

# vRealize Automation の管理

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](http://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](http://www.vmware.com/jp)

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

# 目次

<b>1</b>	<b>vRealize Automation のコンポーネントおよびオプションの保守とカスタマイズ</b>	<b>5</b>
	すべてのユーザーへのメッセージのブロードキャスト	5
	メッセージ ボードの URL 許可リストの作成	7
	vRealize Automation の起動およびシャットダウン	8
	vRealize Automation の起動	8
	vRealize Automation の再起動	9
	vRealize Automation のシャットダウン	10
	vRealize Automation の証明書のアップデート	11
	証明書とプライベート キーの抽出	13
	vRealize Automation アプライアンスでの証明書の置き換え	13
	Infrastructure as a Service (IaaS) 証明書を置き換える	15
	IaaS Manager Service の証明書の置き換え	17
	vRealize Automation 証明書を信頼するように組み込みの vRealize Orchestrator を更新する	19
	vRealize Automation 証明書を信頼するように外部の vRealize Orchestrator を更新する	21
	vRealize Automation アプライアンス管理サイトの証明書のアップデート	22
	管理エージェントの証明書の置き換え	26
	証明書のポーリング方法の変更	29
	vRealize Automation Postgres アプライアンス データベースの管理	29
	アプライアンス データベースの構成	31
	3 台のノードのアプライアンス データベースによる自動フェイルオーバーのシナリオ	32
	シナリオ：アプライアンス データベースの手動フェイルオーバーの実行	35
	シナリオ：メンテナンス データベース フェイルオーバーの実行	36
	アプライアンス データベースの致命的な障害からの手動によるリカバリ	37
	vRealize Automation インストールのバックアップとリカバリ	39
	カスタマ エクスペリエンス改善プログラム	39
	vRealize Automation のカスタマ エクスペリエンス改善プログラムへの参加または離脱	39
	データ収集時刻の構成	40
	システム設定の調整	40
	サービス カタログの [すべてのサービス] アイコンの変更	40
	データのロールオーバー設定のカスタマイズ	42
	Manager Service 構成ファイルでの設定の調整	44
	vRealize Automation の監視	49
	ワークフローの監視とログの表示	49
	イベント ログとサービスの監視	50
	vRealize Automation 監査ログの使用	52
	分散インストール環境におけるクラスタのホスト情報の表示	53
	vRealize Automation の健全性の監視	55
	vRealize Automation のシステム テストの構成	56

vRealize Automation のテナント テストの構成	58
vRealize Orchestrator のテストの構成	60
カスタム テスト スイート	61
vRealize Automation 健全性サービスのテスト スイート結果の表示	63
健全性サービスのトラブルシューティング	64
SNMP を使用した vRealize Automation 環境リソースの監視	64
リソースの監視および管理	65
リソース監視シナリオの選択	65
リソース使用量の用語集	66
クラウド マシンへの接続	66
予約使用の自然減的な減少	69
ストレージ バスの廃止	69
データ収集	70
vCenter Server エンドポイントの vSwap 割り当てチェックについて	73
データセンターの場所の削除	74
コンテナの監視	74
仮想マシンのバルク インポート、アップデート、移行	75
vRealize Automation 環境への仮想マシンのインポート	75
vRealize Automation 環境の仮想マシンの更新	80
別の vRealize Automation 環境への仮想マシンの移行	82

# vRealize Automation のコンポーネントおよびオプションの保守とカスタマイズ

vRealize Automation の導入環境にプロビジョニングされたマシンとその他の要素を管理できます。

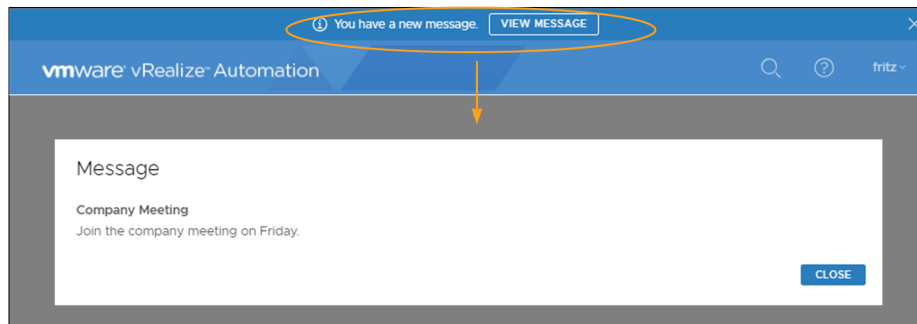
この章には、次のトピックが含まれています。

- [すべてのユーザーへのメッセージのブロードキャスト](#)
- [vRealize Automation の起動およびシャットダウン](#)
- [vRealize Automation の証明書のアップデート](#)
- [vRealize Automation Postgres アプライアンス データベースの管理](#)
- [vRealize Automation インストールのバックアップとリカバリ](#)
- [カスタム エクスペリエンス改善プログラム](#)
- [システム設定の調整](#)
- [vRealize Automation の監視](#)
- [vRealize Automation の健全性の監視](#)
- [SNMP を使用した vRealize Automation 環境リソースの監視](#)
- [リソースの監視および管理](#)
- [コンテナの監視](#)
- [仮想マシンのバルク インポート、アップデート、移行](#)

## すべてのユーザーへのメッセージのブロードキャスト

テナント管理者は、すべてのユーザーにメッセージをブロードキャストできます。ブラウザ ページの最上部にメッセージ通知が表示されます。ユーザーはこの通知をクリックして、メッセージを確認できます。

ユーザーは、バナーから、またはヘッダーにあるユーザー ドロップダウン メニューからメッセージにアクセスできます。



メッセージ ボードを使用して、テキスト メッセージまたは Web ページをブロードキャストします。Web ページによっては、ユーザーがメッセージ ボード内で Web サイトへのナビゲーションを行うことができます。

メッセージ ボードには、以下の制限があります。

表 1-1. メッセージ ボードの制限事項

オプション	制限事項
URL メッセージの制限	<ul style="list-style-type: none"> <li>■ ターゲット URL がメッセージ ボードの許可リストに含まれている必要があります。<a href="#">メッセージ ボードの URL 許可リストの作成</a>を参照してください。</li> <li>■ https サイトでホストされているコンテンツのみを公開できます。</li> <li>■ 自己署名証明書は使用できません。証明書を受理するオプションはメッセージ ボードに表示されません。</li> <li>■ メッセージ ボードの URL は iframe 内に埋め込まれています。一部の Web サイトは iframe で動作せず、エラーが発生します。このエラーの原因の 1 つは、ターゲット Web サイト上のヘッダーにある X-Frame-Options DENY または SAMEORIGIN です。ターゲット Web サイトを自分で管理している場合は、X-Frame-Options ヘッダーを X-Frame-Options: ALLOW-FROM <a href="#">https://&lt;vRealizeAutomationApplianceURL&gt;</a> に設定できます。</li> <li>■ Web サイトによっては、トップレベルのページにリダイレクトされ、vRealize Automation ページ全体が更新される場合があります。このタイプの Web サイトは、メッセージ ボードで動作しません。更新は抑制され、読み込み中というメッセージがメッセージ ボードに表示されます。</li> <li>■ 内部の HTML ページを表示する場合、そのページは vRealize Automation ホストを URL として保持することができません。</li> </ul>
カスタム メッセージの制限	<ul style="list-style-type: none"> <li>■ カスタム メッセージでは単純なマークアップは許可されますが、セキュリティ維持のため、HTML コードはサポートされません。たとえば、&lt;href&gt; を使用して Web サイトへのリンクを設定することはできません。URL メッセージ オプションを使用する必要があります。</li> </ul>

## 前提条件

テナント管理者として vRealize Automation にログインします。

## 手順

- 1 [管理] タブをクリックします。

- 2 [通知] - [メッセージ ボード] の順に選択します。
- 3 [タイプ] ドロップダウン メニューでメッセージのタイプを選択します。

オプション	説明
なし	メッセージ通知を削除します。
カスタム メッセージ	プレーン テキスト メッセージを入力します。
URL	<p>ページの URL を入力します。</p> <p>URL がメッセージ ボードの許可リストに含まれている必要があります。<a href="#">メッセージ ボードの URL 許可リストの作成</a>を参照してください。</p> <p>主に社内 Web サイトなどの Web サイトに、vRealize Automation ユーザー ID に基づいてユーザーをログインさせるには、[ユーザー ID を含める] を選択します。http://company.com/internal/message?userID=richard_dawson@company.com のような形式で URL が Web サイトに渡されます。この方法では、Web サイトで window.location.search JavaScript プロパティを使用することにより、現在のユーザーの ID を Web サイトに指定できます。</p>

- 4 [OK] をクリックします。

#### 結果

すべてのテナント ユーザーに、メッセージがバナーとして送信されます。

メッセージを変更または削除するには、テナント管理者としてログインする必要があります。メッセージを変更するには、同様の手順を繰り返します。メッセージを削除するには、[タイプ] で [なし] を選択し、[OK] をクリックします。

## メッセージ ボードの URL 許可リストの作成

セキュリティ管理者は、メッセージ ボードで使用可能な URL の許可リストを構成します。この許可リストにより、セキュリティの強化が確保されます。

#### 前提条件

セキュリティ管理者として vRealize Automation にログインします。

#### 手順

- 1 [管理] - [メッセージ ボードのホワイトリスト] の順に選択します。
- 2 [新規] をクリックします。
- 3 URL を追加し、[OK] をクリックします。

URL のエントリには、以下のコンテンツを含めることができます。

- IP アドレスまたはサイトの FQDN。例 : https://docs.vmware.com
- HTTPS を含めることができます。
- 許可されているポートを含めることができます。ポートが指定されていない場合、許可されているポートは 80 および 443 です。

- 4 以降の各エントリで繰り返します。

## 結果

このリストに含まれていない場合、テナント管理者はメッセージ ボードに URL を追加できません。

## 次のステップ

メッセージ ボードを使用することにより、許可リストに含まれている URL を追加してブロードキャストできることを確認します。[すべてのユーザーへのメッセージのブロードキャスト](#)を参照してください。

# vRealize Automation の起動およびシャットダウン

システム管理者は、システムとデータの整合性を維持するために vRealize Automation のシャットダウンまたは起動を管理します。

シャットダウンおよび起動を管理することで、初期起動の誤りによって発生するパフォーマンスまたは製品動作の問題を解決できます。一部のコンポーネントの展開が失敗した場合のみ、再起動手順を実行します。

## vRealize Automation の起動

予期した、または予期しない理由で vRealize Automation をパワーオフした後に起動する場合は、指定した順序でコンポーネントを起動する必要があります。

vCenter Server で展開コンポーネントを管理している場合は、そこからゲスト OS を起動できます。

## 前提条件

環境で使用されているロード バランサが実行されていることを確認します。

## 手順

- 1 スタンドアローンのレガシー PostgreSQL データベースを使用している場合は、このサーバを起動します。
- 2 任意の順序で、スタンドアローンの vRealize Automation MS SQL Server を起動します。
- 3 健全性チェックでロード バランサを使用する展開では、ping 以外のすべての健全性チェックを無効にします。
- 4 プライマリ vRealize Automation アプライアンスを起動します。
- 5 プライマリ vRealize Automation アプライアンス管理インターフェイスの [クラスタ] タブで、システムが同期モードか非同期モードかを確認します。シングルアプライアンスの展開は常に非同期です。
  - 展開が同期されている場合は、残りの vRealize Automation アプライアンスを起動します。
  - デプロイが非同期の場合は、プライマリ vRealize Automation アプライアンス管理インターフェイスに移動し、ライセンス サービスが実行されて登録されるまで待機します。

その後、残りの vRealize Automation アプライアンスを起動します。
- 6 すべてのアプライアンスが起動したら、管理インターフェイスを使用して、サービスが実行中で登録されていることを確認します。

アプライアンスが起動するには、15 分以上かかる場合があります。

- 7 すべての IaaS Web ノードを起動して、5 分間待機します。
- 8 プライマリ Manager Service ノードを起動し、2 ～ 5 分間待機します。



- 9 複数の Manager Service ノードがある分散展開では、セカンダリ Manager Service ノードを起動し、2 ～ 5 分間待機します。

セカンダリ マシンでは、Manager Service 自動フェイルオーバーが設定されている場合を除いて、Windows サービスを起動または実行しないでください。

- 10 任意の順序で、DEM オーケストレータ、DEM ワーカー、およびすべての vRealize Automation プロキシ エージェントを起動します。

他の起動タスクを開始する前に、起動タスクが完了するまで待つ必要はありません。

- 11 ロード バランサの健全性チェックを無効にする必要があった場合は、それらを再度有効にします。

- 12 起動したサービスが実行中であり登録済みであることを確認します。

- a ブラウザで、プライマリ vRealize Automation 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。

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

- b [サービス] タブをクリックします。

- c [更新] 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

すべてのサービスが登録されると、展開の準備が完了します。

## vRealize Automation の再起動

vRealize Automation コンポーネントを再起動すると、問題の解決に役立つ可能性があります。指定された順序でコンポーネントを再起動する必要があります。

vCenter Server で展開コンポーネントを管理している場合は、そこからゲスト OS を再起動できます。

再起動が実行できない場合は、代わりに [vRealize Automation のシャットダウン](#) および [vRealize Automation の起動](#) の手順を実行してください。

## 前提条件

- 環境で使用されているすべてのロード バランサが実行されていることを確認します。

## 手順

- 1 vRealize Automation アプライアンス データベースが非同期モードに設定されていることを確認します。必要に応じて、管理インターフェイスを使用して非同期モードに変更します。

手順全体を完了した後に、同期モードに戻れます。詳細については、[vRealize Automation Postgres アプライアンス データベースの管理](#) を参照してください。

- 2 プライマリ vRealize Automation アプライアンスを再起動し、起動が完了するまで待機します。
- 3 プライマリ vRealize Automation アプライアンス管理インターフェイスを使用して、ライセンス サービスが実行中で、登録されていることを確認します。
- 4 残りの vRealize Automation アプライアンスを同時に再起動します。

- 5 アプライアンスが再起動するまで待機し、それらの管理インターフェイスを使用してサービスが実行中で登録されていることを確認します。

アプライアンスが再起動するには、15 分以上かかる場合があります。

- 6 プライマリ Web ノードを再起動し、起動が完了するまで待機します。
- 7 複数の Web ノードを使用する分散型展開を実行している場合は、セカンダリ Web ノードを再起動し、起動が完了するまで待機します。
- 8 Manager Service ノードを再起動し、起動が完了するまで待機します。

Manager Service の自動フェイルオーバーを実行しており、アクティブ ノードとパッシブ ノードを同じ状態で維持するには、次の順序で再起動します。

- a Manager Service パッシブ ノードを再起動せずに停止します。
- b Manager Service アクティブ ノードを完全に再起動します。
- c Manager Service パッシブ ノードを起動します。

- 9 任意の順序で、DEM オーケストレータ、DEM ワーカー、およびすべての vRealize Automation プロキシ エージェントを再起動します。すべての起動が終了するのを待ちます。

他の再起動タスクを開始する前に、再起動タスクが完了するまで待つ必要はありません。

- 10 再起動したサービスが実行中であり登録済みであることを確認します。
  - a ブラウザで、プライマリ vRealize Automation 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。  
<https://vrealize-automation-appliance-FQDN:5480>
  - b [サービス] タブをクリックします。
  - c [更新] 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

すべてのサービスが登録されると、展開の準備が完了します。

## vRealize Automation のシャットダウン

データの整合性を維持するには、指定された順序で vRealize Automation をシャットダウンする必要があります。

vCenter Server で展開コンポーネントを管理している場合は、そこからゲスト OS をシャットダウンできます。

## 手順

- 1 任意の順序で、DEM オーケストレータ、DEM ワーカー、およびすべての vRealize Automation プロキシ エージェントをシャットダウンします。シャットダウンが完了するまで待機します。
- 2 Manager Service ノードをシャットダウンし、シャットダウンが完了するまで待機します。
- 3 複数の Web ノードがある分散展開では、セカンダリ Web ノードをシャットダウンし、シャットダウンが完了するまで待機します。
- 4 プライマリ Web ノードをシャットダウンし、シャットダウンが完了するまで待機します。

- 5 同期モードの複数の vRealize Automation アプライアンスがある分散展開では、vRealize Automation アプライアンス管理インターフェイスを使用して非同期モードに変更します。
- 6 複数の vRealize Automation アプライアンスがある分散展開では、セカンダリ アプライアンスをシャットダウンし、シャットダウンが完了するまで待機します。
- 7 プライマリ vRealize Automation アプライアンスをシャットダウンし、シャットダウンが完了するまで待機します。  
  
プライマリ vRealize Automation アプライアンスには、プライマリまたは書き込み可能なアプライアンスデータベースが含まれます。正しい順序でバックアップを開始できるように、どのアプライアンスがプライマリであるかを書き留めておきます。
- 8 任意の順序で、任意のスタンドアローンの vRealize Automation MS SQL サーバをシャットダウンし、シャットダウンが完了するまで待機します。
- 9 スタンドアローンのレガシー PostgreSQL データベースを使用している場合は、このサーバをシャットダウンします。

## vRealize Automation の証明書のアップデート

システム管理者は、vRealize Automation コンポーネントの証明書をアップデートするか、置き換えることができます。

vRealize Automation には主要なコンポーネントが 3 つあります。これらのコンポーネントでは、相互に安全に通信できるように SSL 証明書を使用します。

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

さらに、vRealize Automation アプライアンス 管理インターフェイス Web サイトの証明書を環境に追加できます。また、各 IaaS マシンでは、証明書を使用する管理エージェントが実行されます。

**注：** vRealize Automation は、さまざまな機能をサポートするために、Rabbit MQ などの複数のサードパーティ製品を使用します。これらの製品の一部は、プライマリ vRealize Automation 証明書を認証局 (CA) から提供された証明書に置き換えても、自己署名の証明書を使用します。そのため、ユーザーは RabbitMQ によって内部通信に使用される 5671 などの特定のポートで、証明書の使用を実質的に制御できません。

1 つの例外を除いて、このリストのうち後コンポーネントを変更しても、そのコンポーネントより前のコンポーネントが影響を受けることはありません。例外として、IaaS コンポーネントの証明書をアップデートする場合は vRealize Automation アプライアンスに登録する必要があります。

通常は、製品のインストール時に自己署名証明書が生成され、これらのコンポーネントに適用されます。自己署名証明書から認証局が提供する証明書に切り替えるとき、または証明書の有効期限が切れたときには、証明書の置き換えが必要になる場合があります。vRealize Automation コンポーネントの証明書を置き換えると、他の vRealize Automation コンポーネントとの信頼関係が自動的にアップデートされます。

たとえば、vRealize Automation アプライアンス のインスタンスが複数存在する分散型システムでは、ある vRealize Automation アプライアンス の証明書をアップデートすると、関連する他のすべての証明書が自動的にアップデートされます。

**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。

vRealize Automation アプライアンス管理インターフェイスには、証明書を更新または置き換えるオプションが用意されています。

クラスタ環境では、プライマリ ノード インターフェイスから変更する必要があります。

- [証明書を生成] — vRealize Automation で自己署名証明書を生成します。
- [証明書をインポート] — 独自の証明書を使用します。
- [証明書サムプリントを付与] — IaaS Windows サーバの証明書ストアの証明書がすでに使用されている証明書サムプリントを付与します。

このオプションを指定しても、証明書は vRealize Automation アプライアンスから IaaS Windows サーバに転送されません。このオプションを指定すると、ユーザーは、vRealize Automation アプライアンス管理インターフェイスに証明書をアップロードせずに、IaaS Windows サーバ上にある既存の証明書を展開できます。

- [既存を保持] — 現在の証明書を引き続き使用します。

vRealize Automation アプライアンス管理インターフェイス Web サイトの証明書には、登録要件はありません。

**注：** 証明書で暗号化用のパスフレーズを使用している場合は、アプライアンス上の証明書を置き換えるときに、そのパスフレーズを入力しないと、証明書の置き換えに失敗し、「Unable to load private key」というメッセージが表示されます。

## 仮想マシン テンプレート

vRealize Automation アプライアンスまたは IaaS Windows サーバの証明書を変更した後、vRealize Automation でテンプレートを再び使用できるように、仮想マシン テンプレートの vRealize Automation ゲスト エージェントおよびソフトウェア エージェントを更新する必要があります。エージェントを更新しないと、ソフトウェア コンポーネントに関する展開要求が次の例のようなエラーで失敗します。

```
The following component requests failed: Linux. Request failed: Machine VM-001:
InstallSoftwareWorkflow. Install software work item timeout.
```

## vRealize Orchestrator

vRealize Automation 証明書を変更した後、vRealize Orchestrator を更新して、新しい証明書を信頼する必要があります。

vRealize Automation 環境に関連付けられている vRealize Orchestrator コンポーネントには、独自の証明書があり、vRealize Automation 証明書も信頼する必要があります。デフォルトで、vRealize Orchestrator コンポーネントは vRealize Automation に組み込まれていますが、外部の vRealize Orchestrator を使用することもできます。いずれの場合も、vRealize Orchestrator 証明書の更新については、vRealize Orchestrator のドキュメントを参照してください。

ロード バランサの背後でマルチノードの vRealize Orchestrator を展開している場合、すべての vRealize Orchestrator ノードで同じ証明書を使用する必要があります。

## 詳細

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関しては、[VMware ナレッジベースの記事 KB 2106583](#) を参照してください。

