

vRealize Automation のインストールおよびアップグレード

2018 年 10 月 5 日

vRealize Automation 7.4



vmware®

VMware Web サイトで最新の技術ドキュメントをご確認いただけます。

<https://docs.vmware.com/jp/>

VMware の Web サイトでは、最新の製品アップデートを提供しています。

本書に関するご意見、ご要望をお寄せください。フィードバック送信先：

docfeedback@vmware.com

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 © 2017–2018 VMware, Inc. All rights reserved. [著作権および商標](#).

内容

| | | |
|---|---|-----|
| 1 | vRealize Automation のインストールまたはアップグレード | 4 |
| | vRealize Automation リファレンス アーキテクチャ | 4 |
| | 初期導入と初期構成に関する推奨事項 | 4 |
| | vRealize Automation の展開 | 5 |
| | vRealize Business for Cloud 導入にあたっての考慮事項 | 7 |
| | vRealize Automation のスケーラビリティ | 7 |
| | vRealize Business for Cloud のスケーラビリティ | 10 |
| | vRealize Automation 高可用性構成の考慮事項 | 10 |
| | vRealize Business for Cloud 高可用性の考慮事項 | 12 |
| | vRealize Automation のハードウェア仕様および最大容量 | 12 |
| | vRealize Automation 小規模展開の要件 | 14 |
| | vRealize Automation を中規模に展開する場合の要件 | 20 |
| | vRealize Automation を大規模に展開する場合の要件 | 25 |
| | vRealize Automation の複数のデータセンター データの展開 | 31 |
| | vRealize Automation の安全な構成 | 32 |
| | vRealize Automation のセキュアなベースラインの概要 | 32 |
| | インストール メディアの整合性の確認 | 33 |
| | VMware システム ソフトウェア インフラストラクチャのセキュリティ強化 | 34 |
| | インストールされたソフトウェアの確認 | 35 |
| | VMware セキュリティ アドバイザリおよびパッチ | 36 |
| | セキュアな構成 | 36 |
| | ホストのネットワーク セキュリティの構成 | 69 |
| | 監査とログ | 84 |
| | vRealize Automation のインストール | 85 |
| | vRealize Automation インストールの概要 | 85 |
| | vRealize Automation のインストールの準備 | 93 |
| | vRealize Automation アプライアンスの展開 | 108 |
| | インストール ウィザードを使用した vRealize Automation のインストール | 113 |
| | 標準 vRealize Automation インストール インターフェイス | 138 |
| | vRealize Automation のサイレントインストール | 211 |
| | vRealize Automation インストール後のタスク | 217 |
| | vRealize Automation インストールのトラブルシューティング | 235 |
| | vRealize Automation のアップグレード | 262 |
| | vRealize Automation 7.1 以降から 7.4 へのアップデート | 265 |
| | vRealize Automation 6.2.5 から 7.4 へのアップグレード | 331 |
| | vRealize Automation 7.4 への移行 | 412 |

vRealize Automation のインストール またはアップグレード

1

vRealize Automation の初回インストールを実行するか、既存の環境を最新のバージョンにアップグレードできます。

この章には、次のトピックが含まれています。

- [vRealize Automation リファレンス アーキテクチャ](#)
- [vRealize Automation の安全な構成](#)
- [vRealize Automation のインストール](#)
- [vRealize Automation のアップグレード](#)

vRealize Automation リファレンス アーキテクチャ

リファレンス アーキテクチャは、標準の vRealize Automation 展開の構造と構成を説明するものです。また、高可用性、スケーラビリティ、およびデプロイ プロファイルの情報を示します。

リファレンス アーキテクチャには、次のコンポーネントに関する情報が含まれます。

- VMware vRealize Automation
- VMware vRealize Business for Cloud

ソフトウェア要件、インストールおよびサポートされるプラットフォームについては、各製品のドキュメントを参照してください。

初期導入と初期構成に関する推奨事項

すべての VMware vRealize Automation コンポーネントを VMware の推奨事項に沿って導入および構成します。

vRealize Automation、vRealize Business for Cloud、vRealize Orchestrator のタイムゾーンを同じにして、時計を同期させます。

vRealize Automation、vRealize Business for Cloud、vRealize Orchestrator を同じ管理クラスタにインストールします。その管理クラスタとは別のクラスタにマシンをプロビジョニングして、ユーザー ワークロードとサーバークロードを分離します。

プロキシ エージェントは通信先のエンドポイントと同じデータセンターに展開します。DEM ワーカーのリモートデータセンターへの配置は、それを必要とするワークフロー スキルに基づく明確な使用事例が存在しない場合には、お勧めしません。プロキシ エージェントと DEM ワーカー以外のすべてのコンポーネントは、同じデータセンターか、同じメトロ エリア ネットワーク内のデータセンターに展開する必要があります。メトロ エリア ネットワーク内のデータセンター間の遅延は 5 ミリ秒位内、帯域幅は 1 GB/s 以上である必要があります。

サポートの表明を含む詳細については、VMware ナレッジベースの記事「Installing the VMware vRealize Automation on a distributed multi-site instance」を参照してください。この記事は、
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2134842 で参照できます。

vRealize Automation の展開

VMware のリソースの推奨事項を vRealize Automation 展開計画の開始点として使用します。

初期のテストと本番環境への展開後も、引き続きパフォーマンスを監視し、必要に応じて「[vRealize Automation のスケーラビリティ](#)」の説明に従って追加のリソースを割り当てます。

認証

vRealize Automation を構成するときに、ユーザー認証にデフォルトのディレクトリ管理コネクタを使用するか、既存の SAML ベースの ID プロバイダを指定してシングル サインオン環境をサポートできます。

2 要素認証が必要な場合、vRealize Automation は RSA SecurID との統合をサポートします。この統合ポイントが構成されると、ユーザーにはユーザー ID およびパスコードを要求されます。

ロード バランサの考慮事項

最小応答時間またはラウンドロビン方式を使用して、vRealize Automation アプライアンスとインフラストラクチャの Web サーバにトラフィックを分散します。セッション アフィニティ（スティッキー セッション）機能を有効にして、後続の要求を各一意のセッションからロード バランサ プール内の同じ Web サーバに送信できます。

ロード バランサを使用して Manager Service のフェイルオーバーを管理できますが、Manager Service は一度に 1 つのみアクティブになるため、ロード バランシング アルゴリズムは使用しないでください。また、ロード バランサでフェイルオーバーを管理するときは、セッション アフィニティを使用しないでください。

vRealize Automation Appliance をロード バランシングする場合は、ポート 443 と 8444 を使用します。Infrastructure Web サイトと Infrastructure Manager Service の場合は、ポート 443 のみロード バランシングする必要があります。

他のロード バランサも使用できますが、NSX、F5 BIG-IP ハードウェア、および F5 BIG-IP Virtual Edition はテスト済みで使用が推奨されます。

ロード バランサの構成の詳細については、vRealize Automation のドキュメントを参照してください。

データベースの展開

vRealize Automation は、7.0 以降のリリースでは、アプライアンス データベースを自動的にクラスタ化します。7.0 以降のすべての新しい展開では、内部アプライアンス データベースを使用する必要があります。7.1 以降にアップグレードする vRealize Automation インスタンスの外部データベースはアプライアンス データベースにマージする必要があります。アップグレード プロセスの詳細については、vRealize Automation の製品ドキュメントを参照してください。

インフラストラクチャ コンポーネントを本番環境に展開する場合は、専用のデータベース サーバを使用して Microsoft SQL Server (MSSQL) データベースをホストします。vRealize Automation には、Microsoft 分散トランザクション コーディネータ サービス (MSDTC) を使用するように構成されているデータベース サーバと通信するマシンが必要です。デフォルトで、MSDTC にはポート 135 とポート 1024 ～ 65535 が必要です。

デフォルトの MSDTC ポートの変更の詳細については、Microsoft のナレッジベース記事「Configuring Microsoft Distributed Transaction Coordinator (DTC) to work through a firewall」を参照してください。この記事は、<https://support.microsoft.com/ja-jp/kb/250367> で参照できます。

IaaS Manager Service ホストでは、IaaS SQL Server データベース ホストの NETBIOS 名を解決できる必要があります。NETBIOS 名を解決できない場合は、Manager Service マシンの **/etc/hosts** ファイルに、SQL Server の NETBIOS 名を追加し、Manager Service を再起動します。

vRealize Automation は、Microsoft SQL Server 2016 でのみ SQL AlwaysON グループをサポートしています。SQL Server 2016 をインストールする場合は、データベースを 100 モードで作成する必要があります。Microsoft SQL Server の古いバージョンを使用する場合は、共有ディスクを使用してフェイルオーバー クラスタ インスタンスを使用します。MSDTC を使用した SQL AlwaysOn グループの構成については、<https://msdn.microsoft.com/ja-jp/library/ms366279.aspx> を参照してください。

データ収集の設定

デフォルトのデータ収集設定では、ほとんどの実装環境に対応する収集開始ポイントが指定されています。本番環境への展開後も、引き続きデータ収集のパフォーマンスを監視して、調製を行う必要があるかどうか確認します。

プロキシ エージェント

パフォーマンスを最大にするには、関連付けられているエンドポイントと同じデータセンターにエージェントを展開します。追加のエージェントをインストールして、システムのスループットと並行性を向上させることができます。分散展開には世界各地に分散された複数のエージェント サーバを含めることができます。

エージェントを関連付けられているエンドポイントと同じデータセンターにインストールした場合、データ収集のパフォーマンスは平均で 200% 向上する可能性があります。測定される収集時間には、プロキシエージェントと Manager Service 間でのデータの転送時間のみが含まれます。Manager Service でデータを処理する時間は含まれません。

たとえば、製品をパロアルトのデータセンターに展開し、vSphere エンドポイントがパロアルト、ボストン、およびロンドンにあるとします。この構成では、vSphere プロキシ エージェントはパロアルト、ボストン、およびロンドンの各エンドポイントに展開されます。エージェントがパロアルトのみに展開された場合は、ボストンとロンドンのデータ収集時間が 200% 増える可能性があります。

Distributed Execution Manager の構成

一般的に、Distributed Execution Manager (DEM) は、Model Manager ホストにできるだけ近い場所に置きます。DEM Orchestrator には常に Model Manager への強力なネットワーク接続が必要です。インストーラは、デフォルトで、Manager Service とともに DEM Orchestrator を配置します。プライマリ データセンターに、フェイルオーバー用と 2 つの DEM ワーカー インスタンス用に 2 つの DEM Orchestrator インスタンスを作成します。

DEM ワーカー インスタンスが場所に固有のワークフローを実行する場合は、その場所にインスタンスをインストールします。

スキルを関連のワークフローと DEM に割り当てて、それらのワークフローが常に適切な場所にある DEM で実行されるようにします。vRealize Automation デザイナ コンソールを使用したワークフローと DEM へのスキルの割り当てについては、vRealize Automation 拡張機能のドキュメントを参照してください。

最適なパフォーマンスにするには、DEM とエージェントを個別のマシンにインストールします。vRealize Automation エージェントのインストールの詳細については、[エージェントのインストール](#)を参照してください。

vRealize Orchestrator

すべての新しい導入環境で、内部 vRealize Orchestrator インスタンスを使用します。必要な場合には、従来の導入環境では引き続き外部 vRealize Orchestrator を使用できます。内部 vRealize Orchestrator インスタンスに割り当てられたメモリを増やす手順については、https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2147109 を参照してください。

最適な製品パフォーマンスを得るためには、vRealize Orchestrator のコンテンツを本番環境にインポートする前に、『vRealize Orchestrator Coding Design Guide』の構成ガイドラインを確認して実装します。

vRealize Business for Cloud 導入にあたっての考慮事項

VMware のガイドラインに従って、vRealize Business for Cloud（旧称 vRealize Business Standard Edition）を導入します。

ロード バランサの考慮事項

データ収集用の接続では、ロード バランシングはサポートされません。詳細については、「[vRealize Automation のスケーラビリティ](#)」を参照してください。ユーザー インターフェイスおよび API クライアント接続用の vRealize Business for Cloud アプライアンスでは、vRealize Automation ロード バランサを使用できます。

vRealize Automation のスケーラビリティ

vRealize Automation システムを構成するときは、適用可能なすべてのスケーラビリティ要因を考慮します。

ユーザー

vRealize Automation アプライアンスは、100,000 人未満のユーザーを同期するよう構成されています。システムにそれ以上のユーザーがいる場合は、vRealize Automation ディレクトリ管理にメモリを追加する必要がある可能性があります。ディレクトリ管理へのメモリの追加の詳細については、[ディレクトリ管理へのメモリの追加](#)を参照してください。

同時プロビジョニングのスケーラビリティ

デフォルトで、vRealize Automation はエンドポイントごとに 8 つの同時プロビジョニングのみ処理します。この制限の増加については、[同時マシン プロビジョニングの構成](#)を参照してください。

すべての展開は、2 つ以上の DEM ワーカーから始めることをお勧めします。vRA 6.x では、DEM ワーカーあたり 15 のワークフローを同時に処理できます。vRealize Automation 7.0 以降では、これが 30 にまで増加しました。

マシンがワークフロー スタブでカスタマイズされている場合は、同時にプロビジョニングされる 20 台のマシンごとに 1 つの DEM ワーカーが必要です。たとえば、100 の同時プロビジョニングをサポートするシステムの場合は、最低 5 つの DEM ワーカーが必要になります。

DEM ワーカーとスケーラビリティの詳細については、「[Distributed Execution Manager のパフォーマンスの分析と調整](#)」を参照してください。

データ収集のスケーラビリティ

データ収集の完了時間は、コンピューティング リソースの容量、コンピューティング リソースまたはエンドポイントのマシンの数、現在のシステム、ネットワークの負荷、その他の変数によって異なります。パフォーマンスは、データ収集のタイプに応じて異なる速度でスケールします。

データ収集のタイプごとに、オーバーライドまたは変更が可能なデフォルトの間隔があります。インフラストラクチャ管理者は、インフラストラクチャ ソース エンドポイントのデータ収集を手動で開始できます。ファブリック管理者は、コンピューティング リソースのデータ収集を手動で開始できます。次の値は、データ収集のデフォルト間隔を示しています。

表 1-1. データ収集のデフォルト間隔

| データ収集タイプ | デフォルト間隔 |
|----------|-------------|
| インベントリ | 24 時間ごと（毎日） |
| 状態 | 15 分ごと |
| パフォーマンス | 24 時間ごと（毎日） |

パフォーマンスの分析と調整

データを収集するリソースの数が増えると、特に状態データの収集の場合、データ収集の完了時間がデータ収集間隔よりも長くなる可能性があります。コンピューティング リソースまたはエンドポイントでのデータ収集が時間内に完了するか、キューに入れられているかを確認する方法については、「データ収集」ページを参照してください。[最終完了日時] フィールドの値が、**キューに登録済み** または **処理中** を示す場合があります。この問題が発生した場合は、データ収集間隔を長くしてデータ収集の頻度を減らすことができます。

あるいは、エージェントあたりの同時データ収集制限を増やすことができます。デフォルトで、vRealize Automation は、同時データ収集アクティビティがエージェントあたり 2 に制限され、この制限を超える要求はキューに登録されます。この制限により、データ収集アクティビティはパフォーマンス全体に影響を与えずにすばやく完了できます。同時データ収集の上限を増やすことはできますが、このオプションと全体的なパフォーマンスの低下のバランスを考慮する必要があります。

構成されている vRealize Automation エージェントあたりの上限を増やす場合は、これらの実行タイムアウト間隔を 1 つ以上を増やすことができます。データ収集の同時実行とタイムアウト間隔の構成方法の詳細については、vRealize Automation システム管理のドキュメントを参照してください。Manager Service のデータ収集は、CPU に負担がかかります。Manager Service ホストの処理能力を増やすと、データ収集全体にかかる時間が削減される可能性があります。

Amazon Elastic Compute Cloud (Amazon AWS) でのデータ収集は、特にシステムで複数の地域のデータを同時に収集する場合、およびデータがそれらの地域で以前に収集されていない場合、CPU の使用量が増える可能性があります。このタイプのデータ収集によって、Web サイトのパフォーマンスが全体的に低下する場合があります。パフォーマンスへの影響が大きい場合は、Amazon AWS インベントリ データの収集頻度を減らしてください。

ワークフロー処理のスケーラビリティ

DEM Orchestrator がワークフローの処理を開始してからワークフローの実行が終了するまでの、平均的なワークフロー処理時間は同時ワークフローの数に合わせて増えます。ワークフローのボリュームは、マシン要求および一部のデータ収集アクティビティを含む、vRealize Automation アクティビティの関数です。

大量のデータを使用する場合の Manager Service の構成

多数のオブジェクト（3,000 台以上の仮想マシンなど）を含む VMware vSphere クラスタを使用する場合は、Manager Service の構成ファイルを編集して設定値を大きくします。この設定変更を行わないと、大きなインベントリデータの収集に失敗する可能性があります。

ManagerService.exe.config ファイルの **ProxyAgentServiceBinding** 設定と **maxStringContentLength** 設定のデフォルト値を変更します。

手順

- 1 テキスト エディタで **ManagerService.exe.config** ファイルを開きます。

このファイルは、通常は **C:\Program Files (x86)\VMware\VCAC\Server** にあります。

- 2 ファイル内で **binding name** 行と **readerQuotas** 行を見つけます。

```
<binding name="ProxyAgentServiceBinding" maxReceivedMessageSize="13107200">
  <readerQuotas maxStringContentLength="13107200" />
```

注: **binding name = "ProvisionServiceBinding"** という行と間違えないように注意してください。

- 3 **maxReceivedMessageSize** 属性と **maxStringContentLength** 属性に割り当てられている値を、より大きな値に置き換えます。

最適なサイズは、VMware vSphere クラスタに含まれるオブジェクトの数が今後どのくらい増えるかによって決まります。たとえば、これらの値を試験的に 10 倍に増やすことができます。

- 4 変更内容を保存し、ファイルを閉じます。
- 5 vRealize Automation Manager Service を再起動します。

Distributed Execution Manager のパフォーマンスの分析と調整

進行中または保留中のワークフローの総数は、いつでも [分散実行のステータス] ページで確認できます。[ワークフロー履歴] ページでは、特定のワークフローの所要時間を調べることもできます。

保留中のワークフローの数が多い場合や、ワークフローの所要時間が予想より長い場合は、ワークフローを取得する Distributed Execution Manager (DEM) ワーカー インスタンスの数を増やします。DEM ワーカー インスタンスはそれぞれ 30 個のワークフローを同時に処理できます。それを超える数のワークフローは実行用のキューに入れられます。

ワークフローのスケジュールを調整して、同時に開始されるワークフローの数を最小限に抑えることもできます。たとえば、1 時間ごとに実行されるすべてのワークフローを、同じ時間に一度に開始するのではなく、実行時間をずらすようにすると、DEM リソースの競合が発生しなくなります。ワークフローの詳細については、vRealize Automation 拡張機能のドキュメントを参照してください。

ワークフロー（特に一部のカスタム ワークフロー）の中には CPU の負荷が高いものがあります。DEM ワーカー マシンの CPU 負荷が高い場合は、DEM マシンの処理能力を強化するか、環境に DEM マシンを追加することを検討します。

vRealize Business for Cloud のスケーラビリティ

VMware のガイドラインに従って、vRealize Business for Cloud インストール環境をスケーラビリティ用に構成します。

vRealize Business for Cloud は、10 個の VMware vCenter Server インスタンスに 20,000 台の仮想マシンまで拡張できます。インベントリ データ収集の最初の同期では、3 つの VMware vCenter Server インスタンスで 20,000 の仮想マシンを同期するのにおよそ 3 時間かかります。VMware vCenter Server から統計を同期するには、20,000 の仮想マシンでおよそ 1 時間かかります。デフォルトで、コスト計算ジョブは毎日実行され、20,000 の仮想マシンでは実行ごとにおよそ 2 時間かかります。

注: vRealize Business for Cloud 1.0 では、デフォルトの仮想アプライアンス構成で最大 20,000 の仮想マシンをサポートできます。仮想アプライアンスの制限をデフォルト設定より増やしても、サポートできる仮想マシンの数は増えません。

vRealize Automation 高可用性構成の考慮事項

システムの堅牢性を最大にする必要がある場合は、VMware ガイドラインに従って vRealize Automation システムを高可用性向けに構成します。

vRealize Automation アプライアンス

vRealize Automation アプライアンスは、アプライアンス データベース以外のすべてのコンポーネントに対してアクティブ/アクティブの高可用性をサポートします。7.3 リリースから、3 台のノードが展開され、2 台のノード間で同期レプリケーションが構成されている場合、データベースのフェイルオーバーは自動で実行されます。vRealize Automation アプライアンス がデータベースの障害を検出すると、適切なデータベース サーバがマスターに昇格されます。アプライアンス データベースの監視と管理は、仮想アプライアンス管理コンソールの [vRA 設定] - [データベース] タブで実行できます。

これらのアプライアンスで高可用性を有効にするには、アプライアンスをロード バランサの配下に置きます。詳細については、「[ロード バランサの構成](#)」を参照してください。リリース 7.0 より、アプライアンス データベース、および vRealize Orchestrator は自動的にクラスタ化され、使用できるようになりました。

vRealize Automation ディレクトリ管理

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

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

高可用性向けのディレクトリ管理構成の詳細については、[Configure Directories Management for High Availability](#) を参照してください。

インフラストラクチャ Web サーバ

インフラストラクチャ Web Server コンポーネントはすべてアクティブ/アクティブ高可用性をサポートします。これらのコンポーネントで高可用性を有効にするには、コンポーネントをロード バランサの下に置きます。

インフラストラクチャ Manager Service

Manager Service コンポーネントは、アクティブ/パッシブの高可用性をサポートします。このコンポーネントで高可用性を有効にするには、2 つの Manager Service をロード バランサの下に置きます。vRealize Automation 7.3 以降では、フェイルオーバーが自動的に実行されます。

アクティブ Manager Service で障害が発生した場合、ロード バランサの下 Windows サービスが停止されていない場合は、これを停止します。パッシブ Manager Service を有効にし、Windows サービスをロード バランサの下で再起動します。[「アクティブな Manager Service のインストール」](#) を参照してください。

エージェント

エージェントは、アクティブ/アクティブの高可用性をサポートします。高可用性向けのエージェント構成の詳細については、vRealize Automation 構成のドキュメントを参照してください。ターゲットサービスの高可用性をチェックします。

Distributed Execution Manager ワーカー

ワーカー ロールで実行されている Distributed Execution Manager (DEM) は、アクティブ/アクティブの高可用性をサポートします。DEM ワーカー インスタンスが失敗すると、DEM Orchestrator は失敗を検出し、DEM ワーカー インスタンスが実行しているワークフローをキャンセルします。DEM ワーカー インスタンスがオンラインに戻ると、DEM Orchestrator がインスタンスのワークフローをキャンセルしたことを検出し、それらのインスタンスの実行を停止します。ワークフローが途中でキャンセルされないようにするには、DEM ワーカー インスタンスを数分オフラインにしてから、そのワークフローをキャンセルします。

Distributed Execution Manager Orchestrator

Orchestrator ロールで実行されている DEM は、アクティブ/ アクティブの高可用性をサポートします。DEM Orchestrator が起動すると、実行中の別の DEM Orchestrator が検索されます。

- 実行中の DEM Orchestrator インスタンスが見つからない場合は、DEM Orchestrator はプライマリ DEM Orchestrator として実行を開始します。
- 実行中の別の DEM Orchestrator が見つかった場合は、もう一方のプライマリ DEM Orchestrator を監視して停止を検出します。
- 停止を検出すると、プライマリ インスタンスとして引き継ぎます。

前のプライマリ インスタンスがもう一度オンラインに戻ると、別の DEM Orchestrator がそのロールをプライマリ として引き継ぎ、プライマリ Orchestrator インスタンスの失敗を監視します。

インフラストラクチャ コンポーネントの MSSQL データベース サーバ

vRealize Automation は、Microsoft SQL Server 2016 でのみ SQL AlwaysON グループをサポートしています。SQL Server 2016 をインストールする場合は、データベースを 100 モードで作成する必要があります。Microsoft SQL Server の古いバージョンを使用する場合は、共有ディスクを使用してフェイルオーバー クラスタ インスタンスを使用します。MSDTC を使用した SQL AlwaysOn グループの設定の詳細については、Microsoft の記事 <https://msdn.microsoft.com/ja-jp/library/ms366279.aspx> を参照してください。

vRealize Orchestrator

vRealize Orchestrator の内部の高可用性インスタンスは、vRealize Automation アプライアンスの一部として提供されます。

vRealize Business for Cloud 高可用性の考慮事項

vRealize Business for Cloud Edition のアプライアンスでは、VMware vSphere HA 機能を使用します。

VMware ESXi ホストで VMware vSphere HA 機能を構成するには、vCenter Server およびホスト管理のドキュメントを参照してください。

vRealize Automation のハードウェア仕様および最大容量

環境内の各 vRealize Automation サーバ プロファイルの構成および容量の要件に適したコンポーネントを配置します。

| サーバ ロール | コンポーネント | 必須のハードウェア仕様 | 推奨されるハードウェア仕様 |
|-------------------------------------|--|---|--|
| vRealize Automation アプライアンス | vRealize Automation サービス、vRealize Orchestrator、vRealize Automation アプライアンス データベース | CPU : 4 つの vCPU RAM : 18 GB (詳細については、 「vRealize Automation のスケーラビリティ」 を参照) ディスク : 140 GB ネットワーク : 1 GB/秒 | 必須ハードウェアの仕様と同じ |
| Infrastructure Core Server | Web サイト、Manager Service、DEM Orchestrator、DEM ワーカー、プロキシ エージェント | CPU : 4 つの vCPU RAM : 8 GB ディスク : 40 GB ネットワーク : 1 GB/秒 | 必須ハードウェアの仕様と同じ |
| インフラストラクチャ Web サーバ | Web サイト | CPU : 2 つの vCPU RAM : 8 GB ディスク : 40 GB ネットワーク : 1 GB/秒 | CPU : 2 つの vCPU RAM : 8 GB ディスク : 40 GB ネットワーク : 1 GB/秒 |
| インフラストラクチャ マネージャ サーバ | Manager Service、DEM Orchestrator | CPU : 2 つの vCPU RAM : 8 GB ディスク : 40 GB ネットワーク : 1 GB/秒 | CPU : 2 つの vCPU RAM : 8 GB ディスク : 40 GB ネットワーク : 1 GB/秒 |
| インフラストラクチャ Web/マネージャ サーバ | インフラストラクチャ Web/マネージャ サーバ | CPU : 2 つの vCPU RAM : 8 GB ディスク : 40 GB ネットワーク : 1 GB/秒 | CPU : 2 つの vCPU RAM : 8 GB ディスク : 40 GB ネットワーク : 1 GB/秒 |
| インフラストラクチャ DEM サーバ | (1 つ以上の) DEM ワーカー | CPU : 2 つの vCPU RAM : 8 GB ディスク : 40 GB ネットワーク : DEM ワーカーあたり 1 GB/秒 | CPU : 2 つの vCPU RAM : 8 GB ディスク : 40 GB ネットワーク : DEM ワーカーあたり 1 GB/秒 |
| インフラストラクチャ エージェント サーバ | (1 つ以上の) プロキシ エージェント | CPU : 2 つの vCPU RAM : 8 GB ディスク : 40 GB ネットワーク : 1 GB/秒 | CPU : 2 つの vCPU RAM : 8 GB ディスク : 40 GB ネットワーク : 1 GB/秒 |
| MSSQL データベース サーバ | インフラストラクチャ データベース | CPU : 2 つの vCPU RAM : 8 GB ディスク : 40 GB ネットワーク : 1 GB/秒 | CPU : 8 つの vCPU RAM : 16 GB ディスク : 80 GB ネットワーク : 1 GB/秒 |
| vRealize Business for Cloud アプライアンス | vRealize Business for Cloud アプライアンス サービス vRealize Business for Cloud データベース サーバ | CPU : 2 つの vCPU RAM : 4 GB ディスク : 50 GB ネットワーク : 1 GB/秒 | 必須ハードウェアの仕様と同じ |

vRealize Automation で推奨される最大容量

次のリソースの最大容量の値は、vRealize Automation の大規模展開プロファイルに適用されます。

表 1-2. vRealize Automation リソースの最大容量

| パラメータ | 最大値 |
|--------------------------------|--|
| テナント | 100 |
| vSphere エンドポイント | 20 |
| コンピュート リソース | 200 |
| 管理対象マシン | 75,000 |
| ピーク同時要求数 | |
| 定数 | 50 |
| バースト | 250 |
| 1 時間あたりのピーク要求数 | 400 |
| ビジネス グループ | 3000 (ビジネス グループごとの一意のユーザー数が 10 で、ユーザーが 50 を超えるビジネス グループのメンバーでない) |
| 予約 | 9,000 (ビジネス グループごとに 3 つの予約) |
| ブループリント | |
| CBP のみ | 6,000 |
| CBP + XaaS | 8,000 |
| カタログ アイテム | |
| 複数のテナント | 4,000 |
| 単一のテナント | 6,000 |
| デフォルトで 18 GB メモリの、ユーザー/グループの同期 | |
| ユーザー数 | 95,027 |
| グループ数 | 20,403 (各グループが 1 つのネスト レベルを含む 4 名のユーザーで構成される) |
| メモリを 30 GB に増加したユーザー/グループ | |
| ユーザー数 | 100,000 |
| グループ数 | 750 (各グループが 4,000 名のユーザーで構成され、各ユーザーが 30 のグループに属する) |

vRealize Automation 小規模展開の要件

vRealize Automation 小規模展開は、10,000 台以下の管理対象マシンで構成され、適切な仮想マシン、ロード バランサ、およびポート構成を含みます。小規模展開は、サポートされている方法で中規模または大規模展開に拡張できる vRealize Automation 展開の出発点としての役割を果たします。

vRealize Automation を展開するときには、エンタープライズ デプロイ プロセスを使用して個別のインフラストラクチャ Web サイトと Manager Service アドレスを提供します。

サポート

小規模展開では次の項目をサポートできます。

- 10,000 台の管理対象マシン
- 500 個のカタログ アイテム
- 10 個の同時マシン プロビジョニング

要件

小規模展開は、適切なコンポーネントを使用して構成する必要があります。

- vRealize Automation アプライアンス : vrava-1.ra.local
- Infrastructure Core Server : inf-1.ra.local
- MSSQL データベース サーバ : mssql.ra.local
- vRealize Business for Cloud アプライアンス : vrb.ra.local

DNS エントリ

| DNS エントリ | 参照先 |
|------------------|------------------|
| vrava.ra.local | vrava-1.ra.local |
| web.ra.local | inf.ra.local |
| manager.ra.local | inf.ra.local |

証明書

この表で使用されているホスト名は単なる例です。

| サーバ ロール | CN または SAN |
|---------------------------------|--|
| vRealize Automation アプライアンス | SAN は vra.va.sqa.local と vra.va-1.sqa.local で構成されます。 |
| Infrastructure Core Server | SAN は web.ra.local、managers.ra.local、および inf-1.ra.local で構成されます。 |
| vRealize Business for Cloud サーバ | CN = vrb.ra.local |

ポート

ユーザーは特定のポートにアクセスする必要があります。記載のポートはいずれもデフォルト ポートです。

| サーバ ロール | ポート |
|-----------------------------|---|
| vRealize Automation アプライアンス | 443, 8444. ポート 8444 は仮想マシン リモート コンソールで必要とされます。ポート 8283 は vRealize Orchestrator コントロール センターにアクセスするために必要です。 |

管理者は、ユーザーが必要とするポートに加えて、特定のポートにアクセスする必要があります。

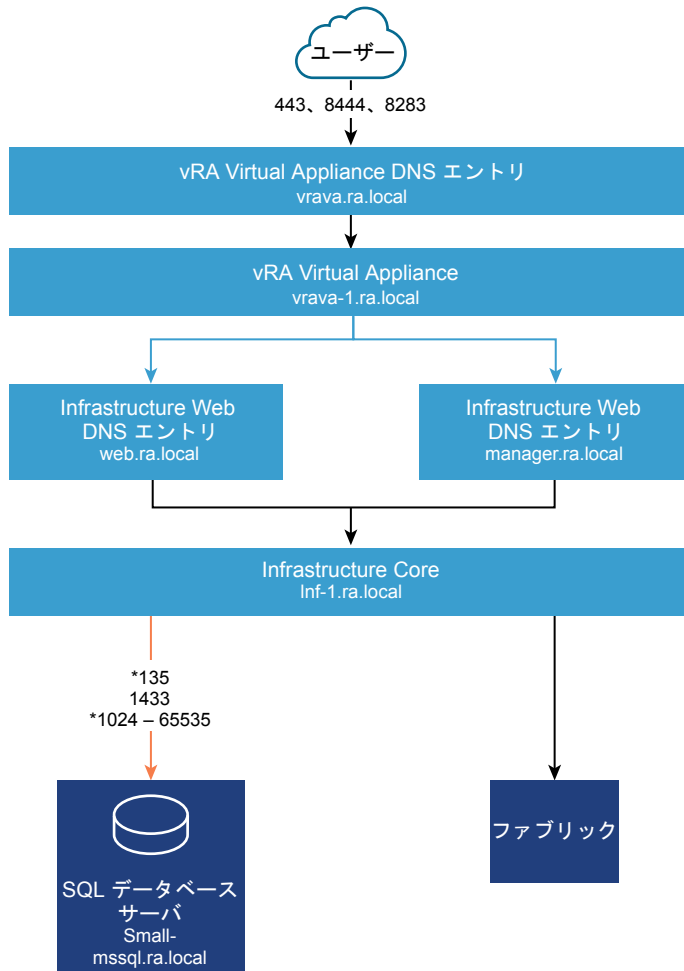
| サーバ ロール | ポート |
|-----------------------------|--|
| vRealize Automation アプライアンス | 5480, 8443. ポート 8443 は ID 管理の詳細構成のために使われます。 VMware Identity Manager から Active Directory : 389、636、3268、3269 VMware Identity Manager からドメイン コントローラ : 88、464、135 |
| vRealize Business for Cloud | 5480 |

| サーバ ロール | 受信用ポート | サービス/システム送信ポート |
|-----------------------------|--|---|
| vRealize Automation アプライアンス | HTTPS : 443 アダプタ構成 : 8443 リモート コンソール プロキシ : 8444 SSH : 22 仮想アプライアンス管理コンソール : 5480 | LDAP : 389 LDAPS : 636 VMware ESXi : 902。 Infrastructure Core は、 VMware Remote Console のチケットを取得するために vSphere エンドポイントの ポート 443 にアクセスする必 要があります。ユーザーへのト ラフィックにプロキシを設定す るため、 vRealize Automation アプラ イアンスは、ESXi ホストの ポート 902 にアクセスできる 必要があります。 Infrastructure Core Server : 443 Kerberos 認証 : 88 コンピュータ オブジェクトの パスワードの更新 : 464 |
| Infrastructure Core Server | HTTPS : 443 MSDTC : 135、 1024-65535。この範囲を絞 り込む方法については、 「vRealize Automation の展 開」 の「データベース展開」 を参照してください。 | vRealize Automation 仮想ア プライアンス : 443、5480 vSphere エンドポイント : 443。Infrastructure Core は、 VMware Remote Console のチケットを取得するために vSphere エンドポイントの ポート 443 にアクセスできる 必要があります。ユーザーへの トラフィックにプロキシを設定 するため、 vRealize Automation アプラ イアンスは、ESXi ホストの ポート 902 にアクセスできる 必要があります。 MSSQL : 135、1433、 1024-65535 MSDTC : 135、 1024-65535。この範囲を絞 り込む方法については、 「vRealize Automation の展 開」 の「データベース展開」 を参照してください。 |

| サーバ ロール | 受信用ポート | サービス/システム送信ポート |
|-------------------------------------|--|---|
| MSSQL データベース サーバ | MSSQL : 1433 MSDTC : 135、 1024-65535。この範囲を絞 り込む方法については、 「vRealize Automation の展 開」 の「データベース展開」 を参照してください。 | Infrastructure Core Server : 135、1024 ~ 65535 この範囲を絞り込む方 法については、 「vRealize Automation の展開」 の 「データベース展開」を参照し てください。 MSDTC : 135、 1024-65535。この範囲を絞 り込む方法については、 「vRealize Automation の展 開」 の「データベース展開」 を参照してください。 |
| vRealize Business for Cloud アプライアンス | HTTPS : 443 SSH : 22 仮想アプライアンス管理コン ソール : 5480 | vRealize Automation 仮想ア プライアンス : 443 Infrastructure Core : 443 |
| グローバル カタログ | | グローバル カタログ : 3268、 3269 |

最小占有量

図 1-1. vRealize Automation の小規模構成の最小占有量



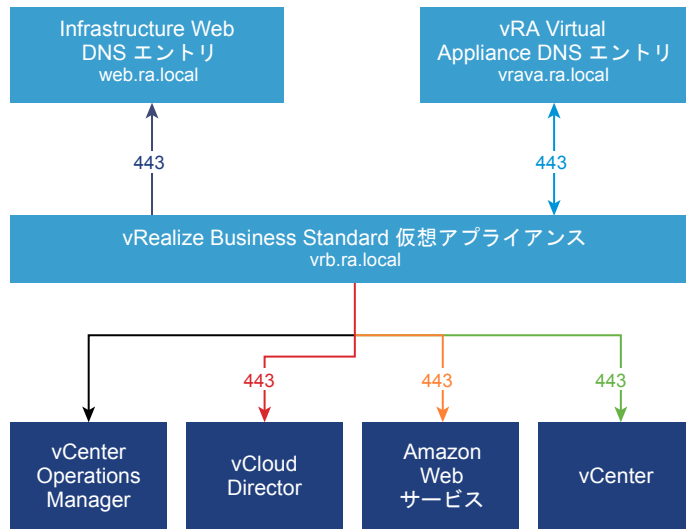
非表示 :
ログ収集 ([vRA 設定] > [クラスター] > [Virtual Appliance:5480 でログを収集]) を機能させるには、すべての Infrastructure システムがすべての vRealize Appliance のポート 5480 にアクセスできる必要があります。

仮想マシン Remote Console の場合は、vRealize Appliance が VMware ESXi のポート 902 に、Infrastructure Core Server が vSphere Endpoint のポート 443 にそれぞれアクセスできる必要があります。

*この範囲を狭める方法については、「データベース展開」セクションを参照してください。

さらに、双方向通信が必要です。

図 1-2. vRealize Business for Cloud の小規模構成の最小占有量



vRealize Automation を中規模に展開する場合の要件

vRealize Automation の中規模導入環境のシステム構成は、管理対象マシン数が最大 30,000 台で、必要に応じて仮想マシン、ロード バランサ、およびポート構成が含まれます。

サポート

中規模導入環境では次のアイテムをサポートできます。

- 管理対象マシン数 30,000 台
- カタログ アイテム数 1,000 個
- マシン プロビジョニング数 50 台

要件

中規模導入環境は、適切なシステム構成要件を満たしている必要があります。

仮想アプライアンス

- vRealize Automation アプライアンス 1 : vrava-1.ra.local
- vRealize Automation アプライアンス 2 : vrava-2.ra.local
- vRealize Automation アプライアンス 3 : vrava-3.ra.local
- vRealize Business for Cloud アプライアンス : vrb.ra.local

Windows Server 仮想マシン

- インフラストラクチャ Web/マネージャ サーバ 1 (アクティブ Web または DEM-O、アクティブ マネージャ) : inf-1.ra.local
- インフラストラクチャ Web/マネージャ サーバ 2 (アクティブ Web または DEM-O、パッシブ マネージャ) : inf-2.ra.local

- インフラストラクチャ DEM サーバ 1 : dem-1.ra.local
- インフラストラクチャ DEM サーバ 2 : dem-2.ra.local
- インフラストラクチャ エージェント サーバ 1 : agent-1.ra.local
- インフラストラクチャ エージェント サーバ 2 : agent-2.ra.local

データベース サーバ

- MSSQL フェイルオーバー クラスタ インスタンス : mssql.ra.local

ロード バランサ

- vRealize Automation アプライアンス ロード バランサ : med-vrava.ra.local
- インフラストラクチャ Web ロード バランサ : med-web.ra.local
- インフラストラクチャ マネージャ サービス ロード バランサ : med-manager.ra.local

証明書

この表で用いられているホスト名は例示用であり、現実のホストではありません。

| サーバ ロール | CN または SAN |
|-------------------------------------|---|
| vRealize Automation アプライアンス | SAN は以下のホスト名を含みます。 <ul style="list-style-type: none"> ■ vrava.ra.local ■ vrava-1.ra.local ■ vrava-2.ra.local |
| インフラストラクチャ Web/マネージャ サーバ | SAN は以下のホスト名を含みます。 <ul style="list-style-type: none"> ■ web.ra.local ■ manager.ra.local ■ inf-1.ra.local ■ inf-2.ra.local |
| vRealize Business for Cloud アプライアンス | CN = vrb.ra.local |

ポート

ユーザーは特定のポートにアクセスする必要があります。記載のポートはいずれもデフォルト ポートです。

| サーバ ロール | ポート |
|--------------------------------------|--|
| vRealize Automation アプライアンス ロード バランサ | 443, 8444. ポート 8444 は仮想マシン リモート コンソールで必要とされます。 |

管理者は、ユーザーが必要とするポートに加えて、特定のポートにアクセスする必要があります。

| サーバ ロール | ポート |
|---|--|
| vRealize Automation アプライアンス fVAMI | 5480, 8443. ポート 8443 は ID 管理の詳細構成のために使われます。 VMware Identity Manager から Active Directory : 389、636、3268、3269 VMware Identity Manager からドメイン コントローラ : 88、464、135 |
| vRealize Appliance Orchestrator コントロール センター | 8283 |
| vRealize Business for Cloud サーバ | 5480 |

次の表にアプリケーション間通信を示します。

| サーバ ロール | 受信用ポート | サービスまたはシステムの送信用ポート |
|-----------------------------|--|---|
| vRealize Automation アプライアンス | HTTPS: アダプタ構成 : 8443 リモート コンソール プロキシ : 8444 Postgres : 5432 RabbitMQ : 4369、25672、5671、5672 ElasticSearch : 9300、40002、40003 Stomp : 61613 SSH : 22 | LDAP : 389 LDAPS : 636 vRealize Automation アプライアンス (その他すべて) : 5432、4369、25672、5671、5672、9300、40002、40003 vRealize Automation インフラストラクチャ Web ロード バランサ : 443 VMware ESXi : 902。インフラストラクチャ Web/マネージャは、仮想マシン リモート コンソールのチケットを取得するために、vSphere エンドポイントのポート 443 にアクセスする必要があります。vRealize Automation アプライアンス は、コンソール データをユーザーに送るために、ESXi ホストのポート 902 にアクセスする必要があります。 Kerberos 認証 : 88 コンピュータ オブジェクトのパスワードの更新 : 464 |
| インフラストラクチャ Web/マネージャ サーバ | HTTPS : 443 MSDTC : 135、1024-65535。この範囲を絞り込む方法については、 「vRealize Automation の展開」 の「データベース展開」を参照してください。 | vRealize Automation アプライアンス ロード バランサ : 443 vRealize Automation インフラストラクチャ Web ロード バランサ : 443 vRealize Automation アプライアンス (仮想アプライアンス) : 5480。 vSphere エンドポイント : 443。インフラストラクチャ Web/マネージャは、仮想マシン リモート コンソールのチケットを取得するために、vSphere エンドポイントのポート 443 にアクセスする必要があります。vRealize Automation アプライアンス は、コンソール データをユーザーに送るために、ESXi ホストのポート 902 にアクセスする必要があります。 MSSQL : 135、1433、1024-65535。この範囲を絞り込む方法については、 「vRealize Automation の展開」 の「データベース展開」を参照してください。 |

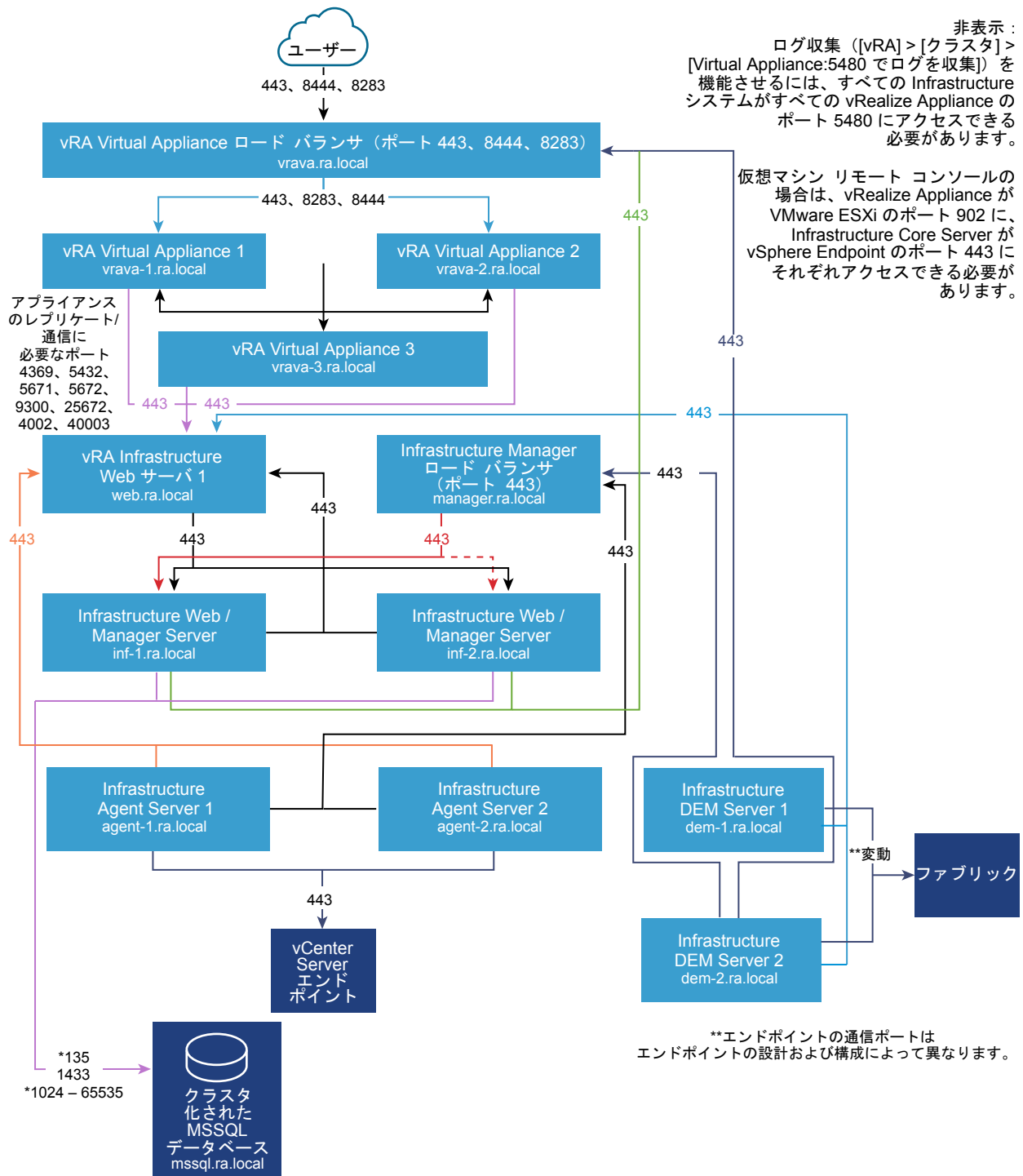
| サーバ ロール | 受信用ポート | サービスまたはシステムの送信用ポート |
|---------------------------------|--|--|
| インフラストラクチャ DEM サーバ | なし | vRealize Automation アプライアンス ロード バランサ : 443 vRealize Automation インフラストラクチャ Web ロード バランサ : 443 vRealize Automation インフラストラクチャ マネージャ ロード バランサ : 443 vRealize Automation アプライアンス (仮想 アプライアンス) : 5480。 |
| インフラストラクチャ エージェント サーバ | なし | vRealize Automation インフラストラクチャ Web ロード バランサ : 443 vRealize Automation インフラストラクチャ マネージャ ロード バランサ : 443 vRealize Automation アプライアンス (仮想 アプライアンス) : 5480。 |
| MSSQL データベース サーバ | MSSQL : 1433 MSDTC : 135、 1024-65535。この範囲を 絞り込む方法については、 「vRealize Automation の 展開」 の「データベース展 開」を参照してください。 | インフラストラクチャ Web/マネージャ サー バ : 135、1024-65535。この範囲を絞り込む 方法については、 「vRealize Automation の 展開」 の「データベース展開」を参照してく ださい。 |
| vRealize Business for Cloud サーバ | HTTPS : 443 SSH : 22 仮想アプライアンス管理コ ンソール : 5480 | vRealize Automation アプライアンス ロー ド バランサ : 443 vRealize Automation インフラストラクチャ Web ロード バランサ : 443 |
| グローバル カタログ | | グローバル カタログ : 3268、3269 |

ロード バランサによるアクセスには以下のポートが必要です。

| ロード バランサ | バランシング済みポート |
|--|-------------|
| vRealize Automation アプライアンス ロード バランサ | 443, 8444 |
| vRealize Automation インフラストラクチャ Web ロード バランサ | 443 |
| vRealize Automation インフラストラクチャ マネージャ サービス ロー ド バランサ | 443 |

グラフィック

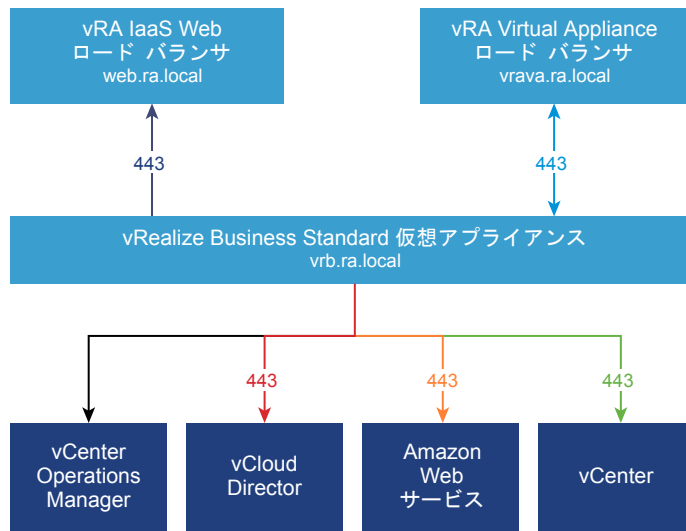
図 1-3. vRealize Automation の中規模構成の最小占有量



*この範囲を狭める方法については、「データベース展開」セクションを参照してください。

さらに、双方向通信が必要です。

図 1-4. vRealize Business for Cloud の中規模構成の最小占有量



vRealize Automation を大規模に展開する場合の要件

vRealize Automation の大規模導入環境のシステム構成は、管理対象マシン数が最大 50,000 台で、必要に応じて仮想マシン、ロード バランサ、およびポート構成が含まれます。

サポート

大規模導入環境では次のアイテムをサポートできます。

- 管理対象マシン数 50,000 台
- カタログ アイテム数 2,500 個
- 同時マシン プロビジョニング数 100 台

要件

大規模導入環境は、適切なシステム構成要件を満たしている必要があります。

仮想アプライアンス

- vRealize Automation アプライアンス 1 : vrava-1.ra.local
- vRealize Automation アプライアンス 2 : vrava-2.ra.local
- vRealize Automation アプライアンス 2 : vrava-3.ra.local
- vRealize Automation アプライアンスのアプライアンス : vrb.ra.local

Windows Server 仮想マシン

- インフラストラクチャ Web サーバ 1 : web-1.ra.local
- インフラストラクチャ Web サーバ 2 : web-2.ra.local
- インフラストラクチャ マネージャ サーバ 1 : manager-1.ra.local

- インフラストラクチャ マネージャ サーバ 2 : manager-2.ra.local
- インフラストラクチャ DEM サーバ 1 : dem-1.ra.local
- インフラストラクチャ DEM サーバ 2 : dem-2.ra.local
- インフラストラクチャ エージェント サーバ 1 : agent-1.ra.local
- インフラストラクチャ エージェント サーバ 2 : agent-2.ra.local
- クラスタ化された MSSQL データベース : mssql.ra.local

ロード バランサ

- vRealize Automation アプライアンス ロード バランサ : vrava.ra.local
- インフラストラクチャ Web ロード バランサ : web.ra.local
- インフラストラクチャ マネージャ サービス ロード バランサ : manager.ra.local

証明書

この表で使用されているホスト名は単なる例です。

| サーバ ロール | CN または SAN |
|-------------------------------------|---|
| vRealize Automation アプライアンス | SAN は以下のホスト名を含みます。 <ul style="list-style-type: none"> ■ vrava.ra.local ■ vrava-1.ra.local ■ vrava-2.ra.local |
| インフラストラクチャ Web サーバ | SAN は以下のホスト名を含みます。 <ul style="list-style-type: none"> ■ web.ra.local ■ web-1.ra.local ■ web-2.ra.local |
| インフラストラクチャ マネージャ サーバ | SAN は以下のホスト名を含みます。 <ul style="list-style-type: none"> ■ manager.ra.local ■ manager-1.ra.local ■ manager-2.ra.local |
| vRealize Business for Cloud アプライアンス | CN = vrb.ra.local |

ポート

ユーザーは特定のポートにアクセスする必要があります。記載のポートはいずれもデフォルト ポートです。

| サーバ ロール | ポート |
|--------------------------------------|--|
| vRealize Automation アプライアンス ロード バランサ | 443、8444。VMware Remote Console にはポート 8444 が必要です。 |

管理者は、ユーザーが必要とするポートに加えて、特定のポートにアクセスする必要があります。

| サーバ ロール | ポート |
|---------------------------------|--|
| vRealize Automation アプライアンス | 5480, 8443. ポート 8443 は ID 管理の詳細構成のために使われます。 VMware Identity Manager から Active Directory : 389、636、3268、3269 VMware Identity Manager からドメイン コントローラ : 88、464、135 |
| vRealize Business for Cloud サーバ | 5480 |

システムが適切なアプリケーション間の通信をサポートしている必要があります。

| サーバ ロール | 受信用ポート | サービスまたはシステムの送信用ポート |
|-----------------------------|---|--|
| vRealize Automation | | |
| vRealize Automation アプライアンス | HTTPS : 443 アダプタ構成 : 8443 リモート コンソール プロキシ : 8444 Postgres : 5432 RabbitMQ : 4369、25672、5671、5672 ElasticSearch : 9300、40002、40003 Stomp : 61613 SSH : 22 コントロール センター : 8283 | LDAP : 389 LDAPS : 636 vRealize Automation アプライアンス : 5432、4369、25672、5671、5672、9300、40002、40003。 vRealize Automation インフラストラクチャ Web ロード バランサ : 443 VMware ESXi : 902。インフラストラクチャ Web は、VMware Remote Console のチケットを取得するために vSphere エンドポイントのポート 443 にアクセスする必要があります。vRealize Automation アプライアンスは、コンソール データをユーザーに送るために、ESXi ホストのポート 902 にアクセスする必要があります。 Kerberos 認証 : 88 コンピュータ オブジェクトのパスワードの更新 : 464 |
| インフラストラクチャ Web サーバ | HTTPS : 443 MSDTC : 443、1024-65535。この範囲を絞り込む方法については、 [vRealize Automation の展開] のデータベース展開に関する説明を参照してください。 | vRealize Automation アプライアンス ロード バランサ : 443 vRealize Automation アプライアンスの仮想アプライアンス : 5480。 vSphere エンドポイント : 443。インフラストラクチャ Web は、VMware Remote Console のチケットを取得するために vSphere エンドポイントのポート 443 にアクセスする必要があります。vRealize Automation アプライアンスは、コンソール データをユーザーに送るために、ESXi ホストのポート 902 にアクセスする必要があります。 MSSQL : 135、1433、1024-65535。この範囲を絞り込む方法については、 [vRealize Automation の展開] のデータベース展開に関する説明を参照してください。 |

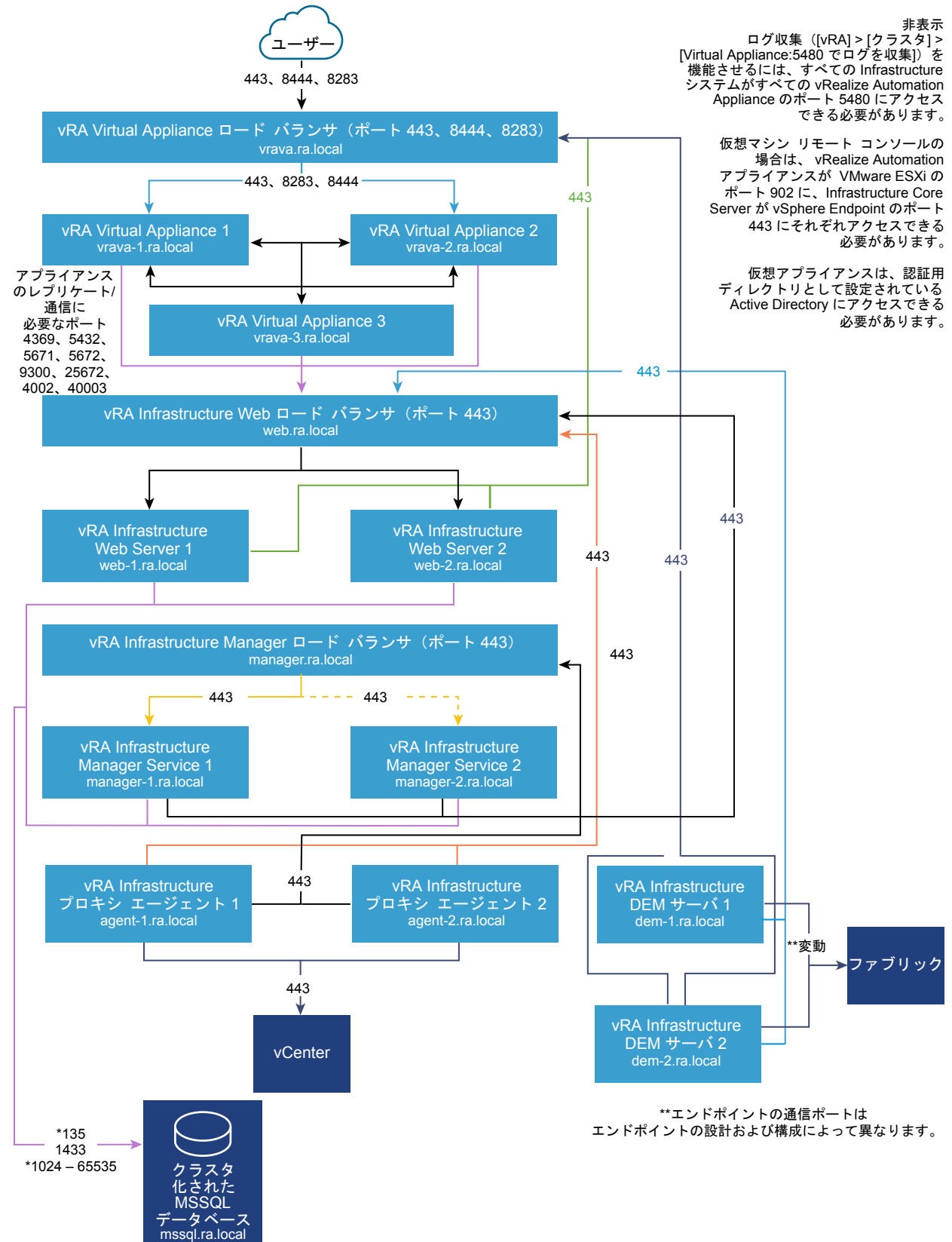
| サーバ ロール | 受信用ポート | サービスまたはシステムの送信用ポート |
|---------------------------------|--|---|
| インフラストラクチャ マネージャ サーバ | HTTPS : 443 MSDTC : 135、1024-65535。この範囲を絞り込む方法については、 [vRealize Automation の展開] のデータベース展開に関する説明を参照してください。 | vRealize Automation アプライアンス ロード バランサ : 443 vRealize Automation インフラストラクチャ Web ロード バランサ : 443 vRealize Automation アプライアンス : 443、5480 MSSQL : 135、1433、1024-65535。この範囲を絞り込む方法については、 [vRealize Automation の展開] のデータベース展開に関する説明を参照してください。 |
| インフラストラクチャ DEM サーバ | なし | vRealize Automation アプライアンス ロード バランサ : 443 vRealize Automation インフラストラクチャ Web ロード バランサ : 443 vRealize Automation インフラストラクチャ マネージャ ロード バランサ : 443 vRealize Orchestrator ロード バランサ : 8281 vRealize Automation アプライアンス : 5480。 |
| インフラストラクチャ エージェント サーバ | なし | vRealize Automation インフラストラクチャ Web ロード バランサ : 443 vRealize Automation インフラストラクチャ マネージャ ロード バランサ : 443 vRealize Automation アプライアンス : 5480。 |
| MSSQL データベース サーバ | MSSQL : 1433 MSDTC : 135、1024-65535。この範囲を絞り込む方法については、 [vRealize Automation の展開] のデータベース展開に関する説明を参照してください。 | インフラストラクチャ Web サーバ : 135、1024-65535。この範囲を絞り込む方法については、 [vRealize Automation の展開] のデータベース展開に関する説明を参照してください。 インフラストラクチャ マネージャ サーバ : 135、1024-65535。この範囲を絞り込む方法については、 [vRealize Automation の展開] のデータベース展開に関する説明を参照してください。 |
| vRealize Business for Cloud サーバ | HTTPS : 443 SSH : 22 仮想アプライアンス管理コンソール : 5480 | vRealize Automation アプライアンス ロード バランサ : 443 vRealize Automation インフラストラクチャ Web ロード バランサ : 443 |
| グローバル カタログ | | グローバル カタログ : 3268、3269 |

ロード バランサによるアクセスには以下のポートが必要です。

| ロード バランサ | バランシング済みポート |
|---|-------------|
| vRealize Automation アプライアンス ロード バランサ | 443, 8444 |
| vRealize Automation インフラストラクチャ Web ロード バランサ | 443 |
| vRealize Automation マネージャ サーバ ロード バランサ | 443 |

グラフィック

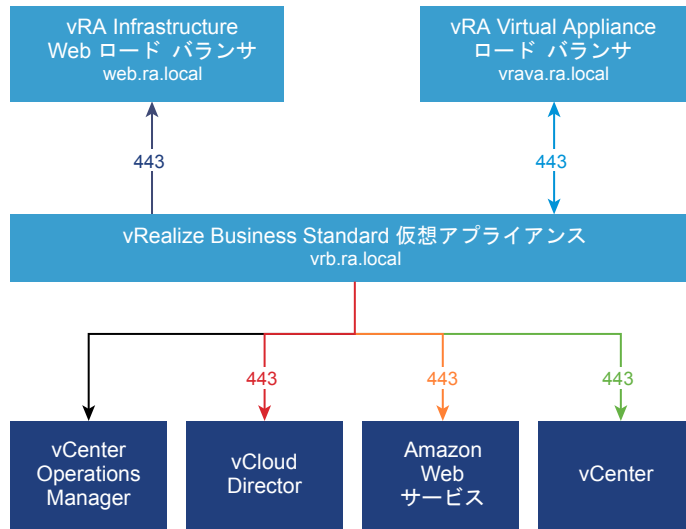
図 1-5. vRealize Automation の大規模構成の最小占有量



*この範囲を狭める方法については、「データベース展開」セクションを参照してください。

VCenter と vRA の双方向通信が必要です。

図 1-6. vRealize Business for Cloud の大規模構成の最小占有量



vRealize Automation の複数のデータセンター データの展開

vRealize Automation では、リモート データセンターのリソースの管理をサポートします。

リモート データセンターで vSphere、HyperV、または Xen のリソースを管理するには、リモート データセンターの仮想マシンにプロキシ エージェントを展開します。

注: 次の図は、vSphere の展開を示しています。その他のエンドポイントでは、追加の構成は必要ありません。

vRealize Orchestrator ワークフローでは WAN 経由で通信する可能性があるため、『vRealize Orchestrator コーディング設計ガイド』に記載されているベスト プラクティスを確認してください。

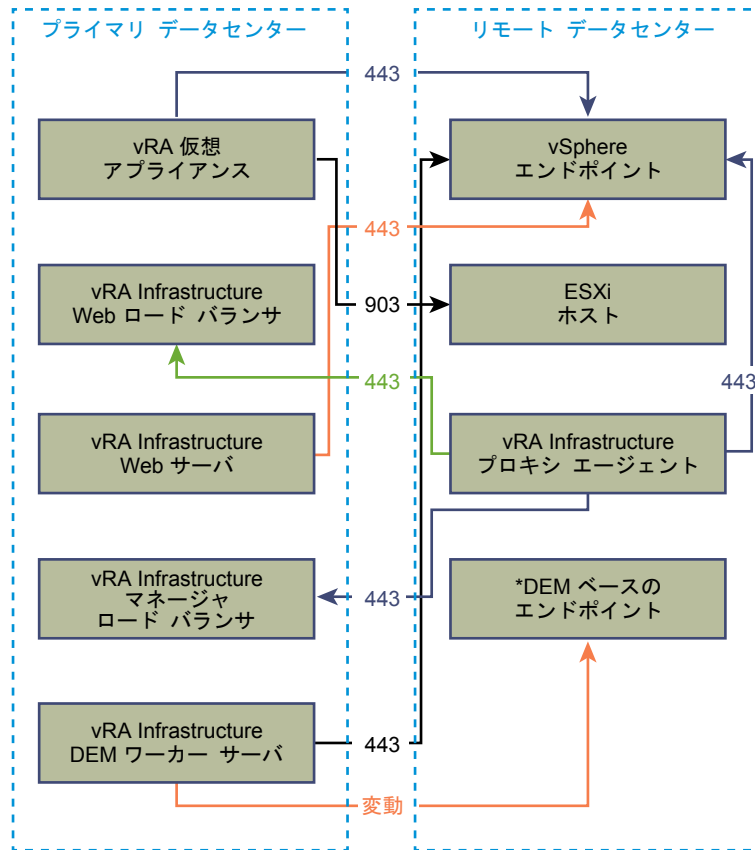
表 1-3. WAN 通信に必要なポート

| ロール | 受信用ポート | サービス/システム送信ポート |
|--|--|---|
| vRealize Automation アプライアンス - 組み込まれた vRealize Orchestrator を含む | 該当なし | vSphere エンドポイント : 443 ESXi ホスト : 903 |
| vRealize Automation インフラストラクチャ ロード バランサ | vRealize Automation インフラストラクチャ プロキシ エージェント : 443 | 該当なし |
| vRealize Automation インフラストラクチャ Web サーバ | 該当なし | vSphere エンドポイント : 443 |
| vRealize Automation インフラストラクチャ マネージャ ロード バランサ | vRealize Automation インフラストラクチャ プロキシ エージェント : 443 | 該当なし |
| vRealize Automation インフラストラクチャ DEM ワーカー サーバ | 該当なし | エンドポイント : **変動 |

* DEM ワーカーが Manager Service マシンまたは別のサーバにインストールされている場合、そのマシンとターゲット エンドポイントの間でこれらのポートを開く必要があります。

** 外部エンドポイントとの通信に必要なポートはエンドポイントによって異なります。vSphere の場合、デフォルトでは、ポート 443 です。

図 1-7. vRealize Automation の複数のサイトの構成



vRealize Automation の安全な構成

安全な構成では、VMware ガイドラインに従って vRealize Automation デプロイのセキュリティ プロファイルを確認、構成、および更新する方法について説明します。

安全な構成では、次のトピックについて説明します。

- ソフトウェア インフラストラクチャのセキュリティ
- デプロイされた構成のセキュリティ
- ホスト ネットワークのセキュリティ

vRealize Automation のセキュアなベースラインの概要

VMware は、vRealize Automation システムのセキュアなベースラインを検証および構成できる包括的な推奨事項を提供します。

VMware が指定した適切なツールおよび手順を使用して、vRealize Automation システムを検証し、セキュリティ強化されたセキュアなベースライン構成を維持します。一部の vRealize Automation コンポーネントのセキュリティはすべて強化された状態または一部強化された状態でインストールされますが、VMware のセキュリティ推奨事項、自社のセキュリティ ポリシー、および既知の脅威を考慮して、各コンポーネントの構成を確認および検証する必要があります。

vRealize Automation のセキュリティ状態

vRealize Automation のセキュリティ状態は、システムとネットワークの構成、組織のセキュリティ ポリシー、およびセキュリティのベスト プラクティスに基づいた包括的にセキュアな環境を想定しています。

vRealize Automation システムのセキュリティ強化を検証および構成する場合、VMware のセキュリティ強化に関する推奨事項に記載されている次の領域について考慮します。

- 安全な展開
- セキュアな構成
- ネットワーク セキュリティ

使用するシステムがセキュリティ強化されていることを確認するには、VMware の推奨事項と各地域のセキュリティ ポリシーがそれぞれの概念的な領域に関連していることについて考慮します。

システム コンポーネント

vRealize Automation システムのセキュリティ強化と安全な構成を考慮する場合、すべてのコンポーネントと、システムの機能をサポートするその仕組みを理解します。

安全なシステムを計画および実装する場合、次のコンポーネントを考慮します。

- vRealize Automation アプライアンス
- IaaS コンポーネント

vRealize Automation とコンポーネントの動作を理解するには、VMware vRealize Automation ドキュメント センターで『[基盤と概念](#)』を参照してください。vRealize Automation の標準展開とアーキテクチャの詳細については、『[vRealize Automation リファレンス アーキテクチャ](#)』を参照してください。

インストール メディアの整合性の確認

ユーザーは、VMware 製品をインストールする前にインストール メディアの整合性を常に確認する必要があります。

ダウンロードしたファイルの整合性と信頼性を確認するために、ISO、オフライン バンドル、またはパッチをダウンロードしたら、必ず SHA1 ハッシュを確認します。VMware から入手した物理メディアのセキュリティ シールが破損している場合は、そのソフトウェアを VMware に返却して交換してください。

メディアをダウンロードしたら、MD5/SHA1 サムの値を使用して、ダウンロードの整合性を確認します。MD5/SHA1 のハッシュ出力と VMware Web サイトに表示されている値を比較します。SHA1 または MD5 ハッシュと一致する必要があります。

インストール メディアの整合性確認の詳細については、<http://kb.vmware.com/kb/1537> を参照してください。

VMware システム ソフトウェア インフラストラクチャのセキュリティ強化

セキュリティ強化プロセスの一環として、VMware システムをサポートしているデプロイ済みソフトウェア インフラストラクチャを評価し、VMware セキュリティ強化ガイドラインを満たしていることを確認します。

VMware システムのセキュリティを強化する前に、サポートするソフトウェア インフラストラクチャ内のセキュリティ上の欠陥を確認して対応し、完全にセキュリティ強化されたセキュアな環境を作成します。考慮すべきソフトウェア インフラストラクチャの要素には、オペレーティング システム コンポーネント、サポートするソフトウェア、およびデータベース ソフトウェアが含まれます。これらの要素や、その他のコンポーネントにおけるセキュリティ上の懸念には、メーカーの推奨およびその他の関連するセキュリティ プロトコルに従って対応します。

VMware vSphere[®] 環境のセキュリティ強化

VMware vSphere[®] 環境を評価し、適切なレベルの vSphere セキュリティ強化ガイダンスが守られ、保守されていることを確認します。

セキュリティ強化に関するガイダンスの詳細については、

<http://www.vmware.com/security/hardening-guides.html> (英語) を参照してください。

包括的にセキュリティ強化された環境の一部として、VMware vSphere[®] インフラストラクチャが VMware によって定められたセキュリティ ガイドラインを満たしている必要があります。

Infrastructure as a Service (IaaS) ホストのセキュリティ強化

IaaS Microsoft Windows ホスト マシンが VMware ガイドラインに従ってセキュリティ強化されていることを確認します。

該当する Microsoft Windows セキュリティ強化およびセキュリティのベスト プラクティスのガイドラインで推奨事項を確認し、Windows Server ホストが確実に適切にセキュリティ強化されるようにします。セキュリティ強化の推奨事項に従わない場合、Windows リリース上の安全でないコンポーネントから既知のセキュリティ脆弱性が狙われる可能性があります。

お使いのバージョンがサポートされていることを確認するには、[vRealize Automation のサポートマトリックス](#) (英語) を参照してください。

Microsoft 製品のセキュリティ強化プラクティスに関する適切なガイダンスについては、Microsoft のベンダーにお問い合わせください。

Microsoft SQL Server のセキュリティ強化

Microsoft SQL Server データベースが Microsoft および VMware によって定められたセキュリティ ガイドラインを満たしていることを確認します。

該当する Microsoft SQL Server セキュリティ強化およびセキュリティのベスト プラクティスのガイドラインで推奨事項を確認します。Microsoft SQL Server のインストールされたバージョンに関するすべての Microsoft セキュリティ通知を確認します。セキュリティ強化の推奨事項に従わない場合、Microsoft SQL Server バージョン上の安全でないコンポーネントから既知のセキュリティ脆弱性が狙われる可能性があります。

お使いのバージョンの Microsoft SQL Server がサポートされていることを確認するには、[vRealize Automation のサポート マトリックス](#)（英語）を参照してください。

Microsoft 製品のセキュリティ強化プラクティスに関するガイダンスについては、Microsoft のベンダーにお問い合わせください。

Microsoft .NET のセキュリティ強化

包括的にセキュリティ強化された環境の一部として、Microsoft .NET が Microsoft および VMware によって定められたセキュリティ ガイドラインを満たしている必要があります。

該当する Microsoft .NET セキュリティ強化およびセキュリティのベスト プラクティスのガイドラインで規定された推奨事項を確認します。また、使用している Microsoft SQL Server のバージョンに関するすべての Microsoft セキュリティ通知を確認します。セキュリティ強化の推奨事項に従わない場合、安全でない Microsoft.NET コンポーネントから既知のセキュリティの脆弱性が狙われる可能性があります。

お使いのバージョンの Microsoft.NET がサポートされていることを確認するには、[vRealize Automation のサポート マトリックス](#)（英語）を参照してください。

Microsoft 製品のセキュリティ強化プラクティスに関するガイダンスについては、Microsoft のベンダーにお問い合わせください。

Microsoft Internet Information Services (IIS) のセキュリティ強化

Microsoft Internet Information Services (IIS) が Microsoft および VMware のセキュリティ ガイドラインをすべて満たしていることを確認します。

該当する Microsoft IIS セキュリティ強化およびセキュリティのベスト プラクティスのガイドラインで規定された推奨事項を確認します。また、使用している IIS のバージョンに関するすべての Microsoft セキュリティ通知を確認します。セキュリティ強化の推奨事項に従わない場合、既知のセキュリティの脆弱性が狙われる可能性があります。

お使いのバージョンがサポートされていることを確認するには、[vRealize Automation のサポート マトリックス](#)（英語）を参照してください。

Microsoft 製品のセキュリティ強化プラクティスに関するガイダンスについては、Microsoft のベンダーにお問い合わせください。

インストールされたソフトウェアの確認

サード パーティ製や使用されていないソフトウェアの脆弱性は未認証のシステム アクセスや可用性の中断のリスクを高めるため、VMware ホスト マシンにインストールされているすべてのソフトウェアを確認し、その使用状況を評価することが重要です。

VMware ホスト マシンには、システムの安全な運用のために必要なソフトウェア以外をインストールしないでください。使用されていない、または関係ないソフトウェアはアンインストールします。

サポート対象外のソフトウェアがインストールされているインベントリ

インストール済み製品の VMware デプロイとインベントリを評価し、関係のないサポート対象外のソフトウェアがインストールされていないことを確認します。

サードパーティ製品に対するサポート ポリシーの詳細については、VMware サポート記事 (<https://www.vmware.com/support/policies/thirdparty.html>) (英語) を参照してください。

サードパーティ製ソフトウェアの確認

VMware は、テストおよび検証が行われていないサードパーティ製ソフトウェアのインストールをサポートせず、推奨しません。VMware ホスト マシンに、セキュアでない、パッチが適用されていない、または認証されていないサードパーティ製ソフトウェアがインストールされている場合、システムが不正アクセスや可用性の中断のリスクにさらされる可能性があります。サポートされていないサードパーティ製ソフトウェアを使用する必要がある場合は、セキュアな構成およびパッチ適用の要件についてサードパーティ ベンダーにお問い合わせください。

VMware セキュリティ アドバイザリおよびパッチ

システムで最高レベルのセキュリティを維持するために、VMware セキュリティ アドバイザリに従って、関連するすべてのパッチを適用します。

VMware は製品のセキュリティ アドバイザリを公開しています。製品を既知の脅威から保護するには、このアドバイザリを注視します。

vRealize Automation のインストール、パッチ、アップグレード履歴を評価し、公開された VMware セキュリティ アドバイザリが順守および適用されていることを確認します。

現在の VMware セキュリティ アドバイザリの詳細については、<http://www.vmware.com/jp/security/advisories.html> を参照してください。

セキュアな構成

システム構成に応じて、vRealize Automation 仮想アプライアンスと Infrastructure as a Service (IaaS) コンポーネントのセキュリティ設定を確認および更新します。また、他のコンポーネントとアプリケーションの構成を確認および更新します。

vRealize Automation インストールをセキュアに構成するには、コンポーネントが連携するように、各コンポーネントの構成に個別に対応します。十分に安全なベースラインを実現できるようにすべてのシステム コンポーネントの構成を検討します。

vRealize Automation アプライアンスのセキュリティ強化

システム構成の必要に応じて、vRealize Automation アプライアンスのセキュリティ設定を確認して更新します。

仮想アプライアンスと、そのホスト オペレーティング システムのセキュリティ設定を構成します。また、その他の関連コンポーネントとアプリケーションの構成も設定または確認します。適切な構成を実現するために、既存の設定の確認が必要な場合や、設定の変更や追加が必要な場合があります。

root パスワードの変更

該当するセキュリティ要件を満たすために、vRealize Automation アプライアンスの root パスワードを変更することができます。

仮想アプライアンス管理インターフェイスを使用して、vRealize Automation アプライアンスで root パスワードを変更します。root パスワードの複雑さが、組織のパスワード要件を満たしていることを確認します。

手順

- 1 vRealize Automation アプライアンスの仮想アプライアンス管理インターフェイスを開きます。
`https://<vRealizeAppliance-url>:5480`
- 2 仮想アプライアンス管理インターフェイスの [管理] タブを選択します。
- 3 [管理] サブメニューを選択します。
- 4 [現在の管理者パスワード] テキスト ボックスに、現在のパスワードを入力します。
- 5 [新しい管理者パスワード] テキスト ボックスに新しいパスワードを入力します。
- 6 [新しい管理者パスワードを再入力] テキスト ボックスに新しいパスワードを入力します。
- 7 [設定の保存] をクリックして、変更を保存します。

root パスワードのハッシュと複雑性の確認

root パスワードの複雑さが、組織のパスワード要件を満たしていることを確認します。

root ユーザーがユーザー アカウントに適用される pam_cracklib モジュール パスワードの複雑性チェックをバイパスするため、root パスワードの複雑性を検証する必要があります。

アカウント パスワードの先頭には **\$6\$** を指定する必要があります。これは sha512 ハッシュを表します。これは、セキュリティ強化されたすべてのアプライアンスの標準ハッシュです。

手順

- 1 root パスワードのハッシュを確認するには、root としてログインして **# more /etc/shadow** コマンドを実行します。

ハッシュ情報が表示されます。

図 1-8. パスワードのハッシュ結果

```
vcac148-084-111:~ $ more /etc/shadow
bin:*:16332:0:60:7:::
daemon:*:16332:0:60:7:::
haldaemon:*:16332:0:60:7:::
mail:*:15870::60:::
man:*:16332:0:60:7:::
messagebus:*:16332:0:60:7:::
nobody:*:15870::60:::
ntp:*:16332:0:60:7:::
polkituser:*:16332:0:60:7:::
postfix:*:16332:0:60:7:::
root:$6$PHxGPY5A$ba8KzK4SS44UEHPfAtgs
P/:16346:0:365:7:::
```

2 root パスワードに sha512 ハッシュが含まれていない場合は、**passwd** コマンドを実行して変更します。

セキュリティ強化されたすべてのアプライアンスでは、**/etc/pam.d/common-password** ファイル内の **pw_history** モジュールの **enforce_for_root** が有効になります。システムは、デフォルトで前回のパスワードを 5 つまで記憶します。古いパスワードは、**/etc/securetty/passwd** ファイルでユーザーごとに保存されます。

root パスワード履歴の確認

root アカウントにパスワード履歴が適用されていることを確認します。

セキュリティ強化されたすべてのアプライアンスでは、**/etc/pam.d/common-password** ファイル内の **pw_history** モジュールの **enforce_for_root** が有効になります。システムは、デフォルトで前回のパスワードを 5 つまで記憶します。古いパスワードは、**/etc/securetty/passwd** ファイルでユーザーごとに保存されます。

手順

1 次のコマンドを実行します。

```
cat /etc/pam.d/common-password-vmware.local | grep pam_pwhistory.so
```

2 返される結果に **enforce_for_root** が表示されていることを確認します。

```
password required pam_pwhistory.so enforce_for_root remember=5 retry=3
```

パスワード有効期限の管理

すべてのアカウントのパスワード有効期限を、組織のセキュリティ ポリシーと一致するように構成します。

デフォルトでは、セキュリティ強化されたすべての VMware 仮想アプライアンス アカウントで 60 日のパスワード有効期限を使用します。大半のセキュリティ強化アプライアンスでは、root アカウントは 365 日のパスワード有効期限に設定されています。ベスト プラクティスとして、すべてのアカウントの有効期限がセキュリティと運用の要件基準を満たしていることを確認します。

root パスワードの有効期限が切れている場合、回復することはできません。管理および root のパスワードの有効期限が切れないようにサイト固有のポリシーを実装する必要があります。

手順

1 仮想アプライアンス マシンに root としてログインし、次のコマンドを実行してすべてのアカウントのパスワード有効期限を確認します。

```
# cat /etc/shadow
```

パスワード有効期限は、シャドウ ファイルの 5 番目のフィールドです（フィールドは、コロンで区切られています）。root の有効期限は日単位で設定されます。

図 1-9. パスワード有効期限フィールド

```
vcac148-084-111:~ # more /etc/shadow
bin:!:16332:0:60:7:::
daemon:!:16332:0:60:7:::
haldaemon:!:16332:0:60:7:::
mail:!:15870::60:::
man:!:16332:0:60:7:::
messagebus:!:16332:0:60:7:::
nobody:!:15870::60:::
ntp:!:16332:0:60:7:::
polkituser:!:16332:0:60:7:::
postfix:!:16332:0:60:7:::
root:$6$PHxGPy5A$ba8KzK4SS44UEHPfAtgsB6iy1nJYbBk
zRbYR1mvJiX.pJpub0AEpP/:16346:0:365:7:::
sshd:!:16332:0:60:7:::
```

- 2 root アカウントの有効期限を変更するには、次の形式のコマンドを実行します。

```
# passwd -x 365 root
```

このコマンドで、365 はパスワード有効期限までの日数を指定します。組織の有効期限基準を満たすために任意のユーザーを変更するには、このコマンドの「root」を対象のアカウントに置き換え、日数を置き換えて実行します。

セキュア シェルと管理者アカウントの管理

リモート接続のため、セキュリティ強化されたすべてのアプライアンスにセキュア シェル (SSH) プロトコルが含まれます。システムのセキュリティを維持するためには、必要な場合にのみ SSH を使用して、適切に管理します。

SSH は、VMware 仮想アプライアンスに対するリモート接続をサポートするインタラクティブなコマンドライン環境です。デフォルトで、SSH アクセスには高い権限を持つユーザー アカウントの認証情報が必要です。root ユーザーの SSH アクティビティは一般にロールベースのアクセス制御 (RBAC) と仮想アプライアンスの監査制御をバイパスします。

ベスト プラクティスとして、本番環境で SSH を無効にし、その他の方法で解決できない問題をトラブルシューティングする場合にのみ有効にします。特定の目的で、組織のセキュリティ ポリシーに従って必要な間だけ有効にします。vRealize Automation アプライアンスではデフォルトで SSH が無効です。vSphere の構成によっては、Open Virtualization Format (OVF) テンプレートを展開するときに SSH を有効または無効にすることがあります。

マシンで SSH が有効になっているかどうかを決定する単純なテストとしては、SSH を使用して接続を開くことを試行します。接続が開き、認証情報が要求される場合、SSH は有効で接続に使用できます。

セキュア シェル root ユーザー アカウント

VMware アプライアンスでは事前構成済みのユーザー アカウントがないため、root アカウントはデフォルトで SSH を使用して直接ログインできます。できるだけ早く root として SSH を無効にします。

非否認に関するコンプライアンス標準を満たすため、すべてのセキュリティ強化アプライアンスで SSH サーバは、セカンダリ グループ wheel への SSH アクセスを制限するように AllowGroups wheel エントリが事前設定されています。役目を分離するため、sshd などの別のグループを使用するように /etc/ssh/sshd_config ファイルの AllowGroups wheel エントリを変更することができます。

wheel グループは **pam_wheel** モジュールによってスーパーユーザーのアクセスが有効になっており、wheel グループのメンバーは **su root** を実行できます (root パスワードが必要です)。グループの分離を使用すると、ユーザーはアプライアンスに対して SSH を実行できますが、**su** を実行して root 権限に切り替えることはできません。AllowGroups フィールドのその他のエントリはアプライアンスの適切な機能に確保しているため、削除したり変更したりしないでください。変更後は、コマンド **# service sshd restart** を実行して SSH デーモンを再起動する必要があります。

vRealize Automation アプライアンス上のセキュア シェルを有効または無効にする

セキュア シェル (SSH) は、トラブルシューティング目的のときにのみ、vRealize Automation アプライアンスで有効にします。通常の本番運用中、次のコンポーネントでは SSH を無効にします。

仮想アプライアンス管理コンソールを使用して、vRealize Automation アプライアンスの SSH を有効または無効にできます。

手順

- 1 vRealize Automation アプライアンスの仮想アプライアンス管理コンソール (VAMI) に移動します。
`https://<vRealizeAppliance url>: 5480`
- 2 [管理者] タブをクリックします。
- 3 [管理者] サブメニューをクリックします。
- 4 [SSH サービスの有効化] チェック ボックスを選択して SSH を有効にするか、または選択解除して無効にします。
- 5 [設定の保存] をクリックして、変更を保存します。

セキュア シェルのローカル管理者アカウントの作成

セキュリティのベスト プラクティスとして、仮想アプライアンス ホスト マシンでセキュア シェル (SSH) のローカル管理アカウントを作成して構成します。また、適切なアカウントを作成した後は、root による SSH アクセスを削除します。

SSH のローカル管理アカウント、またはセカンダリ wheel グループのメンバー、またはその両方を作成します。直接 root アクセスを無効にする前に、許可された管理者が AllowGroups を使用して SSH にアクセスできることと、wheel グループを使用して **su** を実行して root 権限に切り替えられることをテストします。

手順

- 1 root として仮想アプライアンスにログインし、適切なユーザー名で次のコマンドを実行します。

```
# useradd -g users <username> -G wheel -m -d /home/<username>
# passwd username
```

wheel は、AllowGroups に ssh アクセスのために指定されたグループです。複数のセカンダリ グループを追加するには、**-G wheel,sshd** を使用します。

- このユーザーに切り替えて新しいパスワードを指定し、パスワードの複雑性の確認を実施します。

```
# su <-username>
# <username@hostname>:~>passwd
```

パスワードの複雑性が要件を満たしている場合は、パスワードが更新されます。パスワードの複雑性が要件を満たしていない場合、パスワードは元のパスワードに戻され、パスワード コマンドを再実行する必要があります。

- SSH への直接ログインを削除するには、`/etc/ssh/sshd_config` ファイルを編集して、**(#)PermitRootLogin yes** を **PermitRootLogin no** に置き換えます。

または、仮想アプライアンス管理インターフェイス (VAMI) の [管理] タブで [管理者の SSH ログインを有効化] チェック ボックスの選択を切り替えることで、SSH を有効または無効にできます。

次のステップ

root としての直接ログインを無効にします。デフォルトで、強化されたアプライアンスは、コンソールを通じた root への直接ログインを許可します。否認防止のための管理アカウントを作成し、それらのアカウントで `su root` による wheel アクセスをテストしたら、root として `/etc/security` ファイルを編集して、**tty1** エントリを **console** に置き換えて、直接 root ログインを無効にします。

- テキスト エディタで `/etc/securetty` ファイルを開きます。
- tty1** を見つけて **console** で置き換えます。
- ファイルを保存し、終了します。

セキュア シェル サーバ構成のセキュリティ強化

すべての VMware アプライアンスは、可能な場合、デフォルトのセキュリティ強化された構成を備えています。ユーザーは、構成ファイルのグローバル オプション セクションのサーバおよびクライアント サービスの設定を調べることで、構成が適切にセキュリティ強化されていることを確認できます。

手順

- VMware アプライアンスで `/etc/ssh/sshd_config` サーバ構成ファイルを開き、設定が正しいことを確認します。

| 設定 | ステータス |
|----------------|--|
| サーバ デモン プロトコル | Protocol 2 |
| CBC 暗号 | aes256-ctr および aes128-ctr |
| TCP 転送 | AllowTCPForwarding no |
| サーバ ゲートウェイ ポート | Gateway Ports no |
| X11 転送 | X11Forwarding no |
| SSH サービス | AllowGroups フィールドを使用してアクセスを許可されたグループを指定します。 このグループに適切なメンバーを追加します。 |
| GSSAPI 認証 | GSSAPIAuthentication no (未使用の場合) |

| 設定 | ステータス |
|--------------------------------|---|
| Keberos 認証 | KeberosAuthentication no (未使用の場合) |
| ローカル変数 (AcceptEnv グローバル オプション) | コメント アウトにより、無効に設定、または LC_* または LANG 変数に対して有効に設定 |
| トンネルの構成 | PermitTunnel no |
| ネットワーク セッション | MaxSessions 1 |
| ユーザーの同時接続 | root およびその他のユーザーに対して 1 に設定します。 /etc/security/limits.conf ファイルも、同じ設定にする必要があります。 |
| Strict モードの確認 | Strict Modes yes |
| 権限分離 | UsePrivilegeSeparation yes |
| rhosts RSA 認証 | RhostsESAAuthentication no |
| 圧縮 | Compression delayed または Compression no |
| メッセージ認証コード | MACs hmac-sha1 |
| ユーザー アクセス制限 | PermitUserEnvironment no |

2 変更内容を保存し、ファイルを閉じます。

セキュア シェル クライアント構成のセキュリティ強化

システム セキュリティ強化プロセスの一環として、仮想アプライアンス ホスト マシンの SSH クライアント構成ファイルを調べて、VMware ガイドラインに従って構成されていることを確認することによって、SSH クライアントのセキュリティ強化を検証します。

手順

- 1 SSH クライアント構成ファイル **/etc/ssh/ssh_config** を開き、グローバル オプション セクションの設定が正しいことを確認します。

| 設定 | ステータス |
|------------------------------|------------------------------|
| クライアント プロトコル | Protocol 2 |
| クライアント ゲートウェイ ポート | Gateway Ports no |
| GSSAPI 認証 | GSSAPIAuthentication no |
| ローカル変数 (SendEnv グローバル オプション) | LC_* または LANG 変数のみ指定 |
| CBC 暗号 | aes256-ctr および aes128-ctr のみ |
| メッセージ認証コード | MACs hmac-sha1 エントリでのみ使用 |

2 変更内容を保存し、ファイルを閉じます。

セキュア シェル キー ファイルの権限の確認

悪意のある攻撃の可能性を最小限に抑えるためには、仮想アプライアンス ホスト マシンで重要な SSH キー ファイルの権限を維持します。

SSH 構成を設定または更新したら、次の SSH キー ファイルの権限に変更がないことを常に確認します。

- `/etc/ssh/*key.pub` 内のパブリック ホスト キーは root ユーザーが所有し、権限が 0644 (-rw-r--r--) に設定されています。
- `/etc/ssh/*key` 内のプライベート ホスト キーは root ユーザーが所有し、権限が 0600 (-rw-----) に設定されています。

SSH キー ファイルの権限を確認する

パブリック キー ファイルとプライベート キー ファイルの両方に SSH 権限が適用されていることを確認します。

手順

- 1 次のコマンドを実行して SSH パブリック キー ファイルを確認します。 `ls -l /etc/ssh/*key.pub`。
- 2 所有者が root であり、グループの所有者が root であり、ファイル権限が 0644 (-rw-r--r--) に設定されていることを確認します。
- 3 次のコマンドを実行して、問題を修正します。

```
chown root /etc/ssh/*key.pub
```

```
chgrp root /etc/ssh/*key.pub
```

```
chmod 644 /etc/ssh/*key.pub
```

- 4 次のコマンドを実行して SSH プライベート キー ファイルを確認します。 `ls -l /etc/ssh/*key` 。
- 5 次のコマンドを実行して、問題を修正します。

```
chown root /etc/ssh/*key
```

```
chgrp root /etc/ssh/*key
```

```
chmod 644 /etc/ssh/*key
```

仮想アプライアンス管理インターフェイスのユーザーの変更

仮想アプライアンス管理インターフェイスでユーザーを追加および削除して、適切なレベルのセキュリティを作成することができます。

仮想アプライアンス管理インターフェイスの root ユーザー アカウントでは、認証に PAM を使用するため、PAM で設定されたクリップ レベルも適用されます。仮想アプライアンス管理インターフェイスを適切に分離していないと、攻撃者が総当たり攻撃を試みたときにシステムの root アカウントでロックアウトが発生することがあります。さらに、root アカウントが組織内の複数のユーザーによる否認防止を付与するのに不十分とみなされた場合は、管理インターフェイスの管理者ユーザーを変更することになる可能性もあります。

前提条件

手順

- 1 新しいユーザーを作成し、仮想アプライアンス管理インターフェイス グループに追加するには、次のコマンドを実行します。

```
useradd -G vami,root <user>
```

- 2 ユーザーのパスワードを作成します。

```
passwd <user>
```

- 3 (オプション) 仮想アプライアンス管理インターフェイスの root アクセス権を無効にするには、次のコマンドを実行します。

```
usermod -R vami root
```

注: 仮想アプライアンス管理インターフェイスへの root アクセス権を無効にすると、[管理] タブの管理者、または root、パスワードをアップデートする機能も無効になります。

ブートローダー認証の設定

適切なレベルのセキュリティを提供するには、VMware 仮想アプライアンスでブートローダー認証を構成します。

システムのブートローダーに認証が必要ない場合、システム コンソールのアクセス権を持つユーザーが、システム ブート構成を変更したり、シングル ユーザー モードまたはメンテナンス モードでシステムをブートしたりできます。この結果、サービス拒否または未認証のシステム アクセスが可能になります。ブートローダー認証は VMware 仮想アプライアンスでデフォルトで設定されていないため、その構成には GRUB パスワードを作成する必要があります。

手順

- 1 仮想アプライアンスの `/boot/grub/menu.lst` ファイル内で `password --md5 <password-hash>` 行を特定して、ブート パスワードが保存されているかどうかを確認します。

- 2 パスワードが保存されていない場合は、仮想アプライアンスで `# /usr/sbin/grub-md5-crypt` コマンドを実行します。

MD5 パスワードが生成され、コマンドによって md5 ハッシュ出力が指定されます。

- 3 `# password --md5 <hash from grub-md5-crypt>` コマンドを実行して、`menu.lst` ファイルにパスワードを追加します。

NTP の設定

クリティカルなタイムソースでは、ホストの時刻同期を無効にして、vRealize Automation アプライアンスで Network Time Protocol (NTP) を使用します。

vRealize Automation アプライアンスの NTP デーモンは、同期された時間サービスを提供します。NTP は、デフォルトでは無効になっているため、手動で設定する必要があります。可能な場合は、本番環境で NTP を使用して、正確な監査とログ保存を通じてユーザー アクションを追跡し、潜在的な悪意のある攻撃と侵入を検出します。NTP のセキュリティ上の注意事項については、NTP の Web サイトを参照してください。

NTP の構成ファイルは、各アプライアンス上の `/etc/` フォルダに含まれています。仮想アプライアンス管理インターフェイスの [管理] タブで、vRealize Automation アプライアンスの NTP サービスを有効にし、タイム サーバを追加できます。

手順

- 1 仮想アプライアンス ホスト マシン上の `/etc/ntp.conf` 構成ファイルをテキスト エディタを使用して開きます。
- 2 ファイルの所有権を **root:root** に設定します。
- 3 権限を **0640** に設定します。
- 4 NTP サービスに対する DNS amp（サービス拒否増幅）攻撃のリスクを低減するには、`/etc/ntp.conf` ファイルを開き、ファイルに `restrict` 行が表示されることを確認します。

```
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict -6 ::1
```

- 5 変更内容を保存し、ファイルを閉じます。

転送中の vRealize Automation アプライアンス データの TLS の構成

vRealize Automation アプライアンス コンポーネントの転送チャンネルをセキュリティ保護するために、vRealize Automation デプロイで強力な TLS プロトコルを使用していることを確認します。

パフォーマンスに関する考慮事項のために、一部のアプリケーション サービス間のローカルホスト接続に対して TLS は有効になっていません。多層防御が必要な場合は、すべてのローカルホスト通信で TLS を有効にします。

重要: ロード バランサの TLS を終了する場合は、すべてのロード バランサで SSLv2、SSLv3、および TLS 1.0 などのセキュアでないプロトコルを無効にします。

localhost 構成で TLS を有効にする

デフォルトでは、一部の localhost 通信は TLS を使用しません。セキュリティの強化を提供するため、すべての localhost 接続で TLS を有効にできます。

手順

- 1 SSH を使用して vRealize Automation アプライアンスに接続します。
- 2 次のコマンドを実行して、VCAC キーストアの権限を設定します。

```
usermod -A vco,coredump,pivotal vco
chown vcac.pivotal /etc/vcac/vcac.keystore
chmod 640 /etc/vcac/vcac.keystore
```

3 HAProxy の構成を更新します。

- a `/etc/haproxy/conf.d` にある HAProxy 構成ファイルを開き、`20-vcac.cfg` サービスを選択します。
- b 次の文字列を含む行を見つけます。

server local 127.0.0.1...。その後、この行の末尾に次の文字列を追加します：**ssl verify none**

このセクションには、次のような行が含まれています。

| | |
|--------------------|---------------------|
| backend-horizon | backend-vro |
| backend-vra | backend-artifactory |
| backend-vra-health | |

- c backend-horizon のポートを 8080 から 8443 に変更します。

4 keystorePass のパスワードを取得します。

- a `/etc/vcac/security.properties` ファイル内の **certificate.store.password** プロパティを見つけます。

例：**certificate.store.password=s2enc~iom0GXATG+RB8ff7Wdm4Bg==**

- b 次のコマンドを使用して、値を復号化します。

vcac-config prop-util -d --p VALUE

例：**vcac-config prop-util -d --p s2enc~iom0GXATG+RB8ff7Wdm4Bg==**

5 vRealize Automation サービスを構成します。

- a `/etc/vcac/server.xml` ファイルを開きます。
- b 次の属性を Connector タグに追加します。certificate.store.password は、`/etc/vcac/security.properties` にある証明書ストア パスワード値に置き換えます。

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS"
keystoreFile="/etc/vcac/vcac.keystore" keyAlias="apache" keystorePass="
certificate.store.password"
```

6 vRealize Orchestrator サービスを構成します。

- a `/etc/vco/app-server.xml` ファイルを開きます。
- b 次の属性を Connector タグに追加します。certificate.store.password は、`/etc/vcac/security.properties` にある証明書ストア パスワード値に置き換えます。

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS"
keystoreFile="/etc/vcac/vcac.keystore" keyAlias="apache" keystorePass="
certificate.store.password"
```

- 7 vRealize Orchestrator、vRealize Automation、および haproxy サービスを再起動します。

```
service vcac-server restart
service vco-server restart
service haproxy restart
```

注: vco-server が再起動しない場合は、ホスト コンピュータを再起動します。

- 8 仮想アプライアンス管理インターフェイスを構成します。

- a /opt/vmware/share/htdocs/service/café-services/services.py ファイルを開きます。
- b `conn = httplib.HTTP()` の行を `conn = httplib.HTTPS()` に変更してセキュリティを強化します。

連邦情報処理標準 (FIPS) 140-2 準拠の処理を有効にする

vRealize Automation アプライアンスは、すべての受信および送信ネットワーク トラフィックについて、TLS 経由の転送中データに対して OpenSSL の連邦情報処理標準 (FIPS) 140-2 認定済みバージョンを使用するようになりました。

vRealize Automation アプライアンス管理インターフェイスで FIPS モードを有効または無効にできます。root としてログインしているときに、コマンドラインから次のコマンドを使用して FIPS を構成することもできます。

```
vcac-vami fips enable
vcac-vami fips disable
vcac-vami fips status
```

FIPS を有効にすると、ポート 443 の受信および送信 vRealize Automation アプライアンス ネットワーク トラフィックには FIPS 140-2 準拠の暗号化が使用されます。FIPS の設定に関係なく、vRealize Automation では vRealize Automation アプライアンスに保存されたデータには AES-256 が使用され、セキュアに保護されます。

注: 一部の内部コンポーネントでは認定済みの暗号化モジュールがまだ使用されていないため、現在は vRealize Automation の一部のみで FIPS 準拠が有効になっています。認定済みのモジュールがまだ実装されていない場合、すべての暗号化アルゴリズムで AES-256 ベースの暗号化が使用されます。

注: 次の手順では、構成を変更するときに、物理マシンが再起動されます。

手順

- 1 vRealize Automation アプライアンスの管理インターフェイスに root としてログインします。
https:// vrealize-automation-appliance-FQDN:5480
- 2 [vRA 設定] - [ホストの設定] の順に選択します。
- 3 右上にある [アクション] という見出しの下ボタンをクリックして FIPS を有効または無効にします。
- 4 [はい] をクリックして vRealize Automation アプライアンスを再起動します。

SSLv3、TLS 1.0、および TLS 1.1 が無効になっていることを確認する

セキュリティ強化プロセスの一環として、デプロイした vRealize Automation アプライアンス がセキュアな通信チャネルを使用していることを確認します。

注: TLS 1.0/1.1 を無効にし、TLS 1.2 を有効にした後は、クラスタ参加操作を実行することができません。

前提条件

「localhost 構成で TLS を有効にする」を実行します。

手順

- 1 vRealize Automation アプライアンスの HAProxy https ハンドラで SSLv3、TLS 1.0、および TLS 1.1 が無効になっていることを確認します。

| 確認するファイル | 次の記載があることを確認 | 確認する行 |
|---------------------------------------|---------------------------------------|--|
| /etc/haproxy/conf.d/20-vcac.cfg | no-ssl3 no-tls10 no-tls11 force-tls12 | bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:EC DH +AESGCM:RSA+AESGCM:kECDH+AES:EC DH +AES:RSA+AES:@STRENGTH no-ssl3 no-tls10 no-tls11 |
| /etc/haproxy/conf.d/30-vro-config.cfg | no-ssl3 no-tls10 no-tls11 force-tls12 | bind :::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:EC DH +AESGCM:RSA+AESGCM:kECDH+AES:EC DH +AES:RSA+AES:@STRENGTH no-ssl3 no-tls10 no-tls11 |

- 2 サービスを再起動します。

```
service haproxy restart
```

- 3 /opt/vmware/etc/lighttpd/lighttpd.conf ファイルを開いて、無効にするための正しいエントリがあることを確認します。

注: Lighttpd には、TLS 1.0 または TLS 1.1 を無効にするディレクティブがありません。TLS 1.0 と TLS 1.1 の使用に対する制限は、OpenSSL が TLS 1.0 と TLS 1.1 の暗号スイートを使用しないように適用することで、部分的に緩和できます。

```
ssl.use-ssl2 = "disable"  
ssl.use-ssl3 = "disable"
```


- 4 vRealize Automation アプライアンスのコンソール プロキシで SSLv3、TLS 1.0、および TLS 1.1 が無効になっていることを確認します。

- a `/etc/vcac/security.properties` ファイルを編集して、次の行を追加または変更します。

```
consoleproxy.ssl.server.protocols = TLSv1.2
```

- b 次のコマンドを実行して、サーバを再起動します。

```
service vcac-server restart
```

- 5 vCO サービスで SSLv3、TLS 1.0、および TLS 1.1 が無効になっていることを確認します。

- a `/etc/vco/app-server/server.xml` ファイル内の `<Connector>` タグを見つけて、次の属性を追加します。

```
sslEnabledProtocols = "TLSv1.2"
```

- b 次のコマンドを実行して vCO サービスを再起動します。

```
service vco-server restart
```

- 6 vRealize Automation サービスで SSLv3、TLS 1.0、および TLS 1.1 が無効になっていることを確認します。

- a `/etc/vcac/server.xml` ファイル内の `<Connector>` タグに次の属性を追加します。

```
sslEnabledProtocols = "TLSv1.2"
```

- b 次のコマンドを実行して vRealize Automation サービスを再起動します。

```
service vcac-server restart
```

- 7 RabbitMQ で SSLv3、TLS 1.0、および TLS 1.1 が無効になっていることを確認します。

`/etc/rabbitmq/rabbitmq.config` ファイルを開いて、`{versions, ['tlsv1.2', 'tlsv1.1']}` が `ssl` および `ssl_options` セクションに表示されていることを確認します。

```
[
  {ssl, [
    {versions, ['tlsv1.2', 'tlsv1.1']},
    {ciphers, ["AES256-SHA", "AES128-SHA"]}
  ]},
  {rabbit, [
    {tcp_listeners, [{"127.0.0.1", 5672}]},
    {frame_max, 262144},
    {ssl_listeners, [5671]},
    {ssl_options, [
      {cacertfile, "/etc/rabbitmq/certs/ca/cacert.pem"},
      {certfile, "/etc/rabbitmq/certs/server/cert.pem"},
      {keyfile, "/etc/rabbitmq/certs/server/key.pem"},
      {versions, ['tlsv1.2', 'tlsv1.1']},
      {ciphers, ["AES256-SHA", "AES128-SHA"]},
      {verify, verify_peer},
      {fail_if_no_peer_cert, false}
    ]},
    {mnesia_table_loading_timeout, 600000},
```

```
{cluster_partition_handling, autoheal},
{heartbeat, 600}
]],
{kernel, [{net_ticktime, 120}]}
].
```

- 8 RabbitMQ サーバを再起動します。

```
# service rabbitmq-server restart
```

- 9 vIDM サービスで SSLv3、TLS 1.0、および TLS 1.1 が無効になっていることを確認します。

SSLEnabled="true" を含むコネクタの各インスタンスで

opt/vmware/horizon/workspace/conf/server.xml ファイルを開いて、次の行が表示されていることを確認します。

```
sslEnabledProtocols="TLSv1.2"
```

vRealize Automation コンポーネント用の TLS 暗号スイートの構成

セキュリティを最大限高めるには、強力な暗号を使用するように vRealize Automation コンポーネントを設定する必要があります。

サーバとブラウザの間でネゴシエートされる暗号化により、TLS セッションで使用される暗号化の強度が決まります。

強力な暗号のみが確実に選択されるようにするため、vRealize Automation コンポーネントで強度の弱い暗号を無効にします。強力な暗号のみをサポートし、十分に大きいキー サイズを使用するように、サーバを設定します。また、適切な順序ですべての暗号を構成します。

NULL 暗号スイート、aNULL、または eNULL などの認証を提供しない暗号スイートを無効にします。この他に、匿名の Diffie-Hellman キー交換 (ADH)、エクスポート レベルの暗号 (EXP、DES を含んでいる暗号)、ペイロードトラフィックの暗号化に対する 128 ビットより小さいサイズのキー、ペイロードトラフィックのハッシュ メカニズムとしての MD5 の使用、IDEA 暗号スイート、および RC4 暗号スイートも無効にします。また、Diffie-Hellman (DHE) キー交換を使用する暗号スイートが無効になっていることを確認します。

HA プロキシの強度の弱い暗号を無効にする

使用可能な暗号のリストに照らし合わせて、vRealize Automation アプライアンス HA プロキシ サービスの暗号を確認し、強度が弱いとみなされるものすべてを無効にします。

NULL 暗号スイート、aNULL、または eNULL などの認証を提供しない暗号スイートを無効にします。この他に、匿名の Diffie-Hellman キー交換 (ADH)、エクスポート レベルの暗号 (EXP、DES を含んでいる暗号)、ペイロードトラフィックの暗号化に対する 128 ビットより小さいサイズのキー、ペイロードトラフィックのハッシュ メカニズムとしての MD5 の使用、IDEA 暗号スイート、および RC4 暗号スイートも無効にします。

手順

- 1 `/etc/haproxy/conf.d/20-vcac.cfg` ファイルのバインド ディレクティブの暗号エントリを確認し、強度が弱いとみなされるすべてのものを無効にします。

```
bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-sslv3 no-tls1 no-tls11
```

- 2 `/etc/haproxy/conf.d/30-vro-config.cfg` ファイルのバインド ディレクティブの暗号エントリを確認し、強度が弱いとみなされるすべてのものを無効にします。

```
bind :::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-sslv3 no-tls1 no-tls11
```

vRealize Automation アプライアンス vRealize Automation アプライアンス コンソール プロキシ サービスの強度の弱い暗号を無効にする

使用可能な暗号のリストに照らし合わせて、vRealize Automation アプライアンス コンソール プロキシ サービスの暗号を確認し、強度が弱いとみなされるものすべてを無効にします。

NULL 暗号スイート、aNULL、または eNULL などの認証を提供しない暗号スイートを無効にします。この他に、匿名の Diffie-Hellman キー交換 (ADH)、エクスポート レベルの暗号 (EXP、DES を含んでいる暗号)、ペイロードトラフィックの暗号化に対する 128 ビットより小さいサイズのキー、ペイロードトラフィックのハッシュ メカニズムとしての MD5 の使用、IDEA 暗号スイート、および RC4 暗号スイートも無効にします。

手順

- 1 `/etc/vcac/security.properties` ファイルをテキスト エディタで開きます。
- 2 不要な暗号スイートを無効にするには、ファイルに行を追加します。

次の行に必要な変更を加えて使用します。

```
consoleproxy.ssl.ciphers.disabled=<cipher_suite_1, cipher_suite_2,etc>
```

たとえば、AES 128 および AES 256 の暗号スイートを無効にするには、次の行を追加します。

```
consoleproxy.ssl.ciphers.disabled=TLS_DH_DSS_WITH_AES_128_CBC_SHA,
TLS_DH_DSS_WITH_AES_256_CBC_SHA, TLS_DH_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

- 3 次のコマンドを使用してサーバを再起動します。

```
service vcac-server restart
```

vRealize Automation アプライアンス vCO サービスの強度の弱い暗号を無効にする

使用可能な暗号のリストに照らし合わせて、vRealize Automation アプライアンス vCO サービスの暗号を確認し、強度が弱いとみなされるものすべてを無効にします。

NULL 暗号スイート、aNULL、または eNULL などの認証を提供しない暗号スイートを無効にします。この他に、匿名の Diffie-Hellman キー交換 (ADH)、エクスポート レベルの暗号 (EXP、DES を含んでいる暗号)、ペイロードトラフィックの暗号化に対する 128 ビットより小さいサイズのキー、ペイロードトラフィックのハッシュメカニズムとしての MD5 の使用、IDEA 暗号スイート、および RC4 暗号スイートも無効にします。

手順

- 1 `/etc/vco/app/server/server.xml` ファイル内で `<Connector>` タグを見つけます。
- 2 目的の暗号スイートを使用するように、暗号の属性を編集または追加します。

次の例を参照してください。

```
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
```

vRealize Automation アプライアンス RabbitMQ サービスの強度の弱い暗号を無効にする

使用可能な暗号のリストに照らし合わせて、vRealize Automation アプライアンス RabbitMQ サービスの暗号を確認し、強度が弱いとみなされるものすべてを無効にします。

NULL 暗号スイート、aNULL、または eNULL などの認証を提供しない暗号スイートを無効にします。この他に、匿名の Diffie-Hellman キー交換 (ADH)、エクスポート レベルの暗号 (EXP、DES を含んでいる暗号)、ペイロードトラフィックの暗号化に対する 128 ビットより小さいサイズのキー、ペイロードトラフィックのハッシュメカニズムとしての MD5 の使用、IDEA 暗号スイート、および RC4 暗号スイートも無効にします。

手順

- 1 サポートされる暗号スイートを評価します。# `/usr/sbin/rabbitmqctl eval 'ssl:cipher_suites()'` コマンドを実行します。

次の例で返される暗号は、サポートされる暗号のみを表しています。RabbitMQ サーバは、`rabbitmq.config` ファイルでこれらの暗号を使用またはアドバタイズするように構成されていない限り、使用またはアドバタイズを行いません。

```
["ECDHE-ECDSA-AES256-GCM-SHA384","ECDHE-RSA-AES256-GCM-SHA384",
 "ECDHE-ECDSA-AES256-SHA384","ECDHE-RSA-AES256-SHA384",
 "ECDH-ECDSA-AES256-GCM-SHA384","ECDH-RSA-AES256-GCM-SHA384",
 "ECDH-ECDSA-AES256-SHA384","ECDH-RSA-AES256-SHA384",
 "DHE-RSA-AES256-GCM-SHA384","DHE-DSS-AES256-GCM-SHA384",
 "DHE-RSA-AES256-SHA256","DHE-DSS-AES256-SHA256","AES256-GCM-SHA384",
 "AES256-SHA256","ECDHE-ECDSA-AES128-GCM-SHA256",
 "ECDHE-RSA-AES128-GCM-SHA256","ECDHE-ECDSA-AES128-SHA256",
 "ECDHE-RSA-AES128-SHA256","ECDH-ECDSA-AES128-GCM-SHA256",
 "ECDH-RSA-AES128-GCM-SHA256","ECDH-ECDSA-AES128-SHA256",
 "ECDH-RSA-AES128-SHA256","DHE-RSA-AES128-GCM-SHA256",
 "DHE-DSS-AES128-GCM-SHA256","DHE-RSA-AES128-SHA256","DHE-DSS-AES128-SHA256",
 "AES128-GCM-SHA256","AES128-SHA256","ECDHE-ECDSA-AES256-SHA",
 "ECDHE-RSA-AES256-SHA","DHE-RSA-AES256-SHA","DHE-DSS-AES256-SHA",
 "ECDH-ECDSA-AES256-SHA","ECDH-RSA-AES256-SHA","AES256-SHA",
 "ECDHE-ECDSA-DES-CBC3-SHA","ECDHE-RSA-DES-CBC3-SHA","EDH-RSA-DES-CBC3-SHA",
```

```
"EDH-DSS-DES-CBC3-SHA", "ECDH-ECDSA-DES-CBC3-SHA", "ECDH-RSA-DES-CBC3-SHA",
"DES-CBC3-SHA", "ECDHE-ECDSA-AES128-SHA", "ECDHE-RSA-AES128-SHA",
"DHE-RSA-AES128-SHA", "DHE-DSS-AES128-SHA", "ECDH-ECDSA-AES128-SHA",
"ECDH-RSA-AES128-SHA", "AES128-SHA"]
```

- 2 組織のセキュリティ要件を満たす、サポートされる暗号を選択します。

たとえば、**ECDHE-ECDSA-AES128-GCM-SHA256 & ECDHE-ECDSA-AES256-GCM-SHA384** だけを許可するには、**/etc/rabbitmq/rabbitmq.config** ファイルを確認し、**ssl** および **ssl_options** に次の行を追加します。

```
{ciphers, [{"ECDHE-ECDSA-AES128-GCM-SHA256"}, {"ECDHE-ECDSA-AES256-GCM-SHA384"}]}
```

- 3 次のコマンドを使用して、RabbitMQ サーバを再起動します。

```
service rabbitmq-server restart
```

保存データのセキュリティの確認

vRealize Automation で使用されるデータベースのユーザーおよびアカウントのセキュリティを確認します。

Postgres ユーザー

Postgres の Linux ユーザー アカウントは Postgres データベースのスーパーユーザー アカウント ロールに関連付けられています。デフォルトでは、アカウントはロックされています。**root** ユーザー アカウントからしかアクセスできないため、このユーザーには最もセキュアな構成です。このユーザー アカウントのロックを解除しないでください。

データベースのユーザー アカウント ロール

デフォルトの Postgres ユーザー アカウント ロールは、アプリケーション機能以外では使用しないでください。デフォルト以外のデータベースのレビューまたはレポート処理をサポートするには、追加のアカウントを作成して、パスワードを適切に保護する必要があります。

コマンド ラインで次のスクリプトを実行します。

```
vcac-vami add-db-user newUsername newPassword
```

これで、ユーザーによって指定された新しいユーザーとパスワードが追加されます。

注: マスター スレーブ HA Postgres 設定が構成されている場合は、マスター Postgres データベースに対してこのスクリプトを実行する必要があります。

PostgreSQL クライアント認証の構成

ローカル trust 認証が vRealize Automation アプライアンス PostgreSQL データベースで構成されていないことを確認します。この構成では、データベーススーパー ユーザーを含むすべてのローカルユーザーが、任意の PostgreSQL ユーザーとしてパスワードなしで接続することが可能となります。

注: Postgre のスーパー ユーザー アカウントは、ローカル trust のままにする必要があります。

暗号化されたパスワードが送信されるため、md5 認証方法をお勧めします。

クライアント認証構成設定は、`/storage/db/pgdata/pg_hba.conf` ファイル内に存在します。

```
# TYPE      DATABASE         USER                ADDRESS            METHOD
# "local" is for Unix domain socket connections only
local       all             postgres            trust
# IPv4 local connections:
#host       all             all                 127.0.0.1/32      md5
hostssl     all             all                 127.0.0.1/32      md5
# IPv6 local connections:
#host       all             all                 ::1/128           md5
hostssl     all             all                 ::1/128           md5

# Allow remote connections for VCAC user.
#host       vcac             vcac                0.0.0.0/0         md5
hostssl     vcac             vcac                0.0.0.0/0         md5
hostssl     vcac             vcac                ::0/0             md5
# Allow remote connections for VCAC replication user.
#host       vcac             vcac_replication    0.0.0.0/0         md5
hostssl     vcac             vcac_replication    0.0.0.0/0         md5
hostssl     vcac             vcac_replication    ::0/0             md5
# Allow replication connections by a user with the replication privilege.
#host       replication      vcac_replication    0.0.0.0/0         md5
hostssl     replication      vcac_replication    0.0.0.0/0         md5
hostssl     replication      vcac_replication    ::0/0             md5
```

`pg_hba.conf` ファイルを編集する場合、変更を有効にするには、次のコマンドを実行して Postgre サーバを再起動する必要があります。

```
# cd /opt/vmware/vpostgres/9.2/bin
# su postgres
# ./pg_ctl restart -D /storage/db/pgdata/ -m fast
```

vRealize Automation アプリケーション リソースの構成

vRealize Automation アプリケーション リソースを確認し、ファイルの権限を制限します。

手順

- 1 SUID および GUID ビットが設定されたファイルが正しく定義されていることを確認するには、次のコマンドを実行します。

```
find / -path /proc -prune -o -type f -perm +6000 -ls
```

次のリストが表示されます。

```
2197357  24 -rwsr-xr-x  1 polkituser root      23176 Mar 31
2015 /usr/lib/PolicyKit/polkit-set-default-helper
2197354  16 -rwxr-sr-x  1 root    polkituser 14856 Mar 31
2015 /usr/lib/PolicyKit/polkit-read-auth-helper
2197353  12 -rwsr-x---  1 root    polkituser 10744 Mar 31
2015 /usr/lib/PolicyKit/polkit-grant-helper-pam
2197352  20 -rwxr-sr-x  1 root    polkituser 19208 Mar 31
```

```

2015 /usr/lib/PolicyKit/polkit-grant-helper
2197351 20 -rwxr-sr-x 1 root polkituser 19008 Mar 31
2015 /usr/lib/PolicyKit/polkit-explicit-grant-helper
2197356 24 -rwxr-sr-x 1 root polkituser 23160 Mar 31
2015 /usr/lib/PolicyKit/polkit-revoke-helper
2188203 460 -rws--x--x 1 root root 465364 Apr 21 22:38 /usr/lib64/ssh/ssh-
keysign
2138858 12 -rwxr-sr-x 1 root tty 10680 May 10 2010 /usr/sbin/utempter
2142482 144 -rwsr-xr-x 1 root root 142890 Sep 15 2015 /usr/bin/passwd
2142477 164 -rwsr-xr-x 1 root shadow 161782 Sep 15 2015 /usr/bin/chage
2142467 156 -rwsr-xr-x 1 root shadow 152850 Sep 15 2015 /usr/bin/chfn
1458298 364 -rwsr-xr-x 1 root root 365787 Jul 22 2015 /usr/bin/sudo
2142481 64 -rwsr-xr-x 1 root root 57776 Sep 15 2015 /usr/bin/newgrp
1458249 40 -rwsr-x--- 1 root trusted 40432 Mar 18 2015 /usr/bin/crontab
2142478 148 -rwsr-xr-x 1 root shadow 146459 Sep 15 2015 /usr/bin/chsh
2142480 156 -rwsr-xr-x 1 root shadow 152387 Sep 15 2015 /usr/bin/gpasswd
2142479 48 -rwsr-xr-x 1 root shadow 46967 Sep 15 2015 /usr/bin/expiry
311484 48 -rwsr-x--- 1 root messagebus 47912 Sep 16 2014 /lib64/dbus-1/dbus-
daemon-launch-helper
876574 36 -rwsr-xr-x 1 root shadow 35688 Apr 10 2014 /sbin/unix_chkpwd
876648 12 -rwsr-xr-x 1 root shadow 10736 Dec 16 2011 /sbin/unix2_chkpwd
49308 68 -rwsr-xr-x 1 root root 63376 May 27 2015 /opt/likewise/bin/ksu
1130552 40 -rwsr-xr-x 1 root root 40016 Apr 16 2015 /bin/su
1130511 40 -rwsr-xr-x 1 root root 40048 Apr 15 2011 /bin/ping
1130600 100 -rwsr-xr-x 1 root root 94808 Mar 11 2015 /bin/mount
1130601 72 -rwsr-xr-x 1 root root 69240 Mar 11 2015 /bin/umount
1130512 36 -rwsr-xr-x 1 root root 35792 Apr 15 2011 /bin/ping6
2012 /lib64/dbus-1/dbus-daemon-launch-helper

```

- 2 仮想アプライアンスのすべてのファイルに所有者があることを確認するには、次のコマンドを実行します。

```
find / -path /proc -prune -o -nouser -o -nogroup
```

- 3 すべてのファイルの仮想アプライアンスに対する権限を確認し、あらゆるユーザーが書き込み可能なファイルがないことを確認するには、次のコマンドを実行します。

```
find / -name "*. *" -type f -perm -a+w | xargs ls -ldb
```

- 4 vcac ユーザーのみが適切なファイルを所有していることを確認するには、次のコマンドを実行します。

```
find / -name "proc" -prune -o -user vcac -print | egrep -v -e "*/vcac/*" |
egrep -v -e "*/vmware-vcac/*"
```

結果が表示されない場合、すべての正しいファイルが vcac ユーザーによってのみ所有されています。

- 5 次のファイルが vcac ユーザーによってのみ書き込み可能であることを確認します。

```

/etc/vcac/vcac/security.properties
/etc/vcac/vcac/solution-users.properties
/etc/vcac/vcac/sso-admin.properties
/etc/vcac/vcac/vcac.keystore
/etc/vcac/vcac/vcac.properties

```

また、次のファイルおよびそのサブディレクトリも確認します。

```
/var/log/vcac/*
```

```
/var/lib/vcac/*
```

```
/var/cache/vcac/*
```

- 6 vcac または root ユーザーのみが次のディレクトリとそのサブディレクトリにある正しいファイルを読み取ることができることを確認します。

```
/etc/vcac/*
```

```
/var/log/vcac/*
```

```
/var/lib/vcac/*
```

```
/var/cache/vcac/*
```

- 7 次のディレクトリとそのサブディレクトリ内に示されるように、正しいファイルが vco または root ユーザーのみによって所有されていることを確認します。

```
/etc/vco/*
```

```
/var/log/vco/*
```

```
/var/lib/vco/*
```

```
/var/cache/vco/*
```

- 8 次のディレクトリとそのサブディレクトリ内に示されるように、正しいファイルが vco または root ユーザーのみによって書き込み可能であることを確認します。

```
/etc/vco/*
```

```
/var/log/vco/*
```

```
/var/lib/vco/*
```

```
/var/cache/vco/*
```

- 9 次のディレクトリとそのサブディレクトリ内に示されるように、正しいファイルが vco または root ユーザーのみによって読み取り可能であることを確認します。

```
/etc/vco/*
```

```
/var/log/vco/*
```

```
/var/lib/vco/*
```

```
/var/cache/vco/*
```


コンソール プロキシ構成のカスタマイズ

vRealize Automation のリモート コンソールの構成をカスタマイズして、トラブルシューティングや組織の活動を促進できます。

vRealize Automation をインストール、構成、または保守する際に、いくつかの設定を変更してトラブルシューティングやデバッグを行えます。加えた変更を記録して監査し、該当するコンポーネントが用途に従って確実にセキュリティで保護されるようにします。設定の変更が正しくセキュリティで保護されているかどうか分からない場合は、本番環境には適用しないでください。

VMware Remote Console チケットの有効期限のカスタマイズ

VMware Remote Console 接続の確立に使用されるリモート コンソールのチケットの有効期限をカスタマイズすることができます。

ユーザーが VMware Remote Console に接続すると、システムは、仮想マシンへの特定の接続を確立するワンタイム認証情報を作成して返します。チケットの有効期限を分単位の時間枠で設定できます。

手順

- 1 `/etc/vcac/security.properties` ファイルをテキスト エディタで開きます。
- 2 `consoleproxy.ticket.validitySec=30` の形式でファイルに行を追加します。
この行の数値は、チケットの有効期限が切れるまでの分数を指定します。
- 3 ファイルを保存し、終了します。
- 4 `/etc/init.d/vcac-server restart` コマンドを使用して、vcac サーバを再起動します。

チケットの有効期限の値が、指定した分単位の時間枠にリセットされます。

コンソール プロキシ サーバのポートのカスタマイズ

VMware Remote Console のコンソール プロキシがメッセージをリッスンするポートをカスタマイズすることができます。

手順

- 1 `/etc/vcac/security.properties` ファイルをテキスト エディタで開きます。
- 2 `consoleproxy.service.port=8445` の形式でファイルに行を追加します。
数値は、コンソール プロキシ サービスのポート番号を指定します。この場合は 8445 です。
- 3 ファイルを保存し、終了します。
- 4 `/etc/init.d/vcac-server restart` コマンドを使用して、vcac サーバを再起動します。

プロキシ サービス ポートの番号が、指定したポート番号に変更されます。

X-XSS-Protection 応答ヘッダーの構成

Haproxy 構成ファイルに、X-XSS-Protection 応答ヘッダーを追加します。

手順

- 1 編集するために `/etc/haproxy/conf.d/20-vcac.cfg` を開きます。
- 2 フロント エンド セクションで、次の行を追加します。

```
rspdel X-XSS-Protection:\ 1;\ mode=block
rspadd X-XSS-Protection:\ 1;\ mode=block
```

- 3 次のコマンドを使用して、HAProxy 構成を再ロードします。

```
/etc/init.d/haproxy reload
```

HTTP Strict Transport Security 応答ヘッダーの構成

HAProxy 構成に HTTP Strict Transport (HSTS) 応答ヘッダーを追加します。

手順

- 1 編集するために `/etc/haproxy/conf.d/20-vcac.cfg` を開きます。
- 2 フロント エンド セクションで、次の行を追加します。

```
rspdel Strict-Transport-Security:\ max-age=31536000
rspadd Strict-Transport-Security:\ max-age=31536000
```

- 3 次のコマンドを使用して、HAProxy 構成を再ロードします。

```
/etc/init.d/haproxy reload
```

X-Frame-Options 応答ヘッダーの構成

X-Frame-Options 応答ヘッダーは、場合によっては 2 回表示されることがあります。

X-Frame-Options 応答ヘッダーが 2 回表示されることがあるのは、vIDM サービスがこのヘッダーをバックエンドと HAProxy に追加するためです。適切な構成にすることで、2 回表示されることを防止できます。

手順

- 1 編集するために `/etc/haproxy/conf.d/20-vcac.cfg` を開きます。
- 2 フロント エンド セクションで、次の行を見つけます。

```
rspadd X-Frame-Options:\ SAMEORIGIN
```

- 3 上記の手順で見つけた行の前に、次の行を追加します。

```
rspdel X-Frame-Options:\ SAMEORIGIN
```

- 4 次のコマンドを使用して、HAProxy 構成を再ロードします。

```
/etc/init.d/haproxy reload
```

サーバ応答ヘッダーの構成

セキュリティのベスト プラクティスとして、潜在的な攻撃者が使用可能な情報を制限するように vRealize Automation システムを構成します。

可能な範囲で、システムで共有する ID やバージョンに関する情報量を最小限にします。ハッカーや悪意のある攻撃者は、この情報を使用して Web サーバまたはバージョンを標的にした攻撃を作成することができます。

Lighttpd サーバ応答ヘッダーの構成

ベスト プラクティスとして、vRealize Automation アプライアンス lighttpd サーバ用に空白のサーバ ヘッダーを作成します。

手順

- 1 `/opt/vmware/etc/lighttpd/lighttpd.conf` ファイルをテキスト エディタで開きます。
- 2 `server.tag = " "` をファイルに追加します。
- 3 変更内容を保存し、ファイルを閉じます。
- 4 `# /opt/vmware/etc/init.d/vami-lighttp restart` コマンドを実行して、lighttpd サーバを再起動します。

TCServer 応答ヘッダーの vRealize Automation アプライアンス向けの構成

ベスト プラクティスとして、vRealize Automation アプライアンスと連携して使用する TCServer 応答ヘッダーのカスタムの空白サーバ ヘッダーを作成して、有益な情報を取得しようとする悪意のある攻撃の可能性を制限します。

手順

- 1 テキスト エディタで `/etc/vco/app-server/server.xml` ファイルを開きます。
- 2 それぞれの `<Connector>` 要素に `server=" "` を追加します。
たとえば、`<Connector protocol="HTTP/1.1" server="" />` のように指定します。
- 3 変更内容を保存し、ファイルを閉じます。
- 4 次のコマンドを使用してサーバを再起動します。
`service vco-server restart`

Internet Information Services のサーバ応答ヘッダーの構成

ベスト プラクティスとして、Identity Appliance と連携して使用する Internet Information Services (IIS) サーバのカスタムの空白サーバ ヘッダーを作成して、有益な情報を取得しようとする悪意のある攻撃の可能性を制限します。

手順

- 1 `C:\Windows\System32\inetsrv\urlscan\UrlScan.ini` ファイルをテキスト エディタで開きます。
- 2 `RemoveServerHeader=0` を検索し、`RemoveServerHeader=1.` に変更します。
- 3 変更内容を保存し、ファイルを閉じます。

4 `iisreset` コマンドを実行して、サーバを再起動します。

次のステップ

IIS マネージャー コンソールで、リストから HTTP 応答ヘッダーを削除して、IIS X-Powered By ヘッダーを無効にします。

- 1 IIS マネージャー コンソールを開きます。
- 2 HTTP 応答ヘッダーを開き、リストから削除します。
- 3 `iisreset` コマンドを実行して、サーバを再起動します。

vRealize Automation アプライアンス セッション タイムアウトの設定

会社のセキュリティ ポリシーに従って、vRealize Automation アプライアンス でセッションのタイムアウト設定を構成します。

ユーザーによる操作がない場合の vRealize Automation アプライアンス のデフォルト セッション タイムアウトは 30 分です。組織のセキュリティ ポリシーに準拠するようにこのタイムアウト値を調整するには、vRealize Automation アプライアンス ホスト マシンの `web.xml` ファイルを編集します。

手順

- 1 テキスト エディタで `/usr/lib/vcac/server/webapps/vcac/WEB-INF/web.xml` ファイルを開きます。
- 2 `session-config` を特定して、セッション タイムアウト値を設定します。次のコード サンプルを参照してください。

```
<!-- 30 minutes session expiration time -->
<session-config>
  <session-timeout>30</session-timeout>
  <tracking-mode>COOKIE</tracking-mode>
  <cookie-config>
    <path>/</path>
  </cookie-config>
</session-config>
```

- 3 次のコマンドを実行して、サーバを再起動します。

