

vRealize Automation のインストール

2021 年 7 月 21 日

vRealize Automation 7.6

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

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

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

Copyright © 2014-2021 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

目次

vRealize Automation のインストール 7

更新情報 8

1 インストールの概要 9

インストールについて 9

このインストールの新機能 10

インストール コンポーネント 10

vRealize Automation アプライアンス 10

Infrastructure as a Service (IaaS) 11

展開の種類 13

最小インストール 14

分散展開 14

インストール方法の選択 17

2 インストールの準備 18

一般的な準備 18

アカウントとパスワード 19

ホスト名と IP アドレス 21

遅延とバンド幅 21

vRealize Automation アプライアンス 22

vRealize Automation アプライアンス ポート 22

IaaS Windows サーバ 24

IaaS Windows サーバのポート 26

IaaS Web サーバ 27

IaaS Manager Service ホスト 28

IaaS SQL サーバ ホスト 28

IaaS Distributed Execution Manager ホスト 29

Amazon Web Services と DEM ワーカー 30

Openstack または PowerVC と DEM ワーカー 30

Red Hat Enterprise Virtualization と DEM ワーカー 31

SCVMM と DEM ワーカー 31

証明書 32

vRealize Automation 証明書の要件 33

証明書とプライベート キーの抽出 34

3 vRealize Automation アプライアンスの展開 35

アプライアンスの導入について 35

vRealize Automation アプライアンスの展開	35
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	38

4 インストール ウィザードを使用したインストール 41

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	41
ウィザードを使用した最小インストールの開始	41
管理エージェントのインストール	42
インストール ウィザードの完了	44
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	44
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	44
管理エージェントのインストール	45
インストール ウィザードの完了	47

5 標準インストール インターフェイス 48

最小インストールでの標準インターフェイスの使用	48
最小インストールのチェックリスト	49
vRealize Automation アプライアンスの構成	49
IaaS コンポーネントのインストール	52
分散型展開での標準インターフェイスの使用	58
分散インストールのチェックリスト	58
ロード バランサの健全性チェックを無効にする	59
分散型展開における証明書の信頼性の要件	60
Web コンポーネント、Manager Service、DEM ホスト証明書の信頼性の設定	62
インストール ワークシート	62
ロード バランサの構成	65
vRealize Automation のアプライアンスの構成	66
分散構成への IaaS コンポーネントのインストール	72
エージェントのインストール	99
PowerShell 実行ポリシーの RemoteSigned への設定	100
エージェントのインストール シナリオの選択	100
エージェントのインストールの場所および要件	101
vSphere 用のプロキシ エージェントのインストールと構成	101
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	108
XenDesktop 用の VDI エージェントのインストール	112
Citrix 用の EPI エージェントのインストール	116
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	119
リモート WMI 申請用の WMI エージェントのインストール	122

6 サイレント インストール 126

サイレント インストールについて	126
サイレント インストールの実行	127

管理エージェントのサイレント インストールの実行	127
サイレント インストール用の応答ファイル	128
インストール コマンド ライン	129
インストール コマンドラインの基礎	129
インストール コマンド名	130
インストール API	131
サイレント プロパティと JSON の間の変換	132

7 インストール後のタスク 133

タイム ゾーンを変更しない	133
FIPS 準拠の暗号化の設定	134
Manager Service の自動フェイルオーバーの有効化	134
Manager Service の自動フェイルオーバーについて	135
PostgreSQL データベースの自動フェイルオーバー	136
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	136
ホスト名と IP アドレスの変更	136
アプライアンス ホスト名の変更	137
アプライアンスの IP アドレスの変更	137
変更したホスト名に関する SQL データベースの調整	139
IaaS サーバの IP アドレスの変更	139
IaaS サーバ ホスト名の変更	141
ログイン URL のカスタム名への設定	143
vRealize Automation アプライアンス ノードの削除	143
vRealize Log Insight エージェントのインストール	143
VMware Remote Console プロキシ ポートの変更	144
アプライアンスの FQDN を元の FQDN に戻す	144
SQL AlwaysOn 可用性グループの構成	145
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	145
スタティック ルートの設定	147
パッチ管理へのアクセス	148
デフォルト テナントへのアクセスの構成	149

8 インストールのトラブルシューティング 151

失敗したインストールのロールバック	151
最小インストールのロールバック	151
分散インストールのロールバック	152
サポート バンドルの作成	153
一般的なインストールのトラブルシューティング	154
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	154
サーバ時間が同期されない	154
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	155

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	156
プロキシ サーバを介したネットワークへの接続	156
初期コンテンツ構成のためのコンソール手順	157
vRealize Automation のライセンスをダウングレードできない	158
vRealize Automation アプライアンスのトラブルシューティング	158
インストーラのダウンロードに失敗する	158
Encryption.key ファイルに不正な権限がある	159
Horizon Workspace の再起動後に Directories Management Identity Manager が起動に失敗する	160
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	161
レプリカおよびマスター ノードの昇格後の失敗	162
不正なコンポーネント サービス登録	162
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	164
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	165
Active Directory 同期ログの保持期間が短すぎる	165
RabbitMQ でホスト名を解決できない	166
IaaS コンポーネントのトラブルシューティング	167
分散トランザクション コーディネータの接続が拒否される	167
IaaS サーバが切断されていると表示される	168
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	169
IaaS のサーバ証明書の検証	169
IaaS インストーラ実行時の認証情報エラー	170
IaaS のインストール中に設定の保存の警告が表示される	170
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	171
IaaS Web と Model Management のインストール中に IaaS 認証に失敗する	171
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	172
IaaS Windows サーバは FIPS をサポートしない	173
XaaS エンドポイントを追加すると内部エラーが発生する	174
プロキシ エージェントのアンインストールに失敗する	174
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	174
Manager Service 通信のエラー	175
変更された電子メールのカスタマイズ動作	176
ログイン エラーのトラブルシューティング	177
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	177
高可用性でログインに失敗する	177
プロキシが原因で VMware Identity Manager ユーザーがログインできない	178

vRealize Automation のインストール

この『vRealize Automation インストール』ガイドでは、VMware vRealize™ Automation のウィザード インストール、手動インストール、およびサイレント インストールの手順が説明されています。

