブルシューティングを行う場合も履歴を使用します。[失敗したプロビジョニング要求のテストおよびトラブルシューティング](#)を参照してください。

CentOS 7.3-28024375 In Progress

No description

Owner: Jason McCloud
Provisioned on: September 7, 2018 3:32 PM
Project: cmbu-auto-bg
Catalog item: CentOS 7.3

Cost: null
Lease duration: Indefinite
Expires: Never
Destroy date: Never

Components **History** Monitor

Events Request Inputs

#316 - Create Snapshot cmbuauto12 In Progress Requested by: Jason McCloud Requested on: September 10, 2018 4:01 PM

Tasks	Component	Status	Depends On	Start Time	Completion Time
Submitted	Deployment	Successful		09/10/2018 4:01:09 PM	09/10/2018 4:01:09 PM
Pre-approval	Deployment	Approved		09/10/2018 4:01:09 PM	09/10/2018 4:01:09 PM
Create Snapshot	Deployment	In Progress		09/10/2018 4:01:11 PM	
Post-approval	Deployment				
Completed	Deployment				

REQUESTS

9/10/18 4:01 PM **CREATE SNA...** Jason McCloud

9/10/18 3:42 PM **REBOOT CMB...** Jason McCloud

9/7/18 3:32 PM **PROVISION C...** Jason McCloud

Machine Name: cmbuauto12
Snapshot name: cmbuauto12 (Monday, September 10, 2018 10:01:02 PM +00:00)
Snapshot description:
Include memory?: No

vRealize Operations Manager に基づく展開の監視

vRealize Automation では、展開に関する vRealize Operations Manager データを表示できます。

- 展開レベルのアラート
- マシン レベルのメトリック

フィルタリングされた一連のアラートとメトリックを vRealize Automation で直接確認すると、vRealize Operations Manager にアクセスしたり、そこで検索したりする必要がなくなります。その場合、vRealize Operations Manager のコンテキストに沿って起動することはできませんが、必要に応じて vRealize Operations Manager にログインして追加のデータを使用できます。

vRealize Operations Manager データの有効化

vRealize Automation で vRealize Operations Manager データを表示するには、最初にアダプタなどを設定する必要があります。

セットアップでは、vRealize Operations Manager と vRealize Automation の両方で手順を実行する必要があります。

前提条件

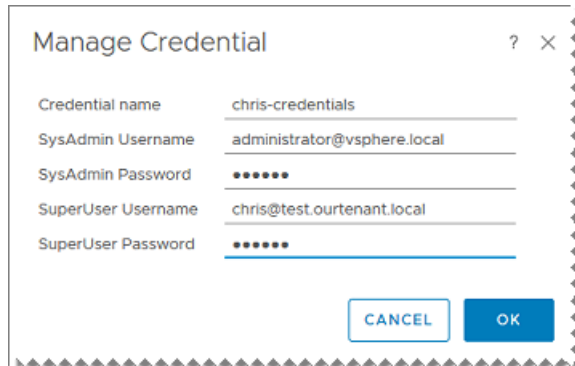
vRealize Operations Manager のバージョンが 6 以降であることを確認します。

手順

- 1 vRealize Operations Manager で、[管理] - [ソリューション] の順に移動します。
- 2 [ソリューション] で、[vRealize Automation ソリューション](#) があることと、それがデータを受信していることを確認します。
 - a vRealize Automation ソリューションを選択します。
 - b ソリューションの上にあるツールバーで、歯車の形をした [構成] アイコンをクリックします。

- c [インスタンスの設定] の [認証情報] に移動し、緑色のプラス記号をクリックして認証情報を追加します。

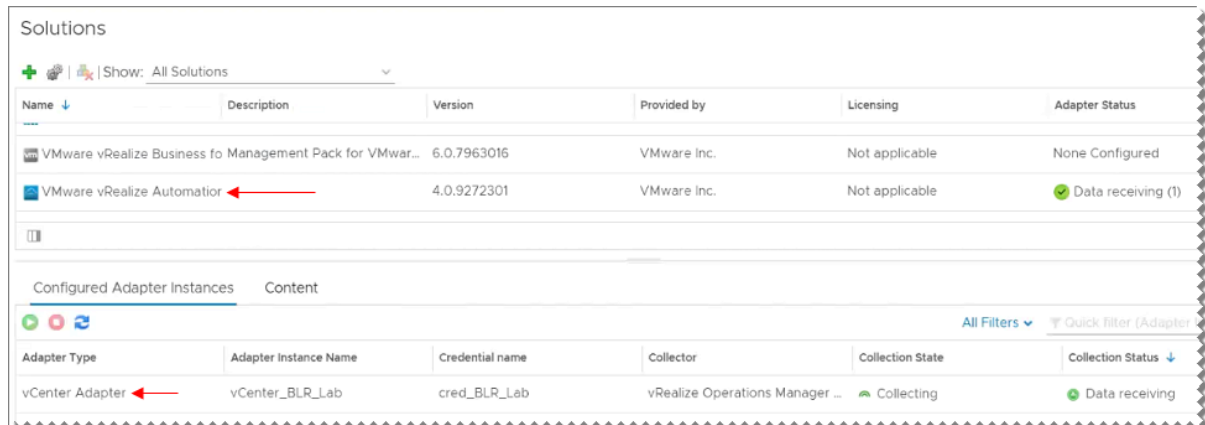
認証情報名	この認証情報のセットの説明
システム管理者	vRealize Automation のデフォルト テナント管理者（通常は administrator@vsphere.local）のユーザー名およびパスワード。
スーパー ユーザー	vRealize Automation 作業テナントに対して高度なアクセス権限を持つアカウントのユーザー名およびパスワード。



- d 認証情報を保存し、適切に接続されるかどうか確認します。

- 3 [設定済みのアダプタ インスタンス] で、vRealize Automation によってプロビジョニングされる vSphere エンドポイント用の **vCenter Server アダプタ** があることと、それがデータを受信していることを確認します。

図 4-1. vRealize Operations Manager のソリューションとアダプタ



- 4 vRealize Operations Manager で、[アラート] - [アラートの設定] の順に移動します。
- 5 アラートおよび症状の定義に基づいて、意図したとおりの vRealize Automation アラートが生成されることを確認します。

ほとんどの vRealize Automation ユーザーは、展開の健全性が保たれていることを確認するだけで十分です。仮想マシン レベルから受け取るそれ以外のアラートは、量が多すぎる上に、その詳細は vRealize Automation を使用して管理することができません。

vRealize Automation アラート は、展開全体が親オブジェクトです。展開内の仮想マシンは子オブジェクトです。アラートは、デフォルトでは展開レベル、すなわち親レベルで発生します。

vRealize Operations Manager を使用して、特定の症状について知らせる展開レベルのアラートを追加で作成できます。たとえば、展開の中で発生した SQL Server の問題をすべて表示する場合などです。

- 6 vRealize Automation で、[管理] - [再利用] - [メトリック プロバイダ] の順に移動します。
- 7 [vRealize Operations Manager エンドポイント] を選択します。
- 8 vRealize Operations Manager URL `https://master-node-FQDN-or-IP/suite-api/` および vRealize Operations Manager 管理者権限を持つアカウントのユーザー名とパスワードを入力します。

注： 認証ソースが複数ある場合は、`user@domain@source` 形式でユーザー名を入力します。`@source` は、vRealize Operations Manager での LDAP インポート ソースです。ユーザー アカウントには、少なくとも読み取り専用のロールと、vCenter Adapter およびクラウド vCenter Server に対するオブジェクト権限が必要です。

- 9 接続をテストし、保存します。
- 10 [展開] をクリックし、展開を選択して、[監視] タブが表示されることを確認します。
[監視] タブは、vRealize Operations Manager がメトリック プロバイダとして選択されている場合にのみ表示されます。

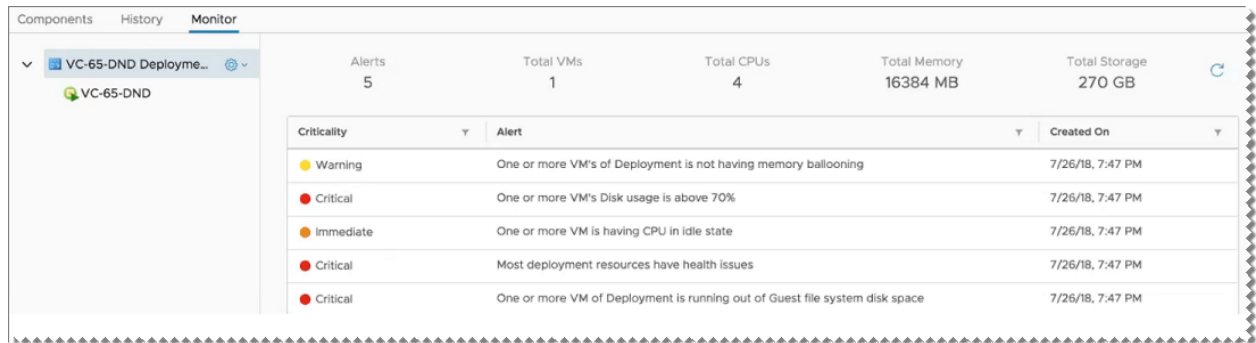
vRealize Operations Manager によるアラート

監視を有効にすると、vRealize Automation は展開に関する vRealize Operations Manager アラートを取得します。

監視にアクセスするには、展開をクリックし、[監視] タブを選択します。タブが表示されない場合は、[vRealize Operations Manager データの有効化](#)を参照してください。

アラートを確認するには、左側のコンポーネント ツリーの一番上に表示されている展開名を選択します。

- アラートの重要度とテキストを確認できます。
- 懸念のある領域に注目するには、列のデータをフィルタリングしたりソートしたりします。
- 健全性アラートのみが表示されます。効率性、リスクなどの他のアラート タイプはサポートされていません。



vRealize Operations Manager によって提供されるメトリック

監視を有効にすると、vRealize Automation は展開に関する vRealize Operations Manager メトリックを取得します。

監視にアクセスするには、展開をクリックし、[監視] タブを選択します。タブが表示されない場合は、[vRealize Operations Manager データの有効化](#)を参照してください。

