

vRealize Automation の 構成

vRealize Automation 7.1



vmware®

最新の技術ドキュメントは VMware の Web サイト (<https://docs.vmware.com/jp/>) にあります
このドキュメントに関するご意見およびご感想がある場合は、docfeedback@vmware.com までお送りください。

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, 2016 VMware, Inc. 無断転載を禁ず。著作権および商標情報。

目次

vRealize Automation の構成 7

更新情報 8

1 プロビジョニングのための外部環境の準備 9

vRealize Automation の管理に向けた環境の準備 9

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 10

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 13

vRealize Automation 用の vCloud Director 環境の準備 16

vRealize Automation 用の vCloud Air 環境の準備 16

Amazon AWS 環境の準備 17

Red Hat OpenStack のネットワークとセキュリティの機能の準備 22

SCVMM 環境の準備 23

マシン プロビジョニングの準備 24

準備するマシン プロビジョニング方法の選択 24

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 26

プロビジョニングでの vRealize Automation ゲスト エージェントの使用 27

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 34

vCloud Air および vCloud Director のプロビジョニングの準備 48

Linux キックスタート プロビジョニングの準備 49

SCCM プロビジョニングの準備 52

WIM プロビジョニングの準備 53

仮想マシン イメージ プロビジョニングの準備 63

Amazon マシン イメージ プロビジョニングの準備 64

シナリオ : Rainpole で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 66

ソフトウェア プロビジョニングの準備 69

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 69

シナリオ : クローン マシンの vSphere CentOS 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する 75

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 79

2 テナント設定の構成 84

ディレクトリ管理構成オプションの選択 85

ディレクトリ管理の概要 86

ディレクトリ管理による Active Directory リンクの作成 89

Active Directory で同期されるユーザー属性の管理 101

コネクタの管理 102

コネクタ マシンをドメインに参加させる 103

ドメイン コントローラの選択	104
アクセス ポリシーの管理	108
代替ユーザー 認証製品とディレクトリ管理との統合	113
シナリオ：高可用性 vRealize Automation に対する Active Directory リンクを構成する	132
vRealize Automation のスマート カード認証の構成	134
コネクタ アクティベーション トークンの生成	135
コネクタ OVA ファイルを展開する	136
コネクタ設定を構成する	137
パブリック証明機関の適用	138
ワークスペース ID プロバイダの作成	140
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	140
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	141
グループとユーザーのロールの構成	143
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	143
カスタム グループの作成	144
ビジネス グループの作成	145
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	147
シナリオ：Rainpole 用のデフォルト テナントを構成する	148
シナリオ：Rainpole 用のローカル ユーザー アカウントを作成する	149
シナリオ：企業 Active Directory を Rainpole 用の vRealize Automation に接続する	150
シナリオ：Rainpole 用のデフォルト テナントのブランディングを構成する	151
シナリオ：Rainpole アーキテクトのカスタム グループを作成する	152
シナリオ：IaaS 管理者の権限を Rainpole アーキテクトのカスタム グループに割り当てる	153
追加テナントの作成	154
テナント情報の指定	154
ローカル ユーザーの構成	155
管理者の指定	155
テナントを削除する	156
カスタム ブランディングの構成	156
テナント ログイン ページのカスタム ブランディング	157
テナント アプリケーションのカスタム ブランディング	157
通知構成のチェックリスト	159
通知用のグローバル電子メール サーバの構成	161
テナント固有の送信電子メール サーバの追加	163
テナント固有の受信電子メール サーバの追加	165
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	166
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	167
システム デフォルトの電子メール サーバに戻す	168
通知の構成	168
マシン有効期限の E メール通知日付のカスタマイズ	168
自動 IaaS 電子メールのテンプレートの構成	169
通知の登録	169

- 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 170
- 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 170
- vRealize Orchestrator およびプラグインの構成 171
 - テナントのデフォルト ワークフロー フォルダの構成 172
 - 外部 vRealize Orchestrator サーバの構成 172
 - vRealize Orchestrator 構成インターフェイスへのログイン 173
 - vRealize Orchestrator クライアントへのログイン 174

3 リソースの構成 176

- laaS リソース設定のチェックリスト 176
 - ユーザー認証情報の格納 177
 - エンドポイントシナリオの選択 179
 - ファブリック グループの作成 197
 - マシン プリフィックスの構成 198
 - キー ペアの管理 199
 - ネットワーク プロファイルの作成 201
 - 予約と予約ポリシーの設定 217
 - シナリオ：Rainpole 用の laaS リソースを構成する 253
 - 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 257
 - 外部 IP アドレス管理プロバイダを使用した vRealize Automation 展開のプロビジョニングのチェックリスト 258
- XaaS リソースの構成 259
 - エンドポイントとしての Active Directory プラグインの構成 259
 - エンドポイントとしての HTTP-REST プラグインの構成 261
 - エンドポイントとしての PowerShell プラグインの構成 263
 - エンドポイントとしての SOAP プラグインの構成 264
 - エンドポイントとしての vCenter Server プラグインの構成 265
- 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 266
- Active Directory ポリシーの操作 267
 - Active Directory ポリシーの作成と適用 268

4 オンデマンド サービスのユーザーへの提供 271

- ブループリントの設計 271
- ブループリントのエクスポートとインポート 273
 - 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 274
 - シナリオ：Dukes Bank サンプル アプリケーションをテストする 278
- デザイン ライブラリの作成 279
 - マシン ブループリントの設計 281
 - NSX ネットワークおよびセキュリティを使用したマシン ブループリントの設計 318
 - ソフトウェア コンポーネントの設計 333
 - XaaS ブループリントおよびリソース アクションの作成 351
 - ブループリントの公開 400

複合ブループリントの組み合わせ	401
ネストされたブループリントの動作について	403
ソフトウェア コンポーネントをサポートするマシン コンポーネントの選択	405
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	406
明示的な依存関係の作成とプロビジョニングの順序の制御	407
シナリオ : Rainpole リンク クローン マシン上の MySQL を提供するためのブループリントを組み合わせ でテストする	408
サービス カタログの管理	411
サービス カタログ構成用のチェックリスト	412
サービスの作成	413
カタログ アイテムとアクションでの作業	415
資格の作成	418
承認ポリシーの操作	424
シナリオ : Rainpole アーキテクトによるブループリントのテスト用にカタログを構成する	442
シナリオ : Rainpole CentOS マシンをテストする	445
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	447
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	450

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。

サポート対象のコンポーネントの詳細については、<https://www.vmware.com/pdf/vrealize-automation-71-support-matrix.pdf> を参照してください。

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。

VMware の技術ドキュメントの用語集

VMware の技術ドキュメントには、新しい用語などをまとめた用語集があります。当社の技術ドキュメントで 사용되는用語の定義については、<http://www.vmware.com/support/pubs> をご覧ください。

更新情報

この vRealize Automation の構成は、製品リリース時に、または必要に応じて更新されます。

vRealize Automation の構成の更新履歴は次のとおりです。

リビジョン	説明
JA-002076-04	<ul style="list-style-type: none">■ 「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」 を更新しました。■ 「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」 を更新しました。■ 「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」 を更新しました。■ 「Active Directory ポリシーの作成」 を更新しました。
JA-002076-03	「テナント情報の指定」 にメモを追加して、テナント URL で使用できるのは小文字のみであることを明確にしました。
JA-002076-02	<ul style="list-style-type: none">■ 「vCloud Air および vCloud Director のプロビジョニングの準備」 を更新しました。■ 「vCloud Director エンドポイントの作成」 を更新しました。■ 「ブループリントのエクスポートとインポート」 を更新しました。■ 「vSphere マシン コンポーネントの設定」 を更新しました。
JA-002076-01	<ul style="list-style-type: none">■ 「テナントを削除する」 を追加しました。■ 「Amazon マシン コンポーネント設定」 を更新しました。■ 「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。
JA-002076-00	初版 7.1 リリース。

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。

この章では次のトピックについて説明します。

- [vRealize Automation の管理に向けた環境の準備](#)
- [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

統合プラットフォームによっては、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	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 NSX 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。
 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。

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

環境	準備
 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。
 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を登録し、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。 「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」 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 ネットワークおよびセキュリティ環境を構成する必要があります。

ブループリントおよび予約で指定するネットワークおよびセキュリティ構成のための vRealize Automation のサポートの多くは、外部で構成され、コンピュート リソースでデータ収集が実行された後に vRealize Automation で使用できるようになります。

vRealize Automation 用に構成することができる、選択可能なネットワークおよび構成オプションの詳細については、[「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
❑ NSX プラグインをインストールおよび構成します。	NSX プラグインを vRealize Orchestrator にインストールします。	[vRealize Orchestrator での NSX プラグインのインストール] および『NSX 管理ガイド』を参照してください。
❑ 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 でネットワーク設定を構成します。	『NSX 管理ガイド』を参照してください。
❑ 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 でセキュリティ設定を構成します。	『NSX 管理ガイド』を参照してください。
❑ NSX ロードバランサの設定を構成します。	vRealize Automation と連携するように NSX ロード バランサを構成します。	『NSX 管理ガイド』を参照してください。 また、『カスタム プロパティのリファレンス』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。

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。

注意 インストール済みの NSX プラグインを含む組み込みの vRealize Orchestrator を使用している場合、NSX プラグインがすでにインストールされているため、以下のプラグイン インストール手順を実行する必要はありません。

一般的な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詳細については、vRealize Orchestrator のドキュメント (https://www.vmware.com/support/pubs/orchestrator_pubs.html) を参照してください。

開始する前に

- 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。
- 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。
- 正しいバージョンの NSX プラグインをインストールしたことを確認します。『vRealize Automation のサポート マトリックス』を参照してください。
- 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。

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 ネットワークとセキュリティ製品のためのプラグイン インストール ファイルは、VMware 製品ダウンロード サイト (<http://vmware.com/web/vmware/downloads>) からダウンロードすることができます。
- 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。

次に進む前に

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。

vRealize Orchestrator および NSX のセキュリティ ワークフローの実行

vRealize Automation から NSX のセキュリティ ポリシー機能を使用する前に、管理者は、vRealize Orchestrator で **Enable security policy support for overlapping subnets** ワークフローを実行する必要があります。

重複サブネット ワークフローのセキュリティ ポリシー サポートは、NSX 6.1 以降のエンドポイントに適用できます。
このワークフローを 1 回だけ実行してこのサポートを有効にしてください。

開始する前に

- vSphere エンドポイントが NSX エンドポイントに登録され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。
- vRealize Orchestrator クライアントに管理者としてログインします。
- **Create NSX endpoint** vRO ワークフローを実行していることを確認します。

手順

- 1 [ワークフロー] タブをクリックし、[NSX] - [VCAC の NSX ワークフロー] を選択します。
- 2 [NSX エンドポイントの作成] ワークフローを実行し、プロンプトに応答します。
- 3 [重複サブネットのセキュリティ ポリシー サポートを有効にする] ワークフローを実行します。
- 4 ワークフローの入力パラメータとして、NSX エンドポイントを選択します。

vSphere エンドポイントを作成して NSX インスタンスに登録したときに指定した IP アドレスを使用します。

このワークフローを実行した後、セキュリティ ポリシーで定義した分散ファイアウォールのルールは、このセキュリティ ポリシーが適用されるセキュリティ グループのメンバーの vNIC でのみ適用されます。

次に進む前に

ブループリントの適用可能なセキュリティ機能を適用します。

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

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外部 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 エンドポイントを使用するには、最初に vRealize Orchestrator IP アドレス管理プロバイダ 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、vRealize Orchestrator で 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、[「外部 IP アドレス管理プロバイダを使用した vRealize Automation 展開のプロビジョニングのチェックリスト」](#) 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	場所	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。	IP アドレス管理プロバイダ パッケージ (Infoblox IP アドレス管理など) を VMware Solution Exchange からダウンロードして、vRealize Orchestrator にインポートします。 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://solutionexchange.vmware.com/store/category_group/s/cloud-management) に存在しない場合は、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。	「外部 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。
<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。	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。	「vRealize Orchestrator でワークフローを実行し、Infoblox IP アドレス管理エンドポイント タイプを登録する」 を参照してください。

外部 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

外部 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、最初に外部 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 パッケージ (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 SDK とそれに付属する SDK ドキュメントを使用して、独自のパッケージを作成することも可能です (たとえば、Bluecat IP アドレス管理で使用するパッケージを作成することができます)。この例では、Infoblox IP アドレス管理パッケージを使用しています。

外部 IP アドレス管理プロバイダ パッケージを入手して 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 タイプを登録します。

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 のパッケージとワークフローで 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。

開始する前に

- vRealize Orchestrator パッケージのインポート、設定、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 VMware Solution Exchange のサイト (https://solutionexchange.vmware.com/store/category_groups/cloud-management) を開きます。
- 2 [クラウド管理マーケットプレイス] を選択します。
- 3 プラグインまたはパッケージ (Infoblox VIPAM Plug-in など) を探して、ダウンロードします。

- 4 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。
- 5 パッケージまたはプラグイン（例：Infoblox IP アドレス管理プラグイン）を選択します。
- 6 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。

次に進む前に

[\[vRealize Orchestrator でワークフローを実行し、Infoblox IP アドレス管理エンドポイント タイプを登録する\]](#)。

vRealize Orchestrator でワークフローを実行し、Infoblox IP アドレス管理エンドポイント タイプを登録する

vRealize Automation による外部 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 Infoblox 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。

vRealize Orchestrator で IP アドレス管理エンドポイント タイプを登録する際、vRealize Automation vRA 管理者の認証情報を指定するように要求されます。T

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 のパッケージとワークフローで 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。

開始する前に

- [「外部 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」](#)
- ワークフローの実行権限を取得し、vRealize Automation を使用して vRealize Orchestrator にログインしていることを確認します。
- プロンプトが表示されたら vRealize Automation IaaS 管理者の認証情報を提供できるように準備しておきます。

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。ワークフロー名は、プロバイダ パッケージが異なっても似ていることがあります。vRealize Orchestrator のワークフローの場所は、プロバイダごとに異なる場合があります。
- 2 **Register IPAM Endpoint** 登録ワークフローを実行し、IP アドレス管理 Infoblox エンドポイント タイプを指定します。
- 3 vRealize Automation の認証情報を求めるプロンプトで、vRealize Automation IaaS 管理者の認証情報を入力します。

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定義するときに、そのエンドポイント タイプが使用可能になります。

次に進む前に

IP アドレス管理 Infoblox タイプのエンドポイントを vRealize Automation で作成できるようになりました。[「外部 IP アドレス管理プロバイダのエンドポイントの作成」](#) を参照してください。

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 でロ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

Amazon AWS に、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構成する必要があります。

vRealize Automation を使用してマシンを正常にプロビジョニングするには、特定の Amazon アクセス権を持っている必要があります。

- 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。

vRealize Automation で AWS エンドポイントを作成するための AWS 認証情報は必要ありません。ただし、vRealize Automation は、Amazon マシン イメージを作成する AWS ユーザーが、Power User ロールを持っているものと想定します。

- Amazon Web Services の認証情報

AWS Power User ロールでは、AWS Identity and Access Management (IAM) のユーザーとグループの管理は行えません。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構成されている必要があります。

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 エンドポイントを作成するために必要なアクセス キーを取得するために、Power User 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。

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 バランサー
- 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 バランサー内のマシンの状態
- 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 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 ブレーブ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。

シナリオ：概念実証の環境のためにネットワークと Amazon との間の VPC 接続を構成する

vRealize Automation を評価する PoC（事前検証）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。

開始する前に

- vRealize Automation をインストールして完全に構成します。『Rainpole シナリオのための vRealize Automation のインストールおよび構成』を参照してください。
- 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。

次に進む前に

- 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。

セキュリティ グループは、予約を作成するときに指定でき、またブループリント キャンバス内にも指定できます。マシンを申請する際にもセキュリティ グループを指定できます。

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。

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 パスを構成してください。

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。

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 1-4. 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です。	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 エージェントの詳細については、 「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。

表 1-4. 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
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。
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	既存の vSphere 仮想マシンが必要です。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。
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」
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	「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。 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。
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	「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。 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。
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 1-4. 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。PEBuilder を使用して、ゲスト エージェントを含む WinPE イメージを作成できます。別の方法を使用して WinPE イメージを作成できますが、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 1-5. 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 7.1 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 Scripts に、サンプル Visual Basic スクリプト PrePostProvisioningExample.vbs 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>注意 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。</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、< %System Drive%>Program Files (x86)\VMware\VCAC Agents\EPI_Agents\Scripts\SendEmail.vbs 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 ExternalPreProvisioningVbScript 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 ExternalPostProvisioningVbScript 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、カスタム仕様 が実行された後で（カスタム仕様 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。

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。

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 1-6. 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
<code>VirtualMachine.Admin.UseGuestAgent</code>	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。
<code>VirtualMachine.Customize.WaitComplete</code>	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。

表 1-6. 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
<code>VirtualMachine.SoftwareN.ScriptPath</code>	<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。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。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、</p> <p>値 \\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、</p> <p>値 \\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>
<code>VirtualMachine.ScriptPath.Decrypt</code>	<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。たとえば、</p> <p>VirtualMachine.Software0.ScriptPath = c:\dosomething.bat <password> 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、使用可能なチェック ボックスをオンに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、<password> は、実際のパスワードの値です。使用可能なチェック ボックスをオンにして暗号化を有効にします。

表 1-6. 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 <code>VirtualMachine.ScriptPath.Decrypt</code> を <code>VirtualMachine.ScriptPath.Decrypt = true</code> として設定します。 ■ カスタム プロパティ <code>VirtualMachine.Software0.ScriptPath</code> を <code>VirtualMachine.Software0.ScriptPath = c:\dosomething.bat [MyPassword]</code> として設定します。 <p><code>VirtualMachine.ScriptPath.Decrypt</code> を <code>false</code> に設定した場合、または <code>VirtualMachine.ScriptPath.Decrypt</code> カスタム プロパティを作成しない場合、角カッコ ([および]) 内の文字列は復号化されません。</p>

ゲスト エージェントで使えるカスタム 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。

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。

開始する前に

- 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。

手順

- 1 vCloud Automation Center Appliance 管理コンソールのインストール ページに移動します。
例: `https://<vcac-hostname.domain.name>:5480/installer/`。
- 2 Linux ゲスト エージェント パッケージをダウンロードして保存します。
- 3 **LinuxGuestAgentPkgs** ファイルを展開します。
- 4 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 ゲスト OS の **LinuxGuestAgentPkgs** サブディレクトリに移動します。
 - 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-
<7.0.0-012715.x86_64>.rpm` を実行します。

- 5 `installgugent.sh <Manager_Service_Hostname_fqdn>:<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 バランサーを使用している場合	Manager Service ロード バランサー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 バランサーがない場合	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>

- 6 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 バランサーまたは 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 バランサー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 バランサーがない場合	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>

- 7 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>

次に進む前に

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 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。

開始する前に

- リファレンス マシンの指定または作成を行います。
- 最も安全な方法でゲスト エージェントと Manager Service マシンの間の信頼を確立するには、Manager Service マシンから PEM 形式の SSL 証明書を取得します。ゲスト エージェントが信頼を確立する方法の詳細については、「[サーバを信頼する Windows ゲスト エージェントの構成](#)」を参照してください。

手順

- 1 vCloud Automation Center Appliance 管理コンソールのインストール ページに移動します。
例： <https://<vcac-hostname.domain.name>:5480/installer/>。
- 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 リファレンス マシンの C ドライブに、Windows ゲスト エージェント インストール ファイルをダウンロードおよび保存します。
 - Windows ゲスト エージェント ファイル ([32 ビット])
 - Windows ゲスト エージェント ファイル ([64 ビット])

4 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ます。

- a ファイルを右クリックして [プロパティ] を選択します。
- b [全般] をクリックします。
- c [ブロック解除] をクリックします。
- d ファイルを抽出します。

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 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 Manager Service マシンを信頼するようにゲスト エージェントを構成します。

オプション	説明
接続する最初のマシンを信頼することをゲスト エージェントに許可する。	構成は必要ありません。
信頼済みの PEM ファイルを手動でインストールする。	Manager Service の PEM ファイルを C:\VRMGuestAgent\ ディレクトリに配置します。

- d **winservice -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、 winservice -i -h <load_balancer_manager_service.mycompany.com:443> -p ssl 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、 winservice -i -h <manager_service_machine.mycompany.com:443> -p ssl 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、 winservice -i -h <manager_service_machine.mycompany.com:443>:<443> -p ssl -c <ec2> と指定します。

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。

次に進む前に

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。

サーバを信頼する Windows ゲスト エージェントの構成

ゲスト エージェントを使用する各テンプレートに信頼済みの PEM ファイルを手動でインストールするのが最も安全ですが、接続する最初のマシンを信頼することをゲスト エージェントに許可することもできます。

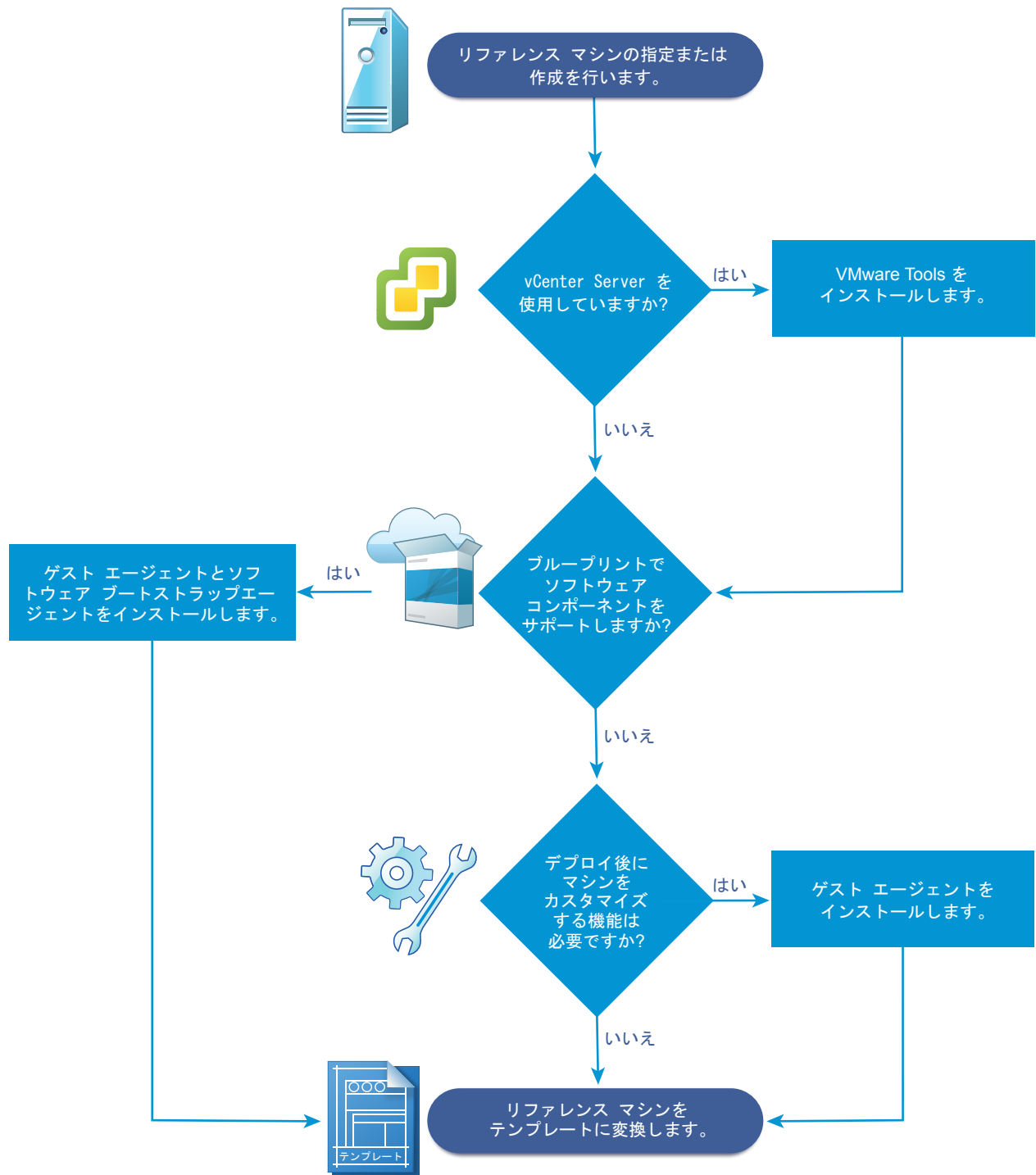
信頼されるサーバの PEM ファイルをゲスト エージェントと一緒に各テンプレートにインストールすることが最も安全なアプローチです。セキュリティ上の理由から、**VRMGuestAgent** ディレクトリに PEM ファイルがすでに存在する場合、ゲスト エージェントは証明書が存在するかどうかをチェックしません。サーバ証明書変更される場合は、新しい PEM ファイルを使用してテンプレートを手動で再構築する必要があります。

最初の使用時に信頼済み PEM ファイルにデータを取り込むようにゲスト エージェントを構成することもできます。これは各テンプレートに PEM ファイルを手動でインストールする方法よりも安全性が劣りますが、複数のサーバに単一のテンプレートを使用する可能性がある環境にとっては柔軟性が高いと言えます。接続する最初のサーバを信頼することをゲスト エージェントに許可するには、PEM ファイルを使用せずに **VRMGuestAgent** ディレクトリ内にテンプレートを作成します。ゲスト エージェントは、初めてサーバに接続するときに PEM ファイルにデータを取り込みます。このテンプレートは、それ自体が接続する最初のシステムを常に信頼します。セキュリティ上の理由から、**VRMGuestAgent** ディレクトリに PEM ファイルがすでに存在する場合、ゲスト エージェントは証明書が存在するかどうかをチェックしません。サーバ証明書が変更される場合は、**VRMGuestAgent** ディレクトリから PEM ファイルを削除する必要があります。ゲスト エージェントは、次にサーバに接続するときに新しい PEM ファイルを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

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 1-7. 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ないものの、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 アーキテククトに転送します。	「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 1-8. 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)		カスタム仕様 オブジェクトなしで Windows マシンをカスタマイズすることはできません。
(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 1-9. 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		<p>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。</p>

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。

注意 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 1-10. 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。<%System Drive %>Program Files (x86)\VMware\vCAC Agents\EPI_Agents\Scripts\SendEmail.vbs
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。<%System Drive %>Program Files (x86)\VMware\vCAC Agents\EPI_Agents\Scripts\SendEmail.vbs

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 1-11. 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		<p>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)。</p>
Linux.ExternalScript.Path		<p>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)。</p>

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 1-12. 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
<code>VirtualMachine.Admin.AddOwnerToAdmins</code>		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、 <code>True</code> （デフォルト）に設定します。
<code>VirtualMachine.Admin.AllowLogin</code>		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、 <code>True</code> （デフォルト）に設定します。
<code>VirtualMachine.Admin.UseGuestAgent</code>		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 <code>True</code> 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、 <code>False</code> に設定します。 <code>False</code> 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 <code>False</code> 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。
<code>VirtualMachine.DiskN.Active</code>		マシンのディスク <N> が有効であることを指定する場合は、 <code>True</code> （デフォルト）に設定します。マシンのディスク <N> が有効ではないことを指定する場合は、 <code>False</code> に設定します。

表 1-12. 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
<code>VirtualMachine.DiskN.Size</code>		<p>ディスク <N> のサイズ (GB) を定義します。たとえば、150 GB のサイズをディスク G に割り当てるには、カスタム プロパティ <code>VirtualMachine.Disk0.Size</code> を定義し、値として 150 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。デフォルトで、マシンには <code>VirtualMachine.Disk0.Size</code> で参照されるディスクが 1 台あります。サイズは、マシンのプロビジョニング元のブループリントにあるストレージ値によって指定されます。ブループリント ユーザー インターフェイスのストレージ値は、<code>VirtualMachine.Disk0.Size</code> プロパティの値に上書きされます。</p> <p><code>VirtualMachine.Disk0.Size</code> プロパティは、ブループリントのストレージオプションとの関係により、カスタム プロパティとして使用することはできません。</p> <p><code>VirtualMachine.Disk1.Size</code>、<code>VirtualMachine.Disk2.Size</code> のように指定することで、ディスクをさらに追加できます。</p> <p><code>VirtualMachine.Admin.TotalDiskUsage</code> は、常に <code>.DiskN.Size</code> プロパティと <code>VMware.Memory.Reservation</code> のサイズ割り当ての合計を表します。</p>
<code>VirtualMachine.DiskN.Label</code>		<p>マシンのディスク <N> 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 <N> のラベルを指定します。</p>
<code>VirtualMachine.DiskN.Letter</code>		<p>マシンのディスク N 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 <code>VirtualMachine.Disk1.Letter</code> 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 <N> をゲスト OS にマウントします。</p>

表 1-12. 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
<code>VirtualMachine.Admin.CustomizeGuestOSDelay</code>		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。
<code>VirtualMachine.Customize.WaitComplete</code>		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。
<code>VirtualMachine.SoftwareName</code>		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 <N> 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。
<code>VirtualMachine.SoftwareNameScriptPath</code>		<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スクリプト ファイルをプログラムできます。</p>

表 1-12. 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.ISO Name		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 </folder_name/subfolder_name/file_name>.iso 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.ISO Location		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 パスを指定します。ホスト予約で表示されるパスの形式に設定します (例: netapp-1:it_nfs_1)。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

NSX と統合していない場合、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。

表 1-13. ネットワーク構成のカスタム プロパティ

カスタム プロパティ	値	説明
VirtualMachine.NetworkN.Add ress		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 <N> の IP アドレスを指定します。
VirtualMachine.NetworkN.Mac AddressType		<p>これにより、ネットワーク デバイス <N> 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。デフォルト値は generated です。値が static の場合は、VirtualMachine.NetworkN.MacAddress を使用して MAC アドレスも指定する必要があります。</p> <p>VirtualMachine.Network<N> 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。</p>

表 1-13. ネットワーク構成のカスタム プロパティ (続き)

カスタム プロパティ	値	説明
<code>VirtualMachine.NetworkN.MacAddress</code>		<p>ネットワーク デバイス <N> 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 <code>generated</code> 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 <code>static</code> 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.Network<N> 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。</p>

表 1-13. ネットワーク構成のカスタム プロパティ (続き)

カスタム プロパティ	値	説明
<code>VirtualMachine.NetworkN.Name</code>		<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 <N> 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 パスからネットワークが割り当てられます。</p> <p>[VirtualMachine.NetworkN.AddressType] 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 <code>N=0</code> および <code>N=1</code> 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.Network<N> 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。</p> <p>このプロパティは、ブループリントにある vCloud Air または vCloud Director マシンコンポーネントに追加できます。</p>
<code>VirtualMachine.NetworkN.PortID</code>		<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 <N> で使用するポート ID を指定します。</p> <p>VirtualMachine.Network<N> 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。</p>

表 1-13. ネットワーク構成のカスタム プロパティ (続き)

カスタム プロパティ	値	説明
VirtualMachine.NetworkN.ProfileName		<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 <N> 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 <N> 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。<N>=0 は最初のデバイス、以降 <N>=1 は 2 番目、2 は 3 番目のデバイスというように指定します。</p> <p>VirtualMachine.NetworkN.ProfileName プロパティを使用する際には、これが指し示すネットワーク プロファイルを使用して、IP アドレスが割り当てられます。ただし、プロビジョニングされたマシンは、ラウンド ロビン方式モデルを使用して予約で選択されたネットワークに接続されます。</p>
<ul style="list-style-type: none"> VirtualMachine.NetworkN.SubnetMask VirtualMachine.NetworkN.Gateway VirtualMachine.NetworkN.PrimaryDns VirtualMachine.NetworkN.SecondaryDns VirtualMachine.NetworkN.PrimaryWins VirtualMachine.NetworkN.SecondaryWins VirtualMachine.NetworkN.DnsSuffix VirtualMachine.NetworkN.DnsSearchSuffixes 		<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.ProfileName 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>

表 1-13. ネットワーク構成のカスタム 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 vCloud Networking and Security 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 <edge/pool> 名またはコンマで区切られた <edge/pool> 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 1-13. ネットワーク構成のカスタム プロパティ (続き)

カスタム プロパティ	値	説明
VCNS.SecurityGroup.Names. <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 1 つ以上の vCloud Networking and Security 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.<name>		<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 vCloud Networking and Security 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

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。

注意 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。

vRealize Automation では、すべての vCloud Director 組織で公開済みカタログを共有する必要があります。 公開されたカタログが、すべての vCloud Director 組織で共有されていない場合、データ収集は失敗します。

次の概要では、vRA 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が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るようにします。

- 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るようにします。
 - 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。

注意 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 vCloud Automation Center Appliance 管理コンソールのインストール ページに移動します。
例： `https://<vcac-hostname.domain.name>:5480/installer/`。
- 2 Linux ゲスト エージェント パッケージをダウンロードして保存します。
- 3 **LinuxGuestAgentPkgs** ファイルを展開します。
- 4 **LinuxGuestAgentPkgs** ファイルに移動し、プロビジョニング中に展開するゲスト OS に対応するサブディレクトリを見つけます。
- 5 **sample-https.cfg** ファイルを開きます。

- 6 文字列 **host=dcac.example.net** のすべてのインスタンスを vRealize Automation サーバホストの IP アドレスまたは完全修飾ドメイン名および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 --host=172.20.9.59 と入力します。
vSphere ESX	たとえば、IP アドレスは --host=172.20.9.58 と入力します。
SUSE 10	たとえば、IP アドレスは --host=172.20.9.57 と入力します。
その他すべて	たとえば、FQDN は --host=mycompany-host1.mycompany.local:443 と入力します。

- 7 **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
```

- 8 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。

スクリプトは、**/usr/share/gugent/site/<workitem>** ディレクトリにある **./properties.xml** ファイルをどれでも参照できます。

開始する前に

- 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
```

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。

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 ネットワーク管理者に問い合わせ、次のネットワーク要件が満たされているかを確認します。
 - SCCM との通信には、SCCM サーバの NetBios 名が必要です。少なくとも 1 つの Distributed Execution Manager (DEM) で、SCCM サーバの完全修飾名が NetBios 名に解決されるようにする必要があります。
 - SCCM サーバおよび vRealize Automation サーバは、同一のネットワーク上にあり、互いに使用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。

注意 プロパティ セットが SCCMProvisioningProperties のプロパティ 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。これにより、ブループリントにこの情報を含めることが容易になります。

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

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 vCloud Automation Center Appliance 管理コンソールのインストール ページに移動します。
例: <https://<vcac-hostname.domain.name>:5480/installer/>。
- 2 Windows ゲスト エージェント ファイルをダウンロードして保存します。
 - Windows ゲスト エージェント ファイル ([32 ビット])
 - Windows ゲスト エージェント ファイル ([64 ビット])
- 3 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。
- 4 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。
- 5 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。
- 6 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。これは、リファレンス マシンにより 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、WinPE イメージをビルドするシステム、およびマシンがプロビジョニングされる仮想ホストでなければなりません。
- 2 DHCP サーバがネットワーク上で使用可能であることを確認します。DHCP が使用できない限り、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。vRealize Automation PEBuilder を使用して、ゲスト エージェントを含む WinPE イメージを作成できます。
 - [「PEBuilder のインストール」](#)。
 - (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、PEBuilder のインストールの作業アイテム ディレクトリにそのスクリプトを配置します。[「PEBuilder WinPE でのカスタム スクリプトの指定」](#) を参照してください。
 - 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 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。
 - [「PEBuilder を使用した WinPE イメージの作成」](#)。

別の方法を使用して WinPE イメージを作成できますが、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、ハイパーバイザーで提供されるドキュメントを参照してください。
- 8 次の情報を収集して、その情報をブループリントに追加できるようにします。
 - 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。

注意 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。

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 7.1 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 1-14. 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 1-15. 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

表 1-15. 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 (続き)

AutoLogon の設定値	値
Username	<p><username></p> <p>(<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。)</p>
Password	<p><password></p> <p>(<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。)</p> <p>注意 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。</p>

PEBuilder のインストール

vRealize Automation が提供している PEBuilder ツールにより、vRealize Automation ゲスト エージェントを簡単に WinPE イメージに含めることができます。

PEBuilder には、32 ビット ゲスト エージェントが組み込まれています。64 ビット固有のコマンドを実行する必要がある場合は、PEBuilder をインストールして **GugentZipx64.zip** ファイルから 64 ビット ファイルを取得します。

PEBuilder は、ステージング環境にアクセスできる場所にインストールしてください。

開始する前に

- NET Framework 4.5 をインストールする。
- Windows Automated Installation Kit (AIK) for Windows 7 (WinPE 3.0 を含む) がインストールされている必要がある。

手順

- 1 vCloud Automation Center Appliance 管理コンソールのインストール ページに移動します。
例：https://<vcac-hostname.domain.name>:5480/installer/。
- 2 PEBuilder をダウンロードします。
- 3 (オプション) Windows 32 ビット ゲスト エージェントの代わりに、Windows 64 ビット ゲスト エージェントを WinPE に組み込む場合は、Windows 64 ビット ゲスト エージェント パッケージをダウンロードします。
- 4 **VCAC-WinPEBuilder-Setup.exe** を実行します。
- 5 プロンプトの指示に従って、PEBuilder をインストールします。

- 6 (オプション) \PE Builder\Plugins\VRM Agent\VRMGuestAgent に格納されている Windows 32 ビット ゲスト エージェント ファイルを 64 ビット ファイルで置き換え、64 ビット エージェントを WinPE に組み込みます。

PEBuilder を使用することにより、WIM プロビジョニングで使用する WinPE を作成できます。

PEBuilder WinPE でのカスタム スクリプトの指定

PEBuilder を使用してマシンをカスタマイズするには、カスタムの **bat** スクリプトをプロビジョニングワークフローの指定されたポイントで実行します。

開始する前に

[PEBuilder のインストール]。

手順

- 1 使用する **bat** スクリプトを作成するか、または特定します。

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。

- 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 スクリプトを実行するプロビジョニングワークフローのポイントに対応する作業アイテム サブディレクトリ内にスクリプトを配置します。

例: C:\Program Files (x86)\VMware\vRA\PE Builder\Plugins\VRM Agent\VRMGuestAgent\site\SetupOS.