```
service vcac-server restart
```

必須でないソフトウェアの管理

セキュリティ リスクを最小限に抑えるため、必須でないソフトウェアは vRealize Automation ホスト マシンから削除または構成します。

セキュリティ侵害を引き起こす可能性を最小限に抑えるため、メーカーの推奨事項とセキュリティのベスト プラクティスに従って削除しないすべてのソフトウェアを構成します。

USB 大容量ストレージ ハンドラのセキュリティ保護

VMware 仮想アプライアンス ホスト マシンで USB デバイス ハンドラとして使用されないように、USB 大容量ストレージ ハンドラをセキュリティ保護します。潜在的な攻撃者がこのハンドラを悪用してシステムに侵入する可能性があります。

手順

- 1 テキスト エディタで `/etc/modprobe.conf.local` ファイルを開きます。
- 2 このファイルに `install usb-storage /bin/true` 行が表示されていることを確認します。
- 3 ファイルを保存し、終了します。

Bluetooth プロトコル ハンドラのセキュリティ保護

潜在的な攻撃者の悪用を防ぐために、仮想アプライアンス ホスト マシンで Bluetooth プロトコル ハンドラをセキュリティ保護します。

Bluetooth プロトコルをネットワーク スタックにバインドすると、ホストの攻撃対象が増える可能性があります。

手順

- 1 テキスト エディタで `/etc/modprobe.conf.local` ファイルを開きます。
- 2 このファイルに次の行が表示されていることを確認します。

```
install bluetooth /bin/true
```

- 3 ファイルを保存し、終了します。

Stream Control Transmission Protocol のセキュリティ保護

Stream Control Transmission Protocol (SCTP) がデフォルトでシステムにロードされないようにします。潜在的な攻撃者がこのプロトコルを悪用してシステムに侵入する可能性があります。

本当に必要な限り、Stream Control Transmission Protocol (SCTP) モジュールがロードされないようにシステムを構成します。SCTP は、未使用の IETF 標準化トランスポート レイヤー プロトコルです。このプロトコルをネットワーク スタックにバインドすると、ホストの攻撃対象が増えます。ローカル プロセスに権限を付与しないと、カーネルがプロトコルを使用してソケットを開くことで、プロトコル ハンドラを動的にロードする可能性があります。

手順

- 1 テキスト エディタで `/etc/modprobe.conf.local` ファイルを開きます。
- 2 このファイルに次の行が表示されていることを確認します。

```
install sctp /bin/true
```

- 3 ファイルを保存し、終了します。

Datagram Congestion Protocol のセキュリティ保護

システムのセキュリティ強化策の一環として、Datagram Congestion Protocol (DCCP) がデフォルトで仮想アプライアンス ホスト マシンにロードされないようにします。潜在的な攻撃者がこのプロトコルを悪用してシステムに侵入する可能性があります。

本当に必要ない限りは、Datagram Congestion Control Protocol (DCCP) モジュールをロードしないでください。DCCP はトランスポート レイヤー プロトコルとして予約されていますが、使用されてはいません。このプロトコルをネットワーク スタックにバインドすると、ホストの攻撃対象が増えます。ローカル プロセスに権限を付与しないと、カーネルがソケットを開くプロトコルを使用してプロトコル ハンドラを動的にロードする可能性があります。

手順

- 1 テキスト エディタで `/etc/modprobe.conf.local` ファイルを開きます。
- 2 このファイルに DCCP 行が表示されていることを確認します。

```
install dccp/bin/true
install dccp_ipv4/bin/true
install dccp_ipv6/bin/true
```

- 3 ファイルを保存し、終了します。

ネットワーク ブリッジのセキュリティ保護

ネットワーク ブリッジ モジュールがデフォルトでシステムにロードされないようにします。潜在的な攻撃者がこのモジュールを悪用してシステムに侵入する可能性があります。

本当に必要ない限り、ネットワーク ブリッジ モジュールがロードされないようにシステムを構成します。潜在的な攻撃者がネットワーク パーティションおよびセキュリティをバイパスすることでこのモジュールを悪用する可能性があります。

手順

- 1 すべての VMware アプライアンス ホスト マシンで次のコマンドを実行します。

```
# rmmod bridge
```

- 2 テキスト エディタで `/etc/modprobe.conf.local` ファイルを開きます。
- 3 このファイルに次の行が表示されていることを確認します。

```
install bridge /bin/false
```

- 4 ファイルを保存し、終了します。

Reliable Datagram Socket プロトコルのセキュリティ保護

システムのセキュリティ強化策の一環として、Reliable Datagram Socket プロトコル (RDS) がデフォルトで仮想アプライアンス ホスト マシンにロードされないようにします。潜在的な攻撃者がこのプロトコルを悪用してシステムに侵入する可能性があります。

Reliable Datagram Socket (RDS) プロトコルをネットワーク スタックにバインドすると、ホストの攻撃対象が増えます。ローカル プロセスに権限を付与しないと、システムがソケットを開くプロトコルを使用してプロトコル ハンドラを動的にロードする可能性があります。

手順

- 1 テキスト エディタで `/etc/modprobe.conf.local` ファイルを開きます。
- 2 このファイルに `install rds /bin/true` 行が表示されていることを確認します。

- 3 ファイルを保存し、終了します。

Transparent Inter-process Communication プロトコルのセキュリティ保護

システムのセキュリティ強化策の一環として、Transparent Inter-Process Communication (TIPC) プロトコルがデフォルトで仮想アプライアンス ホスト マシンにロードされないようにします。潜在的な攻撃者がこのプロトコルを悪用してシステムに侵入する可能性があります。

Transparent Inter-Process Communications (TIPC) プロトコルをネットワーク スタックにバインドすると、ホストの攻撃対象が増えます。ローカル プロセスに権限を付与しないと、カーネルがソケットを開くプロトコルを使用してプロトコル ハンドラを動的にロードする可能性があります。

手順

- 1 テキスト エディタで `/etc/modprobe.conf.local` ファイルを開きます。
- 2 このファイルに `install tipc /bin/true` 行が表示されていることを確認します。
- 3 ファイルを保存し、終了します。

Internetwork Packet Exchange プロトコルのセキュリティ保護

Internetwork Packet Exchange (IPX) プロトコルがデフォルトでシステムにロードされないようにします。潜在的な攻撃者がこのプロトコルを悪用してシステムに侵入する可能性があります。

本当に必要ない限りは、Internetwork Packet Exchange (IPX) プロトコル モジュールをロードしないでください。IPX プロトコルは廃止されたネットワーク レイヤー プロトコルです。このプロトコルをネットワーク スタックにバインドすると、ホストの攻撃対象が増えます。ローカル プロセスに権限を付与しないと、システムがソケットを開くプロトコルを使用してプロトコル ハンドラを動的にロードする可能性があります。

手順

- 1 テキスト エディタで `/etc/modprobe.conf.local` ファイルを開きます。
- 2 このファイルに次の行が表示されていることを確認します。

```
install ipx /bin/true
```

- 3 ファイルを保存し、終了します。

Appletalk プロトコルのセキュリティ保護

Appletalk プロトコルがデフォルトでシステムにロードされないようにします。潜在的な攻撃者がこのプロトコルを悪用してシステムに侵入する可能性があります。

本当に必要ない限りは、Appletalk プロトコル モジュールをロードしないでください。このプロトコルをネットワーク スタックにバインドすると、ホストの攻撃対象が増えます。ローカル プロセスに権限を付与しないと、システムがソケットを開くプロトコルを使用してプロトコル ハンドラを動的にロードする可能性があります。

手順

- 1 テキスト エディタで `/etc/modprobe.conf.local` ファイルを開きます。

- 2 このファイルに次の行が表示されていることを確認します。

```
install appletalk /bin/true
```

- 3 ファイルを保存し、終了します。

DECnet プロトコルのセキュリティ保護

DECnet プロトコルがデフォルトでシステムにロードされないようにします。潜在的な攻撃者がこのプロトコルを悪用してシステムに侵入する可能性があります。

本当に必要ない限りは、DECnet プロトコル モジュールをロードしないでください。このプロトコルをネットワークスタックにバインドすると、ホストの攻撃対象が増えます。ローカル プロセスに権限を付与しないと、システムがソケットを開くプロトコルを使用してプロトコル ハンドラを動的にロードする可能性があります。

手順

- 1 テキスト エディタで **/etc/modprobe.conf.local** ファイルを開きます。
- 2 このファイルに次の行が表示されていることを確認します。

```
install decnet /bin/true
```

- 3 ファイルを保存し、終了します。

Firewire モジュールのセキュリティ保護

Firewire モジュールがデフォルトでシステムにロードされないようにします。潜在的な攻撃者がこのプロトコルを悪用してシステムに侵入する可能性があります。

本当に必要ない限りは、Firewire モジュールをロードしないでください。

手順

- 1 テキスト エディタで **/etc/modprobe.conf.local** ファイルを開きます。
- 2 このファイルに次の行が表示されていることを確認します。

```
install ieee1394 /bin/true
```

- 3 ファイルを保存し、終了します。

Infrastructure as a Service (IaaS) コンポーネントのセキュリティ保護

システムをセキュリティ強化する場合は、vRealize Automation IaaS コンポーネントとそのホスト マシンをセキュリティ保護し、潜在的な攻撃者が悪用できないようにします。

vRealize Automation IaaS コンポーネントとそのコンポーネントが格納されているホストのセキュリティ設定を構成する必要があります。他の関連コンポーネントとアプリケーションの構成を設定または確認する必要があります。場合によっては、既存の設定を確認できます。他の場合には、適切な構成になるように設定を変更または追加する必要があります。

Windows Time サービスを無効にする

セキュリティのベスト プラクティスとして、vRealize Automation 本番環境では、ホストの時刻同期ではなく、認証されたタイム サーバを使用します。

本番環境では、ホストの時刻同期を無効にし、認証されたタイム サーバを使用して、監査とログを通じたユーザー アクションの正確な追跡および潜在的な悪意のある攻撃と侵入の特定をサポートします。

転送中の Infrastructure as a Service (IaaS) データの TLS の構成

IaaS コンポーネントの転送チャネルをセキュリティ保護するために、vRealize Automation デプロイで強力な TLS プロトコルを使用していることを確認します。

Secure Sockets Layer (SSL) や、より新しく開発された Transport Layer Security (TLS) は、異なるシステム コンポーネント間のネットワーク通信中にシステムのセキュリティを確保するために役立つ暗号プロトコルです。SSL はより古い標準であるため、その実装の多くは、潜在的な攻撃に対して適切なセキュリティを提供できなくなっています。SSLv2 および SSLv3 を含む、以前の SSL プロトコルには、重大な脆弱性が見つかっています。これらのプロトコルは、もう安全であるとは認識されません。

組織のセキュリティ ポリシーによっては、TLS 1.0 も無効にする必要がある場合があります。

注: ロード バランサで TLS を終了する場合は、SSLv2 や SSLv3 などの強力でないプロトコルに加えて、必要に応じて TLS 1.0 も無効にします。

Internet Information Services で SSLv3 を無効にする

セキュリティのベスト プラクティスとして、Infrastructure as a Service (IaaS) ホスト サーバ マシンの Internet Information Services (IIS) では、SSLv3 を無効にします。

手順

- 1 管理者として Windows レジストリ エディタを実行します。
- 2 レジストリ ウィンドウで
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\` に移動します。
- 3 [Protocols] を右クリックし、[新規] - [キー] の順に選択します。
- 4 **SSL 3.0** と入力します。
- 5 ナビゲーション ツリーで、新しく作成した [SSL 3.0] キーを右クリックし、ポップアップ メニューで [新規] - [キー] の順に選択して **Client** と入力します。
- 6 ナビゲーション ツリーで、新しく作成した [SSL 3.0] キーを右クリックし、ポップアップ メニューで [新規] - [キー] の順に選択して **Server** と入力します。
- 7 ナビゲーション ツリーで、SSL 3.0 の下の [Client] を右クリックし、[新規] - [DWORD (32 ビット) 値] の順に選択して、**DisabledByDefault** と入力します。
- 8 ナビゲーション ツリーの SSL 3.0 の下の [Client] を選択し、右側のペインで [DisabledByDefault] をダブルクリックして **1** と入力します。

- 9 ナビゲーション ツリーで、SSL 3.0 の下の [Server] を右クリックし、[新規] - [DWORD (32 ビット) 値] の順に選択して **Enabled** と入力します。
- 10 ナビゲーション ツリーで、SSL 3.0 の下の [Server] を選択し、右側のペインで有効になっている [DWORD] をダブルクリックして **0** と入力します。
- 11 Windows Server を再起動します。

laaS の TLS 1.0 を無効にする

最大限のセキュリティを提供するには、プールを使用するように laaS を構成して TLS 1.0 を無効にします。

詳細については、<https://support.microsoft.com/en-us/kb/245030> の Microsoft ナレッジベースの記事を参照してください。

手順

- 1 Web ソケットの代わりにプールを使用するように laaS を構成します。
 - a <appSettings> セクションに次の値を追加することで、Manager Service 構成ファイル (C:\Program Files (x86)\VMware\VCAC\Server\ManagerService.exe.config) を更新します。


```
<add key="Extensibility.Client.RetrievalMethod" value="Polling"/>
<add key="Extensibility.Client.PollingInterval" value="2000"/>
<add key="Extensibility.Client.PollingMaxEvents" value="128"/>
```
 - b Manager Service (VMware vCloud Automation Center Service) を再起動します。
- 2 laaS サーバで TLS 1.0 が無効になっていることを確認します。
 - a 管理者として、レジストリ エディタを実行します。
 - b レジストリ ウィンドウで、
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\ に移動します。
 - c Protocols を右クリックし、[新規] - [キー] の順に選択して **TLS 1.0** と入力します。
 - d ナビゲーション ツリーで、新しく作成した TLS 1.0 キーを右クリックし、ポップアップ メニューで [新規] - [キー] の順に選択して **Client** と入力します。
 - e ナビゲーション ツリーで、新しく作成した TLS 1.0 キーを右クリックし、ポップアップ メニューで [新規] - [キー] の順に選択して **Server** と入力します。
 - f ナビゲーション ツリーで、TLS 1.0 の下の [Client] を右クリックし、[新規] - [DWORD (32 ビット) 値] の順にクリックして、**DisabledByDefault** と入力します。
 - g ナビゲーション ツリーの TLS 1.0 の下の [Client] を選択し、右側のペインで [DisabledByDefault] の DWORD をダブルクリックして **1** と入力します。
 - h ナビゲーション ツリーで、TLS 1.0 の下の [Server] を右クリックし、[新規] - [DWORD (32 ビット) 値] の順に選択して **Enabled** と入力します。

- i ナビゲーション ツリーの TLS 1.0 の下の [Server] を選択し、右側のペインで [Enabled] の DWORD をダブルクリックして **0** と入力します。
- j Windows Server を再起動します。

TLS 暗号スイートの構成

セキュリティを最大限高めるには、強力な暗号を使用するように vRealize Automation コンポーネントを設定する必要があります。サーバとブラウザの間でネゴシエートされる暗号化により、TLS セッションで使用される暗号化の強度が決まります。強力な暗号のみが確実に選択されるようにするため、vRealize Automation コンポーネントで強度の弱い暗号を無効にします。強力な暗号のみをサポートし、十分に大きいキー サイズを使用するように、サーバを設定します。また、適切な順序ですべての暗号を構成します。

使用できない暗号スイート

NULL 暗号スイート、aNULL、または eNULL などの認証を提供しない暗号スイートを無効にします。この他に、匿名の Diffie-Hellman キー交換 (ADH)、エクスポート レベルの暗号 (EXP、DES を含んでいる暗号)、ペイロードトラフィックの暗号化に対する 128 ビットより小さいサイズのキー、ペイロードトラフィックのハッシュメカニズムとしての MD5 の使用、IDEA 暗号スイート、および RC4 暗号スイートも無効にします。また、Diffie-Hellman (DHE) キー交換を使用する暗号スイートが無効になっていることを確認します。

ホスト サーバのセキュリティの確認

セキュリティのベスト プラクティスとして、Infrastructure as a Service (IaaS) ホスト サーバマシンのセキュリティ構成を確認します。

Microsoft は、ホスト サーバマシンのセキュリティの確認に役立ついくつかのツールを提供しています。これらのツールの適切な使用方法については、Microsoft の担当者にお問い合わせください。

ホスト サーバのセキュアなベースラインの確認

Microsoft Baseline Security Analyzer (MBSA) を実行すると、サーバに最新の更新またはホット フィックスが適用されていることを簡単に確認できます。MBSA を使用すると、未適用の Microsoft のセキュリティ パッチをインストールし、Microsoft のセキュリティ推奨事項に関してサーバを最新の状態に維持することができます。

Microsoft の Web サイトから最新版の MBSA ツールをダウンロードします。

ホスト サーバのセキュリティ構成の確認

Windows セキュリティの構成ウィザード (SCW) および Microsoft Security Compliance Manager (SCM) ツールキットを使用して、ホスト サーバが安全に構成されていることを確認します。

Windows サーバの管理ツールから SCW を実行します。このツールにより、サーバのロールと、ネットワーク、Windows ファイアウォール、レジストリ設定などのインストールされている機能を特定できます。Windows サーバに関連する SCM の最新のセキュリティ強化ガイダンスとこのレポートを比較します。結果に基づいて、ネットワーク サービス、アカウント設定、および Windows ファイアウォールなど、各機能のセキュリティ設定を調整して、この設定をサーバに適用します。

SCW ツールの詳細については、Microsoft Technet の Web サイトを参照してください。

アプリケーション リソースの保護

セキュリティのベスト プラクティスとして、関連するすべての Infrastructure as a Service (IaaS) ファイルに適切な権限があることを確認します。

IaaS ファイルを IaaS インストールと突き合わせて確認します。ほとんどの場合、すべてのフォルダのサブフォルダとファイルはフォルダと同じ設定にする必要があります。

| ディレクトリまたはファイル | グループまたはユーザー | 読み取りおよび実行 | | | | |
|--|-------------|-----------|----|------|------|---|
| | | 完全制御 | 変更 | 読み取り | 書き込み | |
| VMware\vCAC\Agents\<agent_name>\logs | システム | X | X | X | X | X |
| | 管理者 | X | X | X | X | X |
| | 管理者 | X | X | X | X | X |
| VMware\vCAC\Agents\<agent_name>\temp | システム | X | X | X | X | X |
| | 管理者 | X | X | X | X | X |
| | 管理者 | X | X | X | X | X |
| VMware\vCAC\Agents\ | システム | X | X | X | X | X |
| | 管理者 | X | X | X | X | X |
| | ユーザー | | | X | X | |
| VMware\vCAC\Distributed Execution Manager\ | システム | X | X | X | X | X |
| | 管理者 | X | X | X | X | X |
| | ユーザー | | | X | X | |
| VMware\vCAC\Distributed Execution Manager\DEM\Logs | システム | X | X | X | X | X |
| | 管理者 | X | X | X | X | X |
| | 管理者 | X | X | X | X | X |
| VMware\vCAC\Distributed Execution Manager\DEO\Logs | システム | X | X | X | X | X |
| | 管理者 | X | X | X | X | X |
| | 管理者 | X | X | X | X | X |
| VMware\vCAC\Management Agent\ | システム | X | X | X | X | X |
| | 管理者 | X | X | X | X | X |
| | ユーザー | | | X | X | |
| VMware\vCAC\Server\ | システム | X | X | X | X | X |
| | 管理者 | X | X | X | X | X |
| | ユーザー | | | X | X | |
| VMware\vCAC\Web API | システム | X | X | X | X | X |
| | 管理者 | X | X | X | X | X |
| | ユーザー | | | X | X | |

Infrastructure as a Service (IaaS) ホスト マシンのセキュリティ保護

セキュリティのベスト プラクティスとして、IaaS ホスト マシンの基本設定を見直して、セキュリティ ガイドラインに準拠していることを確認します。

IaaS ホスト マシンのアカウント、アプリケーション、ポート、およびサービスなどを保護します。

サーバ ユーザー アカウントの設定の確認

不要なローカル ユーザーおよびドメイン ユーザーのアカウントや設定がないことを確認します。アプリケーションの機能に関連していないユーザー アカウントを制限し、管理、メンテナンス、およびトラブルシューティングのために必要なものだけにします。ドメイン ユーザー アカウントからのリモート アクセスを、サーバの保守に必要な最低限のものに制限します。これらのアカウントを厳密に制御して監査します。

不要なアプリケーションの削除

ホスト サーバからすべての不要なアプリケーションを削除します。不要なアプリケーションがあることで、十分な対策が取られていない未知の脆弱性を原因とする漏洩のリスクが増大します。

不要なポートおよびサービスを無効にする

開いているポートのリストについて、ホスト サーバのファイアウォールを確認します。IaaS コンポーネントまたは重大なシステム操作に必要なではないすべてのポートをブロックします。[「ポートおよびプロトコルの構成」](#) を参照してください。ホスト サーバに対して実行中のサービスを監査し、不要なものを無効にします。

ホストのネットワーク セキュリティの構成

既知のセキュリティ脅威に対する最大限の保護を提供するために、すべての VMware ホスト マシンでネットワーク インターフェイスと通信設定を構成します。

包括的なセキュリティ プランの一環として、確立されているセキュリティ ガイドラインに従って、VMware 仮想アプライアンスと Infrastructure as a Service (IaaS) コンポーネントのネットワーク インターフェイスのセキュリティ設定を構成します。

VMware アプライアンスのネットワーク設定の構成

VMware 仮想アプライアンス ホスト マシンで、安全で不可欠な通信のみが確実にサポートされるようにするために、それらのマシンのネットワーク通信設定を確認して編集します。

VMware ホスト マシンのネットワークの IP プロトコル構成を確認し、セキュリティのガイドラインに従ってネットワークの設定を構成します。すべての必須でない通信プロトコルを無効にします。

ネットワーク インターフェイスのユーザーによるコントロールの制限

セキュリティのベスト プラクティスとして、ユーザーには VMware アプライアンス ホスト マシンでジョブを実行するために必要なシステム権限のみを許可します。

ネットワーク インターフェイスを操作する権限をユーザー アカウントに許可すると、ネットワーク セキュリティ メカニズムをバイパスしたり、サービス拒否が発生したりすることがあります。許可されたユーザーだけがネットワーク インターフェイス設定を変更できるようにします。

手順

- 1 各 VMware アプライアンス ホスト マシンで、次のコマンドを実行します。

```
# grep -i '^USERCONTROL=' /etc/sysconfig/network/ifcfg*
```

- 2 各インターフェイスが **N0** に設定されていることを確認します。

TCP バックログのキュー サイズの設定

悪意のある攻撃に対して一定レベルの防御を実現するには、VMware アプライアンス ホスト マシンでデフォルトの TCP バックログのキュー サイズを構成します。

TCP のサービス拒否攻撃を軽減するために、TCP バックログのキュー サイズを適切なデフォルト サイズに設定します。推奨デフォルト設定は 1280 です。

手順

- 1 各 VMware アプライアンス ホスト マシンで次のコマンドを実行します。

```
# cat /proc/sys/net/ipv4/tcp_max_syn_backlog
```

- 2 テキスト エディタで **/etc/sysctl.conf** ファイルを開きます。
- 3 次のエントリをファイルに追加することで、デフォルトの TCP バックログのキュー サイズを設定します。

```
net.ipv4.tcp_max_syn_backlog=1280
```

- 4 変更内容を保存し、ファイルを閉じます。

ブロードキャスト アドレスへの ICMPv4 エコーの拒否

セキュリティのベスト プラクティスとして、VMware アプライアンス ホスト マシンが ICMP ブロードキャスト アドレスのエコー要求を無視することを確認します。

ブロードキャスト Internet Control Message Protocol (ICMP) エコーへの応答は、増幅攻撃に対する攻撃ベクトルを提供し、悪意のあるエージェントによるネットワーク マッピングの利用を容易にする恐れがあります。ICMPv4 エコーを無視するようにアプライアンス ホスト マシンを構成することで、このような攻撃に対する保護を提供します。

手順

- 1 IPv4 ブロードキャスト アドレスのエコー要求を拒否することを確認するために、VMware 仮想アプライアンス ホスト マシンで **# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts** コマンドを実行します。

IPv4 リダイレクトを拒否するようにホスト マシンが構成されている場合、このコマンドは **/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts** に対して 0 の値を返します。

- 2 ICMPv4 ブロードキャスト アドレスのエコー要求を拒否するように仮想アプライアンス ホスト マシンを構成するには、Windows ホスト マシンで、**/etc/sysctl.conf** ファイルをテキスト エディタで開きます。
- 3 **net.ipv4.icmp_echo_ignore_broadcasts=0** というエントリを探します。このエントリの値がゼロに設定されていない場合、またはエントリがない場合は、追加するか、既存のエントリを更新します。
- 4 変更内容を保存し、ファイルを閉じます。

IPv4 プロキシ ARP を無効にする

VMware アプライアンス ホスト マシンで別途必要のない限り、IPv4 プロキシ ARP が無効になっていることを確認して不正な情報共有を防ぎます。

IPv4 プロキシ ARP を使用すると、別のインターフェイスに接続されているホストの代わりに、特定のインターフェイスの ARP 要求にシステムから応答を送信できます。接続されているネットワーク セグメント間でアドレス情報の漏えいを防ぐため、必要でない場合は無効にします。

手順

- 1 IPv4 プロキシ ARP が無効になっていることを確認するために、VMware 仮想アプライアンス ホスト マシンで **# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp | egrep "default|all"** コマンドを実行します。

ホスト マシンで IPv6 プロキシ ARP が無効になっている場合、このコマンドは 0 の値を返します。

```
/proc/sys/net/ipv4/conf/all/proxy_arp:0
/proc/sys/net/ipv4/conf/default/proxy_arp:0
```

ホスト マシンが正しく構成されている場合は、これ以上の操作は必要ありません。

- 2 ホスト マシンで IPv6 プロキシ ARP を構成する必要がある場合は、**/etc/sysctl.conf** ファイルをテキストエディタで開きます。
- 3 次のエントリを確認します。

```
net.ipv4.conf.default.proxy_arp=0
net.ipv4.conf.all.proxy_arp=0
```

エントリがない場合、またはそれらの値がゼロに設定されていない場合は、エントリを追加するか、既存のエントリを更新します。

- 4 変更内容を保存し、ファイルを閉じます。

IPv4 ICMP リダイレクト メッセージの拒否

セキュリティのベスト プラクティスとして、VMware 仮想アプライアンス ホスト マシンが、IPv4 ICMP リダイレクト メッセージを拒否することを確認します。

ルーターでは、ICMP リダイレクト メッセージを使用して、ターゲットに対するより直接的なルートがあることをホストに通知します。悪意のある ICMP リダイレクト メッセージによって、中間者攻撃が行われる恐れがあります。これらのメッセージは、ホストのルート テーブルを変更することで、認証されない状態になります。システムで必要な場合を除いて、これらのメッセージを無視するようにシステムが構成されていることを確認します。

手順

- 1 IPv4 リダイレクト メッセージを拒否することを確認するために、VMware アプライアンス ホスト マシンで **# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects | egrep "default|all"** コマンドを実行します。

IPv4 リダイレクトを拒否するようにホスト マシンが構成されている場合、このコマンドは次を返します。

```
/proc/sys/net/ipv4/conf/all/accept_redirects:0
```

```
/proc/sys/net/ipv4/conf/default/accept_redirects:0
```

- 2 IPv4 リダイレクト メッセージを拒否するように仮想アプライアンス ホスト マシンを構成する必要がある場合には、テキスト エディタで **/etc/sysctl.conf** ファイルを開きます。

- 3 **net.ipv4.conf** で始まる行の値を確認します。

次のエントリの値がゼロに設定されていない場合、またはこれらのエントリがない場合は、ファイルに追加するか既存のエントリを更新します。

```
net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.default.accept_redirects=0
```

- 4 変更内容を保存し、ファイルを閉じます。

IPv6 ICMP リダイレクト メッセージの拒否

セキュリティのベスト プラクティスとして、VMware 仮想アプライアンス ホスト マシンが IPv6 ICMP リダイレクト メッセージを拒否することを確認します。

ルーターでは、ICMP リダイレクト メッセージを使用して、ターゲットに対するより直接的なルートがあることをホストに通知します。悪意のある ICMP リダイレクト メッセージによって、中間者攻撃が行われる恐れがあります。これらのメッセージは、ホストのルート テーブルを変更することで、認証されない状態になります。必要な場合を除き、これらを見捨てるようにシステムが構成されていることを確認します。

手順

- 1 IPv6 リダイレクト メッセージを拒否することを確認するために、VMware 仮想アプライアンス ホスト マシンで **# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects | egrep "default|all"** コマンドを実行します。

ホスト マシンが IPv6 リダイレクトを拒否するように構成されている場合、このコマンドは次を返します。

```
/proc/sys/net/ipv6/conf/all/accept_redirects:0
```

```
/proc/sys/net/ipv6/conf/default/accept_redirects:0
```

- 2 IPv6 リダイレクト メッセージを拒否するように仮想アプライアンス ホスト マシンを構成するには、テキスト エディタで **/etc/sysctl.conf** ファイルを開きます。

- 3 **net.ipv6.conf** で始まる行の値を確認します。

次のエントリの値がゼロに設定されていない場合、またはこれらのエントリがない場合は、ファイルに追加するか既存のエントリを更新します。

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

- 4 変更内容を保存し、ファイルを閉じます。

IPv4 Martian パケットのログ

セキュリティのベスト プラクティスとして、VMware 仮想アプライアンス ホスト マシンが IPv4 Martian パケットをログに記録することを確認します。

Martian パケットには、無効になるとシステムが認識しているアドレスが含まれています。これらのメッセージをログに記録し、不適切な構成や進行中の攻撃を特定できるようにホスト マシンを構成します。

手順

- 1 IPv4 Martian パケットをログ記録していることを確認するために、VMware アプライアンス ホスト マシンで **# grep [01] /proc/sys/net/ipv4/conf/*/log_martians | egrep "default|all"** コマンドを実行します。

Martian パケットをログ記録するように仮想マシンが構成されている場合は、次を返します。

```
/proc/sys/net/ipv4/conf/all/log_martians:1
/proc/sys/net/ipv4/default/log_martians:1
```

ホスト マシンが正しく構成されている場合は、これ以上の操作は必要ありません。

- 2 IPv4 Martian パケットをログ記録するように仮想マシンを構成する必要がある場合は、テキスト エディタで **/etc/sysctl.conf** ファイルを開きます。
- 3 **net.ipv4.conf** で始まる行の値を確認します。

次のエントリの値が 1 に設定されていない場合、またはこれらのエントリがない場合は、ファイルに追加するか既存のエントリを更新します。

```
net.ipv4.conf.all.log_martians=1
net.ipv4.conf.default.log_martians=1
```

- 4 変更内容を保存し、ファイルを閉じます。

IPv4 リバース パス フィルタリングの使用

セキュリティのベスト プラクティスとして、IPv4 リバース パス フィルタリングが VMware 仮想アプライアンス ホスト マシンで使用されていることを確認します。

リバース パス フィルタリングは、ソース アドレスにルートがないパケットや、ソース アドレスのルートが発信元のインターフェイスをポイントしていないパケットがシステムで破棄されるようにすることで、偽装されたソース アドレスに対する保護を行います。可能な限りリバース パス フィルタリングを使用するようにホスト マシンを構成します。システムの役割によっては、リバース パス フィルタリングが、システムで正規のトラフィックが破棄される原因となる場合があります。このような問題が発生する場合、より寛容なモードを使用するか、リバース パス フィルタリングを完全に無効にすることが必要になる可能性があります。

手順

- 1 IPv4 リバース パス フィルタリングを使用していることを確認するために、VMware 仮想アプライアンス ホスト マシンで **# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter|egrep "default|all"** コマンドを実行します。

仮想マシンで IPv4 リバース パス フィルタリングを使用している場合、このコマンドは次を返します。

```
/proc/sys/net/ipv4/conf/all/rp_filter:1
/proc/sys/net/ipv4/conf/default/rp_filter:1
```

仮想マシンが正しく構成されている場合は、これ以上の操作は必要ありません。

- 2 IPv4 リバース パス フィルタリングをホスト マシンに構成する必要がある場合は、テキスト エディタで **/etc/sysctl.conf** ファイルを開きます。
- 3 **net.ipv4.conf** で始まる行の値を確認します。

次のエントリの値が 1 に設定されていない場合、またはこれらのエントリがない場合は、ファイルに追加するか既存のエントリを更新します。

```
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
```

- 4 変更内容を保存し、ファイルを閉じます。

IPv4 転送の拒否

VMware アプライアンス ホスト マシンが IPv4 転送を拒否することを確認します。

システムが IP 転送向けに構成されていて、指定されたルーターではない場合、攻撃者は、このシステムを利用して、ネットワーク デバイスでフィルタされていない通信のパスを提供することでネットワーク セキュリティをバイパスする可能性があります。このリスクを回避するために、IPv4 転送を拒否するように仮想アプライアンス ホスト マシンを構成します。

手順

- 1 IPv4 転送を拒否することを確認するために、VMware アプライアンス ホスト マシンで **# cat /proc/sys/net/ipv4/ip_forward** コマンドを実行します。

IPv4 転送を拒否するようにホスト マシンが構成されている場合、このコマンドは **/proc/sys/net/ipv4/ip_forward** に対して 0 の値を返します。仮想マシンが正しく構成されている場合は、これ以上の操作は必要ありません。

- 2 IPv4 転送を拒否するように仮想アプライアンス ホスト マシンを構成するには、テキスト エディタで **/etc/sysctl.conf** ファイルを開きます。
- 3 **net.ipv4.ip_forward=0** というエントリを探します。このエントリの値がゼロに設定されていない場合、またはエントリがない場合は、追加するか、既存のエントリを更新します。
- 4 変更内容を保存し、ファイルを閉じます。

IPv6 転送の拒否

セキュリティのベスト プラクティスとして、VMware アプライアンスのホストシステムが IPv6 転送を拒否することを確認します。

システムが IP 転送向けに構成されていて、指定されたルーターではない場合、攻撃者は、このシステムを利用して、ネットワーク デバイスでフィルタされていない通信のパスを提供することでネットワーク セキュリティをバイパスする可能性があります。このリスクを回避するために、IPv6 転送を拒否するように仮想アプライアンス ホスト マシンを構成します。

手順

- 1 IPv6 転送を拒否することを確認するために、VMware アプライアンス ホスト マシンで **# grep [01] /proc/sys/net/ipv6/conf/*/forwarding|egrep "default|all"** コマンドを実行します。

IPv6 転送を拒否するようにホスト マシンが構成されている場合、このコマンドは次のように応答します。

```
/proc/sys/net/ipv6/conf/all/forwarding:0
/proc/sys/net/ipv6/conf/default/forwarding:0
```

ホスト マシンが正しく構成されている場合は、これ以上の操作は必要ありません。

- 2 IPv6 転送を拒否するようにホスト マシンを構成する必要がある場合は、**/etc/sysctl.conf** ファイルをテキスト エディタで開きます。
- 3 **net.ipv6.conf** で始まる行の値を確認します。

次のエントリの値がゼロに設定されていない場合、またはこれらのエントリがない場合は、エントリを追加するか既存のエントリを更新します。

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

- 4 変更内容を保存し、ファイルを閉じます。

IPv4 TCP Syncookie の使用

VMware アプライアンス ホスト マシンが IPv4 TCP Syncookie を使用していることを確認します。

TCP SYN フラッド攻撃では、システムの TCP 接続テーブルを SYN_RCVD 状態の接続で満たしてサービス拒否の状態にできる場合があります。Syncookie を使用すると、後続の ACK を受信するまで接続を追跡できないため、インシエータによる接続が有効であり、フラッドソースではないことを確認します。この方法は完全に標準に準拠した方法では動作せず、フラッド状態でのみ作動し、有効な要求を処理しながらシステムを保護できます。

手順

- 1 IPv4 TCP Syncookie を使用していることを確認するために、VMware アプライアンス ホスト マシンで **# cat /proc/sys/net/ipv4/tcp_syncookies** コマンドを実行します。

ホスト マシンが IPv4 転送を拒否するように構成されている場合、**/proc/sys/net/ipv4/tcp_syncookies** コマンドは値 1 を返します。仮想マシンが正しく構成されている場合は、これ以上の操作は必要ありません。

- 2 IPv4 TCP Syncookie を使用するように仮想アプライアンスを構成する必要がある場合は、テキスト エディタで **/etc/sysctl.conf** を開きます。

- 3 **net.ipv4.tcp_syncookies=1** というエントリを探します。

このエントリの値が 1 に現在設定されていない場合、またはこのエントリがない場合は、追加するか、既存のエントリを更新します。

- 4 変更内容を保存し、ファイルを閉じます。

IPv6 ルーター通知の拒否

VMware ホスト マシンが、ルーター通知および ICMP リダイレクトの受け取りを拒否することを確認します（システム操作で必要でない場合）。

IPv6 では、ネットワークからの情報を自動的に使用してシステムがネットワーク デバイスを構成することができます。セキュリティの観点から、重要な構成情報は、認証されていない方法でネットワークから受け入れるよりも、手動で構成することをお勧めします。

手順

- 1 ルーター通知を拒否することを確認するために、VMware アプライアンス ホスト マシンで **# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra | egrep "default|all"** コマンドを実行します。

IPv6 ルーター通知を拒否するようにホスト マシンが構成されている場合、このコマンドは 0 の値を返します。

```
/proc/sys/net/ipv6/conf/all/accept_ra:0
/proc/sys/net/ipv6/conf/default/accept_ra:0
```

ホスト マシンが正しく構成されている場合は、これ以上の操作は必要ありません。

- 2 IPv6 ルーター通知を拒否するようにホスト マシンを構成する必要がある場合は、**/etc/sysctl.conf** ファイルをテキスト エディタで開きます。
- 3 次のエントリを確認します。

```
net.ipv6.conf.all.accept_ra=0
net.ipv6.conf.default.accept_ra=0
```

これらのエントリがない場合、またはそれらの値がゼロに設定されていない場合は、エントリを追加するか、既存のエントリを更新します。

4 変更内容を保存し、ファイルを閉じます。

IPv6 ルーター要請の拒否

セキュリティのベスト プラクティスとして、VMware アプライアンス ホスト マシンが、IPv6 ルーター要請を拒否することを確認します（システム操作で必要でない場合）。

ルーター要請設定は、インターフェイスを構築するときに送信するルーター要請の数を決定します。アドレスが静的に割り当てられる場合は、要請を送信する必要はありません。

手順

- 1 IPv6 ルーター要請を拒否することを確認するために、VMware アプライアンス ホスト マシンで **# grep [01] /proc/sys/net/ipv6/conf/*/router_solicitations | egrep "default|all"** コマンドを実行します。

IPv6 ルーター通知を拒否するようにホスト マシンが構成されている場合、このコマンドは次のように応答します。

```
/proc/sys/net/ipv6/conf/all/router_solicitations:0
/proc/sys/net/ipv6/conf/default/router_solicitations:0
```

ホスト マシンが正しく構成されている場合は、これ以上の操作は必要ありません。

- 2 IPv6 ルーター要請を拒否するようにホスト マシンを構成する必要がある場合は、**/etc/sysctl.conf** ファイルをテキスト エディタで開きます。
- 3 次のエントリを確認します。

```
net.ipv6.conf.all.router_solicitations=0
net.ipv6.conf.default.router_solicitations=0
```

エントリがない場合、またはそれらの値がゼロに設定されていない場合は、エントリを追加するか、既存のエントリを更新します。

4 変更内容を保存し、ファイルを閉じます。

ルーター要請の IPv6 ルーター プリファレンスの拒否

VMware アプライアンス ホスト マシンが、IPv6 ルーター要請を拒否することを確認します（システム操作で必要でない場合）。

要請設定のルーター プリファレンスにより、ルーター プリファレンスが決まります。アドレスが静的に割り当てられる場合は、要請のルーター プリファレンスを受信する必要はありません。

手順

- 1 IPv6 ルーター要請を拒否することを確認するために、VMware アプライアンス ホスト マシンで **# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rtr_pref | egrep "default|all"** コマンドを実行します。

IPv6 ルーター通知を拒否するようにホスト マシンが構成されている場合、このコマンドは次のように応答します。

```
/proc/sys/net/ipv6/conf/all/accept_ra_rtr_pref:0
/proc/sys/net/ipv6/conf/default/accept_ra_rtr_pref:0
```

ホスト マシンが正しく構成されている場合は、これ以上の操作は必要ありません。

- 2 IPv6 ルート要請を拒否するようにホスト マシンを構成する必要がある場合は、**/etc/sysctl.conf** ファイルをテキスト エディタで開きます。
- 3 次のエントリを確認します。

```
net.ipv6.conf.all.accept_ra_rtr_pref=0
net.ipv6.conf.default.accept_ra_rtr_pref=0
```

エントリがない場合、またはそれらの値がゼロに設定されていない場合は、エントリを追加するか、既存のエントリを更新します。

- 4 変更内容を保存し、ファイルを閉じます。

IPv6 ルーター プリフィックスの拒否

VMware アプライアンス ホスト マシンが、IPv6 ルーター プリフィックス情報を拒否することを確認します（システム操作が必要でない場合）。

accept_ra_pinfo 設定により、システムがルーターからプリフィックス情報を受け入れるかどうかが決まります。アドレスが静的に割り当てられる場合は、ルーター プリフィックス情報を受信する必要はありません。

手順

- 1 IPv6 ルーター プリフィックス情報を拒否することを確認するために、VMware アプライアンス ホスト マシンで **# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo | egrep "default|all"** コマンドを実行します。

IPv6 ルーター通知を拒否するようにホスト マシンが構成されている場合、このコマンドは次のように応答します。

```
/proc/sys/net/ipv6/conf/all/accept_ra_pinfo:0
/proc/sys/net/ipv6/conf/default/accept_ra_pinfo:0
```

ホスト マシンが正しく構成されている場合は、これ以上の操作は必要ありません。

- 2 IPv6 ルーター プリフィックス情報を拒否するようにホスト マシンを構成する必要がある場合は、**/etc/sysctl.conf** ファイルをテキスト エディタで開きます。

- 3 次のエントリを確認します。

```
net.ipv6.conf.all.accept_ra_pinfo=0
net.ipv6.conf.default.accept_ra_pinfo=0
```

エントリがない場合、またはそれらの値がゼロに設定されていない場合は、エントリを追加するか、既存のエントリを更新します。

- 4 変更内容を保存し、ファイルを閉じます。

IPv6 ルーター通知のホップ制限設定の拒否

VMware アプライアンス ホスト マシンが、IPv6 ルーターのホップ制限設定を拒否することを確認します（必要がない場合）。

accept_ra_defrtr 設定では、システムがルーター通知からのホップ制限設定を受け入れるかどうかを制御します。これをゼロに設定すると、ルーターは、送信パケットに対するデフォルトの IPv6 ホップ制限を変更できません。

手順

- 1 IPv6 ルーターのホップ制限設定を拒否することを確認するために、VMware アプライアンス ホスト マシンで **# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_defrtr | egrep "default|all"** コマンドを実行します。

IPv6 ルーターのホップ制限設定を拒否するようにホスト マシンが構成されている場合、このコマンドは 0 の値を返します。

```
/proc/sys/net/ipv6/conf/all/accept_ra_defrtr:0
/proc/sys/net/ipv6/conf/default/accept_ra_defrtr:0
```

ホスト マシンが正しく構成されている場合は、これ以上の操作は必要ありません。

- 2 IPv6 ルーターのホップ制限設定を拒否するようにホスト マシンを構成する必要がある場合は、**/etc/sysctl.conf** ファイルをテキスト エディタで開きます。
- 3 次のエントリを確認します。

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

エントリがない場合、またはそれらの値がゼロに設定されていない場合は、エントリを追加するか、既存のエントリを更新します。

- 4 変更内容を保存し、ファイルを閉じます。

IPv6 ルーター通知 Autoconf 設定の拒否

VMware アプライアンス ホスト マシンが、IPv6 ルーターの autoconf 設定を拒否することを確認します（必要がない場合）。

autoconf 設定は、ルーター通知により、システムがインターフェイスにグローバルユニキャストアドレスを割り当てられるかどうかを制御します。

手順

- 1 IPv6 ルーター autoconf 設定を拒否することを確認するために、VMware アプライアンス ホスト マシンで **# grep [01] /proc/sys/net/ipv6/conf/*/autoconf|egrep "default|all"** コマンドを実行します。

IPv6 ルーター autoconf 設定を拒否するようにホスト マシンが構成されている場合、このコマンドは 0 の値を返します。

```
/proc/sys/net/ipv6/conf/all/autoconf:0
/proc/sys/net/ipv6/conf/default/autoconf:0
```

ホスト マシンが正しく構成されている場合は、これ以上の操作は必要ありません。

- 2 IPv6 ルーター autoconf 設定を拒否するようにホスト マシンを構成する必要がある場合は、**/etc/sysctl.conf** ファイルをテキスト エディタで開きます。
- 3 次のエントリを確認します。

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

エントリがない場合、またはそれらの値がゼロに設定されていない場合は、エントリを追加するか、既存のエントリを更新します。

- 4 変更内容を保存し、ファイルを閉じます。

IPv6 近隣要請の拒否

VMware アプライアンス ホスト マシンが、IPv6 近隣要請を拒否することを確認します（必要がない場合）。

dad_transmits 設定は、インターフェイスを構築する際に、目的のアドレスがネットワーク上で確実に一意になるようにするために、アドレス（グローバルおよびリンクローカル）ごとに送信する近隣要請の数を決定します。

手順

- 1 IPv6 近隣要請を拒否することを確認するために、VMware アプライアンス ホスト マシンで **# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits|egrep "default|all"** コマンドを実行します。

IPv6 近隣要請を拒否するようにホスト マシンが構成されている場合、このコマンドは 0 の値を返します。

```
/proc/sys/net/ipv6/conf/all/dad_transmits:0
/proc/sys/net/ipv6/conf/default/dad_transmits:0
```

ホスト マシンが正しく構成されている場合は、これ以上の操作は必要ありません。

- 2 IPv6 近隣要請を拒否するようにホスト マシンを構成する必要がある場合は、**/etc/sysctl.conf** ファイルをテキスト エディタで開きます。

3 次のエントリを確認します。

```
net.ipv6.conf.all.dad_transmits=0
net.ipv6.conf.default.dad_transmits=0
```

エントリがない場合、またはそれらの値がゼロに設定されていない場合は、エントリを追加するか、既存のエントリを更新します。

4 変更内容を保存し、ファイルを閉じます。

IPv6 最大アドレス数の制限

VMware アプライアンス ホスト マシンで IPv6 の最大アドレス数設定がシステムの運用に最小限必要な数に制限されていることを確認します。

最大アドレス数の設定では、各インターフェイスが使用できるグローバルユニキャスト IPv6 アドレスの数を決定します。デフォルトでは 16 ですが、ご使用のシステムに必要な、静的に構成されるグローバルアドレスの正確な数に設定する必要があります。

手順

- 1 VMware アプライアンス ホスト マシンで IPv6 最大アドレス数が適切に制限されていることを確認するために、**# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses | egrep "default|all"** コマンドを実行します。

IPv6 最大アドレス数を制限するようにホストマシンが構成されている場合、このコマンドは 1 の値を返します。

```
/proc/sys/net/ipv6/conf/all/max_addresses:1
/proc/sys/net/ipv6/conf/default/max_addresses:1
```

ホストマシンが正しく構成されている場合は、これ以上の操作は必要ありません。

- 2 ホストマシンで IPv6 最大アドレス数を構成する必要がある場合は、テキストエディタで **/etc/sysctl.conf** ファイルを開きます。
- 3 次のエントリを確認します。

```
net.ipv6.conf.all.max_addresses=1
net.ipv6.conf.default.max_addresses=1
```

エントリがない場合、またはそれらの値が 1 に設定されていない場合は、エントリを追加するか、既存のエントリを更新します。

- 4 変更内容を保存し、ファイルを閉じます。

Infrastructure as a Service (IaaS) ホストのネットワーク設定の構成

セキュリティのベストプラクティスとして、VMware の要件とガイドラインに従って、VMware IaaS コンポーネントのホストマシンのネットワーク通信設定を構成します。

適切なセキュリティで vRealize Automation 機能が完全にサポートされるようにするために、IaaS ホスト マシンのネットワーク構成を設定します。

[「Infrastructure as a Service \(IaaS\) コンポーネントのセキュリティ保護」](#) を参照してください。

ポートおよびプロトコルの構成

セキュリティのベスト プラクティスとして、すべての vRealize Automation アプライアンスとコンポーネントで VMware ガイドラインに従ってポートおよびプロトコルを構成します。

重要なシステム コンポーネントが本番環境で動作する必要がある場合、vRealize Automation コンポーネントの入力ポートと出力ポートを構成します。不要なポートおよびプロトコルをすべて無効にします。[「vRealize Automation リファレンス アーキテクチャ」](#) を参照してください。

必須のユーザー ポート

セキュリティのベスト プラクティスとして、VMware ガイドラインに従って vRealize Automation のユーザー ポートを構成します。

安全なネットワーク上でのみ必要なポートを公開します。

| サーバ | ポート |
|-----------------------------|----------|
| vRealize Automation アプライアンス | 443、8443 |

管理者に必要なポート

セキュリティのベスト プラクティスとして、VMware のガイドラインに従って vRealize Automation の管理者ポートを構成します。

安全なネットワーク上でのみ必要なポートを公開します。

| サーバ | ポート |
|-----------------------------------|------|
| vRealize Application Services サーバ | 5480 |

vRealize Automation アプライアンス ポート

セキュリティのベスト プラクティスとして、VMware の推奨事項に従って vRealize Automation アプライアンスの入出力ポートを構成します。

入力ポート

vRealize Automation アプライアンス に最低限必要な入力ポートを構成します。システム構成に応じてオプションのポートを構成します。

表 1-4. 必要な最小限の入力ポート

| ポート | プロトコル | コメント |
|-----------|-------|--|
| 443 | TCP | vRealize Automation コンソールへのアクセスおよび API 呼び出し。 |
| 8443 | TCP | コンソール プロキシ (VMRC)。 |
| 5480 | TCP | 仮想アプライアンス Web 管理コンソールへのアクセス。 |
| 5488、5489 | TCP | 内部。更新のための vRealize Automation アプライアンスによる使用。 |

表 1-4. 必要な最小限の入力ポート (続き)

| ポート | プロトコル | コメント |
|-------|-------|--|
| 5672 | TCP | RabbitMQ メッセージング。 注: vRealize Automation アプライアンス インスタンスをクラスタ化する場合、状況によっては 4369 と 25672 をオープン ポートに構成する必要があります。 |
| 40002 | TCP | vIDM サービスに必要。HA 構成に追加したときの他の vRealize Automation アプライアンス ノードからのトラフィックを除く、すべての外部トラフィックに対するファイアウォールです。 |

必要に応じて、オプションの入力ポートを構成します。

表 1-5. オプションの入力ポート

| ポート | プロトコル | コメント |
|-----|-------|---|
| 22 | TCP | (オプション) SSH。本番環境で、ポート 22 でリッスンする SSH サービスを無効にして、ポート 22 を閉じます。 |
| 80 | TCP | (オプション) 443 にリダイレクトします。 |

出力ポート

必要な出力ポートを構成します。

表 1-6. 必要な最小限の出力ポート

| ポート | プロトコル | コメント |
|---------------|---------|---|
| 25,587 | TCP、UDP | 出力通知メール送信用の SMTP。 |
| 53 | TCP、UDP | DNS。 |
| 67、68、546、547 | TCP、UDP | DHCP。 |
| 110、995 | TCP、UDP | 入力通知メール受信用の POP。 |
| 143、993 | TCP、UDP | 入力通知メール受信用の IMAP。 |
| 443 | TCP | HTTPS 経由の Infrastructure as a Service (IaaS) Manager Service。 |

必要に応じて、オプションの出力ポートを構成します。

表 1-7. オプションの出力ポート

| ポート | プロトコル | コメント |
|-----|---------|---|
| 80 | TCP | (オプション) ソフトウェア アップデートの取得用。アップデートをダウンロードして個別に適用できます。 |
| 123 | TCP、UDP | (オプション) ホスト時刻を使用する代わりに直接 NTP に接続。 |

Infrastructure as a Service (IaaS) のポート

セキュリティのベスト プラクティスとして、VMware ガイドラインに従って IaaS コンポーネントの入力および出力ポートを構成します。

入力ポート

laaS コンポーネントに必要な最小限の入力ポートを構成します。

表 1-8. 必要な最小限の入力ポート

| コンポーネント | ポート | プロトコル | コメント |
|-----------------|-----|-------|--|
| Manager Service | 443 | TCP | HTTPS 経由の laaS コンポーネントおよび vRealize Automation アプライアンスとの通信。プロキシ エージェントが管理する仮想ホストには、入トラフィック用の TCP ポート 443 も必要です。 |

出力ポート

laaS コンポーネントに必要な最小限の出力ポートを構成します。

表 1-9. 必要な最小限の出力ポート

| コンポーネント | ポート | プロトコル | コメント |
|-------------------------------|------|---------|--|
| すべて | 53 | TCP、UDP | DNS。 |
| すべて | | TCP、UDP | DHCP。 |
| Manager Service | 443 | TCP | HTTPS 経由の vRealize Automation アプライアンスとの通信。 |
| Web サイト | 443 | TCP | HTTPS 経由の Manager Service との通信。 |
| Distributed Execution Manager | 443 | TCP | HTTPS 経由の Manager Service との通信。 |
| プロキシ エージェント | 443 | TCP | HTTPS 経由の Manager Service および仮想化ホストとの通信。 |
| ゲストエージェント | 443 | TCP | HTTPS 経由の Manager Service との通信。 |
| Manager Service、Web サイト | 1433 | TCP | MSSQL。 |

必要な場合は、オプションの出力ポートを構成します。

表 1-10. オプションの出力ポート

| コンポーネント | ポート | プロトコル | コメント |
|---------|-----|---------|---------------|
| すべて | 123 | TCP、UDP | NTP はオプションです。 |

監査とログ

セキュリティのベスト プラクティスとして、VMware の推奨事項に従って監査とログを vRealize Automation システムに設定します。

中央のログ ホストにリモートからログを作成することにより、ログ ファイルを安全に保存できます。中央のホストにログ ファイルを収集すると、単一のツールを使用して環境を監視できます。また、インフラストラクチャ内の複数のエンティティに対して、集計分析や、組織的攻撃などの脅威の証拠の検索を実行できます。セキュリティ保護された中央のログ サーバへのログ記録により、ログの改ざんを防ぐことができ、長期間の監査記録も作成できます。

リモート ログ サーバが安全であることの確認

多くの場合、攻撃者は、ホスト マシンのセキュリティを侵害した後に、ログ ファイルを検索して改ざんすることで痕跡を隠し、発見されることなくシステムをコントロールしようと試みます。リモート ログ サーバを適切にセキュリティ保護することは、ログ改ざんの防止に役立ちます。

認証済み NTP サーバの使用

すべてのホスト マシンが、関連するローカル時間オフセットを含めて同じ相対タイム ソースを使用していることと、その相対タイム ソースを、協定世界時 (UTC) などの承認済みの時間標準に関連付けできることを確認します。統制の取れたアプローチでタイム ソースを扱うことで、関連するログ ファイルを確認するときに、侵入者のアクションを迅速に追跡し、関連付けることができます。時間の設定が正しくないと、ログ ファイルの調査や関連付けを行って攻撃を検出することが難しくなり、監査が不正確になる可能性があります。

少なくとも 3 つの外部タイム ソースの NTP サーバを使用するか、信頼できるネットワーク上にいくつかのローカル NTP サーバを構成し、それらが少なくとも 3 つの外部タイム ソースから順番に時刻を取得するようにします。

vRealize Automation のインストール

vRealize Automation の新規インスタンスをインストールするための手順に従います。

vRealize Automation インストールの概要

vRealize Automation をインストールして、最小限の事前検証 (POC) 環境や、本番のワークロードを処理できるさまざまな規模の分散型エンタープライズ構成をサポートできます。対話型インストールまたはサイレント インストールができます。

インストール後は、設定をカスタマイズし、テナントを構成すると、vRealize Automation が使用できるようになります。これにより、セルフ サービス プロビジョニングやクラウドサービスのライフ サイクル管理に対するアクセス権限がユーザーに付与されます。

vRealize Automation のインストールについて

vRealize Automation のインストールには、ユーザーとの対話レベルが異なるいくつかの方法があります。

インストールするには、vRealize Automation アプライアンスを展開した後、次のオプションのいずれかを使用して実際のインストールを完了します。

- 統合されたブラウザベースのインストール ウィザード
- 個別のブラウザベースのアプライアンス構成、および IaaS サーバ コンポーネントの個別の Windows インストール
- 応答プロパティ ファイルからの入力を受け入れるコマンド ライン ベースのサイレント インストーラ
- JSON 形式の入力を受け入れるインストール REST API

vRealize Suite Lifecycle Manager を使用して vRealize Automation をインストールすることもできます。[vRealize Suite ドキュメント](#)を参照してください。

この vRealize Automation インストールの新機能

vRealize Automation の以前のバージョンをインストールしてある場合は、開始前にこのリリースをインストールすることによる変更を確認してください。

- このリリースでは、vRealize Automation アプライアンスの名前変更プロセスが簡素化されます。[\[vRealize Automation アプライアンス ホスト名の変更\]](#) を参照してください。
- このリリースでは、vRealize Automation アプライアンスがデフォルトで TLS 1.2 を使用します。管理インターフェイスに、既存のエージェントをこのリリースに更新するために必要な、TLS 1.0 および 1.1 を一時的に有効にするためのオプションが含まれています。
- vRealize Automation アプライアンス管理インターフェイスに、パッチをインストールおよび管理するためのページが追加されました。[\[パッチ管理へのアクセス\]](#) を参照してください。
- このリリースでは、VMware Remote Console のデフォルト プロキシ ポートを変更する方法について説明します。[\[VMware Remote Console プロキシ ポートの変更\]](#) を参照してください。
- このリリースでは、インストール ウィザードのいくつかのヘルプのリンク切れが修正されています。

vRealize Automation インストール コンポーネント

一般的な vRealize Automation インストールは、vRealize Automation アプライアンスおよび 1 つ以上の Windows サーバから構成されます。これらは一体となって、vRealize Automation の Infrastructure as a Service (IaaS) を提供します。

vRealize Automation アプライアンス

vRealize Automation アプライアンスは、事前構成された Linux 仮想アプライアンスです。vRealize Automation アプライアンスは、オープン仮想化ファイルとして提供され、vSphere などの既存の仮想インフラストラクチャ上に展開します。

vRealize Automation アプライアンスは、vRealize Automation の中核を成すいくつかの機能を実行します。

- アプライアンスには vRealize Automation 製品ポータルをホストするサーバが含まれています。ユーザーはこのポータルにログインして、セルフサービス プロビジョニングやクラウド サービス管理にアクセスできます。
- アプライアンスはユーザー認証に使用する Single Sign-On (SSO) を管理します。
- アプライアンス サーバは vRealize Automation アプライアンスの設定の管理インターフェイスをホストします。
- アプライアンスには vRealize Automation アプライアンスの内部処理に使用される事前構成済み PostgreSQL データベースが含まれています。

冗長アプライアンスを含む大規模な導入環境では、セカンダリ アプライアンス データベースは高可用性を提供するためのレプリカとして機能します。

- アプライアンスには事前構成された vRealize Orchestrator のインスタンスが含まれています。vRealize Automation は vRealize Orchestrator ワークフローおよびアクションを使用して機能を拡張します。

現在は vRealize Orchestrator の組み込みインスタンスが推奨されています。ただし、古い展開の場合または特別な状況では、vRealize Automation を外部 vRealize Orchestrator に接続することができます。

- アプライアンスには、ダウンロード可能な管理エージェント インストーラが含まれています。
vRealize Automation IaaS を構成するすべての Windows サーバには管理エージェントをインストールする必要があります。

管理エージェントは、IaaS Windows サーバを vRealize Automation アプライアンスに登録し、IaaS コンポーネントのインストールと管理を自動化して、サポートおよびテレメトリ情報を収集します。

Infrastructure as a Service (IaaS)

vRealize Automation IaaS はプライベート、パブリック、またはハイブリッド クラウド インフラストラクチャでモデルおよびプロビジョニング システムと連動する 1 台以上の Windows サーバから構成されます。

1 つ以上の仮想または物理 Windows サーバに vRealize Automation IaaS コンポーネントをインストールします。インストール後は、IaaS の運用が製品インターフェイスの [インフラストラクチャ] タブに表示されます。

IaaS は次のコンポーネントで構成されます。これらのコンポーネントは展開サイズに応じて、一緒にまたは別個にインストール可能です。

Web サーバ

IaaS Web サーバは vRealize Automation 製品インターフェイスにインフラストラクチャ管理およびサービス オペレーティングを提供します。Web サーバ コンポーネントは Manager Service と通信し、Manager Service は Distributed Execution Manager (DEM)、SQL Server データベース、およびエージェントからの更新を提供します。

Model Manager

vRealize Automation ではモデルが使用されるので、外部システムおよびデータベースとの統合が容易になります。モデルにより DEM で使用するビジネス ロジックが実装されます。

Model Manager ではモデル要素の保持、バージョン管理、保護、および配布用のサービスおよびユーティリティが提供されます。Model Manager は IaaS Web サーバのいずれかでホストされ、DEM、SQL Server データベース、および製品インターフェイス Web サイトと通信します。

Manager Service

Manager Service は Windows サービスで、IaaS DEM、SQL Server データベース、エージェント、および SMTP 間の通信を調整します。さらに、Manager Service は、Model Manager を介して Web サーバと通信します。また、すべての IaaS Windows サーバのローカル管理者権限を持つドメイン アカウントによって実行されている必要があります。

Manager Service の自動フェイルオーバーを有効にする場合を除き、IaaS では、一度に 1 台の Windows マシンのみが Manager Service を実行している必要があります。バックアップまたは高可用性のために、追加の Manager Service マシンを導入できますが、バックアップ マシンには、サービスを停止して手動で開始するように構成する手動フェイルオーバー アプローチが必要です。

詳細については、「[Manager Service の自動フェイルオーバーについて](#)」を参照してください。

SQL Server データベース

IaaS では、Microsoft SQL Server データベースを使用して管理するマシンおよび固有の要素とポリシーに関する情報を維持します。ほとんどのユーザーは、インストール時に vRealize Automation を使用してデータベースを作成できます。または、サイト ポリシーに基づいてデータベースを個別に作成できます。

Distributed Execution Manager

laaS DEM コンポーネントはカスタム モデルのビジネス ロジックを実行し、laaS SQL Server データベース、および外部データベースとシステムを操作します。一般的な方法では、アクティブな Manager Service がホストされている laaS Windows サーバに DEM をインストールしますが、これは必須ではありません。

各 DEM インスタンスはワーカーまたは Orchestrator として動作します。このロールは同一サーバまたは個別のサーバにインストールできます。

DEM ワーカー - 1 つの DEM ワーカーは、ワークフローの実行するための 1 つの機能を持ちます。複数の DEM ワーカーを使用するとキャパシティが増加します。DEM ワーカーは、同一サーバまたは個別のサーバにインストールできます。

DEM Orchestrator - 次の監視機能を実行します。

- DEM ワーカーを監視します。ワーカーと Model Manager との接続が停止または失われた場合、DEM Orchestrator はワークフローを別の DEM ワーカーに移動します。
- スケジュール設定された時間にワークフロー インスタンスを作成して、ワークフローのスケジュールを設定します。
- スケジュール設定されたワークフローのインスタンスは、所定の時間に 1 つのみ実行するようにします。
- ワークフローの実行前に前処理をします。前処理には、ワークフローおよびワークフロー実行履歴の作成の前条件の確認が含まれます。

アクティブな DEM Orchestrator には Model Manager ホスト間に安定したネットワーク接続が必要です。複数の DEM Orchestrator が別のサーバに配備された規模の大きい展開では、セカンダリ Orchestrator は、バックアップとして機能します。セカンダリ DEM Orchestrator は、アクティブな DEM Orchestrator を監視し、アクティブな DEM Orchestrator に問題が発生したときに、冗長性とフェイル オーバーを提供します。この種類のフェイルオーバー構成の場合、アクティブな Manager Service ホストにアクティブな DEM Orchestrator をインストールし、スタンバイ Manager Service ホストにセカンダリ DEM Orchestrator をインストールすることを検討します。

エージェント

vRealize Automation laaS はエージェントを使用して外部システムと統合し、vRealize Automation コンポーネント間の情報を管理します。

一般的な方法では、アクティブな Manager Service がホストされている laaS Windows サーバに vRealize Automation エージェントをインストールしますが、これは必須ではありません。複数のエージェントを使用すると容量が増えます。同一サーバまたは個別のサーバにインストールできます。

仮想化プロキシ エージェント

vRealize Automation では、仮想化ホスト上に仮想マシンが作成され、管理されます。仮想化プロキシ エージェントでは、vSphere ESX Server、XenServer、および Hyper-V ホストと、それらにプロビジョニングされた仮想マシンとの間で、コマンドの送信とデータの収集を行います。

仮想化プロキシ エージェントには次の特徴があります。

- 通常、管理対象の仮想化プラットフォームの管理者権限が必要。
- laaS Manager Service と通信する。

- 別個にインストールされ、固有の構成ファイルがある。

ほとんどの vRealize Automation 展開では、vSphere プロキシ エージェントがインストールされます。サイトで使用する仮想化リソースによっては、他のプロキシ エージェントをインストールする場合があります。

仮想デスクトップ統合エージェント

仮想デスクトップ統合 (VDI) PowerShell エージェントを使用して、vRealize Automation を外部仮想デスクトップシステムと統合できます。VDI エージェントには、外部システムの管理者権限が必要です。

Citrix Desktop Delivery Controller (DDC) に XenDesktop を搭載した vRealize Automation でプロビジョニングした仮想マシンを登録できます。DDC を使用すると vRealize Automation から XenDesktop Web インターフェイスにアクセスできます。

外部プロビジョニング統合エージェント

外部プロビジョニング統合 (EPI) PowerShell エージェントを使用して、vRealize Automation で外部システムをマシン プロビジョニング プロセスに統合できます。

たとえば、Citrix Provisioning Server との統合により、オンデマンドのディスク ストリーミングによるマシンのプロビジョニングが可能になります。また、EPI エージェントを使用すると、プロビジョニング プロセス中に追加の手順として Visual Basic スクリプトを実行できます。

EPI エージェントには、操作対象の外部システムの管理者権限が必要です。

Windows Management Instrumentation エージェント

vRealize Automation Windows Management Instrumentation (WMI) エージェントによって、Windows システム情報の監視および制御機能を強化し、一元化された場所からリモート Windows サーバを管理できるようになります。WMI エージェントを使用すると、vRealize Automation で管理する Windows サーバからデータを収集することもできます。

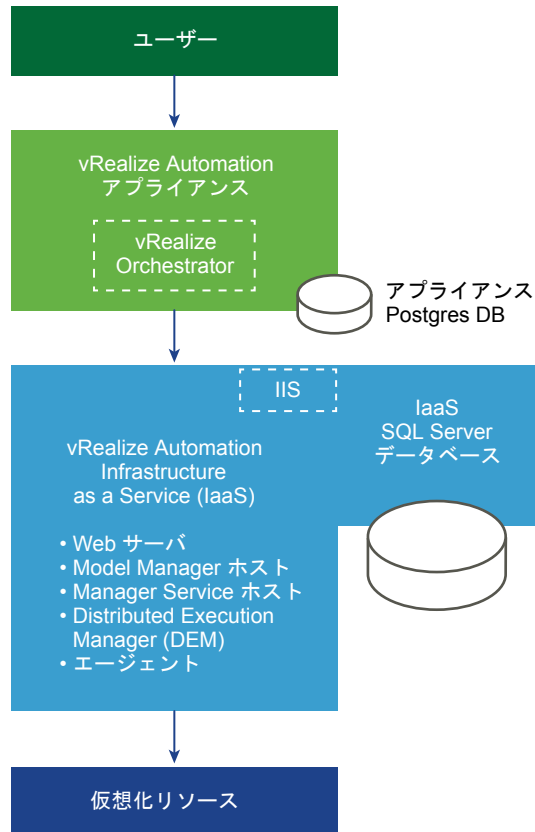
展開の種類

事前検証 (POC) または開発業務用の最小インストールとして vRealize Automation をインストールするか、中規模から大規模の本番環境のワークロードに適した分散構成でインストールできます。

vRealize Automation の最小インストール

最小インストールには、1 つの vRealize Automation アプライアンス、および IaaS コンポーネントをホストする 1 つの Windows サーバが含まれます。最小インストールでは、vRealize Automation SQL Server データベースを IaaS コンポーネントと同じ IaaS Windows サーバに置くことも、別の Windows サーバに置くこともできます。

図 1-10. vRealize Automation の最小インストール



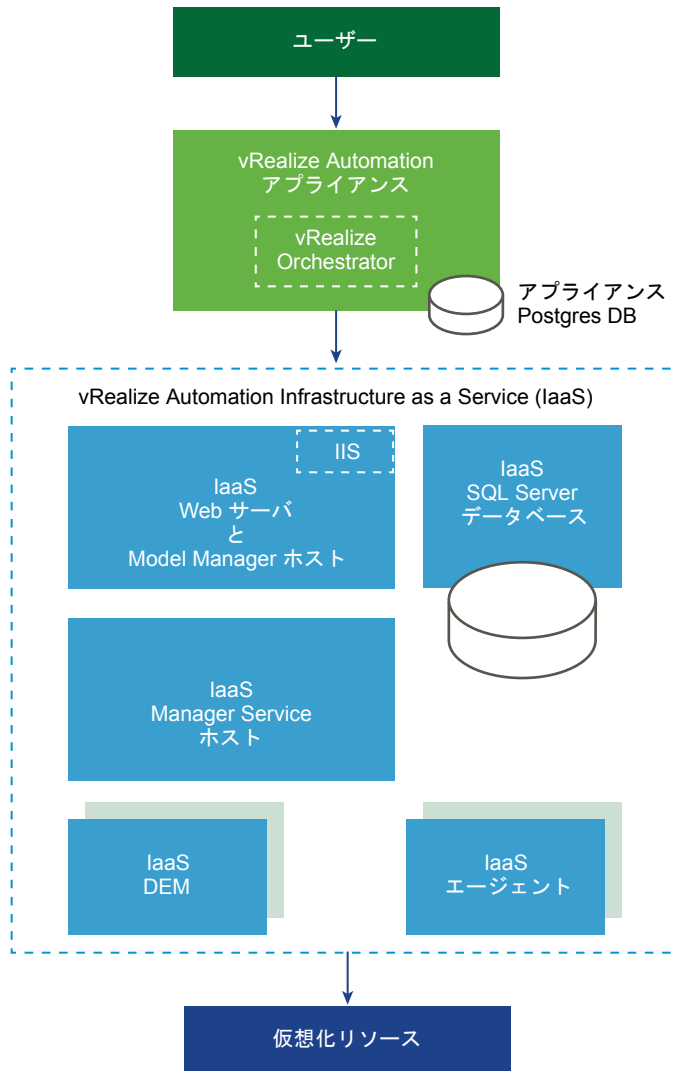
最小インストールは、エンタープライズ インストール環境に変換できません。インストール環境をスケール アップするには、小規模のエンタープライズ環境から開始して、コンポーネントを追加していきます。最小インストールから開始することはできません。

注: vRealize Automation のドキュメントには最小インストール シナリオの完全なサンプルが含まれており、インストール手順および事前検証 (POC) で製品を使用する方法が順を追って説明されています。『Rainpole シナリオの vRealize Automation のインストールおよび構成』を参照してください。

vRealize Automation の分散展開

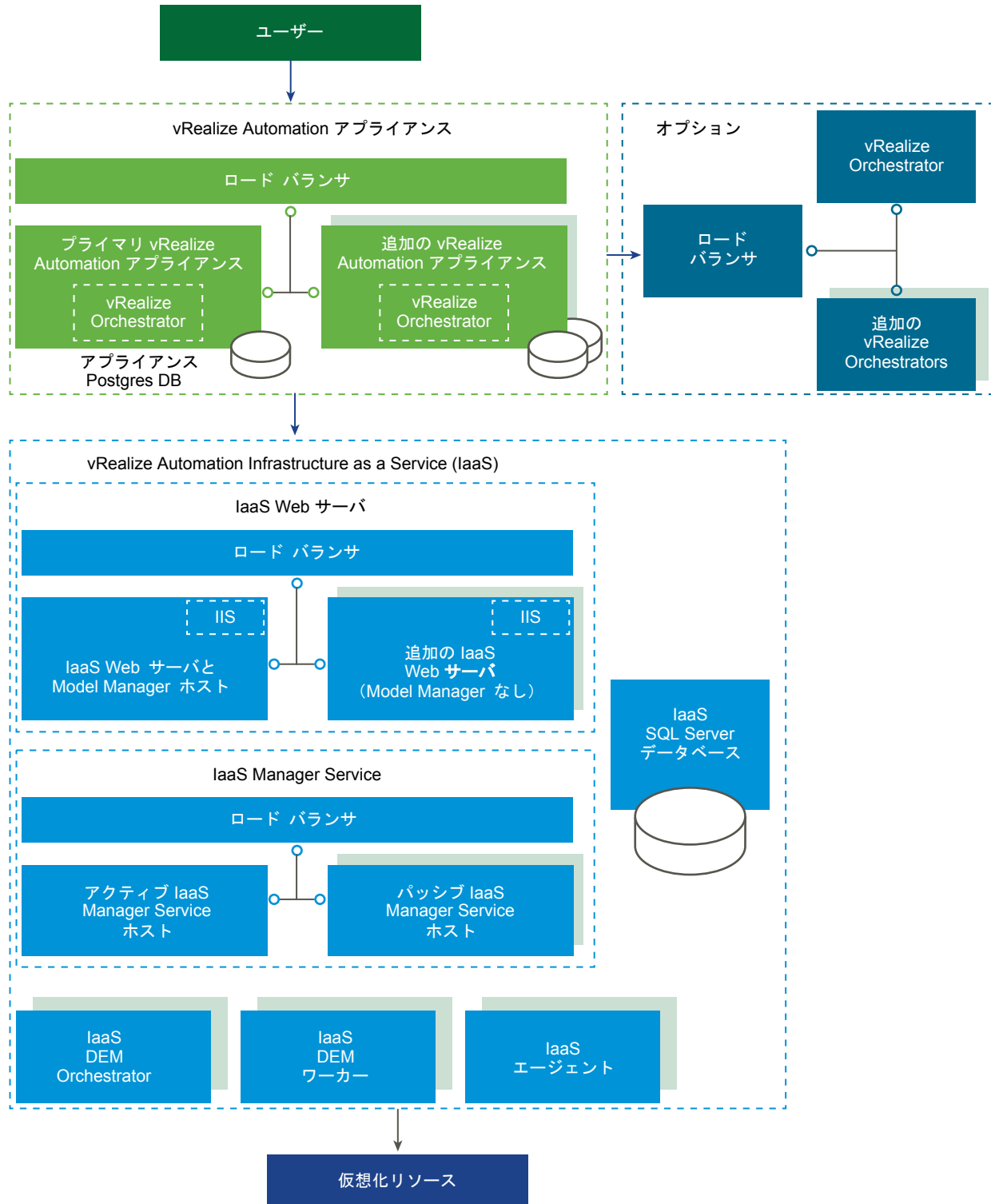
分散エンタープライズ展開はさまざまな規模で実装できます。基本的な分散展開では、次の図に示すように IaaS コンポーネントを個別の Windows サーバでホストするだけで vRealize Automation を強化できる場合があります。

図 1-11. vRealize Automation の分散展開



多くの場合、本番環境への展開では、より多くの容量を確保するために、冗長アプライアンス、冗長サーバ、ロードバランシングが使用されます。大規模な分散展開では、優れたスケーラビリティ、高可用性、ディザスタリカバリが可能になります。vRealize Orchestrator の組み込みインスタンスが現在推奨されていますが、古い環境では vRealize Automation が外部の vRealize Orchestrator に接続されている場合があります。

図 1-12. vRealize Automation の大規模な分散展開と負荷分散展開



スケーラビリティと高可用性については、『vRealize Automation リファレンス アーキテクチャ』ガイドを参照してください。

インストール方法の選択

この統合 vRealize Automation インストール ウィザードは、vRealize Automation を新規インストールする場合の主要なツールです。また、手動で個別にインストールするか、サイレント インストールを実行することもできます。

- 最小インストールから分散したエンタープライズ展開まで、ロード バランサの有無にかかわらず、インストール ウィザードを使用して簡単かつ迅速にインストールを実行できます。ほとんどのユーザーはインストール ウィザードを実行します。
- vRealize Automation 展開を拡張する場合、またはインストール ウィザードが何らかの理由で停止した場合は、手動インストールの手順を実行する必要があります。手動インストールを開始したら、前に戻ってインストール ウィザードを実行することはできません。
- サイトのニーズに合わせて、サイレント、コマンドライン、または API からのインストールそれぞれの利点を活かすことも考えられます。

vRealize Automation のインストールの準備

vRealize Automation は、既存の仮想化インフラストラクチャにインストールします。インストールを開始する前に、いくつかの環境およびシステム要件を整える必要があります。

一般的な準備

vRealize Automation のインストール前に注意が必要な、展開全体に関する考慮事項がいくつかあります。

サポートされているオペレーティングシステムおよびブラウザのバージョンなど、高レベルの環境要件の詳細については、[vRealize Automation のサポート マトリックス](#)を参照してください。

ユーザーの Web ブラウザ

複数のブラウザ ウィンドウおよび複数のタブはサポートされません。vRealize Automation ではユーザーごとに 1 セッションをサポートします。

vSphere 上にプロビジョニングされた VMware Remote Console は、vRealize Automation 対応ブラウザの一部のみをサポートしています。

サードパーティ製ソフトウェア

すべてのサードパーティ製ソフトウェアには、ベンダーが提供する最新のパッチが必要です。サードパーティ製ソフトウェアは、Microsoft Windows、SQL Server などです。

時刻同期

すべての vRealize Automation アプライアンスおよび IaaS Windows サーバは、同じ時間ソースに同期している必要があります。使用できるソースは次のいずれかに限られます。時間ソースを混在させないでください。

- vRealize Automation アプライアンス ホスト
- 単一の外部 NTP サーバ

vRealize Automation アプライアンス ホストを使用するには、ESXi ホストで NTP を実行する必要があります。タイムキーピングの詳細については、[VMware ナレッジベースの記事 KB1318](#) を参照してください。

時間ソースは、インストール ウィザードの [インストールの前提条件] ページで選択します。

アカウントとパスワード

vRealize Automation をインストールする前に、いくつかのユーザー アカウントとパスワードを作成するか、設定を計画する必要があります。

laaS サービス アカウント

laaS では、同一のユーザー アカウントで実行する必要があるいくつかの Windows サービスがインストールされます。

- このアカウントはドメイン ユーザーである必要があります。
- このアカウントは、ドメイン管理者である必要はありませんが、すべての laaS Windows サーバでインストールを開始する前にローカル管理者権限を取得しておく必要があります。
- アカウントのパスワードには、二重引用符 (") 文字を含めることはできません。
- laaS Windows サーバの管理エージェント インストーラでは、アカウントの認証情報が要求されます。
- アカウントには、Manager Service が起動してログ ファイルを生成するために [サービスとしてログオン] 権限が必要です。
- アカウントには、laaS データベースに対する dbo 権限が必要です。

インストーラを使用してデータベースを作成する場合は、インストールを開始する前に、SQL Server へのアカウント ログイン名を追加します。インストーラは、データベースの作成後に dbo 権限を付与します。

- インストーラを使用して SQL でデータベースを作成する場合は、インストールを開始する前に、システム管理者ロールをアカウントに追加します。

システム管理者ロールは、既存の空のデータベースを使用する場合は不要です。

IIS アプリケーション プール ID

Model Manager Web サービスに対して IIS アプリケーション プール ID として使用するアカウントには、[バッチジョブとしてログオンする]権限が必要です。

laaS データベースの認証情報

vRealize Automation インストーラによってデータベースを作成するか、別途 SQL Server を使用して作成します。vRealize Automation インストーラによってデータベースを作成する場合は、次の要件が適用されます。

- vRealize Automation インストーラでは、Windows 認証を選択する場合、プライマリ laaS Web サーバで管理エージェントを実行するアカウントには、データベースの作成とサイズ変更を実行するために SQL のシステム管理者ロールが必要です。
- vRealize Automation インストーラでは、Windows 認証を選択しない場合でも、プライマリ laaS Web サーバで管理エージェントを実行するアカウントには SQL のシステム管理者ロールが必要です。これは、ランタイムにこの認証情報が使用されるためです。

- データベースを別途作成する場合、指定する Windows ユーザーまたは SQL ユーザーの認証情報に必要なのは、データベースに対する dba 権限だけです。

laaS データベースのセキュリティ パスフレーズ

データベースのセキュリティ パスフレーズから、laaS SQL データベースのデータを保護する暗号化キーが生成されます。セキュリティ パスフレーズは、インストール ウィザードの [laaS ホスト] ページで指定します。

- すべてのコンポーネントの暗号化キーが同じになるように、データベースのセキュリティ パスフレーズはインストール全体で同じものを使用してください。
- パスフレーズはメモしておいてください。障害が発生してデータベースをリストアする場合や、初期インストール後にコンポーネントを追加するときにはパスフレーズが必要です。
- データベースのセキュリティ パスフレーズに二重引用符 (") 文字を含めることはできません。作成時には承認されますが、インストールが失敗する原因になります。

vSphere エンドポイント

vSphere エンドポイントをプロビジョニングする場合は、ターゲットに対して操作を実行できる権限を持つドメインアカウントまたはローカル アカウントが必要です。アカウントは、vRealize Orchestrator で適切なレベルの権限が設定されていることも必要です。

vRealize Automation の管理者パスワード

インストール後、vRealize Automation の管理者パスワードによってデフォルト テナントにログインできます。管理者パスワードは、インストール ウィザードの [Single Sign On] ページで指定します。

vRealize Automation の管理者パスワードの末尾に等号 (=) 文字を含めることはできません。パスワードの作成時には承認されますが、あとでエンドポイントの保存などの操作を実行するときにエラーになります。

ホスト名と IP アドレス

vRealize Automation では、一定の要件に従って環境内のホストに名前を付ける必要があります。

- 環境内のすべての vRealize Automation マシンは、完全修飾ドメイン名 (FQDN) による相互解決を行うことができる必要があります。

インストールの実行中、vRealize Automation マシンを特定または選択する際には必ず完全な FQDN を入力します。IP アドレスやマシンの短縮名を入力しないでください。

- この FQDN の要件に加えて、Model Manager Web サービス、Manager Service、および Microsoft SQL Server データベースをホストする Windows マシンは、Windows Internet Name Service (WINS) 名による相互解決を行うことができる必要もあります。

これらの短い WINS のホスト名を解決するためドメイン名システム (DNS) を構成します。

- ドメインおよびマシンの命名について事前に計画し、vRealize Automation マシン名が文字 (a~z、A~Z) で始まり、文字または数字 (0~9) で終わり、その間には文字、数字、またはハイフン (-) のみが使用されるようにします。アンダースコア (_) は、ホスト名や、FQDN のどの部分にも含めないでください。

使用できる名前については、Internet Engineering Task Force (IETF) が提供しているホスト名の仕様を確認してください。 www.ietf.org を参照してください。

- 通常は vRealize Automation システム向けに計画したホスト名と FQDN を変更しません。ホスト名を変更できない場合もあります。変更が可能な場合でも、手順が複雑なことがあります。
- ベスト プラクティスは、すべての vRealize Automation アプライアンスおよび IaaS Windows サーバで固定 IP アドレスを予約して使用することです。vRealize Automation は DHCP をサポートしていますが、本番環境のような長期的な展開では固定 IP アドレスが推奨されます。
 - OVF または OVA 展開時に IP アドレスを vRealize Automation アプライアンスに適用します。
 - IaaS Windows サーバの場合は、通常のオペレーティングシステムの処理に従います。vRealize Automation IaaS をインストールする前に IP アドレスを設定します。

遅延とバンド幅

vRealize Automation では、複数のサイトや分散インストールをサポートしていますが、データ転送速度やボリュームが最小の前提条件を満たす必要があります。

vRealize Automation では、次のコンポーネントに加えて、5 ミリ秒以下のネットワーク遅延、1 GB 以上のバンド幅を備える環境が必要です。

- vRealize Automation アプライアンス
- IaaS Web サーバ
- IaaS Model Manager ホスト
- IaaS Manager Service ホスト
- IaaS SQL Server データベース
- IaaS DEM オーケストレータ

高遅延サイトでは次のコンポーネントも動作する場合がありますが、この構成は推奨されません。

- IaaS DEM ワーカー

通信先のエンドポイントのサイトに、次のコンポーネントをインストールできます。

- IaaS プロキシ エージェント

vRealize Automation アプライアンス

vRealize Automation アプライアンスの要件のほとんどは、展開する OVF または OVA で構成済みです。スタンドアロン、マスター、レプリカの各 vRealize Automation アプライアンスに同じ要件が適用されます。

展開できる最小の仮想マシン ハードウェアは、バージョン 7、または ESX/ESXi 4.x 以降です。『[VMware ナレッジベースの記事 KB2007240](#)』を参照してください。ハードウェア リソースの要求が過大になるため、VMware Workstation には展開しないでください。

展開後に、Active Directory の要件を満たすように vRealize Automation アプライアンスのハードウェア設定を調整するために vSphere を使用する可能性があります。次の表を参照してください。

表 1-11. vRealize Automation アプライアンスの Active Directory 用ハードウェア要件

| 小規模な Active Directory 用の vRealize Automation アプライアンス | 大規模な Active Directory 用の vRealize Automation アプライアンス |
|---|---|
| <ul style="list-style-type: none"> ■ 4 個の CPU ■ 18 GB のメモリ ■ 60 GB のディスク ストレージ | <ul style="list-style-type: none"> ■ 4 個の CPU ■ 22 GB のメモリ ■ 60 GB のディスク ストレージ |

小規模 Active Directory とは、組織単位 (OU) に属する 25,000 人までのユーザーを ID ストア構成で同期する場合です。大規模な Active Directory とは、OU に属するユーザーが 25,000 人を超える場合です。

vRealize Automation アプライアンス ポート

通常、vRealize Automation アプライアンスのポートは、展開する OVF または OVA で構成済みです。

vRealize Automation アプライアンスでは、次のポートが使用されます。

表 1-12. 入力ポート

| ポート | プロトコル | コメント |
|----------------------|-----------------|---|
| 22 | TCP | 任意。SSH セッションのアクセス。 |
| 80 | TCP | 任意。443 ヘリダイレクト。 |
| 88 | TCP (UDP オプション) | 外部モバイル デバイスからのクラウド KDC Kerberos 認証。 |
| 443 | TCP | vRealize Automation コンソールへのアクセスおよび API 呼び出し。 ゲスト エージェントとソフトウェア ブートストラップ エージェントをダウンロードするためのマシンのアクセス。 ロード バランサ、ブラウザのアクセス。 |
| 4369、5671、5672、25672 | TCP | RabbitMQ メッセージング。 |
| 5480 | TCP | 仮想アプライアンス管理インターフェイスへのアクセス。 管理エージェントによる使用。 |
| 5488、5489 | TCP | 更新のための vRealize Automation アプライアンスによる内部使用。 |
| 8230、8280、8281、8283 | TCP | 内部 vRealize Orchestrator インスタンス。 |
| 8443 | TCP | ブラウザのアクセス。HTTPS 経由の Identity Manager 管理者ポート。 |
| 8444 | TCP | vSphere VMware Remote Console 接続のコンソール プロキシ通信。 |
| 9300-9400 | TCP | Identity Manager 監査へのアクセス。 |
| 54328 | UDP | |

表 1-13. 出力ポート

| ポート | プロトコル | コメント |
|---------------|---------|----------------------|
| 25、587 | TCP、UDP | 出力通知 E メール送信用の SMTP。 |
| 53 | TCP、UDP | DNS サーバ。 |
| 67、68、546、547 | TCP、UDP | DHCP。 |

表 1-13. 出力ポート (続き)

| ポート | プロトコル | コメント |
|-------------------|---------|---|
| 80 | TCP | 任意。ソフトウェアアップデートの取得用。アップデートは個別でダウンロードして適用できます。 |
| 88、464、135 | TCP、UDP | ドメイン コントローラ。 |
| 110、995 | TCP、UDP | 入力通知 E メール受信用の POP。 |
| 143、993 | TCP、UDP | 入力通知 E メール受信用の IMAP。 |
| 123 | TCP、UDP | 任意。ホスト時刻を使用する代わりに直接 NTP に接続。 |
| 389 | TCP | View 接続サーバへのアクセス。 |
| 389、636、3268、3269 | TCP | Active Directory。デフォルト ポートが表示されますが、構成可能です。 |
| 443 | TCP | HTTPS 経由の IaaS Manager Service およびインフラストラクチャ エンドポイント ホストとの通信 HTTPS 経由での vRealize Automation ソフトウェア サービスとの通信。 Identity Manager アップグレード サーバへのアクセス。 View 接続サーバへのアクセス。 |
| 445 | TCP | Identity Manager 用 ThinApp リポジトリへのアクセス。 |
| 902 | TCP | ESXi ネットワークのファイル コピー操作および VMware Remote Console の接続。 |
| 5050 | TCP | 任意。vRealize Business for Cloud との通信用。 |
| 5432 | TCP、UDP | 任意。別のアプライアンスの PostgreSQL データベースとの通信用。 |
| 5500 | TCP | RSA SecurID システム。デフォルト ポートが表示されますが、構成可能です。 |
| 8281 | TCP | 任意。外部 vRealize Orchestrator インスタンスとの通信。 |
| 9300-9400 | TCP | Identity Manager 監査へのアクセス。 |
| 54328 | UDP | |

外部システムと通信する特定の vRealize Orchestrator プラグインでは他のポートが必要な場合があります。vRealize Orchestrator プラグインのドキュメントを参照してください。

IaaS Windows サーバ

IaaS コンポーネントをホストするすべての Windows サーバは、一定の要件を満たす必要があります。vRealize Automation インストール ウィザードまたは Windows ベースの標準インストーラを実行する前に、要件に対処してください。

- すべての IaaS Windows サーバを同一のドメインに配置します。ワークグループは使用しないでください。
- 各サーバには、以下の最小ハードウェアが必要です。
 - 2 個の CPU
 - 8 GB のメモリ
 - 40 GB のディスク ストレージ

SQL データベースと IaaS コンポーネントの両方をホストするサーバは、追加のハードウェアを必要とする場合があります。

- ハードウェア リソースの要求が過大になるため、VMware Workstation には展開しないでください。
- Microsoft .NET Framework 3.5 をインストールします。
- Microsoft .NET Framework 4.5.2 以降をインストールします。

.NET は、どの vRealize Automation アプライアンスからも次の URL で入手できます。

<https://<vrealize-automation-appliance-fqdn>:5480/installer/>

ダウンロードに Internet Explorer を使用する場合、セキュリティ強化の構成が無効になっていることを確認します。Windows サーバで <res://iesetup.dll/SoftAdmin.htm> に移動します。

- お使いの Windows のバージョンに基づいて、Microsoft PowerShell 2.0、3.0、または 4.0 をインストールします。
一部の vRealize Automation アップグレードまたは移行では、現在実行している PowerShell のバージョンに加えて、それ以前またはそれ以降のバージョンが必要になる場合があります。
- 複数の IaaS コンポーネントを同じ Windows サーバにインストールする場合は、同じインストール フォルダにインストールするように計画します。異なるパスを使用しないでください。
- IaaS サーバでは、認証に TLS を使用します。これは、一部の Windows サーバでデフォルトで有効です。
一部のサイトでは、セキュリティ上の理由から、TLS が無効ですが、少なくとも 1 つの TLS プロトコルを有効にしておく必要があります。このバージョンの vRealize Automation では、TLS 1.2 をサポートします。
- 分散トランザクション コーディネータ (DTC) サービスを有効にします。IaaS では、データベースのトランザクションや、ワークフロー作成などのアクションを実行するために DTC を使用します。

注: マシンのクローンを作成して IaaS Windows サーバを作成する場合は、クローン作成後、このクローンに DTC をインストールします。DTC が既にインストールされているマシンのクローンを作成した場合、一意の識別子がクローンにコピーされ、通信が失敗します。「[Manager Service 通信のエラー](#)」を参照してください。

DTC が IaaS から切断されている場合は、SQL データベースをホストするサーバで DTC を有効にします。DTC の有効化の詳細については、[VMware ナレッジベースの記事 KB2038943](#) を参照してください。

- セカンダリ ログイン サービスが実行されていることを確認します。このサービスは、必要に応じてインストールの完了後に停止することができます。

IaaS Windows サーバのポート

vRealize Automation をインストールする前に、IaaS Windows サーバのポートを構成する必要があります。

次の表に基づいて、すべての IaaS Windows サーバ間のポートを開きます。SQL データベースをホストするサーバが IaaS と異なる場合は、それも含めます。または、サイト ポリシーで許可される場合は、IaaS Windows サーバと SQL Server 間のファイアウォールを無効にします。

表 1-14. 入力ポート

| ポート | プロトコル | コンポーネント | コメント |
|------|-------|---|---|
| 443 | TCP | Manager Service | HTTPS 経由の IaaS コンポーネントおよび vRealize Automation アプライアンスとの通信 |
| 443 | TCP | vRealize Automation アプライアンス | HTTPS 経由の IaaS コンポーネントおよび vRealize Automation アプライアンスとの通信 |
| 443 | TCP | インフラストラクチャ エンドポイント ホスト | HTTPS 経由の IaaS コンポーネントおよび vRealize Automation アプライアンスとの通信。通常、443 は仮想およびクラウドのインフラストラクチャ エンドポイント ホストのデフォルト通信ポートです。デフォルト ポートおよび必要なポートの完全なリストについては、インフラストラクチャ ホストから提供されているドキュメントを参照してください |
| 443 | TCP | ゲスト エージェント ソフトウェア ブートストラップ エージェント | HTTPS 経由の Manager Service との通信 |
| 443 | TCP | DEM ワーカー | NSX Manager との通信 |
| 1433 | TCP | SQL Server インスタンス | MSSQL |

表 1-15. 出力ポート

| ポート | プロトコル | コンポーネント | コメント |
|---------------|---------|---|---|
| 53 | TCP、UDP | すべて | DNS |
| 67、68、546、547 | TCP、UDP | すべて | DHCP |
| 123 | TCP、UDP | すべて | 任意。NTP |
| 443 | TCP | Manager Service | HTTPS 経由の vRealize Automation アプライアンスとの通信 |
| 443 | TCP | Distributed Execution Manager | HTTPS 経由の Manager Service との通信 |
| 443 | TCP | プロキシ エージェント | HTTPS 経由の Manager Service およびインフラストラクチャ エンドポイント ホストとの通信 |
| 443 | TCP | 管理エージェント | vRealize Automation アプライアンスとの通信 |
| 443 | TCP | ゲスト エージェント ソフトウェア ブートストラップ エージェント | HTTPS 経由の Manager Service との通信 |
| 1433 | TCP | Manager Service Web サイト | MSSQL |
| 5480 | TCP | すべて | vRealize Automation アプライアンスとの通信。 |

また、すべてのサーバ間で DTC を有効にするので、DTC では TCP 上のポート 135 と、1024 から 65535 の間のランダムなポートが 1 つが必要です。前提条件チェッカーは、DTC が実行されていることと、必要なポートが開いていることを検証します。

IaaS Web サーバ

Web コンポーネントをホストする Windows サーバは、すべての IaaS Windows サーバの要件以外に、追加の要件を満たす必要があります。

要件は、Web コンポーネントで Model Manager をホストするかどうかに関係なく同じです。

- Java を設定します。
 - 64 ビット版の Java 1.8 Update 161 以降をインストールします。32 ビット版は使用しないでください。
JRE があれば十分です。JDK 一式は必要としません。
 - JAVA_HOME 環境変数を Java インストール フォルダに設定します。
 - %JAVA_HOME%\bin\java.exe が使用できることを確認します。
- 次の表に基づいて、インターネット インフォメーション サービス (IIS) を構成します。

IIS 7.5 for Windows 2008 シリーズ、IIS 8 for Windows 2012、IIS 8.5 for Windows 2012 R2、IIS 10 for Windows 2016 が必要です。

この構成に加え、IIS で追加の Web サイトをホストしないようにします。vRealize Automation はすべての未割り当ての IP アドレスへの通信ポートにバインドを設定するため、追加のバインドは許可されません。デフォルトの vRealize Automation の通信ポートは 443 です。

表 1-16. IaaS Manager Service ホストのインターネット インフォメーション サービス

| IIS コンポーネント | 設定 |
|------------------------------------|---|
| インターネット インフォメーション サービス (IIS) ロール | <ul style="list-style-type: none"> ■ Windows 認証 ■ 静的なコンテンツ ■ デフォルト ドキュメント ■ ASP.NET 3.5 および ASP.NET 4.5 ■ ISAPI の拡張機能 ■ ISAPI のフィルタ |
| IIS Windows プロセス アクティベーションサービスのロール | <ul style="list-style-type: none"> ■ 構成 API ■ .NET 環境 ■ プロセス モデル ■ WCF アクティベーション (Windows 2008 シリーズのみ) ■ HTTP アクティベーション ■ 非 HTTP アクティベーション (Windows 2008 シリーズのみ) <p>(Windows 2012 シリーズ : [機能] > [.Net Framework 3.5 機能] > [非 HTTP アクティベーション] に移動)</p> |
| IIS 認証設定 | <p>以下をデフォルト以外の値に設定します。</p> <ul style="list-style-type: none"> ■ Windows 認証を有効化 ■ 匿名認証を無効化 <p>以下のデフォルト値は変更しないでください。</p> <ul style="list-style-type: none"> ■ Negotiate Provider を有効化 ■ NTLM Provider を有効化 ■ Windows 認証のカーネル モードを有効化 ■ Windows 認証の拡張保護の無効化 ■ Windows 2012 シリーズでは、SHA512 を使用する証明書の TLS1.2 を無効にする必要があります |

IaaS Manager Service ホスト

Manager Service コンポーネントをホストする Windows サーバは、すべての IaaS Windows サーバの要件以外に、追加の要件を満たす必要があります。

Manager Service ホストがプライマリとバックアップのどちらであっても、要件は同じです。

- Manager Service ホストと DEM ホストの間にファイアウォールを置くことはできません。ポート情報については、[IaaS Windows サーバのポート](#) を参照してください。
- Manager Service ホストでは、SQL Server データベース ホストの NETBIOS 名を解決する必要があります。NETBIOS 名を解決できない場合は、Manager Service マシンの `/etc/hosts` ファイルに、SQL Server の NETBIOS 名を追加します。

laaS SQL サーバ ホスト

laaS SQL データベースをホストする Windows サーバは、一定の要件を満たす必要があります。

SQL Server は、laaS Windows サーバのいずれか、または別のホストに配置できます。laaS コンポーネントとともにホストする場合は、すべての laaS Windows サーバの要件以外にこれらの要件が追加されます。

- vRealize Automation のこのリリースでは、デフォルトの SQL Server 2016 130 互換モードはサポートされません。laaS で使用するために空の SQL Server 2016 データベースを別途作成する場合は、100 または 120 の互換モードを使用します。

vRealize Automation インストーラを使用してデータベースを作成した場合、互換性は構成されています。

- AlwaysOn Availability Group (AAG) は SQL Server 2016 Enterprise でのみサポートされます。AAG を使用する場合は、SQL Server ホストとして AAG リスナーの完全修飾ドメイン名を指定します。
- laaS コンポーネントとともにホストする場合は、Java を設定します。
 - 64 ビット版の Java 1.8 Update 161 以降をインストールします。32 ビット版は使用しないでください。JRE があれば十分です。JDK 一式は必要としません。
 - JAVA_HOME 環境変数を Java インストール フォルダに設定します。
 - %JAVA_HOME%\bin\java.exe が使用でき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、サポートされているバージョンの SQL Server を使用します。
- SQL Server 用に TCP/IP プロトコルを有効にします。
- SQL Server には、SQL インスタンスで作成されるすべてのデータベースのテンプレートとなるモデル データベースが含まれています。laaS を正常にインストールするために、モデルのデータベース サイズは変更しないでください。
- 通常は、[「laaS Windows サーバ」](#)で説明されている最小要件よりも多くのハードウェアが必要です。詳細については、[「vRealize Automation のハードウェア仕様および最大容量」](#)を参照してください。
- vRealize Automation インストーラを実行する前に、アカウントを決定し、SQL に権限を追加する必要があります。[「アカウントとパスワード」](#)を参照してください。

laaS Distributed Execution Manager ホスト

Distributed Execution Manager (DEM) Orchestrator またはワーカー コンポーネントをホストする Windows サーバは、すべての laaS Windows サーバの要件以外に、追加の要件を満たす必要があります。

DEM ホストと Manager Service ホストの間にファイアウォールを置くことはできません。ポート情報については、[「laaS Windows サーバのポート」](#)を参照してください。

DEM ワーカーには、やり取りするプロビジョニング リソースによっては追加の要件が存在する場合があります。

Amazon Web Services と DEM ワーカー

Amazon Web Services (AWS) と通信を行う vRealize Automation laaS DEM ワーカーは、すべての laaS Windows サーバおよび DEM 一般の要件以外に、追加の要件を満たす必要があります。

DEM ワーカーは、プロビジョニングのために AWS と通信することがあります。DEM ワーカーは Amazon EC2 アカウントと通信し、そこからデータを収集します。

- DEM ワーカーには、インターネット アクセスが必要です。
- DEM ワーカーがファイアウォールの背後にある場合は、**aws.amazon.com** や、利用している AWS アカウントがアクセスできる EC2 リージョンの URL（米国東部リージョンの **ec2.us-east-1.amazonaws.com** など）との間でやり取りする HTTPS トラフィックが許可されている必要があります。

各 URL が IP アドレスの範囲を解決するため、ツール（Network Solutions Web サイトから入手可能なツールなど）を使用して、これらの IP アドレスをリストし構成する必要がある場合があります。

- DEM ワーカーがプロキシ サーバ経由でインターネットに接続している場合は、そのプロキシ サーバに対して認証可能な認証情報を使用して DEM サービスが実行されている必要があります。

Openstack または PowerVC と DEM ワーカー

Openstack または PowerVC と通信を行い、データを収集する vRealize Automation IaaS DEM ワーカーは、すべての IaaS Windows サーバおよび DEM 一般の要件以外に、追加の要件を満たす必要があります。

表 1-17. Openstack および PowerVC に関する DEM ワーカーの要件

| インストール | 要件 |
|---------------------------------|---|
| すべて | <p>Windows レジストリで、.NET Framework に対する TLS v1.2 サポートを有効にします。例：</p> <pre>[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319] "SchUseStrongCrypto"=dword:00000001</pre> <pre>[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319] "SchUseStrongCrypto"=dword:00000001</pre> |
| Windows 2008 DEM ホスト | <p>Windows レジストリで、TLS v1.2 プロトコルを有効にします。例：</p> <pre>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2] [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client] "DisabledByDefault"=dword:00000000 "Enabled"=dword:00000001</pre> <pre>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server] "DisabledByDefault"=dword:00000000 "Enabled"=dword:00000001</pre> |
| インフラストラクチャ エンドポイント ホスト上の自己署名証明書 | <p>PowerVC インスタンスまたは Openstack インスタンスが信頼されている証明書を使用していない場合は、vRealize Automation DEM のインストール先となる各 IaaS Windows サーバ上の信頼されているルート認証局ストアに PowerVC インスタンスまたは Openstack インスタンスの SSL 証明書をインポートします。</p> |

Red Hat Enterprise Virtualization と DEM ワーカー

Red Hat Enterprise Virtualization (RHEV) と通信を行い、そこからデータを収集する vRealize Automation IaaS DEM ワーカーは、すべての IaaS Windows サーバおよび DEM 一般の要件以外に、追加の要件を満たす必要があります。

- 各 RHEV 環境を、DEM ワーカーのサーバが含まれるドメインに参加させる必要があります。

- RHEV 環境を示すエンドポイントの管理に使用する認証情報には、RHEV 環境に対する管理者権限が必要です。プロビジョニングに RHEV を使用すると、DEM ワーカーは RHEV のアカウントと通信してデータを収集します。
- 認証情報には、環境内のホスト上にオブジェクトを作成するのに十分な権限が必要です。

SCVMM と DEM ワーカー

System Center Virtual Machine Manager (SCVMM) を通じて仮想マシンを管理する vRealize Automation IaaS DEM ワーカーは、すべての IaaS Windows サーバおよび DEM 一般の要件以外に、追加の要件を満たす必要があります。

- DEM ワーカーは、SCVMM コンソールと同じマシンにインストールします。
ベスト プラクティスは、SCVMM コンソールを別個の DEM ワーカーにインストールすることです。
- DEM ワーカーは、コンソールとともにインストールされた SCVMM PowerShell モジュールへのアクセス権が必要です。
- PowerShell 実行ポリシーは RemoteSigned または Unrestricted に設定する必要があります。

PowerShell 実行ポリシーを確認するには、PowerShell コマンド プロンプトで次のコマンドのいずれかを入力します。

```
help about_signing
help Set-ExecutionPolicy
```

- インスタンス内のすべての DEM ワーカーがこれらの要件を満たすマシン上にない場合、スキル コマンドを使用して、SCVMM 関連のワークフローを、要件を満たすマシン上にある DEM ワーカーに転送します。

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

次の追加の要件が SCVMM に適用されます。

- vRealize Automation は SCVMM 2012 R2 をサポートしています。SCVMM 2012 R2 には PowerShell 3 以降が必要です。
- SCVMM 作業アイテムを使用する vRealize Automation DEM ワーカーをインストールする前に、SCVMM コンソールをインストールします。

SCVMM コンソールの前に DEM ワーカーをインストールすると、次のようなログ エラーが表示されます。

```
Workflow 'ScvmmEndpointDataCollection' failed with the following
exception: The term 'Get-VMMServer' is not recognized as the name of a
cmdlet, function, script file, or operable program.Check the spelling of
the name, or if a path was included, verify that the path is correct and
try again.
```

この問題を修正するには、SCVMM コンソールがインストールされていることを確認し、DEM ワーカー サービスを再起動してください。

- 各 SCVMM インスタンスは、サーバを含むドメインに参加する必要があります。

- SCVMM インスタンスを示すエンドポイントの管理に使用する認証情報には、SCVMM サーバに対する管理者権限が必要です。

これらの証明書では、インスタンス内の Hyper-V サーバに対する管理者権限も必要です。

- SCVMM リソースにマシンをプロビジョニングするには、カタログアイテムを要求している vRealize Automation ユーザーに SCVMM インスタンス内の管理者ロールが必要です。
- 管理対象の SCVMM インスタンス内の Hyper-V サーバは、Hyper-V がインストールされた Windows 2008 R2 SP1 サーバである必要があります。プロセッサには必要な仮想化拡張機能が備わり、.NET Framework 4.5.2 以降がインストールされ、Windows Management Instrumentation (WMI) が有効になっている必要があります。
- SCVMM 2012 R2 リソースに Generation-2 マシンをプロビジョニングするには、ブループリントに次のプロパティを追加する必要があります。

```
Scvmm.Generation2 = true
Hyperv.Network.Type = synthetic
```

Generation-2 ブループリントのビルド情報ページに、データが収集された既存の virtualHardDisk (vHDX) を指定する必要があります。空白にすると、Generation-2 のプロビジョニングが失敗します。

マシン プロビジョニングの準備に関する詳細については、[SCVMM 環境の準備](#)を参照してください。

証明書

vRealize Automation は IaaS コンポーネントおよび vRealize Automation アプライアンスのインスタンス間で安全な通信を行うために SSL 証明書を使用します。アプライアンスおよび Windows インストール マシンは、これらの証明書を交換して信頼できる通信を確立します。証明書は内部または外部の認証局から取得できます。または各コンポーネントの展開プロセスで自己署名証明書を生成できます。

証明書のトラブルシューティング、サポート、および信頼性の要件についての詳細は、[VMware ナレッジベースの記事 KB2106583](#) を参照してください。

注: vRealize Automation では、SHA2 証明書がサポートされます。システムによって生成される自己署名証明書では、RSA 暗号化による SHA-256 が使用されます。オペレーティングシステムまたはブラウザの要件により、SHA2 証明書にアップデートしなければならない場合があります。

導入後に証明書をアップデートまたは置き換えることができます。たとえば、証明書が期限切れになったり、初期展開中に自己署名証明書を使用することを選択した場合でも、後から、vRealize Automation の稼動前に、信頼できる認証局から証明書を取得することができます。

表 1-18. 証明書の実装

| コンポーネント | 最小インストール (非本番環境) | 分散型の展開 (本番環境向け) |
|-----------------------------|--|---|
| vRealize Automation アプライアンス | アプライアンスの構成中に自己署名の証明書を生成します。 | 各アプライアンス クラスタについては、内部または外部の認証局の証明書を使用できます。多目的証明書およびワイルドカード証明書がサポートされています。 |
| IaaS コンポーネント | インストール中、生成された自己署名証明書を受け入れるか、または証明書の抑制を選択します。 | サブジェクトの別名 (SAN) 証明書などの多目的証明書を、Web Client が信頼する内部または外部認証局から取得します。 |

証明書チェーン

証明書チェーンを使用する場合は、次の順序で証明書を指定します。

- 中間 CA 証明書によって署名されたクライアント/サーバ証明書
- 1 つ以上の中間証明書
- ルート CA 証明書

証明書をインポートする際には、各証明書の BEGIN CERTIFICATE ヘッダーと END CERTIFICATE フッターを含めます。

vRealize Automation ログイン URL をカスタマイズする場合の証明書の変更

ユーザーに vRealize Automation アプライアンス以外の URL 名またはロード バランサ名にログインさせたい場合は、[「vRealize Automation ログイン URL のカスタム名への設定」](#) で CNAME のインストールの前および後の手順を参照してください。

vRealize Automation 証明書の要件

vRealize Automation で独自の証明書を使用している場合、証明書は特定の要件を満たしている必要があります。

サポートされる証明書のタイプ

多くの組織で、会社の要件に基づいて外部機関から証明書が発行または要求されます。

次の要件は、一般的な vRealize Automation 展開で使用する共通の ID 形式と証明書タイプに対処します。

| 証明書のプロパティ | 要件 |
|-------------|-------------------------|
| ハッシュ アルゴリズム | SHA1、SHA2、(256、584、512) |
| 署名アルゴリズム | RSASSA-PKCS1_V1_5 |
| キーの長さ | 2084, 4096 |

注: RSASSA-PSS 署名は vRealize Automation 展開ではサポートされていません。この署名は、Windows 2012 R2 の Microsoft CA のデフォルトです。署名は設定可能なパラメータであるため、Microsoft CA の使用時に適切に設定されていることを確認する必要があります。

vRealize Automation 証明書のサポート マトリックス

| ハッシュ アルゴリズム | SHA1 | | | | SHA2-256 | | | |
|---------------------------|-------------------|----------------|------------|------------|-------------------|----------------|------------|------------|
| 署名アルゴリズム | RSASSA-PKCS1_V1_5 | | RSASSA-PSS | | RSASSA-PKCS1_V1_5 | | RSASSA-PSS | |
| キーのサイズ | 2048 | 4096 | 2048 | 4096 | 2048 | 4096 | 2048 | 4096 |
| vRealize Automation のサポート | サポートされていることを確認 | サポートされていることを確認 | サポートされていない | サポートされていない | サポートされていることを確認 | サポートされていることを確認 | サポートされていない | サポートされていない |

| ハッシュアル ゴリズム | SHA2-384 | | | | SHA2-512 | | | |
|----------------------------------|------------------------|------------------------|----------------|----------------|------------------------|------------------------|----------------|----------------|
| 署名アルゴ リズム | RSASSA-PKCS1_V1_5 | | RSASSA-PSS | | RSASSA-PKCS1_V1_5 | | RSASSA-PSS | |
| キーのサイズ | 2048 | 4096 | 2048 | 4096 | 2048 | 4096 | 2048 | 4096 |
| vRealize Automatio n のサポート | サポートさ れているこ とを確認 | サポートさ れているこ とを確認 | サポートされ ていない | サポートされ ていない | サポートされ ていること を確認 | サポートされ ていること を確認 | サポートされ ていない | サポートされ ていない |

証明書とプライベート キーの抽出

仮想アプライアンスとともに使用する証明書は PEM ファイル形式である必要があります。

次の表の例では、GNU の **openssl** コマンドを使用して仮想アプライアンスの構成に必要な証明書情報を抽出します。

表 1-19. サンプルの証明書値とコマンド (openssl)

| 認証局が提供する証明書 | コマンド | 仮想アプライアンスのエントリ |
|-----------------|---|-----------------|
| RSA プライベート キー | openssl pkcs12 -in <path_to_.pfx certificate_file> -nocerts -out key.pem | [RSA プライベート キー] |
| PEM ファイル | openssl pkcs12 -in <path_to_.pfx certificate_file> -clcerts -nokeys -out cert.pem | [証明書チェーン] |
| (オプション) パス フレーズ | なし | [パス フレーズ] |

vRealize Automation アプライアンスの展開

vRealize Automation アプライアンスは、オープン仮想化ファイルとして提供され、既存の仮想インフラストラクチャ上に展開します。

vRealize Automation アプライアンスの導入について

すべてのインストールでは、実際の vRealize Automation インストール オプションのいずれかを実行する前に、まず、導入済みで未構成の vRealize Automation アプライアンスが必要です。

- 統合されたブラウザベースのインストール ウィザード
- ブラウザ ベースの個別のアプライアンス構成と、その後の IaaS サーバ用の個別の Windows インストール
- 応答プロパティ ファイルからの入力を受け入れるコマンド ライン ベースのサイレント インストーラ
- JSON 形式の入力を受け入れるインストール REST API

vRealize Automation アプライアンスの展開

vRealize Automation では、いずれかのインストールパスを使用する前に、少なくとも 1 つの vRealize Automation アプライアンスを展開する必要があります。

アプライアンスを作成するには、vSphere Client を使用して、部分的に構成された仮想マシンをテンプレートからダウンロードして展開します。高可用性とフェイルオーバーを実現するエンタープライズ展開を作成する場合、状況によっては手順を何回か繰り返す必要があります。通常、このような展開では、ロード バランサの背後に複数の vRealize Automation アプライアンスがあります。

前提条件

- OVF テンプレートをインベントリに展開する権限を持つアカウントで vSphere Client にログインします。
- vRealize Automation アプライアンスの **.ovf** または **.ova** ファイルを、vSphere Client からアクセス可能な場所にダウンロードします。

手順

- 1 vSphere の [OVF テンプレートの展開] オプションを選択します。
- 2 vRealize Automation アプライアンスの **.ovf** または **.ova** ファイルへのパスを入力します。
- 3 テンプレートの詳細を確認します。
- 4 エンドユーザー使用許諾契約書を読んで同意します。
- 5 アプライアンス名とインベントリの場所を入力します。

複数のアプライアンスを展開する場合は、それぞれに異なる名前を使用します。その際、アンダースコア (_) などの英数字以外の文字を名前に含めないでください。

- 6 アプライアンスを配置するホストとクラスタを選択します。
- 7 アプライアンスを配置するリソース プールを選択します。
- 8 アプライアンスをホストするストレージを選択します。
- 9 ディスク フォーマットを選択します。

シック フォーマットはパフォーマンスが向上し、シン フォーマットはストレージ容量を節約できます。

フォーマットはアプライアンスのディスク サイズには影響しません。アプライアンスにデータ用の追加容量が必要な場合は、展開後に vSphere を使用してディスクを追加します。

- 10 ドロップダウン メニューから、ターゲット ネットワークを選択します。
- 11 アプライアンスのプロパティを終了します。

- a root パスワードを入力して確定します。

root アカウントの認証情報を使用すると、アプライアンスがホストするブラウザベースの管理インターフェイス、またはアプライアンスのオペレーティング システムのコマンドライン コンソールにログインします。

- b コマンドライン コンソールにリモート SSH 接続を許可するかどうかを選択します。

SSH を無効にする方が安全ですが、別のターミナル クライアントではなく vSphere でコンソールに直接アクセスする必要があります。

- c [ホスト名] に、アプライアンス FQDN を入力します。

最適な結果を得るには、DHCP を使用している場合でも、FQDN を入力します。

注: vRealize Automation は DHCP をサポートしていますが、本番環境への展開には固定 IP アドレスを推奨します。

- d [ネットワーク プロパティ] で、固定 IP アドレスを使用する場合は、ゲートウェイ、ネットマスク、DNS サーバの値を入力します。次の例に示すように、アプライアンス自体の IP アドレス、FQDN、ドメインも入力する必要があります。

図 1-13. サンプル仮想アプライアンスのプロパティ

| | |
|-------------------------------------|---|
| ▼ Application | 3 settings |
| Enable SSH service in the appliance | <p>This will be used as an initial status of the SSH service in the appliance. You can change the status from the appliance Web console.</p> <input checked="" type="checkbox"/> |
| Hostname | <p>The host name for this virtual machine. Provide the fully qualified domain name if you use DHCP. Leave blank to try to reverse look up the IP address if you use DHCP.</p> <input type="text" value="va1.mycompany.com"/> |
| Initial root password | <p>This will be used as an initial password for the root user account. You can change the password using the passwd command or from the appliance Web console).</p> <p>Enter password <input type="password" value="*****"/></p> <p>Confirm password <input type="password" value="*****"/></p> |
| ▼ Networking Properties | 6 settings |
| Default Gateway | <p>The default gateway address for this VM. Leave blank if DHCP is desired.</p> <input type="text" value="12.34.56.79"/> |
| Domain Name | <p>The domain name of this VM. Leave blank if DHCP is desired.</p> <input type="text" value="mycompany.com"/> |
| Domain Name Servers | <p>The domain name server IP Addresses for this VM (comma separated). Leave blank if DHCP is desired.</p> <input type="text" value="12.34.56.80, 12.34.56.81"/> |
| Domain Search Path | <p>The domain search path (comma or space separated domain names) for this VM. Leave blank if DHCP is desired.</p> <input type="text" value="mycompany.com"/> |
| Network 1 IP Address | <p>The IP address for this interface. Leave blank if DHCP is desired.</p> <input type="text" value="12.34.56.78"/> |
| Network 1 Netmask | <p>The netmask or prefix for this interface. Leave blank if DHCP is desired.</p> <input type="text" value="255.255.254.0"/> |

12 展開、vCenter Server、DNS 構成に応じて、展開を完了してアプライアンスを起動する以下の方法のいずれかを選択します。

- vSphere への展開を行い、[デプロイ後にパワーオン] が [設定の確認] ページで表示されている場合は、以下の手順に従います。
 - a [デプロイ後にパワーオン] を選択し、[終了] をクリックします。
 - b このファイルによる vCenter Server への展開が終了した後、[閉じる] をクリックします。
 - c 仮想マシンが起動するのを待ちます。最長で 5 分ほどかかります。
- vSphere への展開を行い、[デプロイ後にパワーオン] が [設定の確認] ページで表示されない場合は、以下の手順に従います。
 - a このファイルによる vCenter Server への展開が終了した後、[閉じる] をクリックします。
 - b vRealize Automation アプライアンスをパワーオンします。
 - c 仮想マシンが起動するのを待ちます。最長で 5 分ほどかかります。
 - d FQDN に ping し、vRealize Automation アプライアンスが展開されていることを確認します。アプライアンスに ping できない場合は、仮想マシンを再起動します。
 - e 仮想マシンが起動するのを待ちます。最長で 5 分ほどかかります。
- vCloud Director を使用して vRealize Automation アプライアンスを展開した場合、OVA 展開時に入力したパスワードが vCloud によってオーバーライドされることがあります。オーバーライドを防ぐには、以下の手順に従います。
 - a vCloud Director への展開後、vApp をクリックして vRealize Automation アプライアンスを表示します。
 - b vRealize Automation アプライアンスを右クリックし、[プロパティ] を選択します。
 - c [ゲスト OS のカスタマイズ] タブをクリックします。
 - d [パスワードリセット] で、[ローカル管理者パスワードを許可] オプションをクリアし、[OK] をクリックします。
 - e vRealize Automation アプライアンスをパワーオンします。
 - f 仮想マシンが起動するのを待ちます。最長で 5 分ほどかかります。

13 FQDN に ping し、vRealize Automation アプライアンスが展開されていることを確認します。

次のステップ

- (オプション) NIC を追加します。[「インストーラの実行前にネットワーク インターフェイス コントローラを追加」](#)を参照してください。
- ブラウザベースの管理インターフェイスにログインして、統合インストール ウィザードを実行するか、アプライアンスを手動で構成することができます。

`https://<vrealize-automation-appliance-FQDN>:5480`

- または、ログインをスキップして、vRealize Automation のサイレント インストールまたは API ベースのインストールを利用することもできます。

インストーラの実行前にネットワーク インターフェイス コントローラを追加

vRealize Automation は、複数のネットワーク インターフェイス コントローラ (NIC) をサポートします。NIC は、インストーラの実行前に、vRealize Automation アプライアンスまたは IaaS Windows サーバに追加することができます。

vRealize Automation インストール ウィザードの実行前に複数の NIC を配置する必要がある場合、vCenter Server をデプロイした後、ウィザードの開始前に追加します。以下のような場合に、追加の NIC を早い段階で配置する必要があります。

- ユーザーとインフラストラクチャ ネットワークを分離する必要がある。
- IaaS サーバが Active Directory ドメインに参加できるように、追加の NIC を必要としている。

複数の NIC のシナリオの詳細については、この [VMware Cloud Management に関するブログ記事](#) を参照してください。

NIC が 3 個以上の場合は、次の制限を考慮してください。

- VIDM が PostgreSQL データベースおよび Active Directory にアクセスする必要がある。
- VIDM が、HA クラスタでロード バランサの URL にアクセスする必要がある。
- 前述の VIDM は最初の 2 個の NIC を通じて接続される必要がある。
- 2 個目以降の NIC は VIDM に使用または認識されないようにする。
- 2 個目以降の NIC は、Active Directory への接続に使用されないようにする。

vRealize Automation でディレクトリを構成する時は、1 個目または 2 個目の NIC を使用する。

前提条件

vRealize Automation アプライアンス OVF と Windows 仮想マシンを展開していますが、ログインもインストール ウィザードの開始もしていません。

手順

- 1 vCenter Server で、NIC を各 vRealize Automation アプライアンスに追加します。
 - a 新しく展開したアプライアンスを右クリックして、[設定の編集] を選択します。
 - b VMXNETn NIC を追加します。
 - c パワーオンされている場合、アプライアンスを再起動します。
- 2 vRealize Automation アプライアンスのコマンドラインに root としてログインします。
- 3 各 NIC に次のコマンドを実行して、NIC を設定します。

必ずデフォルト ゲートウェイのアドレスを含めます。この手順を完了したら、スタティック ルートを構成できます。

```
/opt/vmware/share/vami/vami_set_network <network-interface> (STATICV4|
STATICV4+DHCPV6|STATICV4+AUTOV6) <IPv4-address> <netmask> <gateway-v4-
address>
```


例：

```
/opt/vmware/share/vami/vami_set_network eth1 STATICV4 192.168.100.20
255.255.255.0 192.168.100.1
```

- 4 すべての vRealize Automation ノードが DNS 名で相互に解決されることを確認します。
- 5 すべての vRealize Automation ノードが、vRealize Automation コンポーネントのロード バランシングされた FQDN にアクセスできることを確認します。
- 6 スプリット プレイン DNS を使用している場合、すべての vRealize Automation ノードと仮想 IP アドレスが、各ノードの IP アドレスおよび仮想 IP アドレスに対して DNS で同一の FQDN を持つことを確認します。
- 7 vCenter Server で、NIC を IaaS Windows サーバに追加します。
 - a IaaS サーバを右クリックして、[設定の編集] を選択します。
 - b NIC を IaaS サーバ仮想マシンに追加します。
- 8 Windows で、追加の IaaS サーバの NIC とその IP アドレスを設定します。必要に応じて、Microsoft のドキュメントを参照してください。

次のステップ

- (オプション) スタティック ルートが必要な場合、インストールを続行する前に、[「スタティック ルートの設定」](#)のガイドラインを参照してください。
- ブラウザベースの管理インターフェイスにログインして、統合インストール ウィザードを実行するか、アプライアンスを手動で構成することができます。
<https://<vrealize-automation-appliance-FQDN>:5480>
- または、ログインをスキップして、vRealize Automation のサイレント インストールまたは API ベースのインストールを利用することもできます。

インストール ウィザードを使用した vRealize Automation のインストール

vRealize Automation のインストール ウィザードでは、最小インストールまたはエンタープライズ展開を簡単かつ迅速にインストールできます。

ウィザードを起動する前に、vRealize Automation アプライアンスを展開し、前提条件を満たすように IaaS Windows サーバを構成します。インストール ウィザードは、新しく展開した vRealize Automation アプライアンスに初めてログインするときに表示されます。

- ウィザードを停止して後で戻るには、[ログアウト] をクリックします。
- ウィザードを無効にするには、[キャンセル] をクリックするかログアウトして、標準インターフェイスで手動インストールを開始します。

このウィザードは、vRealize Automation を新規インストールする場合の主要なツールです。ウィザードの実行後に既存の vRealize Automation 展開を拡張する場合は、[「標準 vRealize Automation インストール インターフェイス」](#)の手順を参照してください。

最小インストール向けのインストール ウィザードの使用

最小インストールは vRealize Automation の動作のデモにはなりますが、通常十分な容量がないためエンタープライズ本番環境はサポートされません。

概念実証作業または vRealize Automation に習熟するには最小インストールを選択します。

ウィザードを使用した最小インストールの開始

通常、最小インストールは 1 台の vRealize Automation アプライアンス、1 台の IaaS Windows サーバ、およびエンドポイント用の vSphere エージェントで構成されます。最小インストールでは、すべての IaaS コンポーネントを 1 台の Windows サーバ上に配置します。

前提条件

- [「vRealize Automation のインストールの準備」](#) の前提条件に対処します。
- 未構成のアプライアンスを作成します。[「vRealize Automation アプライアンスの展開」](#) を参照してください。

手順

- 1 vRealize Automation アプライアンスの管理インターフェイスに root としてログインします。
`https://<vrealize-automation-appliance-FQDN>:5480`
- 2 インストール ウィザードが表示されたら、[次へ] をクリックします。
- 3 使用許諾契約に同意し、[次へ] をクリックします。
- 4 [展開タイプ] ページで、[最小インストール] と [IaaS のインストール] を選択し、[次へ] をクリックします。
- 5 [インストールの前提条件] ページで、一時停止して IaaS Windows サーバにログインし、管理エージェントをインストールします。管理エージェントにより、vRealize Automation アプライアンスが IaaS サーバを検出して接続できるようになります。

次のステップ

IaaS Windows サーバに管理エージェントをインストールします。[「vRealize Automation 管理エージェントのインストール」](#) を参照してください。

vRealize Automation 管理エージェントのインストール

すべての IaaS Windows サーバには、特定の vRealize Automation アプライアンスと関連付けるための管理エージェントが必要です。

vRealize Automation SQL Server データベースが、IaaS コンポーネントがホストされていない別の Windows マシンにホストされている場合、SQL Server マシンに管理エージェントは必要ありません。

管理エージェントは、IaaS Windows サーバを vRealize Automation アプライアンスに登録し、IaaS コンポーネントのインストールと管理を自動化して、サポートおよびテレメトリ情報を収集します。管理エージェントは、IaaS Windows サーバ上で管理者権限を持つドメイン アカウント下で Windows サービスとして実行されます。

前提条件

vRealize Automation アプライアンスを作成し、インストール ウィザードを開始します。

[「vRealize Automation アプライアンスの展開」](#) および [「ウィザードを使用した最小インストールの開始」](#) を参照してください。

手順

- 1 vRealize Automation アプライアンス コンソールに root ユーザーとしてログインします。
- 2 次のコマンドを入力します。

```
openssl x509 -in /opt/vmware/etc/lighttpd/server.pem -fingerprint -noout -sha1
```
- 3 後で確認できるようにフィンガープリントをコピーします。例：

```
71:84:47:72:03:57:C8:C2:68:65:00:06:BC:D8:23:98:92:54:BF:89
```
- 4 管理者権限を備えたアカウントを使用して IaaS Windows サーバにログインします。
- 5 Web ブラウザを開き、vRealize Automation アプライアンス インストーラ URL にアクセスします。

```
https://<vrealize-automation-appliance-FQDN>:5480/installer
```
- 6 [管理エージェント インストーラ] をクリックし、**.msi** ファイルを保存して実行します。
- 7 [ようこそ] ページの内容を確認します。
- 8 エンド ユーザー使用許諾契約書に同意します。
- 9 インストール フォルダを承諾または変更します。

```
Program Files (x86)\VMware\VCAC\Management Agent
```

10 vRealize Automation アプライアンスの詳細を入力します。

- a FQDN と :5480 ポート番号など、アプライアンスの HTTPS アドレスを入力します。
- b アプライアンスの root アカountの認証情報を入力します。
- c [ロード] をクリックして、フィンガープリントが以前にコピーしたものと一致することを確認します。コロンは無視します。

フィンガープリントが一致しない場合は、アプライアンスの正しいアドレスが入力されていることを確認します。

図 1-14. 管理エージェント : vRealize Automation アプライアンスの詳細

11 サービス アカountの domain\username およびパスワードを入力します。

サービス アカountは、IaaS Windows サーバ上の管理者権限を持つドメイン アカountである必要があります。全体で同一のサービス アカountを使用します。

12 プロンプトに従って管理エージェントのインストールを完了します。

注: アプライアンス同士は関連付けられているため、vRealize Automation アプライアンスを置き換える場合は、管理エージェントを再インストールする必要があります。

Windows サーバから IaaS をアンインストールしても、管理エージェントは削除されません。管理エージェントをアンインストールするには、Windows の [プログラムの追加と削除] 機能を使用します。

次のステップ

ブラウザベースのインストールウィザードに戻ります。管理エージェントがインストールされた IaaS Windows サーバは、[検出されたホスト] の下に表示されます。

インストールウィザードの実行

管理エージェントをインストールしたら、ウィザードに戻り、手順を続行します。設定について不明な点がある場合は、ウィザードの右上にある [ヘルプ] リンクをクリックします。

- ウィザードの最後のページに、プロパティ ファイルの名前とパスが表示されます。このファイルを編集すると、今回のウィザードと同一または類似の設定で、vRealize Automation のサイレント インストールを実行する際に使用できます。[「vRealize Automation のサイレント インストール」](#)を参照してください。
- 初期コンテンツを作成した場合は、デフォルトのテナントに configurationadmin ユーザーとしてログインし、カタログ アイテムを申請できます。アイテムを申請して手動ユーザー アクションを実行する方法については、[シナリオ : Rainpole 社での事前検証 \(POC\) でコンテンツ展開の初期コンテンツを申請する](#)を参照してください。
- デフォルト テナントへのアクセスを他のユーザー向けに設定するには、[「デフォルト テナントへのアクセスの構成」](#)を参照してください。

エンタープライズ展開向けのインストール ウィザードの使用

組織のニーズに合わせたエンタープライズ インストールが可能です。エンタープライズ 導入環境には、分散コンポーネントまたはロード バランサで構成されている高可用性環境を構成できます。

エンタープライズ インストールは、分散型で冗長性のあるコンポーネントを使用した、より複雑なインストール構造向けに設計されており、通常ロード バランサを含む環境に使用します。IaaS コンポーネントのインストールは、どちらのタイプのインストールでもオプションになります。

ロード バランシングを展開する環境の場合、アクティブな Web サーバ インスタンスおよび vRealize Automation アプライアンスが複数存在すると、インストールに失敗します。インストール中は、1 つの Web サーバ インスタンスおよび 1 台の vRealize Automation アプライアンスだけがアクティブになっている必要があります。

エンタープライズ展開向けのインストール ウィザードの開始

エンタープライズ展開は、本番環境に十分な大きさを持つ展開です。インストール ウィザードを使用して、分散インストールまたは高可用性やフェイルオーバー用のロード バランサを含む分散インストールを実行できます。

ロード バランサを含む分散インストールを展開する場合は、vRealize Automation 環境の構成を担当するチームに通知します。テナント管理者は、Active Directory へのリンクを設定するときに、ディレクトリ管理を高可用性向けに構成する必要があります。

前提条件

- [「vRealize Automation のインストールの準備」](#)に示されている前提条件を満たすように対処します。
- 未構成のアプライアンスを作成します。[「vRealize Automation アプライアンスの展開」](#)を参照してください。

手順

- 1 vRealize Automation アプライアンスの管理インターフェイスに root としてログインします。
`https://<vrealize-automation-appliance-FQDN>:5480`
- 2 インストール ウィザードが表示されたら、[次へ] をクリックします。
- 3 エンド ユーザー使用許諾契約書に同意し、[次へ] をクリックします。
- 4 [展開タイプ] ページで、[エンタープライズ展開] と [IaaS のインストール] を選択します。
- 5 [インストールの前提条件] ページで、一時停止して IaaS Windows サーバにログインし、管理エージェントをインストールします。管理エージェントにより、vRealize Automation アプライアンスがそれらの IaaS サーバを検出して接続できるようになります。

次のステップ

IaaS Windows サーバに管理エージェントをインストールします。[\[vRealize Automation 管理エージェントのインストール\]](#) を参照してください。

vRealize Automation 管理エージェントのインストール

すべての IaaS Windows サーバには、特定の vRealize Automation アプライアンスと関連付けるための管理エージェントが必要です。

vRealize Automation SQL Server データベースが、IaaS コンポーネントがホストされていない別の Windows マシンにホストされている場合、SQL Server マシンに管理エージェントは必要ありません。

管理エージェントは、IaaS Windows サーバを vRealize Automation アプライアンスに登録し、IaaS コンポーネントのインストールと管理を自動化して、サポートおよびテレメトリ情報を収集します。管理エージェントは、IaaS Windows サーバ上で管理者権限を持つドメイン アカウント下で Windows サービスとして実行されます。

前提条件

vRealize Automation アプライアンスを作成し、インストール ウィザードを開始します。

[\[vRealize Automation アプライアンスの展開\]](#) および [\[エンタープライズ展開向けのインストール ウィザードの開始\]](#) を参照してください。

手順

1 vRealize Automation アプライアンス コンソールに root ユーザーとしてログインします。

2 次のコマンドを入力します。