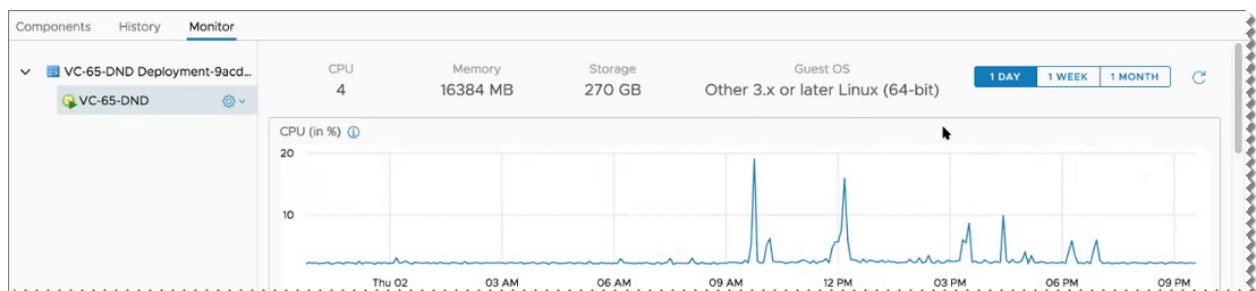
メトリックを表示するには、左側にあるコンポーネント ツリーを展開し、仮想マシンをハイライト表示します。

- メトリックはキャッシュされません。vRealize Operations Manager から直接取得されるため、ロードにしばらくかかる場合があります。
- 仮想マシンのメトリックのみが表示されます。vCloud Director、ソフトウェア、XaaS などの他のコンポーネントのメトリックはサポートされていません。
- vSphere 仮想マシンのメトリックのみが表示されます。AWS や Azure などの他のクラウド プロバイダはサポートされていません。

メトリックは、以下の測定値の最高値と最低値を示すタイムライン グラフとして表示されます。

- CPU
- メモリ
- ストレージの IOPS
- ネットワークの MBPS

特定のメトリックの名前を確認するには、タイムラインの左上隅にある青い情報アイコンをクリックします。



vRealize Operations Manager によって提供されるデータに基づくアクション

vRealize Operations Manager によって提供されるメトリックから問題が明らかになったとき、vRealize Automation で直接、何らかの対応措置を取ることができます。

vRealize Operations Manager によって提供されるメトリックを表示するには、展開をクリックし、[監視] タブを選択します。タブが表示されない場合は、[vRealize Operations Manager データの有効化](#)を参照してください。

問題の特定

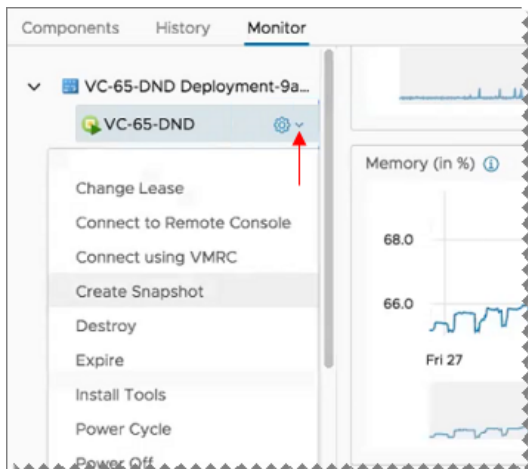
メトリックは、過去の日、週、または月について提供されます。問題のある領域を拡大表示するには、メトリックのタイムラインの下側にある、淡色表示された小さい領域を選択します。



変更

問題が発生したら、同じインターフェイスで直接、何らかの対応措置を取ることができます。

たとえば、メモリ使用量の急増が恒常的に示される場合は、メモリを追加することが考えられます。左側にあるコンポーネント ツリーで仮想マシンのドロップダウン メニューをクリックし、コンテキスト メニューのオプションを使用してメンテナンスまたは再構成を実行します。



展開されたリソースに対するアクションの実行

展開されたリソースで利用できるアクションは、リソースのタイプ、アクションの構成方法、プロビジョニングされたアイテムで使えるようになっているか、アイテムの動作状態によって異なります。

展開または展開コンポーネントで利用できる構成済みのアクションは、選択された展開またはコンポーネントの [アクション] メニューに表示されます。

使用可能なアクションのリストは、展開およびリソース、またはマシン タイプのコンポーネントに対してビジネス グループが実行を許可された内容によって決定されます。アクションが使用可能かどうかは、マシンのタイプまたは状態に依存します。

XaaS ブループリントを使用してアイテムがプロビジョニングされた場合は、アイテムのプロビジョニングに使用される同一のサービスでリソース アクションの作成、公開、資格付与を行う必要があります。使用できるアクションのリストは、アイテムのタイプと現在の状態によって決定します。

IaaS マシンとしてプロビジョニングされたアイテムの使用可能なアクションには、XaaS リソース アクションが含まれる場合もあります（アクションがアイテムにマッピングされている場合）。

プロビジョニングされたリソースのアクション メニュー コマンド

アクションは、プロビジョニングされたリソースに加えることができる変更です。vRealize Automation アクションは、リソースのライフサイクルを管理するために使用されます。

[アクション] メニューで使用可能なコマンドは、そのアクションを実行するリソースを含む資格について、ビジネス グループ マネージャまたはテナント管理者がどのように構成したかによって異なります。使用できるメニュー オプションは、リソースの種類とアイテムの動作状態によっても異なります。

一度に実行できるのは 1 つのアクションのみです。リソースに対して 2 つ目のアクションを実行するには、最初のアクションで要求された変更が完了するまで待機します。

表 4-2. アクション メニュー コマンド

アクション	リソース タイプ	説明
フローティング IP アドレスの関連付け	マシン (OpenStack)	OpenStack マシンとフローティング IP アドレスを関連付けます。
キャンセル	マシン	再構成アクションの実行をキャンセルします。 ユーザーがキャンセルできるアクションは、以前の状態にロールバックできるものに限られます。 パワーオフなど、以前の状態へのロールバックがサポートされていないアクションの場合、要求をキャンセルできるのはテナント管理者権限を持つユーザーのみです。
リースの変更	展開およびマシン	特定のマシン、または展開に含まれるすべてのリソースに対するリースの残り日数を変更します。値を入力しない場合、リースの有効期限が切れることはありません。
NAT ルールの変更	NAT ネットワーク	新しい NAT ポート転送ルールの追加、ルールの順序変更、既存ルールの編集、またはルールの削除を行います。
所有者を変更	展開	展開および含まれているすべてのリソースの所有者を変更します。ビジネス グループ マネージャとサポート ユーザーのみが展開の所有者を変更できます。 所有者の変更アクションを開始するときに、マシンは [オン]、[オフ]、または [有効] の状態になっている必要があります。この状態になっていないと、次のメッセージが表示されてアクションが失敗します。 アクションはこのマシンでは無効です。

表 4-2. アクション メニュー コマンド (続き)

アクション	リソース タイプ	説明
セキュリティの変更	展開	<p>既存の NSX セキュリティ グループおよびセキュリティ タグを追加または削除できます。また、オンデマンド セキュリティ グループを削除することもできます。</p> <p>詳細については、展開内のセキュリティアイテムの追加または削除を参照してください。</p>
VMRC を使用して接続	マシン	<p>VMRC 8.x アプリケーションを使用して仮想マシンに接続します。</p> <p>このアクションを使用するには、アクションを実行する サービス カタログ ユーザーのローカル システム上に VMRC アプリケーションがインストールされている必要があります。</p> <p>インストールおよびユーザー向け手順については、VMware Remote Console ドキュメントを参照してください。ダウンロードするには、VMware Remote Console のダウンロードを参照してください。</p> <p>VMRC 8.x は、これまでの VMware Remote Console の後継となるアプリケーションです。</p>
リモート コンソールに接続	マシン	<p>VMware Remote Console を使用して、選択したマシンに接続します。</p> <p>仮想マシン コンソールはブラウザに表示されます。</p> <p>VMRC 8.x は、VMware Remote Console の後継となるアプリケーションです。</p>
コンソール チケットを使用して接続	マシン (OpenStack および KVM)	<p>VMware Remote Console 接続のコンソール チケットを使用して OpenStack または KVM 仮想マシンに接続します。</p>
ICA を使用して接続	マシン (Citrix)	<p>Independent Computing Architecture (ICA) を使用して、Citrix マシンに接続します。</p>
RDP を使用して接続	マシン	<p>Microsoft Remote Desktop Protocol を使用して、マシンに接続します。</p>
SSH を使用して接続	マシン	<p>SSH を使用して、選択したマシンに接続します。</p> <p>[SSH を使用して接続] オプションを使用するには、SSH をサポートするプラグインがブラウザにインストールされている必要があります (たとえば、Mozilla Firefox および Google Chrome 用の FireSSH SSH ターミナル クライアント)。プラグインが存在する場合、[SSH を使用して接続] を選択すると、SSH コンソールが開き、管理者の認証情報の入力が必要になります。</p> <p>このアクションを使用するには、ブループリントのマシン コンポーネントに、プロパティ グループまたは個々のカスタム プロパティとして Machine.SSH カスタム プロパティが含まれており、なおかつ true に設定されている必要があります。</p>
仮想デスクトップを使用して接続	マシン	<p>Microsoft 仮想デスクトップを使用して、選択したマシンに接続します。</p>

表 4-2. アクション メニュー コマンド (続き)

アクション	リソース タイプ	説明
スナップショットの作成	仮想マシン	仮想マシンのスナップショットを作成します。2 つのスナップショットのみが許可されていてすでに 2 つ存在する場合は、スナップショットを 1 つ削除しない限りこのコマンドを使用できません。
スナップショットの削除	仮想マシン	仮想マシンのスナップショットを削除します。

表 4-2. アクション メニュー コマンド (続き)

アクション	リソース タイプ	説明
削除	展開、マシン、およびオンデマンド セキュリティ グループ	<p>プロビジョニングされたリソースをすぐに削除します。XaaS を除き、展開のコンポーネントを削除することはベスト プラクティスではありません。アクションのスケール インを使用して、展開のマシンの数を減らし、全体の展開を削除します。</p> <p>削除する展開に XaaS リソースが含まれていたとしても、それらのリソースを削除するには、このアクションを実行する必要があります。その他のリソースは、リースまたはアーカイブ期間の終了時に削除されます。</p> <p>[削除] アクションは、次のような展開に使用することはできません。</p> <ul style="list-style-type: none"> ■ 物理マシンの展開 ■ NSX の既存のネットワークまたは NSX の既存のセキュリティ リソースを使用する展開 ■ NSX のオンデマンド ロード バランサ リソースを使用する展開 <p>NSX ロード バランサは、NSX Edge に属しているため、NSX Edge が削除されると、ロード バランサ リソースも削除され、リソースが解放されます。ロード バランシングされたマシン階層が削除されると、各 NSX Edge のロード バランサ プールからも削除されます。</p> <p>注： 破棄アクションは、エンドポイントからマシンの展開を削除できない場合でも、成功を示すメッセージを返すことがあります。たとえば、vSphere マシンが vSAN 以外のデータストア上にあり、その VMX ファイルに破損したデータや無効なデータが含まれている場合です。このメッセージが破棄アクションの成功を示している場合でも、要求ログを確認することで、さらに詳しい情報が得ることができます。この状態のマシンを強制的に破棄すると、エンドポイントで実行が継続され、IP アドレスの競合が発生する可能性があります。破損を vRealize Automation の外部のエンドポイントで修正すると、[破棄] アクションを再試行できます。</p> <p>ビジネス グループ管理者は、破棄要求が失敗したら展開を強制的に破棄できます。展開を削除する間に、エラーを無視して個々のリソースを削除するように強制削除が vRealize Automation に指示されます。強制削除を使用する詳細については、破棄要求が失敗した後の展開環境の強制破棄を参照してください。</p> <p>注： プロビジョニング済みのマシンに予約によって割り当てられたストレージとメモリは、割り当てられたマシンが破棄アクションによって vRealize Automation で削除されると、割り当て解除されます。vCenter Server でマシンが削除される場合は、ストレージとメモリの割り当ては解除されません。</p>