## 証明書とプライベート キーの抽出

仮想アプライアンスとともに使用する証明書は PEM ファイル形式である必要があります。

次の表の例では、GNU の `openssl` コマンドを使用して仮想アプライアンスの構成に必要な証明書情報を抽出します。

表 1-2. サンプルの証明書値とコマンド (openssl)

認証局が提供する証明書	コマンド	仮想アプライアンスのエントリ
RSA プライベート キー	<code>openssl pkcs12 -in <i>path_to_.pfx</i> <i>certificate_file</i> -nocerts -out key.pem</code>	[RSA プライベート キー]
PEM ファイル	<code>openssl pkcs12 -in <i>path_to_.pfx</i> <i>certificate_file</i> -clcerts -nokeys -out cert.pem</code>	[証明書チェーン]
(オプション) パス フレーズ	なし	[パス フレーズ]

## vRealize Automation アプライアンスでの証明書の置き換え

システム管理者は、自己署名証明書を認証局の信頼性のある証明書に更新するまたは置き換えることができます。信頼性の要件を満たす限り、SAN (Subject Alternative Name) 証明書、ワイルドカード証明書、または使用している環境に適した多目的証明書の他の方法を使用できます。

vRealize Automation アプライアンスの証明書を更新するまたは置き換えるときに、他の関連コンポーネントとの信頼も自動的に再初期化されます。証明書の更新の詳細については、[vRealize Automation の証明書のアップデート](#) を参照してください。

### 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] - [証明書] の順に選択します。
- 3 証明書を更新する vRealize Automation コンポーネントを選択します。

#### 4 [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	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>d <b>JP</b> 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。</li> </ul>
署名リクエストを生成	<ul style="list-style-type: none"> <li>a [署名リクエストを生成] を選択します。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>
インポート	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul> <p><b>注：</b> チェーン証明書の場合は、追加の属性が使用可能になることがあります。</p> <ul style="list-style-type: none"> <li>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。</li> </ul>

## 5 [設定の保存] をクリックします。

vRealize Automation アプライアンスの証明書を更新するには、vRealize Automation サービスを正常に再起動する必要があります。環境内の vRealize Automation アプライアンスの数によっては、再起動に 15 分から 1 時間かかることがあります。

再起動すると、vRealize Automation アプライアンスの該当インスタンスすべての証明書の詳細がページ上に表示されます。

## 6 ネットワークまたはロード バランサで証明書を必要とする場合は、インポートした証明書または新しく作成した証明書を仮想アプライアンスのロード バランサにコピーします。

証明書をエクスポートするために、root による SSH アクセスの有効化が必要な場合があります。

a まだログインしていない場合は、vRealize Automation アプライアンスの管理コンソールに root ユーザーとしてログインします。

b [管理者] タブをクリックします。

c [管理者] サブメニューをクリックします。

d [SSH サービス有効] チェック ボックスを選択します。

終了時に SSH を無効にするには、このチェック ボックスを選択解除します。

e [管理者の SSH ログイン] チェック ボックスを選択します。

終了時に SSH を無効にするには、このチェック ボックスを選択解除します。

f [設定の保存] をクリックします。

## 7 vRealize Automation コンソールにログインできることを確認します。

a ブラウザを開いて、<https://vcac-hostname.domain.name/vcac> に移動します。

ロード バランサを使用している場合、ホスト名はロード バランサの完全修飾ドメイン名である必要があります。

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、[ディレクトリ管理] 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。

コンソールで、[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。

## 8 ロード バランサを使用している場合は、該当する健全性チェックを構成して有効にします。

### 結果

証明書がアップデートされます。

## Infrastructure as a Service (IaaS) 証明書を置き換える

分散導入環境のセキュリティを確保するために、システム管理者は有効期限が切れた証明書または自己署名証明書を認証局から取得した証明書に置き換えることができます。



SAN (Subject Alternative Name) 証明書は、複数のマシンで使用できます。IaaS コンポーネント (Website および Manager Service) 用の証明書を発行するときは、SAN 値 (対応するコンポーネントがインストールされるすべての Windows ホストの完全修飾ドメイン名) と、同じその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を指定する必要があります。

#### 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] - [証明書] の順に選択します。
- 3 [コンポーネント タイプ] メニューの [IaaS Web] をクリックします。
- 4 [IaaS Web 証明書] ペインに移動します。
- 5 [証明書のアクション] メニューから証明書置き換えオプ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。

**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	説明
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"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ol>



オプション	説明
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><b>注：</b> 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>
証明書サムプリントを付与	このオプションは、IaaS サーバの証明書ストアにすでに展開されている証明書を使用するために、証明書サムプリントを提供する場合に使用します。このオプションを指定しても、証明書は仮想アプライアンスから IaaS サーバに転送されません。そのため、ユーザーは管理インターフェイスでアップロードしなくても既存の証明書を IaaS サーバに展開できます。

## 6 [設定の保存] をクリックします。

IaaS Windows サーバ証明書を更新するには、vRealize Automation サービスを正常に再起動する必要があります。環境内の vRealize Automation アプライアンスの数によっては、再起動に 15 分から 1 時間かかることがあります。

再起動すると、証明書の詳細がページ上に表示されます。

## IaaS Manager Service の証明書の置き換え

分散導入環境のセキュリティを確保するために、システム管理者は有効期限が切れた証明書または自己署名証明書を認証局から取得した証明書に置き換えることができます。

SAN (Subject Alternative Name) 証明書は、複数のマシンで使用できます。IaaS コンポーネント (Website および Manager Service) 用の証明書を発行するときは、SAN 値 (対応するコンポーネントがインストールされるすべての Windows ホストの完全修飾ドメイン名) と、同じその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を指定する必要があります。

IaaS Manager Service と IaaS Web サービスは、1 つの証明書を共有します。

### 手順

- 1 Web ブラウザを開き、vRealize Automation アプライアンス管理インターフェイス URL にアクセスします。
- 2 vRealize Automation アプライアンス をデプロイしているときに、指定したユーザー名 **root** とパスワードを使用してログインします。
- 3 [vRA] - [証明書] の順に選択します。
- 4 [コンポーネント タイプ] メニューの [Manager Service] をクリックします。
- 5 [証明書のアクション] メニューから証明書タイプを選択します。

分散環境などにおいて PEM でエンコードされた証明書を使用している場合は、[インポート] を選択します。

インポートする証明書は、信頼されており、SAN (Subject Alternative Name) 証明書を使用することによって vRealize Automation アプライアンスおよび任意のロード バランサのすべてのインスタンスに適用可能である必要があります。

**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	説明
既存を保持	現在の SSL 設定のままにします。このオプションを選択して変更をキャンセルします。
証明書の生成	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>d <b>JP</b> 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。</li> </ul>
インポート	<ul style="list-style-type: none"> <li>a ヘッダおよびフッタを含む証明書を 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。</li> <li>b ヘッダおよびフッタを含む証明書を 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、各証明書を BEGIN CERTIFICATE ヘッダと END CERTIFICATE フッタを含めます。</li> </ul> <p><b>注：</b> チェーン証明書の場合は、追加の属性が使用可能になることがあります。</p> <ul style="list-style-type: none"> <li>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。</li> </ul>
証明書サムプリントを付与	このオプションは、IaaS サーバの証明書ストアにすでに展開されている証明書を使用するために、証明書サムプリントを提供する場合に使用します。このオプションを指定しても、証明書は仮想アプライアンスから IaaS サーバに転送されません。そのため、ユーザーは管理インターフェイスでアップロードしなくても既存の証明書を IaaS サーバに展開できます。

- 6 [設定の保存] をクリックします。

数分後に、証明書の詳細がページに表示されます。

- 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ロード バランサにコピーします。
- 8 DEM ワーカーまたはエージェントを実行中のサーバから、ブラウザを開いて <https://managerServiceAddress/vmpsProvision/> に移動します。  
ロード バランサを使用している場合、ホスト名はロード バランサの完全修飾ドメイン名である必要があります。
- 9 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。
- 10 新しい証明書が提供され、信頼されていることを確認します。
- 11 ロード バランサを使用している場合は、該当する健全性チェックを構成して有効にします。

## vRealize Automation 証明書を信頼するように組み込みの vRealize Orchestrator を更新する

vRealize Automation アプライアンス 証明書または IaaS 証明書を更新または変更する場合は、vRealize Orchestrator を更新して、新しい、または更新された証明書を信頼する必要があります。

この手順は、組み込みの vRealize Orchestrator インスタンスを使用しているすべての vRealize Automation 展開に適用されます。外部の vRealize Orchestrator インスタンスを使用する場合は、[vRealize Automation 証明書を信頼するように外部の vRealize Orchestrator を更新する](#)を参照してください。

**注：** この手順では、テナントとグループの認証がデフォルトの設定にリセットされます。認証の設定がカスタマイズされている場合は、手順の完了後に認証を再設定できるよう、変更内容をメモしてください。

vRealize Orchestrator 証明書の更新および置き換えについては、vRealize Orchestrator のドキュメントを参照してください。

クラスタ化構成では、プライマリ vRealize Automation アプライアンス ノード上でこの手順を実行し、その後で各レプリカ vRealize Automation アプライアンス ノードからプライマリに対して `join-cluster` を実行する必要があります。

**注：** クラスタ内で不要なコントロール センターの自動同期が行われないようにするには、手順が完了するまで、すべてのレプリカ ノード上で `vco-configurator` サービスを停止します。

この手順を完了せずに vRealize Automation 証明書の置き換えまたは更新を行うと、vRealize Orchestrator コントロール センターにアクセスできなくなり、`vco-server` と `vco-configurator` のログ ファイルにエラーが表示される場合があります。

vRealize Automation とは異なるテナントとグループに対して認証するように vRealize Orchestrator が設定されている場合にも、証明書を更新する際に問題が発生することがあります。詳細については、VMware ナレッジベースの記事「[vRA 証明書を置換した後に「信頼できない証明書チェーン」の例外が発生する \(2147612\)](#)」を参照してください。

ここに示す `trust` コマンドの構文は、正式なものではなく、代表的な例です。これらの構文は最も一般的な展開に適していますが、状況によっては、さまざまなバリエーションのコマンドを試さなければならないことがあります。

- `--certificate` を指定する場合は、有効な証明書ファイルのパスを PEM 形式で指定する必要があります。
- `--uri` を指定する場合は、信頼されている証明書をコマンドで取得できる URI を指定する必要があります。
- `--registry-certificate` オプションを指定する場合は、要求されている証明書をコンポーネント レジストリの証明書として扱うように指定します。信頼されている証明書は、コンポーネント レジストリの証明書で 사용되는特定のエイリアスを使用してトラスト ストアに追加されます。

vRealize Orchestrator で SSL Trust Manager ワークフローを使用して証明書を管理することもできます。詳細については、[vRealize Orchestrator ドキュメント](#)の「Orchestrator 証明書の管理」を参照してください。

## 手順

- 1 vRealize Orchestrator サーバとコントロール センター サービスを停止します。

```
service vco-server stop
service vco-configurator stop
```

- 2 次のコマンドを実行して vRealize Orchestrator 認証プロバイダをリセットします。

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh reset-authentication
ls -l /etc/vco/app-server/
mv /etc/vco/app-server/vco-registration-id /etc/vco/app-server/vco-registration-id.old
vcac-vami vco-service-reconfigure
```

- 3 /var/lib/vco/tools/configuration-cli/bin にあるコマンド ライン インターフェイス ユーティリティを使用し、次のコマンドで vRealize Orchestrator トラスト ストアの信頼されている証明書をチェックします。

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh list-trust
```

- vco.cafe.component-registry.ssl.certificate というエイリアスを持つ証明書をチェックします。この証明書は、vRealize Orchestrator インスタンスが認証プロバイダとして使用する vRealize Automation 証明書である必要があります。
- また、新たに設定された vRealize Automation 証明書と一致する必要があります。一致しない場合は、次のように変更できます。
  - 1 vRealize Automation 署名アプライアンス証明書 PEM ファイルをアプライアンスの /tmp フォルダにコピーします。
  - 2 次のコマンドを実行して、適切な証明書のパスを追加します。

```
./vro-configure.sh trust --certificate path-to-the-certificate-file-in-PEM-format--registry-certificate
```

次のコマンドの例を参照してください。

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --certificate /var/tmp/test.pem --registry-certificate
```

- 4 証明書を信頼するために、次のコマンドを実行することが必要になる場合があります。

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --uri https://vra.domain.com

/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --registry-certificate --uri https://vra.domain.com
```

- 5 次のコマンドを使用して、vRealize Automation 証明書が vRealize Orchestrator トラスト ストアに挿入されたことを確認します。

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh list-trust
```

## 6 vRealize Orchestrator サーバとコントロール センター サービスを起動します。

```
service vco-server start
service vco-configurator start
```

### 次のステップ

クラスタ化されたシステムで信頼が更新されていることを検証できます。

1 仮想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。

2 [サービス] ページを選択します。

3 重複する vco サービスが表示されていないことを確認します。

vco サービスが重複して表示されている場合は、[登録解除] をクリックして、状態が Registered でないサービスを削除します。

4 すべての仮想アプライアンス ノードで vco-configurator が起動されていることを確認します。

5 vRealize Orchestrator コントロール センターにログインし、[構成の検証] ページに移動して構成を検証します。

6 [認証プロバイダ] ページに移動して、認証設定が正しいことを確認します。

このページでログイン認証情報をテストすることもできます。

## vRealize Automation 証明書を信頼するように外部の vRealize Orchestrator を更新する

vRealize Automation アプライアンス 証明書または IaaS 証明書を更新または変更する場合は、vRealize Orchestrator を更新して、新しい、または更新された証明書を信頼する必要があります。

この手順は、外部の vRealize Orchestrator インスタンスを使用している vRealize Automation 展開に適用されます。

**注：** この手順では、テナントとグループの認証がデフォルトの設定にリセットされます。認証の設定がカスタマイズされている場合は、手順の完了後に認証を再設定できるよう、変更内容をメモしてください。

vRealize Orchestrator 証明書の更新および置き換えについては、vRealize Orchestrator のドキュメントを参照してください。

この手順を完了せずに vRealize Automation 証明書の置き換えまたは更新を行うと、vRealize Orchestrator コントロール センターにアクセスできなくなり、vco-server と vco-configurator のログ ファイルにエラーが表示される場合があります。

vRealize Automation とは異なるテナントとグループに対して認証するように vRealize Orchestrator が設定されている場合にも、証明書を更新する際に問題が発生することがあります。詳細については、[ナレッジベースの記事 KB2147612](#) を参照してください。

**手順**

- 1 vRealize Orchestrator サーバとコントロール センター サービスを停止します。  
`service vco-configurator stop`
- 2 vRealize Orchestrator 認証プロバイダをリセットします。  
`/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh reset-authentication`
- 3 vRealize Orchestrator コントロール センター サービスを開始します。  
`service vco-configurator start`
- 4 仮想アプライアンス管理インターフェイスの root 認証情報を使用して、コントロール センターにログインします。
- 5 認証プロバイダを登録解除し、登録し直します。

**vRealize Automation アプライアンス管理サイトの証明書のアップデート**

システム管理者は、証明書の有効期限が切れたとき、または自己署名証明書を認証局によって発行された証明書で置き換えるために、管理サイト サービスの SSL 証明書を置き換えることができます。ポート 5480 の管理サイト サービスをセキュリティで保護します。

vRealize Automation アプライアンスは、自身の管理サイトに `lighttpd` を使用します。管理サイト証明書を置き換える際には、すべての管理エージェントもまた新しい証明書が認識されるように構成する必要があります。

分散展開環境の場合は、管理エージェントを自動または手動でアップデートできます。最小導入環境の場合は、管理エージェントを手動でアップデートする必要があります。

詳細については、[管理エージェントの手動アップデートによる証明書の認識](#) を参照してください。

**手順****1 管理エージェント ID の検索**

新しい管理サイトのサーバ証明書を作成および登録する際に管理エージェント ID を使用します。

**2 vRealize Automation アプライアンス管理サイトの証明書の置き換え**

管理サイト サービスの SSL 証明書の有効期限が切れた場合や、自己署名証明書でスタートしたものの、サイト ポリシーにより別の証明書が必要な場合には、証明書を置き換えることができます。

**3 管理エージェントのアップデートによる証明書の認識**

vRealize Automation アプライアンス管理サイトの証明書を置換した後、新規の証明書を認識するようにすべての管理エージェントをアップデートして、仮想アプライアンス管理サイトと IaaS ホスト上の管理エージェントの間の信頼性のある通信を再確立する必要があります。

**管理エージェント ID の検索**

新しい管理サイトのサーバ証明書を作成および登録する際に管理エージェント ID を使用します。

## 手順

- 1 `<Vra-installation-dir>\Management Agent\VMware.IaaS.Management.Agent.exe.config` にある管理エージェント構成ファイルを開きます。

- 2 agentConfiguration 要素の ID 属性の値を記録します。

```
<agentConfiguration id="0E22046B-9D71-4A2B-BB5D-70817F901B27">
```

## vRealize Automation アプライアンス管理サイトの証明書の置き換え

管理サイト サービスの SSL 証明書の有効期限が切れた場合や、自己署名証明書でスタートしたもの、サイト ポリシーにより別の証明書が必要な場合には、証明書を置き換えることができます。

ポート 443 の vRealize Automation サービスで使用されている証明書を再利用するか、別の証明書を使用することができます。新しい CA 発行の証明書を申請して既存の証明書を更新するためのベスト プラクティスは、既存の証明書の共通名を再利用することです。

**注：** vRealize Automation アプライアンスは、自身の管理サイトに `lighttpd` を使用します。ポート 5480 の管理サイト サービスをセキュリティで保護します。

## 前提条件

- 証明書は PEM 形式にする必要があります。
- 証明書には、以下の 2 つを以下の順で 1 つのファイルに含める必要があります。
  - a RSA プライベート キー
  - b 証明書チェーン
- プライベート キーは暗号化できません。
- デフォルトの場所とファイル名は、`/opt/vmware/etc/lighttpd/server.pem` です。

Java キーストアから PEM ファイルに証明書とプライベート キーをエクスポートする方法の詳細については、[証明書とプライベート キーの抽出](#)を参照してください。

## 手順

- 1 アプライアンスのコンソールまたは SSH を使用してログインします。
- 2 現在の証明書ファイルをバックアップします。

```
cp /opt/vmware/etc/lighttpd/server.pem /opt/vmware/etc/lighttpd/server.pem-bak
```

- 3 ファイル `/opt/vmware/etc/lighttpd/server.pem` の内容を新しい証明書情報で置換して、新しい証明書をアプライアンスにコピーします。
- 4 次のコマンドを実行し、`lighttpd` サーバを再起動します。

```
service vami-lighttp restart
```

- 5 次のコマンドを実行し、`haproxy` サービスを再起動します。

```
service haproxy restart
```



- 6 管理コンソールにログインし、証明書が置き換えられていることを確認します。ブラウザの再起動が必要となる場合があります。

#### 次のステップ

すべての管理エージェントをアップデートして、新しい証明書が認識されるようにします。

分散導入環境では、管理エージェントを手動または自動でアップデートできます。最小インストールの場合は、エージェントは手動にてアップデートする必要があります。

- 自動アップデートの詳細については、[分散環境での管理エージェントの自動アップデートによる vRealize Automation アプライアンス管理サイトの証明書の認識](#) を参照してください。
- 手動アップデートの詳細については、[管理エージェントの手動アップデートによる証明書の認識](#) を参照してください。

### 管理エージェントのアップデートによる証明書の認識

vRealize Automation アプライアンス管理サイトの証明書を置換した後、新規の証明書を認識するようにすべての管理エージェントをアップデートして、仮想アプライアンス管理サイトと IaaS ホスト上の管理エージェントの間の信頼性のある通信を再確立する必要があります。

各 IaaS ホストは管理エージェントを実行します。各管理エージェントはアップデートされている必要があります。最小インストール環境は手動でアップデートする必要があります。一方、分散インストール環境は手動でアップデートすることも、自動プロセスを使用してアップデートすることもできます。

#### ■ 管理エージェントの手動アップデートによる証明書の認識

vRealize Automation アプライアンス管理サイトの証明書を置換した後、新規の証明書を認識するように管理エージェントを手動でアップデートして、仮想アプライアンス管理サイトと IaaS ホスト上の管理エージェントの間の信頼性のある通信を再確立する必要があります。

#### ■ 分散環境での管理エージェントの自動アップデートによる vRealize Automation アプライアンス管理サイトの証明書の認識

高可用性構成の環境で管理サイトの証明書をアップデートしたら、新しい証明書を認識できるように管理エージェント構成をアップデートして、信頼性の高い通信を再度確立する必要があります。

#### 管理エージェントの手動アップデートによる証明書の認識

vRealize Automation アプライアンス管理サイトの証明書を置換した後、新規の証明書を認識するように管理エージェントを手動でアップデートして、仮想アプライアンス管理サイトと IaaS ホスト上の管理エージェントの間の信頼性のある通信を再確立する必要があります。

vRealize Automation アプライアンス管理サイトの証明書を置換した後、環境内の各管理エージェントで以下の手順を実行してください。

分散導入環境では、管理エージェントを手動アップデートまたは自動アップデートできます。自動アップデートの詳細については、[分散環境での管理エージェントの自動アップデートによる vRealize Automation アプライアンス管理サイトの証明書の認識](#) を参照してください。



## 前提条件

新規の vRealize Automation アプライアンス管理サイトの証明書の SHA1 サムプリントを取得しておく必要があります。

## 手順

- 1 VMware vCloud Automation Center 管理エージェントサービスを停止します。
- 2 管理エージェント構成ファイル [*vcac\_installation\_folder*]\Management Agent \VMware.IaaS.Management.Agent.exe.Config (場所は通常は、C:\Program Files (x86)\VMware \vCAC\Management Agent\VMware.IaaS.Management.Agent.exe.Config) に移動します。
- 3 構成ファイルを編集モードで開いて、古い管理サイトの証明書のエンドポイント設定 (エンドポイント アドレスで特定可能) を見つけます。

例：