このエージェントは、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。

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 WinPE イメージを作成する前に PEBuilder インストール ディレクトリの **Plugins** サブディレクトリに VirtIO ドライバ ファイルをコピーするか、または他の方法で作成した WinPE イメージにドライバを挿入します。

- 3 **rhevms-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。

PEBuilder を使用した WinPE イメージの作成

vRealize Automation により提供される PEBuilder ツールを使用して、vRealize Automation ゲスト エージェントを含む WinPE ISO ファイルを作成します。

開始する前に

- [「PEBuilder のインストール」](#)。
- (オプション) Windows 32 ビット ゲスト エージェントではなく Windows 64 ビット ゲスト エージェントを WinPE に含めるように、PEBuilder を構成します。 [「PEBuilder のインストール」](#) を参照してください。
- (オプション) WinPE イメージに追加するサードパーティ プラグインを PEBuilder インストール ディレクトリの **プラグイン** サブディレクトリに追加します。
- (オプション) [「PEBuilder WinPE でのカスタム スクリプトの指定」](#)。

手順

- 1 PEBuilder を実行します。
- 2 IaaS Manager Service のホスト情報を入力します。

オプション	説明
ロード バランサーを使用している場合	<ol style="list-style-type: none"> a [vCAC ホスト名] テキスト ボックスに、IaaS Manager Service のロード バランサーの完全修飾ドメイン名を入力します。たとえば、manager_service_LB.mycompany.com と入力します。 b [vCAC ポート] テキスト ボックスに、IaaS Manager Service のロード バランサーのポート番号を入力します。たとえば、443 と入力します。
ロード バランサーがない場合	<ol style="list-style-type: none"> a [vCAC ホスト名] テキスト ボックスに、IaaS Manager Service マシンの完全修飾ドメイン名を入力します。たとえば、manager_service.mycompany.com と入力します。 b [vCAC ポート] テキスト ボックスに、IaaS Manager Service マシンのポート番号を入力します。たとえば、443 と入力します。

- 3 PEBuilder プラグイン ディレクトリのパスを入力します。

これは、インストール時に指定したインストール ディレクトリにより異なります。デフォルトは **C:\Program Files (x86)\VMware\VCAC\PE Builder\PlugIns** です。

- 4 [ISO 出力パス] テキスト ボックスに、作成する ISO ファイルの出力パスを入力します。

この場所は、準備したステージング エリア上にある必要があります。

- 5 [ファイル] - [詳細] をクリックします。

注意 [WinPE アーキテクチャ] または [プロトコル] の設定は変更しないでください。

- 6 [WinPE ISO へ vCAC ゲスト エージェントを含める] チェック ボックスを選択します。

- 7 [OK] をクリックします。

- 8 [ビルド] をクリックします。

次に進む前に

統合プラットフォームが要求する場所に WinPE イメージを配置します。場所が分からない場合は、プラットフォームが提供しているドキュメントを参照してください。

HP iLO マシンをプロビジョニングする場合は、Web 上でアクセスできる場所に WinPE イメージを配置します。Dell iDRAC マシンの場合は、NFS または CIFS が利用できる場所にイメージを配置します。アドレスを記録します。

WinPE イメージへのゲスト エージェントの手動挿入

vRealize Automation PEBuilder を使用して WinPE を作成する必要はありません。しかし、PEBuilder を使用しない場合、vRealize Automation ゲスト エージェントを WinPE イメージに手動で挿入する必要があります。

開始する前に

- 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

vRealize Automation PEBuilder を使用して WinPE を作成しない場合は、PEBuilder をインストールしてゲスト エージェント ファイルを手動で WinPE イメージにコピーする必要があります。

2 doagent.bat ファイルの構成

vRealize Automation PEBuilder を使用しない場合は、**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

vRealize Automation PEBuilder を使用しない場合、**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

vRealize Automation PEBuilder を使用しないことを選択する場合、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

vRealize Automation PEBuilder を使用して WinPE を作成しない場合は、PEBuilder をインストールしてゲスト エージェント ファイルを手動で WinPE イメージにコピーする必要があります。

PEBuilder には、32 ビット ゲスト エージェントが組み込まれています。64 ビット固有のコマンドを実行する必要がある場合は、PEBuilder をインストールして **GugentZipx64.zip** ファイルから 64 ビット ファイルを取得します。

開始する前に

- 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 vCloud Automation Center Appliance 管理コンソールのインストール ページに移動します。
例：https://<vcac-hostname.domain.name>:5480/installer/。
- 2 PEBuilder をダウンロードします。
- 3 (オプション) Windows 32 ビット ゲスト エージェントの代わりに、Windows 64 ビット ゲスト エージェントを WinPE に組み込む場合は、Windows 64 ビット ゲスト エージェント パッケージをダウンロードします。
- 4 **VCAC-WinPEBuilder-Setup.exe** を実行します。
- 5 [プラグイン] と [PEBuilder] の選択を解除します。
- 6 [プラグイン] を展開し、[VRMAgent] を選択します。
- 7 プロンプトの指示に従って、インストールを完了します。
- 8 (オプション) インストールが完了したら、**\PE Builder\Plugins\VRM Agent\VRMGuestAgent** に格納されている Windows 32 ビット ゲスト エージェント ファイルを 64 ビット ファイルで置き換え、64 ビット エージェントを WinPE に組み込みます。
- 9 **<%SystemDrive%>\Program Files (x86)\VMware\PE Builder\Plugins\VRM Agent\VRMGuestAgent** のコンテンツを WinPE イメージ内の新しい場所にコピーします。
例：C:\Program Files (x86)\VMware\PE Builder\Plugins\VRM Agent\VRMGuestAgent

次に進む前に

[\[doagent.bat ファイルの構成\]](#)。

doagent.bat ファイルの構成

vRealize Automation PEBuilder を使用しない場合は、**doagent.bat** ファイルを手動で構成する必要があります。

開始する前に

[\[WinPE へのゲスト エージェントのインストール\]](#)。

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\PE Builder\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、 manager_service_LB.mycompany.com:443
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、 manager_service.mycompany.com:443

- 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 **doagent.bat** を含めます。

次に進む前に

[\[doagentc.bat ファイルの構成\]](#)。

doagentc.bat ファイルの構成

vRealize Automation PEBuilder を使用しない場合、**doagentc.bat** ファイルを手動で構成する必要があります。

開始する前に

[「doagent.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\PE Builder\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。

次に進む前に

[「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

vRealize Automation PEBuilder を使用しないことを選択する場合、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。

開始する前に

[「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\PE Builder\Plugins\VRM Agent\VRMGuestAgent

- 2 ファイル **gugent.properties** のコピーを作成し、そのコピーに **gugent.properties.template** という名前を付けます。
- 3 ファイル **gugent.properties.template** のコピーを作成し、そのコピーに **gugentc.properties** という名前を付けます。
- 4 **gugent.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 **gugentc.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。

vRealize Automation は、OpenStack のいくつかのフレーバーをサポートしています。OpenStack フレーバー サポートの最新情報は、<https://www.vmware.com/support/pubs/vcac-pubs.html> の vRealize Automation のサポート マトリックス を参照してください。

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 7.1 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 プ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 プ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 プ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、プループリント アーキテクトが Amazon プループリントを作成または編集するときにプループリント 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。

開始する前に

IaaS 管理者として vRealize Automation コンソールにログインします。

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 [新規インスタンス タイプ] 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。

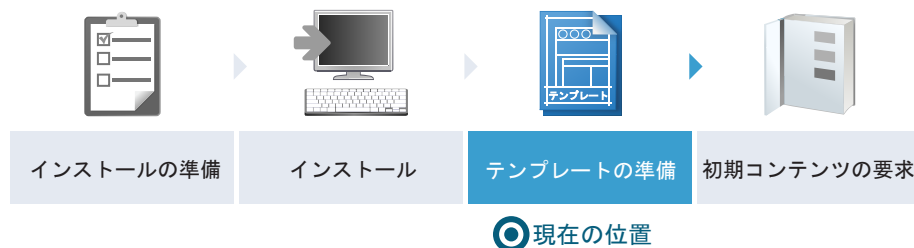
IaaS アーキテクトは、Amazon Web Services ブレープリントを作成するとき、カスタムのインスタンス タイプを使用できます。

次に進む前に

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 : Rainpole で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 Rainpole アーキテクトが vRealize Automation で CentOS マシンのクローン作成用ブレ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 ブレ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。

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 : Rainpole で Linux マシンのクローン作成用のカスタマイズ仕様を作成する

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 リファレンス 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。

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。

次に進む前に

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：Rainpole で Linux マシンのクローン作成用のカスタマイズ仕様を作成する

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。
たとえば、**rainpole.local** と入力します。
 - 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。

Linux マシンのクローン作成用のブループリントを作成するのに使用できる一般的なカスタム仕様を作成しました。

次に進む前に

vRealize Automation コンソールに、インストール時に作成した構成管理者としてログインし、PoC（事前検証）環境を簡単にセットアップするカタログ アイテムを要請します。

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 AWS 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、またはリファレンス マシンをテンプレート、スナップショット、Amazon マシン イメージに変換する前に、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た場合は、ソフトウェアをマシンに展開できます。

表 1-16. 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	必要な準備
vSphere	クローン作成	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	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	クローン作成	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	クローン作成	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 AWS	Amazon マシン イメージ	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 AWS 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。Amazon EBS がサポートする AMI の作成に関する説明については、Amazon AWS のドキュメントを参照してください。 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。

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

サポートされている Java Runtime Environment、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 Windows リファレンス マシンにインストールしてテンプレート、スナップショット、またはソフトウェア コンポーネントをサポートする Amazon マシン インスタンスを作成します。

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 ブート処理は中断してはならないため、最後にオペレーティング システムのログイン プロンプトが表示されるまで、仮想マシンのブート処理が停止しないように仮想マシンを構成します。たとえば、仮想マシンが起動するときに、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。

開始する前に

- リファレンス マシンの指定または作成を行います。
- 以前にゲスト エージェントまたはソフトウェア ブートストラップ エージェントをこのマシンにインストールしたことがある場合、エージェントおよびランタイム ログを削除します。[\[vRealize Automation での既存の仮想マシン テンプレートの更新\]](#) を参照してください。
- 仮想マシンの Windows リモート デスクトップにトラブルシューティングまたはその他の理由でリモートからアクセスすることを計画している場合は、Windows 用 Remote Desktop Services (RDS) をインストールします。
- ネットワーク構成のすべての生成物がネットワーク構成ファイルから削除されていることを確認します。
- 最も安全な方法でゲスト エージェントと Manager Service マシンの間の信頼を確立するには、Manager Service マシンから PEM 形式の SSL 証明書を取得します。Windows マシンにゲスト エージェントをインストールする方法の詳細については、[\[Windows リファレンス マシンへのゲスト エージェントのインストール\]](#) を参照してください。ゲスト エージェントが信頼を確立する方法の詳細については、[\[サーバを信頼する Windows ゲスト エージェントの構成\]](#) を参照してください。

手順

- 1 Windows リファレンス マシンに Windows 管理者としてログインし、コマンド プロンプトを開きます。
- 2 サポートされている Java Runtime Environment 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 Java SE Runtime Environment の .zip ファイルを、
`https://<vRealize_VA_Hostname_fqdn>/software/download/jre-version-win64.zip` からダウンロードします。
 - b `c:\opt\vmware-jre` フォルダを作成し、そのフォルダに JRE .zip ファイルを解凍します。
 - c コマンド プロンプト ウィンドウを開き、`c:\opt\vmware-jre\bin\java -version` と入力して、インストールを確認します。

インストールされている Java のバージョンが表示されます。

- 3 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。

- 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 Manager Service マシンを信頼するようにゲスト エージェントを構成します。

オプション	説明
接続する最初のマシンを信頼することをゲスト エージェントに許可する。	構成は必要ありません。
信頼済みの PEM ファイルを手動でインストールする。	Manager Service の PEM ファイルを C:\VRMGuestAgent\ ディレクトリに配置します。

- d コマンド **winservice -i -h <Manager_Service_Hostname_fqdn>:<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、 winservice -i -h <load_balancer_manager_service.mycompany.com:443> -p ssl 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、 winservice -i -h <manager_service_machine.mycompany.com:443> -p ssl 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、 winservice -i -h <manager_service_machine.mycompany.com:443>:<443> -p ssl -c <ec2> と指定します。

- 5 ソフトウェア エージェント ブートストラップ ファイルを、
https://<vRealize_VA_Hostname_fqdn>/software/index.html からダウンロードします。
 - a ソフトウェア ブートストラップ エージェント ファイルを
https://<vRealize_VA_Hostname_fqdn>/software/download/vmware-vra-software-agent-bootstrap-windows-<version>.zip からダウンロードします。
 - 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。

重要 この Windows セキュリティ機能を無効にしないと、ソフトウェア エージェント ブートストラップ ファイルを使用できません。

- e **vmware-vra-software-agent-bootstrap-windows-<version>.zip** ファイルを、
c:\temp フォルダに解凍します。
- 6 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。
 - a Windows CMD コンソールを開き、**c:\temp** フォルダに移動します。
 - b 次のコマンドを入力してエージェント ブートストラップをインストールします。

```
install.bat password=<Password>
managerServiceHost=<manager_service_machine.mycompany.com> managerServicePort=<443>
httpsMode=<true> cloudProvider=<ec2|vca|vcd|vsphere>
```

Manager Service のデフォルト ポート番号は 443 です。**cloudprovider** で受け入れられる値は、**ec2**、**vca**、**vcd**、および **vsphere** です。**install.bat** スクリプトによって、インストール コマンドで設定されたパスワードを使用してソフトウェア ブートストラップ エージェント用に **darwin** という名前のユーザー アカウントが作成されます。設定した **<Password>** は、Windows のパスワード要件を満たしている必要があります。

.NET の依存関係が原因でインストールが失敗した場合、サポート情報を得るには、記事 (<https://technet.microsoft.com/en-us/library/dn482071.aspx>) を参照してください。

- 7 ユーザー **darwin** が存在することを確認します。
 - a コマンド プロンプトで **lusrmgr.msc** と入力します。
 - b ユーザー **darwin_user** が存在し、管理者グループに属していることを確認します。
 - c パスワードを無期限に設定します。

この設定により、30 日後もテンプレートが使用できます。

このユーザーが使用できない場合は、Windows サーバのパスワードが正しいかどうかを確認します。

- 8 Windows 仮想マシンをシャットダウンします。

次に進む前に

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。

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

1 つのスクリプトを使用して、サポートされている Java Runtime Environment、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 Linux リファレンス マシンにインストールしてテンプレート、スナップショット、またはソフトウェア コンポーネントをサポートする Amazon マシン インスタンスを作成します。

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 ブート処理は中断してはならないため、最終的なオペレーティングシステムのログイン プロンプトに到達するまで、仮想マシンのブート処理が一時的に停止することがないように仮想マシンを構成します。たとえば、仮想マシンが起動するときに、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。

開始する前に

- Linux リファレンス マシンを指定または作成し、使用する Linux システムに応じて次のコマンドが利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

Linux の前提条件の関連情報については、**prepare_vra_template.sh** スクリプトを参照してください。

- トラブルシューティングやその他の理由で、Linux **ssh** ログを使用してリモートから仮想マシンにアクセスすることを計画している場合は、Linux の OpenSSH サーバおよびクライアントをインストールする必要があります。
- 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 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 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。

6 Linux 仮想マシンをシャットダウンします。

ソフトウェア ブートストラップ エージェントの以前のインストール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。

次に進む前に

ハイパーバイザーまたはクラウド プロバイダで、インフラストラクチャ アーキテクトがブループリントを作成するときに使用できるテンプレート、スナップショット、または Amazon マシン イメージにリファレンス マシンを変換します。

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

シナリオ：クローン マシンの vSphere CentOS 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する

vCenter Server 管理者として、vRealize Automation アーキテクトが Linux CentOS マシン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。

開始する前に

- 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 テンプレートで使用するカスタム仕様を作成します。

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。

次に進む前に

vRealize Automation のユーザー、グループ、およびリソースを構成したら、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。[「シナリオ : Rainpole でのクローン作成用の vSphere CentOS ブループリントを作成する」](#)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 Web ブラウザで、次の URL を開きます。
`https://<vrealize-automation-appliance-FQDN>/software/index.html`
- 2 `prepare_vra_template.sh` スクリプトをリファレンス マシンに保存します。
- 3 リファレンス マシンで、`prepare_vra_template.sh` を実行可能にします。

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

- 4 `prepare_vra_template.sh` を実行します。

```
./prepare_vra_template.sh
```

5 プロンプトの指示に従います。

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、`./prepare_vra_template.sh --help` と入力します。

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 リファレンス 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。

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 テンプレートで使え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。

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。

開始する前に

- vRealize Automation をインストールして完全に構成します。『Rainpole シナリオのための vRealize Automation のインストールおよび構成』を参照してください。
- 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。

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 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。

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 コンポーネントが期待ど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
```

- d ソフトウェア ブーストラップ 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 リファレンス 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 が稼働している場合は、[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マイズ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。

vCenter Server は、dukes_bank_template 参照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] ページ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。

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。

次に進む前に

- 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。 [「外部 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。

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	ローカル ユーザー アカウントの作成の例については、「シナリオ：Rainpole 用のローカル ユーザー アカウントを作成する」を参照してください。
<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」
<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 およびプラグインの構成」
<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。

この章では次のトピックについて説明します。

- [ディレクトリ管理構成オプションの選択](#)
- シナリオ：高可用性 vRealize Automation に対する Active Directory リンクを構成する
- [vRealize Automation のスマート カード認証の構成](#)
- 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
- グループとユーザーのロールの構成
- シナリオ：Rainpole 用のデフォルト テナントを構成する
- [追加テナントの作成](#)
- [テナントを削除する](#)
- [カスタム ブランディングの構成](#)
- [通知構成のチェックリスト](#)
- [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
- [vRealize Orchestrator およびプラグインの構成](#)

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 へのリンクの構成」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。ネットワーク範囲を追加したり、既存の範囲を編集したりできます。「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 ID プロバイダ インスタンスを追加したり、両方を組み合わせたりすることができます。「ID プロバイダ インスタンスの構成」 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。

- ユーザーおよびグループ データを Active Directory または LDAP ディレクトリからサービスに同期します。
- 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。サードパーティの ID プロバイダが、企業のセキュリティ ポリシーに適切な場合は、コネクタ がサポートしていない認証タイプにも、コネクタ がサポートする認証タイプにも、サードパーティ ID プロバイダを使用します。

注意 サードパーティの ID プロバイダを使用する場合は、ユーザーおよびグループ データを同期するようにコネクタを構成する、またはジャストインタイムのユーザー プロビジョニングを構成することができます。詳細については、『VMware Identity Manager の管理』の「ジャストインタイム ユーザー プロビジョニング」セクションを参照してください。

注意 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 サービスにはそれ自身のディレクトリの概念があり、これは環境の Active Directory または LDAP ディレクトリに対応しています。このディレクトリは、属性を使用してユーザーとグループを定義します。

- Active Directory
 - LDAP 経由の Active Directory 単一の Active Directory ドメイン環境に接続する場合には、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、また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異なります。通常的环境では、作成するディレクトリは 1 つです。

- LDAP ディレクトリ

サービスは Active Directory または LDAP ディレクトリに直接アクセスすることはできません。コネクタ のみが直接アクセスできます。そのため、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。ワーカーごと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 または LDAP ディレクトリとサービス間でユーザーとグループを同期します。

重要 同じ コネクタ インスタンスでは、統合 Windows 認証タイプの Active Directory 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 へのリンクの構成」](#) 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 へのリンクの構成」](#) 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 へのリンクの構成」](#) 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 へのリンクの構成」](#) 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。

Active Directory へのリンクの構成

Directories Management 機能を使用して Active Directory へのリンクを構成する必要があります。これにより、すべてのテナントのユーザー認証をサポートし、Directories Management ディレクトリと同期するユーザーおよびグループを選択することができます。

Active Directory の通信プロトコルには、LDAP 経由の Active Directory と Active Directory (統合 Windows 認証) の 2 つのオプションがあります。LDAP 経由の Active Directory プロトコルでは、デフォルトで DNS サービス ローケーション検索がサポートされます。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。

通信プロトコルを選択した後、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。

開始する前に

- 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。[「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。
- 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。
- 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。
- **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] - [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 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。
LDAP	[LDAP 経由の Active Directory] 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。

- 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。 ■ 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。 ■ 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。
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	[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。

- 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。

注意 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。

注意 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。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。

- 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。

- 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。

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。

次に進む前に

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。

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、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セカンド 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 つ目の 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 バランサー 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 バランサーに送られ、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。

開始する前に

- 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 の展開で使用できるように最適なロード バランサー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、[第 2 章「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 バランサーにログインします。
ロード バランサーの 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 バランサーをポイントするようにホスト名を変更します。

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。

開始する前に

- 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 コンソールにログインします。

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 (URI 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] の見出しの下にある + 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] ページのフィールドを使用し、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**」の場合、ユーザーは、「**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ります。一般的な展開の場合、ユーザーは **AD FS 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 ポリシーの更新を保存するには [保存] 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。ルールを作成したら、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している必要があります。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 に存在している必要があります。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 sp.xml 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。

開始する前に

- 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 コンソールにログインします。

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は、グループやユーザーを追加する場合に 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 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の数を vRealize Automation の操作に必要な数のみに制限します。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 に適した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 環境で同期を行うと、「同期が進行中」というメッセージが消えてから同期ログの詳細が表示されるまでに遅延が生じることがあります。また、ログ ファイルのタイムスタンプと、ユーザー インターフェイスに表示される同期の完了時間が一致しない場合もあります。

注意 同期を開始すると、キャンセルすることはできません。

開始する前に

- 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。
- Active Directory (統合 Windows 認証) では、マルチフォレスト Active Directory を構成しており、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のメンバーが含まれる場合、バインド ユーザーをドメイン 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必ず追加してください。これを行わなければ、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 コンソールにログインします。

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 同期オプションのダイアログを開くには、[同期設定] をクリックします。
- 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 定義に新しい行を追加して、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 定義に新しい行を追加して、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 変更をすぐに同期しないで保存する場合は [保存] をクリックし、変更の保存後、すぐに同期して実装するには [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。

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、Directories Management のメモリ割り当てを 6 GB に増やすことが推奨されます。

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

注意 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。

開始する前に

- 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働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、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 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。

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す。

[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使用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。

表 2-6. 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
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使用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

コネクタの管理

[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。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。[「ID プロバイダ インスタンスの構成」](#)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。

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

domain_krb.properties ファイルは、DNS サービス ロケーション (SRV レコード) ルックアップが有効なディレクトリに対し、どのドメイン コントローラを使用するかを決定します。このファイルには、各ドメインのドメイン コントローラのリストが含まれます。ファイルは最初にコネクタによって作成されますが、その後はユーザーが管理する必要があります。このファイルの設定は、DNS サービス ロケーション (SRV) ルックアップより優先します。

次のタイプのディレクトリは、DNS サービス ロケーション ルックアップが有効になっています。

- 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] オプションが選択されている場合に有効です。
- Active Directory (統合 Windows 認証) では、DNS サービス ロケーション ルックアップは常に有効です。

DNS サービス ロケーション ルックアップが有効なディレクトリを作成すると、まず仮想マシンの **/usr/local/horizon/conf** ディレクトリに **domain_krb.properties** ファイルが自動的に作成され、各ドメインのドメイン コントローラがファイルに自動的に記載されます。ファイルに記載するため、コネクタは、コネクタと同じサイトにあるドメイン コントローラを探し、アクセス可能で応答が最も速いドメイン コントローラを 2 つ選択します。

DNS サービス ロケーション ルックアップを有効にしたディレクトリを作成したり、新しいドメインを統合 Windows 認証ディレクトリへ追加すると、新しいドメインおよびそのドメインのドメイン コントローラのリストがファイルに追加されます。

domain_krb.properties ファイルを編集することにより、デフォルトの設定をいつでも変更できます。ベスト プラクティスとして、ディレクトリを作成したら **domain_krb.properties** ファイルを表示し、リストに含まれるドメイン コントローラが構成に最適であることを確認してください。グローバルな Active Directory 展開環境で、地理的に分散する複数のドメイン コントローラを使用する場合は、Active Directory との高速通信を確保するため、コネクタに物理的に近い場所にあるドメイン コントローラを使用します。

その他の変更を行う場合も、このファイルを手動で更新する必要があります。次のルールが適用されます。

- **domain_krb.properties** ファイルは、コネクタを含む仮想マシン内で作成されます。追加のコネクタが展開されていない一般的な環境では、Directories Management サービスの仮想マシンにファイルが作成されます。ディレクトリに追加のコネクタを使用している場合は、コネクタの仮想マシンにファイルが作成されます。1 台の仮想マシンが保持できる **domain_krb.properties** ファイルは 1 つのみです。
- DNS サービス ロケーション ルックアップが有効なディレクトリを作成すると、まずファイルが作成され、各ドメインのドメイン コントローラがファイルに自動で記載されます。
- 各ドメインのドメイン コントローラは、優先度が高い順に記載されます。Active Directory への接続を試行する際に、コネクタはリストの一番最初に記載されているドメイン コントローラを使用します。このドメイン コントローラにアクセスできない場合は、リストで 2 番目に表示されているドメイン コントローラから順に使用していきます。

- DNS サービス ロケーション ルックアップが有効になっている新しいディレクトリを作成するとき、またはドメインを統合 Windows 認証ディレクトリに追加するときのみ、ファイルが更新されます。新しいドメイン、およびそのドメインのドメイン コントローラのリストがファイルに追加されます。

ファイルにドメインのエントリがすでに存在する場合は、更新されません。たとえば、ディレクトリを作成し、その後に削除した場合、元のドメイン エントリがファイルに残り、更新されません。

- その他の状況で、ファイルの自動更新が行われることはありません。たとえば、ユーザーがディレクトリを削除した場合でも、ドメイン エントリはファイルから削除されません。
- ファイル内に記載のドメイン コントローラのいずれかにアクセスできない場合は、ファイルを編集して削除します。
- ドメイン エントリを手動で追加または編集した場合、その変更内容が上書きされることはありません。

domain_krb.properties ファイルへの自動入力に使用されるドメイン コントローラの選択方法

domain_krb.properties ファイルに自動入力するため、コネクタが ドメイン コントローラを選択する際は、最初に IP アドレスとネットマスクに基づいて、コネクタが存在するサブネットを検出します。次に、Active Directory 構成を使用してサブネットのサイトを特定し、サイトのドメイン コントローラのリストを取得します。さらに、リストのフィルタリングによって適切なドメインを絞り込み、その中から最も高速に応答するドメイン コントローラを 2 つ選び出します。

最も近い場所にあるドメイン コントローラを検出するための、VMware Identity Manager の要件は次のとおりです。

- コネクタのサブネットが Active Directory 構成内に存在するか、またはサブネットが **runtime-config.properties** ファイルに指定されている必要があります。

サブネットはサイトを判断するために使用されます。

- Active Directory 構成がサイトを認識する必要があります。

サブネットを検出できない場合、または Active Directory 構成がサイトを認識しない場合、DNS サービス ロケーション ルックアップを使用してドメイン コントローラを検出し、アクセス可能なドメイン コントローラがファイルに入力されます。これらのドメイン コントローラとコネクタが地理的に離れている場合があることに注意してください。このようなときは、Active Directory への通信で遅延やタイムアウトが発生することがあります。その場合には、**domain_krb.properties** ファイルを手動で編集して、各ドメインに適切なドメイン コントローラを指定します。

domain_krb.properties ファイルのサンプル

```
example.com=host1.example.com:389,host2.example.com:389
```

- **デフォルトで選択されたサブネットのオーバーライド**

domain_krb.properties ファイルを自動入力するため、コネクタは同一サイトのドメイン コントローラを検出しようと試みます。このため、コネクタと Active Directory の間にわずかな遅延が生じます。

■ `domain_krb.properties` ファイルの編集

`/usr/local/horizon/conf/domain_krb.properties` ファイルは、DNS サービス ロケーション ルックアップが有効になっているディレクトリに使用するドメイン コントローラを決定します。いつでもファイルを編集して、任意のドメインのドメイン コントローラ リストの変更や、ドメイン エントリの追加または削除ができます。ユーザーが加えた変更はオーバーライドされません。

■ `domain_krb.properties` のトラブルシューティング

`domain_krb.properties` ファイルのトラブルシューティングでは、次の情報を使用します。

デフォルトで選択されたサブネットのオーバーライド

`domain_krb.properties` ファイルを自動入力するため、コネクタは同一サイトのドメイン コントローラを検出しようと試みます。このため、コネクタと Active Directory の間にわずかな遅延が生じます。

コネクタはサイトを検出するため、IP アドレスとネットマスクに基づいてコネクタが存在するサブネットを検出します。次に、Active Directory 構成を使用して、そのサブネットのサイトを特定します。仮想マシンのサブネットが Active Directory に含まれていない場合、または自動選択されたサブネットをオーバーライドしたい場合は、`runtime-config.properties` ファイルにサブネットを指定します。

手順

- 1 Directories Management 仮想マシンに root ユーザーとしてログインします。

注意 ディレクトリに追加のコネクタを使用している場合は、コネクタの仮想マシンにログインします。

- 2 `/usr/local/horizon/conf/runtime-config.properties` ファイルを編集して、次の属性を追加します。

`siteaware.subnet.override=<subnet>`

<Subnet> は、使用したいドメイン コントローラを含むサイトのサブネットです。例：

`siteaware.subnet.override=10.100.0.0/20`

- 3 ファイルを保存して閉じます。
- 4 サービスを再起動します。

`service horizon-workspace restart`

`domain_krb.properties` ファイルの編集

`/usr/local/horizon/conf/domain_krb.properties` ファイルは、DNS サービス ロケーション ルックアップが有効になっているディレクトリに使用するドメイン コントローラを決定します。いつでもファイルを編集して、任意のドメインのドメイン コントローラ リストの変更や、ドメイン エントリの追加または削除ができます。ユーザーが加えた変更はオーバーライドされません。

このファイルは、最初にコネクタにより作成され、自動入力されます。シナリオによっては手動で更新する必要があります。

- デフォルトで選択されたドメイン コントローラが構成に最適でない場合は、ファイルを編集して、使用するドメイン コントローラを指定します。

- ディレクトリを削除する場合は、対応するドメイン エントリをファイルから削除します。
- ファイルに含まれるいずれかのドメイン コントローラにアクセスできない場合は、ファイルから削除します。

「[ドメイン コントローラの選択](#)」も参照してください。

手順

- 1 Directories Management 仮想マシンに root ユーザーとしてログインします。

注意 ディレクトリに追加のコネクタを使用している場合は、コネクタの仮想マシンにログインします。

- 2 ディレクトリを `/usr/local/horizon/conf` に変更します。

- 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または編集します。

次の形式を使用します。