表 4-2. アクション メニュー コマンド (続き)

アクション	リソース タイプ	説明
		<p>Amazon マシン コンポーネントを含む展開を破棄する場合、ブループリントでの [ボリュームの削除] 設定の設定方法によっては、一度に複数の EBS ボリュームを破棄できます。詳細については、Amazon マシン コンポーネント設定を参照してください。</p> <p>Amazon マシン コンポーネントを含む展開環境を破棄すると、そのマシンのライフサイクルで追加されたすべての EBS ボリュームは、破棄されずに切り離されます。vRealize Automation には、EBS ボリュームを破棄するオプションは用意されていません。</p>
フローティング IP アドレスの関連付け解除	マシン (OpenStack)	OpenStack マシンからフローティング IP アドレスを削除します。
閉じる	リソース タイプなし。失敗した初期プロビジョニング要求または失敗したアクション。	<p>失敗した要求を破棄します。進行中の要求をキャンセルします。</p> <ul style="list-style-type: none"> ■ 破棄される要求が展開の要求である場合、破棄を実行すると、失敗した展開が展開リストから削除されます。 ■ 破棄される要求がアクションの場合、破棄を実行すると、失敗したアクション要求がカードから削除され、展開は以前の状態のまま維持されます。 <p>関連する展開で他のアクションを実行できるようになるには、失敗したアクション要求を破棄する必要があります。また、展開ユーザーがマシンの履歴を表示するためにも、失敗したアクションを破棄する必要があります。</p> <p>API によって送信された要求に対して破棄を実行することはできません。また、API によって送信されたアクションは破棄によってブロックされません。</p> <p>このアクションは、すべての初期プロビジョニングでの失敗した要求で使用できます。資格は必要ありません。</p>
再構成の実行	マシン	すぐにマシンを再構成するか、または後で再構成アクションを実行するようにスケジュール設定をします。
有効期限	展開およびマシン	展開に含まれているすべてのリソースに対して展開またはマシンのリースを終了します。
証明書のエクスポート	マシン	クラウド マシンから証明書をエクスポートします。
有効期限リマインダーを受け取る	マシン	現在のリースの有効期限日のカレンダー イベント ファイルをダウンロードします。
VMware Tools のインストール	マシン	vSphere 仮想マシンに VMware Tools をインストールします。
電源入れ直し	マシン	マシンをパワーオフしてから再度パワーオンします。
パワーオフ	マシン	ゲスト OS をシャットダウンせずにマシンをパワーオフします。

表 4-2. アクション メニュー コマンド (続き)

アクション	リソース タイプ	説明
パワーオン	マシン	マシンをパワーオンします。マシンがサスペンド中だった場合は、マシンがサスペンドされた時点から通常の操作が再開されます。
再起動	マシン	vSphere 仮想マシンのゲスト OS を再起動します。 このアクションを使用するには、VMware Tools をマシンにインストールしておく必要があります。
再構成	マシン	<p>ビジネス グループ マネージャ、サポート ユーザー、またはマシン所有者は、選択した vSphere 仮想マシンに対して次の再設定アクションを実行できます。</p> <ul style="list-style-type: none"> ■ 説明の変更 ■ CPU、メモリ、ネットワーク、およびディスク設定の変更 ■ カスタム プロパティとプロパティ グループの追加、編集、および削除 ■ NAT ポート転送ルール用のネットワーク アダプタの追加、編集、順序変更、または削除 ■ シャットダウンの再構成 ■ マシン所有者の変更 (ビジネス グループ管理者とサポート ユーザーのみ使用可能) <p>ストレージ予約ポリシーの変更によってディスク上のストレージ プロファイルが変更される可能性がある場合は、ストレージ予約ポリシーを変更できません。</p> <p>詳細については、マシン再構成の指定および再構成の考慮事項を参照してください。</p> <p>ソース ブループリントの [ブループリントの設定] ページで [既存の環境へ更新を伝達] オプションを選択した場合、ブループリントの CPU、メモリ、またはストレージの最小設定値と最大設定値の増加や拡大が、そのブループリントからプロビジョニングされたアクティブな環境にプッシュされます。詳細については、[ブループリントのプロパティ] 設定を参照してください。</p> <p>vRealize Automation で管理する NSX オブジェクトは、vRealize Automation の外部では管理しないでください。たとえば、展開済みの NSX ロードバランサのメンバー ポートを vRealize Automation 内ではなく NSX 内で変更すると、展開済みマシンと、それに関連付けられていたロード バランサ メンバー プールの間の関連付けが NSX データ収集によって切断されます。また、展開済みロード バランサ メンバー ポートが vRealize Automation の外部で変更されると、スケール イン操作とスケールアウト操作によって予期しない結果が生じます。</p>

表 4-2. アクション メニュー コマンド (続き)

アクション	リソース タイプ	説明
再構成	ロード バランサ	<p>資格のあるマシン所有者、サポート ユーザー、テナント管理者、またはビジネス グループ マネージャは、仮想サーバのすべての設定を変更でき、NSX ロード バランサに仮想サーバを追加または削除できます。</p> <p>詳細については、展開内のロード バランサの再構成を参照してください。</p> <p>ロード バランサの仮想サーバ設定の詳細については、オンデマンド ロード バランサ コンポーネントの追加を参照してください。</p> <p>vRealize Automation で管理する NSX オブジェクトは、vRealize Automation の外部では管理しないでください。たとえば、展開済みの NSX ロード バランサのメンバー ポートを vRealize Automation 内ではなく NSX 内で変更すると、展開済みマシンと、それに関連付けられていたロード バランサ メンバー プールの間の関連付けが NSX データ収集によって切断されます。また、展開済みロード バランサ メンバー ポートが vRealize Automation の外部で変更されると、スケール イン操作とスケールアウト操作によって予期しない結果が生じます。</p>
VDI の登録	仮想マシン (XenServer)	XenServer アイテムに仮想ディスク イメージを登録します。
カタログから削除	展開	カタログから XaaS でプロビジョニングされたリソースを削除します。この操作は、既存のオブジェクトおよび Orchestrator インベントリに含まれていないオブジェクトで実行できます。
再プロビジョニング	マシン	<p>マシンを削除した後、プロビジョニングするワークフローを初期化して、同じ名前でマシンを作成します。</p> <p>マシンの再プロビジョニングを申請すると、既知の問題により、vRealize Automation で実際のステータスが処理中にもかかわらず、再プロビジョニングのステータスがカタログ内で完了として表示される可能性があります。マシンの再プロビジョニング申請を送信したら、次のいずれかの手順を使用して再プロビジョニングされるマシンのステータスをチェックできます。</p> <ul style="list-style-type: none"> ■ [インフラストラクチャ] - [管理対象マシン] ■ [展開] タブ ■ [管理] - [イベント] - [イベント ログ] <p>注： Amazon マシンを再プロビジョニングすることはできません。</p> <p>関連情報については、VMware ナレッジベースの記事、「Reprovisioned machine tasks ...」(KB2065873) を http://kb.vmware.com/kb/2065873 から参照してください。</p>

表 4-2. アクション メニュー コマンド (続き)

アクション	リソース タイプ	説明
再送信	リソース タイプなし。失敗した初期プロビジョニング要求。	<p>失敗したプロビジョニング要求を再送信します。再送信された要求は、プロビジョニング プロセスの開始時にすでに値が入力された状態で開始されます。</p> <p>要求が失敗し、問題を解決できる場合は、新しい要求を作成するのではなく、要求を再送信することができます。要求をサポートしないデータストアなど、誤った値がエラーの原因の場合には、新しい値を使用して新しい要求を作成する必要があります。</p> <p>このアクションは、すべての初期プロビジョニングでの失敗した要求で使用できます。資格は必要ありません。</p>
再開	展開	<p>部分的に成功したプロビジョニング要求を再開します。再開は障害の発生時点から続行します。</p> <p>プロビジョニング手順の実行中に展開に失敗した原因が、環境やインフラストラクチャに関する一時的な問題、タイムアウト、または申請を除くその他の修正可能な問題である場合は、新しいプロビジョニング申請を作成せずに、プロビジョニング プロセスを再開することができます。失敗の原因がブループリント内のエラーである場合、再開してもうまくいきません。再開を試みるよりも、新しい展開を申請する必要があります。</p> <p>デプロイ要求が部分的にのみ成功し、問題を解決できる場合は、再開アクションを使用できます。再開した要求は障害の発生時点から続行します。</p> <p>詳細については、再開アクションの動作を参照してください。</p>
スナップショットまで戻る	仮想マシン	<p>マシンの以前のスナップショットに戻ります。このアクションを使用するには、既存のスナップショットが必要です。</p>
スケール イン	展開	<p>キャパシティ要件の低減に合わせて、展開内のマシンの不要なインスタンスを破棄します。マシン コンポーネントとそこにインストールされているすべてのソフトウェア コンポーネントが削除されます。依存関係にあるソフトウェア コンポーネントやネットワークおよびセキュリティ コンポーネントは、新しい展開構成向けに更新されます。XaaS コンポーネントは拡張可能でなく、拡張処理中には更新されません。</p> <p>部分的に完了したスケール アウトを修正するため、環境の拡張を再度試みることができます。しかし、環境を本来のサイズにまで拡張することはできません。部分的にスケール アウトが完了している場合、未解決リソースの割り当ては解除されないからです。申請の詳細画面を表示して、どのノードでどのタスクが失敗したかを確認し、もう一度拡張を実施することで、部分的に完了したスケール アウトを修正できるかどうかを判断します。拡張に失敗したり、部分的に完了した場合でも、元の環境の機能に影響が及ぶことはなく、障害のトラブルシューティングを行いながらカタログ アイテムを引き続き使用することができます。</p>