```
openssl x509 -in /opt/vmware/etc/lighttpd/server.pem -fingerprint -noout -sha1
```

3 後で確認できるようにフィンガープリントをコピーします。例：

```
71:84:47:72:03:57:C8:C2:68:65:00:06:BC:D8:23:98:92:54:BF:89
```

4 管理者権限を備えたアカウントを使用して IaaS Windows サーバにログインします。

5 Web ブラウザを開き、vRealize Automation アプライアンス インストーラ URL にアクセスします。

```
https://<vrealize-automation-appliance-FQDN>:5480/installer
```

6 [管理エージェント インストーラ] をクリックし、**.msi** ファイルを保存して実行します。

7 [ようこそ] ページの内容を確認します。

8 エンド ユーザー使用許諾契約書に同意します。

9 インストール フォルダを承諾または変更します。

```
Program Files (x86)\VMware\VCAC\Management Agent
```

10 vRealize Automation アプライアンスの詳細を入力します。

- a FQDN と :5480 ポート番号など、アプライアンスの HTTPS アドレスを入力します。
- b アプライアンスの root アカountの認証情報を入力します。
- c [ロード] をクリックして、フィンガープリントが以前にコピーしたものと一致することを確認します。コロンは無視します。

フィンガープリントが一致しない場合は、アプライアンスの正しいアドレスが入力されていることを確認します。

図 1-15. 管理エージェント : vRealize Automation アプライアンスの詳細

11 サービス アカountの domain\username およびパスワードを入力します。

サービス アカountは、IaaS Windows サーバ上の管理者権限を持つドメイン アカountである必要があります。全体で同一のサービス アカountを使用します。

12 プロンプトに従って管理エージェントのインストールを完了します。

IaaS コンポーネントをホストするすべての Windows サーバでこの手順を繰り返します。

注: アプライアンス同士は関連付けられているため、vRealize Automation アプライアンスを置き換える場合は、管理エージェントを再インストールする必要があります。

Windows サーバから IaaS をアンインストールしても、管理エージェントは削除されません。管理エージェントをアンインストールするには、Windows の [プログラムの追加と削除] 機能を使用します。

次のステップ

ブラウザベースのインストールウィザードに戻ります。管理エージェントがインストールされた IaaS Windows サーバは、[検出されたホスト] の下に表示されます。

インストールウィザードの完了

管理エージェントをインストールしたら、ウィザードに戻り、プロンプトの指示を実行してください。設定について不明な点がある場合は、ウィザードの右上にある [ヘルプ] リンクをクリックします。

- ウィザードの最後のページに、プロパティ ファイルの名前とパスが表示されます。このファイルを編集すると、今回のウィザードと同一または類似の設定で、vRealize Automation のサイレント インストールを実行する際に使用できます。[「vRealize Automation のサイレント インストール」](#)を参照してください。
- 初期コンテンツを作成した場合は、デフォルトのテナントに configurationadmin ユーザーとしてログインし、カタログ アイテムを申請できます。アイテムを申請して、手動ユーザー アクションを実行する方法の例については、[シナリオ : Rainpole 事前検証の展開に初期コンテンツを申請する](#)を参照してください。
- デフォルト テナントへのアクセスを他のユーザー向けに設定する方法については、[「デフォルト テナントへのアクセスの構成」](#)を参照してください。

vRealize Automation インストール ウィザードによる手順

vRealize Automation インストール ウィザードにより、前提条件のチェック、設定の入力、設定の検証、および vRealize Automation コンポーネントのインストールが容易になります。

注: このウィザードには、ロード バランサや IaaS Windows サーバなどの他のシステムにログインするために一時停止する手順が含まれます。

前提条件

- 1 台以上の未構成のアプライアンスを作成します。[「vRealize Automation アプライアンスの展開」](#)を参照してください。

最小インストールでは、vRealize Automation アプライアンスを 1 台使用します。エンタープライズ展開では、ロード バランシングで複数のアプライアンスを使用する場合があります。

- IaaS コンポーネントをホストする Windows システムを 1 台以上準備します。
- vRealize Automation のアプライアンス管理インターフェイスに root としてログインして、ウィザードを起動します。

`https://<vrealize-automation-appliance-FQDN>:5480`

手順

1 展開の種類

[展開の種類] ページで、インストールする vRealize Automation コンポーネント、およびそれぞれの数を決定します。

2 インストールの前提条件

[インストールの前提条件] ページでは、vRealize Automation IaaS をホストする Windows マシンへの接続を確立します。また、時刻同期のソースを選択します。

3 vRealize Appliance

(エンタープライズ展開のみ) [vRealize Appliance] ページには、複数の vRealize Automation アプライアンスで高可用性環境を作成するオプションがあります。

4 サーバロール

(エンタープライズ環境のみ) [サーバロール] ページでは、以前に管理エージェントをインストールした Windows マシンに vRealize Automation IaaS コンポーネントのロールを割り当てます。

5 前提条件チェッカー

前提条件チェッカーのページで、vRealize Automation Windows サーバが IaaS インストールに対応しているかを確認し、修正します。

6 vRealize Automation ホスト

[vRealize Automation ホスト] ページでは、vRealize Automation のベース URL アドレスを設定します。このアドレスは、通常、vRealize Automation アプライアンスまたはロード バランサ（高可用性構成の場合）になります。

7 シングル サインオン

[シングル サインオン] ページでは、vRealize Automation のデフォルト テナントのシステム管理者ログイン認証情報を設定します。

8 IaaS ホスト

IaaS ホスト ページで、いくつかの IaaS コンポーネントの基本 URL アドレスを設定します。また、vRealize Automation IaaS SQL データベースのセキュリティ パスフレーズを作成します。

9 Microsoft SQL Server

[Microsoft SQL Server] ページでは、vRealize Automation IaaS SQL データベースを構成します。IaaS データベースは、プロビジョニングされたマシン、関連する構成要素、およびポリシーを記録します。

10 Web ロール

(エンタープライズ展開のみ) [Web ロール] ページでは、個別に IIS の vRealize Automation IaaS Web サイトを構成します。

11 マネージャ サービス ロール

(エンタープライズ展開のみ) [マネージャ サービス ロール] ページでは、IaaS マネージャ サービスをホストする別の vRealize Automation Windows マシンを構成します。

12 Distributed Execution Manager

[Distributed Execution Manager] ページでは、IaaS DEM をホストする vRealize Automation Windows マシンを構成します。複数の DEM ホストがサポートされます。

13 エージェント

[エージェント] ページでは、vRealize Automation IaaS とインフラストラクチャのデプロイ先となる仮想化リソースとの間のリンクを作成します。エージェントの種類を選択し、対応するエンドポイントの詳細を入力します。

14 vRealize Appliance 証明書

[vRealize Appliance 証明書] ページでは、vRealize Automation アプライアンスが使用する認証証明書を作成または選択します。自己署名証明書の場合は、エンド ユーザーがブラウザで vRealize Automation にログインするときに、確認のためにその証明書が表示されます。

15 Web 証明書

[Web 証明書] ページでは、IaaS Web サーバが使用する認証証明書を作成または選択します。vRealize Automation アプライアンスは、Web サーバに接続し、それを認証および信頼する必要があります。

16 マネージャ サービス証明書

(エンタープライズ展開のみ) [マネージャ サービス証明書] ページでは、vRealize Automation IaaS のマネージャ サービス ホストが使用する認証証明書を作成または選択します。他の IaaS Windows サーバは、マネージャ サービス ホストに接続し、それを認証および信頼する必要があります。

17 ロード バランサ

(エンタープライズ展開環境のみ) [ロード バランサ] ページでは、vRealize Automation メンバー システムのプールに合わせて、適切にロード バランサを設定します。

18 検証

[検証] ページでは、vRealize Automation インストールを続行できることを確認します。

19 スナップショットの作成

スナップショットの作成ページでは、インストールを続行する前に、すべての vRealize Automation コンポーネントの仮想マシン スナップショットを作成します。

20 インストールの詳細

インストールの詳細ページでは、vRealize Automation のインストールを開始するか、問題が発生した場合は再試行します。

21 ライセンス

[ライセンス] ページでは、インストールされた vRealize Automation 製品を有効化するためのキーを入力します。

22 テレメトリ

テレメトリのページでは、vRealize Automation で、カスタム エクスペリエンス改善プログラムの一部として使用量の統計を VMware に送信するかどうかを決定します。

23 インストール後のオプション

[インストール後のオプション] ページには、新しい vRealize Automation データを作成するオプション、または古い環境のデータを新規インストールに移行するオプションがあります。

24 初期コンテンツの設定

初期コンテンツの設定ページで、新しいローカルの vRealize Automation デフォルト テナント ユーザーを作成します。このユーザーは、vSphere エンドポイントのコンテンツ ワークフローを開始できます。

25 移行の設定

移行の設定ページでは、新規にインストールした環境へ、別の古い vRealize Automation 環境を転送できます。

展開の種類

[展開の種類] ページで、インストールする vRealize Automation コンポーネント、およびそれぞれの数を決定します。

最小

最小展開では、1 台の vRealize Automation アプライアンスと、IaaS コンポーネントをホストする 1 台の Windows サーバのみが使用されます。最小展開では、別の SQL Server システム上の IaaS データベースをホストするか、IaaS Windows サーバに SQL をインストールできます。

最小インストールは、エンタープライズ インストール環境に変換できません。インストール環境をスケール アップするには、小規模のエンタープライズ環境から開始して、コンポーネントを追加していきます。最小インストールから開始することはできません。

エンタープライズ

エンタープライズ展開では、通常はロード バランシングで、複数の個別のアプライアンスと Windows ホストを使用します。エンタープライズ展開では、別の SQL Server システム上で、または IaaS Windows サーバの 1 台で、IaaS データベースをホストすることもできます。

エンタープライズ展開を選択すると、ウィザードの左側の概要リストに追加のインストール ウィザード ページが表示されます。

Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) オプションでは、既存の Windows マシンを vRealize Automation のモデリング機能とプロビジョニング機能で構成するかどうかを選択します。

IaaS を選択すると、ウィザードの左側の概要リストに追加のインストール ウィザード ページが表示されます。

インストールの前提条件

[インストールの前提条件] ページでは、vRealize Automation IaaS をホストする Windows マシンへの接続を確立します。また、時刻同期のソースを選択します。

IaaS Windows サーバ

IaaS コンポーネントホストとして機能する Windows マシンの場合は、**vcac-iaasmanagementagent-setup.msi** をダウンロードして Windows マシンにインストールする必要があります。

管理エージェントのインストールには、実行中の vRealize Automation アプライアンスとの通信が必要です。Windows に管理エージェントをインストールするたびに、そのシステムは特定のアプライアンスおよび展開に一意に関連付けられます。

正しい管理エージェントがインストールされた潜在的な IaaS Windows サーバは、[検出されたホスト] に表示されません。

インストール ウィザードで検出されたホストを無視するには、[削除] をクリックします。Windows ホストを削除しても、管理エージェントは削除されません。エージェントをアンインストールするには、Windows 内で直接、プログラムの追加と削除機能を使用します。

時刻ソース

すべての vRealize Automation アプライアンスと IaaS Windows サーバを同じ時刻ソースに同期する必要があります。次のソースを使用できます。

- ホスト時刻の使用 : vRealize Automation アプライアンスの ESXi ホストに同期します。

- タイム サーバの使用：1 台の外部 Network Time Protocol (NTP) サーバに同期します。NTP サーバの FQDN または IP アドレスを入力します。

vRealize Automation 展開内で時刻ソースを混在させないでください。

vRealize Appliance

(エンタープライズ展開のみ) [vRealize Appliance] ページには、複数の vRealize Automation アプライアンスで高可用性環境を作成するオプションがあります。

別個にインストールしたロード バランサの背後で複数のアプライアンスをホストする必要があります。以降のウィザード ページでは、アプライアンスとロード バランサの設定を確認および完了します。追加する各 vRealize Automation アプライアンスの FQDN と root 認証情報を入力します。

サーバ ロール

(エンタープライズ環境のみ) [サーバ ロール] ページでは、以前に管理エージェントをインストールした Windows マシンに vRealize Automation IaaS コンポーネントのロールを割り当てます。

IaaS Windows マシンは、プライマリおよび追加の Web サーバ、Manager Service ホスト、DEM ホスト、および エージェント ホストに使用される可能性があります。IaaS コンポーネントのロールの詳細については、[「Infrastructure as a Service \(IaaS\)」](#) を参照してください。

IaaS サーバ ロールの分離は、エンタープライズ環境でのみ可能です。最小インストールでは、1 台の Windows マシンですべてのロールを実行します。

前提条件チェッカー

前提条件チェッカーのページで、vRealize Automation Windows サーバが IaaS インストールに対応しているかを確認し、修正します。

前提条件チェッカーは、Management Agent がインストールされ、IaaS コンポーネントをホストする予定の Windows マシンを検査します。前提条件は、Java、インターネット インフォメーション サービス (IIS) 設定、Microsoft 分散トランザクション コーディネータ (DTC) サービスなどです。前提条件の詳細なリストについては、[\[詳細の表示\]](#) をクリックします。

インストール ウィザードを使用すると前提条件の確認なしで処理を進めることができますが、インストールが失敗する可能性があることに注意してください。

- 前提条件を確認するには、[\[実行\]](#) をクリックします。
- 前提条件が満たされていない場合は、[\[詳細の表示\]](#) をクリックして詳細を確認してから、[\[修正\]](#) をクリックします。

インストール ウィザードでは、ほとんどのソフトウェアまたは設定ベースの前提条件を修正できます。変更後は、インストール ウィザードによって IaaS ホストが再起動されます。

ウィザードはメモリや CPU の不足を修正できません。vSphere またはご使用のハードウェアでこれらの問題が発生した場合、修正する必要があります。

vRealize Automation ホスト

[vRealize Automation ホスト] ページでは、vRealize Automation のベース URL アドレスを設定します。このアドレスは、通常、vRealize Automation アプライアンスまたはロード バランサ（高可用性構成の場合）になります。

- ロード バランサなしで 1 台の vRealize Automation アプライアンスのみを導入する場合は、vRealize Automation アプライアンスの FQDN を入力します。クリックして、インストールウィザードが FQDN を入力するようにすることができます。
- ロード バランシングの背後に 1 台以上の vRealize Automation アプライアンスを含むエンタープライズ構成を導入する場合は、ロード バランサの FQDN を入力してください。

単一の vRealize Automation アプライアンスも、ロード バランサの背後に導入できます。この方法を使用すると、環境を拡張するために、後でアプライアンスをより簡単に追加できます。

シングル サインオン

[シングル サインオン] ページでは、vRealize Automation のデフォルト テナントのシステム管理者ログイン認証情報を設定します。

デフォルト テナントのシステム管理者は、追加のテナントを作成する権限を含め、すべてのユーザーの権限の大部分を持ちます。デフォルト テナントのシステム管理者認証情報は、vRealize Automation アプライアンスの root 認証情報とは異なります。

laaS ホスト

laaS ホスト ページで、いくつかの laaS コンポーネントの基本 URL アドレスを設定します。また、vRealize Automation laaS SQL データベースのセキュリティ パスフレーズを作成します。

最小インストール

| 設定 | 説明 |
|-------------------------|--|
| laaS Web アドレス | laaS Windows サーバの FQDN を入力します。 |
| laaS コンポーネントをインストールする場所 | laaS Windows サーバの FQDN を選択または入力します。 |
| ユーザー名 | Domain\username の形式でサービス アカウントを入力します。アカウントは、laaS Windows サーバに対するローカル管理者権限を持つドメイン アカウントである必要があります。 |
| パスワード | アカウントのパスワードを入力します。 |
| セキュリティ パスフレーズ | laaS SQL データベースのデータを暗号化するパスフレーズを作成します。 <ul style="list-style-type: none"> ■ パスフレーズはメモしておいてください。障害が発生してデータベースをリストアする場合や、初期インストール後にコンポーネントを追加するときに必要です。 ■ パスフレーズに二重引用符 (") 文字を含めることはできません。 |
| パスフレーズの確認 | もう一度パスフレーズを入力します。 |

エンタープライズ展開

| 設定 | 説明 |
|----------------------|--|
| laaS Web アドレス | プライマリ laaS Web サーバの FQDN を入力します。ロード バランシングされた複数の laaS Web サーバを含むエンタープライズ構成を展開する場合は、代わりにロード バランサの FQDN を入力します。 |
| Manager Service アドレス | プライマリ Manager Service ホストの FQDN を入力します。ロード バランシングされた複数の Manager Service サーバを含むエンタープライズ構成を展開する場合は、代わりにロード バランサの FQDN を入力します。 |
| セキュリティ パスフレーズ | laaS SQL データベースのデータを暗号化するパスフレーズを作成します。 <ul style="list-style-type: none"> ■ パスフレーズはメモしておいてください。障害が発生してデータベースをリストアする場合や、初期インストール後にコンポーネントを追加するときに必要です。 ■ パスフレーズに二重引用符 (") 文字を含めることはできません。 |
| パスフレーズの確認 | もう一度パスフレーズを入力します。 |

Microsoft SQL Server

[Microsoft SQL Server] ページでは、vRealize Automation laaS SQL データベースを構成します。laaS データベースは、プロビジョニングされたマシン、関連する構成要素、およびポリシーを記録します。

| 設定 | 説明 |
|-------------------|---|
| サーバ名 | SQL Server ホスト (laaS Windows サーバまたは別のサーバ) の FQDN を入力します。 ポート番号または名前付きインスタンスを指定する必要がある場合は、 FQDN,ポート\インスタンス の形式を使用します。 SQL AlwaysOn 可用性グループ (AAG) を使用する場合は、AAG リスナーの完全修飾ドメイン名 (FQDN) を指定します。 |
| データベース名 | [vra] のデフォルトを受け入れるか、laaS データベースの別の名前を入力します。 |
| 新しいデータベースを作成 | インストール ウィザードでデータベースを作成できるようにします。 このオプションを使用するには、プライマリ laaS Web サーバで管理エージェントを実行するアカウントに、SQL の sysadmin ロールが必要です。 |
| 既存の空のデータベースを使用 | インストール ウィザードでデータベースを作成できないようにします。 データベースを個別に作成する場合は、指定した Windows ユーザーまたは SQL ユーザー認証情報に、データベースに対する dbo 権限が必要です。 |
| デフォルト設定 | (新しいデータベースのみ) laaS のデータ ファイルとログ ファイルに別のストレージ場所を使用する場合にのみ、このオプションをオフにします。 オフにする場合は、データ (MDF) とログのディレクトリを入力します。SQL Server サービス アカウントに、ディレクトリへの書き込み権限が必要です。 |
| データベース接続に SSL を使用 | データベースへの接続を暗号化します。このオプションを使用するには、SSL 用に SQL Server ホストを別に構成する必要があります。また、laaS Web サーバおよびマネージャ サービス ホストで、SQL Server ホストからの SSL 証明書を信頼する必要があります。 |

| 設定 | 説明 |
|------------|--|
| Windows 認証 | Windows ではなく SQL 認証を使用する場合にのみ、このオプションをオフにします。 オフにする場合は、SQL 認証情報を入力します。 |
| インストール パス | デフォルトの %ProgramFiles(x86)%\VMware を使用するか、別の場所を入力します。 <ul style="list-style-type: none"> ■ vRealize Automation ファイルは、SQL Server ホストにはインストールされていません。プライマリ IaaS Web サーバに配置されます。 ■ 同じ Windows マシンに複数の IaaS コンポーネントをインストールする場合は、同一のインストール パスですべてインストールします。 |

Web ロール

(エンタープライズ展開のみ) [Web ロール] ページでは、個別に IIS の vRealize Automation IaaS Web サイトを構成します。

エンタープライズ展開では、Web コンポーネントをホストする IaaS Windows マシンを個別に指定します。高可用性を実現するため、複数のホストがサポートされます。

| 設定 | 説明 |
|--------------|--|
| Web サイト名 | 名前をカスタマイズするか、IIS のデフォルトの Web サイトのままにします。 IIS で追加の Web サイトをホストしないでください。 vRealize Automation はすべての未割り当ての IP アドレスへの通信ポートにバインドを設定するため、追加のバインドは許可されません。 |
| Port | ポートをカスタマイズするか、デフォルトの 443 を使用します。 |
| IaaS Web サーバ | IaaS ホスト名 |
| | IaaS Web コンポーネントをホストする各 IaaS Windows マシンの FQDN を入力します。 |
| | Username |
| | ドメイン\ユーザー名の形式で、サービス アカウントを入力します。アカウントは、IaaS Windows サーバ上でローカル管理者権限を持つドメイン アカウントである必要があります。 |
| | パスワード |
| | アカウントのパスワードを入力します。 |
| | インストール パス |
| | デフォルトの %ProgramFiles(x86)%\VMware を使用するか、別の場所を入力します。 同じ Windows マシンに複数の IaaS コンポーネントをインストールする場合は、同一のインストール パスですべてインストールします。 |

マネージャ サービス ロール

(エンタープライズ展開のみ) [マネージャ サービス ロール] ページでは、IaaS マネージャ サービスをホストする別の vRealize Automation Windows マシンを構成します。

エンタープライズ展開では、Windows サービスであるマネージャ サービスのホストを別に指定します。高可用性を実現するため、複数のホストがサポートされます。

| 設定 | 説明 |
|-----------|---|
| 有効 | プライマリ マネージャ サービス ホストを選択します。追加のホストは、プライマリのバックアップとして機能します。 インストール ウィザードを使用してインストールすると、問題が発生したときに、サービスが透過的にバックアップにフェイルオーバーします。 「Manager Service の自動フェイルオーバーについて」 を参照してください。 |
| laaS ホスト名 | マネージャ サービスをホストする各 laaS Windows マシンの FQDN を入力します。 |
| Username | Domain\username の形式でサービス アカウントを入力します。アカウントは、laaS Windows サーバに対するローカル管理者権限を持つドメイン アカウントである必要があります。 |
| パスワード | アカウントのパスワードを入力します。 |
| インストール パス | デフォルトの %ProgramFiles(x86)%\VMware を使用するか、別の場所を入力します。 同じ Windows マシンに複数の laaS コンポーネントをインストールする場合は、同一のインストール パスですべてインストールします。 |

Distributed Execution Manager

[Distributed Execution Manager] ページでは、laaS DEM をホストする vRealize Automation Windows マシンを構成します。複数の DEM ホストがサポートされます。

| 設定 | 説明 |
|-----------|---|
| laaS ホスト名 | DEM をホストする各 laaS Windows マシンの FQDN を入力します。 |
| インスタンス名 | 各 DEM の一意の識別子を入力します。すべての DEM 名が、同じホスト上にあるか異なるホスト上にあるかを問わずに、一意である必要があります。 |
| Username | Domain\username の形式でサービス アカウントを入力します。アカウントは、laaS Windows サーバに対するローカル管理者権限を持つドメイン アカウントである必要があります。 |
| Password | アカウントのパスワードを入力します。 |
| インスタンスの説明 | 必要に応じて、各 DEM に関連付けられたワークフローの説明を入力します。 |
| インストール パス | デフォルトの %ProgramFiles(x86)%\VMware を使用するか、別の場所を入力します。 同じ Windows マシンに複数の laaS コンポーネントをインストールする場合は、同一のインストール パスですべてインストールします。 |

エージェント

[エージェント] ページでは、vRealize Automation laaS とインフラストラクチャのデプロイ先となる仮想化リソースとの間のリンクを作成します。エージェントの種類を選択し、対応するエンドポイントの詳細を入力します。

- 複数のエージェントは、タイプが同じ場合と異なる場合のいずれもサポートされます。
- 複数のエージェントは、インストール先のサーバを同じにすることも、個別にすることもできます。
- 同じサーバにインストールする場合は、任意のタイプの 25 エージェントまでがサポートされます。
- 同じタイプの複数のエージェントが同じサーバにある場合、各エージェントには一意の名前と異なるエンドポイントが必要になります。
- 高可用性の目的で、同じタイプ、名前、エンドポイントのエージェントを個別のサーバにインストールすることができます。

- vSphere は通常、いずれかのエージェント タイプです。
- インストール後にエージェントを追加できます。

エージェント タイプ

表 1-20. vSphere

| 設定 | 説明 |
|------------|---|
| エージェント タイプ | ドロップダウンから [vSphere] を選択します。 |
| laaS ホスト名 | ドロップダウンから、エージェントをホストする laaS Windows マシンの FQDN を選択します。 |
| エージェント名 | 高可用性を実現するために個別のサーバ間で同一のエージェント名およびエンドポイントを追加する場合を除き、一意の識別子を入力します。 |
| エンドポイント | vSphere エンドポイントの名前を入力します。 |
| インストール パス | デフォルトの <code>%ProgramFiles(x86)%\VMware</code> を使用するか、別の場所を入力します。同じ Windows マシンに複数の laaS コンポーネントをインストールする場合は、同一のインストール パスですべてインストールします。 |
| Username | Domain\username の形式でサービス アカウントを入力します。アカウントは、laaS Windows サーバに対するローカル管理者権限を持つドメイン アカウントである必要があります。 |
| パスワード | アカウントのパスワードを入力します。 |

表 1-21. EPI PowerShell

| 設定 | 説明 |
|------------|---|
| エージェント タイプ | ドロップダウンから [EpiPowerShell] を選択します。 |
| laaS ホスト名 | ドロップダウンから、エージェントをホストする laaS Windows マシンの FQDN を選択します。 |
| エージェント名 | 高可用性を実現するために個別のサーバ間で同一のエージェント名およびエンドポイントを追加する場合を除き、一意の識別子を入力します。 |
| タイプ | ドロップダウンから、EpiServer エンドポイントがホストするプロビジョニングのブランドを選択します。 |
| サーバ | EpiServer の FQDN を入力します。 |
| インストール パス | デフォルトの <code>%ProgramFiles(x86)%\VMware</code> を使用するか、別の場所を入力します。同じ Windows マシンに複数の laaS コンポーネントをインストールする場合は、同一のインストール パスですべてインストールします。 |
| Username | Domain\username の形式でサービス アカウントを入力します。アカウントは、laaS Windows サーバに対するローカル管理者権限を持つドメイン アカウントである必要があります。 |
| パスワード | アカウントのパスワードを入力します。 |

表 1-22. HyperV

| 設定 | 説明 |
|------------|--|
| エージェント タイプ | ドロップダウンから、[HyperV] を選択します。 |
| laaS ホスト名 | ドロップダウンから、エージェントをホストする laaS Windows マシンの FQDN を選択します。 |
| エージェント名 | 高可用性を実現するために個別のサーバ間で同一のエージェント名およびエンドポイントを追加する場合を除き、一意の識別子を入力します。 |

表 1-22. HyperV (続き)

| 設定 | 説明 |
|-----------|---|
| Username | HyperV エンドポイント インスタンスへのログイン アカウントを入力します。 |
| パスワード | アカウントのパスワードを入力します。 |
| インストール パス | デフォルトの %ProgramFiles(x86)%\VMware を使用するか、別の場所を入力します。 同じ Windows マシンに複数の IaaS コンポーネントをインストールする場合は、同一のインストール パスですべてインストールします。 |
| Username | Domain\username の形式でサービス アカウントを入力します。アカウントは、IaaS Windows サーバに対するローカル管理者権限を持つドメイン アカウントである必要があります。 |
| パスワード | アカウントのパスワードを入力します。 |

表 1-23. VDI PowerShell

| 設定 | 説明 |
|-------------------|---|
| エージェント タイプ | ドロップダウンから [VdiPowerShell] を選択します。 |
| IaaS ホスト名 | ドロップダウンから、エージェントをホストする IaaS Windows マシンの FQDN を選択します。 |
| エージェント名 | 高可用性を実現するために個別のサーバ間で同一のエージェント名およびエンドポイントを追加する場合を除き、一意の識別子を入力します。 |
| タイプ | エンドポイント タイプは XenDesktop にデフォルト設定され、変更できません。 |
| サーバ | XenDesktop エンドポイントの FQDN を入力します。 |
| XenDesktop のバージョン | ドロップダウンから、バージョンを選択します。 |
| インストール パス | デフォルトの %ProgramFiles(x86)%\VMware を使用するか、別の場所を入力します。 同じ Windows マシンに複数の IaaS コンポーネントをインストールする場合は、同一のインストール パスですべてインストールします。 |
| Username | Domain\username の形式でサービス アカウントを入力します。アカウントは、IaaS Windows サーバに対するローカル管理者権限を持つドメイン アカウントである必要があります。 |
| パスワード | アカウントのパスワードを入力します。 |

表 1-24. Xen

| 設定 | 説明 |
|------------|---|
| エージェント タイプ | ドロップダウンから、[Xen] を選択します。 |
| IaaS ホスト名 | ドロップダウンから、エージェントをホストする IaaS Windows マシンの FQDN を選択します。 |
| エージェント名 | 高可用性を実現するために個別のサーバ間で同一のエージェント名およびエンドポイントを追加する場合を除き、一意の識別子を入力します。 |
| Username | Xen エンドポイント インスタンスへのログイン アカウントを入力します。 |
| パスワード | アカウントのパスワードを入力します。 |
| インストール パス | デフォルトの %ProgramFiles(x86)%\VMware を使用するか、別の場所を入力します。 同じ Windows マシンに複数の IaaS コンポーネントをインストールする場合は、同一のインストール パスですべてインストールします。 |

表 1-24. Xen (続き)

| 設定 | 説明 |
|----------|---|
| Username | Domain\username の形式でサービス アカウントを入力します。アカウントは、IaaS Windows サーバに対するローカル管理者権限を持つドメイン アカウントである必要があります。 |
| パスワード | アカウントのパスワードを入力します。 |

表 1-25. WMI

| 設定 | 説明 |
|------------|--|
| エージェント タイプ | ドロップダウンから [WMI] を選択します。 |
| IaaS ホスト名 | ドロップダウンから、エージェントをホストする IaaS Windows マシンの FQDN を選択します。 |
| エージェント名 | 高可用性を実現するために個別のサーバ間で同一のエージェント名およびエンドポイントを追加する場合を除き、一意の識別子を入力します。 |
| インストール パス | デフォルトの %ProgramFiles(x86)%\VMware を使用するか、別の場所を入力します。同じ Windows マシンに複数の IaaS コンポーネントをインストールする場合は、同一のインストール パスですべてインストールします。 |
| Username | Domain\username の形式でサービス アカウントを入力します。アカウントは、IaaS Windows サーバに対するローカル管理者権限を持つドメイン アカウントである必要があります。 |
| パスワード | アカウントのパスワードを入力します。 |

表 1-26. テスト

| 設定 | 説明 |
|------------|--|
| エージェント タイプ | ドロップダウンから、[Test] を選択します。 |
| IaaS ホスト名 | ドロップダウンから、エージェントをホストする IaaS Windows マシンの FQDN を選択します。 |
| エージェント名 | 高可用性を実現するために個別のサーバ間で同一のエージェント名およびエンドポイントを追加する場合を除き、一意の識別子を入力します。 |
| インストール パス | デフォルトの %ProgramFiles(x86)%\VMware を使用するか、別の場所を入力します。同じ Windows マシンに複数の IaaS コンポーネントをインストールする場合は、同一のインストール パスですべてインストールします。 |
| Username | Domain\username の形式でサービス アカウントを入力します。アカウントは、IaaS Windows サーバに対するローカル管理者権限を持つドメイン アカウントである必要があります。 |
| パスワード | アカウントのパスワードを入力します。 |

vRealize Appliance 証明書

[vRealize Appliance 証明書] ページでは、vRealize Automation アプライアンスが使用する認証証明書を作成または選択します。自己署名証明書の場合は、エンド ユーザーがブラウザで vRealize Automation にログインするときに、確認のためにその証明書が表示されます。

| 設定 | | 説明 |
|-----------|------------|---|
| 証明書のアクション | 既存を保持 | この vRealize Automation アプライアンスの既存の証明書を使用します。シリアル番号やフィンガープリントなどの詳細を、下のエントリで確認してください。 |
| | 証明書の生成 | ウィザードを使用して、vRealize Automation アプライアンスの自己署名証明書を生成します。 |
| | 署名リクエストを生成 | <p>認証局 (CA) 向けの証明書署名リクエスト (CSR) ファイルを作成します。CSR は、インポートする証明書を CA が正しい値で作成するのに役立ちます。</p> <ol style="list-style-type: none"> 1 組織、組織単位、および国コード（下記参照）を入力します。 2 [署名リクエストを生成] をクリックします。 3 認証局向けの CSR ファイルをダウンロードするには、表示されるリンクをクリックします。 |
| | インポート | <p>PEM 形式の証明書ファイルを特定し、ウィザードでそれを正しいストアに追加して、vRealize Automation で使用できるようにロードします。CSR から作成された証明書をインポートする場合を除き、このオプションでは、証明書のプライベート キー、プライベート キーのパスフレーズ（ある場合）、および証明書チェーンを入力する必要があります。CA が提供した、CSR から作成された PEM をインポートする際には、プライベート キーとパスフレーズを空白のままにします。</p> |
| 共通名 | | <p>vRealize Automation アプライアンスの FQDN です。</p> <p>複数のアプライアンスの前にロード バランサが置かれた高可用性エンタープライズ展開では、ロード バランサの FQDN になります。</p> |
| 組織 | | 規模の大きい部門またはビジネス部門を表すテキストを入力します。 |
| 組織単位 | | 規模の小さい部門またはワークグループを表すテキストを入力します。 |
| 国コード | | 運用する国の省略名を入力します。 |
| シリアル | | 英数字の一意の識別子 |
| フィンガープリント | | 証明書の特定や別の証明書との比較に使用される、一意の英数字文字列 |
| 有効期限開始日 | | 証明書が有効になる日時を示すタイムスタンプ |
| 有効期限終了日 | | 証明書が無効になる日時を示すタイムスタンプ |

Web 証明書

[Web 証明書] ページでは、IaaS Web サーバが使用する認証証明書を作成または選択します。vRealize Automation アプライアンスは、Web サーバに接続し、それを認証および信頼する必要があります。

| 設定 | | 説明 |
|-----------|--------|--|
| 証明書のアクション | 既存を保持 | この IaaS Web サーバの既存の証明書を使用します。シリアル番号やフィンガープリントなどの詳細を、下のエントリで確認してください。 |
| | 証明書の生成 | ウィザードを使用して、IaaS Web サーバの自己署名証明書を生成します。 |

| 設定 | | 説明 |
|-----------|--------------|--|
| | 署名リクエストの生成 | <p>認証局 (CA) 向けの証明書署名リクエスト (CSR) ファイルを作成します。CSR により、認証局 (CA) が正しい値で証明書を作成し、これをインポートすることが可能になります。</p> <ol style="list-style-type: none"> 1 組織、組織単位、および国コード（下記参照）を入力します。 2 [署名リクエストを生成] をクリックします。 3 認証局向けの CSR ファイルをダウンロードするには、表示されるリンクをクリックします。 |
| | インポート | <p>PEM 形式の証明書ファイルを特定し、ウィザードでそれを正しいストアに追加して、vRealize Automation で使用できるようにロードします。CSR から作成された証明書をインポートする場合を除き、このオプションでは、証明書のプライベート キー、プライベート キーのパスフレーズ（ある場合）、および証明書チェーンを入力する必要があります。CA が提供した、CSR から作成された PEM をインポートする際には、プライベート キーとパスフレーズを空白のままにします。</p> |
| | 証明書サムプリントを付与 | すでに正しいストアに追加されている証明書をロードします。 |
| 共通名 | | <p>IaaS Web サーバの FQDN です。</p> <p>複数の Web サーバの前にロード バランサが置かれた高可用性エンタープライズ展開では、ロード バランサの FQDN になります。</p> |
| 組織 | | 規模の大きい部門またはビジネス部門を表すテキストを入力します。 |
| 組織単位 | | 規模の小さい部門またはワークグループを表すテキストを入力します。 |
| 国コード | | 運用する国の省略名を入力します。 |
| シリアル | | 英数字の一意の識別子 |
| フィンガープリント | | 証明書の特定や別の証明書との比較に使用される、一意の英数字文字列 |
| 有効期限開始日 | | 証明書が有効になる日時を示すタイムスタンプ |
| 有効期限終了日 | | 証明書が無効になる日時を示すタイムスタンプ |

マネージャ サービス証明書

(エンタープライズ展開のみ) [マネージャ サービス証明書] ページでは、vRealize Automation IaaS のマネージャ サービス ホストが使用する認証証明書を作成または選択します。他の IaaS Windows サーバは、マネージャ サービス ホストに接続し、それを認証および信頼する必要があります。

このページは、IaaS Web サーバから別のマシン上のマネージャ サービスをホストする場合にのみ表示されます。同じマシン上でホストする場合は、Web 証明書が両方のロールの認証を提供します。

| 設定 | | 説明 |
|-----------|--------|--|
| 証明書のアクション | 既存を保持 | この IaaS マネージャ サービス ホスト上の既存の証明書を使用します。シリアル番号やフィンガープリントなどの詳細を、下のエントリで確認してください。 |
| | 証明書の生成 | ウィザードを使用して、IaaS マネージャ サービス ホストの自己署名証明書を生成します。 |

| 設定 | 説明 |
|--------------|--|
| 署名リクエストを生成 | <p>認証局 (CA) 向けの証明書署名リクエスト (CSR) ファイルを作成します。CSR により、認証局 (CA) が正しい値で証明書を作成し、これをインポートすることが可能になります。</p> <ol style="list-style-type: none"> 1 組織、組織単位、および国コード（下記参照）を入力します。 2 [署名リクエストを生成] をクリックします。 3 認証局向けの CSR ファイルをダウンロードするには、表示されるリンクをクリックします。 |
| インポート | <p>PEM 形式の証明書ファイルを特定し、ウィザードでそれを正しいストアに追加して、vRealize Automation で使用できるようにロードします。CSR から作成された証明書をインポートする場合を除き、このオプションでは、証明書のプライベート キー、プライベート キーのパスフレーズ（ある場合）、および証明書チェーンを入力する必要があります。CA が提供した、CSR から作成された PEM をインポートする際には、プライベート キーとパスフレーズを空白のままにします。</p> |
| 証明書サムプリントを付与 | すでに正しいストアに追加されている証明書をロードします。 |
| 共通名 | <p>laaS マネージャ サービス ホストの FQDN です。</p> <p>複数のマネージャ サービス ホストの前にロード バランサが置かれた高可用性エンタープライズ展開では、ロードバランサの FQDN になります。</p> |
| 組織 | 規模の大きい部門またはビジネス部門を表すテキストを入力します。 |
| 組織単位 | 規模の小さい部門またはワークグループを表すテキストを入力します。 |
| 国コード | 運用する国の省略名を入力します。 |
| シリアル | 英数字の一意の識別子 |
| フィンガープリント | 証明書の特定や別の証明書との比較に使用される、一意の英数字文字列 |
| 有効期限開始日 | 証明書が有効になる日時を示すタイムスタンプ |
| 有効期限終了日 | 証明書が無効になる日時を示すタイムスタンプ |

ロード バランサ

(エンタープライズ展開環境のみ) [ロード バランサ] ページでは、vRealize Automation メンバー システムのプールに合わせて、適切にロード バランサを設定します。

ロード バランサのリストでは、情報のみが表示されます。これまでにウィザードに入力した内容に基づいて、展開に含まれる各ロード バランサと、そのメンバー、コンポーネント ロール、FQDN、およびポート番号が示されます。

ここで一時停止し、ロード バランサにログインして、リストに基づいて vRealize Automation メンバーを追加し、ポートを開きます。

検証

[検証] ページでは、vRealize Automation インストールを続行できることを確認します。

すべての vRealize Automation コンポーネント、ロール、およびアカウントが正しいことと、システムが相互に認証できることを確認するには、[検証] をクリックします。環境によっては、この処理に 30 分以上かかる場合があります。

エラーが発生した場合は、障害が発生した項目を展開し、表示されているステータスとメッセージに応じて修正します。検証に合格するまで、vRealize Automation インストールを続行することはできません。

スナップショットの作成

スナップショットの作成ページでは、インストールを続行する前に、すべての vRealize Automation コンポーネントの仮想マシン スナップショットを作成します。

検証にパスした場合でも、インストールに関連する予測できない問題に備えることをお勧めします。インストールを開始する前に、vSphere クライアントを使用して、すべての vRealize Automation アプライアンスおよび IaaS Windows サーバのスナップショットを作成します。これを行わないと、インストール前の時点に戻るために、ウィザード設定のすべてを再入力する必要があります。

十分なリソースがある場合は、稼働中の仮想マシンのスナップショットを作成できます。スナップショットの作成前に、仮想マシンを停止することをお勧めします。

- 1 インストール ウィザードの右上にある [ログアウト] をクリックします。

重要: [ログアウト] せずにウィザードを閉じると、ウィザードを再度開くことができません。

- 2 vSphere で、すべての vRealize Automation アプライアンスおよび IaaS Windows サーバのゲスト OS をシャットダウンします。
 - 3 仮想マシンを右クリックし、[スナップショットの作成] を選択します。
 - 4 スナップショットの名前を付けます。
 - 5 仮想マシン メモリをスナップショットに含めるには、[仮想マシン メモリのスナップショット作成] を選択します。
 - 6 [OK] をクリックします。
- スナップショットが作成されるまで待機します。
- 7 すべての vRealize Automation アプライアンスおよび IaaS Windows サーバのゲスト OS をパワーオンします。
 - 8 root として再度ログインし、インストール ウィザードの [スナップショット] ページに戻ります。

`https://<vrealize-automation-appliance-FQDN>:5480`

インストールの詳細

インストールの詳細ページでは、vRealize Automation のインストールを開始するか、問題が発生した場合は再試行します。

インストールを開始するには、[インストール] をクリックします。環境によっては、インストールに 1 時間以上かかる場合があります。

インストール中またはインストール後に、[ログの収集] ボタンをクリックできます。

- ログを収集すると、ステータス テーブルの上に ZIP ファイルのダウンロード リンクが表示されます。

- ログを複数回収集する場合は、収集するたびに前回収集されたログが上書きされます。

現在のログが必要な場合は、[ログの収集] を再度クリックする前にログをダウンロードしてください。

問題が発生した場合、ウィザードはインストールを停止し、問題の修正に関するメッセージを表示します。メッセージを読んで修正内容を確認した後、場合によっては、事前に作成したスナップショットに戻す必要があります。

スナップショットに戻さない

ウィザードで [インストールの再試行] が可能である場合は、マシンをスナップショットに戻さずに、修正を行ってインストールを再試行できます。

修正を行った後、[インストールの再試行] をクリックします。

laaS Windows サーバをスナップショットに戻す

ウィザードで [laaS をすべて再試行] が可能な場合は、次の手順を実行します。

- 1 vSphere で、すべての laaS Windows マシンを前のウィザード ページで作成したスナップショットに戻します。
- 2 シャットダウン後にスナップショットを作成した場合は、ゲスト OS をパワーオンします。
- 3 外部 SQL Server を使用した場合は、vRealize Automation SQL データベースを削除します。
- 4 修正を行います。
- 5 [laaS をすべて再試行] をクリックします。

アプライアンスおよび laaS Windows サーバをスナップショットに戻す

ウィザードに vRealize Automation アプライアンスに関するメッセージが表示された場合は、次の手順を実行します。

- 1 vSphere で、すべての vRealize Automation アプライアンスおよび laaS Windows マシンを前のウィザード ページで作成したスナップショットに戻します。
- 2 シャットダウン後にスナップショットを作成した場合は、ゲスト OS をパワーオンします。
- 3 外部 SQL Server を使用した場合は、vRealize Automation SQL データベースを削除します。
- 4 修正を行います。
- 5 root として再度ログインして、インストール ウィザードに戻ります。

`https://<vrealize-automation-appliance-FQDN>:5480`

- 6 インストールの詳細ページに戻り、[インストール] をクリックします。

ライセンス

[ライセンス] ページでは、インストールされた vRealize Automation 製品を有効化するためのキーを入力します。

[新規ライセンス キー] にキーを入力し、[キーを送信] をクリックします。スタンドアローンの vRealize Automation、vRealize Suite、vRealize Business for Cloud、および vRealize Code Stream のキーを含め、1 つ以上のキーを個別に送信できます。

このページでは、vRealize Code Stream を有効にするかどうかを選択します。vRealize Code Stream は高可用性または本番 vRealize Automation 環境ではサポートされていないため、vRealize Code Stream 管理パックが必要です。詳細については、[vRealize Code Stream のライセンス](#) を参照してください。

テレメトリ

テレメトリのページでは、vRealize Automation で、カスタマ エクスペリエンス改善プログラムの一部として使用量の統計を VMware に送信するかどうかを決定します。

カスタマ エクスペリエンス改善プログラム (CEIP) に参加するオプションをオンまたはオフにします。

詳細については、[カスタマ エクスペリエンス改善プログラム](#)を参照してください。

インストール後のオプション

[インストール後のオプション] ページには、新しい vRealize Automation データを作成するオプション、または古い環境のデータを新規インストールに移行するオプションがあります。

- [初期コンテンツの構成] では、デフォルト テナントの新しいローカル ユーザーを作成します。作成したローカル ユーザーは、デフォルト テナントで構成プロセスを開始できます。

このオプションを使用するには、少なくとも 1 台の vSphere エンドポイントを、インストール ウィザードの [エージェント] ページに追加している必要があります。
- [環境の移行] では、古い vRealize Automation データを新しくインストールした環境に転送します。移行では、グループ、ブループリント、エンドポイントなどの重要な要素が保持されます。
- [続行] を選択すると、インストール ウィザードの最後に移動します。

初期コンテンツの設定

初期コンテンツの設定ページで、新しいローカルの vRealize Automation デフォルト テナント ユーザーを作成します。このユーザーは、vSphere エンドポイントのコンテンツ ワークフローを開始できます。

注: このオプションは、少なくとも 1 台の vSphere エンドポイントを [エージェント] ページで以前に追加した場合にのみ使用できます。

新規のローカル ユーザー名は、configurationadmin です。vRealize Automation は、configurationadmin に次の権限を付与します。

- テナント管理者
- IaaS 管理者
- 承認管理者
- カタログ管理者
- インフラストラクチャ アーキテクト
- XaaS アーキテクト
- vRealize Orchestrator 管理者

configurationadmin のログイン パスワードを入力し、確認します。configurationadmin がデフォルト テナントにログインした後に構成プロセスを開始できるようにカタログ アイテムを生成するには、[初期コンテンツの作成] をクリックします。

移行の設定

移行の設定ページでは、新規にインストールした環境へ、別の古い vRealize Automation 環境を転送できます。

古い環境を移行する前に、次のガイドラインを確認します。

- 古い環境の製品バージョンに関連する vRealize Automation 移行ガイドを十分に確認します。前提条件やその他の詳細が異なる場合があります。
- 新しい環境の VMware Identity Manager に、古いテナントおよび ID ストアを移行します。
- 古い IaaS SQL Server データベースのクローンを作成し、新しい環境の IaaS データベースにリストアします。クローン作成されたデータベースの名前を確認します。
- 古い IaaS SQL Server データベースの暗号化キーを取得し、メモします。
- 移行したデータを再暗号化するための新しいパスフレーズを作成し、メモします。
- 古い vRealize Automation アプライアンスまたはロード バランサの完全修飾ドメイン名 (FQDN) と root のログイン認証情報を確認します。
- 新しい環境の root のログイン認証情報をメモします。

標準 vRealize Automation インストール インターフェイス

インストール ウィザードの実行後、標準インターフェイスから、特定のインストール タスクの手動による実行が必要になることがあります。

「[インストール ウィザードを使用した vRealize Automation のインストール](#)」で説明されているインストール ウィザードは、新しい vRealize Automation インストールのための基本ツールです。ただし、このウィザードを実行した後も、一部の処理については従来の手動インストール プロセスが必要になります。

vRealize Automation 展開を拡張する場合や、ウィザードが何らかの理由で停止した場合は、手動の手順が必要です。次のような例において、このセクションに記載されている手順を参照する必要があります。

- インストールが完了する前にウィザードをキャンセルした場合。
- ウィザードによるインストールに失敗した場合。
- 高可用性のために別の vRealize Automation アプライアンスを追加する場合。
- 高可用性のために別の IaaS Web サーバを追加する場合。
- 別のプロキシ エージェントが必要な場合。
- 別の DEM ワーカーまたは Orchestrator が必要な場合。

手動によるプロセスは、すべてを使用することも一部のみを使用することもできます。このセクション全体の内容を確認し、該当する状況に適用される手順に従ってください。

最小インストールでの標準インターフェイスの使用

開発環境での使用または POC（事前検証）環境用に、スタンドアロンの最小インストールを実行できます。最小インストールは、本番環境には適していません。

最小インストールのチェックリスト

事前検証（POC）または開発作業のために、vRealize Automation を最小構成でインストールします。最小インストールは少ない手順でインストールできますが、エンタープライズ展開が備えている本番環境の容量はありません。

次の順序で、高レベルのタスクを完了します。

表 1-27. 最小インストールのチェックリスト

| タスク | 詳細 |
|--|---|
| <input type="checkbox"/> 環境を計画し、インストールの前提条件を満たすよう対応します。 | [vRealize Automation のインストールの準備] |
| <input type="checkbox"/> 未構成の vRealize Automation アプライアンスを作成します。 | [vRealize Automation アプライアンスの展開] |
| <input type="checkbox"/> vRealize Automation アプライアンスを手動で構成します。 | [vRealize Automation アプライアンスの構成] |
| <input type="checkbox"/> IaaS コンポーネントを単一の Windows サーバにインストールします。 | [IaaS コンポーネントのインストール] |
| <input type="checkbox"/> 必要に応じて、追加のエージェントをインストールします。 | [vRealize Automation エージェントのインストール] |
| <input type="checkbox"/> デフォルト テナントの構成などインストール後のタスクを実行します。 | [デフォルト テナントへのアクセスの構成] |

vRealize Automation アプライアンスの構成

vRealize Automation アプライアンスは、vRealize Automation サーバとユーザーの Web ポータルをホストする、部分的に構成された仮想マシンです。アプライアンスの Open Virtualization Format (OVF) テンプレートを vCenter Server または ESX/ESXi インベントリにダウンロードして展開します。

前提条件

- 未構成のアプライアンスを作成します。[\[vRealize Automation アプライアンスの展開\]](#) を参照してください。
- vRealize Automation アプライアンスの認証証明書を取得します。

手順

- 1 未構成の vRealize Automation アプライアンス管理インターフェイスに root としてログインします。

`https://<vrealize-automation-appliance-FQDN>:5480`

証明書の警告を無視して続行します。

- 2 インストール ウィザードが表示された場合はキャンセルし、ウィザードではなく管理インターフェイスに進むことができるようにします。
- 3 [管理] - [時刻設定] の順に選択し、時刻同期ソースを設定します。

| オプション | 説明 |
|---------|--|
| ホストの時刻 | vRealize Automation アプライアンスの ESXi ホストに同期します。 |
| タイム サーバ | 単一の外部 Network Time Protocol (NTP) サーバに同期します。NTP サーバの FQDN または IP アドレスを入力します。 |

vRealize Automation アプライアンスおよび IaaS Windows サーバを同一の時刻ソースに同期させる必要があります。vRealize Automation 展開内で時刻ソースを混在させないでください。

4 [vRA 設定] - [ホストの設定] の順に選択します。

| オプション | アクション |
|--------------|---|
| [自動的に解決] | [自動的に解決] を選択し、vRealize Automation アプライアンス の現在のホストの名前を指定します。 |
| [ホストをアップデート] | 新しいホストの場合、[ホストをアップデート] を選択します。[ホスト名] テキスト ボックスに vRealize Automation アプライアンス の完全修飾ドメイン名である <vra-hostname.domain.name> を入力します。 ロード バランサを使用する分散デプロイの場合、[ホストをアップデート] を選択します。[ホスト名] テキスト ボックスにロード バランサ サーバの完全修飾ドメイン名である <vra-loadbalancename.domain.name> を入力します。 |

注: [ホストをアップデート] を使用してホスト名を設定するときは常に、この手順で後述する SSO 設定を構成します。

5 [証明書のアクション] メニューから証明書タイプを選択します。

分散環境などにおいて PEM でエンコードされた証明書を使用している場合は、[インポート] を選択します。

インポートする証明書は、信頼されており、SAN (Subject Alternative Name) 証明書を使用することによって vRealize Automation アプライアンスおよび任意のロード バランサのすべてのインスタンスに適用可能である必要があります。

認証局に送信可能な新しい証明書の CSR 要求を生成するには、[署名リクエストを生成] を選択します。CSR により、認証局 (CA) が正しい値で証明書を作成し、これをインポートすることが可能になります。

注: 証明書チェーンを使用する場合は、次の順序で証明書を指定します。

- a 中間 CA 証明書によって署名されたクライアント/サーバ証明書
- b 1 つ以上の中間証明書
- c ルート CA 証明書

| オプション | アクション |
|--------|---|
| 既存を保持 | 現在の SSL 設定のままにします。このオプションを選択して変更をキャンセルします。 |
| 証明書の生成 | <ol style="list-style-type: none"> a [共通名] テキスト ボックスに表示される値は、ページ上部に表示されるホスト名です。vRealize Automation アプライアンスの追加インスタンスが利用可能な場合は、証明書の SAN 属性にそれらの FQDN が含められます。 b 会社名などの組織名を [組織] テキスト ボックスに入力します。 c 部署名や場所などの組織単位を [組織単位] テキスト ボックスに入力します。 d JP などの 2 文字の ISO 3166 国コードを [国] テキスト ボックスに入力します。 |

| オプション | アクション |
|------------|---|
| 署名リクエストを生成 | <p>a [署名リクエストを生成] を選択します。</p> <p>b [組織]、[組織単位]、[国コード]、[共通名] の各テキスト ボックスの入力内容を確認します。これらは既存の証明書から入力されています。必要に応じて編集できます。</p> <p>c [CSR を生成] をクリックして証明書署名リクエストを生成してから、[生成された CSR をここにダウンロード] リンクをクリックします。ダイアログ ボックスが開くので、認証局に送信するために CSR を保存する場所を指定します。</p> <p>d 完成した証明書を受け取ったら、[インポート] をクリックし、指示のとおり操作して証明書を vRealize Automation にインポートします。</p> |
| インポート | <p>a ヘッダおよびフッタを含む証明書値を BEGIN PRIVATE KEY から END PRIVATE KEY にコピーし、それらを [RSA プライベート キー] テキスト ボックスに貼り付けます。</p> <p>b ヘッダおよびフッタを含む証明書値を BEGIN CERTIFICATE から END CERTIFICATE にコピーし、それらを [証明書チェーン] テキスト ボックスに貼り付けます。複数の証明書値の場合は、各証明書に BEGIN CERTIFICATE ヘッダと END CERTIFICATE フッタを含めます。</p> <p>注: チェーン証明書の場合は、追加の属性が使用可能になることがあります。</p> <p>c (オプション) 証明書でパス フレーズを使用して証明書キーを暗号化する場合、そのパス フレーズをコピーし、[パスフレーズ] テキスト ボックスに貼り付けます。</p> |

6 [設定の保存] をクリックして、ホスト情報と SSL 構成を保存します。

7 SSO 設定を構成します。

8 [メッセージング] をクリックします。アプライアンスのメッセージングの構成設定と状態が表示されます。これらの設定は変更しないでください。

9 [テレメトリ] タブをクリックして、VMware カスタマ エクスペリエンス改善プログラム (CEIP) に参加するかどうかを選択します。

CEIP によって収集されるデータの詳細と、VMware がそのデータを使用する目的については、Trust & Assurance Center (<http://www.vmware.com/trustvmware/ceip.html>) を参照してください。

- このプログラムに参加するには、[VMware カスタマ エクスペリエンス改善プログラムに参加] を選択します。
- このプログラムに参加しない場合は、[VMware カスタマ エクスペリエンス改善プログラムに参加] を選択解除します。

10 [サービス] をクリックし、サービスが登録されていることを確認します。

サイトの構成に応じて、これには約 10 分かかる可能性があります。

注: アプライアンスにログインして `tail -f /var/log/vcac/catalina.out` を実行することにより、サービスの起動を監視できます。

11 ライセンス情報を入力してください。

- a [vRA 設定 > ライセンス] の順にクリックします。
- b [ライセンス] をクリックします。
- c インストール ファイルをダウンロードしたときにダウンロードした有効な vRealize Automation ライセンス キーを入力し、[送信キー] をクリックします。

注: 接続エラーが発生した場合、ロード バランサに問題がある可能性があります。ロード バランサへのネットワーク接続を確認してください。

12 vRealize Code Stream を有効にするかどうかを選択し、vRealize Code Stream ライセンスを入力します。

高可用性または本番の vRealize Automation 環境では、vRealize Code Stream はサポートされていません。

13 vRealize Automation にログインできることを確認します。

- a Web ブラウザを開き、vRealize Automation 製品のインターフェイス URL にアクセスします。
`https://<vrealize-automation-appliance-FQDN>/vcac`
- b vRealize Automation 証明書を受け入れます。
- c SSO 証明書を受け入れます。
- d administrator@vsphere.local と、SSO の構成時に指定したパスワードを使用してログインします。
 インターフェイスで、[テナント] ページの [管理] タブが開きます。リストに vsphere.local というテナントが 1 つだけ表示されます。

vRealize Automation アプライアンス の展開と構成の作業が完了しました。構成後にアプライアンスが正常に機能しない場合、アプライアンスの展開と構成をもう一度行ってください。既存のアプライアンスは変更しないでください。

次のステップ

[「インフラストラクチャ コンポーネントのインストール」](#) を参照してください。

IaaS コンポーネントのインストール

管理者は、インフラストラクチャ (IaaS) コンポーネントの完全なセットを（物理的または仮想的な）Windows マシンにインストールします。これらのタスクを実行するには管理者権限が必要です。

最小インストールでは、別のサーバにインストールできる SQL データベース以外の、同じ Windows サーバ上のすべてのコンポーネントをインストールします。

Windows Server での時刻同期の有効化

インストールを正常に行うには、vRealize Automation サーバと Windows サーバのクロックを同期させる必要があります。

次の手順では、VMware Tools を使用して ESX/ESXi ホストとの時刻同期を有効にする方法を説明します。物理ホストに IaaS コンポーネントをインストールする場合や、時刻同期に VMware Tools を使用しない場合には、希望する方法を使用してサーバの時刻が確実に正確となるようにします。

手順

- 1 Windows インストール マシンでコマンド プロンプトを開きます。
- 2 次のコマンドを入力して VMware Tools ディレクトリに移動します。

```
cd C:\Program Files\VMware\VMware Tools
```

- 3 次のコマンドを入力して timesync ステータスを表示します。

```
VMwareToolboxCmd.exe timesync status
```

- 4 timesync が無効にされている場合、次のコマンドを入力して有効化します。

```
VMwareToolboxCmd.exe timesync enable
```

IaaS 証明書

vRealize Automation IaaS コンポーネントは証明書および SSL を使用してコンポーネント間の通信を保護します。POC（事前検証）を目的とした 最小インストールでは、自己署名証明書を使用できます。

分散環境で、信頼できる認証局からドメイン証明書を取得します。IaaS コンポーネントのドメイン証明書の詳細については、分散インストールの章の [「IaaS 証明書のインストール」](#) を参照してください。

インフラストラクチャ コンポーネントのインストール

システム管理者は Windows マシンにログインし、インストール ウィザードを使用して Windows 仮想マシンまたは物理マシンに IaaS サービスをインストールします。

前提条件

- サーバが [「IaaS Windows サーバ」](#) に示されている要件を満たしていることを確認します。
- [「Windows Server での時刻同期の有効化」](#)。
- vRealize Automation アプライアンスを展開して完全に構成し、必要なサービス（プラグイン サービス、カタログ サービス、IaaS プロキシ プロバイダ）が実行していることを確認します。

手順

- 1 [vRealize Automation IaaS インストーラのダウンロード](#)

最小限の仮想または物理 Windows サーバ上に IaaS をインストールするには、IaaS インストーラのコピーを vRealize Automation アプライアンスからダウンロードします。

- 2 [インストール タイプの選択](#)

システム管理者は、Windows 2008 または 2012 インストール マシンからインストール ウィザードを実行します。

- 3 [前提条件の確認](#)

前提条件チェッカーは、マシンが IaaS インストール要件を満たしていることを確認します。

4 サーバおよびアカウントの設定の指定

vRealize Automation システム管理者は、Windows インストール サーバのサーバおよびアカウント設定を指定し、SQL データベース サーバ インスタンスおよび認証方法を選択します。

5 マネージャおよびエージェントの指定

最小インストールでは、必要な Distributed Execution Manager とデフォルトの vSphere プロキシ エージェントをインストールします。システム管理者は、インストール後にカスタム インストーラを使用して、追加のプロキシ エージェント (XenServer または Hyper-V など) をインストールできます。

6 IaaS コンポーネントの登録

システム管理者は、IaaS 証明書をインストールし、IaaS コンポーネントを SSO に登録します。

7 インストールの完了

システム管理者は IaaS のインストールを完了します。

vRealize Automation IaaS インストーラのダウンロード

最小限の仮想または物理 Windows サーバ上に IaaS をインストールするには、IaaS インストーラのコピーを vRealize Automation アプライアンスからダウンロードします。

この処理中に証明書の警告が表示された場合、それらを無視して続行しインストールを完了させます。

前提条件

- IaaS Windows サーバの要件を確認します。[「IaaS Windows サーバ」](#) を参照してください。
- ダウンロードに Internet Explorer を使用する場合、厳密なセキュリティ設定が有効になっていないことを確認します。Windows サーバで **res://iesetup.dll/SoftAdmin.htm** に移動します。

手順

- 1 管理者権限を備えたアカウントを使用して IaaS Windows サーバにログインします。
- 2 Web ブラウザを開いて vRealize Automation アプライアンス インストーラ URL にアクセスします。
`https://<vrealize-automation-appliance-FQDN>:5480/installer`
- 3 [IaaS インストーラ] をクリックします。
- 4 **setup__<vrealize-automation-appliance-FQDN>@5480** を Windows サーバに保存します。
インストーラ ファイル名は変更しないでください。インストールの vRealize Automation アプライアンスへの接続に使用されます。

インストール タイプの選択

システム管理者は、Windows 2008 または 2012 インストール マシンからインストール ウィザードを実行します。

前提条件

[「vRealize Automation IaaS インストーラのダウンロード」](#)。

手順

- 1 セットアップ ファイル `setup__<vrealize-automation-appliance-FQDN>@5480.exe` を右クリックして、[管理者として実行] を選択します。
- 2 [次へ] をクリックします。
- 3 使用許諾契約に同意し、[次へ] をクリックします。
- 4 ログイン ページで vRealize Automation アプライアンスの管理者認証情報を入力し、SSL 証明書を確認します。
 - a ユーザー名 (**root**) とパスワードを入力します。
 入力するパスワードは、vRealize Automation アプライアンスを展開したときに指定したパスワードです。
 - b [証明書の受け入れ] を選択します。
 - c [証明書の表示] をクリックします。
 証明書のサムプリントを、vRealize Automation アプライアンスに設定されているサムプリントと比較します。管理コンソールにポート 5480 でアクセスしている場合は、クライアント ブラウザで vRealize Automation アプライアンス証明書を表示できます。
- 5 [証明書の受け入れ] を選択します。
- 6 [次へ] をクリックします。
- 7 [完全なインストール] を [インストール タイプ] ページで選択し、[次へ] をクリックします。

前提条件の確認

前提条件チェッカーは、マシンが IaaS インストール要件を満たしていることを確認します。

前提条件

[「インストール タイプの選択」](#)。

手順

- 1 前提条件チェックを完了します。

| オプション | 説明 |
|-----------|---|
| エラーなし | [次へ] をクリックします。 |
| 重要性が低いエラー | [バイパス] をクリックします。 |
| 重大なエラー | 重大なエラーを無視するとインストールの失敗の原因となります。警告が表示された場合は、左側のペインの警告を選択し、右側の指示に従います。すべての重大なエラーに対処し、[再チェック] をクリックして検証します。 |

- 2 [次へ] をクリックします。

マシンはインストール要件を満たしています。

サーバおよびアカウントの設定の指定

vRealize Automation システム管理者は、Windows インストール サーバのサーバおよびアカウント設定を指定し、SQL データベース サーバ インスタンスおよび認証方法を選択します。

前提条件

[「前提条件の確認」](#)。

手順

- 1 **[サーバおよびアカウントの設定]** ページまたは **[検出された設定]** ページで、Windows サービス アカウントのユーザー名とパスワードを入力します。このサービス アカウントは、SQL 管理者権限も備えたローカル管理者アカウントでなければなりません。

- 2 **[パズフレーズ]** テキスト ボックスにパズフレーズを入力します。

パズフレーズは、データベースのデータの保護に使用される暗号化キーを生成する一連の語句です。

注: 以降のインストールやシステム リカバリに使用できるようにパズフレーズを保存します。

- 3 IaaS コンポーネントと同じサーバにデータベース インスタンスをインストールするには、**[SQL Server データベースのインストール情報]** セクションにある **[サーバ]** テキスト ボックスのデフォルト サーバを受け入れます。データベースが別のマシンに存在する場合は、次の形式でサーバを入力します。

<machine-FQDN,port-number\named-database-instance>

- 4 **[データベース名]** テキスト ボックスのデフォルト値を受け入れるか、必要に応じて適切な名前を入力します。

- 5 認証方法を選択します。

- ◆ 現在のユーザーの Windows 認証情報を使用してデータベースを作成する場合は、**[Windows 認証の使用]** を選択します。ユーザーには SQL sys_admin 権限が必要です。
- ◆ SQL 認証を使用してデータベースを作成する場合は、**[Windows 認証の使用]** を選択解除します。SQL サーバ インスタンスに対する SQL sys_admin 権限を持つ SQL Server ユーザーの **[ユーザー名]** および **[パスワード]** を入力します。

Windows 認証が推奨されています。SQL 認証を選択すると、特定の構成ファイルで暗号化されていないデータベース パスワードが表示されます。

- 6 (オプション) **[データベース接続に SSL を使用]** チェックボックスを選択します。

デフォルトでは、このチェックボックスは有効になっています。SSL を使用すると、IaaS サーバと SQL データベースの間の接続の安全性が強化されます。ただし、このオプションをサポートするには、SQL Server に SSL を構成する必要があります。SQL Server での SSL 構成の詳細については、[Microsoft Technet の記事 189067](#) を参照してください。

- 7 **[次へ]** をクリックします。

マネージャおよびエージェントの指定

最小インストールでは、必要な Distributed Execution Manager とデフォルトの vSphere プロキシ エージェントをインストールします。システム管理者は、インストール後にカスタム インストーラを使用して、追加のプロキシ エージェント (XenServer または Hyper-V など) をインストールできます。

前提条件

[「サーバおよびアカウントの設定の指定」](#)。

手順

- 1 **[Distributed Execution Manager とプロキシ vSphere エージェント]** ページで、デフォルト値を受け入れるか、必要に応じて名前を変更します。
- 2 デフォルト値を受け入れて vSphere エージェントをインストールし、vSphere を使用したプロビジョニングを有効にするか、必要に応じて選択解除します。
 - a [vSphere エージェントのインストールと構成] を選択します。
 - b デフォルトのエージェントおよびエンドポイントを受け入れるか、名前を入力します。

エンドポイント名の値をメモします。vRealize Automation コンソールで vSphere エンドポイントを構成する際には、この情報を正確に入力する必要があります。そうしないと構成に失敗することがあります。

- 3 **[次へ]** をクリックします。

IaaS コンポーネントの登録

システム管理者は、IaaS 証明書をインストールし、IaaS コンポーネントを SSO に登録します。

前提条件

[[vRealize Automation IaaS インストーラのダウンロード](#)]。

手順

- 1 デフォルトの [サーバ] 値を受け入れます。この値は、インストーラをダウンロードした vRealize Automation アプライアンス サーバの完全修飾ドメイン名を使用して生成されます。サーバの識別に IP アドレスではなく完全修飾ドメイン名を使用していることを確認します。

複数の仮想アプライアンスがあり、ロード バランサを使用している場合は、ロード バランサの仮想アプライアンス パスを入力します。
- 2 **[ロード]** をクリックして [SSO のデフォルト テナント] (vsphere.local) の値を取り込みます。
- 3 **[ダウンロード]** をクリックして vRealize Automation アプライアンスから証明書を取得します。

[証明書の表示] をクリックして証明書の詳細を表示できます。
- 4 **[証明書の受け入れ]** を選択して SSO 証明書をインストールします。
- 5 SSO 管理者パネルの [ユーザー名] テキストボックスに **administrator**、[パスワード] および [パスワードの確認] に SSO を構成したときにこのユーザーに対して定義したパスワードを入力します。
- 6 [ユーザー名] フィールドの右側にあるテスト リンクをクリックして、入力したパスワードを検証します。
- 7 インストールする Windows マシンのホスト名が含まれる、[IaaS サーバ] のデフォルトを受け入れます。
- 8 [IaaS サーバ] フィールドの右側にあるテスト リンクをクリックして、接続性を検証します。
- 9 **[次へ]** をクリックします。

[次へ] をクリックした後にエラーが表示された場合は、エラーを解決してから作業を続けてください。

インストールの完了

システム管理者は IaaS のインストールを完了します。

前提条件

- [「IaaS コンポーネントの登録」](#)。
- インストール先のマシンがネットワークに接続され、IaaS インストーラのダウンロード元の vRealize Automation アプライアンスに接続できることを確認します。

手順

- 1 **「インストールの準備完了」**ページの情報を確認して **「インストール」** をクリックします。

インストールが開始されます。ネットワーク構成によって異なりますが、インストールには 5 分から 1 時間かかる可能性があります。

- 2 正常に処理が行われたことを伝えるメッセージが表示されたら、**「初期構成をガイド」** チェック ボックスを選択したままにして、**「次へ」** および **「完了」** をクリックします。
- 3 **「システムの構成」** メッセージ ボックスを閉じます。

インストールが完了しました。

次のステップ

[「IaaS サービスの確認」](#)。

分散型展開での標準インターフェイスの使用

エンタープライズ展開は、本番環境におけるより容量の大きい vRealize Automation のために設計されており、複数のマシンにコンポーネントを分散させる必要があります。エンタープライズ展開でもロード バランサの背後に冗長システムが含まれている場合があります。

分散インストールのチェックリスト

システム管理者は、分散構成環境に vRealize Automation を導入して、冗長性によるフェイルオーバー保護および高可用性を実現できます。

分散インストール チェックリストでは、分散インストールの実行に必要な手順の概要が示されています。

表 1-28. 分散インストールのチェックリスト

| タスク | 詳細 |
|---|---|
| <input type="checkbox"/> インストール環境を計画して準備し、すべてのインストール前提条件を満たしていることを確認します。 | 「vRealize Automation のインストールの準備」 |
| <input type="checkbox"/> SSL 証明書の計画を立て、SSL 証明書を取得します。 | 「分散型展開における証明書の信頼性の要件」 |
| <input type="checkbox"/> 最初に vRealize Automation アプライアンス サーバを展開し、冗長性と高可用性のために必要とされる追加のアプライアンスをすべて展開します。 | 「vRealize Automation アプライアンスの展開」 |
| <input type="checkbox"/> ロード バランサを vRealize Automation アプライアンスのトラフィックを処理するように構成します。 | 「ロード バランサの構成」 |
| <input type="checkbox"/> 最初に vRealize Automation アプライアンス サーバを構成し、冗長性と高可用性のために展開した追加のアプライアンスすべてを構成します。 | 「vRealize Automation のアプライアンスの構成」 |

表 1-28. 分散インストールのチェックリスト (続き)

| タスク | 詳細 |
|---|---|
| <input type="checkbox"/> ロード バランサを vRealize Automation IaaS コンポーネント トラフィックを処理するように構成し、vRealize Automation IaaS コンポーネントをインストールします。 | 「分散構成への IaaS コンポーネントのインストール」 |
| <input type="checkbox"/> 必要に応じて、外部システムと統合するエージェントをインストールします。 | 「vRealize Automation エージェントのインストール」 |
| <input type="checkbox"/> デフォルトのテナントを構成し、IaaS ライセンスを提供します。 | 「デフォルト テナントへのアクセスの構成」 |

vRealize Orchestrator

vRealize Automation アプライアンスには、新しいインストールでの使用に推奨される vRealize Orchestrator の組み込みバージョンが含まれています。ただし、古い展開の場合または特別な状況では、vRealize Automation を個別の外部 vRealize Orchestrator に接続することができます。<https://www.vmware.com/products/vrealize-orchestrator.html> を参照してください。

vRealize Automation と vRealize Orchestrator の接続については、[vRealize Automation 用の VMware vRealize Orchestrator プラグイン](#) を参照してください。

ディレクトリ管理

高可用性やフェイルオーバー用のロード バランサを含む分散インストールを実行する場合は、vRealize Automation 環境の構成を担当するチームにご相談ください。テナント管理者は、Active Directory へのリンクを設定するとき、ディレクトリ管理を高可用性向けに構成する必要があります。

ロード バランサの健全性チェックを無効にする

健全性チェックは、ロード バランサによって動作しているノードのみにトラフィックが送信されていることを確認します。ロード バランサは、指定された頻度ですべてのノードに健全性チェックを送信します。エラーしきい値を超えたノードは、新たなトラフィックを受け取る資格を失います。

ワークロードの分散化とフェイルオーバーのために、ロード バランサの背後に複数の vRealize Automation アプライアンスを配置できます。また、複数の IaaS Web サーバと IaaS Manager Service サーバをそれぞれのロード バランサの背後に配置することもできます。

ロード バランサを使用する場合は、インストールの途中でロード バランサによって健全性チェックが送信されないようにしてください。健全性チェックがインストールを妨げたり、インストールで予測できない動作が生じたりする可能性があります。

- vRealize Automation アプライアンスまたは IaaS コンポーネントを既存のロード バランサの背後に展開する際には、コンポーネントをインストールする前に、想定している設定に含まれるすべてのロード バランサで健全性チェックを無効にします。
- すべての vRealize Automation アプライアンスと IaaS コンポーネントを含む、vRealize Automation のすべての要素のインストールおよび構成の後、健全性チェックを再び有効にすることができます。

分散型展開における証明書の信頼性の要件

vRealize Automation は、証明書を使用して信頼関係を維持し、分散型展開のコンポーネント間の安全な通信を提供します。

分散型またはクラスタ化された展開では、vRealize Automation 証明書の組織の大半が vRealize Automation の 3 つの階層化アーキテクチャ構造に準拠します。3 つの階層は、vRealize Automation アプライアンス、IaaS Web サイト コンポーネント、および Manager Service コンポーネントです。分散型システムでは、特定の階層内の各ハードウェア マシンで証明書を共有します。つまり、各 vRealize Automation アプライアンス が共通の証明書を共有し、各 Manager Service マシンがそのレイヤーに適用される共通の証明書を共有します。

システムまたはユーザーが生成した自己署名証明書、または分散型 vRealize Automation 展開で認証局 (CA) が提供した証明書を使用することができます。vRealize Automation 7.0 以降、ユーザーによって証明書が提供されない場合は、インストーラが自動的にすべての該当するノードの自己署名証明書を生成し、適切なトラストストアに配置します。

分散型 vRealize Automation コンポーネントでロード バランサを使用して、高可用性およびフェイルオーバー サポートを提供することができます。vRealize Automation 展開では、ロード バランサを使用する展開にパススルー構成を使用することをお勧めします。パススルー構成では、ロード バランサは、それらを復号化するのではなく、適切なコンポーネントに合わせた要求を渡します。vRealize Automation アプライアンス および IaaS Web サーバは、必要な復号化を実行する必要があります。

ロード バランサの使用や構成に関する詳細については、「vRealize Automation のロード バランシング」を参照してください。

Openssl または別のツールを使用して独自の証明書を指定または生成する場合は、ワイルドカードまたは Subject Alternative Names (SAN) の証明書を使用できます。IaaS 証明書はマルチユースの証明書である必要があります。

証明書を指定している場合は、クラスタに IaaS コンポーネントを含むマルチユースの証明書を取得し、各コンポーネントのトラストストアにその証明書をコピーする必要があります。ロード バランサを使用する場合、クラスタのマルチユースの証明書の信頼されたアドレスにロード バランサの FQDN を含める必要があります。

ユーザーまたは CA が指定した証明書で生成された自己署名証明書をアップデートする必要がある場合は、[vRealize Automation 証明書のアップデート](#)を参照してください。

証明書の信頼性の要件を示す表に、インポートされるさまざまな証明書での信頼性の登録の要件をまとめています。

表 1-29. 証明書の信頼性の要件

| インポート | 登録 |
|----------------------------------|---|
| vRealize Automation アプライアンス クラスタ | IaaS Web コンポーネント クラスタ |
| IaaS Web コンポーネント クラスタ | <ul style="list-style-type: none"> ■ vRealize Automation アプライアンス クラスタ ■ Manager Service コンポーネント クラスタ ■ DEM Orchestrator および DEM ワーカー コンポーネント |
| Manager Service コンポーネント クラスタ | <ul style="list-style-type: none"> ■ DEM Orchestrator および DEM ワーカー コンポーネント ■ エージェントおよびプロキシ エージェント |

Web コンポーネント、Manager Service、DEM ホスト証明書の信頼性の設定

サム プリントを事前インストール済みの PFX ファイルとともに使用してユーザー認証をサポートしているユーザーは、Web ホスト、Manager Service、DEM Orchestrator およびワーカー ホスト マシンでサム プリントの信頼性を設定する必要があります。

PEM ファイルをインポートするか自己署名証明書を使用するユーザーは、この手順を無視してかまいません。

前提条件

サム プリント認証で利用できる有効な **web.pfx** および **ms.pfx**。

手順

- 1 **web.pfx** および **ms.pfx** ファイルを Web コンポーネントおよび Manager Service ホスト マシン上の以下の場所にインポートします。

- <Host Computer>/Certificates/Personal certificate store
- <Host Computer>/Certificates/Trusted People certificate store

- 2 **web.pfx** および **ms.pfx** ファイルを DEM Orchestrator およびワーカー ホスト マシン上の以下の場所にインポートします。

<Host Computer>/Certificates/Trusted People certificate store

- 3 該当するホスト マシンのそれぞれで Microsoft 管理コンソール ウィンドウを開きます。

注: 管理コンソール内の実際のパスとオプションは、Windows のバージョンやシステム構成によって若干異なる場合があります。

- a [スナップインの追加と削除] を選択します。
- b [証明書] を選択します。
- c [ローカル コンピュータ] を選択します。
- d 先ほどインポートした証明書ファイルを開き、サム プリントをコピーします。

次のステップ

Manager Service、Web コンポーネント、DEM コンポーネントについて、vRealize Automation ウィザードの証明書ページにサム プリントを挿入します。

インストール ワークシート

ワークシートには、インストール中に参照する必要がある重要な情報を記録します。

設定では大文字と小文字が区別されます。分散環境をインストールする場合に使用する、追加のコンポーネント設定も用意されています。ワークシート内のすべての情報が必要ということではありません。また、1 つのマシンで複数の IaaS コンポーネントをホストする場合もあります。たとえば、プライマリ Web サーバと DEM Orchestrator を同じ FQDN に配置する場合があります。

表 1-30. vRealize Automation アプライアンス

| 変数 | 値 | 例 |
|---|-------------------------------------|----------------------------------|
| プライマリ vRealize Automation アプライアンスの FQDN | | automation.mycompany.com |
| プライマリ vRealize Automation アプライアンスの IP アドレス | | 123.234.1.105 |
| 参照のみ。IP アドレスは入力しないでください | | |
| 追加 vRealize Automation アプライアンスの FQDN | | automation2.mycompany.com |
| 追加 vRealize Automation アプライアンスの IP アドレス | | 123.234.1.106 |
| 参照のみ。IP アドレスは入力しないでください | | |
| vRealize Automation アプライアンス ロード バランサの FQDN | | Automation-balance.mycompany.com |
| vRealize Automation アプライアンス ロード バランサの IP アドレス | | 123.234.1.201 |
| 参照のみ。IP アドレスは入力しないでください | | |
| 管理インターフェイス (https://<appliance-FQDN>:5480) のユーザー名 | root (デフォルト) | root |
| 管理インターフェイスのパスワード | | admin123 |
| デフォルトのテナント | vsphere.local (デフォルト) | vsphere.local |
| デフォルトのテナント ユーザー名 | administrator@vsphere.local (デフォルト) | administrator@vsphere.local |
| デフォルトのテナント パスワード | | login123 |

表 1-31. IaaS Windows サーバ

| 変数 | 値 | 例 |
|---|---|---------------------------|
| Model Manager Data FQDN を設定したプライマリ IaaS Web サーバ | | web.mycompany.com |
| Model Manager Data IP アドレスを設定したプライマリ IaaS Web サーバ | | 123.234.1.107 |
| 参照のみ。IP アドレスは入力しないでください | | |
| 追加の IaaS Web サーバ FQDN | | web2.mycompany.com |
| 追加の IaaS Web サーバ IP アドレス | | 123.234.1.108 |
| 参照のみ。IP アドレスは入力しないでください | | |
| IaaS Web サーバ ロード バランサ FQDN | | web-balance.mycompany.com |
| IaaS Web サーバ ロード バランサ IP アドレス | | 123.234.1.202 |
| 参照のみ。IP アドレスは入力しないでください | | |
| アクティブ IaaS Manager Service ホスト FQDN | | mgr-svc.mycompany.com |
| アクティブ IaaS Manager Service ホスト IP アドレス | | 123.234.1.109 |
| 参照のみ。IP アドレスは入力しないでください | | |

表 1-31. IaaS Windows サーバ (続き)

| 変数 | 値 | 例 |
|---|---|-------------------------------|
| パッシブ IaaS Manager Service ホスト FQDN | | mgr-svc2.mycompany.com |
| パッシブ IaaS Manager Service ホスト IP アドレス | | 123.234.1.110 |
| 参照のみ。IP アドレスは入力しないでください | | |
| IaaS Manager Service ホスト ロード バランサ FQDN | | mgr-svc-balance.mycompany.com |
| IaaS Manager Service ホスト ロード バランサ IP アドレス | | 123.234.203 |
| 参照のみ。IP アドレスは入力しないでください | | |
| IaaS サービスの場合、ホストの管理者権限を備えたドメイン アカウント | | SUPPORT\provisioner |
| アカウント パスワード | | login123 |

表 1-32. IaaS SQL Server データベース

| 変数 | 値 | 例 |
|-----------------------------------|--------------|----------|
| データベース インスタンス | | IAASSQL |
| データベース名 | vcac (デフォルト) | vcac |
| パスフレーズ (インストール、アップグレード、および移行時に使用) | | login123 |

表 1-33. IaaS Distributed Execution Manager

| 変数 | 値 | 例 |
|-------------------------|---|--------------------|
| DEM ホスト FQDN | | dem.mycompany.com |
| DEM ホスト IP アドレス | | 123.234.1.111 |
| 参照のみ。IP アドレスは入力しないでください | | |
| DEM ホスト FQDN | | dem2.mycompany.com |
| DEM ホスト IP アドレス | | 123.234.1.112 |
| 参照のみ。IP アドレスは入力しないでください | | |
| 一意の DEM Orchestrator 名 | | Orchestrator-1 |
| 一意の DEM Orchestrator 名 | | Orchestrator-2 |
| 一意の DEM ワーカー名 | | Worker-1 |
| 一意の DEM ワーカー名 | | Worker-2 |
| 一意の DEM ワーカー名 | | Worker-3 |
| 一意の DEM ワーカー名 | | Worker-4 |

ロード バランサの構成

vRealize Automation のアプライアンスの展開後、ロード バランサを設定して vRealize Automation アプライアンスの複数のインスタンス間でトラフィックを分散できます。

次のリストに、vRealize Automation トラフィックに対するロード バランサの構成に必要な一般的な手順の概要を示します。

- 1 ロード バランサをインストールします。
- 2 セッション アフィニティ（スティッキー セッションとも呼ばれる）を有効にします。
- 3 ロード バランサのタイムアウトは、必ず 100 秒以上に指定してください。
- 4 ネットワークまたはロード バランサで必要な場合は、証明書をロード バランサにインポートします。信頼関係と証明書の詳細については、「[分散型展開における証明書の信頼性の要件](#)」を参照してください。証明書の抽出の詳細については、「[証明書とプライベート キーの抽出](#)」を参照してください。
- 5 vRealize Automation アプライアンス トラフィックに対するロード バランサを構成します。
- 6 vRealize Automation のアプライアンスを構成します。「[vRealize Automation のアプライアンスの構成](#)」を参照してください。

注: ロード バランサの下に仮想アプライアンスを設定するのは、仮想アプライアンスが、vRealize Automation とともに使用するように構成されている場合のみにしてください。未構成のアプライアンスが設定されていると、フォールト応答が返されます。

ロード バランサの詳細については、[vRealize Automation のロード バランシング](#)を参照してください。

スケーラビリティと高可用性については、『VMware vRealize Automation リファレンス アーキテクチャ』ガイドを参照してください。

vRealize Automation のアプライアンスの構成

アプライアンスの展開およびロード バランシングの構成後、vRealize Automation のアプライアンスを構成します。

クラスタ内の最初の vRealize Automation アプライアンスの構成

vRealize Automation アプライアンスは、vRealize Automation サーバとユーザーの Web ポータルをホストする、部分的に構成された仮想マシンです。アプライアンスの Open Virtualization Format (OVF) テンプレートを vCenter Server または ESX/ESXi インベントリにダウンロードして展開します。

前提条件

- 未構成のアプライアンスを作成します。「[vRealize Automation アプライアンスの展開](#)」を参照してください。
- vRealize Automation アプライアンスの認証証明書を取得します。
ネットワークまたはロード バランサにこの証明書が必要な場合、その後の手順でロード バランサおよび追加のアプライアンスに証明書をコピーします。

手順

- 1 未構成の vRealize Automation アプライアンス管理インターフェイスに root としてログインします。
`https://<vrealize-automation-appliance-FQDN>:5480`
証明書の警告を無視して続行します。
- 2 インストール ウィザードが表示された場合はキャンセルし、ウィザードではなく管理インターフェイスに進むことができるようにします。

3 [管理] - [時刻設定] の順に選択し、時刻同期ソースを設定します。

| オプション | 説明 |
|---------|--|
| ホストの時刻 | vRealize Automation アプライアンスの ESXi ホストに同期します。 |
| タイム サーバ | 単一の外部 Network Time Protocol (NTP) サーバに同期します。NTP サーバの FQDN または IP アドレスを入力します。 |

すべての vRealize Automation アプライアンスおよび IaaS Windows サーバを同一の時刻ソースに同期させる必要があります。vRealize Automation 展開内で時刻ソースを混在させないでください。

4 [vRA 設定] - [ホストの設定] の順に選択します。

| オプション | アクション |
|--------------|--|
| [自動的に解決] | [自動的に解決] を選択し、vRealize Automation アプライアンスの現在のホストの名前を指定します。 |
| [ホストをアップデート] | 新しいホストの場合、[ホストをアップデート] を選択します。[ホスト名] テキストボックスに vRealize Automation アプライアンスの完全修飾ドメイン名である <vra-hostname.domain.name> を入力します。 ロード バランサを使用する分散デプロイの場合、[ホストをアップデート] を選択します。[ホスト名] テキストボックスにロード バランサ サーバの完全修飾ドメイン名である <vra-loadbalancename.domain.name> を入力します。 |

注: [ホストをアップデート] を使用してホスト名を設定するときは常に、この手順で後述する SSO 設定を構成します。

5 [証明書のアクション] メニューから証明書タイプを選択します。

分散環境などにおいて PEM でエンコードされた証明書を使用している場合は、[インポート] を選択します。

インポートする証明書は、信頼されており、SAN (Subject Alternative Name) 証明書を使用することによって vRealize Automation アプライアンスおよび任意のロード バランサのすべてのインスタンスに適用可能である必要があります。

認証局に送信可能な新しい証明書の CSR 要求を生成するには、[署名リクエストを生成] を選択します。CSR により、認証局 (CA) が正しい値で証明書を作成し、これをインポートすることが可能になります。

注: 証明書チェーンを使用する場合は、次の順序で証明書を指定します。

- a 中間 CA 証明書によって署名されたクライアント/サーバ証明書
- b 1 つ以上の中間証明書
- c ルート CA 証明書

| オプション | アクション |
|------------|--|
| 既存を保持 | 現在の SSL 設定のままにします。このオプションを選択して変更をキャンセルします。 |
| 証明書の生成 | <ul style="list-style-type: none"> a [共通名] テキスト ボックスに表示される値は、ページ上部に表示されるホスト名です。vRealize Automation アプライアンスの追加インスタンスが利用可能な場合は、証明書の SAN 属性にそれらの FQDN が含まれます。 b 会社名などの組織名を [組織] テキスト ボックスに入力します。 c 部署名や場所などの組織単位を [組織単位] テキスト ボックスに入力します。 d JP などの 2 文字の ISO 3166 国コードを [国] テキスト ボックスに入力します。 |
| 署名リクエストを生成 | <ul style="list-style-type: none"> a [署名リクエストを生成] を選択します。 b [組織]、[組織単位]、[国コード]、[共通名] の各テキスト ボックスの入力内容を確認します。これらは既存の証明書から入力されています。必要に応じて編集できます。 c [CSR を生成] をクリックして証明書署名リクエストを生成してから、[生成された CSR をここにダウンロード] リンクをクリックします。ダイアログ ボックスが開くので、認証局に送信するために CSR を保存する場所を指定します。 d 完成した証明書を受け取ったら、[インポート] をクリックし、指示のとおり操作して証明書を vRealize Automation にインポートします。 |
| インポート | <ul style="list-style-type: none"> a ヘッドおよびフッタを含む証明書値を BEGIN PRIVATE KEY から END PRIVATE KEY にコピーし、それらを [RSA プライベートキー] テキスト ボックスに貼り付けます。 b ヘッドおよびフッタを含む証明書値を BEGIN CERTIFICATE から END CERTIFICATE にコピーし、それらを [証明書チェーン] テキスト ボックスに貼り付けます。複数の証明書値の場合は、各証明書に BEGIN CERTIFICATE ヘッドと END CERTIFICATE フッタを含めます。 <p>注: チェーン証明書の場合は、追加の属性が使用可能になることがあります。</p> <ul style="list-style-type: none"> c (オプション) 証明書でパス フレーズを使用して証明書キーを暗号化する場合、そのパス フレーズをコピーし、[パスフレーズ] テキスト ボックスに貼り付けます。 |

6 [設定の保存] をクリックして、ホスト情報と SSL 構成を保存します。

7 ネットワークまたはロード バランサで証明書を必要とする場合は、インポートした証明書または新しく作成した証明書を仮想アプライアンスのロード バランサにコピーします。

証明書をエクスポートするために、root による SSH アクセスの有効化が必要な場合があります。

- a まだログインしていない場合は、vRealize Automation アプライアンスの管理コンソールに root ユーザーとしてログインします。
- b [管理者] タブをクリックします。
- c [管理者] サブメニューをクリックします。

- d [SSH サービス有効] チェック ボックスを選択します。

終了時に SSH を無効にするには、このチェック ボックスを選択解除します。

- e [管理者の SSH ログイン] チェック ボックスを選択します。

終了時に SSH を無効にするには、このチェック ボックスを選択解除します。

- f [設定の保存] をクリックします。

8 SSO 設定を構成します。

9 [サービス] をクリックします。

ライセンスをインストールする、またはコンソールにログインするためには、すべてのサービスが実行されている必要があります。これらは、通常、約 10 分で起動します。

注: アプライアンスにログインし、`tail -f /var/log/vcac/catalina.out` を実行してサービスの開始を監視することもできます。

10 ライセンス情報を入力してください。

- a [vRA 設定 > ライセンス] の順にクリックします。

- b [ライセンス] をクリックします。

- c インストール ファイルをダウンロードしたときにダウンロードした有効な vRealize Automation ライセンスキーを入力し、[送信キー] をクリックします。

注: 接続エラーが発生した場合、ロード バランサに問題がある可能性があります。ロード バランサへのネットワーク接続を確認してください。

11 vRealize Code Stream を有効にするかどうかを選択し、vRealize Code Stream ライセンスを入力します。

高可用性または本番の vRealize Automation 環境では、vRealize Code Stream はサポートされていません。

12 [メッセージング] をクリックします。アプライアンスのメッセージングの構成設定と状態が表示されます。これらの設定は変更しないでください。

13 [テレメトリ] タブをクリックして、VMware カスタマ エクスペリエンス改善プログラム (CEIP) に参加するかどうかを選択します。

CEIP によって収集されるデータの詳細と、VMware がそのデータを使用する目的については、Trust & Assurance Center (<http://www.vmware.com/trustvmware/ceip.html>) を参照してください。

- このプログラムに参加するには、[VMware カスタマ エクスペリエンス改善プログラムに参加] を選択します。
- このプログラムに参加しない場合は、[VMware カスタマ エクスペリエンス改善プログラムに参加] を選択解除します。

14 [設定の保存] をクリックします。

15 vRealize Automation にログインできることを確認します。

- a Web ブラウザを開き、vRealize Automation 製品のインターフェイス URL にアクセスします。
https://<vrealize-automation-appliance-FQDN>/vcac
- b プロンプトが表示されたら、証明書の警告を無視して続行します。
- c administrator@vsphere.local と、SSO の構成時に指定したパスワードを使用してログインします。
インターフェイスで、[テナント] ページの [管理] タブが開きます。リストに vsphere.local というテナントが 1 つだけ表示されます。

vRealize Automation アプライアンスの追加インスタンスの設定

システム管理者は vRealize Automation アプライアンスの複数のインスタンスを展開して、高可用性環境での冗長性を確保します。

各 vRealize Automation アプライアンスに対し、時刻同期を有効にして、アプライアンスをクラスタに追加する必要があります。アプライアンスをクラスタに追加する場合、初期（プライマリ）vRealize Automation アプライアンスの設定に基づく構成情報が自動的に追加されます。

高可用性やフェイルオーバー用のロード バランサを含む分散インストールを実行する場合は、vRealize Automation 環境の構成を担当するチームにご相談ください。テナント管理者は、Active Directory へのリンクを設定するとき、ディレクトリ管理を高可用性向けに構成する必要があります。

クラスタへの別の vRealize Automation アプライアンスの追加

高可用性のために、分散型環境では vRealize Automation アプライアンス ノードの手前でロード バランサを使用できます。

新しい vRealize Automation アプライアンス上の管理インターフェイスを使用して、このノードを 1 台以上のアプライアンスによる既存のクラスタに参加させます。この操作により、追加する新しいアプライアンスに、証明書、SSO、ライセンス、データベース、メッセージの情報など、構成情報がコピーされます。

クラスタへのアプライアンスの追加は一度に 1 つずつとし、並行して追加しないようにする必要があります。

前提条件

- クラスタでは、1 台以上の vRealize Automation アプライアンスがすでに存在し、1 台のノードがプライマリノードになっている必要があります。[「クラスタ内の最初の vRealize Automation アプライアンスの構成」](#)を参照してください。
プライマリ ノードになる新しいアプライアンスは、クラスタへの参加後にのみ設定できます。
- 新しいアプライアンス ノードを作成します。[「vRealize Automation アプライアンスの展開」](#)を参照してください。
- ロード バランサが新しいアプライアンスと一緒に使用されるように構成されていることを確認します。
- トラフィックがロード バランサを通過し、既存のすべてのノードとこれから追加する新しいノードに到達できることを確認します。
- 現在のノードですべての vRealize Automation のサービスが開始されていることを確認します。

手順

- 1 新しい vRealize Automation アプライアンス管理インターフェイスに root としてログインします。
https://<vrealize-automation-appliance-FQDN>:5480
証明書の警告を無視して続行します。
- 2 インストール ウィザードが表示された場合はキャンセルし、ウィザードではなく管理インターフェイスに進むことができるようにします。
- 3 [管理] - [時刻設定] の順に選択し、残りのクラスタ アプライアンスが使用しているのと同じ時刻ソースを設定します。
- 4 [vRA 設定] - [クラスタ] の順に選択します。
- 5 以前に構成した vRealize Automation アプライアンスの FQDN を [先頭のクラスタ ノード] テキスト ボックスに入力します。
プライマリ vRealize Automation アプライアンスまたはすでにクラスタに参加している vRealize Automation アプライアンスの FQDN を使用できます。
- 6 [パスワード] テキスト ボックスに root のパスワードを入力します。
- 7 [クラスタに参加] をクリックします。
- 8 証明書の警告を無視して続行します。
クラスタ用のサービスが再起動します。
- 9 サービスが実行していることを確認します。
 - a [サービス] タブをクリックします。
 - b [更新] タブをクリックして、サービス起動の進行状況を監視します。

未使用のサービスの無効化

内部リソースを節約するため、vRealize Orchestrator の外部インスタンスを使用する場合は組み込みの vRealize Orchestrator サービスを無効にすることができます。

前提条件

[「クラスタへの別の vRealize Automation アプライアンスの追加」](#)

手順

- 1 vRealize Automation アプライアンス コンソールにログインします。
- 2 vRealize Orchestrator サービスを停止します。

```
service vco-server stop
chkconfig vco-server off
```

分散インストールの検証

vRealize Automation アプライアンスの追加インスタンスの展開後、クラスタ化されたアプライアンスへアクセス可能であることを検証します。

手順

- 1 ロード バランサ管理インターフェイスまたは構成ファイルで、テスト対象のノード以外のすべてのノードを一時的に無効化します。
- 2 次のロード バランサ アドレスによって vRealize Automation にログインできることを確認します。
`https://<vrealize-automation-appliance-load-balancer-FQDN>/vcac`
- 3 ロード バランサを介して新しい vRealize Automation アプライアンスにアクセスできることを確認した後、他のノードを再度有効にします。

分散構成への IaaS コンポーネントのインストール

システム管理者はアプライアンスが展開され、完全に構成された後に IaaS コンポーネントをインストールします。IaaS コンポーネントは vRealize Automation インフラストラクチャ機能へのアクセスを提供します。

すべてのコンポーネントは、同じサービス アカウント ユーザーで実行する必要があります。このサービス アカウントは、それぞれの分散型 IaaS サーバに対する特権を持つドメイン アカウントである必要があります。ローカル システム アカウントは使用しないでください。

前提条件

- 「[クラスタ内の最初の vRealize Automation アプライアンスの構成](#)」。
- サイトに複数の vRealize Automation アプライアンスが含まれている場合は、「[クラスタへの別の vRealize Automation アプライアンスの追加](#)」を参照してください。
- サーバが「[IaaS Windows サーバ](#)」に示されている要件を満たしていることを確認します。
- コンポーネント Web サイトおよび Model Manager のデータをインストールするマシンの信頼されたルート証明書ストアへインポートするために、信頼された認証局から証明書を取得します。
- 環境内でロード バランサを使用している場合は、それらが構成要件を満たしていることを検証してください。

手順

1 IaaS 証明書のインストール

本番環境の場合は、信頼できる認証局からドメイン証明書を取得します。IaaS のインストール時に Web サイト コンポーネントと Manager Service をインストールするすべてのマシン (IIS マシン) の信頼できるルート証明書ストアに証明書をインポートします。

2 vRealize Automation IaaS インストーラのダウンロード

分散した仮想または物理 Windows サーバ上に IaaS をインストールするには、IaaS インストーラのコピーを vRealize Automation アプライアンスからダウンロードします。

3 IaaS データベース シナリオの選択

vRealize Automation IaaS は、Microsoft SQL Server データベースを使用して、管理対象マシンの情報と固有の要素およびポリシーに関する情報を保守します。

4 IaaS Web サイト コンポーネントと Model Manager Data のインストール

システム管理者は Web サイト コンポーネントをインストールして、vRealize Automation Web コンソールでのインフラストラクチャ機能へのアクセスを提供します。1 つまたは複数の Web サイト コンポーネントのインスタンスをインストールできますが、1 つ目の Web サイト コンポーネントをホストするマシンで Model Manager Data を構成する必要があります。Model Manager Data は一度のみインストールします。

5 IaaS Web サーバ コンポーネントの追加インストール

Web サーバから vRealize Automation のインフラストラクチャ機能にアクセスできます。最初の Web サーバをインストール後、IaaS Web サーバを追加インストールしてパフォーマンスを向上できます。

6 アクティブな Manager Service のインストール

アクティブな Manager Service は IaaS Distributed Execution Manager、データベース、エージェント、プロキシ エージェント、SMTP 間の通信を調整する Windows サービスです。

7 Backup Manager Service コンポーネントのインストール

バックアップの Manager Service は冗長性と高可用性を提供し、アクティブなサービスが停止した場合に手動で起動できます。

8 Distributed Execution Manager のインストール

Distributed Execution Manager は、2 つのロール DEM Orchestrator または DEM ワーカーのいずれかとしてインストールします。各ロールに対して少なくとも 1 つの DEM インスタンスをインストールする必要があり、フェイルオーバーおよび高可用性をサポートするために追加の DEM インスタンスをインストールできます。

9 IaaS データベースにアクセスするための Windows サービスの構成

システム管理者は、実行時（インストールの完了後）に SQL データベースへのアクセスに使用する認証方法を変更できます。デフォルトの場合、インストール後は、現在のログオン アカウントの Windows ID を使用してデータベースに接続します。

10 IaaS サービスの確認

インストール後、システム管理者は IaaS サービスが実行していることを確認します。サービスが実行中の場合、インストールは成功しています。

次のステップ

DEM Orchestrator および少なくとも 1 つの DEM ワーカー インスタンスをインストールします。[「Distributed Execution Manager のインストール」](#) を参照してください。

IaaS 証明書のインストール

本番環境の場合は、信頼できる認証局からドメイン証明書を取得します。IaaS のインストール時に Web サイト コンポーネントと Manager Service をインストールするすべてのマシン（IIS マシン）の信頼できるルート証明書ストアに証明書をインポートします。

前提条件

Windows 2012 マシンでは、SHA512 を使用している証明書で TLS1.2 を無効にする必要があります。TLS1.2 の無効化の詳細については、[Microsoft ナレッジベースの記事 245030](#) を参照してください。

手順

- 1 信頼できる認証局から証明書を取得します。
- 2 インターネット インフォメーション サービス (IIS) マネージャを開きます。
- 3 [機能] ビューで [サーバの証明書] をダブルクリックします。
- 4 [アクション] ペインの [インポート] をクリックします。
 - a [証明書ファイル] テキスト ボックスにファイル名を入力するか、または参照ボタン [...] をクリックして、エクスポートした証明書が格納されているファイルの名前に移動します。
 - b パスワードを指定して証明書をエクスポートした場合は、[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。
 - c [このキーをエクスポート可能にする] を選択します。
- 5 [OK] をクリックします。
- 6 インポートした証明書をクリックし、[表示] を選択します。
- 7 証明書およびそのチェーンが信頼されていることを確認します。
証明書が信頼されていない場合、「この CA ルート証明書は信頼されていません」というメッセージが表示されます。

注: インストール作業を続行するには、信頼問題を解決する必要があります。そのまま続けると導入に失敗します。

- 8 IIS を再起動するか、または管理者権限のコマンド プロンプト ウィンドウを開いて **iisreset** と入力します。

次のステップ

[\[vRealize Automation IaaS インストーラのダウンロード\]](#)。

vRealize Automation IaaS インストーラのダウンロード

分散した仮想または物理 Windows サーバ上に IaaS をインストールするには、IaaS インストーラのコピーを vRealize Automation アプライアンスからダウンロードします。

この処理中に証明書の警告が表示された場合、それらを見捨てて続行しインストールを完了させます。

前提条件

- [「クラスタ内の最初の vRealize Automation アプライアンスの構成」](#) および必要に応じて [「クラスタへの別の vRealize Automation アプライアンスの追加」](#)。
- サーバが [「IaaS Windows サーバ」](#) に示されている要件を満たしていることを確認します。
- IIS に証明書をインポートしており、証明書のルートまたは認証局がインストール マシンの信頼されたルートにあることを確認します。
- 環境内でロード バランサを使用している場合は、それらが構成要件を満たしていることを検証してください。

手順

- 1 (オプション) Windows 2012 マシンにインストールする場合は、HTTP をアクティブにします。
 - a Server Manager で [機能 > 機能の追加] を選択します。
 - b .NET Framework の [機能] で [WCF サービス] を展開します。
 - c [HTTP アクティブ化] を選択します。
- 2 管理者権限を備えたアカウントを使用して IaaS Windows サーバにログインします。
- 3 Web ブラウザを開いて vRealize Automation アプライアンス インストーラ URL にアクセスします。ロードバランサのアドレスは使用しないでください。
`https://<vrealize-automation-appliance-FQDN>:5480/installer`
- 4 [IaaS インストーラ] をクリックします。
- 5 **setup__<vrealize-automation-appliance-FQDN>@5480** を Windows サーバに保存します。
 インストーラ ファイル名は変更しないでください。インストールの vRealize Automation アプライアンスへの接続に使用されます。
- 6 このインストーラ ファイルをコンポーネントのインストール先の各 IaaS Windows サーバにダウンロードします。

次のステップ

IaaS データベースをインストールします。[「IaaS データベース シナリオの選択」](#) を参照してください。

IaaS データベース シナリオの選択

vRealize Automation IaaS は、Microsoft SQL Server データベースを使用して、管理対象マシンの情報と固有の要素およびポリシーに関する情報を保守します。

環境設定および権限に応じて、IaaS データベースを作成するために選択できる複数の手順があります。

注: SQL データベースの作成またはアップグレード時に、セキュア SSL を有効にすることができます。たとえば、SQL データベースを作成またはアップグレードするときには、セキュア SSL のオプションを使用して、SQL Server ですでに指定されている SSL 構成が SQL データベースへの接続時に実行されるように指定することができます。SSL を使用すると、IaaS サーバと SQL データベースの間の接続の安全性が強化されます。カスタム インストール ウィザードで指定できるこのオプションは、SQL Server で SSL がすでに構成されていることが前提となります。SQL Server での SSL の構成に関する関連情報については、[Microsoft Technet の記事 189067](#) を参照してください。

表 1-34. IaaS データベース シナリオの選択

| シナリオ | 手順 |
|---|--|
| 提供されているデータベース スクリプトを使用して、手動で IaaS データベースを作成します。このオプションを使用すると、データベース管理者はデータベースの作成前に変更点を十分に確認することができます。 | 「手動による IaaS データベースの作成」 。 |
| 空のデータベースを準備し、インストーラを使用してデータベース スキーマを取り込みます。このオプションを指定すると、インストーラは dbo 権限を持つデータベース ユーザーを使用してデータベースをポビュレートできます。 | 「空のデータベースの準備」 。 |
| インストーラを使用してデータベースを作成します。これは最も簡単なオプションですが、インストーラで sysadmin 権限を使用する必要があります。 | 「インストール ウィザードを使用した IaaS データベースの作成」 。 |

手動による IaaS データベースの作成

vRealize Automation システム管理者は VMware で提供されるスクリプトを使用して手動でデータベースを作成できます。

前提条件

- Microsoft .NET Framework 4.5.2 以降を SQL Server ホストにインストールします。
- データベースに接続するには、SQL 認証ではなく、Windows 認証を使用します。
- データベースのインストール要件を確認します。[「IaaS SQL サーバ ホスト」](#) を参照してください。
- Web ブラウザを開いて vRealize Automation アプライアンス インストーラ URL にアクセスし IaaS データベース インストール スクリプトをダウンロードします。

<https://<vrealize-automation-appliance-FQDN>:5480/installer>

手順

- 1 インストール zip アーカイブを抽出したディレクトリの **Database** サブディレクトリに移動します。
- 2 **DBInstall.zip** アーカイブをローカル ディレクトリに抽出します。
- 3 SQL Server インスタンスでデータベースを作成およびドロップするために十分な権限 **sysadmin** で Windows データベース ホストにログインします。
- 4 必要に応じてデータベース展開スクリプトを確認します。特に、**CreateDatabase.sql** の **DBSettings** セクションの設定を確認し、必要ならば編集します。

スクリプト内の設定は推奨設定です。**ALLOW_SNAPSHOT_ISOLATION ON** および **READ_COMMITTED_SNAPSHOT ON** のみが必須です。

5 表で説明されている引数を指定して次のコマンドを実行します。

```
BuildDB.bat /p:DBServer=<db_server>;
DBName=<db_name>;DBDir=<db_dir>;
LogDir=[<log_dir>];ServiceUser=<service_user>;
ReportLogin=<web_user>;
VersionString=<version_string>
```

表 1-35. データベース値

| 変数 | 値 |
|------------------|---|
| <db_server> | dbhostname[,port number]\SQL instance の形式で SQL Server インスタンスを指定します。デフォルト以外のポートを使用している場合に限り、ポート番号を指定します。Microsoft SQL のデフォルトポート番号は 1433 です。<db_server> のデフォルト値は localhost です。 |
| <db_name> | データベースの名前です。デフォルト値は vra です。データベース名は、128 文字未満の ASCII 文字で作成する必要があります。 |
| <db_dir> | 最後のスラッシュを除く、データベースのデータ ディレクトリへのパス。 |
| <log_dir> | 最後のスラッシュを除く、データベースのログ ディレクトリへのパス。 |
| <service_user> | Manager Service を実行するユーザー名です。 |
| <Web_user> | Web サービスを実行するユーザー名です。 |
| <version_string> | vRealize Automation のバージョンです。vRealize Automation アプライアンスにログインして [更新] タブをクリックすると表示されます。たとえば、vRealize Automation 6.1 のバージョン文字列は 6.1.0.1200 です。 |

データベースが作成されます。

次のステップ

[「分散構成への IaaS コンポーネントのインストール」](#)。

空のデータベースの準備

vRealize Automation のシステム管理者は、IaaS スキーマを空のデータベースにインストールできます。このインストール方法では、データベースのセキュリティに対して最大限の制御が可能です。

前提条件

- データベースのインストール要件を確認します。[「IaaS SQL サーバ ホスト」](#) を参照してください。
- Web ブラウザを開いて vRealize Automation アプライアンス インストーラ URL にアクセスし IaaS データベース インストール スクリプトをダウンロードします。

<https://<vrealize-automation-appliance-FQDN>:5480/installer>

手順

- 1 インストール zip アーカイブを抽出したディレクトリ内にある **Database** ディレクトリに移動します。

- 2 **DBInstall.zip** アーカイブをローカル ディレクトリに抽出します。
- 3 SQL Server インスタンス内の **sysadmin** 権限で Windows データベース ホストにログインします。
- 4 次のファイルを編集して、表内の変数のすべてのインスタンスを、使用環境に対する正しい値に置き換えます。