```
<domain>=<host>:<port>,<host2>:<port>,<host3>:<port>
```

たとえば、 のように指定します。

```
example.com=examplehost1.example.com:389,examplehost2.example.com:389
```

リスト内のドメイン コントローラを優先度順に並べます。Active Directory への接続を試行する際に、コネクタはリストの一番最初に表示されているドメイン コントローラを使用します。このドメイン コントローラにアクセスできない場合は、リストで 2 番目に表示されているドメイン コントローラから順に使用していきます。

重要 ドメイン名は小文字にする必要があります。

- 4 次のコマンドを使用して、**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
```

- 5 サービスを再起動します。

```
service horizon-workspace restart
```

domain_krb.properties のトラブルシューティング

domain_krb.properties ファイルのトラブルシューティングでは、次の情報を使用します。

「ドメイン解決エラー」の問題

domain_krb.properties ファイルにドメインのエントリがすでに含まれているときに、同じドメインに異なるタイプの新しいディレクトリを作成しようとすると、「ドメイン解決エラー」というエラーが発生します。新しいディレクトリを作成する前に、**domain_krb.properties** ファイルを編集して、ドメイン エントリを手動で削除する必要があります。

ドメイン コントローラにアクセスできない問題

ドメイン エントリが `domain_krb.properties` ファイルに追加されると、自動的に更新されなくなります。ファイルに表示されるいずれかのドメイン コントローラにアクセスできなくなった場合は、手動でファイルを編集して削除します。

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。

注意 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 ベースを決定します。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。

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。

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。

デフォルト ポリシー

ポリシー名: default_access_policy_set

説明: Default access policy set

適用先: すべてのアプリケーション

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。
- 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じになります。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。

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

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時間数を選択します。

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 SecurID 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。

開始する前に

- 環境に適した ID プロバイダを選択または構成します。[\[ID プロバイダ インスタンスの構成\]](#) 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 コンソールにログインします。

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。

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コ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。

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 (続き)

認証タイプ	説明
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。

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て、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。

開始する前に

- 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 コネクタ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。

次に進む前に

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。

開始する前に

- 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 サーバで使用す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す。
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。

オプション	アクション
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 sdconf.rec ）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。

次に進む前に

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。

開始する前に

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 コンソールにログインします。

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。
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。

次に進む前に

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。

Directories Management 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を使用して認証したり、スマート カード アダプタを使用して認証したりできます。証明書による認証は、ユーザーが所有するもの (秘密鍵またはスマート カード) とユーザーが知ること (秘密鍵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。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。

■ 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。

■ 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。

■ 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。

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、電子メール 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 タイプを有効化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。

OCSP レスポンダ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。

開始する前に

- 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、証明書失効リストのファイルの場所および OCSP サーバの URL。
- (オプション) OCSP 応答署名証明書ファイルの場所。
- 認証の前に同意書を表示する必要がある場合は、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 マネージャーのログイン ページにリダイレクトされます。
- 4 証明書認証アダプタのページで構成します。

注意 アスタリスクが付いている情報は、必ず入力する必要があります。

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、CertificateAuthAdapter です。この名前は変更できません。
証明書アダプタを有効にする	証明書認証を有効にするには、このチェック ボックスをオンにします。
*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	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。
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 をさらに追加します。
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。証明書失効チェックにより、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 Online Certificate Status Protocol (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 の両方を構成した場合。このチェック ボックスを選択すると、OCSP チェックが使用できない場合に CRL を使用できます。

オプション	説明
OCSP Nonce を送信する	応答時に、OCSP 要求の一意の ID を送信する場合は、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 レスポンダの署名証明書	レスポンダの 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。

5 [保存] をクリックします。

次に進む前に

- 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。

ID プロバイダ インスタンスの構成

vRealize Automation にはデフォルトの ID プロバイダ インスタンスが付属しています。ユーザーが、別の ID プロバイダ インスタンスを作成することも可能です。

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。既存の企業の 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。

開始する前に

- 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 コンソールにログインします。

手順

- 1 [管理] - [ディレクトリ管理] - [ID プロバイダ] の順に移動します。

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] 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編集します。

フォーム アイテム	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。
ネットワーク	<p>サービス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。
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。

- 3 [追加] をクリックします。

次に進む前に

- サードパーティの ID プロバイダ インスタンスを構成するために必要な 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。

注意 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。

開始する前に

- 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 コンソールにログインします。

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 ポッド	View ポッド 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。

次に進む前に

- 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。

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。

開始する前に

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 編集するポリシー ルール ページを開くには、[認証方法] 列の認証名をクリックします。新しいポリシー ルールを追加する場合は、[+] アイコンをクリックします。
 - a ネットワーク範囲が正しいことを確認します。新しいルールを追加する場合は、このポリシー ルールのネットワーク範囲を選択します。
 - b [およびユーザーのコンテンツ アクセス元が次の場合...] ドロップダウン メニューから、このルールで管理するデバイス タイプを選択します。

- c 認証の順序を構成します。[次に、以下の方法を使用して認証する必要があります] ドロップダウン メニューから、最初に適用する認証方法を選択します。

2 つの認証方法で認証を行うことをユーザーに要求するには、[+] をクリックし、2 番目の認証方法を入力します。

- d (オプション) 最初の認証が失敗したら追加の認証方法を使用するよう構成するには、有効な別の認証方法をその横のドロップダウン メニューから選択します。

ルールには複数のフォールバック認証方法を追加できます。

- e [再認証までの待機時間] テキスト ボックスに、ユーザーによる再認証が必要になるまでの時間数を入力します。

- f (オプション) ユーザー認証が失敗した場合に表示する、アクセス拒否のカスタム メッセージを作成します。最大 4,000 文字、約 650 ワードを使用できます。ユーザーを別のページに誘導する場合は、[リンク URL] テキスト ボックスで URL リンクを追加します。[リンク テキスト] テキスト ボックスに、リンクに表示するテキストを入力します。このテキスト ボックスを空白のままにした場合は、**続行** という文字が表示されます。

- g [保存] をクリックします。

- 4 [保存] をクリックします。

ポリシー ルールの編集

The screenshot displays the 'Policy Rule' configuration page. At the top, there are two dropdown menus for scope: 'ユーザーのネットワーク範囲が次の場合...' (set to 'すべての範囲') and 'およびユーザーのコンテンツアクセス元が次の場合...' (set to 'Web ブラウザ'). Below these, a section titled '次に、以下の方法を使用して認証する必要があります...' contains three dropdowns: 'Password', 'および', and an empty one. Underneath is '前の認証方式に失敗した場合は:' with '認証方法の選択-' and '専用'. A green box with a plus sign and 'フォールバック方法' is highlighted. At the bottom, '再認証までの待機時間:' is set to '8 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。

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 [KerberosldpAdapter] 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 [KerberosldpAdapter] 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、KerberosldpAdapter 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。

次に進む前に

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] 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 Kerberos 認証方法をルールに追加します。

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。

注意 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。

開始する前に

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 イントラネット] 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 イントラネット] 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。

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。

開始する前に

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。

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。

注意 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。

開始する前に

- 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。

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。

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セカンド 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。

開始する前に


- 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 7.1 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 コンソールにログインします。

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_admininfra,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。

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。

次に進む前に

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 のスマート カード認証の構成

システム管理者は、ディレクトリ管理を使用して vRealize Automation 展開にスマート カード認証を構成する必要があります。

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。スマート カード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。

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。[「Directories Management 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。

開始する前に

- 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 コンソールにログインします。

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。

開始する前に

- **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] - [ディレクトリ管理] - [コネクタ] を選択します。
- 2 [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。
- 3 [Enter] キーを押します。

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。

- 4 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。

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。

開始する前に

- 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。

ページ	説明
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、[カスタマ 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> <hr/> <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> <hr/> <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。

次に進む前に

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。

開始する前に

- 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 の内部コネクタに自己署名証明書を使用している場合は、[ルート CA 証明書]情報も入力する必要があります。

ルート CA 証明書は <https://:8443/cfg/ssl> から入手することができます。[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。

次に進む前に

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。

注意 Directories Management 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。

開始する前に

証明書の署名要求 (CSR) を生成し、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 <https://<myconnector.mycompany>:8443/cfg> 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。

- 2 管理コンソールで、[アプライアンス設定] をクリックします。

デフォルトで VA 構成が選択されます。

- 3 [構成の管理] をクリックします。

- 4 表示されるダイアログ ボックスで、Directories Management サーバの管理者ユーザー 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 アプライアンス上の SSL の終了] タブで、[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 秘密キーを [秘密キー] 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-----

jlQvt9WdR9Vpg3WQT5+C3HU17bUOwvhp/r0+

...

...

...

W53+O05j5xsxzDJfWr1lqBIFf/OkiYCPcyK1

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

WdR9Vpg3WQT5+C3HU17bUOwvhp/rjlQvt90+

...

...

...

O05j5xsxzDJfWr1lqBIFf/OkiYCPW53+cyK1

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

証明書チェーンの例

```
dR9Vpg3WQTjIQt9W5+C3HU17bUOwvhp/r0+
...
...
5j5xsxzDJfWr1lqW53+O0BIFF/OkiYCPcyK1
-----END CERTIFICATE-----
```

秘密キーの例

```
-----BEGIN RSA PRIVATE KEY-----
jIQtg3WQT5+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。

開始する前に

- **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] - [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 表示されるメニューで [ワークスペース 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 この 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り、この ID プロバイダを使用した選択で表示されるコネクタが決定されます。
- 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。

注意 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 この ID プロバイダにアクセスするための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。

開始する前に

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] - [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。

開始する前に

- 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 7.1 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 コンソールにログインします。
- 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。

注意 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。

次に進む前に

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。

開始する前に

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] - [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 [アップデート] をクリックします。

現在、vRealize Automation コンソール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 コンソールにログインし直す必要があります。

次に進む前に

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もあります。これらの場合、ロールを割り当てる必要はありません。

開始する前に

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] - [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 [追加] アイコン (+) をクリックします。

- 3 [新規グループ名] 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) [新規グループの説明] 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 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 というフォームでユーザー名またはグループ名全体を入力することで、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 [追加] をクリックします。

現在、vRealize Automation コンソール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 コンソールにログインし直す必要があります。

ビジネス グループの作成

ビジネス グループを使用して、サービスとリソースのセットをユーザー セット（多くの場合、事業、部門、または他の組織単位に対応）に関連付けます。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。

開始する前に

- 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。
- 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。
- ビジネス グループのメンバーによってプロビジョニングされたマシンの名前の先頭に付加される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がマシン プリフィックスを申請します。[「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
名前	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。
マネージャの電子メールの送信先	1 つ以上のユーザー名またはグループ名を入力します。 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 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。この時点でユーザーを指定する必要はありません。後で取り込む空のビジネス 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。
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。

6 [次へ] をクリックします。

7 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	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。 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。ブループリントはデフォルトのプリフィックスを使用するように構成されていますが、ここでデフォルトのプリフィックスを指定しない場合、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。 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。
Active Directory コンテナ	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。 プロビジョニングされたマシンを AD コンテナに追加するには、他のプロビジョニング方法の構成を追加する必要があります。

8 [追加] をクリックします。

ファブリック管理者は、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ことが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。

次に進む前に

- 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。

ビジネス グループ データの不足に関するトラブルシューティング

ビジネス グループが見つからないか、ビジネス グループのデータが欠落しています。

問題

既知のビジネス グループを探す場合、該当のビジネス グループが[管理]-[ユーザーおよびグループ]-[ビジネス グループ]で見つからない、または想定していた予約や資格と連携していないことがあります。

原因

ビジネス グループの情報は CAFE と IaaS の 2 つのデータベースに格納されており、その情報は同一でなければなりません。一般的な運用では、このデータベースの同期が維持されます。前述の問題が発生した場合は、強制的な同期が必要になることがあります。

同期が想定どおりに行われている場合でも、アップグレードをすると、この問題が発生する可能性があります。また、API を使用して、新規または変更したビジネス グループの IaaS データベースをアップデートした場合、この問題が発生する可能性があります。

解決方法

開始する前に

コマンド ラインでコマンドを実行するようにしてください。『プログラミング ガイド』を参照してください。

手順

- ◆ vcac-cli コマンド ラインでコマンドを実行します。

コマンドによるアップデート内容	コマンド	コマンドの短縮形
IaaS 値で CAFE データベースを同期する	Vcac-Config.exe SynchronizeDatabases -- DatabaseSyncSource IaaS -v	Vcac-Config.exe SynchronizeDatabases -dss IaaS -v
CAFE 値で IaaS データベースを同期化する	Vcac-Config.exe SynchronizeDatabases -- DatabaseSyncSource Cafe -v	Vcac-Config.exe SynchronizeDatabases -dss Cafe -v

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で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。

シナリオ：Rainpole 用のデフォルト テナントを構成する

システム管理者として、vRealize Automation インスタンスを継続的な開発環境として構成しようと思います。ローカル ユーザー アカウントを作成し、自分をテナント管理者ロールに割り当てます。テナント管理者の権限を使用して、まず vRealize Automation を開発環境として構成し、ブループリントを作成しテストできるようにします。



手順

1 シナリオ：Rainpole 用のローカル ユーザー アカウントを作成する

デフォルトのシステム管理者権限を使用して、デフォルト テナントに 2 つのローカル ユーザー アカウントを作成します。これらのアカウントのいずれかをテナント管理者ロールに割り当て、デフォルト テナントの構成を開始します。2 つ目のアカウントは、ブループリントとカタログのアクセスをテストするために、アーキテクトのための共有ログインとして後で使用することができます。

2 シナリオ：企業 Active Directory を Rainpole 用の vRealize Automation に接続する

テナント管理者として、vRealize Automation で企業 Active Directory に対するログインの認証を行おうとしています。vRealize Automation とシングル ドメインの Active Directory との間の LDAP による接続を構成します。

3 シナリオ：Rainpole 用のデフォルト テナントのブランディングを構成する

テナント管理者の権限を使用して、vRealize Automation コンソールの外観をカスタマイズします。新しいロゴをアップロードし、色を変更し、ヘッダーおよびフッター情報を更新し、ログイン画面のブランディングを構成します。

4 シナリオ：Rainpole アーキテクトのカスタム グループを作成する

テナント管理者の権限を使用して、vRealize Automation への特権的なアクセスが必要な IT 部門のメンバーのためのカスタム グループを作成します。vRealize Automation を構成するとき、このカスタム グループにロールを割り当てます。

5 シナリオ : IaaS 管理者の権限を Rainpole アーキテクトのカスタム グループに割り当てる

デフォルトのシステム管理者権限を使用して、カスタム グループを IaaS 管理者ロールに割り当てることで、そのグループが IaaS リソースを構成できるようにします。

シナリオ : Rainpole 用のローカル ユーザー アカウントを作成する

デフォルトのシステム管理者権限を使用して、デフォルト テナントに 2 つのローカル ユーザー アカウントを作成します。これらのアカウントのいずれかをテナント管理者ロールに割り当て、デフォルト テナントの構成を開始します。2 つ目のアカウントは、ブループリントとカタログのアクセスをテストするために、アーキテクトのための共有ログインとして後で使用することができます。

手順

- 1 vRealize Automation コンソール(<https://vra01svr01.rainpole.local/vcac>)に移動します。
- 2 デフォルトのシステム管理者ユーザー名 **administrator** と、パスワード **VMware1!** を入力します。
- 3 [管理] - [テナント] を選択します。
- 4 [vsphere.local] をクリックします。
- 5 [ローカル ユーザー] タブを選択します。
- 6 [新規] アイコン (+) をクリックします。
- 7 ローカル ユーザー アカウントを作成し、テナント管理者ロールに割り当てます。

オプション	入力
名	Rainpole
姓	tenant admin
メール	メール アドレスを入力するか、プレースホルダ rainpole_tenant_admin@rainpole.com を使用します。
ユーザー名	Rainpole tenant admin
パスワード	VMware1!

- 8 [OK] をクリックします。
- 9 [新規] アイコン (+) をクリックします。
- 10 ユーザーとアーキテクトが後でブループリントとカタログのアクセスのテストのために構成できる、ローカル ユーザー アカウントを作成します。

オプション	入力
名	test
姓	user
メール	メール アドレスを入力するか、プレースホルダ test_user@rainpole.com を使用します。

オプション	入力
ユーザー名	test_user
パスワード	VMware1!

- 11 [OK] をクリックします。
- 12 [管理者] タブをクリックします。
- 13 [テナント管理者] 検索ボックスに **Rainpole** と入力し、Enter キーを押します。Rainpole テナント管理ユーザーを選択します。
テナント管理者ロールが Rainpole テナント管理ユーザーに割り当てられます。
- 14 [完了] をクリックします。
- 15 コンソールからログアウトします。

Rainpole テナント管理ローカル ユーザーを使用してテナント管理設定にアクセスし、テナントを構成することができます。test_user アカウントは、アーキテクトとカタログ管理者のための共有ログインとして役立ちます。このアカウントを基本ユーザーとして構成し、ブループリントとカタログのアクセスを確認して、承認の動作をテストすることができます。

次に進む前に

既存の企業 Active Directory に対してログインを認証するように vRealize Automation を構成します。

シナリオ：企業 Active Directory を Rainpole 用の vRealize Automation に接続する

テナント管理者として、vRealize Automation で企業 Active Directory 対するログインの認証を行おうとしています。vRealize Automation とシングル ドメインの Active Directory との間の LDAP による接続を構成します。

手順

- 1 vRealize Automation コンソール(<https://vra01svr01.rainpole.local/vcac>)に移動します。
- 2 ユーザー名 **Rainpole tenant admin** とパスワード **VMware1!** を入力します。
- 3 [管理] - [ディレクトリ管理] - [ディレクトリ] を選択します。
- 4 [ディレクトリの追加] をクリックします。
- 5 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	vra01svr01.rainpole.local
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=rainpole,dc=local] と入力します。

オプション	入力例
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=rainpole,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。

- 6 [接続をテスト] ボタンをクリックし、構成したディレクトリへの接続をテストします。
- 7 [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。
- 8 デフォルトのドメイン設定を受け入れ、[次へ] をクリックします。
- 9 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、[次へ] をクリックします。
- 10 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=rainpole,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 [ユーザーの選択] ページのデフォルト設定を受け入れ、[次へ] をクリックします。
- 11 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。

vRealize Automation と同期させたい Active Directory のユーザーやグループに権限を割り当て、アクセス権を付与できます。

次に進む前に

テナント管理者の権限を使用して、vRealize Automation コンソールの外観をカスタマイズします。

シナリオ：Rainpole 用のデフォルト テナントのブランディングを構成する

テナント管理者の権限を使用して、vRealize Automation コンソールの外観をカスタマイズします。新しいロゴをアップロードし、色を変更し、ヘッダーおよびフッター情報を更新し、ログイン画面のブランディングを構成します。

手順

- 1 [管理] - [ブランディング] - [ヘッダおよびフッタのブランディング] を選択します。
- 2 [デフォルトの使用] チェック ボックスをオフにします。

- 3 画面の指示に従ってヘッダーを作成します。
- 4 [次へ] をクリックします。
- 5 画面の指示に従ってフッターを作成します。
- 6 [完了] をクリックします。

行った変更により、コンソールがアップデートされます。

- 7 [管理] - [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。
- 8 画面の指示に従ってログイン画面のブランディングをカスタマイズします。
- 9 [保存] をクリックします。

行った変更により、コンソールがアップデートされます。

デフォルト テナントのコンソールの外観が更新されました。

次に進む前に

vRealize Automation に特権的にアクセスする必要がある IT 部門のメンバーのためにカスタム グループを作成します。

シナリオ : Rainpole アーキテクトのカスタム グループを作成する

テナント管理者の権限を使用して、vRealize Automation への特権的なアクセスが必要な IT 部門のメンバーのためのカスタム グループを作成します。vRealize Automation を構成するとき、このカスタム グループにロールを割り当てます。

複数の場所で個々のユーザーの設定を編集しなくても、グループのメンバーシップを変更すれば、ユーザーに対するハイレベルのアクセス権を追加したり無効にしたりできます。

手順

- 1 [管理] - [ユーザーおよびグループ] - [カスタム グループ] 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、**Rainpole architects** と入力します。
- 4 [このグループにロールを追加する] リストからロールを選択します。

このページでは、IaaS 管理者、ファブリック管理者、ビジネス グループ マネージャ、ビジネス ユーザーのロールを割り当てることはできません。これらのロールは、vRealize Automation を構成するときに割り当てます。

オプション	説明
テナント 管理者	ユーザーとグループの管理、テナントのブランディングと通知、および承認、資格の付与などのビジネス ポリシーを担当します。テナント内のすべてのユーザーのリソース使用量の追跡および仮想マシンの再利用要求の開始も行います。
インフラストラクチャ (IaaS) アーキテクト	マシン ブループリントとアプリケーション ブループリントを作成し管理します。

オプション	説明
XaaS アーキテクト	Advanced および Enterprise のライセンス ユーザーの場合は、XaaS ブループリントを作成して管理します。
ソフトウェア アーキテクト	Enterprise のライセンス ユーザーの場合は、ソフトウェア コンポーネントとアプリケーション ブループリントを作成して管理します。

5 [次へ] をクリックします。

6 企業 Active Directory のユーザーを検索し、カスタム グループに追加するユーザーを選択します。

このグループには、自分の他に、vRealize Automation 開発環境への特に高いアクセス権を必要とするユーザーを割り当てます。

7 [完了] をクリックします。

デフォルト タレントを管理する権限、ブループリントを作成する権限、サービス カタログを管理する権限がカスタム グループに割り当てられました。vRealize Automation を構成するとき、権限やロールをカスタム グループに追加します。

次に進む前に

カスタム グループを IaaS 管理者ロールに割り当てます。

シナリオ：IaaS 管理者の権限を Rainpole アーキテクトのカスタム グループに割り当てる

デフォルトのシステム管理者権限を使用して、カスタム グループを IaaS 管理者ロールに割り当てることで、そのグループが IaaS リソースを構成できるようにします。

手順

- 1 vRealize Automation コンソールからログアウトします。
- 2 [vsphere.local] ドメインを選択し、[次へ] をクリックします。
- 3 デフォルトのシステム管理者ユーザー名 **administrator** と、パスワード **vmware** を入力します。
- 4 [管理] - [テナント] を選択します。
- 5 デフォルトのテナント名 [vsphere.local] をクリックします。
- 6 [管理者] タブをクリックします。
- 7 [IaaS 管理者] 検索ボックスで **Rainpole architects** を検索し、カスタム グループを選択します。
- 8 [完了] をクリックします。
- 9 コンソールからログアウトします。

これで、カスタム グループのメンバーは、vRealize Automation インスタンスのすべてのテナントについて、クラウド、仮想、ネットワーク、ストレージ インフラストラクチャを管理できるようになります。これらの権限は、グループのメンバーシップを更新することにより、いつでも付与したり取り消したりできます。

次に進む前に

カスタム グループに付与した IaaS 管理者の権限を使用して、IaaS リソースを構成できます。

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。

開始する前に

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 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 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 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。

開始する前に

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。

注意 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。

注意 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。

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。

開始する前に

- 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 7.1 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。

開始する前に

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。

これで、vRealize Automation 導入環境からテナントが削除されます。

(オプション) 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。

注意 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。

開始する前に

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 [効果] という見出しの下にあるチェック ボックスで視覚効果を選択します。
すべての効果の使用は任意です。
- 4 [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。
- 5 [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。
- 6 必要に応じて、[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。
- 7 必要に応じて、[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。
- 8 [保存] をクリックして、設定を適用します。

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。

開始する前に

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 ヘッダに表示されます。
 - 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。

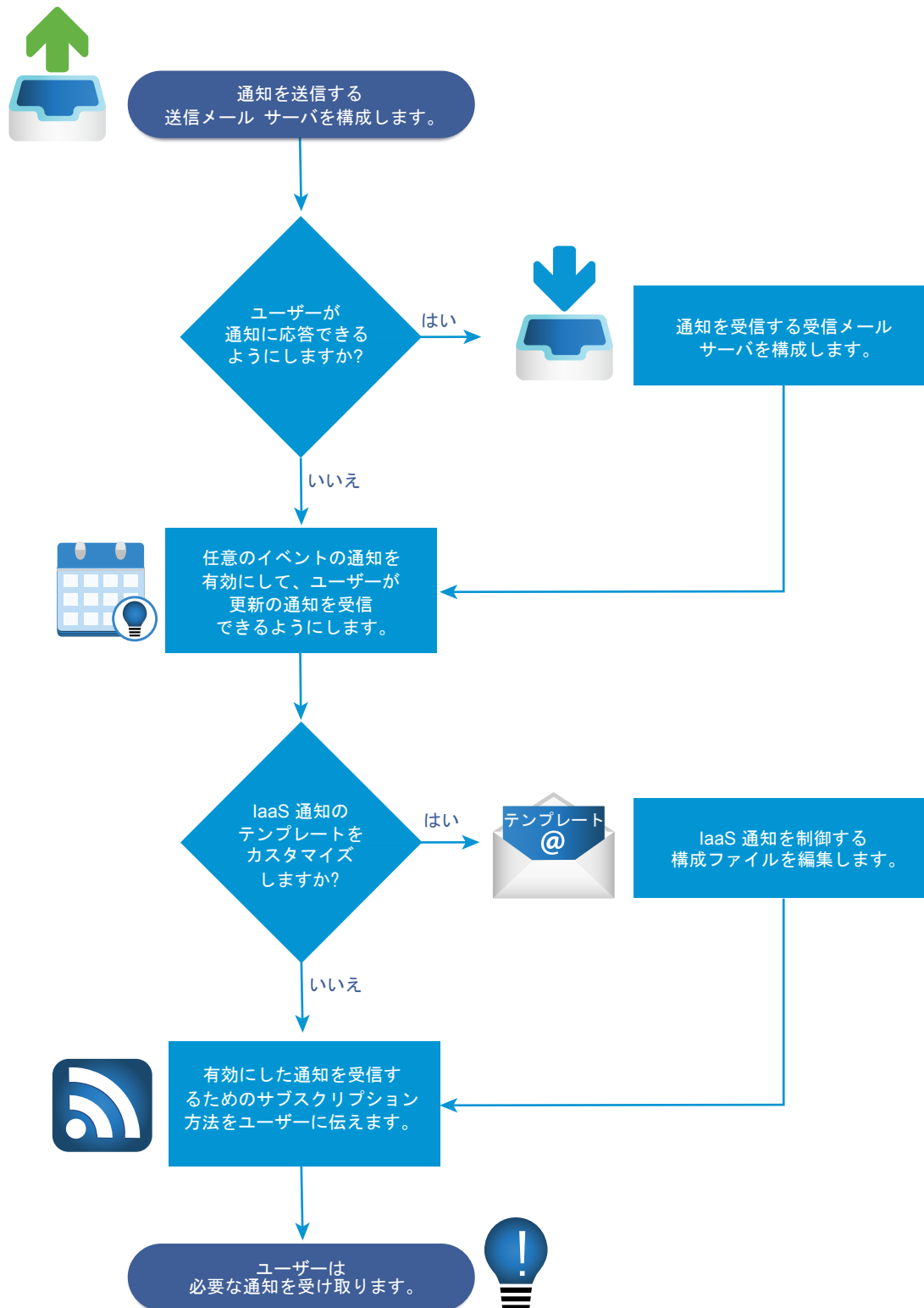
必要に応じて、16 進数の色コードのリストをインターネットで検索します。
 - e [16 進数のテキスト色] フィールドにテキストの色にする 16 進数のコードを入力します。

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。

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。

(オプション) 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 2-9. 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。 ■ テナント管理者は自分のテナントに対してサーバを構成します。 	自分のテナントに対して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"/> 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 <code>%SystemDrive%\Program Files x86\VMware\VCAC\Server</code>) 下のディレクトリ <code>\Templates</code> 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"/> 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します。 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。

開始する前に

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。

開始する前に

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のある電子メール 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。

開始する前に

- 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。
- 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。

開始する前に

- 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。
- 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。

開始する前に

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] - [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。

開始する前に

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] - [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。

開始する前に

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] - [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。

開始する前に

- 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。
- 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。

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
```

次に進む前に

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 メール通知の構成、有効化、無効化の詳細については、次のナレッジベース記事を参照してください。

- [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、vRealize Automation から通知を受信するように登録できます。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。

開始する前に

vRealize Automation コンソールにログインします。

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。

(オプション) 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。

注意 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。

開始する前に

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>\Website\Rdp` にコピーします。

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。

(オプション) 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。



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。

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。

vRealize Orchestrator およびプラグインの構成

VMware 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 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。

構成権限

システムおよびテナント管理者は外部 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。

テナントのデフォルト ワークフロー フォルダの構成

システム管理者はワークフローをさまざまなフォルダにグループ化して、テナントごとにワークフロー カテゴリを定義できます。こうすることで、システム管理者はさまざまなテナントのユーザーに、同一 vRealize Orchestrator サーバ上のさまざまなワークフロー フォルダへのアクセス権を付与できます。

開始する前に

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] - [アドバンスド サービス] - [デフォルトの vRO フォルダ] を選択します。
- 2 編集するテナントの名前をクリックします。
- 3 vRealize Orchestrator ワークフロー ライブラリを参照してフォルダを選択します。
- 4 [追加] をクリックします。

テナントのデフォルトの vRealize Orchestrator ワークフロー フォルダが定義されました。

次に進む前に

デフォルトのワークフロー フォルダを定義するすべてのテナントに対して、手順を繰り返します。

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 申請で 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。

開始する前に

- 外部 vRealize Orchestrator サーバをインストールして構成します。vRealize Orchestrator アプライアンスを展開することもできます。『VMware vCenter 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。
- 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、1 つの共通の vCenter Single Sign-On を使用するように vRealize Orchestrator と vRealize Automation を構成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 [アップデート] をクリックします。

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 アクションが自動的に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。

次に進む前に

vRealize Orchestrator プラグインをエンドポイントとして構成します。[「XaaS リソースの構成」](#)を参照してください。

vRealize Orchestrator 構成インターフェイスへのログイン

vRealize Automation に組み込まれたデフォルトの vRealize Orchestrator インスタンスの構成を編集するには、vRealize Orchestrator 構成サービスを開始し、vRealize Orchestrator 構成インターフェイスにログインする必要があります。

デフォルトでは、vRealize Orchestrator 構成サービスは vRealize Automation アプライアンスで起動されません。vRealize Orchestrator 構成インターフェイスにアクセスするには、vRealize Orchestrator 構成サービスを起動する必要があります。

手順

- 1 vRealize Orchestrator 構成サービスを起動します。
 - a vRealize Automation アプライアンス Linux コンソールに root ユーザーとしてログインします。
 - b **service vco-configurator start** と入力して、Enter を押します。
- 2 完全修飾ドメイン名 (<https://<vra-vd-hostname.domain.name>>) を使用して vRealize Automation アプライアンス 管理コンソールに移動します。
- 3 [vRealize Orchestrator コントロール センター] をクリックします。
<https://<vra-vd-hostname.domain.name>:8283/vco-controlcenter> にリダイレクトされます。
- 4 vRealize Orchestrator コントロール センターにログインします。
 ユーザー名は、vRealize Automation アプライアンス 管理者によって構成されます。
- 5 (オプション) 初めてログインする場合は、デフォルトのパスワードを変更して、[変更の適用] をクリックします。
 新しいパスワードは 8 文字以上で、1 文字以上の数字、1 文字以上の特殊文字、1 文字以上の大文字が含まれている必要があります。

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 完全修飾ドメイン名 (<https://<vra-vd-hostname.domain.name>>) を使用して vRealize Automation アプライアンス 管理コンソールに移動します。
- 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てプロンプトの指示に従います。
- 4 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。
- 5 vRealize Orchestrator クライアントのユーザー名およびパスワードを使用してログインします。
 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。

6 【証明書の警告】 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、証明書の警告を受信します。

オプション	説明
無視	現在の SSL 証明書を使用して続行します。 同じ vRealize Orchestrator サーバに再接続した場合またはリモート 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。
この証明書をインストールし、セキュリティ警告をこれ以上表示しない。	証明書をインストールし、セキュリティ警告が表示されないようにするには、このチェックボックスを選択し、[無視] をクリックします。

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。

次に進む前に

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。

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。

この章では次のトピックについて説明します。

- [IaaS リソース設定のチェックリスト](#)
- [XaaS リソースの構成](#)
- [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](#)
- [Active Directory ポリシーの操作](#)

IaaS リソース設定のチェックリスト

IaaS 管理者とファブリック管理者は、IaaS 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。

IaaS リソースの設定チェックリストを使用すると、IaaS リソースの設定に必要な手順の概要を表示できます。

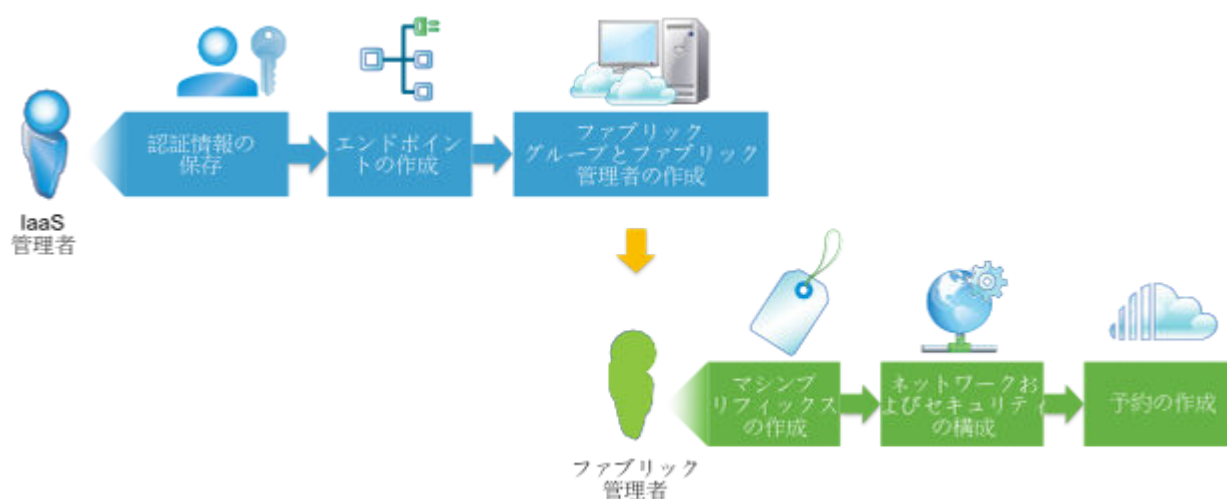


表 3-1. IaaS リソース設定のチェックリスト

タスク	vRealize Automation ロール	詳細
<input type="checkbox"/> 管理者レベルの認証情報をインフラストラクチャに保存します。	IaaS 管理者	「ユーザー認証情報の格納」 。 次のプラットフォームのいずれかを統合する場合、認証情報を提示する必要はありません。 <ul style="list-style-type: none"> ■ XenServer の Xen プール ■ XenServer ■ vSphere (システム管理者が統合認証情報を使用するようにプロキシ エージェントを設定した場合)
<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。	IaaS 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。	IaaS 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。	<ul style="list-style-type: none"> ■ ファブリック管理者としても設定されている場合は、IaaS 管理者 ■ ファブリック管理者 	「予約と予約ポリシーの設定」 。