表 4-2. アクション メニュー コマンド (続き)

アクション	リソース タイプ	説明
スケール アウト	展開	<p>展開のマシンの追加インスタンスをプロビジョニングして、拡張キャパシティ要件に適應させます。マシン コンポーネントとそこにインストールされているすべてのソフトウェア コンポーネントのプロビジョニングが行われます。依存関係にあるソフトウェア コンポーネントやネットワークおよびセキュリティ コンポーネントは、新しい展開構成向けに更新されます。XaaS コンポーネントは拡張可能でなく、拡張処理中には更新されません。</p> <p>部分的に完了したスケール アウトを修正するため、環境の拡張を再度試みるができます。しかし、環境を本来のサイズにまで拡張することはできません。部分的にスケール アウトが完了している場合、未解決リソースの割り当ては解除されないからです。申請の詳細画面を表示して、どのノードでどのタスクが失敗したかを確認し、もう一度拡張を実施することで、部分的に完了したスケール アウトを修正できるかどうかを判断します。拡張に失敗したり、部分的に完了した場合でも、元の環境の機能に影響が及ぶことはなく、障害のトラブルシューティングを行いながらカタログ アイテムを引き続き使用することができます。</p> <p>ソース ブループリントの [ブループリントの設定] ページで [既存の環境へ更新を伝達] オプションを選択した場合、ブループリントの CPU、メモリ、またはストレージの最小設定値と最大設定値の増加が、そのブループリントからプロビジョニングされたアクティブな環境にプッシュされます。詳細については、[ブループリントのプロパティ] 設定を参照してください。</p>
シャットダウン	マシン	ゲスト OS をシャットダウンして、マシンをパワーオフします。このアクションを使用するには、VMware Tools をマシンにインストールしておく必要があります。
サスペンド	マシン	マシンを使用できないように一時停止して、使用しているストレージ以外のシステム リソースが使用されないようにします。
登録解除	マシン	マシンを削除することなくインベントリから除外します。登録解除されたマシンは使用できません。
登録解除	ネットワーク	ネットワークを削除することなくインベントリから除外します。登録解除されたネットワークは使用できません。
VDI の登録解除	仮想マシン (XenServer)	XenServer アイテムの仮想ディスク イメージを登録解除します。

[リソース アクション] メニューに表示されないアクションのトラブルシューティング

マシンまたはリソース所有者は、プロビジョニングされたアイテムに対する使用可能なアクションをすべて確認できるわけではありません。

問題

ユーザーまたはビジネス グループにアクションの使用資格が付与されたことを把握している環境では、[展開] リストでアイテムを選択したときにすべてのアクションが表示されることを想定します。

原因

アクションが使用可能かどうかは、プロビジョニングされたリソースのタイプ、リソースの動作状態、および構成方法と使用可能にされた方法によります。すべての構成済みアクションが表示されない理由の一部を次に示します。

- プロビジョニングされたリソースの現在の状態により、アクションが適用可能ではありません。たとえば、パワーオフはマシンがパワーオンされたときにのみ使用可能です。
- 選択したアイテムのタイプに対してアクションが使用可能ではありません。アイテムがアクションをサポートしていない場合、リスト内にアクションは表示されません。たとえば、[スナップショットの作成] アクションを物理マシンに使用することはできません。また、[RDP を使用して接続] アクションは、選択したアイテムが Linux マシンの場合には使用できません。
- プロビジョニングされたリソース タイプに対してアクションが適用可能になっていても、インフラストラクチャブループリントで無効化されています。アクションが無効化されている場合、そのアクションが、ブループリントを使用してプロビジョニングされたアイテムに対して使用可能なアクションとして表示されることはありません。
- アクションの実行に必要なアイテムをプロビジョニングするための資格に、アクションが含まれていません。使用可能なアクション（IaaS ブループリントの一部として、または XaaS リソース アクションとして）のみを [アクション] メニューに表示できます。
- アクションは XaaS リソース アクションとして作成されたものの、アクションの実行に必要なアイテムをプロビジョニングするための資格に、アクションが含まれていませんでした。使用可能なアクションのみが [アクション] メニューに表示されます。
- XaaS リソース アクションまたはプロビジョニングされた IaaS マシンに対するリソース マッピングの構成済みターゲット基準に基づいて、アクションは制限される可能性があります。

解決方法

- ◆ プロビジョニングされたアイテムまたはプロビジョニングされたアイテムの状態に対し、アクションが適用可能であることを確認してください。
- ◆ アイテムのプロビジョニングに使用される資格に、アクションが構成され、含まれていることを確認してください。

マシンのスナップショットの作成

仮想マシンのスナップショットを作成できる場合があります。作成できるかどうかは、管理者がどのように環境を構成したかによって決まります。スナップショットとは、特定日時における仮想マシンのイメージのことです。これは、容量を効率的に利用した、元の仮想マシンのイメージのコピーです。スナップショットを使用すると、障害、データ消失、セキュリティの脅威からシステムを簡単に復旧できます。仮想マシンのスナップショットを作成した後、そのスナップショットを適用すると、システムはそのスナップショットが取得された時点にリセットされます。

メモリ スナップショットを作成する場合、スナップショットでは、仮想マシンの電源設定の状態と、任意で仮想マシンのメモリを取得します。仮想マシンのメモリの状態を取得する場合、スナップショット操作の完了に時間がかかります。ネットワークに応じて瞬間的に中断が生じる場合もあります。

前提条件

- 既存の仮想マシンの電源がオン、オフ、またはサスペンド状態。
- 1 つ以上の独立したディスク用に仮想マシンが構成されている場合は、スナップショットを作成する前にマシンをパワーオフしておきます。マシンがパワーオン状態になっていると、スナップショットを作成できません。ディスク構成の詳細については、「カスタム プロパティ V テーブル」を参照してください。
- テナント管理者またはビジネス グループ マネージャが、ユーザーにスナップショット アクションを使用する資格を付与しました。

手順

- 1 [展開] をクリックします。
- 2 スナップショットを作成するマシンを含む展開を見つけて展開名をクリックします。
- 3 [コンポーネント] タブで、仮想マシンをクリックし、アクションの歯車アイコンをクリックします。
コンポーネントのアクション メニューが表示されます。
- 4 [アクション] メニューで [スナップショットの作成] をクリックします。
- 5 名前と説明（説明は任意）を入力します。
- 6 マシンのメモリおよびパワー設定を取得する場合は、[メモリを含む] を選択します。
- 7 [送信] をクリックします。

マシンへのリモート接続

マシンへは vRealize Automation コンソールからリモートで接続できます。

VMware Remote Console を使用して接続している場合は、ナレッジベースの記事 [Troubleshooting VMRC connectivity in vRealize Automation \(KB2114235\)](#) を参照してください。

前提条件

- マシン所有者、テナント管理者、またはビジネス グループ マネージャとして vRealize Automation にログインします。
- VMware Tools がインストールされていることを確認します。

VMware Tools が vRealize Automation クライアントにインストールされ、VMware Remote Console との接続時に十分に機能するアクセス権がサポートされている必要があります。VMware Tools がインストールされていない場合、ターゲット マシンへの接続後にマウス ポインタとマウス キーが機能しないなどの問題が発生します。サポートされている VMware Tools バージョンの詳細については、[vRealize Automation 製品ドキュメント](#)の vRealize Automation のサポート マトリックスを参照してください。
- プロビジョニングされたマシンがパワーオンされていることを確認します。

- vRealize Automation アプライアンスと ESXi サーバ間のネットワーク トラフィックがポート 902 を経由できるようにします。
- vRealize Automation アプライアンスとクライアント ブラウザ間のネットワーク トラフィックがポート 8444 を経由できるようにします。
- IaaS Web コンポーネント Windows サーバと関連する vSphere エンドポイント間のネットワーク トラフィックがポート 443 を経由できるようにします。

手順

- 1 [展開] をクリックします。
- 2 接続が必要なマシンを含む展開を見つけて展開名をクリックします。
- 3 [コンポーネント] タブで、マシンを見つけ、アクションの歯車アイコンをクリックします。
コンポーネントのアクション メニューが表示されます。
- 4 リモート接続方法を選択します。
 - [RDP を使用して接続] を選択し、RDP を使用して接続します。
 - [リモート コンソールに接続] を選択し、VMware Remote Console を使用して接続します。
プロンプトへ応答します。
- 5 [接続] をクリックし、手順に従ってマシンにログインします。
- 6 完了したら、ログアウトしてブラウザ ウィンドウを閉じます。

信頼されていない SSL 証明書を使用した vSphere のリモート コンソールの構成

vRealize Automation の展開で信頼されていない証明書を使用する場合、VMware Remote Console でリモート コンソールを使用する前に、証明書を信頼するようにクライアント ブラウザを構成する必要があります。この手順は、ブラウザごとに異なります。

信頼されている SSL 証明書を使用し、環境に合わせて vRealize Automation を構成する場合、VMware Remote Console でクライアントのブラウザを個別に設定する必要はありません。vRealize Automation アプライアンス証明書を信頼性のある証明書に置き換えたら、Web ブラウザ クライアントの証明書情報をアップデートする必要はありません。

証明書を置き換える場合は、vRealize Automation のシステム管理ガイドに記載された vRealize Automation アプライアンス証明書の置き換えに関するトピックを参照してください。

vSphere 上にプロビジョニングされたマシン用の VMware Remote Console を使用したリモート接続は、プロキシ コンソールを通じて vRealize Automation アプライアンス証明書で保護されます。VMware Remote Console では ブラウザが WebSockets をサポートし、ブラウザは vRealize Automation アプライアンス証明書を信頼する必要があります。https://vra-va.eng.mycompany.com/ 形式のアドレスにあるルートレベルの仮想アプライアンスに移行すると、証明書を取得することができます。

ブラウザと vSphere のサポート要件の詳細については、「vRealize Automation のサポート マトリックス」を参照してください。

vRealize Automation の証明書を信頼するための Firefox の構成

vSphere 上にプロビジョニングされたクライアントの VMware Remote Console をサポートするには、vRealize Automation アプライアンスの信頼されていない証明書をクライアント ブラウザに手動でインポートする必要があります。

サポートされている Firefox バージョンについては、vRealize Automation [情報センター](#)で VMware vRealize サポート マトリックスを参照してください。

注： 信頼されている SSL 証明書を使用し、環境に合わせて vRealize Automation を設定する場合、VMware Remote Console でクライアントのブラウザを個別に設定する必要はありません。