注： vRealize Automation のすべての特徴と機能がすべてのエディションで使用できるわけではありません。各エディションの機能セットの比較については、<https://www.vmware.com/products/vrealize-automation/>を参照してください。

対象者

この情報は、Windows または Linux のシステム管理者としての経験があり、仮想マシン テクノロジーおよびデータ センターの運用に詳しい方を対象としています。

更新情報

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

リビジョン	説明
202X 年 XX TBD	<ul style="list-style-type: none">■ vRealize Automation 管理エージェントのインストールを更新しました。■ Manager Service の自動フェイルオーバーの有効化を更新しました。■ 不正な vRealize Automation コンポーネント サービス登録を更新しました。
2020 年 8 月 12 日	証明書とプライベート キーの抽出 を更新しました。
2020 年 2 月 14 日	<ul style="list-style-type: none">■ IaaS Windows サーバを更新しました。■ IaaS Manager Service ホストを更新しました。■ IaaS SQL サーバ ホストを更新しました。■ vRealize Automation タイム ゾーンを変更しないを更新しました。■ バッチ管理へのアクセスを更新しました。■ 分散トランザクション コーディネータの接続が拒否されるを追加しました。■ 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を更新しました。
2019 年 10 月 24 日	コネクタ リマインダを クラスタへの別の vRealize Automation アプライアンスの追加 に追加しました。
2019 年 9 月 9 日	<ul style="list-style-type: none">■ vRealize Automation アプライアンスを更新しました。■ vRealize Automation タイム ゾーンを変更しないを追加しました。
2019 年 6 月 14 日	<ul style="list-style-type: none">■ アカウントとパスワードのグループ ポリシー設定を更新しました。■ IaaS Windows サーバで英語のロケールを更新しました。■ IaaS サーバが切断されていると表示されるを追加しました。
2019 年 5 月 30 日	<ul style="list-style-type: none">■ アカウントとパスワードのグループ ポリシー設定を追加しました。■ IaaS Windows サーバの PowerShell 2 が削除され、英語ロケールが追加されました。
2019 年 5 月 7 日	いくつかのハイパーリンクを修正しました。
2019 年 4 月 11 日	初版リリース。

vRealize Automation インストールの概要

1

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。

この章には、次のトピックが含まれています。

- [vRealize Automation のインストールについて](#)
- [この vRealize Automation インストールの新機能](#)
- [vRealize Automation インストール コンポーネント](#)
- [展開の種類](#)
- [インストール方法の選択](#)

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

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。詳細については、[vRealize Suite Lifecycle Manager Installation, Upgrade, and Management Guide](#) を参照してください。

vRealize Suite Lifecycle Manager は、インストール、構成、アップグレード、パッチ適用、構成管理、エラー修正、および健全性チェックを単一の管理画面から自動的に実行します。vRealize Suite Lifecycle Manager をインストールするには、[こちら](#)をクリックしてください。Lifecycle Manager を使用すると、クラウド管理リソースの IT マネージャはビジネスクリティカルなイニシアティブに重点を置きながら、価値の提供、信頼性、および一貫性を向上させることができます。

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、このリリースではインストール プロセスが変更されていることに注意してください。

- インストール後にログインすると、システム情報、ステータス、および使用状況の統計情報を示す新しい [サマリ] ページに、vRealize Automation アプライアンス管理インターフェイスが表示されます。
- vRealize Automation アプライアンス管理インターフェイスの [クラスタ] タブに、各種の健全性統計のレポートを表示できるようになりました。

デフォルトのクラスタ レポートを変更するには、vRealize Automation アプライアンスで次のファイルを編集します。

```
/etc/vcac/validation.properties
```

ファイルの設定によっては、[サマリ] ページのステータスにも影響します。

- リリース ノートに詳しく記載されているように、このリリースでは、レポートされている複数の問題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 AutomationIaaS 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 AutomationIaaS 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ーサリングを提供します。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

IaaS 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、IaaS 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 IaaS 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 IaaS 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 IaaS 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。
- IaaS 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。

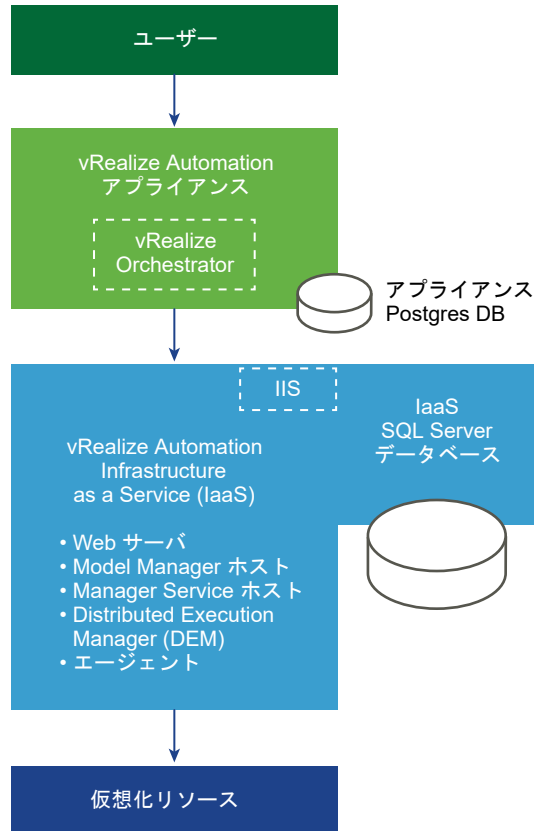
展開の種類

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 1-1. vRealize Automation の最小インストール