ユーザー認証情報の格納

vRealize Automation がエンドポイントと通信できるようにするため、環境に適した管理者レベルの認証情報を格納する必要があります。複数のエンドポイントに同じ認証情報を使用できるため、認証情報はエンドポイントとは別に管理し、エンドポイントを作成または編集するときに関連付けるようにする必要があります。

開始する前に

IaaS 管理者として vRealize Automation コンソールにログインします。

手順

- 1 [インフラストラクチャ] - [エンドポイント] - [認証情報] を選択します。
- 2 [新規認証情報] 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 [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。

プラットフォーム	フォーマットと詳細
vSphere	domain\username カスタム属性を変更できる権限を持つ認証情報を入力します。
vCloud Air	エンドポイント ユーザー インターフェイスで指定された username 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。
vCloud Director	エンドポイント ユーザー インターフェイスで指定された username 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。 <ul style="list-style-type: none"> ■ 単一のエンドポイントを持つすべての組織を管理するには、システム管理者の認証情報を入力します。 ■ 別々のエンドポイントを持つ各組織の仮想データセンター (vDC) を管理するには、各 vDC の個別の組織管理認証情報を作成します。 同一の vCloud Director インスタンスに対して、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。
vRealize Orchestrator	username@domain vRealize Automation から呼び出すすべてのワークフローで実行権限を持つ各 vRealize Orchestrator インスタンスの認証情報を入力します。
vCloud Networking and Security (vSphere のみ)	domain\username
NSX (vSphere のみ)	username
Amazon AWS	アクセス キー ID を入力します。アクセス キー ID と秘密アクセス キーの取得については、Amazon AWS のドキュメントを参照してください。
Cisco UCS Manager	username
Dell iDRAC	username
HP iLO	username
Hyper-V (SCVMM)	domain\username
KVM (RHEV)	username@domain
NetApp ONTAP	username
Red Hat OpenStack	username すべての Red Hat OpenStack テナントで管理者である単一ユーザーの認証情報を入力するか、各テナントの個別の認証情報を作成します。

6 [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。

プラットフォーム	フォーマット
Amazon AWS	秘密アクセス キーを入力します。アクセス キー ID と秘密アクセス キーの取得については、Amazon AWS のドキュメントを参照してください。
その他すべて	入力したユーザー名のパスワードを入力します。

7 [保存] アイコン (👍) をクリックします。

次に進む前に

これで、認証情報が格納され、エンドポイントを作成する準備ができました。[「エンドポイント シナリオの選択」](#)を参照してください。

エンドポイント シナリオの選択

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ます。エンドポイントの作成手順は、マシン プロビジョニングのニーズに応じて異なります。

ターゲットのエンドポイント タイプに基づいてエンドポイント シナリオを選択します。

表 3-2. エンドポイント シナリオの選択

環境	エンドポイントの作成
vSphere	「vSphere エンドポイントの作成」
vSphere と NSX	「ネットワークとセキュリティが統合された vSphere エンドポイントの作成」
ストレージ用の Net App FlexClone テクノロジーを使用する vSphere	「NetApp ONTAP エンドポイントの作成」
vRealize Orchestrator	「vRealize Orchestrator エンドポイントの作成」
外部 IP アドレス管理プロバイダのエンドポイント	「外部 IP アドレス管理プロバイダのエンドポイントの作成」
vCloud Air サブスクリプションまたは OnDemand	「vCloud Air エンドポイントの作成」
vCloud Director	「vCloud Director エンドポイントの作成」
Hyper-V Standalone	「スタンドアロン Hyper-V エンドポイントの作成」
SCVMM (Microsoft Center Virtual Machine Manager) を使用する Hyper-V	「Hyper-V (SCVMM) エンドポイントの作成」
KVM (RHEV)	「KVM (RHEV) エンドポイントの作成」
Amazon クラウド サービス アカウント	<ul style="list-style-type: none"> ■ 「Amazon エンドポイントの作成」 ■ (オプション) 「Amazon インスタンス タイプの追加」
OpenStack テナント	「OpenStack エンドポイントまたは PowerVC エンドポイントの作成」
PowerVC	「OpenStack エンドポイントまたは PowerVC エンドポイントの作成」
XenServer の Xen プール	「Xen プール エンドポイントの作成」
XenServer	「XenServer エンドポイントの作成」
エンドポイントのリストをインポートする	<ul style="list-style-type: none"> ■ 「インポート用のエンドポイント CSV ファイルの準備」 ■ 「エンドポイントのリストのインポート」

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行えるようにします。

vSphere 環境が NSX と統合されている場合は、[「ネットワークとセキュリティが統合された vSphere エンドポイントの作成」](#)を参照してください。

開始する前に

- **laaS 管理者**として vRealize Automation コンソールにログインします。
- 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 7.1 のインストールを参照してください。
- システム管理者が、統合された認証情報を使用できるようにプロキシを構成しなかった場合は、エンドポイントの管理者レベルの認証情報を保存する必要があります。 [「ユーザー認証情報の格納」](#) 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] - [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。
これは、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 [認証情報] をクリックして、このエンドポイント用に保存した管理者レベルの認証情報を選択します。
システム管理者が、統合された認証情報を使用できるように vSphere プロキシ エージェントを構成した場合、[統合] 認証情報を選択できます。
- 7 構成で NSX をサポートしない限り、[ネットワークおよびセキュリティ プラットフォームのマネージャを指定] を選択しないでください。
この設定は、NSX を使用する実装のために、追加の設定が必要になります。
- 8 (オプション) [カスタム プロパティ] セクションで [新規] をクリックして、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意味のあるエンドポイント 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。
- 9 [OK] をクリックします。

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。

重要 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。

次に進む前に

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。

ネットワークとセキュリティが統合された vSphere エンドポイントの作成

vRealize Automation が、vSphere 環境や NSX インスタンスと通信できるエンドポイントを作成できます。

開始する前に

- **laaS 管理者**として vRealize Automation コンソールにログインします。
- vSphere プロキシ エージェントをインストールして、vSphere エンドポイント进行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 7.1 のインストールを参照してください。
- vSphere エンドポイントと、ネットワークおよびセキュリティ エンドポイント用の管理者レベルの認証情報を保存します。[「ユーザー認証情報の格納」](#)を参照してください。システム管理者がプロキシ エージェントを構成して、統合された認証情報を使用している場合は、NSX の認証情報のみを保存する必要があります。
- 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。

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。

これは、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 [認証情報] をクリックして、このエンドポイント用に保存した管理者レベルの認証情報を選択します。

システム管理者が、統合された認証情報を使用できるように vSphere プロキシ エージェントを構成した場合、[統合] 認証情報を選択できます。

7 ネットワーク ソリューション プラットフォームを構成します。

この手順は、NSX のネットワーク機能およびセキュリティ機能を有効にするために必要です。

- a [ネットワークおよびセキュリティ プラットフォームのマネージャを指定] を選択します。
- b [アドレス] テキスト ボックスに NSX 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://nsx-manager** と指定します。

- c [認証情報] をクリックして、このエンドポイント用に保存した管理者レベルの認証情報を選択します。

8 (オプション) カスタム プロパティを追加します。

9 [OK] をクリックします。

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。

重要 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。

次に進む前に

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。

vRealize Orchestrator エンドポイントの作成

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。

開始する前に

- **laaS 管理者**として vRealize Automation コンソールにログインします。
- ユーザー認証情報を設定します。『vRealize Automation の構成』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] - [オーケストレーション] - [vCenter Orchestrator] を選択します。
- 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 エンドポイントの優先度を指定します。
 - 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、**VMware.VCenterOrchestrator.Priority** と入力します。
このプロパティ名は大文字と小文字が区別されます。
 - c [値] 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。
 - d [保存] アイコン (🟢) をクリックします。
- 6 [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。テスト環境で vRealize Automation ワークフローを実行するときや、POC（事前検証）を作成するときに、vRealize Orchestrator エンドポイントとしてこのインスタンスを使用することをお勧めします。

外部 vRealize Orchestrator サーバにプラグインをインストールすることもできます。

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。

プラグインをインストールするには、VMware の製品ダウンロード サイト (<http://vmware.com/web/vmware/downloads>) の vCloud Networking and Security または NSX のリンクからプラグインのインストーラ ファイルと一緒に取得できる README を参照してください。

外部 IP アドレス管理プロバイダのエンドポイントの作成

IP アドレス管理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 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 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。

注意 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。

開始する前に

- 「外部 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 でワークフローを実行し、Infoblox IP アドレス管理エンドポイント タイプを登録する」。
- IaaS 管理者として vRealize Automation コンソールにログインします。
- ユーザー認証情報を設定します。『vRealize Automation の構成』を参照してください。

この例では、インポート済みの **Infoblox VMware Plug-in for vCenter Orchestrator** パッケージに登録されているエンドポイント タイプを使用して、Infoblox の 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] 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) [カスタム プロパティ] セクションで [新規] をクリックして、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意味のあるエンドポイント 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。

次に進む前に

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。

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。

注意 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。

開始する前に

- **laaS 管理者**として vRealize Automation コンソールにログインします。
- 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。
- [「ユーザー認証情報の格納」](#)。

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 [認証情報] をクリックして、このエンドポイント用に保存した管理者レベルの認証情報を選択します。

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。

- 6 (オプション) [プロキシ サーバの使用] チェック ボックスをオンにして、追加のセキュリティを構成し、強制的に接続がプロキシ サーバを通過するようにします。

- a [ホスト名] テキスト ボックスに、プロキシ サーバのホスト名を入力します。
- b [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。
- c (オプション) [認証情報] テキスト ボックスの横にある [参照] アイコンをクリックします。

プロキシ構成が必要な場合は、プロキシ サーバのユーザー名とパスワードを示す認証情報を選択または作成します。

- 7 (オプション) 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。

次に進む前に

[「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。

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。

注意 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。

開始する前に

- **laaS 管理者**として vRealize Automation コンソールにログインします。
- [「ユーザー認証情報の格納」](#)。

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 [認証情報] をクリックして、このエンドポイント用に保存した管理者レベルの認証情報を選択します。
 - 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 へ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。

- 7 (オプション) [プロキシ サーバの使用] チェック ボックスをオンにして、追加のセキュリティを構成し、強制的に接続がプロキシ サーバを通過するようにします。
 - a [ホスト名] テキスト ボックスに、プロキシ サーバのホスト名を入力します。
 - b [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。
 - c (オプション) [認証情報] テキスト ボックスの横にある [参照] アイコンをクリックします。
プロキシ構成が必要な場合は、プロキシ サーバのユーザー名とパスワードを示す認証情報を選択または作成します。
- 8 (オプション) カスタム プロパティを追加します。
- 9 [OK] をクリックします。

次に進む前に

[「ファブリック グループの作成」](#)。

Hyper-V (SCVMM) エンドポイントの作成

IaaS 管理者はエンドポイントを作成して、vRealize Automation が 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行えるようにします。

開始する前に

- IaaS 管理者として vRealize Automation コンソールにログインします。
- [「ユーザー認証情報の格納」](#)。

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 [認証情報] をクリックして、このエンドポイント用に保存した管理者レベルの認証情報を選択します。
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) 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。

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。

次に進む前に

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。

スタンドアロン Hyper-V 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 サーバ環境と通信し、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行えるようにします。

開始する前に

- IaaS 管理者として vRealize Automation コンソールにログインします。
- 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 7.1 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 [コンピュート リソース] テキスト ボックスに Hyper-V サーバの完全修飾 DNS 名を入力します。
- 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。

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。

次に進む前に

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。

NetApp ONTAP 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 Net App FlexClone テクノロジーを使用するストレージ デバイスと通信できるようにします。

開始する前に

- **IaaS 管理者**として vRealize Automation コンソールにログインします。
- [「ユーザー認証情報の格納」](#)。

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] - [ストレージ] - [NetApp ONTAP] 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: **netapp-1.mycompany.local**。
- 6 [認証情報] をクリックして、このエンドポイント用に保存した管理者レベルの認証情報を選択します。
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) 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。

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。

次に進む前に

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。

KVM (RHEV) 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 KVM (RHEV) 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行えるようにします。

開始する前に

- **laaS 管理者**として vRealize Automation コンソールにログインします。
- [「ユーザー認証情報の格納」](#)。

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] - [KVM (RHEV)] 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、**https://<FQDN>** または **https://<IP_address>** のいずれかのタイプにする必要があります。

例: **https://mycompany-kvmrhev1.mycompany.local**

- 6 [認証情報] をクリックして、このエンドポイント用に保存した管理者レベルの認証情報を選択します。
認証情報をまだ保存していない場合は、ここで保存できます。
- 7 (オプション) 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。

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。

次に進む前に

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。

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 と Xen プール マスターが通信し、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行えるようにします。

開始する前に

- **laaS 管理者**として vRealize Automation コンソールにログインします。

- 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 7.1 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 [コンピュート リソース] テキスト ボックスに Xen プール マスターの名前を入力します。

注意 Xen プールの名前は入力しないでください。プール マスターの名前を入力する必要があります。

vRealize Automation のコンピュート 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、構成済みの Xen プール マスター 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 マスター アドレスがホスト名を使用している場合、FQDN 以外のホスト名を入力します。Xen プール マスター アドレスが FQDN を使用する場合は、FQDN と入力します。

- 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。

vRealize Automation では、エンドポイントからデータを収集して、コンピュート リソースを検出します。

次に進む前に

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。

XenServer 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 XenServer 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行えるようにします。

開始する前に

- **IaaS 管理者**として vRealize Automation コンソールにログインします。
- 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 7.1 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 [コンピュート リソース] テキスト ボックスに XenServer サーバの完全修飾 DNS 名を入力します。
- 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。

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。

次に進む前に

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 エンドポイントの作成

エンドポイントを作成して、Amazon Web Services インスタンスに接続できます。

開始する前に

- **laaS 管理者**として vRealize Automation コンソールにログインします。
- [「ユーザー認証情報の格納」](#)。

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 Web Services アカウントを示します。
- 4 [認証情報] をクリックして、このエンドポイント用に保存した管理者レベルの認証情報を選択します。
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 つだけです。
- 5 (オプション) [プロキシ サーバの使用] チェックボックスをクリックして追加のセキュリティを構成し、Amazon Web Services への接続を強制してプロキシ サーバを通過させます。
 - a [ホスト名] テキスト ボックスに、プロキシ サーバのホスト名を入力します。
 - b [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。
 - c (オプション) [認証情報] テキスト ボックスの横にある [参照] アイコンをクリックします。
プロキシ構成が必要な場合は、プロキシ サーバのユーザー名とパスワードを示す認証情報を選択または作成します。
- 6 (オプション) カスタム プロパティを追加します。
- 7 [OK] をクリックします。

エンドポイントが作成されると、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。

次に進む前に

vRealize Automation は、ブループリント作成時に使用する複数の Amazon Web Services 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。

開始する前に

IaaS 管理者として vRealize Automation コンソールにログインします。

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 [新規インスタンス タイプ] 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。

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。

次に進む前に

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 エンドポイントまたは PowerVC エンドポイントの作成

vRealize Automation が OpenStack や PowerVC 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。

開始する前に

- **laaS 管理者**として vRealize Automation コンソールにログインします。
- [「ユーザー認証情報の格納」](#)。
- 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 7.1 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。

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 https://<FQDN>/powervc/openstack/<service> の形式にする必要があります。たとえば、 https://openstack.mycompany.com/powervc/openstack/admin のように指定します。
Openstack	URL は <FQDN>:5000 または <IP_address>:5000 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 /v2.0 サフィックスを含めないでください。たとえば、 https://openstack.mycompany.com:5000 のように指定します。

- 5 [認証情報] をクリックして、このエンドポイント用に保存した管理者レベルの認証情報を選択します。
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 (オプション) 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。

次に進む前に

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。

エンドポイントのリストのインポート

エンドポイントの CSV ファイルのインポートは、vRealize Automation コンソールを使用してエンドポイントを 1 つずつ追加するよりも効率的です。

開始する前に

- **laaS 管理者**として vRealize Automation コンソールにログインします。
- エンドポイントの認証情報を保存します。
- インポート用にエンドポイント CSV ファイルを準備します。

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 [エンドポイントのインポート] をクリックします。
- 3 [参照] をクリックします。
- 4 エンドポイントを含む CSV ファイルを特定します。
- 5 [開く] をクリックします。

エンドポイントのリストを含む CSV ファイルが次の形式で開きます。

```
InterfaceType,Address,Credentials,Name,Description
vCloud,https://abxpoint2vco,svc-admin,abxpoint2vco,abxpoint
```

- 6 [インポート] をクリックします。

エンドポイントは、vRealize Automation コンソールを介して編集および管理できます。

インポート用のエンドポイント CSV ファイルの準備

vRealize Automation コンソールを使用して一度に 1 つずつエンドポイントを追加する代わりに、CSV ファイルをアップロードして、エンドポイントのリストをインポートできます。

CSV ファイルには、必要なフィールドが入ったヘッダー行を含める必要があります。フィールドは、大文字と小文字が区別され、特定の順序で並んでいる必要があります。同じ CSV ファイルを使用し、さまざまなタイプのエンドポイントを複数アップロードできます。vCloud Director の場合は、組織管理者エンドポイントではなく、システム管理者アカウントがインポートされます。

表 3-3. エンドポイントをインポートするための CSV ファイル フィールドとその順序

フィールド	説明
InterfaceType	(必要) さまざまなタイプのエンドポイントを単一のファイルでアップロードできます。 <ul style="list-style-type: none"> ■ vCloud Air ■ vCloud Director ■ vRealize Orchestrator ■ vSphere ■ Amazon EC2 ■ OpenStack ■ NetAppOnTap ■ SCVMM ■ KVM
Address	(Amazon を除くすべてのインターフェイス タイプに必要) エンドポイント用の URL。使用しているプラットフォーム タイプに要求される形式の詳細については、そのプラットフォームのエンドポイントの作成に対応する手順を参照してください。
Credentials	(必須) vRealize Automation でユーザー認証情報を格納したときにその認証情報に指定した名前。
Name	(必須) エンドポイントの名前を指定します。OpenStack の場合、デフォルトの名前としてアドレスが使用されます。
Description	(オプション) エンドポイントの説明を入力します。
OpenstackProject	(OpenStack のみに必要) エンドポイントのプロジェクト名を指定します。

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 エンドポイントに対するデータ収集に失敗するのは、多くの場合、プロキシ名とエンドポイント名の不一致が原因です。

問題

vSphere エンドポイントに対する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。

例、

```
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。

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。

組織の仮想データ センターで vCloud Air の管理 URL を特定することに関するトラブルシューティング

vCloud Air エンドポイントを作成するには、vRealize Automation に必須の vCloud Air リージョンおよび管理 URL を提供する必要があります。

解決方法

vCloud Air 管理 URL は、特定の仮想データ センター (vDC) の管理に使用される vCloud Director サーバの URL でもあります。 リージョン情報と管理 URL を使用して、vCloud Air エンドポイントを構成できます。

vCloud Air コンソールから、各リージョン vDC の管理 URL を指定します。

手順

- 1 vCloud Air コンソールに管理権限でログインします。
- 2 vCloud Air ダッシュボードから、仮想データ センターを選択します。
- 3 リンクをクリックして、API コマンドで使用する仮想データ センターの URL を表示します。

例: <https://mycompany.com:443/cloud/org/vCloudAutomation/>。

vRealize Automation に入力する必要がある管理 URL は API コマンド URL のホストおよびポート部分、またリージョンは **cloud/org/** に続く URL の部分です。 例において、管理 URL は <https://mycompany.com:443>、リージョンは **vCloudAutomation** です。

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。

開始する前に

- **laaS 管理者**として vRealize Automation コンソールにログインします。
- 1 つ以上のエンドポイントを作成する。

手順

- 1 [インフラストラクチャ]-[ファブリック グループ] を選択します。
- 2 [新規ファブリック グループ] 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名またはグループ名を入力し、Enter を押します。

この手順を繰り返して、複数のユーザーまたはグループをそのロールに追加します。

- 6 1 つ以上の [コンピュー トリソース] をクリックし、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。

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 コンソール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 コンソール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。

開始する前に

ファブリック管理者として vRealize Automation コンソールにログインします。

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] 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 [桁数] テキスト ボックスに、カウンタの桁数を入力します。
- 5 [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。
- 6 [保存] アイコン (🟢) をクリックします。

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。

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。

開始する前に

- ファブリック管理者として vRealize Automation コンソールにログインします。
- 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 [保存] アイコン () をクリックします。

[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。

開始する前に

- ファブリック管理者として vRealize Automation コンソールにログインします。
- 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。

開始する前に

- **ファブリック管理者**として vRealize Automation コンソールにログインします。
- 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。

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。外部ネットワーク 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 プロバイダの外部 IP アドレス管理パッケージを使用して定義できます。

ネットワーク プロファイルで利用できる 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。ネットワーク プロファイルは、予約上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。

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。

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。

表 3-4. 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>提供されている VMware の内部 IP アドレス管理プロバイダから取得される IP アドレス範囲や、vRealize Orchestrator でインポート、登録した外部 IP アドレス管理プロバイダソリューション (Infoblox IP アドレス管理など) から取得される IP アドレス範囲を使用することもできます。</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>
NAT	<p>プロビジョニング中に作成されます。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ネットワークです。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>NAT ネットワーク プロファイルでは、双方向通信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>
経路指定済み	<p>プロビジョニング中に作成されます。分散論理ルータ (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 空間を示します。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>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>分散論理ルータの詳細については、『NSX 管理ガイド』を参照してください。</p>

ネットワーク プロファイルの使用による固定 IP アドレス範囲の割り当て

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 キャンパスに追加し、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。

必要な場合は、提供されている VMware 内部 IP アドレス管理サービス プロバイダまたは登録済みの外部 IP アドレス管理サービス プロバイダを使用して、IP アドレスを取得および設定できます。外部 IP アドレス管理の要件については、「[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](#)」を参照してください。

ネットワーク プロファイルで外部 IP アドレス管理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。

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。

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。ただし、固定 IP アドレスを回収するプロセスは 30 分ごとに実行されるため、マシンが削除されて未使用状態になったアドレスが、すぐに他のマシンで使用可能になるわけではありません。ネットワーク プロファイルの IP アドレスが使用できない場合、マシンを、関連付けられたネットワーク パスの固定 IP 割り当てを使用してプロビジョニングすることはできません。

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。

次のエントリの例では、NIC オフセットが指定されていません。

```
100.10.100.1,mymachine01,Unallocated
```

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、外部 IP アドレス管理プロバイダから IP アドレスを取得することもできます。

- IP アドレスの初期範囲を vRealize Automation ネットワーク プロファイルにインポートします。
- インポートした値を適用して、最初の名前付きのネットワーク範囲をネットワーク プロファイルに作成します。
- 1 つまたは複数の IP アドレスをネットワーク範囲から削除します。vRealize Automation
- 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。

外部 IP アドレス管理エンドポイント タイプを使用するネットワーク プロファイルの場合、IP アドレスが vRealize Automation ではなく外部 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] オプションはありません。

開始する前に

- **ファブリック管理者**として vRealize Automation コンソールにログインします。
- 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。[「外部 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。そこで、最初の 2 つのタブで、基本的なネットワーク プロファイル情報を入力します。
- 5 オプションで、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。

■ [追加] をクリックします。

- a [ネットワーク範囲] テキスト ボックスに新しい名前を入力します。
- 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 [開始 IP アドレス] テキスト ボックスに入力します。
- d 範囲の終了 IP アドレスを [終了 IP アドレス] テキスト ボックスに入力します。

■ [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
```

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。

- 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。

次に進む前に

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。

外部ネットワーク プロファイルの作成

既存のネットワーク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ネットワークのプロパティと固定 IP アドレスの範囲は、外部ネットワーク プロファイルを作成することによって定義できます。

必要に応じて、提供されている内部 IP アドレス管理プロバイダを使用するか、または vRealize Orchestrator でインポート、設定、登録したサードパーティの外部 IP アドレス管理プロバイダ (Infoblox など) パッケージを使用することができます。

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、[「外部 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 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。

2 外部ネットワーク プロファイルの IP アドレス範囲の設定

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。

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、[「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」](#)と [「外部 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。

開始する前に

- **ファブリック管理者**として vRealize Automation コンソールにログインします。

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 [既存] または [外部] を選択します。
- 3 名前と説明（説明は任意）を入力します。
- 4 (オプション) [IP アドレス管理エンドポイント] ドロップダウン メニューに表示される内部 [VMware] IP アドレス管理エンドポイントを受け入れます。
- 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。
たとえば、255.255.0.0 のように入力します。
- 6 Edge またはルーティング ゲートウェイのアドレスを [ゲートウェイ] テキスト ボックスに入力します。
- 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。

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、外部 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。

DNS サフィックスは、DNS 名を登録および解決する際に使用されます。

- 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。

次に進む前に

固定 IP アドレスの IP アドレス範囲を設定できます。 [「外部ネットワーク プロファイルの IP アドレス範囲の設定」](#)を参照してください。

外部ネットワーク プロファイルの IP アドレス範囲の設定

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。

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。

開始する前に

[「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。

■ [追加] をクリックします。

- a [ネットワーク範囲] テキスト ボックスに新しい名前を入力します。
- 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 [開始 IP アドレス] テキスト ボックスに入力します。
- d 範囲の終了 IP アドレスを [終了 IP アドレス] テキスト ボックスに入力します。

■ [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
```

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。

- 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] をクリックして、ネットワーク プロファイルを完了します。

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。

外部 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

マシンをプロビジョニングにするとときに使用するネットワークのプロパティと固定 IP アドレスの範囲は、既存のネットワークを使用して外部ネットワーク プロファイルを作成することによって定義できます。vRealize Orchestrator でインポート、設定、登録した外部 IP アドレス管理プロバイダを使用することができます。

登録されている 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、「[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 [登録済み IP アドレス管理エンドポイントの外部ネットワーク 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 登録されている IP アドレス管理エンドポイント用に外部ネットワーク 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。

次に進む前に

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、オンデマンド NAT ネットワーク プロファイル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。

登録済み IP アドレス管理エンドポイントの外部ネットワーク 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。

開始する前に

- 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。[「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」](#)を参照してください。
- [「外部 IP アドレス管理プロバイダの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 コンソールにログインします。

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 [既存] または [外部] を選択します。
- 3 名前と説明（説明は任意）を入力します。
- 4 外部 IP アドレス管理サービス プロバイダが設定されている場合は、[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、登録済みの IP アドレス管理エンドポイント名を選択できます。

vRealize Orchestrator で登録した外部 IP アドレス管理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 エンドポイントから取得されます。サブネット マスク、ゲートウェイ、および DNS/WINS の各オプションは使用できません。これらの機能は、選択した IP アドレス管理エンドポイントで制御されるためです。サブネット マスク、ゲートウェイ、および DNS/WINS の各オプションの値は、選択した IP アドレス管理エンドポイントによって提供されます。

次に進む前に

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。

登録されている IP アドレス管理エンドポイント用に外部ネットワーク 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。

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 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。

開始する前に

[「登録済み IP アドレス管理エンドポイントの外部ネットワーク 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。

- 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。

次に進む前に

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。

NAT ネットワーク プロファイルの作成

オンデマンドの NAT ネットワーク プロファイルを作成して NAT ネットワークを定義し、固定 IP アドレスと DHCP アドレスの範囲を割り当てることができます。

手順

1 NAT ネットワーク プロファイル情報の指定

ネットワーク プロファイルにより、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するその他の値が指定されます。

2 NAT ネットワーク プロファイルの 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。

NAT ネットワーク プロファイル情報の指定

ネットワーク プロファイルにより、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するその他の値が指定されます。

開始する前に

- ファブリック管理者として vRealize Automation コンソールにログインします。
- 外部ネットワーク プロファイルを作成します。[「外部ネットワーク プロファイルの作成」](#)または[「外部 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 [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 表示される内部 [VMware] IP アドレス管理プロバイダのデフォルトの [IP アドレス管理エンドポイント] 値を受け入れるか、または vRealize Orchestrator にインポートして登録した別の IP アドレス管理プロバイダ エンドポイント（Infoblox など）を選択します。

注意 オンデマンド NAT ネットワークとオンデマンドルーティング ネットワークでは、外部 IP アドレス管理を使用できません。

- 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	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。
1 対多	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。

- 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。

たとえば、255.255.0.0 のように入力します。

- 8 Edge またはルーティング ゲートウェイのアドレスを [ゲートウェイ] テキスト ボックスに入力します。

標準的な IPv4 アドレス形式を使用します。たとえば、10.10.110.1 のように入力します。

- 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。

- 10 (オプション) リース時間を設定して、マシンで 1 つの IP アドレスを使用可能な時間を定義します。

- 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。

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、外部 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。

DNS サフィックスは、DNS 名を登録および解決する際に使用されます。

- 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。

次に進む前に

[\[NAT ネットワーク プロファイルの IP アドレス範囲の設定\]](#) .

NAT ネットワーク プロファイルの 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。

開始する前に

[\[NAT ネットワーク プロファイル情報の指定\]](#) .

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。

■ [追加] をクリックします。

- [ネットワーク範囲] テキスト ボックスに新しい名前を入力します。
- ネットワーク範囲の説明を入力します。
- 範囲の開始 IP アドレスを [開始 IP アドレス] テキスト ボックスに入力します。
- 範囲の終了 IP アドレスを [終了 IP アドレス] テキスト ボックスに入力します。

■ [CSV からインポート] をクリックします。

- 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
```

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。

- [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。

ルーティング ネットワーク プロファイルの作成

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して、ルーティング ネットワークで使用できるルーティング可能な IP アドレス空間とサブネットを定義できます。

手順

1 ルーティング ネットワーク プロファイル情報の指定

ネットワーク プロファイル情報では、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。

2 ルーティング ネットワーク プロファイルの 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。

ルーティング ネットワーク プロファイル情報の指定

ネットワーク プロファイル情報では、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。

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。

開始する前に

- **ファブリック管理者**として vRealize Automation コンソールにログインします。
- 外部ネットワーク プロファイルを作成します。[「外部ネットワーク プロファイルの作成」](#) または [「外部 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。
- NSX 論理ルータがルーティング ネットワーク プロファイルを使用するように vSphere Client 内で設定されていることを確認します。[『NSX 管理ガイド』](#) を参照してください。

手順

- 1 [インフラストラクチャ] - [予約] - [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 [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ネットワーク プロファイルを選択します。
- 5 表示される内部 [VMware] IP アドレス管理プロバイダのデフォルトの [IP アドレス管理エンドポイント] 値を受け入れるか、または vRealize Orchestrator にインポートして登録した別の IP アドレス管理プロバイダ エンドポイント (Infoblox など) を選択します。

注意 オンデマンド NAT ネットワークとオンデマンド ルーティング ネットワークでは、外部 IP アドレス管理を使用できません。

- 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。
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 ボックスに値を入力し、**[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。
- 8 最初の使用可能な IP アドレスを [ベース IP] テキスト ボックスに入力します。[ベース IP] と [サブネット マスク範囲] の設定を使用して範囲が生成されます。
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。

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、外部 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。

DNS サフィックスは、DNS 名を登録および解決する際に使用されます。

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。

次に進む前に

[「ルーティング ネットワーク プロファイルの IP アドレス範囲の設定」](#)。

ルーティング ネットワーク プロファイルの 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。

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 空間として使用します。

開始する前に

[「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 ~ Range<n> 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。

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ボ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。

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。

注意 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 上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

- Hyper-V
- KVM
- OpenStack
- SCVMM
- XenServer

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 3-5. 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 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」

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。

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。

注意 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.Disk<N>.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.Disk<N>.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 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 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 の予約に割り当てる必要があります。を参照してください。

注意 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。

注意 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。

開始する前に

- **ファブリック管理者**として vRealize Automation コンソールにログインします。

- 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] を選択します。
- 3 (オプション) [既存の予約からコピー] ドロップダウン メニューから、既存の予約を選択します。
選択した予約のデータが表示されます。新規予約は必要に応じて変更できます。
- 4 [名前] テキスト ボックスに名前を入力します。
- 5 [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。
- 6 [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。
- 7 (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。
- 8 [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。
- 9 (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。

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。

ロード バランサーの詳細については、vRealize Automation の構成を参照してください。

開始する前に

「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 グループごとに自動生成	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。
マシンごとに自動生成	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 バランサーのオプションが表示されます。

- 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。

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 バランサー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 バランサーを選択します。

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。

開始する前に

[\[Amazon の予約用のリソースおよびネットワーク設定の指定\]](#)。

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 [受信者] テキスト ボックスに、アラート通知を受け取るユーザーのメール アドレスまたはグループ名を 1 つ以上入力します。
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。
- 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。

予約が保存され、[予約] リストに表示されます。

次に進む前に

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。

注意 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。

開始する前に

- **ファブリック管理者**として vRealize Automation コンソールにログインします。
- 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 (オプション) [既存の予約からコピー] ドロップダウン メニューから、既存の予約を選択します。
選択した予約のデータが表示されます。新規予約は必要に応じて変更できます。
- 4 [名前] テキスト ボックスに名前を入力します。
- 5 [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。
- 6 [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。
- 7 (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。
- 8 [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。
- 9 (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。

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。

開始する前に

[「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 グループごとに自動生成	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。
マシンごとに自動生成	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 この予約によっ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 [ネットワーク パス] リストから選択します。
- c (オプション) [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、リストに表示されたネットワーク プロファイルを選択します。

このオプションを選択するには、1 つ以上のネットワーク プロファイルが存在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 パスを選択できますが、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。

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。

開始する前に

[「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 スライダーを使用して、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 [受信者] テキスト ボックスに、アラート通知を受け取るユーザーのメール アドレスまたはグループ名を 1 つ以上入力します。
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。
- 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。

予約が保存され、[予約] リストに表示されます。

次に進む前に

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 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。

次に進む前に

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 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。

注意 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。

開始する前に

- **ファブリック管理者**として vRealize Automation コンソールにログインします。
- 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 (オプション) [既存の予約からコピー] ドロップダウン メニューから、既存の予約を選択します。
 選択した予約のデータが表示されます。新規予約は必要に応じて変更できます。
- 4 [名前] テキスト ボックスに名前を入力します。
- 5 [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。
- 6 [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。
- 7 (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。
- 8 [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。

- 9 (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。

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。

vCloud Director の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。

注意 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。

開始する前に

[\[vCloud Director 予約情報の指定\]](#) .