手順

- 1 Firefox ブラウザで、vRealize Automation アプライアンスにログインします。
証明書が信頼されていないというメッセージが表示されます。
- 2 [メニューを開く] - [オプション] の順に選択します。
- 3 [プライバシーとセキュリティ] をクリックし、[証明書の表示] をクリックします。
- 4 [証明書マネージャ] ダイアログ ボックスで、[サーバ] をクリックし、[例外の追加] をクリックします。
- 5 8444 のポートを使用して、ご使用の vRealize Automation アプライアンスの URL を追加します。
たとえば、https://your-vra-fqdn-domain:8444 のように指定します。
- 6 [証明書の取得] をクリックし、[セキュリティ例外の確認] をクリックします。
- 7 [OK] をクリックします。

結果

証明書のエラーが発生せずに、リモート コンソールに接続できます。

vRealize Automation アプライアンスの証明書を信頼するための Internet Explorer の構成
vSphere 上にプロビジョニングされたクライアントの VMware Remote Console をサポートするには、vRealize Automation アプライアンスの信頼されていない証明書をクライアント ブラウザに手動でインポートする必要があります。

注： 信頼されている SSL 証明書を使用し、環境に合わせて vRealize Automation を構成する場合、VMware Remote Console でクライアントのブラウザを個別に構成する必要はありません。

この手順のこのステップは、自己署名証明書および認証局によって発行された証明書に適用されます。

サポートされている Internet Explorer のバージョンについては、VMware Web サイトの「VMware vRealize Support Matrix」を参照してください。

手順

- 1 Internet Explorer ブラウザで、vRealize Automation アプライアンスにログインします。
- 2 ブラウザのアドレス バーに表示される証明書エラー メッセージの [証明書の表示] をクリックします。
- 3 証明書情報ウィンドウの [全般] タブをクリックします。
- 4 証明書に関する情報が正しいことを確認し、[証明書をインストール] をクリックします。

- 5 証明書ストアのダイアログ ボックスで [証明書をすべて次のストアに配置する] を選択します。
- 6 [参照] をクリックして証明書ストアを検索します。
- 7 [信頼されたルート証明書機関] を選択し、[OK] をクリックします。
- 8 証明書ストアのダイアログ ボックスで [次へ] をクリックします。
- 9 セキュリティ警告のダイアログ ボックスで [はい] をクリックし、証明書をインストールします。
- 10 ブラウザを再起動します。

結果

証明書のエラーが発生せずに、リモート コンソールに接続できます。

vRealize Automation アプライアンスの証明書を信頼するための Chrome の構成

vSphere 上にプロビジョニングされたクライアントの VMware Remote Console をサポートするには、vRealize Automation アプライアンス の信頼されていない証明書をクライアント ブラウザに手動でインポートする必要があります。

サポートされている Chrome のバージョンの詳細については、[vRealize Automation 製品ドキュメント](#)の vRealize Automation のサポート マトリックスを参照してください。

注： 信頼されている SSL 証明書を使用し、環境に合わせて vRealize Automation を設定する場合、VMware Remote Console でクライアントのブラウザを個別に設定する必要はありません。

Windows では、Chrome と Internet Explorer は同一の証明書ストアを使用します。つまり、Internet Explorer によって信頼された証明書は、Chrome でも信頼されることになります。Chrome の信頼された証明書を確認するには、Internet Explorer を使用して証明書をインポートします。この手順の詳細については、[vRealize Automation アプライアンスの証明書を信頼するための Internet Explorer の構成](#)を参照してください。

手順を完了したら、Chrome を再起動します。

Macintosh オペレーティング システムで証明書を永続的に信頼するには、証明書ファイルをダウンロードし、証明書管理ツールにこの証明書を信頼済みとしてインストールします。

手順

- 1 Chrome ブラウザで、vRealize Automation アプライアンス にログインします。
- 2 ブラウザのアドレス バーの横にある *サイト情報の表示アイコン* をクリックし、[証明書] アイコンをクリックして証明書情報を表示します。
- 3 証明書を保存します。
- 4 通常、アプリケーション フォルダのユーティリティ フォルダにあるキーチェーン アクセス アプリケーションを起動します。
- 5 [ファイル] - [アイテムのインポート] を選択します。
- 6 キーチェーン アクセスの画面で、以前に保存した証明書ファイルを選択します。
[ターゲット キー] の値を [システム] に設定します。
- 7 [開く] をクリックし、証明書をインポートします。

8 ブラウザを再起動します。

マシン再構成の指定および再構成の考慮事項

vSphere、vCloud Air、および vCloud Director プラットフォームでは、展開内の既存のマシンを再構成して、CPU、メモリ、およびストレージなどの仕様を変更できます。

再構成の申請は、ブループリントのマシン コンポーネントで有効になっている資格、ポリシー、およびアクションに基づいて承認されます。

オンデマンド ネットワークに割り当てられている仮想マシンの再構成はサポートされていません。オンデマンド ネットワークに接続されている NIC を再構成することはできません。オンデマンド NAT またはルーティング ネットワークの再構成を試みると、「Original network [<network>] is not selected in the machine's reservation.」エラーが表示されます。マシンが接続されているネットワークは影響を受けず、マシンの IP アドレスは変更されません。

再構成のキャンセル（マシン）および再構成の実行（マシン）に資格を割り当てた場合、再構成をキャンセルしたり失敗した再構成を再試行したりできます。

リンク クローン ブループリントからプロビジョニングされた仮想マシンでは、ディスクの拡張はサポートされていません。

Size または Image コンポーネント プロファイルを使用してマシンを再構成することはできませんが、プロファイルに基づいて計算される CPU、メモリ、およびストレージの範囲は、引き続き再構成することができます。たとえば、小（1 個の CPU、1,024 MB のメモリ、10 GB のストレージ）、中（3 個の CPU、2,048 MB のメモリ、12 GB のストレージ）、大（5 個の CPU、3,072 MB のメモリ、15 GB のストレージ）という Size 値セットを使用した場合、マシンの再構成時に使用可能な範囲は、1 個 ~ 5 個の CPU、1,024 MB ~ 3,072 MB のメモリ、および 1 GB ~ 15 GB のストレージです。

vRealize Automation により、展開でブループリントのスナップショットが作成されます。展開で CPU や RAM などのマシン プロパティを更新する際に再構成の問題が発生した場合は、ナレッジベースの記事 [KB2150829 vRA 7.x Blueprint Snapshotting](#) を参照してください。

前提条件

- マシン所有者、サポート ユーザー、共有アクセス ロールを持つビジネス グループ ユーザー、またはビジネス グループ マネージャとして vRealize Automation にログインします。
- 再構成するマシンのステータスはオンまたはオフであることが必要で、再構成ステータスが有効であってはなりません。
- マシン タイプは、vSphere、vCloud Air、または vCloud Director である必要があります。ただし、NSX の設定は vSphere にのみ適用されます。
- マシンを再構成する資格が付与されていることを確認します。

手順

- 1 [展開] をクリックします。
- 2 再構成が必要なマシンを含む展開を見つけて展開名をクリックします。

- 3 [コンポーネント] タブで、仮想マシンをクリックし、アクションの歯車アイコンをクリックします。
コンポーネントのアクション メニューが表示されます。
- 4 [再構成] を選択します。
- 5 再構成する設定に応じて適切なタブを選択します。

表 4-3. 再構成の変更の申請

タブ	トピック
一般	CPU およびメモリの再構成
ストレージ	ストレージ設定の編集
ネットワーク	ネットワーク設定の変更 NAT ルールを変更するには、 展開内の NAT ルールの変更 を参照してください。
セキュリティ	セキュリティ設定を再構成するには、 展開内のセキュリティアイテムの追加または削除 を参照してください。
プロパティ	カスタム プロパティとプロパティ グループの設定の変更

次のステップ

[申請されたマシン再構成の実行](#)。

CPU およびメモリの再構成

プロビジョニング ブループリントで設定された制限内で、プロビジョニングされたマシンが使用する CPU 数やメモリおよびストレージの容量を変更できます。

プロビジョニングされた Amazon の展開では、root ボリュームを除き、展開内のすべてのストレージ ボリュームを再構成できます。

リンク クローン ブループリントからプロビジョニングされた仮想マシンでは、ディスクの拡張はサポートされていません。

前提条件

[マシン再構成の指定および再構成の考慮事項](#)。

手順

- 1 [全般] タブをクリックします。
- 2 [CPU 数] テキスト ボックスに CPU の数を入力します。
- 3 [メモリ (MB)] テキスト ボックスにメモリの容量を入力します。
- 4 [ストレージ (GB)] テキスト ボックスにストレージの容量を入力します。

次のステップ

追加のマシン再構成設定を指定します。マシン設定の変更が完了したら、マシン再構成の申請を開始します。[申請されたマシン再構成の実行](#) を参照してください。

ストレージ設定の編集

プロビジョニングされた仮想マシンのストレージ ボリュームは、追加、削除、またはサイズ変更できます。

IDE ディスク タイプのストレージは、再構成できません。

プロビジョニング済みのマシンに予約によって割り当てられたストレージとメモリは、割り当てられたマシンが破棄アクションによって vRealize Automation で削除されると、割り当て解除されます。vCenter Server でマシンが削除される場合は、ストレージとメモリの割り当ては解除されません。

たとえば、既存の展開でマシンに関連付けられている予約を削除することはできません。vCenter Server で展開済みのマシンを手動で移動または削除する場合、vRealize Automation では引き続き、展開済みのマシンをライブとして認識するため、関連付けられた予約を削除することはできません。

マシンのプロビジョニングや展開を行った後に、キャパシティやストレージ予約ポリシーなどの一部の設定を変更できます。

プロビジョニング時に、[ドライブ文字/マウント パス] および [ラベル] の値がゲスト エージェントに適用されます。これらの値はプロビジョニング後に更新されないため、最新でない可能性があります。データを収集して現在の値を表示するには、カスタムの vRealize Orchestrator ワークフローを作成して実行します。

前提条件

[マシン再構成の指定および再構成の考慮事項](#)。

プロビジョニングされた Amazon の展開では、ルート ボリュームを除くすべてのストレージ ボリュームを展開内で再構成できます。

手順

1 [ストレージ] タブをクリックします。

2 必要に応じて、ストレージ オプションを表示または編集します。

- 可能な場合は、新しいボリュームを追加します。
- 可能な場合は、ボリュームを削除します。

アイコンが選択できない場合、リンク クローンからのボリュームなど、ボリュームが削除できないことを意味します。

- 可能な場合は、ボリューム サイズを変更します。

既存のボリュームのサイズを減らすことはできません。ボリュームのサイズは、ブループリントに指定されたストレージの総量から、他のボリュームに割り当てられた量を引いた値に制限されます。