```
<agentConfiguration id="C816CFBC-4830-4FD2-8951-C17429CEA291" pollingInterval="00:03:00">
  <managementEndpoints>
    <endpoint address="https://vra-va.local:5480"
thumbprint="D1542471C30A9CE694A512C5F0F19E45E6FA32E6" />
  </managementEndpoints>
</agentConfiguration>
```

- 4 サムプリントを新規証明書の SHA1 サムプリントに変更します。

例：

```
<agentConfiguration id="C816CFBC-4830-4FD2-8951-C17429CEA291" pollingInterval="00:03:00">
  <managementEndpoints>
    <endpoint address="https://vra-va.local:5480"
thumbprint="8598B073359BAE7597F04D988AD2F083259F1201" />
  </managementEndpoints>
</agentConfiguration>
```

- 5 VMware vCloud Automation Center 管理エージェント サービスを起動します。
- 6 仮想アプライアンス管理サイトにログインし、[クラスタ] タブを選択します。
- 7 [分散型展開の情報] テーブルで、IaaS サーバが最近仮想アプライアンスにアクセスしたことを確認します。これにより、アップデートが正常に終了したことを確認できます。

## 分散環境での管理エージェントの自動アップデートによる vRealize Automation アプライアンス管理サイトの証明書の認識

高可用性構成の環境で管理サイトの証明書をアップデートしたら、新しい証明書を認識できるように管理エージェント構成をアップデートして、信頼性の高い通信を再度確立する必要があります。

複数のシステムが分散している場合でも、vRealize Automation アプライアンス管理サイトの証明書情報は、手動または自動でアップデートできます。管理エージェントの手動アップデートの詳細については、[管理エージェントの手動アップデートによる証明書の認識](#) を参照してください。

証明書情報を自動でアップデートする手順は次のとおりです。

#### 手順

- 1 管理エージェントが実行されている場合は、環境内の 1 つの vRealize Automation アプライアンス管理サイト上で、証明書を置き換えます。
- 2 管理エージェントが新規の vRealize Automation アプライアンス管理サイト証明書と同期されるまで 15 分間待機します。
- 3 環境内の他の vRealize Automation アプライアンス管理サイトで、証明書を置き換えます。  
管理エージェントが、新しい証明書情報で自動的にアップデートされます。

## 管理エージェントの証明書の置き換え

システム管理者は、有効期限が切れた管理エージェントの証明書または自己署名証明書を、認証局が発行した証明書と置き換えることができます。

各 IaaS ホストは独自の管理エージェントを実行します。アップデートする管理エージェントの IaaS ノードごとに、この手順を繰り返します。

#### 前提条件

- レコードを削除する前に、ノード ID 列の管理エージェント ID をコピーします。この ID は、新しい管理エージェントの証明書を作成するときや、その証明書を登録するときに使用します。
- 新しい証明書を申請するときは、次の形式で、共通名 (CN) 属性が新しい証明書の証明書サブジェクト フィールドに入力されていることを確認してください。

```
VMware Management Agent 00000000-0000-0000-0000-000000000000
```

文字列 VMware Management Agent を入力し、その後にスペースを 1 つと、数値形式の管理エージェントの GUID を入力します。

#### 手順

- 1 Windows サービス スナップインから管理エージェント サービスを停止します。
  - a Windows マシンで、[スタート] をクリックします。
  - b Windows の [スタート] の [検索] ボックスに **services.msc** と入力して、Enter キーを押します。
  - c [VMware vCloud Automation Center Management Agent] サービスを右クリックし、[停止] をクリックしてサービスを停止します。

- 2 マシンから現在の証明書を削除します。Windows Server 2008 R2 で証明書を管理する方法の詳細については、<http://technet.microsoft.com/en-us/library/cc772354.aspx> の Microsoft のナレッジ ベースの記事か、<http://social.technet.microsoft.com/wiki/contents/articles/2167.how-to-use-the-certificates-console.aspx> の Microsoft の Wiki の記事を参照してください。
  - a コマンド **mmc.exe** を入力して、Microsoft 管理コンソールを開きます。
  - b Ctrl + M キーを押して、コンソールに新しいスナップインを追加するか、または [ファイル] ドロップダウンメニューからオプションを選択します。
  - c [証明書] を選択して [追加] をクリックします。
  - d [コンピュータ アカウント] を選択して [次へ] をクリックします。
  - e [ローカル コンピュータ : (このコンソールを実行しているコンピュータ)] を選択します。
  - f [OK] をクリックします。
  - g コンソールの左側にある [証明書 (ローカル コンピュータ)] を展開します。
  - h [個人] を展開して [証明書] フォルダを選択します。
  - i 現在の管理エージェントの証明書を選擇して [削除] をクリックします。
  - j [はい] をクリックして削除アクションを確定します。
- 3 新しく生成された証明書をローカルの `computer.personal` ストアにインポートします。ただし、システムで新しい自己署名証明書を自動生成する場合はインポートしないでください。

**4** vRealize Automation アプライアンス管理サイトに管理エージェントの証明書を登録します。

- a 管理者としてコマンド プロンプトを開き、管理エージェントがインストールされているマシンの Cafe ディレクトリ `<vra-installation-dir>\Management Agent\Tools\Cafe` (通常は `C:\Program Files (x86)\VMware\VCAC\Management Agent\Tools\Cafe`) に移動します。
- b 管理エージェント ID と証明書をワンステップで登録するオプションを付加して、`Vcac-Config.exe RegisterNode` コマンドを入力します。-nd オプションのための値として前に記録した管理エージェントの識別子を含めます。

表 1-3. Vcac-Config.exe RegisterNode の必須オプションと引数

[illegible]

次の例は、コマンドの形式を示したものです。

[illegible]

**5** 管理エージェントを再起動します。

例： 管理エージェントの証明書を登録するコマンド

```
Vcac-Config.exe RegisterNode -v -vamih "vra-va.eng.mycompany:5480" -cu "root" -cp
"secret" -hn "iaas.eng.mycompany" -nd "C816CFBX-4830-4FD2-8951-C17429CEA291" -tp
"70928851D5B72B206E4B1CF9F6ED953EE1103DED "
```

## 証明書のポーリング方法の変更

IaaS 証明書の OU（組織単位）セクションにコンマがある場合、Manager Service のログ ファイルに STOMP WebSocket エラーが記録されることがあります。また、仮想マシンのプロビジョニングが失敗することもあります。コンマを削除するか、ポーリング方法を WebSocket から HTTP に変更することができます。

ポーリング方法を変更するには、次の手順を実行します。

### 手順

- 1 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

- 2 <appSettings> セクション内に次の行を追加します。

```
<add key="Extensibility.Client.RetrievalMethod" value="Polling"/>
<add key="Extensibility.Client.PollingInterval" value="2000"/>
<add key="Extensibility.Client.PollingMaxEvents" value="128"/>
```

- 3 保存して Manager Service.exe.config を閉じます。

- 4 Manager Service を再起動します。

### 結果

Manager Service の詳細については、『vRealize Automation のインストール』を参照してください。

## vRealize Automation Postgres アプライアンス データベースの管理

vRealize Automation では、システムの運用にアプライアンス データベースが必要です。アプライアンス データベースは、vRealize Automation アプライアンス仮想アプライアンス管理インターフェイスによって管理できます。

---

**注：** この情報は、組み込みのアプライアンス データベースを使用している展開にのみ適用されます。外部の Postgres データベースを使用している展開には適用されません。

---

データベースは単一ノードとして構成することも、フェイルオーバーによる高可用性を実現しやすくするために複数ノードを使用して構成することもできます。vRealize Automation のインストーラでは、vRealize Automation アプライアンス のインストールごとにデータベース ノードが含まれます。そのため、vRealize Automation アプライアンス のインスタンスを 3 つインストールすると、3 台のデータベース ノードができます。自動フェイルオーバーは、適用可能な展開で実装されます。マシンの構成を変更しないかぎり、アプライアンス データベースのメンテナンスは不要です。クラスタ化構成を使用している場合、別のノードをプライマリに昇格します。

---

**注：** データベースのクラスタ化構成は、[クラスタに参加] 操作を使用して仮想アプライアンスをクラスタに参加させると自動的に設定されます。データベース クラスタは、仮想アプライアンスのクラスタに直接依存しているわけではありません。たとえば、クラスタに参加済みの仮想マシンは、組み込みのアプライアンス データベースが起動していなかったり、障害によって動作していなかったりする場合でも正常に動作できます。

---

vRealize Automation は、高可用性を実現するために、PostgreSQL のプライマリ レプリカ モデルを使用してデータのレプリケーションをサポートします。これは、すべてのデータベース ノードが、プライマリと呼ばれる 1 台のリーディング ノードと、レプリカと呼ばれる複数のレプリケーション ノードから構成されるクラスタ形式で動作することを意味します。プライマリ ノードは、すべてのデータベース要求を処理します。レプリカ ノードは、プライマリからのトランザクションをローカルでストリーミングおよび再生します。

クラスタ化構成には、1 台のプライマリ ノードと 1 台以上のレプリカ ノードが含まれています。プライマリ ノードとは、システム機能をサポートするプライマリ データベースを備えた vRealize Automation アプライアンス ノードです。レプリカ ノードは、プライマリ ノードに障害が発生した時に稼動状態になるデータベースのコピーを含んでいます。

複数の高可用性アプライアンス データベース オプションが存在します。レプリケーション モードの選択は、特に重要なデータベース構成オプションです。レプリケーション モードにより、vRealize Automation 環境でデータの整合性を維持する方法が決定されます。また、高可用性構成の場合は、プライマリまたはプライマリ ノードの障害をフェイルオーバーする方法が決定されます。同期および非同期という 2 つの利用可能なレプリケーション モードがあります。

どちらのレプリケーション モードもデータベースのフェイルオーバーをサポートしていますが、それぞれに長所と短所があります。高可用性データベース フェイルオーバーをサポートするには、非同期モードでは 2 台のノードが必要ですが、同期モードでは 3 台のノードが必要になります。また、同期モードでは自動フェイルオーバーも実行されます。

レプリケーション モード	メリット	デメリット
同期	<ul style="list-style-type: none"> <li>■ データ損失の可能性が最小限に抑えられる。</li> <li>■ 自動フェイルオーバーを起動します。</li> </ul>	<ul style="list-style-type: none"> <li>■ システムのパフォーマンスに影響する可能性がある。</li> <li>■ 3 台のノードが必要です。</li> </ul>
非同期	<ul style="list-style-type: none"> <li>■ 必要なノードは 2 台のみ。</li> <li>■ システムのパフォーマンスに及ぼす影響が同期モードより小さい。</li> </ul>	データ損失防止の点で同期モードほど堅牢ではない。

vRealize Automation は両方のモードをサポートしますが、デフォルトでは非同期モードで動作し、2 つ以上のアプライアンス データベース ノードが配備されている場合にのみ高可用性を実現します。仮想アプライアンス管理インターフェイスの [クラスタ] タブでは、同期モードの切り替えやデータベース ノードの追加を必要に応じて実行できます。

同期モードで使用する場合、vRealize Automation によって自動フェイルオーバーが実行されます。

高可用性を備えていない構成の単一ノードで開始した場合でも、必要に応じて高可用性を強化するために後からノードを追加できます。該当するハードウェアおよびデータ損失に対する最大限の保護を必要としている場合は、環境を同期モードで運用するように構成することを検討してください。

## アプライアンス データベースのフェイルオーバー

高可用性構成では、プライマリは、常にトランザクションをレプリカ サーバにストリーミングします。プライマリが動作しなくなった場合、アクティブな動作中のレプリカは、読み取り専用要求の処理を続行できます。手動または自動で新しいプライマリが昇格されると、その後の要求はすべてそのプライマリに移動されます。

## アプライアンス データベースの構成

仮想アプライアンス管理インターフェイスのデータベース ページを使用すると、アプライアンス データベースの構成を監視したりアップデートしたりすることができます。また、プライマリ ノードの指定や、データベースによって使用される同期モードを変更することもできます。

アプライアンス データベースは vRealize Automation システムのインストールおよび構成時にインストールされ、構成されます。構成の監視と変更は、仮想アプライアンス管理インターフェイスの [データベース] タブから行うことができます。

[接続状態] テキスト ボックスは、データベースが vRealize Automation システムに接続されているかどうか、正しく機能しているかどうかを示します。

アプライアンス データベースがフェイルオーバーをサポートするために複数のノードを使用する場合、ページ下部のテーブルにノードとそのステータスが表示され、どのノードがプライマリかが示されます。[レプリケーション モード] テキスト ボックスは、システムに現在構成されている操作モードが同期モードか非同期モードかを示します。アプライアンス データベースの構成をアップデートするには、このページを使用します。

データベース ノード テーブルの [同期の状態\*] 列は、クラスタの同期方式を示します。この列は [ステータス] 列と連携し、クラスタ ノードの状態を示します。表示されるステータスは、クラスタが非同期レプリケーションと同期レプリケーションのどちらを使用しているかによって異なります。

表 1-4. アプライアンス データベースのレプリケーション モードの同期状態

モード	同期状態のメッセージ
同期レプリケーション	プライマリ ノード - 状態なし レプリカ ノード - 同期 その他のノード - 可能性あり
非同期レプリケーション	プライマリ ノード - 状態なし その他のノード - 可能性あり

[有効] 列は、レプリカがプライマリ ノードと同期されるかどうかを示します。プライマリ ノードは常に有効です。

[優先度] 列は、プライマリ ノードに対するレプリカ ノードの位置を示します。プライマリ ノードに優先度の値はありません。レプリカを昇格させてプライマリにする場合は、優先度の値が最低のノードを選択します。

同期モードで使用する場合、vRealize Automation によって自動フェイルオーバーが実行されます。プライマリ ノードに障害が発生した場合、次に使用可能なレプリカ ノードが自動的に新しいプライマリになります。フェイルオーバー操作に必要な時間は、vRealize Automation の一般的な環境で 10 ～ 30 秒です。

### 前提条件

- 『vRealize Automation のインストール』の適切な手順に従って、vRealize Automation をインストールして構成します。
- vRealize Automation アプライアンスを展開したときに入力したパスワードを使用して、root として vRealize Automation アプライアンス管理にログインします。
- 適切な組み込みの Postgres アプライアンス データベース クラスタを vRealize Automation 展開の一部として構成します。

## 手順

- 1 仮想アプライアンス管理インターフェイスで、[vRA 設定] - [データベース] の順に選択します。
- 2 データベースが複数のノードを使用する場合は、ページの下部のテーブルを確認し、システムが適切に動作していることを確認します。
  - すべてのノードがリストされていることを確認します。
  - 適切なノードがプライマリ ノードに指定されていることを確認します。

**注：** データが保護されていることが確実でない限り、[同期モード] をクリックしてデータベースの同期モードを変更しないでください。準備なく同期モードを変更すると、データが失われる可能性があります。

- 3 いずれかのノードをプライマリに昇格させるには、該当する列で [昇格] をクリックします。
- 4 変更を行った場合は、[設定の保存] をクリックして構成を保存します。

### 3 台のノードのアプライアンス データベースによる自動フェイルオーバーのシナリオ

アプライアンス データベースの高可用性フェイルオーバー シナリオはいくつかあり、vRealize Automation の動作は、アプライアンス データベースの構成および障害が発生したノードの数によって異なります。

#### 1 台のノードでの障害のシナリオ

3 台のノードのうち 1 つで障害が発生した場合、vRealize Automation は自動フェイルオーバーを開始します。3 台のノードがすべてリストアされるまで、追加の自動フェイルオーバー処理は行われません。

次の表では、高可用性環境でのプライマリ ノードの障害に関連する動作と操作について説明します。

表 1-5. プライマリ ノードの障害

想定される動作	<ul style="list-style-type: none"> <li>■ 構成した同期レプリカ ノードがプライマリになり、アプライアンス データベースの機能を自動的に引き継ぎます。</li> <li>■ 潜在同期レプリカは、同期スタンバイ ノードになります。</li> <li>■ vRealize Automation 環境は、自動フェイルオーバーが完了するまで読み取り専用モードで機能します。</li> </ul>
その後の操作	<ul style="list-style-type: none"> <li>■ 以前のプライマリは、リカバリされるとフェイルオーバー エージェントの修復ロジックにより、自動的にレプリカとしてリセットされます。手動での操作は必要ありません。</li> <li>■ 以前のプライマリをリカバリできない場合は、手動でアプライアンス データベースを非同期モードに設定します。</li> </ul>

次の表では、高可用性環境での同期レプリカ ノードの障害に関連する動作と操作について説明します。



表 1-6. 同期レプリカの障害

想定される動作	<ul style="list-style-type: none"> <li>■ vRealize Automation 環境にダウンタイムは発生しません。潜在レプリカが新しい同期レプリカになるまで、データベース要求に数秒の遅延が発生します。アプライアンス データベースでは、この操作が自動的に実行されます。</li> </ul>
その後の操作	<ul style="list-style-type: none"> <li>■ 以前の同期レプリカはオンラインになると、自動的に潜在レプリカになります。手動での操作は必要ありません。</li> <li>■ 以前の同期レプリカを修復できない場合は、手動でアプライアンス データベースを非同期モードに設定します。</li> </ul>

次の表では、高可用性環境でのプライマリ ノードの障害に関連する動作と操作について説明します。

表 1-7. 潜在レプリカの障害

想定される動作	環境でダウンタイムは発生しません。
その後の操作	<ul style="list-style-type: none"> <li>■ 以前の潜在レプリカはオンラインになると、自動的に潜在レプリカになります。手動での操作は必要ありません。</li> <li>■ 以前の潜在レプリカを修復できない場合は、アプライアンス データベースを非同期モードに設定します。</li> </ul>

## 2 台のノードでの障害のシナリオ

3 台のノードのうち 2 台に同時に障害が発生した場合、手動による修復が実行されるまで、vRealize Automation は読み取り専用モードに切り替わります。

次の表では、高可用性環境でのプライマリ ノードと潜在レプリカ ノードの障害に関連する動作と操作について説明します。

表 1-8. プライマリ ノードと潜在レプリカの障害

想定される動作	<ul style="list-style-type: none"> <li>■ 同期レプリカは、自動的にプライマリに昇格しません。vRealize Automation は読み取り専用モードで機能します。手動による昇格が実行されるまで、読み取り専用トランザクションを処理できます。</li> </ul>
その後の操作	<ul style="list-style-type: none"> <li>■ 手動による昇格が必要です。アプライアンス データベースを非同期モードに設定します。</li> <li>■ プライマリと潜在レプリカがリカバリされたら、これらを新しいプライマリに対して同期するように手動で設定します。この時点で、vRealize Automation を同期モードに戻すことができます。</li> <li>■ 3 台のノードのうち 2 台が同時に停止すると、手動による修復を有効にするまで vRealize Automation は読み取り専用モードに切り替わります。1 台のデータベース ノードだけが使用可能な場合は、環境を非同期モードに切り替えます。</li> </ul>

次の表は、高可用性環境での同期ノードおよび潜在ノードの障害に関連する動作と操作について説明します。

表 1-9. 同期レプリカと潜在レプリカの障害

想定される動作	<ul style="list-style-type: none"> <li>■ vRealize Automation は読み取り専用モードで機能します。手動による修復が実行されるまで、読み取り専用トランザクションを処理できます。</li> </ul>
その後の操作	<ul style="list-style-type: none"> <li>■ 手動による昇格が必要です。アプライアンス データベースを非同期モードに設定します。</li> <li>■ 同期レプリカと潜在レプリカがリカバリされたら、これらをプライマリに対して同期するように手動でリセットする必要があります。この時点で、vRealize Automation を同期モードに戻すことができます。</li> <li>■ 3 台のノードのうち 2 台が同時に停止すると、手動による修復を有効にするまで vRealize Automation は読み取り専用モードに切り替わります。1 台のデータベース ノードだけが使用可能な場合は、環境を非同期モードに切り替えます。</li> </ul>

## ノード間のリンクの障害

分散導入環境でノード間にリンクの障害が発生した場合、自動フェイルオーバー エージェントは、構成の修復を試みます。

次の表は、すべてのノードが動作しオンラインの状態を維持しているときに、次の構成の高可用性環境で発生した 2 つのサイト間のリンクの障害に関連する動作と操作について説明します。

サイト A：プライマリと潜在レプリカ

サイト B：同期レプリカ

表 1-10. すべてのノードが動作しオンラインの状態を維持しているときの 2 つのサイト間のリンクの障害

想定される動作	vRealize Automation 環境にダウンタイムは発生しません。潜在レプリカは、自動的に同期レプリカになります。
その後の操作	手動での操作は必要ありません。

次の表は、すべてのノードが動作しオンラインの状態を維持しているときに、次の構成の高可用性環境で発生した 2 つのサイト間のリンクの障害に関連する動作と操作について説明します。

サイト A：プライマリ

サイト B：同期レプリカと潜在レプリカ

表 1-11. すべてのノードが動作しオンラインの状態を維持しているときの 2 つのサイト間のリンクの障害 - 代替構成

想定される動作	同期レプリカがプライマリになり、アプライアンス データベースの機能を自動的に引き継ぎます。自動フェイルオーバー エージェントが、潜在レプリカを昇格させ、新しい同期レプリカにします。この昇格が完了するまで、vRealize Automation 環境は読み取り専用モードで動作します。
その後の操作	手動での操作は必要ありません。リンクがリカバリされると、自動フェイルオーバー エージェントによって、以前のプライマリはレプリカとしてリセットされます。

## シナリオ: vRealize Automation アプライアンス データベースの手動フェイルオーバーの実行

vRealize Automation アプライアンス Postgres データベースに問題がある場合は、クラスタ内のレプリカ vRealize Automation アプライアンス ノードに手動でフェイルオーバーします。

プライマリ vRealize Automation アプライアンス ノードの Postgres データベースに障害が発生したときや、実行が停止したときは、次の手順を実行します。

**注：** ノードが不良状態になった場合は、フェイルオーバーを含むすべての操作に、その仮想アプライアンス管理インターフェイスを使用しないでください。

### 前提条件

- vRealize Automation アプライアンス ノードからなるクラスタを構成します。各ノードが組み込みの Postgres アプライアンス データベースのコピーをホストします。

### 手順

- 1 外部ロード バランサからプライマリ ノードの IP アドレスを削除します。
- 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 [クラスタ] を選択します。
- 4 データベース ノードのリストで、優先度が最低のレプリカ ノードを探します。  
レプリカ ノードは、優先度の昇順に表示されています。
- 5 [昇格] をクリックして、操作が終了するのを待ちます。  
操作が終了すると、このレプリカ ノードは、新しいプライマリ ノードとしてリストに表示されます。
- 6 以前のプライマリ ノードの問題を修正して、クラスタに戻します。
  - a 以前のプライマリ ノードを隔離します。  
ノードを現在のネットワーク（残りの vRealize Automation アプライアンス ノードとの間の経路の役割を担っているネットワーク）から切断します。このノードの管理のために別の NIC を選択するか、または仮想マシン管理コンソールから直接このノードを管理します。
  - b 以前のプライマリ ノードをリカバリします。  
ノードをパワーオンにするか、もしくは問題を修正します。たとえば、仮想マシンが応答しない場合はリセットします。
  - c コンソール セッションからルートとして vpostgres サービスを停止します。  
`service vpostgres stop`
  - d 以前のプライマリ ノードを元のネットワーク（他の vRealize Automation アプライアンス ノードとの間の経路の役割を担っていたネットワーク）に戻します。
  - e コンソール セッションからルートとして haproxy サービスを再起動します。