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 この予約によっ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 [ネットワーク パス] リストから選択します。
- c (オプション) [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、リストに表示されたネットワーク プロファイルを選択します。

このオプションを選択するには、1 つ以上のネットワーク プロファイルが存在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 パスを選択できますが、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。

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。

開始する前に

[\[vCloud Air の予約用のリソースおよびネットワーク設定の指定\]](#)

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 [受信者] テキスト ボックスに、アラート通知を受け取るユーザーのメール アドレスまたはグループ名を 1 つ以上入力します。
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。
- 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。

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 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。

次に進む前に

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。

注意 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。

開始する前に

- **ファブリック管理者**として vRealize Automation コンソールにログインします。
- 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 (オプション) [既存の予約からコピー] ドロップダウン メニューから、既存の予約を選択します。

選択した予約のデータが表示されます。新規予約は必要に応じて変更できます。

- 4 [名前] テキスト ボックスに名前を入力します。

- 5 [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。

- 6 [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。

- 7 (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。

- 8 [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。

- 9 (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。

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。

注意 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。

開始する前に

[\[vCloud Director 予約情報の指定\]](#) .

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 この予約によっ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 [ネットワーク パス] リストから選択します。
- c (オプション) [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、リストに表示されたネットワーク プロファイルを選択します。

このオプションを選択するには、1 つ以上のネットワーク プロファイルが存在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 パスを選択できますが、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。

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。

開始する前に

[\[vCloud Director の予約用のリソースおよびネットワーク設定の指定\]](#)。

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 [受信者] テキスト ボックスに、アラート通知を受け取るユーザーのメール アドレスまたはグループ名を 1 つ以上入力します。
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。
- 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。

予約が保存され、[予約] リストに表示されます。

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。

開始する前に

- **ファブリック管理者**として vRealize Automation コンソールにログインします。
- 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。[「シナリオ：概念実証の環境のためにネットワークと Amazon との間の VPC 接続を構成する」](#)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。エージェントを構成するには、予約にカスタム 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。

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。

注意 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。

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。

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。

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
Software.ebs.url	https://<Private_IP:1443>/event-broker-service/api
software.agent.service.url	https://<Private_IP:1443>/software-service/api
agent.download.url	https://<Private_IP:1443>/software-service/resources/nobel-agent.jar

- 4 [保存] をクリックします。

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たコンピュート リソースの共有メモリ、CPU、ネットワーク、およびストレージ リソースのことです。

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。

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が (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 ト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 ト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。

注意 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仮想化のための vSphere 予約の作成

vSphere 予約を作成すると、外部ネットワークとルーティング ゲートウェイをネットワーク用のネットワーク プロファイルに割り当てたり、トランスポート ゾーンを指定したり、セキュリティ グループをマシン コンポーネントに割り当てたりできます。

VMware NSX を設定し、vRealize Automation の NSX プラグインをインストールした場合、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（転送ゾーン）、Edge およびルーティング ゲートウェイの予約ポリシー、アプリケーションの分離設定を指定できます。これらは、**[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 **[NSX 設定]** タブで設定できます。

ブループリント デザイン キャンバス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 構成に基づいており、NSX プラグインがインストールされており、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する必要があります。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。

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、コンピュータ 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。

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。

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。

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。

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。

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。

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。

注意 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。

開始する前に

- **ファブリック管理者**として vRealize Automation コンソールにログインします。
- 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 (オプション) [既存の予約からコピー] ドロップダウン メニューから、既存の予約を選択します。
選択した予約のデータが表示されます。新規予約は必要に応じて変更できます。
- 4 [名前] テキスト ボックスに名前を入力します。
- 5 [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。
- 6 [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。
- 7 (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。
- 8 [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。
- 9 (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。

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。

開始する前に

[「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 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。

- 6 コンピュート リソースで使える場合は、[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。
- 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 この予約によっ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 [ネットワーク パス] リストから選択します。
- c (オプション) [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、リストに表示されたネットワーク プロファイルを選択します。

このオプションを選択するには、1 つ以上のネットワーク プロファイルが存在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 パスを選択できますが、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。

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。

開始する前に

[「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 [受信者] テキスト ボックスに、アラート通知を受け取るユーザーのメール アドレスまたはグループ名を 1 つ以上入力します。
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。
- 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。

予約が保存され、[予約] リストに表示されます。

次に進む前に

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。

注意 この情報は Amazon Web Services には適用されません。

開始する前に

- **ファブリック管理者**として vRealize Automation コンソールにログインします。

- 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。

注意 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。

注意 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 クラスター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 クラスター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 クラスター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。

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。

開始する前に

ファブリック管理者として vRealize Automation コンソールにログインします。

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 [追加] 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 [アップデート] をクリックしてポリシーを保存します。

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。

開始する前に

[「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。

注意 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 クラスター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 クラスター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 クラスター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。

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。

開始する前に

ファブリック管理者として vRealize Automation コンソールにログインします。

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 [追加] 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 [アップデート] をクリックしてポリシーを保存します。

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。

開始する前に

[「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 [保存] アイコン (✓) をクリックします。
- 8 [OK] をクリックします。
- 9 (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。

シナリオ : Rainpole 用の IaaS リソースを構成する

IaaS 管理者の権限とテナント管理者の権限を組み合わせ使用して、vRealize Automation で作成された vSphere マシンの先頭に付加するプリフィックスを作成し、vSphere リソースをファブリック グループとして構成し、リソースを vRealize Automation アーキテクトのカスタム グループに割り当てます。



手順

1 シナリオ : Rainpole 用のファブリック グループを作成する

IaaS 管理者の権限を使用して、ファブリック グループを作成します。このグループには vSphere エンドポイントの作成時に発見されたコンピュート リソースが含まれています。vRealize Automation のアーキテクトや開発者のカスタム グループを、このグループのファブリック管理者ロールに割り当てます。

2 シナリオ : Rainpole 用のマシン プリフィックスを構成する

ファブリック管理者の権限を使用してプリフィックスを作成します。開発およびテスト中に vRealize Automation のアーキテクトや開発者がプロビジョニングしたマシンの先頭に付加されるようにこれを構成できます。

3 シナリオ : Rainpole アーキテクトのためにカタログ アイテムのテスト用のビジネス グループを作成する

テナント管理者の権限を使用して、vRealize Automation ブループリントの設計とテストを担う IT チームのためにビジネス グループを作成します。

4 シナリオ : リソースを Rainpole アーキテクトに割り当てる予約を作成する

ファブリック管理者の権限を使用して、予約を作成します。これで、Rainpole ビジネス グループは、vSphere リソースを自分に割り当てることができます。

シナリオ : Rainpole 用のファブリック グループを作成する

IaaS 管理者の権限を使用して、ファブリック グループを作成します。このグループには vSphere エンドポイントの作成時に発見されたコンピュート リソースが含まれています。vRealize Automation のアーキテクトや開発者のカスタム グループを、このグループのファブリック管理者ロールに割り当てます。

vSphere エンドポイントを作成する必要はありません。初期コンテンツ カタログ アイテムを要請した時点で作成済みです。

手順

- 1 [インフラストラクチャ]-[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、**Rainpole fabric** と入力します。
- 4 [ファブリック管理者] 検索ボックスで **Rainpole アーキテクト** を検索し、カスタム グループを選択します。
- 5 ファブリック グループに含めるコンピュート リソースを vSphere 環境から選択します。
- 6 [OK] をクリックします。
- 7 ブラウザの表示を更新します。ファブリック管理者として利用できるようになった新しいメニュー オプションが表示されます。

次に進む前に

ファブリック管理者の権限を使用して、マシン プリフィックスを作成します。これで、Rainpole アーキテクトは開発時にプロビジョニングしたすべてのマシンを利用できるようになります。また、テストの識別が簡単になります。

シナリオ：Rainpole 用のマシン プリフィックスを構成する

ファブリック管理者の権限を使用してプリフィックスを作成します。開発およびテスト中に vRealize Automation のアーキテクトや開発者がプロビジョニングしたマシンの先頭に付加されるようにこれを構成できます。

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] を選択します。
- 2 [新規] をクリックします。
- 3 [マシン プリフィックス] テキスト ボックスに **Rainpole** と入力します。
- 4 [桁数] テキスト ボックスに **3** と入力します。
- 5 [次の番号] テキスト ボックスに **1** と入力します。
- 6 [保存] アイコン (🟢) をクリックします。

次に進む前に

テナント管理者の権限を使用して、vRealize Automation ブループリントの設計やテストを担う IT チームのビジネス グループを作成します。

シナリオ：Rainpole アーキテクトのためにカタログ アイテムのテスト用のビジネス グループを作成する

テナント管理者の権限を使用して、vRealize Automation ブループリントの設計とテストを担う IT チームのためにビジネス グループを作成します。

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 [名前] テキスト ボックスに、**Rainpole business group** と入力します。
- 4 [マネージャの電子メールの送信先] テキスト ボックスに 1 つ以上のメール アドレスを入力します。
たとえば、自分のメール アドレス、または IT マネージャのメール アドレスを入力します。
- 5 アーキテクトのためにブループリントの問題解決用のカスタム プロパティを追加します。
 - a [新規] アイコン (🟢) をクリックします。
 - b [名前] テキスト ボックスに、**_debug_deployment** 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 [プロンプト表示] を選択します。これで、アーキテクトはカタログ アイテムを要請するときにこの機能をオン/オフできるようになります。

通常、カタログ アイテムの 1 つのコンポーネントがプロビジョニングに失敗すると、vRealize Automation はカタログ アイテム全体のすべてのリソースをロールバックします。このカスタム プロパティでこの動作をオーバーライドすれば、アーキテクトはブループリントがどこで失敗するかを詳しく指定できます。このカスタム プロパティをブループリントではなくビジネス グループに追加すると、この動作をオーバーライドするかどうかをアーキテクトが常に変更できるようになり、その選択肢が誤ってユーザーに提供されることがなくなります。

- 6 [次へ] をクリックします。
- 7 [グループ マネージャ ロール] 検索ボックスで **Rainpole アーキテクト** を検索し、カスタム グループを選択します。
- 8 [ユーザー ロール] 検索ボックスで **test_user** を検索し、ブループリントをテストするために共有ログインとしてセットアップしたローカル ユーザーを選択します。
- 9 [次へ] をクリックします。
- 10 ドロップダウン メニューから [Rainpole] をデフォルトのマシン プリフィックスとして選択します。
- 11 [完了] をクリックします。

次に進む前に

ファブリック管理者の権限を使用して、予約を作成することにより IaaS リソースを Rainpole ビジネス グループに割り当てます。

シナリオ：リソースを Rainpole アーキテクトに割り当てる予約を作成する

ファブリック管理者の権限を使用して、予約を作成します。これで、Rainpole ビジネス グループは、vSphere リソースを自分に割り当てることができます。

注意 予約を作成した後は、ビジネス グループもコンピュート リソースも変更できません。

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 (+) をクリックします。
- 3 ドロップダウン メニューから [vSphere] を選択します。
- 4 予約情報を入力します。

オプション	入力
名前	Rainpole 予約
テナント	vsphere.local
ビジネス グループ	Rainpole ビジネス グループ
優先度	1

- 5 [リソース] タブを選択します。
- 6 導入環境からリソース情報を入力します。

オプション	入力
コンピュート リソース	ドロップダウン メニューからリソース クラスタを選択します。
マシン割り当て	この予約の電源投入マシンの最大数を指定します。
メモリ	この予約で使用できる最大メモリ量 (MB) を指定します。
ストレージ	この予約に対する 1 つ以上のストレージ パスと予約容量 (GB) を選択します。ストレージ パスの優先度 (1 が最も高い) を指定します。

- 7 [ネットワーク] タブを選択します。
- 8 1 つ以上の vSphere ネットワーク パスを選択します。
- 9 [OK] をクリックします。

vSphere インフラストラクチャを vRealize Automation 管理下で購入し、vSphere リソースをチームに割り当てました。

次に進む前に

IaaS アーキテクトの権限を使用して、vSphere CentOS マシンのクローン作成用のマシン ブループリントを作成します。

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。

開始する前に

- ファブリック管理者として vRealize Automation コンソールにログインします。

- 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 ポ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 メニューからポ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 リソースおよびポストンとロンドンの場所を関連付けます。

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ポ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。[「シナリオ：ユーザーが地域間展開のための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。

外部 IP アドレス管理プロバイダを使用した vRealize Automation 展開のプロビジョニングのチェックリスト

既にある外部の vRealize Automation ネットワーク プロファイルに使用する IP アドレスと範囲は、サポートされている外部 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atalog 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、Infoblox 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 3-6. 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	場所	詳細
外部 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、構成する。❑	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://solutionexchange.vmware.com/store/category_groups/cloud-management) に存在しない場合は、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。	「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」 を参照してください。
❑外部 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。	「外部 IP アドレス管理プロバイダの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 プロファイルで外部 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。	「外部 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。

表 3-6. 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 (続き)

タスク	場所	詳細
<input type="checkbox"/> 外部ネットワーク プロファイルを使用して既存のネットワークパスの予約を定義する。	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。
<input type="checkbox"/> 外部ネットワーク 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。	
<input type="checkbox"/> ブループリントに資格を付与してカタログに追加する。	vRealize Automation でブループリントに資格を付与してカタログに追加します。	
<input type="checkbox"/> ブループリント カatalog 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atalog 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。	
<input type="checkbox"/> 展開先となる IP アドレスを [アイテム] ページで照会する。	展開に使用するネットワーク IP アドレスを vRealize Automation で調べます。	

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。

開始する前に

- 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 コンソールにログインします。

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。

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。

次に進む前に

- 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。

開始する前に

- **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。
- 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。

注意 Kerberos アクセス認証を使用する場合、ホスト アドレスは FQDN 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。

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 プラゲイン 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ようにできます。

開始する前に

- 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 コンソールにログインします。

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>注意 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>注意 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。

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。

開始する前に

- 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 コンソールにログインします。

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	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。 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	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。 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	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。 a ユーザー認証情報を指定します。 ■ [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。 ■ [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	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。 a ユーザー認証情報を指定します。 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。

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。

開始する前に

- 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 コンソールにログインします。

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。

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。

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、[「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」](#)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。

vRealize Automation 7.1 では、Active Directory ポリシーは Tech プレビュー機能であるため、本番環境では使用しないでください。

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。

vRealize Automation 7.1 では、Active Directory ポリシーは Tech プレビュー機能であるため、本番環境では使用しないでください。

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。

開始する前に

- 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 コンソールにログインします。

手順

- 1 [管理] - [AD 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。<mycompany.com> 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、 ou=development,dc=corp,dc=domain,dc=com のようにします。

4 [OK] をクリックします。

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。

次に進む前に

- 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。

開始する前に

- 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、キャンパ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。

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。

次に進む前に

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。

オンデマンド サービスのユーザーへの提供

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。

この章では次のトピックについて説明します。

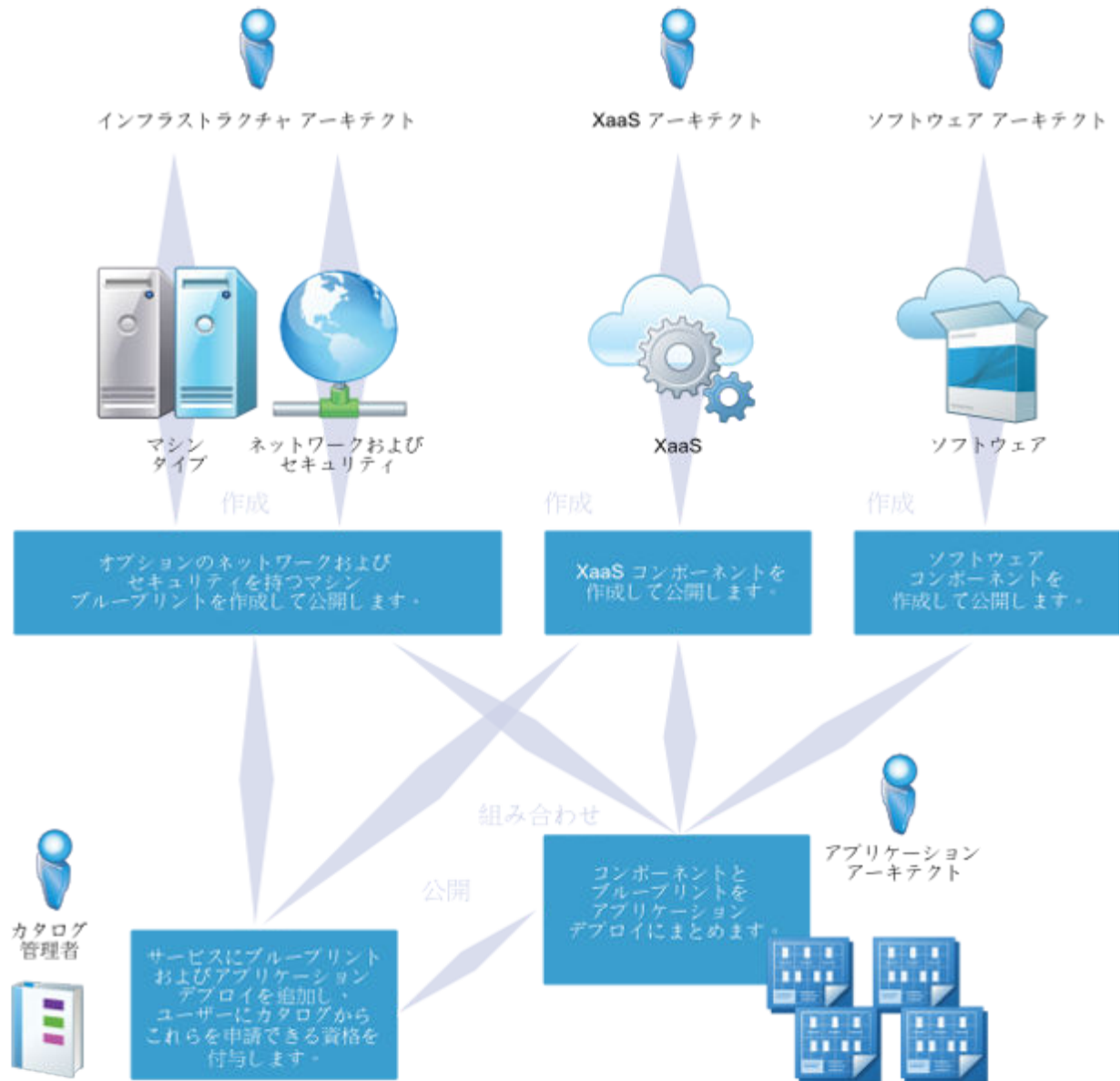
- [ブループリントの設計](#)
- [ブループリントのエクスポートとインポート](#)
- [デザイン ライブラリの作成](#)
- [複合ブループリントの組み合わせ](#)
- [サービス カatalogの管理](#)

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。

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。

マシンのブループリント

単一のブループリントを作成および公開し、単一のマシンをプロビジョニングするか、または複数の異なるタイプのマシン コンポーネントを含む複数マシンのブループリントを作成することができます。また、セキュリティ グループやネットワーク プロファイルなど、マシンのブループリントにネットワーク コンポーネントおよびセキュリティ コンポーネントを追加することもできます。

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。

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。

ブループリントのエクスポートとインポート

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
- 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 4-1. 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 開発者サイトを参照してください。
vRealize Automation REST API	https://www.vmware.com/support/pubs/vcac-pubs.html の vRealize Automation 情報センターの「プログラミング ガイド」を参照してください。

注意 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。

開始する前に

- 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。[「外部 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。

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 Cloud Client バージョン 4.x を <http://developercenter.vmware.com/tool/cloudclient> から `/tmp` にダウンロードします。
- 4 `cloudclient-4<x>-dist.zip` パッケージを解凍します。
- 5 `/bin` ディレクトリ下で Cloud Client 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 Cloud Client 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
```

<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
```

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オンすると、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せん。
- 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。

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。

次に進む前に

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。

開始する前に

- 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。**[申請]** タブのステータスを監視したり、アプリケーションのプロビジョニング後には、**[アイテム]** タブでカタログ アイテムの詳細を表示したりできます。

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 [アイテム] - [展開] を選択します。
- b Dukes Bank サンプル アプリケーションの展開を拡張し、Apache ロード バランサ サーバを選択します。
- c [詳細表示] をクリックします。
- 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。

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。

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。

表 4-2. 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 ネットワークおよびセキュリティを使用したマシン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】 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 4-2. 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 アクションの作成」
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。	「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て、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。

Thin Provisioning

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 環境で作業している場合、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。それ以外の場合は、マシンのプロビジョニングが失敗します。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。[「NetApp ONTAP エンドポイントの作成」](#) 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。
- 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。

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。

開始する前に

- 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。
- 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。
- テナントを設定します ([第 2 章「テナント設定の構成」](#))。
- laaS リソースを構成します ([「laaS リソース設定のチェックリスト」](#))。

- 『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 キャンパスにドラッグします。
- 7 各タブでプロンプトの指示に従って、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。

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。

次に進む前に

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、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」](#)を参照してください。

マシンのブループリント設定

マシン ブループリントを作成する場合は、構成可能な設定とオプションについて理解します。

[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] の設定

[新規ブループリント] ダイアログ ボックスで、構成可能な設定とオプションについて理解します。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] ダイアログ ボックスで編集できます。

[全般] タブ

今すぐまたはあとで追加するコンポーネントもすべて含め、ブループリント全体に設定を適用します。

表 4-3. [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。

表 4-3. [全般] タブの設定 (続き)

設定	説明
[説明]	ほかのアーキテクトが利用できるよう、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。
[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（デフォルト）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。
リース日数：[最小値] および [最大値]	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。

[NSX 設定] タブ

VMware NSX を設定し、vRealize Automation の NSX プラグインをインストールした場合、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（転送ゾーン）、Edge およびルーティングゲートウェイの予約ポリシー、アプリケーションの分離設定を指定できます。これらは、[\[新規ブループリント\]](#) および [\[ブループリントのプロパティ\]](#) ページの [\[NSX 設定\]](#) タブで設定できます。

NSX の設定の詳細については、[\[NSX を使用する \[新規ブループリント\] および \[ブループリントのプロパティ\] 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。ただし、これらのプロパティは、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。

表 4-4. [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。
	[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。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。

表 4-4. [プロパティ] タブの設定 (続き)

タブ	設定	説明
[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。
	[名前]	カスタム プロパティの名前と動作の一覧については、「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。

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 キャンパスで、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 キャンパスで 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構成します。

表 4-5. [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ト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。

表 4-5. [全般] タブの設定 (続き)

設定	説明
[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。
[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。</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設定します。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、ユーザーが拡張処理後に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 コンポーネントの拡張または更新を行うことができます。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設定を構成します。

表 4-6. [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> ■ LinkedClone <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> ■ NetAppFlexClone <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 4-6. [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> ■ [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>クローンまたは NetApp FlexClone の場合、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。</p> <p>リンク クローンの場合、マシンのリストからマシンを選択します。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 4-6. [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。このオプションは、リンク クローン アクションで使用できます。</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 4-7. [マシン リソース] タブ

設定	説明
[CPU : 最小値] および [最大値]	このマシン コンポーネントでプロビジョニング可能な 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]	このマシン コンポーネントでプロビジョニングされるマシンで使用可能なメモリの最小値と最大値を入力します。
[ストレージ (GB) : 最小値] および [最大値]	<p>このマシン コンポーネントでプロビジョニングされるマシンで使用可能なストレージ容量の最小値と最大値を入力します。vSphere、KVM (RHEV)、SCVMM、vCloud Air、および vCloud Director の場合、最小のストレージ容量は [ストレージ] タブでの入力値に基づいて設定されます。</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 4-8. [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。

表 4-8. [ストレージ] タブの設定 (続き)

設定	説明
[ドライブ文字/マウント パス]	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。
[ラベル]	ストレージ ポリ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。
[ストレージ予約ポリシー]	このストレージ ポリ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。
[カスタム プロパティ]	このストレージ ポリ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 ポリリュームの最大数を入力します。ストレージ ポリ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。ブループリント デザイン キャンパスに定義された、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 を使用する \[新規ブループリント\] および \[ブループリントのプロパティ\] の設定](#)」を参照してください。

表 4-9. [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。ブループリント デザイン キャンパ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。
[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。[DCHP] 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 の外部で設定された 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設定できます。必要に応じて、ブループリント デザイン キャンパ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。

ブループリント デザイン キャンパ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 を使用する \[新規ブループリント\] および \[ブループリントのプロパティ\] の設定」](#)を参照してください。

表 4-10. [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。名前はブループリント デザイン キャンパスのセキュリティ 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。
[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。作成時には[\[新規ブループリント\]](#) ページを、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 4-11. [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。たとえば、カスタム プロパティ名 Machine.SSH を入力し、ブループリントを使用してプロビジョニングされるマシンで SSH 接続を許可するかどうかを指定します。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、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に資格のあるユーザーが SSH を使用して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 4-12. [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。

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構成します。

表 4-13. [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]	<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ト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。</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。</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設定します。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、ユーザーが拡張処理後に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 コンポーネントの拡張または更新を行うことができます。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設定を構成します。

表 4-14. [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>次のアクションを使用できます。</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>
[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>次のアクションを使用できます。</p> <ul style="list-style-type: none"> ■ CloneWorkflow <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>クローンまたは NetApp FlexClone の場合、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。</p> <p>リンク クローンの場合、マシンのリストからマシンを選択します。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 4-15. [マシン リソース] タブ

設定	説明
[CPU : 最小値] および [最大値]	このマシン コンポーネントでプロビジョニング可能な 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]	このマシン コンポーネントでプロビジョニングされるマシンで使用可能なメモリの最小値と最大値を入力します。
[ストレージ (GB) : 最小値] および [最大値]	このマシン コンポーネントでプロビジョニングされるマシンで使用可能なストレージ容量の最小値と最大値を入力します。vSphere、KVM (RHEV)、SCVMM、vCloud Air、および vCloud Director の場合、最小のストレージ容量は [ストレージ] タブでの入力値に基づいて設定されます。

[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 ボ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 4-16. [ストレージ] タブの設定

設定	説明
[ID]	ストレージ ボリュームの ID または名前を入力します。
[容量 (GB)]	ストレージ ボ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 ボ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。
[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。
[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。
[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。作成時には **[新規ブループリント]** ページを、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 4-17. [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。たとえば、カスタム プロパティ名 Machine.SSH を入力し、ブループリントを使用してプロビジョニングされるマシンで SSH 接続を許可するかどうかを指定します。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、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に資格のあるユーザーが SSH を使用して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 4-18. [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 4-19. [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。
[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ト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。</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。</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設定します。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、ユーザーが拡張処理後に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 コンポーネントの拡張または更新を行うことができます。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 4-20. [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]	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。 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。
[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。
[キー ペア]	キー ペアは、Amazon Web Services のプロビジョニングに必要です。 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。 次のキー ペア オプションを使用できます。 <ul style="list-style-type: none"> ■ 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 グループごとに自動生成 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 ペアを持つように指定します。同じコンピュート 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。 ■ マシンごとに自動生成 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。
[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仮想プライベート クラウド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]	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。 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。 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。

[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。

表 4-21. [マシン リソース] タブ

設定	説明
[CPU : 最小値] および [最大値]	このマシン コンポーネントでプロビジョニング可能な 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]	このマシン コンポーネントでプロビジョニングされるマシンで使用可能なメモリの最小値と最大値を入力します。
[ストレージ (GB) : 最小値] および [最大値]	このマシン コンポーネントでプロビジョニングされるマシンで使用可能なストレージ容量の最小値と最大値を入力します。vSphere、KVM (RHEV)、SCVMM、vCloud Air、および vCloud Director の場合、最小のストレージ容量は [ストレージ] タブでの入力値に基づいて設定されます。
[EBS ストレージ (GB) : 最小値] および [最大値]	このマシン コンポーネントでプロビジョニングされるマシン リソースで使用可能な Amazon Elastic Block Store (EBS) ストレージ ボリュームの最小値と最大値を入力します。 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。

[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。作成時には **[新規ブループリント]** ページを、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 4-22. [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。たとえば、カスタム プロパティ名 Machine.SSH を入力し、ブループリントを使用してプロビジョニングされるマシンで SSH 接続を許可するかどうかを指定します。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せん。
[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、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に資格のあるユーザーが SSH を使用して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 4-22. [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 4-23. [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 キャンパスで、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 4-24. [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리를記載します。

表 4-24. [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。</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。</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設定します。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、ユーザーが拡張処理後に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 コンポーネントの拡張または更新を行うことができます。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 4-25. [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 マシン イメージを選択します。OpenStack 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 OpenStack アカウントによって管理されます。

表 4-25. [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 グループごとに自動生成 <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。同じコンピュート 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> ■ マシンごとに自動生成 <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>
[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 4-26. [マシン リソース] タブ

設定	説明
[CPU : 最小値] および [最大値]	このマシン コンポーネントでプロビジョニング可能な 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]	このマシン コンポーネントでプロビジョニングされるマシンで使用可能なメモリの最小値と最大値を入力します。
[ストレージ (GB) : 最小値] および [最大値]	<p>このマシン コンポーネントでプロビジョニングされるマシンで使用可能なストレージ容量の最小値と最大値を入力します。vSphere、KVM (RHEV)、SCVMM、vCloud Air、および vCloud Director の場合、最小のストレージ容量は [ストレージ] タブでの入力値に基づいて設定されます。</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。作成時には **[新規ブループリント]** ページを、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 4-27. [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。たとえば、カスタム プロパティ名 Machine.SSH を入力し、ブループリントを使用してプロビジョニングされるマシンで SSH 接続を許可するかどうかを指定します。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せん。
[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、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に資格のあるユーザーが SSH を使用して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 4-28. [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 4-28. [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。

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。

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。

表 4-29. 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検討します。
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 VirtualMachine.Admin.CustomizeGuestOSDelay 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 VirtualMachine.Admin.CustomizeGuestOSDelay 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。
SDRS を使用しているときは、リンク クローン プロビジョニングが失敗します。	リンク クローン プロビジョニングおよび SDRS を使用する場合は、新しいマシンは同一クラスタ上に配置されている必要があります。ソース マシンのディスクが、あるクラスタ上に配置されている場合、異なるクラスタ上へのマシンのプロビジョニングを申請すると、プロビジョニング エラーが発生します。	SDRS およびリンク クローン プロビジョニングを使用する場合は、リンク クローン ソースと同一のクラスタにマシンをプロビジョニングします。異なるクラスタにプロビジョニングしないでください。
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。

マシン コンポーネントへのネットワークおよびセキュリティ プロパティの追加

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。カスタム プロパティを使用し、ブループリント デザイン キャンパスの vSphere 以外のマシン コンポーネントに、ネットワークおよびセキュリティ オプションを追加できます。

[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。

[ネットワーク] または [セキュリティ] タブが表示されないマシン コンポーネントの場合は、

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、ブループリント キャンパスの [プロパティ] タブに追加できます。NSX ロード バランサ プロパティは、vSphere マシンのみに適用可能です。

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。

シナリオ : Rainpole でのクーロン作成用の vSphere CentOS ブループリントを作成する

IaaS アーキテクトの権限を使用して、vSphere CentOS マシンのクーロン作成用の基本的なブループリントを作成して発行します。



公開したブループリントは、他のアーキテクトが新しいブループリントでコンポーネントとして再利用できます。ブループリントをカタログから表示したり要請したりできるようにするには、テナント管理者の権限を使用して、そのように設定する必要があり、それ以前は誰も表示したり要請したりできません。

手順

1 シナリオ : Rainpole マシン コンポーネントのブループリントを作成する

IaaS アーキテクトの権限を使用してブループリントを作成し、vSphere CentOS マシンのブループリントの名前と説明を構成します。一意の識別子がブループリントに適用されるため、必要に応じて、プログラムによるブループリントとの連携やプロパティ バインドの作成を行うことができます。ユーザーが最長 1 か月のリース期間を選択できるようにブループリントを構成して、ブループリント リースの柔軟性を向上させたいと考えています。

2 シナリオ : Rainpole マシン コンポーネントの全般的な詳細を構成する

IaaS アーキテクト権限を使用して、vSphere マシン コンポーネントをデザイン キャンパスにドラッグし、ブループリントを使用してプロビジョニングしたマシンの全般的な詳細を構成します。

3 シナリオ : Rainpole マシン コンポーネントのビルド情報を指定する

laaS アーキテクト権限を使用して、vSphere で作成した CentOS テンプレートからマシンのクローンを作成するようにブループリントを構成します。

4 シナリオ : Rainpole マシン用のマシン リソースを構成する

laaS アーキテクトの権限を使用して、メモリおよび使用可能 CPU 数の最小値と最大値を設定するパラメータをユーザーに提供します。これはリソースの節約になるだけでなく、ユーザーのニーズに対応する意味もあります。

シナリオ : Rainpole マシン コンポーネントのブループリントを作成する

laaS アーキテクトの権限を使用してブループリントを作成し、vSphere CentOS マシンのブループリントの名前と説明を構成します。一意の識別子がブループリントに適用されるため、必要に応じて、プログラムによるブループリントとの連携やプロパティ バインドの作成を行うことができます。ユーザーが最長 1 か月のリース期間を選択できるようにブループリントを構成して、ブループリント リースの柔軟性を向上させたいと考えています。

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 **Centos on vSphere** と入力します。
- 4 生成された一意の識別子を確認します。

このフィールドはここで編集できますが、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。

[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。

- 5 [説明] テキスト ボックスに **Golden Standard CentOS machine configuration** と入力します。
- 6 ユーザーが選択するリース範囲を構成します。[最小値] テキスト ボックスに **1**、[最大値] テキスト ボックスに **30** と入力します。
- 7 [OK] をクリックします。

次に進む前に

vSphere マシン コンポーネントをキャンバスにドラッグし、vSphere で作成した CentOS テンプレートのクローンを作成するように構成します。

シナリオ : Rainpole マシン コンポーネントの全般的な詳細を構成する

laaS アーキテクト権限を使用して、vSphere 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、ブループリントを使用してプロビジョニングしたマシンの全般的な詳細を構成します。