次のステップ

追加のマシン再構成設定を指定します。マシン設定の変更が完了したら、マシン再構成の申請を開始します。 [申請されたマシン再構成の実行](#) を参照してください。

ネットワーク設定の変更

ネットワーク アダプタを追加、削除、または編集できます。

マシンの再構成中に次のネットワーク設定を変更できます。

- NIC の追加または削除

- 既存の NIC の IP アドレスの割り当てまたは解放
- ネットワークがオンデマンドの NAT ネットワークまたはオンデマンドのルーティング ネットワークでない場合は、NIC への新規 IP アドレスの割り当て

オンデマンドのルーティング NAT ネットワークまたはオンデマンドの NAT ネットワークは構成できません。

ネットワークを再構成するには、ソースおよびターゲットのネットワークを予約で選択する必要があります。

NIC を追加すると、IP アドレスが割り当てられます。NIC を削除すると、IP アドレスは解放されます。

予約情報およびネットワーク プロファイル情報に基づいてネットワーク設定を変更すると、新しいネットワーク IP アドレスが vRealize Automation で割り当てられますが、エンドポイントの展開済みマシンに新しい IP アドレス情報が反映されることはありません。再構成プロセスが完了した後に、手動でマシンに IP アドレスを割り当てる必要があります。

オンデマンド ネットワークに割り当てられている仮想マシンの再構成はサポートされていません。オンデマンド ネットワークに接続されている NIC を再構成することはできません。オンデマンド NAT またはルーティング ネットワークの再構成を試みると、「Original network [<network>] is not selected in the machine's reservation.」エラーが表示されます。マシンが接続されているネットワークは影響を受けず、マシンの IP アドレスは変更されません。

NSX ネットワーク設定の変更は、vRealize Automation 6.2.x からこの vRealize Automation のリリースにアップグレードまたは移行した展開ではサポートされません。

前提条件

[マシン再構成の指定および再構成の考慮事項。](#)

手順

- 1 [ネットワーク] タブをクリックします。
- 2 (オプション) ネットワーク アダプタを追加します。
 - a [新規ネットワーク アダプタ] をクリックします。
 - b [ネットワーク パス] ドロップダウン メニューからネットワークを選択します。
マシンの予約で選択されているネットワークはすべて選択可能です。
 - c [アドレス] テキスト ボックスにネットワークの固定 IP アドレスを入力します。
予約で割り当てられたネットワーク プロファイルでは、IP アドレスを未割り当てにする必要があります。
 - d [保存] アイコン (👍) をクリックします。
- 3 (オプション) ネットワーク アダプタを削除します。
 - a ネットワーク アダプタを探します。
 - b [削除] アイコン (🗑️) をクリックします。
ネットワーク アダプタ O は削除できません。

4 (オプション) ネットワーク アダプタを編集します。

- a ネットワーク アダプタを探します。
- b [編集] アイコン (✎) をクリックします。
- c [ネットワーク パス] ドロップダウン メニューからネットワークを選択します。
- d [保存] アイコン (✓) をクリックします。

次のステップ

追加のマシン再構成設定を指定します。マシン設定の変更が完了したら、マシン再構成の申請を開始します。 [申請されたマシン再構成の実行](#) を参照してください。

カスタム プロパティとプロパティ グループの設定の変更

展開済みのマシンのカスタム プロパティを編集、追加、または削除することができます。

カスタム プロパティを使用して、ボリューム ディスク番号、容量、ラベル、ストレージ予約ポリシーの値を入力することはできません。これらの値は、ストレージ ボリューム テーブルでボリュームを追加または編集して入力する必要があります。 [ストレージ設定の編集](#) を参照してください。

前提条件

[マシン再構成の指定および再構成の考慮事項](#)。

手順

- 1 [プロパティ] タブをクリックします。
- 2 プロパティを追加するには、[新規プロパティ] をクリックします。
- 3 [名前] テキスト ボックスにプロパティ名を入力します。
- 4 [値] テキスト ボックスにプロパティ値を入力します。
- 5 値を暗号化するには、[暗号化済み] チェック ボックスを選択します。
- 6 ユーザーがマシンを申請するときに、値を入力するためのプロンプトを表示するには、[プロンプト表示] チェック ボックスを選択します。
- 7 別のプロパティを追加、既存のプロパティを編集、またはプロパティを削除します。

次のステップ

追加のマシンの再構成の内容を指定します。マシン設定の変更が完了したら、マシンの再構成の要求を開始します。 [申請されたマシン再構成の実行](#) を参照してください。

申請されたマシン再構成の実行

申請されたマシン再構成は、直ちに開始すること、特定の日に開始するようにスケジューリングすることもできます。また、マシンを再構成する前に、その電源オプションを指定することもできます。

前提条件

[マシン再構成の指定および再構成の考慮事項](#)。

手順

- 1 [実行] タブが表示されている場合は、このタブを選択して追加の再構成設定を指定できます。表示されていない場合は、[送信] をクリックしてマシンの再構成を開始します。
- 2 [実行] タブが表示されている場合は、[実行] をクリックして再構成アクションをスケジューリングします。
- 3 (オプション) [申請の実行] ドロップダウン メニューからオプションを選択します。

オプション	説明
緊急	承認後、直ちに再構成を開始します。
スケジュール設定	指定された日時に再構成を開始します。表示されるテキスト ボックスで日時を入力します。

スケジュールした時刻は、vRealize Automation Web サーバが配置されている場所のローカル時刻です。
[申請の実行] が使用可能でない場合は、再構成が直ちに開始されます。

- 4 (オプション) [電源操作] ドロップダウン メニューから電源操作を選択します。

オプション	説明
必要に応じて再起動	(デフォルト) 必要に応じて、マシンを再構成する前に再起動します。
再起動	再起動の必要性の有無に関わらず、マシンを再構成する前に再起動します。
再起動しない	再起動が必要な場合でも、マシンを再構成する前に再起動しません。

次の条件の場合は、マシンを再構成する前に再起動する必要があります。

- ホット アドがサポートされていないか無効になっている状態で、CPU が変更された
- ホット メモリがサポートされていないか無効な状態で、メモリが変更された
- ホット ストレージが無効な状態で、ストレージが変更された

シャットダウン状態のマシンは再起動されません。

注： `VirtualMachine.Reconfigure.DisableHotCpu` カスタム プロパティを使用して、vSphere のホット アド オプションを無効にできます。

- 5 [OK] をクリックします。

次のステップ

ユーザー インターフェイスに表示されるワークフローの状態を確認することにより、再構成の進行状況を監視できます。[再構成操作のワークフローの状態](#)を参照してください。

再構成操作のワークフローの状態

再構成が開始してワークフローで処理が行われると、[編集] ページでその進行状況を監視できます。

表 4-4. 再構成操作のワークフローの状態

状態	説明
再構成を保留中	状態操作が作成されました。
スケジュール設定	Distributed Execution Manager (DEM) 用のスケジュールされたワークフローが作成されました。

表 4-4. 再構成操作のワークフローの状態（続き）

状態	説明
再構成中	インターフェイス固有のワークフローが実行されています。
再構成が失敗し、再試行を待機中	再構成が失敗し、所有者が再試行を申請するのを待機しています。マシン所有者に再構成アクションまたは再構成のキャンセル アクションの権限がある場合、所有者は再構成を再試行またはキャンセルできます。
ReconfigureFailed	再構成が失敗し、ワークフローが次のアクションを実行するのを待機しています。
ReconfigureSuccessful	再構成が成功し、ワークフローが次のアクションを実行するのを待機しています。
キャンセル済み	ユーザーが再構成をキャンセルしました。マシンの所有者が資格を付与されている場合、再構成をキャンセルできます。
完了	この状態は、クリーンアップ終了後に完了ワークフローで設定されます。これにより、ワークフローは、状態操作と承認のクリーンアップに進むことができます。完了ステータスは、vRealize Automation からの申請が完了したことを示すものであり、マシンの再構成が正常に完了したことを示すものではありません。

展開内のロード バランサの再構成

展開された NSX ロード バランサの仮想サーバを追加、編集、または削除できます。

次の考慮事項は vRealize Automation 7.2 以前のバージョンを使用した展開に適用されます。

- ロード バランサの再構成は、単一のロード バランサを含む展開に制限されます。
- 展開環境内のロード バランサの [アイテムの詳細] ページには、環境内のすべてのロード バランサで使用されている仮想サーバが表示されます。詳細については、[ナレッジベースの記事 KB2150276](#) を参照してください。
- ロード バランサの再構成の操作は、vRealize Automation 6.2.x からこの vRealize Automation のリリースにアップグレードまたは移行された環境ではサポートされません。

アップデートしたロード バランサおよび現在の vRealize Automation リリースに展開されているロード バランサの場合は、仮想サーバの編集と仮想サーバの追加を同じ要求で実行しないようにします。詳細については、[ナレッジベースの記事 KB2150240](#) を参照してください。

注： NSX-T ロード バランサでは、[再構成] アクションはサポートされていません。

環境で別のアクションが実行されている間、たとえば環境のスケールアウトの進行中に、ロード バランサの再構成の申請を送信した場合、再構成は失敗し、メッセージが表示されます。このような状況では、アクションが完了するまで待機してから再構成の申請を送信します。

注： 展開に関連付けられているブループリントを、オンデマンドのロード バランサが含まれている YAML ファイルからインポートした場合、名前フィールドの値が ID フィールドの値と異なっていると、[再構成] アクションが失敗します。インポートされたブループリントに基づく展開のために、ロード バランサ再構成オプションを有効にするには、ブループリントで次の手順を実行し、将来の展開環境でロード バランサ コンポーネントのプロビジョニング後のアクションを許可します。

- 1 vRealize Automation コンソールで、ブループリントを選択します。
- 2 [編集] をクリックし、ブループリント名を変更します。これにより、名前と組み込みの ID が同じ値に設定されます。
- 3 ブループリントでロード バランサ コンポーネントを選択します。
- 4 [編集] をクリックし、コンポーネント名を再入力します。これにより、名前と組み込みの ID が同じ値に設定されます。
- 5 ブループリントのすべてのロード バランサ コンポーネントにこの手順を繰り返します。
- 6 ブループリントを保存します。

編集したブループリントを使用して新しい展開をプロビジョニングすると、[ロード バランサの再構成] アクションが機能するようになります。この問題を回避するには、すべてのロード バランサ、ネットワーク、およびセキュリティコンポーネントに対して、すべての YAML ファイルがインポート前に同一の名前および ID 値を持つようにします。

vRealize Automation で管理する NSX オブジェクトは、vRealize Automation の外部では管理しないでください。たとえば、展開済みの NSX ロード バランサのメンバー ポートを vRealize Automation 内ではなく NSX 内で変更すると、展開済みマシンと、それに関連付けられていたロード バランサ メンバー プールの間の関連付けが NSX データ収集によって切断されます。また、展開済みロード バランサ メンバー ポートが vRealize Automation の外部で変更されると、スケール イン操作とスケールアウト操作によって予期しない結果が生じます。