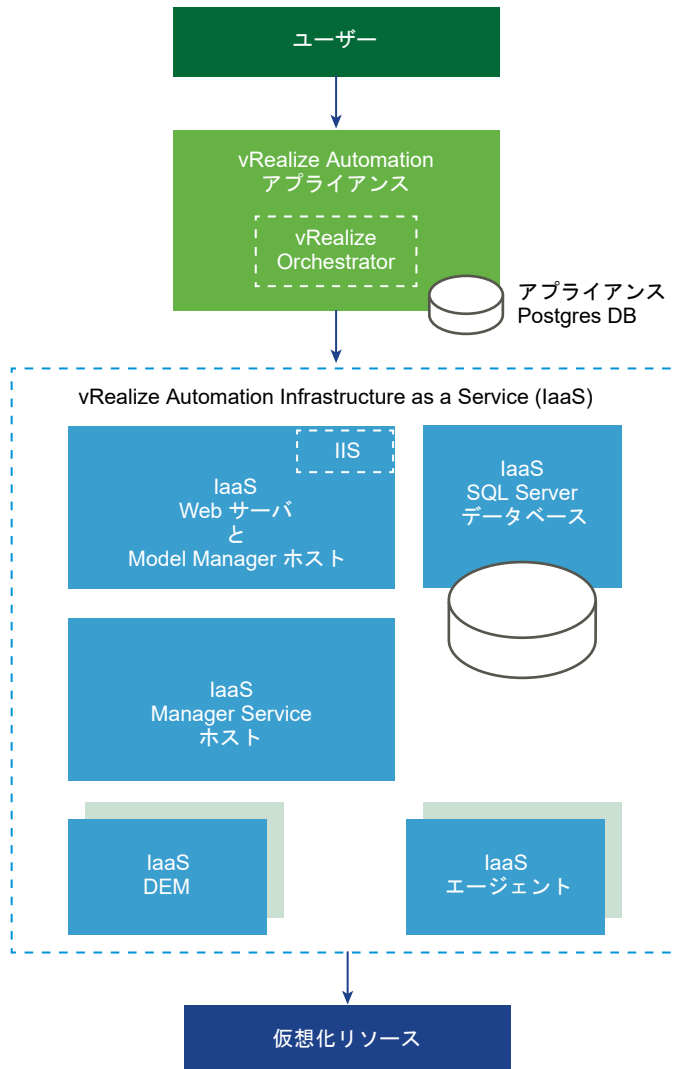


最小インストールは、エンタープライズ インストール環境に変換できません。インストール環境をスケール アップするには、小規模のエンタープライズ環境から開始して、コンポーネントを追加していきます。最小インストールから開始することはできません。

vRealize Automation の分散展開

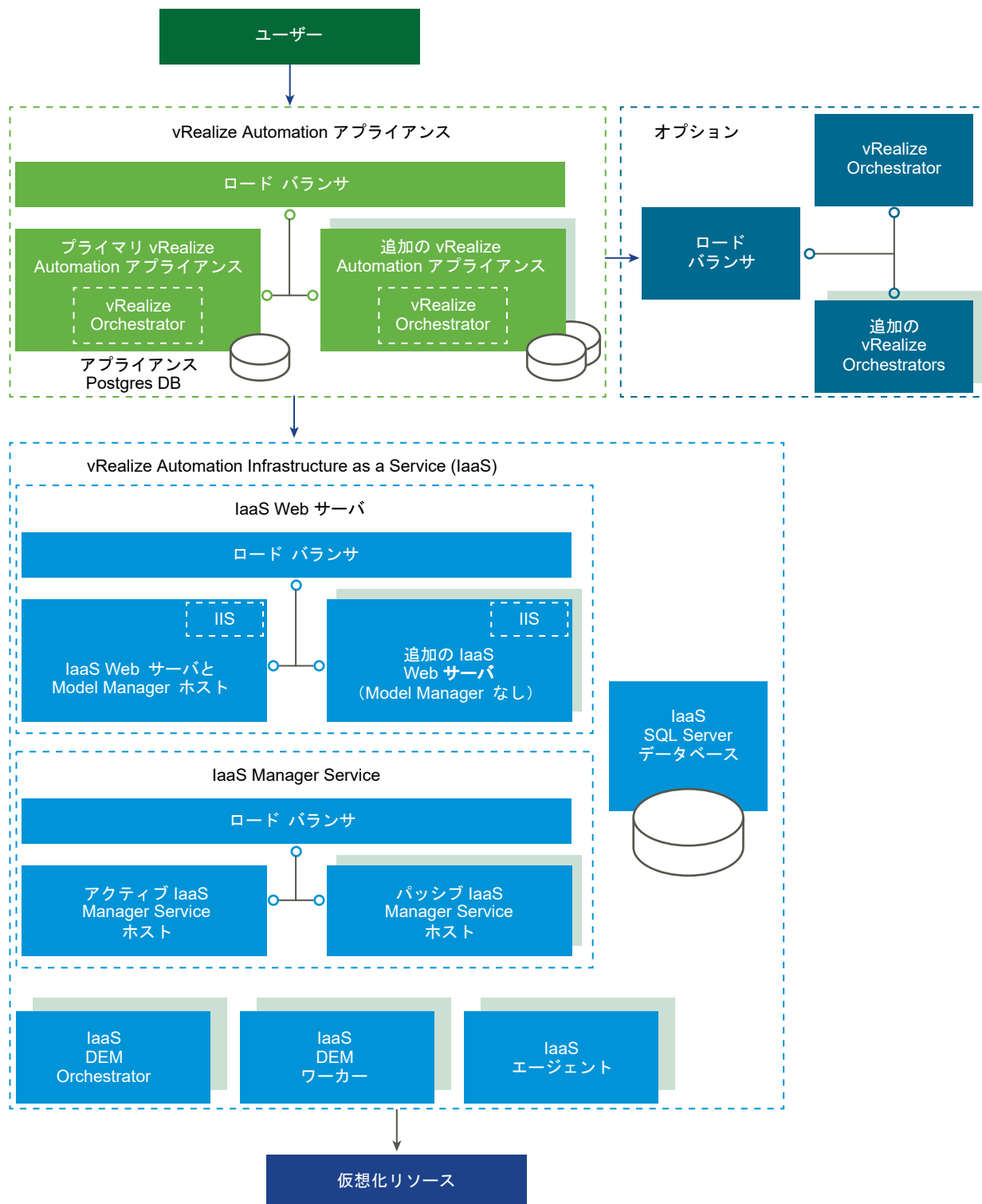
分散エンタープライズ展開はさまざまな規模で実装できます。基本的な分散展開では、次の図に示すように IaaS コンポーネントを個別の Windows サーバでホストするだけで vRealize Automation を強化できる場合があります。

図 1-2. 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 1-3. 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