マシン コンポーネントを構成できるのは laaS アーキテクトだけです。アプリケーション アーキテクトおよびソフトウェア アーキテクトは、作成した公開済みのマシン ブループリントを再利用することでのみ、マシン コンポーネントの使用が許可されています。

手順

- 1 左側のナビゲーション ペインで [マシン タイプ] をクリックします。
下のパネルにマシン コンポーネントのタイプが表示されます。
- 2 vSphere マシン コンポーネントをキャンパスにドラッグ アンド ドロップします。
- 3 [説明] テキスト ボックスに **Golden Standard CentOS Machine** と入力します。
- 4 **マシン プリフィックス** ドロップダウン メニューから [グループのデフォルトを使用] を選択します。

これらのブループリントをその他の環境にインポートする場合は、特定の Rainpole プリフィックスの代わりにグループのデフォルトを選択すると、使用できない可能性があるマシン プリフィックスを使用してブループリントを構成できなくなります。

次に進む前に

作成済みの CentOS テンプレートからマシンのクローンを作成するようにマシン コンポーネントを構成します。

シナリオ : Rainpole マシン コンポーネントのビルド情報を指定する

IaaS アーキテクト権限を使用して、vSphere で作成した CentOS テンプレートからマシンのクローンを作成するようにブループリントを構成します。

クローン アクションを実行するマシン コンポーネントを構成し、クローン作成元のオブジェクトとして作成したテンプレートを選択します。同一の設定で複数の仮想マシンを展開する場合に発生する可能性がある競合を回避するために作成したカスタム仕様を指定します。

手順

- 1 [ビルド情報] タブをクリックします。
- 2 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を [デスクトップ] または [サーバ] のどちらに分類するか、[ブループリントのタイプ] ドロップダウン メニューから選択します。
この情報は記録保存とライセンス目的のみです。
- 3 [アクション] ドロップダウン メニューから [クローン作成] を選択します。
- 4 [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。
- 5 [クローン作成元] テキスト ボックスの横にある [参照] アイコンをクリックします。
- 6 **Rainpole_centos_63_x86** を選択して、vSphere 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。
- 7 [OK] をクリックします。
- 8 [カスタマイズ仕様] テキスト ボックスに **Linux** と入力して、vSphere で作成したカスタマイズ仕様を使用します。

注意 この値は大文字と小文字が区別されます。

次に進む前に


ブループリントを使用してプロビジョニングしたマシンの CPU、メモリ、ストレージの設定を構成します。

シナリオ : Rainpole マシン用のマシン リソースを構成する

IaaS アーキテクトの権限を使用して、メモリおよび使用可能 CPU 数の最小値と最大値を設定するパラメータをユーザーに提供します。これはリソースの節約になるだけでなく、ユーザーのニーズに対応する意味もあります。

ソフトウェア アーキテクトとアプリケーション アーキテクトは、マシン コンポーネントを構成することを許可されていませんが、マシン コンポーネントが含まれているブループリントを再利用できます。マシン コンポーネントの編集が完了したら、ブループリントを公開します。これで、他のアーキテクトがマシンのブループリントを再利用して独自のカタログ アイテムを設計できるようになります。公開されたブループリントは、カタログ管理者およびテナント管理者も利用可能で、サービス カタログに追加できます。

手順

- 1 [マシン リソース] タブをクリックします。
- 2 プロビジョニングされるマシンの CPU 設定を指定します。
 - a [最小] テキスト ボックスに **1** を入力します。
 - b [最大] テキスト ボックスに **4** を入力します。
- 3 プロビジョニングされるマシンのメモリ設定を指定します。
 - a [最小] テキスト ボックスに **1024** を入力します。
このフィールドの値はメモリ上のテンプレートに基づいて自動的に設定されます。
 - b [最大] テキスト ボックスに **4096** を入力します。
- 4 プロビジョニングされるマシンのストレージ設定を指定します。
一部のストレージ情報は構成上のテンプレートに基づいて設定されますが、ストレージをさらに追加することもできます。
 - a [新規] アイコン () をクリックします。
 - b [容量 (GB)] テキスト ボックスに **10** と入力します。
 - c [OK] をクリックします。
- 5 [完了] をクリックします。
- 6 vSphere 上の CentOS を含む行を選択し、[公開] をクリックします。
カタログ準備の完了したブループリントを作成して、クローン作成された vSphere CentOS マシンをユーザーに配信し、CentOS マシンの標準として他のブループリントで再利用できるようになりました。

次に進む前に

テナント管理者の権限を使用して、アーキテクトのためにカタログ サービスを作成します。アーキテクトは、これで自分のブループリントを検証できます。CentOS を vSphere マシン ブループリントでカタログ アイテムとして公開し、それに作業の検証を要請します。

シナリオ : Rainpole マシンを ソフトウェア コンポーネントを提供するためのベースにする

IaaS アーキテクト権限を使用して、プロビジョニング済みのマシンのスナップショットをクローン元のリファレンスマシンとして使用して、ソフトウェア コンポーネントをサポートするブループリントを作成します。ソフトウェア コンポーネントをサポートするため、スナップショットを作成する前にプロビジョニング済みマシンにゲスト エージェントとブートストラップ エージェントをインストールします。



手順

1 シナリオ : Rainpole 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

ビジネス グループ マネージャの権限を使用して、テスト ユーザーとしてプロビジョニングした Rainpole001 マシンにログインします。ゲスト エージェントとソフトウェア ブートストラップ エージェントをマシン上にインストールして、ソフトウェア プロビジョニングの準備を行います。終了したら、ソフトウェア コンポーネントで使用するマシンのクローンを作成するベースとなるマシンのスナップショットを作成します。

2 シナリオ : Rainpole スナップショットに基づいてリンク クローン ブループリントを作成する

準備しておいたプロビジョニング済み CentOS マシンのコピー（容量を効率的に利用するもの）を、IaaS アーキテクトの権限を使用してソフトウェア アーキテクトに提供したいと考えています。

シナリオ : Rainpole 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

ビジネス グループ マネージャの権限を使用して、テスト ユーザーとしてプロビジョニングした Rainpole001 マシンにログインします。ゲスト エージェントとソフトウェア ブートストラップ エージェントをマシン上にインストールして、ソフトウェア プロビジョニングの準備を行います。終了したら、ソフトウェア コンポーネントで使用するマシンのクローンを作成するベースとなるマシンのスナップショットを作成します。

手順

- 1 [アイテム] - [マシン] を選択します。
- 2 vSphere 上の CentOS アイテムをクリックし、アイテムの詳細を表示します。
- 3 右側の [アクション] メニューから [リモート コンソールに接続] をクリックします。
- 4 root ユーザーとしてマシンにログインします。

- 5 vRealize Automation アプライアンスからインストール 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
```

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

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

- 7 **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。

- 8 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。

- 9 vRealize Automation コンソールに戻り、スナップショットを作成します。

- a 右側の [アクション] メニューから [スナップショットの作成] をクリックし、プロンプトの指示に従います。
- b [スナップショット] タブをクリックし、プロセスを監視します。

これで、ソフトウェア ブートストラップ エージェントとゲスト エージェントがインストールされて、ソフトウェア コンポーネントを含むブループリントでスナップショットをクローンのベースとして使用できるようになりました。

シナリオ：Rainpole スナップショットに基づいてリンク クローン ブループリントを作成する

準備しておいたプロビジョニング済み CentOS マシンのコピー（容量を効率的に利用するもの）を、IaaS アーキテクトの権限を使用してソフトウェア アーキテクトに提供したいと考えています。

vSphere ブループリント上の既存の CentOS をコピーして出発点とし、このコピーを編集して、準備しておいたスナップショットのリンク クローン コピーを作成します。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。リンク クローンのプロビジョニングは簡単で、ストレージ コストを削減でき、パフォーマンスの優先度が低い場合に最適です。

手順

- 1 [設計] - [ブループリント] を選択します。
- 2 vSphere 上の CentOS を含む行を選択し、[コピー] をクリックします。
vSphere 上の CentOS マシン ブループリントの独立したコピーが作成されました。

- 3 [名前] テキスト ボックスに **CentOS for Software Testing** と入力します。
- 4 [説明] テキスト ボックスに **Space-efficient vSphere CentOS for software testing** と入力します。
- 5 [OK] をクリックします。
- 6 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。
- 7 [ビルド情報] タブをクリックします。
- 8 [アクション] ドロップダウン メニューから [リンク クローン] を選択します。
- 9 [クローン作成元] テキスト ボックスの横にある [参照] アイコンをクリックします。
- 10 ソフトウェア ブートストラップ エージェントとゲスト エージェントをインストールしたプロビジョニング済みマシン [Rainpole001] を選択します。
- 11 [スナップショットからクローン作成] ドロップダウン メニューからスナップショットを選択します。
- 12 [終了] をクリックします。
- 13 CentOS for Software Testing を含む行を選択し、[公開] をクリックします。

自分や他のアーキテクトが CentOS マシンにソフトウェアを配信するために利用できるリンク クローン ブループリントが作成されました。

次に進む前に

ソフトウェア アーキテクトの権限を使用して、MySQL インストール用のソフトウェア コンポーネントを作成します。

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をユーザーに付与できるようにする場合は、マシン ブループリントに RDP カスタム プロパティを追加し、システム管理者が準備したカスタム RDP ファイルを参照する必要があります。

注意 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。

開始する前に

- **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 コンソールにログインします。
- 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
(必要) RDP.File.Name	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している必要があります。
(必要) VirtualMachine.Rdp.SettingN	特定の RDP を設定します。<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。RDP リンクを開いて設定の指定に使用します。 使用可能な設定および正しい構文のリストについては、Microsoft Windows RDP の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 <my-machine-name>.myCompany.com 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 ブループリントを含む行を選択し、[公開] をクリックします。

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。

シナリオ：CentOS ブループリントに Active Directory クリーンアップを追加する

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、既存の vSphere CentOS 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

開始する前に

注意 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 コンソールにログインします。
- Active Directory 環境について次の情報を収集します。
 - Active Directory アカount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。[「シナリオ : Rainpole でのクローン作成用の vSphere CentOS ブループリントを作成する」](#)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 [vSphere 上の Centos] 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 [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ountのユーザー名を入力します。これは、Active Directory アカountの削除、無効化、移動、名前変更を行うための十分な権限があるユーザーでなければなりません。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ount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ount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ountを新しい Active Directory の組織単位に移動します。値はアカount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ount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。

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。

シナリオ：申請者にマシン ホスト名の指定を許可する

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、既存の CentOS vSphere 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。

注意 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。

開始する前に

- 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。
- マシン ブループリントを作成します。[「シナリオ：Rainpole でのクーロン作成用の vSphere CentOS ブループリントを作成する」](#)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 [vSphere 上の Centos] 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。

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。

シナリオ：ユーザーが地域間展開のための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し、既存の vSphere CentOS ブループリントを編集し、場所の機能を有効します。



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。

開始する前に

- 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。
- 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。[「シナリオ：Rainpole でのクーロン作成用の vSphere CentOS ブループリントを作成する」](#)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 [vSphere 上の Centos] 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 [vSphere 上の Centos] ブループリントをポイントし、[公開] をクリックします。

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。

NSX ネットワークおよびセキュリティを使用したマシン ブループリントの設計

vRealize Automation と統合されている NSX インスタンスがある場合、ネットワークおよびセキュリティの仮想化に NSX を活用するように vSphere ブループリントを構成することができます。

vRealize Automation と NSX 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。新規ブループリントの作成や既存のブループリントの編集時に、次の NSX ネットワークおよびセキュリティの設定をブループリント全体に追加することもできます。

- トランスポート 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
- Edge およびルーティング ゲートウェイ予約ポリシー - 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
- App 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

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 を使用する [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] の設定

ブループリント全体に適用す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] ダイアログ ボックスで編集できます。

[全般] タブ

今すぐまたはあとで追加するコンポーネントもすべて含め、ブループリント全体に設定を適用します。

表 4-30. [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、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。
[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（デフォルト）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。
リース日数：[最小値] および [最大値]	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。

[NSX 設定] タブ

VMware NSX を設定し、vRealize Automation の NSX プラグインをインストールした場合、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（転送ゾーン）、Edge およびルーティング ゲートウェイの予約ポリシー、アプリケーションの分離設定を指定できます。これらは、**[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 **[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 4-31. [NSX 設定] タブの設定

設定	説明
[トランスポート ゾーン（転送ゾーン）]	<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（転送ゾーン）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。</p> <p>トランスポート ゾーンが必要となるのは、オンデマンド ネットワークを含むブループリントのみです。セキュリティ グループ、セキュリティ タグ、ロード バランサの場合、トランスポート ゾーンは任意で指定します。トランスポート ゾーンを指定しない場合、ロード バランサの接続先となるセキュリティ グループ、セキュリティ タグ、またはネットワークの場所によってエンドポイントが決まります。</p>
[Edge およびルーティング ゲートウェイの予約ポリシー]	<p>NSX Edge またはルーティング ゲートウェイ予約ポリシーを選択します。この予約ポリシーは、ルーティング ゲートウェイと、プロビジョニングの一部として展開されるすべての Edge に適用されます。各展開でプロビジョニングされる Edge は 1 つのみです。</p> <p>ルーティング ネットワークの場合、Edge はプロビジョニングされませんが、予約ポリシーを使用すると、ルーティング ネットワークのプロビジョニングに使用されるルーティング ゲートウェイとともに予約を選択できます。</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>
[アプリケーションの隔離]	<p>NSX 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 NSX のセキュリティ 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>

[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。ただし、これらのプロパティは、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。

表 4-32. [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。
	[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。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]		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。
	[名前]	カスタム プロパティの名前と動作の一覧については、「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。

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。

ブループリントにオンデマンド ネットワークが含まれる場合は、プロビジョニングされたマシン展開によって使用されるネットワークを含む NSX トランスポート ゾーンを指定する必要があります。同じトランスポート ゾーンを予約に指定する必要があります。

ブループリントへの NSX Edge またはルーティング ゲートウェイ予約ポリシーの適用

予約ポリシーを指定し、ブループリントによってプロビジョニングされるマシンのネットワーク通信を管理することができます。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。ルーティング ゲートウェイ予約ポリシーは、Edge 予約ポリシーとも呼ばれます。

ネットワーク情報は、各予約に含まれています。マシンがプロビジョニングされると、Edge またはルーティング ゲートウェイは、展開内でプロビジョニングされたマシンのネットワーク通信を管理するためのネットワーク ルータとして割り当てられます。ブループリント レベルのプロパティを追加または編集するには、[ブループリントのプロパティ] ページを使用します。

ルーティング ゲートウェイの予約ポリシーはオプションです。ルーティング ゲートウェイの予約ポリシーは、ブループリントに指定されたオンデマンド ネットワーク コンポーネントおよびオンデマンド ロード バランサ コンポーネントに関連付けられた NSX Edge をプロビジョニングするためにどの予約を使用できるかを制御します。

予約ポリシーを使用して、予約の選択内容を制御します。ブループリントに含まれる仮想マシン定義で予約ポリシーを選択して、仮想マシンで使用する予約にこのポリシーを割り当てます。

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。

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 (ESG) 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。

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 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。

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。

ブループリントを使用してマシン展開をプロビジョニングする場合、vRealize Automation は、指定された予約ポリシーに関連付けられている予約のみを使用して 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を試みません。

ブループリントへの NSX のアプリケーションの隔離セキュリティ ポリシーの適用

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。

[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]** ダイアログを使用して、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 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 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。詳細については、「[ネットワークとセキュリティが統合された vSphere エンドポイントの作成](#)」を参照してください。

注意 NSX Edge ロード バランサと NSX 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 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 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、その 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、そのサービスでは、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 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展開の 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。

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。

ブループリントのマシン コンポーネントに適用可能なセキュリティ機能の詳細については、「[ブループリント キャンパスでのセキュリティ コンポーネントの使用](#)」を参照してください。

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、vCloud Networking and Security および NSX プラットフォームに基づく仮想化ネットワークをサポートしています。

ネットワークおよびセキュリティの仮想化により、仮想マシンは、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することができます。

ネットワークおよびセキュリティを vRealize Automation と統合するため、IaaS 管理者は、NSX プラグインを vRealize Orchestrator にインストールし、vRealize Orchestrator および vSphere のエンドポイントを作成する必要があります。

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 キャンバス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。NAT およびルーティング プロファイルは、NSX 論理スイッチと新しいネットワーク パス用の適切なルーティング設定を構築し、仮想マシンのプロビジョニングおよび NSX Edge デバイスの構成時にネットワーク パスに接続するためのネットワーク インターフェイスを設定するためのテンプレートです。

ブループリント デザイン キャンバス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 構成に基づいており、NSX プラグインがインストールされており、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する必要があります。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。

[ネットワーク] または [セキュリティ] タブが表示されないマシン コンポーネントの場合は、**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、ブループリント キャンバスの [プロパティ] タブに追加できます。NSX ロード バランサ プロパティは、vSphere マシンのみに適用可能です。

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 ト 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され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。NSX 管理ガイドを参照してください。

ブループリント キャンバスでのセキュリティ コンポーネントの使用

NSX セキュリティ コンポーネントを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 デザイン キャンバス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 構成に基づいており、NSX プラグインがインストールされており、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する必要があります。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。

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。

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（ウィ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セキュリティ グループを追加できます。

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、ベンダーのドキュメントを参照してください。

NSX の既存またはオンデマンドのセキュリティ グループをブループリント キャンバスに追加できます。

セキュリティ タグ

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。

セキュリティ タグは、ブループリント キャンバスに追加できます。

セキュリティ ポリシー

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 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。

アプリケーションの隔離

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。

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ことで、その設定をブループリントの 1 つ以上のマシン 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。

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に構成できます。

複数のネットワークおよびセキュリティ コンポーネントをブループリントのデザイン キャンバスに追加できます。

開始する前に

- 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 の構成および『NSX 管理ガイド』を参照してください。
- vRealize Automation 用の NSX プラグインがインストールされ、NSX インベントリがクラスタで正常に実行されたことを確認します。

vRealize Automation で NSX 設定を使用するには、NSX プラグインをインストールして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 コンソールにログインします。
- 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 [カテゴリ] セクションの [ネットワークとセキュリティ] をクリックすると、使用可能なネットワークおよびセキュリティ コンポーネントの一覧が表示されます。
- 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 [完了] をクリックしてブループリントをドラフトとして保存するか、ブループリントの構成を続行します。

セキュリティの設定を続行するには、セキュリティ コンポーネントをさらに追加し、ブループリント キャンバス内の vSphere マシン コンポーネントの [セキュリティ] タブで各種設定を選択します。

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 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。

開始する前に

- 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。
- vRealize Automation 用の NSX プラグインがインストールされ、NSX インベントリがクラスタで正常に実行されたことを確認します。

vRealize Automation で NSX 設定を使用するには、NSX プラグインをインストールして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 コンソールにログインします。
- 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 [カテゴリ] セクションの [ネットワークとセキュリティ] をクリックすると、使用可能なネットワークおよびセキュリティ コンポーネントの一覧が表示されます。
- 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 [完了] をクリックしてブループリントをドラフトとして保存するか、ブループリントの構成を続行します。

セキュリティの設定を続行するには、セキュリティ コンポーネントをさらに追加し、ブループリント キャンバス内の vSphere マシン コンポーネントの [セキュリティ] タブで各種設定を選択します。

既存のセキュリティ タグ コンポーネントの追加

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。

セキュリティ タグ コンポーネントを使用して NSX セキュリティ タグをデザイン 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 コンポーネントで使用するよう構成できます。

複数のネットワークおよびセキュリティ コンポーネントをブループリントのデザイン キャンバスに追加できます。

開始する前に

- NSX のセキュリティ タグを作成および構成します。vRealize Automation の構成および『NSX 管理ガイド』を参照してください。
- vRealize Automation 用の NSX プラグインがインストールされ、NSX インベントリがクラスターで正常に実行されたことを確認します。
vRealize Automation で NSX 設定を使用するには、NSX プラグインをインストールしてデータ収集を実行する必要があります。
- vRealize Automation 用の NSX プラグインがインストールされ、NSX インベントリがクラスターで正常に実行されたことを確認します。
vRealize Automation で NSX 設定を使用するには、NSX プラグインをインストールして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 コンソールにログインします。
- 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 [カテゴリ] セクションの [ネットワークとセキュリティ] をクリックすると、使用可能なネットワークおよびセキュリティ コンポーネントの一覧が表示されます。

- 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 [完了] をクリックしてブループリントをドラフトとして保存するか、ブループリントの構成を続行します。

セキュリティの設定を続行するには、セキュリティ コンポーネントをさらに追加し、ブループリント キャンバス内の vSphere マシン コンポーネントの [セキュリティ] タブで各種設定を選択します。

ブループリント キャンバスでのネットワーク コンポーネントの使用

1 つ以上の NSX 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。

セキュリティ コンポーネントを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 マシン コンポーネントで利用できるようになります。

ブループリント デザイン キャンバス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 構成に基づいており、NSX プラグインがインストールされており、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する必要があります。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。

既存のネットワーク コンポーネントの追加

既存の NSX 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るようになります。

既存のネットワーク コンポーネントを使用して NSX 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 コンポーネントをブループリントのデザイン キャンバスに追加できます。

[ネットワーク] または [セキュリティ] タブが表示されないマシン コンポーネントの場合は、

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、ブループリント キャンバスの [プロパティ] タブに追加できます。NSX ロード バランサ プロパティは、vSphere マシンのみに適用可能です。

開始する前に

- NSX のネットワーク設定の作成と構成をします。vRealize Automation の構成および『NSX 管理ガイド』を参照してください。

- vRealize Automation 用の NSX プラグインがインストールされ、NSX インベントリがクラスタで正常に実行されたことを確認します。

vRealize Automation で NSX 設定を使用するには、NSX プラグインをインストールして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 コンソールにログインします。
- 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 [カテゴリ] セクションの [ネットワークとセキュリティ] をクリックすると、使用可能なネットワークおよびセキュリティ コンポーネントの一覧が表示されます。
- 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 の設定を指定するか、入力されている設定を承認します。
 - 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 [完了] をクリックしてブループリントをドラフトとして保存するか、ブループリントの構成を続行します。

次に進む前に

ネットワーク設定を続行するには、ネットワーク コンポーネントを追加し、ブループリント キャンバス内の vSphere マシン コンポーネントの [ネットワーク] タブで各種設定を選択します。

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 コンポーネントの追加

NSX オンデマンド NAT ネットワーク コンポーネントまたは NSX 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るようになります。

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 コンポーネントをブループリントのデザイン キャンバスに追加できます。

[ネットワーク] または [セキュリティ] タブが表示されないマシン コンポーネントの場合は、

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、ブループリント キャンバスの [プロパティ] タブに追加できます。NSX ロード バランサ プロパティは、vSphere マシンのみに適用可能です。

開始する前に

- NSX のネットワーク設定の作成と構成をします。vRealize Automation の構成および『NSX 管理ガイド』を参照してください。
- vRealize Automation 用の NSX プラグインがインストールされ、NSX インベントリがクラスターで正常に実行されたことを確認します。

vRealize Automation で NSX 設定を使用するには、NSX プラグインをインストールして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。

たとえば、オンデマンド NAT ネットワーク コンポーネントを追加する場合、NAT のネットワーク 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 コンソールにログインします。
- 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 [カテゴリ] セクションの [ネットワークとセキュリティ] をクリックすると、使用可能なネットワークおよびセキュリティ コンポーネントの一覧が表示されます。
- 2 オンデマンド NAT またはオンデマンド ルーティングのどちらのコンポーネントを構成するかに応じて、いずれかのオンデマンド 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 名前と説明（説明は任意）を入力します。
- 4 [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、[オンデマンド NAT ネットワーク] コンポーネントを追加する場合、NAT ネットワーク プロファイルを選択します。

ネットワーク設定の次の項目に、選択したネットワーク プロファイルの値が使用されます。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 ネットワーク）
- 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 ネットワーク）

- サブネット マスク範囲 (オンデマンド ルーティング ネットワーク)
- 基本 IP アドレス (オンデマンド ルーティング ネットワーク)

5 (オプション) [DNS/WINS] タブをクリックします。

6 (オプション) ネットワーク プロファイルの DNS と WINS の設定を指定するか、入力されている設定を承認します。

- 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。

7 (オプション) オンデマンド NAT ネットワーク コンポーネントの場合、[DHCP] タブをクリックし、IP アドレス範囲およびリースの長さを指定します。

DHCP に設定する IP アドレス範囲の開始および終了値を編集します。DHCP を使用して仮想マシンがプロビジョニングされると、ネットワーク アダプタによってこの範囲内の IP アドレスが割り当てられます。これは、デフォルトでは固定ネットワーク アダプタです。IP アドレスの値を、関連付けられているサブネットで使用されているネットワーク アドレスやブロードキャスト アドレスの値にすることはできません。固定 IP 範囲と重複させることはできません。

DHCP は、一対多のオンデマンド NAT ネットワーク コンポーネントに対してのみ使用可能です。

8 (オプション) [IP 範囲開始] テキスト ボックスに開始 IP アドレスの値を入力します。

9 (オプション) [IP 範囲終了] テキスト ボックスに終了 IP アドレスの値を入力します。

10 [リース時間 (秒)] テキスト ボックスに DHCP リースの長さを秒単位で入力するか、何も入力せずにリースの長さを無制限にします。

11 (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。

12 [完了] をクリックしてブループリントをドラフトとして保存するか、ブループリントの構成を続行します。

次に進む前に

ネットワーク設定を続行するには、ネットワーク コンポーネントを追加し、ブループリント キャンパス内の vSphere マシン コンポーネントの [ネットワーク] タブで各種設定を選択します。

ブループリント キャンパスでのロード バランサー コンポーネントの使用

1 つ以上のオンデマンド NSX ロード バランサー コンポーネントをデザイン キャンパスに追加して、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 デザイン キャンバス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 構成に基づいており、NSX プラグインがインストールされており、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する必要があります。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。

次のルールをブループリントのロード バランサー 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 プロファイルに NAT が設定されている場合、VIP ネットワーク プロファイルとして、同一の NAT ネットワーク内の同一の NAT ネットワーク プロファイルを設定できます。
- 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。

NSX Edge リソースが作成され、VIP、負荷分散された層、構成されたサービスなどのロード バランサーの詳細が Edge リソースのプロパティとして記録されます。

オンデマンド ロード バランサ コンポーネントの追加

オンデマンド ロード バランサ コンポーネントを使用して NSX ロード バランサをデザイン 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。

ロード バランサの設定によって、ネットワーク内でプロビジョニングされたマシン間のタスク処理が分散されます。

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 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 管理ガイド』を参照してください。

開始する前に

- 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。
- vRealize Automation 用の NSX プラグインがインストールされ、NSX インベントリがクラスターで正常に実行されたことを確認します。
vRealize Automation で NSX 設定を使用するには、NSX プラグインをインストールして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 コンソールにログインします。
- 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 コンポーネントがブループリント デザイン キャンバスに設定されていることを確認します。

手順

- 1 [カテゴリ] セクションの [ネットワークとセキュリティ] をクリックすると、使用可能なネットワークおよびセキュリティ コンポーネントの一覧が表示されます。

- 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 [名前] テキスト ボックスに名前を入力します。
- 4 [マシン] ドロップダウン メニューからマシン名を選択します。

この一覧には、アクティブなブループリントの vSphere マシン コンポーネントのみが含まれます。

- 5 [NIC] ドロップダウン メニューから NIC を選択します。
- 6 [VIP ネットワーク] ドロップダウン メニューから VIP ネットワークを選択します。
- 7 (オプション) [IP アドレス] から NIC の VIP 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、次に利用可能な IP アドレスがネットワーク プロファイルから VIP に割り当てられます。IP アドレスを指定できるのは、VIP が NAT ネットワーク上に作成される場合のみです。

- 8 ロード バランシング を実行する各サービスの横のチェック ボックスを選択します。
- 9 (オプション) 選択したサービスごとに、ポートとヘルス チェックの設定を受け入れるか、編集します。
- 10 [HTTP サービスの URL] テキスト ボックスに、選択したサービスのアドレスを入力します。

各ロード バランサの HTTP サービス コントロールに使用可能な URL は 1 つだけです。

入力した URL は、サービスの健全性チェックに使用されます。

HTTP トラフィックをリダイレクトするアドレスの URL を入力します。たとえば、http://myweb.com から https://myweb.com にトラフィックをリダイレクトすることができます。入力する値は、NSX アプリケーションの [HTTP リダイレクト URL] 設定に指定した値と一致させる必要があります。

- 11 [完了] をクリックしてブループリントをドラフトとして保存するか、ブループリントの構成を続行します。

構成の設定は、関連付けられた vSphere マシン コンポーネントの [ネットワーク] タブで使用できます。

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 バランサー 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。

ブループリント デザイン キャンバス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 構成に基づいており、NSX プラグインがインストールされており、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する必要があります。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。

たとえば、オンデマンド NAT ネットワーク コンポーネントをブループリントのデザイン キャンバスにドラッグすることで、やはりキャンバス内に存在する vSphere マシン コンポーネントで使用可能にすることができます。

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 4-33. 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。

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』と『vRealize Automation API リファレンス』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。

オプション	説明
[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 4-34. 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	<pre>export my_unique_id="01234 56789"</pre>
	Windows CMD - %my_unique_id%	<pre>set my_unique_id=012345 6789</pre>
	Windows PowerShell - \$my_unique_id	<pre>\$my_unique_id = "0123456789"</pre>

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	<pre>echo \$admin_email</pre>
	Windows CMD - %admin_email%	<pre>echo %admin_email%</pre>
	Windows PowerShell - \$admin_email	<pre>write-output \$admin_email</pre>

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 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、ブループリント 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 - <code>\${operating_systems[@]}</code> (文字列のアレイ全体の場合) <code>\${operating_systems[N]}</code> (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 - <code>%operating_systems_<N>%</code> 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 - <code>\$operating_systems</code> (文字列のアレイ全体の場合) <code>\$operating_systems[N]</code> (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 4-35. 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 4-36. 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"

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"`

注意 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。

注意 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。

開始する前に

ソフトウェア アーキテクトとして vRealize Automation コンソールにログインします。

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。

- [追加] アイコン (+) をクリックします。
- プロパティの名前を入力します。
- 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。

- プロパティの値として希望するタイプを選択します。
- 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 4-37. 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。

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。

次に進む前に

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。

シナリオ：Rainpole 用の MySQL ソフトウェア コンポーネントを作成する

MySQL を vSphere CentOS マシンにインストールするために、ソフトウェア アーキテクトの権限を使用して MySQL ソフトウェア コンポーネントを作成します。CentOS 仮想マシン用の MySQL ソフトウェア コンポーネントを設計する場合は、Linux オペレーティングシステム用のインストール、構成、開始パラメータ、およびスクリプトを構成します。

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 [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 **MySQL for Linux Virtual Machines** と入力します。
- 4 指定した名前に基づいて ID が割り当てられることを確認します。
例：Software.MySQLforLinuxVirtualMachines
- 5 [説明] テキスト ボックスに **MySQL installation and configuration** と入力します。
- 6 [コンテナ] ドロップダウン メニューから [マシン] を選択します。
MySQL だけをマシンに直接インストールするため、アーキテクトが MySQL ソフトウェア コンポーネントを他のソフトウェア コンポーネントの上にドロップすることを禁止します。
- 7 [次へ] をクリックします。
- 8 [新規] をクリックし、インストール スクリプトの次のプロパティをそれぞれ追加および構成します。
[OK] をクリックして、各プロパティを保存します。

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。

名前	説明	タイプ	値	暗号化 済み	オーバー ライドを 許可	必須	計算値
db_root_username	データベースの root ユーザー名	文字列	root	いいえ	はい	はい	いいえ
JAVA_HOME	JRE 1.8 以降のインストール先ディレクトリ	文字列	/opt/vmware-jre	いいえ	はい	はい	いいえ
global_ftp_proxy	FTP プロキシ URL (該当する場合)。省略可能。	文字列		いいえ	はい	いいえ	いいえ
db_port	MySQL データベース ポート	文字列		いいえ	はい	はい	いいえ
db_root_password	データベースの root ユーザーパスワード	文字列	パスワード	はい	はい	はい	いいえ
global_http_proxy	HTTP プロキシ URL (該当する場合)。省略可能。	文字列		いいえ	はい	いいえ	いいえ

名前	説明	タイプ	値	暗号化 済み	オーバー ライドを 許可	必須	計算値
global_https_proxy	HTTPS プロキシ URL (該当する 場合)。省略可能。	文字列		いいえ	はい	いいえ	いいえ
max_allowed_packet_size	サーバの許可される最大パケッ トサイズ	Integer	1024	いいえ	はい	いいえ	いいえ

9 [次へ] をクリックします。

10 インストール アクションを構成します。

- a [スクリプト タイプ] ドロップダウン メニューから [Bash] を選択します。
- b [ここをクリックして編集します] をクリックします。

- C 次のスクリプトを貼り付けます。

```
#!/bin/bash

#Setting proxies
export ftp_proxy=${ftp_proxy:-$global_ftp_proxy}
echo "Setting ftp_proxy to $ftp_proxy"

export http_proxy=${http_proxy:-$global_http_proxy}
echo "Setting http_proxy to $http_proxy"

export https_proxy=${https_proxy:-$global_https_proxy}
echo "Setting https_proxy to $https_proxy"

#
# Determine operating system and version
#
export OS=
export OS_VERSION=

if [ -f /etc/redhat-release ]; then
    # For CentOS the result will be 'CentOS'
    # For RHEL the result will be 'Red'
    OS=$(cat /etc/redhat-release | awk '{print $1}')

    if [ -n $OS ] && [ $OS = 'CentOS' ]; then
        OS_VERSION=$(cat /etc/redhat-release | awk '{print $3}')
    else
        # RHEL
        OS_VERSION=$(cat /etc/redhat-release | awk '{print $7}')
    fi

elif [ -f /etc/SuSE-release ]; then
    OS=SuSE

    MAJOR_VERSION=$(cat /etc/SuSE-release | grep VERSION | awk '{print $3}')
    PATCHLEVEL=$(cat /etc/SuSE-release | grep PATCHLEVEL | awk '{print $3}')