```
service haproxy restart
```

- f 新しい vRealize Automation アプライアンス プライマリ ノード管理インターフェイスにルートとしてログインします。
- g [クラスタ] を選択します。
- h 以前のプライマリ ノードを探して、[リセット] をクリックします。
- i リセットが成功したら、以前のプライマリ ノードを再起動します。
- j 以前のプライマリ がパワーオンの状態になっており、次のサービスが稼働していることを確認します。

```
haproxy horizon-workspace rabbitmq-server vami-lighttpd vcac-server vco-server
```

- k 以前のプライマリ ノードを外部ロード バランサに再び追加します。

**注：** レプリカに降格されたプライマリ ノードが依然としてプライマリとしてリストに表示されている場合は、問題を修正するために、そのノードを手動でクラスタに再参加させるが必要な場合があります。

## シナリオ：メンテナンス データベース フェイルオーバーの実行

vRealize Automation のシステム管理者として、アプライアンス データベースのメンテナンス フェイルオーバー操作を実行する必要があります。

このシナリオでは、現在のプライマリ ノードが起動し、正常に実行されていることを前提としています。データベースのメンテナンス フェイルオーバーには、プライマリ ノードのメンテナンスとレプリカ ノードのメンテナンスの 2 つの手順があります。プライマリ ノードがレプリカとなるように置き換えたら、必要に応じて、再度プライマリ ノードとして使用できるようにメンテナンスを実行する必要があります。

**注：** メンテナンス フェイルオーバーの実行中は、該当するホスト マシンで HAProxy サービスの停止や再起動を行わないでください。

### 前提条件

- 『vRealize Automation のインストール』の適切な手順に従って、vRealize Automation をインストールおよび構成します。
- vRealize Automation アプライアンスを展開したときに入力したパスワードを使用して、root として vRealize Automation アプライアンス管理にログインします。
- 該当する組み込みの Postgres アプライアンス データベース クラスタをインストールして構成します。
- データベースで同期レプリケーション モードを使用する場合、クラスタ内に 3 台の有効なノードがあることを確認します。

### 手順

- 1 外部ロード バランサからプライマリ ノードの IP アドレスを削除します。
- 2 プライマリ ノードを隔離します。

ノードを現在のネットワークから切断します。このネットワークは、他の vRealize Automation アプライアンス ノードにルーティングするネットワークです。

- 3 このノードの管理のために別の NIC を選択するか、または仮想アプライアンス管理インターフェイスから直接このノードを管理します。
- 4 仮想アプライアンス管理インターフェイスの [クラスタ] を選択します。
- 5 プライマリへの昇格の優先順位が最も低いレプリカ ノードを選択し、[昇格] をクリックします。  
レプリカ ノードは、優先度の昇順に表示されています。  
古いプライマリはレプリカ状態に降格され、新しいプライマリが昇格します。
- 6 適切なレプリカ メンテナンスを実行します。
- 7 メンテナンスが完了したら、仮想アプライアンスがネットワークに接続された状態で実行され、その HAProxy サービスが動作していることを確認します。
  - a vRealize Automation 管理コンソールにルートとしてログインします。
  - b レプリカ ノードへの ping と名前による解決が可能であること、および仮想アプライアンス管理インターフェイスの [クラスタ] タブに最近のステータスがあることを確認します。
- 8 レプリカ ノードに対して [リセット] をクリックします。  
この操作を実行すると、データベースが現在のプライマリにレプリケートするように構成され、最新の haproxy 構成を持つレプリカ ノードとプライマリ ノードを再同期できるようにデータベースがリセットされます。
- 9 リセットが成功した場合は、レプリカ仮想アプライアンス ノードの IP アドレスを外部の仮想アプライアンス ロード バランサの IP アドレス プールに戻すことができます。
- 10 データベース テーブルにレプリカ ノードが正常に表示されていること、およびレプリカ ノードの ping と名前による解決が可能であることを確認します。

#### 次のステップ

以前のプライマリ ノードの問題を修正して、クラスタに戻します。

## アプライアンス データベースの致命的な障害からの手動によるリカバリ

アプライアンス データベースに障害が発生し、プライマリに障害が発生した際に、実行中のデータベース ノードがないか、すべてのレプリカ ノードが同期されていない場合、次の手順に沿ってデータベースのリカバリを試みます。

この手順は、非同期モードで実行されているクラスタ全体で、動作しているデータベース ノードがない場合に適用されます。このシナリオでは通常、[仮想アプライアンス管理インターフェイス] ページの読み込みまたは更新を試みると、次のようなエラーがページに表示されます。

データベース サービスの初期化エラー: トランザクションの JDBC 接続を開けませんでした。ネストされた例外: org.postgresql.util.PSQLException: 接続の試みに失敗しました。

## 手順

- 1 いずれかのデータベース ノードから仮想アプライアンス管理インターフェイスを使用して、データベースのリカバリを試みます。
  - a 可能な場合は、最新の状態を保持しているノードの仮想アプライアンス管理インターフェイスの [クラスタ] ページを開きます。通常、このノードは、データベースに障害が発生する前にプライマリ ノードとして機能していたものです。
  - b プライマリ ノードの仮想アプライアンス管理インターフェイスを開けない場合は、他のレプリカ ノードでこのインターフェイスを開きます。
  - c 仮想アプライアンス管理インターフェイスが機能しているデータベース ノードが見つかったら、手動フェイルオーバーを実行してリカバリを試みます。

[シナリオ：vRealize Automation アプライアンス データベースの手動フェイルオーバーの実行](#)を参照してください。

- 2 手順 1 が失敗した場合、シェル セッションを開始して、最新の状態にあるノードを特定します。すべての使用可能なクラスタ ノードに対するシェル セッションを開始し、次のシェル コマンド `service vpostgres start` を実行して、データベースを起動します。
- 3 ローカル データベースが動作している各ノードで次の手順を実行し、最新の状態にあるノードを特定します。
  - a 次のコマンドを実行して、最新の状態にあるノードを特定します。このコマンドで `f` が返される場合、そのノードは最新の状態にあり、手順 4 に進むことができます。

```
su - postgres
psql vcac
vcac=# select pg_is_in_recovery();
pg_is_in_recovery
```

- このコマンドで `f` が返される場合、このノードは最新の状態にあります。
- ノードから `t` が返された場合は、ノードで次のコマンドを実行します。

```
SELECT pg_last_xlog_receive_location() as receive_loc, pg_last_xlog_replay_location() as
replay_loc, extract(epoch from pg_last_xact_replay_timestamp()) as replay_timestamp;
```

このコマンドによって、次のような結果が返されます。

```
vcac=# SELECT pg_last_xlog_receive_location() as receive_loc, pg_last_xlog_replay_location()
as replay_loc, extract(epoch from pg_last_xact_replay_timestamp()) as replay_timestamp;
 receive_loc | replay_loc | replay_timestamp
-----+-----+-----
 0/200000000 | 0/203228A0 | 1491577215.68858
(1 row)
```

- 4 各ノードの結果を比較して、最新の状態が保持されているノードを確認します。  
`receive_loc` 列の値が最も大きいノードを選択します。値が等しい場合は、`replay_loc` 列の値が最も大きいノードを選択します。この値も等しい場合は、`replay_timestamp` の値が最も大きいノードを選択します。
- 5 最新の状態が保持されているノードで `vcac-vami psql-promote-master -force` コマンドを実行します。

- 6 テキスト エディタで `/etc/haproxy/conf.d/10-psql.cfg` ファイルを開き、次の行を更新します。

```
server masterserver sc-rdops-vm06-dhcp-170-156.eng.vmware.com:5432 check on-marked-up shutdown-
backup-sessions
```

現在のノードの FQDN を使用して、次のように指定します。

```
server masterserver current-node-fqdn:5432 check on-marked-up shutdown-backup-sessions
```

- 7 ファイルを保存します。
- 8 `service haproxy restart` コマンドを実行します。
- 9 最新のノードの仮想アプライアンス管理インターフェイスの [クラスタ] ページを開きます。
- このノードはプライマリ ノードとして、他のノードは無効なレプリカとして表示されます。さらに、レプリカの [リセット] ボタンが有効になります。
- 10 クラスタの状態が修復されるまで、連続する各レプリカに対して [リセット] をクリックします。

## vRealize Automation インストールのバックアップとリカバリ

障害発生時にシステムのダウンタイムとデータの損失を最小限に留めるため、管理者は、vRealize Automation インストール環境全体を定期的にバックアップします。 システムで障害が発生した場合は、動作することが分かっている最後のバックアップをリストアし、いくつかのコンポーネントを再インストールすることでリカバリできます。

vRealize Automation のバックアップおよびリストアについては、[vRealize Suite ドキュメント](#)の次のトピックを参照してください。

- vRealize Automation のバックアップ準備
- vRealize Automation システムのリカバリ

## カスタマ エクスペリエンス改善プログラム

本製品は、VMware のカスタマ エクスペリエンス改善プログラム (CEIP) に参加しています。VMware は、CEIP で収集された情報を活用して、VMware 製品およびサービスの改善、問題の解決、各製品の展開および使用に関する最適な方法の提案を行うことができますようになります。vRealize Automation の CEIP の参加と離脱は随時可能です。

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。

## vRealize Automation のカスタマ エクスペリエンス改善プログラムへの参加または離脱

vRealize Automation のカスタマ エクスペリエンス改善プログラム (CEIP) の参加と離脱は随時可能です。

vRealize Automation 製品は、最初のインストールと構成時に、カスタマ エクスペリエンス改善プログラム (CEIP) への参加を選ぶことができます。インストール後、CEIP に参加または CEIP から離脱するには、次の手順に従います。

## 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 [テレメトリ] タブをクリックします。
- 3 [VMware カスタマ エクスペリエンス改善プログラムに参加] オプションを選択または選択解除します。  
チェック ボックスを選択すると、このプログラムが起動し、`https://vmware.com` にデータが送信されます。
- 4 [設定の保存] をクリックします。

## データ収集時刻の構成

カスタマ エクスペリエンス改善プログラム (CEIP) から VMware にデータを送信する日時を設定できます。

## 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 テキスト エディタで次のファイルを開きます。  
`/etc/telemetry/telemetry-collector-vami.properties`
- 3 曜日と時刻のプロパティを編集します。

プロパティ	説明
<code>frequency.dow=&lt;day-of-week&gt;</code>	データの収集が開始される曜日。
<code>frequency.hod=&lt;hour-of-day&gt;</code>	データの収集が開始される時刻（現地時間）。0～23 の値を指定できます。

- 4 `telemetry-collector-vami.properties` を保存して閉じます。
- 5 次のコマンドを入力して設定を適用します。