2

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。

この章には、次のトピックが含まれています。

- 一般的な準備
- アカウントとパスワード
- ホスト名と IP アドレス
- 遅延とバンド幅
- vRealize Automation アプライアンス
- IaaS Windows サーバ
- IaaS Web サーバ
- IaaS Manager Service ホスト
- IaaS SQL サーバ ホスト
- IaaS Distributed Execution Manager ホスト
- 証明書

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。

IaaS サービス アカウント

IaaS 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 IaaS 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。
- IaaS 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、IaaS 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。

- サイトでグループ ポリシーのセキュリティ設定を使用している場合は、アカウントの次の設定を確認します。
gpedit.msc グループ ポリシー エディタを実行し、[コンピューターの構成] - [Windows の設定] - [セキュリティの設定] - [ローカル ポリシー] - [ユーザー権利の割り当て] を確認します。
 - ローカル ログインを拒否 — アカウントは追加しません。
 - ローカル ログインを許可 — アカウントを追加します。
 - ネットワーク経由でコンピュータへアクセスを拒否する — アカウントは追加しません。
 - ネットワーク経由でコンピュータへアクセス — アカウントを追加します。

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。

IaaS 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 IaaS 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 IaaS 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 dbo 権限だけです。

IaaS 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、IaaS 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 [IaaS 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。

アプライアンスでは SUSE Linux Enterprise 11 (64 ビット) が実行されています。VMware は、アプライアンスの変更またはカスタマイズをサポートしていません。ウイルス対策ソフトウェアを含む、パッケージまたはカスタム スクリプトの追加、削除、更新は行わないでください。

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 2-1. 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 ■ 140 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 ■ 140 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 2-2. 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。
8494	TCP	コンテナ サービスのクラスタの同期
9300-9400	TCP	Identity Manager 監査へのアクセス。
54328	UDP	
40002、40003	TCP	vIDM クラスタの同期
8090、8092	TCP	健全性サービスが vRA ノード間の接続のために使用

表 2-3. 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。
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。

表 2-3. 出力ポート（続き）

ポート	プロトコル	コメント
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。
8494	TCP	コンテナ サービスのクラスタの同期
9300-9400	TCP	Identity Manager 監査へのアクセス。
54328	UDP	
40002, 40003	TCP	vIDM クラスタの同期

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。

重要： インストールすると、Windows ファイアウォールは無効になります。サイト ポリシーで Windows ファイアウォールが必須になっている場合は、インストール後に再度有効にし、IaaS Windows サーバ ポートを個別に開きます。 [IaaS Windows サーバのポート](#) を参照してください。

- 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。

- IaaS Windows サーバと SQL Server データベース ホストは、NETBIOS 名で相互に解決できる必要があります。必要に応じて、各 IaaS Windows サーバおよび SQL Server データベース ホストの `/etc/hosts` ファイルに NETBIOS 名を追加し、マシンを再起動します。
- 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 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。

- 最小サイズより大きい展開の場合は、IaaS Windows サーバを英語のロケールに設定します。
- 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 2-4. 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 2-5. 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

表 2-5. 出力ポート（続き）

ポート	プロトコル	コンポーネント	コメント
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 201 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 2-6. IaaS Internet Information Services

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 アクティブ化サービスのロール	<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 アクティブ化] 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。

IaaS SQL サーバ ホスト

IaaS 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、IaaS Windows サーバのいずれか、または別のホストに配置できます。IaaS コンポーネントとともにホストする場合は、すべての IaaS 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。IaaS 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。

同じ動作は SQL Server 2017 にも適用されます。

- AlwaysOn Availability Group (AAG) がサポートされるのは、SQL Server 2016 Enterprise または SQL Server 2017 Enterprise のみです。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。AAG を作成する場合は、DTC_Support = Per_DB を設定します。AAG の作成後に設定することはできません。
- IaaS コンポーネントとともにホストする場合は、Java を構成します。
 - 64 ビット版の Java 1.8 Update 201 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。IaaS 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ください。
- 通常は、[IaaS 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 リファレンス アーキテクチャ ガイドの「ハードウェアの仕様とキャパシティの上限」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。

IaaS 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 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。

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、[IaaS 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 AutomationIaaS 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、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 AutomationIaaS 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 2-7. 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	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： <pre>[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319] "SchUseStrongCrypto"=dword:00000001 [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319] "SchUseStrongCrypto"=dword:00000001</pre>
Windows 2008 DEM ホスト	Windows レジストリで、TLS v1.2 プロトコルを有効にします。例： <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 [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	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。

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 AutomationIaaS 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 AutomationIaaS 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。

SCVMM 環境の準備の詳細については、vRealize Automation の構成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 2-8. 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作成します。	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	2048、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 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

証明書とプライベート キーの抽出

仮想アプライアンスの証明書は PEM 形式である必要があります。

認証局から提供された証明書が PFX 形式の場合は、OpenSSL を使用して PFX から PEM に変換します。

```
openssl pkcs12 -in path-to-pfx -out desired-path-to-pem -nodes
```

例：

```
openssl pkcs12 -in C:\vra-cert.pfx -out C:\vra-cert.pem -nodes
```

PFX 証明書にパスフレーズが含まれている場合は、パスフレーズの入力を求められる可能性があります。

vRealize Automation アプライアンスの展開

3

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。

この章には、次のトピックが含まれています。

- [vRealize Automation アプライアンスの導入について](#)
- [vRealize Automation アプライアンスの展開](#)
- [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 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 3-1. 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	This will be used as an initial status of the SSH service in the appliance. You can change it later from the appliance Web console. <input checked="" type="checkbox"/>
Hostname	The host name for this virtual machine. Provide the fully qualified domain name if you use a static IP. Leave blank to try to reverse look up the IP address if you use DHCP. <input type="text" value="va1.mycompany.com"/>
Initial root password	This will be used as an initial password for the root user account. You can change the password later (by using the passwd command or from the appliance Web console). Enter password <input type="password" value="*****"/> Confirm password <input type="password" value="*****"/>
▼ Networking Properties	6 settings
Default Gateway	The default gateway address for this VM. Leave blank if DHCP is desired. <input type="text" value="12.34.56.79"/>
Domain Name	The domain name of this VM. Leave blank if DHCP is desired. <input type="text" value="mycompany.com"/>
Domain Name Servers	The domain name server IP Addresses for this VM (comma separated). Leave blank if DHCP is desired. <input type="text" value="12.34.56.80, 12.34.56.81"/>
Domain Search Path	The domain search path (comma or space separated domain names) for this VM. Leave blank if DHCP is desired. <input type="text" value="mycompany.com"/>
Network 1 IP Address	The IP address for this interface. Leave blank if DHCP is desired. <input type="text" value="12.34.56.78"/>
Network 1 Netmask	The netmask or prefix for this interface. Leave blank if DHCP is desired. <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 Postgres 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-addressnetmaskgateway-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 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。
- 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