    OS_VERSION="$MAJOR_VERSION.$PATCHLEVEL"

elif [ -f /usr/bin/lsb_release ]; then
    # For Ubuntu the result is 'Ubuntu'
    OS=$(lsb_release -a 2> /dev/null | grep Distributor | awk '{print $3}')
    OS_VERSION=$(lsb_release -a 2> /dev/null | grep Release | awk '{print $2}')

fi

echo "Using operating system '$OS' and version '$OS_VERSION'"

if [ "x${global_http_proxy}" == "x" ] || [ "x${global_https_proxy}" == "x" ] ||
[ "x${global_ftp_proxy}" == "x" ]; then
    echo ""
    echo "#####"
    echo "# One or more PROXY(s) not set. Network downloads may fail  #"
    echo "#####"
```



```

    echo ""
fi

export PATH=$PATH:
$JAVA_HOME/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
set -e

# Tested on CentOS
if [ -x /usr/sbin/selinuxenabled ] && /usr/sbin/selinuxenabled; then
    # SELinux can be disabled by setting "/usr/sbin/setenforce Permissive"
    echo 'SELinux is enabled on this VM template. This service requires SELinux to
be disabled to install successfully'
    exit 1
fi

if [ "x$OS" != "x" ] && [ "$OS" = 'Ubuntu' ]; then
    # Fix the linux-firmware package
    export DEBIAN_FRONTEND=noninteractive
    apt-get install -y linux-firmware < /dev/console > /dev/console
    # Install MySQL package
    apt-get install -y mysql-server
else
    yum --nogpgcheck --noplugins -y install -x MySQL-server-community mysql-server
fi

# Set Install Path to the default install path (For monitoring)
Install_Path=/usr
echo Install_Path is set to $Install_Path, please modify this script if the install
path is not correct.

```

d [OK] をクリックします。

11 構成アクションを構成します。

a [スクリプト タイプ] ドロップダウン メニューから [Bash] を選択します。

b [ここをクリックして編集します] をクリックします。

- C 次のスクリプトを貼り付けます。

```
#!/bin/bash

#Setting proxies
export ftp_proxy=${ftp_proxy:-$global_ftp_proxy}
echo "Setting ftp_proxy to $ftp_proxy"

export http_proxy=${http_proxy:-$global_http_proxy}
echo "Setting http_proxy to $http_proxy"

export https_proxy=${https_proxy:-$global_https_proxy}
echo "Setting https_proxy to $https_proxy"

#
# Determine operating system and version
#
export OS=
export OS_VERSION=

if [ -f /etc/redhat-release ]; then
    # For CentOS the result will be 'CentOS'
    # For RHEL the result will be 'Red'
    OS=$(cat /etc/redhat-release | awk '{print $1}')

    if [ -n $OS ] && [ $OS = 'CentOS' ]; then
        OS_VERSION=$(cat /etc/redhat-release | awk '{print $3}')
    else
        # RHEL
        OS_VERSION=$(cat /etc/redhat-release | awk '{print $7}')
    fi

elif [ -f /etc/SuSE-release ]; then
    OS=SuSE

    MAJOR_VERSION=$(cat /etc/SuSE-release | grep VERSION | awk '{print $3}')
    PATCHLEVEL=$(cat /etc/SuSE-release | grep PATCHLEVEL | awk '{print $3}')

    OS_VERSION="$MAJOR_VERSION.$PATCHLEVEL"

elif [ -f /usr/bin/lsb_release ]; then
    # For Ubuntu the result is 'Ubuntu'
    OS=$(lsb_release -a 2> /dev/null | grep Distributor | awk '{print $3}')
    OS_VERSION=$(lsb_release -a 2> /dev/null | grep Release | awk '{print $2}')

fi

echo "Using operating system '$OS' and version '$OS_VERSION'"

if [ "x${global_http_proxy}" == "x" ] || [ "x${global_https_proxy}" == "x" ] ||
[ "x${global_ftp_proxy}" == "x" ]; then
    echo ""
    echo "#####"
    echo "# One or more PROXY(s) not set. Network downloads may fail  #"
    echo "#####"
```

```

    echo ""
fi

export PATH=$PATH:
$JAVA_HOME/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
set -e

# Locate the my.cnf file
my_cnf_file=
if [ -f /etc/my.cnf ]; then
    my_cnf_file=/etc/my.cnf
elif [ -f /etc/mysql/my.cnf ]; then
    my_cnf_file=/etc/mysql/my.cnf
fi

if [ "x$my_cnf_file" = "x" ]; then
    echo "Neither /etc/my.cnf nor /etc/mysql/my.cnf can be found, stopping
configuration"
    exit 1
fi

# update mysql configuration to handle big packets
sed -ie "s/\[mysqld\]/\[mysqld\]\n\
max_allowed_packet=$max_allowed_packet/g" $my_cnf_file
# update listening port
sed -ie "s/\[mysqld\]/\[mysqld\]\n\
port=$db_port/g" $my_cnf_file

sed -i "s/port.*=[0-9]*/port=$db_port/g" $my_cnf_file

if [ "x$OS" != "x" ] && [ "$OS" = 'Ubuntu' ]; then
    # Make sure that MySQL is started
    service mysql restart
else
    # set up auto-start on booting
    chkconfig mysqld on
    # restart mysqld service
    service mysqld start
fi

# this will assign a password for mysql admin user 'root'
mysqladmin -u $db_root_username password $db_root_password

```

d [OK] をクリックします。

12 開始アクションを構成します。

- a [スクリプト タイプ] ドロップダウン メニューから [Bash] を選択します。
- b [ここをクリックして編集します] をクリックします。

- c 次のスクリプトを貼り付けます。

```
#!/bin/sh

echo "The maximum allowed packet size is: "
```

- d コロンと引用符の間にカーソルを合わせます。
- e [挿入するプロパティの選択] ドロップダウン メニューから **max_allowed_packet_size** を選択します。
- スクリプトに次のプロパティが含まれます。

```
#!/bin/sh

echo "The maximum allowed packet size is: $max_allowed_packet_size"
```

- f [OK] をクリックします。

13 [次へ] をクリックします。

14 [終了] をクリックします。

15 MySQL for Linux Virtual Machines を含む行を選択し、[公開] をクリックします。

MySQL ソフトウェア コンポーネントは、ブループリント デザイン ページの他のアーキテクトも利用できますが、マシンに統合するまでは ソフトウェア コンポーネントを利用可能にすることはできません。

次に進む前に

ソフトウェア アーキテクト、アプリケーション アーキテクト、または IaaS アーキテクトの権限を使用して、ソフトウェア マシン ブループリント用の CentOS に MySQL コンポーネントを統合します。

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、全般設定の構成、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 4-38. 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。
[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。

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 4-39. 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 4-39. 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。</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]	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。

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 4-40. 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 アクションの作成

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、プロビジョニング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、グループ内の Active Directory ユーザー、または PowerShell スクリプトを作成できます。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。

ブループリント デザイン キャンバスでの XaaS ブループリントの使用

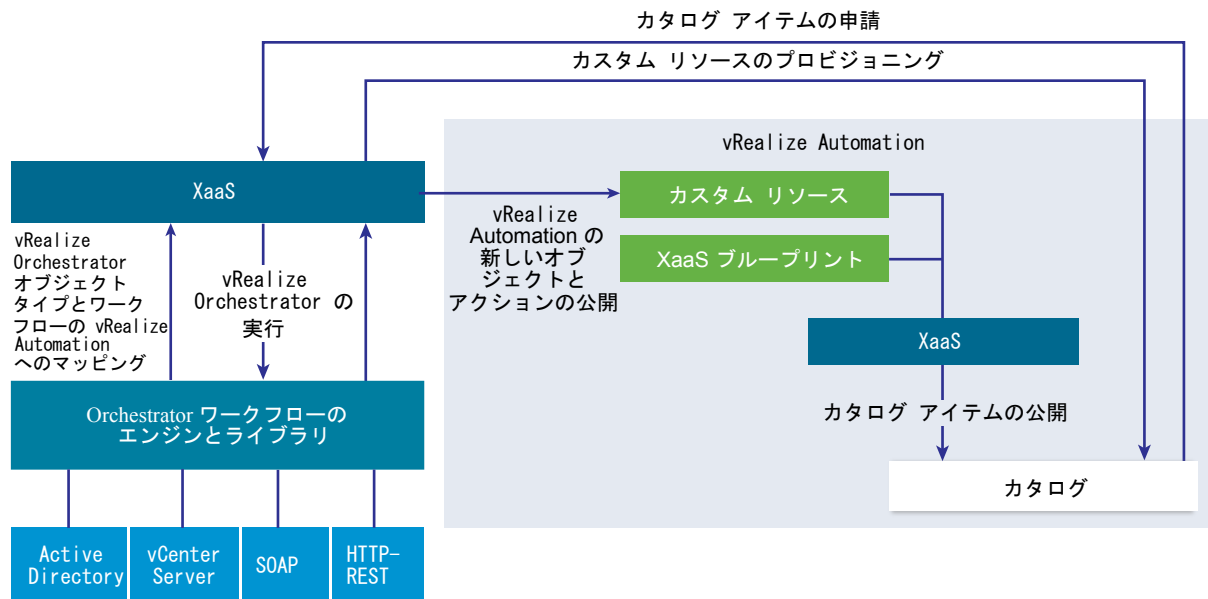
デザイン キャンバスで XaaS ブループリントをマシン ブループリント コンポーネントとして使用すると、XaaS ブループリントは展開で実行されるスケール イン アクションおよびスケール アウト アクションから除外されます。展開の XaaS コンポーネントに加えた変更はスケール アクションで認識されません。XaaS コンポーネントを展開に加えたスケールの変更に対応させるには、これらのアクションを XaaS コンポーネント上で XaaS リソース アクションを使用して個別に実行する必要があります。

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。

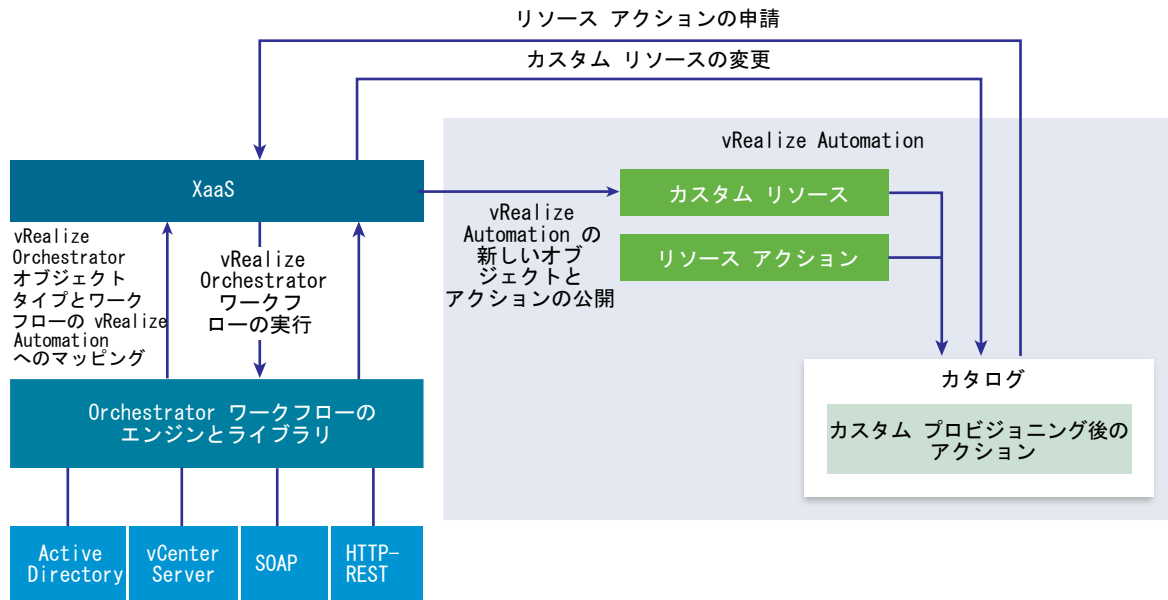
図 4-1. XaaS に含まれているカタログ アイテムを作成および申請して、カスタム リソースをプロビジョニングする



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 4-2. 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な 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 4-41. 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替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 VMware 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 4-42. 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 4-42. 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 Automation に組み込みのインスタンスのみ)	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。

カスタム リソースの作成

カスタム リソースは、ブループリントとリソース アクションを作成できるように、vRealize Orchestrator のオブジェクト タイプを XaaS リソースとしてマップします。

たとえば、vCenter Server 仮想マシンをプロビジョニングして、このマシン上で実行するリソース アクションを追加するブループリントを作成できるように、VC：仮想マシンに基づいてカスタム リソースを作成します。

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。


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 リソースを作成して、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。

カスタム リソースの作成プロセス中、[詳細フォーム] ページで、プロビジョニングされたアイテムの詳細ビューで情報を表示するリソースに対する、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。

開始する前に

XaaS アーキテクトとして vRealize Automation コンソールにログインします。

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 vRealize Orchestrator オブジェクト タイプを入力して Enter を押します。

たとえば、文字 v を含むすべてのタイプを表示するには **v** を入力します。すべてのタイプを表示するには、スペースを入力して [検索] をクリックします。
- 4 名前と説明（説明は任意）を入力します。
- 5 バージョンを入力します。

バージョンは整数のみを入力できます。<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。
- 6 [次へ] をクリックします。

7 カスタム リソースのフォームを編集します。

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。新規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。

オプション	説明
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 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。 使用可能な要素は vRealize Orchestrator オブジェクト タイプに固有です。
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。
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。

8 [完了] をクリックします。

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。

次に進む前に

XaaS ブループリントを作成します。[「XaaS ブループリントの作成」](#)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 キャンパスを使用して 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ように変更することができます。

カタログ アイテムとしての XaaS ブループリントの作成

XaaS ブループリントはプロビジョニング用のブループリントです。提供されているプロビジョニング 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。

開始する前に

- XaaS アーキテクトとして vRealize Automation コンソールにログインします。
- ターゲット リソース タイプのカスタム リソースを作成します。[「カスタム リソースの追加」](#)を参照してください。

手順

1 XaaS ブループリントの作成

XaaS ブループリントは、プロビジョニングの完全な仕様です。ブループリントには、入力パラメータ、送信および読み取り専用フォーム、アクションのシーケンス、プロビジョニングを含めることができます。

2 カタログ アイテムとしての XaaS ブループリントの公開

XaaS ブループリントの作成後はドラフト状態となるため、カタログ アイテムとして公開する必要があります。

3 アプリケーション ブループリントへの XaaS ブループリントの追加

アプリケーション ブループリントに XaaS ブループリントを追加する方法は、デザイン キャンパスに他のブループリントを追加する方法と同様です。

XaaS ブループリントの作成

XaaS ブループリントは、プロビジョニングの完全な仕様です。ブループリントには、入力パラメータ、送信および読み取り専用フォーム、アクションのシーケンス、プロビジョニングを含めることができます。

以前に作成したカスタム リソースをプロビジョニングするサービス ブループリントを作成できます。ユーザーがこれらのカタログ アイテムを申請する場合、プロビジョニングされたアイテムは [アイテム] タブに保存され、このタイプのプロビジョニングされたリソースに対するプロビジョニング後の操作を定義できます。

出力パラメータを指定せずにプロビジョニング用のサービス ブループリントを作成する場合、ユーザーがこのカタログ アイテムを申請すると、ブループリントによりプロビジョニングは行われますが、プロビジョニングされたアイテムは [アイテム] タブに追加されません。このタイプのプロビジョニングされたリソースでは、プロビジョニング後の操作を実行できません。

出力パラメータを指定せず、プロビジョニングされない申請用のサービス ブループリントを作成することもできます。たとえば、通知の送信用のサービス ブループリントを作成できます。

サービス ブループリントを作成することで、vRealize Orchestrator ワークフローをカタログ アイテムとして公開します。このプロセス中、デフォルトで生成されたフォームを編集できます。[「XaaS ブループリント フォームの設計」](#)を参照してください。

開始する前に

- **XaaS アーキテクト**として vRealize Automation コンソールにログインします。
- アイテムのプロビジョニングの場合、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。[「カスタム リソースの追加」](#)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 vRealize Orchestrator ワークフロー ライブラリに移動して、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 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。

6 (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。

7 バージョンを入力します。

バージョンは整数のみを入力できます。<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。

8 [次へ] をクリックします。

9 (オプション) [ブループリント フォーム] ページでサービス ブループリントのフォームを編集します。

デフォルトで、サービス ブループリント フォームは vRealize Orchestrator ワークフロー プレゼンテーションにマッピングされます。フォーム内で要素を削除、編集、再配置することにより、ブループリント フォームを編集できます。新規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。

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。

10 [次へ] をクリックします。

11 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。

オプション	説明
以前に作成したカスタム リソース	ユーザーがこのカタログ アイテムを申請する場合、プロビジョニングされたアイテムは [アイテム] タブに保存されます。
プロビジョニングなし	サービス ブループリントは新しいアイテムを [アイテム] タブに追加しません。

12 [完了] をクリックします。

サービス ブループリントが作成され、[XaaS ブループリント] ページに表示されます。

次に進む前に

ブループリントをカタログ アイテムとして公開します。[「カタログ アイテムとしての XaaS ブループリントの公開」](#)を参照してください。

カタログ アイテムとしての XaaS ブループリントの公開

XaaS ブループリントの作成後はドラフト状態となるため、カタログ アイテムとして公開する必要があります。

開始する前に

XaaS アーキテクトとして vRealize Automation コンソールにログインします。

手順

- 1 [設計] - [XaaS] - [XaaS ブループリント] を選択します。
- 2 公開する XaaS ブループリントの行を選択して、[公開] をクリックします。

XaaS ブループリントのステータスが公開済みに変わります。[管理] - [カタログ管理] - [カタログ アイテム] の順に選択すると、ブループリントがカタログ アイテムとして公開されていることを確認できます。

次に進む前に

- XaaS ブループリントをサービス カatalog内で使用できるようにするには、アイテムをサービスに追加する必要があります。[「サービスの作成」](#)を参照してください。
- アプリケーション ブループリントで使用する場合は、XaaS ブループリントをデザイン キャンバスに追加します。[「アプリケーション 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。
- プロビジョニングされたアイテムで実行するリソース アクションを作成できます。[「リソース アクションの作成」](#)を参照してください。

アプリケーション ブループリントへの XaaS ブループリントの追加

アプリケーション ブループリントに XaaS ブループリントを追加する方法は、デザイン キャンバスに他のブループリントを追加する方法と同様です。

この方法を使用して、他のブループリントを含むアプリケーション ブループリントに XaaS を追加します。XaaS ブループリントのみをユーザーに提供する場合、XaaS ブループリントをアプリケーション 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 インまたはスケール アウトのアクションを実行しても、XaaS ブループリントはスケーリングされません。

開始する前に

- XaaS ブループリントを作成して公開します。[「カタログ アイテムとしての XaaS ブループリントの作成」](#)を参照してください。
- XaaS ブループリント フォームをカスタマイズする方法を確認します。[「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。
- 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。

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 [XaaS] をクリックします。
- 4 ブループリントをキャンパスにドラッグします。
- 5 一般的なパラメータおよびインフラストラクチャ オプションのデフォルト値を設定します。
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atalog フォームに表示されます。
- 6 [終了] をクリックします。

現在、XaaS ブループリントは、アプリケーション ブループリントの一部になっています。

次に進む前に

アプリケーション ブループリントがサービスに追加されており、ユーザーが使用できることを確認します。[「サービス カatalog の管理」](#)を参照してください。

カタログ アイテムとしての 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。

開始する前に

- XaaS アーキテクトとして vRealize Automation コンソールにログインします。
- 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。[「カスタム リソースの追加」](#)を参照してください。
- XaaS カatalog 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 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。

開始する前に

- XaaS アーキテクトとして vRealize Automation コンソールにログインします。
- 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 ライブラリに移動して、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。

バージョンは整数のみを入力できます。<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、[アイテム] 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 [アイテム] 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では、vRealize Orchestrator ワークフロー プレゼンテーションをマッピングします。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。

オプション	アクション
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。

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。

次に進む前に

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。

開始する前に

XaaS アーキテクトとして vRealize Automation コンソールにログインします。

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。

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。

次に進む前に

アイコンをリソース アクションに割り当てます。[「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。

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。

開始する前に

XaaS アーキテクトとして vRealize Automation コンソールにログインします。

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。

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。

開始する前に

- **XaaS アーキテクト**として vRealize Automation コンソールにログインします。
- 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。

バージョンは整数のみを入力できます。<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 4-43. 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atalog 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 4-44. 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
[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

表 4-44. 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
[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
[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 デザイナでの制約と値

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 ワークフローで指定されている制約より優先されます。

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。条件を使用することで、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	vRealize Orchestrator スクリプト アクションを選択して値を定義します。

表 4-45. 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。

表 4-45. フォーム デザイナでの制約 (続き)

制約	説明
値	要素の値を設定することができます。
表示	ユーザーが要素を表示できるかどうかを示します。
最小長	文字列入力要素の最小文字数を設定できます。
最大長	文字列入力要素の最大文字数を設定できます。
最小値	数値入力要素の最小値を設定できます。
最大値	数値入力要素の最大値を設定できます。
増分	[小数] または [整数] フィールドなどの要素の増分を設定できます。たとえば、[整数] フィールドを [スライダ] 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	選択できる要素の最小アイテム数を設定できます。 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。
最大数	選択できる要素の最大アイテム数を設定できます。 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。

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 4-46. 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 インベントリに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 アクションを選択して、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を定義します。

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 デザイナー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。

フォーム デザイナーの操作

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 デザイナーを使用して、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。

Create cluster - ブループリントの編集

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み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み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み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。

開始する前に

- テナント管理者または XaaS アーキテクトとして vRealize Automation コンソールにログインします。
- [「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。

開始する前に

- テナント管理者または XaaS アーキテクトとして vRealize Automation コンソールにログインします。
- [「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。

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。

開始する前に

- テナント管理者または XaaS アーキテクトとして vRealize Automation コンソールにログインします。
- [「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。

開始する前に

- テナント管理者または XaaS アーキテクトとして vRealize Automation コンソールにログインします。
- [「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。

開始する前に

- テナント管理者または XaaS アーキテクトとして vRealize Automation コンソールにログインします。
- [「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。

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。

開始する前に

- テナント管理者または XaaS アーキテクトとして vRealize Automation コンソールにログインします。
- [「XaaS ブループリントの作成」](#)。

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、[申請] 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。

次に進む前に

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。

開始する前に

- テナント管理者または XaaS アーキテクトとして vRealize Automation コンソールにログインします。
- [「XaaS ブループリントの作成」](#)。

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	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。 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。
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。 <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。

開始する前に

- テナント管理者または XaaS アーキテクトとして vRealize Automation コンソールにログインします。
- [「XaaS ブループリントの作成」](#)。

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。

次に進む前に

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。

開始する前に

- テナント 管理者または XaaS アーキテクトとして vRealize Automation コンソールにログインします。
- [「XaaS ブループリントの作成」](#)。

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。

開始する前に

- テナント 管理者または XaaS アーキテクトとして vRealize Automation コンソールにログインします。
- [「XaaS ブループリントの作成」](#)。

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。

開始する前に

- テナント管理者または XaaS アーキテクトとして vRealize Automation コンソールにログインします。
- [「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、[申請] 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。

次に進む前に

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。

開始する前に

- テナント管理者または XaaS アーキテクトとして vRealize Automation コンソールにログインします。
- [「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。

次に進む前に

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。

開始する前に

- テナント管理者または XaaS アーキテクトとして vRealize Automation コンソールにログインします。
- [「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 インベントリの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	<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 [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。

開始する前に

- テナント 管理者または XaaS アーキテクトとして vRealize Automation コンソールにログインします。
- [「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。

開始する前に

- テナント 管理者または XaaS アーキテクトとして vRealize Automation コンソールにログインします。
- [「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。たとえば、ユーザーにユーザー パスワードの変更を許可する操作など、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。

XaaS アーキテクトとして、新しいカスタム 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。

開始する前に

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

カスタム リソースの作成後、カタログ アイテムとしてグループ内のユーザーの作成ワークフローを公開する XaaS ブループリントを作成できます。

3 カatalog アイテムとしてのユーザー ブループリントの作成を公開する

[テスト ユーザーの XaaS ブループリントを作成する] を作成したら、カタログ アイテムとして公開できます。

4 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。

5 パスワード変更のリソース アクションの公開

[テスト ユーザーのパスワードを変更する] 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。

6 テスト ユーザーを作成するためのカタログ サービスの作成

サービスを作成して、[ユーザーの作成] カatalog アイテムをサービス カatalog に表示し、テスト ユーザーの作成に関連するカatalog アイテムをユーザーが簡単に探せるようにします。

7 カatalog アイテムと「テスト ユーザーの作成」サービスとの関連付け

「テスト ユーザーの作成」カatalog アイテムを「テスト ユーザーの作成」サービスに含めるには、このサービスに関連付ける必要があります。

8 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 マネージャおよびテナント管理者は、カatalog のサービスを表示し、サービスに含まれる [テスト ユーザーの作成] カatalog アイテムの作成を要求できるように、個別のユーザーまたはユーザー グループにサービスおよびリソース アクションの使用資格を付与することができます。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。

開始する前に

XaaS アーキテクトとして vRealize Automation コンソールにログインします。

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 Type] 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 フォームはそのままにしておきます。
- 9 [終了] をクリックします。

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。

次に進む前に

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

カスタム リソースの作成後、カタログ アイテムとしてグループ内のユーザーの作成ワークフローを公開する XaaS ブループリントを作成できます。

開始する前に

XaaS アーキテクトとして vRealize Automation コンソールにログインします。

手順

- 1 [設計] - [XaaS] - [XaaS ブループリント] を選択します。
- 2 [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] - [Microsoft] - [Active Directory] - [ユーザー] の順に移動し、[グループ内のユーザーの作成] ワークフローを選択します。
- 4 [次へ] をクリックします。
- 5 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。
- 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。
ドメイン名を定数値に設定します。
 - 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 [終了] をクリックします。

テスト ユーザーの作成用のブループリントが作成され、XaaS ブループリント ページに表示されます。

次に進む前に

Create a test user ブループリントを公開して、アクティブなカタログ アイテムにします。

カタログ アイテムとしてのユーザー ブループリントの作成を公開する

[テスト ユーザーの XaaS ブループリントを作成する] を作成したら、カタログ アイテムとして公開できます。

開始する前に

XaaS アーキテクトとして vRealize Automation コンソールにログインします。

手順

- 1 [設計] - [XaaS] - [XaaS ブループリント] を選択します。
- 2 [テスト ユーザーのブループリントを作成する] の行を選択して、[公開] ボタンをクリックします。

[テスト ユーザーのブループリントを作成する] のステータスが公開済みに変わります。[管理] - [カタログ管理] - [カタログ アイテム] に移動すると、[テスト ユーザーのブループリントを作成する] がカタログ アイテムとして公開されていることを確認できます。

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

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。

開始する前に

XaaS アーキテクトとして vRealize Automation コンソールにログインします。

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 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 [追加] をクリックします。

ユーザーのパスワードを変更するリソース 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。

次に進む前に

[テスト ユーザーのパスワードの変更] リソース アクションを公開します。

パスワード変更のリソース アクションの公開

[テスト ユーザーのパスワードを変更する] 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。

開始する前に

XaaS アーキテクトとして vRealize Automation コンソールにログインします。

手順

- 1 [設計] - [XaaS] - [リソース アクション] を選択します
- 2 [テスト ユーザーのパスワードを変更する] 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。

[テスト ユーザーのパスワードを変更する] 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。

次に進む前に

アイコンをリソース アクションに割り当てます。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。リソース アクションにアイコンを割り当てる方法については、「[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。

テスト ユーザーを作成するためのカタログ サービスの作成

サービスを作成して、[ユーザーの作成] カタログ アイテムをサービス カタログに表示し、テスト ユーザーの作成に関連するカタログ アイテムをユーザーが簡単に探せるようにします。

開始する前に

テナント 管理者またはカタログ管理者として vRealize Automation コンソールにログインします。

手順

- 1 [管理] - [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 **Create a Test User** を入力します。
- 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。

テスト ユーザーの作成というサービスが作成され、[サービス] ページに表示されます。

次に進む前に

テスト ユーザーの作成カタログ アイテムを編集してサービスに含めます。

カタログ アイテムと「テスト ユーザーの作成」 サービスとの関連付け

「テスト ユーザーの作成」 カatalog アイテムを 「テスト ユーザーの作成」 サービスに含めるには、このサービスに関連付ける必要があります。

開始する前に

テナント 管理者またはカタログ管理者として vRealize Automation コンソールにログインします。

手順

- 1 [管理] - [カタログ管理] - [カタログ アイテム] を選択します。
- 2 「テスト ユーザーの作成」 カatalog アイテムを探し、カタログ アイテム名をクリックします。
- 3 (オプション) [ファイルの選択] をクリックして、カタログ アイテムのアイコンを変更します。
- 4 [サービス] ドロップダウン メニューから [テスト ユーザーの作成] サービスを選択します。
- 5 [完了] をクリックします。

「テスト ユーザーの作成」 カatalog アイテムが 「テスト ユーザーの作成」 サービスに関連付けられました。

次に進む前に

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。


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 マネージャおよびテナント管理者は、カタログのサービスを表示し、サービスに含まれる [テスト ユーザーの作成] カatalog アイテムの作成を要求できるように、個別のユーザーまたはユーザー グループにサービスおよびリソース アクションの使用資格を付与することができます。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。

開始する前に

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 コンソールにログインします。

手順

- 1 [管理] - [カタログ管理] - [資格] を選択します。
- 2 [新規] アイコン () をクリックします。
- 3 [名前] テキスト ボックスで **ユーザーの作成** 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。
- 7 [ユーザーおよびグループ] テキスト ボックスにユーザー名を入力し、Enter を押します。

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。

- 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 ボックスで [テスト ユーザーの作成] と入力し、Enter を押します。
- 10 [使用可能なアクション] テキスト ボックスで [テスト ユーザーのパスワードの変更] と入力し、Enter を押します。
- 11 [追加] をクリックします。

アクティブな資格が作成され、サービスがユーザーのカatalogに公開されました。

サービス ログの利用者が vRealize Automation コンソールにログインすると、管理者が事前に作成したサービス、「テスト ユーザーの作成」が [Catalog] タブに表示されます。ユーザーは、管理者が事前に作成し、サービスに含めた Catalog アイテムである「グループ内のユーザーの作成」を申請できます。利用者はユーザーを作成した後、パスワードを変更できます。

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。

開始する前に

XaaS アーキテクトとして vRealize Automation コンソールにログインします。

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。

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。

次に進む前に

[\[vSphere 仮想マシンを移行するためのアクションの公開\]](#)

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。

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。[\[リソース アクションへのアイコンの割り当て\]](#) を参照してください。

次に進む前に

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。

開始する前に

XaaS アーキテクトとして vRealize Automation コンソールにログインします。

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atalog 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。

次に進む前に

[「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。

[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。



次に進む前に

[「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  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。

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。

次に進む前に

[「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。

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。「[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。

次に進む前に

ビジネス グループ マネージャとテナント管理者は、「vMotion で仮想マシンを移行する」 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。

開始する前に

XaaS アーキテクトとして vRealize Automation コンソールにログインします。

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。

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。

次に進む前に

[「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。

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。[「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。

次に進む前に

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。

開始する前に

- 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。

開始する前に

- XaaS アーキテクトとして vRealize Automation コンソールにログインします。
- 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。

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。

次に進む前に

[「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。

開始する前に

XaaS アーキテクトとして vRealize Automation コンソールにログインします。

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。

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。

次に進む前に

[「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。

開始する前に

XaaS アーキテクトとして vRealize Automation コンソールにログインします。

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。

[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。

次に進む前に

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かを確認します。

```
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。

開始する前に

- 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。
- 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。

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。

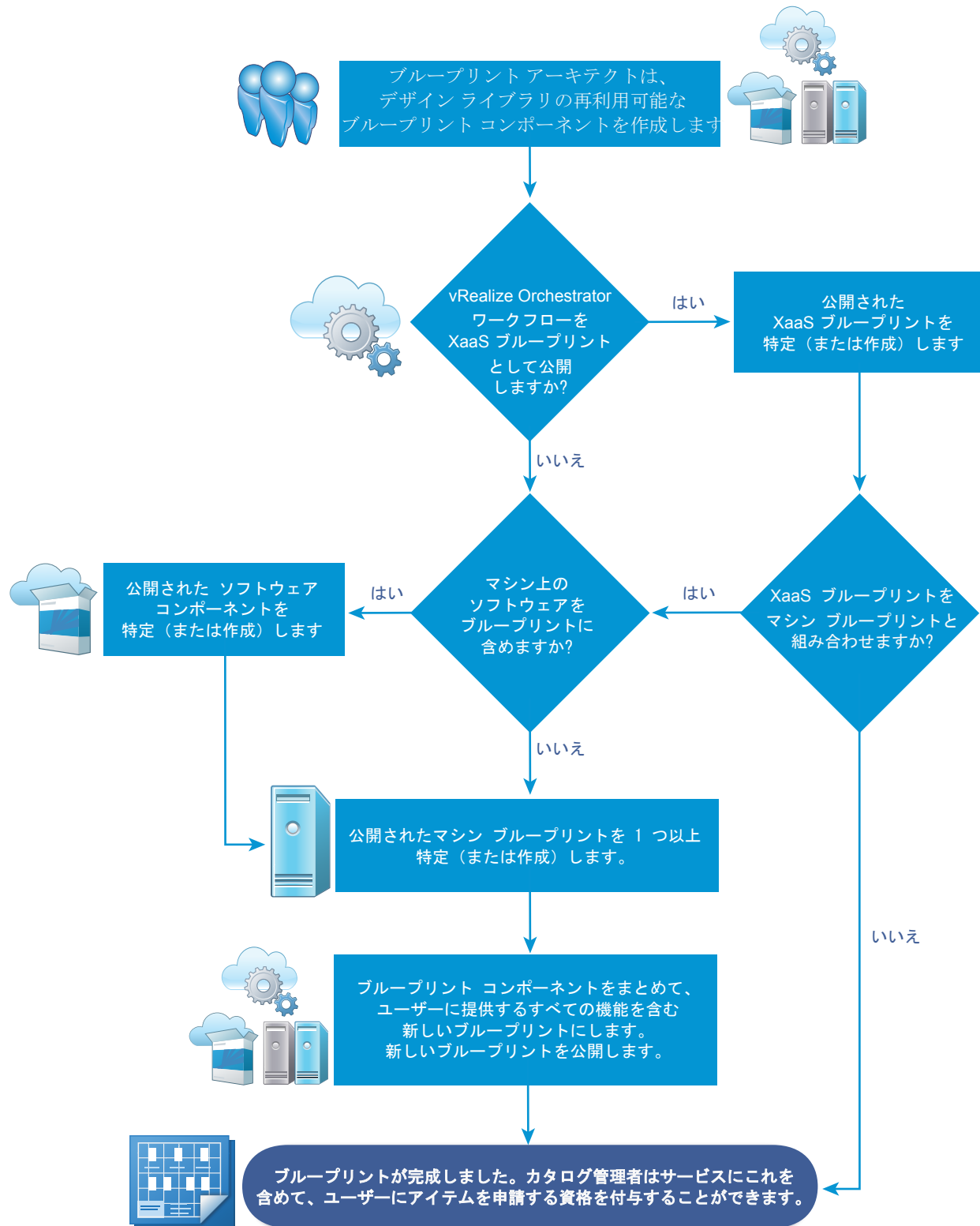
次に進む前に

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。

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、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。