```
vcac-config telemetry-config-update --update-info
```

環境内のすべてのノードに変更が適用されます。

## システム設定の調整

システム管理者として、ログの調整や、IaaS のメール テンプレートのカスタマイズを行います。各テナントのデフォルト設定（通知を処理するメール サーバなど）も管理できます。テナントで異なる設定が必要な場合は、テナント管理者がこれらのデフォルトをオーバーライドすることができます。

## サービス カタログの [すべてのサービス] アイコンの変更

サービス カタログのデフォルト アイコンを変更して、カスタムの画像を表示できます。アイコンを変更すると、そのアイコンはすべてのテナントで変更されます。カタログでテナント固有のアイコンは設定できません。

Linux、Mac、Windows 用のコマンドが用意されているので、これらのどのオペレーティング システム上でも cURL コマンドを実行できます。



## 前提条件

- イメージを base64 エンコード文字列に変換します。
- コマンドを実行するマシンに cURL をインストールする必要があります。
- システム管理者ロールを持つ vRealize Automation ユーザーの認証情報が必要です。

## 手順

- 1 cURL コマンドのターミナル セッションで VCAC 変数を設定します。

オペレーティング システム	コマンド
Linux/Mac	<code>export VCAC=&lt;VA URL&gt;</code>
Windows	<code>set VCAC=&lt;VA URL&gt;</code>

- 2 システム管理者ユーザーの認証トークンを取得します。

オペレーティング システム	コマンド
Linux/Mac	<code>curl https://\$VCAC/identity/api/tokens --insecure -H "Accept: application/json" -H 'Content-Type: application/json' --data '{"username": "&lt;Catalog Administrator User&gt;", "password": "&lt;password&gt;", "tenant": "vsphere.local"}'</code>
Windows	<code>curl https://\$VCAC/identity/api/tokens --insecure -H "Accept: application/json" -H 'Content-Type: application/json' --data '{"username": "&lt;Catalog Administrator User&gt;", "password": "&lt;password&gt;", "tenant": "vsphere.local"}'</code>

認証トークンが生成されます。

- 3 <Auth Token> を前の手順で生成したトークン文字列に置き換えて、認証トークン変数を設定します。

オペレーティング システム	コマンド
Linux/Mac	<code>export AUTH="Bearer &lt;Auth Token&gt;"</code>
Windows	<code>set AUTH=Bearer &lt;Auth Token&gt;</code>

- 4 base64 でエンコードされた画像の文字列を追加します。

オペレーティング システム	コマンド
Linux/Mac	<code>curl https://\$VCAC/catalog-service/api/icons --insecure -H "Accept: application/json" -H 'Content-Type: application/json' -H "Authorization: \$AUTH" --data '{"id": "cafe_default_icon_genericAllServices", "fileName": "&lt;filename&gt;", "contentType": "image/png", "image": "&lt;IMAGE DATA as base64 string&gt;"}</code>
Windows	<code>curl https://\$VCAC/catalog-service/api/icons --insecure -H "Accept: application/json" -H 'Content-Type: application/json' -H "Authorization: %AUTH%" --data '{"id": "cafe_default_icon_genericAllServices", "fileName": "&lt;filename&gt;", "contentType": "image/png", "image": "&lt;IMAGE DATA as base64 string&gt;"}</code>

## 結果

約 5 分後に新しいサービス アイコンがサービス カタログに表示されます。

デフォルト アイコンに戻す場合は、手順 1-3 を実行した後に次のコマンドを実行します。

オペレーティング システム	Command
[Linux/Mac]	<code>curl https://\$VCAC/catalog-service/api/icons/cafe_default_icon_genericAllServices --insecure -H "Authorization: \$AUTH" --request DELETE</code>
[Windows]	<code>curl https://%VCAC%/catalog-service/api/icons/cafe_default_icon_genericAllServices --insecure -H "Authorization: %AUTH%" --request DELETE</code>

## データのロールオーバー設定のカスタマイズ

vRealize Automation のデータのロールオーバー設定を行うと、システムによるレガシー データの保持、アーカイブ、および削除に関する方法を制御できます。

データのロールオーバー機能を使用してロールオーバーを有効にし、vRealize Automation がデータのアーカイブや削除、およびその他のデータ ロールオーバーの制御を行う前に、IaaS SQL Server のデータベースでデータを保持する最大日数を設定します。

デフォルトでは、データのロールオーバー機能は無効になっています。

vRealize Automation の [グローバル設定] ページでデータのロールオーバー設定を行います。この機能を有効にすると、次の SQL Server のデータベース テーブルからデータをクエリまたは削除します。

- UserLog
- Audit
- CategoryLog
- VirtualMachineHistory
- VirtualMachineHistoryProp
- AuditLogItems
- AuditLogItemsProperties
- TrackingLogItems
- WorkflowHistoryInstances
- WorkflowHistoryResults

DataRolloverIsArchiveEnabled を True 設定すると、テーブルのアーカイブ バージョンが dbo スキーマで作成されます。たとえば、UserLog のアーカイブ バージョンは UserLogArchive で、VirtualMachineHistory のアーカイブ バージョンは VirtualMachineHistoryArchive になります。

データのロールオーバー機能を有効にすると、vRealize Automation アプライアンスのタイムゾーン設定に応じ、事前定義された午前 3 時に 1 日 1 回実行されます。DataRollover MaximumAgeInDays 設定を使用すると、データを保持する最大日数を設定できます。このプロセスは、通常は数分から 1 時間以内にすばやく実行されます。ただし、この機能を最初に有効にするときは、大量のデータをアーカイブ/削除することでプロセスに遅延が生じ、完了までにかかる時間が大幅に長くなる可能性があります。このプロセスは、完了するまで実行を継続するように設計されています。同時実行の問題が発生しないように、短時間で処理できる小さなバッチサイズのトランザクションが処理単位として実行されます。以下で説明しているとおり、このプロセスは安全に停止できます。

**注：** DataRollover プロセスは、DataRollover Status 設定を実行中から無効または有効に変更することで停止できます。これにより、現在実行中のプロセスは安全に終了します。処理中のデータが失われることはありません。プロセスを停止した時点までにアーカイブまたは削除されたデータはすべて保存されます。

DataRollover IsArchiveEnabled を True に設定すると、DataRollover MaximumAgeInDays 設定で指定した日より古いデータはアーカイブテーブルに移動されます。DataRollover IsArchiveEnabled を False に設定すると、データは完全に削除され、データはアーカイブされません。削除されたデータは回復不能です。

#### 手順

- 1 システム管理者として vRealize Automation コンソールにログインします。
- 2 [インフラストラクチャ] - [管理] - [グローバル設定] を選択します。
- 3 [グローバル設定] ページで、テーブルの [データのロールオーバー] セクションを見つけ、設定の確認や変更を行います。

設定	説明
DataRollover BatchSize	これはデフォルトで 2,000 に設定されており、通常は、変更する必要はありません。ただし、パフォーマンスに影響していると思われる場合は、BatchSize の設定値を小さくすることで改善する可能性があります。設定値を大きくすると、ジョブの実行時間が短くなる可能性があります。同時処理にかかる負荷が大きくなります。有効な範囲は、100 ~ 20,000 です。
DataRollover IsArchiveEnabled	最大日数の経過後、ロールオーバー データを移動し、テーブルをアーカイブするかどうかを指定します。 デフォルトでは、この値は True に設定されています。 この値を False に設定すると、DataRollover MaximumAgeInDays 設定で指定した日より古いデータはすべて完全に削除されます。
DataRollover MaximumAgeInDays	データのアーカイブへの移動または完全削除の前に、システムがデータベース内にデータを保持する最大日数を指定します。 デフォルトでは、この値は 90 日間 に設定されています。
DataRollover Status	データのロールオーバーを有効にするかどうかを指定します。 デフォルトでは、この値は Disabled に設定されています。データのロールオーバーを有効にするには、この値を Enabled に設定します。

設定	説明
DataRollover VirtualMachineHistory BatchSize	1 ～ 5 レコードの範囲内で、VirtualMachineHistory テーブルのバッチ サイズを指定します。デフォルトは 1 です。
DataRollover UpdateStatistics	UpdateStatistics はデフォルトでオフになっていますが、クエリパフォーマンスが向上する効果があるため、オンにする（1 に設定する）ことを強くお勧めします。これにより、[dbo].[usp_DataRollover] ストアド プロシージャで、アーカイブ プロセスの実行後にテーブルに対して統計情報の更新コマンドが実行されるようになります。

- 4 最初のテーブル列で [編集] アイコン (✎) をクリックし、設定を編集します。

該当する設定の [値] 領域が編集可能になります。

- 5 最初のテーブル列の [保存] アイコン (✔) をクリックし、変更を保存します。

## Manager Service 構成ファイルでの設定の調整

Manager Service 構成ファイル (managerService.exe.config) を使用して、マシン展開の共通の設定を調整することができます。

managerService.exe.config ファイルは通常、%System-Drive%\Program Files x86\VMware\VCAC\Server ディレクトリ内にあります。このファイルを編集する前に必ずコピーをとっておいてください。

managerService.exe.config ファイルの次の設定を使用して、マシン展開のさまざまな特性を制御することができます。デフォルト値が表示されています。

- <add key="ProcessLeaseWorkflowTimerCallbackIntervalMilliseconds" value="3600000"/>
- <add key="BulkRequestWorkflowTimerCallbackMilliseconds" value="10000"/>
- <add key="MachineRequestTimerCallbackMilliseconds" value="10000"/>
- <add key="MachineWorkflowCreationTimerCallbackMilliseconds" value="10000"/>
- <add key="RepositoryConnectionMaxRetryCount" value="100"/>
- <add key="MachineCatalogRegistrationRetryTimerCallbackMilliseconds" value="120000"/>
- <add key="MachineCatalogUnregistrationRetryTimerCallbackMilliseconds" value="120000"/>
- <add key="MachineCatalogUpdateMaxRetryCount" value="15"/>

## リソースを集中的に使用する同時実行制限の設定

リソースを節約するために、vRealize Automation ではマシン プロビジョニングおよびデータ収集のインスタンスの同時実行数を制限します。この制限は変更できます。

### 同時マシン プロビジョニングの構成

複数の同時マシン プロビジョニング申請が発生すると、vRealize Automation のパフォーマンスに影響を与える可能性があります。パフォーマンスを改善する手段として、プロキシ エージェントとワークフロー アクティビティに設定されている制限を変更できます。

サイトのマシン所有者のニーズ次第で、vRealize Automation サーバは複数の同時マシンプロビジョニング申請を受け取ることがあります。このような状態は次のような状況で発生します。

- 1人のユーザーが複数マシンの申請を送信する。
- 多数のユーザーが同時にマシンを申請する。
- 1人以上のグループ マネージャが、保留中の複数のマシン申請を相次いで承認する。

vRealize Automation によるマシンのプロビジョニングにかかる時間は、通常、同時申請の数が多いときに増えます。プロビジョニング時間の増加は、次に示す 3 つの重要要因に左右されます。

- リソースを集中的に使用する同時 vRealize Automation ワークフロー アクティビティ（WIM ベース プロビジョニングにおけるような、仮想プラットフォーム内で作成されたマシンの SetupOS アクティビティや、仮想プラットフォーム内でクローン作成されたマシンのクローン アクティビティなど）のパフォーマンスに対する影響。
- 同時に実行できる、リソースを集中的に使用する（一般に時間もかかる）プロビジョニング アクティビティの数に対して構成された vRealize Automation 制限。デフォルトの場合、これは 8 です。構成されている制限を超える同時アクティビティは待機状態になります。
- 同時に実行できる vRealize Automation 作業アイテム（リソースを集中的に使用するかどうかに関わらず）の数に関する、仮想プラットフォームまたはクラウド サービス アカウント内の制限。たとえば、vCenter Server におけるデフォルトの制限は 4 であり、この制限を超える作業アイテムは待機状態になります。

デフォルトの場合、vRealize Automation はプロキシ エージェントを使用するハイパーバイザーの同時仮想プロビジョニング アクティビティを、エンドポイントあたり 8 に制限します。このため、特定のエージェントによって管理される仮想プラットフォームは、他のアイテムの実行を阻止できるだけの十分なリソースを集中的に使用する作業アイテムを受け取ることがありません。制限を変更する前に変更の影響を慎重にテストするように計画してください。サイトに最適な制限を決定するためには、vRealize Automation 内でのワークフロー アクティビティ実施だけでなく、仮想プラットフォームにおける作業アイテムの実行についても調査する必要があります。

構成されている、エージェントあたりの vRealize Automation 制限数を増やす場合は、次に示す方法で vRealize Automation で付加的な構成調整を行う必要が生じることがあります。

- SetupOS およびクローンのワークフロー アクティビティのデフォルトの実行タイムアウト間隔は、それぞれ 2 時間です。これらのアクティビティのどちらかを実行するために必要な時間がこの制限を超える場合には、そのアクティビティは取り消されて、プロビジョニングは失敗します。この失敗を防止するには、これらの実行タイムアウト間隔の一方または両方を増やします。
- SetupOS およびクローンのワークフロー アクティビティのデフォルトのデリバリ タイムアウト間隔は、それぞれ 20 時間です。いったんこれらのアクティビティの 1 つが開始されると、そのアクティビティにより生成されたマシンが 20 時間経ってもプロビジョニングされていない場合、そのアクティビティは取り消され、プロビジョニングは失敗します。したがって、このような状況が時折発生するポイントに制限数を増やした場合には、これらのデリバリ タイムアウト間隔の一方または両方を増やす必要があります。

## 同時データ収集の構成

デフォルトの場合、vRealize Automation は同時データ収集アクティビティに制限をかけます。この制限を変更すると、各種のデータ収集のデフォルトの実行タイムアウト間隔を変更することによって、不要なタイムアウトを回避できます。

vRealize Automation は、定期的にそのプロキシ エージェントを介して既知の仮想コンピュート リソースからデータを収集するとともに、クラウド サービス アカウントと物理マシンからもそれらのエンドポイントを介してデータを収集します。サイト内の仮想コンピュート リソース、エージェント、およびエンドポイントの数により、同時データ収集処理が頻繁に発生する可能性があります。

データ収集の実行時間は、エンドポイントのオブジェクト（仮想マシン、データストア、テンプレート、コンピュート リソースなど）の数によって決まります。個々のデータ収集は、さまざまな状況により、相当の時間がかかる場合があります。マシンのプロビジョニングと同様に、同時実行によりデータ収集の完了に必要な時間が増加します。

デフォルトの場合、同時データ収集アクティビティはエージェントあたりで 2 つに制限され、この制限を超えたものは待機状態になります。このため、各データ収集の完了は比較的速やかであり、同時データ収集アクティビティが IaaS パフォーマンスに影響を与えることはまずありません。

ただし、サイトのリソースと状況によっては、プロキシ データ収集で同時実行を利用するのに十分な速度のパフォーマンスを維持したまま、構成された制限数を増やすことができる場合があります。制限数を増やすと個々のデータ収集にかかる時間が増加する可能性があります、より多くのコンピュート リソースとマシンから一度により多くの情報を収集できるため、十分に補える可能性があります。

構成されているエージェントあたりの制限数を増やす場合は、プロキシ エージェントを使用する各種のデータ収集（インベントリ、パフォーマンス、状態、および WMI）のデフォルトの実行のタイムアウト間隔を調整する必要があります。これらのアクティビティのどれかを実行するために必要な時間が構成したタイムアウト間隔を超える場合には、そのアクティビティはキャンセルされ、再開されます。アクティビティのキャンセルを防止するには、これらの実行タイムアウト間隔を 1 つ以上増やします。

### 同時実行制限とタイムアウト間隔の調整

同時プロビジョニング、データ収集アクティビティ、およびデフォルトのタイムアウト間隔について、エージェントごとに制限を変更できます。

時間を入力するときには、hh:mm:ss という形式（hh は時間、mm は分、ss は秒）を使用します。

#### 前提条件

IaaS Manager Service をホストするサーバに、管理者としてログインします。分散インストールの場合、これは Manager Service のインストールされたサーバです。

#### 手順

- 1 エディタで `ManagerService.exe.config` ファイルを開きます。このファイルは vRealize Automation サーバのインストール ディレクトリ、通常は `%SystemDrive%\Program Files x86\VMware\VCAC\Server` に置かれます。
- 2 `workflowTimeoutConfigurationSection` というセクションを見つけます。
- 3 必要に応じて、次の変数をアップデートします。

パラメータ	説明
<b><code>MaxOutstandingResourceIntensive WorkItems</code></b>	同時プロビジョニングの制限（デフォルトは 8）
<b><code>CloneExecutionTimeout</code></b>	仮想プロビジョニングのタイムアウト間隔
<b><code>SetupOSExecutionTimeout</code></b>	仮想プロビジョニングのタイムアウト間隔

パラメータ	説明
<b>CloneTimeout</b>	仮想プロビジョニングのクローン配信のタイムアウト間隔
<b>SetupOSTimeout</b>	仮想プロビジョニングのセットアップ OS 配信のタイムアウト間隔
<b>CloudInitializeProvisioning</b>	クラウド プロビジョニング初期化のタイムアウト間隔
<b>MaxOutstandingDataCollectionWorkItems</b>	同時データ収集の制限
<b>InventoryTimeout</b>	インベントリ データ収集のタイムアウト間隔
<b>PerformanceTimeout</b>	パフォーマンス データ収集のタイムアウト間隔
<b>StateTimeout</b>	状態データ収集のタイムアウト間隔

- 4 ファイルを保存して閉じます。
- 5 [スタート] - [管理ツール] - [サービス] の順にを選択します。
- 6 vRealize Automation サービスを停止し、再起動します。
- 7 (オプション) vRealize Automation を高可用性モードで実行している場合、インストールの後で `ManagerService.exe.config` ファイルに加える変更は、すべてプライマリ サーバとフェイルオーバー サーバの両方で行う必要があります。

#### マシン コールバックの実行頻度の調整

マシンのリース期間が変更された場合に vRealize Automation コールバック手順を実行する頻度など、複数のコールバック手順の頻度を変更できます。

vRealize Automation では、Model Manager サービスに対して実行するさまざまなコールバック手順の構成済みの実行間隔を使用します。たとえば、`ProcessLeaseWorkflowTimerCallbackIntervalMiliSeconds` は、リース期間が変更されたマシンの検索間隔を表します。これらの時間間隔を変更して、チェックの頻度を調整できます。

これらの変数の値はミリ秒単位で入力してください。たとえば、10000 ミリ秒 = 10 秒、3600000 ミリ秒 = 60 分 = 1 時間となります。

#### 前提条件

IaaS Manager Service をホストするサーバに、管理者としてログインします。分散インストールの場合、これは Manager Service のインストールされたサーバです。

#### 手順

- 1 エディタで `ManagerService.exe.config` ファイルを開きます。このファイルは vRealize Automation サーバのインストール ディレクトリ、通常は `%SystemDrive%\Program Files x86\VMware\vCAC\Server` に置かれます。

## 2 必要に応じて、次の変数をアップデートします。

パラメータ	説明
<b>RepositoryWorkflowTimerCallbackMiliSeconds</b>	リポジトリ サービス、Model Manager Web サービスがアクティブかどうかをチェックします。デフォルト値は 10000 です。
<b>ProcessLeaseWorkflowTimerCallbackIntervalMiliSeconds</b>	マシンがリース期限切れになっていないかチェックします。デフォルト値は 3600000 です。
<b>BulkRequestWorkflowTimerCallbackMiliSeconds</b>	バルク申請がないかチェックします。デフォルト値は 10000 です。
<b>MachineRequestTimerCallbackMiliSeconds</b>	マシン申請がないかチェックします。デフォルト値は 10000 です。
<b>MachineWorkflowCreationTimerCallbackMiliSeconds</b>	新規マシンがないかチェックします。デフォルト値は 10000 です。

- 3 ファイルを保存して閉じます。
- 4 [スタート] - [管理ツール] - [サービス] の順にを選択します。
- 5 vCloud Automation Center サービスを停止し、再起動します。
- 6 (オプション) vRealize Automation を高可用性モードで実行している場合、インストールの後で ManagerService.exe.config ファイルに加える変更は、すべてプライマリ サーバとフェイルオーバー サーバの両方で行う必要があります。

## laaS ログ設定の調整

vRealize Automation を調整し、Manager Service ログに表示する情報のみを記録できます。

vRealize Automation が高可用性モードで実行されているとき、インストールの後に ManagerService.exe.config ファイルに変更を加える場合は、プライマリおよびフェイルオーバーの vRealize Automation サーバでその変更を行う必要があります。

### 手順

- 1 管理アクセス権が付与されている認証情報を使用して vRealize Automation サーバにログインします。
- 2 %SystemDrive%\Program Files x86\VMware\VCAC\Server、または別の場所にある場合は vRealize Automation サーバのインストール ディレクトリにある ManagerService.exe.config ファイルを編集します。



- 3 RepositoryLogSeverity キーと RepositoryLogCategory キーを編集し、ログ ファイルに書き込まれるイベントのタイプを構成します。

オプション	説明
<b>RepositoryLogSeverity</b>	<p>重要度を指定し、その重要度を下回るイベントを無視します。</p> <ul style="list-style-type: none"> <li>■ エラーはリカバリ可能なエラーとそれよりも重要なエラーのみを記録します</li> <li>■ 警告は重要性が低いエラーとそれよりも重要なエラーを記録します</li> <li>■ 詳細情報はすべての情報メッセージとそれよりも重要なエラーを記録します</li> <li>■ 詳細はデバッグ追跡を記録します。パフォーマンスが低下する可能性があります</li> </ul> <p>たとえば、<code>&lt;add key="RepositoryLogSeverity" value="Warning" /&gt;</code> のように指定します。</p>
<b>RepositoryLogCategory</b>	<p>カテゴリを指定し、重要度に関係なく、そのカテゴリのイベントをすべて記録します。たとえば、<code>&lt;add key="RepositoryLogCategory" value="MissingMachines,UnregisteredMachines,AcceptMachineRequest,RejectMachineRequest" /&gt;</code> は、見つからないマシンまたは未登録のマシンに関するすべてのイベントと、承認されたマシン要求や却下されたマシン要求をすべて記録します。</p>

- 4 ファイルを保存して閉じます。
- 5 [スタート] - [管理ツール] - [サービス] を選択し、vCloud Automation Center サービスを再起動します。

#### 結果

変更がログ設定に与える影響を確認するには、Manager Service をインストールしたマシン上の %SystemDrive%\Program Files (x86)\VMware\VCAC\Server\Logs 内、または Manager Service を別の場所にインストールした場合は、vRealize Automation サーバ インストール ディレクトリ内に配置された Manager Service ログ ファイルを表示します。

## vRealize Automation の監視

ルールに応じて、分散型展開内のすべてのホストについてワークフローまたはサービスの監視、イベントまたは監査ログの表示、ログの収集ができます。

### ワークフローの監視とログの表示

お使いのルールに応じてワークフローを監視し、アクティビティ ログを表示することができます。

表 1-12. 監視およびログ表示のオプション

目標	ロール	メニュー シーケンスと説明
アクション タイプ、アクションの日時などの、発生したアクションについての情報を表示します。	laaS 管理者	デフォルトのログ情報を表示したり、列およびフィルタのオプションを使用して表示コンテンツを制御したりします。 [インフラストラクチャ] - [監視] - [監査ログ] を選択します。 監査ログには、管理対象の仮想マシンのステータスについての詳細と、再構成中にこれらのマシンに対して実行されたアクティビティが示されます。このログには、マシン プロビジョニング、NSX、再利用、およびアクションの再構成に関する情報が含まれます。
利用できるスケジュールされたワークフロー (Distributed Execution Manager など) のステータスを表示する。	laaS 管理者	ワークフロー ステータスを表示し、必要に応じて特定のワークフローを開いてその詳細を表示します。 [インフラストラクチャ] - [監視] - [DEM ステータス] を選択します。
ログ データを表示し、必要に応じてエクスポートする。	laaS 管理者	デフォルトのログ情報を表示したり、列およびフィルタのオプションを使用して表示コンテンツを制御したりします。 [インフラストラクチャ] - [監視] - [ログ] を選択します。
実行された Distributed Execution Manager などのワークフローのステータスと履歴を表示する。	laaS 管理者	ワークフロー履歴を表示し、必要に応じて特定のワークフローを開いてその実行の詳細を表示します。 [インフラストラクチャ] - [監視] - [ワークフロー履歴] を選択します。
イベント タイプ、時間、ユーザー ID などのイベントのリストを表示し、必要に応じてイベント詳細ページを表示する。	システム管理者	実行時間、イベントの説明、テナント名、ターゲット タイプ、ID その他の特性などの、イベントとそれらに関連した属性のリストを表示します。 [管理] - [イベント] - [イベント ログ] を選択します。
申請のステータスを監視して、申請の詳細を表示します。	テナント管理者またはビジネス グループ マネージャ	責任を負う申請または自分の申請のステータスを表示します。 [申請] をクリックします。
最近のイベントに関する情報を表示します。	laaS 管理者またはテナント管理者	現在ログインしているユーザーの最近のイベントを表示します。 [インフラストラクチャ] - [最近のイベント] の順に選択します

## イベント ログとサービスの監視

vRealize Automation イベント ログおよびサービスを監視して、それらの現在および過去の状態を特定できます。

イベント ログのデフォルトの保持期間は 90 日です。この期間は、`/etc/vcac/vcac.properties` ファイルで変更できます。

データのロールオーバー設定をカスタマイズしてログを消去する方法の詳細については、『vRealize Automation の構成』を参照してください。

## vRealize Automation サービス

システム管理者は、システム管理者コンソール上のイベント ログから vRealize Automation サービスのステータスを確認できます。

個々の製品コンポーネントを実行するためには、サービスのサブセットが必要です。たとえば、テナントを設定する前に ID サービスと UI コア サービスが実行されている必要があります。

次の表に、vRealize Automation の機能に関連付けられているサービスを示します。

**表 1-13. ID サービス グループ**

サービス	説明
management-service	ID サービス グループ
sts-service	Single Sign On アプライアンス
権限	認証サービス
認証	認証
eventlog-service	イベント ログ サービス
licensing-service	ライセンス サービス

**表 1-14. UI コア サービス**

サービス	説明
shel-ui-app	シェル サービス
branding-service	ブランディング サービス
plugin-service	拡張（プラグイン）サービス
portal-service	ポータル サービス

IaaS コンポーネントを実行するためには、次のサービスがすべて必要です。

**表 1-15. サービス カタログ グループ（ガバナンス サービス）**

サービス	説明
notification-service	通知サービス
workitem-service	作業アイテム サービス
approval-service	承認サービス
catalog-service	サービス カタログ

**表 1-16. IaaS サービス グループ**

サービス	説明
iaas-proxy-provider	IaaS プロキシ
iaas-server	IaaS Windows マシン

表 1-17. XaaS

サービス	説明
vco	vRealize Orchestrator
advanced-designer-service	XaaS ブループリントおよびリソース アクション

## vRealize Automation 監査ログの使用

vRealize Automation の監査ログでは、重要なシステム イベントの収集と保持をサポートしています。

現在、vRealize Automation ではイベント ログの拡張機能として監査ログをサポートしています。この機能により、基本的な監査情報が提供されます。保持設定を指定するには、適切な vRealize Automation REST API イベント ブローカ サービス呼び出しを使用する必要があります。監査ログは現在、テナント管理者と、テナントにログインできるシステム管理者が利用できます。これにより、イベントの検索およびフィルタリング機能が提供されます。

デフォルトで、vRealize Automation では、ワークフロー サブスクリプション、エンドポイント、ファブリック グループの作成、更新、削除のイベントについて監査ログをサポートしています。vRealize Automation では、さまざまな IaaS イベントについて監査ログをカスタマイズすることもできます。

vRealize Automation 監査ログはデフォルトで無効です。仮想アプライアンス管理インターフェイスの [vRA] - [ログ] ページに表示される [監査ログの統合] セクションで、[有効] チェックボックスのオンとオフを切り替えることができます。

監査ログ情報は、標準の [イベント ログ] ページに表示されます。テナント管理者は、[管理] - [イベント ログ] を選択して、このページを表示できます。監査イベントは、イベント ログ テーブルで [イベント タイプ] フィールドに示された「監査」で確認します。各エントリには、各イベントの説明に加えて、テナント、時間、ユーザー、および関連するサービス名が表示されます。

他の任意の IaaS イベントの監査ログを有効にするには、カスタム構成ファイルが必要になるほか、IaaS ホスト マシン上で適切なコマンドを実行する必要もあります。サポートが必要な場合は、VMware プロフェッショナル サービスまでお問い合わせください。

外部の Syslog サーバ、特に VMware Log Insight にイベントをエクスポートするように、vRealize Automation を設定できます。

## Log Insight 監査ログのための vRealize Automation の設定

監査イベントを表示しやすくするため、VMware Log Insight に監査イベントをエクスポートするように vRealize Automation を設定できます。

監査ログはデフォルトで無効になっているため、監査ログ イベントを生成および表示するには、有効にする必要があります。

SSL を使用する場合、SSL は Log Insight エージェントが配置されている vRealize Automation アプライアンスで設定され、Log Insight Syslog サーバへの接続に関与します。SSL を使用するには、適切な証明書と、vRealize Automation と環境にインストールされた Log Insight サーバの間の接続を設定する必要があります。

## 前提条件

vRealize Automation は、vRealize Automation 環境にデフォルトでインストールされる Log Insight エージェントを使用し、Log Insight で表示するためのログ エントリを読み取ります。

## 手順

- 1 仮想アプライアンス管理インターフェイスにシステム管理者としてログインします。
- 2 [vRA] - [ログ] の順に選択します。
- 3 [監査ログの統合] の見出しの下で、監査ログの [有効化] チェック ボックスが選択されていることを確認します。
- 4 [Log Insight エージェントの設定] の見出しの下で、Log Insight サーバの [ホスト] マシン名を入力します。

- a Log Insight エージェントの [ホスト] マシンの名前を入力します。
- b Log Insight エージェントとの通信に使用する [ポート] を入力します。
- c 適切な通信プロトコルを選択します。
- d [SSL 有効] チェック ボックスを使用して、Log Insight エージェントとサーバとの間の通信に SSL を使用するかどうかを示します。

SSL を使用しない場合は、このページにある残りの設定は無視してかまいません。SSL を使用する場合は、これらを設定する必要があります。

- 5 SSL を使用する場合は、[SSL 信頼済みルート証明書] セクションで、適切な選択を行います。

vRealize Automation アプライアンス では、デフォルトで自己署名証明書が使用されます。信頼されたルート証明書を使用する場合は、証明書をインポートする必要があります。

- a 適切なチェック ボックスを選択して、新しい証明書を使用するか、または既存の証明書を使用するかを示します。

詳細については、仮想アプライアンス管理インターフェイスの [vRealize Automation ログの構成] ページにある注を参照してください。

- 6 [設定の保存] をクリックします。
- 7 [SSL サーバ証明書] セクションで、適切な選択を行います。
- 8 [エージェントの動作の構成] セクションを使用して、エージェントによるログ ファイルの処理方法を構成します。

## 結果

vRealize Automation 監査ログ イベントは、Log Insight インターフェイスから表示できます。

## 分散インストール環境におけるクラスタのホスト情報の表示

vRealize Automation アプライアンス管理コンソールから、分散導入環境内のクラスタ化されたすべてのノードのログを収集できます。

デプロイ内の各ホストの情報を表示することもできます。vRealize Automation 管理コンソールの [クラスタ] タブには、次の情報を表示する分散デプロイ情報テーブルがあります：

- デプロイ内の全ノードのリスト

- ノードのホスト名。ホスト名を完全修飾ドメイン名で表示。
- ホストが最後に管理コンソールに応答してからの経過時間。IaaS コンポーネント レポートが 3 分間隔で取得できるノードと、仮想アプライアンス レポートが 9 分間隔で取得できるノード。
- vRealize Automation コンポーネント タイプ。ノードが仮想アプライアンスか、IaaS サーバかの指定。

図 1-1. 分散導入環境の情報テーブル

	Host / Node Name	Version	Last Connected	Type	State*	Valid*
▶	cava-n-80-175.eng.vmware.com	7.5.0.378	7 minutes ago	MASTER	Up	<button>Delete</button>
▶	cava-n-85-043.eng.vmware.com	7.5.0.14528	14 seconds ago	IAAS		<button>Delete</button>

このテーブルを使用すると、デプロイ内のアクティビティを監視できます。たとえば、[最終接続] 列で最近接続されていないホストを見つけた場合、そのホスト サーバに問題が発生している可能性があります。

## ログ収集

[vRA] - [ログ] ページで [サポート バンドルの作成] ボタンを使用して、環境内のすべてのホストのログ ファイルを含む zip ファイルを作成できます。詳細については、[クラスタおよび分散型展開のログの収集](#)を参照してください。

## テーブルからのノードの削除

デプロイからホストを削除した場合は、分散デプロイ情報テーブルから対応するノードを削除して、ログ収集時間を最適化します。テーブルからノードを削除するには、[削除] ボタンをクリックします。

## クラスタおよび分散型展開のログの収集

トラブルシューティングと記録の保存アクティビティをサポートするために、導入環境内のサーバのすべてのログ ファイルを含む zip ファイルを作成できます。

仮想アプライアンス管理インターフェイスの [クラスタ] タブにある [分散導入環境の情報] テーブルには、ログ ファイルが収集されるノードが一覧表示されます。このテーブルからノードを削除することもできます。

vRealize Automation アプライアンスの展開構成の詳細については、vRealize Automation のインストールを参照してください。

### 手順

- 1 仮想アプライアンス管理インターフェイスにシステム管理者としてログインします。
- 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。

各ノードのログ ファイルが収集され、zip ファイルにコピーされます。

## 分散導入環境の情報テーブルからのノードの削除

展開クラスタからノードを削除する場合、または管理エージェント証明書を置き換える場合は、ノードを削除します。

仮想アプライアンス管理インターフェイスの [クラスタ] タブにある [分散導入環境の情報] テーブルには、該当するクラスタのノードが一覧表示されます。テーブルの任意のノードの [削除] ボタンをクリックして、クラスタからそのノードを削除するか、以下の手順を使用できます。

#### 手順

- 1 ユーザー名 **root** と、アプライアンスを展開したときに指定したパスワードを使用して、vRealize Automation アプライアンスにログインします。

- 2 [クラスタ] タブをクリックします。

[分散型展開の情報] テーブルには、分散環境内のノードの一覧が示されます。

- 3 コマンド プロンプトを開いて次のコマンドを実行し、削除するノードのノード ID を見つけます。