```
CreateDatabase.sql
SetDatabaseSettings.sql
```

表 1-36. データベース値

| 変数 | 値 |
|---------------------------------|---|
| <code>\$(<DBName>)</code> | vra などのデータベースの名前。データベース名は、128 文字未満の ASCII 文字で作成する必要があります。 |
| <code>\$(<DBDir>)</code> | 最後のスラッシュを除く、データベースのデータ ディレクトリへのパス。 |
| <code>\$(<LogDir>)</code> | 最後のスラッシュを除く、データベースのログ ディレクトリへのパス。 |

- 5 **SetDatabaseSettings.sql** の **DB Settings** セクションの設定を確認し、必要に応じて編集します。
IaaS データベースの設定には、スクリプト内の設定が推奨されます。**ALLOW_SNAPSHOT_ISOLATION ON** および **READ_COMMITTED_SNAPSHOT ON** のみが必要です。
- 6 SQL Server Management Studio を開きます。
- 7 [新規クエリ] をクリックします。
SQL クエリ ウィンドウが開きます。
- 8 [クエリ] メニューで、[SQLCMD モード] が選択されていることを確認します。
- 9 **CreateDatabase.sql** の変更されたコンテンツ全体をクエリ ペインに貼り付けます。
- 10 **CreateDatabase.sql** のコンテンツの下に、**SetDatabaseSettings.sql** の変更されたコンテンツ全体を貼り付けます。
- 11 [実行] をクリックします。
スクリプトが実行し、データベースを作成します。

次のステップ

[「分散構成への IaaS コンポーネントのインストール」](#)。

インストール ウィザードを使用した IaaS データベースの作成

vRealize Automation では、Microsoft SQL Server データベースを使用して管理するマシンおよび固有の要素とポリシーに関する情報を維持します。

次の手順で、インストーラを使用して IaaS データベースを作成する方法または既存の空のデータベースを取り込む方法について説明します。データベースを手動で作成することもできます。[「手動による IaaS データベースの作成」](#)を参照してください。

前提条件

- SQL 認証の代わりに、Windows 認証を使用してデータベースを作成している場合、インストーラを実行するユーザーに SQL サーバでの **sysadmin** 権限があることを確認します。
- [\[vRealize Automation IaaS インストーラのダウンロード\]](#)。

手順

- 1 セットアップ ファイル **setup__<vrealize-automation-appliance-FQDN>@5480.exe** を右クリックして、[管理者として実行] を選択します。
- 2 [次へ] をクリックします。
- 3 使用許諾契約に同意し、[次へ] をクリックします。
- 4 ログイン ページで vRealize Automation アプライアンスの管理者認証情報を入力し、SSL 証明書を確認します。
 - a ユーザー名 (**root**) とパスワードを入力します。
 入力するパスワードは、vRealize Automation アプライアンスを展開したときに指定したパスワードです。
 - b [証明書の受け入れ] を選択します。
 - c [証明書の表示] をクリックします。
 証明書のサムプリントを、vRealize Automation アプライアンスに設定されているサムプリントと比較します。管理コンソールにポート 5480 でアクセスしている場合は、クライアント ブラウザで vRealize Automation アプライアンス証明書を表示できます。
- 5 [次へ] をクリックします。
- 6 [インストール タイプ] ページで [カスタム インストール] を選択します。
- 7 [インストール タイプ] ページの [コンポーネントの選択] で [IaaS サーバ] を選択します。
- 8 ルートのインストール場所を受け入れるか、[変更] をクリックしてインストール パスを選択します。
 分散型展開の場合でも、同じ Windows サーバに複数の IaaS コンポーネントをインストールする場合があります。
 複数の IaaS コンポーネントをインストールする場合は、常に同じパスにインストールしてください。
- 9 [次へ] をクリックします。
- 10 [IaaS サーバのカスタム インストール] ページで、[データベース] を選択します。
- 11 [データベース インスタンス] テキスト ボックスで、データベース インスタンスを指定するか、[スキャン] をクリックしてインスタンスのリストから選択します。デフォルト以外のポートにデータベース インスタンスが存在する場合は、<dbhost,SQL_port_number\SQLinstance> 形式を使用して、インスタンスの仕様にポート番号を含めます。Microsoft SQL のデフォルト ポート番号は 1443 です。
- 12 (オプション) [データベース接続に SSL を使用] チェックボックスを選択します。
 デフォルトでは、このチェックボックスは有効になっています。SSL を使用すると、IaaS サーバと SQL データベースの間の接続の安全性が強化されます。ただし、このオプションをサポートするには、SQL Server に SSL を構成する必要があります。SQL Server での SSL 構成の詳細については、[Microsoft Technet の記事 189067](#) を参照してください。

13 [データベース名] パネルから、データベースのインストール タイプを選択します。

- 既存のデータベースにスキーマを作成するには、[既存の空のデータベースの使用] を選択します。
- 新しいデータベース名を入力するか、デフォルトの名前 **vra** を使用して、新しいデータベースを作成します。
データベース名は、128 文字未満の ASCII 文字で作成する必要があります。

14 他の場所を指定するには [デフォルト データおよびログ ディレクトリの使用] の選択を解除しますが、デフォルトのディレクトリを使用するには選択したままにします (推奨)。

15 [認証] リストからデータベースのインストール用の認証方法を選択します。

- インストーラを実行してデータベースを作成する際の認証情報を使用するには、[Windows ID を使用...] を選択します。
- SQL 認証を使用するには、[Windows ID を使用...] の選択を解除します。ユーザーおよびパスワードのテキスト ボックスに SQL 認証情報を入力します。

デフォルトの場合、Windows サービス ユーザー アカウントがデータベースへの実行時アクセス中に使用され、SQL Server インスタンスへの sysadmin 権限が必要です。 実行時にデータベースへのアクセスに使用される認証情報は、SQL 認証情報を使用するように構成できます。

Windows 認証が推奨されています。SQL 認証を選択すると、特定の構成ファイルで暗号化されていないデータベース パスワードが表示されます。

16 [次へ] をクリックします。

17 前提条件チェックを完了します。

| オプション | 説明 |
|-----------|---|
| エラーなし | [次へ] をクリックします。 |
| 重要性が低いエラー | [バイパス] をクリックします。 |
| 重大なエラー | 重大なエラーを無視するとインストールの失敗の原因となります。警告が表示された場合は、左側のペインの警告を選択し、右側の指示に従います。すべての重大なエラーに対処し、[再チェック] をクリックして検証します。 |

18 [インストール] をクリックします。

19 成功のメッセージが表示されたら、[初期構成をガイド] の選択を解除し、[次へ] をクリックします。

20 [完了] をクリックします。

データベースの使用準備ができました。

laaS Web サイト コンポーネントと Model Manager Data のインストール

システム管理者は Web サイト コンポーネントをインストールして、vRealize Automation Web コンソールでのインフラストラクチャ機能へのアクセスを提供します。1 つまたは複数の Web サイト コンポーネントのインスタンスをインストールできますが、1 つ目の Web サイト コンポーネントをホストするマシンで Model Manager Data を構成する必要があります。Model Manager Data は一度のみインストールします。

前提条件

- laaS データベースをインストールします。[「laaS データベース シナリオの選択」](#) を参照してください。

- IaaS の他のコンポーネントがすでにインストールされている場合は、作成したデータベースのパスフレーズを確認します。
- 環境内でロード バランサを使用している場合は、それらが構成要件を満たしていることを検証してください。

手順

1 最初の IaaS Web サーバ コンポーネントのインストール

vRealize Automation のインフラストラクチャ機能にアクセスするための IaaS Web サーバ コンポーネントをインストールします。

2 Model Manager Data の設定

最初の Web サーバ コンポーネントをホストするマシンと同じマシンに、Model Manager コンポーネントをインストールします。Model Manager Data は 1 回のみインストールできます。

追加の Web サイト コンポーネントまたは Manager Service をインストールできます。[IaaS Web サーバ コンポーネントの追加インストール](#) または [アクティブな Manager Service のインストール](#) を参照してください。

最初の IaaS Web サーバ コンポーネントのインストール

vRealize Automation のインフラストラクチャ機能にアクセスするための IaaS Web サーバ コンポーネントをインストールします。

複数の IaaS Web サーバをインストールできますが、最初の Web サーバのみに Model Manager Data をインストールします。

前提条件

- [「インストール ウィザードを使用した IaaS データベースの作成」](#)。
- サーバが [IaaS Windows サーバ](#) に示されている要件を満たしていることを確認します。
- IaaS の他のコンポーネントがすでにインストールされている場合は、作成したデータベースのパスフレーズを確認します。
- 環境内でロード バランサを使用している場合は、それらが構成要件を満たしていることを検証してください。

手順

- 1 ロード バランサを使用している場合は、ロード バランサの下他のノードを無効にして、トラフィックが目的のノードに転送されることを確認します。

さらに、すべての vRealize Automation コンポーネントがインストールされて設定されるまで、ロード バランサの健全性チェックを無効にします。
- 2 セットアップ ファイル `setup__<vrealize-automation-appliance-FQDN>@5480.exe` を右クリックして、[管理者として実行] を選択します。
- 3 [次へ] をクリックします。
- 4 使用許諾契約に同意し、[次へ] をクリックします。

- 5 ログイン ページで vRealize Automation アプライアンスの管理者認証情報を入力し、SSL 証明書を確認します。
 - a ユーザー名 (**root**) とパスワードを入力します。
 入力するパスワードは、vRealize Automation アプライアンスを展開したときに指定したパスワードです。
 - b [証明書の受け入れ] を選択します。
 - c [証明書の表示] をクリックします。
 証明書のサムプリントを、vRealize Automation アプライアンスに設定されているサムプリントと比較します。管理コンソールにポート 5480 でアクセスしている場合は、クライアント ブラウザで vRealize Automation アプライアンス証明書を表示できます。
- 6 [次へ] をクリックします。
- 7 [インストール タイプ] ページで [カスタム インストール] を選択します。
- 8 [インストール タイプ] ページの [コンポーネントの選択] で [IaaS サーバ] を選択します。
- 9 ルートのインストール場所を受け入れるか、[変更] をクリックしてインストール パスを選択します。
 分散型展開の場合でも、同じ Windows サーバに複数の IaaS コンポーネントをインストールする場合があります。
 複数の IaaS コンポーネントをインストールする場合は、常に同じパスにインストールしてください。
- 10 [次へ] をクリックします。
- 11 [IaaS サーバのカスタム インストール] ページで [Web サイト] および [ModelManagerData] を選択します。
- 12 [管理と Model Manager Web サイト] タブで使用可能な Web サイトから Web サイトを選択するか、デフォルトの Web サイトを受け入れます。
- 13 [ポート番号] テキスト ボックスに使用可能なポート番号を入力するか、デフォルト ポート 443 を受け入れます。
- 14 [バインドのテスト] をクリックしてポート番号が使用できることを確認します。
- 15 このコンポーネント用の証明書を選択します。
 - a インストールを開始した後に証明書をインポートした場合、[更新] をクリックしてリストをアップデートします。
 - b [使用可能な証明書] から使用する証明書を選択します。
 - c フレンドリ名を持たない証明書をインポートし、それがリストに表示されない場合には、[フレンドリ名を使用して証明書を表示] を選択解除し、[更新] をクリックします。
 ロード バランサを使用しない環境にインストールする場合には、証明書を選択する代わりに[自己署名証明書の生成] を選択できます。ロード バランサ配下に追加 Web サイト コンポーネントをインストールする場合、自己署名証明書は生成しないでください。ロード バランサ配下のすべてのサーバ上で同じ証明書を使用するには、メインの IaaS Web サーバから証明書をインポートします。
- 16 (オプション) [証明書の表示] をクリックし、証明書を表示し、[OK] をクリックして情報ウィンドウを閉じます。
- 17 (オプション) [証明書の不一致の抑止] を選択して証明書エラーを抑止します。インストールでは、証明書名不一致エラーおよびリモート証明書失効リストの一致エラーを無視します。
 これは安全性の低いオプションです。

Model Manager Data の設定

最初の Web サーバ コンポーネントをホストするマシンと同じマシンに、Model Manager コンポーネントをインストールします。Model Manager Data は 1 回のみインストールできます。

前提条件

「[最初の IaaS Web サーバ コンポーネントのインストール](#)」。

手順

- 1 [Model Manager Data] タブをクリックします。
- 2 [サーバ] テキスト ボックスに vRealize Automation アプライアンスの完全修飾ドメイン名を入力します。
<vrealize-automation-appliance.mycompany.com>
IP アドレスは入力しないでください。
- 3 [ロード] をクリックして [SSO のデフォルト テナント] を表示します。
シングル サインオンを設定すると、**vsphere.local** デフォルト テナントが自動的に作成されます。これは変更できません。
- 4 [ダウンロード] をクリックして仮想アプライアンスから証明書をインポートします。
証明書のダウンロードには数分かかる場合があります。
- 5 (オプション) [証明書の表示] をクリックし、証明書を表示し、[OK] をクリックして情報ウィンドウを閉じます。
- 6 [証明書の受け入れ] をクリックします。
- 7 [ユーザー名] テキスト ボックスに **administrator@vsphere.local** と入力し、SSO の設定時に作成したパスワードを [パスワード] および [確認] テキスト ボックスに入力します。
- 8 (オプション) [テスト] をクリックして認証情報を確認します。
- 9 [IaaS サーバ] テキスト ボックスで IaaS Web サーバ コンポーネントを見つけます。

| オプション | 説明 |
|---------------|--|
| ロード バランサがある場合 | IaaS Web サーバ コンポーネントのロード バランサの完全修飾ドメイン名とポート番号 (<web-load-balancer.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |
| ロード バランサがない場合 | IaaS Web サーバ コンポーネントをインストールしたマシンの完全修飾ドメイン名とポート番号 (<web.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |

デフォルト ポートは 443 です。

- 10 [テスト] をクリックしてサーバ接続を確認します。
- 11 [次へ] をクリックします。

12 前提条件チェックを完了します。

| オプション | 説明 |
|-----------|---|
| エラーなし | [次へ] をクリックします。 |
| 重要性が低いエラー | [バイパス] をクリックします。 |
| 重大なエラー | 重大なエラーを無視するとインストールの失敗の原因となります。警告が表示された場合は、左側のペインの警告を選択し、右側の指示に従います。すべての重大なエラーに対処し、[再チェック] をクリックして検証します。 |

13 [サーバとアカウントの設定] ページの [サーバー インストール情報] テキスト ボックスに、現在のインストールサーバに対する管理者権限を持ったサービス アカウント ユーザーのユーザー名とパスワードを入力します。

サービス アカウント ユーザーは、分散された各 IaaS サーバに対する権限を持った単一のドメイン アカウントである必要があります。ローカル システムのアカウントは使用しないでください。

14 データベースを保護する暗号化キーの生成に使用したパスフレーズを指定します。

| オプション | 説明 |
|------------------------------|---|
| この環境にすでにコンポーネントをインストールしている場合 | [パスフレーズ] および [確認] テキスト ボックスに以前に作成したパスフレーズを入力します。 |
| 初めてのインストールの場合 | [パスフレーズ] および [確認] テキスト ボックスにパスフレーズを入力します。このパスフレーズは、新しいコンポーネントをインストールするたびに使用する必要があります。 |

今後の使用のために、このパスフレーズは安全な場所に保管してください。

15 [Microsoft SQL データベースのインストール情報] テキスト ボックスに IaaS データベース サーバ、データベース名、およびデータベース サーバの認証方法を指定します。

これは以前に作成した IaaS データベース サーバ、名前、および認証情報です。

16 [次へ] をクリックします。

17 [インストール] をクリックします。

18 インストールが完了したら、[初期構成へガイド] を選択解除し、[次へ] をクリックします。

次のステップ

追加の Web サーバ コンポーネントまたは Manager Service をインストールできます。[\[IaaS Web サーバ コンポーネントの追加インストール\]](#) または [\[アクティブな Manager Service のインストール\]](#) を参照してください。

IaaS Web サーバ コンポーネントの追加インストール

Web サーバから vRealize Automation のインフラストラクチャ機能にアクセスできます。最初の Web サーバをインストール後、IaaS Web サーバを追加インストールしてパフォーマンスを向上できます。

追加の Web サーバ コンポーネントには Model Manager Data をインストールしないでください。最初の Web サーバ コンポーネントのみで、Model Manager Data をホストします。

前提条件

- [\[IaaS Web サイト コンポーネントと Model Manager Data のインストール\]](#)。
- 新しいサーバが [\[IaaS Windows サーバ\]](#) に示されている要件を満たしていることを確認します。

- vRealize Automation アプライアンス管理インターフェイスを使用して、新しいノードの FQDN を含めるように証明書を置き換えます。vRealize Automation アプライアンスでの証明書の置き換えを参照してください。
- IaaS の他のコンポーネントがすでにインストールされている場合は、作成したデータベースのパスフレーズを確認します。
- 環境内でロード バランサを使用している場合は、それらが構成要件を満たしていることを検証してください。

手順

- 1 ロード バランサを使用している場合は、ロード バランサの下他のノードを無効にして、トラフィックが目的のノードに転送されることを確認します。

さらに、すべての vRealize Automation コンポーネントがインストールされて設定されるまで、ロード バランサの健全性チェックを無効にします。
- 2 セットアップ ファイル `setup__<vrealize-automation-appliance-FQDN>@5480.exe` を右クリックして、[管理者として実行] を選択します。
- 3 [次へ] をクリックします。
- 4 使用許諾契約に同意し、[次へ] をクリックします。
- 5 ログイン ページで vRealize Automation アプライアンスの管理者認証情報を入力し、SSL 証明書を確認します。
 - a ユーザー名 (**root**) とパスワードを入力します。

入力するパスワードは、vRealize Automation アプライアンスを展開したときに指定したパスワードです。
 - b [証明書の受け入れ] を選択します。
 - c [証明書の表示] をクリックします。

証明書のサムプリントを、vRealize Automation アプライアンスに設定されているサムプリントと比較します。管理コンソールにポート 5480 でアクセスしている場合は、クライアント ブラウザで vRealize Automation アプライアンス証明書を表示できます。
- 6 [次へ] をクリックします。
- 7 [インストール タイプ] ページで [カスタム インストール] を選択します。
- 8 [インストール タイプ] ページの [コンポーネントの選択] で [IaaS サーバ] を選択します。
- 9 ルートのインストール場所を受け入れるか、[変更] をクリックしてインストール パスを選択します。

分散型展開の場合でも、同じ Windows サーバに複数の IaaS コンポーネントをインストールする場合があります。複数の IaaS コンポーネントをインストールする場合は、常に同じパスにインストールしてください。
- 10 [次へ] をクリックします。
- 11 [IaaS サーバのカスタム インストール] ページで [Web サイト] を選択します。
- 12 [管理と Model Manager Web サイト] タブで使用可能な Web サイトから Web サイトを選択するか、デフォルトの Web サイトを受け入れます。
- 13 [ポート番号] テキスト ボックスに使用可能なポート番号を入力するか、デフォルト ポート 443 を受け入れます。

14 [バインドのテスト] をクリックしてポート番号が使用できることを確認します。

15 このコンポーネント用の証明書を選択します。

- a インストールを開始した後に証明書をインポートした場合、[更新] をクリックしてリストをアップデートします。
- b [使用可能な証明書] から使用する証明書を選択します。
- c フレンドリ名を持たない証明書をインポートし、それがリストに表示されない場合には、[フレンドリ名を使用して証明書を表示] を選択解除し、[更新] をクリックします。

ロード バランサを使用しない環境にインストールする場合には、証明書を選択する代わりに[自己署名証明書の生成] を選択できます。ロード バランサ配下に追加 Web サイト コンポーネントをインストールする場合、自己署名証明書は生成しないでください。ロード バランサ配下のすべてのサーバ上で同じ証明書を使用するには、メインの IaaS Web サーバから証明書をインポートします。

16 (オプション) [証明書の表示] をクリックし、証明書を表示し、[OK] をクリックして情報ウィンドウを閉じます。

17 (オプション) [証明書の不一致の抑止] を選択して証明書エラーを抑止します。インストールでは、証明書名不一致エラーおよびリモート証明書失効リストの一致エラーを無視します。

これは安全性の低いオプションです。

18 [IaaS サーバ] テキスト ボックスに最初の IaaS Web サーバ コンポーネントを指定します。

| オプション | 説明 |
|---------------|--|
| ロード バランサがある場合 | IaaS Web サーバ コンポーネントのロード バランサの完全修飾ドメイン名とポート番号 (<web-load-balancer.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |
| ロード バランサがない場合 | IaaS の最初の Web サーバ コンポーネントをインストールしたマシンの完全修飾ドメイン名とポート番号 (<web.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |

デフォルト ポートは 443 です。

19 [テスト] をクリックしてサーバ接続を確認します。

20 [次へ] をクリックします。

21 前提条件チェックを完了します。

| オプション | 説明 |
|-----------|---|
| エラーなし | [次へ] をクリックします。 |
| 重要性が低いエラー | [バイパス] をクリックします。 |
| 重大なエラー | 重大なエラーを無視するとインストールの失敗の原因となります。警告が表示された場合は、左側のペインの警告を選択し、右側の指示に従います。すべての重大なエラーに対処し、[再チェック] をクリックして検証します。 |

22 [サーバとアカウントの設定] ページの [サーバー インストール情報] テキスト ボックスに、現在のインストールサーバに対する管理者権限を持ったサービス アカウント ユーザーのユーザー名とパスワードを入力します。

サービス アカウント ユーザーは、分散された各 IaaS サーバに対する権限を持った単一のドメイン アカウントである必要があります。ローカル システム アカウントは使用しないでください。

23 データベースを保護する暗号化キーの生成に使用したパスフレーズを指定します。

| オプション | 説明 |
|------------------------------|---|
| この環境にすでにコンポーネントをインストールしている場合 | [パスフレーズ] および [確認] テキスト ボックスに以前に作成したパスフレーズを入力します。 |
| 初めてのインストールの場合 | [パスフレーズ] および [確認] テキスト ボックスにパスフレーズを入力します。このパスフレーズは、新しいコンポーネントをインストールするたびに使用する必要があります。 |

今後の使用のために、このパスフレーズは安全な場所に保管してください。

24 [Microsoft SQL データベースのインストール情報] テキスト ボックスに IaaS データベース サーバ、データベース名、およびデータベース サーバの認証方法を指定します。

これは以前に作成した IaaS データベース サーバ、名前、および認証情報です。

25 [次へ] をクリックします。

26 [インストール] をクリックします。

27 インストールが完了したら、[初期構成ヘガイド] を選択解除し、[次へ] をクリックします。

次のステップ

[「アクティブな Manager Service のインストール」](#)。

アクティブな Manager Service のインストール

アクティブな Manager Service は IaaS Distributed Execution Manager、データベース、エージェント、プロキシ エージェント、SMTP 間の通信を調整する Windows サービスです。

Manager Service の自動フェイルオーバーを有効にする場合を除き、IaaS の展開で Manager Service を同時に実行できる Windows マシンは 1 台だけです。バックアップのマシンは、サービスを停止し、手動で開始するように構成する必要があります。

[「Manager Service の自動フェイルオーバーについて」](#) を参照してください。

前提条件

- IaaS の他のコンポーネントがすでにインストールされている場合は、作成したデータベースのパスフレーズを確認します。
- (オプション) Manager Service をデフォルトとは異なる Web サイトにインストールする場合には、最初にインターネット インフォメーション サービスに Web サイトを作成します。
- 認証局の証明書が IIS にインポートされており、ルート証明書または認証局が信頼できることを確認します。ロード バランサのすべてのコンポーネントが同じ証明書を持っている必要があります。
- Web サイトのロード バランサが構成されており、そのロード バランサのタイムアウト値が最小値の 180 秒に設定されていることを確認します。
- [「IaaS Web サイト コンポーネントと Model Manager Data のインストール」](#)。

手順

- 1 ロード バランサを使用している場合は、ロード バランサの下の他のノードを無効にして、トラフィックが目的のノードに転送されることを確認します。

さらに、すべての vRealize Automation コンポーネントがインストールされて設定されるまで、ロード バランサの健全性チェックを無効にします。
- 2 セットアップ ファイル **setup__<vrealize-automation-appliance-FQDN>@5480.exe** を右クリックして、[管理者として実行] を選択します。
- 3 使用許諾契約に同意し、[次へ] をクリックします。
- 4 ログイン ページで vRealize Automation アプライアンスの管理者認証情報を入力し、SSL 証明書を確認します。
 - a ユーザー名 (**root**) とパスワードを入力します。

入力するパスワードは、vRealize Automation アプライアンスを展開したときに指定したパスワードです。
 - b [証明書の受け入れ] を選択します。
 - c [証明書の表示] をクリックします。

証明書のサムプリントを、vRealize Automation アプライアンスに設定されているサムプリントと比較します。管理コンソールにポート 5480 でアクセスしている場合は、クライアント ブラウザで vRealize Automation アプライアンス証明書を表示できます。
- 5 [次へ] をクリックします。
- 6 [インストール タイプ] ページで [カスタム インストール] を選択します。
- 7 [インストール タイプ] ページの [コンポーネントの選択] で [IaaS サーバ] を選択します。
- 8 ルートのインストール場所を受け入れるか、[変更] をクリックしてインストール パスを選択します。

分散型展開の場合でも、同じ Windows サーバに複数の IaaS コンポーネントをインストールする場合があります。複数の IaaS コンポーネントをインストールする場合は、常に同じパスにインストールしてください。
- 9 [次へ] をクリックします。
- 10 [IaaS サーバのカスタム インストール] ページで [Manager Service] を選択します。
- 11 [IaaS サーバ] テキスト ボックスで IaaS Web サーバ コンポーネントを見つけます。

| オプション | 説明 |
|---------------|--|
| ロード バランサがある場合 | IaaS Web サーバ コンポーネントのロード バランサの完全修飾ドメイン名とポート番号 (<web-load-balancer.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |
| ロード バランサがない場合 | IaaS Web サーバ コンポーネントをインストールしたマシンの完全修飾ドメイン名とポート番号 (<web.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |

デフォルト ポートは 443 です。

- 12 [起動タイプが自動に設定されているアクティブ ノード] を選択します。

- 13 [管理と Model Manager Web サイト] タブで使用可能な Web サイトから Web サイトを選択するか、デフォルトの Web サイトを受け入れます。
- 14 [ポート番号] テキスト ボックスに使用可能なポート番号を入力するか、デフォルト ポート 443 を受け入れます。
- 15 [バインドのテスト] をクリックしてポート番号が使用できることを確認します。
- 16 このコンポーネント用の証明書を選択します。
 - a インストールを開始した後に証明書をインポートした場合、[更新] をクリックしてリストをアップデートします。
 - b [使用可能な証明書] から使用する証明書を選択します。
 - c フレンドリ名を持たない証明書をインポートし、それがリストに表示されない場合には、[フレンドリ名を使用して証明書を表示] を選択解除し、[更新] をクリックします。

ロード バランサを使用しない環境にインストールする場合には、証明書を選択する代わりに[自己署名証明書の生成]を選択できます。ロード バランサ配下に追加 Web サイト コンポーネントをインストールする場合、自己署名証明書は生成しないでください。ロード バランサ配下のすべてのサーバ上で同じ証明書を使用するには、メインの IaaS Web サーバから証明書をインポートします。
- 17 (オプション) [証明書の表示] をクリックし、証明書を表示し、[OK] をクリックして情報ウィンドウを閉じます。
- 18 [次へ] をクリックします。
- 19 前提条件を確認し、[次へ] をクリックします。
- 20 [サーバとアカウントの設定] ページの [サーバー インストール情報] テキスト ボックスに、現在のインストールサーバに対する管理者権限を持ったサービス アカウント ユーザーのユーザー名とパスワードを入力します。

サービス アカウント ユーザーは、分散された各 IaaS サーバに対する権限を持った単一のドメイン アカウントである必要があります。ローカル システム アカウントは使用しないでください。
- 21 データベースを保護する暗号化キーの生成に使用したパスフレーズを指定します。

| オプション | 説明 |
|------------------------------|---|
| この環境にすでにコンポーネントをインストールしている場合 | [パスフレーズ] および [確認] テキスト ボックスに以前に作成したパスフレーズを入力します。 |
| 初めてのインストールの場合 | [パスフレーズ] および [確認] テキスト ボックスにパスフレーズを入力します。このパスフレーズは、新しいコンポーネントをインストールするたびに使用する必要があります。 |

今後の使用のために、このパスフレーズは安全な場所に保管してください。

- 22 [Microsoft SQL データベースのインストール情報] テキスト ボックスに IaaS データベース サーバ、データベース名、およびデータベース サーバの認証方法を指定します。

これは以前に作成した IaaS データベース サーバ、名前、および認証情報です。
- 23 [次へ] をクリックします。
- 24 [インストール] をクリックします。
- 25 インストールが完了したら、[初期構成へガイド] を選択解除し、[次へ] をクリックします。
- 26 [完了] をクリックします。

次のステップ

- インストールした Manager Service がアクティブなインスタンスとなるようにするには、vCloud Automation Center Service が実行中であることを確認して、「自動」起動タイプに設定します。
- アクティブなインスタンスに障害が発生した場合に手動実行可能なパッシブ バックアップとして、Manager Service コンポーネントの別のインスタンスをインストールできます。[「Backup Manager Service コンポーネントのインストール」](#)を参照してください。
- システム管理者は、実行時（インストールの完了後）に SQL データベースへのアクセスに使用する認証方法を変更できます。[「IaaS データベースにアクセスするための Windows サービスの構成」](#)を参照してください。

Backup Manager Service コンポーネントのインストール

バックアップの Manager Service は冗長性と高可用性を提供し、アクティブなサービスが停止した場合に手動で起動できます。

Manager Service の自動フェイルオーバーを有効にする場合を除き、IaaS の展開で Manager Service を同時に実行できる Windows マシンは 1 台だけです。バックアップのマシンは、サービスを停止し、手動で開始するように構成する必要があります。

[「Manager Service の自動フェイルオーバーについて」](#)を参照してください。

前提条件

- IaaS の他のコンポーネントがすでにインストールされている場合は、作成したデータベースのパスフレーズを確認します。
- (オプション) Manager Service をデフォルトとは異なる Web サイトにインストールする場合には、最初にインターネット インフォメーション サービスに Web サイトを作成します。
- vRealize Automation アプライアンス管理インターフェイスを使用して、新しいノードの FQDN を含めるように証明書を置き換えます。[vRealize Automation アプライアンスでの証明書の置き換え](#)を参照してください。
- 認証局の証明書が IIS にインポートされており、ルート証明書また認証局が信頼できることを確認します。ロード バランサのすべてのコンポーネントが同じ証明書を持っている必要があります。
- Web サイト ロード バランサが構成されていることを確認します。
- [「IaaS Web サイト コンポーネントと Model Manager Data のインストール」](#)。

手順

- 1 ロード バランサを使用している場合は、ロード バランサの下他のノードを無効にして、トラフィックが目的のノードに転送されることを確認します。

さらに、すべての vRealize Automation コンポーネントがインストールされて設定されるまで、ロード バランサの健全性チェックを無効にします。
- 2 セットアップ ファイル `setup__<vrealize-automation-appliance-FQDN>@5480.exe` を右クリックして、[管理者として実行] を選択します。
- 3 [次へ] をクリックします。
- 4 使用許諾契約に同意し、[次へ] をクリックします。

- 5 ログイン ページで vRealize Automation アプライアンスの管理者認証情報を入力し、SSL 証明書を確認します。
 - a ユーザー名 (**root**) とパスワードを入力します。
 入力するパスワードは、vRealize Automation アプライアンスを展開したときに指定したパスワードです。
 - b [証明書の受け入れ] を選択します。
 - c [証明書の表示] をクリックします。
 証明書のサムプリントを、vRealize Automation アプライアンスに設定されているサムプリントと比較します。管理コンソールにポート 5480 でアクセスしている場合は、クライアント ブラウザで vRealize Automation アプライアンス証明書を表示できます。
- 6 [次へ] をクリックします。
- 7 [インストール タイプ] ページで [カスタム インストール] を選択します。
- 8 [インストール タイプ] ページの [コンポーネントの選択] で [IaaS サーバ] を選択します。
- 9 ルートのインストール場所を受け入れるか、[変更] をクリックしてインストール パスを選択します。
 分散型展開の場合でも、同じ Windows サーバに複数の IaaS コンポーネントをインストールする場合があります。
 複数の IaaS コンポーネントをインストールする場合は、常に同じパスにインストールしてください。
- 10 [次へ] をクリックします。
- 11 [IaaS サーバのカスタム インストール] ページで [Manager Service] を選択します。
- 12 [IaaS サーバ] テキスト ボックスで IaaS Web サーバ コンポーネントを見つけます。

| オプション | 説明 |
|---------------|--|
| ロード バランサがある場合 | IaaS Web サーバ コンポーネントのロード バランサの完全修飾ドメイン名とポート番号 (<web-load-balancer.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |
| ロード バランサがない場合 | IaaS Web サーバ コンポーネントをインストールしたマシンの完全修飾ドメイン名とポート番号 (<web.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |

デフォルト ポートは 443 です。

- 13 [ディザスタ リカバリ コールド スタンバイ ノード] を選択します。
- 14 [管理と Model Manager Web サイト] タブで使用可能な Web サイトから Web サイトを選択するか、デフォルトの Web サイトを受け入れます。
- 15 [ポート番号] テキスト ボックスに使用可能なポート番号を入力するか、デフォルト ポート 443 を受け入れます。
- 16 [バインドのテスト] をクリックしてポート番号が使用できることを確認します。

17 このコンポーネント用の証明書を選択します。

- a インストールを開始した後に証明書をインポートした場合、[更新] をクリックしてリストをアップデートします。
- b [使用可能な証明書] から使用する証明書を選択します。
- c フレンドリ名を持たない証明書をインポートし、それがリストに表示されない場合には、[フレンドリ名を使用して証明書を表示] を選択解除し、[更新] をクリックします。

ロード バランサを使用しない環境にインストールする場合には、証明書を選択する代わりに[自己署名証明書の生成] を選択できます。ロード バランサ配下に追加 Web サイト コンポーネントをインストールする場合、自己署名証明書は生成しないでください。ロード バランサ配下のすべてのサーバ上で同じ証明書を使用するには、メインの IaaS Web サーバから証明書をインポートします。

18 (オプション) [証明書の表示] をクリックし、証明書を表示し、[OK] をクリックして情報ウィンドウを閉じます。

19 [次へ] をクリックします。

20 前提条件を確認し、[次へ] をクリックします。

21 [サーバとアカウントの設定] ページの [サーバー インストール情報] テキスト ボックスに、現在のインストールサーバに対する管理者権限を持ったサービス アカウント ユーザーのユーザー名とパスワードを入力します。

サービス アカウント ユーザーは、分散された各 IaaS サーバに対する権限を持った単一のドメイン アカウントである必要があります。ローカル システム アカウントは使用しないでください。

22 データベースを保護する暗号化キーの生成に使用したパスフレーズを指定します。

| オプション | 説明 |
|------------------------------|---|
| この環境にすでにコンポーネントをインストールしている場合 | [パスフレーズ] および [確認] テキスト ボックスに以前に作成したパスフレーズを入力します。 |
| 初めてのインストールの場合 | [パスフレーズ] および [確認] テキスト ボックスにパスフレーズを入力します。このパスフレーズは、新しいコンポーネントをインストールするたびに使用する必要があります。 |

今後の使用のために、このパスフレーズは安全な場所に保管してください。

23 [Microsoft SQL データベースのインストール情報] テキスト ボックスに IaaS データベース サーバ、データベース名、およびデータベース サーバの認証方法を指定します。

これは以前に作成した IaaS データベース サーバ、名前、および認証情報です。

24 [次へ] をクリックします。

25 [インストール] をクリックします。

26 インストールが完了したら、[初期構成へガイド] を選択解除し、[次へ] をクリックします。

27 [完了] をクリックします。

次のステップ

- インストールした Manager Service がパッシブ バックアップ インスタンスとなるようにするには、vRealize Automation サービスが実行されていないことを確認して、「手動」起動タイプに設定します。

- システム管理者は、実行時（インストールの完了後）に SQL データベースへのアクセスに使用する認証方法を変更できます。[「IaaS データベースにアクセスするための Windows サービスの構成」](#)を参照してください。

Distributed Execution Manager のインストール

Distributed Execution Manager は、2 つのロール DEM Orchestrator または DEM ワーカーのいずれかとしてインストールします。各ロールに対して少なくとも 1 つの DEM インスタンスをインストールする必要があり、フェイルオーバーおよび高可用性をサポートするために追加の DEM インスタンスをインストールできます。

システム管理者は、事前定義済みのシステム要件を満たすインストール マシンを選択する必要があります。DEM Orchestrator およびワーカーは、同じマシンに配置できます。

Distributed Execution Manager のインストールを計画する際、次の点を考慮してください。

- DEM Orchestrator はアクティブ - アクティブの高可用性をサポートしています。通常は、各 Manager Service マシンに 1 つの DEM Orchestrator をインストールします。
- Model Manager ホストに対して強いネットワーク接続のあるマシンに Orchestrator をインストールします。
- フェイルオーバーのため、2 目目の DEM Orchestrator を別のマシンにインストールします。
- 通常、DEM ワーカーは IaaS Manager Service サーバまたは個別のサーバにインストールします。このサーバは Model Manager ホストに対してネットワーク接続がある必要があります。
- 冗長性およびスケーラビリティを得るため、追加 DEM インスタンスをインストールできます。同じマシン上に複数のインスタンスをインストールすることも可能です。

使用するエンドポイントに応じて、DEM インストールについての特定の要件があります。[「IaaS Distributed Execution Manager ホスト」](#)を参照してください。

Distributed Execution Manager のインストール

DEM ワーカーおよび DEM Orchestrator を 1 つ以上インストールする必要があります。インストール手順はいずれのロールでも同じです。

DEM Orchestrator はアクティブ - アクティブの高可用性をサポートしています。通常は、各 Manager Service マシンに 1 つの DEM Orchestrator をインストールします。DEM Orchestrator と DEM ワーカーは同じマシンにインストールできます。

前提条件

[「vRealize Automation IaaS インストーラのダウンロード」](#)。

手順

- 1 セットアップ ファイル `setup__<vrealize-automation-appliance-FQDN>@5480.exe` を右クリックして、[管理者として実行] を選択します。
- 2 [次へ] をクリックします。
- 3 使用許諾契約に同意し、[次へ] をクリックします。

- 4 ログイン ページで vRealize Automation アプライアンスの管理者認証情報を入力し、SSL 証明書を確認します。
 - a ユーザー名 (**root**) とパスワードを入力します。

入力するパスワードは、vRealize Automation アプライアンスを展開したときに指定したパスワードです。

- b [証明書の受け入れ] を選択します。
- c [証明書の表示] をクリックします。

証明書のサムプリントを、vRealize Automation アプライアンスに設定されているサムプリントと比較します。管理コンソールにポート 5480 でアクセスしている場合は、クライアント ブラウザで vRealize Automation アプライアンス証明書を表示できます。

- 5 [次へ] をクリックします。
- 6 [インストール タイプ] ページで [カスタム インストール] を選択します。
- 7 [インストール タイプ] ページの [コンポーネントの選択] で [Distributed Execution Manager] を選択します。
- 8 ルートのインストール場所を受け入れるか、[変更] をクリックしてインストール パスを選択します。

分散型展開の場合でも、同じ Windows サーバに複数の IaaS コンポーネントをインストールする場合があります。

複数の IaaS コンポーネントをインストールする場合は、常に同じパスにインストールしてください。

- 9 [次へ] をクリックします。
- 10 前提条件を確認し、[次へ] をクリックします。
- 11 サービスを実行するときのログイン認証情報を入力します。

サービス アカウントは、ローカル管理者特権を持ち、かつ IaaS のインストールで使ったドメイン アカウントである必要があります。サービス アカウントは、それぞれの分散型 IaaS サーバに対する特権を持ち、ローカル システム アカウントであってははいけません。

- 12 [次へ] をクリックします。
- 13 [DEM ロール] ドロップダウン メニューからインストール タイプを選択します。

| オプション | 説明 |
|----------------|--|
| [ワーカー] | ワーカーはワークフローを実行します。 |
| [Orchestrator] | Orchestrator は、ワークフローのスケジューリングおよび前処理などの DEM ワーカーのアクティビティを監視し、DEM ワーカーのオンライン ステータスを監視します。 |

- 14 [DEM 名] テキスト ボックスにこの DEM を識別する一意の名前を入力します。

名前にはスペースは含まれず、128 文字を超えてはなりません。以前に使用した名前を入力すると、次のメッセージが表示されます。「DEM 名はすでに存在します。この DEM に別の名前を入力するには、[はい] をクリックしてください。同じ名前の DEM をリストアまたは再インストールするには [いいえ] をクリックしてください。」

- 15 (オプション) [DEM の説明] にこのインスタンスの説明を入力します。

- 16 [Manager Service のホスト名] および [Model Manager Web サービスのホスト名] テキスト ボックスにホスト名とポートを入力します。

| オプション | 説明 |
|---------------|---|
| ロード バランサがある場合 | Manager Service コンポーネントおよび Model Manager をホストしている Web サーバのロード バランサの完全修飾ドメイン名とポート番号 (<mgr-svc-load-balancer.mycompany.com>:443 および <web-load-balancer.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |
| ロード バランサがない場合 | Manager Service コンポーネントをインストールしたマシンおよび Model Manager をホストしている Web サーバの完全修飾ドメイン名とポート番号 (<mgr-svc.mycompany.com>:443 および <web.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |

デフォルト ポートは 443 です。

- 17 (オプション) [テスト] をクリックして、Manager Service および Model Manager Web サービスへの接続をテストします。
- 18 [追加] をクリックします。
- 19 [次へ] をクリックします。
- 20 [インストール] をクリックします。
- 21 インストールが完了したら、[初期構成へガイド] を選択解除し、[次へ] をクリックします。
- 22 [完了] をクリックします。

次のステップ

- サービスが実行されており、ログにエラーが記録されていないことを検証します。サービス名は、VMware DEM <ロール> - <名前> です。ロールは、Orchestrator またはワーカーになります。ログの場所は、<インストール場所>\Distributed Execution Manager\Name\Logs です。
- この手順を繰り返して、追加の DEM インスタンスをインストールします。

異なるインストール パスで SCVMM に接続する DEM の構成

デフォルトでは、DEM ワーカー構成ファイルには Microsoft System Center Virtual Machine Manager (SCVMM) コンソールのデフォルトのインストール パスが使用されています。デフォルト以外の場所に SCVMM コンソールをインストールする場合は、このファイルを更新する必要があります。

SCVMM エンドポイントとエージェントがある場合は、この手順のみが必要です。

前提条件

- SCVMM コンソールがインストールされているデフォルト以外のパスを確認します。

構成ファイルで置き換える必要のあるデフォルトのパスを次に示します。

```
path="{ProgramFiles}\Microsoft System Center 2012 R2\Virtual Machine Manager\bin"
```

手順

- 1 DEM ワーカー サービスを停止します。
- 2 テキスト エディタで次のファイルを開きます。

Program Files (x86)\VMware\VCAC\Distributed Execution Manager\<instance-name>\DynamicOps.DEM.exe.config

- 3 <assemblyLoadConfiguration> セクションを見つけます。
- 4 次の例をガイドラインにして、各 path を更新します。

```
<assemblyLoadConfiguration>
  <assemblies>
    <!-- List of required assemblies for Scvmm -->
    <add name="Errors" path="D:\Microsoft System Center 2012 R2\Virtual Machine
Manager\bin"/>
    <add name="Microsoft.SystemCenter.VirtualMachineManager" path="D:\Microsoft System
Center 2012 R2\Virtual Machine Manager\bin"/>
    <add name="Remoting" path="D:\Microsoft System Center 2012 R2\Virtual Machine
Manager\bin"/>
    <add name="TraceWrapper" path="D:\Microsoft System Center 2012 R2\Virtual Machine
Manager\bin"/>
    <add name="Utils" path="D:\Microsoft System Center 2012 R2\Virtual Machine
Manager\bin"/>
  </assemblies>
</assemblyLoadConfiguration>
```

- 5 DynamicOps.DEM.exe.config を保存して閉じます。
- 6 DEM ワーカー サービスを再起動します。

詳細については、[「SCVMM と DEM ワーカー」](#) を参照してください。

SCVMM 環境の準備と、SCVMM エンドポイントの作成の詳細については、[SCVMM 環境の準備](#)および [Hyper-V \(SCVMM\) エンドポイントの作成](#)を参照してください。

laaS データベースにアクセスするための Windows サービスの構成

システム管理者は、実行時（インストールの完了後）に SQL データベースへのアクセスに使用する認証方法を変更できます。デフォルトの場合、インストール後は、現在のログオン アカウントの Windows ID を使用してデータベースに接続します。

サービス ユーザーからの laaS データベース アクセスの有効化

SQL データベースを Manager Service とは別のホストにインストールする場合、Manager Service からのデータベース アクセスを有効にする必要があります。Manager Service を実行するユーザー名がデータベースの所有者の場合は、操作は必要ありません。ユーザーがデータベースの所有者ではない場合、システム管理者がアクセス権を付与する必要があります。

前提条件

- [「laaS データベース シナリオの選択」](#)。

- Manager Service を実行するユーザー名がデータベースの所有者ではないことを確認します。

手順

- 1 インストール zip アーカイブを抽出したディレクトリ内にある **Database** サブディレクトリに移動します。
- 2 **DBInstall.zip** アーカイブをローカル ディレクトリに抽出します。
- 3 SQL Server インスタンスの **sysadmin** ロールを持つユーザーとしてデータベース ホストにログインします。
- 4 **VMPSOpsUser.sql** を編集し、**\$(Service User)** のすべてのインスタンスを Manager Service を実行するユーザー（手順 3）に置き換えます。

WHERE name = N'ServiceUser' で終わる行の **ServiceUser** は置き換えないでください。

- 5 SQL Server Management Studio を開きます。
- 6 左側のペインの [データベース] 内のデータベース（デフォルトでは vCAC）を選択します。
- 7 [新規クエリ] をクリックします。
右側のペインに SQL クエリ ウィンドウが開きます。
- 8 **VMPSOpsUser.sql** の変更されたコンテンツをクエリ ウィンドウに貼り付けます。
- 9 [実行] をクリックします。

Manager Service からのデータベース アクセスが有効になります。

SQL 認証を使用するための Windows サービス アカウントの構成

デフォルトでは、SQL 認証用にデータベースを設定した場合でも、Windows サービス アカウントは実行中にデータベースにアクセスします。ランタイムの認証方法を Windows から SQL へ変更できます。

ランタイムの認証方法を変更する理由の 1 つは、データベースが信頼されていないドメインにある場合などです。

前提条件

vRealize Automation SQL Server データベースがあることを確認します。まずは [IaaS データベース シナリオの選択](#) の手順を実行します。

手順

- 1 管理者権限を持つアカウントを使用して、Manager Service がホストされている IaaS Windows サーバにログインします。
- 2 [管理ツール] - [サービス] で [VMware vCloud Automation Center] サービスを停止します。
- 3 テキスト エディタで次のファイルを開きます。

```
C:\Program Files (x86)\VMware\vCAC\Server\ManagerService.exe.config
C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Web\Web.config
```

- 4 各ファイルで <connectionStrings> セクションを見つけます。

- 5 次の文字列を見つけます。

```
Integrated Security=True;
```

上記の文字列を次のように置き換えます。

```
User Id=<database-username>;Password=<database-password>;
```

- 6 ファイルを保存して閉じます。

```
ManagerService.exe.config
Web.config
```

- 7 [VMware vCloud Automation Center] サービスを開始します。

- 8 **iisreset** コマンドを使用して IIS を再起動します。

laaS サービスの確認

インストール後、システム管理者は laaS サービスが実行していることを確認します。サービスが実行中の場合、インストールは成功しています。

手順

- 1 laaS マシンの Windows デスクトップから、[管理ツール] - [サービス] を選択します。
- 2 次のサービスを見つけ、そのステータスが [開始済み] であることと、[起動タイプ] が [自動] に設定されていることを確認します。
 - VMware DEM – Orchestrator – <Name>。<Name> は、インストール中に [DEM 名] ボックスに入力された文字列です。
 - VMware DEM – Worker – <Name>。<Name> は、インストール中に [DEM 名] ボックスに入力された文字列です。
 - VMware vCloud Automation Center エージェント <Agent name>
 - VMware vCloud Automation Center サービス
- 3 [サービス] ウィンドウを閉じます。

vRealize Automation エージェントのインストール

vRealize Automation はエージェントを使用して外部システムと統合されます。システム管理者は、他の仮想プラットフォームとの通信のためにインストールするエージェントを選択できます。

vRealize Automation は次のエージェントのタイプを使用して外部システムを管理します。

- ハイパーバイザー プロキシ エージェント (vSphere、Citrix Xen サーバおよび Microsoft Hyper-V サーバ)
- 外部プロビジョニング インフラストラクチャ (EPI) 統合エージェント
- 仮想デスクトップ インフラストラクチャ (VDI) エージェント
- Windows Management Instrumentation (WMI) エージェント

高可用性を実現するため、1 つのエンドポイントに対して複数のエージェントをインストールすることができます。各冗長エージェントを個別のサーバにインストールしますが、エージェントの名前および構成は同一にします。冗長エージェントには、ある程度のフォールトトレランスがありますが、フェイルオーバー機能はありません。たとえば、サーバ A とサーバ B にそれぞれ 1 つずつ、計 2 つの vSphere エージェントをインストールしている場合は、サーバ A が動作を停止すると、サーバ B にインストールされているエージェントが作業アイテムの処理を続けます。ただし、サーバ B のエージェントは、サーバ A のエージェントがすでに開始済みの作業アイテムの処理を終了することはできません。

最小インストールの一部として vSphere エージェントをインストールするオプションを選択することもできますが、インストール後は、追加の vSphere エージェントを含む他のエージェントを追加することもできます。分散導入環境では、基本分散インストールを完了した後にすべてのエージェントをインストールします。インストールするエージェントは、使用するインフラストラクチャのリソースにより異なります。

vSphere エージェントの使用の詳細については、[\[vSphere エージェントの要件\]](#) を参照してください。

PowerShell 実行ポリシーの RemoteSigned への設定

ローカルの PowerShell スクリプトを実行できるようにするには、PowerShell 実行ポリシーを Restricted から RemoteSigned または Unrestricted に設定する必要があります。

PowerShell 実行ポリシーの詳細については、[実行ポリシーに関する Microsoft PowerShell の記事](#)を参照してください。PowerShell 実行ポリシーがグループポリシーレベルで管理されている場合は、IT サポートに連絡し、ポリシー変更に関する制限について確認するとともに、[グループポリシー設定に関する Microsoft PowerShell の記事](#)も参照してください。

前提条件

- ホストにエージェントをインストールする前に Microsoft PowerShell がホストにインストールされていることを確認します。必要なバージョンはホストのオペレーティングシステムにより異なります。Microsoft のヘルプおよびサポートを参照してください。
- PowerShell 実行ポリシーの詳細については、PowerShell のコマンドプロンプトで **help about_signing** または **help Set-ExecutionPolicy** を実行してください。

手順

- 1 管理者アカウントを使用して、エージェントがインストールされている IaaS ホストマシンにログインします。
- 2 [スタート]-[すべてのプログラム]-[Windows PowerShell バージョン]-[Windows PowerShell] を選択します。
- 3 Remote Signed では **Set-ExecutionPolicy RemoteSigned** を実行します。
- 4 Unrestricted では **Set-ExecutionPolicy Unrestricted** を実行します。
- 5 コマンドによりエラーが発生していないことを確認します。
- 6 PowerShell コマンドプロンプトで **Exit** と入力します。

エージェントのインストールシナリオの選択

インストールが必要なエージェントは、統合する外部システムによって異なります。

表 1-37. エージェント シナリオの選択

| 統合シナリオ | エージェントの要件と手順 |
|--|---|
| Amazon Web Services や Red Hat Enterprise Linux OpenStack Platform などのクラウド環境と統合することにより、クラウドマシンをプロビジョニングします。 | エージェントをインストールする必要はありません。 |
| vSphere 環境と統合することにより、仮想マシンをプロビジョニングします。 | 「vSphere 用のプロキシ エージェントのインストールと構成」 |
| Microsoft Hyper-V Server 環境と統合することにより、仮想マシンをプロビジョニングします。 | 「Hyper-V または XenServer 用のプロキシ エージェントのインストール」 |
| XenServer 環境と統合することにより、仮想マシンをプロビジョニングします。 | <ul style="list-style-type: none"> ■ 「Hyper-V または XenServer 用のプロキシ エージェントのインストール」 ■ 「Citrix 用の EPI エージェントのインストール」 |
| XenDesktop 環境と統合することにより、仮想マシンをプロビジョニングします。 | <ul style="list-style-type: none"> ■ 「XenDesktop 用の VDI エージェントのインストール」 ■ 「Citrix 用の EPI エージェントのインストール」 |
| マシンのプロビジョニング前後またはプロビジョニング解除時に、プロビジョニング プロセスの追加手順として Visual Basic スクリプトを実行します。 | 「Visual Basic スクリプト処理用の EPI エージェントのインストール」 |
| プロビジョニングされた Windows マシンから、マシン所有者の Active Directory ステータスなどのデータを収集します。 | 「リモート WMI 申請用の WMI エージェントのインストール」 |
| サポートされている他の仮想プラットフォームと統合することにより、仮想マシンをプロビジョニングします。 | エージェントをインストールする必要はありません。 |

エージェントのインストールの場所および要件

システム管理者は通常、アクティブな Manager Service コンポーネントをホストする vRealize Automation サーバにエージェントをインストールします。

エージェントが別のホストにインストールされている場合、ネットワーク構成で、エージェントと Manager Service をインストールするマシンとの間での通信を可能にする必要があります。

各エージェントは、vRealize Automation インストール ディレクトリ（通常は **Program Files(x86)\VMware\VCAC**）の下にある固有のディレクトリ **Agents\<agentname>** に一意の名前でインストールされ、その構成はそのディレクトリのファイル **VRMAgent.exe.config** に保存されます。

vSphere 用のプロキシ エージェントのインストールと構成

システム管理者は、vSphere サーバ インスタンスとの通信のためにプロキシ エージェントをインストールします。エージェントは、使用可能な作業を検出し、ホスト情報を取得し、完了した作業アイテムや他のホスト ステータスの変更をレポートします。

vSphere エージェントの要件

vSphere エンドポイントの認証情報、またはエージェント サービスの実行の際に使用される認証情報には、インストール ホストへの管理アクセスが含まれている必要があります。複数の vSphere エージェントが vRealize Automation の構成要件を満たしている必要があります。

認証情報

vSphere エージェントによって管理される vCenter Server インスタンスを示すエンドポイントの作成時に、エージェントは vCenter Server と対話するためにサービスが実行している認証情報を使用するか、別のエンドポイント認証情報を指定することができます。

次の表は vCenter Server インスタンスを管理するために vSphere エンドポイントの認証情報に付与されている必要がある権限の一覧です。これらの権限は、エンドポイントをホストするクラスタだけでなく、vCenter Server 内のすべてのクラスタで有効になっている必要があります。

表 1-38. vCenter Server インスタンス管理に vSphere エージェントに必要な権限

| 属性値 | | 権限 |
|-------------|--------|----------------------|
| データストア | | 容量の割り当て |
| | | データストアの参照 |
| データストア クラスタ | | データストア クラスタの構成 |
| フォルダ | | フォルダの作成 |
| | | フォルダの削除 |
| グローバル | | カスタム属性の管理 |
| | | カスタム属性の設定 |
| ネットワーク | | ネットワークの割り当て |
| 権限 | | 権限の変更 |
| リソース | | VM のリソース プールへの割り当て |
| | | パワーオフ状態の仮想マシンの移行 |
| | | パワーオン状態の仮想マシンの移行 |
| 仮想マシン | インベントリ | 既存のものから作成 |
| | | 新規作成 |
| | | 移動 |
| | | 削除 |
| | 相互作用 | CD メディアの構成 |
| | | コンソールでの相互作用 |
| | | デバイス接続 |
| | | パワーオフ |
| | | パワーオン |
| | | リセット |
| | | サスペンド |
| | | VMware Tools のインストール |
| | 設定 | 既存ディスクの追加 |
| | | 新しいディスクの追加 |
| | | デバイスの追加または削除 |

表 1-38. vCenter Server インスタンス管理に vSphere エージェントに必要な権限 (続き)

| 属性値 | | 権限 |
|----------|--|----------------------|
| | | ディスクの削除 |
| | | 詳細 |
| | | CPU カウントの変更 |
| | | リソースの変更 |
| | | 仮想ディスクの拡張 |
| | | ディスク変更の追跡 |
| | | メモリ |
| | | デバイス設定の変更 |
| | | 名前の変更 |
| | | 注釈の設定 (バージョン 5.0 以降) |
| | | 設定 |
| | | スワップファイルの配置 |
| プロビジョニング | | カスタマイズ |
| | | テンプレートのクローン作成 |
| | | 仮想マシンのクローン作成 |
| | | テンプレートのデプロイ |
| | | カスタム仕様の読み取り |
| 状態 | | スナップショットの作成 |
| | | スナップショットの削除 |
| | | スナップショットまで戻る |

vRealize Automation 外部の仮想マシンの電源状態を変更する可能性のあるサードパーティー製ソフトウェアを無効または再構成します。このような変更は、vRealize Automation によるマシン ライフ サイクルの管理を妨害する可能性があります。

vSphere エージェントのインストール

vSphere エージェントをインストールして vCenter Server のインスタンスを管理します。高可用性を実現するため、同じ vCenter Server インスタンスについて、2 つ目の冗長 vSphere エージェントをインストールすることができます。両方の vSphere エージェントの名前および構成を同一にし、異なるマシンにインストールする必要があります。

前提条件

- Web サーバと Manager Service ホストを含め IaaS をインストールします。
- エージェントをインストールするマシンは、IaaS コンポーネントがインストールされているドメインによって信頼されるドメインに配備されていることを確認します。
- [\[vSphere エージェントの要件\]](#) の要件が満たされていることを確認します。

- このエージェントとともに使用する vSphere エンドポイントをすでに作成している場合、エンドポイント名をメモします。
- [\[vRealize Automation IaaS インストーラのダウンロード\]](#)。

手順

- 1 セットアップ ファイル `setup__<vrealize-automation-appliance-FQDN>@5480.exe` を右クリックして、[管理者として実行] を選択します。
- 2 [次へ] をクリックします。
- 3 使用許諾契約に同意し、[次へ] をクリックします。
- 4 ログイン ページで vRealize Automation アプライアンスの管理者認証情報を入力し、SSL 証明書を確認します。
 - a ユーザー名 (**root**) とパスワードを入力します。

入力するパスワードは、vRealize Automation アプライアンスを展開したときに指定したパスワードです。
 - b [証明書の受け入れ] を選択します。
 - c [証明書の表示] をクリックします。

証明書のサムプリントを、vRealize Automation アプライアンスに設定されているサムプリントと比較します。管理コンソールにポート 5480 でアクセスしている場合は、クライアント ブラウザで vRealize Automation アプライアンス証明書を表示できます。
- 5 [インストール タイプ] ページで [カスタム インストール] を選択します。
- 6 [コンポーネントの選択] 領域で [プロキシ エージェント] を選択します。
- 7 ルートのインストール場所を受け入れるか、[変更] をクリックしてインストール パスを選択します。

分散型展開の場合でも、同じ Windows サーバに複数の IaaS コンポーネントをインストールする場合があります。複数の IaaS コンポーネントをインストールする場合は、常に同じパスにインストールしてください。
- 8 [次へ] をクリックします。
- 9 インストール マシンの Windows サービスの管理者権限でログインします。

サービスは、同じインストール マシンで実行する必要があります。
- 10 [次へ] をクリックします。
- 11 [エージェント タイプ] リストから vSphere を選択します。

12 [エージェント名] テキスト ボックスに、このエージェントの識別子を入力します。

各エージェントのエージェント名、認証情報、エンドポイント名、およびプラットフォーム インスタンスの情報を記録しておきます。この情報は、エンドポイントを構成し、後ほどホストを追加するために必要です。

重要: 高可用性のために、冗長エージェントを追加して、同じ設定を構成できます。それ以外の場合は、固有のエージェントを構成します。

| オプション | 説明 |
|----------------|---|
| 冗長エージェント | 異なるサーバに冗長エージェントをインストールします。 冗長エージェントに同じ名前と設定を構成します。 |
| スタンドアロン エージェント | エージェントに一意の名前を割り当てます。 |

13 IaaS Manager Service ホストへの接続を構成します。

| オプション | 説明 |
|---------------|---|
| ロード バランサがある場合 | Manager Service コンポーネントのロード バランサの完全修飾ドメイン名とポート番号 (<mgr-svc-load-balancer.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |
| ロード バランサがない場合 | Manager Service コンポーネントをインストールしたマシンの完全修飾ドメイン名とポート番号 (<mgr-svc.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |

デフォルト ポートは 443 です。

14 IaaS Web サーバへの接続を構成します。

| オプション | 説明 |
|---------------|---|
| ロード バランサがある場合 | Web サーバ コンポーネントのロード バランサの完全修飾ドメイン名とポート番号 (<web-load-balancer.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |
| ロード バランサがない場合 | Web サーバ コンポーネントをインストールしたマシンの完全修飾ドメイン名とポート番号 (<web.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |

デフォルト ポートは 443 です。

15 [テスト] をクリックし、各ホストへの接続を確認します。

16 エンドポイントの名前を入力します。

vRealize Automation で設定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。一致しないと、エンドポイントは機能しません。

17 [追加] をクリックします。

18 [次へ] をクリックします。

19 [インストール] をクリックして、インストールを開始します。

数分後、正常に処理が行われたことを伝えるメッセージが表示されます。

- 20 [次へ] をクリックします。
- 21 [完了] をクリックします。
- 22 正常にインストールされたことを検証します。
- 23 (オプション) 同じシステムで、構成の異なる複数のエージェントと、1 つのエンドポイントを追加します。

次のステップ

[「vSphere エージェントの設定」](#)。

vSphere エージェントの設定

vRealize Automation ブループリント内で vSphere エンドポイントを作成し使用するのに備え、vSphere エージェントを設定します。

プロキシ エージェント ユーティリティを使用して、エージェントの構成ファイルの暗号化された部分を変更するか、仮想化プラットフォームのマシン削除ポリシーを変更します。VRMAgent.exe.config エージェントの構成ファイルの一部のみが暗号化されています。たとえば、**serviceConfiguration** セクションは暗号化されていません。

前提条件

管理者権限を備えたアカウントを使用して、vSphere エージェントをインストールした IaaS Windows サーバにログインします。

手順

- 1 管理者として Windows コマンド プロンプトを開きます。
- 2 エージェントのインストール フォルダに移動します。 <agent-name> フォルダに vSphere エージェントが含まれています。

```
cd %SystemDrive%\Program Files (x86)\VMware\VCAC\Agents\<agent-name>
```

- 3 (オプション) 現在の設定を表示するには、以下のコマンドを入力します。

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get
```

このコマンドの出力例を、次に示します。

```
managementEndpointName: VCendpoint
doDeletes: True
```

- 4 (オプション) インストール時に設定したエンドポイント名を変更するには、以下のコマンドを使用します。

```
set managementEndpointName
```

たとえば、**DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set managementEndpointName <my-endpoint>** と入力します。

エンドポイントを変更する代わりにこのプロセスを使用して、vRealize Automation 内のエンドポイントの名前を変更します。

- 5 (オプション) 仮想マシンの削除ポリシーを設定するには、以下のコマンドを使用します。

set doDeletes

たとえば、`DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set doDeletes <false>` と入力します。

| オプション | 説明 |
|-------|---|
| true | (デフォルト) vRealize Automation で破棄された仮想マシンを vCenter Server から削除します。 |
| false | vRealize Automation で破棄された仮想マシンを vCenter Server の VRMDeleted ディレクトリに移動します。 |

- 6 [管理ツール] - [サービス] を開いて vRealize Automation エージェント - <agent-name> サービスを再起動します。

次のステップ

高可用性を実現するため、エンドポイントの冗長エージェントをインストールおよび構成します。各冗長エージェントを別個のサーバにインストールしますが、エージェントの名前および構成は同一にします。

Hyper-V または XenServer 用のプロキシ エージェントのインストール

システム管理者は、Hyper-V および XenServer サーバ インスタンスとの通信のためにプロキシ エージェントをインストールします。エージェントは、使用可能な作業を検出し、ホスト情報を取得し、完了した作業アイテムや他のホスト ステータスの変更をレポートします。

Hyper-V および XenServer の要件

Hyper-V Hypervisor のプロキシ エージェントでは、インストールにシステム管理者の認証情報を必要とします。

エージェント サービスを実行するための認証情報には、インストール ホストへの管理アクセス権が必要です。

管理者レベルの認証情報は、エージェントによって管理されるホスト上のすべての XenServer または Hyper-V インスタンスで必要になります。

Xen プールを使用する場合には、Xen プール内のすべてのノードが完全修飾ドメイン名で識別される必要があります。

注: デフォルトでは、Hyper-V はリモート管理用に構成されていません。vRealize AutomationHyper-V のプロキシ エージェントは、リモート管理が有効にされていないと Hyper-V サーバと通信できません。

Hyper-V のリモート管理用の構成方法については、Microsoft Windows Server のドキュメントを参照してください。

Hyper-V または XenServer エージェントのインストール

Hyper-V エージェントは Hyper-V サーバ インスタンスを管理します。XenServer エージェントは XenServer サーバ インスタンスを管理します。

前提条件

- Web サーバと Manager Service ホストを含め IaaS をインストールします。
- [「vRealize Automation IaaS インストーラのダウンロード」](#)。

- Hyper-V Hypervisor のプロキシ エージェントにシステム管理者の認証情報があることを確認します。
- エージェント サービスを実行するための認証情報に、インストール ホストへの管理アクセス権があることを確認します。
- ホスト上のすべての XenServer または Hyper-V インスタンスが管理者レベルの認証情報を持つエージェントに管理されることを確認します。
- Xen プールを使用する場合には、Xen プール内のすべてのノードが完全修飾ドメイン名で識別される必要があります。

vRealize Automation は、Xen プール内の完全修飾ドメイン名により識別されないノードに対して通信や管理ができません。

- Hyper-V をリモート管理用に構成して、Hyper-V サーバの vRealize AutomationHyper-V プロキシ エージェントとの通信を有効にします。

Hyper-V のリモート管理用の構成方法については、Microsoft Windows Server のドキュメントを参照してください。

手順

- 1 セットアップ ファイル `setup__<vrealize-automation-appliance-FQDN>@5480.exe` を右クリックして、[管理者として実行] を選択します。
- 2 [次へ] をクリックします。
- 3 使用許諾契約に同意し、[次へ] をクリックします。
- 4 ログイン ページで vRealize Automation アプライアンスの管理者認証情報を入力し、SSL 証明書を確認します。
 - a ユーザー名 (**root**) とパスワードを入力します。
 入力するパスワードは、vRealize Automation アプライアンスを展開したときに指定したパスワードです。
 - b [証明書の受け入れ] を選択します。
 - c [証明書の表示] をクリックします。
 証明書のサムプリントを、vRealize Automation アプライアンスに設定されているサムプリントと比較します。管理コンソールにポート 5480 でアクセスしている場合は、クライアント ブラウザで vRealize Automation アプライアンス証明書を表示できます。
- 5 [インストール タイプ] ページで [カスタム インストール] を選択します。
- 6 インストール タイプ ページで [Component Selection (コンポーネントの選択)] をクリックします。
- 7 ルートのインストール場所を受け入れるか、[変更] をクリックしてインストール パスを選択します。
 分散型展開の場合でも、同じ Windows サーバに複数の IaaS コンポーネントをインストールする場合があります。
 複数の IaaS コンポーネントをインストールする場合は、常に同じパスにインストールしてください。
- 8 [次へ] をクリックします。
- 9 インストール マシンの Windows サービスの管理者権限でログインします。
 サービスは、同じインストール マシンで実行する必要があります。

10 [次へ] をクリックします。

11 [エージェント タイプ] リストからエージェントを選択します。

- Xen
- Hyper-V

12 [エージェント名] テキスト ボックスに、このエージェントの識別子を入力します。

各エージェントのエージェント名、認証情報、エンドポイント名、およびプラットフォーム インスタンスの情報を記録しておきます。この情報は、エンドポイントを構成し、後ほどホストを追加するために必要です。

重要: 高可用性のために、冗長エージェントを追加して、同じ設定を構成できます。それ以外の場合は、固有のエージェントを構成します。

| オプション | 説明 |
|----------------|---|
| 冗長エージェント | 異なるサーバに冗長エージェントをインストールします。 冗長エージェントに同じ名前と設定を構成します。 |
| スタンドアロン エージェント | エージェントに一意の名前を割り当てます。 |

13 エンドポイントを構成する IaaS 管理者に [エージェント名] を通知します。

アクセスおよびデータ収集を有効にするには、エンドポイントをそのために構成されているエージェントにリンクさせる必要があります。

14 IaaS Manager Service ホストへの接続を構成します。

| オプション | 説明 |
|---------------|---|
| ロード バランサがある場合 | Manager Service コンポーネントのロード バランサの完全修飾ドメイン名とポート番号 (<mgr-svc-load-balancer.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |
| ロード バランサがない場合 | Manager Service コンポーネントをインストールしたマシンの完全修飾ドメイン名とポート番号 (<mgr-svc.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |

デフォルト ポートは 443 です。

15 IaaS Web サーバへの接続を構成します。

| オプション | 説明 |
|---------------|---|
| ロード バランサがある場合 | Web サーバ コンポーネントのロード バランサの完全修飾ドメイン名とポート番号 (<web-load-balancer.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |
| ロード バランサがない場合 | Web サーバ コンポーネントをインストールしたマシンの完全修飾ドメイン名とポート番号 (<web.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |

デフォルト ポートは 443 です。

16 [テスト] をクリックし、各ホストへの接続を確認します。

- 17 管理対象サーバのインスタンスに対して管理レベルの権限を持つユーザーの認証情報を入力します。
- 18 [追加] をクリックします。
- 19 [次へ] をクリックします。
- 20 (オプション) 別のエージェントを追加します。

たとえば、以前に Hyper-V エージェントを追加している場合には、Xen エージェントを追加できます。

- 21 [インストール] をクリックして、インストールを開始します。
- 数分後、正常に処理が行われたことを伝えるメッセージが表示されます。
- 22 [次へ] をクリックします。
- 23 [完了] をクリックします。
- 24 正常にインストールされたことを検証します。

次のステップ

高可用性を実現するため、エンドポイントの冗長エージェントをインストールおよび構成します。各冗長エージェントを別個のサーバにインストールしますが、エージェントの名前および構成は同一にします。

[「Hyper-V または XenServer エージェントの構成」](#)。

Hyper-V または XenServer エージェントの構成

システム管理者は、仮想化プラットフォームの削除ポリシーなどのプロキシ エージェント構成の設定を変更できます。プロキシ エージェント ユーティリティを使用して、エージェント構成ファイルで暗号化されている初期構成を変更できます。

前提条件

エージェントをインストールしたマシンに**システム管理者**としてログインします。

手順

- 1 エージェントのインストール ディレクトリに変更します。ここで、<agent_name> はプロキシ エージェントを含むディレクトリで、エージェントのインストール先の名前でもあります。

```
cd Program Files (x86)\VMware\vCAC Agents\<agent_name>
```

- 2 現在の構成設定を表示します。

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config get
```

 と入力します。

次に、コマンドの出力の例を示します。

```
Username: XSadmin
```

- 3 **set** コマンドを入力してプロパティを変更します。ここでの <property> は表に示されたオプションの 1 つです。

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set <property value>
```

<value> を省略すると、ユーティリティは新しい値を求めます。

| プロパティ | 説明 |
|----------|---|
| username | エージェントが通信する XenServer または Hyper-V サーバ用の管理者レベルの認証情報を表すユーザー名。 |
| password | 管理者レベルのユーザー名のパスワード。 |

- 4 [スタート] - [管理ツール] - [サービス] をクリックし、vRealize Automation エージェント - <agentname> サービスを再起動します。

例：管理者レベルの認証情報の変更

次のコマンドを入力し、エージェントのインストール時に指定した仮想化プラットフォームの管理者レベルの認証情報を変更します。

```
Dynamic0ps.Vrm.VRMencrypt.exe VRMAgent.exe.config set username jsmith
```

```
Dynamic0ps.Vrm.VRMencrypt.exe VRMAgent.exe.config set password
```

次のステップ

高可用性を実現するため、エンドポイントの冗長エージェントをインストールおよび構成します。各冗長エージェントを別個のサーバにインストールしますが、エージェントの名前および構成は同一にします。

XenDesktop 用の VDI エージェントのインストール

vRealize Automation は、仮想デスクトップ インフラストラクチャ (VDI) PowerShell エージェントを使用して、外部デスクトップ管理システムとともにプロビジョニングする XenDesktop マシンを登録します。

VDI 統合エージェントでは、登録されたマシンの所有者が XenDesktop Web インターフェイスへ直接接続できるようにします。VDI エージェントは、単一の Desktop Delivery Controller (DDC) と対話する専用のエージェントとしてインストールするか、複数の DDC と対話できる汎用エージェントとしてインストールできます。

XenDesktop の要件

システム管理者は仮想デスクトップ インフラストラクチャ (VDI) エージェントをインストールして XenDesktop サーバを vRealize Automation に統合します。

汎用 VDI エージェントをインストールして複数のサーバと通信することができます。ロード バランシングまたは認証上の理由で、サーバごとに 1 つの専用エージェントをインストールしている場合、エージェントのインストール時に XenDesktop DDC サーバの名前を指定する必要があります。専用エージェントは、その構成で指定されたサーバに向けた登録申請のみを処理できます。

XenDesktop DDC サーバ向け XenDesktop のサポート対象バージョンの情報については、VMware Web サイトで vRealize Automation のサポート マトリックスを調べてください。

インストール ホストおよび認証情報

エージェントが実行する際の認証情報には、通信するすべての XenDesktop DDC サーバへの管理アクセスが含まれている必要があります。

XenDesktop の要件

XenDesktop サーバの XenServer ホストに付けられた名前は、XenCenter の Xen プールの UUID と一致する必要があります。詳細については、「[XenServer のホスト名の設定](#)」を参照してください。

マシンを登録する各 XenDesktop DDC サーバは、次の方法で構成されている必要があります。

- vRealize Automation と使用する場合、グループとカタログのタイプを [既存] に設定する必要があります。
- DDC サーバの vCenter Server ホストの名前は、ドメインを除く、vRealize Automation vSphere エンドポイントで入力した vCenter Server インスタンスの名前と一致している必要があります。エンドポイントは、IP アドレスではなく完全修飾ドメイン名 (FQDN) で構成する必要があります。たとえば、エンドポイントのアドレスが <https://virtual-center27.domain/sdk> の場合、DDC サーバ上のホストの名前は、virtual-center27 と設定する必要があります。

vRealize Automation vSphere エンドポイントが IP アドレスで構成されている場合、FQDN を使用するように変更する必要があります。エンドポイントの設定の詳細については、[IaaS 構成](#)を参照してください。

XenDesktop エージェント ホストの要件

Citrix XenDesktop SDK がインストールされている必要があります。XenDesktop 用の SDK は XenDesktop インストール ディスクに含まれています。

ホストにエージェントをインストールする前に Microsoft PowerShell がホストにインストールされていることを確認します。必要なバージョンはホストのオペレーティング システムにより異なります。Microsoft のヘルプおよびサポートを参照してください。

MS PowerShell 実行ポリシーは RemoteSigned または Unrestricted に設定します。[「PowerShell 実行ポリシーの RemoteSigned への設定」](#)を参照してください。

PowerShell 実行ポリシーの詳細については、PowerShell のコマンド プロンプトで **help about_signing** または **help Set-ExecutionPolicy** を実行してください。

XenServer のホスト名の設定

XenDesktop では、XenDesktop サーバの XenServer ホストに付けられた名前は、XenCenter の Xen プールの UUID と一致する必要があります。Xen プールが構成されていない場合には、名前は XenServer 自体の UUID と一致する必要があります。

手順

- 1 Citrix XenCenter で、Xen プールまたはスタンドアロン XenServer を選択し、[全般] タブをクリックします。UUID を記録します。
- 2 XenServer プールまたはスタンドアロン ホストを XenDesktop に追加する場合には、前の手順で [接続] 名として記録した UUID を入力します。

XenDesktop エージェントのインストール

仮想デスクトップ統合 (VDI) PowerShell エージェントは、XenDesktop や Citrix などの外部の仮想デスクトップ システムと連携します。XenDesktop マシンを管理するには、VDI PowerShell エージェントを使用します。

前提条件

- Web サーバと Manager Service ホストを含め IaaS をインストールします。
- [「XenDesktop の要件」](#)の要件が満たされていることを確認します。
- [「vRealize Automation IaaS インストーラのダウンロード」](#)。

手順

- 1 セットアップ ファイル `setup__<vrealize-automation-appliance-FQDN>@5480.exe` を右クリックして、[管理者として実行] を選択します。
- 2 [次へ] をクリックします。
- 3 使用許諾契約に同意し、[次へ] をクリックします。
- 4 ログイン ページで vRealize Automation アプライアンスの管理者認証情報を入力し、SSL 証明書を確認します。
 - a ユーザー名 (**root**) とパスワードを入力します。

入力するパスワードは、vRealize Automation アプライアンスを展開したときに指定したパスワードです。
 - b [証明書の受け入れ] を選択します。
 - c [証明書の表示] をクリックします。

証明書のサムプリントを、vRealize Automation アプライアンスに設定されているサムプリントと比較します。管理コンソールにポート 5480 でアクセスしている場合は、クライアント ブラウザで vRealize Automation アプライアンス証明書を表示できます。
- 5 [次へ] をクリックします。
- 6 [インストール タイプ] ページで [カスタム インストール] を選択します。
- 7 [コンポーネントの選択] ペインの [プロキシ エージェント] を選択します。
- 8 ルートのインストール場所を受け入れるか、[変更] をクリックしてインストール パスを選択します。

分散型展開の場合でも、同じ Windows サーバに複数の IaaS コンポーネントをインストールする場合があります。

複数の IaaS コンポーネントをインストールする場合は、常に同じパスにインストールしてください。
- 9 [次へ] をクリックします。
- 10 インストール マシンの Windows サービスの管理者権限でログインします。

サービスは、同じインストール マシンで実行する必要があります。
- 11 [次へ] をクリックします。
- 12 [エージェント タイプ] リストから [VdiPowerShell] を選択します。

13 [エージェント名] テキスト ボックスに、このエージェントの識別子を入力します。

各エージェントのエージェント名、認証情報、エンドポイント名、およびプラットフォーム インスタンスの情報を記録しておきます。この情報は、エンドポイントを構成し、後ほどホストを追加するために必要です。

重要: 高可用性のために、冗長エージェントを追加して、同じ設定を構成できます。それ以外の場合は、固有のエージェントを構成します。

| オプション | 説明 |
|----------------|---|
| 冗長エージェント | 異なるサーバに冗長エージェントをインストールします。 冗長エージェントに同じ名前と設定を構成します。 |
| スタンドアロン エージェント | エージェントに一意の名前を割り当てます。 |

14 IaaS Manager Service ホストへの接続を構成します。

| オプション | 説明 |
|---------------|---|
| ロード バランサがある場合 | Manager Service コンポーネントのロード バランサの完全修飾ドメイン名とポート番号 (<mgr-svc-load-balancer.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |
| ロード バランサがない場合 | Manager Service コンポーネントをインストールしたマシンの完全修飾ドメイン名とポート番号 (<mgr-svc.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |

デフォルト ポートは 443 です。

15 IaaS Web サーバへの接続を構成します。

| オプション | 説明 |
|---------------|---|
| ロード バランサがある場合 | Web サーバ コンポーネントのロード バランサの完全修飾ドメイン名とポート番号 (<web-load-balancer.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |
| ロード バランサがない場合 | Web サーバ コンポーネントをインストールしたマシンの完全修飾ドメイン名とポート番号 (<web.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |

デフォルト ポートは 443 です。

16 [テスト] をクリックし、各ホストへの接続を確認します。

17 [VDI バージョン] を選択します。

18 [VDI サーバ] テキスト ボックスに、この管理対象サーバの完全修飾ドメイン名を入力します。

19 [追加] をクリックします。

20 [次へ] をクリックします。

21 [インストール] をクリックして、インストールを開始します。

数分後、正常に処理が行われたことを伝えるメッセージが表示されます。

22 [次へ] をクリックします。

23 [完了] をクリックします。

24 正常にインストールされたことを検証します。

25 (オプション) 同じシステムで、構成の異なる複数のエージェントと、1 つのエンドポイントを追加します。

次のステップ

高可用性を実現するため、エンドポイントの冗長エージェントをインストールおよび構成します。各冗長エージェントを別個のサーバにインストールしますが、エージェントの名前および構成は同一にします。

Citrix 用の EPI エージェントのインストール

外部プロビジョニング統合 (EPI) PowerShell エージェントは、Citrix 外部マシンをプロビジョニング プロセスに統合します。EPI エージェントでは、マシンが起動および実行する Citrix ディスク イメージのオンデマンドストリーミングが提供されます。

専用の EPI エージェントは、単一の外部プロビジョニング サーバと対話します。各 Citrix プロビジョニング サーバ インスタンスに対して 1 つの EPI エージェントをインストールする必要があります。

Citrix Provisioning Server の要件

システム管理者は、External Provisioning Infrastructure (EPI) エージェントを使用して Citrix プロビジョニング サーバを統合し、プロビジョニング プロセスで Visual Basic スクリプトを使用できるようにします。

インストールの場所および認証情報

Citrix プロビジョニング サービスのインスタンス用の PVS ホストにエージェントをインストールします。エージェントをインストールする前に、インストール ホストが「[Citrix エージェント ホストの要件](#)」を満たしていることを確認します。

通常、EPI エージェントは複数のサーバと通信できますが、Citrix Provisioning Server には専用の EPI エージェントが必要です。Citrix Provisioning Server のインスタンスごとに 1 つの EPI エージェントをインストールする必要があります。その際、ホストするサーバの名前を指定します。エージェントが実行する際の認証情報には、Citrix Provisioning Server のインスタンスへの管理アクセスが含まれている必要があります。

サポートされている Citrix PVS のバージョンについては、vRealize Automation のサポート マトリックスを調べてください。

Citrix エージェント ホストの要件

PowerShell および Citrix Provisioning Services SDK は、エージェントのインストールの前にインストール ホストにインストールされている必要があります。詳細については、VMware Web サイトで vRealize Automation のサポート マトリックスを調べてください。

ホストにエージェントをインストールする前に Microsoft PowerShell がホストにインストールされていることを確認します。必要なバージョンはホストのオペレーティング システムにより異なります。Microsoft のヘルプおよびサポートを参照してください。

PowerShell スナップインがインストールされていることも確認する必要があります。詳細については、Citrix Web サイトで『Citrix Provisioning Services PowerShell Programmer's Guide』を参照してください。

MS PowerShell 実行ポリシーは RemoteSigned または Unrestricted に設定します。[\[PowerShell 実行ポリシーの RemoteSigned への設定\]](#) を参照してください。

PowerShell 実行ポリシーの詳細については、PowerShell のコマンド プロンプトで **help about_signing** または **help Set-ExecutionPolicy** を実行してください。

Citrix エージェントのインストール

外部プロビジョニング統合 (EPI) PowerShell エージェントは、外部システムをマシン プロビジョニング プロセスに統合します。EPI PowerShell エージェントを使用して Citrix プロビジョニング サーバと統合し、オンデマンド ディスク ストリーミングによるマシンのプロビジョニングを有効にします。

前提条件

- Web サーバと Manager Service ホストを含め IaaS をインストールします。
- [\[Citrix Provisioning Server の要件\]](#) の要件が満たされていることを確認します。
- [\[vRealize Automation IaaS インストーラのダウンロード\]](#)。

手順

- 1 セットアップ ファイル **setup_<vrealize-automation-appliance-FQDN>@5480.exe** を右クリックして、[管理者として実行] を選択します。
- 2 [次へ] をクリックします。
- 3 使用許諾契約に同意し、[次へ] をクリックします。
- 4 ログイン ページで vRealize Automation アプライアンスの管理者認証情報を入力し、SSL 証明書を確認します。
 - a ユーザー名 (**root**) とパスワードを入力します。
 入力するパスワードは、vRealize Automation アプライアンスを展開したときに指定したパスワードです。
 - b [証明書の受け入れ] を選択します。
 - c [証明書の表示] をクリックします。
 証明書のサムプリントを、vRealize Automation アプライアンスに設定されているサムプリントと比較します。管理コンソールにポート 5480 でアクセスしている場合は、クライアント ブラウザで vRealize Automation アプライアンス証明書を表示できます。
- 5 [インストール タイプ] ページで [カスタム インストール] を選択します。
- 6 インストール タイプ ページで [Component Selection (コンポーネントの選択)] をクリックします。
- 7 ルートのインストール場所を受け入れるか、[変更] をクリックしてインストール パスを選択します。
 分散型展開の場合でも、同じ Windows サーバに複数の IaaS コンポーネントをインストールする場合があります。
 複数の IaaS コンポーネントをインストールする場合は、常に同じパスにインストールしてください。
- 8 [次へ] をクリックします。
- 9 インストール マシンの Windows サービスの管理者権限でログインします。
 サービスは、同じインストール マシンで実行する必要があります。

- 10 [次へ] をクリックします。
- 11 エージェント タイプ リストから [EPIPowerShell] を選択します。
- 12 [エージェント名] テキスト ボックスに、このエージェントの識別子を入力します。

各エージェントのエージェント名、認証情報、エンドポイント名、およびプラットフォーム インスタンスの情報を記録しておきます。この情報は、エンドポイントを構成し、後ほどホストを追加するために必要です。

重要: 高可用性のために、冗長エージェントを追加して、同じ設定を構成できます。それ以外の場合は、固有のエージェントを構成します。

| オプション | 説明 |
|----------------|---|
| 冗長エージェント | 異なるサーバに冗長エージェントをインストールします。 冗長エージェントに同じ名前と設定を構成します。 |
| スタンドアロン エージェント | エージェントに一意の名前を割り当てます。 |

- 13 IaaS Manager Service ホストへの接続を構成します。

| オプション | 説明 |
|---------------|---|
| ロード バランサがある場合 | Manager Service コンポーネントのロード バランサの完全修飾ドメイン名とポート番号 (<mgr-svc-load-balancer.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |
| ロード バランサがない場合 | Manager Service コンポーネントをインストールしたマシンの完全修飾ドメイン名とポート番号 (<mgr-svc.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |

デフォルト ポートは 443 です。

- 14 IaaS Web サーバへの接続を構成します。

| オプション | 説明 |
|---------------|---|
| ロード バランサがある場合 | Web サーバ コンポーネントのロード バランサの完全修飾ドメイン名とポート番号 (<web-load-balancer.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |
| ロード バランサがない場合 | Web サーバ コンポーネントをインストールしたマシンの完全修飾ドメイン名とポート番号 (<web.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |

デフォルト ポートは 443 です。

- 15 [テスト] をクリックし、各ホストへの接続を確認します。
- 16 EPI タイプを選択します。
- 17 [EPI サーバ] テキスト ボックスに、この管理対象サーバの完全修飾ドメイン名を入力します。
- 18 [追加] をクリックします。
- 19 [次へ] をクリックします。

20 [インストール] をクリックして、インストールを開始します。

数分後、正常に処理が行われたことを伝えるメッセージが表示されます。

21 [次へ] をクリックします。

22 [完了] をクリックします。

23 正常にインストールされたことを検証します。

24 (オプション) 同じシステムで、構成の異なる複数のエージェントと、1 つのエンドポイントを追加します。

次のステップ

高可用性を実現するため、エンドポイントの冗長エージェントをインストールおよび構成します。各冗長エージェントを別個のサーバにインストールしますが、エージェントの名前および構成は同一にします。

Visual Basic スクリプト処理用の EPI エージェントのインストール

システム管理者は、マシンのプロビジョニングの前または後、あるいはマシンのプロビジョニング解除時に、プロビジョニング プロセスの追加手順として Visual Basic スクリプトを指定できます。Visual Basic スクリプトを実行する前に、外部プロビジョニング統合 (EPI) PowerShell をインストールする必要があります。

Visual Basic スクリプトは、マシンのプロビジョニング元となるブループリントで指定されます。このようなスクリプトは、マシンに関連付けられたすべてのカスタム プロパティへアクセスし、その値をアップデートできます。ワークフローの次の手順では、これらの新しい値へアクセスできます。

たとえば、プロビジョニングの前にスクリプトを使用して証明書またはセキュリティ トークンを生成し、それらをマシン プロビジョニングで使用することもできます。

プロビジョニングでスクリプトを有効にするには、特定のタイプの EPI エージェントをインストールし、エージェントがインストールされるシステムに、使用するスクリプトを配置します。

スクリプトの実行時、EPI エージェントは引数としてすべてのマシンのカスタム プロパティをスクリプトに渡します。アップデートされたプロパティ値を返すには、これらのプロパティをディクショナリに配置し、vRealize Automation 関数を呼び出す必要があります。サンプルのスクリプトは、EPI エージェントのインストール ディレクトリのスクリプト サブディレクトリ内にあります。このスクリプトには、ディクショナリにすべての引数をロードするためのヘッダー、関数を含めることができる本文、およびアップデートされたカスタム プロパティ値を返すフッターが含まれます。

注: 複数のサーバに複数の EPI/VB スクリプト エージェントをインストールし、そのエージェントのホスト上で特定のエージェントおよび Visual Basic スクリプトを使用してプロビジョニングできます。これを行う必要がある場合には、VMware カスタム サポートにお問い合わせください。

Visual Basic スクリプト処理の要件

システム管理者は External Provisioning Infrastructure (EPI) エージェントをインストールし、プロビジョニング プロセスで Visual Basic スクリプトを使用できるようにします。

次の表に、EPI エージェントをインストールしてプロビジョニング プロセスで Visual Basic のスクリプトを使用できるようにする際に適用される要件を示します。

表 1-39. Visual スクリプト処理用の EPI エージェント

| 要件 | 説明 |
|----------------------|--|
| 認証情報 | エージェントが実行する際の認証情報には、インストール ホストへの管理アクセスが含まれている必要があります。 |
| Microsoft PowerShell | Microsoft PowerShell はエージェントのインストール前にインストール ホストにインストールされている必要があります。必要なバージョンは、インストール ホストのオペレーティング システムにより異なり、オペレーティング システムにインストールされている可能性があります。詳細については http://support.microsoft.com を参照してください。 |
| MS PowerShell 実行ポリシー | <p>MS PowerShell 実行ポリシーは、[RemoteSigned] または [Unrestricted] に設定される必要があります。</p> <p>PowerShell 実行ポリシーの詳細については、Power-Shell コマンド プロンプトで次のコマンドのいずれかを発行します。</p> <pre>help about_signing help Set-ExecutionPolicy</pre> |

Visual Basic スクリプト処理用のエージェントのインストール

外部プロビジョニング統合 (EPI) PowerShell エージェントでは、外部システムをマシン プロビジョニング プロセスに統合できます。EPI エージェントを使用して Visual Basic スクリプトをプロビジョニング プロセス中の追加の手順として実行します。

前提条件

- Web サーバと Manager Service ホストを含め IaaS をインストールします。
- [「Visual Basic スクリプト処理の要件」](#) の要件が満たされていることを確認します。
- [「vRealize Automation IaaS インストーラのダウンロード」](#)。

手順

- 1 セットアップ ファイル `setup__<vrealize-automation-appliance-FQDN>@5480.exe` を右クリックして、[管理者として実行] を選択します。
- 2 [次へ] をクリックします。
- 3 使用許諾契約に同意し、[次へ] をクリックします。
- 4 ログイン ページで vRealize Automation アプライアンスの管理者認証情報を入力し、SSL 証明書を確認します。
 - a ユーザー名 (**root**) とパスワードを入力します。

入力するパスワードは、vRealize Automation アプライアンスを展開したときに指定したパスワードです。

- b [証明書の受け入れ] を選択します。
- c [証明書の表示] をクリックします。

証明書のサムプリントを、vRealize Automation アプライアンスに設定されているサムプリントと比較します。管理コンソールにポート 5480 でアクセスしている場合は、クライアント ブラウザで vRealize Automation アプライアンス証明書を表示できます。

- 5 [インストール タイプ] ページで [カスタム インストール] を選択します。
- 6 インストール タイプ ページで [Component Selection (コンポーネントの選択)] をクリックします。
- 7 ルートのインストール場所を受け入れるか、[変更] をクリックしてインストール パスを選択します。
分散型展開の場合でも、同じ Windows サーバに複数の IaaS コンポーネントをインストールする場合があります。
複数の IaaS コンポーネントをインストールする場合は、常に同じパスにインストールしてください。
- 8 [次へ] をクリックします。
- 9 インストール マシンの Windows サービスの管理者権限でログインします。
サービスは、同じインストール マシンで実行する必要があります。
- 10 [次へ] をクリックします。
- 11 エージェント タイプリストから [EIPowerShell] を選択します。
- 12 [エージェント名] テキスト ボックスに、このエージェントの識別子を入力します。

各エージェントのエージェント名、認証情報、エンドポイント名、およびプラットフォーム インスタンスの情報を記録しておきます。この情報は、エンドポイントを構成し、後ほどホストを追加するために必要です。

重要: 高可用性のために、冗長エージェントを追加して、同じ設定を構成できます。それ以外の場合は、固有のエージェントを構成します。

| オプション | 説明 |
|----------------|---|
| 冗長エージェント | 異なるサーバに冗長エージェントをインストールします。 冗長エージェントに同じ名前と設定を構成します。 |
| スタンドアロン エージェント | エージェントに一意の名前を割り当てます。 |

- 13 IaaS Manager Service ホストへの接続を構成します。

| オプション | 説明 |
|---------------|---|
| ロード バランサがある場合 | Manager Service コンポーネントのロード バランサの完全修飾ドメイン名とポート番号 (<mgr-svc-load-balancer.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |
| ロード バランサがない場合 | Manager Service コンポーネントをインストールしたマシンの完全修飾ドメイン名とポート番号 (<mgr-svc.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |

デフォルト ポートは 443 です。

14 IaaS Web サーバへの接続を構成します。

| オプション | 説明 |
|---------------|---|
| ロード バランサがある場合 | Web サーバ コンポーネントのロード バランサの完全修飾ドメイン名とポート番号 (<web-load-balancer.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |
| ロード バランサがない場合 | Web サーバ コンポーネントをインストールしたマシンの完全修飾ドメイン名とポート番号 (<web.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |

デフォルト ポートは 443 です。

15 [テスト] をクリックし、各ホストへの接続を確認します。

16 EPI タイプを選択します。

17 [EPI サーバ] テキスト ボックスに、この管理対象サーバの完全修飾ドメイン名を入力します。

18 [追加] をクリックします。

19 [次へ] をクリックします。

20 [インストール] をクリックして、インストールを開始します。

数分後、正常に処理が行われたことを伝えるメッセージが表示されます。

21 [次へ] をクリックします。

22 [完了] をクリックします。

23 正常にインストールされたことを検証します。

24 (オプション) 同じシステムで、構成の異なる複数のエージェントと、1 つのエンドポイントを追加します。

リモート WMI 申請用の WMI エージェントのインストール

システム管理者は、Windows Management Instrumentation (WMI) プロトコルを有効にし、すべての管理対象 Windows マシンに WMI エージェントをインストールして、データおよび操作の管理を有効にします。このエージェントは、マシンの所有者の Active Directory のステータスなどの Windows マシンからのデータの収集に必要になります。

Windows マシンでのリモート WMI 申請の有効化

WMI エージェントを使用するには、管理された Windows サーバでリモート WMI 申請が有効にされている必要があります。

手順

- 1 プロビジョニング済みの管理された Windows 仮想マシンを含む各ドメイン内に Active Directory グループを作成し、プロビジョニング済みのマシン上でリモート WMI 申請を実行する WMI エージェントのサービス認証情報をこのグループに追加します。
- 2 プロビジョニング済みの各 Windows マシン上での、エージェント認証情報を含む Active Directory グループに対するリモート WMI 申請を有効にします。

WMI エージェントのインストール

Windows Management Instrumentation (WMI) エージェントでは、Windows が管理するマシンからのデータ収集が可能です。

前提条件

- Web サーバと Manager Service ホストを含め IaaS をインストールします。
- [「Windows マシンでのリモート WMI 申請の有効化」](#) の要件が満たされていることを確認します。
- [「vRealize Automation IaaS インストーラのダウンロード」](#)。

手順

- 1 セットアップ ファイル `setup__<vrealize-automation-appliance-FQDN>@5480.exe` を右クリックして、[管理者として実行] を選択します。
- 2 [次へ] をクリックします。
- 3 使用許諾契約に同意し、[次へ] をクリックします。
- 4 ログイン ページで vRealize Automation アプライアンスの管理者認証情報を入力し、SSL 証明書を確認します。
 - a ユーザー名 (**root**) とパスワードを入力します。

入力するパスワードは、vRealize Automation アプライアンスを展開したときに指定したパスワードです。
 - b [証明書の受け入れ] を選択します。
 - c [証明書の表示] をクリックします。

証明書のサムプリントを、vRealize Automation アプライアンスに設定されているサムプリントと比較します。管理コンソールにポート 5480 でアクセスしている場合は、クライアント ブラウザで vRealize Automation アプライアンス証明書を表示できます。
- 5 [インストール タイプ] ページで [カスタム インストール] を選択します。
- 6 インストール タイプ ページで [Component Selection (コンポーネントの選択)] をクリックします。
- 7 ルートのインストール場所を受け入れるか、[変更] をクリックしてインストール パスを選択します。

分散型展開の場合でも、同じ Windows サーバに複数の IaaS コンポーネントをインストールする場合があります。複数の IaaS コンポーネントをインストールする場合は、常に同じパスにインストールしてください。
- 8 [次へ] をクリックします。
- 9 インストール マシンの Windows サービスの管理者権限でログインします。

サービスは、同じインストール マシンで実行する必要があります。
- 10 [次へ] をクリックします。
- 11 [エージェント タイプ] リストから [WMI] を選択します。

12 [エージェント名] テキスト ボックスに、このエージェントの識別子を入力します。

各エージェントのエージェント名、認証情報、エンドポイント名、およびプラットフォーム インスタンスの情報を記録しておきます。この情報は、エンドポイントを構成し、後ほどホストを追加するために必要です。

重要: 高可用性のために、冗長エージェントを追加して、同じ設定を構成できます。それ以外の場合は、固有のエージェントを構成します。

| オプション | 説明 |
|----------------|---|
| 冗長エージェント | 異なるサーバに冗長エージェントをインストールします。 冗長エージェントに同じ名前と設定を構成します。 |
| スタンドアロン エージェント | エージェントに一意の名前を割り当てます。 |

13 IaaS Manager Service ホストへの接続を構成します。

| オプション | 説明 |
|---------------|---|
| ロード バランサがある場合 | Manager Service コンポーネントのロード バランサの完全修飾ドメイン名とポート番号 (<mgr-svc-load-balancer.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |
| ロード バランサがない場合 | Manager Service コンポーネントをインストールしたマシンの完全修飾ドメイン名とポート番号 (<mgr-svc.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |

デフォルト ポートは 443 です。

14 IaaS Web サーバへの接続を構成します。

| オプション | 説明 |
|---------------|---|
| ロード バランサがある場合 | Web サーバ コンポーネントのロード バランサの完全修飾ドメイン名とポート番号 (<web-load-balancer.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |
| ロード バランサがない場合 | Web サーバ コンポーネントをインストールしたマシンの完全修飾ドメイン名とポート番号 (<web.mycompany.com>:443) を入力します。 IP アドレスは入力しないでください。 |

デフォルト ポートは 443 です。

15 [テスト] をクリックし、各ホストへの接続を確認します。

16 [追加] をクリックします。

17 [次へ] をクリックします。

18 [インストール] をクリックして、インストールを開始します。

数分後、正常に処理が行われたことを伝えるメッセージが表示されます。

19 [次へ] をクリックします。

20 [完了] をクリックします。

21 正常にインストールされたことを検証します。

22 (オプション) 同じシステムで、構成の異なる複数のエージェントと、1 つのエンドポイントを追加します。

vRealize Automation のサイレント インストール

vRealize Automation には、コマンドラインからスクリプトを使用したサイレント インストールと API ベースのサイレント インストールのオプションが含まれています。どちらの方法でも、従来型のインストールで通常手動で入力する値を事前に準備しておく必要があります。

vRealize Automation のサイレント インストールについて

vRealize Automation のサイレント インストールでは、テキストベースの応答ファイルを参照する実行ファイルを使用します。

この応答ファイルには、システムの FQDN やアカウントの認証情報など、通常であれば、従来のウィザードベースのインストールや手動インストールで追加する設定を事前に構成します。サイレント インストールは、次のタイプの展開で便利です。

- 複数のほぼ同一の環境を展開する
- 同じ環境を繰り返し再展開する
- 無人インストールを実行する
- スクリプト インストールを実行する

vRealize Automation のサイレント インストールの実行

新しく展開された vRealize Automation アプライアンスのコンソールから vRealize Automation を無人でサイレント インストールすることができます。

前提条件

- 未構成のアプライアンスを作成します。[「vRealize Automation アプライアンスの展開」](#)を参照してください。
- IaaS Windows サーバを作成または識別し、その前提条件を構成します。
- IaaS Windows サーバに管理エージェントをインストールします。

管理エージェントをインストールするには、従来の **.msi** ファイルをダウンロードして使用方法と、[「vRealize Automation 管理エージェントのサイレント インストールの実行」](#)で説明されているサイレント プロセスを使用する方法があります。

手順

- 1 vRealize Automation アプライアンス コンソールに root ユーザーとしてログインします。
- 2 次のディレクトリに移動します。
`/usr/lib/vcac/tools/install`
- 3 テキスト エディタで応答ファイル **ha.properties** を開きます。

- 展開に固有のエントリを **ha.properties** に追加し、このファイルを保存して閉じます。

デフォルト ファイル全体を編集せずに、別の展開の **ha.properties** ファイルをコピーして変更すれば、時間を節約することができます。

- 同じディレクトリから次のコマンドを実行し、インストールを開始します。

```
vra-ha-config.sh
```

展開する環境やサイズによっては、インストールの完了に最大で 1 時間かそれ以上かかる場合があります。

- (オプション) インストールが完了したら、ログ ファイルを確認します。

```
/var/log/vcac/vra-ha-config.log
```

サイレント インストーラでは、パスワード、ライセンス、証明書などの独自のデータはログに保存されません。

vRealize Automation 管理エージェントのサイレント インストールの実行

コマンド ラインを使用して、vRealize Automation 管理エージェントを任意の IaaS Windows サーバにインストールできます。

管理エージェントのサイレント インストールは、いくつかの設定をカスタマイズした Windows PowerShell スクリプトから構成されます。すべての IaaS Windows サーバに管理エージェントをサイレント インストールするには、導入環境に固有の設定をスクリプトに追加した後、そのスクリプトのコピーを各サーバで実行します。

前提条件

- 未構成のアプライアンスを作成します。[\[vRealize Automation アプライアンスの展開\]](#) を参照してください。
- IaaS Windows サーバを作成または識別し、その前提条件を構成します。

手順

- 1 管理者権限を備えたアカウントを使用して IaaS Windows サーバにログインします。
- 2 Web ブラウザを開き、vRealize Automation アプライアンス インストーラ URL にアクセスします。
`https://<vrealize-automation-appliance-FQDN>:5480/installer`
- 3 **InstallManagementAgent.ps1** PowerShell スクリプト ファイルのリンクを右クリックして、IaaS Windows サーバのデスクトップまたはフォルダに保存します。
- 4 テキスト エディタで **InstallManagementAgent.ps1** を開きます。
- 5 スクリプト ファイルの先頭付近に、導入環境に固有の設定を追加します。
 - vRealize Automation アプライアンス URL
`https://<vrealize-automation-appliance-FQDN>:5480`
 - vRealize Automation アプライアンスの root ユーザー アカウントの認証情報
 - vRealize Automation サービスのユーザー認証情報 (IaaS Windows サーバに対する管理者権限を備えたドメイン アカウント)
 - 管理エージェントをインストールするフォルダ (デフォルトでは、**Program Files (x86)**)

- (オプション) 認証に使用する PEM 形式の証明書のサムプリント

6 **InstallManagementAgent.ps1** を保存して閉じます。

7 管理エージェントをサイレント インストールするために、**InstallManagementAgent.ps1** をダブルクリックします。

8 (オプション) インストールが完了したことを確認するには、Windows の [プログラムと機能] の [コントロールパネル] リストと、稼働中の Windows サービスのリストで [VMware vCloud Automation Center 管理エージェント] を探します。

vRealize Automation サイレント インストール用の応答ファイル

vRealize Automation をサイレント インストールするには、テキストベースの応答ファイルを事前に用意しておく必要があります。

新しく展開されたすべての vRealize Automation アプライアンスには、デフォルトの応答ファイルが含まれています。

/usr/lib/vcac/tools/install/ha.properties

サイレント インストールを実行するには、テキスト エディタで、インストールする導入環境に合わせて **ha.properties** の設定をカスタマイズする必要があります。追加する必要のある設定と情報の例を次に示します。

- vRealize Automation または Suite のライセンス キー
- vRealize Automation アプライアンス ノードの完全修飾ドメイン名
- vRealize Automation アプライアンスの root ユーザー アカウントの認証情報
- Web ノードや Manager Service ノードなどとして機能する IaaS Windows サーバの完全修飾ドメイン名
- vRealize Automation サービスのユーザー認証情報 (IaaS Windows サーバに対する管理者権限を備えたドメイン アカウント)
- ロード バランサの完全修飾ドメイン名
- SQL Server データベースのパラメータ
- 仮想化リソースに接続するためのプロキシ エージェントのパラメータ
- IaaS Windows サーバの前提条件が欠落している場合にサイレント インストーラがその修正を試みるかどうか
サイレント インストーラは、欠落している多くの Windows 前提条件を修正できます。ただし、構成の問題によっては、サイレント インストーラが変更できないものもあります (CPU が不十分であるなど)。

別の展開用に構成された、設定が似ている **ha.properties** ファイルを再利用して変更すれば、時間を節約できます。また、サイレント インストールではなく、インストール ウィザードを使用して vRealize Automation をインストールしたときは、ウィザードによって設定が作成され、**ha.properties** ファイルに保存されます。このファイルは、類似した導入環境をサイレント インストールする場合、再利用して変更できるので便利です。

ウィザードでは、パスワードやライセンス、証明書などの独自の設定は **ha.properties** ファイルに保存されません。

vRealize Automation インストール コマンド ライン

vRealize Automation には、初期インストール後に必要になることがあるインストール調整を実行するための、コンソール ベースのコマンド ライン インターフェイスが含まれています。

コマンド ライン インターフェイス (CLI) では、初期インストール後にブラウザベースのインターフェイスでは実行できなくなったインストールおよび構成タスクを実行できます。CLI の機能として、前提条件の再チェック、IaaS コンポーネントのインストール、ユーザーが Web ブラウザで参照する vRealize Automation ホスト名の設定が挙げられます。

CLI は、特定の操作のスクリプトを作成する上級ユーザーにとっても有用です。一部の CLI 機能はサイレント インストールで使用されており、両方の機能に習熟することで vRealize Automation インストールのスクリプト作成に関する理解が深まります。

vRealize Automation インストール コマンドラインの基礎

vRealize Automation インストール コマンドライン インターフェイスには、上位の、基本操作コマンドが含まれます。

基本操作では、vRealize Automation ノード ID の表示、コマンドの実行、コマンド ステータスのレポート、またはヘルプ情報の表示を行います。これらの操作とオプションをコンソール ディスプレイに表示するには、オプションや修飾子を指定せずに以下のコマンドを入力します。

vra-command

ノード ID の表示

適切なターゲット システムに対してコマンドを実行できるように、vRealize Automation ノード ID が必要です。ノード ID を表示するには、次のコマンドを入力します。

vra-command list-nodes

特定のマシンに対してコマンドを実行する前に、ノード ID をメモします。

コマンドの実行

ほとんどのコマンド ライン機能では、vRealize Automation クラスタ内のノードに対するコマンドの実行が必要です。コマンドを実行するには、次の構文を使用します。

```
vra-command execute --node <node-ID> <command-name> --<parameter-name>
<parameter-value>
```

先ほどの構文にあるように、多くのコマンドには、パラメータとユーザーが選択するパラメータ値が必要です。

コマンド ステータスの表示

一部のコマンドでは表示に時間がかかる場合があります。入力したコマンドの進行状況を監視するには、以下のコマンドを入力します。

vra-command status

ステータス コマンドは、展開規模が大きいと実行に時間がかかるサイレント インストールを監視する場合に特に便利です。

ヘルプの表示

使用可能なすべてのコマンドについてのヘルプを表示するには、次のコマンドを入力します。

```
vra-command help
```

1 つのコマンドについてのヘルプ情報を表示するには、次のコマンドを入力します。

```
vra-command help <command-name>
```

vRealize Automation インストール コマンド名

コマンドにより、初期インストール後に実行が必要になることがある多くの vRealize Automation インストールおよび構成タスクにコンソールからアクセスできます。

使用可能なコマンドの例として、以下の機能があります。

- 既存の環境に対する別の vRealize Automation アプライアンスの追加
- vRealize Automation にアクセスする際にユーザーが Web ブラウザで参照するホスト名の設定
- IaaS SQL Server データベースの作成
- IaaS Windows サーバに対する前提条件チェッカーの実行
- 証明書のインポート

使用可能な vRealize Automation コマンドの完全なリストを参照するには、vRealize Automation アプライアンスコンソールにログインし、次のコマンドを入力します。

```
vra-command help
```

コマンド名とパラメータの一覧は、別のドキュメントでは再現されていません。このリストを効果的に使用するには、関連するコマンドを特定し、次のコマンドを入力して対象範囲を絞り込みます。

```
vra-command help <command-name>
```

vRealize Automation のインストール API

インストール用の vRealize Automation REST API を使用すると、完全にソフトウェアで制御する vRealize Automation のインストール プログラムを作成できます。

インストール API には、CLI ベースのインストールが **ha.properties** 応答ファイルから取得するものと同じエントリの JSON 形式のバージョンが必要です。次のガイドラインで API のしくみを理解しておきます。これにより、プログラムによる API の呼び出しを設計して vRealize Automation をインストールできます。

- API のドキュメントにアクセスするには、Web ブラウザで次の vRealize Automation アプライアンス ページを参照します。

```
https://<vrealize-automation-appliance-FQDN>:5480/config
```

未構成の vRealize Automation アプライアンスが必要です。[\[vRealize Automation アプライアンスの展開\]](#) を参照してください。

- API ベースのインストールを試すには、次の PUT コマンドを見つけて展開します。

```
PUT /vra-install
```

- 未入力の JSON を [install_json] ボックスからテキスト エディタにコピーします。**ha.properties** に記入するのと同じ方法で応答値を記入します。JSON 形式の応答の準備が整ったら、コードを [install_json] にコピーして戻し、JSON を上書きします。

または、次のテンプレート JSON を編集して、結果を [install_json] にコピーすることもできます。

```
/usr/lib/vcac/tools/install/installationProperties.json
```

また、編集が完了した **ha.properties** は JSON に変換できます。その逆も可能です。

- アクション ボックスで [検証] を選択し、[試す] をクリックします。
検証アクションでは vRealize Automation の前提条件チェッカーと修正が実行されます。

- 検証応答には英数字のコマンド ID が含まれており、次の GET コマンドに挿入できます。

```
GET /commands/<command-id>/aggregated-status
```

GET への応答には検証処理の進行状況が含まれています。

- 検証が成功すると、プロセスを繰り返すことによって実際のインストールを実行できます。ただし、アクションボックスでは、[検証] の代わりに [インストール] を選択します。

展開規模によってはインストールに長時間かかる場合があります。もう一度、コマンド ID を見つけて、集計されたステータスの GET コマンドを使用し、インストールの進行状況を取得します。GET の応答は次の例のようになります。

```
"progress": "78%", "counts": {"failed": 0, "completed": 14, "total": 18, "queued": 3, "processing": 1}, "failed-commands": 0
```

- インストールで問題が発生した場合は、次のコマンドを使用して、すべてのノードのログ収集をトリガできます。

```
PUT /commands/log-bundle
```

インストールと同様に、返された英数字のコマンド ID を使用して、ログ収集ステータスを監視できます。

vRealize Automation サイレント プロパティと JSON の間の変換

vRealize Automation のサイレント CLI または API ベースのインストールの場合、完了したプロパティ応答ファイルを JSON に変換できます。その逆も可能です。サイレント CLI インストールにはプロパティ ファイルが必要で、API には JSON 形式が必要です。

前提条件

完了したプロパティ応答ファイルまたは完了した JSON ファイル

```
/usr/lib/vcac/tools/install/ha.properties
```

または

```
/usr/lib/vcac/tools/install/installationProperties.json
```

手順

- 1 vRealize Automation アプライアンス コンソール セッションに root ユーザーとしてログインします。

2 適切なコンバータ スクリプトを実行します。

- JSON からプロパティへの変換

```
/usr/lib/vcac/tools/install/convert-properties --from-json
installationProperties.json
```

スクリプトによって新しいプロパティ ファイルが作成されます。ファイル名には次のようにタイムスタンプが含まれています。

```
ha.2016-10-17_13.02.15.properties
```

- プロパティから JSON への変換

```
/usr/lib/vcac/tools/install/convert-properties --to-json ha.properties
```

スクリプトによって新しい **installationProperties.json** ファイルが作成されます。ファイル名には次のようにタイムスタンプが含まれています。

```
installationProperties.2016-10-17_13.36.13.json
```

スクリプトのヘルプを表示することもできます。

```
/usr/lib/vcac/tools/install/convert-properties --help
```

vRealize Automation インストール後のタスク

vRealize Automation をインストールした後、インストール後のタスクを実行しますが、作業には注意が必要です。

連邦情報処理規格準拠の暗号化の設定

受信および送信 vRealize Automation アプライアンス ネットワーク トラフィックに、連邦情報処理規格 (FIPS) 140-2 準拠の暗号化を有効または無効にできます。

FIPS 設定を変更するには vRealize Automation を再起動する必要があります。FIPS はデフォルトでは無効になっています。

手順

- 1 vRealize Automation アプライアンスの管理インターフェイスに root としてログインします。

```
https://<vrealize-automation-appliance-FQDN>:5480
```

- 2 [vRA 設定] - [ホストの設定] をクリックします。

- 3 右上のボタンをクリックして FIPS を有効または無効にします。

有効にすると、ポート 443 の受信および送信 vRealize Automation アプライアンス ネットワーク トラフィックには FIPS 140-2 準拠の暗号化が使用されます。FIPS の設定に関係なく、vRealize Automation では vRealize Automation アプライアンスに保存されたデータには AES-256 準拠のアルゴリズムが使用され、セキュアに保護されます。

注: 一部の内部コンポーネントでは認定済みの暗号化モジュールがまだ使用されていないため、この vRealize Automation リリースの一部のみで FIPS 準拠が有効になっています。認定済みモジュールが実装されていない場合は、AES-256 準拠アルゴリズムが使用されます。

- 4 [はい] をクリックして vRealize Automation を再起動します。

root ユーザーの vRealize Automation アプライアンス コンソール セッションから以下のコマンドを使用して FIPS を設定することもできます。

```
vcac-vami fips enable
vcac-vami fips disable
vcac-vami fips status
```

Manager Service の自動フェイルオーバーの有効化

標準の vRealize Automation Windows インストーラで Manager Service をインストールまたはアップグレードすると、Manager Service の自動フェイルオーバーはデフォルトで無効になります。

標準の Windows インストーラの実行後に Manager Service の自動フェイルオーバーを有効にするには、次の手順を実行します。

手順

- 1 vRealize Automation アプライアンスのコンソール セッションに root としてログインします。
- 2 次のディレクトリに移動します。

```
/usr/lib/vcac/tools/vami/commands
```

- 3 次のコマンドを入力します。

```
python ./manager-service-automatic-failover ENABLE
```

laaS 展開全体で自動フェイルオーバーを無効にする必要がある場合は、代わりに次のコマンドを入力します。

```
python ./manager-service-automatic-failover DISABLE
```

Manager Service の自動フェイルオーバーについて

vRealize Automation laaS Manager Service は、プライマリの Manager Service が停止した場合、バックアップへのフェイルオーバーを実行するように設定できます。

vRealize Automation 7.3 以降では、サーバをプライマリまたはバックアップに設定する際、Windows サーバごとに手動で Manager Service を開始または停止する必要がなくなりました。Manager Service の自動フェイルオーバーは、次の場合デフォルトで有効になります。

- サイレントインストールまたはインストール ウィザードを使用して vRealize Automation をインストールする。
- 管理インターフェイスまたは自動アップグレード スクリプトを使用して IaaS をアップグレードする。

標準の Windows ベースのインストーラを使用して Manager Service ホストを追加する場合、または IaaS をアップグレードする場合、フェイルオーバーは有効になっていません。有効にする方法については、[「Manager Service の自動フェイルオーバーの有効化」](#)を参照してください。

自動フェイルオーバーを有効にすると、バックアップを含むすべての Manager Service ホストで自動的に Manager Service が開始されます。自動フェイルオーバー機能を使用すると、ホストは透過的に互いを監視し、必要に応じてフェイルオーバーできます。この機能を使用するには、すべてのホストで Windows サービスが実行されている必要があります。

注: 自動フェイルオーバーの使用は必須ではありません。自動フェイルオーバーを無効にして、引き続き手動で Windows サービスを開始および停止し、プライマリまたはバックアップ ホストの設定を制御することもできます。手動でフェイルオーバーを行う際は、一度に 1 台ずつホストのサービスを開始してください。自動フェイルオーバーが無効の場合、同時に複数の IaaS サーバでサービスを実行すると、vRealize Automation を使用できなくなります。

自動フェイルオーバーをホストごとに有効または無効に設定しないでください。IaaS 環境では、自動フェイルオーバーを有効または無効にする設定は、すべての Manager Service ホストで同一にする必要があります。

自動フェイルオーバーが機能しない場合、トラブルシューティングのヒントについては、[「Manager Service の自動フェイルオーバーが有効にならない」](#)を参照してください。

vRealize Automation PostgreSQL データベースの自動フェイルオーバー

vRealize Automation の高可用性環境の場合、一部の構成では、組み込みの vRealize Automation PostgreSQL データベースの自動フェイルオーバーが可能です。

自動フェイルオーバーは、次の条件下で自動的に有効になります。

- 高可用性環境に 3 台の vRealize Automation アプライアンスが含まれている。
2 台のアプライアンスでは自動フェイルオーバーはサポートされていません。
- vRealize Automation 管理インターフェイスの [vRA 設定] > [データベース] で、データベースのレプリケーションが同期モードに設定されている。

通常は、自動フェイルオーバーが有効なときは手動フェイルオーバーを実行しないでください。ただし、ノードにある種の問題がある場合には、自動フェイルオーバーが有効であっても機能しないことがあります。そのような場合は、手動フェイルオーバーを実行する必要があるかどうかを確認します。

- 1 プライマリの PostgreSQL データベース ノードが停止したあと、クラスタ内の他のノードが安定するまで最大で 5 分待ちます。
- 2 正常に動作している vRealize Automation アプライアンス ノードのブラウザで、次の URL を開きます。

`https://<vrealize-automation-appliance-FQDN>:5434/api/status`

3 `manualFailoverNeeded` を検索します。

4 `manualFailoverNeeded` が `true` の場合は、手動フェイルオーバーを実行します。

詳細については、[vRealize Automation アプライアンス データベースのフェイルオーバーを実行する](#)を参照してください。

認証局から提供された証明書での自己署名証明書の置き換え

自己署名証明書を使用して vRealize Automation をインストールした場合は、本番環境への展開前に、その証明書を認証局から提供された証明書で置き換えることができます。

証明書の更新に関する詳細については、[vRealize Automation 証明書の更新](#)を参照してください。

ホスト名と IP アドレスの変更

一般に、vRealize Automation システム用に計画したホスト名、FQDN、および IP アドレスは維持します。インストール後の変更は可能ですが、複雑になることがあります。

- IaaS SQL Server データベースをホストする Windows マシンのホスト名を変更する場合は、[新しいホスト名の SQL データベースの構成](#)を参照してください。
- IaaS コンポーネントをリストアするときに、ホスト名を変更すると IaaS Web ホスト、Manager Service ホスト、またはそれぞれのロード バランサ ホストに影響する可能性があります。vRealize Suite のバックアップとリストアの指示どおりに、これらのホストまたはロード バランサをリストアします。

vRealize Automation アプライアンスのホスト名または IP アドレスを変更するには、次のセクションを参照してください。

vRealize Automation アプライアンス ホスト名の変更

環境またはネットワークを維持するために、別のホスト名を vRealize Automation アプライアンスに割り当てる必要が生じる場合があります。

重要: 名前を変更すると、vRealize Automation は数分間オフライン状態になります。

スタンドアローン、マスター、レプリカの vRealize Automation アプライアンスには、同じ手順が適用されます。

手順

- 1 DNS に新しいノードのホスト名を指定したレコードを追加します。
古いホスト名の既存の DNS レコードはまだ削除しないでください。
- 2 DNS のレプリケーションとゾーン分散が実行されるまで待機します。
- 3 vRealize Automation アプライアンスのコマンド ラインに `root` としてログインします。
- 4 次のコマンドを実行します。

```
vcac-config hostname-change --host <new-hostname> --certificate
<certificate-file-name>
```

証明書ファイルはオプションです。ただし、証明書で古いアプライアンスのホスト名が使用されている場合を除きます。その場合には、新しいホスト名を持つ更新された証明書を指定します。

証明書ファイルを指定すると、名前の変更コマンドで、証明書がインポートされ、証明書 ID が返されます。

証明書ファイルは、`/config/ssl/generate-certificate` API コマンドのテキスト出力と同じフォーマットで、その SAN フィールドに新しい DNS 名が含まれます。

- 5 名前の変更プロセスが完了するまで、最大 15 分間待機します。コマンドのアクションに数分かかるほか、サービスの再登録にさらに数分間を要します。
- 6 古いアプライアンス ホスト名が HA 環境のロード バランサで使用されていた場合は、確認後、ロード バランサを新しい名前で再構成します。
- 7 DNS で、古いホスト名を使用している既存の DNS レコードを削除します。

ホスト名を変更すると問題が発生する場合は、vRealize Automation 7.3 のドキュメントに掲載されている別の手順を試してください。

vRealize Automation アプライアンスの IP アドレスの変更

環境またはネットワークを維持するために、既存の vRealize Automation アプライアンスに別の IP アドレスを割り当てる必要が生じる場合があります。

前提条件

- 予防措置として、vRealize Automation アプライアンスと IaaS サーバのスナップショットを作成します。
- vRealize Automation アプライアンスの root としてのコンソール セッションで、`/etc/hosts` ファイルのエントリを検査します。

新しい IP アドレス プランと競合する可能性のあるアドレス割り当てを検索し、必要に応じて変更を加えます。

すべての IaaS サーバで、`Windows\system32\drivers\etc\hosts` ファイルについてこの操作を繰り返します。

- すべての vRealize Automation アプライアンスをシャットダウンします。
- IaaS サーバ上のすべての vRealize Automation サービスを停止します。

手順

- 1 vSphere で、変更する vRealize Automation アプライアンスを見つけ、[アクション] - [設定の編集] の順に選択します。
- 2 [vApp オプション] をクリックします。
- 3 [IP の割り当て] を展開し、[OVF 環境] オプションを有効にします。

- 4 [OVF 設定] を展開し、[ISO イメージ] オプションを有効にします。

図 1-16. OVF 環境と ISO イメージのオプション

| Virtual Hardware | VM Options | SDRS Rules | vApp Options |
|---|------------|------------|--------------|
| <div>▼ IP allocation</div> <div>IP allocation scheme</div> <p>A vApp can obtain its network configuration through the OVF environment or a DHCP server. Specify the network configuration schemes supported by this vApp:</p> <p><input type="checkbox"/> DHCP</p> <p><input checked="" type="checkbox"/> OVF environment</p> <p>The IP allocation schemes determine what IP allocation policy options are enabled.</p> | | | |
| <div>IP protocol</div> <p>Specify the IP protocols supported by this vApp:</p> <p>Both ▼</p> | | | |
| <div>▼ OVF settings</div> <div>OVF environment</div> <p>View...</p> <p>The OVF environment is only available when the VM is powered on.</p> | | | |
| <div>OVF environment transport</div> <p><input checked="" type="checkbox"/> ISO image</p> <p>An ISO image, containing the OVF environment document, is mounted on the first available CD-ROM drive.</p> | | | |
| <p><input checked="" type="checkbox"/> VMware Tools</p> <p>The VMware tools guestInfo.ovfEnv variable is initialized with the OVF environment document.</p> | | | |
| <div>Installation boot</div> <p><input type="checkbox"/> Enable</p> <p>The installation boot automatically gets reset upon first power-on of the virtual machine.</p> <p>0</p> <p>Specify the delay in seconds to wait for the VM to power off. A value of zero means wait until the VM is powered off</p> | | | |

- 5 [OK] をクリックします。
- 6 変更対象の vRealize Automation アプライアンスを起動します。
- 7 vRealize Automation アプライアンスの管理インターフェイスに root としてログインします。
https://<vrealize-automation-appliance-FQDN>:5480
- 8 [ネットワーク] タブをクリックします。
- 9 このタブで、[アドレス] をクリックします。
- 10 IP アドレスを更新します。
- 11 右上にある [設定の保存] をクリックします。
- 12 変更対象の vRealize Automation アプライアンスをシャットダウンします。

13 DNS で、新しい IP アドレスのエントリを更新します。

既存の A 型レコードのみを更新します。FQDN は変更しないでください。

ロード バランサを使用する場合は、バックエンド ノード、サービス プール、および仮想サーバに対するロード バランサの IP アドレス設定も必要に応じて更新します。

14 DNS のレプリケーションとゾーン分散が実行されるまで待機します。

15 すべての vRealize Automation アプライアンスを起動します。

16 IaaS サーバの vRealize Automation サービスを開始します。

17 vRealize Automation アプライアンスの管理インターフェイスに root としてログインします。

`https://<vrealize-automation-appliance-FQDN>:5480`

18 次の領域で vRealize Automation アプライアンスのステータスを確認します。

- データベースの接続状態：[vRA 設定] > [データベース]
- RabbitMQ のステータス：[vRA 設定] > [メッセージング]
- Xenon のステータス：[vRA 設定] > [Xenon]
- [サービス] で [登録済み] と表示されているすべてのサービス

変更したホスト名に関する SQL データベースの調整

vRealize Automation IaaS SQL データベースを別のホスト名に移動する場合は、設定を修正する必要があります。

SQL データベースをバックアップから同じホスト名にリストアする場合、追加の手順は必要ありません。別のホスト名にリストアする場合は、構成ファイルを編集して、追加の変更を加える必要があります。

別のホスト名に SQL データベースを移動する場合に必要な変更については、[VMware ナレッジベースの記事 KB2074607](#) を参照してください。

IaaS サーバの IP アドレスの変更

環境またはネットワークを維持するために、既存の vRealize Automation IaaS Windows サーバに別の IP アドレスを割り当てる必要が生じる場合があります。

前提条件

- vRealize Automation アプライアンスの IP アドレスを変更する必要がある場合は、最初にその操作を実行します。[「vRealize Automation アプライアンスの IP アドレスの変更」](#) を参照してください。
- 予防措置として、vRealize Automation アプライアンスと IaaS サーバのスナップショットを作成します。
- vRealize Automation アプライアンスの root としてのコンソールセッションで、`/etc/hosts` ファイルのエントリを検査します。

新しい IP アドレス プランと競合する可能性のあるアドレス割り当てを検索し、必要に応じて変更を加えます。

すべての IaaS サーバで、`Windows\system32\drivers\etc\hosts` ファイルについてこの操作を繰り返します。

- vRealize Automation アプライアンスをシャットダウンします。

- IaaS サーバ上のすべての vRealize Automation サービスを停止します。

手順

- 1 管理者権限を備えたアカウントを使用して IaaS サーバにログインします。

- 2 Windows で、IP アドレスを変更します。

Windows ネットワーク アダプタの設定で、インターネット プロトコルのプロパティに含まれる IP アドレスを確認します。

- 3 変更を保存してローカル DNS を更新します。

DNS を更新することにより、IaaS Windows サーバが互いを見つけ、Windows サーバから切断された場合に再接続できるようになります。

- 4 Manager Service ホストで、テキスト エディタを使用して次のファイルを検査します。

<インストール フォルダ>\vCAC\Server\ManagerService.exe.config

デフォルトのインストール フォルダは、**C:\Program Files (x86)\VMware** です。

vRealize Automation アプライアンスおよび IaaS Windows サーバの IP アドレスまたは FQDN を確認します。

- 5 すべての IaaS Windows サーバで、テキスト エディタを使用して次のファイルを検査します。

<インストール フォルダ>\vCAC\Management

Agent\VMware.IaaS.Management.Agent.exe.Config

vRealize Automation アプライアンスの IP アドレスまたは FQDN を確認します。

- 6 SQL Server ホストにログインします。

- 7 リポジトリ アドレスがConnectionString 列の FQDN を使用するように正しく設定されていることを確認します。

たとえば、SQL Management Studio を開き、次のクエリを実行します。

```
"SELECT Name, ConnectionString FROM [<データベース名>].
[DynamicOps.RepositoryModel].[Models]"
```

- 8 vRealize Automation アプライアンスを起動します。

- 9 IaaS サーバの vRealize Automation サービスを開始します。

- 10 ログ ファイルを検査して、エージェント、DEM ワーカー、Manager Service、および Web ホスト サービスが正常に開始されたことを確認します。

- 11 インフラストラクチャ管理者ロールを持つユーザーとして vRealize Automation にログインします。

- 12 [インフラストラクチャ] - [監視] - [分散実行ステータス] の順に移動し、すべてのサービスが実行されていることを確認します。

- 13 アプライアンス サービスのチェック、プロビジョニングのテスト、または vRealize Production Test Tool の使用により、正常な動作をテストします。

laaS サーバ ホスト名の変更

環境またはネットワークを維持するために、既存の vRealize Automation laaS Windows サーバに別のホスト名を割り当てる必要が生じる場合があります。

手順

- 1 laaS サーバのスナップショットを作成します。
- 2 laaS サーバで、IIS マネージャを使用して vRealize Automation アプリケーション プール（リポジトリ、VMware vRealize Automation、Wapi）を停止します。
- 3 laaS サーバで、[管理ツール] > [サービス] の順に移動して、vRealize Automation のすべてのサービス、エージェント、および DEM を停止します。
- 4 DNS に新しいホスト名を指定したレコードを追加します。
古いホスト名の既存の DNS レコードはまだ削除しないでください。
- 5 DNS のレプリケーションとゾーン分散が実行されるまで待機します。
- 6 laaS サーバ上でホスト名を変更します。プロンプトで要求されても、サーバを再起動しないでください。
Windows システム プロパティのコンピュータ名、ドメイン、ワークグループ設定で、このホスト名を探します。
再起動のプロンプトが表示されたら、後で再起動するオプションをクリックします。
- 7 古いホスト名を使用して証明書が生成されている場合は、証明書を更新します。
詳細については、[vRealize Automation 証明書の更新](#)を参照してください。
- 8 テキスト エディタを使用し、構成ファイル内のホスト名を見つけて更新します。
どの laaS サーバのホスト名を変更したかに基づいて、更新します。分散型の高可用性環境では、1 台以上のサーバへのアクセスが必要な場合があります。DEM オーケストレータまたは DEM ワーカーのホスト名を変更する場合、更新は必要ありません。

注: 以前の Windows サーバのホスト名のみを更新します。代わりにロード バランサ名が表示されている場合は、ロード バランサ名をそのまま使用します。

表 1-40. Web ノードのホスト名を変更する際に更新するファイル

| laaS サーバ | パス | ファイル |
|--------------------------------------|---|---------------------------|
| Web ノード | <install-folder>\Server\Website | Web.config |
| | <install-folder>\Server\Website\Cafe | Vcac-Config.exe.config |
| | <install-folder>\Web API | Web.config |
| | <install-folder>\Web API\ConfigTool | Vcac-Config.exe.config |
| Model Manager コンポーネントがインストールされているノード | <install-folder>\Server\Model Manager Data | Repoutil.exe.config |
| | <install-folder>\Server\Model Manager Data\Cafe | Vcac-Config.exe.config |
| Manager Service ノード | <install-folder>\Server | ManagerService.exe.config |

表 1-40. Web ノードのホスト名を変更する際に更新するファイル (続き)

| laaS サーバ | パス | ファイル |
|------------------|---|---------------------------|
| DEM オーケストレータ ノード | <install-folder>\Distributed Execution Manager\dem | DynamicOps.DEM.exe.config |
| DEM ワーカー ノード | <install-folder>\Distributed Execution Manager\<DEM-name> | DynamicOps.DEM.exe.config |
| エージェント ノード | <install-folder>\Agents\<agent-name> | RepoUtil.exe.config |
| | <install-folder>\Agents\<agent-name> | VRMAgent.exe.config |

表 1-41. Manager Service ノードのホスト名を変更する際に更新するファイル

| laaS サーバ | パス | ファイル |
|------------------|---|---------------------------|
| DEM オーケストレータ ノード | <install-folder>\Distributed Execution Manager\<DEM-name> | DynamicOps.DEM.exe.config |
| DEM ワーカー ノード | <install-folder>\Distributed Execution Manager\dem | DynamicOps.DEM.exe.config |
| エージェント ノード | <install-folder>\Agents\<agent-name> | VRMAgent.exe.config |

表 1-42. エージェント ノードのホスト名を変更する際に更新するファイル

| laaS サーバ | パス | ファイル |
|------------|--------------------------------------|---------------------|
| エージェント ノード | <install-folder>\Agents\<agent-name> | VRMAgent.exe.config |

- 9 ホスト名を変更した laaS サーバを再起動します。
- 10 先ほど停止した vRealize Automation アプリケーション プールを起動します。
- 11 先ほど停止した vRealize Automation サービス、エージェント、および DEM を起動します。
- 12 古い laaS サーバ ホスト名が HA 環境のロード バランサで使用されていた場合は、確認後、ロード バランサを新しい名前で再構成します。
- 13 DNS で、古いホスト名を使用している既存の DNS レコードを削除します。
- 14 DNS のレプリケーションとゾーン分散が実行されるまで待機します。
- 15 Manager Service ホストのホスト名を変更した場合は、次の追加の手順を実行します。
 - a 既存の仮想マシンでソフトウェア エージェントをアップデートします。
 - b ゲスト エージェントを含む ISO またはテンプレートを再作成します。

次のステップ

vRealize Automation の使用準備が完了していることを検証します。 [vRealize Suite Backup and Restore](#) ドキュメントを参照してください。

vRealize Automation ログイン URL のカスタム名への設定

vRealize Automation ユーザーが vRealize Automation アプライアンスまたはロード バランサの名前以外の URL 名にログインするように設定する場合は、カスタマイズ手順をインストールの前後に実行します。

手順

- 1 インストール前に、CNAME、vRealize Automation アプライアンスとロード バランサの名前を含む証明書を準備します。
- 2 vRealize Automation をインストールして、通常の手順でアプライアンスまたはロード バランサの名前を入力します。インストール時に、カスタマイズした証明書をインポートします。
- 3 インストール後、DNS でコモン ネームの CNAME エイリアスを作成し、アプライアンスまたはロード バランサの仮想 IP アドレスで参照するようにします。
- 4 vRealize Automation アプライアンス管理者インターフェイスに root としてログインします。
`https://<vrealize-automation-appliance-FQDN>:5480`
- 5 [vRA 設定] - [ホストの設定] の [ホスト名] を選択した CNAME に変更します。

vRealize Code Stream のライセンス

vRealize Automation で vRealize Code Stream ライセンスを入力すると、vRealize Code Stream を有効にすることができます。

vRealize Code Stream ライセンスは、次のいずれかの場所を入力できます。

- vRealize Automation インストールウィザードの [ライセンス] ページ。詳細については、[vRealize Code Stream Installation](#) を参照してください。
- vRealize Automation アプライアンス管理インターフェイスの [ライセンス] タブ。詳細については、[Apply a vRealize Code Stream License to an Appliance](#) を参照してください。

IaaS サーバ上での vRealize Log Insight エージェントのインストール

vRealize Automation IaaS 構成内の Windows サーバには vRealize Log Insight エージェントがデフォルトでは含まれていません。

vRealize Log Insight は、ログ集計とインデックス作成の機能を提供し、システムの問題を明らかにするためにログの収集、インポート、分析を行うことができます。vRealize Log Insight によって IaaS サーバからログを取得して分析する場合は、Windows 用の vRealize Log Insight エージェントを別途インストールする必要があります。

詳細については、[VMware vRealize Log Insight のドキュメント](#)を参照してください。

vRealize Automation アプライアンスには、デフォルトで vRealize Log Insight エージェントが含まれています。

VMware Remote Console プロキシ ポートの変更

サイトがポート 8444 をブロックしている場合、またはその他の方法で予約している場合は、VMware Remote Console によって使用されるデフォルトのプロキシ ポートを変更できます。

手順

- 1 root として vRealize Automation アプライアンス コマンド プロンプトを開きます。
- 2 テキスト エディタで次のファイルを開きます。
`/etc/vcac/security.properties`
- 3 `consoleproxy.service.port` を、デフォルトの 8444 から未使用のポートに変更します。
- 4 `security.properties` を保存して閉じます。
- 5 vRealize Automation アプライアンスを再起動します。

HA 環境では、すべての vRealize Automation アプライアンスに同じ変更を行います。

vRealize Automation アプライアンスの完全修飾ドメイン名 (FQDN) を元の FQDN に戻す

vRealize Automation アプライアンスの FQDN が意図せずに変更される場合があります。たとえば、アプライアンスが配置されているドメイン以外で統合 Windows 認証 (IWA) ディレクトリを作成する場合、FQDN が変更されます。

別のドメインの IWA ディレクトリを作成する場合は、次の手順に沿って、アプライアンスの FQDN を元の FQDN に戻します。

手順

- 1 vRealize Automation にログインし、通常どおり IWA ディレクトリを作成します。
[Active Directory over LDAP/IWA リンクの構成](#)を参照してください。
- 2 高可用性環境の場合は、[高可用性を実現するためのディレクトリ管理の構成](#)の手順にも沿って操作します。
- 3 アプライアンスが配置されているドメイン以外で IWA ディレクトリを作成すると、アプライアンスの FQDN が自動的に変更されます。

たとえば、domain2.local で IWA ディレクトリを作成すると、va1.domain1.local が va1.domain2.local に変更されます。

この変更を元に戻すには、各アプライアンスを元の FQDN に設定し直します。[「ホスト名と IP アドレスの変更」](#)で説明されている関連手順を参照してください。

- 4 アプライアンスが元の FQDN に戻り、完全にオンラインになった後、各 IaaS ノードにログインし、次の手順を実行します。
 - a テキスト エディタで次のファイルを開きます。
`C:\Program Files (x86)\VMware\VCAC\Management Agent\VMware.IaaS.Management.Agent.exe.Config`
 - b 各アプライアンスの `endpoint address=` FQDN を元の FQDN に戻します。

変更前の例：

```
<endpoint address="https://va1.domain2.local:5480/"
thumbprint="90C55BAEC53E31609EE1614CE4A8336848A8D4CF" />
<endpoint address="https://va2.domain2.local:5480/"
thumbprint="0468BF6EDBC6F2209BE01D0D7FD1094197E324ED" />
```

変更後の例：

```
<endpoint address="https://va1.domain1.local:5480/"
thumbprint="90C55BAEC53E31609EE1614CE4A8336848A8D4CF" />
<endpoint address="https://va2.domain1.local:5480/"
thumbprint="0468BF6EDBC6F2209BE01D0D7FD1094197E324ED" />
```

c **VMware.IaaS.Management.Agent.exe.Config** を保存して閉じます。

5 vRealize Automation アプライアンスの管理インターフェイスに root としてログインします。

https://<vrealize-automation-appliance-FQDN>:5480

6 [vRA 設定] > [メッセージング] の順に移動して、[RabbitMQ クラスタのリセット] をクリックします。

7 リセットが完了したら、各アプライアンス管理インターフェイスにログインします。

8 [vRA 設定] > [クラスタ] の順に移動して、すべてのノードがクラスタに接続されていることを確認します。

SQL AlwaysOn 可用性グループの構成

vRealize Automation をインストールした後に、SQL AlwaysOn 可用性グループ (AAG) セットアップした場合は、構成の変更を行う必要があります。

インストール後に SQL AAG をセットアップする場合は、[VMware ナレッジベースの記事 KB2074607](#) の手順に沿って、AAG リスナーの完全修飾ドメイン名 (FQDN) を使用し、SQL Server ホストとして vRealize Automation を構成します。

vRealize Automation のインストール後にネットワーク インターフェイス コントローラを追加

vRealize Automation は、複数のネットワーク インターフェイス コントローラ (NIC) をサポートします。インストール後、NIC を vRealize Automation アプライアンスまたは IaaS Windows サーバに追加することができます。

vRealize Automation 展開環境では、以下のような場合に複数の NIC が必要になることがあります。

- ユーザーとインフラストラクチャ ネットワークを分離する必要がある。
- IaaS サーバが Active Directory ドメインに参加できるように、追加の NIC を必要としている。

複数の NIC のシナリオの詳細については、この [VMware Cloud Management に関するブログ記事](#) を参照してください。

NIC が 3 個以上の場合は、次の制限を考慮してください。

- VIDM が PostgreSQL データベースおよび Active Directory にアクセスする必要がある。
- VIDM が、HA クラスタでロード バランサの URL にアクセスする必要がある。

- 前述の VIDM は最初の 2 個の NIC を通じて接続される必要がある。
- 2 個目以降の NIC は VIDM に使用または認識されないようにする。
- 2 個目以降の NIC は、Active Directory への接続に使用されないようにする。

vRealize Automation でディレクトリを構成する時は、1 個目または 2 個目の NIC を使用する。

前提条件

vRealize Automation を vCenter 環境に完全にインストールします。

手順

- 1 vCenter Server で、NIC を各 vRealize Automation アプライアンスに追加します。
 - a アプライアンスを右クリックして、[設定の編集] を選択します。
 - b VMXNETn NIC を追加します。
 - c パワーオンされている場合、アプライアンスを再起動します。
- 2 vRealize Automation アプライアンス管理インターフェイスにルートとしてログインします。
<https://<vrealize-automation-appliance-FQDN>:5480>
- 3 [ネットワーク] を選択して、複数の NIC が使用できることを確認します。
- 4 [アドレス] を選択して、NIC の IP アドレスを設定します。

表 1-43. NIC 設定の例

| 設定 | 値 |
|---------------|---------------|
| IPv4 アドレス タイプ | Static |
| IPv4 アドレス | 172.22.0.2 |
| ネットマスク | 255.255.255.0 |

- 5 すべての vRealize Automation ノードが DNS 名で相互に解決されることを確認します。
- 6 すべての vRealize Automation ノードが、vRealize Automation コンポーネントのロード バランシングされた FQDN にアクセスできることを確認します。
- 7 スプリット ブレイン DNS を使用している場合、すべての vRealize Automation ノードと仮想 IP アドレスが、各ノードの IP アドレスおよび仮想 IP アドレスに対して DNS で同一の FQDN を持つことを確認します。
- 8 vCenter Server で、NIC を IaaS Windows サーバに追加します。
 - a IaaS サーバを右クリックして、[設定の編集] を選択します。
 - b NIC を IaaS サーバ仮想マシンに追加します。
- 9 Windows で、追加の IaaS サーバの NIC とその IP アドレスを設定します。必要に応じて、Microsoft のドキュメントを参照してください。

次のステップ

(オプション) スタティック ルートが必要な場合は、[「スタティック ルートの設定」](#) を参照してください。

スタティック ルートの設定

NIC を vRealize Automation インストールに追加する際に、スタティック ルートが必要な場合、コマンド プロンプト セッションを開いて設定します。

前提条件

複数の NIC を vRealize Automation アプライアンスまたは IaaS Windows サーバに追加します。

手順

- 1 vRealize Automation アプライアンスのコマンド ラインに **root** としてログインします。
- 2 テキスト エディタでルート ファイルを開きます。

```
/etc/sysconfig/network/routes
```

- 3 デフォルト ゲートウェイの **default** 行を特定します。ここでは変更しないでください。

注: デフォルト ゲートウェイを変更する必要がある場合は vRealize Automation 管理インターフェイスを使用します。

- 4 **default** 行の下にスタティック ルートの新しい行を追加します。例：

```
default 10.10.10.1 --
172.30.30.0 192.168.100.1 255.255.255.0 eth0
192.168.210.0 192.168.230.1 255.255.255.0 eth2
```

- 5 ルート ファイルを保存して閉じます。
- 6 アプライアンスを再起動します。
- 7 HA クラスタで、各アプライアンスに対してこのプロセスを繰り返します。
- 8 IaaS Windows サーバに管理者としてログインします。
- 9 管理者としてコマンド プロンプトを開きます。
- 10 スタティック ルートを設定するには、**route -p add** コマンドを入力します。この **-p** によって、再起動後もスタティック ルートが維持されます。例：

```
C:\Windows\system32> route -p add 172.30.30.0 mask 255.255.255.0 192.168.100.1 metric 1
OK!
```

Windows でのスタティック ルートの設定に関する詳細については、Microsoft のドキュメントを参照してください。

パッチ管理へのアクセス

vRealize Automation インストールのテクニカル サポートには、vRealize Automation アプライアンス管理インターフェイスを使用してインストールまたは削除するソフトウェア パッチが含まれていることがあります。

パッチ インターフェイスは、次の vRealize Automation コンポーネントにパッチを適用できません。

- 管理エージェント
- XenServer、VDI、Hyper-V などの非 vSphere エージェント

前提条件

- vRealize Automation インストールのすべてのノードのスナップショットを作成します。
 - vRealize Automation インストールのすべてのノードが起動して稼動していることを確認します。
- すべてのノードが動作していない状態でパッチをインストールまたは削除しようとする、vRealize Automation アプライアンス管理インターフェイスが応答しなくなる可能性があります。この現象が発生した場合、テクニカル サポートにお問い合わせください。この問題が解決するまで、他の方法でパッチを管理したり、vRealize Automation を使用したりしないでください。
- HA 環境でロード バランサを使用している場合、パッチがインストールまたは削除されるまで、セカンダリ ノードへのトラフィックを無効にします。
 - 新しいパッチをインストールする場合、パッチ ファイルを取得し、vRealize Automation アプライアンス管理インターフェイスに使用するブラウザで使用可能なファイル システムにコピーします。
 - パッチに関する最新情報や新たなリリース情報については、[VMware のナレッジベース](#)を確認してください。
- ナレッジベースを開き、検索ボックスに「vRealize Automation のパッチ適用」と入力します。たとえば、[VMware ナレッジベースの記事 51708](#) は、最新の vRealize Automation 7.4 パッチの情報を活用して確認および更新されています。

手順

- 1 vRealize Automation アプライアンス管理インターフェイスにルートとしてログインします。
https://<vrealize-automation-appliance-FQDN>:5480
- 2 [vRA 設定] - [パッチ] の順にクリックします。
- 3 [パッチ管理] の下に必要なオプションをクリックして、プロンプトの手順を実行します。

| オプション | 説明 |
|--------------|---|
| 新しいパッチ | ダウンロードした新しいパッチをインストールします。 |
| インストール済みのパッチ | 最近インストールされたパッチを新しく追加されたクラスタ ノードに追加します。 |
| ロールバック | 最近インストールされたパッチを削除して、以前のパッチ レベルに vRealize Automation をロールバックします。 |
| 履歴 | インストール済みのパッチと削除されたパッチのリストを調べます。 |

[パッチ管理] を有効または無効にするには、root として vRealize Automation アプライアンスのコマンド プロンプトにログインして、次のコマンドのいずれかを入力します。

```
/opt/vmware/share/htdocs/service/hotfix/scripts/hotfix.sh enable
/opt/vmware/share/htdocs/service/hotfix/scripts/hotfix.sh disable
```


新しいパッチのインストール

新しい vRealize Automation パッチは、vRealize Automation アプライアンス管理インターフェイスを使用してインストールします。

前提条件

前提条件を確認して、パッチ管理インターフェイスに移動します。[「パッチ管理へのアクセス」](#)を参照してください。

手順

- 1 [新しいパッチ] をクリックします。
- 2 [パッチのアップロード] をクリックします。
- 3 パッチ ファイルを検索して選択します。
- 4 パッチのアップロード後、パッチの詳細を確認します。
- 5 誤ったパッチがある場合、[削除] をクリックしてキャンセルします。ない場合は、[インストール] をクリックします。
- 6 前提条件を満たしていることを確認して、[インストール] をクリックします。

パッチのインストールには数分かかる場合があります。

- 7 [終了] をクリックします。

パッチのインストールが失敗した場合、[再試行] をクリックしてもう一度やり直すか、[削除] をクリックしてキャンセルすることができます。キャンセルすると、vRealize Automation は、パッチのインストールを開始する前の状態にロールバックされます。

新しいノードに最新のパッチをインストールする

最近インストールした vRealize Automation パッチを新しく追加されたクラスタ ノードに追加できます。

前提条件

前提条件を確認して、パッチ管理インターフェイスに移動します。[「パッチ管理へのアクセス」](#)を参照してください。

手順

- 1 [インストール済みのパッチ] をクリックします。
- 2 最新のパッチを選択します。
- 3 [インストール] をクリックします。
- 4 プロンプトの指示に従います。

最新のパッチの削除

最近インストールした vRealize Automation パッチを削除して、以前のパッチにロールバックすることができます。

前提条件

パッチ管理インターフェイスに移動します。[「パッチ管理へのアクセス」](#)を参照してください。

手順

- 1 [ロールバック] をクリックします。
- 2 最新のパッチを選択します。
- 3 [ロールバック] をクリックします。
- 4 プロンプトの指示に従います。

デフォルト テナントへのアクセスの構成

チームが vRealize Automation の構成を開始する前に、デフォルト テナントへのアクセス権をチームに与える必要があります。

インストール ウィザードでシングル サインオンを構成すると、デフォルト テナントが自動的に作成されます。名前や URL トークンなどのテナントの詳細は編集できませんが、新規のローカル ユーザーを作成し、テナント管理者または IaaS 管理者を追加で指定することはいつでも可能です。

手順

- 1 vRealize Automation に、デフォルトのテナントの管理者としてログインします。
 - a vRealize Automation 製品のインターフェイスに移動します。
`https://<vrealize-automation-FQDN>/vcac`
 - b ユーザー名 **administrator** と、SSO を構成したときにこのユーザー用に指定したパスワードを使用してログインします。
- 2 [管理] - [テナント] を選択します。
- 3 デフォルト テナントの名前である [vsphere.local] をクリックします。
- 4 [ローカル ユーザー] タブをクリックします。
- 5 vRealize Automation デフォルト テナントのローカル ユーザー アカウントを作成します。
 ローカル ユーザーはテナント固有であり、ローカル ユーザーを作成したテナントにのみアクセスできます。
 - a 追加 (+) アイコンをクリックします。
 - b インフラストラクチャの管理を担当するユーザーの詳細を入力します。
 - c [追加] をクリックします。
 - d この手順を繰り返し、デフォルト テナントの構成を担当するユーザーを 1 人以上追加します。
- 6 [管理者] タブをクリックします。
- 7 ローカル ユーザーをテナント管理者と IaaS 管理者ロールに割り当てます。
 - a [テナント管理者] 検索ボックスにユーザー名を入力し、Enter を押します。
 - b [IaaS 管理者] 検索ボックスにユーザー名を入力し、Enter を押します。
 IaaS 管理者は、vRealize Automation のインフラストラクチャのエンドポイントの作成と管理を担当します。システム管理者だけがこのロールを付与できます。

8 [アップデート] をクリックします。

次のステップ

チームが vRealize Automation の構成を開始する前に、作成したユーザー アカウントのアクセス URL とログイン情報をチームに提供してください。

- テナント管理者がユーザー認証などを設定します。これには、高可用性を実現するための [ディレクトリ管理] の設定が含まれます。[テナント設定](#)を参照してください。
- IaaS 管理者が、プロビジョニングのための外部リソースを準備します。[プロビジョニングのための外部環境の準備](#)を参照してください。
- インストールの際に初期コンテンツ作成を設定した場合、事前検証をすばやく実施するために、構成管理者は初期コンテンツのカatalog アイテムを申請することができます。アイテムを要求して、手動ユーザー アクションを実行する方法については、[シナリオ : Rainpole 事前検証の展開に初期コンテンツを申請する](#)を参照してください。

vRealize Automation インストールのトラブルシューティング

vRealize Automation のトラブルシューティングでは、vRealize Automation のインストールまたは構成時に発生する可能性のある問題を解決する手順を紹介します。

デフォルトのログの場所

失敗したインストールについての情報は、システムおよび製品のログ ファイルを参照してください。

注: ログを収集する場合は、vRealize Log Insight 用の vRealize Automation および vRealize Orchestrator コンテンツ パックの利用を検討してください。コンテンツ パックと Log Insight は、vRealize Suite のコンポーネントに対するログ イベントを統合されたサマリ形式で提供します。詳細については、[VMware Solution Exchange](#) を参照してください。

最新のログの場所のリストについては、[VMware ナレッジベースの記事 KB2141175](#) を参照してください。

Windows ログ

Windows イベントのログ ファイルは次の場所にあります。

| ログ | 場所 |
|----------------------|---|
| Windows イベント ビューアのログ | [スタート] - [コントロール パネル] - [管理ツール] - [イベント ビューア] |