4

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、[5 章 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。

この章には、次のトピックが含まれています。

- [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](#)
- [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](#)

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

- [2 章 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 4-1. 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。

結果

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。[6 章 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。
- 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。

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

- [2 章 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、プライマリ 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 サーバをプライマリ 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

1 つ以上の 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 プライマリ 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、プライマリ 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 プライマリ 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、プライマリ アプライアンスの HTTPS アドレスを入力します。
- b プライマリ 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 4-2. 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。

結果

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。[6 章 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。
- 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。

標準 vRealize Automation インストール インターフェイス

5

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。

4 章 [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。

この章には、次のトピックが含まれています。

- [最小インストールでの標準インターフェイスの使用](#)
- [分散型展開での標準インターフェイスの使用](#)
- [vRealize Automation エージェントのインストール](#)

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 5-1. 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。	2 章 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] - [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 <code>vra-hostname.domain.name</code> 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 <code>vra-loadbalancename.domain.name</code> 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] メニューから適切なアクションを選択します。

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。

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] > [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 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。

結果

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。

laaS 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 (laaS) 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 laaS 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。vRealize Automation 管理インターフェイスにポート 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。

結果

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 [パスフレーズ] テキスト ボックスにパスフレーズを入力します。

パスフレーズは、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ス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。

結果

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 5-2. 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。	2 章 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
<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 プラグインの使用」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。

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、『vRealize Automation の構成』ガイドを参照してください。

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。

分散型展開でもクラスタ化された展開でも、証明書の組織は多くの場合、3 階層から成る vRealize Automation アーキテクチャに準拠します。

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

分散型の展開では、特定の階層内の各マシンで証明書を共有します。たとえば、各 vRealize Automation アプライアンスが共通の証明書を共有し、各 Manager Service ホストが共通の証明書を共有します。

Web および Manager Service コンポーネントが同一のマシンにホストされている場合は、両階層に対して 1 つの証明書で十分です。

システムが生成した証明書

バージョン 7.0 以降では、独自の証明書を提供しない場合、vRealize Automation インストール ウィザードで自己署名証明書を自動的に生成され、それらを必要とする分散コンポーネント上の適切なトラストストアに配置されます。

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 の管理」を参照してください。

独自の証明書の指定

標準の手動インストーラを実行する場合は、独自に生成された自己署名証明書または認証局 (CA) 証明書を提供します。

OpenSSL または別の方法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。

laaS 証明書は、マルチユースの証明書である必要があります。証明書を指定するときは、クラスタに laaS 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

高可用性とフェイルオーバーのために、分散 vRealize Automation コンポーネントの手前にロード バランサを追加できます。vRealize Automation ロード バランサには、パススルー構成をお勧めします。パススルー構成では、ロード バランサは、要求を復号化せずにコンポーネントに渡します。その後、vRealize Automation アプライアンスと laaS ホストで必要な復号化が実行されます。

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。

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。

証明書の信頼性の要件

次の表に、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。

インポート	登録
vRealize Automation アプライアンス クラスタ	laaS Web コンポーネント クラスタ
laaS 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
laaS 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

証明書の信頼性と標準のインストーラ

標準の手動インストーラを実行または再実行して laaS コンポーネントを作成する場合は、いずれの場合でもそれらの laaS コンポーネントで証明書の信頼性を設定する必要があります。たとえば、標準のインストーラを使用して、既存の展開をスケール アウトする場合です。

■ laaS Web および Manager Service ホスト

web.pfx および ms.pfx ファイルを次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
```

■ laaS DEM Orchestrator、DEM ワーカー、およびプロキシ エージェント ホスト

web.pfx および ms.pfx ファイルを次の場所にインポートします。