```
/usr/sbin/vcac-config cluster-config-node --action list
```

- 4 JSON 出力の中からノード ID (cafe.node.46686239.17144 など) を見つけます。

- 5 コマンド プロンプトを開き、前の手順で取得したノード ID を使用して、次の形式でコマンドを入力します。

```
/usr/sbin/vcac-config cluster-config-node  
--action delete --id node-UID
```

たとえばノード ID cafe.node.46686239.17144 の場合は、次のコマンドを入力します。

```
/usr/sbin/vcac-config cluster-config-node --action delete --id cafe.node.46686239.17144
```

- 6 [更新] をクリックします。

ノードはディスプレイに表示されなくなります。

## vRealize Automation の健全性の監視

vRealize Automation の健全性サービスは、vRealize Automation の機能の健全性を評価します。

IaaS 管理者は、健全性サービスを構成して、コンポーネントが登録されているかどうか、および必要なリソースが使用できるかどうかを判断するテスト スイートを実行します。以下の表に、各健全性サービスで提供されるテスト スイートと、各スイートのテストの例を示します。

健全性サービスのテスト スイート	テストの例
vRealize Automation のシステム テスト	<ul style="list-style-type: none"> <li>■ SSO/Identity 仮想アプライアンスの接続テスト</li> <li>■ vRealize Automation ライセンスのチェック - ライセンスの有効期限が切れているかどうか</li> <li>■ vRealize Automation 仮想アプライアンスの root パスワードのチェック - パスワードの有効期限切れが近いかどうか</li> </ul>
vRealize Automation のテナント テスト	<ul style="list-style-type: none"> <li>■ vSphere 予約ストレージ パスのチェック</li> <li>■ 予約割り当てを行う予約ポリシーのチェック</li> <li>■ ポータル サービスのステータスのチェック</li> </ul>
vRealize Orchestrator のテスト	<ul style="list-style-type: none"> <li>■ vRO のアクティブ ノード数のチェック</li> <li>■ vRO ノードの java メモリ ヒープの使用率のチェック</li> <li>■ vRO ノードの vro サーバ サービスのステータスのチェック</li> </ul>

仮想マシンに対するテスト スイートの実行が完了すると、健全性サービスは合格または失敗したテストの数を報告します。健全性サービスは、失敗したテストごとに以下のリンクを提供します。

リンク	コンテンツ
原因	テストが失敗した理由についての説明。
修正	問題の解決に使用できる情報。

健全性サービスによるテストは、スケジュールに沿って、または必要な場合にのみ実行するように構成できます。

Python を使用して、カスタム テストを作成することができます。『vRealize Automation Health Service Extensibility Guide』を参照してください。

健全性サービス ユーザー ロールを保持しているテナント管理者は、自分のテナントのテスト結果を確認することはできますが、テストを構成したり実行することはできません。

## vRealize Automation のシステム テストの構成

IaaS 管理者は、選択した vRealize Automation 仮想アプライアンスでシステム テストを実行する健全性サービスを構成します。このテストでは、vRealize Automation ライセンスなどのコンポーネントが登録済みであり、メモリなどの必要なリソースが仮想アプライアンスで使用可能であるかどうか判断されます。システム テストを構成すると、[健全性] ページにテストがテスト カードとして表示されます。

健全性サービスを構成して vRealize Automation のシステム テストを実行するには、以下の手順を実行します。

### 前提条件

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

### 手順

- 1 [管理] - [健全性] の順に選択します。
- 2 [新しい構成] をクリックします。



3 [構成の詳細] ページで、必要な情報を提供します。

オプション	説明
Name	この構成のタイトル。このタイトルは、テスト カードに表示されます。
説明	テスト スイートの説明。
製品	vRealize Automation を選択します。
スケジュール	テスト スイートを実行する頻度を選択します。

4 [次へ] をクリックします。

5 [テスト スイートの選択] ページで、[vRealize Automation のシステム テスト] を選択します。

6 [次へ] をクリックします。

7 [パラメータの構成] ページで、必要な情報を提供します。

表 1-18. vRealize Automation 仮想アプライアンス

オプション	説明
公開 Web サーバのアドレス	<ul style="list-style-type: none"> <li>■ 最小インストールの場合、vRealize Automation アプライアンス ホストのベース URL。例: <code>https://va-host.domain/</code></li> <li>■ 高可用性展開の場合、vRealize Automation ロード バランサのベース URL。例: <code>https://load-balancer-host.domain/</code></li> </ul>
SSH コンソールのアドレス	vRealize Automation アプライアンスの完全修飾ドメイン名。 例: <code>va-host.domain</code>
SSH コンソール ユーザー	root
SSH コンソール パスワード	root のパスワード。

表 1-19. vRealize Automation システム テナント

オプション	説明
システム テナント管理者	管理者
システム テナント パスワード	管理者のパスワード。

表 1-20. vRealize Automation ディスク容量の監視

オプション	説明
警告レベルしきい値の割合	仮想アプライアンスのディスク容量の許容可能な使用率。これを超えると警告レベルとなります。
重大レベルしきい値の割合	仮想アプライアンスのディスク容量の許容可能な使用率。これを超えると重大レベルとなります。

8 [次へ] をクリックします。

9 [サマリ] ページで情報を確認します。

**10** [完了] をクリックします。

選択したスケジュールに沿ってテストが実行されます。

## 次のステップ

[vRealize Automation 健全性サービスのテスト スイート結果の表示](#)

**vRealize Automation のテナント テストの構成**

IaaS 管理者は、選択した vRealize Automation 仮想アプライアンスでテナント テストを実行する健全性サービスを構成します。このテストでは、ソフトウェア サービスなどのテナント関連コンポーネントが登録済みであり、vSphere 仮想マシンなどの必要なリソースが仮想アプライアンスで使用可能であるかどうか判断されます。テナント テストを構成すると、[健全性] ページにテストがテスト カードとして表示されます。

健全性サービスを構成して vRealize Automation のテナント テストを実行するには、以下の手順を実行します。

**前提条件**

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

**手順**

- 1** [管理] - [健全性] の順に選択します。
- 2** [新しい構成] をクリックします。
- 3** [構成の詳細] ページで、必要な情報を提供します。

オプション	説明
Name	この構成のタイトル。このタイトルは、テスト カードに表示されます。
説明	テストの説明。
製品	vRealize Automation を選択します。
スケジュール	これらのテストを実行する頻度を選択します。

- 4** [次へ] をクリックします。
- 5** [テスト スイートの選択] ページで、[vRealize Automation のテナント テスト] を選択します。
- 6** [次へ] をクリックします。

## 7 [パラメータの構成] ページで、必要な情報を提供します。

表 1-21. vRealize Automation 仮想アプライアンス

オプション	説明
vRealize Automation Web アドレス	<ul style="list-style-type: none"> <li>■ 最小インストールの場合、vRealize Automation アプライアンス ホストのベース URL。例 : <code>https://va-host.domain/</code></li> <li>■ 高可用性展開の場合、vRealize Automation ロード バランサのベース URL。例 : <code>https://load-balancer-host.domain/</code></li> </ul>
SSH コンソールのアドレス	SSH ホストの完全修飾ドメイン名。例 : <code>ssh-host.domain</code>
SSH コンソール ユーザー	root
SSH コンソール パスワード	root のパスワード。
サービスの応答の最大時間 (ミリ秒)	システムが応答を待機する時間の最大値 (ミリ秒)。

表 1-22. vRealize Automation テナント

オプション	説明
テスト対象テナント	qe
ファブリック管理者ユーザー名	ファブリック管理者のユーザー名。  <b>注：</b> すべてのテストを実行するために、このファブリック管理者にはテナント管理者と IaaS 管理者のロールも必要です。
ファブリック管理者パスワード	ファブリック管理者のパスワード。

表 1-23. vRealize Automation システム テナント

オプション	説明
システム テナント管理者	管理者
システム テナント パスワード	管理者のパスワード。

表 1-24. vRealize Automation ディスク容量の監視

オプション	説明
重大レベルしきい値の割合	仮想アプライアンスのディスク容量の許容可能な使用率。これを超えると重大レベルとなります。

## 8 [次へ] をクリックします。

## 9 [サマリ] ページで情報を確認します。

## 10 [完了] をクリックします。

選択したスケジュールに沿ってテストが実行されます。

### 次のステップ

[vRealize Automation 健全性サービスのテスト スイート結果の表示](#)

## vRealize Orchestrator のテストの構成

IaaS 管理者は、vRealize Orchestrator ホスト上の vRealize Orchestrator にテストを実行する健全性サービスを構成します。このテストでは、vro サーバ サービスなどのコンポーネントが登録済みであり、Java メモリ ヒープなどの必要なリソースがホスト マシン上で使用可能であるかどうか判断されます。vRealize Orchestrator テストを構成すると、[健全性] ページにテストがテスト カードとして表示されます。

### 前提条件

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

### 手順

- 1 [管理] - [健全性] の順に選択します。
- 2 [新しい構成] をクリックします。
- 3 [構成の詳細] ページで、必要な情報を提供します。

オプション	説明
Name	この構成のタイトル。このタイトルは、テスト カードに表示されます。
説明	テストの説明。
製品	vRealize Orchestrator を選択します。
スケジュール	これらのテストを実行する頻度を選択します。

- 4 [次へ] をクリックします。
- 5 [テスト スイートの選択] ページで、[vRealize Orchestrator のテスト] を選択します。
- 6 [次へ] をクリックします。
- 7 [パラメータの構成] ページで、必要な情報を提供します。

表 1-25. vRealize Orchestrator ホスト/ロード バランサ

オプション	説明
クライアント アドレス	<ul style="list-style-type: none"> <li>■ 最小インストールの場合は、vRealize Orchestrator ホストの完全修飾ドメイン名。たとえば、<code>vro-host.domain</code>。</li> <li>■ 高可用性展開の場合、vRealize Orchestrator ロード バランサのベース URL (<code>https://load-balancer-host.domain/</code>)。</li> </ul>
クライアント ユーザー名	管理者
クライアント パスワード	管理者のパスワード。
SSH コンソール ユーザー名	root

表 1-25. vRealize Orchestrator ホスト/ロード バランサ （続き）

オプション	説明
SSH コンソール パスワード	root のパスワード。
ヒープ使用率のしきい値	ヒープ容量の許容可能な使用率。これを超えると警告レベルとなります。

表 1-26. ロード バランサの背後にある vRealize Orchestrator インスタンス

オプション	説明
SSH コンソールのアドレス	ロード バランサの背後にある vRealize Orchestrator インスタンスの IP アドレスまたは URL。
SSH コンソール ユーザー名	このインスタンスへのアクセス権を持つユーザー名。
SSH コンソール パスワード	このユーザー名のパスワード。

- vRealize Orchestrator インスタンスをリストに追加するには、[追加] をクリックします。
- 選択した vRealize Orchestrator インスタンスをロード バランサの背後にあるインスタンスのリストから削除するには、[削除] をクリックします。

8 [次へ] をクリックします。

9 [サマリ] ページで情報を確認します。

10 [完了] をクリックします。

選択したスケジュールに沿ってテストが実行されます。

#### 次のステップ

[vRealize Automation 健全性サービスのテスト スイート結果の表示](#)

## カスタム テスト スイート

Python を使用して、vRealize Automation の健全性サービスのカスタム テスト スイートを作成できます。

カスタム テスト スイートを作成すると、追加の vRealize Automation コンポーネントの健全性を判断するテスト スイートを追加して、健全性サービス用に指定したテストを拡張することができます。カスタム テスト スイートの作成については、『vRealize Automation Health Service Extensibility Guide』を参照してください。

### カスタム テスト スイートの追加

IaaS 管理者は、テスト スイートを実行する前に vRealize Automation 健全性サービスにカスタム テスト スイートを追加する必要があります。

vRealize Automation アセットのカスタム テストを追加するには、この手順を完了します。

#### 前提条件

- カスタム テスト スイート ファイル用の Python Wheel を作成します。詳細については、「vRealize Automation Health Service Extensibility Guide」を参照してください。

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

#### 手順

- 1 [管理] - [健全性] の順にクリックします。
- 2 右上の歯車アイコンをクリックし、[拡張] を選択します。
- 3 [新規アセット] をクリックします。
- 4 [アセットの追加] ダイアログ ボックスで、必要な情報を提供します。

オプション	説明
アセットのタイトル	Infoblox 1.0 など、実行しているテスト スイートの名前とバージョン番号。
アセットの説明	Python Wheel に含まれているテストの説明。
アセットのバージョン	テスト スイートのバージョン番号。
アセット ファイル	[ファイルの選択] をクリックし、カスタム テスト スイートのファイルを選択します。

- 5 [追加] をクリックします。

新しい行がアセット テーブルに追加され、ステータスが [アップロード済み] になります。ステータスが [インストール済み] になると、テスト スイートを使用する準備が整ったことになります。インストール プロセスが失敗した場合、理由を示すポップアップが表示されます。

**注：** ページが更新されない場合は、更新アイコンをクリックします。

#### 次のステップ

[カスタム テスト スイートの実行。](#)

### カスタム テスト スイートの実行

IaaS 管理者は、vRealize Automation 環境でカスタム テスト スイートを実行する健全性サービスを構成します。カスタム テスト スイートを構成すると、[健全性] ページにテスト スイートがテスト カードとして表示されます。

健全性サービスを構成して vRealize Automation のカスタム テスト スイートを実行するには、以下の手順を実行します。

#### 前提条件

- [カスタム テスト スイートの追加。](#)
- IaaS 管理者として vRealize Automation にログインします。

#### 手順

- 1 [管理] - [健全性] の順に選択します。
- 2 [新しい構成] をクリックします。

### 3 [構成の詳細] ページで、必要な情報を提供します。

オプション	説明
Name	この構成のタイトル。このタイトルは、テスト カードに表示されます。
説明	テスト スイートの説明。
製品	[製品] ドロップダウン メニューから、テストする製品を選択します。
スケジュール	このテスト スイートを実行する頻度を選択します。

### 4 [次へ] をクリックします。

### 5 [テスト スイートの選択] ページで、カスタム テスト スイートを選択し、[次へ] をクリックします。

### 6 [パラメータの構成] ページで必要な情報を入力し、[次へ] をクリックします。

### 7 [サマリ] ページで情報を確認し、[完了] をクリックします。

選択したスケジュールどおりにカスタム テスト スイートが実行されます。

#### 次のステップ

[vRealize Automation 健全性サービスのテスト スイート結果の表示](#)

## vRealize Automation 健全性サービスのテスト スイート結果の表示

テストを実行した後、健全性サービスのテスト結果を表示できます。

[健全性] ページに、設定済みの各テスト スイートがテスト カードとして表示されます。テスト スイートを実行すると、テスト カードの中に結果が表示されます。

[健全性] ページに表示されるテスト カードは、権限でフィルタされます。

- IaaS 管理者は、すべてのテスト カードを表示できます。
- 健全性サービス ユーザー ロールを持つテナント管理者は、自分のテナントのテスト カードのみを表示できます。

#### 前提条件

- 設定済みのテスト スイートがスケジュールどおりに実行されました。
- IaaS 管理者またはテナント管理者として、vRealize Automation コンソールにログインします。

#### 手順

- 1 [管理] - [健全性] の順に選択します。
- 2 テストの実行をスケジュール設定していない場合、テスト カードの [実行] をクリックします。
- 3 テストの完了後、テスト カードの中央をクリックします。

各テストのステータスを示すページが表示されます。テストが失敗した理由を表示するには、[原因] をクリックします。[修正] リンクが使用できる場合には、リンクをクリックし、問題を解決する方法についてのトピックを開きます。

## 健全性サービスのトラブルシューティング

健全性サービスのトラブルシューティングに関するトピックでは、健全性サービスを使用する場合に発生する可能性のある問題の解決策について説明します。

### サービス ステータス テストの失敗

失敗したサービス テストは、テストのスケジュール設定を変更することで解決できます。

#### 問題

サービス ステータス テストが失敗した場合、[原因] をクリックすると、「SSH 接続を確立できません。例外メッセージ: [認証失敗]」というメッセージが表示されます。

#### 原因

テスト スイートを 15 分ごとに実行するようにスケジューリングされている場合、システムのログインによって root ユーザー アカウントがロックされます。

#### 解決方法

- ◆ テスト スケジュールを [なし] に変更し、15 分間待ってから、もう一度テスト スイートを実行します。

### アップグレード後、アプライアンス コンソールの [健全性] ページに何も表示されない

vRealize Automation をアップグレードした後、アプライアンス コンソールの [健全性] ページに何も表示されません。

#### 問題

健全性サービスは、アップグレード後に開始されません。

#### 解決方法

- ◆ 各 vRealize Automation 仮想アプライアンスで **root** ユーザーとしてコマンド プロンプトを開き、次のコマンドを実行します。

- a 健全性サービスが自動的に開始されるように設定するには、次のコマンドを実行します。