仮想サーバを追加または編集するときに使用できる設定については、[オンデマンド ロード バランサ コンポーネントの追加](#)を参照してください。

vRealize Automation でロード バランサを再構成するとき、NSX で構成された設定のうち、vRealize Automation の設定として使用できないものは、デフォルト値に戻されます。ロード バランサ再構成アクションを vRealize Automation で実行した後、必要に応じて次の設定を NSX で確認および更新します。

- Insert-X-Forwarded-For HTTP ヘッダー
- HTTP リダイレクト URL
- サービス監視拡張機能

前提条件

- マシン所有者、サポート ユーザー、共有アクセス ロールを持つビジネス グループ ユーザー、またはビジネス グループ マネージャとして vRealize Automation にログインします。

- 展開内のロード バランサを再構成する資格が付与されていることを確認します。必要なカタログ資格は再構成（ロード バランサ）です。

手順

- 1 [展開] をクリックします。
- 2 再構成が必要なロード バランサを含む展開を見つけて展開名をクリックします。
- 3 [コンポーネント] タブで、ロード バランサをクリックし、アクションの歯車アイコンをクリックします。
コンポーネントのアクション メニューが表示されます。
- 4 [再構成] を選択します。
- 5 仮想サーバを追加、編集、または削除します。

Virtual servers:

Protocol	Port	Description	Member Protocol	Member Port	Health Check Protocol	Health Check Port
HTTP	80		HTTP	80	HTTP	80
HTTP	81		HTTP	81	HTTP	81

- 6 [送信] をクリックします。

展開内の NAT ルールの変更

展開された NAT の 1 対多のネットワーク内の既存の NSX NAT ルールを追加、編集、および削除することができます。

NAT ルールの処理順序を変更することもできます。

注： 展開のソース ブループリントが NAT ネットワーク コンポーネントを含む YAML ファイルからインポートされており、NAT ネットワーク コンポーネントの名前と ID の値が同一でない場合、[NAT ルールの変更] アクションは停止します。インポートされたブループリントに基づく展開に対して [NAT ルールの変更] アクションを許可するには、展開のプロビジョニング前にブループリントで次の手順を実行します。

- 1 vRealize Automation を起動し、[設計] タブをクリックしてブループリントを開きます。
- 2 [編集] をクリックし、ブループリント名を変更します。これにより、名前と組み込みの ID が同じ値に設定されます。
- 3 ブループリントで NAT ネットワーク コンポーネントを選択します。
- 4 [編集] をクリックし、コンポーネント名を再入力します。これにより、名前と組み込みの ID が同じ値に設定されます。
- 5 ブループリントのすべての NAT ネットワーク コンポーネントにこの手順を繰り返します。
- 6 ブルー プリントを保存します。

この問題を回避するには、すべてのブループリント、ロード バランサ、ネットワーク、およびセキュリティ コンポーネントに対して、すべての YAML ファイルがインポート前に同一の名前および ID 値を持つようにします。

詳細については、[NSX for vSphere の NAT ルールの作成と使用](#)および[オンデマンド NAT またはオンデマンドルーティング ネットワーク コンポーネントの追加](#)を参照してください。

前提条件

- マシン所有者、サポート ユーザー、共有アクセス ロールを持つビジネス グループ ユーザー、またはビジネス グループ マネージャとして vRealize Automation にログインします。
- ネットワーク内で NAT ルールを変更する資格が付与されていることを確認します。
- NAT ネットワークが NAT の 1 対多ネットワークとして構成されていることを確認します。1 対 1 の NAT ネットワークのアクションは使用できません。

NSX for vSphere では 1 対 1 の NAT と 1 対多の NAT ネットワークをサポートしていますが、NSX-T では 1 対多の NAT のみをサポートしています。

手順

- 1 [展開] をクリックします。
- 2 変更が必要なネットワーク コンポーネントを含む展開を見つけて展開名をクリックします。
- 3 [コンポーネント] タブで、NAT ネットワーク コンポーネントをクリックします。

サードパーティ製の IP アドレス管理プロバイダに関連付けられたオンデマンド NAT ネットワークの場合、コンポーネントの編集はできません。ただし、新しい宛先 IP アドレスを手動で追加することはできます。新しい宛先 IP アドレスを追加すると、コンポーネントの値は null になります。再構成の申請を送信すると、新しい宛先 IP アドレスと、null のマシン ID が処理されます。

- 4 アクションの歯車アイコンをクリックします。
コンポーネントのアクション メニューが表示されます。
- 5 [NAT ルールの変更] をクリックします。
- 6 新しい NAT ポート転送ルールの追加、ルールの順序変更、既存ルールの編集、またはルールの削除を行います。
- 7 [送信] をクリックします。

既存の NSX Edge のすべての NAT ルールの表示

アクティブな展開で使用される NSX Edge に関する NAT ルールを表示できます。

NAT ルールは、展開で使用されるすべての NAT ルールの集約として Edge ビューに表示されます。Edge ビューでは、ルールは必ずしも処理される順序で表示されません。

1 対多の NAT ネットワークでの NAT ルールの処理順序を表示して必要に応じて変更するには、[展開内の NAT ルールの変更](#)を参照してください。

前提条件

- マシン所有者、サポート ユーザー、共有アクセス ロールを持つビジネス グループ ユーザー、またはビジネス グループ マネージャとして vRealize Automation にログインします。

手順

- 1 [展開] をクリックします。
- 2 表示している NSX Edge を含む展開を見つけて展開名をクリックします。

- 3 [コンポーネント] タブで、NSX Edge コンポーネントを見つけます。
- 4 表示する NSX Edge を選択します。
- 5 終了したら [閉じる] をクリックします。

展開内のセキュリティアイテムの追加または削除

マシン展開の既存の NSX セキュリティ グループとセキュリティ タグを追加または削除できます。オンデマンド セキュリティ グループの追加はできませんが、削除はできます。

セキュリティの変更アクションは、マシン コンポーネントまたはクラスタに基づきます。たとえば、2 台のマシンから成る AppTier2 という名前のクラスタにセキュリティが 関連付けられている場合は、クラスタ内の個々のマシンではなく、AppTier2 クラスタにセキュリティの変更操作を実行します。

セキュリティの変更操作は、vRealize Automation 6.2.x からこの vRealize Automation リリースにアップグレードまたは移行された展開ではサポートされていません。

前提条件

- マシン所有者、サポート ユーザー、共有アクセス ロールを持つビジネス グループ ユーザー、またはビジネス グループ マネージャとして vRealize Automation にログインします。
- 展開でセキュリティを変更する資格が付与されていることを確認します。必要なカタログ資格は、セキュリティの変更（展開）です。

手順

- 1 [展開] をクリックします。
- 2 セキュリティ グループとタグを含む展開を見つけて展開名をクリックします。
- 3 [コンポーネント] タブで、セキュリティ コンポーネントをクリックし、アクションの歯車アイコンをクリックします。
コンポーネントのアクション メニューが表示されます。
- 4 [セキュリティの変更] をクリックします。
- 5 展開済みのマシン コンポーネントまたはクラスタを選択して、セキュリティ アイテムを追加または削除します。
- 6 必要に応じて、展開内の各マシン コンポーネントまたはクラスタの既存のセキュリティ グループとセキュリティ タグを追加または削除します。
- 7 必要に応じて、展開内の各マシン コンポーネントまたはクラスタのオンデマンド セキュリティ グループを削除します。
- 8 (オプション) [理由] タブをクリックし、要求の理由を入力します。
- 9 [送信] をクリックします。

その他の展開の管理方法

展開したリソースは資格を付与されたアクションを使用して管理できますが、アクションとして含まれていないその他の方法もあります。

これらの方法は、[展開] タブでは使用できませんが、プロビジョニングしたリソースに変更を加える際に使用します。

vRealize Operations Manager メトリックに基づくリソースの再利用

再利用は、リソースを効率的に使用するのに役立ちます。vRealize Operations Manager を使用して環境内のリソースを管理する場合は、メトリックを使用して展開リソースを再利用できる場所を計算するように vRealize Automation を構成します。

手順

1 メトリック プロバイダの設定

vSphere 仮想マシンの vRealize Operations Manager 健全性メトリックとリソース メトリックを使用するように、vRealize Automation を設定することができます。

2 回収要請の送信

展開を表示および管理して、回収申請を展開所有者に送信することが可能です。回収要請では、新規リースの長さ（日数）、展開所有者の応答のために与える時間、および再利用の対象にするマシンを指定します。

3 回収要請の追跡

回収要請の現在の状態やその他の詳細を追跡できます。

メトリック プロバイダの設定

vSphere 仮想マシンの vRealize Operations Manager 健全性メトリックとリソース メトリックを使用するように、vRealize Automation を設定することができます。

vRealize Operations Manager の健全性バッジとメトリックの詳細については、vRealize Operations Manager のドキュメントを参照してください。

前提条件

- テナント管理者、ビジネス グループ マネージャ、またはマシン所有者として vRealize Automation コンソールにログインします。

再利用：再利用申請を作成するユーザーには、テナント管理者ロールが必要です。また、そのテナント管理者アカウントは、テナント内の 1 つ以上のビジネス グループのメンバーである必要があります。

テナント管理者アカウントのビジネス グループへの追加に失敗すると、[再利用] - [展開] タブを開くとシステム例外が発生します。

- vRealize Automation と統合するすべての vSphere サーバに対して、表示とリソース メトリック問い合わせの権限を持つ vRealize Operations Manager ユーザー アカウントを作成します。
- vRealize Automation でエンドポイントとして追加するすべての vSphere サーバの vRealize Operations Manager アダプタ インスタンスを作成します。アダプタ インスタンスの作成に関する詳細については、vRealize Operations Manager のドキュメントを参照してください。

手順

- 1 [管理] - [再利用] - [メトリック プロバイダ] を選択します。

2 メトリック プロバイダを選択します。

オプション	説明
(デフォルト) vRealize Automation メトリック プロバイダ	vRealize Operations Manager インスタンスがない場合は、vRealize Automation によって基本のマシン メトリックが提供されます。
vRealize Operations Manager エンドポイント	vSphere 仮想マシンのメトリック プロバイダとして使用する vRealize Operations Manager インスタンスの接続情報を提供します。