インストール ログ

インストール ログは次の場所にあります。

| ログ | デフォルトの場所 |
|----------------|---|
| インストール ログ | C:\Program Files (x86)\vCAC\InstallLogs C:\Program Files (x86)\VMware\vCAC\Server\ConfigTool\Log |
| WAPI インストール ログ | C:\Program Files (x86)\VMware\vCAC\Web API\ConfigTool\Logfilename WapiConfiguration-<XXX> |

laaS ログ

laaS ログは次の場所にあります。

| ログ | デフォルトの場所 |
|---------------------|--|
| Web サイト ログ | C:\Program Files (x86)\VMware\vCAC\Server\Website\Logs |
| リポジトリ ログ | C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Web\Logs |
| Manager Service ログ | C:\Program Files (x86)\VMware\vCAC\Server\Logs |
| DEM Orchestrator ログ | C:\Users\<<user-name>>\AppData\Local\Temp\VMware\vCAC\Distributed Execution Manager\<<system-name>> DEO \Logs |
| エージェント ログ | C:\Users\<<user-name>>\AppData\Local\Temp\VMware\vCAC\Agents\<<agent- name>>\logs |

vRealize Automation フレームワーク ログ

vRealize Automation フレームワークのログ エントリは次の場所にあります。

| ログ | デフォルトの場所 |
|------------|-----------------|
| フレームワーク ログ | /var/log/vmware |

ソフトウェア コンポーネント プロビジョニングのログ

ソフトウェア コンポーネント プロビジョニングのログは次の場所にあります。

| ログ | デフォルトの場所 |
|-------------------------------|---|
| ソフトウェア エージェント ブートストラップ のログ | /opt/vmware-appdirector (Linux の場合) または \opt\vmware- appdirector (Windows の場合) |
| ソフトウェア ライフサイクル スクリプトのログ | /tmp/taskId (Linux の場合) \Users\darwin\AppData\Local\Temp\taskId (Windows の場合) |

分散導入環境のログ収集

分散導入環境のコンポーネントのすべてのログをまとめた zip ファイルを作成できます。

失敗したインストールのロールバック

インストールが失敗しロールバックする際、システム管理者は、別のインストールを開始する前に、すべての必要なファイルがアンインストールされていることを確認します。一部のファイルは手動でアンインストールする必要があります。

最小インストールのロールバック

失敗した vRealize Automation IaaS インストールを完全にアンインストールするには、システム管理者は、一部のファイルを手動で削除し、データベースを戻す必要があります。

手順

- 1 次のコンポーネントがある場合には、Windows アンインストーラでそれらをアンインストールします。

- vRealize Automation エージェント
- vRealize Automation DEM-ワーカー
- vRealize Automation DEM-Orchestrator
- vRealize Automation サーバ
- vRealize Automation WAPI

注: 次のメッセージが表示された場合、マシンを再起動してこの手順を実行します。「インストール ログ ファイルを開くときにエラーが発生しました。指定されたログ ファイルの場所が存在し、書き込み可能であることを確認してください」

注: Windows システムが元に戻された場合、または IaaS をアンインストールした場合は、vRealize Automation IaaS を再インストールする前に **iisreset** コマンドを実行する必要があります。

- 2 データベースを、インストールが開始された前の状態に戻します。使用する方法は、元のデータベース インストール モードにより異なります。
- 3 IIS (インターネットインフォメーションサービス マネージャ) で [既定の Web サイト] (またはカスタムのサイト) を選択し、[バインド] を選択します。https バインド (デフォルトは 443) を削除します。
- 4 アプリケーション リポジトリ、vRealize Automation、および WAPI が削除され、RepositoryAppPool、vCACAppPool、WapiAppPool の各アプリケーション プールも削除されていることを確認します。

インストールは完全に削除されます。

分散インストールのロールバック

失敗した IaaS インストールを完全にアンインストールするには、システム管理者は、一部のファイルを手動で削除し、データベースを戻す必要があります。

手順

- 1 次のコンポーネントがある場合には、Windows アンインストーラでそれらをアンインストールします。

- vRealize Automation サーバ

■ vRealize Automation WAPI

注: 次のメッセージが表示された場合、マシンを再起動してこの手順を実行します。「インストール ログ ファイルを開くときにエラーが発生しました。指定されたログ ファイルの場所が存在し、書き込み可能であることを確認してください」。

注: Windows システムが元に戻された場合、または IaaS をアンインストールした場合は、vRealize Automation IaaS を再インストールする前に **iisreset** コマンドを実行する必要があります。

- 2 データベースを、インストールが開始された前の状態に戻します。使用する方法は、元のデータベース インストール モードにより異なります。
- 3 IIS (インターネット インフォメーション サービス マネージャ) で [既定の Web サイト] (またはカスタムのサイト) を選択し、[バインド] を選択します。https バインド (デフォルトは 443) を削除します。
- 4 アプリケーション リポジトリ、vCAC、および WAPI が削除され、アプリケーション プールの RepositoryAppPool、vCACAppPool、WapiAppPool も削除されていることを確認します。

表 1-44. 障害ポイントのロールバック

| 障害ポイント | アクション |
|--------------------------|--|
| Manager Service のインストール | 存在する場合、vCloud Automation Center Server をアンインストールします。 |
| DEM-Orchestrator のインストール | DEM Orchestrator が存在する場合は、アンインストールします。 |
| DEM-ワーカーのインストール | DEM ワーカーがある場合は、すべてアンインストールします。 |
| エージェントのインストール | vRealize Automation エージェントが存在する場合は、すべてアンインストールします。 |

vRealize Automation サポート バンドルの作成

vRealize Automation アプライアンス管理インターフェイスを使用して、vRealize Automation サポート バンドルを作成できます。サポート バンドルでは、ログを収集してお客様または VMware テクニカル サポートが vRealize Automation の問題のトラブルシューティングを行うために支援します。

手順

- 1 Web ブラウザを開き、vRealize Automation アプライアンス管理インターフェイス URL にアクセスします。
https://<vrealize-automation-appliance-FQDN>:5480
- 2 root としてログインし、[vRA 設定] - [クラスタ] の順にクリックします。
- 3 [サポート バンドルの作成] をクリックします。
- 4 [ダウンロード] をクリックして、システムにサポート バンドル ファイルを保存します。

サポート バンドルには、vRealize Automation アプライアンスおよび IaaS Windows サーバからの情報が含まれます。vRealize Automation アプライアンスと IaaS コンポーネント間の接続が失われた場合は、サポート バンドルに IaaS コンポーネントのログが含まれないことがあります。

どのログ ファイルが収集されたかを確認するには、サポート バンドルを展開して、**Environment.html** ファイルを Web ブラウザで開きます。接続が失われている場合は、[ノード] テーブルに IaaS コンポーネントが赤色で表示されることがあります。IaaS ログが含まれない原因としては、赤く表示されている IaaS Windows サーバで vRealize Automation 管理エージェント サービスが停止している場合もあります。

一般的なインストールのトラブルシューティング

vRealize Automation アプライアンスのトラブルシューティングに関するトピックでは、vRealize Automation を使用するときには発生する可能性がある潜在的なインストール関連の問題に対するソリューションを提供します。

ロード バランサのタイムアウト エラーでインストールまたはアップグレードに失敗する

ロード バランサを使用した分散環境を実現するための vRealize Automation のインストールまたはアップグレードが、503 サービス利用不能エラーで失敗します。

問題

ロード バランサ タイムアウトの設定が原因でタスクを完了するための十分な時間が確保できないため、インストールまたはアップグレードに失敗します。

原因

ロード バランサ タイムアウトの設定値が小さいとエラーになる可能性があります。この問題を修正するには、ロード バランサ タイムアウトの設定値を 100 秒以上に増やしてタスクを再実行します。

ソリューション

- 1 ロード バランサ タイムアウト値を最低でも 100 秒に増やします。
- 2 インストールまたはアップグレードを再実行します。

サーバ時間が同期されない

IaaS タイム サーバが vRealize Automation アプライアンスと同期していない場合は、インストールに失敗することがあります。

問題

インストール後にログインできないまたは完了中にインストールが失敗します。

原因

すべてのサーバのタイム サーバが同期していない可能性があります。

ソリューション

すべての vRealize Automation アプライアンスと IaaS Windows サーバを同じ時刻ソースに同期します。vRealize Automation 展開内で時刻ソースを混在させないでください。

- vRealize Automation アプライアンスの時刻ソースを設定します。
 - a vRealize Automation アプライアンス管理インターフェイスにルートとしてログインします。
<https://<vrealize-automation-appliance-FQDN>:5480>

- b [管理] - [時刻設定] の順に選択し、時刻同期ソースを設定します。

| オプション | 説明 |
|---------|--|
| ホストの時刻 | vRealize Automation アプライアンスの ESXi ホストに同期します。 |
| タイム サーバ | 単一の外部 Network Time Protocol (NTP) サーバに同期します。NTP サーバの FQDN または IP アドレスを入力します。 |

- IaaS Windows サーバについては、[「Windows Server での時刻同期の有効化」](#)を参照してください。

Windows 7 で Internet Explorer 9 または 10 を使用しているとき空白のページが表示されることがある

Windows 7 で Internet Explorer 9 または 10 を使用していて互換モードが有効な場合、一部のページでコンテンツが表示されません。

問題

Windows 7 で Internet Explorer 9 または 10 を使用している場合、次のページにコンテンツが表示されません。

- インフラストラクチャ
- Orchestrator ページのデフォルトのテナント フォルダ
- Orchestrator ページのサーバ構成

原因

この問題は有効になっている互換モードに関連している可能性があります。次の手順で、Internet Explorer の互換モードを無効にできます。

ソリューション

前提条件

メニュー バーが表示されていることを確認します。Internet Explorer 9 または 10 を使用している場合、Alt を押してメニュー バーを表示します（またはアドレス バーを右クリックしてから [メニュー バー] を選択します）。

手順

- 1 [ツール] - [互換表示設定] を選択します。
- 2 [互換表示でイントラネット サイトを表示] の選択を解除します。
- 3 [閉じる] をクリックします。

SSL/TLS のセキュリティで保護されているチャネルに対して信頼関係を確立できない

「vCloud Automation Center のセキュリティ証明書のアップグレード中に SSL/TLS のセキュリティで保護されているチャネルに対する信頼関係を確立できませんでした。」というメッセージを受信することがあります。

問題

セキュリティ証明書のアップグレード中に `vcac-config.exe` で証明書の問題が発生した場合、次のメッセージが表示されることがあります。

基になる接続が閉じられました。SSL/TLS のセキュリティで保護されているチャネルに対する信頼関係を確立できません

次の手順を使用して、問題の原因に関する詳細を確認できます。

ソリューション

- 1 テキストエディタで `vcac-config.exe.config` を開き、次のリポジトリ アドレスを見つけます。

```
<add key="repositoryAddress" value="https://<IaaS-address>:443/repository/" />
```

- 2 Internet Explorer でこのアドレスを開きます。
- 3 証明書の信頼性の問題に関するエラー メッセージが続きます。
- 4 Internet Explorer からセキュリティ レポートを取得し、それを使用してこの証明書が信頼できない理由をトラブルシューティングします。

問題が解決されない場合は、登録する必要があるアドレス (`vcac-config.exe` への登録に使用したエンドポイント アドレス) で参照して、この手順を繰り返します。

プロキシ サーバを介したネットワークへの接続

サイトによっては、インターネットへの接続にプロキシ サーバが使用されている場合があります。

問題

展開環境から外部のインターネットに接続できません。たとえば、ソフトウェアやアップデートのダウンロード元となるベンダーのアドレス、管理対象のパブリック クラウド、Web サイトにアクセスできません。

原因

ご利用のサイトは、プロキシ サーバを介してインターネットに接続しています。

ソリューション

前提条件

サイトの管理者からプロキシ サーバの名前、ポート番号、認証情報を入手してください。

手順

- 1 Web ブラウザを開き、vRealize Automation アプライアンス管理インターフェイス URL にアクセスします。
`https://<vrealize-automation-appliance-FQDN>:5480`
- 2 root としてログインし、[ネットワーク] をクリックします。
- 3 サイトのプロキシ サーバの FQDN (または IP アドレス) とポート番号を入力します。
- 4 プロキシ サーバから認証情報を求められた場合は、ユーザー名とパスワードを入力します。

5 [設定の保存] をクリックします。

次のステップ

プロキシの設定によっては、VMware Identity Manager ユーザーのアクセスに影響が生じる可能性があります。この問題を解消するには、[「プロキシが原因で VMware Identity Manager ユーザーがログインできない」](#) を参照してください。

初期コンテンツ構成のためのコンソール手順

vRealize Automation インストール インターフェイスを使用しなくても、構成管理者アカウントおよび初期コンテンツを作成することができます。

問題

vRealize Automation のインストールの最後の部分で、新しいパスワードの入力、configurationadmin ローカルユーザー アカウントの作成、初期コンテンツの作成を行う処理に従います。エラーが発生すると、インターフェイスはリカバリできない状態になります。

ソリューション

このインターフェイスを使用する代わりに、コンソール コマンドを入力して、configurationadmin ユーザーや初期コンテンツを作成します。処理が正常に完了した後、インターフェイスでエラーが発生する可能性があり、その場合は一部のコマンドのみが必要になります。

たとえば、ログと vRealize Orchestrator ワークフローの実行を確認すると、インターフェイスベースのセットアップによって configurationadmin ユーザーは作成されたものの、初期コンテンツは作成されなかったことがわかる場合があります。その場合は、最後の 2 つのコンソール コマンドを入力するだけで処理を完了できます。

手順

- 1 vRealize Automation アプライアンス コンソールに root ユーザーとしてログインします。

- 2 次のコマンドを入力して、vRealize Orchestrator ワークフローをインポートします。

```
/usr/sbin/vcac-config -e content-import --
workflow /usr/lib/vcac/tools/initial-config/vra-initial-config-bundle-
workflow.package --user $SSO_ADMIN_USERNAME --password
$SSO_ADMIN_PASSWORD --tenant $TENANT
```

- 3 ワークフローを実行して、configurationadmin ユーザーを作成します。

```
/usr/bin/python /opt/vmware/share/htdocs/service/wizard/initialcontent/
workflowexecutor.py --host $CURRENT_VA_HOSTNAME --username
$SSO_ADMIN_USERNAME --password $SSO_ADMIN_PASSWORD --workflowid
f2b3064a-75ca-4199-a824-1958d9c1efed --configurationAdminPassword
$CONFIGURATIONADMIN_PASSWORD --tenant $TENANT
```

- 4 次のコマンドを入力して、ASD ブループリントをインポートします。

```
/usr/sbin/vcac-config -e content-import --
blueprint /usr/lib/vcac/tools/initial-config/vra-initial-config-
bundle-asd.zip --user $CONFIGURATIONADMIN_USERNAME --password
$CONFIGURATIONADMIN_PASSWORD --tenant $TENANT
```

- 5 ワークフローを実行して、初期コンテンツを構成します。

```
/usr/bin/python /opt/vmware/share/htdocs/service/wizard/initialcontent/workflowexecutor.py --host $CURRENT_VA_HOSTNAME --username
$SSO_ADMIN_USERNAME --password $SSO_ADMIN_PASSWORD --workflowid
ef00fce2-80ef-4b48-96b5-fdee36981770 --configurationAdminPassword
$CONFIGURATIONADMIN_PASSWORD
```

vRealize Automation のライセンスをダウングレードできない

下位の製品エディションのライセンス キーを送信すると、エラーが発生します。

問題

vRealize Automation 管理インターフェイスの [ライセンス] ページを使用して、現在のエディションより低い製品エディションのキーを送信すると、次のメッセージが表示されます。たとえば、Enterprise のライセンスで使用を開始し、Advanced のライセンスを入力した場合です。

Unable to downgrade existing license edition

原因

この vRealize Automation リリースでは、ライセンスのダウングレードをサポートしていません。同等以上のエディションのライセンスのみを追加できます。

ソリューション

下位のエディションに変更するには、vRealize Automation を再インストールします。

vRealize Automation アプライアンスのトラブルシューティング

vRealize Automation アプライアンスのトラブルシューティングに関するトピックでは、vRealize Automation アプライアンスを使用するときに発生する可能性がある潜在的なインストール関連の問題に対するソリューションを提供します。

インストーラのダウンロードに失敗する

インストーラが vRealize Automation アプライアンスからのダウンロードに失敗します。

問題

setup__<vrealize-automation-appliance-FQDN>@5480.exe の実行時、インストーラがダウンロードを行わない。

原因

- vRealize Automation アプライアンス マシンへの接続中のネットワーク接続の問題。
- vRealize Automation アプライアンス マシンにアクセスできないまたは接続のタイムアウト前に応答できないために、このマシンに接続できない。

ソリューション

- 1 Web ブラウザで vRealize Automation の URL に接続できることを確認します。
https://<vrealize-automation-appliance-FQDN>
- 2 他の vRealize Automation アプライアンスのトラブルシューティングのトピックを確認します。
- 3 設定ファイルをダウンロードし、vRealize Automation アプライアンスに再接続します。

Encryption.key ファイルに不正な権限がある

仮想アプライアンスの Encryption.key ファイルに不正な権限が割り当てられている場合には、システム エラーが発生する場合があります。

問題

vRealize Automation アプライアンス にログインすると [テナント] ページが表示されます。このページのロードが開始された後に、「システム エラー」メッセージが表示されます。

原因

Encryption.key ファイルに不正な権限があるか、グループまたは所有者ユーザー レベルが不正に割り当てられています。

ソリューション

前提条件

エラーを表示している仮想アプライアンスにログインします。

注: 複数の仮想アプライアンスがロード バランサーの下で実行している場合には、各仮想アプライアンスをチェックする必要があります。

手順

- 1 ログ ファイル `/var/log/vcac/catalina.out` を表示してメッセージ「**Cannot write to /etc/vcac/Encryption.key**」を検索します。
- 2 `/etc/vcac/` ディレクトリに移動し、Encryption.key ファイルの権限と所有者を確認します。次のような行があるはずです。

```
-rw----- 1 vcac vcac 48 Dec 4 06:48 encryption.key
```

読み取りおよび書き込み権限が必要で、ファイルの所有者およびグループは **vcac** である必要があります。

- 3 出力が異なる場合、必要に応じてファイルの権限または所有者を変更します。

次のステップ

[テナント] ページにログインして、エラーなしでログインできることを確認します。

Horizon Workspace の再起動後に Directories Management Identity Manager が起動に失敗する

vRealize Automation の高可用性環境で、Horizon Workspace サービスを再起動した後、Directories Management Identity Manager が起動に失敗することがあります。

問題

Horizon Workspace サービスは、次のようなエラーが原因で起動できなくなります。

```
Error creating bean with name
'liquibase' defined in class path resource [spring/datastore-wireup.xml]:
Invocation of init method failed; nested exception is
liquibase.exception.LockException: Could not acquire change log lock. Currently
locked by fe80:0:0:0:250:56ff:fea8:7d0c%eth0
(fe80:0:0:0:250:56ff:fea8:7d0c%eth0) since 10/29/15
```

原因

Identity Manager は、vRealize Automation が使用する liquibase データ管理ユーティリティの問題が原因で、高可用性環境で起動に失敗する可能性があります。

ソリューション

1 vRealize Automation アプライアンスのコンソール セッションに root としてログインします。

2 次のコマンドを入力して、horizon-workspace サービスを停止します。

```
#service horizon-workspace stop
```

3 スーパー ユーザーとして、Postgres シェルを開きます。

```
su postgres
```

4 正しい bin ディレクトリに移動します。

```
cd /opt/vmware/vpostgres/current/bin
```

5 データベースに接続します。

```
psql vcac
```

6 saas.databasechangelock から次の SQL クエリを実行します。

```
select * from databasechangelock;
```

true を意味する「t」の値が出力に表示される場合は、ロックを手動で解除する必要があります。

7 手動でロックを解除する必要がある場合は、次の SQL クエリを実行します。

```
update saas.databasechangelock set locked=FALSE, lockgranted=NULL,
lockedby=NULL where id=1;
```

- 8 `saas.databasechangelock` から次の SQL クエリを実行します。

```
select * from databasechangelock;
```

`false` を意味する「f」の値が出力に表示され、ロックが解除されたことを表します。

- 9 Postgres `vcac` データベースを終了します。

```
vcac=# \q
```

- 10 Postgres シェルを終了します。

```
exit
```

- 11 `horizon-workspace` サービスを開始します。

```
#service horizon-workspace start
```

フェイルオーバー後の誤ったアプライアンス ロールの割り当て

フェイルオーバーの発生後、vRealize Automation アプライアンスのマスター ノードおよびレプリカ ノードで適切なロール割り当てが行われていないことがあります。これは、データベースへの書き込みアクセスを必要とするすべてのサービスに影響を及ぼします。

問題

vRealize Automation アプライアンスの高可用性クラスターで、マスター データベース ノードをシャットダウンするか、アクセスできないようにします。別のノード上の管理コンソールを使用して、そのノードを新しいマスターに昇格させます。この操作により、vRealize Automation データベースへの書き込みアクセスが回復します。

その後、古いマスター ノードをオンライン状態に戻すと、その管理コンソールの [データベース] タブで、そのノードはマスター ノードではないにも関わらず、依然としてマスター ノードとして表示されます。いずれかのノードの管理コンソールを使用して古いノードを正式にマスターに昇格させることで、この問題を解決しようとしても失敗します。

ソリューション

フェイルオーバーが発生した場合は、古いマスター ノードと新しいマスター ノードを構成する際に以下のガイドラインに従います。

- 別のノードをマスターに昇格させる前に、以前のマスター ノードを vRealize Automation アプライアンス ノードのロード バランサ プールから削除します。
- vRealize Automation によって古いマスター ノードをクラスターに戻すには、古いマシンをオンライン状態にします。その後、新しいマスターの管理コンソールを開きます。[データベース] タブで **invalid** と表示されている古いノードを探し、その [リセット] ボタンをクリックします。

リセットに成功したら、古いノードを vRealize Automation アプライアンス ノードのロード バランサ プールに戻すことができます。

- 古いノードをクラスターに手動で戻すには、そのマシンをオンライン状態にしたうえで新しいノードとしてクラスターに参加させます。参加させる際には、新たに昇格させるノードをプライマリ ノードに指定します。

正常に参加させたら、古いノードを vRealize Automation アプライアンス ノードのロード バランサ プールに戻すことができます。

- 古いマスター ノードのリセットまたは再参加が正しく行われるまでは、そのノードがオンライン状態に戻っても、その管理コンソールをクラスタ管理操作に使用しないでください。
- リセットまたは再参加が正しく行われた後は、古いノードを再びマスターに昇格させることができます。

レプリカおよびマスター ノードの昇格後の失敗

レプリカおよびマスター vRealize Automation アプライアンス データベース ノードの昇格によりディスク容量が不足すると、プロビジョニングの問題が発生する場合があります。

問題

マスター ノードのディスク容量が不足する。管理インターフェイスの [データベース] ページにログインし、新規マスターになるための十分な容量があるレプリカ ノードを昇格します。管理インターフェイス ページを更新すると、エラー メッセージが出ていても、昇格が成功しているように見えます。

その後、古いマスター ノードでディスク容量を開放します。このノードを昇格してマスターに戻すと、IN_PROGRESS 状態のままとなりプロビジョニング処理が失敗します。

原因

容量が十分ではないことが問題の場合、vRealize Automation では古いマスター ノード構成を適切に更新できません。

ソリューション

昇格中に管理インターフェイスにエラーが表示される場合は、一時的にロード バランサからそのノードを除外します。ディスクを追加するなど、ノードの問題を解決してから、ロード バランサに再度追加します。管理インターフェイスの [データベース] ページを更新し、正しいノードがマスターおよびレプリカになっていることを確認します。

不正な vRealize Automation コンポーネント サービス登録

vRealize Automation アプライアンス管理インターフェイスは vRealize Automation コンポーネント サービスの登録問題の解決に役立ちます。

問題

正常な運用では、vRealize Automation コンポーネント サービスはすべて一意で、[登録済み] 状態にある必要があります。それ以外の状態では vRealize Automation が予期せぬ動作をする場合があります。

原因

vRealize Automation コンポーネント サービスで発生する可能性のある問題の例を次に示します。

- サービスが無効になっている。
- サーバ設定が原因でサービスが [登録済み] 以外の状態になった。
- 別のサービスの依存関係が原因でサービスが [登録済み] 以外の状態になった。

ソリューション

問題があると思われるコンポーネント サービスを再登録します。

- 1 vRealize Automation アプライアンスのスナップショットを作成します。

別のサービス変更を行う場合や、アプライアンスが予期しない状態になった場合には、スナップショットに戻すことが必要になる可能性があります。

- 2 vRealize Automation アプライアンス管理インターフェイスにルートとしてログインします。

`https://<vrealize-automation-appliance-FQDN>:5480`

- 3 [サービス] をクリックします。

- 4 サービス リストで、正しい状態にないサービス、または他の問題があるサービスを見つけます。

- 5 障害のあるサービスが **iaas-service** である場合、次の手順に移動します。

そうでない場合、vRealize Automation でサービスを再登録するには、root ユーザーとして vRealize Automation アプライアンスのコンソール セッションにログインし、以下のコマンドを入力して vRealize Automation を再起動します。

service vcac-server restart

組み込み vRealize Orchestrator インスタンスと関連付けられたサービスがある場合は、以下のコマンドを入力します。

service vco-restart restart

- 6 障害のあるサービスが **iaas-service** である場合は、次の手順を実行して再登録します。

- a このサービスは登録解除しないでください。
- b プライマリ IaaS Web サーバで、管理者権限を持つアカウントを使用してログインします。
- c 管理者としてコマンド プロンプトを開きます。
- d 次のコマンドを実行します。

```
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager
Data\Cafe\Vcac-Config.exe" RegisterSolutionUser -url
https://<appliance-or-load-balancer-IP-or-FQDN>/ -t vsphere.local -cu
administrator -cp <password> -f "C:\Program Files
(x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.data" -v
```

パスワードは、administrator@vsphere.local のパスワードです。

- e IaaS データベースの登録情報を更新するためのコマンドを実行します。

Windows 認証が設定された SQL Server :

```
"C:\Program Files (x86)\VMware\vCAC\Server\Model Manager
Data\Cafe\Vcac-Config.exe" MoveRegistrationDataToDb -s <IaaS-SQL-
server-IP-or-FQDN> -d <SQL-database-name> -f "C:\Program Files
(x86)\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.data" -v
```


ネイティブの SQL 認証が設定された SQL Server :

```
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager
Data\Cafe\Vcac-Config.exe" MoveRegistrationDataToDb -s <SQL-server-IP-
or-FQDN> -d <SQL-database-name> -su <SQL-user> -sp <SQL-user-password>
-f "C:\Program Files (x86)\VMware\VCAC\Server\Model Manager
Data\Cafe\Vcac-Config.data" -v
```

サーバまたはデータベースの名前を見つけるには、テキスト エディタで次のファイルを調べ、**repository** を検索します。データ ソースと初期カタログの値には、それぞれサーバ アドレスとデータベース名が含まれています。

```
C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Web\Web.config
```

SQL ユーザーには、データベースに対する DBO 権限が必要です。

- f 次のコマンドを実行して、エンドポイントを登録します。

```
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://<IaaS-Web-server-or-load-balancer-IP-or-
FQDN> /vcac --Endpoint ui -v
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://<IaaS-Web-server-or-load-balancer-IP-or-
FQDN> /WAPI --Endpoint wapi -v
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://<IaaS-Web-server-or-load-balancer-IP-or-
FQDN> /repository --Endpoint repo -v
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe"
RegisterEndpoint --EndpointAddress https://<IaaS-Web-server-or-load-balancer-IP-or-
FQDN> /WAPI/api/status --Endpoint status -v
```

- g 次のコマンドを実行してカタログ アイテムを登録します。

```
"C:\Program Files (x86)\VMware\VCAC\Server\Model Manager
Data\Cafe\Vcac-Config.exe" RegisterCatalogTypesAsync -v
```

- h IIS を再起動します。

```
iisreset
```

- i プライマリ IaaS Manager Service ホストにログインします。

- j vRealize Automation Windows サービスを再起動します。

VMware vCloud Automation Center Service

- 7 外部 vRealize Orchestrator インスタンスなどの外部システムと関連付けられたサービスを再登録するには、外部システムにログインしてそのサービスを再起動します。

追加の NIC によって管理インターフェイスのエラーが発生する

vRealize Automation アプライアンスに 2 つ目のネットワーク インターフェイス カード (NIC) を追加した後、一部の vRealize Automation 管理インターフェイスのページが正常にロードされません。

問題

vCenter Server を使用して 2 番目の NIC を正常に追加した後、次の vRealize Automation 管理インターフェイスのページがロードされず、エラーが表示されます。

- [ネットワーク]-[ステータス] ページには、スクリプトが応答していないことを示すエラーが表示されます。
- [ネットワーク]-[アドレス] ページでは、ネットワーク インターフェイス情報の読み取りに失敗したというエラーが表示されます。

原因

バージョン 7.3 以降の vRealize Automation アプライアンスでは、2 つの NIC がサポートされます。ただし、アプライアンスの基盤となっているエンジニア テンプレートでは、ソリューションを適用しない限り管理インターフェイスは適切に動作しません。

ソリューション

NIC を追加した後、vRealize Automation アプライアンスを再起動します。

セカンダリ仮想アプライアンスをマスターに昇格できない

vRealize Automation では、仮想アプライアンスのメモリ不足が原因で、クラスタ内の仮想アプライアンスを昇格できない場合があります。

問題

マスター ノードでメモリ不足が発生している場合です。管理インターフェイスの [データベース] ページにログインし、セカンダリ ノードを新しいマスターに昇格させます。次のようなエラーが発生します。

```
Fail to execute on Node <node-name>, host is <master-FQDN>
because of: Could not read remote lock command result for node: <node-name>
on address: <master-FQDN>, reason is: 500 Internal Server Error
```

原因

新たに昇格したマスターへの再構成を、すべてのノードから確認できる場合にのみ、昇格が成功します。すべてのノードにアクセス可能でも、メモリ不足のために旧マスターが確認できません。

ソリューション

メモリ不足のマスター ノードをパワーオフします。セカンダリ ノード管理インターフェイスの [データベース] ページにログインし、セカンダリ ノードを昇格します。

Active Directory 同期ログの保持期間が短すぎる

vRealize Automation の Active Directory 同期ログには、数日分のみが記録されます。

問題

2 日が経過すると、Active Directory 同期ログは管理インターフェイスから削除されます。ログのフォルダも、次の vRealize Automation アプライアンス ディレクトリから削除されます。

`/db/elasticsearch/horizon/nodes/0/indices`

原因

容量を節約するため、vRealize Automation では Active Directory 同期ログの最長保持期間が 3 日間に設定されています。

ソリューション

- 1 vRealize Automation アプライアンスのコンソール セッションに root としてログインします。
- 2 テキスト エディタで次のファイルを開きます。
`/usr/local/horizon/conf/runtime-config.properties`
- 3 `analytics.maxQueryDays` プロパティの値を増やします。
- 4 `runtime-config.properties` を保存して、閉じます。
- 5 Identity Manager と Elasticsearch サービスを再起動します。

```
service horizon-workspace restart
service elasticsearch restart
```

RabbitMQ でホスト名を解決できない

RabbitMQ はデフォルトで vRealize Automation アプライアンスに対してホストの省略名を使用します。これにより、ノードが相互に解決されない可能性があります。

問題

別の vRealize Automation アプライアンスをクラスタに追加しようとする、次のようなエラーが発生します。

```
Clustering node 'rabbit@sc2-rdops-vm01-dhcp-62-2' with rabbit@company ...
Error: unable to connect to nodes [rabbit@company]: nodedown

DIAGNOSTICS
=====

attempted to contact: [rabbit@company]

rabbit@company:
  * unable to connect to epmd (port 4369) on company: nxdomain (non-existing domain)

current node details:
- node name: 'rabbitmq-cli-11@sc2-rdops-vm01-dhcp-62-2'
- home dir: /var/lib/rabbitmq
- cookie hash: 4+kP1tKnxGYaGjrPL2C8bQ==

[2017-09-01 14:58:04] [root] [INFO] RabbitMQ join failed with exit code: 69, see RabbitMQ
logs for details.
```

原因

このネットワーク構成では、ホストの省略名による vRealize Automation アプライアンスの相互解決はできません。

ソリューション

- 1 環境内のすべての vRealize Automation アプライアンスで、コンソール セッションに root としてログインします。

- 2 RabbitMQ サービスを停止します。

```
service rabbitmq-server stop
```

- 3 テキスト エディタで次のファイルを開きます。

```
/etc/rabbitmq/rabbitmq-env.conf
```

- 4 次のプロパティを True に設定します。

```
USE_LONGNAME=true
```

- 5 `rabbitmq-env.conf` を保存して閉じます。

- 6 RabbitMQ をリセットします。

```
vcac-vami rabbitmq-cluster-config reset-rabbitmq-node
```

- 7 1 台の vRealize Automation アプライアンス ノードで、次のスクリプトを実行します。

```
vcac-config cluster-config-ping-nodes --services rabbitmq-server
```

- 8 すべてのノードで RabbitMQ サービスが開始されていることを確認します。

```
vcac-vami rabbitmq-cluster-config get-rabbitmq-status
```

IaaS コンポーネントのトラブルシューティング

vRealize Automation IaaS コンポーネントのトラブルシューティングに関するトピックでは、vRealize Automation を使用するときが発生する可能性がある潜在的なインストール関連の問題に対するソリューションを提供します。

前提条件となる修正で .NET の機能をインストールできない

vRealize Automation の前提条件チェッカーの [修正] オプションが失敗し、.NET 3.5.1 のインストール元が見つからないというメッセージが表示されます。

問題

前提条件チェッカーでは、Windows Server 2008 R2 システムの場合は IIS 7.5、Windows Server 2012 R2 システムの場合は IIS 8 の要件をそれぞれ満たすために、.NET 3.5.1 がインストールされていることを確認する必要があります。

原因

Windows Server 2012 R2 では、インターネットに接続できないと .NET を自動インストールできないことがあります。また、一部の Windows 2012 R2 更新プログラムによってインストールが妨げられることもあります。この問題は、このバージョンの Windows に .NET Framework 3.5 のインストール元となるローカル コピーがないために発生します。

ソリューション

.NET Framework 3.5 のインストール元を手動で指定します。

- 1 Windows ホストで、Windows Server 2012 R2 のインストール メディアの ISO イメージをマウントします。
- 2 Server Manager で、役割と機能の追加ウィザードを使用して .NET Framework 3.5 を有効にします。
- 3 ウィザードで、ISO メディアに含まれている .NET Framework 3.5 のインストール パスに移動します。
- 4 .NET Framework 3.5 を追加したら、vRealize Automation の前提条件チェッカーを再実行します。

laaS のサーバ証明書の検証

vcac-Config.exe コマンドを使用して、laaS サーバが vRealize Automation アプライアンスおよび SSO アプライアンスの証明書を受け入れることを検証できます。

問題

laaS 機能を使用しているときに、認証エラーが発生します。

原因

laaS が他のコンポーネントからのセキュリティ証明書を認識しないと、認証エラーが発生する可能性があります。

ソリューション

- 1 管理者としてコマンド プロンプトを開き、<vra-installation-dir>\Server\Model Manager Data\Cafe (通常は C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Data\Cafe) の Cafe ディレクトリに移動します。
- 2 **Vcac-Config.exe CheckServerCertificates -d [<vra-database>] -s [<vRA SQL server>] -v** の形式でコマンドを入力します。オプションのパラメータは、**-su [<SQL user name>]** と **-sp [<password>]** です。

コマンドが成功すると、次のメッセージが表示されます。

```
Certificates validated successfully.
Command succeeded.
```

コマンドが失敗すると、詳細なエラー メッセージが表示されます。

注: このコマンドは、Model Manager Data コンポーネントのノードでのみ使用できます。

laaS インストーラ実行時の認証情報エラー

laaS コンポーネントをインストールすると、仮想アプライアンスの認証情報の入力時にエラーが発生します。

問題

laaS インストーラの認証情報を入力した後に、**org.xml.sax.SAXParseException** エラーが表示されます。

原因

不正な認証情報または認証情報形式が使用されました。

ソリューション

- ◆ 正しいテナント値とユーザー名の値を使用していることを確認してください。

たとえば、SSO のデフォルト テナントでは、administrator@vsphere.local ではなく vsphere.local などのドメイン名を使用します。

laaS のインストール中に設定の保存の警告が表示される

laaS インストール中にメッセージが表示されます。警告: IaaS インストール中に仮想アプライアンスに設定を保存できませんでした。

問題

laaS インストール中に、ユーザー設定が保存されなかったことを示す確ではないエラー メッセージが表示されます。

原因

通信またはネットワークの問題によりこのメッセージが誤って表示されます。

ソリューション

エラー メッセージを無視してインストールを続行します。このメッセージにより、セットアップが失敗することはありません。

Web サイト サーバおよび Distributed Execution Manager のインストールに失敗する

laaS サービス アカウントのパスワードに二重引用符が含まれていると、vRealize Automation アプライアンス インフラストラクチャの Web サイト サーバおよび Distributed Execution Manager のインストールを続行できません。

問題

無効な msixexec パラメータが原因で、vRealize Automation アプライアンスの Distributed Execution Manager (DEM) および Web サイト サーバのインストールが失敗したことを示すメッセージが表示されます。

原因

laaS サービス アカウントのパスワードで、二重引用符が使用されています。

ソリューション

- 1 laaS サービス アカウントのパスワードに、二重引用符が含まれていないことを確認します。
- 2 パスワードに二重引用符が含まれている場合は、新しいパスワードを作成します。
- 3 インストールを再開します。

laaS Web と Model Management のインストール中に laaS 認証に失敗する

前提条件チェッカーの実行中に、IIS 認証チェックに失敗したことを示すメッセージが表示されます。

問題

認証は有効になっていないが、IIS 認証チェック ボックスがオンになっていることを示すメッセージが表示されます。

ソリューション

- 1 [Windows 認証] チェック ボックスをオフにします。
- 2 [保存] をクリックします。
- 3 [Windows 認証] チェック ボックスをオンにします。
- 4 [保存] をクリックします。
- 5 前提条件チェッカーを再実行します。

Model Manager Data および Web コンポーネントのインストールに失敗した

IaaS インストーラが Model Manager Data コンポーネントおよび Web コンポーネントを保存できない場合、vRealize Automation インストールに失敗する可能性があります。

問題

次のメッセージが表示されて、インストールが失敗します。

IaaS インストーラは Model Manager Data および Web コンポーネントの保存に失敗しました。

原因

失敗には潜在的な原因がいくつかあります。

- vRealize Automation アプライアンスへの接続の問題、またはアプライアンス間の接続の問題。応答がないまたは接続ができなかったために、接続の試行は失敗します。
- 分散構成の使用時の、IaaS での信頼性のある証明書の問題。
- 分散構成での証明書名の不一致。
- 証明書が無効であるか、証明書チェーンにエラーがある。
- リポジトリ サービスの起動の失敗。
- 分散環境でのロード バランサの不正な構成。

ソリューション

- 接続性

Web ブラウザで vRealize Automation の URL に接続できることを確認します。

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

- 信頼性のある証明書の問題

- IaaS において、コマンド **mmc.exe** を使用して Microsoft 管理コンソールを開き、インストールに使用された証明書がマシンの信頼されたルート証明書ストアに追加されていることを確認します。
- Web ブラウザから以下の URL にアクセスして、MetaModel サービスのステータスを確認し、証明書のエラーがないことを確認します。

`https://<FQDN-or-IP>/repository/data/MetaModel.svc`

■ 証明書名の不一致

このエラーは、証明書が特定の名前に対して発行され、異なった名前または IP アドレスが使用された場合に発生する場合があります。証明書名の不一致のエラーはインストール中に、[証明書の不一致の抑止] を選択すると抑止できます。

また、[証明書の不一致の抑止] オプションを使用すると、リモート証明書失効リストの一致エラーを無視することもできます。

■ 無効な証明書

コマンド **mmc.exe** を使用して Microsoft 管理コンソールを開きます。証明書の期限が切れておらず、ステータスが正常であることを確認します。これを証明書チェーンのすべての証明書に対して行います。証明書の階層を使用しているときには、このチェーンの他の証明書を信頼されたルート証明書ストアにインポートする必要があります。

■ リポジトリ サービス

次の操作を行って、リポジトリ サービスのステータスを確認します。

- Web ブラウザから以下の URL にアクセスして、MetaModel サービスのステータスを確認します。

`https://<FQDN-or-IP>/repository/data/MetaModel.svc`

- **Repository.log** をエラーがないか確認します。
- Web サイト（リポジトリ、vRealize Automation または WAPI）上にホストされたアプリケーションに問題がある場合、IIS をリセット (**iisreset**) します。
- 追加のログ情報について、<%SystemDrive%>\inetpub\logs\LogFiles の Web サイト ログを確認します。
- 要件の確認時に前提条件チェッカーがパスしたことを確認します。
- Windows 2012 で .NET Framework の下の WCF サービスがインストールされ、HTTP アクティブ化がインストールされていることを確認します。

IaaS Windows サーバは FIPS をサポートしない

連邦情報処理規格 (FIPS) が有効な場合、インストールが成功しません。

問題

IaaS Web コンポーネントのインストール中に次のエラーが発生してインストールが失敗します。

この実装は Windows プラットフォーム FIPS 検証暗号化アルゴリズムの一部ではありません。

原因

vRealize Automation IaaS は、FIPS がサポートされない Microsoft Windows Communication Foundation (WCF) に組み込まれています。

ソリューション

IaaS Windows サーバで、FIPS ポリシーを無効にします。

- 1 [スタート > コントロール パネル > 管理ツール > ローカル セキュリティ ポリシー] に移動します。
- 2 [グループ ポリシー] ダイアログの [ローカル ポリシー] の下で、[セキュリティ オプション] を選択します。
- 3 次のエントリを見つけて無効にします。

システム暗号化：暗号化、ハッシュ、署名のための FIPS 準拠アルゴリズムを使う

XaaS エンドポイントを追加すると内部エラーが発生する

XaaS エンドポイントを作成しようとすると、内部エラー メッセージが表示されます。

問題

エンドポイントの作成に失敗し、次の内部エラー メッセージが表示されます。**内部エラーが発生しました。問題が解決しない場合は、システム管理者にお問い合わせください。その際、次の参照番号を使用してください： <c0DD0C01>。**参照コードはランダムに生成され、特定のエラー メッセージにリンクされるものではありません。

ソリューション

- 1 vRealize Automation アプライアンス ログ ファイルを開きます。
`/var/log/vcac/catalina.out`
- 2 エラー メッセージに表示された参照コードを検索します。
たとえば、<c0DD0C01> などです。
- 3 ログ ファイル内で参照コードを検索して、関連付けられたエントリを見つけます。
- 4 関連付けられたエントリの前後のエントリを確認して、問題のトラブルシューティングを実行します。
関連付けられたログ エントリには、問題の明確な原因は記述されていません。

プロキシ エージェントのアンインストールに失敗する

Windows インストーラ ロギングが有効になっていると、プロキシ エージェントの削除に失敗することがあります。

問題

Windows コントロール パネルでプロキシ エージェントをアンインストールしようとすると、アンインストールに失敗して次のエラーが表示されます。

Error opening installation log file. Verify that the specified log file location exists and is writable

原因

この問題は、Windows インストーラ ロギングは有効になっているが、Windows インストーラ エンジンがアンインストール ログ ファイルに正しく書き込むことができない場合に発生します。詳細については、『[Microsoft ナレッジ ベースの記事 2564571](#)』を参照してください。

ソリューション

- 1 マシンを再起動するか、タスク マネージャから explorer.exe を再起動します。
- 2 エージェントをアンインストールします。

リモート トランザクションが無効のときにマシン申請に失敗する

Windows サーバ マシンで Microsoft 分散トランザクション コーディネーター サービス (DTC) のリモート トランザクションが無効になっていると、マシン申請が失敗します。

問題

Model Manager ポータルまたは SQL Server でリモート トランザクションが無効になっているときにマシンをプロビジョニングすると、申請は完了しません。データ収集に失敗し、マシン申請の状態は CloneWorkflow のままになります。

原因

DTC リモート トランザクションは、vRealize Automation システムが使用する IaaS SQL インスタンスで無効にされます。

ソリューション

- 1 Windows Server Manager を起動し、すべての vRealize サーバおよび関連付けられた SQL Server で DTC を有効にしてください。

Windows 7 では、[スタート] - [管理ツール] - [コンポーネント サービス] に移動します。

注: すべての Windows サーバの MSDTC 構成での SID が一意になるようにします。

さらに、IaaS Manager Service ホストでは、IaaS SQL Server データベース ホストの NETBIOS 名を解決する必要があります。NETBIOS 名を解決できない場合は、Manager Service マシンの **/etc/hosts** ファイルに、SQL Server の NETBIOS 名を追加し、Manager Service を再起動します。

- 2 すべてのノードを開き、ローカル DTC を見つけるか、クラスタ システムを使用する場合はクラスタ化 DTC を見つけます。

[コンポーネント サービス] - [コンピューター] - [マイ コンピューター] - [分散トランザクション コーディネーター] に移動します。

- 3 ローカルまたはクラスタ化 DTC を右クリックし、[プロパティ] を選択します。
- 4 [セキュリティ] タブをクリックします。
- 5 [ネットワーク DTC アクセス] オプションをオンにします。
- 6 [リモート クライアントを許可する] オプションと [リモート管理を許可する] オプションをオンにします。
- 7 [受信を許可する] オプションと [送信を許可する] オプションをオンにします。
- 8 DTC ログオン アカウントの [アカウント] フィールドで、NT AUTHORITY\Network Service と入力するか、または選択します。
- 9 [OK] をクリックします。

10 CloneWorkflow 状態のままになっているマシンを削除します。

- a vRealize Automation 製品インターフェイスにログインします。
`https://<vrealize-automation-appliance-FQDN>/vcac/org/<tenant-name>`
- b [インフラストラクチャ] - [管理対象マシン] に移動します。
- c ターゲット マシンを右クリックします。
- d [削除] を選択してマシンを削除します。

Manager Service 通信のエラー

DTC が既にインストールされているテンプレートからクローン作成された IaaS サーバには、DTC の重複した識別子が含まれ、これによりノード間の通信が妨げられます。

問題

IaaS Manager Service に障害が発生し、次のエラーが Manager Service ログにポストされます。

基礎となるトランザクション マネージャとの通信に失敗しました。----> System.Runtime.InteropServices.COMException: MSDTC トランザクション マネージャは、通信に問題が発生したため、ソース トランザクション マネージャからトランザクションを引き出すことができませんでした。
 考えられる原因: ファイアウォールが設けられており、MSDTC プロセスの例外が設定されていない、2 台のマシンが NetBIOS 名で相互に検出できない、または 2 つのトランザクション マネージャのいずれかでネットワーク トランザクションのサポートが有効に設定されていないためです。

原因

DTC が既にインストールされている IaaS サーバのクローンを作成すると、そのクローンには DTC の同じ一意の識別子が親として含まれます。2 台のマシン間の通信が失敗します。

ソリューション

- 1 クローンで、管理者としてコマンド プロンプトを開きます。
- 2 次のコマンドを実行します。

```
msdtc -uninstall
```

- 3 クローンを再起動します。
- 4 別のコマンド プロンプトを開き、次のコマンドを実行します。

```
msdtc -install <manager-service-host-FQDN>
```

変更された電子メールのカスタマイズ動作

vRealize Automation 6.0 以降の場合、以前のバージョンの電子メール テンプレート機能を使用してカスタマイズできるのは、IaaS コンポーネントによって生成された通知のみです。

ソリューション

次の XSLT テンプレートを使用できます。

- ArchivePeriodExpired
- EpiRegister

- EpiUnregister
- LeaseAboutToExpire
- LeaseExpired
- LeaseExpiredPowerOff
- ManagerLeaseAboutToExpire
- ManagerLeaseExpired
- ManagerReclamationExpiredLeaseModified
- ManagerReclamationForcedLeaseModified
- ReclamationExpiredLeaseModified
- ReclamationForcedLeaseModified
- VdiRegister
- VdiUnregister

電子メール テンプレートは、サーバのインストール ディレクトリの **\Templates** ディレクトリ（通常は、< %SystemDrive%\Program Files x86\VMware\VCAC\Server）にあります。 **\Templates** ディレクトリには XSLT テンプレートもありますが、すでにサポートされていないので変更できません。

ログイン エラーのトラブルシューティング

vRealize Automation のログイン エラーのトラブルシューティングに関するトピックでは、vRealize Automation を使用するときが発生する可能性のある潜在的なインストール関連の問題に対する解決策を提供します。

誤った UPN 形式の認証情報を使用して IaaS 管理者としてログインを試みると説明もなく失敗する

IaaS 管理者として vRealize Automation へのログインを試みると、説明もなくログイン ページにリダイレクトされます。

問題

ユーザー名に @<yourdomain> の部分を含めない UPN 認証情報を使用して IaaS 管理者として vRealize Automation にログインしようとすると、即座に SSO からログアウトされ、説明なくログイン ページにリダイレクトされます。

原因

入力する UPN は、<yourname>.admin@<yourdomain> の形式に準拠する必要があります。たとえば、ユーザー名として jsmith.admin@sqa.local を使用してログインし、Active Directory の UPN に jsmith.admin のみが設定されていると、ログインは失敗します。

ソリューション

この問題を修正するには、必要な @<yourdomain> を含めて **userPrincipalName** 値を変更し、ログインを再試行します。この例では、UPN 名を jsmith.admin@sqa.local にする必要があります。この情報は **log/vcac** フォルダのログ ファイルに提供されています。

高可用性でログインに失敗する

vRealize Automation アプライアンスが 1 つ以上ある場合、各アプライアンスは短いホスト名によって相互に識別できる必要があります。識別できないと、ログインすることができません。

問題

追加の vRealize Automation アプライアンスをインストールして、vRealize Automation を高可用性向けに構成します。vRealize Automation へのログインを試みると、無効なライセンスに関するメッセージが表示されます。ただし、ライセンスが有効であることは確認済みなので、このメッセージは誤りです。

原因

vRealize Automation アプライアンス ノードは、クラスタ内の各ノードの短いホスト名を解決できないと、高可用性クラスタを正しく構成しません。

ソリューション

高可用性 vRealize Automation アプライアンスのクラスタが短いホスト名を解決できるようにするには、以下の方法のいずれかを実行します。クラスタ内のすべてのアプライアンスを変更する必要があります。

手順

- `/etc/resolv.conf` で検索行を編集または作成します。この行には、vRealize Automation アプライアンスを保持するドメインを含める必要があります。複数のドメインはスペースで区切ります。例：


```
search sales.mycompany.com support.mycompany.com
```
- `/etc/resolv.conf` でドメイン行を編集または作成します。各行には、vRealize Automation アプライアンスを保持するドメインを含める必要があります。例：


```
domain support.mycompany.com
```
- 各 vRealize Automation アプライアンスの短縮名がそのアプライアンスの完全修飾ドメイン名にマッピングされるように、`/etc/hosts` ファイルに行を追加します。例：

```
node1    node1.support.mycompany.com
node2    node2.support.mycompany.com
```

プロキシが原因で VMware Identity Manager ユーザーがログインできない

プロキシを使用するための設定によって、VMware Identity Manager ユーザーがログインできない場合があります。

問題

プロキシ サーバ経由でネットワークにアクセスするように vRealize Automation を設定すると、VMware Identity Manager ユーザーがログインしようとしたときに、次のエラーが表示されます。

Error Unable to get metadata

ソリューション

前提条件

プロキシ サーバ経由でネットワークにアクセスするように vRealize Automation を設定します。[「プロキシ サーバを介したネットワークへの接続」](#) を参照してください。

手順

- 1 vRealize Automation アプライアンスのコンソールに root としてログインします。
- 2 テキスト エディタで次のファイルを開きます。
/etc/sysconfig/proxy
- 3 VMware Identity Manager のログインではプロキシ サーバが無視されるように **NO_PROXY** 行を更新します。

NO_PROXY=<vrealize-automation-hostname>

たとえば、**NO_PROXY="localhost, 127.0.0.1, automation.mycompany.com"** のように指定します。

- 4 **proxy** を保存して閉じます。
- 5 次のコマンドを入力して、Horizon ワークスペース サービスを再起動します。

service horizon-workspace restart

vRealize Automation のアップグレード

既存の vRealize Automation 環境から最新バージョンにアップグレードできます。

既存の vRealize Automation 環境に応じて、インプレース アップグレードまたはサイドバイサイド アップグレードを実行することで、最新バージョンにアップグレードできます。環境に最適なアップグレード方法を決定するために、このページで情報を確認します。

インプレース アップグレードには、複数の手順が必要です。既存環境のさまざまなコンポーネントを、指定された順序でアップデートします。すべての製品コンポーネントを同一バージョンにアップグレードする必要があります。インプレース アップグレードは、次のアップグレード パスでのみ実行できます。

- vRealize Automation 6.2.5 から 7.4
- vRealize Automation 7.1 から 7.4
- vRealize Automation 7.2 から 7.4
- vRealize Automation 7.3.x から 7.4

サイドバイサイド アップグレードでは、vRealize Automation の最新バージョンが展開されているターゲット環境に、既存の vRealize Automation 環境のデータを移行します。サイドバイサイド アップグレードは、次のアップグレード パスで実行できます。

- vRealize Automation 6.2.0 - 6.2.5 から 7.4
- vRealize Automation 7.0 および 7.0.1 から 7.4

■ vRealize Automation 7.1、7.2、7.3.x から 7.4

移行を行う場合、既存の環境が変更されることはありません。既存の環境が、vCloud Director、vCloud Air に統合されている場合、または物理的なエンドポイントがある場合は、アップグレード時に移行を行う必要があります。移行により、サポートされていないすべてのエンドポイントと、これらに関連付けられたすべての要素がターゲット環境から削除されます。

次の表で現在の vRealize Automation バージョンを見つけます。右側のドキュメントを使用して、vRealize Automation 環境の最新バージョンへのアップグレードを実行します。

表 1-45. サポートされる vRealize Automation 7.4 へのアップグレード パス

| 現在インストールされているバージョン | 増分アップグレードのためのドキュメント |
|---|--|
| vRealize Automation 7.1、7.2、または 7.3.x | これらのトピックのいずれかを参照してください。 <ul style="list-style-type: none"> ■ 「vRealize Automation 7.1 以降から 7.4 へのアップデート」 ■ 「vRealize Automation 7.4 への移行」 |
| vRealize Automation 7.0 または 7.0.1 | 「vRealize Automation 7.4 への移行」 を参照してください。 |
| vRealize Automation 6.2.5 | これらのトピックのいずれかを参照してください。 <ul style="list-style-type: none"> ■ 「vRealize Automation 6.2.5 から 7.4 へのアップグレード」 ■ 「vRealize Automation 7.4 への移行」 |
| vRealize Automation 6.2.0、6.2.1、6.2.2、6.2.3、6.2.4 | 「vRealize Automation 7.4 への移行」 を参照してください。 |

次の表には、以前の vCloud Automation Center リリースからのアップグレードに関する情報が記載されています。vRealize Automation の最新バージョンにアップグレードする前に、vRealize Automation 6.2.5 にアップグレードする必要があります。<https://www.vmware.com/support/pubs/vcac-pubs.html> に、vCloud Automation Center と vRealize Automation のバージョン 5.x および 6.x に関するドキュメントへのリンクがあります。

表 1-46. サポートされている vRealize Automation 6.2.5 へのアップグレード パス

| 現在インストールされているバージョン | 増分アップグレードのためのドキュメント |
|--------------------------------|--|
| vCloud Automation Center 6.0 | 次の順序でアップグレードを実行します。 <ol style="list-style-type: none"> 1 vCloud Automation Center 6.0 から 6.0.1 へのアップグレード 2 vCloud Automation Center 6.1 へのアップグレード 3 vRealize Automation 6.2.x へのアップグレード |
| vCloud Automation Center 6.0.1 | 次の順序でアップグレードを実行します。 <ol style="list-style-type: none"> 1 vCloud Automation Center 6.1 へのアップグレード 2 vRealize Automation 6.2.x へのアップグレード |
| vCloud Automation Center 6.1.x | vRealize Automation 6.2.x へのアップグレード |
| vRealize Automation 6.2.x | 『vRealize Automation 6.2.x へのアップグレード』で説明されている方法で、6.2.5 リリースに直接アップグレードします。 |

注: vCloud Automation Center は、バージョン 6.2.0 で vRealize Automation に商標変更されました。ユーザーインターフェイスとサービス名のみが変更されています。**vcac** が含まれるディレクトリ名とプログラム名は変更されていません。

6.2.x 環境からアップグレードする場合は、次の項目を参照してください。

- VMware vRealize Production Test Upgrade Assessment Tool は、vRealize Automation 6.2.x 環境を分析してアップグレードに関する問題を引き起こす可能性がある機能構成を特定し、使用環境のアップグレード準備ができていることを確認します。このツールおよび関連ドキュメントをダウンロードするには、[VMware vRealize Production Test Tool](#) の製品のダウンロード ページに移動します。
- vRealize Automation 6.2.x 環境から最新バージョンの vRealize Automation にアップグレードすると、変更されたさまざまな機能を利用できるようになります。詳細については、「[この vRealize Automation バージョンへのアップグレードに関する考慮事項](#)」を参照してください。
- vRealize Automation 6.2.x 環境をカスタマイズしている場合には、CCE サポート スタッフに連絡してアップグレードの考慮事項に関する追加情報を確認してください。
- アップグレード後にサポートされないプロパティ ディクショナリの制御は、vRealize Orchestrator およびプロパティ ディクショナリを使用して復元することができます。
- 元の環境に廃止されたコードを含むワークフローがある場合は、『[vRealize Automation Extensibility Migration Guide](#)』に掲載されている、イベント ブローカ サブスクリプションへの変換に必要なコード変更に関する情報を参照してください。

vRealize Automation 6.2.0 からアップグレードする際に既知の問題を回避するには、アップグレードする前に、各 IaaS Web サイト ノードに対して次の手順を実行します。この問題は 6.2.0 にのみ影響します。他の 6.2.x バージョンは影響を受けません。

- 1 管理者権限でメモ帳を開きます。[スタート] で [メモ帳] アイコンを右クリックし、[管理者として実行] を選択します。
- 2 次のファイルを開きます。
`C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Web\web.config`
- 3 ファイル内で次の文を見つけます。
`<!-- add key="DisableMessageSignatureCheck" value="false"-->`
- 4 文のコメントを解除し、値を `false` から `true` に変更します。
`<add key="DisableMessageSignatureCheck" value="true" />`
- 5 ファイルを保存します。
メモ帳で **名前を付けて保存** が表示された場合は、管理者としてメモ帳を開いていません。手順 1 に戻る必要があります。
- 6 管理者権限でコマンド プロンプトを開きます。[スタート] で [コマンド プロンプト] アイコンを右クリックし、[管理者として実行] を選択します。
- 7 リセットを実行します。
- 8 すべての Web サイト ノードに対して手順 1 ～ 7 を繰り返します。

vRealize Automation 7.1 以降から 7.4 へのアップデート

vRealize Automation 7.1 以降の環境を最新バージョンにアップデートする場合は、7.1 以降の環境に固有のアップデート手順を使用します。

これは vRealize Automation 7.1 以降から 7.4 へのアップデートに固有の情報です。他のサポート対象のアップグレードパスについては、[「vRealize Automation のアップグレード」](#)を参照してください。

vRealize Automation 7.1、7.2、または 7.3.x の 7.4 へのアップグレード

現在の vRealize Automation 7.1、7.2、または 7.3.x 環境を 7.4 にアップグレードすることができます。環境のアップグレードには、このバージョンに固有のアップグレード手順を使用します。

インプレース アップグレードは 3 段階のプロセスです。次の順序で、現在の環境のコンポーネントをアップグレードします。

- 1 vRealize Automation アプライアンス
- 2 IaaS Web サーバ
- 3 vRealize Orchestrator

すべての製品コンポーネントを同一バージョンにアップグレードする必要があります。

vRealize Automation 7.2 以降、JFrog Artifactory Pro は vRealize Automation アプライアンスにはバンドルされなくなりました。vRealize Automation の以前のバージョンからアップグレードする場合、アップグレード プロセスで JFrog Artifactory Pro は削除されます。詳細については、[ナレッジベースの記事 KB2147237](#)を参照してください。

vRealize Automation のアップグレードの前提条件

vRealize Automation 7.1、7.2、7.3.x 環境の 7.4 へのアップグレードを実行する前に、次の前提条件を確認します。

システム構成要件

アップグレードを開始する前に、次の前提条件が完了していることを確認します。

- 環境内のアプライアンスとサーバのすべてが、最新バージョンのシステム要件を満たしているか確認します。
[VMware vRealize Automation のドキュメント](#)の vRealize Automation サポート マトリックスを参照してください。
- VMware の他の製品との互換性の詳細については、VMware Web サイトの VMware 製品の相互運用性マトリックスを参照してください。
- アップグレードする vRealize Automation の動作状況が安定していることを確認します。アップグレード前にすべての問題を修正します。
- ロード バランサのタイムアウト設定を、デフォルト設定から 10 分以上に変更したことを確認します。

ハードウェア構成要件

お使いの環境のハードウェアが vRealize Automation 7.4 に適していることを確認します。

[「vRealize Automation のハードウェア仕様および最大容量」](#)を参照してください。

アップグレードを開始する前に、次の前提条件が完了していることを確認します。

- アップグレードを実行するには、少なくとも 18 GB の RAM、4 つの CPU、Disk1 = 50 GB、Disk3=25 GB、Disk4=50 GB が必要です。

仮想マシンが vCloud Networking and Security 上に配置されている場合は、多くの RAM 容量の割り当てが必要になる場合があります。

vCloud Networking and Security の一般的なサポートは終了しましたが、VCNS カスタム プロパティは NSX の用途に対して引き続き有効です。詳細については、[ナレッジベースの記事 KB2144733](#) を参照してください。

- これらのノードには、少なくとも 5 GB の空きディスク容量が必要です。
 - プライマリ IaaS Web サイト
 - Microsoft SQL データベース
 - Model Manager
- Model Manager Data がインストールされているプライマリ IaaS Web サイト ノードに、JAVA SE Runtime Environment 8 Update 161 (64 ビット) 以降がインストールされている必要があります。Java をインストールした後、JAVA_HOME 環境変数に新しいバージョンを設定する必要があります。
- アップグレードをダウンロードして実行するには、次のリソースが必要です。
 - ルートパーティションに少なくとも 5 GB
 - マスター vRealize Automation アプライアンスの **/storage/db** パーティションに 5 GB
 - 各レプリカ仮想アプライアンスのルートパーティションに 5 GB
- **/storage/log** サブフォルダを確認し、以前のアーカイブ ZIP ファイルがあれば削除して容量をクリーンアップします。

一般的な前提条件

アップグレードを開始する前に、次の前提条件が完了していることを確認します。

- アップグレードする前に、Windows IaaS システムに PowerShell 3.0 以降をインストールする必要があります。PowerShell 3.0 以降がインストールされていない場合、アップグレードは失敗します。
- Microsoft IIS がインストールされている場合は、IaaS Web サーバと Manager Service マシンで IISRESET を実行します。IISRESET を実行すると、起動モードで無効な IIS 依存サービスがないことが確認されます。
- vRealize Automation アップグレードの影響を受けるまたはこのアップグレードに参加する、すべてのデータベースおよびロード バランサにアクセスできる。
- アップグレードの実行中、ユーザーがシステムを使用できないようにする。
- vRealize Automation に対してクエリを実行するアプリケーションがあれば、それを無効にする。
- Microsoft 分散トランザクション コーディネーター (MSDTC) が、すべての vRealize Automation および関連する SQL サーバ上で有効であることを確認する。手順については、[ナレッジベースの記事 KB2089503](#) を参照してください。

- 組み込みの PostgreSQL データベースで構成されている分散環境をアップグレードする場合は、次の手順を実行します。
 - a レプリカ ホストをアップグレードする前に、マスター ホストで **pgdata** ディレクトリ内のファイルを調べます。
 - b マスター ホスト上の PostgreSQL データ フォルダ (`/var/vmware/vpostgres/current/pgdata/`) に移動します。
 - c **pgdata** ディレクトリ内で開かれているファイルがあればすべて閉じ、**.swp** サフィックスを持つすべてのファイルを削除します。
 - d このディレクトリ内のすべてのファイルの所有者 (`postgres:users`) が正しいことを確認します。

さらに、カスタム プロパティの名前にスペースが使用されていないことを確認します。vRealize Automation のこのリリースにアップグレードする前に、カスタム プロパティ名からスペース文字を削除します。たとえば、スペースをアンダースコア文字で置き換えます。これにより、アップグレードされた vRealize Automation 環境でカスタム プロパティが認識されるようになります。vRealize Automation カスタム プロパティ名にスペースは使用できません。この問題は、以前のリリースの vRealize Automation、vRealize Orchestrator、またはその両方で使用されるカスタム プロパティにスペースが含まれており、この vRealize Orchestrator をアップグレードした環境を使用する場合に影響があります。

vRealize Automation のアップグレード チェックリスト

vRealize Automation 7.1、7.2 または 7.3.x を 7.4 にアップデートする際は、vRealize Automation 内のすべてのコンポーネントを特定の順序で更新します。

アップグレードの順序は、アップグレードする対象が最小環境なのか、それとも複数の vRealize Automation アプライアンスがある分散環境なのかによって異なります。

アップグレードを完了するまでの作業を追跡するため、チェックリストを使用します。タスクは示された順序で行うようにしてください。

表 1-47. vRealize Automation 最小環境をアップグレードする場合のチェックリスト

| タスク | 方法 |
|--|--|
|  vRealize Automation 7.1、7.2、または 7.3.x を 7.4 にアップデートする前に、NSX ネットワークおよびセキュリティ インベントリ データ収集を実行します。これは vRealize Automation が NSX と統合されている場合のみ必要です。 | [vRealize Automation のアップグレード前の NSX ネットワークおよびセキュリティ インベントリ データ収集の実行] を参照してください。 |
|  現在のインストール環境をバックアップする。これは重要な手順です。 | システムのバックアップ方法とリストア方法の詳細については、 「既存の vRealize Automation 環境のバックアップ」 を参照してください。 一般情報については、 http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf の「Symantec Netbackup を使用したバックアップとリストアの構成」を参照してください。 |
|  vRealize Automation アプライアンスにアップデートをダウンロードする。 | [vRealize Automation アプライアンスの更新のダウンロード] を参照してください。 |
|  vRealize Automation アプライアンスと IaaS コンポーネントのアップデートをインストールする。 | [vRealize Automation アプライアンスと IaaS コンポーネントへのアップデートのインストール] を参照してください。 |

表 1-48. vRealize Automation 分散環境をアップグレードする場合のチェックリスト

| タスク | 方法 |
|---|--|
|  vRealize Automation 7.1、7.2、または 7.3.x を 7.4 にアップグレードする前に、NSX ネットワークおよびセキュリティ インベントリ データ収集を実行します。これは vRealize Automation が NSX と統合されている場合のみ必要です。 | [vRealize Automation のアップグレード前の NSX ネットワークおよびセキュリティ インベントリ データ収集の実行] を参照してください。 |
|  現在のインストールをバックアップする。これは重要な手順です。 | システムのバックアップ方法とリストア方法の詳細については、「 既存の vRealize Automation 環境のバックアップ 」を参照してください。 詳細情報については、 http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf の「Symantec Netbackup を使用したバックアップとリストアの構成」(Configuring Backup and Restore by Using Symantec Netbackup) を参照してください。 |
|  vRealize Automation 7.3.x からアップグレードする場合は、PostgreSQL の自動フェイルオーバーを無効にします。 | [vRealize Automation PostgreSQL レプリケーション モードの非同期設定] を参照してください。 |
|  vRealize Automation アプライアンスにアップデートをダウンロードする。 | [vRealize Automation アプライアンスの更新のダウンロード] を参照してください。 |
|  ロード バランサを無効にする。 | ロード バランサのドキュメントを参照してください。 |
|  マスター vRealize Automation アプライアンスと IaaS コンポーネントのアップデートをインストールする。 | [vRealize Automation アプライアンスと IaaS コンポーネントへのアップデートのインストール] を参照してください。 |
| 注: 分散環境のマスター アプライアンスにアップデートをインストールする必要があります。 | |
|  ロード バランサを有効にする。 | [ロード バランサの有効化] |

vRealize Automation 環境のユーザー インターフェイス

vRealize Automation 環境は、複数のインターフェイスで使用および管理します。

ユーザー インターフェイス

これらの表は、vRealize Automation 環境を管理するために使用するインターフェイスを示しています。

表 1-49. vRealize Automation 管理コンソール

| 目的 | アクセス | 必要な認証情報 |
|--|--|------------------------------|
| 以下のシステム管理者のタスクには、vRealize Automation コンソールを使用します。 | 1 ブラウザを起動し、仮想アプライアンスの完全修飾ドメイン名を使用して、vRealize Automation アプライアンスのダッシュボード ページを開きます。 | システム管理者ロールを持つユーザーである必要があります。 |
| <ul style="list-style-type: none"> テナントを追加します。 vRealize Automation ユーザー インターフェイスをカスタマイズします。 メール サーバを構成します。 イベント ログを表示します。 vRealize Orchestrator を構成します。 | 2 <a href="https://<vra-virtual-hostname.domain.name>">https://<vra-virtual-hostname.domain.name> [vRealize Automation コンソール] をクリックします。 vRealize Automation コンソールを開くには、次の URL を使用することもできます : <a href="https://<vra-virtual-hostname.domain.name>/vcac">https://<vra-virtual-hostname.domain.name>/vcac 3 ログインします。 | |

表 1-50. vRealize Automation テナント コンソール。このインターフェイスは、サービスやリソースの作成および管理に使用するプライマリ ユーザー インターフェイスです。

| 目的 | アクセス | 必要な認証情報 |
|---|---|---|
| <p>以下のタスクには、vRealize Automation を使用します。</p> <ul style="list-style-type: none"> ■ 新しい IT サービス ブループリントを申請します。 ■ クラウドおよび IT リソースを作成および管理します。 ■ カスタム グループを作成および管理します。 ■ ビジネス グループを作成、管理します。 ■ ユーザーにロールを割り当てます。 | <ol style="list-style-type: none"> 1 ブラウザを起動し、仮想アプライアンスの完全修飾ドメイン名とテナントの URL 名を使用して、テナントの URL を入力します。 https://<vra-va-hostname.domain.name>/vcac/org/<tenant_URL_name> 2 ログインします。 | <p>以下の 1 つ以上のロールを持つユーザーである必要があります。</p> <ul style="list-style-type: none"> ■ アプリケーション アーキテクト ■ 承認管理者 ■ カタログ管理者 ■ コンテナ管理者 ■ コンテナ アーキテクト ■ 健全性サービス ユーザー ■ インフラストラクチャ アーキテクト ■ セキュアなエクスポートの利用者 ■ ソフトウェア アーキテクト ■ テナント管理者 ■ XaaS アーキテクト |

表 1-51. vRealize Automation アプライアンス管理。このインターフェイスは、仮想アプライアンス管理インターフェイス (VAMI) と呼ばれます。

| 目的 | アクセス | 必要な認証情報 |
|---|--|--|
| <p>以下のタスクには vRealize Automation アプライアンス管理を使用します。</p> <ul style="list-style-type: none"> 登録されているサービスのステータスを表示します。 システム情報を表示、およびアプライアンスを再起動またはシャットダウンします。 カスタム エクスペリエンス改善プログラムへの参加を管理します。 ネットワーク ステータスを表示します。 更新ステータスを表示、およびアップデートをインストールします。 管理設定を管理します。 vRealize Automation ホスト設定を管理します。 SSO の設定を管理します。 製品ライセンスを管理します。 vRealize Automation Postgres データベースを設定します。 vRealize Automation メッセージングを設定します。 vRealize Automation ログを設定します。 IaaS コンポーネントをインストールします。 既存の vRealize Automation 環境から移行します。 IaaS コンポーネントの証明書を管理します。 Xenon サービスを設定します。 | <ol style="list-style-type: none"> ブラウザを起動し、仮想アプライアンスの完全修飾ドメイン名を使用して、vRealize Automation アプライアンスのブラッシュ ページを開きます。 https://<vra-va-hostname.domain.name> [vRealize Automation アプライアンス管理] をクリックします。 次の URL を使用して vRealize Automation アプライアンス管理を開くこともできます : https://<vra-va-hostname.domain.name:5480> ログインします。 | <ul style="list-style-type: none"> ユーザー名 : root パスワード : vRealize Automation アプライアンスを展開したときに 入力したパスワード。 |

表 1-52. vRealize Orchestrator クライアント

| 目的 | アクセス | 必要な認証情報 |
|---|--|--|
| <p>以下のタスクには、vRealize Orchestrator クライアントを使用します。</p> <ul style="list-style-type: none"> アクションを作成します。 ワークフローを作成します。 ポリシーを管理します。 パッケージをインストールします。 ユーザーおよびユーザー グループの権限を管理します。 URI オブジェクトにタグを追加します。 インベントリを表示します。 | <ol style="list-style-type: none"> ブラウザを起動し、仮想アプライアンスの完全修飾ドメイン名を使用して、vRealize Automation のブラッシュ ページを開きます。 https://<vra-va-hostname.domain.name> ローカル コンピュータに client.jnlp ファイルをダウンロードするには、[vRealize Orchestrator Client] をクリックします。 client.jnlp ファイルを右クリックして [起動] を選択します。 [続行しますか?] ダイアログボックスで、[続行] をクリックします。 ログインします。 | <p>システム管理者ロールを持つユーザーであるか、または vRealize Orchestrator コントロール センターの認証プロバイダの設定で構成されている vcoadmins グループに属している必要があります。</p> |

表 1-53. vRealize Orchestrator コントロール センター

| 目的 | アクセス | 必要な認証情報 |
|---|---|---|
| vRealize Automation に組み込まれているデフォルトの vRealize Orchestrator インスタンスの設定を編集するには、vRealize Orchestrator コントロール センターを使用します。 | <ol style="list-style-type: none"> 1 ブラウザを起動し、仮想アプライアンスの完全修飾ドメイン名を使用して、vRealize Automation アプライアンスのスプラッシュ ページを開きます。 https://<vra-vd-hostname.domain.name> 2 [vRealize Automation アプライアンス管理] をクリックします。 次の URL を使用して vRealize Automation アプライアンス管理を開くこともできます : https://<vra-vd-hostname.domain.name:5480> 3 ログインします。 4 [vRA 設定] - [Orchestrator] の順にクリックします。 5 [Orchestrator ユーザー インターフェイス] を選択します。 6 [開始] をクリックします。 7 Orchestrator ユーザー インターフェイスの URL をクリックします。 8 ログインします。 | <p>ユーザー名</p> <ul style="list-style-type: none"> ■ ロールベースの認証が設定されていない場合は、root と入力します。 ■ ロールベースの認証で設定されている場合は、vRealize Automation ユーザー名を入力します。 <p>パスワード</p> <ul style="list-style-type: none"> ■ ロールベースの認証が設定されていない場合、vRealize Automation アプライアンスを展開したときに入力したパスワードを入力します。 ■ ロールベースの認証でユーザー名が設定されている場合は、ユーザー名に対するパスワードを入力します。 |

表 1-54. Linux コマンド プロンプト

| 目的 | アクセス | 必要な認証情報 |
|--|---|---|
| <p>vRealize Automation アプライアンス ホストなどのホストでは、以下のタスクには Linux コマンド プロンプトを使用します。</p> <ul style="list-style-type: none"> ■ サービスの開始または停止 ■ 構成ファイルの編集 ■ コマンドの実行 ■ データの取得 | <ol style="list-style-type: none"> 1 vRealize Automation アプライアンス ホストで、コマンド プロンプトを開きます。 ローカル コンピュータでコマンド プロンプトを開く方法の 1 つは、PuTTY などのアプリケーションを使用して、ホストでセッションを開始することです。 2 ログインします。 | <ul style="list-style-type: none"> ■ ユーザー名 : root ■ パスワード : vRealize Automation アプライアンスを展開したときに作成したパスワード。 |

表 1-55. Windows コマンド プロンプト

| 目的 | アクセス | 必要な認証情報 |
|---|--|--|
| laaS ホストなどのホスト上で、Windows コマンド プロンプトを使用してスクリプトを実行できます。 | <ol style="list-style-type: none"> 1 laaS ホスト上で、Windows にログインします。 ローカル コンピュータからログインする方法の 1 つは、リモート デスクトップ セッションを開始することです。 2 Windows コマンド プロンプトを開きます。 コマンド プロンプトを開く方法の 1 つは、ホスト上で [スタート] アイコンを右クリックし、[コマンド プロンプト] または [コマンド プロンプト (管理者)] を選択することです。 | <ul style="list-style-type: none"> ■ ユーザー名 : 管理者権限を持つユーザー。 ■ パスワード : ユーザーのパスワード。 |

vRealize Automation に統合された VMware 製品のアップグレード

vRealize Automation をアップグレードする場合、vRealize Automation 環境に統合されているすべての VMware 製品を管理する必要があります。

vRealize Automation 環境が 1 つ以上の他の製品に統合されている場合は、他の製品をアップデートする前に vRealize Automation をアップグレードする必要があります。vRealize Business for Cloud が vRealize Automation に統合されている場合は、vRealize Automation をアップグレードする前に vRealize Business for Cloud を登録解除する必要があります。

vRealize Automation をアップグレードする場合は、統合製品を管理するための推奨ワークフローを実行します。

- 1 vRealize Automation をアップグレードします。
- 2 VMware vRealize Operations Manager をアップグレードします。
- 3 VMware vRealize Log Insight をアップグレードします。
- 4 VMware vRealize Business for Cloud をアップグレードします。

このセクションでは、vRealize Automation 環境に統合する場合の vRealize Business for Cloud の管理について詳細に説明します。

vRealize Automation に統合された vRealize Operations Manager のアップグレード

vRealize Automation のアップグレード後に vRealize Operations Manager をアップグレードします。

手順

- 1 vRealize Automation をアップグレードします。
- 2 vRealize Operations Manager をアップグレードします。詳細については、[VMware vRealize Operations Manager のドキュメント](#)の「Updating Your Software」を参照してください。

vRealize Automation に統合された vRealize Log Insight のアップグレード

vRealize Automation のアップグレード後に vRealize Log Insight をアップグレードします。

手順

- 1 vRealize Automation をアップグレードします。
- 2 vRealize Log Insight をアップグレードします。詳細については、[VMware vRealize Log Insight のドキュメント](#)の「vRealize Log Insight のアップグレード」を参照してください。

vRealize Automation に統合された vRealize Business for Cloud のアップグレード

vRealize Automation 環境をアップグレードする場合は、vRealize Business for Cloud への接続を一度登録解除して、再度登録する必要があります。

vRealize Automation 環境をアップグレードする場合は、この手順を実行して vRealize Business for Cloud のサービスの継続を確認します。

手順

- 1 vRealize Automation から vRealize Business for Cloud を登録解除します。[VMware vRealize Business for Cloud のドキュメント](#)の「vRealize Business for Cloud の vRealize Automation からの登録解除」を参照してください。
- 2 vRealize Automation をアップグレードします。

- 3 必要に応じて、vRealize Business for Cloud をアップグレードします。[VMware vRealize Business for Cloud のドキュメント](#)の「vRealize Business for Cloud のアップグレード」を参照してください。
- 4 vRealize Automation に vRealize Business for Cloud を登録します。[VMware vRealize Business for Cloud のドキュメント](#)の「vRealize Business for Cloud の vRealize Automation への登録」を参照してください。

vRealize Automation のアップグレードの準備

vRealize Automation 7.1、7.2、7.3 を 7.4 にアップグレードする前に、次のタスクを完了します。

これらのタスクはチェックリストに表示されている順序で実行します。[「vRealize Automation のアップグレード チェックリスト」](#)を参照してください。

vRealize Automation のアップグレード前の NSX ネットワークおよびセキュリティ インベントリ データ収集の実行
vRealize Automation 7.1、7.2、7.3.x から 7.4 にアップグレードする前に、vRealize Automation 7.1、7.2、7.3.x 環境で NSX ネットワークとセキュリティ インベントリのデータ収集を実行する必要があります。

このデータ収集は、vRealize Automation 7.4 で 7.1、7.2、および 7.3.x の展開用にロード バランサの再構成アクションを行うために必要です。

手順

- ◆ vRealize Automation 7.4 にアップグレードする前に、バージョン 7.1、7.2、7.3.x で NSX ネットワークとセキュリティ インベントリ データの収集を実行します。[手動によるエンドポイント データ収集の開始](#)を参照してください。

次のステップ

[「vRealize Automation 7.1、7.2、または 7.3 から 7.4 にアップグレードする場合のバックアップの前提条件」](#)。

vRealize Automation 7.1、7.2、または 7.3 から 7.4 にアップグレードする場合のバックアップの前提条件

アップグレードを開始する前に、バックアップの前提条件を満たします。

前提条件

- 移行前の環境が正しくインストールされ、構成されていることを確認します。
- vSphere Client にログインし、移行前の環境の各アプライアンスで、次のディレクトリのすべての vRealize Automation アプライアンス構成ファイルをバックアップします。
 - `/etc/vcac/`
 - `/etc/vco/`
 - `/etc/apache2/`
 - `/etc/rabbitmq/`
- IaaS Microsoft SQL Server データベースをバックアップします。詳細については、SQL Server データベースの完全バックアップの作成に関する記事 [Microsoft Developer Network](#) を参照してください。
- カスタマイズしたすべてのファイル (`DataCenterLocations.xml` など) をバックアップします。

- 各仮想アプライアンスおよび IaaS サーバのスナップショットを作成します。vRealize Automation のアップグレードが失敗した場合に備えて、システム全体のバックアップに関する基本ガイドラインには必ず従ってください。[vRealize Automation インストールのバックアップおよびリカバリ](#)を参照してください。

既存の vRealize Automation 環境のバックアップ

vRealize Automation 7.1、7.2、または 7.3.x から 7.4 へアップデートする前に、各 Windows ノードの vRealize Automation IaaS サーバおよび各 Linux ノードの vRealize Automation アプライアンスのシャットダウンおよびスナップショットの作成を行います。アップグレードが失敗した場合は、スナップショットを使用して以前の正常な構成に戻り、別のアップグレードを試します。

vRealize Automation の起動については、[vRealize Automation の起動](#)を参照してください。

前提条件

- [「vRealize Automation 7.1、7.2、または 7.3 から 7.4 にアップデートする場合のバックアップの前提条件」](#)。
- vRealize Automation 7.0 以降では、PostgreSQL データベースが常に高可用性モードで構成されます。vRealize Automation アプライアンス管理コンソールにログインし、[vRA 設定 > データベース] の順に選択して現在のマスター ノードを特定します。データベース構成が外部データベースとしてリストされている場合は、この外部データベースの手動バックアップを作成します。
- vRealize Automation Microsoft SQL データベースが IaaS サーバ上でホストされていない場合は、データベース バックアップ ファイルを作成します。
- アップグレードのためのバックアップの前提条件が完了していることを確認します。
- シャットダウン時にシステムのスナップショットを作成したことを確認します。スナップショットを作成するときには、この方法が推奨されます。『vSphere 6.0 のドキュメント』を参照してください。

注: vRealize Automation アプライアンスと IaaS コンポーネントをバックアップする場合、インメモリ スナップショットと静止スナップショットを無効にします。

- **app.config** ファイルを変更した場合は、そのファイルのバックアップを作成します。[「app.config ファイルに行ったログの変更のリストア」](#)を参照してください。
- 外部ワークフロー構成 (xmldb) ファイルのバックアップを作成します。[「外部ワークフローのタイムアウト ファイルのリストア」](#)を参照してください。
- 現在のフォルダの外にバックアップ ファイルを保存する場所があることを確認します。[「.xml ファイルのバックアップ コピーによってシステムがタイムアウトする」](#)を参照してください。

手順

- 1 vSphere クライアントにログインします。
- 2 各 vRealize Automation IaaS Windows マシン、および各 vRealize Automation アプライアンス ノードを見つけます。
- 3 各マシンで、[ゲストのシャットダウン] を次の順序でクリックします。
 - a IaaS Windows サーバ マシン
 - b vRealize Automation アプライアンス

- 4 各 vRealize Automation マシンのスナップショットを作成します。
- 5 好みのバックアップ方法を使用して、各アプライアンス ノードの完全バックアップを作成します。
- 6 システムをパワーオンします。『vRealize Automation の管理』の「vRealize Automation の起動」を参照してください。

高可用性の環境がある場合は、この手順に従って仮想アプライアンスをパワーオンします。

- a マスター vRealize Automation アプライアンスを起動します。
- b vRealize Automation アプライアンス管理にログインし、[サービス] をクリックして、ライセンスサービスのステータスが [登録済み] になるまで待機します。
- c 残りの vRealize Automation アプライアンスを同時に起動します。
- d プライマリ Web ノードを起動し、起動が完了するまで待機します。
- e プライマリ Manager Service マシンを起動し、2 ～ 5 分間待機します。

実際の所要時間はサイトの構成によって異なります。

注: セカンダリ マシンでは、Manager Service 自動フェイルオーバーが設定されている場合を除いて、Windows サービスを起動または実行しないでください。

- f Distributed Execution Manager の Orchestrator とワーカー、およびすべての vRealize Automation プロキシ エージェントを起動します。

注: これらのコンポーネントは、任意の順序で起動することができます。他のコンポーネントを起動する前に、コンポーネントの起動が完了するまで待つ必要はありません。

- 7 各 vRealize Automation アプライアンス管理コンソールにログインし、システムが完全に機能することを確認します。
 - a [サービス] をクリックします。
 - b 各サービスが登録済みであることを確認します。

次のステップ

[\[vRealize Automation PostgreSQL レプリケーション モードの非同期設定\]](#)。

vRealize Automation PostgreSQL レプリケーション モードの非同期設定

PostgreSQL 同期レプリケーション モードで動作する分散 vRealize Automation 環境からアップグレードを実行する場合、アップグレード前に、モードを非同期に変更する必要があります。

前提条件

- アップグレード対象となる分散 vRealize Automation 環境があります。
- `https://<vra-va-hostname.domain.name>:5480` の vRealize Automation アプライアンス管理に **root** としてログインしています。

手順

- 1 [vRA 設定] - [データベース] の順にクリックします。
- 2 [非同期モード] をクリックして、アクションが完了するまで待機します。
- 3 [同期の状態] 列のすべてのノードのステータスが **非同期** と表示されていることを確認します。

次のステップ

[\[vRealize Automation アプライアンスの更新のダウンロード\]](#)

vRealize Automation アプライアンスの更新のダウンロード

アプライアンス管理コンソールでアップデートの有無をチェックし、次の方法のいずれかを使用して、アップデートをダウンロードすることができます。

最適なアップグレード パフォーマンスを得るためには、ISO ファイルによる方法を使用します。

アプライアンスをアップグレードする際の潜在的な問題を回避する場合や、アプライアンスのアップグレード中に問題が発生した場合は、[VMware ナレッジベースの記事](#)「vRealize Automation upgrade fails due to duplicates in the vRealize Orchestrator database (KB54987)」を参照してください。

CD-ROM ドライブで使用する仮想アプライアンスのアップデートのダウンロード

仮想アプライアンスは、アプライアンスが仮想 CD-ROM ドライブから読み取る ISO ファイルからアップデートできます。これが推奨される方法です。

ISO ファイルをダウンロードし、プライマリ アプライアンスを設定したら、このファイルを使用してアプライアンスをアップグレードします。

前提条件

- 既存の vRealize Automation 環境をバックアップします。
- vRealize Automation アプライアンスをアップデートする前に、アップグレードで使用するすべての CD-ROM ドライブが有効になっていることを確認します。vSphere クライアントで仮想マシンに CD-ROM ドライブを追加する際の詳細については、vSphere のドキュメントを参照してください。

手順

- 1 アップデート リポジトリ ISO ファイルをダウンロードします。
 - a ブラウザを起動し、www.vmware.com の [vRealize Automation 製品ページ](#) に移動します。
 - b [vRealize Automation ダウンロード リソース] をクリックして VMware ダウンロード ページに移動します。
 - c 適切なファイルをダウンロードします。
- 2 システム上でダウンロードしたファイルを探し、このサイズが VMware ダウンロード ページ上のファイルと同一であることを確認します。ダウンロード ページに記載されているチェックサムを使用して、ダウンロードしたファイルの整合性を検証します。詳細については、VMware ダウンロード ページの下にあるリンクを参照してください。
- 3 プライマリ仮想アプライアンスが起動していることを確認します。
- 4 プライマリ仮想アプライアンスの CD-ROM ドライブを、ダウンロードした ISO ファイルに接続します。

- 5 プライマリ vRealize Automation アプライアンスで、vRealize Automation アプライアンスを展開したときに入力したパスワードを使用して、**root** として vRealize Automation アプライアンス管理にログインします。
- 6 [アップデート] タブをクリックします。
- 7 [設定] をクリックします。
- 8 [アップデートリポジトリ] で、[CD-ROM アップデートを使用] を選択します。
- 9 [設定の保存] をクリックします。

VMware リポジトリからの vRealize Automation アプライアンス更新のダウンロード

vmware.com Web サイトの公開リポジトリから vRealize Automation アプライアンスのアップデートをダウンロードできます。

前提条件

- 既存の vRealize Automation 環境をバックアップします。
- vRealize Automation アプライアンスが起動していることを確認します。

手順

- 1 プライマリ vRealize Automation アプライアンスで、vRealize Automation アプライアンスを展開したときに入力したパスワードを使用して、**root** として vRealize Automation アプライアンス管理にログインします。
- 2 [アップデート] タブをクリックします。
- 3 [設定] をクリックします。
- 4 (オプション) [自動アップデート] パネルで、アップデートをチェックする頻度を設定します。
- 5 [リポジトリをアップデート] パネルで、[デフォルトリポジトリの使用] を選択します。
デフォルト リポジトリが正しい VMware.com URL に設定されます。
- 6 [設定の保存] をクリックします。

vRealize Automation アプライアンスと IaaS コンポーネントのアップデート

アップグレードの前提条件を満たすことを確認し、仮想アプライアンスのアップデートをダウンロードしたら、vRealize Automation 7.1、7.2、7.3.x アプライアンスに更新をインストールして、7.4 にアップグレードします。

最小環境の場合、vRealize Automation アプライアンスにアップデートをインストールします。分散環境の場合、アップデートはマスター アプライアンス ノードにインストールします。アップデートに必要な時間は、環境およびネットワークによって異なります。アップデートが完了すると、変更された項目が vRealize Automation アプライアンス管理の [アップデート ステータス] ページに表示されます。アプライアンスのアップデートが完了したら、アプライアンスを再起動する必要があります。分散環境でマスター アプライアンスを再起動すると、システムによって各レプリカ ノードが再起動されます。

再起動すると、[アップデート ステータス] ページに「**仮想アプライアンスサービスの開始を待機しています**」と表示されます。IaaS のアップデートは、システムが完全に初期化され、すべてのサービスが実行されると開始されます。[アップデート ステータス] ページで、IaaS のアップグレードの進行を確認できます。最初の IaaS サーバ コンポーネントは、アップデートが完了するまで約 30 分かかります。アップデート中は、「**web1-vra.mycompany.com ノードのサーバ コンポーネントをアップグレード中**」のようなメッセージが表示されます。

各 Manager Service ノードのアップグレード プロセスが完了するたびに、「**mgr-vra.mycompany.com ノードに対して ManagerService の自動フェイルオーバー モードを有効にします**」のようなメッセージが表示されます。

vRealize Automation 7.3 以降、アクティブな Manager Service ノードからフェイルオーバー サーバを選択する方法を、以前の手動による選択からシステムによる決定に変更しています。この機能は、アップグレード時に有効になります。この機能によって問題が発生する場合は、「[更新で管理エージェントのアップグレードに失敗する](#)」を参照してください。

vRealize Automation アプライアンスと IaaS コンポーネントへのアップデートのインストール

vRealize Automation 7.1、7.2、7.3.x 仮想アプライアンスにアップデートをインストールして vRealize Automation と IaaS コンポーネントをバージョン 7.4 にアップデートします。

アップデートのインストール中は管理コンソールを閉じないでください。

アップグレード プロセスで問題が発生する場合は、「[vRealize Automation アップグレードのトラブルシューティング](#)」を参照してください。

注: IaaS 仮想マシン上の管理エージェントのアップグレード中、VMware パブリック証明書が一時的に Trusted Publishers 証明書ストアにインストールされます。管理エージェントのアップグレード プロセスでは、この証明書を使って署名された PowerShell スクリプトが使用されます。アップグレードが終了すると、この証明書は証明書ストアから削除されます。

前提条件

- ダウンロード方法を選択し、その方法の手順を完了していることを確認します。「[vRealize Automation アプライアンスの更新のダウンロード](#)」を参照してください。
- すべての高可用性環境については、「[既存の vRealize Automation 環境のバックアップ](#)」を参照してください。
- ロード バランサを備えた環境では、すべての冗長ノードが無効になっていて、健全性モニターが削除されていることを確認します。詳細については、ロード バランサのドキュメントを参照してください。
 - vRealize Automation アプライアンス
 - IaaS Web サイト
 - IaaS Manager Service
- ロード バランサを備えた環境では、トラフィックがプライマリ ノードのみに送られていることを確認します。
- 以下の手順を実行することで、Microsoft Internet Information Services (IIS) でホストされている IaaS サービスが稼動していることを確認します。
 - a ブラウザを起動し、**https://<webhostname>/Repository/Data/MetaModel.svc** という URL を入力して、Web リポジトリが実行されていることを確認します。成功した場合、エラーは返されず、XML 形式のモデルのリストが表示されます。

- b laaS Web サイトにログインし、**Repository.log** ファイルに記録されたステータスが OK であることを確認します。このファイルは VCAC ホーム フォルダの **/Server/Model Manager Web/Logs/Repository.log** にあります。

注: 分散型 laaS Web サイトの場合は、MMD なしでセカンダリ Web サイトにログインし、Microsoft IIS を一時的に停止します。ロード バランサのトラフィックがプライマリ Web ノードのみを通過していることを確認するには、MetaModel.svc の接続を確認して、Microsoft IIS を再起動します。

- 以下の手順を実行して、すべての laaS ノードが健全な状態であることを確認します。
 - a プライマリ仮想アプライアンスで、vRealize Automation アプライアンスを展開したときに入力したパスワードを使用して、**root** として vRealize Automation アプライアンス管理にログインします。
 - b [vRA 設定] - [クラスタ] の順に選択します。
 - c [最終接続] の下で、次のことを確認します。
 - テーブル内の laaS ノードに 30 秒未満の最終接続時間があること。
 - 仮想アプライアンス ノードに 10 分未満の最終接続時間があること。
 laaS ノードが vRealize Automation アプライアンスと通信していない場合、アップグレードは失敗します。管理エージェントと仮想アプライアンス間の接続の問題を診断するには、次の手順を実行します。
 - 1 リストにない、または [最終接続] 時間が 30 秒を超える各 laaS ノードにログインします。
 - 2 管理エージェント ログに何らかのエラーが記録されているかどうかを確認します。
 - 3 管理エージェントが実行されていない場合は、サービス コンソールでエージェントを再起動します。
 - d 表に実体のないノードが示されていないことを確認します。実体のないノードとは、ホスト上で報告されているのにそのホストに存在しない重複ノードです。実体のないノードはすべて削除する必要があります。詳細については、[「vRealize Automation での実体のないノードの削除」](#)を参照してください。
- クラスタに属していないレプリカ仮想アプライアンスがある場合は、クラスタ テーブルから削除する必要があります。このアプライアンスを削除しないと、レプリカの更新が失敗したことを示す警告メッセージがアップグレード プロセスで表示されます。
- アップグレードの前に、すべての保存済みおよび進行中の申請が正常に完了したことを確認します。
- vRealize Automation 7.1、7.2、または 7.3.x アプライアンスのアップデート後に laaS コンポーネントを手動でアップグレードする場合は、[「laaS アップグレードの除外」](#)を参照してください。laaS を手動でアップグレードする場合は、各 laaS ノードで、管理エージェントを除くすべての laaS サービスを停止する必要もあります。

手順

- 1 プライマリ vRealize Automation アプライアンスで、vRealize Automation アプライアンスを展開したときに入力したパスワードを使用して、**root** として vRealize Automation アプライアンス管理にログインします。
分散環境では、マスター アプライアンスで管理コンソールを開きます。
- 2 [サービス] をクリックし、すべてのサービスが登録されていることを確認します。

- 3 [vRA 設定] - [データベース] の順に選択し、このアプライアンスがマスター vRealize Automation アプライアンスであることを確認します。

マスター vRealize Automation アプライアンスのみにアップデートをインストールします。各レプリカ vRealize Automation アプライアンスがマスター アプライアンスによって更新されます。

- 4 [更新] - [ステータス] の順に選択します。
- 5 [アップデートの確認] をクリックし、アップデートが利用可能かどうかを確認します。
- 6 (オプション) vRealize Automation アプライアンスのインスタンスの場合は、[アプライアンスのバージョン] 領域で [詳細] をクリックすると、リリース ノートの場所が表示されます。
- 7 [アップデートをインストール] をクリックします。
- 8 [OK] をクリックします。

アップデート処理が進行していることを示すメッセージが表示されます。アップグレード中に行われた変更がシステムによって [更新のサマリ] ページに表示されます。アップデートに必要な時間は、環境およびネットワークによって異なります。

- 9 (オプション) より詳細に更新を監視するには、ターミナル エミュレータを使用してプライマリ アプライアンスにログインします。/opt/vmware/var/log/vami/updatecli.log で updatecli.log ファイルを表示します。

その他のアップグレード進行状況の情報は次のファイルでも参照できます。

- /opt/vmware/var/log/vami/vami.log
- /var/log/vmware/horizon/horizon.log
- /var/log/bootstrap/*.log

アップグレード中にログアウトした場合、ログ ファイルで更新の進捗状況を継続することができます。

updatecli.log ファイルに、アップグレード前のバージョンの vRealize Automation の情報が表示される場合があります。表示されたバージョンは、アップグレード プロセスの中で適切なバージョンに変わります。

- 10 vRealize Automation アプライアンスの更新が完了したら、管理コンソールで [システム] - [再起動] をクリックします。

分散環境では、マスター アプライアンスを再起動するときに、正常にアップグレードされたすべてのレプリカ アプライアンス ノードが再起動されます。

システムが初期化され、すべてのサービスが稼働していると、IaaS の更新が開始されます。IaaS のアップグレードの進行状況を表示するには、[更新] - [ステータス] をクリックします。

- 11 IaaS の更新が完了したら、アプライアンス管理コンソールで [クラスタ] をクリックして、すべての IaaS ノードとコンポーネントのバージョン番号が最新のバージョンになっていることを確認します。

- 12 アプライアンス管理コンソールで [テレメトリ] をクリックします。カスタマー エクスペリエンス向上プログラム (CEIP) への参加に関する注意を読み、プログラムに参加するかどうかを選択します。

CEIP によって収集されるデータの詳細と、VMware がそのデータを使用する目的については、Trust & Assurance Center (<http://www.vmware.com/trustvmware/ceip.html>) を参照してください。

カスタマ エクスペリエンス改善プログラムの詳細については、「[vRealize Automation のカスタマ エクスペリエンス改善プログラムへの参加または脱退](#)」を参照してください。

次のステップ

環境でロード バランサを使用している場合は、次の手順を実行します。

- 1 ロード バランサの vRealize Automation 健全性チェックを有効にします。
- 2 すべての vRealize Automation ノードでロード バランサのトラフィックを再度有効にします。

laaS コンポーネントのアップグレードに失敗した場合は、「[更新プロセスが失敗する場合に laaS サーバ コンポーネントを個別にアップグレードする](#)」を参照してください。

更新プロセスが失敗する場合に laaS サーバ コンポーネントを個別にアップグレードする

自動更新プロセスが失敗した場合、laaS コンポーネントを個別にアップグレードすることができます。

vRealize Automation laaS Web サイトおよび Manager Service が正常にアップグレードされた場合は、アップグレード前に作成したスナップショットに戻さずに再度 laaS アップグレード シェル スクリプトを実行できます。同じ仮想マシンにインストールされた複数の laaS コンポーネントのアップグレード時に、再起動の保留イベントが生成されると、アップグレードが失敗することがあります。この場合は、手動による laaS ノードの再起動と、アップグレードの再実行により問題を解決します。アップグレードの失敗が解消されない場合は、VMware サポートに問い合わせるか、以下の手順で手動アップグレードを実行します。

- 1 vRealize Automation アプライアンスを更新前の状態に戻します。
- 2 laaS コンポーネントを更新プロセスから除外するためのコマンドを実行します。[\[laaS アップグレードの除外\]](#)を参照してください。
- 3 vRealize Automation アプライアンスで更新プロセスを実行します。
- 4 アップグレード シェル スクリプトまたは vRealize Automation 7.4 laaS インストーラ msi パッケージを使用して、laaS コンポーネントを個別に更新します。

vRealize Automation アプライアンスのアップグレード後にアップグレード シェル スクリプトを使用して laaS コンポーネントをアップグレード

各 vRealize Automation 7.1、7.2、7.3.x アプライアンスを 7.4 にアップデートした後に、アップグレード シェル スクリプトを使用して laaS コンポーネントをアップグレードします。

アップデートした vRealize Automation アプライアンスには、各 laaS ノードおよびコンポーネントのアップグレードに使用するシェル スクリプトが含まれています。

仮想マシンの vSphere コンソールまたは SSH コンソール セッションを使用すると、アップグレード スクリプトを実行できます。vSphere コンソールを使用する場合は、スクリプトの実行が中断する断続的なネットワーク接続の問題を回避します。

コンポーネントのアップグレード中にスクリプトを停止すると、そのスクリプトはコンポーネントのアップグレードを完了したときに停止します。ノード上の別のコンポーネントをアップグレードする必要がある場合は、もう一度スクリプトを実行します。

アップグレードが完了すると、アップグレード ログ ファイル (`/opt/vmware/var/log/vami/upgrade-iaas.log`) を開くことによってアップグレード結果を確認できます。

前提条件

- [「vRealize Automation アップグレードのトラブルシューティング」](#)を確認します。
- すべての vRealize Automation アプライアンスのアップデートが成功していることを確認します。
- すべての vRealize Automation アプライアンスをアップデートしてから、IaaS コンポーネントをアップグレードする前に IaaS サーバを再起動する場合、管理エージェント サービスを除く、Windows のすべての IaaS サービスを停止します。
- マスター vRealize Automation アプライアンス ノードでアップグレード シェル スクリプトを実行する前に、アプライアンス管理コンソールで [サービス] をクリックします。各サービス（iaas-service を除く）が登録済みであることを確認します。
- 各 IaaS ノードに手動で IaaS 管理エージェントをインストールするには、次の手順を実行します。
 - a ブラウザを開き、アプライアンス上の VMware vRealize Automation IaaS インストール ページ (https://<virtual_appliance_host_FQDN>:5480/installer) に移動します。
 - b 管理エージェントのインストーラ (vCAC-iaasManagementAgent-Setup.msi) をダウンロードします。
 - c 各 vRealize Automation IaaS マシンにログインし、管理エージェントのインストーラを使用して管理エージェントをアップグレードします。Windows 管理エージェント サービスを再起動します。
- プライマリ IaaS Web サイトおよび Model Manager ノードに JAVA SE Runtime Environment 8 Update 161 (64 ビット) 以降がインストールされていることを確認します。Java をインストールした後、各サーバ ノード上で環境変数 JAVA_HOME に新しいバージョンを設定する必要があります。
- 各 IaaS Web サイト ノードにログインして、作成日が **web.config** ファイルの変更日よりも前であることを確認します。**web.config** ファイルの作成日が変更日以降である場合は、[「IaaS Web サイト コンポーネントのアップグレードに失敗する」](#)の手順を実行します。
- 各 IaaS ノードにアップグレードされた IaaS 管理エージェントが存在することを確認するには、各 IaaS ノードで次の手順を実行します。
 - a vRealize Automation アプライアンス管理コンソールにログインします。
 - b [vRA 設定] - [クラスタ] の順に選択します。
 - c 各 IaaS ノードですべてのインストール済みコンポーネントのリストを展開して、IaaS 管理エージェントを見つけます。
 - d 管理エージェントのバージョンが最新であることを確認します。
- [「IaaS アップグレードの除外」](#)。
- ロールバックする必要がある場合に備えて、IaaS Microsoft SQL Server データベースのバックアップにアクセスできることを確認します。
- 展開で IaaS サーバのスナップショットが利用できることを確認します。

アップグレードが失敗した場合、スナップショットとデータベース バックアップに戻り、別のアップグレードを試します。

手順

- 1 vRealize Automation アプライアンス ホスト上で新しいコンソール セッションを開きます。root アカウントを使用してログインします。
- 2 ディレクトリを `/usr/lib/vcac/tools/upgrade/` に変更します。

`./upgrade` シェル スクリプトを実行する前に、すべての IaaS 管理エージェントがアップグレードされており、健全な状態にする必要があります。アップグレード シェル スクリプトを実行したときにいずれかの IaaS 管理エージェントに問題がある場合は、「[更新で管理エージェントのアップグレードに失敗する](#)」を参照してください。

- 3 アップグレード スクリプトを実行します。

a コマンド プロンプトで `./upgrade` と入力します。

b Enter キーを押します。

IaaS アップグレード プロセスの説明については、「[vRealize Automation アプライアンスと IaaS コンポーネントのアップデート](#)」を参照してください。

アップグレード シェル スクリプトが失敗した場合は、`upgrade-iaas.log` ファイルを確認します。

問題を修正した後、もう一度アップグレード スクリプトを実行できます。

次のステップ

- 1 [「組み込み vRealize Orchestrator コントロール センターへのアクセスのリストア」](#)。
- 2 展開環境でロード バランサを使用している場合、vRealize Automation 健全性モニターとすべてのノードへのトラフィックを再度有効にします。

詳細については、vRealize Automation のロード バランシングを参照してください。

vRealize Automation アプライアンスをアップグレードした後に IaaS インストーラ実行可能ファイルを使用して IaaS コンポーネントをアップグレード

vRealize Automation 7.1、7.2、または 7.3.x アプライアンスを 7.4 にアップグレードした後、この代替方法を使用して IaaS コンポーネントをアップグレードすることができます。

vRealize Automation アプライアンスのアップグレード後に IaaS コンポーネントをアップグレードするための IaaS インストーラのダウンロード

vRealize Automation アプライアンスを 7.4 に アップグレードした後、アップグレードする IaaS コンポーネントがインストールされているマシンに IaaS インストーラをダウンロードします。

この手順の間に証明書の警告が表示された場合は、無視して構いません。

注: アップグレード プロセスでは、Manager Service のパッシブ バックアップ インスタンスを除き、すべてのサービスの起動タイプを [自動] に設定する必要があります。サービスを [手動] に設定すると、アップグレード プロセスが失敗します。

前提条件

- IaaS のインストール マシンに、Microsoft .NET Framework 4.5.2 以降がインストールされていることを確認します。.NET インストーラは、vRealize Automation のインストーラ Web ページからダウンロードできます。サービスをシャットダウンし、インストールの一環としてマシンを再起動した後、.NET を 4.5.2 に更新した場合は、管理エージェントを除くすべての IaaS サービスを手動で停止する必要があります。
- ダウンロードに Internet Explorer を使用する場合、厳密なセキュリティ設定が有効になっていないことを確認します。検索バー に **res://iesetup.dll/SoftAdmin.htm** と入力して、Enter キーを押します。
- アップグレードする IaaS コンポーネントが 1 つ以上インストールされている Windows サーバにローカル管理者としてログインします。

手順

- 1 Web ブラウザを起動します。
- 2 Windows インストーラのダウンロード ページの URL を入力します。
たとえば、**https://<vcac-va-hostname.domain.name>:5480/installer** などとし、ここで <vcac-va-hostname.domain.name> はプライマリ (マスター) vRealize Automation アプライアンス ノードの名前になります。
- 3 [IaaS インストーラ] リンクをクリックします。
- 4 プロンプトが表示されたら、インストーラファイル (setup__<vcac-va-hostname.domain.name>@5480.exe) をデスクトップに保存します。
ファイル名は変更しないでください。インストールの vRealize Automation アプライアンス への接続に使用されます。

次のステップ

[「vRealize Automation 7.1 または 7.2 から 7.3 にアップグレードした後に IaaS コンポーネントをアップグレードする」](#)。

vRealize Automation 7.1 または 7.2 から 7.3 にアップグレードした後に IaaS コンポーネントをアップグレードする SQL データベースをアップグレードし、IaaS コンポーネントがインストールされたすべてのシステムを構成する必要があります。これらの手順は、最小および分散インストールに対して使用できます。

注: IaaS インストーラは、アップグレードする IaaS コンポーネントが含まれているマシンに存在する必要があります。外部の場所からインストーラを実行することはできません。ただし、Microsoft SQL データベースは Web ノードからリモートでアップグレードすることもできます。

展開で IaaS サーバのスナップショットが利用できることを確認します。アップグレードが失敗した場合は、スナップショットに戻り、別のアップグレードを試すことができます。

サービスが次の順序でアップグレードされるようにアップグレードを実行します。

1 IaaS Web サイト

ロード バランサを使用している場合は、プライマリ以外のすべてのノードのトラフィックを無効にします。

1 つのサーバのアップグレードを完了してから、Web サイト サービスを実行している次のサーバをアップグレードします。Model Manager Data コンポーネントがインストールされているサーバからアップグレードします。

外部 Microsoft SQL データベースの手動アップグレードを実行している場合は、外部 SQL をアップグレードしてから、Web ノードをアップグレードする必要があります。外部 SQL は Web ノードからリモートでアップグレードできます。

2 Manager Service

パッシブ Manager Service をアップグレードする前に、アクティブな Manager Service をアップグレードします。

SQL インスタンスで SSL 暗号化が有効にされていない場合には、[アップグレード構成] ダイアログ ボックスの SQL 定義の横にある [SSL 暗号化] チェックボックスのチェックを外します。

3 DEM orchestrator とワーカー

すべての DEM orchestrator とワーカーをアップグレードします。1 台のサーバのアップグレードを完了してから、次のサーバをアップグレードします。

4 エージェント

1 台のサーバのアップグレードを完了してから、エージェントを実行している次のサーバをアップグレードします。

5 管理エージェント

アップグレード手順の一部として自動的にアップデートされます。

あるサーバで異なるサービスを使用している場合は、アップグレードにより、サービスが正しい順序でアップデートされます。たとえば、サイト内に同一のサーバ上に Web サイトと Manager Service がある場合、両方をアップデート対象として選択します。アップグレード インストーラがアップデートを正しい順序で適用します。1 台のサーバのアップグレードを完了してから、別のサーバのアップグレードを開始する必要があります。

注: 環境でロード バランサを使用する場合は、プライマリ アプライアンスがロード バランサに接続されている必要があります。vRealize Automation アプライアンス アプライアンスの他のすべてのインスタンスは、キャッシュ エラーを回避するためにアップグレードを適用する前に、ロード バランサのトラフィックに対して無効にする必要があります。

前提条件

- 既存の vRealize Automation 環境をバックアップします。
- すべての vRealize Automation アプライアンスをアップデートしてから、IaaS コンポーネントをアップグレードする前に IaaS サーバを再起動する場合、管理エージェント サービスを除く、サーバ上のすべての IaaS Windows サービスを停止します。
- [\[vRealize Automation アプライアンスのアップグレード後に IaaS コンポーネントをアップグレードするための IaaS インストーラのダウンロード\]](#)。
- プライマリ IaaS Web サイト、Microsoft SQL データベース、および Model Manager ノードに JAVA SE Runtime Environment 8 Update 111 (64 ビット) 以降がインストールされていることを確認します。Java をインストールした後、各サーバ ノード上で環境変数 JAVA_HOME に新しいバージョンを設定する必要があります。

- 作成日が **web.config** ファイルの変更日よりも前であることを確認します。**web.config** ファイルの作成日が変更日以降である場合は、[「IaaS Web サイト コンポーネントのアップグレードに失敗する」](#)の手順を実行します。
- 次の手順を実行して、Microsoft 分散トランザクション コーディネータ (DTC) を再構成します。

注: 分散トランザクション コーディネータが有効になっていても、ファイアウォールがオンになっている場合は分散トランザクションが失敗する可能性があります。

- a vRealize Automation アプライアンスで、[スタート] - [管理ツール] - [コンポーネント サービス] の順に選択します。
- b [コンポーネント サービス] - [コンピューター] - [マイ コンピューター] - [分散トランザクション コーディネーター] の順に展開します。
- c 該当するタスクを選択します。
 - ローカル スタンドアロン DTC の場合、[ローカル DTC] を右クリックして [プロパティ] を選択します。
 - クラスタ化された DTC の場合、[クラスタ化された DTC] を展開し、名前付きのクラスタ化された DTC を右クリックして [プロパティ] を選択します。
- d [セキュリティ] をクリックします。
- e 次のすべてのオプションを選択します。
 - [ネットワーク DTC アクセス]
 - [リモート クライアントを許可する]
 - [受信を許可する]
 - [送信を許可する]
 - [相互認証を必要とする]
- f [OK] をクリックします。

手順

- 1 ロード バランサを使用している場合は、使用環境で次の準備を行います。
 - a Model Manager Data が含まれている IaaS Web サイト ノードが、ロード バランサのトラフィックに対して有効になっていることを確認します。
 <vCAC Folder>\Server\ConfigTool フォルダがあれば、このノードを特定できます。
 - b ロード バランサのトラフィックに対し、その他すべての IaaS Web サイトと、プライマリ以外の Manager Service を無効にします。
- 2 セットアップ ファイル **setup__<vrealize-automation-appliance-FQDN>@5480.exe** を右クリックして、[管理者として実行] を選択します。
- 3 [次へ] をクリックします。
- 4 使用許諾契約に同意し、[次へ] をクリックします。

5 [ログイン] ページで現在の導入環境の管理者認証情報を入力します。

ユーザー名は **root** で、パスワードはアプライアンスを展開したときに指定したパスワードです。

6 [証明書の受け入れ] を選択します。

7 [インストール タイプ] ページで、[アップグレード] が選択されていることを確認します。

[アップグレード] が選択されていない場合は、このシステム上のコンポーネントがすでにこのバージョンにアップグレードされています。

8 [次へ] をクリックします。

9 アップグレード設定を構成します。

| オプション | アクション |
|--|--|
| Model Manager Data をアップグレードする場合 | vCAC Server セクションで [Model Manager Data] チェック ボックスを選択します。 デフォルトではこのチェック ボックスは選択されています。Model Manager Data のアップグレードは 1 度のみです。複数のマシンで設定ファイルを実行し、分散インストールをアップグレードする場合、Web サーバは、Web サーバと Model Manager Data とのバージョンが一致しないと機能が停止します。Model Manager Data とすべての Web サーバをアップグレードしたら、すべての Web サーバが機能します。 |
| Model Manager Data をアップグレードしない場合 | vCAC Server セクションで [Model Manager Data] を選択解除します。 |
| Model Manager Data でカスタマイズされたワークフローを最新バージョンで保存するには | Model Manager Data をアップグレードする場合は、拡張性ワークフロー セクションで [ワークフローを最新バージョンに維持する] チェック ボックスを選択します。 デフォルトではこのチェック ボックスは選択されています。カスタマイズされたワークフローが常に維持されます。このチェック ボックスはバージョン順のみを決定します。vRealize Automation Designer を使用して Model Manager でワークフローをカスタマイズする場合は、このオプションを選択して、アップグレード後に最新バージョンとなるようにアップグレードする前に、カスタマイズされた各ワークフローを最新バージョンに維持します。 このオプションを選択しない場合、vRealize Automation Designer で提供される各ワークフローはアップグレード後に最新バージョンとなり、アップグレード前の最新バージョンは 2 番目に新しいバージョンとなります。 vRealize Automation Designer の詳細については、 vRealize Automation Designer を使用してマシン ライフ サイクルを延長する (Extending Machine Life Cycles By Using vRealize Automation Designer) を参照してください。 |
| Distributed Execution Manager またはプロキシ エージェントをアップグレードする場合 | サービス アカウント セクションで管理者アカウントの認証情報を入力します。 アップグレードするすべてのサービスがこのアカウントで実行されます。 |
| Microsoft SQL Server データベースを指定するには | Model Manager Data をアップグレードする場合、Microsoft SQL Server データベース インストール情報セクションの [サーバ] テキスト ボックスにデータベース サーバとデータベース インスタンスの名前を入力します。[データベース名] にデータベース サーバ名の完全修飾ドメイン名 (FQDN) を入力します。 データベース インスタンスがデフォルト以外の SQL ポートにある場合、サーバインスタンス仕様にポート番号を含めます。Microsoft SQL のデフォルト ポート番号は 1433 です。 マネージャ ノードをアップグレードする場合、MSSQL SSL オプションはデフォルトで選択されています。データベースで SSL を使用しない場合には、[データベース接続に SSL を使用] のチェックを外します。 |

10 [次へ] をクリックします。

- 11 アップグレードするすべてのサービスが [アップグレードの準備完了] ページに表示されていることを確認し、[アップグレード] をクリックします。

[アップグレード] ページおよび進行状況インジケータが表示されます。アップグレード手順を完了すると、[次へ] ボタンが有効になります。

- 12 [次へ] をクリックします。

- 13 [完了] をクリックします。

- 14 すべてのサービスが再起動されたことを確認します。

- 15 導入環境内の各 IaaS サーバに対し、推奨されている順序でこの手順を繰り返します。

- 16 すべてのコンポーネントをアップグレードしたら、アプライアンスの管理コンソールにログインし、IaaS を含むすべてのサービスが登録されていることを確認します。

- 17 (オプション) Manager Service の自動フェイルオーバーを有効にします。[「アップグレード後に Manager Service の自動フェイルオーバーを有効にする」](#) を参照してください。

選択したすべてのコンポーネントが新しいリリースにアップグレードされました。

次のステップ

- 1 [「組み込み vRealize Orchestrator コントロール センターへのアクセスのリストア」](#)。

- 2 導入環境でロード バランサを使用する場合、vRealize Automation 健全性チェックを使用するために各ロード バランサ ノードをアップグレードし、接続されていないノードのロード バランサのトラフィックを再度有効にします。

詳細については、vRealize Automation のロード バランシングを参照してください。

組み込み vRealize Orchestrator コントロール センターへのアクセスのリストア

IaaS サーバ コンポーネントをアップグレードした後、vRealize Orchestrator へのアクセスをリストアする必要があります。

vRealize Automation 7.3 以前を 7.4 にアップグレードする場合、新しいロール ベースのアクセス コントロール機能に対応するには、この手順を実行する必要があります。ここには、高可用性環境での手順を記載しています。

前提条件

vRealize Automation 環境のスナップショットを作成します。

手順

- 1 アプライアンス ホストの完全修飾ドメイン名を使用して (<https://<va-hostname.domain.name>:5480>)、vRealize Automation アプライアンス 管理コンソールに root としてログインします。
- 2 [vRA 設定] - [データベース] の順に選択します。
- 3 マスター ノードとレプリカ ノードを特定します。
- 4 各レプリカ ノードで SSH セッションを開き、管理者としてログインして、次のコマンドを実行します。

```
service vco-server stop && service vco-configurator stop
```


- 5 マスター ノードで SSH セッションを開き、管理者としてログインして、次のコマンドを実行します。

```
rm /etc/vco/app-server/vco-registration-id
```

- 6 マスター ノードで、`/etc/vco/app-server/` ディレクトリに移動します。

- 7 `sso.properties` ファイルを開きます。

- 8 プロパティ名 `com.vmware.o11n.sso.admin.group.name` にスペースや、Bash コマンドで特殊文字として使用できる他の Bash 関連文字（ハイフン (-) やドル記号 (\$) など）が含まれる場合は、次の手順を実行します。

- a `com.vmware.o11n.sso.admin.group.name` プロパティが含まれる行をコピーし、値に `AdminGroup` を入力します。

- b `com.vmware.o11n.sso.admin.group.name` プロパティが含まれる元の行の先頭に # を追加して、この行をコメントアウトします。

- c `sso.properties` ファイルを保存して閉じます。

- 9 次のコマンドを実行します。

```
vcac-vami vco-service-reconfigure
```

- 10 `sso.properties` ファイルを開きます。ファイルが変更されている場合は、次の手順を実行します。

- a `com.vmware.o11n.sso.admin.group.name` プロパティが含まれる元の行の先頭にある # を削除して、この行をコメント解除します。

- b `com.vmware.o11n.sso.admin.group.name` プロパティが表示されている行のコピーを削除します。

- c `sso.properties` ファイルを保存して閉じます。

- 11 次のコマンドを実行して、vco-server サービスを再起動します。

```
service vco-server restart
```

- 12 次のコマンドを実行して、vco-configurator サービスを再起動します。

```
service vco-configurator restart
```

- 13 vRealize Automation アプライアンス 管理コンソールで、[サービス] をクリックし、マスター ノードのすべてのサービスが [登録済み] になるまで待機します。

- 14 すべてのサービスが [登録済み] になったら、vRealize Automation レプリカ ノードを vRealize Automation クラスタに参加させ、vRealize Orchestrator 構成を同期します。詳細については、[「組み込みの vRealize Orchestrator で高可用性をサポートするための再構成」](#) を参照してください。

次のステップ

[「vRealize Automation をアップグレードした後の vRealize Orchestrator のアップグレード」](#)。

vRealize Automation をアップグレードした後の vRealize Orchestrator のアップグレード

vRealize Automation 7.1、7.2、または 7.3.x から 7.4 にアップデートする場合は、vRealize Orchestrator インスタンスをアップグレードする必要があります。

vRealize Orchestrator 7.4 リリースでは、vRealize Automation 7.4 にアップデートする場合に vRealize Orchestrator をアップグレードする方法が 2 つあります。

- 既存の外部 vRealize Orchestrator サーバを vRealize Automation 7.4 に組み込まれた vRealize Orchestrator に移行できます。
- 既存のスタンドアロンまたはクラスタ化された vRealize Orchestrator サーバをアップグレードして、vRealize Automation 7.4 と連携することができます。

外部 vRealize Orchestrator サーバから vRealize Automation への移行

既存の外部 vRealize Orchestrator サーバは、vRealize Automation 7.4 に組み込まれている vRealize Orchestrator インスタンスに移行することができます。

vRealize Orchestrator を外部サーバ インスタンスとして導入し、その外部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。または、vRealize Automation アプライアンスに含まれている vRealize Orchestrator サーバを構成して使用することもできます。

VMware では、外部 vRealize Orchestrator を、vRealize Automation に組み込まれた Orchestrator サーバに移行することをお勧めします。外部 Orchestrator から組み込み Orchestrator への移行には、次の利点があります。

- 総所有コストが削減されます。
- デプロイ モデルが簡素化されます。
- 運用効率が向上します。

注: 外部 vRealize Orchestrator の使用は、次の場合に考慮します。

- vRealize Automation 環境内の複数のテナント
 - 物理的に分散した環境
 - ワークロードの処理
 - 特定のプラグイン（古いバージョンの Site Recovery Manager プラグインなど）の使用
-

外部 Orchestrator および組み込み Orchestrator のコントロール センターの違い

外部 vRealize Orchestrator のコントロール センターで使用可能な一部のメニュー項目は、組み込み Orchestrator インスタンスのデフォルトのコントロール センター ビューに含まれていません。

組み込み Orchestrator サーバのコントロール センターでは、いくつかのオプションがデフォルトで非表示になっています。

| メニュー項目 | 詳細 |
|-------------------|---|
| [ライセンス] | 組み込み Orchestrator では vRealize Automation をライセンス プロバイダとして使用するよう事前構成されています。 |
| [設定をエクスポート/インポート] | エクスポートされた vRealize Automation コンポーネントに、組み込み Orchestrator の構成が含まれています。 |

| メニュー項目 | 詳細 |
|------------------------|--|
| [データベースを構成] | 組み込み Orchestrator では、vRealize Automation で使用されているデータベースを使用します。 |
| [カスタマ エクスペリエンス改善プログラム] | <p>カスタマ エクスペリエンス改善プログラム (CEIP) には vRealize Automation アプライアンス管理インターフェイスから参加できます。</p> <p>『vRealize Automation の管理』の「カスタマ エクスペリエンス改善プログラム」を参照してください。</p> |

デフォルトのコントロール センター ビューでは非表示になっている別のオプションには、[認証プロバイダを設定] ページの [ホスト アドレス] テキスト ボックスや [登録解除] ボタンがあります。

注: vRealize Automation に組み込まれている vRealize Orchestrator でコントロール センターのオプションをすべて表示するには、Orchestrator 管理の詳細ページ (https://<vra-vahostname.domain.name_or_load_balancer_address>:8283/vco-controlcenter/#/?advanced) にアクセスし、キーボードの [F5] ボタンを押してページを更新する必要があります。

外部 vRealize Orchestrator 7.x から vRealize Automation 7.4 への移行

既存の外部 Orchestrator インスタンスから構成をエクスポートし、これを vRealize Automation に組み込まれている Orchestrator サーバにインポートすることができます。

注: 複数の vRealize Automation アプライアンス ノードがある場合は、プライマリの vRealize Automation ノードに対してのみ移行手順を実行します。

前提条件

- vRealize Automation のバージョンを 7.4 にアップグレードまたは移行します。詳細については、『vRealize Automation のインストールまたはアップグレード』の「vRealize Automation のアップグレード」を参照してください。
- 外部 Orchestrator の Orchestrator サーバ サービスを停止します。
- 外部 Orchestrator サーバのデータベースを、データベース スキーマを含めバックアップします。

手順

- 1 外部 Orchestrator サーバから構成をエクスポートします。
 - a 移行元のバージョンに応じて、**root** または**管理者**として外部 Orchestrator サーバのコントロール センターにログインします。
 - b [起動オプション] ページから Orchestrator サーバ サービスを停止して、データベースに不要な変更が加えられないようにします。
 - c [設定のエクスポート/インポート] ページに移動します。
 - d [設定をエクスポート] ページで、[サーバ設定をエクスポート]、[バンドル プラグイン]、[プラグイン設定をエクスポート] を選択します。

2 エクスポートした設定を組み込み Orchestrator インスタンスに移行します。

- a エクスポートした Orchestrator 構成ファイルを vRealize Automation アプライアンスの `/usr/lib/vco/tools/configuration-cli/bin` ディレクトリにアップロードします。
- b 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。
- c 組み込み vRealize Orchestrator サーバの Orchestrator サーバサービスとコントロール センター サービスを停止します。

```
service vco-server stop && service vco-configurator stop
```

- d **import** コマンドを使用して **vro-configure** スクリプトを実行し、Orchestrator 構成ファイルを組み込み vRealize Orchestrator サーバにインポートします。

```
./vro-configure.sh import --type embedded --path orchestrator-config-export-  
<orchestrator_appliance_ip>-<date>_<hour>.zip
```

3 移行元とする外部 Orchestrator サーバが組み込み PostgreSQL データベースを使用している場合は、データベース構成ファイルを編集します。

- a `/var/vmware/vpostgres/current/pgdata/postgresql.conf` ファイルで、**listen_addresses** 行をコメント解除します。
- b **listen_addresses** の値をワイルドカード (*) に設定します。

```
listen_addresses = '*'
```

- c `/var/vmware/vpostgres/current/pgdata/pg_hba.conf` ファイルに行を追加します。

```
host all all <vra-va-ip-address>/32 md5
```

注: `pg_hba.conf` ファイルでは、IP アドレスとサブネット マスクの代わりに CIDR プリフィックス形式を使用する必要があります。

- d PostgreSQL サーバ サービスを再起動します。

```
service vpostgres restart
```

- 4 **db-migrate** コマンドを使用して **vro-configure** スクリプトを実行し、データベースを内部 PostgreSQL データベースに移行します。

```
./vro-configure.sh db-migrate --sourceJdbcUrl <JDBC_connection_URL> --sourceDbUsername <database_user> --sourceDbPassword <database_user_password>
```

注: 特殊文字を含むパスワードは一重引用符で囲んでください。

<JDBC_connection_URL> は、使用するデータベースのタイプによって異なります。

PostgreSQL: jdbc:postgresql://<host>:<port>/<database_name>

MSSQL: jdbc:jtds:sqlserver://<host>:<port>/<database_name>; if using SQL authentication and MSSQL:
jdbc:jtds:sqlserver://<host>:<port>/<database_name>;domain=<domain>;useNTLMv2=TRUE if using Windows authentication.