```
chkconfig vrhb-service on
```

- b この仮想アプライアンスで健全性サービスを開始するには、次のコマンドを実行します。

```
service vrhb-service start
```

## SNMP を使用した vRealize Automation 環境リソースの監視

SNMP に精通したシステム管理者は、vSNMP の vRealize Automation REST API を使用して vRealize Automation ノードを効率的に監視できます。vSNMP を使用すると、vRealize Automation で CPU、RAM、ディスク容量が不足しているときにパフォーマンスの低下を回避するために、暗号化された早期警告システムとして SNMP を使用できます。

SNMP OID を手動で監視することも、SNMP トラップを設定してリソースをアクティブに監視することもできます。



たとえば、「高い CPU 使用率が検出されました」などのイベントが vSNMP から送信された場合に、CPU 使用の多いプロセスに関する情報の収集を開始し、リソースを余分に使用しているプロセスを決定できます。CPU やメモリなどの使用率を関連付けることで、その他の問題をトラブルシューティングすることもできます。

vRealize Automation vSNMP を使用すると、REST API を使用するか vRealize Automation インスタンスで実行されている vSNMPD デーモンを使用することにより、Linux ツリー全体を公開し、データを監視および取得することができます。

vRealize Automation SNMP には汎用的なユーザー インターフェイスがありません。REST API またはデーモン コマンドを使用する必要があります。

詳細については、vRealize Automation プログラミング ガイドで「Using SNMP to Monitor vRealize Automation」を参照してください。プログラミング ガイドについては、[vRealize Automation API ドキュメント](#)にアクセスし、該当するバージョンのリンクを選択してください。

## リソースの監視および管理

さまざまな vRealize Automation ロールがリソース使用量を監視し、異なる方法でインフラストラクチャを管理します。

### リソース監視シナリオの選択

ファブリック管理者、テナント管理者、およびビジネス グループ マネージャには、リソース監視に関して異なる課題があります。このため、vRealize Automation により、リソース使用量のさまざまな側面を監視できます。

たとえば、ファブリック管理者は、予約およびコンピュート リソースのリソース消費の監視に注目し、テナント管理者は、テナント内のプロビジョニング グループのリソース使用量に注目します。ユーザーのロールおよび監視する特定のリソース使用量に応じて、vRealize Automation により、リソース消費をさまざまな方法で追跡できます。

表 1-27. リソース監視シナリオの選択

リソース監視シナリオ	必要な権限	場所
現在使用しているコンピュート リソースの物理ストレージとメモリの容量を監視し、空き容量を特定します。また、各コンピュート リソースにプロビジョニングされた予約マシンおよび割り当てマシンの数を監視できます。	ファブリック管理者（ファブリック グループ内のコンピュート リソースのリソース使用量の監視）	[インフラストラクチャ] - [コンピュート リソース] - [コンピュート リソース]
現在プロビジョニングされており、vRealize Automation の管理下にあるマシンを監視します。	ファブリック管理者	[インフラストラクチャ] - [マシン] - [管理対象マシン]

表 1-27. リソース監視シナリオの選択（続き）

リソース監視シナリオ	必要な権限	場所
現在割り当てられている予約のストレージとメモリの容量およびマシン割り当てを監視し、予約に使用可能な残りの容量を特定します。	ファブリック管理者（コンピュート リソースおよび物理マシンの予約のリソース使用量の監視）	[インフラストラクチャ] - [予約] - [予約]
ビジネス グループが現在使用しているストレージとメモリの容量およびマシンの割り当てを監視し、ビジネス グループの予約に残された容量を特定します。	<ul style="list-style-type: none"> <li>■ テナント管理者（テナント内のすべてのグループのリソース使用量の監視）</li> <li>■ ビジネス グループ マネージャ（管理するグループのリソース使用量の監視）</li> </ul>	[管理] - [ユーザーおよびグループ] - [ビジネス グループ]

## リソース使用量の用語集

vRealize Automation では、使用できるリソース、特定の用途のために確保されているリソース、プロビジョニングされたマシンによってアクティブに消費されているリソースなどが、明示的な用語を使用して区別されています。

以下の表「リソース使用量の用語集」では、vRealize Automation でリソース使用量を表示するために使用する用語を説明します。

表 1-28. リソース使用量の用語集

用語	説明
[物理]	コンピュート リソースの実際のメモリまたはストレージ容量を示します。
[予約済み]	予約のために確保されたマシン割り当て、メモリ、ストレージ容量などを示します。たとえば、コンピュート リソースの物理容量が 600 GB で、100 GB の予約が 3 つ存在する場合、このコンピュート リソースの予約済みストレージの量は 300 GB で、予約済みストレージの割合は 50% です。
[管理対象]	マシンがプロビジョニングされ、現在 vRealize Automation の管理下にあることを示します。
[割り当て済み]	プロビジョニングされたマシンでアクティブに消費されているマシン割り当て、メモリ、ストレージ リソースなどを示します。たとえば、マシン割り当てが 10 である予約があるとしします。この予約にプロビジョニングされたマシンが 15 台存在しても、そのうちの 6 台だけがパワーオン状態の場合、マシン割り当ては 60% が割り当てられていることになります。
[使用済み]	[使用済み] 列の値は、[割り当て済み] 列の値と常に等しくなります。
[空き]	ストレージ パス上の未使用の物理容量を示します。

## クラウド マシンへの接続

クラウド マシンに初めて接続するときは、管理者としてログインする必要があります。

マシンのユーザーとして vRealize Automation コンソールにログインする認証情報を追加すると、それ以降は vRealize Automation 認証情報でログインできます。

**重要：** Amazon Web Services を使用している場合、Amazon マシンのインスタンスで RDP または SSH が有効化され、正しいポートが開かれている Security Group にマシンが属している必要があります。

## Amazon マシンのユーザー証明書の収集

Amazon マシンに管理者としてログインするには、マシンの管理者パスワードを知る必要があります。

管理者パスワードは、[マシン情報詳細] ページにあります。Amazon マシンがプロビジョニングされたマシン イメージがブートごとに管理者パスワードを生成するように構成されていない場合、別の方法でパスワードを見つける必要があります。管理者パスワードの他の取得方法については、Amazon のドキュメントのトピック「*Amazon EC2 インスタンスへの接続*」を検索してください。

必要に応じて、必要な vRealize Automation ユーザー認証情報を作成できます。ユーザー認証情報は、そのマシンに対する以降のログインで有効になります。

### 前提条件

- Amazon マシンはすでにプロビジョニングされています。
- マシン所有者、ビジネス グループ マネージャ、またはサポート ユーザーとして vRealize Automation にログインします。
- プロビジョニングに使用する Amazon マシン イメージでは RDP または SSH は有効です。
- マシンは、正しいポートが開かれているセキュリティ グループに属しています。

### 手順

- 1 [アイテム] ページに移動し、管理するグループまたは特定のグループでフィルタリングします。
- 2 マシンのリストで Amazon マシンを選択します。  
[アクション] ドロップダウン メニューで [詳細表示] をクリックすると、マシン タイプなどの詳細を表示できます。
- 3 [アクション] ドロップダウン メニューで [編集] を選択します。
- 4 [管理者パスワードの表示] をクリックし、マシンの管理者パスワードを取得します。  
または、外部の Amazon の手順を使用してパスワードを取得することもできます。
- 5 [アクション] ドロップダウン メニューから [RDP を使用して接続] をクリックします。
- 6 ログイン認証情報を求められたら、[ユーザーの別のアカウント] をクリックします。
- 7 ユーザー名を求められたら、**LOCAL\Administrator** と入力します。
- 8 プロンプトが表示された場合は、管理者パスワードを入力します。
- 9 [OK] をクリックします。  
これで、管理者としてマシンにログインしました。
- 10 必要に応じて vRealize Automation 認証情報を追加します。たとえば、Windows サーバ マシンでサーバ マネージャを開き、[構成] - [ローカル ユーザーとグループ] を選択します。**DOMAIN\username** の形式を使用して、[リモート デスクトップ ユーザー] グループに認証情報を追加します。  
vRealize Automation のユーザー名とパスワードは、このマシンに対する以降のログインで有効な認証情報になりました。
- 11 Amazon マシンからログアウトします。

12 [アクション] ドロップダウン メニューから [RDP を使用して接続] をクリックします。

13 ログインを求められたら、vRealize Automation のユーザー名とパスワードの認証情報を入力してマシンにログインします。

## 結果

マシン所有者は、vRealize Automation の認証情報を使用してマシンにログインできます。

## vCloud マシンのユーザー認証情報の収集

vCloud Air または vCloud Director マシンに管理者としてログインするには、マシンの管理者パスワードを知る必要があります。

管理者パスワードは、[マシン情報詳細] ページにあります。マシンがプロビジョニングされたマシン イメージがブートごとに管理者パスワードを生成するように構成されていない場合、別の方法でパスワードを見つけることができません。管理者パスワードの別の取得方法については、vCloud Air または vCloud Director のドキュメントを参照してください。

必要に応じて、必要な vRealize Automation ユーザー認証情報を作成できます。ユーザー認証情報は、そのマシンに対する以降のログインで有効になります。

## 前提条件

- vCloud Air または vCloud Director マシンはすでにプロビジョニングされています。
- マシン所有者、ビジネス グループ マネージャ、またはサポート ユーザーとして vRealize Automation にログインします。
- プロビジョニングに使用する vCloud Air または vCloud Director マシン イメージでは RDP または SSH は有効です。
- マシンは、正しいポートが開かれているセキュリティ グループに属しています。

## 手順

1 [アイテム] ページに移動し、管理するグループまたは特定のグループでフィルタリングします。

2 マシンのリストで vCloud Air または vCloud Director マシンを選択します。

[アクション] ドロップダウン メニューで [詳細表示] をクリックすると、マシン タイプなどの詳細を表示できます。

3 [アクション] ドロップダウン メニューで [編集] を選択します。

4 [管理者パスワードの表示] をクリックし、マシンの管理者パスワードを取得します。

または、外部の vCloud Air または vCloud Director の手順を使用してパスワードを取得することもできます。

5 [アクション] ドロップダウン メニューから [RDP を使用して接続] をクリックします。

6 ログイン認証情報を求められたら、[ユーザーの別のアカウント] をクリックします。

7 ユーザー名を求められたら、**LOCAL\Administrator** と入力します。

8 プロンプトが表示された場合は、管理者パスワードを入力します。

## 9 [OK] をクリックします。

これで、管理者としてマシンにログインしました。

## 10 必要に応じて vRealize Automation 認証情報を追加します。たとえば、Windows サーバ マシンでサーバ マネージャを開き、[構成] - [ローカル ユーザーとグループ] を選択します。DOMAIN\username の形式を使用して、[リモート デスクトップ ユーザー] グループに認証情報を追加します。

vRealize Automation のユーザー名とパスワードは、このマシンに対する以降のログインで有効な認証情報になりました。

## 11 vCloud Air または vCloud Director マシンからログアウトします。

## 12 [アクション] ドロップダウン メニューから [RDP を使用して接続] をクリックします。

## 13 ログインを求められたら、vRealize Automation のユーザー名とパスワードの認証情報を入力してマシンにログインします。

### 結果

マシン所有者は、vRealize Automation の認証情報を使用してマシンにログインできます。

## 予約使用の自然減的な減少

ファブリック管理者は、特定の予約とその予約でプロビジョニングされている既存のマシンをアクティブな状態に保持したまま、その予約のマシン数を長期的に減らしていくことができます。

管理者は、仮想予約に予約されたマシン割り当て、メモリ、およびストレージを、現在割り当てられている量を下回るように減らすことができます。このように減らすと、既存マシンを変更することなくそれらの管理を継続し、割り当てが新しい予約量を下回るまで、新しいマシンのプロビジョニングを防止できます。

**注：** パワーオフ状態の仮想マシンは、割り当て済みメモリ（割り当てられるメモリ）とマシン割り当て合計に含まれることはありません。このため、予約のメモリまたはマシンの割り当てを減らすと、現在パワーオフ状態にあるマシンがパワーオン状態に戻らなくなることがあります。

たとえば、あるビジネス グループに、次の 90 日以内に期限が切れるように設定されたプロビジョニング済みマシンを 20 台含む予約が存在するとします。マシンが 15 台未満になるまでこの予約を自然減的に減らす場合には、予約を編集して割り当てを 20 マシンから 15 に減らすことができます。今後の期限切れによって予約のマシンの数が自然に減るまでは、この予約でこれ以上マシンをプロビジョニングすることはできません。

## ストレージ パスの廃止

ストレージ パスを廃止して、新しいパスにマシンを移動する場合、ファブリック管理者は、vRealize Automation でこのストレージ パスを無効にする必要があります。

ストレージ パスを廃止するのに必要な手順の概要は次のとおりです。

- 1 ファブリック管理者は、ストレージ パスを使用するすべての予約でこのストレージ パスを無効にします。[ストレージ パスの無効化](#)を参照してください。
- 2 vRealize Automation の外にある新しいストレージ パスにマシンを移動します。

- 3 vRealize Automation が、インベントリ データの収集を自動で実行したり、インベントリ データの収集を手動で開始するのを待ちます。[コンピュー ト リソース データ収集の設定](#)を参照してください。

## ストレージ パスの無効化

ストレージ パスが廃止された場合、ファブリック管理者は、予約時にストレージ パスを無効にすることができます。

**注：** ストレージ パスを無効にする予約ごとに、他の有効なストレージ パスに十分な容量が残されていることを確認します。

### 前提条件

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

### 手順

- 1 [インフラストラクチャ] - [予約] - [予約] を選択します。
- 2 廃止するストレージ パスを使用している予約をポイントして、[編集] をクリックします。
- 3 [リソース] タブをクリックします。
- 4 廃止するストレージ パスを特定します。
- 5 [編集] アイコン (✎) をクリックします。
- 6 [無効化] 列のチェック ボックスを選択し、このストレージ パスを無効にします。
- 7 [保存] アイコン (✓) をクリックします。
- 8 [OK] をクリックします。
- 9 廃止するストレージ パスを使用しているすべての予約に対してこの手順を繰り返します。

## データ収集

vRealize Automation は、インフラストラクチャ ソース エンドポイントとそれらのコンピュー ト リソースからデータを収集します。

データは定期的に収集されます。データ収集のタイプごとに、オーバーライドまたは変更が可能なデフォルトの間隔があります。また、データ収集のタイプごとに、オーバーライドまたは変更が可能なデフォルトのタイムアウト間隔があります。

IaaS 管理者は、インフラストラクチャ ソース エンドポイントのデータ収集を手動で開始することができ、ファブリック管理者は、コンピュー ト リソースのデータ収集を手動で開始できます。

表 1-29. データ収集タイプ

データ収集タイプ	説明
インフラストラクチャ ソース エンドポイント データの収集	仮想化環境用の仮想化ホスト、テンプレート、および ISO イメージに関する情報を更新します。vCloud Director の仮想データセンターとテンプレートをアップデートします。Amazon リージョンと Amazon リージョンでプロビジョニングされたマシンを更新します。エンドポイント データの収集は 4 時間ごとに実行されます。
インベントリ データの収集	リソース使用状況が特定のコンピュート リソースに関連付けられている、仮想マシンのレコード（ネットワーク、ストレージ、および仮想マシンに関する詳細情報を含む）を更新します。このレコードには、管理されていない仮想マシン（vRealize Automation 以外でプロビジョニングされたマシン）に関する情報も含まれます。 インベントリ データの収集は 24 時間ごとに実行されます。 インベントリ データの収集のデフォルトのタイムアウト間隔は 2 時間です。
状態データの収集	インベントリ データの収集によって検出された各マシンの電源状態のレコードを更新します。また、状態データの収集では、vRealize Automation で管理されているにもかかわらず、仮想化コンピュート リソースまたはクラウド エンドポイントで検出できなかった不明マシンを記録します。 状態データの収集は 15 分ごとに実行されます。 状態データの収集のデフォルトのタイムアウト間隔は 1 時間です。
パフォーマンス データの収集（vSphere コンピュート リソースのみ）	インベントリ データの収集によって検出された各仮想マシンの CPU、ストレージ、メモリ、およびネットワークの平均使用量のレコードを更新します。 パフォーマンス データの収集は 24 時間ごとに実行されます。 パフォーマンス データの収集のデフォルトのタイムアウト間隔は 2 時間です。
ネットワークおよびセキュリティ インベントリ データの収集（vSphere コンピュート リソースのみ）	インベントリ データの収集によって検出された各マシンの vCloud Networking and Security と NSX に関連するネットワークおよびセキュリティ データのレコード（特に、セキュリティ グループとロード バランシングに関する情報）を更新します。
WMI データの収集（Windows コンピュート リソースのみ）	各 Windows マシンの管理データのレコードを更新します。WMI エージェントは、通常 Manager Service ホストにインストールして、Windows マシンからデータを収集できるようにする必要があります。

## 手動によるエンドポイント データ収集の開始

エンドポイント データ収集は 4 時間ごとに自動的に実行されますが、プロキシ エージェントを必要としないエンドポイントについては、IaaS 管理者が任意の時点でエンドポイント データ収集を手動で開始できます。

[データ収集] ページには、データ収集のステータスおよび存続期限についての情報が表示されます。このページで、新しいエンドポイント データ収集を手動で開始できます。

### 前提条件

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

**手順**

- 1 [インフラストラクチャ] - [エンドポイント] - [エンドポイント] を選択します。
- 2 データ収集を実行するエンドポイントの行をクリックします。
- 3 使用可能なデータ収集アクションを選択します。

**コンピュート リソース データ収集の設定**

データ収集の有効化や無効化、データ収集の頻度の設定、あるいはデータ収集の手動による申請を実行することができます。

[データ収集] ページには、データ収集のステータスおよび経過時間に関する情報が表示されます。また、コンピュート リソースのデータ収集を設定することもできます。

**前提条件**

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

**手順**

- 1 [インフラストラクチャ] - [コンピュート リソース] - [コンピュート リソース] を選択します。
- 2 データ収集を設定するコンピュート リソースを指定し、[データ収集] をクリックします。
- 3 [コンピュート リソース] データ収集の仕様を構成します。
  - データ収集を有効にするには [オン] を選択します。
  - データ収集を無効にするには [オフ] を選択します。
- 4 [インベントリ] データ収集を構成します。
  - データ収集を有効にするには [オン] を選択します。
  - データ収集を無効にするには [オフ] を選択します。
  - [頻度] テキスト ボックスに数字を入力してインベントリ データ収集の時間間隔（時間単位）を構成します。
  - 手動でデータ収集を開始する場合は、[今すぐ申請] をクリックします。
- 5 [状態] データ収集を構成します。
  - データ収集を有効にするには [オン] を選択します。
  - データ収集を無効にするには [オフ] を選択します。
  - [頻度] テキスト ボックスに数字を入力して状態データ収集の時間間隔（分単位）を構成します。
  - 手動でデータ収集を開始する場合は、[今すぐ申請] をクリックします。
- 6 [パフォーマンス] データ収集を構成します。
 

このオプションを選択できるのは、vSphere の統合の場合だけです。

  - データ収集を有効にするには [オン] を選択します。
  - データ収集を無効にするには [オフ] を選択します。



- [頻度] テキスト ボックスに数字を入力してパフォーマンス データ収集の時間間隔（時間単位）を構成します。
- 手動でデータ収集を開始する場合は、[今すぐ申請] をクリックします。

## 7 [スナップショット インベントリ] データ収集を構成します。

このオプションは、vRealize Business for Cloud によって管理されるコンピュート リソースの場合に選択できます。

- データ収集を有効にするには [オン] を選択します。
- データ収集を無効にするには [オフ] を選択します。
- [頻度] テキスト ボックスに数字を入力してスナップショット データ収集の時間間隔（時間単位）を構成します。
- 手動でデータ収集を開始する場合は、[今すぐ申請] をクリックします。

## 8 [OK] をクリックします。

## すべてのコンピュート リソースのコスト データのアップデート

ファブリック管理者は、vRealize Business for Cloud により管理されるすべてのコンピュート リソースについて、コスト情報を手動でアップデートできます。

### 前提条件

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

### 手順

- 1 [インフラストラクチャ] - [コンピュート リソース] - [コンピュート リソース] を選択します。
- 2 [コストのアップデート] をクリックします。
- 3 [今すぐ申請] をクリックします。

### 結果

コストのアップデートが完了すると、状態は正常に変更されます。

## vCenter Server エンドポイントの vSwap 割り当てチェックについて

vSwap を使用すると、ターゲット マシン上で最大サイズのスワップ ファイルを作成するためのスワップ空き容量が存在するかどうかを確認できます。vSwap チェックは、vRealize Automation から仮想マシンを作成または再構成する場合に実行されます。vSwap 割り当てチェックは、vCenter Server エンドポイントでのみ使用できます。

vRealize Automation ストレージ割り当てでは、申請の作成や再構成時に仮想マシン ディスクを収容するだけの十分な空き容量がデータストア上に存在するかどうかをチェックします。ただし、マシンをパワーオンする際に、vCenter Server エンドポイントにスワップ ファイルを作成するだけの十分な空き容量がないと、マシンはパワーオンに失敗します。パワーオン操作が失敗すると、そのマシンに依存するすべてのカスタマイズも失敗します。マシンは破棄される場合もあります。申請のサイズによっては、マシンがパワーオンしていない、またはプロビジョニングを実行していないというフィードバックがすぐに得られないことがあります。

vSwap 割り当てチェックを使用して、vCenter Server エンドポイントの vRealize Automation の作成および再構成プロセスの一部として、最大サイズのスワップ ファイルを作成するためのスワップ空き容量が残されているかどうかをチェックすることで、こうした制限を解消することができます。vSwap 割り当てチェックを有効にするには、マシン コンポーネントまたはブループリント全体のカスタム プロパティ `VirtualMachine.Storage.ReserveMemory` を `True` に設定します。

vSwap 割り当てチェックの次の動作に留意してください。

- スワップ ファイルは仮想マシンが格納されているデータストア上に配置されます。スワップ ファイルを専用のまたは異なるデータストア上に配置するための代替 vCenter Server 構成は、サポートされていません。
- スワップ サイズは、仮想マシンを作成または再構成する際に考慮されます。最大スワップ サイズは、仮想マシンのメモリ サイズです。
- ホストの vRealize Automation ストレージ予約の予約値は、コンピュート リソースの物理容量を超えないようにする必要があります。
- 予約を作成するときは、予約値の合計が使用可能なストレージ容量を超えないようにする必要があります。
- vSphere のリソース プール、ホスト レベル、または仮想マシンレベルのメモリ予約は、vSphere エンドポイントからは収集されず、vRealize Automation 上での計算時には考慮されません。
- 既存マシンについては、vSwap によるパワーオン操作時のスワップ空き容量の検証は実行されません。
- vSphere エンドポイントに対する vSwap 関連の変更を取得するには、データ収集を再実行する必要があります。

## データセンターの場所の削除

ユーザー メニューからデータセンターの場所を削除するには、システム管理者は場所ファイルから場所情報を削除し、ファブリック管理者はコンピュート リソースから場所情報を削除する必要があります。

たとえば、場所ファイルにロンドンを追加し、ロンドンと 10 台のコンピュート リソースを関連付け、ファイルからロンドンを削除しても、コンピュート リソースは場所であるロンドンと関連付けられたままで、ロンドンが [マシン申請の確認] ページの場所ドロップダウン リストに引き続き表示されます。ドロップダウン リストから場所を削除するには、ファブリック管理者は、コンピュート リソースを編集して、場所と関連付けられたすべてのコンピュート リソースの場所を空白にリセットする必要があります。

データセンターの場所を削除するのに必要な手順の概要は次のとおりです。

- 1 システム管理者は、場所ファイルからデータセンターの場所情報を削除します。
- 2 ファブリック管理者は、関連付けされた各コンピュート リソースの場所を編集することで、場所とすべてのコンピュート リソースとの関連を削除します。

## コンテナの監視

vRealize Automation のコンテナ で作成したコンテナのステータスを監視することができます。

テンプレートに基づいてコンテナを作成した後、その状態を監視することができます。コンテナの [詳細] をクリックすると、そのコンテナのネットワーク帯域幅、CPU 使用率、メモリ使用量、ログ、プロパティが表示されます。

## 仮想マシンのバルク インポート、アップデート、移行

バルク インポート 機能を使用して、仮想マシンを vRealize Automation にインポート、更新、または移行することができます。バルク インポート は、複数の環境にある複数マシンの管理を効率化します。

バルク インポート では、予約、ストレージ パス、ブループリント、所有者、カスタム プロパティなどの仮想マシンデータの定義を含む CSV ファイルを作成します。この CSV ファイルを使用して、vRealize Automation 環境に仮想マシンをインポートします。バルク インポート は、次の管理タスクをサポートします。

- vRealize Automation 環境で管理できるように、1 台以上の管理対象外の仮想マシンをインポートする。
- ストレージ パスなどの仮想マシンのプロパティをグローバルに変更する。
- vRealize Automation 環境間で仮想マシンを移行する。

**注：** vCloud Director および vSphere のみで、バルク インポートがサポートされます。別のエンドポイント タイプにフィルタを設定すると、CSV ファイルのデータは生成されません。

バルク インポート 機能のコマンドは、vRealize Automation コンソールまたは CloudUtil コマンドライン インターフェイスを使用して実行できます。CloudUtil コマンドライン インターフェイスの使用についての詳細は、ライフ サイクルの拡張性のドキュメントを参照してください。

**注：** マシンのバルク インポートは、通常のプロビジョニング手順をバイパスしません。プロビジョニング中にイベント ブローカによってトリガされた既存の外部ワークフローは、インポートされたマシンに対して実行されます。次のいずれかを実行すると、インポートされたマシンのワークフローを一時的に無効にすることができます。

- すべてのイベント ブローカ サブスクリプションを無効にします。サブスクリプションを無効にする場合は、その間にプロビジョニングされた通常のマシンに拡張が適用されないため、vRealize Automation クラスタのサービス停止をスケジュール設定する必要があります。
- マシンのインポート時にトリガされないように、イベント サブスクリプションに条件を追加します。この条件を追加するには、[イベント サブスクリプション] に移動し、無効にするサブスクリプションを選択して、次のようなカスタム プロパティを追加します: `VirtualMachine.Imported.ConvergedBlueprint` が次と等しくない <インポート ブループリントの ID>。この条件は、通常のプロビジョニングされたマシンには影響せず、代わりに、インポートされたマシンにのみ適用されます。

### 前提条件

- ファブリック管理者およびビジネス グループ マネージャとして vRealize Automation にログインします。
- 固定 IP アドレスを使用する仮想マシンをインポートする場合は、適切に構成されたアドレス プールを準備します。

## vRealize Automation 環境への仮想マシンのインポート

管理対象外の仮想マシンを vRealize Automation 環境にインポートできます。

管理対象外の仮想マシンはハイパーバイザーに存在しますが、vRealize Automation 環境では管理されず、コンソールに表示できません。管理対象外の仮想マシンをインポートすると、その仮想マシンが vRealize Automation 管理インターフェイスで管理されるようになります。必要な権限があれば、その仮想マシンを [管理対象マシン] タブや [展開] タブで確認できます。

バルク インポート オプションは、NSX ネットワークおよびセキュリティ コンポーネントまたはソフトウェア コンポーネントを含むブループリントからプロビジョニングされる展開をサポートしていません。

#### 前提条件

- ファブリック管理者およびビジネス グループ マネージャとして vRealize Automation にログインします。
- 固定 IP アドレスを使用する仮想マシンをインポートする場合は、適切に構成されたアドレス プールを準備します。ネットワーク プロファイルを使用して IP アドレス範囲を制御する方法の詳細については、『vRealize Automation の構成』を参照してください。
- 別の仮想マシンに割り当てられている固定 IP アドレスで仮想マシンをバルク インポートすると、インポートが失敗します。

#### 手順

- 1 イベント ブローカ サブスクリプションを一時的に無効にします。

---

**注：** サブスクリプションを無効にする場合は、vRealize Automation クラスタのサービスを停止するスケジュールを設定する必要があります。このプロセスでは、正常にプロビジョニングされたマシンには拡張性が適用されません。サブスクリプションの無効化に失敗すると、データが失われ、バックアップ インフラストラクチャからマシンが完全に削除される可能性があります。

---

- 2 仮想マシンの CSV データ ファイルを生成します。

- a [インフラストラクチャ] - [管理] - [バルク インポート] を選択します。
- b [CSV ファイルを生成] をクリックします。
- c [マシン] ドロップダウン メニューから [管理されていない] を選択します。
- d [ビジネス グループ] で、ドロップダウン メニューからデフォルト値を選択します。
- e [所有者] のデフォルト値を入力します。
- f [ブループリント] で、ドロップダウン メニューからデフォルト値を選択します。

インポートが成功するためには、このブループリントが公開されていて、資格に追加されている必要があります。

- g [コンポーネント マシン] で、ドロップダウン メニューからデフォルト値を選択します。

[ビジネス グループ] と [ブループリント] の値を選択すると、CSV データ ファイルに次のような結果が含まれることがあります。

- Host Reservation (Name or ID) = INVALID\_RESERVATION
- Host To Storage (Name or ID) = INVALID\_HOST\_RESERVATION\_TO\_STORAGE

これらのメッセージは、選択したビジネス グループに、管理対象外の仮想マシンもホストするホスト仮想マシンの予約がない場合に表示されます。管理対象外の仮想マシンのホストのビジネス グループに予約がある場合、Host Reservation および Host to Storage の値は適切に設定されます。

- h [リソース] ドロップダウン メニューから、使用可能なリソース タイプのいずれかを選択します。

メニュー項目	説明
エンドポイント	仮想ホストへのアクセスに必要な情報。
コンピュータ リソース	同様の機能を実行している仮想マシンのグループへのアクセスに必要な情報。

- i [名前] ドロップダウン メニューから仮想マシン リソースの名前を選択します。
- j [OK] をクリックします。

### 3 仮想マシンの CSV データ ファイルを編集します。

- a CSV ファイルを開いて、データ カテゴリをターゲットである vRealize Automation 環境の既存のカテゴリと一致するように編集します。

CSV データ ファイルに含まれている仮想マシンをインポートするには、各仮想マシンが次のアイテムに関連付けられている必要があります。

- 予約
- ストレージの場所
- ブループリント
- 仮想マシン コンポーネント
- ターゲットの導入環境に存在する所有者

インポートを正常に完了するには、各仮想マシンのすべての値がターゲットの vRealize Automation 環境に存在している必要があります。予約、ストレージの場所、ブループリント、および所有者の値を変更したり、CSV ファイルを編集して個別の仮想マシンに固定 IP アドレス値を追加したりできます。

見出し	コメント
# Import—Yes or No	特定の仮想マシンがインポートされないようにするには、[いいえ]に変更します。
仮想マシン名	変更しないでください。
Virtual Machine ID	変更しないでください。
Host Reservation (Name or ID)	ターゲットの vRealize Automation 環境の予約名または予約 ID を入力します。
Host To Storage (Name or ID)	ターゲットの vRealize Automation 環境のストレージ場所の名前または ID を入力します。
展開名	<p>ターゲットの vRealize Automation 環境で作成する導入単位の新しい名前（仮想マシン名など）を入力します。</p> <p><b>注：</b> 各仮想マシンを固有の導入単位にインポートする必要があります。1 台の仮想マシンを既存の導入単位にインポートしたり、複数の仮想マシンを 1 つの導入単位にインポートすることはできません。</p>
ブループリント ID	<p>仮想マシンのインポートに使用する、ターゲットの vRealize Automation 環境のブループリントの ID を入力します。</p> <p><b>注：</b> ブループリント名ではなく、ブループリント ID のみを入力します。1 つの仮想マシン コンポーネントのみを含むブループリントを選択する必要があります。そのブループリントは、公開されていて、資格に追加されている必要があります。</p> <p>インポートされた仮想マシンの場合は、コンポーネント プロファイルを含むブループリントを関連付けしないでください。メモリやストレージ サイズなど、インポートされた仮想マシンの既存の設定は、プロファイルの制限範囲外の場合があります。その場合、今後のブループリントベースの仮想マシンの再構成に関する検証は失敗します。</p>
コンポーネント マシン ID	選択したブループリントに含まれる仮想マシン コンポーネント名を入力します。複数のコンポーネントを含むブループリントに仮想マシンをインポートすることはできません。
所有者名	そのブループリントに対する資格を付与された、ターゲットの vRealize Automation 環境のユーザーを入力します。

1 つ以上のカスタム プロパティを持つ仮想マシンをインポートする場合は、そのマシンの値を使用して、この行に 3 つのカンマ区切り値を付加することで、各カスタム プロパティを特定します。それぞれのカスタム プロパティに、この形式を使用します。

*,Custom.Property.Name, Value, FLAGS*

FLAGS は、vRealize Automation でプロパティがどのように扱われるかを示す 3 つの文字です。フラグは次の順序で使用され、次の内容を意味します。

- 1 H または N = 非表示または表示
- 2 E または O = 暗号化または非暗号化
- 3 R または P = ランタイムまたは非ランタイム

たとえば、マシンの固定 IP アドレスを構成するカスタム プロパティを追加できます。次の形式を使用すると、このカスタム プロパティにより、ネットワーク プロファイルから使用可能な固定 IP アドレスが割り当てられます。

*,VirtualMachine.Network#.Address, w.x.y.z, HOP*

仮想マシンの適切な情報を使用して、変数を変更します。

- # を、この固定 IP アドレスを使用して構成するネットワーク インターフェイスの番号に変更します。たとえば、VirtualMachine.Network0.Address のように指定します。
- w.x.y.z を、仮想マシンの固定 IP アドレスに変更します。たとえば、11.27.42.57 のように指定します。

HOP のフラグ文字列（非表示、非暗号化、非ランタイム）によって、プロパティを表示するかどうかを設定します。この特定のプロパティはバルク インポートでのみ使用されるため、インポートの完了後に仮想マシンから削除されます。

このカスタム プロパティが動作するためには、適切に構成されたアドレス プールで IP アドレスが使用可能である必要があります。アドレスが見つからない、またはすでに使用されている場合、インポートは固定 IP アドレスの定義をせずに実行され、エラーがログに記録されます。

b CSV ファイルを保存します。

- 4 vRealize Automation 管理インターフェイスを使用して、仮想マシンを vRealize Automation 環境にインポートします。
  - a [インフラストラクチャ] - [管理] - [バルク インポート] を選択します。
  - b [新規] をクリックします。
  - c [名前] テキスト ボックスにこのタスクの一意の名前を入力します（例：unmanaged import 10）。
  - d CSV ファイル名を参照して [CSV ファイル] テキスト ボックスに CSV ファイル名を入力します。

- e インポート オプションを選択します。

オプション	説明
開始時間	開始日のスケジュールを設定します。選択される開始時間はサーバのローカル時間であり、ユーザーのワークステーションのローカル時間ではありません。
現在	インポート処理を直ちに開始します。
遅延 (秒)	多くの仮想マシンをインポートする場合、各仮想マシンの登録を遅延させる秒数を選択します。このメニュー項目を選択すると、インポート処理が遅くなります。遅延なしを選択する場合は空白にします。
バッチ サイズ	多くの仮想マシンをインポートする場合、所定の時間に登録する仮想マシンの総数を選択します。このメニュー項目を選択すると、インポート処理が遅くなります。制限なしを選択する場合は空白にします。
管理対象のマシンを無視	選択しないままにします。
ユーザー検証をスキップ	このメニュー項目を選択すると、ユーザーが存在するかどうかを検証せずに、CSV データファイルの [所有者] 列にリストされた値に仮想マシンの所有者が設定されます。このメニュー項目を選択すると、インポート時間が短くなります。
インポートのテスト	仮想マシンをインポートせずにインポート処理をテストして、CSV ファイルのエラーを検証できます。

- f [OK] をクリックします。

処理の進行状況は、[バルク インポート] ページに表示されます。

## vRealize Automation 環境の仮想マシンの更新

ストレージ パスなどの仮想マシンのプロパティを変更して、vRealize Automation 環境の 1 台以上の管理対象仮想マシンを更新することができます。

管理対象仮想マシンとは、vRealize Automation 環境で管理されているマシンで、コンソールに表示されます。

### 前提条件

- ファブリック管理者およびビジネス グループ マネージャとして vRealize Automation にログインします。

### 手順

- 1 仮想マシンの CSV データ ファイルを生成します。
  - a [インフラストラクチャ] - [管理] - [バルク インポート] を選択します。
  - b [CSV ファイルを生成] をクリックします。
  - c [マシン] ドロップダウン メニューから [管理対象] を選択します。
  - d [リソース] ドロップダウン メニューから、使用可能なリソース タイプのいずれかを選択します。

オプション	説明
エンドポイント	仮想ホストへのアクセスに必要な情報。
コンピュート リソース	同様の機能を実行している仮想マシンのグループへのアクセスに必要な情報。



- e [名前] ドロップダウン メニューから仮想マシン リソースの名前を選択します。
- f (オプション) 仮想マシンのカスタム プロパティを移行する場合は、[カスタム プロパティを含める] を選択します。
- g [OK] をクリックします。

## 2 仮想マシンの CSV データ ファイルを編集します。

- a テキスト エディタで CSV ファイルを開いて、グローバルに変更するデータ カテゴリを編集します。

CSV データ ファイルに含まれている仮想マシンを更新するには、各マシンが次のアイテムに関連付けられている必要があります。

- 予約
- ストレージの場所
- ブループリント
- マシン コンポーネント
- ターゲットの導入環境に存在する所有者

更新を正常に完了するには、各マシンのすべての値がターゲットの vRealize Automation 環境に設定されている必要があります。CSV ファイルを編集して、予約、ストレージ場所、ブループリント、および所有者の値を変更し、個々のマシンに固定 IP アドレス値を追加することができます。

- b 仮想マシンの固定 IP アドレスを変更する場合は、次の形式のコマンドを CSV ファイルに追加します。