3 [テスト接続] をクリックします。

4 [保存] をクリックします。

結果

マシンが存在するグループのテナント管理者、マシン所有者、ビジネス グループ マネージャは、vSphere 仮想マシンのアイテムの詳細ページで健全性バッジや健全性アラートを表示できます。また、[回収要請] ページからプラットフォーム タイプ vSphere でフィルタリングして、vRealize Operations Manager のメトリックや健全性バッジを表示することもできます。

次のステップ

[回収要請の送信](#)。

回収要請の送信

展開を表示および管理して、回収申請を展開所有者に送信することが可能です。回収要請では、新規リースの長さ（日数）、展開所有者の応答のために与える時間、および再利用の対象にするマシンを指定します。

前提条件

- テナント管理者として vRealize Automation にログインします。
- (オプション) 健全性バッジを表示したり、vRealize Operations Manager によって提供されているメトリックを確認するには、[メトリック プロバイダの設定](#)を参照してください。

手順

1 [管理] - [再利用] - [展開] を選択します。

2 検索条件に一致する仮想マシン展開を検索します。

vRealize Operations Manager によって提供されているメトリックを確認するには、プラットフォーム タイプとして vSphere を選択する必要があります。

- a [詳細検索] の下矢印をクリックし、検索ボックスを開きます。
- b 1 つ以上の検索値を入力または選択します。

オプション	アクション
仮想マシン名に次の文字を含む	このテキスト ボックスに 1 つ以上の文字を入力すると、一致する仮想マシン名が検索されます。
所有者名に次の文字を含む	このテキスト ボックスに名前を入力すると、一致する所有者名が検索されます。
ビジネス グループ名に次の文字を含む	このテキスト ボックスに名前を入力すると、一致するビジネス グループ名が検索されます。
プラットフォーム タイプ	ドロップダウン メニューからプラットフォーム タイプを選択します。vSphere を選択すると、vRealize Operations Manager によって提供されているメトリックが表示されます。 vRealize Operations Manager で必要です。
パワー状態	このドロップダウン メニューからパワー状態の値を選択すると、パワー状態が一致する仮想マシンが検索されます。
有効期限日が次の範囲内	カレンダー アイコンをクリックして、開始日と終了日を選択すると、その範囲内で有効期限日が検索されます。
CPU 使用率	このドロップダウン メニューから値を選択すると、CPU 使用率の高い (80% より高い) 仮想マシン、CPU 使用率の低い (5% 未満の) 仮想マシン、または CPU を使用していない (CPU 使用率の値がない) 仮想マシンが検索されます。 vRealize Operations Manager メトリックを検索する場合は、このフィルタを使用して検索することはできません。また、結果を CPU 使用量でソートすることはできません。
メモリ使用量	このドロップダウン メニューから値を選択すると、メモリ使用率の高い (80% より高い) 仮想マシン、メモリ使用率の低い (10% 未満の) 仮想マシン、またはメモリを使用していない (メモリ使用率の値がない) 仮想マシンが検索されます。 vRealize Operations Manager メトリックを検索する場合は、このフィルタを使用して検索することはできません。また、結果をメモリ使用率でソートすることはできません。
ディスク使用率	このドロップダウン メニューから値を選択すると、ハード ディスク使用率の低い (1 秒あたり 2 KB 未満の) 仮想マシン、またはハード ディスクを使用していない (ハード ディスク使用率の値がない) 仮想マシンが検索されます。 vRealize Operations Manager メトリックを検索する場合は、このフィルタを使用して検索することはできません。また、結果をディスク使用率でソートすることはできません。
ネットワーク使用率	このドロップダウン リストから値を選択すると、ネットワーク使用率の低い (1 秒あたり 1 KB 未満の) 仮想マシン、またはネットワークを使用していない (ネットワーク使用率の値がない) 仮想マシンが検索されます。 vRealize Operations Manager メトリックを検索する場合は、このフィルタを使用して検索することはできません。また、結果をネットワーク使用率でソートすることはできません。
複合メトリック	このドロップダウン メニューから値を選択すると、複合メトリックに基づいて仮想マシンが検索されます。たとえば、[アイドル] を選択すると、CPU、ネットワーク、メモリ、ディスクの使用率がすべて 20% 未満のマシンが検索されます。

オプション	アクション
	vRealize Operations Manager メトリックを検索する場合は、このフィルタを使用できません。

c 検索アイコン (🔍) をクリックします。

- 3 [展開] ページで、親展開が回収されるマシンを 1 つ以上選択します。

選択したマシンのうち、現在の結果ページに表示されているマシンのみが回収されます。

- 4 [回収] をクリックします。

現在のページで選択済みの仮想マシンを含む展開が申請に含まれます。

注： [回収展開] ページには、リース期限切れのマシンなど、回収対象外のマシンもリストされる可能性があります。回収対象外のマシンを指定すると、次のエラーが表示されます。

```
Selection Error: Virtual machine 名前 is not in valid state for reclamation.
```

- 5 [新規リースの長さ (日単位)] テキスト ボックスに新規リースの期間を入力します。

最小値は 1 日、最大値は 365 日、デフォルト値は 7 日です。

- 6 回収要請に応答する展開所有者の応答期限を [リース強制までの待機時間 (日単位)] テキスト ボックスに入力します

この期間が終了すると、展開は新しい長さの新しいリースを取得します。待機期間の最小値は 1 日、最大値は 365 日、デフォルト値は 3 日です。

- 7 [申請の理由] テキスト ボックスに、申請の理由を入力します。

- 8 [送信] をクリックします。

- 9 [OK] をクリックします。

結果

回収申請を送信すると、展開所有者の受信箱にその申請が表示されます。所有者が所定の日数で申請に応答しない場合、展開は、現在のリース期間のほうが短い場合を除いて、指定された長さの新規リースを取得します。所有者が回収要請で [使用中のアイテム] をクリックすると、展開のリースは未変更のままとなります。所有者が [再利用のためにリリース] をクリックすると、展開のリースは直ちに有効期限切れになります。

次のステップ

回収要請の追跡

回収要請の追跡

回収要請の現在の状態やその他の詳細を追跡できます。

次のいずれかの方法を使用して最近の回収要請を確認できます。

- [受信箱] タブをクリックし、[回収要請] を選択して回収要請の情報を表示します。
- [回収要請] タブをクリックし、最近の要請のリストを表示します。

- [展開] をクリックし、最近の展開の変更を表示します。

前提条件

テナント管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [再利用] - [回収要請] を選択します。
- 2 検索条件に一致する仮想マシンを検索します。
 - a [詳細検索] の下矢印をクリックし、検索ボックスを開きます。
 - b 1 つ以上の検索値を入力または選択します。

オプション	アクション
仮想マシン名に次の文字を含む	このテキスト ボックスに 1 つ以上の文字を入力すると、一致する仮想マシン名が検索されます。
所有者名に次の文字を含む	このテキスト ボックスに 1 つ以上の文字を入力すると、一致する所有者名が検索されます。
申請理由に次の文字を含む	このテキスト ボックスに 1 つ以上の文字を入力すると、一致する申請理由が検索されます。
申請状態	このドロップダウン メニューから申請状態の値を選択すると、申請状態が一致する仮想マシンが検索されます。

- c [検索] アイコン (🔍) をクリックするか、Enter を押して検索を開始します。
 - d [詳細検索] の上矢印をクリックし、検索ボックスを閉じます。
- 3 (オプション) [データのアップデート] をクリックすると、回収要請の表示がアップデートされます。

管理対象マシンの予約の変更

管理対象マシンの予約またはストレージ設定を変更できます。この機能は、現在の予約では使用できない新しいストレージ バスにマシンを移動する場合に役立ちます。展開するマシンが 1 つであれば、そのマシンのビジネス グループを変更することもできます。

単一マシンの展開では、特定のマシンを別のビジネス グループに移動することができます (マシン所有者が、移動先のビジネス グループのメンバーである場合)。ビジネス グループ設定を変更するには、移動元のビジネス グループおよび移動先のビジネス グループのビジネス グループ マネージャである必要があります。

注： そのマシンに割り当てられた予約ポリシーが存在する場合、そのビジネス グループを変更することはできません。

[管理] - [コンピュート リソース] メニュー オプションを使用して、関連するコンピュート リソースの追加の予約を作成できます。

プロビジョニング済みのマシンに予約によって割り当てられたストレージとメモリは、割り当てられたマシンが破棄アクションによって vRealize Automation で削除されると、割り当て解除されます。vCenter Server でマシンが削除される場合は、ストレージとメモリの割り当ては解除されません。

たとえば、既存の展開でマシンに関連付けられている予約を削除することはできません。vCenter Server で展開済みのマシンを手動で移動または削除する場合、vRealize Automation では引き続き、展開済みのマシンをライブとして認識するため、関連付けられた予約を削除することはできません。

予約を変更することで、vCenter Server 内のマシンが、vRealize Automation にあるそのマシンの予約の一部ではない新しいストレージ パスに移動する場合は、マシンのターゲット予約で、ターゲットまたは新しいストレージパスが選択されていることを確認してから、マシンの予約を変更します。

前提条件

ファブリック管理者として vRealize Automation にログインします。

手順

- 1 [インフラストラクチャ] - [管理対象マシン] を選択します。
- 2 変更する予約が含まれるマシンを特定します。
- 3 ドロップダウン メニューで [予約の変更] をクリックします。
ドロップダウン メニューの [表示] をクリックすると、関連するブループリントやコンピュート リソースなどの、管理対象マシンに関する情報を表示できます。
- 4 (オプション) [ビジネス グループ] ドロップダウン メニューから、ビジネス グループを選択します。
- 5 (オプション) [予約] ドロップダウン メニューから予約を選択する。
- 6 (オプション) [ストレージ] ドロップダウン メニューからストレージ ポリシーを選択します。
- 7 [OK] をクリックします。

受信箱の操作

受信箱は、カタログ要求の承認、プロビジョニング中に要求された操作、および vRealize Operations Manager メトリックに基づく回収要請のステータスに関する製品内通知を提供します。

各タブを確認して、アクションを必要とする保留中の通知の有無を確認できます。

- [承認。]承認を必要とするカタログ要求を追跡できます。カタログ要求の承認者として指定されている場合は、承認要求に応答することができます。[承認ポリシー設定へのレベル情報の追加](#) を参照してください。
- [手動ユーザー アクション。]一部のカタログ要求では、プロビジョニング中に操作が必要です。操作要求に応答することができます。[vRealize Automation 内での vRealize Orchestrator の統合](#)を参照してください。
- [回収要請。] vRealize Operations Manager を使用してリソースを再利用できる場所を確認する場合は、回収要請を追跡できます。[回収要請の追跡](#)を参照してください。