Oracle: jdbc:oracle:thin:@<host>:<port>:<database_name>

デフォルトのデータベースのログイン情報は以下のとおりです。

| | |
|--------------------------|--------|
| <database_name> | vmware |
| <database_user> | vmware |
| <database_user_password> | vmware |

- 5 データベースのキーストアからすべての証明書を削除します。

```
./vro-configuration.sh untrust --reset-db
```

- 6 Orchestrator プラグインを再インストールします。
- コントロール センターに **root** としてログインします。
 - [トラブルシューティング] をクリックします。
 - [プラグインを強制的に再インストール] をクリックします。

- 7 Orchestrator サーバ サービスを開始します。

- 8 **postgresql.conf** および **pg_hba.conf** ファイルをデフォルトの構成に戻します。

- PostgreSQL サーバ サービスを再起動します。

外部 Orchestrator サーバ インスタンスが vRealize Automation に組み込まれている vRealize Orchestrator インスタンスに正常に移行されました。

次のステップ

組み込み vRealize Orchestrator サーバを設定します。「[組み込み vRealize Orchestrator サーバの構成](#)」を参照してください。

組み込み vRealize Orchestrator サーバの構成

外部 Orchestrator サーバの構成をエクスポートして vRealize Automation 7.4 にインポートしたら、vRealize Automation に組み込まれた Orchestrator サーバを構成する必要があります。

前提条件

設定を外部から内部 vRealize Orchestrator に移行します。

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 コントロール センター サービスと、組み込み vRealize Orchestrator サーバの Orchestrator サーバ サービスを開始します。

```
service vco-configurator start && service vco-server start
```

- 3 組み込み Orchestrator サーバのコントロール センターに**管理者**としてログインします。

注: 外部 vRealize Orchestrator 7.4 インスタンスから移行する場合は、手順 5 に進んでください。

- 4 コントロール センターの [設定を検証] ページで、Orchestrator が正しく設定されていることを確認します。
- 5 外部 Orchestrator がクラスタ モードで動作するように構成されている場合は、vRealize Automation で Orchestrator クラスタを再構成します。

- a 詳細な [Orchestrator クラスタ管理] ページ (https://<vra-vd-hostname.domain.name_or_load_balancer_address>:8283/vco-controlcenter/#/control-app/ha?remove-nodes) に移動します。

注: クラスタの既存のノードの横に [削除] チェック ボックスが表示されない場合は、キーボードの [F5] ボタンをクリックして、ブラウザ ページを更新する必要があります。

- b 外部 Orchestrator ノードの横にあるチェック ボックスをオンにし、[削除] をクリックしてクラスタから削除します。
 - c 詳細なクラスタ管理ページを終了するには、URL から **remove-nodes** 文字列を削除し、キーボードの [F5] ボタンをクリックしてブラウザ ページを更新します。
 - d コントロール センターの [設定を検証] ページで、Orchestrator が適切に設定されていることを確認します。
- 6 (オプション) [証明書] ページの [パッケージ署名証明書] タブの下で、新しいパッケージ署名証明書を生成します。
 - 7 (オプション) [認証プロバイダを設定] ページの [デフォルト テナント] と [管理グループ] の値を変更します。
 - 8 vRealize Automation アプライアンス 管理コンソールの [サービス] タブの下で **vco-server** サービスが REGISTERED と表示されていることを確認します。

9 外部 Orchestrator サーバの **vco** サービスを選択し、[登録解除] をクリックします。

次のステップ

- 外部 Orchestrator サーバにある信頼された証明書を、組み込み Orchestrator のトラスト ストアにインポートします。
- vRealize Automation レプリカ ノードを vRealize Automation クラスタに参加させて、Orchestrator 構成を同期します。

詳細については、『vRealize Automation のインストールまたはアップグレード』の「Reconfigure the Target Embedded vRealize Orchestrator to Support High Availability」を参照してください。

注: vRealize Orchestrator のインスタンスは自動的にクラスタ化されており、使用可能です。

- クラスタ内のすべてのノードで **vco-configurator** サービスを再起動します。
- 移行した組み込み Orchestrator サーバをポイントするように、vRealize Orchestrator エンドポイントを更新します。
- vRealize Automation ホストと IaaS ホストを vRealize Automation プラグインのインベントリに追加します。これは vRA ホスト ワークフローの vRA ホストの追加と IaaS ホストの追加を実行して行います。

vRealize Automation で使用するスタンドアローン vRealize Orchestrator アプライアンスのアップグレード

vRealize Automation で使用する vRealize Orchestrator のスタンドアローンの外部インスタンスを維持している場合は、vRealize Automation を 7.1、7.2、または 7.3.x から 7.4 にアップデートするときに vRealize Orchestrator をアップグレードする必要があります。

vRealize Orchestrator の組み込みインスタンスは、vRealize Automation アプライアンスのアップグレードの一部としてアップグレードされます。組み込みインスタンスの場合、追加のアクションは必要ありません。

vRealize Orchestrator アプライアンス クラスタをアップグレードする場合は、[「vRealize Automation 7.4 で使用するための vRealize Orchestrator Appliance クラスタのアップグレード」](#)を参照してください。

前提条件

- [「vRealize Automation アプライアンスと IaaS コンポーネントへのアップデートのインストール」](#)。
- すべてのネットワーク ファイル システムをマウント解除します。vSphere のドキュメントの『vSphere 仮想マシン管理』を参照してください。
- vSphere Orchestrator Appliance のメモリを 6 GB 以上に増やします。vSphere のドキュメントの『vSphere 仮想マシン管理』を参照してください。
- vSphere Orchestrator 仮想マシンのスナップショットを作成します。vSphere のドキュメントの『vSphere 仮想マシン管理』を参照してください。
- 外部データベースを使用する場合は、データベースをバックアップします。
- vSphere Orchestrator の事前構成された PostgreSQL データベースを使用する場合は、vSphere コントロールセンターの [データベースをエクスポート] メニューを使用して、データベースをバックアップします。

手順

- ◆ 次のいずれかの方法を使用してスタンドアロン vRealize Orchestrator をアップグレードします。
 - 「デフォルトの VMware リポジトリを使用した Orchestrator Appliance のアップグレード」。
 - 「ISO イメージを使用した Orchestrator Appliance のアップグレード」。
 - 「指定したリポジトリを使用した Orchestrator Appliance のアップグレード」。

デフォルトの VMware リポジトリを使用した Orchestrator Appliance のアップグレード

Orchestrator を構成して、デフォルトの VMware リポジトリからアップグレード パッケージをダウンロードできます。

前提条件

- すべてのネットワーク ファイル システムをマウント解除します。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。
- Orchestrator Appliance のメモリを 6 GB 以上増やします。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。
- vRealize Orchestrator 仮想マシンのディスク サイズを、Disk1=7 GB、Disk2=10 GB に増やします。
- Orchestrator Appliance の root パーティションに 3 GB 以上の使用可能な空き容量があることを確認してください。ディスク パーティションのサイズを増やす方法については、KB1004071 (<http://kb.vmware.com/kb/1004071>) を参照してください。
- Orchestrator 仮想マシンのスナップショットを作成します。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。
- 外部データベースを使用する場合は、データベースをバックアップします。
- 事前構成された Orchestrator PostgreSQL データベースを使用する場合は、コントロール センターの[データベースをエクスポート]メニューを使用して、データベースをバックアップします。

手順

- 1 仮想アプライアンス管理インターフェイス (VAMI : https://<orchestrator_server>:5480) にアクセスし、**root** としてログインします。
- 2 [更新] タブで、[設定] をクリックします。
[デフォルト リポジトリの使用] オプションの横にあるラジオ ボタンが選択されます。
- 3 [ステータス] ページで、[更新チェック] をクリックします。
- 4 アップデートが利用可能な場合は、[アップデートのインストール] をクリックします。
- 5 VMware エンドユーザー使用許諾契約に同意し、アップデートをインストールすることを確認します。
- 6 アップデートを完了するには、Orchestrator Appliance を再起動します。
 - a 仮想アプライアンス管理インターフェイス (VAMI) に **root** として再度ログインします。

- 7 (オプション) [更新] タブで、最新バージョンの Orchestrator Appliance が正常にインストールされていることを確認します。
- 8 コントロール センターに **root** としてログインします。
- 9 Orchestrator インスタンスのクラスタを作成する予定の場合は、ホスト設定を再構成します。
 - a コントロール センターの [ホスト設定] ページで [変更] をクリックします。
 - b vRealize Orchestrator のアプライアンス名ではなく、ロード バランサ サーバのホスト名を入力します。
- 10 認証を再構成します。
 - a アップグレードする前に、Orchestrator サーバが [LDAP] または [SSO (レガシー)] を認証方式として使用するように構成されていた場合は、[vSphere] または [vRealize Automation] を認証プロバイダとして構成します。
 - b 認証がすでに [vSphere] または [vRealize Automation] に設定されている場合は、設定を登録解除し、それらを再度登録します。

注: アップグレード前に、Orchestrator が認証プロバイダとして [vSphere] を使用し、vCenter Server の完全修飾ドメイン名または IP アドレスに接続するように構成されており、外部に Platform Services Controller がある場合、アップグレード後に、Orchestrator を vCenter Single Sign-On を含む Platform Services Controller インスタンスの完全修飾ドメイン名または IP アドレスに接続するように構成する必要があります。同一の vCenter Single Sign-On ドメインを共有するすべての Platform Services Controller の証明書を手動で Orchestrator にインポートする必要もあります。

これで、Orchestrator Appliance が正常にアップグレードされました。

次のステップ

コントロール センターの [設定を検証] ページで、Orchestrator が正しく設定されていることを確認します。

ISO イメージを使用した Orchestrator Appliance のアップグレード

Orchestrator を構成することにより、アプライアンスの CD-ROM ドライブにマウントされている ISO イメージ ファイルからアップグレードパッケージをダウンロードできます。

前提条件

- すべてのネットワーク ファイル システムをマウント解除します。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。
- Orchestrator Appliance のメモリを 6 GB 以上増やします。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。
- vRealize Orchestrator 仮想マシンのディスク サイズを、Disk1=7 GB、Disk2=10 GB に増やします。
- Orchestrator Appliance の root パーティションに 3 GB 以上の使用可能な空き容量があることを確認してください。ディスク パーティションのサイズを増やす方法については、KB1004071 (<http://kb.vmware.com/kb/1004071>) を参照してください。

- Orchestrator 仮想マシンのスナップショットを作成します。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。
- 外部データベースを使用する場合は、データベースをバックアップします。
- 事前構成された Orchestrator PostgreSQL データベースを使用する場合は、コントロール センターの[データベースをエクスポート]メニューを使用して、データベースをバックアップします。

手順

- 1 VMware の公式なダウンロードサイトで **VMware-vR0-Appliance-<version>-<build_number>-updaterepo.iso** アーカイブをダウンロードします。
- 2 Orchestrator Appliance 仮想マシンの CD-ROM ドライブを接続します。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。
- 3 ISO イメージ ファイルをアプライアンスの CD-ROM ドライブにマウントします。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。
- 4 仮想アプライアンス管理インターフェイス (VAMI : https://<orchestrator_server>:5480) にアクセスし、**root** としてログインします。
- 5 [更新] タブで、[設定] をクリックします。
- 6 [CD-ROM アップデートの使用] オプションの横にあるラジオ ボタンを選択します。
- 7 [ステータス] ページに戻ります。
使用可能なアップグレードのバージョンが表示されます。
- 8 [アップデートをインストール] をクリックします。
- 9 VMware エンドユーザー使用許諾契約に同意し、アップデートをインストールすることを確認します。
- 10 アップデートを完了するには、Orchestrator Appliance を再起動します。
 - a 仮想アプライアンス管理インターフェイス (VAMI) に **root** として再度ログインします。
- 11 (オプション) [更新] タブで、最新バージョンの Orchestrator Appliance が正常にインストールされていることを確認します。
- 12 コントロール センターに **root** としてログインします。
- 13 Orchestrator インスタンスのクラスタを作成する予定の場合は、ホスト設定を再構成します。
 - a コントロール センターの [ホスト設定] ページで [変更] をクリックします。
 - b vRealize Orchestrator のアプライアンス名ではなく、ロード バランサ サーバのホスト名を入力します。

14 認証を再構成します。

- a アップグレードする前に、Orchestrator サーバが [LDAP] または [SSO (レガシー)] を認証方式として使用するように構成されていた場合は、[vSphere] または [vRealize Automation] を認証プロバイダとして構成します。
- b 認証がすでに [vSphere] または [vRealize Automation] に設定されている場合は、設定を登録解除し、それらを再度登録します。

注: アップグレード前に、Orchestrator が認証プロバイダとして [vSphere] を使用し、vCenter Server の完全修飾ドメイン名または IP アドレスに接続するように構成されており、外部に Platform Services Controller がある場合、アップグレード後に、Orchestrator を vCenter Single Sign-On を含む Platform Services Controller インスタンスの完全修飾ドメイン名または IP アドレスに接続するように構成する必要があります。同一の vCenter Single Sign-On ドメインを共有するすべての Platform Services Controller の証明書を手動で Orchestrator にインポートする必要もあります。

これで、Orchestrator Appliance が正常にアップグレードされました。

次のステップ

コントロール センターの [設定を検証] ページで、Orchestrator が正しく設定されていることを確認します。

指定したリポジトリを使用した Orchestrator Appliance のアップグレード

Orchestrator を構成して、アップグレード アーカイブのアップロード先であるローカル リポジトリを使用できます。

前提条件

- すべてのネットワーク ファイル システムをマウント解除します。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。
- Orchestrator Appliance のメモリを 6 GB 以上増やします。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。
- vRealize Orchestrator 仮想マシンのディスク サイズを、Disk1=7 GB、Disk2=10 GB に増やします。
- Orchestrator Appliance の root パーティションに 3 GB 以上の使用可能な空き容量があることを確認してください。ディスク パーティションのサイズを増やす方法については、KB1004071 (<http://kb.vmware.com/kb/1004071>) を参照してください。
- Orchestrator 仮想マシンのスナップショットを作成します。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。
- 外部データベースを使用する場合は、データベースをバックアップします。
- 事前構成された Orchestrator PostgreSQL データベースを使用する場合は、コントロール センターの[データベースをエクスポート]メニューを使用して、データベースをバックアップします。

手順

- 1 アップグレード用のローカル リポジトリを準備します。
 - a ローカル Web サーバをインストールして構成します。
 - b VMware の公式なダウンロード サイトで **VMware-vR0-Appliance-<version>-<build_number>-updaterepo.zip** アーカイブをダウンロードします。
 - c **.ZIP** アーカイブをローカル リポジトリに抽出します。
- 2 仮想アプライアンス管理インターフェイス (VAMI : https://<orchestrator_server>:5480) にアクセスし、**root** としてログインします。
- 3 [更新] タブで、[設定] をクリックします。
- 4 [指定したリポジトリを使用] オプションの横にあるラジオ ボタンを選択します。
- 5 ローカル リポジトリの URL アドレスを **Update_Repo** ディレクトリをポイントして入力します。
http://<local_web_server>:<port>/build/mts/release/bora-<build_number>/publish/exports/Update_Repo
- 6 ローカル リポジトリで認証が必要になる場合は、ユーザー名とパスワードを入力します。
- 7 [設定の保存] をクリックします。
- 8 [ステータス] ページで、[更新チェック] をクリックします。
- 9 アップデートが利用可能な場合は、[アップデートのインストール] をクリックします。
- 10 VMware エンドユーザー使用許諾契約に同意し、アップデートをインストールすることを確認します。
- 11 アップデートを完了するには、Orchestrator Appliance を再起動します。
 - a 仮想アプライアンス管理インターフェイス (VAMI) に **root** として再度ログインします。
- 12 (オプション) [更新] タブで、最新バージョンの Orchestrator Appliance が正常にインストールされていることを確認します。
- 13 コントロール センターに **root** としてログインします。
- 14 Orchestrator インスタンスのクラスタを作成する予定の場合は、ホスト設定を再構成します。
 - a コントロール センターの [ホスト設定] ページで [変更] をクリックします。
 - b vRealize Orchestrator のアプライアンス名ではなく、ロード バランサ サーバのホスト名を入力します。

15 認証を再構成します。

- a アップグレードする前に、Orchestrator サーバが [LDAP] または [SSO (レガシー)] を認証方式として使用するように構成されていた場合は、[vSphere] または [vRealize Automation] を認証プロバイダとして構成します。
- b 認証がすでに [vSphere] または [vRealize Automation] に設定されている場合は、設定を登録解除し、それらを再度登録します。

注: アップグレード前に、Orchestrator が認証プロバイダとして [vSphere] を使用し、vCenter Server の完全修飾ドメイン名または IP アドレスに接続するように構成されており、外部に Platform Services Controller がある場合、アップグレード後に、Orchestrator を vCenter Single Sign-On を含む Platform Services Controller インスタンスの完全修飾ドメイン名または IP アドレスに接続するように構成する必要があります。同一の vCenter Single Sign-On ドメインを共有するすべての Platform Services Controller の証明書を手動で Orchestrator にインポートする必要もあります。

これで、Orchestrator Appliance が正常にアップグレードされました。

次のステップ

コントロール センターの [設定を検証] ページで、Orchestrator が正しく設定されていることを確認します。

vRealize Automation 7.4 で使用するための vRealize Orchestrator Appliance クラスタのアップグレード

vRealize Automation で vRealize Orchestrator Appliance クラスタを使用する場合は、いずれか 1 つのインスタンスをアップグレードした後に、新しくインストールした 7.4 ノードをアップグレード済みのインスタンスに参加させることで Orchestrator Appliance クラスタをバージョン 7.4 にアップグレードする必要があります。

vRealize Orchestrator のインスタンスを 1 つのみアップグレードする場合は、[「vRealize Automation で使用するスタンドアローン vRealize Orchestrator アプライアンスのアップグレード」](#)を参照してください。

前提条件

- [「vRealize Automation アプライアンスと IaaS コンポーネントへのアップデートのインストール」](#)。
- VRealize Orchestrator の複数のインスタンス間でトラフィックを分散するロード バランサを設定します。
[vRealize Orchestrator ロード バランシング構成ガイド](#)を参照してください。
- すべての vRealize Orchestrator サーバ ノードのスナップショットを作成します。
- vRealize Orchestrator の共有データベースをバックアップします。

手順

- 1 すべてのクラスタ ノードで **vco-server** および **vco-configurator** Orchestrator サービスを停止します。
- 2 ドキュメントで説明されている手順のいずれかを使用して、クラスタ内の Orchestrator サーバ インスタンスのいずれか 1 つのみをアップグレードします。
- 3 バージョン 7.3 で新しい Orchestrator Appliance を展開します。
 - a クラスタに含まれているアップグレード済みインスタンスではなく、既存のネットワーク設定を使用して新しいノードを構成します。

- 4 コントロール センターの 2 番目のノードにアクセスして、構成ウィザードを開始します。
 - a https://<your_orchestrator_server_IP_or_DNS_name>:8283/vco-controlcenter に移動します。
 - b OVA の展開時に入力したパスワードを使用して **root** としてログインします。
- 5 [クラスタ化された Orchestrator] デプロイ タイプを選択します。

このタイプを選択することで、ノードが既存の Orchestrator クラスタに参加することを指定できます。
- 6 [ホスト名] テキスト ボックスに、最初の Orchestrator サーバ インスタンスのホスト名または IP アドレスを入力します。

注: これは、2 番目のノードを参加させている Orchestrator インスタンスのローカル IP アドレスまたはホスト名にする必要があります。ロード バランサのアドレスを使用することはできません。

- 7 [ユーザー名] および [パスワード] テキスト ボックスに、最初の Orchestrator サーバ インスタンスの root 認証情報を入力します。
- 8 [参加] をクリックします。Orchestrator インスタンスが参加先のノードの構成をクローン作成します。

両方のノードの Orchestrator サーバ サービスが自動的に再起動されます。
- 9 ロード バランサのアドレスおよび**管理者**としてのログインを介してアップグレードされた Orchestrator クラスタのコントロール センターにアクセスします。
- 10 [Orchestrator クラスタ管理] ページで、[アクティブな設定フィンガー プリント] の文字列と [保留中の設定フィンガー プリント] の文字列が、クラスタのすべてのノードで一致することを確認します。

注: 2 つの文字列が一致するまでページを数回更新する必要があることがあります。

- 11 コントロール センターの [設定を検証] ページを開いて、vRealize Orchestrator クラスタが適切に構成されていることを確認します。
- 12 (オプション) クラスタ内の追加ノードごとに手順 3 から手順 8 を繰り返します。

Orchestrator クラスタが正常にアップグレードされました。

次のステップ

[「ロード バランサの有効化」](#)。

ロード バランサの有効化

環境内でロード バランサを使用する場合は、セカンダリ ノードと健全性チェックを再度有効にして、ロード バランサのタイムアウト設定を元に戻します。

vRealize Automation の健全性チェックは、バージョンによって異なります。詳細については、[VMware vRealize Automation ドキュメント](#)の『vRealize Automation Load Balancing Configuration Guide』を参照してください。

ロード バランサのタイムアウト設定を変更して、10 分からデフォルトに戻します。

vRealize Automation のアップグレード後のタスク

vRealize Automation 7.1、7.2、7.3.x から 7.4 へのアップデート後、アップグレード後のタスクを実行する必要があります。

ソフトウェア エージェントの TLS 1.2 へのアップグレード

vRealize Automation 7.4 へのアップグレード後、ソフトウェア エージェントを vRealize Automation 7.1、7.2、7.3、または 7.3.1 環境から TLS 1.2 にアップグレードするには、いくつかのタスクを実行する必要があります。

vRealize Automation 7.4 以降、トランスポート レイヤー セキュリティ (TLS) 1.2 は、vRealize Automation とブラウザの間のデータ通信で唯一サポートされる TLS プロトコルです。

移行後、既存のすべての仮想マシンと、vRealize Automation 7.1、7.2、7.3、または 7.3.1 環境からの既存の仮想マシン テンプレートをアップグレードする必要があります。

vRealize Automation 仮想マシン テンプレートの更新

ソフトウェア エージェントが TLS 1.2 プロトコルを使用できるように vRealize Automation 7.4 への更新が完了した後、既存のテンプレートを更新する必要があります。

ゲスト エージェントおよびエージェント ブートストラップ コードを、vRealize Automation 7.1、7.2、7.3 または 7.3.1 のテンプレートで更新する必要があります。リンク クローン オプションを使用している場合、新規作成した仮想マシンおよびそれらのスナップショットを使用したテンプレートの再マッピングが必要になることがあります。

テンプレートをアップグレードするには、次のタスクを実行します。

- 1 vSphere にログインします。
- 2 vRealize Automation 7.1、7.2、7.3 または 7.3.1 の各テンプレートを仮想マシンに変換し、そのマシンをオンにします。
- 3 適切なソフトウェアのインストーラをインポートし、各仮想マシンでソフトウェアのインストーラを実行します。
- 4 各仮想マシンを再度テンプレートに変換します。

この手順を使用すると、Linux または Windows 用のソフトウェア インストーラを特定できます。

前提条件

vRealize Automation 7.4 への正常なアップグレード

手順

- 1 ブラウザを起動し、仮想アプライアンスの完全修飾ドメイン名 (<https://<vra-virtual-machine-hostname.domain.name>>) を使用して、vRealize Automation 7.4 アプライアンスのスプラッシュ ページを開きます。
- 2 [ゲストおよびソフトウェア エージェント] ページをクリックします。
- 3 Linux または Windows ソフトウェアのインストーラの手順を実行してください。

次のステップ

[「ソフトウェア エージェントのアップグレードが必要な仮想マシンの特定」](#)。

ソフトウェア エージェントのアップグレードが必要な仮想マシンの特定

vRealize Automation の健全性サービスを使用して、TLS 1.2 へのソフトウェア エージェントの更新が必要な仮想マシンを特定できます。

健全性サービスを使用して、TLS 1.2 へのソフトウェア エージェントの更新が必要な仮想マシンを特定できます。ブラウザと vRealize Automation の間の安全な通信を必要とするプロビジョニング後の手順を実行できるように、vRealize Automation 7.4 環境のすべてのソフトウェア エージェントを更新する必要があります。

前提条件

- vRealize Automation 7.4 に正常にアップグレードしている。
- テナント管理者としてプライマリ仮想アプライアンスで vRealize Automation 7.4 にログインしている。

手順

- 1 [管理] - [健全性] の順にクリックします。
- 2 [新しい構成] をクリックします。
- 3 [構成の詳細] ページで、必要な情報を提供します。

| オプション | コメント |
|--------|--|
| 名前 | SW Agent verification と入力します。 |
| 説明 | Locate software agents for upgrade to TLS 1.2 などの、オプションの説明を追加します。 |
| 製品 | vRealize Automation 7.4.0 を選択します。 |
| スケジュール | [なし] を選択します。 |

- 4 [次へ] をクリックします。
- 5 [テストスイートの選択] ページで、[vRealize Automation のシステム テスト] と [vRealize Automation のテナント テスト] を選択します。
- 6 [次へ] をクリックします。
- 7 [パラメータの構成] ページで、必要な情報を提供します。

表 1-56. vRealize Automation 仮想アプライアンス

| オプション | 説明 |
|-----------------|--|
| 公開 Web サーバのアドレス | <ul style="list-style-type: none"> ■ 最小インストールの場合、vRealize Automation アプライアンス ホストのベース URL。例：https://<va-host.domain>/ ■ 高可用性展開の場合、vRealize Automation ロード バランサのベース URL。例：https://<load-balancer-host.domain>/ |
| SSH コンソールのアドレス | vRealize Automation アプライアンスの完全修飾ドメイン名。例：<va-host.domain> |
| SSH コンソール ユーザー | root |

表 1-56. vRealize Automation 仮想アプライアンス (続き)

| オプション | 説明 |
|--------------------|------------------|
| SSH コンソール パスワード | root のパスワード。 |
| サービスの応答の最大時間 (ミリ秒) | デフォルトを受け入れ: 2000 |

表 1-57. vRealize Automation システム テナント

| オプション | 説明 |
|----------------|------------|
| システム テナント管理者 | 管理者 |
| システム テナントパスワード | 管理者のパスワード。 |

表 1-58. vRealize Automation ディスク容量の監視

| オプション | 説明 |
|--------------|----------------|
| 警告レベルしきい値の割合 | デフォルトを受け入れ: 75 |
| 重大レベルしきい値の割合 | デフォルトを受け入れ: 90 |

表 1-59. vRealize Automation テナント

| オプション | 説明 |
|-----------------|---|
| テスト対象テナント | テスト対象として選択されたテナント。 |
| ファブリック管理者のユーザー名 | ファブリック管理者のユーザー名。たとえば、admin@va-host.local。 <small>注: すべてのテストを実行するために、このファブリック管理者にはテナント管理者と laaS 管理者のロールも必要です。</small> |
| ファブリック管理者パスワード | ファブリック管理者のパスワード。 |

- 8 [次へ] をクリックします。
- 9 [サマリ] ページで情報を確認し、[完了] をクリックします。
ソフトウェア エージェントの検証設定が完了しました。
- 10 SW Agent verification カードで、[実行] をクリックします。
- 11 テストが完了したら、SW Agent verification カードの中央をクリックします。
- 12 SW Agent verification の結果ページで、テスト結果を参照して、[名前] 列の [ソフトウェア エージェントのバージョン チェック] テストを見つけます。テスト結果が失敗の場合は、[原因] 列の [原因] リンクをクリックして、ソフトウェア エージェントが古い仮想マシンを表示します。

次のステップ

ソフトウェア エージェントが古い仮想マシンがある場合は、[「vSphere 上のソフトウェア エージェントのアップグレード」](#) を参照してください。

vSphere 上のソフトウェア エージェントのアップグレード

vRealize Automation アプライアンス管理を使用して、アップグレード後に vSphere の古いソフトウェア エージェントを TLS 1.2 にアップグレードできます。

この手順は、アップグレードされた環境内の仮想マシンで、古いソフトウェア エージェントを TLS 1.2 にアップグレードします。vRealize Automation 7.4 へのアップグレードで必要になります。

前提条件

- vRealize Automation 7.4 への正常なアップグレード
- 健全性サービスを使用して、古いソフトウェア エージェントを持つ仮想アプライアンスを識別している。

手順

- 1 プライマリ vRealize Automation アプライアンスで、vRealize Automation アプライアンスを展開したときに入力したパスワードを使用して、**root** として vRealize Automation アプライアンス管理にログインします。
高可用性環境の場合、マスター アプライアンスでアプライアンス管理を開きます。
- 2 [vRA 設定] - [ソフトウェア エージェント] の順にクリックします。
- 3 [Toggle TLS 1.0、1.1] をクリックします。
[TLS v1.0, v1.1 Status] が有効になります。
- 4 テナント認証情報には、vRealize Automation 7.4 アプライアンスに要求される情報を入力します。

| オプション | 説明 |
|-------|---|
| テナント名 | アップグレードされた vRealize Automation アプライアンス上のテナントの名前。 <small>注: テナントユーザーにはソフトウェア アーキテクト ロールが割り当てられている必要があります。</small> |
| ユーザー名 | vRealize Automation アプライアンス上のテナント管理者のユーザー名。 |
| パスワード | テナント管理者のパスワード。 |

- 5 [接続をテスト] をクリックします。
接続が確立されると、成功のメッセージが表示されます。
- 6 [バッチの一覧表示] をクリックします。
バッチ選択肢リスト テーブルが表示されます。
- 7 [表示] をクリックします。
古いソフトウェア エージェントを持つ仮想マシンのリストがテーブルに表示されます。
- 8 アップグレード可能状態の仮想マシンのソフトウェア エージェントをアップグレードします。
 - 個々の仮想マシンのソフトウェア エージェントをアップグレードするには、仮想マシンのグループの [表示] をクリックして、アップグレードする仮想マシンを識別します。それから [実行] をクリックし、アップグレード プロセスを開始します。

- 仮想マシンのバッチのソフトウェア エージェントをアップグレードするには、アップグレードするグループを識別し、[実行] をクリックしてアップグレード プロセスを開始します。

アップグレードする仮想マシンが 200 台以上ある場合は、次のパラメータの値を入力して、バッチ アップグレード プロセスの速度を制御できます。

| オプション | 説明 |
|-----------|--|
| バッチ サイズ | バッチ アップグレードで選択した仮想マシンの数。この数を変えると、アップグレードの速度を調整することができます。 |
| キュー深度 | 同時に実行されるアップグレードの平行実行の数。たとえば、20 と指定します。この数を変えると、アップグレードの速度を調整することができます。 |
| バッチ エラー | バッチ アップグレードの低速化の原因となった REST エラーの数。たとえば、アップグレードの安定性を向上するために 5 回エラーが発生したときに現在のバッチ アップグレードを停止する場合は、テキスト フィールドに 5 と入力します。 |
| バッチ の失敗 | バッチ アップグレードの低速化の原因となった、失敗したソフトウェア エージェント アップグレードの数。たとえば、アップグレードの安定性を向上するために 5 回エラーが発生したときに現在のバッチ アップグレードを停止する場合は、テキスト フィールドに 5 と入力します。 |
| バッチ ポーリング | アップグレード プロセスをチェックするためにアップグレード プロセスをポーリングする頻度。この数を変えると、アップグレードの速度を調整することができます。 |

アップグレード プロセスが低速すぎるか、失敗したアップグレードが多すぎる場合は、これらのパラメータを調整してアップグレードのパフォーマンスを向上できます。

注: [更新] をクリックすると、バッチのリストがクリアされます。アップグレード プロセスには影響しません。TLS 1.2 が設定されるかどうかに関する情報も更新されます。また、[更新] をクリックすると vRealize Automation サービスの健全性チェックも実行されます。サービスが実行されていない場合、エラー メッセージが表示され、他のすべてのアクション ボタンが無効になります。

9 [Toggle TLS 1.0、1.1] をクリックします。

[TLS v1.0, v1.1 Status] が無効になります。

Amazon Web Service または Azure 上のソフトウェア エージェントのアップグレード

Amazon Web Service (AWS) または Azure 上の仮想マシンの古いソフトウェア エージェントは手動でアップグレードすることができます。

前提条件

- vRealize Automation 7.4 への正常なアップグレード
- ソフトウェア トンネルが存在し、トンネル仮想マシンの IP アドレスが既知である。

手順

- 1 アップグレードする必要がある各ノードのノード ファイルを作成します。

```
/usr/lib/vcac/server/webapps/ROOT/software/initializeUpdateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> -S <$SourceVRAServer>
```

注: インプレース アップグレードでは、**\$DestinationVRAServer** は **\$SourceVRAServer** と同一です。

- 2 Linux または Windows 仮想マシン上のソフトウェア エージェントをアップグレードするプラン ファイルを作成します。

- /var/log/vcac/agentupdate/{tenant}/{subtenant-UUID} にある migrate params ファイルを変更し、AWS または Azure エンドポイントに対応するプライベート IP アドレスの値を含めます。

```
"key": "ipAddress",
  "value": {
    "type": "string",
    "value": "<$PrivateIp:$PrivatePort>"
  }
}
```

- Linux マシンをアップデートする場合は、このコマンドを使用します。

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CL
Software.LinuxAgentUpdate74 --source_cloud_provider azure
```

- Windows マシンをアップデートする場合は、このコマンドを使用します。

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CW
Software.WindowsAgentUpdate74 --source_cloud_provider azure
```

- このコマンドは、プラン ファイルを実行します。

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> --
plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan
```

- 3 手順 1 のノード ファイルと手順 2 のプラン ファイルを使用してソフトウェア エージェントをアップデートするには、このコマンドを使用します。

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$tenant> -tu <$TenantUser> --component_windows
Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --
plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --
node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure
--action plan_batch -S <$SourceVRAServer>
```

代わりに、ノードのインデックスを指定することでノード ファイルから一度に 1 台のノードを実行するには、このコマンドを使用します。

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$tenant> -tu <$TenantUser> --component_windows
Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --
plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --
node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure
--action execute_node -S <$SourceVRAServer> --node_index <0 through n-1>
```

この手順を実行するとき、vRealize Automation 仮想アプライアンスおよびホスト マシンからログの末尾を監視してサーバ エージェントのアップグレード プロセスを表示することができます。

アップグレード後、アップグレード プロセスにより、Windows または Linux 用のソフトウェア アップデート スクリプトは vRealize Automation 7.4 仮想アプライアンスにインポートされます。vRealize Automation 仮想アプライアンス ホストにログインすると、ソフトウェア コンポーネントが正常にインポートされていることを確認できます。コンポーネントをインポートした後、ソフトウェア アップデートは古いイベント ブローカ サービス (EBS) に送信され、指定された仮想マシンにソフトウェア アップデート スクリプトが中継されます。アップグレードが完了し、新しいソフトウェア エージェントが稼動すると、ping 要求を送信して新しい vRealize Automation 仮想アプライアンスにバインドします。

注: 有用なログ ファイル

- ソース vRealize Automation の Catalina 出力 : /var/log/vcac/catalina.out。このファイルでは、エージェントの移行が行われるときに行われるアップグレード要求を確認できます。このアクティビティは、ソフトウェア プロビジョニング要求を実行する場合と同様です。
- ターゲット vRealize Automation の Catalina 出力 : /var/log/vcac/catalina.out。このファイルでは、ping 要求をレポートする移行された仮想マシンが確認できます。バージョン番号 7.4.0-SNAPSHOT が含まれます。これらは、sw-agent-UUID などの EBS トピック名を比較することで照合できます。
- ターゲット vRealize Automation マシン マスター アップグレード ログ ファイルのエージェント アップデート フォルダ : var/log/vmware/vcac/agentupdate/updateSoftwareAgents.log。このファイルの末尾を監視すると、どのアップグレード処理が進行中なのかを確認できます。
- テナント フォルダ下で利用可能な個々のログ : /var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}。個々のノードがエラーや進行中の拡張機能がある多数のファイルとしてここに表示されます。

- 移行された仮想マシン : /opt/vmware-appdirector/agent/logs/darwin*.log。この場所をスポットチェックすると、受信されているソフトウェア アップデート要求、および agent_bootstrap + ソフトウェア エージェントの最後に発生する再起動のリストを確認できます。

vRealize Automation PostgreSQL レプリケーション モードの同期設定

アップグレード前に PostgreSQL レプリケーション モードを非同期に設定していても、分散 vRealize Automation 環境のアップグレード後に、PostgreSQL レプリケーション モードを同期に設定することができます。

前提条件

- 分散 vRealize Automation 環境をアップグレードしています。
- <https://vra-virtual-hostname.domain.name:5480> の適切な vRealize Automation アプライアンス管理に **root** としてログインしています。

手順

- 1 [vRA 設定] - [データベース] の順にクリックします。
- 2 [同期モード] をクリックして、アクションが完了するまで待機します。
- 3 [同期の状態] 列のすべてのノードのステータスが **同期** と表示されていることを確認します。

次のステップ

[「接続テストの実行とアップグレード後のエンドポイントの確認」](#)。

接続テストの実行とアップグレード後のエンドポイントの確認

vRealize Automation 7.3 以前から 7.4 にアップグレードすると、ターゲット環境のエンドポイントが変更されます。

vRealize Automation 7.4 へのアップグレード後には、該当するすべてのエンドポイントに対して [接続をテスト] アクションを実行する必要があります。また、アップグレード後の一部のエンドポイントで調整が必要になる場合があります。詳細については、[アップグレードまたは移行後のエンドポイントを使用する場合の考慮事項](#)を参照してください。

アップグレードまたは移行されたエンドポイントのデフォルトのセキュリティ設定では、信頼されていない証明書を受け入れません。

信頼されていない証明書を使用していた場合、以前の vRealize Automation インストール環境からアップグレードまたは移行した後、vSphere と NSX のすべてのエンドポイントに対して、次の手順を実行して証明書の検証を有効にする必要があります。そうしないと、エンドポイントの操作が証明書エラーで失敗します。詳細については、VMware ナレッジベースの記事「Endpoint communication is broken after upgrade to vRA 7.3 (KB2150230)」(<http://kb.vmware.com/kb/2150230>) および「How to download and install vCenter Server root certificates to avoid Web Browser certificate warnings (KB2108294)」(<http://kb.vmware.com/kb/2108294>) を参照してください。

- 1 アップグレード後または移行後に、vRealize Automation vSphere エージェント マシンにログインし、[サービス] タブを使用して vSphere エージェントを再起動します。

移行ではすべてのエージェントが再起動されない場合があるため、必要に応じて手動で再起動します。

- 2 少なくとも 1 つの ping レポートが終了するのを待ちます。ping レポートの完了には 1、2 分かかります。

- 3 vSphere エージェントがデータ収集を開始したら、IaaS 管理者として vRealize Automation にログインします。
- 4 [インフラストラクチャ] - [エンドポイント] - [エンドポイント] の順にクリックします。
- 5 vSphere エンドポイントを編集し、[接続をテスト] をクリックします。
- 6 証明書のプロンプトが表示されたら、[OK] をクリックして証明書を受け入れます。
 証明書のプロンプトが表示されない場合、証明書が現在、プロキシ エージェント マシンや DEM マシンなどのエンドポイントのサービスをホストする Windows マシンの信頼されたルート認証局に正しく保存されていない可能性があります。
- 7 [OK] をクリックして、証明書の承認を適用し、エンドポイントを保存します。
- 8 vSphere エンドポイントごとにこの手順を繰り返します。
- 9 NSX エンドポイントごとにこの手順を繰り返します。

[接続をテスト] 操作は成功したものの、一部のデータ収集やプロビジョニング操作が失敗した場合、エンドポイントとして機能するすべてのエージェント マシンとすべての DEM マシンに同じ証明書をインストールできます。または、既存のマシンから証明書をアンインストールして、問題のあるエンドポイントに対して上記の手順を繰り返します。

vRealize Automation からのアップグレード後の NSX ネットワークおよびセキュリティ インベントリ データ収集の実行

vRealize Automation 7.1、7.2、7.3 から 7.4 にアップグレードした後は、vRealize Automation 7.4 環境内で NSX ネットワークおよびセキュリティ インベントリ データ収集を実行する必要があります。

このデータ収集は、vRealize Automation 7.4 で 7.1、7.2、および 7.3.x の展開用にロード バランサの再構成アクションを行うために必要です。

前提条件

- [\[vRealize Automation のアップグレード前の NSX ネットワークおよびセキュリティ インベントリ データ収集の実行\]](#)。
- vRealize Automation 7.4 への正常なアップグレード

手順

- ◆ アップグレードの後、vRealize Automation 7.4 で NSX ネットワークおよびセキュリティ インベントリ データ収集を実行します。[手動によるエンドポイント データ収集の開始](#)を参照してください。

レプリカ アプライアンスのクラスタへの参加

マスター vRealize Automation アプライアンスのアップデートが完了すると、更新されたレプリカ ノードはそれぞれ自動的にマスター ノードに参加します。レプリカ ノードを個別に更新する必要がある場合は、次の手順を使用して手動でレプリカ ノードをクラスタに参加させます。

クラスタに参加していないレプリカ ノードのアプライアンス管理コンソールにアクセスして、次の手順を実行します。

手順

- 1 [vRA 設定] - [クラスタ] の順に選択します。
- 2 [クラスタに参加] をクリックします。

高可用性を展開する環境でのポート構成

リモート コンソール機能をサポートするには、高可用性を展開している環境をアップグレードした後、ポート 8444 のトラフィックが vRealize Automation アプライアンスに渡されるようにロード バランサを構成する必要があります。

詳細については、[vRealize Automation ドキュメント](#)の『vRealize Automation Load Balancing Configuration Guide』を参照してください。

組み込みの vRealize Orchestrator で高可用性をサポートするための再構成

高可用性環境では、各ターゲット レプリカ vRealize Automation アプライアンスを手動でクラスタに再参加させて、組み込みの vRealize Orchestrator で高可用性のサポートを有効にする必要があります。

前提条件

ターゲット レプリカ vRealize Automation アプライアンス管理コンソールにログインします。

- 1 ブラウザを起動し、ターゲット レプリカ仮想アプライアンスの完全修飾ドメイン名 (FQDN) `https://<vra-vr-hostname.domain.name>:5480` を使用して、ターゲット レプリカ vRealize Automation 管理コンソールを開きます。
- 2 ユーザー名 **root** と、ターゲット レプリカ vRealize Automation アプライアンスの展開時に入力したパスワードを使用してログインします。

手順

- 1 [vRA 設定] - [クラスタ] の順に選択します。
- 2 [先頭のクラスタ ノード] テキスト ボックスに、ターゲット マスター vRealize Automation アプライアンスの FQDN を入力します。
- 3 [パスワード] テキスト ボックスに root パスワードを入力します。
- 4 [クラスタに参加] をクリックします。
証明書の警告を無視して続行します。システムによってクラスタのサービスが再起動されます。
- 5 サービスが実行されていることを確認します。
 - a 最上部のタブ バーで、[サービス] をクリックします。
 - b サービスの起動の進行状況を監視するには、[更新] をクリックします。

外部ワークフローのタイムアウト ファイルのリストア

アップグレード プロセスによって xmldb ファイルが上書きされてしまうため、vRealize Automation の外部ワークフローのタイムアウト ファイルを再構成する必要があります。

手順

- 1 次のディレクトリから、システム上の外部ワークフロー構成 (xmldb) ファイルを開きます。
`\\VMware\\vCAC\\Server\\ExternalWorkflows\\xmldb\\`
- 2 xmldb ファイルを移行の前にバックアップしたファイルに置き換えます。バックアップ ファイルがない場合は、外部ワークフローのタイムアウト設定を再構成します。

3 設定を保存します。

ユーザー用リモート コンソール アクションとの接続の有効化

ユーザー用リモート コンソール アクションは、vRealize Automation で vSphere によってプロビジョニングされるアプライアンスでサポートされています。

このリリースをアップグレードしたらブループリントを編集し、[アクション] タブの [リモート コンソールに接続] アクションを選択します。

詳細については、[ナレッジ ベースの記事 2109706](#) を参照してください。

app.config ファイルに行ったログの変更のリストア

アップグレード プロセスでは、構成ファイルのログへの変更が上書きされます。アップグレードが終了した後、アップグレード前に **app.config** ファイルに行った変更をリストアする必要があります。

アップグレード後に Manager Service の自動フェイルオーバーを有効にする

vRealize Automation をアップグレードすると、Manager Service の自動フェイルオーバーがデフォルトで無効になります。

アップグレード後に Manager Service の自動フェイルオーバーを有効にするには、次の手順を実行します。

手順

- 1 vRealize Automation アプライアンスで、root ユーザーとしてコマンド プロンプトを開きます。
- 2 ディレクトリを **/usr/lib/vcac/tools/vami/commands** に変更します。
- 3 Manager Service の自動フェイルオーバーを有効にするには、次のコマンドを実行します。

```
python ./manager-service-automatic-failover ENABLE
```

laaS 環境全体で自動フェイルオーバーを無効にするには、次のコマンドを実行します。

```
python ./manager-service-automatic-failover DISABLE
```

Manager Service の自動フェイルオーバーについて

vRealize Automation laaS Manager Service は、プライマリの Manager Service が停止した場合、バックアップへのフェイルオーバーを自動的に実行するように設定できます。

vRealize Automation 7.3 以降では、サーバをプライマリまたはバックアップに設定する際、Windows サーバごとに手動で Manager Service を開始または停止する必要がなくなりました。アップグレードシェル スクリプトまたは laaS インストーラ実行可能ファイルを使用して laaS をアップグレードするときに、自動の Manager Service のフェイルオーバーはデフォルトで無効になります。

自動フェイルオーバーを有効にすると、バックアップを含むすべての Manager Service ホストで自動的に Manager Service が開始されます。自動フェイルオーバー機能により、ホストは透過的に互いを監視し、必要に応じてフェイルオーバーを実行しますが、すべてのホストで Windows サービスが実行されている必要があります。

注: 自動フェイルオーバーの使用は必須ではありません。自動フェイルオーバーを無効にして、引き続き手動で Windows サービスを開始および停止し、プライマリまたはバックアップ ホストの設定を制御することもできます。手動でフェイルオーバーを行う際は、一度に 1 台ずつホストのサービスを開始してください。自動フェイルオーバーが無効の場合、同時に複数の IaaS サーバでサービスを実行すると、vRealize Automation を使用できなくなります。

自動フェイルオーバーをホストごとに有効または無効に設定しないでください。IaaS 環境では、自動フェイルオーバーを有効または無効にする設定は、すべての Manager Service ホストで同一にする必要があります。

vRealize Automation アップグレードのトラブルシューティング

アップグレードのトラブルシューティングに関するトピックでは、vRealize Automation 7.1、7.2、7.3.x から 7.4 へのアップグレード時に発生する可能性のある問題の解決策を示します。

Manager Service の自動フェイルオーバーが有効にならない

manager-service-automatic-failover コマンドのトラブルシューティングに関する推奨事項。

ソリューション

- manager-service-automatic-failover コマンドが失敗するか、2 分間以上次のメッセージが表示されます：**ノードで Manager Service の自動フェイルオーバー モードが有効になっています**：
<IAAS_MANAGER_SERVICE_NODEID>。
 - a アプライアンスを展開したときに入力したユーザー名 **host** とパスワードを使用して、https://<va-hostname.domain.name>:5480 で vRealize Automation アプライアンス管理にログインします。
 - b [vRA 設定] - [クラスタ] の順に選択します。
 - c すべての Manager Service ホストで管理エージェント サービスが実行されていることを確認します。
 - d すべての IaaS Manager Service ノードの最終接続時間が 30 秒未満であることを確認します。

管理エージェント接続の問題が見つかった場合は、手動で解決し、Manager Service の自動フェイルオーバーを有効にするコマンドをもう一度実行してください。
- Manager-service-automatic-failover コマンドが、Manager Service ノード上でのフェイルオーバーを有効にするのに失敗します。この問題を解決するためにコマンドを再実行するのは問題ありません。
- IaaS 展開の一部の Manager Service ホストでフェイルオーバーが有効になっていますが、他のホストでは有効になっていません。IaaS 展開のすべての Manager Service ホストの機能は有効になっていますが、機能していません。この問題を修正するには、次のいずれかを実行します。
 - すべての Manager Service ノードのフェイルオーバーを無効にし、代わりに手動のフェイルオーバーのアプローチを使用します。一度に 1 台のホストでのみフェイルオーバーを実行します。
 - Manager Service ノードで何度かこの機能を有効にしようとして失敗した場合は、このノード上の Windows の VMware vCloud Automation Center サービスを停止し、問題を解決するまでノードの起動タイプを手動に設定します。

- Python を使用して、各 Manager Service ノードでフェイルオーバーが有効であることを検証します。
 - a SSH を使用して、マスター vRealize Automation アプライアンス ノードに **root** としてログインします。
 - b `python /usr/lib/vcac/tools/vami/commands/manager-service-automatic-failover ENABLE` を実行します。
 - c 次のメッセージが返されることを確認します。ノードで **Manager Service 自動フェイルオーバー モードが有効になっています:<IAAS_MANAGER_SERVICE_NODEID> 完了。**
- Manager Service 構成ファイルを調べることによって各 Manager Service ノードでフェイルオーバーが有効になっていることを確認します。
 - a Manager Service ノードでコマンド プロンプトを開きます。
 - b vRealize Automation インストール フォルダに移動し、
VMware\VCAC\Server\ManagerService.exe.config で Manager Service 構成ファイルを開きます。
 - c 次の要素が <appSettings> セクションに存在することを確認します。
 - <add key="FailoverModeEnabled" value="True" />
 - <add key="FailoverPingIntervalMilliseconds" value="30000" />
 - <add key="FailoverNodeState" value="active" />
 - <add key="FailoverMaxFailedDatabasePingAttempts" value="5" />
 - <add key="FailoverMaxFailedRepositoryPingAttempts" value="5" />
- Windows の VMware vCloud Automation Center サービスのステータスが起動し、起動タイプが自動であることを確認します。
- Python を使用して、各 Manager Service ノードでフェイルオーバーが無効であることを検証します。
 - a SSH を使用して、マスター vRealize Automation アプライアンス ノードに **root** としてログインします。
 - b `python /usr/lib/vcac/tools/vami/commands/manager-service-automatic-failover DISABLE` を実行します。
 - c 次のメッセージが返されることを確認します。ノードで **Manager Service 自動フェイルオーバー モードが無効になっています:<IAAS_MANAGER_SERVICE_NODEID> 完了。**
- Manager Service 構成ファイルを調べることによって各 Manager Service ノードでフェイルオーバーが無効になっていることを確認します。
 - a Manager Service ノードでコマンド プロンプトを開きます。
 - b vRealize Automation インストール フォルダに移動し、
VMware\VCAC\Server\ManagerService.exe.config で Manager Service 構成ファイルを開きます。
 - c 次の要素が <appSettings> セクションに存在することを確認します。
 - <add key="FailoverModeEnabled" value="False" />

- コールドスタンバイの Manager Service ノードを作成するには、ノードの Windows の VMware vCloud Automation Center サービスのステータスを停止にして、起動タイプを手動に設定します。
- アクティブな Manager Service ノードでは、ノードの Windows の VMware vCloud Automation Center サービスのステータスを開始にして、起動タイプを自動にする必要があります。
- `manager-service-automatic-failover` コマンドでは、Manager Service ノードの内部 ID (<IAAS_MANAGER_SERVICE_NODEID>) を使用します。この内部 ID に対応するホスト名を検索するには、コマンド `vra-command list-nodes` を実行し、ノード ID <IAAS_MANAGER_SERVICE_NODEID> を使用して Manager Service ホストを探します。
- 自動で現在アクティブになるように選択されている Manager Service を見つけるには、次の手順を実行します。
 - a SSH を使用して、マスター vRealize Automation アプライアンス ノードに **root** としてログインします。
 - b `vra-command list-nodes --components` を実行します。
 - フェイルオーバーが有効になっている場合は、ステータスがアクティブの Manager Service ノードを検索します。
 - フェイルオーバーが無効になっている場合は、ステータスが開始済みの Manager Service ノードを検索します。

ロード バランサのタイムアウト エラーでインストールまたはアップグレードに失敗する

ロード バランサを使用した分散環境を実現するための vRealize Automation のインストールまたはアップグレードが、503 サービス利用不能エラーで失敗します。

問題

ロード バランサ タイムアウトの設定が原因でタスクを完了するための十分な時間が確保できないため、インストールまたはアップグレードに失敗します。

原因

ロード バランサ タイムアウトの設定値が小さいとエラーになる可能性があります。この問題を修正するには、ロード バランサ タイムアウトの設定値を 100 秒以上に増やしてタスクを再実行します。

ソリューション

- 1 ロード バランサ タイムアウト値を最低でも 100 秒に増やします。
- 2 インストールまたはアップグレードを再実行します。

laaS Web サイト コンポーネントのアップグレードに失敗する

laaS のアップグレードに失敗し、アップグレードを続行できません。

問題

Web サイト コンポーネントの IaaS アップグレードに失敗します。インストーラ ログ ファイルに次のエラー メッセージが表示されます。

- System.Data.Services.Client.DataServiceQueryException:
An error occurred while processing this request. --->
System.Data.Services.Client.DataServiceClientException: <!DOCTYPE html>
- Description: An application error
occurred on the server. The current custom error settings for this application
prevent the details of the application error from being viewed remotely (for
security reasons). It could, however, be viewed by browsers running on the
local server machine.
- Warning: Non-zero return code. Command failed.
- Done Building Project "C:\Program Files
(x86)\VMware\vCAC\Server\Model Manager Data\DeployRepository.xml"
(InstallRepoModel target(s)) -- FAILED.

リポジトリ ログ ファイルに次のエラー メッセージが表示されます。

- [Error]: [sub-thread-Id="20"
context="" token=""] Failed to start repository service. Reason:
System.InvalidOperationException: Configuration section encryptionKey is not
protected
at
DynamicOps.Common.Utils.EncryptionHelpers.ReadKeyFromConfiguration(Configuration
config)
at DynamicOps.Common.Utils.EncryptionHelpers.Decrypt(String value)
at DynamicOps.Repository.Runtime.CoreModel.GlobalPropertyItem.Decrypt(Func`2
decryptFunc)
at
DynamicOps.Common.Entity.ContextHelpers.OnObjectMaterializedCallbackEncryptable(Object
sender, ObjectMaterializedEventArgs e)
at
System.Data.Common.Internal.Materialization.Shaper.RaiseMaterializedEvents()
at

```

System.Data.Common.Internal.Materialization.Shaper`1.SimpleEnumerator.MoveNext()
System.Linq.Enumerable.FirstOrDefault[TSource](IEnumerable`1 source)
System.Linq.Queryable.FirstOrDefault[TSource](IQueryable`1 source)
at
DynamicOps.Repository.Runtime.Common.GlobalPropertyHelper.GetGlobalPropertyItemValue(Core
ModelEntities
coreModelContext, String propertyName, Boolean throwIfPropertyNotFound)
at
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.LoadSolutionUserCertificate()
at
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.InitializeFromDb(String
coreModelConnectionString)
DynamicOps.Repository.Runtime.Common.RepositoryRuntime.Initialize()。

```

原因

laas アップグレードは、**web.config** ファイルの作成日が、変更日と同じまたはそれ以降の日付になっている場合に失敗します。

ソリューション

- 1 laaS ホスト上で、Windows にログインします。
- 2 Windows コマンド プロンプトを開きます。
- 3 vRealize Automation インストール フォルダに移動します。
- 4 [管理者として実行] オプションで任意のテキスト エディタを起動します。
- 5 **web.config** ファイルの場所を特定して選択し、ファイルを保存し直すことで、このファイルの変更日を作成日より後に変更できます。
- 6 **web.config** ファイルのプロパティを調べて、ファイル変更日が作成日より後であることを確認します。
- 7 laaS をアップグレードします。

実行中の SSL 検証エラーが原因で Manager Service の実行に失敗する

SSL 検証エラーが原因で、Manager Service の実行に失敗します。

問題

Manager Service が失敗し、ログに次のエラー メッセージが記録されます。

[Info]: Thread-Id="6" - context="" token="" Failed to connect to the core database, will retry in 00:00:05, error details: A connection was successfully established with the server, but then an error occurred during the login process. (provider: SSL Provider, error: 0 - The certificate chain was issued by an authority that is not trusted.)

原因

実行時、SSL 検証エラーが原因で、Manager Service の実行に失敗します。

ソリューション

- 1 **ManagerService.config** 構成ファイルを開きます。
- 2 次の行で **Encrypt=False** に更新します。

```
<add name="vcac-repository" providerName="System.Data.SqlClient"
connectionString="Data Source=iaas-db.sqa.local;Initial
Catalog=vcac;Integrated Security=True;Pooling=True;Max Pool
Size=200;MultipleActiveResultSets=True;Connect Timeout=200,
Encrypt=True" />
```

アップグレード後のログインの失敗

同期されていないユーザー アカウントを使用するセッションでは、アップグレード後にブラウザを終了し、もう一度ログインする必要があります。

問題

vRealize Automation をアップグレードすると、ログイン時に同期されていないユーザー アカウントへのアクセスは拒否されます。

ソリューション

ブラウザを終了し、vRealize Automation を再起動します。

vRealize Automation での実体のないノードの削除

実体のないノードとは、ホスト上で報告されているのにそのホストに存在しない重複ノードです。

問題

各 IaaS ノードおよび仮想アプライアンス ノードが健全な状態にあることを確認するとき、あるホストに実体のないノードが 1 つ以上あることに気付くことがあります。実体のないノードはすべて削除する必要があります。

ソリューション

- 1 プライマリ vRealize Automation アプライアンスで、vRealize Automation アプライアンスを展開したときに入力したパスワードを使用して、**root** として vRealize Automation アプライアンス管理にログインします。
- 2 [vRA 設定] - [クラスタ] の順に選択します。
- 3 表内のそれぞれの実体のないノードに対して、[削除] をクリックします。

高可用性環境アップグレード後にクラスタへの参加コマンドが失敗したように表示される

セカンダリ クラスタ ノードの管理コンソールで [クラスタに参加] をクリックした後、進行状況インジケータが表示されなくなります。

問題

アップグレード後に vRealize Automation アプライアンス管理コンソールを使用してセカンダリ クラスタ ノードをプライマリ ノードに参加させると、進行状況インジケータが消え、エラー メッセージも正常完了メッセージも表示されなくなります。この挙動は断続的に確認される問題です。

原因

進行状況インジケータが消えるのは、一部のブラウザがサーバからの応答待ちを中止するためです。この挙動によってクラスタへの参加プロセスが停止することはありません。正常にクラスタへの参加が完了した場合、ログ ファイル (/var/log/vmware/vcac/vcac-config.log) を表示することで確認できます。

PostgreSQL データベースのアップグレード マージが成功しない

外部の PostgreSQL データベースは組み込みの PostgreSQL データベースと正常にマージされません。

問題

PostgreSQL データベースと正常にアップグレード マージが行われない場合は、手動によるマージを実行できます。

ソリューション

- 1 vRealize Automation 仮想アプライアンスを、アップグレード前に作成したスナップショットの状態に戻します。
- 2 vRealize Automation 仮想アプライアンスにログインし、次のコマンドを実行して、データベースが正常にマージされなくてもアップグレードを完了するようにします。

touch /tmp/allow-external-db

このコマンドは自動マージを無効にしません。

- 3 リモート PostgreSQL データベース ホストで、psql ツールを使用して PostgreSQL データベースに接続し、以下のコマンドを実行します。

```
CREATE EXTENSION IF NOT EXISTS "hstore";
```

```
CREATE EXTENSION IF NOT EXISTS "uuid-oss";
```

```
CREATE SCHEMA saas AUTHORIZATION vcac;
```

このコマンドではユーザーが vcac になっています。vRealize Automation が別のユーザーによって外部データベースに接続している場合は、このコマンド内の vcac をそのユーザーの名前で置き換えます。

```
CREATE EXTENSION IF NOT EXISTS "citext" SCHEMA saas;
```


4 アップグレードを実行します。

アップグレードが正常に完了した場合、システムは外部の PostgreSQL データベースを使用して期待どおりに動作します。外部 PostgreSQL データベースが適切に動作していることを確認します。

5 vRealize Automation 仮想アプライアンスにログインし、以下のコマンドを実行します。

```
/etc/bootstrap/postupdate.d/00-20-db-merge-external
```

```
/etc/bootstrap/postupdate.d/11-db-merge-external
```

レプリカ vRealize Automation アプライアンスのアップデートに失敗する

マスター アプライアンスのアップデート中に、レプリカ vRealize Automation アプライアンスのアップデートに失敗します。

原因

接続の問題やその他の障害により、レプリカ アプライアンスがアップデートに失敗する場合があります。その場合、マスター vRealize Automation アプライアンスの [更新] タブに警告メッセージが表示され、アップデートに失敗したレプリカが強調表示されます。

ソリューション

- 1 レプリカの仮想アプライアンスのスナップショットまたはバックアップをアップデート前の状態に戻して、パワーオンします。
- 2 レプリカの vRealize Automation アプライアンスの管理インターフェイスに root としてログインします。
`https://<vrealize-automation-appliance-FQDN>:5480`
- 3 [更新] - [設定] の順にクリックします。
- 4 [リポジトリをアップデート] セクションで、アップデートを VMware リポジトリからダウンロードするか CD-ROM から取得するかを選択します。
- 5 [ステータス] をクリックします。
- 6 [アップデートの確認] をクリックし、アップデートが利用可能かどうかを確認します。
- 7 [アップデートをインストール] をクリックします。
- 8 [OK] をクリックします。

アップデート処理が進行していることを示すメッセージが表示されます。

9 ログ ファイルを開いて、アップグレードが正常に進行していることを確認します。

- `/opt/vmware/var/log/vami/vami.log`
- `/var/log/vmware/horizon/horizon.log`

アップグレード中にログアウトし、アップグレードの完了前に再度ログインした場合は、ログ ファイルで更新の進行状況を継続して確認できます。**updatecli.log** ファイルに、アップグレード前のバージョンの vRealize Automation の情報が表示される場合があります。表示されたバージョンは、アップグレード プロセスの中で適切なバージョンに変わります。

アップデートが終了するまでの時間は、環境によって異なります。

10 アップデートが完了したら、仮想アプライアンスを再起動します。

- a [システム] をクリックします。
- b [再起動] をクリックし、選択を確認します。

11 [vRA 設定] - [クラスタ] の順に選択します。

12 マスター vRealize Automation アプライアンスの FQDN を入力し、[クラスタに参加] をクリックします。

.xml ファイルのバックアップ コピーによってシステムがタイムアウトする

vRealize Automation は、\VMware\vCAC\Server\ExternalWorkflows\xml\ ディレクトリにある拡張子が.xml であるすべてのファイルを登録します。このディレクトリに拡張子が.xml のバックアップ ファイルが含まれていると、システムは重複するワークフローを実行するため、システムがタイムアウトします。

ソリューション

回避策：このディレクトリのファイルをバックアップするときは、バックアップ ファイルを別のディレクトリに移動するか、バックアップ ファイルの拡張子を.xml 以外の拡張子に変更します。

laaS アップグレードの除外

laaS コンポーネントをアップグレードせずに vRealize Automation アプライアンスをアップデートできます。

laaS コンポーネントをアップグレードせずに vRealize Automation アプライアンスをアップデートする場合は、この手順を使用します。この手順では、

- laaS サービスは停止しません。
- 管理エージェントの更新をスキップします。
- vRealize Automation アプライアンスの更新後に、laaS コンポーネントの自動更新が行われないようにします。

手順

- 1 プライマリ vRealize Automation アプライアンス ノードへのセキュアなシェル接続を開きます。
- 2 コマンド プロンプトで、以下のコマンドを実行してグル ファイルを作成します。

touch /tmp/disable-iaas-upgrade

- 3 IaaS サービスを手動で停止します。
 - a IaaS Windows サーバにログインします。
 - b [スタート] - [管理ツール] - [サービス] を選択します。
 - c 次の順序でサービスを停止します。

注: IaaS Windows サーバはシャットダウンしないでください。

- 1 各 VMware vRealize Automation プロキシ エージェント。
 - 2 各 VMware DEM ワーカー。
 - 3 VMware DEM orchestrator。
 - 4 VMware vCloud Automation Center サービス。
- 4 プライマリ vRealize Automation アプライアンス管理コンソールにアクセスして、プライマリ vRealize Automation アプライアンスをアップデートします。

vRealize Automation で新規ディレクトリを作成できない

最初の同期コネクタを使用して新規ディレクトリを追加しようとすると失敗します。

問題

この問題は、`usr/local/horizon/conf/states/VSPHERE.LOCAL/3001/`にある、正しくない `config-state.json` ファイルが原因で発生します。

この問題の解決方法については、[ナレッジベースの記事 KB2145438](#) を参照してください。

vRealize Automation レプリカ仮想アプライアンスのアップデートがタイムアウトになる

マスター仮想アプライアンスをアップデートする際、vRealize Automation レプリカ仮想アプライアンスのアップデートがタイムアウトになります。

問題

マスター仮想アプライアンスをアップデートする際、マスター vRealize Automation 管理コンソールの更新タブには、アップデートのタイムアウト制限を超えたレプリカ仮想アプライアンスが強調表示されます。

原因

アップデートがタイムアウトするのは、パフォーマンスまたはインフラストラクチャの問題が原因です。

ソリューション

- 1 レプリカ仮想アプライアンスのアップデート状況を確認します。
 - a 完全修飾ドメイン名 (FQDN) `https://<va-hostname.domain.name>:5480` を使用してレプリカ仮想アプライアンスの管理コンソールに移動します。
 - b ユーザー名 **root** と、アプライアンスを展開したときに入力したパスワードを使用してログインします。
 - c [更新] - [ステータス] の順に選択し、アップデート状況を確認します。

次のいずれかの操作を行います。

 - アップデートに失敗した場合は、トラブルシューティングトピック [「レプリカ vRealize Automation アプライアンスのアップデートに失敗する」](#) の手順を実行します。
 - レプリカ仮想アプライアンスのアップグレードが進行中の場合は、アップグレードが完了するまで待機し、手順 2 に進みます。
- 2 仮想アプライアンスを再起動します。
 - a [システム] をクリックします。
 - b [再起動] をクリックし、選択を確認します。
- 3 [vRA 設定] - [クラスタ] の順に選択します。
- 4 マスター vRealize Automation 仮想アプライアンスの FQDN を入力し、[クラスタに参加] をクリックします。

アップグレード中に作成された展開が一部の仮想マシンに存在しない

アップグレード時に仮想マシンの状態が指定なしの場合、ターゲット環境で対応する展開が作成されません。

問題

アップグレード時に仮想マシンの状態がソース環境で指定なしの場合、対応する展開がターゲット環境で作成されません。アップグレード後に仮想マシンの状態が指定なしから変わると、バルク インポートを使用してターゲット展開にマシンをインポートすることができます。

信頼されていない証明書に関するエラー

vRealize Automation アプライアンス コンソールの [ログ ビューア] ページでインフラストラクチャを表示すると、**Certificate is not trusted** のような文言を含むエンドポイント接続障害レポートが表示されることがあります。

問題

vRealize Automation アプライアンス コンソールで、[インフラストラクチャ] - [監視] - [ログ] の順に選択します。[ログ ビューア] ページに、次のようなレポートが表示される場合があります。

エンドポイントへの接続に失敗しました。このエンドポイントへの安全な接続を確立できることを検証するには、[エンドポイント] ページで vSphere エンドポイントに移動し、[テスト接続] ボタンをクリックします。

内部例外: 証明書が信頼されていません (RemoteCertificateChainErrors)。件名: C=US, CN=vc6.mycompany.com
サムプリント: DC5A8816231698F4C9013C42692B0AF93D7E35F1

原因

vRealize Automation 7.3 以前のバージョンから 7.4 にアップグレードすると、元の環境にあったエンドポイントに変更が加えられます。最近 vRealize Automation 7.4 にアップグレードした環境では、安全な https 接続を使用するそれぞれの既存のエンドポイントを IaaS 管理者が確認する必要があります。「**Certificate is not trusted**」エラーが発生したエンドポイントは、適切に機能しません。

ソリューション

- 1 インフラストラクチャ管理者として vRealize Automation コンソールにログインします。
- 2 [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。
- 3 安全な接続が使用されている各エンドポイントについて、次の手順を実行します。
 - a [編集] をクリックします。
 - b [テスト接続] をクリックします。
 - c 証明書の詳細を確認し、この証明書を信頼する場合は、[OK] をクリックします。
 - d このエンドポイントによって使用されるすべての IaaS プロキシ エージェントの Windows サービスを再起動します。
- 4 インフラストラクチャの [ログ ビューア] ページに「**Certificate is not trusted**」エラーが表示されなくなったことを確認します。

vRealize Automation のインストールまたはアップグレードが失敗する

vRealize Automation のインストールまたはアップグレードが失敗し、エラー メッセージがログ ファイルに表示されます。

問題

vRealize Automation のインストールまたはアップグレードが失敗します。これは通常、インストールまたはアップグレード中に適用される修正に失敗した場合に発生します。ログ ファイルに次のようなエラー メッセージが表示されます。**Security error. Applying automatic fix for FIREWALL prerequisite failed. RPM Status 1: Pre install script failed, package test and installation skipped**

原因

Windows 環境のグループ ポリシーで、PowerShell スクリプトの実行が [有効] に設定されています。

ソリューション

- 1 Windows ホスト マシンで **gpedit.msc** を実行してローカル グループ ポリシー エディターを開きます。
- 2 [コンピューターの構成] の下にある左側のペインで、展開ボタンをクリックして [管理用テンプレート] - [Windows コンポーネント] - [Windows PowerShell] の順に開きます。
- 3 [スクリプトの実行を有効にする] で、状態を **Enabled** から **Not Configured** に変更します。

DEM および DEO コンポーネントを更新できない

vRealize Automation 7.2 から 7.3.x へのアップデート中に、DEM および DEO コンポーネントを更新できません

問題

vRealize Automation 7.2 から 7.3.x へのアップデート後、D: ドライブなどのカスタム パスにインストールされている DEM および DEO コンポーネントが更新されません。

[ナレッジベースの記事 KB2150517](#) を参照してください。

更新で管理エージェントのアップグレードに失敗する

vRealize Automation アプライアンス 管理コンソールの [ステータスの更新] ページで [更新のインストール] をクリックすると、管理エージェントに関するエラー メッセージが表示されます。

問題

アップグレード プロセスが成功しない。「**ノード x で管理エージェントをアップグレードできません**」というメッセージが表示されます。メッセージに複数のノードがリストされる場合もあります。

原因

この問題はさまざまな条件によって発生します。エラー メッセージには、影響を受けるマシンのノード ID のみが表示されます。コマンドが失敗したマシン上の管理エージェントについての詳細情報は、**All.log** ファイルに含まれています。

状況に応じて、影響を受けるノードで次のタスクを実行します。

ソリューション

- 管理エージェント サービスが実行されていない場合は、このサービスを開始し、仮想アプライアンスでアップグレードを再開します。
- 管理エージェント サービスが実行されており、管理エージェントがアップグレードされている場合は、仮想アプライアンスでアップグレードを再開します。
- 管理エージェント サービスが実行されているものの、管理エージェントがアップグレードされていない場合は、手動でアップグレードを実行します。
 - a ブラウザを開き、vRealize Automation アプライアンス上の [vRealize Automation IaaS のインストール] ページ (<https://<va-hostname.domain.name>:5480/install>) に移動します。
 - b 管理エージェントのインストーラをダウンロードして、実行します。
 - c 管理エージェントのマシンを再起動します。
 - d 仮想アプライアンスでアップグレードを再開します。

管理エージェントのアップグレードに失敗する

vRealize Automation から 7.2- 7.3.x へのアップグレード時に、管理エージェントのアップグレードに失敗します。

問題

フェイルオーバーの発生によってプライマリとセカンダリの管理エージェントのホストが入れ替わった場合、自動化されたアップグレード プロセスによって想定されるホストを見つけることができないため、アップグレードに失敗します。管理エージェントがアップグレードされていない各 IaaS ノードで、この手順を実行します。

ソリューション

- 1 管理エージェント ログ フォルダ (C:\Program Files (x86)\VMware\VCAC\Management Agent\Logs\) にある All.log を開きます。

インストール フォルダの場所は、デフォルトの場所とは異なる場合があります。

- 2 ログ ファイル内を検索して、古くなった仮想アプライアンスやパワーオフされている仮想アプライアンスに関するメッセージを探します。

たとえば、次のようなものです。INNER EXCEPTION: System.Net.WebException: Unable to connect to the remote server ---> System.Net.Sockets.SocketException: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond <IP_Address>:5480

- 3 管理エージェントの構成ファイル (C:\Program Files (x86)\VMware\VCAC\Management Agent\VMware.IaaS.Management.Agent.exe.config) を編集して、既存の alternativeEndpointaddress の値をプライマリ仮想アプライアンス エンドポイントの URL で置き換えます。

インストール フォルダの場所は、デフォルトの場所とは異なる場合があります。

VMware.IaaS.Management.Agent.exe.config での alternativeEndpointaddress の例を次に示します。

```
<alternativeEndpoint address="https://<FQDN>:5480/"
thumbprint="<thumbprint number>" />
```

- 4 管理エージェント Windows サービスを再起動し、All.log ファイルを参照してこのサービスが機能していることを確認します。
- 5 プライマリ vRealize Automation アプライアンスでアップグレード手順を実行します。

デフォルトのタイムアウト設定が原因で vRealize Automation のアップデートに失敗する

使用環境で、データベース同期のデフォルトの時間設定が短すぎる場合は、アップデートの時間設定を長くすることができます。

問題

データベースの同期にデフォルトのタイムアウト設定値である 3,600 秒よりも長い時間を要する一部の環境では、Vcac-Config SynchronizeDatabases コマンドのタイムアウト設定は不十分です。

API と Vcac-config.exe ユーティリティ ツール間の通信は、Vcac-Config.exe.config ファイルの cafeTimeoutInSeconds および cafeRequestPageSize プロパティの値によって制御されています。このファイルのパスは、<IaaS installation location>\VMware\VCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe.config です。

これらのオプション パラメータに値を指定して、SynchronizeDatabases コマンドのみに対して、デフォルトのタイムアウト値をオーバーライドすることができます。

| パラメータ | 短縮名 | 説明 |
|------------------------|-------|---|
| --DatabaseSyncTimeout | -dstm | SynchronizeDatabases に対してのみ HTTP 要求のタイムアウト値を秒単位で設定します。 |
| --DatabaseSyncPageSize | -dsps | 予約または予約ポリシーの同期に対してのみ、同期要求のページサイズを設定します。デフォルトは 10 です。 |

これらのパラメータが **Vcac-Config.exe.config** ファイルに設定されていない場合は、デフォルトのタイムアウト値が使用されます。

高可用性環境での IaaS のアップグレードが失敗する

プライマリ Web サーバ ノードでロード バランシングを有効にして IaaS アップグレード処理を実行すると失敗します。次のエラー メッセージが表示される可能性があります。「System.Net.WebException: 処理がタイムアウトしました」または「401 - Unauthorized: 無効な認証情報のため、アクセスは拒否されました。」

問題

ロード バランシングを有効にして IaaS をアップグレードすると、断続的に障害が発生する可能性があります。この場合、ロード バランシングを無効にして、再度 vRealize Automation アップグレードを実行する必要があります。

ソリューション

- 1 環境を更新前のスナップショットに戻します。
- 2 プライマリ IaaS Web サーバ ノードへのリモート デスクトップ接続を開きます。
- 3 C:\windows\system32\drivers\etc の Windows の hosts ファイルに移動します。
- 4 hosts ファイルを開き、Web サーバ ロード バランサをバイパスするように次の行を追加します。
<IP_address_of_primary_iaas_website_node vrealizeautomation_iaas_website_lb_fqdn>
例：
10.10.10.5 vra-iaas-web-lb.domain.com
- 5 hosts ファイルを保存して vRealize Automation の更新を再度実行します。
- 6 vRealize Automation の更新が完了したら、hosts ファイルを開いて、手順 4 で追加した行を削除します。

アップグレードの問題の回避

アップグレード プロセスを変更してアップグレードの問題を回避することができます。

ソリューション

vRealize Automation 環境のアップグレードで問題が発生した場合は、この手順を使用して、使用可能なフラグのいずれかを選択することによりアップグレード プロセスを変更します。

手順

- 1 プライマリ vRealize Automation アプライアンス ノードへのセキュアなシェル接続を開きます。

2 コマンド プロンプトで、以下のコマンドを実行してグル ファイルを作成します。

touch <available_flag>

例：**touch /tmp/disable-iaas-upgrade**

表 1-60. 使用可能なフラグ

| フラグ | 説明 |
|-----------------------------|--|
| /tmp/disable-iaas-upgrade | <ul style="list-style-type: none"> ■ 仮想アプライアンスの再起動後の IaaS アップグレード プロセスが実行されないようにします。 ■ 管理エージェントがアップグレードされないようにします。 ■ 自動の前提条件チェックおよび修正が実行されないようにします。 ■ IaaS サービスが停止しないようにします。 |
| /tmp/do-not-upgrade-ma | 管理エージェントがアップグレードされないようにします。このフラグは、管理エージェントを手動でアップグレードする場合に適しています。 |
| /tmp/skip-prereq-checks | 自動の前提条件チェックおよび修正が実行されないようにします。このフラグは、前提条件の自動修正に問題があるために手動で修正を適用した場合に適しています。 |
| /tmp/do-not-stop-services | IaaS サービスが停止しないようにします。アップグレードで、Manager Service、DEM、エージェントなどの IaaS Windows サービスを停止しません。 |
| /tmp/do-not-upgrade-servers | データベース、Web サイト、WAPI、リポジトリ、モデル Mfrontanager データ、Manager Service など、すべてのサーバ IaaS コンポーネントの自動アップグレードが実行されないようにします。 注: また、このフラグは、Manager Service 自動フェイルオーバー モードが有効にされないようにします。 |
| /tmp/do-not-upgrade-dems | DEM がアップグレードされないようにします。 |
| /tmp/do-not-upgrade-agents | IaaS プロキシ エージェントがアップグレードされないようにします。 |

3 選択したフラグのタスクを実行します。

表 1-61. 追加のタスク

| フラグ | タスク |
|-----------------------------|---|
| /tmp/disable-iaas-upgrade | <ul style="list-style-type: none"> ■ 管理エージェントを手動でアップグレードします。 ■ 必要なすべての IaaS 前提条件を手動で適用します。 ■ IaaS サービスを手動で停止します。 <ol style="list-style-type: none"> a IaaS Windows サーバにログインします。 b [スタート] - [管理ツール] - [サービス] を選択します。 c 次の順序でサービスを停止します。 <p>注: IaaS Windows サーバはシャットダウンしないでください。</p> <ol style="list-style-type: none"> a 各 VMware vRealize Automation プロキシ エージェント。 b 各 VMware DEM ワーカー。 c VMware DEM orchestrator。 d VMware vCloud Automation Center サービス。 ■ 仮想アプライアンス アップグレードが完了した後、IaaS アップグレードを手動で開始します。 |
| /tmp/do-not-upgrade-ma | 管理エージェントを手動でアップグレードします。 |
| /tmp/skip-prereq-checks | 必要なすべての IaaS 前提条件を手動で適用します。 |
| /tmp/do-not-stop-services | <p>IaaS サービスを手動で停止します。</p> <ol style="list-style-type: none"> 1 IaaS Windows サーバにログインします。 2 [スタート] - [管理ツール] - [サービス] を選択します。 3 次の順序でサービスを停止します。 <p>注: IaaS Windows サーバはシャットダウンしないでください。</p> <ol style="list-style-type: none"> a 各 VMware vRealize Automation プロキシ エージェント。 b 各 VMware DEM ワーカー。 c VMware DEM orchestrator。 d VMware vCloud Automation Center サービス。 |
| /tmp/do-not-upgrade-servers | |
| /tmp/do-not-upgrade-dems | |
| /tmp/do-not-upgrade-agents | |

4 プライマリ vRealize Automation アプライアンス管理コンソールにアクセスして、プライマリ vRealize Automation アプライアンスをアップデートします。

注: 各フラグは削除されるまでアクティブなままになるため、アップグレード後は次のコマンド **rm /<flag_path>/<flag_name>** を実行して選択したフラグを削除してください。例：
rm /tmp/disable-iaas-upgrade

vRealize Automation 6.2.5 から 7.4 へのアップグレード

vRealize Automation 6.2.5 環境を最新バージョンにアップグレードする場合は、6.2.5 環境に固有のアップグレード手順を使用します。

これは vRealize Automation 6.2.5 から 7.4 へのアップグレードに固有の情報です。他のサポート対象のアップグレードパスについては、[「vRealize Automation のアップグレード」](#)を参照してください。

vRealize Automation 6.2.5 から 7.4 へのアップグレード

現在の vRealize Automation 6.2.5 環境を 7.4 にインプレース アップグレードすることができます。環境のアップグレードには、このバージョンに固有のアップグレード手順を使用します。

インプレース アップグレードは 3 段階のプロセスです。次の順序で、現在の環境のコンポーネントを更新します。

- 1 vRealize Automation アプライアンス
- 2 IaaS Web サーバ
- 3 vRealize Orchestrator

すべての製品コンポーネントを同一バージョンにアップグレードする必要があります。

vRealize Production Test Upgrade Assist Tool は、vRealize Automation 6.2.x 環境を分析してアップグレードに関する問題を引き起こす可能性がある機能構成を特定し、使用環境のアップグレード準備ができていることを確認します。このツールおよび関連ドキュメントをダウンロードするには、[VMware vRealize Production Test Tool](#) の製品のダウンロード ページに移動します。

アップグレード後にサポートされないプロパティ ディクショナリの制御は、vRealize Orchestrator およびプロパティ ディクショナリの関係を使用して復元することができます。

元の環境に廃止されたコードを含むワークフローがある場合は、『[vRealize Automation Extensibility Migration Guide](#)』に掲載されている、イベント ブローカ サブスクリプションへの変換に必要なコード変更に関する情報を参照してください。

vRealize Automation 7.2 以降、JFrog Artifactory Pro は vRealize Automation アプライアンス にはバンドルされなくなりました。vRealize Automation の以前のバージョンからアップグレードする場合、アップグレード プロセスで JFrog Artifactory Pro は削除されます。詳細については、[ナレッジベースの記事 KB2147237](#) を参照してください。

注: vRealize Automation 6.2.5 環境をカスタマイズしている場合には、CCE サポート スタッフに連絡してアップグレードの追加情報を確認してください。

vRealize Automation のアップグレードの前提条件

vRealize Automation 6.2.5 からアップグレードする前に、次の前提条件を確認します。

システム構成要件

アップグレードを開始する前に、次のシステム要件を満たしていることを確認します。

- 環境内のアプライアンスとサーバのすべてが、最新バージョンのシステム要件を満たしているか確認します。
[VMware vRealize Automation のドキュメント](#)の vRealize Automation サポート マトリックスを参照してください。
- VMware の他の製品との互換性の詳細については、VMware Web サイトの VMware 製品の相互運用性マトリックスを参照してください。
- アップグレードする vRealize Automation の動作状況が安定していることを確認します。アップグレード前にすべての問題を修正します。
- vRealize Automation 6.2.5 からアップグレードする場合は、現在の vRealize Automation 環境に使用する vCloud Suite ライセンス キーを記録します。アップグレード時、既存のライセンス キーはデータベースから削除されます。
- ロード バランサのタイムアウト設定を、デフォルト設定から 10 分以上に変更したことを確認します。

ハードウェア構成要件

お使いの環境のハードウェアが vRealize Automation のターゲット リリースに適していることを確認します。

[\[vRealize Automation のハードウェア仕様および最大容量\]](#) を参照してください。

アップグレードを開始する前に、次のシステム要件を満たしていることを確認します。

- アップグレードをダウンロードする前に、現在のハードウェアを構成する必要があります。[\[vRealize Automation 6.2.5 の vCenter Server ハードウェア リソースの拡張\]](#) を参照してください。
- アップグレードを実行するには、少なくとも 18 GB の RAM、4 つの CPU、Disk1 = 50 GB、Disk3=25 GB、Disk4=50 GB が必要です。

仮想マシンが vCloud Networking and Security 上に配置されている場合は、多くの RAM 容量の割り当てが必要になる場合があります。

vCloud Networking and Security の一般的なサポートは終了しましたが、VCNS カスタム プロパティは NSX の用途に対して引き続き有効です。詳細については、[ナレッジベースの記事 KB2144733](#) を参照してください。

- これらのノードには、少なくとも 5 GB の空きディスク容量が必要です。
 - プライマリ IaaS Web サイト
 - Microsoft SQL データベース
 - Model Manager
- Model Manager Data がインストールされているプライマリ IaaS Web サイト ノードに、JAVA SE Runtime Environment 8 Update 161 (64 ビット) 以降がインストールされている必要があります。Java をインストールした後、JAVA_HOME 環境変数に新しいバージョンを設定する必要があります。
- アップグレードをダウンロードして実行するには、次のリソースが必要です。
 - ルートパーティションに少なくとも 5 GB
 - マスター vRealize Automation アプライアンス の `/storage/db` パーティションに 5 GB

- 各レプリカ仮想アプライアンスのルートパーティションに 5 GB
- **/storage/log** サブフォルダを確認し、以前のアーカイブ ZIP ファイルがあれば削除して容量をクリーンアップします。

一般的な前提条件

アップグレードを開始する前に、次のシステム要件を満たしていることを確認します。

- ディレクトリにバインドする権限を備えた `username@domain` 形式の Active Directory アカウントを利用できる。
- 次の条件を満たしている。
 - SAMaccountName 形式のアカウントへのアクセス権がある。
 - 動的なコンピュータ オブジェクトの作成によるドメインへのシステムの参加、または事前に作成されたオブジェクトへのマージを行うための、適切な権限を持っている。
- vRealize Automation アップグレードの影響を受けるまたはこのアップグレードに参加する、すべてのデータベースおよびロード バランサにアクセスできる。
- アップグレードの実行中、ユーザーがシステムを使用できないようにする。
- vRealize Automation に対してクエリを実行するアプリケーションがあれば、それを無効にする。
- Microsoft 分散トランザクション コーディネーター (MSDTC) が、すべての vRealize Automation および関連する SQL サーバ上で有効であることを確認する。手順については、[ナレッジベースの記事 KB2089503](#) を参照してください。
- お使いの環境に外部 vRealize Orchestrator アプライアンスがあり、外部 vRealize Orchestrator アプライアンスが Identity Appliance に接続されている場合は、vRealize Automation をアップグレードする前に vRealize Orchestrator をアップグレードします。
- アップグレード前に、vRealize Automation 仮想マシンを準備する追加のタスクを完了する必要があります。アップグレード前に、[ナレッジベースの記事 KB51531](#) を確認してください。
- ロード バランサのタイムアウト設定を、デフォルト設定から 10 分以上に変更したことを確認します。
- DynamicTypes プラグインを使用している場合は、vRealize Orchestrator DynamicType プラグイン設定をパッケージ ワークフローとしてエクスポートする必要があります。

/Library/Dynamic Types/Configuration/Export Configuration As Package

- 組み込みの PostgreSQL データベースで構成されている分散環境をアップグレードする場合は、次の手順を実行します。
 - a レプリカ ホストをアップグレードする前に、マスター ホストで **pgdata** ディレクトリ内のファイルを調べます。
 - b マスター ホスト上の PostgreSQL データ フォルダ (**/var/vmware/vpostgres/current/pgdata/**) に移動します。
 - c **pgdata** ディレクトリ内で開かれているファイルがあればすべて閉じ、**.swp** サフィックスを持つすべてのファイルを削除します。

- d このディレクトリ内のすべてのファイルの所有者 (postgres:users) が正しいことを確認します。

この vRealize Automation バージョンへのアップグレードに関する考慮事項

vRealize Automation 7 以降では、アップグレード プロセスの間、およびプロセス後にさまざまな機能が変更されます。vRealize Automation 6.2.5 環境を新しいバージョンにアップグレードする前に、変更内容を確認する必要があります。

アップグレード前に、これらの考慮事項を確認します。

アップグレードおよび Identity Appliance の仕様

vRealize Automation のアップグレード プロセスの間に、プロンプトに答えて Identity Appliance をアップグレードします。

ターゲット展開では VMware Identity Manager を使用します。

アップグレードおよびライセンス

アップグレードの際、vRealize Automation 6.2.5 ライセンス、および vCloud Suite 6.x ライセンスがある場合、これらは削除されます。vRealize Automation 7.4 の vRealize Automation アプライアンス管理コンソールで再度ライセンスを入力する必要があります。

ここでは、vRealize Automation アプライアンスにライセンス キー情報を入力して、仮想アプライアンスおよび IaaS の vRealize Automation ライセンスを使用します。ライセンス情報が、IaaS ユーザー インターフェイスに表示されなくなります。IaaS はライセンス確認を実行しなくなります。エンドポイントおよび割り当ては、エンド ユーザー 使用許諾契約書 (EULA) に基づいて適用されます。

注: vCloud Suite 6.x ライセンス キーを vRealize Automation 6.2.5 に使用する場合は、アップグレード前に書き留めます。アップグレード時、既存のライセンス キーはデータベースから削除されます。

アップグレード中またはアップグレード後のライセンス情報の再入力については、「[ライセンス キーの更新](#)」を参照してください。

ロールのアップグレード方法について

vRealize Automation をアップグレードする場合、組織の既存のロール割り当ては維持されます。また、アップグレードでは、追加されたブループリント アーキテクト ロールをサポートするために、いくつかのロール割り当てが作成されます。

次のアーキテクト ロールは、デザイン キャンパスのブループリント定義をサポートするために使用します。

- アプリケーション アーキテクト：既存のコンポーネントとブループリントを組み合わせ、複合ブループリントを作成
- インフラストラクチャ アーキテクト：仮想マシン ブループリントの作成および管理
- XaaS アーキテクト：XaaS ブループリントの作成と管理
- ソフトウェア アーキテクト：ソフトウェア コンポーネントの作成と管理

vRealize Automation 7 では、デフォルトではテナント管理者およびビジネス グループ マネージャはブループリントを設計できません。アップグレード後のテナント管理者およびビジネス グループ マネージャには、インフラストラクチャ アーキテクト ロールが付与されます。

vRealize Automation 6.2.x のソース バージョンで仮想マシンを再構成できるユーザーは、新しいバージョンにアップグレードした後、仮想マシンの所有権を変更できます。

次のロール割り当ては、アップグレード中に実行されます。表にリストされていないロールは、アップデート後の環境で同一のロール名にアップグレードされます。

表 1-62. アップグレード中に割り当てられるロール

| アップグレード前のロール | アップグレード後のロール |
|-----------------|-------------------------------------|
| テナント管理者 | テナント管理者およびインフラストラクチャ アーキテクト |
| ビジネス グループ マネージャ | ビジネス グループ マネージャおよびインフラストラクチャ アーキテクト |
| サービス アーキテクト | XaaS 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 |

ロールの詳細については、[vRealize Automation でのテナントのロールと責任](#)を参照してください。

ブループリントのアップグレード方法について

原則として、公開済みのブループリントは公開済みのブループリントとしてアップグレードされます。

ただし、この原則には例外があります。マルチマシン ブループリントは、ブループリント コンポーネントを含む複合ブループリントとしてアップグレードされます。サポートされていない設定が含まれるマルチマシン ブループリントは未公開としてアップグレードされます。

注: vRealize Automation 7.x により、展開でブループリントのスナップショットが作成されます。展開で CPU や RAM などのマシン プロパティを更新する際に再構成の問題が発生した場合は、ナレッジベースの記事 [KB2150829 vRA 7.x Blueprint Snapshotting](#) を参照してください。

ブループリントのアップグレードの詳細については、「[アップグレードおよび vApp ブループリント、vCloud エンドポイント、および vCloud 予約](#)」および「[マルチマシン ブループリントをアップグレードする方法について](#)」を参照してください。

アップグレードおよび vApp ブループリント、vCloud エンドポイント、および vCloud 予約

vApp (vCloud) エンドポイントを含む環境はアップグレードできません。vApp (vCloud) エンドポイントがあると、この vRealize Automation バージョンにアップグレードできません。

アップグレード前の展開環境に vApp (vCloud) エンドポイントがある場合は、マスター仮想アプライアンスでアップグレードが失敗します。ユーザー インターフェイスとログにメッセージが表示されます。アップグレード前の展開環境に vApp (vCloud) エンドポイントが含まれているかどうかを確認するには、IaaS 管理者ユーザーとして vRealize Automation コンソールにログインします。[インフラストラクチャ] - [エンドポイント] を選択します。エンドポイントのリストに vApp (vCloud) エンドポイントが含まれている場合は、この vRealize Automation バージョンにアップグレードできません。

vCloud Air または vCloud Director リソース向けの管理対象 vApp は、ターゲットの vRealize Automation 環境でサポートされません。

注: 次の承認ポリシー タイプは廃止されています。アップグレードの完了後に使用可能な承認ポリシー タイプのリストに表示されても、使用することはできません。

- サービス カタログ - カタログ アイテム申請 - vApp
- サービス カタログ - カタログ アイテム申請 - vApp コンポーネント

ターゲット展開では vCloud Air および vCloud Director のエンドポイントおよび予約を作成できます。vCloud Air または vCloud Director の仮想マシン コンポーネントを使用してブループリントを作成することもできます。

マルチマシン ブループリントをアップグレードする方法について

サポートされる vRealize Automation 6.2.x バージョンの展開から、管理対象サービス、マルチマシン ブループリントをアップグレードできます。

マルチマシン ブループリントをアップグレードすると、コンポーネント ブループリントは別個の単一マシン ブループリントとしてアップグレードされます。マルチマシン ブループリントは、以前の子ブループリントが別個のブループリント コンポーネントとしてネストされた複合ブループリントとしてアップグレードされます。

アップグレードにより、ソース マルチマシン ブループリントの各コンポーネント ブループリントに対応する 1 台の仮想マシン コンポーネントを含むターゲット展開に、単一の複合ブループリントが作成されます。新しいバージョンでサポートされていない設定がブループリントにある場合、そのブループリントはアップグレードされ、ドラフト ステータスに設定されます。たとえば、マルチマシン ブループリントにプライベート ネットワーク プロファイルが含まれる場合、そのプロファイル設定はアップグレードの間無視され、ブループリントはドラフト ステータスでアップグレードされます。ドラフトのブループリントを編集してサポートされるネットワーク プロファイル情報を入力し、公開することができます。

注: 移行前の環境内の公開済みブループリントがドラフト ステータスのブループリントにアップグレードされると、ブループリントはサービスまたは資格の一部ではなくなります。アップグレードされた vRealize Automation バージョンでブループリントを更新および公開した後は、必要な承認ポリシーと資格を再度作成する必要があります。

マルチマシン ブループリント設定の一部は、ターゲットの vRealize Automation 環境でサポートされません。これには、プライベート ネットワーク プロファイル、PLR エッジ設定が関連付けられたルーティング ネットワーク プロファイルが含まれます。カスタム プロパティを使用して PLR エッジ設定 (`VCNS.LoadBalancerEdgePool.Names`) を指定していた場合、このカスタム プロパティはアップグレードされます。

マルチマシン ブループリントを、vSphere エンドポイントおよび NSX のネットワーク設定とセキュリティ設定を使用してアップグレードできます。アップグレードしたブループリントでは、デザイン キャンパスに NSX のネットワーク コンポーネントとセキュリティ コンポーネントが含まれます。

注: マルチマシン ブループリントのルーティング ゲートウェイ仕様は、予約で定義されたように、アップグレードされます。ただし、ターゲットの vRealize Automation 展開は、関連付けられた PLR エッジ設定を含むルーティング プロファイルの予約をサポートしません。ソース予約に PLR エッジのルーティング ゲートウェイ値が含まれる場合、予約はアップグレードされますが、ルーティング ゲートウェイ設定は無視されます。その結果、アップグレードでログ ファイルにエラー メッセージが生成され、予約は無効になります。

アップグレードでは、参照されているネットワークおよびセキュリティ コンポーネント名からスペースと特殊文字が削除されます。

注: vRealize Automation 7.x により、展開でブループリントのスナップショットが作成されます。展開で CPU や RAM などのマシン プロパティを更新する際に再構成の問題が発生した場合は、ナレッジベースの記事 [KB2150829 vRA 7.x Blueprint Snapshotting](#) を参照してください。

設定タイプに応じて、ネットワークおよびセキュリティ情報は新規ブループリントで複数の異なる設定としてキャプチャされます。

- プロパティ ページのブループリント全体に対する設定。この情報には、アプリケーションの隔離、トランスポート ゾーン、およびルーティング ゲートウェイまたは NSX Edge 予約ポリシーの情報が含まれます。
- デザイン キャンパスの NSX ネットワークおよびセキュリティ コンポーネントの vSphere 仮想マシン コンポーネントに対して使用できる設定。
- デザイン キャンパスの個々の vSphere 仮想マシン コンポーネントの [ネットワークおよびセキュリティ] タブの設定。

アップグレードおよび物理エンドポイント、予約、およびブループリント

物理エンドポイントを含む環境はアップグレードできません。物理エンドポイントがあると、vRealize Automation のアップグレード プロセスが失敗します。

vRealize Automation 6.2.x 展開環境に物理エンドポイントがある場合は、マスター仮想アプライアンスでアップグレードが失敗します。移行のインターフェイスとログにエラー メッセージが表示されます。vRealize Automation 6.2.x 展開環境に物理エンドポイントがあるかどうかを確認するには、vRealize Automation に IaaS 管理者ユーザーとしてログインします。[インフラストラクチャ]-[エンドポイント] の順に選択し、エンドポイントのリストを確認します。リストに **Platform Type Physical** エンドポイントがある場合は、vRealize Automation 7.0 以降にアップグレードできません。

ブループリントの物理エンドポイント、予約、および仮想マシン コンポーネントは、vRealize Automation 7.0 以降ではサポートされません。

アップグレードおよびネットワーク プロファイルの設定

プライベート ネットワーク プロファイルは、vRealize Automation 7 以降ではサポートされません。これらのプロファイルは、アップグレード中に無視されます。PLR エッジ設定が関連付けられたルーティング ネットワーク プロファイルも、vRealize Automation 7 以降ではサポートされません。これらのプロファイルもアップグレード時に無視されます。

プライベート ネットワーク プロファイル タイプは、vRealize Automation 7 以降ではサポートされません。

vRealize Automation アップグレード プロセスで、アップグレード前の環境のプライベート ネットワーク プロファイルが検出された場合、そのネットワーク プロファイルは無視されます。これらのプライベート ネットワークを参照するロード バランサもまた、アップグレードでは無視されます。PLR Edge 設定が関連付けられたルーティング ネットワーク プロファイルにも同様のアップグレード条件が当てはまります。ネットワーク プロファイル構成もアップグレードされません。

予約にプライベート ネットワーク プロファイルが含まれる場合、そのプライベート ネットワーク プロファイル設定はアップグレード時に無視されます。予約はアップグレード環境で無効としてアップグレードされます。

予約に PLR エッジ設定が関連付けられたルーティング ネットワーク プロファイルが含まれる場合、ルーティング ネットワーク プロファイル仕様はアップグレード時に無視されます。予約はアップグレード環境で無効としてアップグレードされます。

ネットワーク設定を含むマルチマシン ブループリントのアップグレードの詳細については、「[マルチマシン ブループリントをアップグレードする方法について](#)」を参照してください。

アップグレードと使用可能なアクション

仮想マシン アクションをアップグレードすることはできません。

ブループリント仕様に基づいて、プロビジョニングされた仮想マシン上で実行できるアクションはアップグレードされません。仮想マシンで実行できるアクションを再作成するには、特定のアクションのみを有効にするようにブループリントの資格をカスタマイズします。

詳細については、[資格に含まれるアクション](#)を参照してください。

アップグレードおよびカスタム プロパティ

vRealize Automation が提供するカスタム プロパティは、アップグレードされた環境ですべて利用できます。カスタム プロパティとプロパティ グループはアップグレードされます。

用語および関連する変更

アップグレード前の環境で作成したすべてのビルド プロファイルは、プロパティ グループとしてアップグレードされます。用語「ビルド プロファイル」は使用されなくなりました。

用語「プロパティ セット」は使用されなくなり、CSV プロパティ セット ファイルは使用できなくなりました。

カスタム プロパティ名の大文字と小文字の区別

vRealize Automation 7.0 より前のバージョンでは、カスタム プロパティ名で大文字と小文字が区別されました。vRealize Automation 7.0 以降では、カスタム プロパティ名の大文字と小文字が区別されます。アップグレード中に、カスタム プロパティ名が正確に一致する必要があります。これにより、プロパティ値が相互にオーバーライドせず、プロパティ ディクショナリの定義と確実に一致するようになります。たとえば、カスタム プロパティ **hostname** と別のカスタム プロパティ **HOSTNAME** は、vRealize Automation 7.0 以降では異なるカスタム プロパティと見なされます。カスタム プロパティ **hostname** とカスタム プロパティ **HOSTNAME** は、アップグレード中に互いにオーバーライドしません。

カスタム プロパティ名に含まれるスペース

vRealize Automation のこのリリースにアップグレードする前に、カスタム プロパティ名からスペース文字を削除します。たとえば、スペースをアンダースコア文字で置き換えます。これにより、アップグレードされた vRealize Automation 環境でカスタム プロパティが認識されるようになります。vRealize Automation カスタム プロパティ名にスペースは使用できません。この問題は、以前のリリースの vRealize Automation、vRealize Orchestrator、またはその両方で使用されるカスタム プロパティにスペースが含まれており、この vRealize Orchestrator をアップグレードした環境を使用する場合にも影響があります。

予約されたプロパティ名

いくつかのキーワードが予約済みになっているため、アップグレードされるプロパティの一部が影響を受ける場合があります。ブループリント コードで使用される一部のキーワードは、vRealize CloudClient のブループリント インポート機能を使用するなどの方法でインポートできます。これらのキーワードは予約済みと見なされ、アップグレードされるプロパティには使用できません。これらのキーワードには、**cpu**、**storage**、**memory** が含まれますが、これに限定されるわけではありません。

Application Services のアップグレード

Application Services のアップグレードは、vRealize Automation 7 以降でサポートされます。

vRealize Automation 7.4 に正常に移行した後で、vRealize Automation Application Services Migration Tool を使用して、アプリケーション サービスをアップグレードできます。このツールをダウンロードするには、次の手順を実行します。

- 1 [ダウンロード VMware vRealize Automation](#) をクリックします。
- 2 [ドライバとツール] - [VMware vRealize Application Services Migration Tool] を選択します。

アップグレードおよびアドバンスド サービス設計

vRealize Automation 7 以降にアップグレードすると、アドバンスド サービス設計のアイテムが XaaS 要素にアップグレードされます。

XaaS コンポーネントはデザイン キャンパスで使用できます。

アップグレードおよびブループリント 価格情報

vRealize Automation 7.0 から価格プロファイルがサポートされなくなり、アップグレード時にターゲットの展開に移行されません。ただし、vRealize Business for Cloud との高度な統合を利用することで、vRealize Automation リソース コストを管理できます。

vRealize Business for Cloud は現在、vRealize Automation と緊密に連携しており、次の価格計算の拡張機能をサポートしています。

- vRealize Business for Cloud では中央から、次の項目の価格ポリシーを柔軟に定義：
 - インフラストラクチャのリソース、マシン、およびアプリケーションのブループリント
 - vCenter Server、vCloud Director、Amazon Web Services、Azure、OpenStack などのサポート対象エンドポイント向けの、vRealize Automation 内のプロビジョニングされた仮想マシン
 - プロビジョニングされた仮想マシンの運用価格、1 回限りの価格、およびカスタム プロパティの価格
 - 環境内の仮想マシンの価格を含む、導入価格
- vRealize Business for Cloud のロールベースのショーバック レポート
- vRealize Business for Cloud の新しい機能を最大限に活用

アップグレード前に、ソース vRealize Automation インスタンスから既存のコスト レポートをリファレンス用にエクスポートできます。アップグレードの終了後、vRealize Business for Cloud のインストールと設定を行って、価格計算を行うことができます。

注: vRealize Automation 7.4 には、vRealize Business for Cloud 7.4 以降のみとの互換性があります。

アップグレードとカタログ アイテム

vRealize Automation 6.2.x から最新バージョンにアップグレードした後、サービス カタログに表示される一部のカタログ アイテムが申請できません。

vRealize Automation を最新バージョンに移行した後、以下のプロパティ定義を使用したカタログ アイテムはサービス カタログに表示されますが、申請できません。

- コントロール タイプ：チェック ボックスまたはリンク。
- 属性：関係、正規表現、またはプロパティのレイアウト。

vRealize Automation 7.x では、プロパティ定義でこれらの要素が使用されなくなりました。プロパティ定義を再作成するか、組み込みのコントロール タイプまたは属性以外の vRealize Orchestrator スクリプト アクションを使用するようにプロパティ定義を構成する必要があります。詳細については、「[アップグレード後にサービス カタログに表示されるカタログ アイテムを申請できない](#)」を参照してください。

vRealize Automation のアップグレード チェックリスト

vRealize Automation 6.2.5 から 7.4 にアップグレードする場合は、特定の順序ですべての vRealize Automation コンポーネントを更新します。

アップグレードを完了するまでの作業を追跡するため、チェックリストを使用します。タスクは示された順序で行うようにしてください。

注： コンポーネントは、規定の順序で、すべてアップグレードする必要があります。順序を変えると、アップグレード後に予想外の動作が発生したり、アップグレードを完了できない場合があります。

アップグレードの順序は、アップグレードする対象が最小環境なのか、それとも複数の vRealize Automation アプライアンスがある分散環境なのかによって異なります。

表 1-63. vRealize Automation 最小環境をアップグレードするためのチェックリスト

| タスク | 方法 |
|--|---|
|  現在のインストールをバックアップする。バックアップを作成することは非常に重要です。 | システムのバックアップ方法とリストア方法の詳細については、「 既存の vRealize Automation 6.2.5 環境のバックアップ 」を参照してください。 一般情報については、 http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf の「Symantec Netbackup を使用したバックアップとリストアの構成」(Configuring Backup and Restore by Using Symantec Netbackup)を参照してください。 |
|  vRealize Automation 6.2.x 仮想マシンをアップグレードするために準備する。 | ナレッジベースの記事 KB51531 を アップグレード前に参照して、関連する修正を環境で実行する必要があります。 |
|  IaaS サーバ上の vRealize Automation Windows サービスをシャットダウンする。 | IaaS Windows サーバ上の vRealize Automation サービスの停止 を参照してください。 |

表 1-63. vRealize Automation 最小環境をアップグレードするためのチェックリスト (続き)

| タスク | 方法 |
|---|--|
| <input type="checkbox"/> 共通のコンポーネント カタログがインストールされている場合は、アップグレード前にアンインストールする必要があります。 | <p>共通コンポーネント カタログのコンポーネントのアンインストール方法については、『共通のコンポーネント カタログのインストール ガイド』を参照してください。</p> <p>このガイドが入手できない場合は、各 IaaS ノードで次の手順を実行します。</p> <ol style="list-style-type: none"> 1 IaaS ノードにログインします。 2 [開始] をクリックします。 3 [プログラムとファイルの検索] テキスト ボックスに services と入力します。 4 [サービス] をクリックします。 5 [サービス] ウィンドウの右ペインで各 IaaS サービスを右クリックし、[停止] を選択して各サービスを停止します。 6 [スタート] > [コントロール パネル] > [プログラムと機能] の順にクリックします。 7 インストール済みの共通コンポーネント カタログの各コンポーネントを右クリックし、[アンインストール] を選択します。 8 [スタート] > [コマンド プロンプト] の順にクリックします。 9 コマンド プロンプトで iisreset を実行します。 |
| <input type="checkbox"/> この vRealize Automation バージョンへのアップグレードの考慮事項を確認して、何をアップグレードできるか、できないか、アップグレードしたアイテムの動作がどのように異なるのかを確認します。 プループリント、予約、エンドポイントを含む、一部のアイテムはアップグレードできません。サポート対象外の構成があるとアップグレードはブロックされます。 | <p>「この vRealize Automation バージョンへのアップグレードに関する考慮事項」 を参照してください。</p> |
| <input type="checkbox"/> ハードウェア リソースを構成する。 | <p>「vRealize Automation 6.2.5 の vCenter Server ハードウェア リソースの拡張」 を参照してください。</p> |
| <input type="checkbox"/> vRealize Automation アプライアンスにアップデートをダウンロードする。 | <p>「vRealize Automation アプライアンスの更新のダウンロード」 を参照してください。</p> |
| <input type="checkbox"/> vRealize Automation アプライアンスにアップデートをインストールする。 | <p>「vRealize Automation アプライアンスでのアップデートのインストール」 を参照してください。</p> |
| <input type="checkbox"/> シングルサインオンユーティリティを VMware Identity Manager ユーティリティにアップデードする。 | <p>「VMware Identity Manager 用の Single Sign-On パスワードの更新」 を参照してください。</p> |
| <input type="checkbox"/> ライセンス キーを更新する。 | <p>「ライセンス キーの更新」 を参照してください。</p> |
| <input type="checkbox"/> ID ストアを VMware Identity Manager に移行する。 | <p>「VMware Identity Manager への ID ストアの移行」</p> |
| <input type="checkbox"/> IaaS コンポーネントをアップグレードする。 | <p>「vRealize Automation のアップグレード後の IaaS サーバ コンポーネントのアップグレード」 を参照してください。</p> |

表 1-63. vRealize Automation 最小環境をアップグレードするためのチェックリスト (続き)

| タスク | 方法 |
|---|---|
|  外部 vRealize Orchestrator をアップグレードする。 | 「vRealize Automation で使用するスタンドアロン vRealize Orchestrator アプライアンスのアップグレード」 を参照してください。 「vRealize Automation で使用するための外部 vRealize Orchestrator Appliance クラスタのアップグレード」 を参照してください。 |
|  Active Directory 接続にユーザーまたはグループを追加する。 | 「Active Directory 接続へのユーザーまたはグループの追加」 を参照してください。 |

表 1-64. vRealize Automation 分散環境をアップグレードするためのチェックリスト

| タスク | 方法 |
|--|--|
|  現在のインストールをバックアップする。バックアップを作成することは非常に重要です。 | システムのバックアップ方法とリストア方法の詳細については、 「既存の vRealize Automation 6.2.5 環境のバックアップ」 を参照してください。 詳細情報については、 http://www.vmware.com/pdf/vrealize-backup-and-restore-netbackup.pdf の「Symantec Netbackup を使用したバックアップとリストアの構成」(Configuring Backup and Restore by Using Symantec Netbackup) を参照してください。 |
|  vRealize Automation 6.2.x 仮想マシンをアップグレードするために準備する。 | ナレッジベースの記事 KB51531 を アップグレード前に参照して、関連する修正を環境で実行する必要があります。 |
|  IaaS Windows サーバの vRealize Automation サービスをシャットダウンする。 | 「IaaS Windows サーバ上の vRealize Automation サービスの停止」 を参照してください。 |
|  共通のコンポーネント カタログがインストールされている場合は、アップグレード前にアンインストールする必要があります。 | 共通コンポーネント カタログのコンポーネントのアンインストール方法については、『 共通のコンポーネント カタログのインストール ガイド 』を参照してください。 このガイドが入手できない場合は、各 IaaS ノードで次の手順を実行します。 <ol style="list-style-type: none"> 1 IaaS ノードにログインします。 2 [開始] をクリックします。 3 [プログラムとファイルの検索] テキスト ボックスに services と入力します。 4 [サービス] をクリックします。 5 [サービス] ウィンドウの右ペインで各 IaaS サービスを右クリックし、[停止] を選択して各サービスを停止します。 6 [スタート] > [コントロール パネル] > [プログラムと機能] の順にクリックします。 7 インストール済みの共通コンポーネント カタログの各コンポーネントを右クリックし、[アンインストール] を選択します。 8 [スタート] > [コマンド プロンプト] の順にクリックします。 9 コマンド プロンプトで iisreset を実行します。 |
|  アップグレードのためのハードウェア リソースを構成する。 | 「vRealize Automation 6.2.5 の vCenter Server ハードウェア リソースの拡張」 を参照してください。 |

表 1-64. vRealize Automation 分散環境をアップグレードするためのチェックリスト (続き)

| タスク | 方法 |
|--|--|
|  ロード バランサを無効にする。 | <p>各セカンダリ ノードを無効にし、次のアイテムの vRealize Automation 健全性モニタを削除します。</p> <ul style="list-style-type: none"> ■ vRealize Automation アプライアンス ■ IaaS Web サイト ■ IaaS Manager Service <p>正常にアップグレードするには、次の手順を確認します。</p> <ul style="list-style-type: none"> ■ ロード バランサのトラフィックは、プライマリ ノードにのみ送信されます。 ■ vRealize Automation 健全性モニタは、アプライアンス、Web サイトおよび Manager Service で削除されます。 |
|  vRealize Automation アプライアンスにアップデートをダウンロードする。 | 「vRealize Automation アプライアンスの更新のダウンロード」 を参照してください。 |
|  インストール環境で最初の vRealize Automation アプライアンスにアップデートをインストールする。アプライアンスをマスターとして指定している場合は、このアプライアンスを最初にアップグレードします。 | 「vRealize Automation アプライアンスでのアップデートのインストール」 を参照してください。 |
|  シングル サインオン ユーティリティを VMware Identity Manager ユーティリティにアップグレードする。 | 「VMware Identity Manager 用の Single Sign-On パスワードの更新」 を参照してください。 |
|  ライセンス キーを更新する。 | 「ライセンス キーの更新」 を参照してください。 |
|  ID ストアを VMware Identity Manager ユーティリティに移行する。 | 「VMware Identity Manager への ID ストアの移行」 |
|  残りの vRealize Automation アプライアンスにアップデートをインストールする。 | 「追加の vRealize Automation アプライアンスでのアップデートのインストール」 |
|  IaaS コンポーネントをアップグレードする。 | 「vRealize Automation のアップグレード後の IaaS サーバ コンポーネントのアップグレード」 を参照してください。 |
|  外部 vRealize Orchestrator をアップグレードする。 | <p>「vRealize Automation で使用するスタンドアロン vRealize Orchestrator アプライアンスのアップグレード」 を参照してください。</p> <p>「vRealize Automation で使用するための外部 vRealize Orchestrator Appliance クラスターのアップグレード」 を参照してください。</p> |
|  ロード バランサを有効にする。 | 「ロード バランサの有効化」 |

vRealize Automation 環境のユーザー インターフェイス

vRealize Automation 環境は、複数のインターフェイスで使用および管理します。

ユーザー インターフェイス

これらの表は、vRealize Automation 環境を管理するために使用するインターフェイスを示しています。

表 1-65. vRealize Automation 管理コンソール

| 目的 | アクセス | 必要な認証情報 |
|---|---|-------------------------------------|
| <p>以下のシステム管理者のタスクには、vRealize Automation コンソールを使用します。</p> <ul style="list-style-type: none"> ■ テナントを追加します。 ■ vRealize Automation ユーザー インターフェイスをカスタマイズします。 ■ メール サーバを構成します。 ■ イベント ログを表示します。 ■ vRealize Orchestrator を構成します。 | <ol style="list-style-type: none"> 1 ブラウザを起動し、仮想アプライアンスの完全修飾ドメイン名を使用して、vRealize Automation アプライアンスのスプラッシュ ページを開きます。 https://<vra-vd-hostname.domain.name> 2 [vRealize Automation コンソール] をクリックします。 vRealize Automation コンソールを開くには、次の URL を使用することもできます : https://<vra-vd-hostname.domain.name>/vcac 3 ログインします。 | <p>システム管理者ロールを持つユーザーである必要があります。</p> |

表 1-66. vRealize Automation テナント コンソール。このインターフェイスは、サービスやリソースの作成および管理に使用するプライマリ ユーザー インターフェイスです。

| 目的 | アクセス | 必要な認証情報 |
|---|---|---|
| <p>以下のタスクには、vRealize Automation を使用します。</p> <ul style="list-style-type: none"> ■ 新しい IT サービス ブループリントを申請します。 ■ クラウドおよび IT リソースを作成および管理します。 ■ カスタム グループを作成および管理します。 ■ ビジネス グループを作成、管理します。 ■ ユーザーにロールを割り当てます。 | <ol style="list-style-type: none"> 1 ブラウザを起動し、仮想アプライアンスの完全修飾ドメイン名とテナントの URL 名を使用して、テナントの URL を入力します。 https://<vra-vd-hostname.domain.name>/vcac/org/<tenant_URL_name> 2 ログインします。 | <p>以下の 1 つ以上のロールを持つユーザーである必要があります。</p> <ul style="list-style-type: none"> ■ アプリケーション アーキテクト ■ 承認管理者 ■ カタログ管理者 ■ コンテナ管理者 ■ コンテナ アーキテクト ■ 健全性サービス ユーザー ■ インフラストラクチャ アーキテクト ■ セキュアなエクスポートの利用者 ■ ソフトウェア アーキテクト ■ テナント管理者 ■ XaaS アーキテクト |

表 1-67. vRealize Automation アプライアンス管理。このインターフェイスは、仮想アプライアンス管理インターフェイス (VAMI) と呼ばれます。

| 目的 | アクセス | 必要な認証情報 |
|---|--|--|
| <p>以下のタスクには vRealize Automation アプライアンス管理を使用します。</p> <ul style="list-style-type: none"> 登録されているサービスのステータスを表示します。 システム情報を表示、およびアプライアンスを再起動またはシャットダウンします。 カスタム エクスペリエンス改善プログラムへの参加を管理します。 ネットワーク ステータスを表示します。 更新ステータスを表示、およびアップデートをインストールします。 管理設定を管理します。 vRealize Automation ホスト設定を管理します。 SSO の設定を管理します。 製品ライセンスを管理します。 vRealize Automation Postgres データベースを設定します。 vRealize Automation メッセージングを設定します。 vRealize Automation ログを設定します。 IaaS コンポーネントをインストールします。 既存の vRealize Automation 環境から移行します。 IaaS コンポーネントの証明書を管理します。 Xenon サービスを設定します。 | <ol style="list-style-type: none"> ブラウザを起動し、仮想アプライアンスの完全修飾ドメイン名を使用して、vRealize Automation アプライアンスのブラッシュ ページを開きます。 https://<vra-va-hostname.domain.name> [vRealize Automation アプライアンス管理] をクリックします。 次の URL を使用して vRealize Automation アプライアンス管理を開くこともできます : https://<vra-va-hostname.domain.name:5480> ログインします。 | <ul style="list-style-type: none"> ユーザー名 : root パスワード : vRealize Automation アプライアンスを展開したときに 入力したパスワード。 |

表 1-68. vRealize Orchestrator クライアント

| 目的 | アクセス | 必要な認証情報 |
|---|--|--|
| <p>以下のタスクには、vRealize Orchestrator クライアントを使用します。</p> <ul style="list-style-type: none"> アクションを作成します。 ワークフローを作成します。 ポリシーを管理します。 パッケージをインストールします。 ユーザーおよびユーザー グループの権限を管理します。 URI オブジェクトにタグを追加します。 インベントリを表示します。 | <ol style="list-style-type: none"> ブラウザを起動し、仮想アプライアンスの完全修飾ドメイン名を使用して、vRealize Automation のブラッシュ ページを開きます。 https://<vra-va-hostname.domain.name> ローカル コンピュータに client.jnlp ファイルをダウンロードするには、[vRealize Orchestrator Client] をクリックします。 client.jnlp ファイルを右クリックして [起動] を選択します。 [続行しますか?] ダイアログボックスで、[続行] をクリックします。 ログインします。 | <p>システム管理者ロールを持つユーザーであるか、または vRealize Orchestrator コントロール センターの認証プロバイダの設定で構成されている vcoadmins グループに属している必要があります。</p> |

表 1-69. vRealize Orchestrator コントロール センター

| 目的 | アクセス | 必要な認証情報 |
|---|---|---|
| vRealize Automation に組み込まれているデフォルトの vRealize Orchestrator インスタンスの設定を編集するには、vRealize Orchestrator コントロール センターを使用します。 | <ol style="list-style-type: none"> 1 ブラウザを起動し、仮想アプライアンスの完全修飾ドメイン名を使用して、vRealize Automation アプライアンスのスプラッシュ ページを開きます。 https://<vra-vd-hostname.domain.name> 2 [vRealize Automation アプライアンス管理] をクリックします。 次の URL を使用して vRealize Automation アプライアンス管理を開くこともできます : https://<vra-vd-hostname.domain.name:5480> 3 ログインします。 4 [vRA 設定] - [Orchestrator] の順にクリックします。 5 [Orchestrator ユーザー インターフェイス] を選択します。 6 [開始] をクリックします。 7 Orchestrator ユーザー インターフェイスの URL をクリックします。 8 ログインします。 | <p>ユーザー名</p> <ul style="list-style-type: none"> ■ ロールベースの認証が設定されていない場合は、root と入力します。 ■ ロールベースの認証で設定されている場合は、vRealize Automation ユーザー名を入力します。 <p>パスワード</p> <ul style="list-style-type: none"> ■ ロールベースの認証が設定されていない場合、vRealize Automation アプライアンスを展開したときに入力したパスワードを入力します。 ■ ロールベースの認証でユーザー名が設定されている場合は、ユーザー名に対するパスワードを入力します。 |

表 1-70. Linux コマンド プロンプト

| 目的 | アクセス | 必要な認証情報 |
|--|---|---|
| <p>vRealize Automation アプライアンス ホストなどのホストでは、以下のタスクには Linux コマンド プロンプトを使用します。</p> <ul style="list-style-type: none"> ■ サービスの開始または停止 ■ 構成ファイルの編集 ■ コマンドの実行 ■ データの取得 | <ol style="list-style-type: none"> 1 vRealize Automation アプライアンス ホストで、コマンド プロンプトを開きます。 ローカル コンピュータでコマンド プロンプトを開く方法の 1 つは、PuTTY などのアプリケーションを使用して、ホストでセッションを開始することです。 2 ログインします。 | <ul style="list-style-type: none"> ■ ユーザー名 : root ■ パスワード : vRealize Automation アプライアンスを展開したときに作成したパスワード。 |

表 1-71. Windows コマンド プロンプト

| 目的 | アクセス | 必要な認証情報 |
|---|--|--|
| laaS ホストなどのホスト上で、Windows コマンド プロンプトを使用してスクリプトを実行できます。 | <ol style="list-style-type: none"> 1 laaS ホスト上で、Windows にログインします。 ローカル コンピュータからログインする方法の 1 つは、リモート デスクトップ セッションを開始することです。 2 Windows コマンド プロンプトを開きます。 コマンド プロンプトを開く方法の 1 つは、ホスト上で [スタート] アイコンを右クリックし、[コマンド プロンプト] または [コマンド プロンプト (管理者)] を選択することです。 | <ul style="list-style-type: none"> ■ ユーザー名 : 管理者権限を持つユーザー。 ■ パスワード : ユーザーのパスワード。 |

vRealize Automation に統合された VMware 製品のアップグレード

vRealize Automation をアップグレードする場合、vRealize Automation 環境に統合されているすべての VMware 製品を管理する必要があります。

vRealize Automation 環境が 1 つ以上の他の製品に統合されている場合は、他の製品をアップデートする前に vRealize Automation をアップグレードする必要があります。vRealize Business for Cloud が vRealize Automation に統合されている場合は、vRealize Automation をアップグレードする前に vRealize Business for Cloud を登録解除する必要があります。

vRealize Automation をアップグレードする場合は、統合製品を管理するための推奨ワークフローを実行します。

- 1 vRealize Automation をアップグレードします。
- 2 VMware vRealize Operations Manager をアップグレードします。
- 3 VMware vRealize Log Insight をアップグレードします。
- 4 VMware vRealize Business for Cloud をアップグレードします。

このセクションでは、vRealize Automation 環境に統合する場合の vRealize Business for Cloud の管理について詳細に説明します。

vRealize Automation に統合された vRealize Operations Manager のアップグレード

vRealize Automation のアップグレード後に vRealize Operations Manager をアップグレードします。

手順

- 1 vRealize Automation をアップグレードします。
- 2 vRealize Operations Manager をアップグレードします。詳細については、[VMware vRealize Operations Manager のドキュメント](#)の「Updating Your Software」を参照してください。

vRealize Automation に統合された vRealize Log Insight のアップグレード

vRealize Automation のアップグレード後に vRealize Log Insight をアップグレードします。

手順

- 1 vRealize Automation をアップグレードします。
- 2 vRealize Log Insight をアップグレードします。詳細については、[VMware vRealize Log Insight のドキュメント](#)の「vRealize Log Insight のアップグレード」を参照してください。

vRealize Automation に統合された vRealize Business for Cloud のアップグレード

vRealize Automation 環境をアップグレードする場合は、vRealize Business for Cloud への接続を一度登録解除して、再度登録する必要があります。

vRealize Automation 環境をアップグレードする場合は、この手順を実行して vRealize Business for Cloud のサービスの継続を確認します。

手順

- 1 vRealize Automation から vRealize Business for Cloud を登録解除します。[VMware vRealize Business for Cloud のドキュメント](#)の「vRealize Business for Cloud の vRealize Automation からの登録解除」を参照してください。
- 2 vRealize Automation をアップグレードします。

- 3 必要に応じて、vRealize Business for Cloud をアップグレードします。[VMware vRealize Business for Cloud のドキュメント](#)の「vRealize Business for Cloud のアップグレード」を参照してください。
- 4 vRealize Automation に vRealize Business for Cloud を登録します。[VMware vRealize Business for Cloud のドキュメント](#)の「vRealize Business for Cloud の vRealize Automation への登録」を参照してください。

vRealize Automation のアップグレードの準備

vRealize Automation を 6.2.5 から 7.4 にアップグレードする前に、さまざまなタスクを実行する必要があります。

タスクはアップグレード チェックリストに表示されている順序で実行します。[「vRealize Automation のアップグレード チェックリスト」](#)を参照してください。

vRealize Automation をアップグレードする場合のバックアップの前提条件

vRealize Automation 6.2.5 を 7.4 にアップグレードする前に、バックアップの前提条件を満たします。

前提条件

- 移行前の環境が正しくインストールされ、構成されていることを確認します。
- 移行前の環境の各アプライアンスで、次のディレクトリのすべての vRealize Automation アプライアンス構成ファイルをバックアップします。
 - `/etc/vcac/`
 - `/etc/vco/`
 - `/etc/apache2/`
 - `/etc/rabbitmq/`
- ご使用のシステム上の vRealize Automation 外部ワークフロー構成 (xmldb) ファイルをバックアップします。バックアップ ファイルは、一時ディレクトリに格納します。これらのファイルは、`\VMware\VC\Server\ExternalWorkflows\xmldb\` にあります。移行後に、新しいシステムで xmldb ファイルをリストアします。[「外部ワークフローのタイムアウト ファイルのリストア」](#)を参照してください。
 関連する問題については、[「xml ファイルのバックアップ コピーによってシステムがタイムアウトする」](#)を参照してください。
- 外部 vRealize Automation PostgreSQL データベースをバックアップします。PostgreSQL データベースが外部のものかどうかを確認するには、これらの手順を実行します。
 - a 完全修飾ドメイン名 `https://<va-hostname.domain.name>:5480/` を使用して、vRealize Automation アプライアンス管理コンソールにログインします。
 分散環境では、プライマリ vRealize Automation アプライアンス管理コンソールにログインします。
 - b [vRA 設定] - [データベース] の順に選択します。
 - c vRealize Automation PostgreSQL データベース ノードのホストが vRealize Automation アプライアンスのホストと異なる場合は、データベースをバックアップします。データベース ノードのホストがアプライアンスのホストと同じ場合は、データベースをバックアップする必要はありません。

PostgreSQL データベースのバックアップについては、<https://www.postgresql.org/>を参照してください。

- テナントの構成と、割り当てられているユーザーのスナップショットを作成します。
- カスタマイズしたすべてのファイル (**DataCenterLocations.xml** など) をバックアップします。
- 各仮想アプライアンスおよび IaaS サーバのスナップショットを作成します。vRealize Automation のアップグレードが失敗した場合に備えて、システム全体のバックアップに関する基本ガイドラインには必ず従ってください。[vRealize Automation インストールのバックアップおよびリカバリ](#)を参照してください。

既存の vRealize Automation 6.2.5 環境のバックアップ

アップグレードする前に、vRealize Automation 6.2.5 環境コンポーネントのシャットダウンおよびスナップショットの作成を行います。

アップグレードする前に、システムのシャットダウンと次のコンポーネントのスナップショットの作成を行います。

- vRealize Automation IaaS サーバ (Windows ノード)
- vRealize Automation アプライアンス (Linux ノード)
- vRealize Automation (SSO) ID ノード

アップグレードが失敗した場合は、スナップショットを使用して前回の正常な構成に戻り、別のアップグレードを試します。

前提条件

- 組み込み PostgreSQL データベースが高可用性モードであることを確認します。その場合は、現在のマスターノードを特定します。<http://kb.vmware.com/kb/2105809> のナレッジベースの記事を参照してください。
- 環境内に外部 PostgreSQL データベースがある場合は、データベース バックアップ ファイルを作成します。
- vRealize Automation Microsoft SQL データベースが IaaS サーバ上でホストされていない場合は、データベース バックアップ ファイルを作成します。詳細については、SQL Server データベースの完全バックアップの作成に関する記事 [Microsoft Developer Network](#) を参照してください。
- アップグレードのためのバックアップの前提条件が完了していることを確認します。
- シャットダウン時にシステムのスナップショットを作成したことを確認します。スナップショットを作成するときには、この方法が推奨されます。『vSphere 6.0 のドキュメント』を参照してください。

注: vRealize Automation アプライアンスと IaaS コンポーネントをバックアップする場合、インメモリ スナップショットと静止スナップショットを無効にします。

- **app.config** ファイルを変更した場合は、そのファイルのバックアップを作成します。[\[app.config ファイルに行ったログの変更のリストア\]](#)を参照してください。
- 外部ワークフロー構成 (xmldb) ファイルのバックアップを作成します。[\[外部ワークフローのタイムアウト ファイルのリストア\]](#)を参照してください。
- 現在のフォルダの外にバックアップ ファイルを保存する場所があることを確認します。[\[.xml ファイルのバックアップ コピーによってシステムがタイムアウトする\]](#)を参照してください。

手順

- 1 vCenter Server にログインします。

- 2 これらの vRealize Automation 6.2.5 コンポーネントを見つけます。
 - vRealize Automation IaaS サーバ (Windows ノード)
 - vRealize Automation アプライアンス (Linux ノード)
 - vRealize Automation (SSO) ID ノード
- 3 次の仮想マシンのそれぞれについて、仮想マシンを選択し、[ゲストのシャットダウン] をクリックして、仮想マシンが停止するのを待ちます。次の順序でこれらの仮想マシンをシャットダウンします。
 - a IaaS プロキシ エージェント仮想マシン
 - b DEM ワーカー仮想マシン
 - c DEM Orchestrator 仮想マシン
 - d Manager Service 仮想マシン
 - e Web サービス仮想マシン
 - f セカンダリ vRealize Automation 仮想マシン
 - g プライマリ vRealize Automation 仮想マシン
 - h Manager 仮想マシン (配置されている場合)
 - i Identity Appliance
- 4 各 vRealize Automation 6.2.5 仮想マシンのスナップショットを作成します。
- 5 各 vRealize Automation アプライアンス ノードのクローンを作成します。

クローン作成された仮想マシン上でアップグレードを実行します。
- 6 クローン作成された仮想マシンをアップグレードする前に、それぞれ元の vRealize Automation アプライアンス仮想マシンをパワーオフします。

元の仮想マシンはパワーオフ状態で保持し、システムを復旧する必要がある場合にのみ使用します。

次のステップ

[\[vRealize Automation 6.2.5 の vCenter Server ハードウェア リソースの拡張\]](#)。

vRealize Automation 6.2.5 の vCenter Server ハードウェア リソースの拡張

vRealize Automation 6.2.5 からアップグレードする前に、各 vRealize Automation アプライアンスのハードウェア リソースを拡張する必要があります。

この手順では、Windows vCenter Server クライアントを使用していることを前提としています。

前提条件

- 各 vRealize Automation アプライアンスのクローンがあることを確認します。
- 各アプライアンスのクローンに対して、vCenter Server 内に 140 GB 以上の空き容量があることを確認します。
- 元のアプライアンスがパワーオフしていることを確認します。

手順

- 1 vCenter Server にログインします。
- 2 クローンを作成した vRealize Automation アプライアンスのアイコンを右クリックし、[設定の編集] を選択します。
- 3 [メモリ] を選択し、値を 18 GB に設定します。
- 4 [CPU] を選択し、仮想ソケット数の値を 4[]に設定します。
- 5 仮想ディスク 1 のサイズを 50 GB に拡張します。
 - a ディスク 1 を選択します。
 - b サイズを 50 GB に変更します。
 - c [OK] をクリックします。
- 6 ディスク 3 がない場合は、次の手順を実行して、ディスク サイズが 25 GB のディスク 3 を追加します。
 - a [リソース] テーブルの上の [追加] をクリックして仮想ディスクを追加します。
 - b [デバイス タイプ] の [ハード ディスク] を選択し、[次へ] をクリックします。
 - c [新規仮想ディスクを作成] を選択し、[次へ] をクリックします。
 - d [ディスク サイズ] の値を 25 GB に設定します。
 - e [仮想マシンで格納] を選択し、[次へ] をクリックします。
 - f [モード] の [非依存] オプションが選択解除されており、[仮想デバイス モード] の [SCSI (0:2)] が選択されていることを確認し、[次へ] をクリックします。

推奨設定の承認を促されたら、推奨設定を承認します。
 - g [完了] をクリックします。
 - h [OK] をクリックします。
- 7 以前の vRealize Automation リリースの既存の仮想ディスク 4 がある場合は、次の手順を実行します。
 - a プライマリ仮想アプライアンスのクローンをパワーオンして、1 分間待機します。
 - b セカンダリ仮想アプライアンスのクローンをパワーオンします。
 - c プライマリ仮想アプライアンスのクローンで新しいコマンド プロンプトを開き、**/etc/fstab** に移動します。
 - d プライマリ仮想アプライアンスのクローンで **fstab** ファイルを開き、Wal_Archive ログ先行書き込みが含まれている **/dev/sdd** で始まる行を削除します。
 - e プライマリ仮想アプライアンスのクローンでファイルを保存します。
 - f セカンダリ仮想アプライアンスのクローンで新しいコマンド プロンプトを開き、**/etc/fstab** に移動します。
 - g セカンダリ仮想アプライアンスのクローンで **fstab** ファイルを開き、Wal_Archive ログ先行書き込みが含まれている **/dev/sdd** で始まる行を削除します。

- h セカンダリ仮想アプライアンスのクローンでファイルを保存します。
 - i セカンダリ仮想アプライアンスのクローンをパワーオフして、1 分間待機します。
 - j プライマリ仮想アプライアンスのクローンをパワーオフします。
 - k クローンを作成した vRealize Automation プライマリ アプライアンスのアイコンを右クリックし、[設定の編集] を選択します。
 - l クローンを作成したプライマリ仮想アプライアンス マシンでディスク 4 を削除します。
 - m クローンを作成した vRealize Automation セカンダリ アプライアンスのアイコンを右クリックし、[設定の編集] を選択します。
 - n クローンを作成したセカンダリ仮想アプライアンス マシンでディスク 4 を削除します。
- 8 クローン作成されたプライマリおよびセカンダリの仮想アプライアンス マシンにディスク サイズが 50 GB のディスク 4 を追加するには、この手順を実行します。
- a [リソース] テーブルの上の [追加] をクリックして仮想ディスクを追加します。
 - b [デバイス タイプ] の [ハード ディスク] を選択し、[次へ] をクリックします。
 - c [新規仮想ディスクを作成] を選択し、[次へ] をクリックします。
 - d [ディスク サイズ] の値を 50 GB に設定します。
 - e [仮想マシンで格納] を選択し、[次へ] をクリックします。
 - f [モード] の [非依存] オプションが選択解除されており、[仮想デバイス モード] の [SCSI (0:3)] が選択されていることを確認し、[次へ] をクリックします。
- 推奨設定の承認を促されたら、推奨設定を承認します。
- g [完了] をクリックします。
 - h [OK] をクリックします。
- 9 クローン作成されたプライマリ仮想アプライアンス マシンとクローン作成されたセカンダリ仮想アプライアンス マシンのスナップショットを作成します。

次のステップ

[「システム全体のパワーオン」](#)。

システム全体のパワーオン

アップグレードを行うために vCenter Server のハードウェア リソースを増加させた後、アップグレードを実行する前にシステムをパワーオンします。

前提条件

- [「既存の vRealize Automation 6.2.5 環境のバックアップ」](#)。
- [「vRealize Automation 6.2.5 の vCenter Server ハードウェア リソースの拡張」](#)。

手順

1 システム全体をパワーオンします。

手順については、vRealize Automation バージョン 6.2 のトピック [vRealize Automation の起動](#) を参照してください。

注: 高可用性の環境がある場合は、この手順を実行して仮想アプライアンスをパワーオンします。

- a 最後にパワーオフした仮想アプライアンスをパワーオンします。
 - b 1 分待ちます。
 - c 残りの仮想アプライアンスをパワーオンします。
-

2 システムが完全に機能することを確認します。

次のステップ

[\[IaaS Windows サーバ上の vRealize Automation サービスの停止\]](#)。

IaaS Windows サーバ上の vRealize Automation サービスの停止

必要な場合は、次の手順を使用して、IaaS サービスを実行している各サーバ上で vRealize Automation サービスを停止できます。

アップグレードの開始前に、各 IaaS Windows サーバ上の vRealize Automation サービスを停止します。

注: アップグレード プロセスでは、Manager Service のパッシブ バックアップ インスタンスを除き、すべてのサービスの起動タイプを [自動] に設定する必要があります。サービスを [手動] に設定すると、アップグレード プロセスが失敗します。

手順

1 IaaS Windows サーバにログインします。

2 [スタート] - [管理ツール] - [サービス] を選択します。

3 次の順序でサービスを停止します。仮想マシンをシャットダウンしないようにしてください。

各仮想マシンには管理エージェントがあります。この管理エージェントは各サービス セットと一緒に停止する必要があります。

- a 各 VMware vCloud Automation Center エージェント
- b 各 VMware DEM-ワーカー
- c VMware DEM-Orchestrator
- d VMware vCloud Automation Center Service

- 4 ロード バランサを使用する分散展開の場合は、各セカンダリ ノードを無効にして、次のアイテムの vRealize Automation 健全性モニターを削除します。

- a vRealize Automation アプライアンス
- b IaaS Web サイト
- c IaaS Manager Service

ロード バランサのトラフィックがプライマリ ノードのみに送られていること、および vRealize Automation の健全性モニターが、アプライアンス、Web サイト、管理サービスで削除されていることを確認します。これらの条件が揃わない場合、アップグレードは失敗します。

- 5 以下の手順を実行することで、Microsoft Internet Information Services (IIS) でホストされている IaaS サービスが稼動していることを確認します。

- a ブラウザで **<https://webhostname/Repository/Data/MetaModel.svc>** という URL に移動して、Web リポジトリが稼動していることを確認します。成功した場合、エラーは返されず、XML 形式のモデルのリストが表示されます。
- b IaaS 仮想マシンの Web ノードにある **Repository.log** ファイルを調べて、OK のステータスが報告されていることを確認します。このファイルは VCAC ホーム フォルダの **/Server/Model Manager Web/Logs/Repository.log** にあります。

分散型 IaaS Web サイトの場合は、MMD なしでセカンダリ Web サイトにログインし、Microsoft IIS サーバを一時的に停止します。MetaModel.svc の接続を確認します。ロード バランサのトラフィックがプライマリ Web ノードのみを通過することを確認するには、Microsoft IIS サーバを起動します。

次のステップ

[「vRealize Automation アプライアンスの更新のダウンロード」](#)。

vRealize Automation アプライアンスの更新のダウンロード

アプライアンス管理コンソールでアップデートの有無をチェックし、次の方法のいずれかを使用して、アップデートをダウンロードすることができます。

最適なアップグレード パフォーマンスを得るためには、ISO ファイルによる方法を使用します。

アプライアンスをアップグレードする際の潜在的な問題を回避する場合や、アプライアンスのアップグレード中に問題が発生した場合は、[VMware ナレッジベースの記事「vRealize Automation upgrade fails due to duplicates in the vRealize Orchestrator database \(KB54987\)」](#)を参照してください。

■ [VMware リポジトリからの vRealize Automation アプライアンス更新のダウンロード](#)

vmware.com Web サイトの公開リポジトリから vRealize Automation アプライアンスのアップデートをダウンロードできます。

■ [CD-ROM ドライブで使用する仮想アプライアンスのアップデートのダウンロード](#)

仮想アプライアンスは、アプライアンスが仮想 CD-ROM ドライブから読み取る ISO ファイルからアップデートできます。これが推奨される方法です。

VMware リポジトリからの vRealize Automation アプライアンス更新のダウンロード

vmware.com Web サイトの公開リポジトリから vRealize Automation アプライアンスのアップデートをダウンロードできます。

前提条件

- 既存の vRealize Automation 環境をバックアップします。
- vRealize Automation アプライアンスが起動していることを確認します。

手順

- 1 プライマリ vRealize Automation アプライアンスで、vRealize Automation アプライアンスを展開したときに入力したパスワードを使用して、**root** として vRealize Automation アプライアンス管理にログインします。
- 2 [アップデート] タブをクリックします。
- 3 [設定] をクリックします。
- 4 (オプション) [自動アップデート] パネルで、アップデートをチェックする頻度を設定します。
- 5 [リポジトリをアップデート] パネルで、[デフォルト リポジトリの使用] を選択します。
デフォルト リポジトリが正しい VMware.com URL に設定されます。
- 6 [設定の保存] をクリックします。

CD-ROM ドライブで使用する仮想アプライアンスのアップデートのダウンロード

仮想アプライアンスは、アプライアンスが仮想 CD-ROM ドライブから読み取る ISO ファイルからアップデートできます。これが推奨される方法です。

ISO ファイルをダウンロードし、プライマリ アプライアンスを設定したら、このファイルを使用してアプライアンスをアップグレードします。

前提条件

- 既存の vRealize Automation 環境をバックアップします。
- vRealize Automation アプライアンスをアップデートする前に、アップグレードで使用するすべての CD-ROM ドライブが有効になっていることを確認します。vSphere クライアントで仮想マシンに CD-ROM ドライブを追加する際の詳細については、vSphere のドキュメントを参照してください。

手順

- 1 アップデート リポジトリ ISO ファイルをダウンロードします。
 - a ブラウザを起動し、www.vmware.com の [vRealize Automation 製品ページ](#) に移動します。
 - b [vRealize Automation ダウンロード リソース] をクリックして VMware ダウンロード ページに移動します。
 - c 適切なファイルをダウンロードします。

- 2 システム上でダウンロードしたファイルを探し、このサイズが VMware ダウンロード ページ上のファイルと同一であることを確認します。ダウンロード ページに記載されているチェックサムを使用して、ダウンロードしたファイルの整合性を検証します。詳細については、VMware ダウンロード ページの下にあるリンクを参照してください。
- 3 プライマリ仮想アプライアンスが起動していることを確認します。
- 4 プライマリ仮想アプライアンスの CD-ROM ドライブを、ダウンロードした ISO ファイルに接続します。
- 5 プライマリ vRealize Automation アプライアンスで、vRealize Automation アプライアンスを展開したときに入力したパスワードを使用して、**root** として vRealize Automation アプライアンス管理にログインします。
- 6 [アップデート] タブをクリックします。
- 7 [設定] をクリックします。
- 8 [アップデートリポジトリ] で、[CD-ROM アップデートを使用] を選択します。
- 9 [設定の保存] をクリックします。

vRealize Automation アプライアンスの更新

アップグレードの前提条件をすべて満たして仮想アプライアンスの更新をダウンロードした後、vRealize Automation 6.2.5 アプライアンスを 7.4 に更新します。また、プライマリ vRealize Automation アプライアンスの再設定も実行します。

プライマリ vRealize Automation アプライアンスをアップグレードした後、環境内のその他のノードを次の順序でアップグレードします。

- 1 各セカンダリ vRealize Automation アプライアンス
- 2 IaaS Web サイト
- 3 IaaS Manager Service
- 4 IaaS DEM
- 5 IaaS エージェント
- 6 各外部 vRealize Orchestrator インスタンスのアップグレードまたは移行

vRealize Automation アプライアンスでのアップデートのインストール

vRealize Automation 6.2.5 アプライアンスに vRealize Automation アップデートをインストールし、アプライアンスを設定します。

PostgreSQL 外部データベースのサポートは vRealize Automation 7.1 で廃止になります。アップグレード プロセスにより、既存の PostgreSQL 外部データベースのデータは vRealize Automation アプライアンスに含まれる PostgreSQL 内部データベースにマージされます。

CEIP によって収集されるデータの詳細と、VMware がそのデータを使用する目的については、Trust & Assurance Center (<http://www.vmware.com/trustvmware/ceip.html>) を参照してください。

アップデートのインストール中は管理コンソールを閉じないでください。

アップグレード プロセスで問題が発生する場合は、[「vRealize Automation アップグレードのトラブルシューティング」](#)を参照してください。

前提条件

- ダウンロード方法を選択し、アップデートをダウンロードしたことを確認します。[「vRealize Automation アプライアンスの更新のダウンロード」](#)を参照してください。
- 分散型展開の場合は、[「既存の vRealize Automation 6.2.5 環境のバックアップ」](#)を参照してください。
- ロード バランサを伴うデプロイの場合は、トラフィックがプライマリ ノードのみに送られていること、および健全性モニターが無効になっていることを確認します。
- 共通のコンポーネント カタログのコンポーネントが環境にインストールされている場合は、アップグレード前にこのコンポーネントをアンインストールします。詳細については、『共通のコンポーネント カタログのインストール ガイド』を参照してください。このガイドが利用できない場合は、[「vRealize Automation のアップグレード チェックリスト」](#)の別の手順を参照してください。
- jdbc:postgresql データベース接続が、マスター PostgreSQL ノードの外部 IP アドレスをポイントしていることを確認します。
 - a 各 vRealize Automation アプライアンスで、新しいコマンド プロンプトを開きます。
 - b `/etc/vcac/server.xml` に移動し、`server.xml` をバックアップします。
 - c `server.xml` を開きます。
 - d 必要に応じて、Postgres データベースをポイントしている `server.xml` ファイルのエントリ `jdbc:posgresql` を編集して、外部 PostgreSQL 用のマスター PostgreSQL ノードまたは組み込みの PostgreSQL 用のプライマリ仮想アプライアンスの外部 IP アドレスをポイントするようにします。
 例: `jdbc:postgresql://198.15.100.60:5432/vcac`
- アップグレードの前に、すべての保存済みおよび進行中の申請が正常に完了したことを確認します。

手順

- 1 vRealize Automation アプライアンス管理コンソールを開きます。
 - a プライマリ vRealize Automation アプライアンスで、vRealize Automation アプライアンスを展開したときに入力したパスワードを使用して、**root** として vRealize Automation アプライアンス管理にログインします。
 - b ユーザー名 **root** と、アプライアンスの展開時に入力したパスワードを使用してログインします。
- 2 [サービス] をクリックし、各サービス (iaas-service を除く) が登録済みとしてリストされていることを確認します。
- 3 [更新] - [設定] の順に選択します。
- 4 次のいずれかのオプションを選択します。
 - [デフォルト リポジトリの使用]。
 - [CDROM の更新を使用]
- 5 [設定の保存] をクリックします。
- 6 [ステータス] を選択します。

- 7 [アップデートの確認] をクリックし、アップデートが利用可能かどうかを確認します。
- 8 (オプション) vRealize Automation アプライアンスのインスタンスの場合は、[アプライアンスのバージョン] 領域で [詳細] をクリックすると、リリース ノートの場所が表示されます。
- 9 [アップデートをインストール] をクリックします。
- 10 [OK] をクリックします。

アップデート処理が進行していることを示すメッセージが表示されます。

- 11 (オプション) ディスク 1 のサイズを 50 GB に手動で変更していない場合は、以下の手順を実行します。
 - a 仮想アプライアンスの再起動を要求するシステム プロンプトが表示されたら、[システム] をクリックし、[再起動] をクリックします。
再起動中、アップデートに必要な容量がシステムによって調整されます。
 - b システムの再起動後、再度 vRealize Automation アプライアンス管理コンソールにログインし、各サービス (iaas-service を除く) が登録済みとしてリストされていることを確認して、[更新] - [ステータス] を選択します。
 - c [アップデートのチェック] および [アップデートのインストール] をクリックします。

- 12 アップグレードの進行状況を表示するには、次のログ ファイルを開きます。

- /opt/vmware/var/log/vami/updatecli.log
- /opt/vmware/var/log/vami/vami.log
- /var/log/vmware/horizon/horizon.log
- /var/log/bootstrap/*.log

アップグレード中にログアウトし、アップグレードの完了前に再度ログインした場合は、ログ ファイルで更新の進行状況を継続して確認できます。updatecli.log ファイルに、アップグレード前のバージョンの vRealize Automation の情報が表示される場合があります。表示されたバージョンは、アップグレード プロセスの中で適切なバージョンに変わります。

アップデートが終了するまでの時間は、環境によって異なります。

- 13 アプライアンス管理コンソールで [テレメトリ] をクリックします。カスタマー エクスペリエンス向上プログラム (CEIP) への参加に関する注意を読み、プログラムに参加するかしないかを選択します。

CEIP によって収集されるデータの詳細と、VMware がそのデータを使用する目的については、Trust & Assurance Center (<http://www.vmware.com/trustvmware/ceip.html>) を参照してください。

カスタマ エクスペリエンス改善プログラムの詳細については、「[vRealize Automation のカスタマ エクスペリエンス改善プログラムへの参加または脱退](#)」を参照してください。

次のステップ

[\[VMware Identity Manager 用の Single Sign-On パスワードの更新\]](#)。

VMware Identity Manager 用の Single Sign-On パスワードの更新

アップデートをインストールしたら、VMware Identity Manager 用の Single Sign-On のパスワードを更新する必要があります。

VMware Identity Manager は、Identity Appliance および vSphere SSO の各コンポーネントを置き換えます。

手順

- 1 vRealize Automation アプライアンス管理コンソールからログアウトし、ブラウザを終了してから再びブラウザを開いてログインし直します。

- 2 [vRA 設定] - [SSO] の順に選択します。

- 3 VMware Identity Manager の新しいパスワードを入力して [設定の保存] をクリックします。

簡単なパスワードは使用しないでください。表示されるエラー メッセージ「SSO サーバが接続されていません。サービスの再起動には数分必要です。」は無視してかまいません。

パスワードが許可されます。

高可用性を展開している場合、パスワードを最初の vRealize Automation アプライアンス ノードに入力すると、すべてのセカンダリ vRealize Automation アプライアンス ノードに伝達されます。

- 4 仮想アプライアンスを再起動します。

- a [システム] タブをクリックします。

- b [再起動] をクリックし、選択を確認します。

- 5 すべてのサービスが実行されていることを確認します。

- a vRealize Automation アプライアンス管理コンソールにログインします。

- b コンソールの [サービス] タブをクリックします。

- c [更新] タブをクリックして、サービス起動の進行状況を監視します。

35 個以上のサービスが表示されます。

- 6 IaaS サービス以外のすべてのサービスが登録されていることを確認します。

vRealize Code Stream ライセンス キーなしでは、release-management service は開始されません。

次のステップ

[「ライセンス キーの更新」](#)。

ライセンス キーの更新

最新バージョンの vRealize Automation アプライアンスを使用するには、ライセンス キーをアップグレードする必要があります。

手順

- 1 完全修飾ドメイン名 `https://<va-hostname.domain.name>:5480` を使用して仮想アプライアンスの管理コンソールに移動します。

- 2 ユーザー名 **root** と、アプライアンスを展開したときに入力したパスワードを使用してログインします。

3 [vRA 設定] - [ライセンス] の順に選択します。

[ライセンス] タブが利用できない場合は、以下の手順に従って作業を繰り返します。

- a 管理コンソールからログアウトします。
- b ブラウザのキャッシュを消去します。

4 [新規ライセンス キー] テキスト ボックスに新しいライセンス キーを入力します。

エンドユーザー使用許諾契約書 (EULA) に従って、エンドポイントと割り当てにフラグが付けられます。

5 [送信キー] をクリックします。

次のステップ

[「VMware Identity Manager への ID ストアの移行」](#)。

VMware Identity Manager への ID ストアの移行

vRealize Automation 6.2.5 から最新のバージョンにアップグレードする場合、ID ストアを移行する必要があります。

以下の手順では必要に応じて、6.2.5 テナント構成情報のスナップショットを参照してください。

注: ID ストアを移行後、vRealize Code Stream のユーザーは手動で vRealize Code Stream ロールを再割り当てする必要があります。

手順

1 テナントのローカル ユーザー アカウントの作成

ローカル ユーザー アカウントを使用してテナントを設定し、そのローカル ユーザー アカウントにテナント管理者権限を割り当てる必要があります。

2 Active Directory リンクのユーザーとグループの同期

ディレクトリ管理機能を使用してユーザーとグループを vRealize Automation にインポートするには、Active Directory リンクに接続する必要があります。

3 ターゲット VMware Identity Manager へのカスタム グループの移行

VMware Identity Manager (vIDM) の移行先の展開環境には、移行元の環境からすべてのカスタム グループを移行する必要があります。

4 複数のテナントと IaaS 管理者の移行

テナント管理者または IaaS 管理者が指定されている各 vRealize Automation テナントに対し、各管理者を手動で削除して復旧する必要があります。

テナントのローカル ユーザー アカウントの作成

ローカル ユーザー アカウントを使用してテナントを設定し、そのローカル ユーザー アカウントにテナント管理者権限を割り当てる必要があります。

テナントごとに次の手順を繰り返します。

前提条件

新たに VMware Identity Manager のパスワードを設定したことを確認します。[「VMware Identity Manager 用の Single Sign-On パスワードの更新」](#)を参照してください。

手順

- 1 デフォルトのシステム管理者のユーザー名 **administrator** とパスワードを使用して vRealize Automation コンソールにログインします。
コンソールは **<https://<vra-appliance>/vcac/>** にあります。
- 2 テナントをクリックします。
たとえば、デフォルト テナントの場合は [vsphere.local] をクリックします。
- 3 [ローカル ユーザー] タブを選択します。
- 4 [新規] をクリックします。
- 5 ローカル ユーザー アカウントを作成します。
このユーザーにテナント管理者ロールを割り当てます。ローカル ユーザー名が vsphere.local Active Directory で一意であることを確認します。
- 6 [OK] をクリックします。
- 7 [管理者] をクリックします。
- 8 [テナント管理者] 検索ボックスにローカル ユーザー名を入力し、Enter を押します。
- 9 [完了] をクリックします。
- 10 コンソールからログアウトします。

次のステップ

[「Active Directory リンクのユーザーとグループの同期」](#)。

Active Directory リンクのユーザーとグループの同期

ディレクトリ管理機能を使用してユーザーとグループを vRealize Automation にインポートするには、Active Directory リンクに接続する必要があります。

各テナントで次の手順を実行します。

前提条件

Active Directory へのアクセス権限があることを確認します。

手順

- 1 vRealize Automation コンソール (**https://<vra-appliance>/vcac/org/<tenant_name>**) にログインします。
- 2 [管理] - [ディレクトリ管理] - [ディレクトリ] の順に選択します。
- 3 [ディレクトリを追加] をクリックし、[Active Directory over LDAP/IWA の追加] を選択します。

4 Active Directory のアカウント設定を入力します。

◆ ネイティブ以外の Active Directory

| オプション | 入力例 |
|---------------------------|---|
| ディレクトリ名 | 一意のディレクトリ名を入力します。 ネイティブ以外の Active Directory を使用する場合は、LDAP 経由の Active Directory を選択します。 |
| このディレクトリは DNS サービスをサポートする | このオプションは選択解除します。 |
| 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=rainpole,dc=local] と入力します。 |
| バインド DN | 共通名 (CN) など、ユーザーを検索する権限がある Active Directory ユーザー アカウントの完全識別名 (DN) を入力します。 たとえば、[cn=config_admin infra,cn=users,dc=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。 |

◆ ネイティブの Active Directory

| オプション | 入力例 |
|---------------|--|
| ディレクトリ名 | 一意のディレクトリ名を入力します。 ネイティブの Active Directory を使用する場合は、Active Directory (統合 Windows 認証) を選択します。 |
| ドメイン名 | 参加するドメインの名前を入力します。 |
| ドメイン管理者ユーザー名 | ドメイン管理者のユーザー名を入力します。 |
| ドメイン管理者パスワード | ドメイン管理者アカウントのパスワードを入力します。 |
| バインド ユーザー UPN | メール アドレス形式を使用して、ドメインを認証できるユーザーの名前を入力します。 |
| 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 バインド アカウント パスワードを入力します。 |

5 [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。

6 [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。

7 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。

8 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。

9 同期するグループおよびユーザーを選択します。

a [新規] 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、**dc=vcac,dc=local** と入力します。

c 同期するグループを選択するには、[選択] をクリックし、[次へ] をクリックします。

d [ユーザーの選択] ページで、同期するユーザーを選択し、[次へ] をクリックします。

- 10 ユーザーおよびグループがディレクトリと同期しているかを確認し、[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に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ます。
- 11 [管理] - [ディレクトリ管理] - [ID プロバイダ] の順に選択して、新しい ID プロバイダをクリックします。
たとえば、[WorkspaceIDP__1] をクリックします。
- 12 ページの一番下までスクロールして、[IdP ホスト名] プロパティの値を、vRealize Automation ロード バランサの FQDN を指すように更新します。
- 13 [保存] をクリックします。
- 14 各テナントと ID プロバイダについて、手順 11 ~ 13 を繰り返します。
- 15 すべての vRealize Automation ノードをアップグレードした後、各テナントにログインし、[管理] - [ディレクトリ管理] - [ID プロバイダ] の順に選択します。
各 ID プロバイダにすべての vRealize Automation コネクタが追加されます。
たとえば、環境に 2 台の vRealize Automation アプライアンスがある場合は、ID プロバイダに 2 つのコネクタが関連付けられます。

ターゲット VMware Identity Manager へのカスタム グループの移行

VMware Identity Manager (vIDM) の移行先の展開環境には、移行元的环境からすべてのカスタム グループを移行する必要があります。

この手順で、カスタム グループを移行します。

前提条件

- 「テナントのローカル ユーザー アカウントの作成」。
- vRealize Automation 仮想アプライアンスで horizon-workspace サービスが実行されていることを確認します。

手順

- 1 vRealize Automation 仮想アプライアンスで SSH セッションを開始します。
- 2 コマンド プロンプトで、vRealize Automation 仮想アプライアンスのインストール時に作成したパスワードを使用して **root** としてログインします。
- 3 次のコマンドを実行します。