```
Host Computer/Certificates/Trusted People certificate store
```

信頼されたユーザーの証明書ストアでは、証明書とともにプライベート キーをインポートする必要はありません。自動インストール プロセスでは、信頼されたユーザーの証明書ストアに証明書のみがインストールされます。

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 5-3. 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 参照のみ。IP アドレスは入力しないでください		123.234.1.105
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 参照のみ。IP アドレスは入力しないでください		123.234.1.106
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 参照のみ。IP アドレスは入力しないでください		123.234.1.201
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 5-4. 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 参照のみ。IP アドレスは入力しないでください		123.234.1.107
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 参照のみ。IP アドレスは入力しないでください		123.234.1.108
IaaS Web サーバ ロード バランサ FQDN		web-balance.mycompany.com

表 5-4. IaaS Windows サーバ（続き）

変数	値	例
IaaS Web サーバ ロード バランサ IP アドレス 参照のみ。IP アドレスは入力しないでください		123.234.1.202
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 参照のみ。IP アドレスは入力しないでください		123.234.1.109
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 参照のみ。IP アドレスは入力しないでください		123.234.1.110
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 参照のみ。IP アドレスは入力しないでください		123.234.203
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 5-5. 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 5-6. 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 参照のみ。IP アドレスは入力しないでください		123.234.1.111

表 5-6. IaaS Distributed Execution Manager（続き）

変数	値	例
DEM ホスト FQDN		dem2.mycompany.com
DEM ホスト IP アドレス 参照のみ。IP アドレスは入力しないでください		123.234.1.112
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 バランシング構成ガイド』テクニカル ホワイト ペーパー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] - [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 <i>vra-hostname.domain.name</i> 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 <i>vra-loadbalancename.domain.name</i> 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] メニューから適切なアクションを選択します。

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。

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 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インターフェイスに root ユーザーとしてログインします。

`https://vrealize-automation-appliance-FQDN:5480`

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] > [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 [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。**12** [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。

13 [設定の保存] をクリックします。**14** 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。

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。

Active Directory — 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。別のアプライアンスを追加した後は、追加したアプライアンスに対応する 2 つ目のコネクタを構成してください。2 つ目のコネクタは ID プロバイダに接続し、同じ Active Directory を参照します。この方法では、最初のアプライアンスに障害が発生した場合、2 つ目のアプライアンスがユーザー認証の管理を引き継ぎます。

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] - [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。

結果

クラスタへの参加の処理に時間がかかり、最終的にタイムアウトになった場合は、[VMware ナレッジベースの記事 KB58708](#) を参照してください。

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、それらを無視し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 5-7. 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 5-8. データベース値

変数	値
<i>db_server</i>	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。 <i>db_server</i> のデフォルト値は localhost です。
<i>db_name</i>	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。
<i>db_dir</i>	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。
<i>log_dir</i>	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。
<i>service_user</i>	Manager Service を実行するユーザー名です。
<i>Web_user</i>	Web サービスを実行するユーザー名です。
<i>version_string</i>	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。

結果

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 5-9. データベース値

変数	値
\$(DBName)	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。
\$(DBDir)	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。
\$(LogDir)	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。vRealize Automation 管理インターフェイスにポート 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。**結果**

データベースの使用準備ができました。

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。

前提条件

- 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 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。

結果

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 バランサの下そ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 [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。vRealize Automation 管理インターフェイスにポート 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 の管理』ガイドの「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。vRealize Automation 管理インターフェイスにポート 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 (<i>web-load-balancer.mycompany.com:443</i>) 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 (<i>web.mycompany.com:443</i>) 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

[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。vRealize Automation 管理インターフェイスにポート 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 (<i>web-load-balancer.mycompany.com:443</i>) 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 (<i>web.mycompany.com:443</i>) 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 の管理』ガイドの「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。vRealize Automation 管理インターフェイスにポート 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 (<i>web-load-balancer.mycompany.com:443</i>) 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 (<i>web.mycompany.com:443</i>) 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 つ目の 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](#)。

新しい DEMWorker をインストールする前に、vRA がインストールされた仮想アプライアンスから証明書をエクスポートし、ローカル マシンの信頼されたルート証明書ストレージの場所にインポートします。

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。vRealize Automation 管理インターフェイスにポート 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 (<i>mgr-svc-load-balancer.mycompany.com:443</i> および <i>web-load-balancer.mycompany.com:443</i>) 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 (<i>mgr-svc.mycompany.com:443</i> および <i>web.mycompany.com:443</i>) 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。

結果

詳細については、[SCVMM と DEM ワーカー](#)を参照してください。

SCVMM 環境の準備および SCVMM エンドポイントの作成についての追加情報は『vRealize Automation の構成』で入手できます。

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

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 IaaS 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

- [IaaS 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 VMPS0psUser.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 VMPS0psUser.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。

結果

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継続します。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 5-10. 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。

VApp.Import 権限では、OVF からインポートした設定を使用して vSphere マシンを展開することができます。vSphere 権限の詳細は、[vSphere SDK のドキュメント](#)に記載されています。vSphere エンドポイントを使用して OVF テンプレートから仮想マシンを展開する場合、エンドポイントに関連付けられている vCenter Server で、認証情報に vSphere 権限 VApp.Import が含まれていることを確認します。

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 5-11. 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
vApp		インポート
		vApp アプリケーションの設定
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

表 5-11. 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
設定	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
	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
	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）
プロビジョニング	設定
	スワップファイルの配置
	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
状態	カスタム仕様 の読み取り
	スナップショットの作成

表 5-11. 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
	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。vRealize Automation 管理インターフェイスにポート 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 (<i>mgr-svc-load-balancer.mycompany.com:443</i>) 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 (<i>mgr-svc.mycompany.com:443</i>) 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 (<i>web-load-balancer.mycompany.com:443</i>) 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 (<i>web.mycompany.com:443</i>) 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。vRealize Automation 管理インターフェイスにポート 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 (<code>mgr-svc-load-balancer.mycompany.com:443</code>) 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 (<code>mgr-svc.mycompany.com:443</code>) 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 (<code>web-load-balancer.mycompany.com:443</code>) 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 (<code>web.mycompany.com:443</code>) 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。

```
DynamicOps.Vrm.VRMencrypt.exe VRMAgent.exe.config set username jsmith
DynamicOps.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する必要があります。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。vRealize Automation 管理インターフェイスにポート 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 (<i>mgr-svc-load-balancer.mycompany.com:443</i>) 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 (<i>mgr-svc.mycompany.com:443</i>) 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 (<i>web-load-balancer.mycompany.com:443</i>) 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 (<i>web.mycompany.com:443</i>) 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。vRealize Automation 管理インターフェイスにポート 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 (<i>mgr-svc-load-balancer.mycompany.com:443</i>) 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 (<i>mgr-svc.mycompany.com:443</i>) 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 (<i>web-load-balancer.mycompany.com:443</i>) 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 (<i>web.mycompany.com:443</i>) 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 5-12. 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	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。 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。 <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。vRealize Automation 管理インターフェイスにポート 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 (<i>mgr-svc-load-balancer.mycompany.com:443</i>) 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 (<i>mgr-svc.mycompany.com:443</i>) 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 (<i>web-load-balancer.mycompany.com:443</i>) 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 (<i>web.mycompany.com:443</i>) 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。vRealize Automation 管理インターフェイスにポート 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 (<i>mgr-svc-load-balancer.mycompany.com:443</i>) 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 (<i>mgr-svc.mycompany.com:443</i>) 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 (<i>web-load-balancer.mycompany.com:443</i>) 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 (<i>web.mycompany.com:443</i>) 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