図 4-3. 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。

■ ソフトウェア コンポーネントをサポートするマシン コンポーネントの選択

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。

■ 明示的な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常にトリガされます。

■ シナリオ : Rainpole リンク クローン マシン上の MySQL を提供するためのブループリントを組み合わせでテストする

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 IaaS アーキテクトの権限を使用して、MySQL コンポーネントを、作成した vSphere CentOS リンク クローン ブループリントに組み合わせるためのブループリントを作成します。

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に活用するには、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。
- ユーザーに最上位のブループリントの使用資格が付与されると、このユーザーは、ネストされたブループリントを含む、すべての種類のブループリントの使用資格が得られます。

- 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。
- 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。

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られます。
- 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オンデマンドのロード 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。

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。

ソフトウェア コンポーネントをサポートするマシン コンポーネントの選択

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 エージェントではインターネット プロトコル バージョン 6 (IPv6) がサポートされないため、使用するマシン ブループリント、予約、ネットワーク コンポーネントおよびセキュリティ コンポーネントは、IPv6 ではなく IPv4 を使用するように構成する必要があります。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。

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。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。

表 4-47. 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

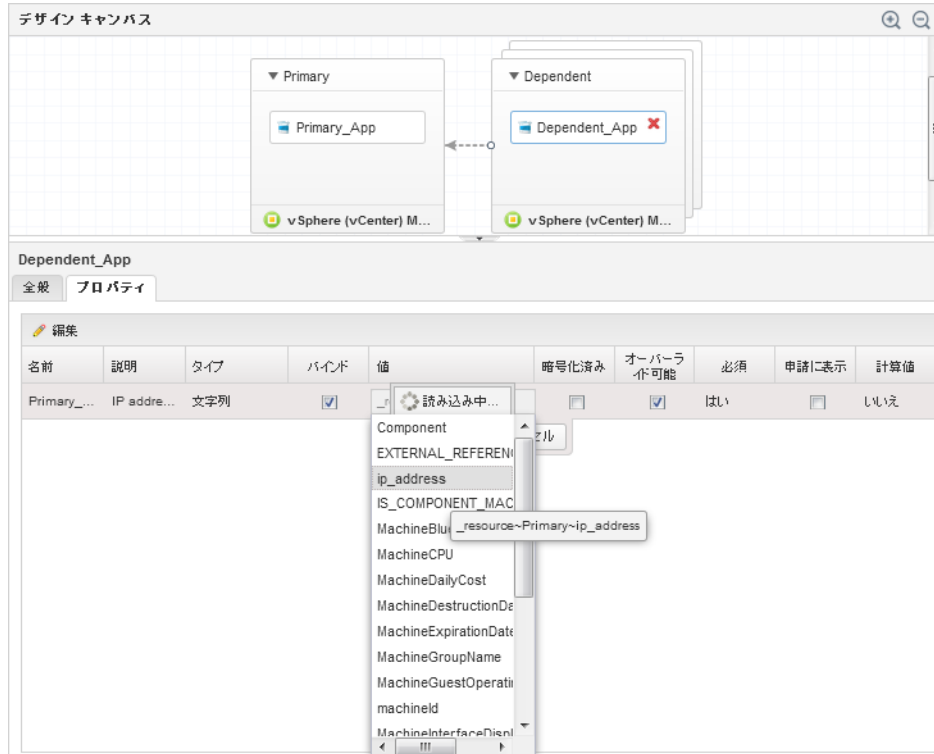
ブループリント コンポーネント間でのプロパティ バインドの作成

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。

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 4-4. 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



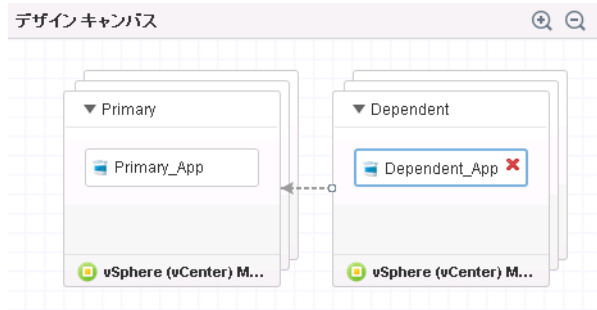
明示的な依存関係の作成とプロビジョニングの順序の制御

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常にトリガされます。

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。

ブループリントの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 4-5. 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。

シナリオ：Rainpole リンク クローン マシン上の MySQL を提供するためのブループリントを組み合わせてテストする

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 IaaS アーキテクトの権限を使用して、MySQL コンポーネントを、作成した vSphere CentOS リンク クローン ブループリントに組み合わせるためのブループリントを作成します。



開始する前に

- Linux マシンに MySQL をインストールするためのソフトウェア コンポーネントを作成します。[「シナリオ：Rainpole 用の MySQL ソフトウェア コンポーネントを作成する」](#)を参照してください。
- vRealize Automation コンソールに Rainpole アーキテクト カスタム グループのメンバーとしてログインします。[「シナリオ：Rainpole アーキテクトのカスタム グループを作成する」](#)を参照してください。

手順

1 [シナリオ：MySQL on CentOS Rainpole ブループリント用にコンテナを作成する](#)

IaaS、ソフトウェア、またはアプリケーション アーキテクトの権限を使用して、MySQL on CentOS vSphere ブループリント用にブループリント コンテナを作成し、名前、説明、および一意の識別子を構成します。

2 シナリオ : Rainpole 向けに MySQL on CentOS ブループリントにソフトウェアとマシンを追加する

IaaS、ソフトウェア、またはアプリケーション アーキテクトの権限を使用して、公開済みの CentOS for Software Testing マシンのブループリントをマシンとして再利用するためにキャンパスにドラッグします。公開済みのソフトウェア コンポーネントを仮想マシンにドラッグし、ソフトウェア コンポーネントで指定したソフトウェア プロパティを構成します。

3 シナリオ : MySQL を搭載した CentOS カタログ アイテムを Rainpole サービスに追加する

テナント管理者の権限を使用して、新しいブループリントを Rainpole カタログ サービスに追加して、作業結果を確認できるようにします。

4 シナリオ : Rainpole 用の MySQL 搭載 CentOS カタログ アイテムをプロビジョニングする

テスト ユーザー アカウントを使用して、MySQL を使用した CentOS マシンのプロビジョニングを行うため、サービス カタログ アイテムを申請します。

シナリオ : MySQL on CentOS Rainpole ブループリント用にコンテナを作成する

IaaS、ソフトウェア、またはアプリケーション アーキテクトの権限を使用して、MySQL on CentOS vSphere ブループリント用にブループリント コンテナを作成し、名前、説明、および一意の識別子を構成します。

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 **MySQL on CentOS** と入力します。

4 生成された一意の識別子を確認します。

[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こで編集できますが、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。

5 [説明] テキスト ボックスに **MySQL Software on vSphere CentOS Machine** と入力します。

6 ユーザーが選択するリース範囲を構成します。[最小値] テキスト ボックスに **1**、[最大値] テキスト ボックスに **7** と入力します。

ユーザーは、リースの更新が必要になる、またはマシンを破棄する前に、申請したマシンを最長 1 週間リースすることを選択できます。

7 [OK] をクリックします。

次に進む前に

MySQL コンポーネントと公開済みのソフトウェア用 CentOS マシン ブループリントをキャンパスにドラッグします。

シナリオ：Rainpole 向けに MySQL on CentOS ブループリントにソフトウェアとマシンを追加する

IaaS、ソフトウェア、またはアプリケーション アーキテクトの権限を使用して、公開済みの CentOS for Software Testing マシンのブループリントをマシンとして再利用するためにキャンパスにドラッグします。公開済みのソフトウェア コンポーネントを仮想マシンにドラッグし、ソフトウェア コンポーネントで指定した ソフトウェア プロパティを構成します。

手順

- 1 [カテゴリ] リストで [ブループリント] をクリックします。
- 2 [ソフトウェア テスト用 CentOS] をキャンパスにドラッグします。
- 3 [カテゴリ] リストで [ソフトウェア コンポーネント] をクリックします。
- 4 [MySQL for Linux Virtual Machines] を vSphere マシンにドラッグします。
- 5 [プロパティ] タブをクリックします。
- 6 このブループリントの db_port プロパティをアップデートします。
 - a db_port プロパティを選択して、[編集] をクリックします。
 - b [値] テキスト ボックスに **3308** と入力します。
サービス カタログ ユーザーがアイテムを申請すると、3308 がデフォルト値になります。
 - c [OK] をクリックします。
- 7 [終了] をクリックします。
- 8 MySQL を搭載した CentOS を含む行を選択し、[公開] をクリックします。

CentOS マシンと MySQL ソフトウェア コンポーネントを含むブループリントを公開しました。

シナリオ：MySQL を搭載した CentOS カタログ アイテムを Rainpole サービスに追加する

テナント管理者の権限を使用して、新しいブループリントを Rainpole カタログ サービスに追加して、作業結果を確認できるようにします。

手順

- 1 [管理] - [カタログ管理] - [サービス] を選択します。
- 2 [サービス] リストで Rainpole カタログ サービスの行を選択し、[カタログ 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。

MySQL を搭載した CentOS のカタログ アイテムを要求できる状態になりました。Rainpole ビジネス グループに Rainpole サービス全体への資格を割り当てたため、新しいカタログ アイテムに資格を付与する必要はありません。

次に進む前に

MySQL を搭載した CentOS のカタログ アイテムを要求して、作業結果を確認します。

シナリオ：Rainpole 用の MySQL 搭載 CentOS カatalog アイテムをプロビジョニングする

テスト ユーザー アカウントを使用して、MySQL を使用した CentOS マシンのプロビジョニングを行うため、サービス カatalog アイテムを申請します。

手順

- 1 vRealize Automation コンソールからログアウトします。
- 2 ユーザー名 **test_user**、パスワード **VMware1!** で再ログインします。
- 3 [カタログ] タブをクリックします。
- 4 [申請] ボタンをクリックして、カタログ アイテムを申請します。
- 5 [説明] テキスト ボックスに **verifying functionality** と入力します。
- 6 [送信] をクリックして、カタログ項目を要求します。
- 7 [申請] タブをクリックして、申請のステータスを監視します。

マシンが正常にプロビジョニングされると、**成功**というステータス メッセージが表示されます。

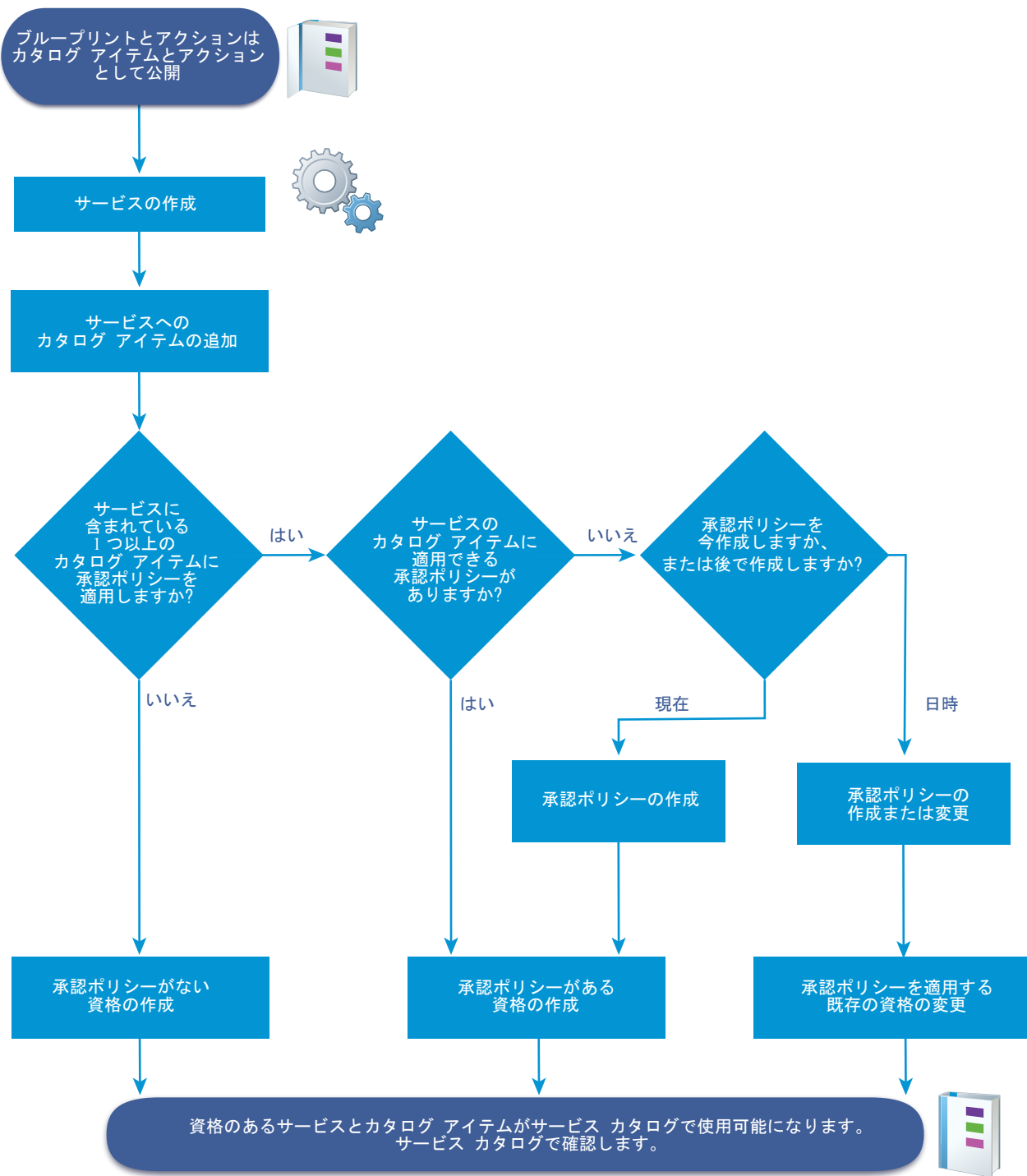
次に進む前に

- 本番環境のインストールを計画します。『リファレンス アーキテクチャ』を参照してください。
- vRealize Automation の構成、ブループリントの設計とエクスポート、およびサービス カatalog の管理のためのその他のオプションを確認します。『vRealize Automation の構成』を参照してください。

サービス カatalog の管理

顧客は、サービス カatalog 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atalog 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atalog 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 4-48. 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す。 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。

開始する前に

テナント 管理者またはカタログ管理者として vRealize Automation コンソールにログインします。

手順

- 1 [管理] - [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。

次に進む前に

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 カタログ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。

開始する前に

- **テナント管理者**または**カタログ管理者**として vRealize Automation コンソールにログインします。
- 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。

次に進む前に

- 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 [アイテム] 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。

[アイテム] 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。

開始する前に

- **テナント 管理者**または**カタログ管理者**として vRealize Automation コンソールにログインします。
- 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。アイテムは使用中止としてカタログ 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、これを示すために使用します。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。
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。
新規と注目	カタログ アイテムは、[ホーム] ページの [新規と注目] 領域に表示されます。

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。

次に進む前に

- カatalog アイテムをサービス カタログで使用できるようにするには、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、[アイテム] 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。

開始する前に

- テナント 管理者または **カタログ管理者** として vRealize Automation コンソールにログインします。
- 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、[詳細表示] 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 [アップデート] をクリックします。

次に進む前に

[「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 カタログ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 カタログに表示するには、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 カタログに表示されるアイテムが決まります。サービス カタログ 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 カタログ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 カタログ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、[アイテム] 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。

■ [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内では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内では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atalog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atalog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 [アイテム] 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、[アイテム] 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。

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 [アイテム] 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atalog 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atalog 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を付与します。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atalog 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atalog 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atalog ユーザーを付与する場合、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とグループは、サービス カタログ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 [アイテム] 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。
- カタログ管理者は、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、ビジネス グループを選択し、資格作成対象のビジネス グループ内で個々のユーザーおよびグループを指定する必要があります。

資格の作成方法を理解し、サービス、カタログ アイテム、アクションと承認との相互作用を利用してサービス カタログ内の正しいアイテムを提供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。

開始する前に

- **テナント 管理者**または**カタログ管理者**として vRealize Automation コンソールにログインします。
- ユーザーに資格が付与されるカタログ 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。 [「サービスへのカタログ 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。ユーザーにサービス カタログ内アイテムに対する資格を承認なしで付与する場合は、1 つ以上のサービス、カタログ アイテム、およびアクションに後で承認を追加するように資格を変更できます。

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] 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 カタログ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>指定可能な値として、ドラフト、有効、無効があります。</p> <ul style="list-style-type: none"> ■ ドラフト。アイテムはサービス カタログ内で使用可能ではなく、有効になりません。資格を有効にした後は、ドラフト ステータスに戻すことはできません。 ■ 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。サービス カタログ内では使用不可になっていますが、以前有効だった資格です。資格は、有効期限日が過ぎたため、またはユーザーによって無効化されました。
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>ある資格をすべてのユーザーが利用できるようにする場合は、[すべてのユーザー] ビジネス グループを用意して、すべてのユーザーを含むカスタムのユーザー グループを作成するか、ビジネス グループごとに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>1 つ以上のユーザーまたはグループを追加します。使用可能なユーザーまたはグループは、選択したビジネス グループのメンバーに限定されます。</p> <p>ステータスがドラフトの場合、ユーザーまたはグループを指定する必要はありません。資格を有効にするには、少なくとも 1 つのユーザーまたはグループを指定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資格です。このサービスに後でアイテムを追加すると、資格のあるユーザーのサービス カタログにそのアイテムが追加されます。資格には、サービスと個別のカタログ 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だけで使用できません。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>登録されたアクションは、サービス カタログに表示されません。これらのアクションは、プロビジョニング済みアイテムの [アイテム] 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>選択すると、アクションは、この資格の該当するアイテムに対するビジネス グループ メンバーを使用可能です。アクションに資格を与える方法としては、特定のアイテムに対してアクションを指定できるようになるため、この方法が推奨されます。</p> <p>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。

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。

次に進む前に

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 カタログ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 Connie 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 4-49. 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：Connie
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

Connie 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 Connie の申請に適用されます。


表 4-50. 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。 Connie 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 Connie 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 Connie 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。

開始する前に

テナント 管理者またはカタログ管理者として vRealize Automation コンソールにログインします。

手順

- 1 [管理] - [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、その優先度が変わります。
- 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atalog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atalog ユーザーが申請したときに、承認者が [承認] ページの [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、[申請] 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atalog 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atalog 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、承認ポリシーを構成して異なるタイプのガバナンスを実現可能にするいくつかの方法を示しています。

表 4-51. 承認ポリシーおよび結果の例

ガバナンスの目的	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] タブヘ 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] タブヘ 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。

表 4-51. 承認ポリシーおよび結果の例 (続き)

ガバナンスの目的	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
仮想インフラストラクチャリソースを管理し、コストを制御するには、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用に、もう 1 つを 1 日あたりのマシンのコスト用にします。	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。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、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。
			レベル 2 [条件に応じて必要] を選択します。 条件 [コスト] > [1 日あたり 15.00] を選択します。	[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。		

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 4-52. 資格の構成

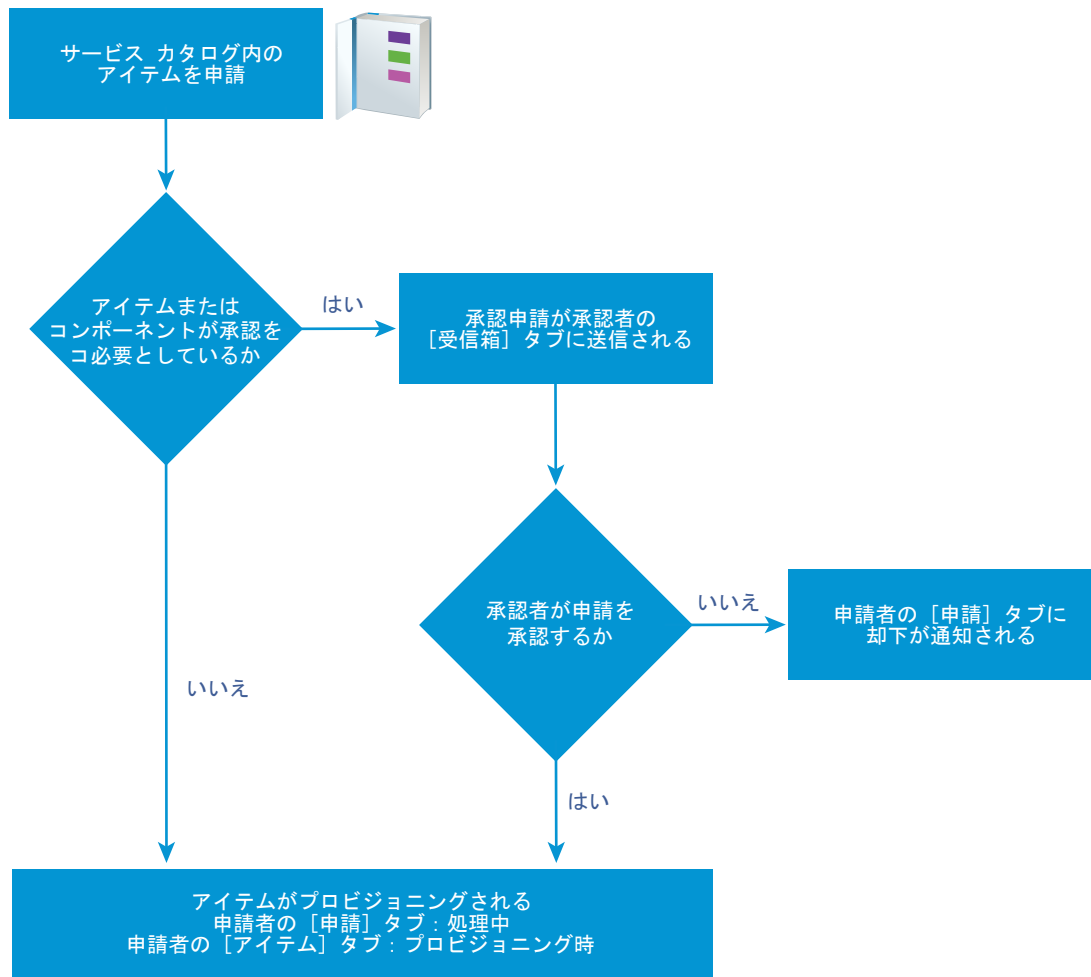
資格名	ビジネス グループ	使用可能なサービス	使用可能なアイテム
資格 1	QE	テスト	カタログ アイテム申請 - 仮想マシン コンポーネントに適用される仮想マシン
資格 2	QE	トレーニング	

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。

開始する前に

テナント 管理者または承認管理者として vRealize Automation コンソールにログインします。

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、リース、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。

開始する前に

テナント 管理者または承認管理者として vRealize Automation コンソールにログインします。

手順

- 1 [管理] - [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。

次に進む前に

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。

開始する前に

[「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	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。
イベント サブスクリプションを使用する	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。 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。

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	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。
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。

次に進む前に

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、リソース、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。

開始する前に

- テナント管理者または承認管理者として vRealize Automation コンソールにログインします。
- [「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
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。

- 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。

次に進む前に

- 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 4-53. 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>

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 4-54. 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すが、承認ポリシーは適用されません。
ポリシー タイプ	<p>承認ポリシーの申請タイプを表示します。</p> <p>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。</p>
アイテム	<p>選択したカタログ アイテムが表示されます。</p> <p>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。</p>
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	<p>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。</p> <p>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。</p>
リンクされた資格の表示	<p>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。</p> <p>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。</p>

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 4-55. 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。
[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]	承認ポリシーがすべての申請でトリガされます。 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。
[条件に応じて必要]	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。 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。 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。 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。 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。 <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]	承認申請を選択したユーザーに送信します。 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atalog 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。

表 4-55. レベル情報のオプション (続き)

オプション	説明
[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>
[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。</p> <p>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。</p> <p>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。</p> <p>[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。</p>
[全員の承認が必要]	<p>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。</p> <p>[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。</p>

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 4-56. 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]	<p>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によって異なります。</p> <p>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。</p>

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 4-57. 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。

開始する前に

テナント 管理者または承認管理者として vRealize Automation コンソールにログインします。

手順

- [管理] - [承認ポリシー] を選択します。
- コピーする承認ポリシーの行を選択します。
- [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。
- 編集する新しい承認ポリシーを選択します。
- [名前] テキスト ボックスに名前を入力します。
- (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。

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。

次に進む前に

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。

開始する前に

テナント **管理者** または **承認管理者** として vRealize Automation コンソールにログインします。

手順

- 1 [管理] - [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す。
 - 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。

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。

次に進む前に

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。

開始する前に

- 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 コンソールにログインします。

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。

承認ポリシーを削除します。

シナリオ：Rainpole アーキテクトによるブループリントのテスト用にカタログを構成する

テナント管理者の権限を使用して、ガバナンスの範囲が限られた特別なカタログ サービスを作成します。このサービスを使用して、Rainpole アーキテクトは、本番環境にブループリントをエクスポートする前に、作業結果を効果的にテストすることができます。ブループリント テスト サービスを作成し、vSphere CentOS ブループリントをサービスに追加して、サービスに関連するすべてのカタログ アイテムとアクションの使用資格を Rainpole アーキテクトに付与します。このようにすることで、アーキテクトはカタログ アイテムをプロビジョニングして作業結果を確認できます。



手順

1 シナリオ : Rainpole ブループリント テスト用のカタログ サービスを作成する

テナント管理者の権限を使用して、「Rainpole サービス」というカタログ サービスを作成します。自分をこのサービスの所有者およびサポート連絡先として割り当てます。これにより、何か問題があれば、Rainpole アーキテクトからの連絡を受けることができます。

2 シナリオ : vSphere CentOS カタログ アイテムを Rainpole サービスに追加する

テナント管理者の権限を使用して、公開済みの vSphere CentOS マシン ブループリントを Rainpole サービスに追加します。

3 シナリオ : カタログ アイテムを要求するための資格を Rainpole アーキテクトに付与する

テナント管理者の権限を使用して、Rainpole サービスに属するすべてのアクションおよびアイテムへの資格を Rainpole アーキテクトに付与します。

シナリオ : Rainpole ブループリント テスト用のカタログ サービスを作成する

テナント管理者の権限を使用して、「Rainpole サービス」というカタログ サービスを作成します。自分をこのサービスの所有者およびサポート連絡先として割り当てます。これにより、何か問題があれば、Rainpole アーキテクトからの連絡を受けることができます。

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 **Rainpole サービス** を入力します。

4 [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。

5 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、自分を [所有者] と [サポート連絡先] に追加します。

6 [OK] をクリックします。

次に進む前に

テナント管理者の権限を使用して、公開済みの vSphere CentOS マシン ブループリントを Rainpole サービスに追加します。

シナリオ : vSphere CentOS カタログ アイテムを Rainpole サービスに追加する

テナント管理者の権限を使用して、公開済みの vSphere CentOS マシン ブループリントを Rainpole サービスに追加します。

プロビジョニングする公開済みのすべてのブループリントをカタログ アイテムとしてサービスに含める必要がありますが、各ブループリントを同時に複数のサービスでカタログ アイテムにすることはできません。複数のカタログ サービスに同時に公開する必要がある場合は、ブループリントのコピーを作成します。

手順

1 [管理] - [カタログ管理] - [サービス] を選択します。

- 2 [サービス] リストで、[ブループリント テスト] 行を選択して [カタログ アイテムの管理] をクリックします。
- 3 [新規] アイコン (+) をクリックします。
- 4 [vSphere 上の CentOS] チェック ボックスを選択します。

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。

次に進む前に

テナント管理者の権限を使用して、Rainpole サービスからカタログ アイテムを申請する資格を Rainpole アーキテクトに付与します。

シナリオ：カタログ アイテムを要求するための資格を Rainpole アーキテクトに付与する

テナント管理者の権限を使用して、Rainpole サービスに属するすべてのアクションおよびアイテムへの資格を Rainpole アーキテクトに付与します。

サービスに含まれるすべてのアクションとアイテムに対する資格を Rainpole アーキテクトに付与することで、そのアーキテクトは、テスト用の新しいカタログ アイテムを簡単にサービスに追加できるようになります。本番環境では、さまざまな資格を使用して、厳密なガバナンスを構成できます。それぞれのユーザーにどのカタログ アイテムの要求を許可し、各ユーザーが自分の所有する特定のカタログ アイテムに対してどのアクションを実行できるかの管理が必要になる場合があります。

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 **Rainpole architect entitlement** を入力します。
 - b [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。
 - c [ビジネス グループ] ドロップダウン メニューから Rainpole のビジネス グループを選択します。
 - d [ユーザーおよびグループ] 検索ボックスを使用して Rainpole アーキテクトを追加します。
 - e [次へ] をクリックします。

4 Rainpole カタログ サービスの資格を付与します。

- 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 [Rainpole サービス] を選択します。
- c [OK] をクリックします。

これで、資格に含まれるユーザーにはすべて、Rainpole サービス内のすべてのカタログ アイテムの使用資格が付与されるようになりました。

5 すべてのユーザー アクションの使用資格を付与します。

- 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 列ヘッダのチェックボックスを選択し、すべてのアクションの使用資格を付与します。
- c [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] チェックボックスを選択すると、他のカタログ サービスのユーザーに対して厳しいガバナンスを後で適用できます。
- d [OK] をクリックします。

アーキテクトが Rainpole サービスからプロビジョニングするカタログ アイテムに対して、適用可能なアクションを実行する資格がアーキテクトに付与されます。アーキテクトが異なるサービスから、または異なる資格を介してプロビジョニングしたアイテムに対して、これらのアクションを実行する資格はアーキテクトに付与されません。

6 [終了] をクリックします。

これで、すべてのアーキテクトが vSphere CentOS マシン プループリントと、自分のサービスに追加された新しいカタログ アイテムを表示および要求できるようになりました。

次に進む前に

設定したローカル テスト ユーザーのアカウントを使用して vSphere CentOS カタログ アイテムのプロビジョニングを要求し、プループリントとカタログ構成をテストします。

シナリオ : Rainpole CentOS マシンをテストする

作成したローカル テスト ユーザー アカウントを使用して、vSphere CentOS マシンのプロビジョニングを要求します。プロビジョニングされたマシンにログインし、そのマシンが正常に機能していることを確認します。



手順

1 シナリオ : Rainpole 仮想マシンを要求する

テスト ユーザー アカウントを使用して、vSphere 仮想マシン上の CentOS をプロビジョニングするためのサービス カタログ アイテムを要求します。

2 シナリオ : プロビジョニング済みの Rainpole マシンにログインする

テスト ユーザー アカウントを使用して、プロビジョニングに成功した vSphere CentOS マシンにログインします。

シナリオ : Rainpole 仮想マシンを要求する

テスト ユーザー アカウントを使用して、vSphere 仮想マシン上の CentOS をプロビジョニングするためのサービス カタログ アイテムを要求します。

手順

- 1 vRealize Automation コンソールからログアウトします。
- 2 ユーザー名 **test_user**、パスワード **VMware1!** で再ログインします。
- 3 [カタログ] タブをクリックします。
- 4 [申請] ボタンをクリックして、カタログ アイテムを申請します。
- 5 [説明] テキスト ボックスに **verifying functionality** と入力します。
- 6 [送信] をクリックして、カタログ項目を要求します。
- 7 [申請] タブをクリックして、申請のステータスを監視します。

マシンが正常にプロビジョニングされると、**成功**というステータス メッセージが表示されます。

次に進む前に

プロビジョニング済みのマシンにログインします。

シナリオ : プロビジョニング済みの Rainpole マシンにログインする

テスト ユーザー アカウントを使用して、プロビジョニングに成功した vSphere CentOS マシンにログインします。

手順

- 1 [アイテム] - [マシン] を選択します。
- 2 vSphere 上の CentOS アイテムの隣にある矢印を選択します。
展開された項目の下に、プロビジョニング済みのマシンが表示されます。
- 3 プロビジョニング済みのマシンをクリックします。
- 4 右側のパネルの [マシンへのリモート ログイン] をクリックします。
- 5 マシンにログインします。

ブループリントを継続的に開発するために、vRealize Automation を最小インストールを行い、事前検証を設定して、環境を構成します。

次に進む前に

- vRealize Automation の Enterprise ライセンスをお持ちの場合は、引き続きこのドキュメントを参照して、ソフトウェア コンポーネントを使用したマシンのプロビジョニングについて理解します。
- 本番環境のインストールを計画します。『リファレンス アーキテクチャ』を参照してください。
- vRealize Automation の構成、ブループリントの設計とエクスポート、およびサービス カタログの管理のためのその他のオプションを確認します。『vRealize Automation の構成』を参照してください。

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

テナント管理者として、ブループリント アーキテクトがカタログ アイテムを作成し、テスト ケースを実行する開発と品質管理グループに CentOS 仮想マシン上の MySQL を配信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るようにするには、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。

開始する前に

- テナント管理者またはカタログ管理者として vRealize Automation コンソールにログインします。
- MySQL を vSphere CentOS 仮想マシンで配信するためのブループリントを公開します。[「シナリオ：Rainpole リンク クローン マシン上の MySQL を提供するためのブループリントを組み合わせる」](#)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。[「ブループリントのエクスポートとインポート」](#)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。

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] - [カタログ管理] - [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、[カタログ 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。

開発と品質管理サービスに MySQL カタログ 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 カタログ 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カタログ 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。

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。

次に進む前に

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。

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atalog 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。

開始する前に

- **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。

手順

1 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。

2 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。

3 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。

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 - カタログ 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。

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。

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atalog - カatalog 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atalog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atalog - カatalog 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。

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。

次に進む前に

ビジネス グループのメンバーとして、サービス カatalog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。