```
vcac-config migrate-custom-groups
```

- 移行が完了すると、次のメッセージが表示されます：**カスタム グループの移行が正常に完了しました。**
- 移行元的环境にカスタム グループがない場合は、次のメッセージが表示されます：**vRA データベースにカスタム グループが見つかりませんでした。移行プロセスはスキップされます。**

注: カスタム グループの移行に失敗した場合は、`/var/log/vmware/vcac/vcac-config.log` にあるログ ファイルで詳細を確認できます。

複数のテナントと IaaS 管理者の移行

テナント管理者または IaaS 管理者が指定されている各 vRealize Automation テナントに対し、各管理者を手動で削除して復旧する必要があります。

vRealize Automation コンソールで、テナントごとに次の手順を実行します。

前提条件

アップグレードされた仮想アプライアンスで vRealize Automation コンソールにログインします。

- 1 完全修飾ドメイン名 (https://<va-hostname.domain_name>/vcac) を使用して、アップグレードされた仮想アプライアンスで vRealize Automation コンソールを開きます。

分散環境では、マスター仮想アプライアンスでコンソールを開きます。

- 2 [vsphere.local] ドメインを選択します。
- 3 ユーザー名 **administrator** と、仮想アプライアンスの展開時に入力したパスワードを使用してログインします。

手順

- 1 [管理] - [テナント] を選択します。
- 2 テナント名をクリックします。
- 3 [管理者] をクリックします。
- 4 各テナントと IaaS の管理者名とユーザー名のリストを作成します。
- 5 すべての管理者を削除するまで、各管理者をポイントして削除アイコン (✖) をクリックします。
- 6 [終了] をクリックします。
- 7 [テナント] ページで、テナント名をもう一度クリックします。
- 8 [管理者] をクリックします。
- 9 適切な検索ボックスに削除した各ユーザーの名前を入力し、Enter キーを押します。
- 10 検索結果から該当するユーザー名をクリックして、そのユーザーを管理者として追加して戻します。

完了すると、テナント管理者と IaaS 管理者のリストは、削除した管理者のリストと同じようになります。

- 11 [終了] をクリックします。

次のステップ

セカンダリ アプライアンスをアップグレードします。[\[追加の vRealize Automation アプライアンスでのアップデートのインストール\]](#) を参照してください。

追加の vRealize Automation アプライアンスでのアップデートのインストール

高可用性環境の場合、マスター仮想アプライアンスは、マスター モードで組み込み PostgreSQL データベースを実行するノードです。この環境内にある他のノードは、組み込み PostgreSQL データベースをレプリカ モードで実行します。アップグレード中、レプリカの仮想 6.2.5 アプライアンスでは、データベースを変更する必要はありません。

アップデートのインストール中は管理コンソールを閉じないでください。

前提条件

- 仮想アプライアンスのアップデートをダウンロードしたことを確認します。[\[vRealize Automation アプライアンスの更新のダウンロード\]](#) を参照してください。
 - jdbc:postgresql データベース接続が、マスター PostgreSQL ノードの外部 IP アドレスをポイントしていることを確認します。
 - a vRealize Automation アプライアンスで、新しいコマンド プロンプトを開きます。
 - b `/etc/vcac/server.xml` に移動して、`server.xml` ファイルをバックアップします。
 - c `server.xml` ファイルを開きます。
 - d 必要に応じて、使用する PostgreSQL データベースを示すように `server.xml` ファイルのエントリ `jdbc:postgresql` を編集します。
 - 外部の PostgreSQL データベースの場合、マスター PostgreSQL ノードの外部 IP アドレスを入力します。
 - 組み込みの PostgreSQL データベースの場合、マスター仮想アプライアンスの IP アドレスを入力します。
- 例: `jdbc:postgresql://198.15.100.60:5432/vcac`

手順

- 1 アップグレードのために vRealize Automation アプライアンス管理コンソールを開きます。
 - a 各セカンダリ vRealize Automation アプライアンスで、vRealize Automation アプライアンスを展開したときに入力したパスワードを使用して、**root** として vRealize Automation アプライアンス管理にログインします。
 - b ユーザー名 **root** と、アプライアンスの展開時に入力したパスワードを使用してログインします。
 - c [アップデート] をクリックします。
- 2 [設定] をクリックします。
- 3 [リポジトリをアップデート] セクションで、アップデートを VMware リポジトリからダウンロードするか CD-ROM から取得するかを選択します。
- 4 [ステータス] をクリックします。
- 5 [アップデートの確認] をクリックし、アップデートが利用可能かどうかを確認します。
- 6 [アップデートをインストール] をクリックします。
- 7 [OK] をクリックします。

アップデート処理が進行していることを示すメッセージが表示されます。

8 (オプション) ディスク 1 のサイズを 50 GB に手動で変更していない場合は、以下の手順を実行します。

- a 仮想アプライアンスの再起動を要求するシステム プロンプトが表示されたら、[システム] をクリックし、[再起動] をクリックします。

再起動中、アップデートに必要なディスク 1 の容量がシステムによって調整されます。

- b システムが再起動した後、ログアウトして、もう一度 vRealize Automation アプライアンス 管理コンソールにログインし、[更新] - [ステータス] の順に選択します。
- c [アップデートのチェック] および [アップデートのインストール] をクリックします。

9 アップグレードが正常に進行していることを確認するには、ログ ファイルを開きます。

- `/opt/vmware/var/log/vami/vami.log`
- `/opt/vmware/var/log/vami/updatecli.log`
- `/var/log/vmware/horizon/horizon.log`
- `/var/log/bootstrap/*.log`

アップグレード手順中にログアウトし、再度ログインした場合は、ログ ファイル (`/opt/vmware/var/log/vami/updatecli.log`) で更新の進行状況を継続して確認できます。

アップデート処理が終了するまでの所要時間は、環境によって異なります。

10 アップデートの完了後、vRealize Automation アプライアンス 管理コンソールをログアウトし、Web ブラウザのキャッシュをクリアして、vRealize Automation アプライアンス 管理コンソールにログインします。

11 仮想アプライアンスを再起動します。

- a [システム] をクリックします。
- b [再起動] をクリックし、選択を確認します。

12 仮想アプライアンスが再起動したら、レプリカの vRealize Automation アプライアンス 管理コンソールにログインします。

13 [vRA 設定] - [クラスタ] の順に選択します。

14 マスター vRealize Automation アプライアンスのユーザー名とパスワードを入力します。

15 [クラスタに参加] をクリックします。

16 [サービス] をクリックし、各サービス (iaas-service を除く) が登録済みとしてリストされていることを確認します。

次のステップ

[「vRealize Automation のアップグレード後の IaaS サーバ コンポーネントのアップグレード」](#)。

vRealize Automation のアップグレード後の IaaS サーバ コンポーネントのアップグレード

vRealize Automation の 6.2.5 から 7.4 へのアップグレード後、システム管理者は、Microsoft SQL Server データベースなどの IaaS サーバ コンポーネントをアップグレードします。

IaaS サーバ コンポーネントをアップグレードするには、2 つの方法があります。

- 自動化された IaaS アップグレード シェル スクリプトを使用する
- vRealize Automation 7.4 IaaS インストーラ実行可能ファイルを使用する。

共通のコンポーネント カatalogのコンポーネントがインストールされている場合は、アップグレード前にこのコンポーネントをアンインストールする必要があります。アップグレードが完了した後、該当するバージョンのコンポーネントを再インストールできます。詳細については、『共通のコンポーネント カatalogのインストール ガイド』を参照してください。このガイドが利用できない場合は、[「vRealize Automation のアップグレード チェックリスト」](#)の別の手順を参照してください。

アップグレード シェル スクリプトを使用した IaaS コンポーネントのアップグレード

各 vRealize Automation 6.2.5 アプライアンスをバージョン 7.4 にアップグレードした後に、アップグレード シェル スクリプトを使用して IaaS コンポーネントをアップグレードします。

アップデートしたプライマリまたはマスターの vRealize Automation アプライアンスには、各 IaaS ノードおよびコンポーネントのアップグレードに使用するシェル スクリプトが含まれています。

仮想マシンの vSphere コンソールまたは SSH コンソール セッションを使用すると、アップグレード スクリプトを実行できます。vSphere コンソールを使用する場合は、スクリプトの実行が中断する断続的なネットワーク接続の問題を回避します。

スクリプトによってコンポーネントがアップグレードされている間にスクリプトを停止した場合、コンポーネントのアップグレードが完了するまでスクリプトの実行が継続されます。ノード上にアップグレードされていないコンポーネントがある場合は、もう一度スクリプトを実行する必要があります。

アップグレードが完了すると、アップグレード ログ ファイル

(`/usr/lib/vcac/tools/upgrade/upgrade.log`)を開くことによってアップグレード結果を確認できます。

前提条件

- すべての vRealize Automation アプライアンスのアップデートが成功していることを確認します。
- すべての vRealize Automation アプライアンスの更新後に、IaaS サーバを再起動する場合は、Windows の IaaS サービスを停止する必要があります。IaaS コンポーネントをアップグレードする前に、サーバで、管理エージェント サービスを除く Windows のすべての IaaS サービスを停止します。
- マスターまたはプライマリ vRealize Automation アプライアンス ノードでアップグレード シェル スクリプトを実行する前に、各サービスが登録済みであることを確認します。
 - a 完全修飾ドメイン名 `https://<va-hostname.domain.name>:5480` を使用して仮想アプライアンスのアプライアンス管理コンソールに移動します。
 - b ユーザー名 **root** と、アプライアンスを展開したときに入力したパスワードを使用してログインします。
 - c [サービス] をクリックします。
 - d 各サービス (iaas-service を除く) が登録済みであることを確認します。
- 各 vRealize Automation IaaS 仮想マシン上で管理エージェントをアップグレードします。
 - a ブラウザを開き、完全修飾ドメイン名 (`https://<virtual_appliance_host>:5480/installer`) を使用して、vRealize Automation アプライアンス上の VMware vRealize Automation IaaS インストール ページに移動します。

- b [Management Agent Installer (管理エージェント インストーラ)] をクリックします。
デフォルトでは、インストーラは Downloads フォルダにダウンロードされます。
- c 各 vRealize Automation IaaS 仮想マシンにログインし、[管理エージェントのインストーラ ファイル] を使用して管理エージェントをアップグレードします。
- Model Manager Data がインストールされているプライマリ IaaS Web サイト ノードに JAVA SE Runtime Environment 8 Update 161 (64 ビット) 以降がインストールされていることを確認します。Java をインストールした後、環境変数 JAVA_HOME に新しいバージョンを設定する必要があります。
- 各 IaaS Web サイト ノードにログインして、作成日が **web.config** ファイルの変更日よりも前であることを確認します。**web.config** ファイルの作成日が変更日以降である場合は、[\[IaaS Web サイト コンポーネントのアップグレードに失敗する\]](#) の手順を実行します。
- 各 IaaS ノードにアップグレードされた IaaS 管理エージェントが存在することを確認するには、各 IaaS ノードで次の手順を実行します。
 - a vRealize Automation アプライアンス管理コンソールにログインします。
 - b [vRA 設定] - [クラスタ] の順に選択します。
 - c 各 IaaS ノードですべてのインストール済みコンポーネントのリストを展開して、IaaS 管理エージェントを見つけます。
 - d 管理エージェントのバージョンが最新であることを確認します。
- ロールバックする必要がある場合に備えて、IaaS Microsoft SQL Server データベースのバックアップにアクセスできることを確認します。
- すべての実体のない IaaS ノードを削除します。[\[vRealize Automation での実体のないノードの削除\]](#) を参照してください。
- 展開で IaaS サーバのスナップショットが利用できることを確認します。
アップグレードが失敗した場合、スナップショットとデータベース バックアップに戻り、別のアップグレードを試します。

手順

- 1 プライマリまたはマスター vRealize Automation アプライアンス ノード上で新しいコンソール セッションを開き、root アカウントでログインします。
SSH を使用してアップグレード スクリプトを実行する場合は、SSH コンソール セッションを開きます。
- 2 ディレクトリを **/usr/lib/vcac/tools/upgrade/** に変更します。
- 3 プロンプトで、次のコマンドを実行して **upgrade.properties** ファイルを作成します。
./generate_properties
- 4 **upgrade.properties** ファイルを開き、必須の値をすべて入力します。
次の表に必須の値を示します。必須の値は環境によって異なります。たとえば、DEM ワーカーまたは Orchestrator を含むノードでは DEM 認証情報が必須です。

| 必須の値 | 説明 | 認証情報形式 | 値の例 |
|---------------------|--|---------------|-----------------------|
| web_username | プライマリ Web ノード用のユーザー名。1 度のみ必要です。 | ドメイン\ユーザー | iaasDomain\webuser |
| web_password | プライマリ Web ノード用のパスワード。1 度のみ必要です。 | パスワード | pa\$\$w0rd! |
| dem_username | DEM ワーカーまたは DEM Orchestrator 用のユーザー名。DEM コンポーネントがインストールされている各ノードに必要です。 | ドメイン\ユーザー | iaasDomain\demuser |
| dem_password | DEM ワーカーまたは DEM Orchestrator 用のパスワード。DEM コンポーネントがインストールされている各ノードに必要です。 | パスワード | pa\$\$w0rd! |
| agent_username | vSphere エージェントなどのエージェント用のユーザー名。エージェント コンポーネントがインストールされている各ノードに必要です。 | ドメイン\ユーザー | iaasDomain\agent_user |
| agent_password | vSphere エージェントなどのエージェント用のパスワード。エージェント コンポーネントがインストールされている各ノードに必要です。 | パスワード | pa\$\$w0rd! |
| vidm_admin_password | VIDM 管理者パスワード。vRealize Automation 6.2.5 からアップグレードする場合のみ必要です。 | vidm_password | pa\$\$w0rd! |

セキュリティ上の理由から、アップグレードシェル スクリプトを実行すると、**upgrade.properties** ファイルは削除されます。ファイル内のプロパティは、IaaS 管理エージェントを通じて取得される各 IaaS コンポーネントの情報を使用して定義されます。**./generate_properities** または **./upgrade_from_62x** シェル スクリプトを実行する前に、すべての IaaS 管理エージェントがアップグレードされており、正常な状態であることが重要です。アップグレードシェル スクリプトを実行したときにいずれかの IaaS 管理エージェントに問題がある場合は、[「更新で管理エージェントのアップグレードに失敗する」](#)を参照してください。

upgrade.properties ファイルを作成するには、手順 2 および 3 を繰り返します。

5 アップグレード スクリプトを実行します。

- a コマンド プロンプトで **./upgrade_from_62x** と入力します。
- b Enter キーを押します。

各 IaaS ノードと、ノードにインストールされているすべてのコンポーネントが表示されます。スクリプトは、アップグレードをインストールする前に各コンポーネントを検証します。**upgrade.properties** ファイルに正しくない値があると、スクリプトは失敗します。

最初の IaaS サーバ コンポーネントは、完了まで 30 分以上かかります。アップグレード中に、「**Upgrading server components for node web1-vra.mycompany.com**」というようなメッセージが表示されます。

アップグレードシェル スクリプトが失敗した場合は、**upgrade.log** ファイルを確認します。

問題を修正した後、もう一度アップグレード スクリプトを実行できます。アップグレード スクリプトをもう一度実行する前に、**upgrade.properties** ファイルを再作成して開き、必須の値をすべて入力します。

- 6 (オプション) Manager Service の自動フェイルオーバーを有効にします。「[アップグレード後に Manager Service の自動フェイルオーバーを有効にする](#)」を参照してください。

次のステップ

「[組み込み vRealize Orchestrator コントロール センターへのアクセスのリストア](#)」。

laaS インストーラを使用した laaS コンポーネントのアップグレード

vRealize Automation 6.2.5 からバージョン 7.4 にアップグレードした後、この代替方法を使用して laaS コンポーネントをアップグレードすることができます。

laaS インストーラをダウンロードして laaS コンポーネントをアップグレードする

vRealize Automation 6.2.5 から 7.4 へアップグレードした後、アップグレードする laaS コンポーネントがインストールされている仮想マシンに laaS インストーラをダウンロードします。

この手順の間に証明書の警告が表示された場合は、無視して構いません。

注: アップグレード プロセスでは、Manager Service のパッシブ バックアップ インスタンスを除き、すべてのサービスの起動タイプを [自動] に設定する必要があります。サービスを [手動] に設定すると、アップグレード プロセスが失敗します。

前提条件

- laaS のインストール仮想マシンに、Microsoft .NET Framework 4.5.2 以降がインストールされていることを確認します。.NET インストーラは、VMware vRealize Automation laaS インストール ページからダウンロードできます。サービスをシャットダウンした後に .NET Framework を .NET Framework 4.5.2 にアップデートすると、インストール手順の一部として仮想マシンが再起動される場合があります。この場合、仮想マシン上の管理エージェント以外の laaS サービスをすべて手動で停止する必要があります。
- ダウンロードに Internet Explorer を使用する場合、厳密なセキュリティ設定が有効になっていないことを確認します。検索バーに **res://iesetup.dll/SoftAdmin.htm** と入力して、Enter キーを押します。
- アップグレードする laaS コンポーネントが 1 つ以上インストールされている Windows サーバにローカル管理者としてログインします。

手順

- 1 Web ブラウザを開きます。
- 2 VMware vRealize Automation laaS インストール ページの URL を入力します。
たとえば、**https://<vcac-va-hostname.domain.name>:5480/installer** と入力します。ここで、<vcac-va-hostname.domain.name> は、プライマリまたはマスター vRealize Automation アプライアンス ノードの名前です。
- 3 [laaS インストーラ] をクリックします。

- 4 `setup__<vcac-va-hostname.domain.name>@5480.exe` インストーラ ファイルが、デフォルトでダウンロード フォルダに送信されます。

ファイル名は変更しないでください。インストールの vRealize Automation アプライアンスへの接続に使用されます。

次のステップ

- スタンドアロン vRealize Orchestrator がある場合は、[「vRealize Automation で使用するスタンドアロン vRealize Orchestrator アプライアンスのアップグレード」](#)を参照してください。
- 外部 vRealize Orchestrator アプライアンス クラスタがある場合は、[「vRealize Automation で使用するための 外部 vRealize Orchestrator Appliance クラスタのアップグレード」](#)を参照してください。
- [「vRealize Automation のアップグレード後の IaaS コンポーネントのアップグレード」](#)を参照してください。

vRealize Automation のアップグレード後の IaaS コンポーネントのアップグレード

vRealize Automation 6.2.5 からバージョン 7.4 へのアップグレード後、SQL データベースをアップグレードし、IaaS コンポーネントがインストールされたすべてのシステムを構成する必要があります。これらの手順は、最小および分散インストールに対して使用できます。

注: IaaS インストーラは、アップグレードする IaaS コンポーネントが含まれている仮想マシンに存在する必要があります。外部の場所からインストーラを実行することはできません。ただし、Microsoft SQL データベースは Web ノードからリモートでアップグレードすることもできます。

展開で IaaS サーバのスナップショットが利用できることを確認します。アップグレードが失敗した場合は、スナップショットに戻り、別のアップグレードを試すことができます。

サービスが次の順序でアップグレードされるようにアップグレードを実行します。

1 IaaS Web サイト

ロード バランサを使用している場合は、プライマリ以外のすべてのノードのトラフィックを無効にします。

1 つのサーバのアップグレードを完了してから、Web サイト サービスを実行している次のサーバをアップグレードします。Model Manager Data コンポーネントがインストールされているサーバからアップグレードします。

外部 Microsoft SQL データベースの手動アップグレードを実行している場合は、外部 SQL をアップグレードしてから、Web ノードをアップグレードする必要があります。外部 SQL は Web ノードからリモートでアップグレードできます。

2 Manager Service

パッシブ Manager Service をアップグレードする前に、アクティブな Manager Service をアップグレードします。

SQL インスタンスで SSL 暗号化が有効になっていない場合は、[IaaS アップグレード構成] ダイアログ ボックスで [SSL 暗号化] を選択解除します。

3 DEM orchestrator とワーカー

すべての DEM orchestrator とワーカーをアップグレードします。1 台のサーバのアップグレードを完了してから、次のサーバをアップグレードします。

4 エージェント

1 台のサーバのアップグレードを完了してから、エージェントを実行している次のサーバをアップグレードします。

5 管理エージェント

アップグレード手順の一部としてアップデートされます。

あるサーバで異なるサービスを使用している場合は、アップグレードにより、サービスが正しい順序でアップデートされます。たとえば、サイト内に同一サーバ上の Web サイトと Manager Service がある場合、両方をアップデート対象として選択します。アップグレード インストーラがアップデートを正しい順序で適用します。1 台のサーバのアップグレードを完了してから、別のサーバのアップグレードを開始する必要があります。

注: 環境でロード バランサを使用する場合は、アップグレードの対象となる 1 台目のアプライアンスがロード バランサに接続されている必要があります。vRealize Automation アプライアンス の他のすべてのインスタンスは、キャッシュ エラーを回避するために、アップグレードを適用する前にロード バランサのトラフィックに対して無効にする必要があります。

前提条件

- 既存の vRealize Automation 6.2.5 環境をバックアップします。
- すべての vRealize Automation アプライアンスの更新後に、IaaS サーバを再起動する場合は、Windows の IaaS サービスを停止する必要があります。IaaS コンポーネントをアップグレードする前に、サーバで、管理エージェント サービスを除く Windows のすべての IaaS サービスを停止します。
- [「IaaS インストーラをダウンロードして IaaS コンポーネントをアップグレードする」](#)。
- Model Manager Data がインストールされているプライマリ IaaS Web サイト ノードに適切なバージョンの Java がインストールされていることを確認します。JAVA SE Runtime Environment 8 Update 161 (64 ビット) 以降がインストールされている必要があります。Java をインストールした後、環境変数 JAVA_HOME に新しいバージョンを設定します。
- 作成日が **web.config** ファイルの変更日よりも前であることを確認します。**web.config** ファイルの作成日が変更日以降である場合は、[「IaaS Web サイト コンポーネントのアップグレードに失敗する」](#)の手順を実行します。
- 外部 Microsoft SQL データベースがある場合に vRealize Automation 6.2.5 からアップグレードするには、適切なバージョンの管理エージェントが必要です。IaaS web サイトのアップグレードを実行するには、外部データベースの管理エージェントがバージョン 7.0 以降である必要があります。外部の SQL 仮想マシンのコントロール パネルで管理エージェントのバージョンを確認します。管理エージェントがバージョン 7.0 以降でない場合は、次の手順を実行して、管理エージェントをアップグレードします。
 - a ブラウザを開き、完全修飾ドメイン名 (https://<virtual_appliance_host>:5480/installer) を使用して、vRealize Automation アプライアンス 上の VMware vRealize Automation IaaS インストール ページに移動します。
 - b [Management Agent Installer (管理エージェント インストーラ)] をクリックします。

デフォルトでは、インストーラは Downloads フォルダにダウンロードされます。

- c 外部データベースにログインし、[Management Agent Installer (管理エージェント インストーラ)] ファイルを使用して管理エージェントをアップグレードし、Windows 管理エージェント サービスを再起動します。
- 共通のコンポーネント カタログのコンポーネントがインストールされている場合は、アップグレード前にこのコンポーネントをアンインストールする必要があります。詳細については、『共通のコンポーネント カタログのインストール ガイド』を参照するか、[\[vRealize Automation のアップグレード チェックリスト\]](#)に記載された手順を実行します。

手順

- 1 ロード バランサを使用している場合は、使用環境で次の準備を行います。
 - a Model Manager Data が含まれている IaaS Web サイト ノードが、ロード バランサのトラフィックに対して有効になっていることを確認します。

`<vCAC Folder>\Server\ConfigTool` フォルダがあれば、このノードを特定できます。
 - b ロード バランサのトラフィックに対し、その他すべての IaaS Web サイトと、プライマリ以外の Manager Service を無効にします。
- 2 セットアップ ファイル `setup__<vrealize-automation-appliance-FQDN>@5480.exe` を右クリックして、[管理者として実行] を選択します。
- 3 [次へ] をクリックします。
- 4 使用許諾契約に同意し、[次へ] をクリックします。
- 5 [ログイン] ページで現在の導入環境の管理者認証情報を入力します。
 ユーザー名は **root** で、パスワードはアプライアンスを展開したときに入力したパスワードです。
- 6 [証明書の受け入れ] を選択します。
- 7 [インストール タイプ] ページで、[アップグレード] が選択されていることを確認します。
 [アップグレード] が選択されていない場合は、このシステム上のコンポーネントがすでにこのバージョンにアップグレードされています。
- 8 [次へ] をクリックします。
- 9 アップグレード設定を構成します。

| オプション | アクション |
|----------------------------------|---|
| Model Manager Data をアップグレードする場合 | vCAC Server セクションで [Model Manager Data] チェック ボックスを選択します。 デフォルトではこのチェック ボックスは選択されています。Model Manager Data のアップグレードは 1 度のみです。分散インストールをアップグレードすると、Web サーバと Model Manager Data のバージョンが一致しない間、Web サーバは機能を停止します。Model Manager Data のアップグレードが完了すると、Web サーバは通常どおり機能します。 |
| Model Manager Data をアップグレードしない場合 | vCAC Server セクションで [Model Manager Data] を選択解除します。 |

| オプション | アクション |
|--|---|
| Model Manager Data でカスタマイズされたワークフローを最新バージョンで保存するには | <p>Model Manager Data をアップグレードする場合は、拡張性ワークフロー セクションで [ワークフローを最新バージョンに維持する] チェック ボックスを選択します。</p> <p>デフォルトではこのチェック ボックスは選択されています。カスタマイズされたワークフローが常に維持されます。チェック ボックスを選択すると、バージョン順のみが決定されます。Model Manager でワークフローをカスタマイズした場合は、このオプションを選択して、アップグレード後にも最新のワークフローが最新バージョンとして維持されるようにします。</p> <p>このオプションを選択しない場合、vRealize Automation Designer で提供される各ワークフローはアップグレード後に最新バージョンとなり、アップグレード前の最新バージョンは 2 番目に新しいバージョンとなります。</p> <p>vRealize Automation Designer 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。</p> |
| Distributed Execution Manager または プロキシ エージェント をアップグレードする場合 | <p>サービス アカウント セクションで管理者アカウントの認証情報を入力します。</p> <p>アップグレードするすべてのサービスがこのアカウントで実行されます。</p> |
| Microsoft SQL Server データベースを指定するには | <p>Model Manager Data をアップグレードする場合は、[サーバ] テキスト ボックスにデータベース サーバとデータベース インスタンスの名前を入力します。[データベース名] にデータベース サーバ名の完全修飾ドメイン名 (FQDN) を入力します。</p> <p>データベース インスタンスがデフォルト以外の SQL ポートにある場合、サーバ インスタンス仕様にポート番号を含めます。Microsoft SQL のデフォルト ポート番号は 1433 です。</p> <p>マネージャ ノードをアップグレードする場合、MSSQL SSL オプションはデフォルトで選択されています。データベースで SSL を使用しない場合には、[データベース接続に SSL を使用] を選択解除します。</p> |

10 [次へ] をクリックします。

11 アップグレードするすべてのサービスが [アップグレードの準備完了] ページに表示されていることを確認し、[アップグレード] をクリックします。

[アップグレード] ページおよび進行状況インジケータが表示されます。アップグレード手順を完了すると、[次へ] ボタンが有効になります。

12 [次へ] をクリックします。

13 [完了] をクリックします。

14 すべてのサービスが再起動されたことを確認します。

15 導入環境内の各 IaaS サーバに対し、記載されている順序でこの手順を繰り返します。

16 すべてのコンポーネントをアップグレードしたら、アプライアンスの管理コンソールにログインし、IaaS を含むすべてのサービスが登録されていることを確認します。

選択したすべてのコンポーネントが新しいリリースにアップグレードされました。

次のステップ

- [「組み込み vRealize Orchestrator コントロール センターへのアクセスのリストア」](#)。

- 導入環境でロード バランサを使用する場合、vRealize Automation 健全性チェックを使用するために各ロード バランサ ノードをアップグレードし、接続されていないノードのロード バランサのトラフィックを再度有効にします。以前の導入環境で PostgreSQL データベースに組み込まれたロード バランサを使用していた場合、PostgreSQL プール内のすべてのノードは必要ないため無効にします。プールはいつでも削除できます。

詳細については、[vRealize Automation のロード バランシング](#)を参照してください。

- (オプション) Manager Service の自動フェイルオーバーを有効にします。[「アップグレード後に Manager Service の自動フェイルオーバーを有効にする」](#)を参照してください。

組み込み vRealize Orchestrator コントロール センターへのアクセスのリストア

IaaS サーバ コンポーネントをアップグレードした後、vRealize Orchestrator へのアクセスをリストアする必要があります。

vRealize Automation 6.2.5 を 7.4 にアップグレードする場合、新しいロール ベースのアクセス コントロール機能に対応するには、この手順を実行する必要があります。ここには、高可用性環境での手順を記載しています。

前提条件

vRealize Automation 環境のスナップショットを作成します。

手順

- 1 アプライアンス ホストの完全修飾ドメイン名を使用して (<https://<va-hostname.domain.name>:5480>)、vRealize Automation アプライアンス 管理コンソールに root としてログインします。
- 2 [vRA 設定] - [データベース] の順に選択します。
- 3 マスター ノードとレプリカ ノードを特定します。
- 4 各レプリカ ノードで SSH セッションを開き、管理者としてログインして、次のコマンドを実行します。
service vco-server stop && service vco-configurator stop
- 5 マスター ノードで SSH セッションを開き、管理者としてログインして、次のコマンドを実行します。
rm /etc/vco/app-server/vco-registration-id
- 6 マスター ノードで、**/etc/vco/app-server/** ディレクトリに移動します。
- 7 **sso.properties** ファイルを開きます。
- 8 プロパティ名 **com.vmware.o11n.sso.admin.group.name** にスペースや、Bash コマンドで特殊文字として使用できる他の Bash 関連文字 (ハイフン (-) やドル記号 (\$)) など) が含まれる場合は、次の手順を実行します。
 - a **com.vmware.o11n.sso.admin.group.name** プロパティが含まれる行をコピーし、値に **AdminGroup** を入力します。
 - b **com.vmware.o11n.sso.admin.group.name** プロパティが含まれる元の行の先頭に # を追加して、この行をコメントアウトします。
 - c **sso.properties** ファイルを保存して閉じます。

9 次のコマンドを実行します。

```
vcac-vami vco-service-reconfigure
```

10 手順 8 が完了している場合は、**sso.properties** ファイルを開き、次の手順を実行します。

- a **com.vmware.o11n.sso.admin.group.name** プロパティが含まれる元の行の先頭にある # を削除して、この行をコメント解除します。
- b **com.vmware.o11n.sso.admin.group.name** プロパティが表示されている行のコピーを削除します。
- c **sso.properties** ファイルを保存して閉じます。

11 次のコマンドを実行して、vco-server サービスを再起動します。

```
service vco-server restart
```

12 次のコマンドを実行して、vco-configurator サービスを再起動します。

```
service vco-configurator restart
```

13 vRealize Automation アプライアンス 管理コンソールで、[サービス] をクリックし、マスター ノードのすべてのサービスが [登録済み] になるまで待機します。

14 すべてのサービスが [登録済み] になったら、vRealize Automation レプリカ ノードを vRealize Automation クラスタに参加させ、vRealize Orchestrator 構成を同期します。詳細については、[「組み込みの vRealize Orchestrator で高可用性をサポートするための再構成」](#)を参照してください。

次のステップ

[「vRealize Automation をアップグレードした後の vRealize Orchestrator のアップグレード」](#)。

vRealize Automation をアップグレードした後の vRealize Orchestrator のアップグレード

vRealize Automation 6.2.5 から 7.4 にアップグレードした後、vRealize Orchestrator インスタンスをアップグレードする必要があります。

vRealize Orchestrator 7.4 リリースでは、vRealize Automation 7.4 に正常にアップグレードした後に vRealize Orchestrator をアップグレードする方法が 2 つあります。

- 既存の外部 vRealize Orchestrator サーバを vRealize Automation 7.4 に組み込まれた vRealize Orchestrator に移行できます。
- 既存のスタンドアロンまたはクラスタ化された vRealize Orchestrator サーバをアップグレードして、vRealize Automation 7.4 と連携することができます。

外部 vRealize Orchestrator サーバから vRealize Automation への移行

既存の外部 vRealize Orchestrator サーバは、vRealize Automation 7.4 に組み込まれている vRealize Orchestrator インスタンスに移行することができます。

vRealize Orchestrator を外部サーバ インスタンスとして導入し、その外部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。または、vRealize Automation アプライアンスに含まれている vRealize Orchestrator サーバを構成して使用することもできます。

VMware では、外部 vRealize Orchestrator を、vRealize Automation に組み込まれた Orchestrator サーバに移行することをお勧めします。外部 Orchestrator から組み込み Orchestrator への移行には、次の利点があります。

- 総所有コストが削減されます。
- デプロイ モデルが簡素化されます。
- 運用効率が向上します。

注: 外部 vRealize Orchestrator の使用は、次の場合に考慮します。

- vRealize Automation 環境内の複数のテナント
- 物理的に分散した環境
- ワークロードの処理
- 特定のプラグイン（古いバージョンの Site Recovery Manager プラグインなど）の使用

外部 Orchestrator および組み込み Orchestrator のコントロール センターの違い

外部 vRealize Orchestrator のコントロール センターで使用可能な一部のメニュー項目は、組み込み Orchestrator インスタンスのデフォルトのコントロール センター ビューに含まれていません。

組み込み Orchestrator サーバのコントロール センターでは、いくつかのオプションがデフォルトで非表示になっています。

| メニュー項目 | 詳細 |
|------------------------|---|
| [ライセンス] | 組み込み Orchestrator では vRealize Automation をライセンス プロバイダとして使用するよう事前構成されています。 |
| [設定をエクスポート/インポート] | エクスポートされた vRealize Automation コンポーネントに、組み込み Orchestrator の構成が含まれています。 |
| [データベースを構成] | 組み込み Orchestrator では、vRealize Automation で使用されているデータベースを使用します。 |
| [カスタム エクスペリエンス改善プログラム] | カスタム エクスペリエンス改善プログラム (CEIP) には vRealize Automation アプライアンス管理インターフェイスから参加できます。 【vRealize Automation の管理】の「カスタム エクスペリエンス改善プログラム」を参照してください。 |

デフォルトのコントロール センター ビューでは非表示になっている別のオプションには、[認証プロバイダを設定] ページの [ホスト アドレス] テキスト ボックスや [登録解除] ボタンがあります。

注: vRealize Automation に組み込まれている vRealize Orchestrator でコントロール センターのオプションをすべて表示するには、Orchestrator 管理の詳細ページ (https://<vra-vd-hostname.domain.name_or_load_balancer_address>:8283/vco-controlcenter/#/?advanced) にアクセスし、キーボードの [F5] ボタンを押してページを更新する必要があります。

Windows 上の外部 vRealize Orchestrator から vRealize Automation への移行

vRealize Automation をバージョン 6.x からバージョン 7.4 にアップグレードしたら、Windows 上にインストールされている既存の外部 Orchestrator 6.x を、vRealize Automation 7.4 に組み込まれている Orchestrator サーバに移行できます。

注: 複数の vRealize Automation ノードがある分散 vRealize Automation 環境では、プライマリの vRealize Automation ノードに対してのみ移行手順を実行します。

前提条件

- vRealize Automation 7.4 への正常な移行。
- 外部 Orchestrator の Orchestrator サーバ サービスを停止します。
- 外部 Orchestrator サーバのデータベースを、データベース スキーマを含めバックアップします。

手順

- 1 移行先の Orchestrator サーバから移行ツールをダウンロードします。
 - a 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。
 - b `/var/lib/vco/downloads` ディレクトリにある **migration-tool.zip** アーカイブをダウンロードします。
- 2 移行元 Orchestrator サーバから Orchestrator 構成をエクスポートします。
 - a **PATH** 環境変数は、Orchestrator とともにインストールされる Java JRE の **bin** フォルダをポイントするように設定します。
 - b 移行ツールを、外部 Orchestrator がインストールされている Windows サーバにアップロードします。
 - c Orchestrator のインストール フォルダにダウンロードされたアーカイブを抽出します。
Windows ベースのインストールの場合、Orchestrator インストール フォルダのデフォルトのパスは **C:\Program Files\VMware\Orchestrator** です。
 - d 管理者として Windows コマンド プロンプトを実行して、Orchestrator インストール フォルダ内の **bin** フォルダに移動します。
デフォルトでは、**bin** フォルダのパスは **C:\Program Files\VMware\Orchestrator\migration-cli\bin** です。
 - e コマンド ラインから **export** コマンドを実行します。

```
C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
```

このコマンドは vRealize Orchestrator 構成ファイルとプラグインを 1 つのエクスポート アーカイブに結合します。

アーカイブは **migration-cli** フォルダと同じフォルダ内に作成されます。

3 エクスポートした構成を、vRealize Automation 7.4 に組み込まれた Orchestrator サーバに移行します。

- a エクスポートした構成ファイルを vRealize Automation アプライアンスの `/usr/lib/vco/tools/configuration-cli/bin` ディレクトリにアップロードします。
- b `/usr/lib/vco/tools/configuration-cli/bin` ディレクトリの下で、エクスポートした Orchestrator 構成ファイルの所有権を変更します。

```
chown vco:vco orchestrator-config-export-<orchestrator_ip_address>-<date>_<hour>.zip
```

- c `import` コマンドを使用して `vro-configure` スクリプトを実行し、Orchestrator 構成ファイルを組み込み vRealize Orchestrator サーバにインポートします。

```
./vro-configure.sh import --skipDatabaseSettings --skipLicense --skipSettings --skipSslCertificate --notForceImportPlugins --notRemoveMissingPlugins --skipTrustStore --path orchestrator-config-export-<orchestrator_appliance_ip>-<date>_<hour>.zip
```

4 `db-migrate` コマンドを使用して `vro-configure` スクリプトを実行し、データベースを内部 PostgreSQL データベースに移行します。

```
./vro-configure.sh db-migrate --sourceJdbcUrl <JDBC_connection_URL> --sourceDbUsername <database_user> --sourceDbPassword <database_user_password>
```

注: 特殊文字を含むパスワードは一重引用符で囲んでください。

<JDBC_connection_URL> は、使用するデータベースのタイプによって異なります。

PostgreSQL: `jdbc:postgresql://<host>:<port>/<database_name>`

MSSQL: `jdbc:jtds:sqlserver://<host>:<port>/<database_name>\;` if using SQL authentication and MSSQL:
`jdbc:jtds:sqlserver://<host>:<port>/<database_name>\;domain=<domain>\;useNTLMv2=TRUE` if using Windows authentication.

Oracle: `jdbc:oracle:thin:@<host>:<port>:<database_name>`

デフォルトのデータベースのログイン情報は以下のとおりです。

| | |
|--------------------------|--------|
| <database_name> | vmware |
| <database_user> | vmware |
| <database_user_password> | vmware |

- 5 vRealize Automation をアップグレードではなく移行した場合は、信頼されている Single Sign-On の証明書を組み込み Orchestrator インスタンスのデータベースから削除します。

```
sudo -u postgres -i -- /opt/vmware/vpostgres/current/bin/psql vcac -c "DELETE FROM vmo_keystore WHERE id='cakestore-id';"
```

これで、Windows にインストールされている外部 vRealize Orchestrator 6.x が vRealize Automation 7.4 に組み込まれた vRealize Orchestrator インスタンスに正常に移行されました。

次のステップ

組み込み vRealize Orchestrator サーバを設定します。[「組み込み vRealize Orchestrator サーバの構成」](#)を参照してください。

外部 vRealize Orchestrator 6.x 仮想アプライアンスから vRealize Automation 7.4 への移行

vRealize Automation をバージョン 6.x からバージョン 7.4 にアップグレードしたら、既存の外部 Orchestrator 6.x 仮想アプライアンスを vRealize Automation 7.4 に組み込まれている Orchestrator サーバに移行できます。

注: 複数の vRealize Automation アプライアンス ノードがある分散 vRealize Automation 環境では、プライマリの vRealize Automation ノードに対してのみ移行手順を実行します。

前提条件

- vRealize Automation 7.4 への正常な移行。
- 外部 Orchestrator の Orchestrator サーバサービスを停止します。
- 外部 Orchestrator サーバのデータベースを、データベース スキーマを含めバックアップします。

手順

- 1 移行先の Orchestrator サーバから移行元 Orchestrator に移行ツールをダウンロードします。
 - a SSH を使用して vRealize Orchestrator 6.x 仮想アプライアンスに **root** としてログインします。
 - b `/var/lib/vco` ディレクトリの下で、**scp** コマンドを実行して **migration-tool.zip** アーカイブをダウンロードします。

```
scp root@<vra-va-hostname.domain.name>:/var/lib/vco/downloads/migration-tool.zip ./
```

- c **unzip** コマンドを実行して、移行ツールのアーカイブを抽出します。

```
unzip migration-tool.zip
```

2 移行元 Orchestrator サーバから Orchestrator 構成をエクスポートします。

- a `/var/lib/vco/migration-cli/bin` ディレクトリで、**export** コマンドを実行します。

```
./vro-migrate.sh export
```

このコマンドは VMware vRealize Orchestrator 構成ファイルとプラグインを 1 つのエクスポート アーカイブに結合します。

ファイル名 `orchestrator-config-export-<orchestrator_ip_address>-<date>_<hour>.zip` を使用したアーカイブが `/var/lib/vco` フォルダに作成されます。

3 エクスポートした構成を、vRealize Automation 7.4 に組み込まれた Orchestrator サーバに移行します。

- a 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。
- b `/usr/lib/vco/tools/configuration-cli/bin` ディレクトリの下で、**scp** コマンドを実行して、エクスポートした構成アーカイブをダウンロードします。

```
scp root@<orchestrator_ip_or_DNS_name>:/var/lib/vco/orchestrator-config-export-<orchestrator_ip_address>-<date>_<hour>.zip ./
```

- c エクスポートした Orchestrator 構成ファイルの所有権を変更します。

```
chown vco:vco orchestrator-config-export-<orchestrator_ip_address>-<date>_<hour>.zip
```

- d 組み込み vRealize Orchestrator サーバの Orchestrator サーバサービスとコントロール センター サービスを停止します。

```
service vco-server stop && service vco-configurator stop
```

- e **import** コマンドを使用して `vro-configure` スクリプトを実行し、Orchestrator 構成ファイルを組み込み vRealize Orchestrator サーバにインポートします。

```
./vro-configure.sh import --skipDatabaseSettings --skipLicense --skipSettings --skipSslCertificate --notForceImportPlugins --notRemoveMissingPlugins --skipTrustStore --path orchestrator-config-export-<orchestrator_appliance_ip>-<date>_<hour>.zip
```

4 移行元とする外部 Orchestrator サーバが組み込み PostgreSQL データベースを使用している場合は、データベース構成ファイルを編集します。

- a `/var/vmware/vpostgres/current/pgdata/postgresql.conf` ファイルで、`listen_addresses` 行をコメント解除します。
- b `listen_addresses` の値をワイルドカード (*) に設定します。

```
listen_addresses = '*'
```

- c `/var/vmware/vpostgres/current/pgdata/pg_hba.conf` ファイルに行を追加します。

```
host all all <vra-va-ip-address>/32 md5
```

注: `pg_hba.conf` ファイルでは、IP アドレスとサブネット マスクの代わりに CIDR プリフィックス形式を使用する必要があります。

- d PostgreSQL サーバ サービスを再起動します。

```
service vpostgres restart
```

- 5 `db-migrate` コマンドを使用して `vro-configure` スクリプトを実行し、データベースを内部 PostgreSQL データベースに移行します。

```
./vro-configure.sh db-migrate --sourceJdbcUrl <JDBC_connection_URL> --sourceDbUsername <database_user> --sourceDbPassword <database_user_password>
```

注: 特殊文字を含むパスワードは一重引用符で囲んでください。

<JDBC_connection_URL> は、使用するデータベースのタイプによって異なります。

PostgreSQL: `jdbc:postgresql://<host>:<port>/<database_name>`

MSSQL: `jdbc:jtds:sqlserver://<host>:<port>/<database_name>\;` if using SQL authentication and MSSQL:
`jdbc:jtds:sqlserver://<host>:<port>/<database_name>\;domain=<domain>\;useNTLMv2=TRUE` if using Windows authentication.

Oracle: `jdbc:oracle:thin:@<host>:<port>:<database_name>`

デフォルトのデータベースのログイン情報は以下のとおりです。

| | |
|--------------------------|--------|
| <database_name> | vmware |
| <database_user> | vmware |
| <database_user_password> | vmware |

- 6 vRealize Automation をアップグレードではなく移行した場合は、信頼されている Single Sign-On の証明書を組み込み Orchestrator インスタンスのデータベースから削除します。

```
sudo -u postgres -i -- /opt/vmware/vpostgres/current/bin/psql vcac -c "DELETE FROM vmo_keystore WHERE id='cakeystore-id';"
```

- 7 `postgresql.conf` および `pg_hba.conf` ファイルをデフォルトの構成に戻します。

- a PostgreSQL サーバ サービスを再起動します。

これで、外部 vRealize Orchestrator 6.x 仮想アプライアンスが vRealize Automation 7.4 に組み込まれた vRealize Orchestrator インスタンスに正常に移行されました。

次のステップ

組み込み vRealize Orchestrator サーバを設定します。「[組み込み vRealize Orchestrator サーバの構成](#)」を参照してください。

組み込み vRealize Orchestrator サーバの構成

外部 Orchestrator サーバの構成をエクスポートして vRealize Automation 7.4 にインポートしたら、vRealize Automation に組み込まれた Orchestrator サーバを構成する必要があります。

前提条件

設定を外部から内部 vRealize Orchestrator に移行します。

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 コントロール センター サービスと、組み込み vRealize Orchestrator サーバの Orchestrator サーバ サービスを開始します。

```
service vco-configurator start && service vco-server start
```

- 3 組み込み Orchestrator サーバのコントロール センターに**管理者**としてログインします。

注: 外部 vRealize Orchestrator 7.4 インスタンスから移行する場合は、手順 5 に進んでください。

- 4 コントロール センターの [設定を検証] ページで、Orchestrator が正しく設定されていることを確認します。
- 5 外部 Orchestrator がクラスタ モードで動作するように構成されている場合は、vRealize Automation で Orchestrator クラスタを再構成します。

- a 詳細な [Orchestrator クラスタ管理] ページ (https://<vra-vahostname.domain.name_or_load_balancer_address>:8283/vco-controlcenter/#/control-app/ha?remove-nodes) に移動します。

注: クラスタの既存のノードの横に [削除] チェック ボックスが表示されない場合は、キーボードの [F5] ボタンをクリックして、ブラウザ ページを更新する必要があります。

- b 外部 Orchestrator ノードの横にあるチェック ボックスをオンにし、[削除] をクリックしてクラスタから削除します。
 - c 詳細なクラスタ管理ページを終了するには、URL から **remove-nodes** 文字列を削除し、キーボードの [F5] ボタンをクリックしてブラウザ ページを更新します。
 - d コントロール センターの [設定を検証] ページで、Orchestrator が適切に設定されていることを確認します。
- 6 (オプション) [証明書] ページの [パッケージ署名証明書] タブの下で、新しいパッケージ署名証明書を生成します。
 - 7 (オプション) [認証プロバイダを設定] ページの [デフォルト テナント] と [管理グループ] の値を変更します。

- 8 vRealize Automation アプライアンス 管理コンソールの [サービス] タブの下で **vco-server** サービスが REGISTERED と表示されていることを確認します。
- 9 外部 Orchestrator サーバの **vco** サービスを選択し、[登録解除] をクリックします。

次のステップ

- 外部 Orchestrator サーバにある信頼された証明書を、組み込み Orchestrator のトラスト ストアにインポートします。
- vRealize Automation レプリカ ノードを vRealize Automation クラスタに参加させて、Orchestrator 構成を同期します。

詳細については、『vRealize Automation のインストールまたはアップグレード』の「Reconfigure the Target Embedded vRealize Orchestrator to Support High Availability」を参照してください。

注: vRealize Orchestrator のインスタンスは自動的にクラスタ化されており、使用可能です。

- クラスタ内のすべてのノードで **vco-configurator** サービスを再起動します。
- 移行した組み込み Orchestrator サーバをポイントするように、vRealize Orchestrator エンドポイントを更新します。
- vRealize Automation ホストと IaaS ホストを vRealize Automation プラグインのインベントリに追加します。これは vRA ホスト ワークフローの vRA ホストの追加と IaaS ホストの追加を実行して行います。

vRealize Automation で使用するスタンドアロン vRealize Orchestrator アプライアンスのアップグレード

vRealize Automation で使用するスタンドアロン vRealize Orchestrator アプライアンスを維持している場合は、vRealize Automation を 6.2.5 から 7.4 にアップグレードするときにスタンドアロン アプライアンスをアップグレードする必要があります。

vRealize Orchestrator の組み込みインスタンスは、vRealize Automation アプライアンスのアップグレードの一部としてアップグレードされます。組み込みインスタンスの場合、追加のアクションは必要ありません。

vRealize Orchestrator アプライアンス クラスタをアップグレードする場合は、[「vRealize Automation で使用するための外部 vRealize Orchestrator Appliance クラスタのアップグレード」](#)を参照してください。

前提条件

- [「vRealize Automation アプライアンスでのアップデートのインストール」](#)。
- [「vRealize Automation のアップグレード後の IaaS サーバ コンポーネントのアップグレード」](#) の説明に従って IaaS コンポーネントをアップグレードします。
- すべてのネットワーク ファイル システムをマウント解除します。vSphere のドキュメントの『vSphere 仮想マシン管理』を参照してください。
- vSphere Orchestrator Appliance のメモリを 6 GB 以上に増やします。vSphere のドキュメントの『vSphere 仮想マシン管理』を参照してください。
- vSphere Orchestrator 仮想マシンのスナップショットを作成します。vSphere のドキュメントの『vSphere 仮想マシン管理』を参照してください。

- 外部データベースを使用する場合は、データベースをバックアップします。
- vSphere Orchestrator の事前構成された PostgreSQL データベースを使用する場合は、vSphere コントロールセンターの [データベースをエクスポート] メニューを使用して、データベースをバックアップします。

手順

- 1 次のいずれかの方法を使用してスタンドアロン vRealize Orchestrator をアップグレードします。
 - 「デフォルトの VMware リポジトリを使用した Orchestrator Appliance のアップグレード」。
 - 「ISO イメージを使用した Orchestrator Appliance のアップグレード」。
 - 「指定したリポジトリを使用した Orchestrator Appliance のアップグレード」。
- 2 コントロール センターから vRealize Automation NSX プラグインをアップグレードします。

デフォルトの VMware リポジトリを使用した Orchestrator Appliance のアップグレード

Orchestrator を構成して、デフォルトの VMware リポジトリからアップグレード パッケージをダウンロードできます。

前提条件

- すべてのネットワーク ファイル システムをマウント解除します。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。
- Orchestrator Appliance のメモリを 6 GB 以上増やします。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。
- vRealize Orchestrator 仮想マシンのディスク サイズを、Disk1=7 GB、Disk2=10 GB に増やします。
- Orchestrator Appliance の root パーティションに 3 GB 以上の使用可能な空き容量があることを確認してください。ディスク パーティションのサイズを増やす方法については、KB1004071 (<http://kb.vmware.com/kb/1004071>) を参照してください。
- Orchestrator 仮想マシンのスナップショットを作成します。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。
- 外部データベースを使用する場合は、データベースをバックアップします。
- 事前構成された Orchestrator PostgreSQL データベースを使用する場合は、コントロール センターの [データベースをエクスポート] メニューを使用して、データベースをバックアップします。

手順

- 1 仮想アプライアンス管理インターフェイス (VAMI : https://<orchestrator_server>:5480) にアクセスし、**root** としてログインします。
- 2 [更新] タブで、[設定] をクリックします。
[デフォルト リポジトリの使用] オプションの横にあるラジオ ボタンが選択されます。
- 3 [ステータス] ページで、[更新チェック] をクリックします。
- 4 アップデートが利用可能な場合は、[アップデートのインストール] をクリックします。

- 5 VMware エンドユーザー使用許諾契約に同意し、アップデートをインストールすることを確認します。
- 6 アップデートを完了するには、Orchestrator Appliance を再起動します。
 - a 仮想アプライアンス管理インターフェイス (VAMI) に **root** として再度ログインします。
- 7 (オプション) [更新] タブで、最新バージョンの Orchestrator Appliance が正常にインストールされていることを確認します。
- 8 コントロール センターに **root** としてログインします。
- 9 Orchestrator インスタンスのクラスタを作成する予定の場合は、ホスト設定を再構成します。
 - a コントロール センターの [ホスト設定] ページで [変更] をクリックします。
 - b vRealize Orchestrator のアプライアンス名ではなく、ロード バランサ サーバのホスト名を入力します。
- 10 認証を再構成します。
 - a アップグレードする前に、Orchestrator サーバが [LDAP] または [SSO (レガシー)] を認証方式として使用するように構成されていた場合は、[vSphere] または [vRealize Automation] を認証プロバイダとして構成します。
 - b 認証がすでに [vSphere] または [vRealize Automation] に設定されている場合は、設定を登録解除し、それらを再度登録します。

注: アップグレード前に、Orchestrator が認証プロバイダとして [vSphere] を使用し、vCenter Server の完全修飾ドメイン名または IP アドレスに接続するように構成されており、外部に Platform Services Controller がある場合、アップグレード後に、Orchestrator を vCenter Single Sign-On を含む Platform Services Controller インスタンスの完全修飾ドメイン名または IP アドレスに接続するように構成する必要があります。同一の vCenter Single Sign-On ドメインを共有するすべての Platform Services Controller の証明書を手動で Orchestrator にインポートする必要もあります。

これで、Orchestrator Appliance が正常にアップグレードされました。

次のステップ

コントロール センターの [設定を検証] ページで、Orchestrator が正しく設定されていることを確認します。

ISO イメージを使用した Orchestrator Appliance のアップグレード

Orchestrator を構成することにより、アプライアンスの CD-ROM ドライブにマウントされている ISO イメージ ファイルからアップグレードパッケージをダウンロードできます。

前提条件

- すべてのネットワーク ファイル システムをマウント解除します。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。
- Orchestrator Appliance のメモリを 6 GB 以上増やします。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。
- vRealize Orchestrator 仮想マシンのディスク サイズを、Disk1=7 GB、Disk2=10 GB に増やします。

- Orchestrator Appliance の root パーティションに 3 GB 以上の使用可能な空き容量があることを確認してください。ディスク パーティションのサイズを増やす方法については、KB1004071 (<http://kb.vmware.com/kb/1004071>) を参照してください。
- Orchestrator 仮想マシンのスナップショットを作成します。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。
- 外部データベースを使用する場合は、データベースをバックアップします。
- 事前構成された Orchestrator PostgreSQL データベースを使用する場合は、コントロール センターの[データベースをエクスポート]メニューを使用して、データベースをバックアップします。

手順

- 1 VMware の公式なダウンロード サイトで **VMware-vR0-Appliance-<version>-<build_number>-updaterepo.iso** アーカイブをダウンロードします。
- 2 Orchestrator Appliance 仮想マシンの CD-ROM ドライブを接続します。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。
- 3 ISO イメージ ファイルをアプライアンスの CD-ROM ドライブにマウントします。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。
- 4 仮想アプライアンス管理インターフェイス (VAMI : https://<orchestrator_server>:5480) にアクセスし、**root** としてログインします。
- 5 [更新] タブで、[設定] をクリックします。
- 6 [CD-ROM アップデートの使用] オプションの横にあるラジオ ボタンを選択します。
- 7 [ステータス] ページに戻ります。
使用可能なアップグレードのバージョンが表示されます。
- 8 [アップデートをインストール] をクリックします。
- 9 VMware エンドユーザー使用許諾契約に同意し、アップデートをインストールすることを確認します。
- 10 アップデートを完了するには、Orchestrator Appliance を再起動します。
 - a 仮想アプライアンス管理インターフェイス (VAMI) に **root** として再度ログインします。
- 11 (オプション) [更新] タブで、最新バージョンの Orchestrator Appliance が正常にインストールされていることを確認します。
- 12 コントロール センターに **root** としてログインします。
- 13 Orchestrator インスタンスのクラスタを作成する予定の場合は、ホスト設定を再構成します。
 - a コントロール センターの [ホスト設定] ページで [変更] をクリックします。
 - b vRealize Orchestrator のアプライアンス名ではなく、ロード バランサ サーバのホスト名を入力します。

14 認証を再構成します。

- a アップグレードする前に、Orchestrator サーバが [LDAP] または [SSO (レガシー)] を認証方式として使用するように構成されていた場合は、[vSphere] または [vRealize Automation] を認証プロバイダとして構成します。
- b 認証がすでに [vSphere] または [vRealize Automation] に設定されている場合は、設定を登録解除し、それらを再度登録します。

注: アップグレード前に、Orchestrator が認証プロバイダとして [vSphere] を使用し、vCenter Server の完全修飾ドメイン名または IP アドレスに接続するように構成されており、外部に Platform Services Controller がある場合、アップグレード後に、Orchestrator を vCenter Single Sign-On を含む Platform Services Controller インスタンスの完全修飾ドメイン名または IP アドレスに接続するように構成する必要があります。同一の vCenter Single Sign-On ドメインを共有するすべての Platform Services Controller の証明書を手動で Orchestrator にインポートする必要もあります。

これで、Orchestrator Appliance が正常にアップグレードされました。

次のステップ

コントロール センターの [設定を検証] ページで、Orchestrator が正しく設定されていることを確認します。

指定したリポジトリを使用した Orchestrator Appliance のアップグレード

Orchestrator を構成して、アップグレード アーカイブのアップロード先であるローカル リポジトリを使用できます。

前提条件

- すべてのネットワーク ファイル システムをマウント解除します。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。
- Orchestrator Appliance のメモリを 6 GB 以上増やします。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。
- vRealize Orchestrator 仮想マシンのディスク サイズを、Disk1=7 GB、Disk2=10 GB に増やします。
- Orchestrator Appliance の root パーティションに 3 GB 以上の使用可能な空き容量があることを確認してください。ディスク パーティションのサイズを増やす方法については、KB1004071 (<http://kb.vmware.com/kb/1004071>) を参照してください。
- Orchestrator 仮想マシンのスナップショットを作成します。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。
- 外部データベースを使用する場合は、データベースをバックアップします。
- 事前構成された Orchestrator PostgreSQL データベースを使用する場合は、コントロール センターの[データベースをエクスポート]メニューを使用して、データベースをバックアップします。

手順

- 1 アップグレード用のローカル リポジトリを準備します。
 - a ローカル Web サーバをインストールして構成します。
 - b VMware の公式なダウンロード サイトで **VMware-vR0-Appliance-<version>-<build_number>-updaterepo.zip** アーカイブをダウンロードします。
 - c **.ZIP** アーカイブをローカル リポジトリに抽出します。
- 2 仮想アプライアンス管理インターフェイス (VAMI : https://<orchestrator_server>:5480) にアクセスし、**root** としてログインします。
- 3 [更新] タブで、[設定] をクリックします。
- 4 [指定したリポジトリを使用] オプションの横にあるラジオ ボタンを選択します。
- 5 ローカル リポジトリの URL アドレスを **Update_Repo** ディレクトリをポイントして入力します。
http://<local_web_server>:<port>/build/mts/release/bora-<build_number>/publish/exports/Update_Repo
- 6 ローカル リポジトリで認証が必要になる場合は、ユーザー名とパスワードを入力します。
- 7 [設定の保存] をクリックします。
- 8 [ステータス] ページで、[更新チェック] をクリックします。
- 9 アップデートが利用可能な場合は、[アップデートのインストール] をクリックします。
- 10 VMware エンドユーザー使用許諾契約に同意し、アップデートをインストールすることを確認します。
- 11 アップデートを完了するには、Orchestrator Appliance を再起動します。
 - a 仮想アプライアンス管理インターフェイス (VAMI) に **root** として再度ログインします。
- 12 (オプション) [更新] タブで、最新バージョンの Orchestrator Appliance が正常にインストールされていることを確認します。
- 13 コントロール センターに **root** としてログインします。
- 14 Orchestrator インスタンスのクラスタを作成する予定の場合は、ホスト設定を再構成します。
 - a コントロール センターの [ホスト設定] ページで [変更] をクリックします。
 - b vRealize Orchestrator のアプライアンス名ではなく、ロード バランサ サーバのホスト名を入力します。

15 認証を再構成します。

- a アップグレードする前に、Orchestrator サーバが [LDAP] または [SSO (レガシー)] を認証方式として使用するように構成されていた場合は、[vSphere] または [vRealize Automation] を認証プロバイダとして構成します。
- b 認証がすでに [vSphere] または [vRealize Automation] に設定されている場合は、設定を登録解除し、それらを再度登録します。

注: アップグレード前に、Orchestrator が認証プロバイダとして [vSphere] を使用し、vCenter Server の完全修飾ドメイン名または IP アドレスに接続するように構成されており、外部に Platform Services Controller がある場合、アップグレード後に、Orchestrator を vCenter Single Sign-On を含む Platform Services Controller インスタンスの完全修飾ドメイン名または IP アドレスに接続するように構成する必要があります。同一の vCenter Single Sign-On ドメインを共有するすべての Platform Services Controller の証明書を手動で Orchestrator にインポートする必要もあります。

これで、Orchestrator Appliance が正常にアップグレードされました。

次のステップ

コントロール センターの [設定を検証] ページで、Orchestrator が正しく設定されていることを確認します。

vRealize Automation で使用するための外部 vRealize Orchestrator Appliance クラスタのアップグレード

vRealize Automation で vRealize Orchestrator Appliance クラスタを使用する場合は、いずれか 1 つのインスタンスをアップグレードした後に、新しくインストールした 7.4 ノードをアップグレード済みのインスタンスに参加させることで Orchestrator Appliance クラスタをバージョン 7.4 にアップグレードする必要があります。

前提条件

- [「vRealize Automation アプライアンスでのアップデートのインストール」](#)。
- IaaS コンポーネントをアップグレードします。[「vRealize Automation のアップグレード後の IaaS サーバ コンポーネントのアップグレード」](#) を参照してください。
- vRealize Orchestrator の複数のインスタンス間でトラフィックを分散するロード バランサを設定します。[vRealize Orchestrator ロード バランシング構成ガイド](#) を参照してください。
- すべての vRealize Orchestrator サーバ ノードのスナップショットを作成します。
- vRealize Orchestrator の共有データベースをバックアップします。

手順

- 1 コントロール センターから vRealize Automation NSX プラグインをアップグレードします。
- 2 すべてのクラスタ ノードで **vco-server** および **vco-configurator** Orchestrator サービスを停止します。
- 3 ドキュメントで説明されている手順のいずれかを使用して、クラスタ内の Orchestrator サーバ インスタンスのいずれか 1 つのみをアップグレードします。

- 4 バージョン 7.4 で新しい Orchestrator Appliance を展開します。
 - a クラスタに含まれているアップグレード済みインスタンスではなく、既存のネットワーク設定を使用して新しいノードを構成します。
- 5 コントロール センターの 2 番目のノードにアクセスして、構成ウィザードを開始します。
 - a `https://<your_orchestrator_server_ip_or_dns_name>:8283/vco-controlcenter` に移動します。
 - b OVA の展開時に入力したパスワードを使用して **root** としてログインします。
- 6 [クラスタ化された Orchestrator] デプロイ タイプを選択します。
このタイプを選択することで、ノードが既存の Orchestrator クラスタに参加することを指定できます。
- 7 [ホスト名] テキスト ボックスに、最初の Orchestrator サーバ インスタンスのホスト名または IP アドレスを入力します。

注: これは、2 番目のノードに参加させている Orchestrator インスタンスのローカル IP アドレスまたはホスト名にする必要があります。ロード バランサのアドレスを使用することはできません。

- 8 [ユーザー名] および [パスワード] テキスト ボックスに、最初の Orchestrator サーバ インスタンスの root 認証情報を入力します。
- 9 [参加] をクリックします。Orchestrator インスタンスが参加先のノードの構成をクローン作成します。
両方のノードの Orchestrator サーバ サービスが自動的に再起動されます。
- 10 ロード バランサのアドレスおよび**管理者**としてのログインを介してアップグレードされた Orchestrator クラスタのコントロール センターにアクセスします。
- 11 [Orchestrator クラスタ管理] ページで、[アクティブな設定フィンガー プリント] の文字列と [保留中の設定フィンガー プリント] の文字列が、クラスタのすべてのノードで一致することを確認します。

注: 2 つの文字列が一致するまでページを数回更新する必要があることがあります。

- 12 コントロール センターの [設定を検証] ページを開いて、vRealize Orchestrator クラスタが適切に構成されていることを確認します。
- 13 (オプション) クラスタ内の追加ノードごとに手順 3 から手順 8 を繰り返します。
- 14 コントロール センターから vRealize Automation NSX プラグインをアップグレードします。

Orchestrator クラスタが正常にアップグレードされました。

次のステップ

[「ロード バランサの有効化」](#)。

Active Directory 接続へのユーザーまたはグループの追加

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

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

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

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

注: 同期アクションは、アクションの開始後にキャンセルできません。

前提条件

- コネクタがインストールされ、アクティベーション コードで有効になっている必要があります。[ユーザー属性] ページで必須のデフォルト属性を選択し、その他の属性を追加します。
[PLUGINS_ROOT/com.vmware.vra.prepare.use.doc/GUID-9B25F502-EC8C-40CF-8ACF-4731B5A6903A.html](https://plugins.root.com.vmware.vra.prepare.use.doc/GUID-9B25F502-EC8C-40CF-8ACF-4731B5A6903A.html) 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。
- Windows 認証と統合されたマルチ フォレスト Active Directory があり、ドメイン ローカル グループに異なるフォレストのメンバーが含まれている場合は、次の操作を実行します。バインド ユーザーをドメイン ローカル グループの管理者グループに追加します。バインド ユーザーを追加しない場合、これらのメンバーはドメイン ローカル グループに含まれません。
- **テナント管理者**として vRealize Automation にログインします。

手順

- 1 [管理] - [ディレクトリ管理] - [ディレクトリ] を選択します。
- 2 目的のディレクトリ名をクリックします。
- 3 [同期設定] をクリックして、同期オプションのダイアログ ボックスを開きます。

- 4 ユーザーまたはグループの構成を変更するかどうかに応じて、適切なアイコンをクリックします。

グループ構成を編集するには：

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

ユーザー構成を編集するには：

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

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

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

ロード バランサの有効化

環境内でロード バランサを使用する場合は、セカンダリ ノードと健全性チェックを再度有効にして、ロード バランサのタイムアウト設定を元に戻します。

vRealize Automation の健全性チェックは、バージョンによって異なります。詳細については、[VMware vRealize Automation ドキュメント](#)の『vRealize Automation Load Balancing Configuration Guide』を参照してください。

ロード バランサのタイムアウト設定を変更して、10 分からデフォルトに戻します。

vRealize Automation のアップグレード後のタスク

vRealize Automation 6.2.5 から 7.4 へのアップグレードが完了したら、アップグレード後に必要なタスクを実行します。

高可用性を展開する環境でのポート構成

リモート コンソール機能をサポートするには、高可用性を展開している環境をアップグレードした後、ポート 8444 のトラフィックが vRealize Automation アプライアンスに渡されるようにロード バランサを構成する必要があります。

詳細については、[vRealize Automation ドキュメント](#)の『vRealize Automation Load Balancing Configuration Guide』を参照してください。

組み込みの vRealize Orchestrator で高可用性をサポートするための再構成

高可用性環境では、各ターゲット レプリカ vRealize Automation アプライアンスを手動でクラスタに再参加させて、組み込みの vRealize Orchestrator で高可用性のサポートを有効にする必要があります。

前提条件

ターゲット レプリカ vRealize Automation アプライアンス管理コンソールにログインします。

- 1 ブラウザを起動し、ターゲット レプリカ仮想アプライアンスの完全修飾ドメイン名 (FQDN) `https://<vra-va-hostname.domain.name>:5480` を使用して、ターゲット レプリカ vRealize Automation 管理コンソールを開きます。

- 2 ユーザー名 **root** と、ターゲット レプリカ vRealize Automation アプライアンスの展開時に入力したパスワードを使用してログインします。

手順

- 1 [vRA 設定] - [クラスタ] の順に選択します。
- 2 [先頭のクラスタ ノード] テキスト ボックスに、ターゲット マスター vRealize Automation アプライアンスの FQDN を入力します。
- 3 [パスワード] テキスト ボックスに root パスワードを入力します。
- 4 [クラスタに参加] をクリックします。
証明書の警告を無視して続行します。システムによってクラスタのサービスが再起動されます。
- 5 サービスが実行されていることを確認します。
 - a 最上部のタブ バーで、[サービス] をクリックします。
 - b サービスの起動の進行状況を監視するには、[更新] をクリックします。

ユーザー用リモート コンソール アクションとの接続の有効化

ユーザー用リモート コンソール アクションは、vRealize Automation で vSphere によってプロビジョニングされるアプライアンスでサポートされています。

このリリースをアップグレードしたらブループリントを編集し、[アクション] タブの [リモート コンソールに接続] アクションを選択します。

詳細については、[ナレッジ ベースの記事 2109706](#) を参照してください。

外部ワークフローのタイムアウト ファイルのリストア

アップグレード プロセスによって xmldb ファイルが上書きされてしまうため、vRealize Automation の外部ワークフローのタイムアウト ファイルを再構成する必要があります。

手順

- 1 次のディレクトリから、システム上の外部ワークフロー構成 (xmldb) ファイルを開きます。
`\\VMware\\vCAC\\Server\\ExternalWorkflows\\xmldb\\`
- 2 xmldb ファイルを移行の前にバックアップしたファイルに置き換えます。バックアップ ファイルがない場合は、外部ワークフローのタイムアウト設定を再構成します。
- 3 設定を保存します。

vRealize Orchestrator サービスが使用可能かどうかの確認

vRealize Automation の最新バージョンにアップグレードした後、vRealize Automation と vRealize Orchestrator の接続を確認する必要があります。アップグレード後に接続の復旧が必要な場合があります。

前提条件

vRealize Orchestrator 構成インターフェイスにログインします。

手順

- 1 [構成の検証] をクリックします。
- 2 [認証] セクションに緑のチェックが示されている場合は、手順 5 に進んでください。
- 3 [認証] セクションに緑のチェックが示されていない場合は、以下の手順を実行して vRealize Orchestrator への接続を復元します。
 - a [ホーム] をクリックします。
 - b [認証プロバイダの構成] をクリックします。
 - c [管理者グループ] テキスト ボックスで、[変更] をクリックし、正しく解決できる新しい管理者グループを選択します。

vcoadmins グループは、デフォルトの vsphere.local テナントでのみ選択できます。vRealize Orchestrator 用に別のテナントを使用している場合は、別のグループを選択する必要があります。
 - d [変更を保存] をクリックし、要求された場合は、vRealize Orchestrator サーバを再起動します。
 - e [ホーム] をクリックします。
- 4 手順 1 を繰り返して、[認証] セクションに緑のチェックが依然として示されることを確認します。
- 5 [ホーム] をクリックし、vRealize Orchestrator コントロール センターを閉じます。

ターゲット vRealize Automation に組み込まれた vRealize Orchestrator インフラストラクチャ エンドポイントの再構成

vRealize Automation 6.2.x 環境から移行する場合は、ターゲットの組み込み vRealize Orchestrator サーバを指しているインフラストラクチャ エンドポイントの URL を更新する必要があります。

前提条件

- vRealize Automation 7.4 に正常に移行します。
- ターゲットの vRealize Automation コンソールにログインします。
 - a ターゲット仮想アプライアンスの完全修飾ドメイン名 `https://<vra-va-hostname.domain.name>/vcac` を使用して vRealize Automation コンソールを開きます。

高可用性環境の場合は、ターゲット仮想アプライアンス ロード バランサの完全修飾ドメイン名 `https://<vra-va-lb-hostname.domain.name>/vcac` を使用してコンソールを開きます。
 - b Infrastructure as a Service (IaaS) 管理者ユーザーとしてログインします。

手順

- 1 [インフラストラクチャ] - [エンドポイント] - [エンドポイント] の順に選択します。
- 2 [エンドポイント] ページで、vRealize Orchestrator エンドポイントを選択し、[編集] をクリックします。
- 3 [アドレス] テキスト ボックスで、vRealize Orchestrator エンドポイントの URL を編集します。
 - 最小環境に移行した場合は、vRealize Orchestrator エンドポイント URL を `https://<vra-va-hostname.domain.name>:443/vco` に置き換えます。

- 高可用性環境に移行した場合は、vRealize Orchestrator エンドポイント URL を **https://<vra-vault-hostname.domain.name>:443/vco** に置き換えます。

4 [OK] をクリックします。

5 vRealize Orchestrator エンドポイントでデータ収集を手動で実行します。

- a [エンドポイント] ページで、vRealize Orchestrator エンドポイントを選択します。
- b [アクション] - [データ収集] の順に選択します。

データ収集が成功したことを確認します。

app.config ファイルに行ったログの変更のリストア

アップグレード プロセスでは、構成ファイルのログへの変更が上書きされます。アップグレードが終了した後、アップグレード前に **app.config** ファイルに行った変更をリストアする必要があります。

アップグレード後に Manager Service の自動フェイルオーバーを有効にする

vRealize Automation をアップグレードすると、Manager Service の自動フェイルオーバーがデフォルトで無効になります。

アップグレード後に Manager Service の自動フェイルオーバーを有効にするには、次の手順を実行します。

手順

- 1 vRealize Automation アプライアンスで、root ユーザーとしてコマンド プロンプトを開きます。
- 2 ディレクトリを **/usr/lib/vcac/tools/vami/commands** に変更します。
- 3 Manager Service の自動フェイルオーバーを有効にするには、次のコマンドを実行します。

```
python ./manager-service-automatic-failover ENABLE
```

laaS 環境全体で自動フェイルオーバーを無効にするには、次のコマンドを実行します。

```
python ./manager-service-automatic-failover DISABLE
```

Manager Service の自動フェイルオーバーについて

vRealize Automation laaS Manager Service は、プライマリの Manager Service が停止した場合、バックアップへのフェイルオーバーを自動的に実行するように設定できます。

vRealize Automation 7.3 以降では、サーバをプライマリまたはバックアップに設定する際、Windows サーバごとに手動で Manager Service を開始または停止する必要がなくなりました。アップグレードシェル スクリプトまたは laaS インストーラ実行可能ファイルを使用して laaS をアップグレードするときに、自動の Manager Service のフェイルオーバーはデフォルトで無効になります。

自動フェイルオーバーを有効にすると、バックアップを含むすべての Manager Service ホストで自動的に Manager Service が開始されます。自動フェイルオーバー機能により、ホストは透過的に互いを監視し、必要に応じてフェイルオーバーを実行しますが、すべてのホストで Windows サービスが実行されている必要があります。

注: 自動フェイルオーバーの使用は必須ではありません。自動フェイルオーバーを無効にして、引き続き手動で Windows サービスを開始および停止し、プライマリまたはバックアップ ホストの設定を制御することもできます。手動でフェイルオーバーを行う際は、一度に 1 台ずつホストのサービスを開始してください。自動フェイルオーバーが無効の場合、同時に複数の IaaS サーバでサービスを実行すると、vRealize Automation を使用できなくなります。

自動フェイルオーバーをホストごとに有効または無効に設定しないでください。IaaS 環境では、自動フェイルオーバーを有効または無効にする設定は、すべての Manager Service ホストで同一にする必要があります。

接続テストの実行とアップグレード後のエンドポイントの確認

vRealize Automation 7.3 以前から 7.4 にアップグレードすると、ターゲット環境のエンドポイントが変更されます。

vRealize Automation 7.4 へのアップグレード後には、該当するすべてのエンドポイントに対して [接続をテスト] アクションを実行する必要があります。また、アップグレード後の一部のエンドポイントで調整が必要になる場合があります。詳細については、[アップグレードまたは移行後のエンドポイントを使用する場合の考慮事項](#)を参照してください。

アップグレードまたは移行されたエンドポイントのデフォルトのセキュリティ設定では、信頼されていない証明書を受け入れません。

信頼されていない証明書を使用していた場合、以前の vRealize Automation インストール環境からアップグレードまたは移行した後、vSphere と NSX のすべてのエンドポイントに対して、次の手順を実行して証明書の検証を有効にする必要があります。そうしないと、エンドポイントの操作が証明書エラーで失敗します。詳細については、VMware ナレッジベースの記事「Endpoint communication is broken after upgrade to vRA 7.3 (KB2150230)」(<http://kb.vmware.com/kb/2150230>) および「How to download and install vCenter Server root certificates to avoid Web Browser certificate warnings (KB2108294)」(<http://kb.vmware.com/kb/2108294>) を参照してください。

- 1 アップグレード後または移行後に、vRealize Automation vSphere エージェント マシンにログインし、[サービス] タブを使用して vSphere エージェントを再起動します。

移行ではすべてのエージェントが再起動されない場合があるため、必要に応じて手動で再起動します。

- 2 少なくとも 1 つの ping レポートが終了するのを待ちます。ping レポートの完了には 1、2 分かかります。
- 3 vSphere エージェントがデータ収集を開始したら、IaaS 管理者として vRealize Automation にログインします。
- 4 [インフラストラクチャ] - [エンドポイント] - [エンドポイント] の順にクリックします。
- 5 vSphere エンドポイントを編集し、[接続をテスト] をクリックします。
- 6 証明書のプロンプトが表示されたら、[OK] をクリックして証明書を受け入れます。

証明書のプロンプトが表示されない場合、証明書が現在、プロキシ エージェント マシンや DEM マシンなどのエンドポイントのサービスをホストする Windows マシンの信頼されたルート認証局に正しく保存されていない可能性があります。

- 7 [OK] をクリックして、証明書の承認を適用し、エンドポイントを保存します。

8 vSphere エンドポイントごとにこの手順を繰り返します。

9 NSX エンドポイントごとにこの手順を繰り返します。

[接続をテスト] 操作は成功したものの、一部のデータ収集やプロビジョニング操作が失敗した場合、エンドポイントとして機能するすべてのエージェント マシンとすべての DEM マシンに同じ証明書をインストールできます。または、既存のマシンから証明書をアンインストールして、問題のあるエンドポイントに対して上記の手順を繰り返します。

DynamicTypes プラグインのインポート

DynamicTypes プラグインを使用していて、アップグレード前にパッケージとして構成をエクスポートした場合は、次のワークフローをインポートする必要があります。

/Library/Dynamic Types/Configuration/Import Configuration From Package

/Library コマンドは、vRealize Orchestrator Java クライアントから実行されます。

vRealize Automation アップグレードのトラブルシューティング

アップグレードのトラブルシューティングに関するトピックでは、vRealize Automation 6.2.5 から 7.4 のアップグレード時に発生する可能性のある問題の解決策について説明します。

ロード バランサのタイムアウト エラーでインストールまたはアップグレードに失敗する

ロード バランサを使用した分散環境を実現するための vRealize Automation のインストールまたはアップグレードが、503 サービス利用不能エラーで失敗します。

問題

ロード バランサ タイムアウトの設定が原因でタスクを完了するための十分な時間が確保できないため、インストールまたはアップグレードに失敗します。

原因

ロード バランサ タイムアウトの設定値が小さいとエラーになる可能性があります。この問題を修正するには、ロード バランサ タイムアウトの設定値を 100 秒以上に増やしてタスクを再実行します。

ソリューション

- 1 ロード バランサ タイムアウト値を最低でも 100 秒に増やします。
- 2 インストールまたはアップグレードを再実行します。

laaS Web サイト コンポーネントのアップグレードに失敗する

laaS のアップグレードに失敗し、アップグレードを続行できません。

問題

Web サイト コンポーネントの laaS アップグレードに失敗します。インストーラ ログ ファイルに次のエラー メッセージが表示されます。

- System.Data.Services.Client.DataServiceQueryException:
An error occurred while processing this request. --->
System.Data.Services.Client.DataServiceClientException: <!DOCTYPE html>

- **Description:** An application error occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed remotely (for security reasons). It could, however, be viewed by browsers running on the local server machine.
- Warning: Non-zero return code. Command failed.
- Done Building Project "C:\Program Files (x86)\VMware\vCAC\Server\Model Manager Data\DeployRepository.xml" (InstallRepoModel target(s)) -- FAILED.

リポジトリ ログ ファイルに次のエラー メッセージが表示されます。

- [Error]: [sub-thread-Id="20" context="" token=""] Failed to start repository service. Reason: System.InvalidOperationException: Configuration section encryptionKey is not protected at DynamicOps.Common.Utils.EncryptionHelpers.ReadKeyFromConfiguration(Configuration config) at DynamicOps.Common.Utils.EncryptionHelpers.Decrypt(String value) at DynamicOps.Repository.Runtime.CoreModel.GlobalPropertyItem.Decrypt(Func`2 decryptFunc) at DynamicOps.Common.Entity.ContextHelpers.OnObjectMaterializedCallbackEncryptable(Object sender, ObjectMaterializedEventArgs e) at System.Data.Common.Internal.Materialization.Shaper.RaiseMaterializedEvents() at System.Data.Common.Internal.Materialization.Shaper`1.SimpleEnumerator.MoveNext() System.Linq.Enumerable.FirstOrDefault[TSource](IEnumerable`1 source) System.Linq.Queryable.FirstOrDefault[TSource](IQueryable`1 source) at DynamicOps.Repository.Runtime.Common.GlobalPropertyHelper.GetGlobalPropertyItemValue(Core ModelEntities

```
coreModelContext, String propertyName, Boolean throwIfPropertyNotFound)
at
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.LoadSolutionUserCertificate()
at
DynamicOps.Repository.Runtime.CafeClientAbstractFactory.InitializeFromDb(String
coreModelConnectionString)
DynamicOps.Repository.Runtime.Common.RepositoryRuntime.Initialize()。
```

原因

laas アップグレードは、**web.config** ファイルの作成日が、変更日と同じまたはそれ以降の日付になっている場合に失敗します。

ソリューション

- 1 laaS ホスト上で、Windows にログインします。
- 2 Windows コマンド プロンプトを開きます。
- 3 vRealize Automation インストール フォルダに移動します。
- 4 [管理者として実行] オプションで任意のテキスト エディタを起動します。
- 5 **web.config** ファイルの場所を特定して選択し、ファイルを保存し直すことで、このファイルの変更日を作成日より後に変更できます。
- 6 **web.config** ファイルのプロパティを調べて、ファイル変更日が作成日よりも後であることを確認します。
- 7 laaS をアップグレードします。

実行中の SSL 検証エラーが原因で Manager Service の実行に失敗する

SSL 検証エラーが原因で、Manager Service の実行に失敗します。

問題

Manager Service が失敗し、ログに次のエラー メッセージが記録されます。

```
[Info]: Thread-Id="6" - context="" token="" Failed to connect to the core
database, will retry in 00:00:05, error details: A connection was successfully
established with the server, but then an error occurred during the login
process. (provider: SSL Provider, error: 0 - The certificate chain was issued
by an authority that is not trusted.)
```

原因

実行時、SSL 検証エラーが原因で、Manager Service の実行に失敗します。

ソリューション

- 1 **ManagerService.config** 構成ファイルを開きます。

2 次の行で **Encrypt=False** に更新します。

```
<add name="vcac-repository" providerName="System.Data.SqlClient"
connectionString="Data Source=iaas-db.sqa.local;Initial
Catalog=vcac;Integrated Security=True;Pooling=True;Max Pool
Size=200;MultipleActiveResultSets=True;Connect Timeout=200,
Encrypt=True" />
```

アップグレード後のログインの失敗

同期されていないユーザー アカウントを使用するセッションでは、アップグレード後にブラウザを終了し、もう一度ログインする必要があります。

問題

vRealize Automation をアップグレードすると、ログイン時に同期されていないユーザー アカウントへのアクセスは拒否されます。

ソリューション

ブラウザを終了し、vRealize Automation を再起動します。

アップグレード後にサービス カタログに表示されるカタログ アイテムを申請できない

vRealize Automation の最新バージョンにアップグレードすると、前のバージョンの特定のプロパティ定義を使用するカタログ アイテムがサービス カタログに表示されますが、申請することはできません。

問題

6.2.x 以前のバージョンからアップグレードしていて、次のコントロール タイプまたは属性を持つプロパティ定義が設定されている場合は、これらの属性がアップグレード後のプロパティ定義に含まれていないため注意が必要です。これらの定義を使用するカタログ アイテムは、アップグレード前と同様に動作しなくなります。

- コントロール タイプ：チェック ボックスまたはリンク
- 属性：関係、正規表現、またはプロパティのレイアウト

原因

vRealize Automation 7.0 以降では、プロパティ定義でこれらの属性が使用されなくなりました。プロパティ定義を再作成するか、組み込みのコントロール タイプまたは属性ではなく vRealize Orchestrator スクリプト アクションを使用するようにプロパティ定義を設定する必要があります。

スクリプト アクションを使用して、これらのコントロール タイプまたは属性を vRealize Automation 7.x に移行します。

ソリューション

- 1 vRealize Orchestrator でこれらのプロパティ値を返すスクリプト アクションを作成します。このアクションは単純な値を返す必要があります。たとえば、文字列、整数、またはその他のサポートされているタイプです。このアクションは、依存する他のプロパティを入力パラメータとして取ることがあります。

2 vRealize Automation コンソールで、製品の定義を設定します。

- a [管理] - [プロパティ ディクショナリ] - [プロパティ定義] の順に選択します。
- b プロパティ定義を選択して、[[編集]] をクリックします。
- c [アドバイスの表示] ドロップダウン メニューで、[ドロップダウン] を選択します。
- d [値] ドロップダウン メニューで、[外部値] を選択します。
- e スクリプト アクションを選択します。
- f [OK] をクリックします。
- g スクリプト アクションに含まれる入力パラメータを設定します。既存の関係を維持するには、パラメータを他のプロパティにバインドします。
- h [OK] をクリックします。

外部の PostgreSQL データベースのマージが失敗する

外部の PostgreSQL データベースは組み込みの PostgreSQL データベースと正常にマージされません。

問題

外部の PostgreSQL データベース バージョンが組み込みの PostgreSQL データベース バージョンよりも新しい場合、マージは成功しません。

ソリューション

- 1 外部の PostgreSQL データベースのホストにログインします。
- 2 **psql --version** コマンドを実行します。
外部データベースの PostgreSQL バージョンをメモします。
- 3 組み込みの PostgreSQL データベースのホストにログインします。
- 4 **psql --version** コマンドを実行します。
組み込みデータベースの PostgreSQL バージョンをメモします。

外部の PostgreSQL バージョンが組み込みの PostgreSQL バージョンよりも新しい場合は、外部 PostgreSQL データベースのマージについて、サポートにお問い合わせください。

高可用性環境アップグレード後にクラスタへの参加コマンドが失敗したように表示される

セカンダリ クラスタ ノードの管理コンソールで [クラスタに参加] をクリックした後、進行状況インジケータが表示されなくなります。

問題

アップグレード後に vRealize Automation アプライアンス管理コンソールを使用してセカンダリ クラスタ ノードをプライマリ ノードに参加させると、進行状況インジケータが消え、エラー メッセージも正常完了メッセージも表示されなくなります。この挙動は断続的に確認される問題です。

原因

進行状況インジケータが消えるのは、一部のブラウザがサーバからの応答待ちを中止するためです。この挙動によってクラスタへの参加プロセスが停止することはありません。正常にクラスタへの参加が完了した場合、ログ ファイル (`/var/log/vmware/vcac/vcac-config.log`) を表示することで確認できます。

ルート パーティションに十分な空き容量がない場合にアップグレードが失敗する

vRealize Automation アプライアンス ホストのルート パーティションに十分な空き容量がない場合、アップグレードを続行できません。

ソリューション

この手順では、vRealize Automation アプライアンス ホストのディスク 1 ルート パーティションの空き容量を増やします。分散型展開では、この手順を実行して各レプリカ ノードの空き容量を増やしたうえで、マスター ノードの空き容量を増やします。

注: この手順を実行すると、次の警告メッセージが表示される場合があります。

- **WARNING: Re-reading the partition table failed with error 16:**
Device or resource busy. The kernel still uses the old table. The new table will be used at the next reboot or after you run `partprobe(8)` or `kpartx(8)` Syncing disks.
- **Error: Partition(s) 1 on /dev/sda have been written, but we have been unable to inform the kernel of the change, probably because it/they are in use. As a result, the old partition(s) will remain in use. You should reboot now before making further changes.**

「変更を行う前に今すぐ再起動する必要があります。」このメッセージは無視してください。手順 10 の前にシステムを再起動すると、アップグレード プロセスが失敗します。

手順

- 1 vRealize Automation アプライアンス ホストの仮想マシンをパワーオンし、SSH 接続で root ユーザーとしてログインします。
- 2 以下のコマンドを実行してサービスを停止します。
 - a `service vcac-server stop`
 - b `service vco-server stop`
 - c `service vpostgres stop`
- 3 次のコマンドを実行してスワップ パーティションをマウント解除します。


```
swapoff -a
```

- 4 次のコマンドを実行して、既存のディスク 1 パーティションを削除し、44 GB のルート パーティションと 6 GB のスワップ パーティションを作成します。

```
(echo d; echo 2; echo d; echo 1; echo n; echo p; echo ; echo ; echo '+44G'; echo n; echo p; echo ; echo ; echo ; echo w; echo p; echo q) | fdisk /dev/sda
```

- 5 次のコマンドを実行して、スワップ パーティションのタイプを変更します。

```
(echo t; echo 2; echo 82; echo w; echo p; echo q) | fdisk /dev/sda
```

- 6 次のコマンドを実行して、ディスク 1 にブート可能フラグを設定します。

```
(echo a; echo 1; echo w; echo p; echo q) | fdisk /dev/sda
```

- 7 次のコマンドを実行して、パーティション変更を Linux カーネルに登録します。

```
partprobe
```

変更前の再起動を促すメッセージが表示されても、そのメッセージは無視してください。手順 10 の前にシステムを再起動すると、アップグレード プロセスが失敗します。

- 8 次のコマンドを実行して、新しいスワップ パーティションをフォーマットします。

```
mkswap /dev/sda2
```

- 9 次のコマンドを実行してスワップ パーティションをマウントします。

```
swapon -a
```

- 10 vRealize Automation アプライアンスを再起動します。

- 11 アプライアンスの再起動後、次のコマンドを実行して、ディスク 1 パーティション テーブルのサイズを変更します。

```
resize2fs /dev/sda1
```

- 12 ディスクの拡張に成功したことを確認するために、**df -h** を実行し、**/dev/sda1** の利用可能なディスク容量が 30 GB より大きいことを確かめます。

.xml ファイルのバックアップ コピーによってシステムがタイムアウトする

vRealize Automation は、\VMware\VCAC\Server\ExternalWorkflows\xml\ディレクトリにある拡張子が.xml であるすべてのファイルを登録します。このディレクトリに拡張子が.xml のバックアップ ファイルが含まれていると、システムは重複するワークフローを実行するため、システムがタイムアウトします。

ソリューション

回避策：このディレクトリのファイルをバックアップするときは、バックアップ ファイルを別のディレクトリに移動するか、バックアップ ファイルの拡張子を.xml 以外の拡張子に変更します。

vRealize Automation での実体のないノードの削除

実体のないノードとは、ホスト上で報告されているのにそのホストに存在しない重複ノードです。

問題

各 IaaS ノードおよび仮想アプライアンス ノードが健全な状態にあることを確認するとき、あるホストに実体のないノードが 1 つ以上あることに気付くことがあります。実体のないノードはすべて削除する必要があります。

ソリューション

- 1 プライマリ vRealize Automation アプライアンスで、vRealize Automation アプライアンスを展開したときに入力したパスワードを使用して、**root** として vRealize Automation アプライアンス管理にログインします。
- 2 [vRA 設定] - [クラスタ] の順に選択します。
- 3 表内のそれぞれの実体のないノードに対して、[削除] をクリックします。

vRealize Automation で新規ディレクトリを作成できない

最初の同期コネクタを使用して新規ディレクトリを追加しようとすると失敗します。

問題

この問題は、`usr/local/horizon/conf/states/VSPHERE.LOCAL/3001/` にある、正しくない `config-state.json` ファイルが原因で発生します。

この問題の解決方法については、[ナレッジベースの記事 KB2145438](#) を参照してください。

アップグレード中に作成された展開が一部の仮想マシンに存在しない

アップグレード時に仮想マシンの状態が指定なしの場合、ターゲット環境で対応する展開が作成されません。

問題

アップグレード時に仮想マシンの状態がソース環境で指定なしの場合、対応する展開がターゲット環境で作成されません。アップグレード後に仮想マシンの状態が指定なしから変わると、バルク インポートを使用してターゲット展開にマシンをインポートすることができます。

信頼されていない証明書に関するエラー

vRealize Automation アプライアンス コンソールの [ログ ビューア] ページでインフラストラクチャを表示すると、**Certificate is not trusted** のような文言を含むエンドポイント接続障害レポートが表示されることがあります。

問題

vRealize Automation アプライアンス コンソールで、[インフラストラクチャ] - [監視] - [ログ] の順に選択します。[ログ ビューア] ページに、次のようなレポートが表示される場合があります。

エンドポイントへの接続に失敗しました。このエンドポイントへの安全な接続を確立できることを検証するには、[エンドポイント] ページで vSphere エンドポイントに移動し、[テスト接続] ボタンをクリックします。

内部例外: 証明書が信頼されていません (RemoteCertificateChainErrors)。件名: C=US, CN=vc6.mycompany.com
サムプリント: DC5A8816231698F4C9013C42692B0AF93D7E35F1

原因

vRealize Automation 7.3 以前のバージョンから 7.4 にアップグレードすると、元の環境にあったエンドポイントに変更が加えられます。最近 vRealize Automation 7.4 にアップグレードした環境では、安全な https 接続を使用するそれぞれの既存のエンドポイントを IaaS 管理者が確認する必要があります。「**Certificate is not trusted**」エラーが発生したエンドポイントは、適切に機能しません。

ソリューション

- 1 インフラストラクチャ管理者として vRealize Automation コンソールにログインします。
- 2 [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。
- 3 安全な接続が使用されている各エンドポイントについて、次の手順を実行します。
 - a [編集] をクリックします。
 - b [テスト接続] をクリックします。
 - c 証明書の詳細を確認し、この証明書を信頼する場合は、[OK] をクリックします。
 - d このエンドポイントによって使用されるすべての IaaS プロキシ エージェントの Windows サービスを再起動します。
- 4 インフラストラクチャの [ログ ビューア] ページに「**Certificate is not trusted**」エラーが表示されなくなったことを確認します。

vRealize Automation のインストールまたはアップグレードが失敗する

vRealize Automation のインストールまたはアップグレードが失敗し、エラー メッセージがログ ファイルに表示されます。

問題

vRealize Automation のインストールまたはアップグレードが失敗します。これは通常、インストールまたはアップグレード中に適用される修正に失敗した場合に発生します。ログ ファイルに次のようなエラー メッセージが表示されます。**Security error. Applying automatic fix for FIREWALL prerequisite failed. RPM Status 1: Pre install script failed, package test and installation skipped**

原因

Windows 環境のグループ ポリシーで、PowerShell スクリプトの実行が [有効] に設定されています。

ソリューション

- 1 Windows ホスト マシンで **gpedit.msc** を実行してローカル グループ ポリシー エディターを開きます。
- 2 [コンピューターの構成] の下にある左側のペインで、展開ボタンをクリックして [管理用テンプレート] - [Windows コンポーネント] - [Windows PowerShell] の順に開きます。
- 3 [スクリプトの実行を有効にする] で、状態を **Enabled** から **Not Configured** に変更します。

更新で管理エージェントのアップグレードに失敗する

vRealize Automation アプライアンス 管理コンソールの [ステータスの更新] ページで [更新のインストール] をクリックすると、管理エージェントに関するエラー メッセージが表示されます。

問題

アップグレード プロセスが成功しない。「ノード x で管理エージェントをアップグレードできません」というメッセージが表示されます。メッセージに複数のノードがリストされる場合もあります。

原因

この問題はさまざまな条件によって発生します。エラー メッセージには、影響を受けるマシンのノード ID のみが表示されます。コマンドが失敗したマシン上の管理エージェントについての詳細情報は、**All.log** ファイルに含まれています。

状況に応じて、影響を受けるノードで次のタスクを実行します。

ソリューション

- 管理エージェント サービスが実行されていない場合は、このサービスを開始し、仮想アプライアンスでアップグレードを再開します。
- 管理エージェント サービスが実行されており、管理エージェントがアップグレードされている場合は、仮想アプライアンスでアップグレードを再開します。
- 管理エージェント サービスが実行されているものの、管理エージェントがアップグレードされていない場合は、手動でアップグレードを実行します。
 - a ブラウザを開き、vRealize Automation アプライアンス上の [vRealize Automation IaaS のインストール] ページ (<https://<va-hostname.domain.name>:5480/install>) に移動します。
 - b 管理エージェントのインストーラをダウンロードして、実行します。
 - c 管理エージェントのマシンを再起動します。
 - d 仮想アプライアンスでアップグレードを再開します。

管理エージェントのアップグレードに失敗する

vRealize Automation から 7.2- 7.3.x へのアップグレード時に、管理エージェントのアップグレードに失敗します。

問題

フェイルオーバーの発生によってプライマリとセカンダリの管理エージェントのホストが入れ替わった場合、自動化されたアップグレード プロセスによって想定されるホストを見つけることができないため、アップグレードに失敗します。管理エージェントがアップグレードされていない各 IaaS ノードで、この手順を実行します。

ソリューション

- 1 管理エージェント ログ フォルダ (**C:\Program Files (x86)\VMware\VCAC\Management Agent\Logs**) にある All.log を開きます。

インストール フォルダの場所は、デフォルトの場所とは異なる場合があります。

- 2 ログ ファイル内を検索して、古くなった仮想アプライアンスやパワーオフされている仮想アプライアンスに関するメッセージを探します。

たとえば、次のようなものです。INNER EXCEPTION: System.Net.WebException: Unable to connect to the remote server ---> System.Net.Sockets.SocketException: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond <IP_Address>:5480

- 3 管理エージェントの構成ファイル (C:\Program Files (x86)\VMware\vCAC\Management Agent\VMware.IaaS.Management.Agent.exe.config) を編集して、既存の alternativeEndpointaddress の値をプライマリ仮想アプライアンス エンドポイントの URL で置き換えます。

インストール フォルダの場所は、デフォルトの場所とは異なる場合があります。

VMware.IaaS.Management.Agent.exe.config での alternativeEndpointaddress の例を次に示します。