6

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。

この章には、次のトピックが含まれています。

- [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 インストールの実行](#)
- [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](#)
- [vRealize Automation サイレント インストール用の応答ファイル](#)
- [vRealize Automation インストール コマンド ライン](#)
- [vRealize Automation のインストール API](#)
- [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 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する方法と、[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。
- 4 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。
- 5 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。
- 6 (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。追加する必要が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
```

結果

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

7

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。

この章には、次のトピックが含まれています。

- [vRealize Automation タイム ゾーンを変更しない](#)
- [連邦情報処理規格準拠の暗号化の設定](#)
- [Manager Service の自動フェイルオーバーの有効化](#)
- [vRealize Automation PostgreSQL データベースの自動フェイルオーバー](#)
- [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](#)
- [ホスト名と IP アドレスの変更](#)
- [vRealize Automation アプライアンス ノードの削除](#)
- [IaaS サーバ上での vRealize Log Insight エージェントのインストール](#)
- [VMware Remote Console プロキシ ポートの変更](#)
- [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](#)
- [SQL AlwaysOn 可用性グループの構成](#)
- [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](#)
- [スタティック ルートの設定](#)
- [パッチ管理へのアクセス](#)
- [デフォルト テナントへのアクセスの構成](#)

vRealize Automation タイム ゾーンを変更しない

vRealize Automation アプライアンス管理インターフェイスにはタイム ゾーンを変更するオプションが提供されていますが、vRealize Automation のタイム ゾーンは常に Etc/UTC に設定しておきます。

Etc/UTC 以外のタイム ゾーンを使用すると、移行が失敗したり、ログ バンドルにすべての vRealize Automation ノードからのエントリが含まれなかったりするなど、異常なエラーが発生することが知られています。

設定しないようにする必要がある vRealize Automation アプライアンス管理インターフェイス オプションは、[システム] - [タイム ゾーン] にあります。

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] - [ホストの設定] の順にクリックします。

- 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。

結果

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。

マルチノード構成では、いずれかの vRealize Automation アプライアンス ノードで手順を 1 回のみ実行します。

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
```

結果

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 laaS 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 laaS 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 laaS 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。laaS 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、「vRealize Automation 7.1 または 7.2 から 7.3 へのアップグレード」を参照してください。

Manager Service ホストのロード バランシング方法の詳細については、[vRealize Automation のロード バランシング](#)を参照してください。

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。
- データベース レプリケーションが vRealize Automation 管理インターフェイスの [クラスタ] タブで [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。

手動フェイルオーバーを実行する方法については、『vRealize Automation の管理』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。

証明書のアップデートの詳細については、vRealize Automation の管理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、「vRealize Automation の管理」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。

結果

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。

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。
 - データベース接続のステータス : [クラスタ]
 - RabbitMQ のステータス : [vRA] > [メッセージング]
 - Xenon のステータス : [vRA] > [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。

IaaS 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 IaaS Windows サーバに別のホスト名を割り当てて必要が生じる場合があります。

手順

- 1 IaaS サーバのスナップショットを作成します。
- 2 IaaS 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 IaaS 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 IaaS 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。
証明書の更新の詳細については、「vRealize Automation の管理」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 IaaS 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 7-1. 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	<i>install-folder\Server\Website</i>	Web.config
	<i>install-folder\Server\Website\Cafe</i>	Vcac-Config.exe.config
	<i>install-folder\Web API</i>	Web.config
	<i>install-folder\Web API\ConfigTool</i>	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	<i>install-folder\Server\Model Manager Data</i>	Repoutil.exe.config
	<i>install-folder\Server\Model Manager Data\Cafe</i>	Vcac-Config.exe.config
Manager Service ノード	<i>install-folder\Server</i>	ManagerService.exe.config
DEM オーケストレータ ノード	<i>install-folder\Distributed Execution Manager\dem</i>	DynamicOps.DEM.exe.config
DEM ワーカー ノード	<i>install-folder\Distributed Execution Manager\DEM-name</i>	DynamicOps.DEM.exe.config
エージェント ノード	<i>install-folder\Agents\agent-name</i>	RepoUtil.exe.config
	<i>install-folder\Agents\agent-name</i>	VRMAgent.exe.config

表 7-2. 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	<i>install-folder\Distributed Execution Manager\DEM-name</i>	DynamicOps.DEM.exe.config
DEM ワーカー ノード	<i>install-folder\Distributed Execution Manager\dem</i>	DynamicOps.DEM.exe.config
エージェント ノード	<i>install-folder\Agents\agent-name</i>	VRMAgent.exe.config

表 7-3. 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	<i>install-folder\Agents\agent-name</i>	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] - [ホストの設定] の [ホスト名] を選択した CNAME に変更します。

vRealize Automation アプライアンス ノードの削除

HA 環境を維持するときは、失敗した vRealize Automation アプライアンス ノードをクラスタから削除する必要があります。

ノードを削除するには、[VMware ナレッジベースの記事 KB2149866](#) のガイドラインを実行します。

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 Agent 管理ガイド』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。

結果

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。
『vRealize Automation の構成』を参照してください。
- 2 高可用性環境の場合は、『vRealize Automation の構成』で説明されている、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] > [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 [クラスタ] 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 Postgres 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 7-4. 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。

問題はリアルタイムで発生する可能性があるため、パッチ、前提条件、インストール手順は [VMware のナレッジベース](#) でリリースされています。たとえば、[VMware ナレッジベースの記事 70911](#) は、最新の vRealize Automation 7.6 パッチの情報をを使用して確認および更新されています。

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

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] - [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ー 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
```

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。『vRealize Automation の構成』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。『vRealize Automation の構成』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。

vRealize Automation インストール のトラブルシューティング

8

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。

この章には、次のトピックが含まれています。

- [失敗したインストールのロールバック](#)
- [vRealize Automation サポート バンドルの作成](#)
- [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](#)
- [IaaS コンポーネントのトラブルシューティング](#)
- [ログイン エラーのトラブルシューティング](#)

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。

結果

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。

結果

表 8-1. 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 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] - [ログ] 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。

結果

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。

コマンドライン: root として vRealize Automation アプライアンスのコマンドラインからサポート バンドルを生成するには、`vcac-support` または `vcac-config log-bundle` を実行します。

または、次の例に示すように `log-bundle` コマンド全体を実行することもできます。`vra-command` の実行に関する一般的な情報については、[vRealize Automation インストール コマンドラインの基礎](#)を参照してください。

```
# vra-command execute --node cafe.node.497772175.21500 log-bundle --requestor va-1.mycompany.com

Parent command with id='981e3028-c99b-5c92-1bae-7d2bf5b6aaaa' was created.
Waiting for all child commands to complete...
...
```

```

Command execution result:
Command id: 3d64d122-0af1-28dd-b5a5-d932b78b3678
  Type: log-bundle
  Node id: cafe.node.497772175.21500
  Node host: va-1.mycompany.com
  Result: The command was successfully executed.
  Result description: {"path": "/opt/vmware/var/support-bundle/log/
va-1.mycompany.com_cafe.node.497772175.21500-VA.zip"}

Status: COMPLETED

```

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。

解決方法

- 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。

解決方法

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。

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）。

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。

解決方法

- 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。

解決方法

- 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。

解決方法

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。

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。

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。

解決方法

- 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。

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。

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。

解決方法

- 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。

解決方法

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。

解決方法

- 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。

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。

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。

解決方法

- 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。

解決方法

- 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インターフェイスを使用して、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、その管理インターフェイスの [クラスター] 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インターフェイス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。

解決方法

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 バランサー 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インターフェイスを開きます。[クラスター] 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 バランサー 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、その管理インターフェイス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。

解決方法

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。
- SQL サービスが実行されていない可能性があります。

解決方法

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。

解決方法

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。

解決方法

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。

解決方法

- 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と、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。

解決方法

- 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
```

laaS コンポーネントのトラブルシューティング

vRealize Automation laaS 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。

分散トランザクション コーディネータの接続が拒否される

Microsoft リモート プロシージャ コール (RPC) の設定が vRealize Automation の分散トランザクション コーディネータ (DTC) に影響を与える可能性があります。

問題

laaS Windows サーバまたは vRealize Automation SQL データベース サーバの間の DTC 接続が拒否されていることを示すエラーが発生します。

原因

RPC 接続設定によってアクセスが制限されているため、これを無効にする必要があります。

解決方法

すべての IaaS Windows サーバおよび vRealize Automation SQL データベース サーバで、次のレジストリ キーを削除するかゼロに設定します。

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\RPC\RestrictRemoteClients

IaaS サーバが切断されていると表示される

Windows のパフォーマンス カウンタの問題により、IaaS サーバが切断状態であると報告されることがあります。

問題

管理エージェントをインストールまたはアップグレードすると、IaaS サーバは、vRealize Automation アプライアンスに ping を送信します。この問題は、ping が失敗した場合に発生し、[vRealize Automation アプライアンス管理インターフェイス クラスタ] タブの IaaS サーバのステータスに未接続であると示されます。

IaaS サーバの管理エージェントの All.log ファイルに、次のようなエラーが記録されます。

```
[UTC:2019-05-25 16:09:37 Local:2019-05-25 18:09:37] [Error]: [sub-thread-Id="4" context="" token=""]
System.InvalidOperationException: Category does not exist.
at System.Diagnostics.PerformanceCounterLib.CounterExists(String machine, String category, String
counter)
at System.Diagnostics.PerformanceCounter.InitializeImpl()
at System.Diagnostics.PerformanceCounter.NextSample()
at System.Diagnostics.PerformanceCounter.NextValue()
at VMware.IaaS.Component.Metrics.MetricsUtility.CalculateMachineProcessorMeasure(Int32
samplePeriodMilliseconds)
at VMware.IaaS.Management.Agent.ManagementEndpointService.CollectEnvironmentInfo()
at VMware.IaaS.Management.Agent.ManagementEndpointService.<PingAsync>d__0.MoveNext()
--- End of stack trace from previous location where exception was thrown ---
at System.Runtime.CompilerServices.TaskAwaiter.ThrowForNonSuccess(Task task)
at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
at System.Runtime.CompilerServices.ConfiguredTaskAwaitable`1.ConfiguredTaskAwaiter.GetResult()
at VMware.IaaS.Management.Agent.ManagementAgent.<<PingManagementEndpointAsync>b__1f>d__23.MoveNext()
--- End of stack trace from previous location where exception was thrown ---
at System.Runtime.CompilerServices.TaskAwaiter.ThrowForNonSuccess(Task task)
at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
at VMware.IaaS.Management.Agent.ManagementAgent.<ExecutePeriodicAction>d__8.MoveNext()
```

原因

Windows のパフォーマンス カウンタは、時間の経過とともに破損し、エラーが発生するという既知の問題があります。

解決方法

拡張可能カウンタやサードパーティ カウンタなど、すべてのパフォーマンス カウンタを再構築します。

- 1 IaaS サーバで、管理者としてコマンド プロンプトを開きます。
- 2 以下のコマンドを使用して、カウンタを再構築します。

```
cd C:\Windows\system32
```



```
lodctr /R

cd C:\Windows\sysWOW64

lodctr /R
```

- 3 以下のコマンドで、カウンタを Windows Management Instrumentation (WMI) と再同期します。

```
WINMGMT.EXE /RESYNCPERF
```

- 4 パフォーマンス ログと警告サービスを停止し、再起動します。
- 5 Windows Management Instrumentation サービスを停止し、再起動します。

次のステップ

上記の手順で問題が解決しない場合は、[Microsoft サポートの記事 300956](#) または [KB2554336](#) を参照してください。これらの記事では、関連するレジストリ レコードを手動でリセットする方法について説明されています。レジストリは、先にバックアップすることをお勧めします。

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。

解決方法

.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。

IaaS のサーバ証明書の検証

vcac-Config.exe コマンドを使用して、IaaS 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

IaaS 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

IaaS 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。

解決方法

- 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。

IaaS インストーラ実行時の認証情報エラー

IaaS 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

IaaS 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。

解決方法

- ◆ 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。

IaaS のインストール中に設定の保存の警告が表示される

IaaS 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

IaaS 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的確ではないエラー 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。

解決方法

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

IaaS 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

IaaS 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。

解決方法

- 1 IaaS 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。

IaaS Web と Model Management のインストール中に IaaS 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。

解決方法

- 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。

解決方法

◆ 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。

laaS 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

laaS 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 laaS 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。

解決方法

laaS 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、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。

解決方法

- 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 ログिंग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、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 ログ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。

解決方法

- 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。

解決方法

- 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] の順に移動します。

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。

- 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。

解決方法

- 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。

解決方法

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。

解決方法

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する必要があります。識別できないと、ログインすることができません。

高可用性 vRealize Automation アプライアンスのクラスター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。クラスター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。

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。

解決方法

- ◆ `/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。

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。

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
```

解決方法

- 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`