```
<alternativeEndpoint address="https://<FQDN>:5480/"
thumbprint="<thumbprint number>" />
```

- 4 管理エージェント Windows サービスを再起動し、All.log ファイルを参照してこのサービスが機能していることを確認します。

- 5 プライマリ vRealize Automation アプライアンスでアップグレード手順を実行します。

デフォルトのタイムアウト設定が原因で vRealize Automation のアップデートに失敗する

使用環境で、データベース同期のデフォルトの時間設定が短すぎる場合は、アップデートの時間設定を長くすることができます。

問題

データベースの同期にデフォルトのタイムアウト設定値である 3,600 秒よりも長い時間を要する一部の環境では、Vcac-Config SynchronizeDatabases コマンドのタイムアウト設定は不十分です。

API と Vcac-config.exe ユーティリティ ツール間の通信は、Vcac-Config.exe.config ファイルの cafeTimeoutInSeconds および cafeRequestPageSize プロパティの値によって制御されています。このファイルのパスは、<IaaS installation location>\VMware\vCAC\Server\Model Manager Data\Cafe\Vcac-Config.exe.config です。

これらのオプション パラメータに値を指定して、SynchronizeDatabases コマンドのみに対して、デフォルトのタイムアウト値をオーバーライドすることができます。

| パラメータ | 短縮名 | 説明 |
|------------------------|-------|---|
| --DatabaseSyncTimeout | -dstm | SynchronizeDatabases に対してのみ HTTP 要求のタイムアウト値を秒単位で設定します。 |
| --DatabaseSyncPageSize | -dsps | 予約または予約ポリシーの同期に対してのみ、同期要求のページサイズを設定します。デフォルトは 10 です。 |

これらのパラメータが **Vcac-Config.exe.config** ファイルに設定されていない場合は、デフォルトのタイムアウト値が使用されます。

高可用性環境での IaaS のアップグレードが失敗する

プライマリ Web サーバ ノードでロード バランシングを有効にして IaaS アップグレード処理を実行すると失敗します。次のエラー メッセージが表示される可能性があります。「System.Net.WebException: 処理がタイムアウトしました」または「401 - Unauthorized: 無効な認証情報のため、アクセスは拒否されました。」

問題

ロード バランシングを有効にして IaaS をアップグレードすると、断続的に障害が発生する可能性があります。この場合、ロード バランシングを無効にして、再度 vRealize Automation アップグレードを実行する必要があります。

ソリューション

- 1 環境を更新前のスナップショットに戻します。
- 2 プライマリ IaaS Web サーバ ノードへのリモート デスクトップ接続を開きます。
- 3 C:\windows\system32\drivers\etc の Windows の hosts ファイルに移動します。
- 4 hosts ファイルを開き、Web サーバ ロード バランサをバイパスするように次の行を追加します。
<IP_address_of_primary_iaas_website_node vrealizeautomation_iaas_website_lb_fqdn>
例：
10.10.10.5 vra-iaas-web-lb.domain.com
- 5 hosts ファイルを保存して vRealize Automation の更新を再度実行します。
- 6 vRealize Automation の更新が完了したら、hosts ファイルを開いて、手順 4 で追加した行を削除します。

アップグレードの問題の回避

アップグレード プロセスを変更してアップグレードの問題を回避することができます。

ソリューション

vRealize Automation 環境のアップグレードで問題が発生した場合は、この手順を使用して、使用可能なフラグのいずれかを選択することによりアップグレード プロセスを変更します。

手順

- 1 プライマリ vRealize Automation アプライアンス ノードへのセキュアなシェル接続を開きます。

2 コマンド プロンプトで、以下のコマンドを実行してグル ファイルを作成します。

touch <available_flag>

例：**touch /tmp/disable-iaas-upgrade**

表 1-72. 使用可能なフラグ

| フラグ | 説明 |
|-----------------------------|--|
| /tmp/disable-iaas-upgrade | <ul style="list-style-type: none"> ■ 仮想アプライアンスの再起動後の IaaS アップグレード プロセスが実行されないようにします。 ■ 管理エージェントがアップグレードされないようにします。 ■ 自動の前提条件チェックおよび修正が実行されないようにします。 ■ IaaS サービスが停止しないようにします。 |
| /tmp/do-not-upgrade-ma | 管理エージェントがアップグレードされないようにします。このフラグは、管理エージェントを手動でアップグレードする場合に適しています。 |
| /tmp/skip-prereq-checks | 自動の前提条件チェックおよび修正が実行されないようにします。このフラグは、前提条件の自動修正に問題があるために手動で修正を適用した場合に適しています。 |
| /tmp/do-not-stop-services | IaaS サービスが停止しないようにします。アップグレードで、Manager Service、DEM、エージェントなどの IaaS Windows サービスを停止しません。 |
| /tmp/do-not-upgrade-servers | データベース、Web サイト、WAPI、リポジトリ、モデル Mfrontanager データ、Manager Service など、すべてのサーバ IaaS コンポーネントの自動アップグレードが実行されないようにします。 <small>注: また、このフラグは、Manager Service 自動フェイルオーバー モードが有効にされないようにします。</small> |
| /tmp/do-not-upgrade-dems | DEM がアップグレードされないようにします。 |
| /tmp/do-not-upgrade-agents | IaaS プロキシ エージェントがアップグレードされないようにします。 |

3 選択したフラグのタスクを実行します。

表 1-73. 追加のタスク

| フラグ | タスク |
|-----------------------------|---|
| /tmp/disable-iaas-upgrade | <ul style="list-style-type: none"> ■ 管理エージェントを手動でアップグレードします。 ■ 必要なすべての IaaS 前提条件を手動で適用します。 ■ IaaS サービスを手動で停止します。 <ol style="list-style-type: none"> a IaaS Windows サーバにログインします。 b [スタート] - [管理ツール] - [サービス] を選択します。 c 次の順序でサービスを停止します。 <p>注: IaaS Windows サーバはシャットダウンしないでください。</p> <ol style="list-style-type: none"> a 各 VMware vRealize Automation プロキシ エージェント。 b 各 VMware DEM ワーカー。 c VMware DEM orchestrator。 d VMware vCloud Automation Center サービス。 ■ 仮想アプライアンス アップグレードが完了した後、IaaS アップグレードを手動で開始します。 |
| /tmp/do-not-upgrade-ma | 管理エージェントを手動でアップグレードします。 |
| /tmp/skip-prereq-checks | 必要なすべての IaaS 前提条件を手動で適用します。 |
| /tmp/do-not-stop-services | <p>IaaS サービスを手動で停止します。</p> <ol style="list-style-type: none"> 1 IaaS Windows サーバにログインします。 2 [スタート] - [管理ツール] - [サービス] を選択します。 3 次の順序でサービスを停止します。 <p>注: IaaS Windows サーバはシャットダウンしないでください。</p> <ol style="list-style-type: none"> a 各 VMware vRealize Automation プロキシ エージェント。 b 各 VMware DEM ワーカー。 c VMware DEM orchestrator。 d VMware vCloud Automation Center サービス。 |
| /tmp/do-not-upgrade-servers | |
| /tmp/do-not-upgrade-dems | |
| /tmp/do-not-upgrade-agents | |

4 プライマリ vRealize Automation アプライアンス管理コンソールにアクセスして、プライマリ vRealize Automation アプライアンスをアップデートします。

注: 各フラグは削除されるまでアクティブなままになるため、アップグレード後は次のコマンド **rm /<flag_path>/<flag_name>** を実行して選択したフラグを削除してください。例：
rm /tmp/disable-iaas-upgrade

vRealize Automation 7.4 への移行

移行を使用すると、既存の vRealize Automation 環境から最新バージョンへのサイドバイサイド アップグレードを実行できます。

この情報は、vRealize Automation の 7.4 への、移行を使用したアップグレードに固有のものです。サポートされている他のアップグレードパスの詳細については、[「vRealize Automation のアップグレード」](#)を参照してください。

vRealize Automation の移行

移行を使用すると、既存の vRealize Automation 環境のサイドバイサイド アップグレードを実行できます。

移行は、現在の vRealize Automation の移行前の環境から vRealize Automation の最新バージョンのターゲット展開に、テナントと ID ストアを除くすべてのデータを移動します。さらに、移行によりすべてのデータが組み込みの vRealize Orchestrator 7.x から移行先の環境に移動します。

移行では、データを収集してそのデータをターゲット環境に安全にコピーするために必要な時間の間、vRealize Automation サービスを停止する以外に、移行前の環境を変更しません。ソース vRealize Automation データベースのサイズによって、移行は数分から数時間かかることがあります。

移行前の環境を最小インストールまたは高可用性展開に移行できます。

移行後にターゲット環境を本番環境にする場合は、移行前の環境を再開しないでください。移行後の移行前の環境への変更は、ターゲット環境と同期されません。

移行前の環境が vCloud Air または vCloud Director に統合されている場合、または物理的なエンドポイントがある場合は、移行を使用してアップグレードを実行する必要があります。移行により、これらのエンドポイントと、エンドポイントに関連付けられたすべてのものがターゲット環境から削除されます。また、移行により、ターゲット環境から 6.x VMware vRealize Application Services 統合も削除されます。

注: 移行前に、vRealize Automation 仮想マシンを準備する追加のタスクを完了する必要があります。移行前に、ナレッジベースの記事 [KB51531](#) を確認してください。

vRealize Automation 6.2.x から最新バージョンに移行する場合は、次の問題が発生する可能性があります。

| 問題 | 解決方法 |
|--|--|
| <p>vRealize Automation 6.2.x を最新バージョンに移行した後、以下のプロパティ定義を使用したカタログ アイテムはサービス カタログに表示されますが、申請できません。</p> <ul style="list-style-type: none"> ■ コントロール タイプ：チェック ボックスまたはリンク。 ■ 属性：関係、正規表現、またはプロパティのレイアウト。 <p>vRealize Automation 7.x では、プロパティ定義でこれらの要素が使用されなくなりました。</p> | <p>プロパティ定義を再作成するか、組み込みのコントロール タイプまたは属性ではなく vRealize Orchestrator スクリプト アクションを使用するようにプロパティ定義を設定する必要があります。詳細については、「移行後にサービス カタログに表示されるカタログ アイテムを申請できない」 を参照してください。</p> |
| <p>vRealize Automation 6.2.x のドロップ ダウン メニューで親子関係の定義に使用されていた正規表現は、バージョン 7.x ではサポートされていません。バージョン 6.2.x では、特定の親メニュー項目でのみ使用可能な 1 つ以上の子メニュー項目を定義するのに正規表現を使用できます。これらの子メニュー項目は、親メニュー項目を選択したときのみ表示されます。</p> <p>バージョン 7.x に移行すると、親ドロップ ダウン メニューでの選択とは無関係に、子ドロップダウン メニューにはすべての利用可能なメニュー項目が表示されます。以前に定義された動的な値が機能していないことを示すために、子ドロップダウン メニューの最初のメニュー項目には以下のメッセージが表示されます：警告: vRO ワークフローを使用して動的な値を定義してください。</p> | <p>移行後、以前の動的な値を復元するにはプロパティ定義を再作成する必要があります。親ドロップダウン メニューと子ドロップダウン メニューの間で親子関係を作成する方法の詳細については、How to use dynamic property definitions in vRA 7.2 を参照してください。</p> |

vRealize Automation 環境のユーザー インターフェイス

vRealize Automation 環境は、複数のインターフェイスで使用および管理します。

ユーザー インターフェイス

これらの表は、vRealize Automation 環境を管理するために使用するインターフェイスを示しています。

表 1-74. vRealize Automation 管理コンソール

| 目的 | アクセス | 必要な認証情報 |
|---|---|-------------------------------------|
| <p>以下のシステム管理者のタスクには、vRealize Automation コンソールを使用します。</p> <ul style="list-style-type: none"> ■ テナントを追加します。 ■ vRealize Automation ユーザー インターフェイスをカスタマイズします。 ■ メール サーバを構成します。 ■ イベント ログを表示します。 ■ vRealize Orchestrator を構成します。 | <ol style="list-style-type: none"> 1 ブラウザを起動し、仮想アプライアンスの完全修飾ドメイン名を使用して、vRealize Automation アプライアンスのブラッシュ ページを開きます。 https://<vra-virtual-hostname.domain.name> 2 [vRealize Automation コンソール] をクリックします。 vRealize Automation コンソールを開くには、次の URL を使用することもできます : https://<vra-virtual-hostname.domain.name>/vra 3 ログインします。 | <p>システム管理者ロールを持つユーザーである必要があります。</p> |

表 1-75. vRealize Automation テナント コンソール。このインターフェイスは、サービスやリソースの作成および管理に使用するプライマリ ユーザー インターフェイスです。

| 目的 | アクセス | 必要な認証情報 |
|---|---|---|
| <p>以下のタスクには、vRealize Automation を使用します。</p> <ul style="list-style-type: none"> ■ 新しい IT サービス ブループリントを申請します。 ■ クラウドおよび IT リソースを作成および管理します。 ■ カスタム グループを作成および管理します。 ■ ビジネス グループを作成、管理します。 ■ ユーザーにロールを割り当てます。 | <ol style="list-style-type: none"> 1 ブラウザを起動し、仮想アプライアンスの完全修飾ドメイン名とテナントの URL 名を使用して、テナントの URL を入力します。 https://<vra-va-hostname.domain.name>/vcac/org/<tenant_URL_name> 2 ログインします。 | <p>以下の 1 つ以上のロールを持つユーザーである必要があります。</p> <ul style="list-style-type: none"> ■ アプリケーション アーキテクト ■ 承認管理者 ■ カタログ管理者 ■ コンテナ管理者 ■ コンテナ アーキテクト ■ 健全性サービス ユーザー ■ インフラストラクチャ アーキテクト ■ セキュアなエクスポートの利用者 ■ ソフトウェア アーキテクト ■ テナント管理者 ■ XaaS アーキテクト |

表 1-76. vRealize Automation アプライアンス管理。このインターフェイスは、仮想アプライアンス管理インターフェイス (VAMI) と呼ばれます。

| 目的 | アクセス | 必要な認証情報 |
|---|--|--|
| <p>以下のタスクには vRealize Automation アプライアンス管理を使用します。</p> <ul style="list-style-type: none"> 登録されているサービスのステータスを表示します。 システム情報を表示、およびアプライアンスを再起動またはシャットダウンします。 カスタム エクスペリエンス改善プログラムへの参加を管理します。 ネットワーク ステータスを表示します。 更新ステータスを表示、およびアップデートをインストールします。 管理設定を管理します。 vRealize Automation ホスト設定を管理します。 SSO の設定を管理します。 製品ライセンスを管理します。 vRealize Automation Postgres データベースを設定します。 vRealize Automation メッセージングを設定します。 vRealize Automation ログを設定します。 IaaS コンポーネントをインストールします。 既存の vRealize Automation 環境から移行します。 IaaS コンポーネントの証明書を管理します。 Xenon サービスを設定します。 | <ol style="list-style-type: none"> ブラウザを起動し、仮想アプライアンスの完全修飾ドメイン名を使用して、vRealize Automation アプライアンスのブラッシュ ページを開きます。 https://<vra-va-hostname.domain.name> [vRealize Automation アプライアンス管理] をクリックします。 次の URL を使用して vRealize Automation アプライアンス管理を開くこともできます : https://<vra-va-hostname.domain.name:5480> ログインします。 | <ul style="list-style-type: none"> ユーザー名 : root パスワード : vRealize Automation アプライアンスを展開したときに 入力したパスワード。 |

表 1-77. vRealize Orchestrator クライアント

| 目的 | アクセス | 必要な認証情報 |
|---|--|--|
| <p>以下のタスクには、vRealize Orchestrator クライアントを使用します。</p> <ul style="list-style-type: none"> アクションを作成します。 ワークフローを作成します。 ポリシーを管理します。 パッケージをインストールします。 ユーザーおよびユーザー グループの権限を管理します。 URI オブジェクトにタグを追加します。 インベントリを表示します。 | <ol style="list-style-type: none"> ブラウザを起動し、仮想アプライアンスの完全修飾ドメイン名を使用して、vRealize Automation のブラッシュ ページを開きます。 https://<vra-va-hostname.domain.name> ローカル コンピュータに client.jnlp ファイルをダウンロードするには、[vRealize Orchestrator Client] をクリックします。 client.jnlp ファイルを右クリックして [起動] を選択します。 [続行しますか?] ダイアログボックスで、[続行] をクリックします。 ログインします。 | <p>システム管理者ロールを持つユーザーであるか、または vRealize Orchestrator コントロール センターの認証プロバイダの設定で構成されている vcoadmins グループに属している必要があります。</p> |

表 1-78. vRealize Orchestrator コントロール センター

| 目的 | アクセス | 必要な認証情報 |
|---|---|---|
| vRealize Automation に組み込まれているデフォルトの vRealize Orchestrator インスタンスの設定を編集するには、vRealize Orchestrator コントロール センターを使用します。 | <ol style="list-style-type: none"> 1 ブラウザを起動し、仮想アプライアンスの完全修飾ドメイン名を使用して、vRealize Automation アプライアンスのスプラッシュ ページを開きます。 https://<vra-virtual-hostname.domain.name> 2 [vRealize Automation アプライアンス管理] をクリックします。 次の URL を使用して vRealize Automation アプライアンス管理を開くこともできます : https://<vra-virtual-hostname.domain.name:5480> 3 ログインします。 4 [vRA 設定] - [Orchestrator] の順にクリックします。 5 [Orchestrator ユーザー インターフェイス] を選択します。 6 [開始] をクリックします。 7 Orchestrator ユーザー インターフェイスの URL をクリックします。 8 ログインします。 | <p>ユーザー名</p> <ul style="list-style-type: none"> ■ ロールベースの認証が設定されていない場合は、root と入力します。 ■ ロールベースの認証で設定されている場合は、vRealize Automation ユーザー名を入力します。 <p>パスワード</p> <ul style="list-style-type: none"> ■ ロールベースの認証が設定されていない場合、vRealize Automation アプライアンスを展開したときに入力したパスワードを入力します。 ■ ロールベースの認証でユーザー名が設定されている場合は、ユーザー名に対するパスワードを入力します。 |

表 1-79. Linux コマンド プロンプト

| 目的 | アクセス | 必要な認証情報 |
|--|---|---|
| <p>vRealize Automation アプライアンス ホストなどのホストでは、以下のタスクには Linux コマンド プロンプトを使用します。</p> <ul style="list-style-type: none"> ■ サービスの開始または停止 ■ 構成ファイルの編集 ■ コマンドの実行 ■ データの取得 | <ol style="list-style-type: none"> 1 vRealize Automation アプライアンス ホストで、コマンド プロンプトを開きます。 ローカル コンピュータでコマンド プロンプトを開く方法の 1 つは、PuTTY などのアプリケーションを使用して、ホストでセッションを開始することです。 2 ログインします。 | <ul style="list-style-type: none"> ■ ユーザー名 : root ■ パスワード : vRealize Automation アプライアンスを展開したときに作成したパスワード。 |

表 1-80. Windows コマンド プロンプト

| 目的 | アクセス | 必要な認証情報 |
|---|--|--|
| laaS ホストなどのホスト上で、Windows コマンド プロンプトを使用してスクリプトを実行できます。 | <ol style="list-style-type: none"> 1 laaS ホスト上で、Windows にログインします。 ローカル コンピュータからログインする方法の 1 つは、リモート デスクトップ セッションを開始することです。 2 Windows コマンド プロンプトを開きます。 コマンド プロンプトを開く方法の 1 つは、ホスト上で [スタート] アイコンを右クリックし、[コマンド プロンプト] または [コマンド プロンプト (管理者)] を選択することです。 | <ul style="list-style-type: none"> ■ ユーザー名 : 管理者権限を持つユーザー。 ■ パスワード : ユーザーのパスワード。 |

移行の前提条件

移行の前提条件はターゲット環境によって異なります。

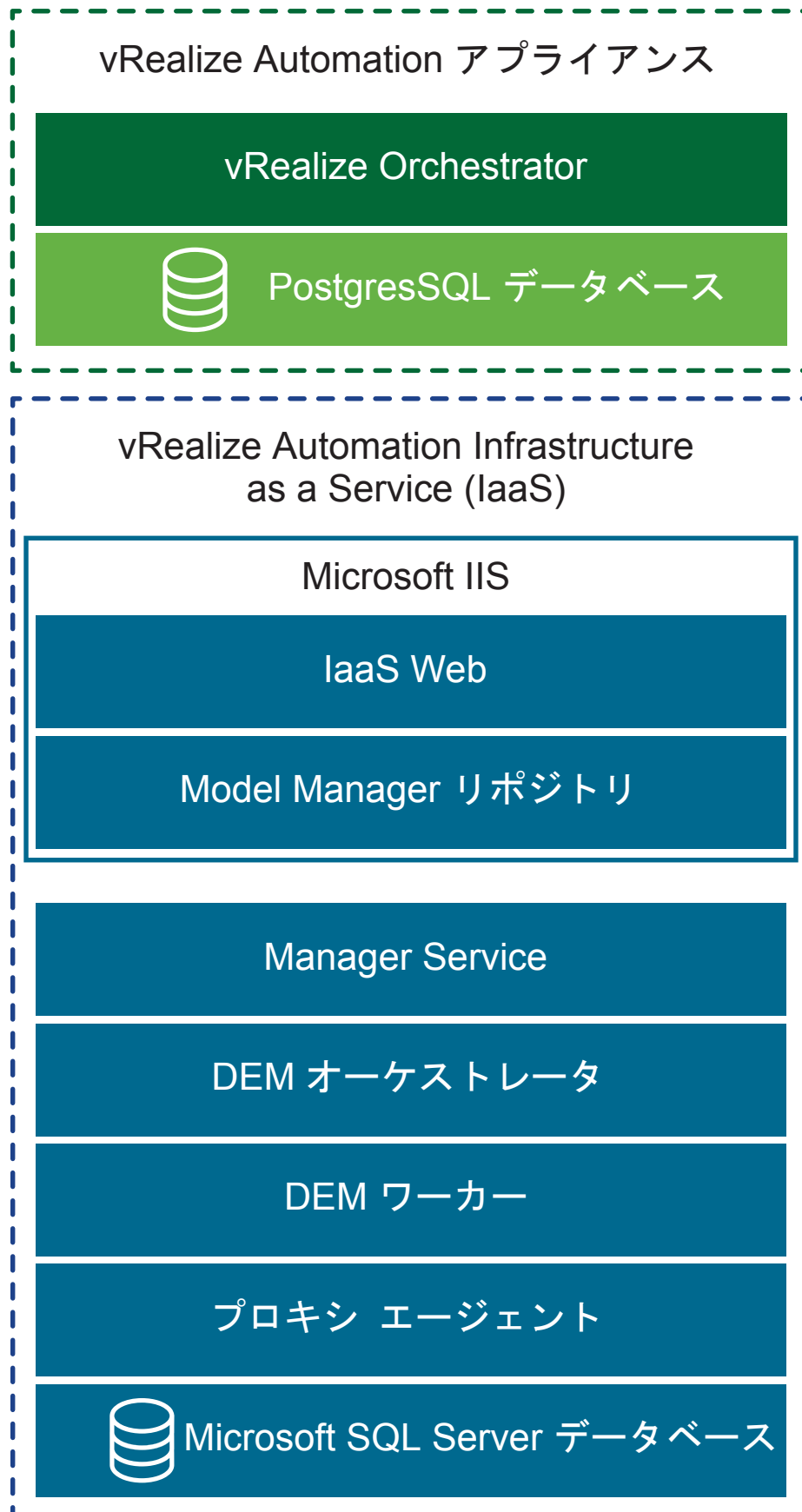
最小環境または高可用性環境に移行することができます。

最小環境に移行するための前提条件

最小環境への移行が確実に成功するように、次の前提条件を確認します。

最小インストールには、1 台の vRealize Automation アプライアンス、および IaaS コンポーネントをホストする 1 台の Windows サーバが含まれます。最小インストールでは、vRealize Automation SQL Server データベースを IaaS コンポーネントと同じ IaaS Windows サーバに置くことも、別の Windows サーバに置くこともできます。

図 1-17. vRealize Automation 最小インストール



前提条件

- vRealize Automation の新しいターゲット環境があることを確認します。
- 次の要件に基づいて、適切なプロキシ エージェントをターゲット環境にインストールします。
 - ターゲット プロキシ エージェント名は、vSphere 用、Hyper-V 用、Citrix XenServer 用、およびテスト用の各プロキシ エージェントのソース プロキシ エージェント名と一致する必要があります。

注: 次の手順を実行してエージェント名を取得します。

- 1 IaaS ホストで、**管理者権限**を持つローカル ユーザーとして Windows にログインします。
 - 2 Windows Explorer を使用して、エージェントのインストール ディレクトリに移動します。
 - 3 **VRMAgent.exe.config** ファイルを開きます。
 - 4 ServiceConfiguration タグで、agentName 属性の値を特定します。
-

- ナレッジベースの記事 [KB51531](#) を確認します。
- ターゲット プロキシ エージェント エンドポイント名は、vSphere 用、Hyper-V 用、Citrix XenServer 用、およびテスト用の各プロキシ エージェントのソース プロキシ エージェント エンドポイント名と一致する必要があります。
- ターゲット環境で vSphere 用、Hyper-V 用、Citrix XenServer 用、またはテスト用の各プロキシ エージェントのエンドポイントを作成しないでください。
- ターゲット vRealize Automation アプライアンスの vRealize Automation コンポーネントのバージョン番号を確認します。
 - a ターゲット vRealize Automation アプライアンスを展開したときに入力したパスワードを使用して、**root** としてターゲット vRealize Automation アプライアンス管理にログインします。
 - b [vRA 設定] - [クラスタ] の順に選択します。
 - c 三角形をクリックして、[ホスト/ノード名] のレコードを展開します。

vRealize Automation IaaS コンポーネントのバージョン番号が一致していることを確認します。
- vRealize Automation ターゲット IaaS データベース用のターゲット Microsoft SQL Server のバージョンが 2012、2014、または 2016 であることを確認します。
- ポート 22 がソースとターゲットの vRealize Automation 環境間で開いていることを確認します。ポート 22 は、ソースとターゲットの仮想アプライアンス間のセキュア シェル (SSH) 接続を確立するために必要です。
- エンドポイント vCenter に、移行を完了するための十分なリソースがあることを確認します。
- Cafe と IaaS コンポーネントの間で、ターゲット vRealize Automation 環境のシステム時刻が同期していることを確認します。
- ターゲット環境の IaaS サーバ ノードに Java SE Runtime Environment (JRE) 8 Update 161 (64 ビット) 以降がインストールされていることを確認します。JRE をインストールしたら、JAVA_HOME 環境変数が、各 IaaS ノードにインストールされた Java バージョンをポイントしていることを確認します。必要に応じて、パスを変更します。

- IaaS の各ノードに PowerShell 3.0 以降がインストールされていることを確認します。
- ソースおよびターゲットの vRealize Automation 環境が稼動していることを確認します。
- ソース vRealize Automation 環境で、ユーザー アクティビティやプロビジョニング アクティビティが発生していないことを確認します。
- オペレーティング システムと通信する可能性のあるターゲット vRealize Automation 環境の IaaS ノードで、ウイルス対策またはセキュリティ ソフトウェアが実行されていること、およびコンポーネントが適切に設定、または無効にされていることを確認します。
- Windows インストールの更新が保留中であるため、IaaS Web サービスおよび Model Manager を再起動する必要がないことを確認します。更新が保留中であるため、移行で World Wide Web 発行サービスが開始または終了されない場合があります。

次のステップ

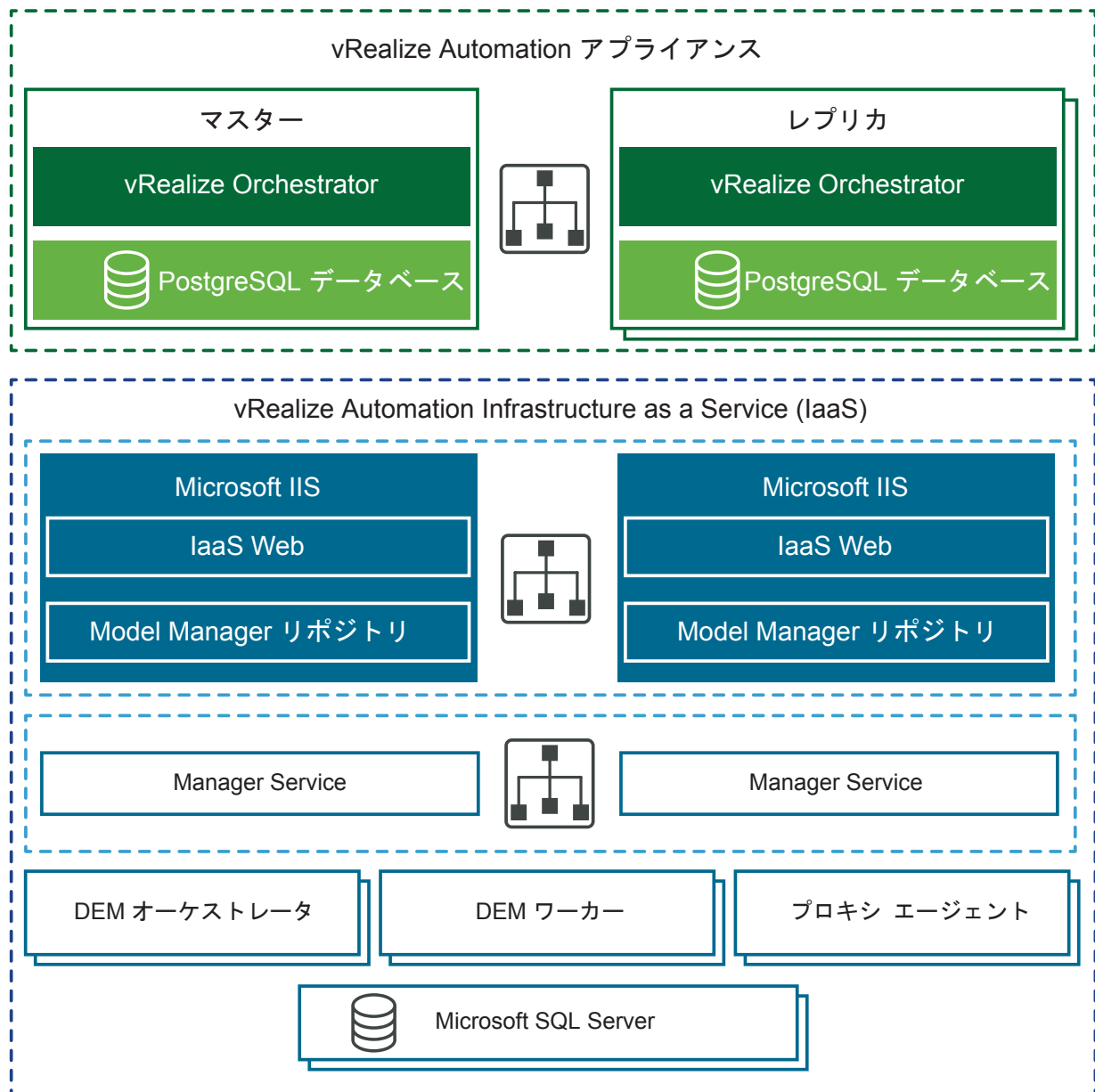
[「移行前のタスク」](#)。

高可用性環境に移行するための前提条件

次の前提条件を確認し、高可用性環境に問題なく確実に移行できるようにします。

高可用性環境には、さまざまなサイズを使用できます。基本的な分散展開では、各 Windows サーバ上で IaaS コンポーネントをホストするだけで vRealize Automation のパフォーマンスを向上させることができます。多くの場合、高可用性環境では、より多くの容量を確保するために、冗長アプライアンス、冗長サーバ、ロード バランシングが使用されます。大規模な分散展開では、優れたスケーラビリティ、高可用性、ディザスタ リカバリが可能になります。

図 1-18. vRealize Automation 高可用性環境



前提条件

- 高可用性向けに構成されたマスターおよびレプリカ仮想アプライアンスでターゲット vRealize Automation が新しくインストールされていることを確認します。[vRealize Automation 高可用性構成の考慮事項](#)を参照してください。
- すべての vRealize Automation 仮想アプライアンスが root ユーザーの同一のパスワードを使用していることを確認します。
- 次の要件に基づいて、適切なプロキシ エージェントをターゲット環境にインストールします。
 - ターゲット プロキシ エージェント名は、vSphere 用、Hyper-V 用、Citrix XenServer 用、およびテスト用の各プロキシ エージェントのソース プロキシ エージェント名と一致する必要があります。

注: 次の手順を実行してエージェント名を取得します。

- 1 IaaS ホストで、**管理者**権限を持つローカル ユーザーとして Windows にログインします。
 - 2 Windows Explorer を使用して、エージェントのインストール ディレクトリに移動します。
 - 3 **VRMAgent.exe.config** ファイルを開きます。
 - 4 ServiceConfiguration タグで、agentName 属性の値を特定します。
-

- ターゲット プロキシ エージェント エンドポイント名は、vSphere 用、Hyper-V 用、Citrix XenServer 用、およびテスト用の各プロキシ エージェントのソース プロキシ エージェント エンドポイント名と一致する必要があります。
- ターゲット環境で vSphere 用、Hyper-V 用、Citrix XenServer 用、またはテスト用の各プロキシ エージェントのエンドポイントを作成しないでください。
- ターゲット vRealize Automation アプライアンスの vRealize Automation コンポーネントのバージョン番号を確認します。
 - a ターゲット vRealize Automation 7.3 環境で、ブラウザを起動し、**https:// vra-va-hostname.domain.name:5480** にある vRealize Automation アプライアンス管理コンソールにアクセスします。
 - b ユーザー名 root と、アプライアンスの展開時に入力したパスワードを使用してログインします。
 - c [vRA 設定] - [クラスタ] の順に選択します。
 - d [ホスト/ノード名] のレコードを展開してコンポーネントを表示するために、展開ボタンをクリックします。

すべての仮想アプライアンス ノード間で vRealize Automation コンポーネントのバージョン番号が一致していることを確認します。

すべての IaaS ノード間で vRealize Automation IaaS コンポーネントのバージョン番号が一致していることを確認します。
- ナレッジベースの記事 [KB51531](#) を確認します。
- トラフィックをマスター ノードのみに転送するために、次の手順を実行します。
 - a すべての冗長ノードを無効にします。

- b ロード バランサのドキュメントのとおり、次のアイテムの健全性モニタを削除します。
 - vRealize Automation 仮想アプライアンス
 - IaaS Web サイト
 - IaaS Manager Service
- vRealize Automation ターゲット IaaS データベース用のターゲット Microsoft SQL Server のバージョンが 2012、2014、または 2016 であることを確認します。
- ポート 22 がソースとターゲットの vRealize Automation 環境間で開いていることを確認します。ポート 22 は、ソースとターゲットの仮想アプライアンス間のセキュア シェル (SSH) 接続を確立するために必要です。
- エンドポイント vCenter に、移行を完了するための十分なリソースがあることを確認します。
- ロード バランサのタイムアウト設定を、デフォルト設定から 10 分以上に変更したことを確認します。
- Cafe と IaaS コンポーネントの間で、ターゲット vRealize Automation 環境のシステム時刻が同期していることを確認します。
- ターゲット環境の IaaS Web サービス ノードと Model Manager ノードに適切な Java Runtime Environment があることを確認します。Java SE Runtime Environment (JRE) 8 Update 161 (64 ビット) 以降がインストールされている必要があります。JAVA_HOME システム変数が IaaS の各ノードにインストールされている Java のバージョンを指していることを確認します。必要に応じて、パスを変更します。
- 各 IaaS ノードに PowerShell 3.0 以降がインストールされていることを確認します。
- ソースおよびターゲットの vRealize Automation 環境が稼動していることを確認します。
- ソース vRealize Automation 環境で、ユーザー アクティビティやプロビジョニング アクティビティが発生していないことを確認します。
- オペレーティング システムと通信する可能性のあるターゲット vRealize Automation 環境の IaaS ノードで、ウイルス対策またはセキュリティ ソフトウェアが実行されていること、およびコンポーネントが適切に設定、または無効にされていることを確認します。
- Windows インストールの更新が保留中であるため、IaaS Web サービスおよび Model Manager を再起動する必要がないことを確認します。更新が保留中であるため、移行で World Wide Web 発行サービスが開始または終了されない場合があります。

次のステップ

[「移行前のタスク」](#)。

移行前のタスク

移行する前に、いくつかの移行前のタスクを実行する必要があります。

ソース vRealize Automation 環境のデータからターゲット vRealize Automation 環境に移行する前に実行する移行前タスクは、移行前の環境に応じて異なります。

vRealize Automation 6.2.x から 7.x への移行で導入される変更の確認

vRealize Automation 7 以降では、アップグレード プロセスの間、およびプロセス後にさまざまな機能が変更されます。vRealize Automation 6.2.x 環境を最新バージョンにアップグレードする前に、これらの変更を確認する必要があります。

vRealize Automation 6.2.x と 7.x の違いについては、『Upgrading vRealize Automation 6.2.5 to 7.4』の [Considerations About Upgrading to This vRealize Automation Version](#) を参照してください。

注: vRealize Production Test Upgrade Assist Tool は、vRealize Automation 6.2.x 環境を分析してアップグレードに関する問題を引き起こす可能性がある機能構成を特定し、使用環境のアップグレード準備ができていることを確認します。このツールおよび関連ドキュメントをダウンロードするには、[VMware vRealize Production Test Tool](#) の製品のダウンロード ページに移動します。

vRealize Automation 6.2.x を最新バージョンに移行した後、以下のプロパティ定義を使用したカタログ アイテムは サービス カタログに表示されますが、申請できません。

- コントロール タイプ：チェック ボックスまたはリンク。
- 属性：関係、正規表現、またはプロパティのレイアウト。

vRealize Automation 7.x では、プロパティ定義でこれらの要素が使用されなくなりました。プロパティ定義を再作成するか、組み込みのコントロール タイプまたは属性以外の vRealize Orchestrator スクリプト アクションを使用するようにプロパティ定義を構成する必要があります。詳細については、『[移行後にサービス カタログに表示されるカタログ アイテムを申請できない](#)』を参照してください。

ソフトウェア エージェント パッチの適用

vRealize Automation 7.1 または 7.3 から 7.4 へ移行する前に、ソース アプライアンスにホット フィックスを適用して、ソフトウェア エージェントを TLS 1.2 にアップグレードできるようにする必要があります。

トランスポート レイヤー セキュリティ (TLS) プロトコルは、ブラウザと vRealize Automation 間のデータの整合性を確保します。このホット フィックスにより、移行前の環境のソフトウェア エージェントを TLS 1.2 にアップグレードできます。このアップグレードでは最高レベルのセキュリティが確保され、vRealize Automation 7.1 または 7.3 では必須です。各バージョンには独自のホット フィックスがあります。

前提条件

移行元となる実行中の vRealize Automation 7.1 または 7.3 の環境。

手順

- ◆ 7.4 に移行する前に、移行元の vRealize Automation 7.1 または 7.3 アプライアンスにこのホット フィックスを適用します。[ナレッジベースの記事 KB52897](#) を参照してください。

次のステップ

[\[vSphere エージェントでの DoDeletes 設定の False への変更\]](#)。

vSphere エージェントでの DoDeletes 設定の False への変更

vRealize Automation 6.2.x 環境から移行する場合、移行前にターゲットの vSphere エージェントで DoDeletes 値を **true** から **false** に変更する必要があります。

前提条件

移行の前提条件を完成させます。

手順

- 1 DoDeletes 値を **false** に変更します。

これにより、ソース環境から仮想マシンが削除されるのを回避します。ソース環境とターゲット環境は並行して実行されます。本番環境での移行が検証された後、リースの不一致が発生する可能性があります。

- 2 本番環境での移行が検証され、ソース環境がシャットダウンされた後、DoDeletes 値を **true** に設定します。

- 3 DoDeletes を **false** に設定するには、[vSphere エージェントの構成](#)に記載されている手順を実行してください。

次のステップ

[\[vRealize Automation 仮想マシンの移行準備\]](#)。

vRealize Automation 6.x 移行前環境のテンプレートの確認

vRealize Automation 6.x から 7.4 に移行する前に、すべてのテンプレートに少なくとも 4 MB の最小メモリ設定があることを確認するために仮想マシン テンプレートを確認する必要があります。

vRealize Automation 6.x 移行前環境にメモリが 4 MB 未満の仮想マシン テンプレートがあると、移行は失敗します。6.x の移行前環境のブループリントに 4 MB 未満のメモリがあるかどうかを判断するには、この手順を完了します。

前提条件

vRealize Automation 6.x から 7.4 に移行しています。

手順

- 1 SSH を使用して、プライマリ vRealize Automation アプライアンスに **root** としてログインします。

vRealize Orchestrator が外部の場合、Orchestrator ホスト マシンにログインします。

- 2 プライマリ ホスト上の PostgreSQL データ フォルダ (/var/vmware/vpostgres/current/pgdata/) にディレクトリを変更します。

- 3 次のスクリプトを実行して、すべてのブループリントで 4 MB 未満に指定されているメモリがあるかどうかを確認します。

```
select * from [vCAC].[dbo].[VirtualMachineTemplate] where IsHidden = 0 and
MemoryMB < 4;
```

vCAC はデータベース名です。

- 4 スクリプトで 4 MB 未満に指定されているメモリがあるブループリントが検出された場合は、次のスクリプトを実行してメモリを 4 MB 以上に更新します。

```
update [vCAC].[dbo].[VirtualMachineTemplate] set MemoryMB = 4 where
IsHidden = 0 and MemoryMB < 4;
```

vCAC はデータベース名です。

次のステップ

[[vRealize Automation 仮想マシンの移行準備](#)].

vRealize Automation 仮想マシンの移行準備

vRealize Automation 6.2.x 仮想マシンの移行に関する既知の問題により、移行後に問題が発生する場合があります。

ナレッジベースの記事 [KB000051531](#) を 移行前に参照して、関連する修正を環境で実行する必要があります。

次のステップ

[[移行に必要な情報の収集](#)].

移行に必要な情報の収集

以下のテーブルを使用して、移行前の環境からターゲット環境への移行に必要な情報を記録します。

前提条件

移行の前提条件の検証を完了します。

- [[最小環境に移行するための前提条件](#)].
- [[高可用性環境に移行するための前提条件](#)].

表 1-81. ソース vRealize Automation アプライアンス

| オプション | 説明 | 値 |
|------------|--|---|
| ホスト名 | ソース vRealize Automation アプライアンス管理にログインします。[システム] タブでホスト名を見つけます。ホスト名は、完全修飾ドメイン名 (FQDN) を使用する必要があります。 | |
| root ユーザー名 | root | |
| root パスワード | ソース vRealize Automation アプライアンスを展開したときに入力した root パスワード。 | |
| 移行パッケージの場所 | 移行パッケージが作成された、移行元の vRealize Automation 6.2.x または 7.x アプライアンス上の既存のディレクトリへのパス。ディレクトリは、vRealize Automation データベースのサイズの 2 倍の容量が使用できる必要があります。デフォルトの場所は、 <code>/storage</code> です。 | |

表 1-82. ターゲット vRealize Automation アプライアンス

| オプション | 説明 | 値 |
|------------|--|---|
| root ユーザー名 | root | |
| root パスワード | ターゲット vRealize Automation アプライアンスを展開したときに入力した root パスワード。 | |
| デフォルトのテナント | vsphere.local | |
| 管理者ユーザー名 | 管理者 | |
| 管理者パスワード | ターゲット vRealize Automation 環境を展開したときに入力した administrator@vsphere.local ユーザーのパスワード。 | |

表 1-83. ターゲット IaaS データベース

| オプション | 説明 | 値 |
|------------------|--|---|
| データベース サーバ | クローン作成されたデータベースが配置される Microsoft SQL Server インスタンスの場所。名前付きインスタンスでデフォルト以外のポートが使用されている場合は、「SERVER,PORT\INSTANCE-NAME」という形式で指定します。 | |
| クローン作成されたデータベース名 | 移行のためにクローン作成されたソース vRealize Automation 6.2.x/7.x IaaS Microsoft SQL データベースの名前。 | |
| 認証モード | Windows または SQL Server のいずれかを選択します。[SQL Server] を選択する場合は、ログイン名とパスワードを入力する必要があります。 | |
| ログイン名 | クローン作成された IaaS Microsoft SQL データベースの db_owner ロールを持つ SQL Server ユーザーのログイン名。 | |
| パスワード | SQL Server ユーザーのパスワード。 | |
| 元の暗号化キー | 移行前の環境から取得する元の暗号化キー。 「ソース vRealize Automation 環境からの暗号化キーの取得」 を参照してください。 | |
| 新しいパスフレーズ | 新しい暗号化キーを生成するために使用する一連の単語。このパスフレーズは、ターゲット vRealize Automation 環境に新しい IaaS コンポーネントをインストールするときに使用します。 | |

次のステップ

[「ソース vRealize Automation 環境からの暗号化キーの取得」](#)。

ソース vRealize Automation 環境からの暗号化キーの取得

移行手順の一環として、ソース vRealize Automation 環境の暗号化キーを入力する必要があります。

前提条件

移行前の環境内のアクティブな Manager Service ホスト仮想マシンに対して、管理者権限があることを確認します。

手順

- 1 移行前の環境内のアクティブな Manager Service をホストする仮想マシン上で、管理者としてコマンド プロンプトを開き、次のコマンドを実行します。

```
"C:\Program Files
(x86)\VMware\VCAC\Server\ConfigTool\EncryptionKeyTool\DynamicOps.Tools.EncryptionKeyTool.exe" key-read -c "C:\Program Files
(x86)\VMware\VCAC\Server\ManagerService.exe.config" -v
```

インストール ディレクトリがデフォルトの場所 (C:\Program Files (x86)\VMware\VCAC) にない場合は、パスを編集して、実際のインストール ディレクトリを表示します。

2 コマンドを実行して表示されるキーを保存します。

キーは次の例のような長い文字列です。

NRH+f/BlnCB6yvasLS3sxespdkcFWAEuyV0g4lfryg=。

次のステップ

- vRealize Automation 6.2.x 環境から移行する場合は、[「vRealize Automation の移行前の環境からターゲット環境への各テナントの追加」](#)。
- vRealize Automation 7.x 環境から移行する場合は、[「ソース vRealize Automation 6.2.x 環境からテナントと IaaS 管理者のリスト作成」](#)。

ソース vRealize Automation 6.2.x 環境からテナントと IaaS 管理者のリスト作成

vRealize Automation 6.2.x 環境を移行する前に、テナントと各テナントの IaaS 管理者のリストを作成する必要があります。

ソース vRealize Automation コンソールで、テナントごとに次の手順を実行します。

注: vRealize Automation 7.x 環境から移行する場合は、この手順を実行する必要はありません。

前提条件

ソース vRealize Automation アプライアンスを展開したときに入力したパスワードを使用して、**管理者**としてソース vRealize Automation コンソールにログインします。

注: 高可用性環境の場合は、ソース仮想アプライアンスのロード バランサの完全修飾ドメイン名 (<https://<vra-vault-hostname.domain.name>/vcac>) を使用して、コンソールを開きます。

手順

- 1 [管理] - [テナント] を選択します。
- 2 テナント名をクリックします。
- 3 [管理者] をクリックします。
- 4 各テナントと IaaS 管理者のユーザー名のリストを作成します。
- 5 [キャンセル] をクリックします。

次のステップ

[「vRealize Automation の移行前の環境からターゲット環境への各テナントの追加」](#)。

vRealize Automation の移行前の環境からターゲット環境への各テナントの追加

ターゲット環境にテナントを追加するには、移行前の環境での各テナントの名前を使用する必要があります。

移行が正常に実行されるためには、移行前の環境の各テナントがターゲット環境に作成されることが必要です。また、移行前の環境のテナント URL 名を使用して追加する各テナントに、固有のアクセス URL を使用することも必要です。移行前の環境に未使用のテナントがあり、それを移行しない場合は、移行する前に移行元の環境から削除します。

注: 移行の検証により、少なくとも、前提条件の要求どおりに移行元で設定されているのと同じだけのテナントが、移行先のシステムにあることが確認されます。テナント名ではなくテナント URL 名に基づいて、大文字と小文字を区別してテナントが比較されます。

移行前の環境の各テナントに対してこの手順を実行します。

- vRealize Automation 6.2.x 環境から移行する場合は、移行前の環境からターゲット環境の VMware Identity Manager に既存の SSO2 テナントおよび ID ストアを移行します。
- vRealize Automation 7.x 環境から移行する場合は、移行前の環境からターゲット環境の VMware Identity Manager に既存の VMware Identity Manager テナントおよび ID ストアを移行します。

前提条件

- [「移行に必要な情報の収集」](#)。
- ターゲット vRealize Automation アプライアンスを展開したときに入力したパスワードを使用して、**管理者**としてターゲット vRealize Automation コンソールにログインします。

注: 高可用性環境の場合は、ターゲット仮想アプライアンス ロード バランサの完全修飾ドメイン名 `https://<vra-vb-lb-hostname.domain.name>/vcac` を使用してコンソールを開きます。

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、移行前の環境のテナント名と一致するテナント名を入力します。
たとえば、移行前の環境のテナント名が DEVTenant の場合は、**DEVTenant** と入力します。
- 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 [URL 名] テキスト ボックスに、移行前の環境のテナント URL 名と一致するテナント URL 名を入力します。
この URL 名は、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、移行前の環境の DEVTenant の URL 名が dev の場合は、**dev** と入力して `https://<vra-vb-lb-hostname.domain.name>/vcac/org/dev` という URL を作成します。
- 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。

次のステップ

[「追加された各テナントの管理者の作成」](#)。

追加された各テナントの管理者の作成

ターゲット環境に追加したテナントごとに、管理者を作成する必要があります。管理者を作成するには、ローカル ユーザー アカウントを作成し、そのアカウントにテナント管理者権限を割り当てます。

ターゲット環境の各テナントに対してこの手順を実行します。

前提条件

- [「vRealize Automation の移行前の環境からターゲット環境への各テナントの追加」](#)。
- ターゲット vRealize Automation アプライアンスを展開したときに入力したパスワードを使用して、**管理者**としてターゲット vRealize Automation コンソールにログインします。

注: 高可用性環境の場合は、ターゲット仮想アプライアンス ロード バランサの完全修飾ドメイン名 `https://<vra-va-lb-hostname.domain.name>/vcac` を使用してコンソールを開きます。

手順

- 1 [管理] - [テナント] を選択します。
- 2 追加したテナントをクリックします。
たとえば、DEVTenant の場合は、[DEVTenant] をクリックします。
- 3 [ローカル ユーザー] をクリックします。
- 4 [新規] アイコン (+) をクリックします。
- 5 [ユーザー詳細] で、必要な情報を入力して、テナント管理者ロールを割り当てるローカル ユーザー アカウントを作成します。
ローカル ユーザー名は、デフォルトのローカル ディレクトリ (vsphere.local) で一意である必要があります。
- 6 [OK] をクリックします。
- 7 [管理者] をクリックします。
- 8 [テナント管理者] 検索ボックスにローカル ユーザー名を入力し、Enter を押します。
- 9 検索の結果から適切な名前をクリックして、テナント管理者のリストにユーザーを追加します。
- 10 [完了] をクリックします。
- 11 コンソールからログアウトします。

次のステップ

- 最小インストールの場合：「[最小環境への移行前に Active Directory リンクのユーザーとグループを同期する](#)」
- 高可用性展開の場合：「[高可用性環境への移行前に Active Directory リンクのユーザーとグループを同期する](#)」

最小環境への移行前に Active Directory リンクのユーザーとグループを同期する

vRealize Automation の最小インストールにユーザーおよびグループをインポートするには、移行先の vRealize Automation を Active Directory リンクに接続する必要があります。

テナントごとに次の手順を実行します。テナントに複数の Active Directory がある場合は、テナントが使用する Active Directory ごとにこの手順を実行します。

前提条件

- 「追加された各テナントの管理者の作成」。
- Active Directory へのアクセス権限があることを確認します。
- テナント 管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [ディレクトリ管理] - [ディレクトリ] の順に選択します。
- 2 [ディレクトリを追加] アイコン (+) をクリックし、[Active Directory over LDAP/IWA の追加] を選択します。
- 3 Active Directory のアカウント設定を入力します。

◆ ネイティブ以外の Active Directory 用

| オプション | 入力例 |
|------------------------------------|---|
| ディレクトリ名 | 一意のディレクトリ名を入力します。 ネイティブ以外の Active Directory を使用する場合は、[LDAP 経由の Active Directory] を選択します。 |
| このディレクトリは DNS サービス ローケーションをサポートします | このオプションは選択解除します。 |
| 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=rainpole,dc=local] と入力します。 |
| バインド DN | 共通名 (CN) など、ユーザーを検索する権限がある Active Directory ユーザー アカウントの完全識別名 (DN) を入力します。 たとえば、[cn=config_admin infra,cn=users,dc=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、[接続をテスト] をクリックして構成したディレクトリへの接続をテストします。 |

◆ ネイティブの Active Directory 用

| オプション | 入力例 |
|---------------|--|
| ディレクトリ名 | 一意のディレクトリ名を入力します。 ネイティブの Active Directory を使用する場合は、[Active Directory (統合 Windows 認証)] を選択します。 |
| ドメイン名 | 参加するドメインの名前を入力します。 |
| ドメイン管理者ユーザー名 | ドメイン管理者のユーザー名を入力します。 |
| ドメイン管理者パスワード | ドメイン管理者のパスワードを入力します。 |
| バインド ユーザー UPN | メール アドレス形式を使用して、ドメインで認証できるユーザーの名前を入力します。 |
| 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 バインド アカウント パスワードを入力します。 |

- 4 [保存して次へ] をクリックします。

[ドメインの選択] にドメインのリストが表示されます。

- 5 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。
- 6 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。
- 7 同期するグループおよびユーザーを選択します。
 - a [新規] 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、**dc=vcac,dc=local** と入力します。
 - c 同期するグループを選択するには、[選択] をクリックし、[次へ] をクリックします。
 - d [ユーザーの選択] で、同期するユーザーを選択し、[次へ] をクリックします。
vRealize Automation の使用を必要とするユーザーおよびグループのみを追加します。[ネストされたグループの同期] は、ネスト内のすべてのグループが vRealize Automation の使用を必要とする場合以外には、選択しないでください。
- 8 ディレクトリと同期しているユーザーおよびグループを確認し、[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に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ます。

次のステップ

[\[ソース vRealize Automation 環境での NSX ネットワークおよびセキュリティ インベントリ データ収集の実行\]](#)

高可用性環境への移行前に Active Directory リンクのユーザーとグループを同期する

高可用性の vRealize Automation 環境にユーザーおよびグループをインポートするには、Active Directory リンクに接続する必要があります。

- 各テナントに対して手順 1 ～ 8 を実行します。テナントに複数の Active Directory がある場合は、テナントが使用する Active Directory ごとにこの手順を実行します。
- テナントに関連付けられている ID プロバイダごとに、手順 9 と 10 を繰り返します。

前提条件

- [\[追加された各テナントの管理者の作成\]](#)。
- Active Directory へのアクセス権限があることを確認します。
- テナント管理者として vRealize Automation にログインします。

手順

- 1 [管理] - [ディレクトリ管理] - [ディレクトリ] の順に選択します。
- 2 [ディレクトリを追加] アイコン (+) をクリックし、[Active Directory over LDAP/IWA の追加] を選択します。

3 Active Directory のアカウント設定を入力します。

◆ ネイティブ以外の Active Directory 用

| オプション | 入力例 |
|------------------------------------|---|
| ディレクトリ名 | 一意のディレクトリ名を入力します。 ネイティブ以外の Active Directory を使用する場合は、[LDAP 経由の Active Directory] を選択します。 |
| このディレクトリは DNS サービス ローケーションをサポートします | このオプションは選択解除します。 |
| 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=rainpole,dc=local] と入力します。 |
| バインド DN | 共通名 (CN) など、ユーザーを検索する権限がある Active Directory ユーザー アカウントの完全識別名 (DN) を入力します。 たとえば、[cn=config_admin infra,cn=users,dc=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、[接続をテスト] をクリックして構成したディレクトリへの接続をテストします。 |

◆ ネイティブの Active Directory 用

| オプション | 入力例 |
|---------------|--|
| ディレクトリ名 | 一意のディレクトリ名を入力します。 ネイティブの Active Directory を使用する場合は、[Active Directory (統合 Windows 認証)] を選択します。 |
| ドメイン名 | 参加するドメインの名前を入力します。 |
| ドメイン管理者ユーザー名 | ドメイン管理者のユーザー名を入力します。 |
| ドメイン管理者パスワード | ドメイン管理者アカウントのパスワードを入力します。 |
| バインド ユーザー UPN | メール アドレス形式を使用して、ドメインで認証できるユーザーの名前を入力します。 |
| 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 バインド アカウント パスワードを入力します。 |

4 [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。

5 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。

6 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。

7 同期するグループおよびユーザーを選択します。

a [新規] 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、**dc=vcac,dc=local** と入力します。

- c 同期するグループを選択するには、[選択] をクリックし、[次へ] をクリックします。
- d **[ユーザーの選択]** ページで、同期するユーザーを選択し、[次へ] をクリックします。
vRealize Automation の使用を必要とするユーザーおよびグループのみを追加します。[ネストされたグループの同期] は、ネスト内のすべてのグループが vRealize Automation の使用を必要とする場合以外には、選択しないでください。
- 8 ディレクトリと同期しているユーザーおよびグループを確認し、[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に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ます。
- 9 [管理] - [ディレクトリ管理] - [ID プロバイダ] の順に選択して、新しい ID プロバイダをクリックします。
たとえば、[WorkspaceIDP__1] をクリックします。
- 10 選択した ID プロバイダのページで各ノードのコネクタを追加します。
 - a [コネクタの追加] については説明に従ってください。
 - b vRealize Automation ロード バランサの完全修飾ドメイン名 (FQDN) をポイントするように [IdP ホスト名] プロパティの値を更新します。
 - c [保存] をクリックします。

次のステップ

[\[ソース vRealize Automation 環境での NSX ネットワークおよびセキュリティ インベントリ データ収集の実行\]](#)。

ソース vRealize Automation 環境での NSX ネットワークおよびセキュリティ インベントリ データ収集の実行

移行の前に、ソース vRealize Automation 環境で NSX ネットワークおよびセキュリティ インベントリ データ収集を実行する必要があります。

このデータ収集は、7.1、7.2、7.3 の展開からの移行時に、vRealize Automation 7.4 でロード バランサの再構成アクションを行うために必要です。

注: vRealize Automation 6.2.x から移行する場合は、ソース環境でこのデータ収集を実行する必要はありません。vRealize Automation 6.2.x では、ロード バランサの再構成アクションをサポートしていません。

手順

- ◆ vRealize Automation 7.4 に移行する前に、ソースの vRealize Automation 環境で NSX ネットワークとセキュリティ インベントリのデータ収集を実行します。『vRealize Automation の管理』の[手動によるエンドポイント データ収集の開始](#)を参照してください。

次のステップ

[\[ソース vRealize Automation IaaS Microsoft SQL データベースの手動によるクローン作成\]](#)。

ソース vRealize Automation IaaS Microsoft SQL データベースの手動によるクローン作成

移行の前に、vRealize Automation 移行前の環境の IaaS Microsoft SQL データベースをバックアップし、それを vRealize Automation ターゲット環境に作成した新しい空のデータベースにリストアする必要があります。

前提条件

- [「ソース vRealize Automation 環境での NSX ネットワークおよびセキュリティ インベントリ データ収集の実行」](#).
- SQL Server データベースのバックアップとリストアに関する情報を取得します。SQL Server データベースの完全バックアップの作成および SQL Server データベースの新しい場所へのリストアに関する [Microsoft Developer Network](#) の記事を参照してください。

手順

- ◆ ソースの vRealize Automation 6.2.x または 7.x IaaS Microsoft SQL データベースのフル バックアップを作成します。このバックアップを使用して、ターゲット環境に作成した新しい空のデータベースに SQL データベースをリストアします。

次のステップ

[「ターゲット vRealize Automation 環境のスナップショット作成」](#) .

ターゲット vRealize Automation 環境のスナップショット作成

各 vRealize Automation ターゲット仮想マシンのスナップショットを作成します。移行に失敗した場合は、仮想マシンのスナップショットを使用して再び移行できます。

詳細については、vSphere のドキュメントを参照してください。

前提条件

[「ソース vRealize Automation IaaS Microsoft SQL データベースの手動によるクローン作成」](#) .

次のステップ

次のいずれかの手順を実行します。

- [「vRealize Automation 7.4 最小環境への vRealize Automation ソース データの移行」](#)。
- [「vRealize Automation 7.4 高可用性環境への vRealize Automation ソース データの移行」](#)。

移行手順

ソース vRealize Automation 環境のデータを移行するために実行する手順は、最小環境と高可用性環境のどちらに移行するかによって異なります。

vRealize Automation 7.4 最小環境への vRealize Automation ソース データの移行

vRealize Automation 環境のデータを vRealize Automation 7.4 の新しいインストールに移行することができます。

ソース システムのすべてのテナントは、ターゲットで再作成し、「ID ストアの移行」手順を実行する必要があります。詳細については、[「VMware Identity Manager への ID ストアの移行」](#) を参照してください。

前提条件

- [「移行に必要な情報の収集」](#)。
- [「ソース vRealize Automation 環境からの暗号化キーの取得」](#)。
- [「vRealize Automation の移行前の環境からターゲット環境への各テナントの追加」](#)。

- 「追加された各テナントの管理者の作成」。
- 「最小環境への移行前に Active Directory リンクのユーザーとグループを同期する」。
- 「ソース vRealize Automation IaaS Microsoft SQL データベースの手動によるクローン作成」。
- 「ターゲット vRealize Automation 環境のスナップショット作成」。
- ターゲット vRealize Automation アプライアンスを展開したときに入力したパスワードを使用して、**root** としてターゲット vRealize Automation アプライアンス管理にログインします。

手順

- 1 [vRA 設定] - [移行] の順に選択します。
- 2 ソース vRealize Automation アプライアンスの情報を入力します。

| オプション | 説明 |
|------------|--|
| ホスト名 | ソース vRealize Automation アプライアンスのホスト名。 |
| root ユーザー名 | root |
| root パスワード | vRealize Automation アプライアンスを展開したときに入力した root パスワード。 |
| 移行パッケージの場所 | 移行パッケージが作成された、移行元の vRealize Automation 6.2.x または 7.x アプライアンス上の既存のディレクトリへのパス。 |

- 3 ターゲット vRealize Automation アプライアンスの情報を入力します。

| オプション | 説明 |
|------------|--|
| root ユーザー名 | root |
| root パスワード | ターゲット vRealize Automation アプライアンスを展開したときに入力した root パスワード。 |
| デフォルトのテナント | vsphere.local このフィールドを変更することはできません。 |
| 管理者ユーザー名 | 管理者 このフィールドを変更することはできません。 |
| 管理者パスワード | ターゲット vRealize Automation 環境を展開したときに入力した administrator@vsphere.local ユーザーのパスワード。 |

- 4 ターゲット IaaS データベース サーバの情報を入力します。

| オプション | 説明 |
|------------------|---|
| データベース サーバ | リストアされた vRealize Automation IaaS Microsoft SQL データベースがある Microsoft SQL Server の場所。名前付きインスタンスとデフォルト以外のポートが使用されている場合は、「<SERVER,PORT\INSTANCE-NAME>」という形式で入力します。AlwaysOn 可用性グループ (AAG) 機能を使用するように、移行先の Microsoft SQL Server を構成する場合は、ポートやインスタンス名を使用せずに、AAG リスナーの名前として移行先の SQL Server を入力します。 |
| クローン作成されたデータベース名 | ソースでバックアップを作成し、ターゲット環境でリストアしたソース vRealize Automation 6.2.x または 7.x IaaS Microsoft SQL データベースの名前。 |

| オプション | 説明 |
|-----------|---|
| 認証モード | <ul style="list-style-type: none"> ■ [Windows] Windows 認証モードを使用する場合、IaaS サービスのユーザーには、SQL Server の db_owner ロールを指定する必要があります。SQL Server 認証モードを使用する場合も同じ権限が適用されます。 ■ [SQL Server] [SQL Server] の場合は、[ログイン名] テキスト ボックスおよび [パスワード] テキスト ボックスが開きます。 |
| ログイン名 | クローン作成された IaaS Microsoft SQL データベースで db_owner ロールを持つ SQL Server ユーザーのログイン名。 |
| パスワード | クローン作成された IaaS Microsoft SQL データベースで db_owner ロールを持つ SQL Server ユーザーのパスワード。 |
| 元の暗号化キー | 移行前の環境から取得する元の暗号化キー。 「ソース vRealize Automation 環境からの暗号化キーの取得」 を参照してください。 |
| 新しいパスフレーズ | 新しい暗号化キーを生成するために使用する一連の単語。このパスフレーズは、ターゲット vRealize Automation 環境に新しい IaaS コンポーネントをインストールするたびに使用します。 |

5 [検証] をクリックします。

ページに検証の進行状況が表示されます。

- すべてのアイテムが正常に検証された場合は、手順 8 に進みます。
- アイテムが検証に失敗した場合は、エラー メッセージと IaaS ノードの検証ログ ファイルを検査します。ログ ファイルの場所については、[「移行ログの場所」](#)を参照してください。[設定の編集] をクリックし、問題のアイテムを編集します。手順 7 に進みます。

6 [移行] をクリックします。

ページに移行の進行状況が表示されます。

- 移行が正常に完了した場合は、このページにすべての移行タスクが完了と表示されます。
- 移行が失敗した場合は、仮想アプライアンスと IaaS ノードで移行ログ ファイルを検査します。ログ ファイルの場所については、[「移行ログの場所」](#)を参照してください。

移行を再開する前に、次の手順を完了します。

- ターゲット vRealize Automation 環境を、移行前にスナップショットを作成したときにキャプチャした状態に戻します。
- ソース IaaS データベースのバックアップを使用して、ターゲット IaaS Microsoft SQL データベースを復旧します。

次のステップ

[「移行後のタスク」](#)。

vRealize Automation 7.4 高可用性環境への vRealize Automation ソース データの移行

高可用性環境として構成された vRealize Automation 7.4 の新しいインストールに、現在の vRealize Automation 環境データを移行できます。

ソース システムのすべてのテナントは、ターゲットで再作成し、「ID ストアの移行」手順を実行する必要があります。詳細については、「[VMware Identity Manager への ID ストアの移行](#)」を参照してください。

前提条件

- 「移行に必要な情報の収集」。
- 「ソース vRealize Automation 環境からの暗号化キーの取得」。
- 「vRealize Automation の移行前の環境からターゲット環境への各テナントの追加」。
- 「追加された各テナントの管理者の作成」。
- 「高可用性環境への移行前に Active Directory リンクのユーザーとグループを同期する」。
- 「ソース vRealize Automation IaaS Microsoft SQL データベースの手動によるクローン作成」。
- 「ターゲット vRealize Automation 環境のスナップショット作成」。
- ターゲット vRealize Automation アプライアンスを展開したときに入力したパスワードを使用して、**root** としてターゲット vRealize Automation アプライアンス管理にログインします。

手順

- 1 [vRA 設定] - [移行] の順に選択します。
- 2 ソース vRealize Automation アプライアンス の情報を入力します。

| オプション | 説明 |
|------------|---|
| ホスト名 | ソース vRealize Automation アプライアンスのホスト名。 |
| root ユーザー名 | root |
| root パスワード | ソース vRealize Automation アプライアンスを展開したときに入力した root パスワード。 |

- 3 移行元 vRealize Automation アプライアンス上の移行パッケージの場所を入力します。

| オプション | 説明 |
|------------|--|
| 移行パッケージの場所 | 移行パッケージが作成された、移行元の vRealize Automation 6.2.x または 7.x アプライアンス上の既存のディレクトリへのパス。 |

- 4 ターゲット vRealize Automation アプライアンスの情報を入力します。

| オプション | 説明 |
|------------|--|
| root ユーザー名 | root |
| root パスワード | ターゲット vRealize Automation アプライアンスを展開したときに入力した root パスワード。 |
| デフォルトのテナント | vsphere.local |
| 管理者ユーザー名 | 管理者 |
| 管理者パスワード | ターゲット vRealize Automation 環境を展開したときに入力した administrator@vsphere.local ユーザーのパスワード。 |

5 ターゲット IaaS データベース サーバの情報を入力します。

| オプション | 説明 |
|------------------|--|
| データベース サーバ | リストアされた vRealize Automation IaaS Microsoft SQL データベースが配置された Microsoft SQL Server インスタンスの場所。名前付きインスタンスとデフォルト以外のポートが使用されている場合は、「<SERVER,PORT\INSTANCE-NAME>」という形式で入力します。AlwaysOn 可用性グループ (AAG) 機能を使用するように、移行先の Microsoft SQL Server を構成する場合は、ポートやインスタンス名を使用せずに、AAG リスナーの名前として移行先の SQL Server を入力します。 |
| クローン作成されたデータベース名 | ソースでバックアップを作成し、ターゲット環境でリストアしたソース vRealize Automation 6.2.x または 7.x IaaS Microsoft SQL データベースの名前。 |
| 認証モード | <ul style="list-style-type: none"> ■ [Windows] Windows 認証モードを使用する場合、IaaS サービスのユーザーには、SQL Server の db_owner ロールを指定する必要があります。SQL Server 認証モードを使用する場合も同じ権限が適用されます。 ■ [SQL Server] [SQL Server] の場合は、[ログイン名] テキスト ボックスおよび [パスワード] テキスト ボックスが開きます。 |
| ログイン名 | クローン作成された IaaS Microsoft SQL データベースで db_owner ロールを持つ SQL Server ユーザーのログイン名。 |
| パスワード | クローン作成された IaaS Microsoft SQL データベースで db_owner ロールを持つ SQL Server ユーザーのパスワード。 |
| 元の暗号化キー | 移行前の環境から取得する元の暗号化キー。 「ソース vRealize Automation 環境からの暗号化キーの取得」 を参照してください。 |
| 新しいパスフレーズ | 新しい暗号化キーを生成するために使用する一連の単語。このパスフレーズは、ターゲット vRealize Automation 環境に新しい IaaS コンポーネントをインストールするときに使用します。 |

6 [検証] をクリックします。

ページに検証の進行状況が表示されます。

- すべてのアイテムが正常に検証された場合は、手順 8 に進みます。
- アイテムが検証に失敗した場合は、エラー メッセージと IaaS ノードの検証ログ ファイルを検査します。ログ ファイルの場所については、[「移行ログの場所」](#)を参照してください。[設定の編集] をクリックし、問題のアイテムを編集します。手順 7 に進みます。

7 [移行] をクリックします。

ページに移行の進行状況が表示されます。

- 移行が正常に完了した場合は、このページにすべての移行タスクが完了と表示されます。
- 移行が失敗した場合は、仮想アプライアンスと IaaS ノードで移行ログ ファイルを検査します。ログ ファイルの場所については、[「移行ログの場所」](#)を参照してください。

移行を再開する前に、次の手順を完了します。

- ターゲット vRealize Automation 環境を、移行前にスナップショットを作成したときにキャプチャした状態に戻します。

- b ソース IaaS データベースのバックアップを使用して、ターゲット IaaS Microsoft SQL データベースを復旧します。

次のステップ

[「移行後のタスク」](#)。

移行後のタスク

vRealize Automation を移行した後、状況に応じて移行後のタスクを実行します。

注: ID ストアを移行後、vRealize Code Stream のユーザーは手動で vRealize Code Stream ロールを再割り当てする必要があります。

ソース vRealize Automation 6.2.x 環境からのテナントと IaaS 管理者の追加

移行後、各テナントの vRealize Automation 6.2.x テナント管理者を削除し、復旧する必要があります。

ターゲット vRealize Automation コンソールの各テナントで、次の手順を実行します。

注: vRealize Automation 7.x 環境から移行する場合は、この手順を実行する必要はありません。

前提条件

- vRealize Automation の最新バージョンへの正常な移行。
- ターゲット vRealize Automation アプライアンスを展開したときに入力したパスワードを使用して、**管理者**としてターゲット 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 テナント名をクリックします。
- 3 [管理者] をクリックします。
- 4 各テナント管理者名とユーザー名のリストを作成します。
- 5 すべての管理者を削除するまで、各管理者をポイントして削除アイコン（[削除]）をクリックします。
- 6 [完了] をクリックします。
- 7 [テナント] ページで、テナント名をもう一度クリックします。
- 8 [管理者] をクリックします。
- 9 適切な検索ボックスに削除した各ユーザーの名前を入力し、Enter キーを押します。
- 10 検索結果から該当するユーザー名をクリックして、そのユーザーを管理者として追加して戻します。
完了すると、テナント管理者のリストは、削除した管理者のリストと同じになります。
- 11 [完了] をクリックします。

接続テストの実行と移行後のエンドポイントの確認

vRealize Automation 7.4 に移行すると、ターゲット環境のエンドポイントに変更が加えられます。

vRealize Automation 7.4 への移行後には、該当するすべてのエンドポイントに対して [接続をテスト] アクションを実行する必要があります。また、移行後の一部のエンドポイントで調整が必要になる場合があります。詳細については、[アップグレードまたは移行後のエンドポイントを使用する場合の考慮事項](#)を参照してください。

アップグレードまたは移行されたエンドポイントのデフォルトのセキュリティ設定では、信頼されていない証明書を受け入れません。

信頼されていない証明書を使用していた場合、以前の vRealize Automation インストール環境からアップグレードまたは移行した後、vSphere と NSX のすべてのエンドポイントに対して、次の手順を実行して証明書の検証を有効にする必要があります。そうしないと、エンドポイントの操作が証明書のエラーで失敗します。詳細については、VMware ナレッジベースの記事「Endpoint communication is broken after upgrade to vRA 7.3 (KB2150230)」(<http://kb.vmware.com/kb/2150230>) および「How to download and install vCenter Server root certificates to avoid Web Browser certificate warnings (KB2108294)」(<http://kb.vmware.com/kb/2108294>) を参照してください。

- 1 アップグレード後または移行後に、vRealize Automation vSphere エージェント マシンにログインし、[サービス] タブを使用して vSphere エージェントを再起動します。

移行ではすべてのエージェントが再起動されない場合があるため、必要に応じて手動で再起動します。

- 2 少なくとも 1 つの ping レポートが終了するのを待ちます。ping レポートの完了には 1、2 分かかります。
- 3 vSphere エージェントがデータ収集を開始したら、IaaS 管理者として vRealize Automation にログインします。
- 4 [インフラストラクチャ] - [エンドポイント] - [エンドポイント] の順にクリックします。
- 5 vSphere エンドポイントを編集し、[接続をテスト] をクリックします。
- 6 証明書のプロンプトが表示されたら、[OK] をクリックして証明書を受け入れます。

証明書のプロンプトが表示されない場合、証明書が現在、プロキシ エージェント マシンや DEM マシンなどのエンドポイントのサービスをホストする Windows マシンの信頼されたルート認証局に正しく保存されていない可能性があります。

- 7 [OK] をクリックして、証明書の承認を適用し、エンドポイントを保存します。
- 8 vSphere エンドポイントごとにこの手順を繰り返します。
- 9 NSX エンドポイントごとにこの手順を繰り返します。

[接続をテスト] 操作は成功したものの、一部のデータ収集やプロビジョニング操作が失敗した場合、エンドポイントとして機能するすべてのエージェント マシンとすべての DEM マシンに同じ証明書をインストールできます。または、既存のマシンから証明書をアンインストールして、問題のあるエンドポイントに対して上記の手順を繰り返します。

ターゲット vRealize Automation 7.4 環境での NSX ネットワークおよびセキュリティ インベントリ データ収集の実行

移行の後には、ターゲット vRealize Automation 7.4 環境で NSX ネットワークおよびセキュリティ インベントリ データ収集を実行する必要があります。

このデータ収集は、vRealize Automation 7.4 で 7.1、7.2、および 7.3 の展開用にロード バランサの再構成アクションを行うために必要です。

注: このデータ収集は、vRealize Automation 6.2.x から 7.4 に移行した場合は、実行する必要はありません。

前提条件

- [「ソース vRealize Automation 環境での NSX ネットワークおよびセキュリティ インベントリ データ収集の実行」](#) .
- vRealize Automation 7.4 に正常に移行します。

手順

- ◆ vRealize Automation 7.4 に移行する前に、ターゲットの vRealize Automation 環境で NSX ネットワークとセキュリティ インベントリのデータ収集を実行します。『vRealize Automation の管理』の「[手動によるエンドポイント データ収集の開始](#)」を参照してください。

移行後のロード バランサを高可用性環境に再構成する

高可用性環境に移行する場合、移行の完了後に各ロード バランサに対して次のタスクを実行する必要があります。

前提条件

[「vRealize Automation 7.4 高可用性環境への vRealize Automation ソース データの移行」](#) .

手順

- 1 次の項目についてロード バランサを構成することで、健全性チェック設定を元に戻し、レプリカ ノードが受信トラフィックを受け入れられるようにします。
 - vRealize Automation アプライアンス
 - Model Manager をホストする IaaS Web サーバ
 - Manager Service
- 2 ロード バランサのタイムアウト設定を変更してデフォルトに戻します。

外部 Orchestrator サーバから vRealize Automation 7.4 への移行

既存の外部 Orchestrator サーバは、vRealize Automation に組み込まれている vRealize Orchestrator インスタンスに移行することができます。

vRealize Orchestrator を外部サーバ インスタンスとして導入し、その外部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。または、vRealize Automation アプライアンスに含まれている vRealize Orchestrator サーバを構成して使用することもできます。

VMware では、外部 vRealize Orchestrator を、vRealize Automation に組み込まれた Orchestrator サーバに移行することをお勧めします。外部 Orchestrator から組み込み Orchestrator への移行には、次の利点があります。

- 総所有コストが削減されます。
- デプロイ モデルが簡素化されます。

- 運用効率が向上します。

注: 外部 vRealize Orchestrator の使用は、次の場合に考慮します。

- vRealize Automation 環境内の複数のテナント
- 物理的に分散した環境
- ワークロードの処理
- 特定のプラグイン（6.5 以前のバージョンの Site Recovery Manager プラグインなど）の使用

Migration Scenarios

The procedure of migrating an external vRealize Orchestrator instance to a vRealize Orchestrator instance embedded in vRealize Automation varies depending on the setup that you have. Several migration scenarios exist based on whether the external Orchestrator server is Windows-based or a virtual appliance, using the embedded database or an external one, and other conditions. You can combine the migration process with an upgrade of vRealize Orchestrator, vRealize Automation, or both. In this case, the migration procedure depends on the source versions of the products.

Migration Scenario Matrix

You can choose a migration scenario based on the source deployment.

| vRealize Orchestrator Deployment | vRealize Automation Deployment | Migration Scenario |
|--|-----------------------------------|--|
| vRealize Orchestrator 6.0.3 Virtual Appliance | vRealize Automation 6.2.3 | 「外部 vRealize Orchestrator 6.x 仮想アプライアンスから vRealize Automation 7.4 への移行」 |
| vRealize Orchestrator 6.0.4 on Windows | vRealize Automation 6.2.4 | 「Windows 上の外部 vRealize Orchestrator 6.x から vRealize Automation 7.4 への移行」 |
| vRealize Orchestrator 6.0.4 Virtual Appliance | vRealize Automation 6.2.4 | 「外部 vRealize Orchestrator 6.x 仮想アプライアンスから vRealize Automation 7.4 への移行」 |
| vRealize Orchestrator 6.0.5 Virtual Appliance | vRealize Automation 6.2.5 | 「外部 vRealize Orchestrator 6.x 仮想アプライアンスから vRealize Automation 7.4 への移行」 |
| vRealize Orchestrator 7.0 Virtual Appliance with an external Oracle Database 12 c | vRealize Automation 7.0 or IaaS | Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2 |
| vRealize Orchestrator 7.0.1 Virtual Appliance with an external PostgreSQL 9.3.9 database | vRealize Automation 7.0.1 or IaaS | Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2 |
| vRealize Orchestrator 7.1 Virtual Appliance | vRealize Automation 7.1 | Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2 |
| vRealize Orchestrator 7.2 Virtual Appliance | vRealize Automation 7.2 | Migrate an External vRealize Orchestrator 7.x to vRealize Automation 7.2 |
| vRealize Orchestrator 7.3 Virtual Appliance | vRealize Automation 7.3 | 「外部 vRealize Orchestrator 7.x から vRealize Automation 7.4 への移行」 |
| vRealize Orchestrator 6.0.3 on Windows | vRealize Automation 6.2.3 | 「Orchestrator 構成を Windows から仮想アプライアンスに移行」 |

Orchestrator 構成を Windows から仮想アプライアンスに移行

Orchestrator 5.5.x および 6.x の Windows スタンドアロン構成を Orchestrator Appliance に移行します。

前提条件

- 移行先のバージョンの Orchestrator ノードを展開および構成します。 [スタンドアロン Orchestrator サーバの構成](#)を参照してください。
- 送信元の Orchestrator が SHA1 パッケージ署名証明書を使用している場合は、より強力な署名アルゴリズムを使用する証明書を再生成してください。推奨される署名アルゴリズムは SHA2 です。
- 移行元と移行先の Orchestrator インスタンスの両方で、Orchestrator サーバ サービスを停止します。
- 移行元 Orchestrator サーバのデータベースを、データベース スキーマとともにバックアップします。

注: 新しい環境が完全に構成されるまで移行元の Orchestrator 環境を使用する場合は、移行元のデータベースのコピーを作成します。作成しない場合は移行先 Orchestrator を構成して同じデータベースを使用することができますが、その場合は移行元の Orchestrator 環境が機能しなくなります。これはデータベース スキーマが移行先 Orchestrator のバージョンにアップグレードされるためです。

手順

- 1 移行先の Orchestrator サーバから移行ツールをダウンロードします。
 - a コントロール センターに **root** としてログインします。
 - b [設定をエクスポート/インポート] ページを開いて、[設定をインポート] タブをクリックします。
 - c 移行ツールをページ説明に従ってダウンロードするか、
`https://<orchestrator_server_IP_or_DNS_name>:8283/vco-controlcenter/api/server/migration-tool` から直接ダウンロードします。
- 2 移行元 Orchestrator サーバから Orchestrator 構成をエクスポートします。
 - a Orchestrator のインストール フォルダにダウンロードされたアーカイブを抽出します。
Windows ベースのインストールの場合、Orchestrator インストール フォルダのデフォルトのパスは **C:\Program Files\VMware\Orchestrator** です。
 - b **PATH** 環境変数は、Orchestrator とともにインストールされる Java JRE の **bin** フォルダをポイントするように設定します。

- c Windows コマンド プロンプトを使用して、Orchestrator インストール フォルダ下の **bin** フォルダに移動します。

デフォルトでは、**bin** フォルダのパスは **C:\Program Files\VMware\Orchestrator\migration-cli\bin** です。

- d コマンド ラインから **export** コマンドを実行します。

```
C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
```

このコマンドは VMware vRealize Orchestrator 構成ファイルとプラグインを 1 つのエクスポート アーカイブに結合します。

ファイル名が **orchestrator-config-export-orchestrator_ip_address-date_hour.zip** のアーカイブは、**migration-cli** と同じフォルダに作成されます。

3 構成を移行先の Orchestrator インスタンスにインポートします。

- a コントロール センターに **root** としてログインします。
- b コントロール センターの [設定をエクスポート/インポート] を開き、[設定をインポート] タブをクリックします。
- c 移行元 Orchestrator インスタンスからエクスポートした **.ZIP** ファイルを参照して、選択します。
- d 構成をエクスポートするときに使用したパスワードを入力します。
パスワードを使用して構成をエクスポートしていない場合は空白のままにします。
- e インポート タイプを選択します。
- f 構成を外部 Orchestrator サーバにインポートする場合は、データベース設定をインポートするかどうかを選択します。

注: 移行元および移行先の Orchestrator サーバが同じ外部データベースを使用するように構成されていない場合は、[データベース設定を移行] チェック ボックスをオフにして、データベース スキーマが新しいバージョンにアップグレードされないようにします。オフにしない場合、移行元 Orchestrator 環境の機能が停止します。

移行の前に移行先 Orchestrator を使用するデータベースを構成しておく必要があります。

- g [インポート] をクリックして移行を終了します。

構成が正常にインポートされたことがメッセージに示されます。移行先の Orchestrator インスタンスの Orchestrator サーバ サービスが自動的に再起動されます。

4 移行先の vRealize Orchestrator で、移行元 Orchestrator で使用されているサーバとは異なる認証プロバイダのサーバを使用している場合は、認証プロバイダで使用するよう構成された SSL 証明書を移行先 Orchestrator のトラストストアにインポートします。

- a コントロール センターの [証明書] ページで、[URL からインポート] をクリックします。
- b vRealize Automation または vSphere インスタンスの URL を指定します。

移行が正常に終了したことを示すメッセージが表示されます。Orchestrator サーバ サービスが自動的に再起動されます。

次のステップ

コントロール センターの [設定を検証] ページで、Orchestrator が正しく設定されていることを確認します。

Windows 上の外部 vRealize Orchestrator 6.x から vRealize Automation 7.4 への移行

vRealize Automation をバージョン 6.x からバージョン 7.4 にアップグレードしたら、Windows 上にインストールされている既存の外部 Orchestrator 6.x を、vRealize Automation 7.4 に組み込まれている Orchestrator サーバに移行できます。

注: 複数の vRealize Automation アプライアンス ノードがある分散 vRealize Automation 環境では、プライマリ の vRealize Automation ノードに対してのみ移行手順を実行します。

前提条件

- vRealize Automation のバージョンを 7.4 にアップグレードまたは移行します。詳細については、『vRealize Automation のインストールまたはアップグレード』の「vRealize Automation のアップグレード」を参照してください。
- 送信元の Orchestrator が SHA1 パッケージ署名証明書を使用している場合は、より強力な署名アルゴリズムを使用する証明書を再生成してください。推奨される署名アルゴリズムは SHA2 です。
- 外部 Orchestrator の Orchestrator サーバ サービスを停止します。
- 外部 Orchestrator サーバのデータベースを、データベース スキーマを含めバックアップします。

手順

- 1 移行先の Orchestrator サーバから移行ツールをダウンロードします。
 - a 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。
 - b `/var/lib/vco/downloads` ディレクトリにある **migration-tool.zip** アーカイブをダウンロードします。
- 2 移行元 Orchestrator サーバから Orchestrator 構成をエクスポートします。
 - a **PATH** 環境変数は、Orchestrator とともにインストールされる Java JRE の **bin** フォルダをポイントするように設定します。
 - b 移行ツールを、外部 Orchestrator がインストールされている Windows サーバにアップロードします。
 - c Orchestrator のインストール フォルダにダウンロードされたアーカイブを抽出します。

Windows ベースのインストールの場合、Orchestrator インストール フォルダのデフォルトのパスは **C:\Program Files\VMware\Orchestrator** です。

- d 管理者として Windows コマンド プロンプトを実行して、Orchestrator インストール フォルダ内の **bin** フォルダに移動します。

デフォルトでは、**bin** フォルダのパスは **C:\Program Files\VMware\Orchestrator\migration-cli\bin** です。

- e コマンド ラインから **export** コマンドを実行します。

```
C:\Program Files\VMware\Orchestrator\migration-cli\bin\vro-migrate.bat export
```

このコマンドは VMware vRealize Orchestrator 構成ファイルとプラグインを 1 つのエクスポート アーカイブに結合します。

アーカイブは **migration-cli** フォルダと同じフォルダ内に作成されます。

- 3 エクスポートした構成を、vRealize Automation 7.4 に組み込まれた Orchestrator サーバに移行します。

- a vRealize Automation アプライアンス で、組み込み vRealize Orchestrator サーバの Orchestrator サーバ サービスとコントロール センター サービスを停止します。

```
service vco-server stop && service vco-configurator stop
```

- b エクスポートした構成ファイルを vRealize Automation アプライアンス の **/usr/lib/vco/tools/configuration-cli/bin** ディレクトリにアップロードします。
- c エクスポートした Orchestrator 構成ファイルの所有権を変更します。

```
chown vco:vco orchestrator-config-export-<orchestrator_ip_address>-<date>_<hour>.zip
```

- d **import** コマンドを使用して **vro-configure** スクリプトを実行し、Orchestrator 構成ファイルを組み込み vRealize Orchestrator サーバにインポートします。

```
./vro-configure.sh import --type embedded --path orchestrator-config-export-<orchestrator_appliance_ip>-<date>_<hour>.zip
```

- e データベースのキーストアからすべての証明書を削除します。

```
./vro-configuration.sh untrust --reset-db
```

4 db-migrate コマンドを使用して vro-configure スクリプトを実行し、データベースを内部 PostgreSQL データベースに移行します。

```
./vro-configure.sh db-migrate --sourceJdbcUrl <JDBC_connection_URL> --sourceDbUsername <database_user> --sourceDbPassword <database_user_password>
```

注: 特殊文字を含むパスワードは一重引用符で囲んでください。

<JDBC_connection_URL> は、使用するデータベースのタイプによって異なります。

PostgreSQL: jdbc:postgresql://<host>:<port>/<database_name>

MSSQL: jdbc:jtds:sqlserver://<host>:<port>/<database_name>; if using SQL authentication and MSSQL:
jdbc:jtds:sqlserver://<host>:<port>/<database_name>;domain=<domain>;useNTLMv2=TRUE if using Windows authentication.

Oracle: jdbc:oracle:thin:@<host>:<port>:<database_name>

デフォルトのデータベースのログイン情報は以下のとおりです。

| | |
|--------------------------|--------|
| <database_name> | vmware |
| <database_user> | vmware |
| <database_user_password> | vmware |

これで、Windows にインストールされている外部 vRealize Orchestrator 6.x が vRealize Automation 7.4 に組み込まれた vRealize Orchestrator インスタンスに正常に移行されました。

次のステップ

組み込み vRealize Orchestrator サーバを設定します。[「組み込み vRealize Orchestrator サーバの構成」](#)を参照してください。

外部 vRealize Orchestrator 6.x 仮想アプライアンスから vRealize Automation 7.4 への移行

vRealize Automation をバージョン 6.x からバージョン 7.4 にアップグレードしたら、既存の外部 Orchestrator 6.x 仮想アプライアンスを vRealize Automation 7.4 に組み込まれている Orchestrator サーバに移行できます。

注: 複数の vRealize Automation アプライアンス ノードがある分散 vRealize Automation 環境では、プライマリの vRealize Automation ノードに対してのみ移行手順を実行します。

前提条件

- vRealize Automation のバージョンを 7.4 にアップグレードまたは移行します。詳細については、『vRealize Automation のインストールまたはアップグレード』の「vRealize Automation のアップグレード」を参照してください。

- 送信元の Orchestrator が SHA1 パッケージ署名証明書を使用している場合は、より強力な署名アルゴリズムを使用する証明書を再生成してください。推奨される署名アルゴリズムは SHA2 です。
- 外部 Orchestrator の Orchestrator サーバサービスを停止します。
- 外部 Orchestrator サーバのデータベースを、データベース スキーマを含めバックアップします。

手順

- 1 移行先の Orchestrator サーバから移行元 Orchestrator に移行ツールをダウンロードします。
 - a SSH を使用して vRealize Orchestrator 6.x 仮想アプライアンスに **root** としてログインします。
 - b `/var/lib/vco` ディレクトリの下で、**scp** コマンドを実行して **migration-tool.zip** アーカイブをダウンロードします。

```
scp root@<vra-vr-hostname.domain.name>:/var/lib/vco/downloads/migration-tool.zip ./
```

- c **unzip** コマンドを実行して、移行ツールのアーカイブを抽出します。

```
unzip migration-tool.zip
```

- 2 移行元 Orchestrator サーバから Orchestrator 構成をエクスポートします。
 - a `/var/lib/vco/migration-cli/bin` ディレクトリで、**export** コマンドを実行します。

```
./vro-migrate.sh export
```

このコマンドは VMware vRealize Orchestrator 構成ファイルとプラグインを 1 つのエクスポート アーカイブに結合します。

ファイル名 **orchestrator-config-export-<orchestrator_ip_address>-<date>_<hour>.zip** を使用したアーカイブが `/var/lib/vco` フォルダに作成されます。

- 3 エクスポートした構成を、vRealize Automation 7.4 に組み込まれた Orchestrator サーバに移行します。
 - a 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。
 - b 組み込み vRealize Orchestrator サーバの Orchestrator サーバサービスとコントロール センター サービスを停止します。

```
service vco-server stop && service vco-configurator stop
```

- c `/usr/lib/vco/tools/configuration-cli/bin` ディレクトリの下で、**scp** コマンドを実行して、エクスポートした構成アーカイブをダウンロードします。

```
scp root@<orchestrator_ip_or_DNS_name>:/var/lib/vco/orchestrator-config-export-<orchestrator_ip_address>-<date>_<hour>.zip ./
```

- d エクスポートした Orchestrator 構成ファイルの所有権を変更します。

```
chown vco:vco orchestrator-config-export-<orchestrator_ip_address>-<date>_<hour>.zip
```

- e **import** コマンドを使用して **vro-configure** スクリプトを実行し、Orchestrator 構成ファイルを組み込み vRealize Orchestrator サーバにインポートします。

```
./vro-configure.sh import --type embedded --path orchestrator-config-export-<orchestrator_appliance_ip>-<date>_<hour>.zip
```

- 4 移行元とする外部 Orchestrator サーバが組み込み PostgreSQL データベースを使用している場合は、データベース構成ファイルを編集します。

- a `/var/vmware/vpostgres/current/pgdata/postgresql.conf` ファイルで、**listen_addresses** 行をコメント解除します。

- b **listen_addresses** の値をワイルドカード (*) に設定します。

```
listen_addresses = '*'
```

- c `/var/vmware/vpostgres/current/pgdata/pg_hba.conf` ファイルに行を追加します。

```
host all all <vra-va-ip-address>/32 md5
```

注: `pg_hba.conf` ファイルでは、IP アドレスとサブネット マスクの代わりに CIDR プリフィックス形式を使用する必要があります。

- d PostgreSQL サーバ サービスを再起動します。

```
service vpostgres restart
```

- 5 **db-migrate** コマンドを使用して **vro-configure** スクリプトを実行し、データベースを内部 PostgreSQL データベースに移行します。

```
./vro-configure.sh db-migrate --sourceJdbcUrl <JDBC_connection_URL> --sourceDbUsername <database_user> --sourceDbPassword <database_user_password>
```

注: 特殊文字を含むパスワードは一重引用符で囲んでください。

<JDBC_connection_URL> は、使用するデータベースのタイプによって異なります。

PostgreSQL: jdbc:postgresql://<host>:<port>/<database_name>

MSSQL: jdbc:jtds:sqlserver://<host>:<port>/<database_name>; if using SQL authentication and MSSQL:
jdbc:jtds:sqlserver://<host>:<port>/<database_name>;domain=<domain>;useNTLMv2=TRUE if using Windows authentication.

Oracle: jdbc:oracle:thin:@<host>:<port>:<database_name>

デフォルトのデータベースのログイン情報は以下のとおりです。

| | |
|--------------------------|--------|
| <database_name> | vmware |
| <database_user> | vmware |
| <database_user_password> | vmware |

- 6 データベースのキーストアからすべての証明書を削除します。

```
./vro-configure.sh untrust --reset-db
```

- 7 Orchestrator プラグインを再インストールします。
- コントロール センターに **root** としてログインします。
 - [トラブルシューティング] をクリックします。
 - [プラグインを強制的に再インストール] をクリックします。

- 8 Orchestrator サーバ サービスを開始します。

- 9 **postgresql.conf** および **pg_hba.conf** ファイルをデフォルトの構成に戻します。

- PostgreSQL サーバ サービスを再起動します。

これで、外部 vRealize Orchestrator 6.x 仮想アプライアンスが vRealize Automation 7.4 に組み込まれた vRealize Orchestrator インスタンスに正常に移行されました。

次のステップ

組み込み vRealize Orchestrator サーバを設定します。[「組み込み vRealize Orchestrator サーバの構成」](#)を参照してください。

外部 vRealize Orchestrator 7.x から vRealize Automation 7.4 への移行

既存の外部 Orchestrator インスタンスから構成をエクスポートし、これを vRealize Automation に組み込まれている Orchestrator サーバにインポートすることができます。

注: 複数の vRealize Automation アプライアンス ノードがある場合は、プライマリの vRealize Automation ノードに対してのみ移行手順を実行します。

前提条件

- vRealize Automation のバージョンを 7.4 にアップグレードまたは移行します。詳細については、『vRealize Automation のインストールまたはアップグレード』の「vRealize Automation のアップグレード」を参照してください。
- 外部 Orchestrator の Orchestrator サーバサービスを停止します。
- 外部 Orchestrator サーバのデータベースを、データベース スキーマを含めバックアップします。

手順

- 1 外部 Orchestrator サーバから構成をエクスポートします。
 - a 移行元のバージョンに応じて、**root** または **管理者** として外部 Orchestrator サーバのコントロール センターにログインします。
 - b [起動オプション] ページから Orchestrator サーバサービスを停止して、データベースに不要な変更が加えられないようにします。
 - c [設定のエクスポート/インポート] ページに移動します。
 - d [設定をエクスポート] ページで、[サーバ設定をエクスポート]、[バンドル プラグイン]、[プラグイン設定をエクスポート] を選択します。
- 2 エクスポートした設定を組み込み Orchestrator インスタンスに移行します。
 - a エクスポートした Orchestrator 構成ファイルを vRealize Automation アプライアンスの `/usr/lib/vco/tools/configuration-cli/bin` ディレクトリにアップロードします。
 - b 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。

- c 組み込み vRealize Orchestrator サーバの Orchestrator サーバ サービスとコントロール センター サービスを停止します。

```
service vco-server stop && service vco-configurator stop
```

- d **import** コマンドを使用して **vro-configure** スクリプトを実行し、Orchestrator 構成ファイルを組み込み vRealize Orchestrator サーバにインポートします。

```
./vro-configure.sh import --type embedded --path orchestrator-config-export-  
<orchestrator_appliance_ip>--<date>_<hour>.zip
```

- 3 移行元とする外部 Orchestrator サーバが組み込み PostgreSQL データベースを使用している場合は、データベース構成ファイルを編集します。

- a `/var/vmware/vpostgres/current/pgdata/postgresql.conf` ファイルで、`listen_addresses` 行をコメント解除します。

- b `listen_addresses` の値をワイルドカード (*) に設定します。

```
listen_addresses = '*'
```

- c `/var/vmware/vpostgres/current/pgdata/pg_hba.conf` ファイルに行を追加します。

```
host all all <vra-va-ip-address>/32 md5
```

注: `pg_hba.conf` ファイルでは、IP アドレスとサブネット マスクの代わりに CIDR プリフィックス形式を使用する必要があります。

- d PostgreSQL サーバ サービスを再起動します。

```
service vpostgres restart
```

- 4 **db-migrate** コマンドを使用して **vro-configure** スクリプトを実行し、データベースを内部 PostgreSQL データベースに移行します。

```
./vro-configure.sh db-migrate --sourceJdbcUrl <JDBC_connection_URL> --sourceDbUsername
<database_user> --sourceDbPassword <database_user_password>
```

注: 特殊文字を含むパスワードは一重引用符で囲んでください。

<JDBC_connection_URL> は、使用するデータベースのタイプによって異なります。

PostgreSQL: jdbc:postgresql://<host>:<port>/<database_name>

MSSQL: jdbc:jtds:sqlserver://<host>:<port>/<database_name>; if using SQL authentication and MSSQL:
jdbc:jtds:sqlserver://<host>:<port>/<database_name>;domain=<domain>;useNTLMv2=TRUE if using Windows authentication.

Oracle: jdbc:oracle:thin:@<host>:<port>:<database_name>

デフォルトのデータベースのログイン情報は以下のとおりです。

| | |
|--------------------------|--------|
| <database_name> | vmware |
| <database_user> | vmware |
| <database_user_password> | vmware |

- 5 データベースのキーストアからすべての証明書を削除します。

```
./vro-configuration.sh untrust --reset-db
```

- 6 Orchestrator プラグインを再インストールします。
- コントロール センターに **root** としてログインします。
 - [トラブルシューティング] をクリックします。
 - [プラグインを強制的に再インストール] をクリックします。

- 7 Orchestrator サーバ サービスを開始します。

- 8 **postgresql.conf** および **pg_hba.conf** ファイルをデフォルトの構成に戻します。

- PostgreSQL サーバ サービスを再起動します。

外部 Orchestrator サーバ インスタンスが vRealize Automation に組み込まれている vRealize Orchestrator インスタンスに正常に移行されました。

次のステップ

組み込み vRealize Orchestrator サーバを設定します。[「組み込み vRealize Orchestrator サーバの構成」](#) を参照してください。

組み込み vRealize Orchestrator サーバの構成

外部の vRealize Orchestrator 構成をエクスポートし、vRealize Automation にインポートしてから、vRealize Automation に組み込まれた vRealize Orchestrator サーバを構成します。

前提条件

設定を外部から内部 vRealize Orchestrator に移行します。

手順

- 1 vRealize Automation アプライアンスのコマンド プロンプト セッションに root としてログインします。
- 2 vRealize Orchestrator コントロール センターのサービスおよびサーバを起動します。

```
service vco-configurator start && service vco-server start
```

- 3 組み込みの vRealize Orchestrator コントロール センターに root としてログインします。

<https://<vrealize-automation-appliance-FQDN>:8283/vco-controlcenter/config>

注: 外部および内部の vRealize Orchestrator バージョンが同じである場合、次の手順を省略することができます。

- 4 コントロール センターで、[設定を検証] をクリックし、vRealize Orchestrator が適切に設定されていることを確認します。
- 5 コントロール センターで、[証明書]、[パッケージ署名証明書] の順にクリックして、新しいパッケージ署名証明書を生成します。
- 6 コントロール センターで、[認証プロバイダを設定] をクリックします。
[デフォルト テナント] と [管理グループ] は、デフォルト値 **vsphere.local** および **vsphere.local\vcadmins** に設定されています。デフォルトの値を環境に応じて変更します。
- 7 vRealize Automation アプライアンスの管理インターフェイスの、[サービス] で、**vco-server** が登録済みであることを確認します。
- 8 外部 vRealize Orchestrator サーバの **vco** サービスを選択し、[登録解除] をクリックします。

次のステップ

- 外部 vRealize Orchestrator サーバにある信頼された証明書を、組み込み vRealize Orchestrator のトラスト ストアにインポートします。詳細については、[Orchestrator の証明書の管理](#)を参照してください。
- vRealize Automation レプリカ ノードを vRealize Automation クラスタに参加させて、vRealize Orchestrator 構成を同期します。

詳細については、『vRealize Automation のインストールまたはアップグレード』の「Reconfigure the Target Embedded vRealize Orchestrator to Support High Availability」を参照してください。

注: vRealize Orchestrator のインスタンスは自動的にクラスタ化されており、使用可能です。

- クラスタ内のすべてのノードで **vco-configurator** サービスを再起動します。
- 移行した組み込み vRealize Orchestrator サーバをポイントするように、vRealize Orchestrator エンドポイントを更新します。
- vRealize Automation ホストと IaaS ホストを vRealize Automation プラグインのインベントリに追加します。これは vRA ホスト ワークフローの vRA ホストの追加と IaaS ホストの追加を実行して行います。

vRealize Automation 証明書を信頼するように組み込みの vRealize Orchestrator を更新する

vRealize Automation アプライアンス 証明書または IaaS 証明書を更新または変更する場合は、vRealize Orchestrator を更新して、新しい、または更新された証明書を信頼する必要があります。

この手順は、組み込みの vRealize Orchestrator インスタンスを使用しているすべての vRealize Automation 展開に適用されます。外部 vRealize Orchestrator インスタンスを使用する場合は、「[Update External vRealize Orchestrator to Trust vRealize Automation Certificates](#)」を参照してください。

注: この手順では、テナントとグループの認証がデフォルトの設定にリセットされます。認証の設定がカスタマイズされている場合は、手順の完了後に認証を再設定できるよう、変更内容をメモしてください。

vRealize Orchestrator 証明書の更新および置き換えについては、vRealize Orchestrator のドキュメントを参照してください。

この手順を完了せずに vRealize Automation 証明書の置き換えまたは更新を行うと、vRealize Orchestrator コントロール センターにアクセスできなくなり、vco-server と vco-configurator のログ ファイルにエラーが表示される場合があります。

vRealize Automation とは異なるテナントとグループに対して認証するように vRealize Orchestrator が設定されている場合にも、証明書を更新する際に問題が発生することがあります。<https://kb.vmware.com/kb/2147612> を参照してください。

手順

- 1 vRealize Orchestrator サーバとコントロール センター サービスを停止します。

```
service vco-server stop
service vco-configurator stop
```

- 2 vRealize Orchestrator 認証プロバイダをリセットします。
 - a `/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh reset-authentication` コマンドを実行します。
 - b `/etc/vco/app-server/vco-registration-id` を削除します。
 - c `vcac-vami vco-service-reconfigure` を実行します。

3 vRealize Orchestrator サーバとコントロール センター サービスを起動します。

```
service vco-server start
service vco-configurator start
```

外部 Orchestrator および組み込み Orchestrator のコントロール センターの違い

外部 vRealize Orchestrator のコントロール センターで使用可能な一部のメニュー項目は、組み込み Orchestrator インスタンスのデフォルトのコントロール センター ビューに含まれていません。

組み込み Orchestrator サーバのコントロール センターでは、いくつかのオプションがデフォルトで非表示になっています。

| メニュー項目 | 詳細 |
|------------------------|--|
| [ライセンス] | 組み込み Orchestrator では vRealize Automation をライセンス プロバイダとして使用するよう事前構成されています。 |
| [設定をエクスポート/インポート] | エクスポートされた vRealize Automation コンポーネントに、組み込み Orchestrator の構成が含まれています。 |
| [データベースを構成] | 組み込み Orchestrator では、vRealize Automation で使用されているデータベースを使用します。 |
| [カスタム エクスペリエンス改善プログラム] | カスタマー エクスペリエンス向上プログラム (CEIP) には vRealize Automation アプライアンス管理インターフェイスから参加できます。 『vRealize Automation の管理』の「カスタム エクスペリエンス改善プログラム」を参照してください。 |

デフォルトのコントロール センター ビューでは非表示になっている別のオプションには、[認証プロバイダを設定] ページの [ホスト アドレス] テキスト ボックスや [登録解除] ボタンがあります。

注: vRealize Automation に組み込まれている vRealize Orchestrator でコントロール センターのオプションをすべて表示するには、Orchestrator 管理の詳細ページ (https://<vra-vd-hostname.domain.name_or_load_balancer_address>:8283/vco-controlcenter/#/?advanced) にアクセスし、キーボードの [F5] ボタンを押してページを更新する必要があります。

ターゲットの vRealize Orchestrator の vRealize Automation エンドポイントの再構成

次の手順を使用して、組み込みのターゲット vRealize Orchestrator の vRealize Automation エンドポイントを再構成します。

前提条件

- vRealize Automation の最新バージョンへの正常な移行。
- vRealize Orchestrator クライアントを使用して、ターゲットの vRealize Orchestrator に接続します。詳細については、[vRealize Orchestrator のドキュメント](#)で、「VMware vRealize Orchestrator クライアントの使用」を参照してください。

手順

- 1 上部のドロップダウン メニューから [設計] を選択します。
- 2 [インベントリ] をクリックします。
- 3 [vRealize Automation] を展開します。

- 4 最小環境から移行した場合は、移行元 vRealize Automation アプライアンス ホストの完全修飾ドメイン名 (FQDN) を含むエンドポイントを識別します。高可用性環境から移行した場合は、移行元アプライアンスのロード バランサの FQDN を含むエンドポイントを識別します。

| FQDN を含むエンドポイントを検索する場合は、次の手順を実行します。 | FQDN を含むエンドポイントが見つからない場合は、次の手順を実行します。 |
|---|--|
| <ol style="list-style-type: none"> 1 [ワークフロー] をクリックします。 2 展開ボタンをクリックし、[ライブラリ] - [vRealize Automation] - [構成] の順に選択します。 3 次のいずれかを実行します。 <ul style="list-style-type: none"> ■ 最小環境から移行した場合は、移行元 vRealize Automation アプライアンス ホストの FQDN を含むすべてのエンドポイントで [vRA ホストの削除] ワークフローを実行します。 ■ 高可用性環境から移行した場合は、移行元アプライアンスのロード バランサの FQDN を含むすべてのエンドポイントで [vRA ホストの削除] ワークフローを実行します。 | <ol style="list-style-type: none"> 1 [リソース] をクリックします。 2 上部のツールバーの更新アイコンをクリックします。 3 展開ボタンをクリックし、[ライブラリ] - [vCACCAFE] - [構成] の順に選択します。 4 次のいずれかを実行します。 <ul style="list-style-type: none"> ■ 最小環境から移行した場合、移行元 vRealize Automation アプライアンス ホストの FQDN を含む URL プロパティを持つ各リソースを削除します。 ■ 高可用性環境から移行した場合は、移行元 vRealize Automation アプライアンスのロード バランサの FQDN を含む URL プロパティを持つ各リソースを削除します。 |

- 5 [ワークフロー] をクリックします。
- 6 展開ボタンをクリックし、[ライブラリ] - [vRealize Automation] - [構成] の順に選択します。
- 7 ターゲットの vRealize Automation のアプライアンス ホスト（高可用性展開から移行した場合は、ロード バランシングされたホスト）を追加するには、[コンポーネント レジストリを使用して vRA ホストを追加] ワークフローを実行します。

ターゲットの vRealize Orchestrator の vRealize Automation インフラストラクチャ エンドポイントの再構成

次の手順を使用して、組み込みのターゲット vRealize Orchestrator の vRealize Automation インフラストラクチャ エンドポイントを再構成します。

前提条件

- vRealize Automation の最新バージョンへの正常な移行。
- vRealize Orchestrator クライアントを使用して、ターゲットの vRealize Orchestrator に接続します。詳細については、[vRealize Orchestrator のドキュメント](#)で、「VMware vRealize Orchestrator クライアントの使用」を参照してください。

手順

- 1 上部のドロップダウン メニューから [設計] を選択します。
- 2 [インベントリ] をクリックします。
- 3 [vRealize Automation Infrastructure] を展開します。

- 4 最小環境から移行した場合は、移行元 vRealize Automation インフラストラクチャ ホストの完全修飾ドメイン名 (FQDN) を含むエンドポイントを識別します。高可用性環境から移行した場合は、移行元アプライアンスのロード バランサの FQDN を含むエンドポイントを識別します。

| FQDN を含むエンドポイントを検索する場合は、次の手順を実行します。 | FQDN を含むエンドポイントが見つからない場合は、次の手順を実行します。 |
|---|--|
| <ol style="list-style-type: none"> 1 [ワークフロー] をクリックします。 2 展開ボタンをクリックし、[ライブラリ] - [vRealize Automation] - [インフラストラクチャ管理] - [構成] の順に選択します。 3 次のいずれかを実行します。 <ul style="list-style-type: none"> ■ 最小環境から移行した場合は、移行元 vRealize Automation インフラストラクチャ ホストの FQDN を含むすべてのエンドポイントで [IaaS ホストの削除] ワークフローを実行します。 ■ 高可用性環境から移行した場合は、移行元 vRealize Automation インフラストラクチャ ホストのロード バランサの FQDN を含むすべてのエンドポイントで [IaaS ホストの削除] ワークフローを実行します。 | <ol style="list-style-type: none"> 1 [リソース] をクリックします。 2 上部のツールバーの更新アイコンをクリックします。 3 展開ボタンをクリックし、[ライブラリ] - [vCAC] - [構成] の順に選択します。 4 次のいずれかを実行します。 <ul style="list-style-type: none"> ■ 最小環境から移行した場合、移行元 vRealize Automation インフラストラクチャ ホストの FQDN を含む host プロパティを持つ各リソースを削除します。 ■ 高可用性環境から移行した場合は、移行元 vRealize Automation インフラストラクチャ ホストのロード バランサの FQDN を含む host プロパティを持つ各リソースを削除します。 |

- 5 [ワークフロー] をクリックします。
- 6 展開ボタンをクリックし、[ライブラリ] - [vRealize Automation] - [構成] の順に選択します。
- 7 ターゲットの vRealize Automation のインフラストラクチャ ホスト（高可用性展開から移行した場合は、ロード バランシングされたホスト）を追加するには、[vRA ホストの IaaS ホストを追加] ワークフローを実行します。

vRealize Orchestrator カスタマイズのインストール

ワークフローを実行して、カスタマイズされた状態変更ワークフロー スタブと vRealize Orchestrator メニュー操作ワークフローをインストールできます。

詳細については、[vRealize Orchestrator カスタマイズのインストール](#)を参照してください。

前提条件

vRealize Automation の最新バージョンへの正常な移行。

ターゲット vRealize Automation に組み込まれた vRealize Orchestrator インフラストラクチャ エンドポイントの再構成

vRealize Automation 6.2.x 環境から移行する場合は、ターゲットの組み込み vRealize Orchestrator サーバを指しているインフラストラクチャ エンドポイントの URL を更新する必要があります。

前提条件

- vRealize Automation 7.4 に正常に移行します。
- ターゲットの vRealize Automation コンソールにログインします。
 - a ターゲット仮想アプライアンスの完全修飾ドメイン名 `https://<vra-va-hostname.domain.name>/vcac` を使用して vRealize Automation コンソールを開きます。

高可用性環境の場合は、ターゲット仮想アプライアンス ロード バランサの完全修飾ドメイン名 `https://<vra-va-lb-hostname.domain.name>/vcac` を使用してコンソールを開きます。

- b Infrastructure as a Service (IaaS) 管理者ユーザーとしてログインします。

手順

- 1 [インフラストラクチャ] - [エンドポイント] - [エンドポイント] の順に選択します。
- 2 [エンドポイント] ページで、vRealize Orchestrator エンドポイントを選択し、[編集] をクリックします。
- 3 [アドレス] テキスト ボックスで、vRealize Orchestrator エンドポイントの URL を編集します。
 - 最小環境に移行した場合は、vRealize Orchestrator エンドポイント URL を **https://<vra-vd-hostname.domain.name>:443/vco** に置き換えます。
 - 高可用性環境に移行した場合は、vRealize Orchestrator エンドポイント URL を **https://<vra-vd-lb-hostname.domain.name>:443/vco** に置き換えます。
- 4 [OK] をクリックします。
- 5 vRealize Orchestrator エンドポイントでデータ収集を手動で実行します。
 - a [エンドポイント] ページで、vRealize Orchestrator エンドポイントを選択します。
 - b [アクション] - [データ収集] の順に選択します。

データ収集が成功したことを確認します。

ターゲット vRealize Automation 環境の Azure エンドポイントの再構成

移行後に、Microsoft Azure エンドポイントを再構成する必要があります。

各 Azure エンドポイントで次の手順を実行します。

前提条件

- 最新バージョンの vRealize Automation 7.4 に正常に移行します。
- ターゲットの vRealize Automation コンソールにログインします。
 - a ターゲット仮想アプライアンスの完全修飾ドメイン名 **https://<vra-vd-hostname.domain.name>/vcac** を使用して vRealize Automation コンソールを開きます。

高可用性環境の場合は、ターゲット仮想アプライアンス ロード バランサの完全修飾ドメイン名 **https://<vra-vd-lb-hostname.domain.name>/vcac** を使用してコンソールを開きます。
 - b Infrastructure as a Service (IaaS) 管理者ユーザーとしてログインします。

手順

- 1 [管理] - [vRO 構成] - [エンドポイント] を選択します。
- 2 Azure エンドポイントを選択します。
- 3 [編集] をクリックします。
- 4 [詳細] をクリックします。
- 5 [クライアント シークレット] テキスト ボックスで、元のクライアント シークレットを入力します。
- 6 [完了] をクリックします。

7 Azure エンドポイントごとにこの手順を繰り返します。

vRealize Automation 6.2.x Automation Application Services から 7.4 への移行

VMware vRealize Application Services の移行ツールを使用して、既存のアプリケーション サービスのブループリントと展開プロファイルを VMware vRealize Application Services 6.2.x から vRealize Automation 7.4 に移行できます。

前提条件

vRealize Automation の最新バージョンへの正常な移行。

手順

- ◆ VMware vRealize Application Services の移行ツールをダウンロードするには、次の手順を完了します。
 - a [ダウンロード VMware vRealize Automation](#) をクリックします。
 - b [ドライバとツール] - [VMware vRealize Application Services Migration Tool] を選択します。

元のターゲット vRealize Automation IaaS Microsoft SQL データベースの削除

移行の完了後、元の IaaS データベースを削除できます。

前提条件

vRealize Automation の最新バージョンへの正常な移行。

移行後の環境では、ターゲット vRealize Automation 環境をインストールしたときに作成した元の vRealize Automation IaaS Microsoft SQL データベースは使用しません。移行が完了したら、元の IaaS データベースを Microsoft SQL Server から削除しても問題ありません。

移行後にデータセンターの [場所] メニューの内容を更新する

移行後、欠落しているカスタム データセンターの場所があれば、[場所] ドロップダウン メニューに追加する必要があります。

vRealize Automation の最新バージョンへの移行後、[コンピュー ト リソース] ページの [場所] ドロップダウン メニュー内のデータセンターの場所は、デフォルトのリストに戻ります。カスタム データセンターの場所が欠落していますが、すべてのコンピュー ト リソースの構成が正常に移行され、**Vrm.DataCenter.Location** プロパティは影響を受けていません。[場所] メニューにカスタム データセンターの場所を追加することができます。

前提条件

vRealize Automation の最新バージョンに移行します。

手順

- ◆ [場所] ドロップダウン メニューに欠落しているデータセンターの場所を追加します。[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。

ソフトウェア エージェントの TLS 1.2 へのアップグレード

vRealize Automation 7.1、7.2、7.3、または 7.3.1 を 7.4 に移行した後、ソフトウェア エージェントを移行前の環境からトランスポート レイヤー セキュリティ (TLS) 1.2 にアップグレードするには、いくつかのタスクを実行する必要があります。

vRealize Automation 7.4 以降、TLS 1.2 は、vRealize Automation とブラウザの間のデータ通信で唯一サポートされる TLS プロトコルです。移行後、既存のすべての仮想マシンと、移行前の vRealize Automation 7.1 または 7.3 環境からの既存の仮想マシン テンプレートをアップグレードする必要があります。

ソース環境の仮想マシン テンプレートの更新

ソフトウェア エージェントが TLS 1.2 プロトコルを使用できるように 7.4 への移行が完了した後、既存の vRealize Automation 7.1、7.2、7.3 または 7.3.1 のテンプレートを更新する必要があります。

ゲスト エージェントおよびエージェント ブートストラップ コードを、ソース環境のテンプレートで更新する必要があります。リンク クローン オプションを使用している場合、新規作成した仮想マシンおよびそれらのスナップショットを使用したテンプレートの再マッピングが必要になることがあります。

テンプレートをアップグレードするには、次のタスクを実行します。

- 1 vSphere にログインします。
- 2 vRealize Automation 7.1、7.2、7.3 または 7.3.1 の各テンプレートを仮想マシンに変換し、そのマシンをオンにします。
- 3 適切なソフトウェアのインストーラをインポートし、各仮想マシンでソフトウェアのインストーラを実行します。
- 4 各仮想マシンを再度テンプレートに変換します。

この手順を使用すると、Linux または Windows 用のソフトウェア インストーラを特定できます。

前提条件

- [「ソフトウェア エージェント パッチの適用」](#) (vRealize Automation 7.1 または 7.3 から 7.4 に移行した場合)。
- vRealize Automation 7.1、7.2、7.3 または 7.3.1 から 7.4 への正常な移行。

手順

- 1 ブラウザを起動し、仮想アプライアンスの完全修飾ドメイン名 (<https://<vra-va-hostname.domain.name>>) を使用して、vRealize Automation 7.4 アプライアンスのスプラッシュ ページを開きます。
- 2 [ゲストおよびソフトウェア エージェント] ページをクリックします。
- 3 Linux または Windows ソフトウェアのインストーラの手順を実行してください。

次のステップ

[「ソフトウェア エージェントのアップグレードが必要な仮想マシンの特定」](#)。

ソフトウェア エージェントのアップグレードが必要な仮想マシンの特定

vRealize Automation コンソールの健全性サービスを使用して、TLS 1.2 へのソフトウェア エージェントの更新が必要な仮想マシンを特定できます。

vRealize Automation ソース環境にパッチを適用したときに、すべての仮想マシンがアップグレードされないことがあります。健全性サービスを使用して、TLS 1.2 へのソフトウェア エージェントの更新が必要な仮想マシンを特定できます。プロビジョニング後の手順のために、ターゲット環境のすべてのソフトウェア エージェントを更新する必要があります。

前提条件

- 「ソフトウェア エージェント パッチの適用」 (vRealize Automation 7.1 または 7.3 から 7.4 に移行した場合)。
- vRealize Automation 7.1、7.2、7.3 または 7.3.1 から 7.4 に正常に移行している。
- プライマリ仮想アプライアンスで vRealize Automation 7.4 にログインしている。

手順

- 1 [管理] - [健全性] の順にクリックします。
- 2 [新しい構成] をクリックします。
- 3 [構成の詳細] ページで、必要な情報を提供します。

| オプション | コメント |
|--------|--|
| 名前 | SW Agent verification と入力します。 |
| 説明 | Locate software agents for upgrade to TLS 1.2 などの、オプションの説明を追加します。 |
| 製品 | vRealize Automation 7.4.0 を選択します。 |
| スケジュール | [なし] を選択します。 |

- 4 [次へ] をクリックします。
- 5 [テストスイートの選択] ページで、[vRealize Automation のシステム テスト] と [vRealize Automation のテナント テスト] を選択します。
- 6 [次へ] をクリックします。
- 7 [パラメータの構成] ページで、必要な情報を提供します。

表 1-84. vRealize Automation 仮想アプライアンス

| オプション | 説明 |
|--------------------|--|
| 公開 Web サーバのアドレス | <ul style="list-style-type: none"> ■ 最小インストールの場合、vRealize Automation アプライアンス ホストのベース URL。例：https://<va-host.domain>/ ■ 高可用性展開の場合、vRealize Automation ロード バランサのベース URL。例：https://<load-balancer-host.domain>/ |
| SSH コンソールのアドレス | vRealize Automation アプライアンスの完全修飾ドメイン名。例：<va-host.domain> |
| SSH コンソール ユーザー | root |
| SSH コンソール パスワード | root のパスワード。 |
| サービスの応答の最大時間 (ミリ秒) | デフォルトを受け入れ：2000 |

表 1-85. vRealize Automation システム テナント

| オプション | 説明 |
|-----------------|------------|
| システム テナント管理者 | 管理者 |
| システム テナント パスワード | 管理者のパスワード。 |

表 1-86. vRealize Automation ディスク容量の監視

| オプション | 説明 |
|--------------|---------------|
| 警告レベルしきい値の割合 | デフォルトを受け入れ：75 |
| 重大レベルしきい値の割合 | デフォルトを受け入れ：90 |

表 1-87. vRealize Automation テナント

| オプション | 説明 |
|-----------------|---|
| テスト対象テナント | テスト対象として選択されたテナント。 |
| ファブリック管理者のユーザー名 | ファブリック管理者のユーザー名。たとえば、admin@va-host.local。 <small>注: すべてのテストを実行するために、このファブリック管理者にはテナント管理者と IaaS 管理者のロールも必要です。</small> |
| ファブリック管理者パスワード | ファブリック管理者のパスワード。 |

- 8 [次へ] をクリックします。
- 9 [サマリ] ページで情報を確認し、[完了] をクリックします。
ソフトウェア エージェントの検証設定が完了しました。
- 10 SW Agent verification カードで、[実行] をクリックします。
- 11 テストが完了したら、SW Agent verification カードの中央をクリックします。
- 12 SW Agent verification の結果ページで、テスト結果を参照して、[名前] 列の [ソフトウェア エージェントのバージョン チェック] テストを見つけます。テスト結果が失敗の場合は、[原因] 列の [原因] リンクをクリックして、ソフトウェア エージェントが古い仮想マシンを表示します。

次のステップ

ソフトウェア エージェントが古い仮想マシンがある場合は、[「vSphere 上のソフトウェア エージェントのアップグレード」](#)を参照してください。

vSphere 上のソフトウェア エージェントのアップグレード

vRealize Automation アプライアンス管理を使用して、移行後に vSphere の古いソフトウェア エージェントを TLS 1.2 にアップグレードできます。

この手順により、仮想マシンの古いソフトウェア エージェントをソース環境から TLS 1.2 にアップデートします。これは vRealize Automation 7.4 への移行に必要です。

前提条件

- [「ソフトウェア エージェント パッチの適用」](#) (vRealize Automation 7.1 または 7.3 から 7.4 に移行した場合)。

- vRealize Automation 7.1、7.2、7.3 または 7.3.1 から 7.4 への正常な移行。
- 健全性サービスを使用して、古いソフトウェア エージェントを持つ仮想アプライアンスを識別している。

手順

- 1 プライマリ vRealize Automation アプライアンスで、vRealize Automation アプライアンスを展開したときに入力したパスワードを使用して、**root** として vRealize Automation アプライアンス管理にログインします。
高可用性環境の場合、マスター アプライアンスでアプライアンス管理を開きます。
- 2 [vRA 設定] - [ソフトウェア エージェント] の順にクリックします。
- 3 [Toggle TLS 1.0、1.1] をクリックします。
[TLS v1.0, v1.1 Status] が有効になります。
- 4 テナント認証情報には、ソース vRealize Automation アプライアンスに要求される情報を入力します。

| オプション | 説明 |
|-------|--|
| テナント名 | ソース vRealize Automation アプライアンス上のテナントの名前。 <small>注: テナントユーザーにはソフトウェア アーキテクト ロールが割り当てられている必要があります。</small> |
| ユーザー名 | ソース vRealize Automation アプライアンス上のテナント管理者のユーザー名。 |
| パスワード | テナント管理者のパスワード。 |

- 5 [接続をテスト] をクリックします。
接続が確立されると、成功のメッセージが表示されます。
- 6 ソース アプライアンスには、ソース vRealize Automation アプライアンスの IP アドレスまたは完全修飾ドメイン名を入力します。
ソースとターゲット アプライアンス両方が同一のテナント認証情報を使用する必要があります。
- 7 [バッチの一覧表示] をクリックします。
バッチ選択肢リスト テーブルが表示されます。
- 8 [表示] をクリックします。
古いソフトウェア エージェントを持つ仮想マシンのリストがテーブルに表示されます。
- 9 アップグレード可能状態の仮想マシンのソフトウェア エージェントをアップグレードします。
 - 個々の仮想マシンのソフトウェア エージェントをアップグレードするには、仮想マシンのグループの [表示] をクリックして、アップグレードする仮想マシンを識別します。それから [実行] をクリックし、アップグレード プロセスを開始します。
 - 仮想マシンのバッチのソフトウェア エージェントをアップグレードするには、アップグレードするグループを識別し、[実行] をクリックしてアップグレード プロセスを開始します。

アップグレードする仮想マシンが 200 台以上ある場合は、次のパラメータの値を入力して、バッチ アップグレード プロセスの速度を制御できます。

| オプション | 説明 |
|-----------|--|
| バッチ サイズ | バッチ アップグレードで選択した仮想マシンの数。この数を変えると、アップグレードの速度を調整することができます。 |
| キュー深度 | 同時に実行されるアップグレードの平行実行の数。たとえば、20 と指定します。この数を変えると、アップグレードの速度を調整することができます。 |
| バッチ エラー | バッチ アップグレードの低速化の原因となった REST エラーの数。たとえば、アップグレードの安定性を向上するために 5 回エラーが発生したときに現在のバッチ アップグレードを停止する場合は、テキスト フィールドに 5 と入力します。 |
| バッチ の失敗 | バッチ アップグレードの低速化の原因となった、失敗したソフトウェア エージェント アップグレードの数。たとえば、アップグレードの安定性を向上するために 5 回エラーが発生したときに現在のバッチ アップグレードを停止する場合は、テキスト フィールドに 5 と入力します。 |
| バッチ ポーリング | アップグレード プロセスをチェックするためにアップグレード プロセスをポーリングする頻度。この数を変えると、アップグレードの速度を調整することができます。 |

アップグレード プロセスが低速すぎるか、失敗したアップグレードが多すぎる場合は、これらのパラメータを調整してアップグレードのパフォーマンスを向上できます。

注: [更新] をクリックすると、バッチのリストがクリアされます。アップグレード プロセスには影響しません。TLS 1.2 が設定されるかどうかに関する情報も更新されます。また、[更新] をクリックすると vRealize Automation サービスの健全性チェックも実行されます。サービスが実行されていない場合、エラー メッセージが表示され、他のすべてのアクション ボタンが無効になります。

10 [Toggle TLS 1.0、1.1] をクリックします。

[TLS v1.0, v1.1 Status] が無効になります。

Amazon Web Service または Azure 上のソフトウェア エージェントのアップグレード

Amazon Web Service (AWS) または Azure 上の古いソフトウェア エージェントは手動でアップグレードすることができます。

- 移行した vRealize Automation サーバの予約で指定されたトンネル プロパティを更新する必要があります。

前提条件

- [「ソフトウェア エージェント パッチの適用」](#) (vRealize Automation 7.1 または 7.3 から 7.4 に移行した場合)。
- vRealize Automation 7.1、7.2、7.3 または 7.3.1 から 7.4 への正常な移行。
- ソフトウェア トンネルが存在し、トンネル仮想マシンの IP アドレスが既知である。

手順

- 1 アップグレードする必要がある各ノードのノード ファイルを作成します。

```
/usr/lib/vcac/server/webapps/ROOT/software/initializeUpdateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> -S <$SourceVRAServer>
```

- 2 Linux または Windows 仮想マシン上のソフトウェア エージェントをアップグレードするプラン ファイルを作成します。

- /var/log/vcac/agentupdate/{tenant}/{subtenant-UUID} にある migrate params ファイルを変更し、AWS または Azure エンドポイントに対応するプライベート IP アドレスの値を含めます。

```
"key": "ipAddress",
  "value": {
    "type": "string",
    "value": "<$PrivateIp:$PrivatePort>"
  }
```

- Linux マシンをアップデートする場合は、このコマンドを使用します。

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CL
Software.LinuxAgentUpdate74 --source_cloud_provider azure
```

- Windows マシンをアップデートする場合は、このコマンドを使用します。

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -S <$SourceVRAServer> -tu <$TenantUser> -CW
Software.WindowsAgentUpdate74 --source_cloud_provider azure
```

- このコマンドは、プラン ファイルを実行します。

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$Tenant> -tu <$TenantUser> --
plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan
```

- 3 手順 1 のノード ファイルと手順 2 のプラン ファイルを使用してソフトウェア エージェントをアップデートするには、このコマンドを使用します。

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$tenant> -tu <$TenantUser> --component_windows
Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --
plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --
node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure
--action plan_batch -S <$SourceVRAServer>
```

代わりに、ノードのインデックスを指定することでノード ファイルから一度に 1 台のノードを実行するには、このコマンドを使用します。

```
/usr/lib/vcac/server/webapps/ROOT/software/updateSoftwareAgents.py -a <
$DestinationVRAServer> -t <$tenant> -tu <$TenantUser> --component_windows
Software.WindowsAgentUpdate74 --component_linux Software.LinuxAgentUpdate74 --
plan_file /usr/lib/vcac/server/webapps/ROOT/software/plan --plan_index 0 --
node_file /usr/lib/vcac/server/webapps/ROOT/software/node --source_cloud_provider azure
--action execute_node -S <$SourceVRAServer> --node_index <0 through n-1>
```

この手順を実行するとき、vRealize Automation 仮想アプライアンスおよびホスト マシンからログの末尾を監視してサーバ エージェントのアップグレード プロセスを表示することができます。

アップグレード後、アップグレード プロセスにより、Windows または Linux 用のソフトウェア アップデート スクリプトは vRealize Automation 7.4 仮想アプライアンスにインポートされます。vRealize Automation 仮想アプライアンス ホストにログインすると、ソフトウェア コンポーネントが正常にインポートされていることを確認できます。コンポーネントをインポートした後、ソフトウェア アップデートは古いイベント ブローカ サービス (EBS) に送信され、指定された仮想マシンにソフトウェア アップデート スクリプトが中継されます。アップグレードが完了し、新しいソフトウェア エージェントが稼動すると、ping 要求を送信して新しい vRealize Automation 仮想アプライアンスにバインドします。

注: 有用なログ ファイル

- ソース vRealize Automation の Catalina 出力 : /var/log/vcac/catalina.out。このファイルでは、エージェントの移行が行われるときに行われるアップグレード要求を確認できます。このアクティビティは、ソフトウェア プロビジョニング要求を実行する場合と同様です。
- ターゲット vRealize Automation の Catalina 出力 : /var/log/vcac/catalina.out。このファイルでは、ping 要求をレポートする移行された仮想マシンが確認できます。バージョン番号 7.4.0-SNAPSHOT が含まれます。これらは、sw-agent-UUID などの EBS トピック名を比較することで照合できます。
- ターゲット vRealize Automation マシン マスター アップグレード ログ ファイルのエージェント アップデート フォルダ : var/log/vmware/vcac/agentupdate/updateSoftwareAgents.log。このファイルの末尾を監視すると、どのアップグレード処理が進行中なのかを確認できます。
- テナント フォルダ下で利用可能な個々のログ : /var/log/vcac/agentupdate/{tenant}/{subtenant-UUID}。個々のノードがエラーや進行中の拡張機能がある多数のファイルとしてここに表示されます。

- 移行された仮想マシン : /opt/vmware-appdirector/agent/logs/darwin*.log。この場所をスポットチェックすると、受信されているソフトウェア アップデート要求、および agent_bootstrap + ソフトウェア エージェントの最後に発生する再起動のリストを確認できます。

移行後にプロパティ ディクショナリ設定を変更する

vRealize Automation 6.2.x から移行した後、プロパティ ディクショナリの **Label** コントロール タイプ プロパティを、ブループリントでオーバーライド不可と設定します。

vRealize Automation 6.2.x プロパティ ディクショナリにあった Label コントロールは、vRealize Automation 7.x にはありません。移行の際、**Label** コントロールは変換され、移行後のプロパティ ディクショナリでは **TextBox** タイプのコントロールになります。

移行後に、vRealize Automation プロパティ ディクショナリで手動により、またはエクスポートおよびインポート機能を使用して、影響を受けるプロパティをオーバーライド不可と設定します。

ターゲット vRealize Automation 7.4 環境の検証

ターゲット vRealize Automation 環境にすべてのデータが正常に移行されたかどうかを確認できます。

前提条件

- vRealize Automation の最新バージョンに移行します。
- ターゲットの vRealize Automation コンソールにログインします。
 - ターゲット仮想アプライアンスの完全修飾ドメイン名 `https://<vra-vd-hostname.domain.name>/vcac` を使用して vRealize Automation コンソールを開きます。
高可用性環境の場合は、ターゲット仮想アプライアンス ロード バランサの完全修飾ドメイン名 `https://<vra-vd-hostname.domain.name>/vcac` を使用してコンソールを開きます。
 - テナント管理者のユーザー名とパスワードを使用してログインします。

手順

- 1 [インフラストラクチャ] - [管理対象マシン] の順に選択し、すべての管理対象仮想マシンが存在することを確認します。
- 2 [コンピューティングリソース] をクリックし、[データ収集]、[今すぐ申請]、[更新] の順にクリックし、エンドポイントが機能していることを確認します。
- 3 [設計] をクリックし、[ブループリント] ページで各ブループリントの要素を検証します。
- 4 [XaaS] をクリックし、[カスタム リソース]、[リソース マッピング]、[XaaS ブループリント]、および [リソース アクション] の内容を確認します。
- 5 [管理] - [カタログ管理] を選択し、[サービス]、[カタログ アイテム]、[アクション]、[資格] の内容を確認します。
- 6 [アイテム] - [デプロイ] を選択し、プロビジョニングされた仮想マシンの詳細を確認します。
- 7 [展開] ページで、プロビジョニングされたパワーオフの仮想マシンを選択し、[アクション] - [パワーオン] を選択します。次に、[送信] > [OK] の順にクリックします。仮想マシンが正常にパワーオンになっていることを確認します。
- 8 [カタログ] をクリックし、新しいカタログ アイテムを申請します。

9 [全般] タブで、申請情報を入力します。

10 マシンのアイコンをクリックし、すべてのデフォルト設定を受け入れて [送信] > [OK] の順にクリックします。

11 申請が正常に終了したことを確認します。

移行に関するトラブルシューティング

移行に関するトラブルシューティングのトピックでは、vRealize Automation の移行時に問題が発生した場合の解決策について説明します。

PostgreSQL バージョンが原因のエラー

更新された PostgreSQL データベースが含まれているソースの vRealize Automation 6.2.x 環境では、管理者アクセスがブロックされます。

問題

アップグレードされた PostgreSQL データベースが vRealize Automation 6.2.x で使用されている場合、管理者は vRealize Automation からこのデータベースへのアクセスを提供するエントリを **pg_hba.conf** ファイルに追加する必要があります。

ソリューション

- 1 **pg_hba.conf** ファイルを開きます。
- 2 このデータベースへのアクセス権を付与するには、次のエントリを追加します。

```
host all <vcac-database-user> <vra-va-ip> <trust-method>
```

移行中に作成された展開が一部の仮想マシンに存在しない

移行時に仮想マシンの状態が指定なしの場合、ターゲット環境で対応する展開が作成されません。

問題

移行時に、移行前の環境で仮想マシンの状態が「情報なし」であった場合、移行先で対応する展開環境が作成されません。

ソリューション

- ◆ 移行後に仮想マシンが「情報なし」の状態でなくなると、パルク インポートを使用して移行先に仮想マシンをインポートすることができます。

移行ログの場所

検証または移行の問題をトラブルシューティングするには、移行プロセスを記録したログを確認します。

表 1-88. ソース vRealize Automation アプライアンス

| ログ | 場所 |
|-----------|--|
| パッケージ作成ログ | /var/log/vmware/vcac/migration-package.log |

表 1-89. ターゲット vRealize Automation アプライアンス

| ログ | 場所 |
|----------|--|
| 移行ログ | /var/log/vmware/vcac/migrate.log |
| 移行実行ログ | /var/log/vmware/vcac/mseq.migration.log |
| 移行実行出力ログ | /var/log/vmware/vcac/mseq.migration.out.log |
| 検証実行ログ | /var/log/vmware/vcac/mseq.validation.log |
| 検証実行出力ログ | /var/log/vmware/vcac/mseq.validation.out.log |

表 1-90. ターゲット vRealize Automation インフラストラクチャ ノード

| ログ | 場所 |
|------|---|
| 移行ログ | C:\Program Files (x86)\VMware\VCAC\InstallLogs- YYYYMMDDHHMMXX\Migrate.log |
| 検証ログ | C:\Program Files (x86)\VMware\VCAC\InstallLogs- YYYYMMDDHHMMXX\Validate.log |

移行後にサービス カタログに表示されるカタログ アイテムを申請できない

vRealize Automation の最新バージョンに移行すると、前のバージョンの特定のプロパティ定義を使用するカタログ アイテムがサービス カタログに表示されますが、申請することはできません。

問題

6.2.x 以前のバージョンから移行していて、次のコントロール タイプまたは属性を持つプロパティ定義が設定されている場合は、これらの要素がアップグレード後のプロパティ定義に含まれていないため注意が必要です。これらの定義を使用するカタログ アイテムは、移行前のように動作しなくなります。

- コントロール タイプ：チェック ボックスまたはリンク
- 属性：関係、正規表現、またはプロパティのレイアウト

原因

vRealize Automation 7.0 以降では、プロパティ定義でこれらの要素が使用されなくなりました。プロパティ定義を再作成するか、組み込みのコントロール タイプまたは属性ではなく vRealize Orchestrator スクリプト アクションを使用するようにプロパティ定義を設定する必要があります。

スクリプト アクションを使用して、これらのコントロール タイプまたは属性を vRealize Automation 7.x に移行します。

ソリューション

- 1 vRealize Orchestrator でこれらのプロパティ値を返すスクリプト アクションを作成します。このアクションは単純な値を返す必要があります。たとえば、文字列、整数、またはその他のサポートされているタイプです。このアクションは、依存する他のプロパティを入力パラメータとして取ることがあります。

2 vRealize Automation コンソールで、製品の定義を設定します。

- a [管理] - [プロパティ ディクショナリ] - [プロパティ定義] の順に選択します。
- b プロパティ定義を選択して、[[編集]] をクリックします。
- c [アドバイスの表示] ドロップダウン メニューで、[ドロップダウン] を選択します。
- d [値] ドロップダウン メニューで、[外部値] を選択します。
- e スクリプト アクションを選択します。
- f [OK] をクリックします。
- g スクリプト アクションに含まれる入力パラメータを設定します。既存の関係を維持するには、パラメータを他のプロパティにバインドします。
- h [OK] をクリックします。

vRealize Automation の無効になった [データ収集] のラジオ ボタン

vRealize Automation 6.2.x から 7.x への移行後、移行先の vRealize Automation の [コンピュート リソース] ページでは [データ収集] のラジオボタンが無効になります。

原因

エンドポイントを参照する移行元環境にエージェントをインストールし、同じエンドポイントを参照する移行先環境に別の名前のエージェントをインストールすると、移行先環境で管理者としてエンドポイントに対するテスト接続を実行できます。ただし、移行先環境の vRealize Automation にファブリック管理者としてログインした場合、[データ収集] の [コンピュート リソース] ページにあるラジオ ボタンが無効になります。

ソリューション

この状況を回避するには、移行先環境にインストールされているエージェントに、移行元環境にインストールされているエージェントと同じ名前を付けます。

ソフトウェア エージェントのアップグレードのトラブルシューティング

vRealize Automation アプライアンス管理を使用してソフトウェア エージェントをアップグレードする際に、ログ ファイルを確認して発生した問題の原因を特定することができます。

問題

ソフトウェア エージェントのアップグレード時、問題が発生することがあります。ソフトウェア エージェントのアップグレード処理時に、ログ ファイルを確認すると、問題の発生箇所を特定することができます。

注: サーバ ログ

- プロセスを観察するには、サーバの updateSoftwareAgents.log ファイル (/storage/log/vmware/vcac/agentupdate/updateSoftwareAgents.log) に tail コマンドを実行します。
- どのソフトウェア エージェントが成功しているか確認するには、ターゲット アプライアンスの catalina.out ファイル (/var/log/vcac/catalina.out) に tail コマンドを実行します。

7.4.0-SNAPSHOT に対してレポートされる「ping」などの文字列を検索します。

詳細情報は、次の場所で確認できます。

- `/var/cache/vcac/agentupdate/{Tenant}/{UUID}/UUID.plan`
- `/var/cache/vcac/agentupdate/{Tenant}/{UUID}/UUID.log`
- `/var/cache/vcac/agentupdate/sqa/UUID/UUID.log` (OS 単位)

メジャー バッチのアップグレードを開始する前に、テスト仮想アプライアンス ソフトウェア エージェントのアップグレードを必ず実行する必要があります。プロセスの概要は以下のとおりです。

- ターゲット仮想アプライアンスに行われた最初の要求を確認して、エージェントのバージョンを識別します。
- アップグレードでソース仮想アプライアンスに行われた要求を確認します。
- ターゲット仮想アプライアンスの新しい 7.4 バージョンをレポートするエージェントを確認します。
- これらのイベントの間、`/storage/log/vmware/vcac/agentupdate/updateSoftwareAgents.log` の `updateSoftwareAgents.log` ファイルを確認します。

注: クライアント ログ

Linux エージェントのログは `appdirector` のエージェント ログ フォルダにあります: `/opt/vmware-appdirector/agent/logs/*.log`

次のようなログ エラーが表示される可能性があります。これは、アップグレード処理中に EBS キューが断続的に機能することによる一時的なものです。

```
Feb 15 2018 16:54:10.105 ERROR [EventPoller-sw-agent-0ad2418d-5b42-4231-a839-a05dd618e43e] []
com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler - Error while polling events
for subscription '{}'.

```

```
org.springframework.web.client.HttpClientErrorException: 404 Not Found

```

```
at

```

```
org.springframework.web.client.DefaultResponseErrorHandler.handleError(DefaultResponseErrorHandler.java:91) ~[nobel-agent.jar:na]

```

```
at org.springframework.web.client.RestTemplate.handleResponse(RestTemplate.java:641) ~[nobel-agent.jar:na]

```

```
at org.springframework.web.client.RestTemplate.doExecute(RestTemplate.java:597) ~[nobel-agent.jar:na]

```

```
at org.springframework.web.client.RestTemplate.execute(RestTemplate.java:557) ~[nobel-agent.jar:na]

```

```
at org.springframework.web.client.RestTemplate.exchange(RestTemplate.java:503) ~[nobel-agent.jar:na]

```

```
at

```

```
com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler.pollEvents(RestEventSubscribeHandler.java:297) ~[nobel-agent.jar:na]

```

```
at com.vmware.vcac.platform.event.broker.client.rest.RestEventSubscribeHandler
$EventPoller.run(RestEventSubscribeHandler.java:329) ~[nobel-agent.jar:na]

```