```
,VirtualMachine.Network#.Address, w.x.y.z, HOP
```

仮想マシンに適切な情報を使用して、コマンドを構成します。

- # を、この固定 IP アドレスを使用して構成するネットワーク インターフェイスの番号に変更します。たとえば、VirtualMachineNetwork0.Address のように指定します。
- w.x.y.z を、仮想マシンの固定 IP アドレスに変更します。たとえば、11.27.42.57 のように指定します。
- HOP 文字列の Hidden、Not encrypted、Not runtime は、プロパティの可視性を設定します。このデフォルトのプロパティは、インポートの成功後、仮想マシンから削除されます。

更新が成功するには、適切に構成されたアドレス プールで IP アドレスが利用できる必要があります。アドレスが見つからない、またはすでに使用されている場合、更新は固定 IP アドレスの定義をせずに実行され、エラーがログに記録されます。

- c CSV ファイルを保存し、テキスト エディタを閉じます。

## 3 vRealize Automation 管理インターフェイスを使用して、vRealize Automation 環境の 1 つ以上の仮想マシンを更新します。

- a [インフラストラクチャ] - [管理] - [バルク インポート] を選択します。
- b [新規] をクリックします。
- c [名前] テキスト ボックスにこのタスクの一意の名前を入力します (例 : managed global update 10)。

- d CSV ファイル名を参照して [CSV ファイル] テキスト ボックスに CSV ファイル名を入力します。
- e インポート オプションを選択します。

オプション	説明
開始時間	開始日のスケジュールを設定します。 指定される開始時間はサーバのローカル時間であり、ユーザーのワークステーションのローカル時間ではありません。
現在	インポート処理を直ちに開始します。
遅延 (秒)	多数の仮想マシンを更新する場合、各仮想マシンの更新を遅延させる秒数を選択します。このオプションを選択すると、更新処理が遅くなります。遅延を指定しない場合は空白にします。
バッチ サイズ	多数の仮想マシンを更新する場合、所定の時間に更新するマシンの総数を選択します。このオプションを選択すると、更新処理が遅くなります。制限を指定しない場合は空白にします。
管理対象のマシンを無視	選択しないままにします。
ユーザー検証をスキップ	このオプションを選択すると、ユーザーが存在するかどうかを検証せずに、CSV データ ファイルの [所有者] 列にリストされた値にマシンの所有者が設定されます。このオプションを選択すると、更新時間が短くなります。
インポートのテスト	選択しないままにします。

- f [OK] をクリックします。

処理の進行状況は、[バルク インポート] ページに表示されます。

## 別の vRealize Automation 環境への仮想マシンの移行

VMware vRealize™ Automation 環境の 1 つ以上の管理対象仮想マシンを別の vRealize Automation 環境に移行することができます。

管理対象仮想マシンは vRealize Automation 環境で管理されている仮想マシンで、コンソールに表示されます。

### 前提条件

- ファブリック管理者およびビジネス グループ マネージャとして vRealize Automation にログインします。
- 固定 IP アドレスを使用する仮想マシンをインポートする場合は、適切に構成されたアドレス プールを準備します。ネットワーク プロファイルを使用して IP アドレス範囲を制御する方法の詳細については、『vRealize Automation の構成』を参照してください。

### 手順

- 1 仮想マシンの CSV データ ファイルを生成します。
  - a [インフラストラクチャ] - [管理] - [バルク インポート] を選択します。
  - b [CSV ファイルを生成] をクリックします。
  - c [マシン] ドロップダウン メニューから [管理対象] を選択します。

- d [リソース] ドロップダウン メニューから、使用可能なリソース タイプのいずれかを選択します。

オプション	説明
エンドポイント	仮想ホストへのアクセスに必要な情報。
コンピュート リソース	同様の機能を実行している仮想マシンのグループへのアクセスに必要な情報。

- e [名前] ドロップダウン メニューから仮想マシン リソースの名前を選択します。

- f (オプション) [カスタム プロパティを含める] を選択します。

カスタム プロパティを含めるのは、同じプロパティを持つ新しい展開に仮想マシンをインポートする場合です。

- g [OK] をクリックします。

## 2 仮想マシンの CSV データ ファイルを編集します。

CSV データ ファイルを編集する必要があるかどうかは、ソースとターゲットの環境がどのくらい似ているかによって決まります。ソース環境の設定値がターゲット環境の値と一致しない場合は、移行を開始する前に、値が一致するように CSV データ ファイルを編集する必要があります。

- a CSV ファイルを開いて、データ カテゴリをターゲットである vRealize Automation 環境の既存のカテゴリと一致するように編集します。

CSV データ ファイルに含まれている仮想マシンを移行するには、各仮想マシンが予約、ストレージ場所、ブループリント、マシン コンポーネント、ターゲットの vRealize Automation 環境に存在する所有者と関連付けられている必要があります。移行を正常に完了するには、各仮想マシンのすべての値がターゲットの vRealize Automation 環境に存在している必要があります。予約、ストレージの場所、ブループリント、および所有者の値を変更したり、CSV ファイルを編集して個別の仮想マシンに固定 IP アドレス値を追加したりできます。

見出し	コメント	例
# Import--Yes or No	特定の仮想マシンがインポートされないようにするには、[いいえ]に変更します。	はい
Virtual Machine Name	変更しないでください。	MyMachine
Virtual Machine ID	変更しないでください。	a6e05812-0b06-4d4e-a84a-fed242340426a
Host Reservation (Name or ID)	ターゲットの vRealize Automation 環境の予約名または予約 ID を入力します。	DevReservation
Host To Storage (Name or ID)	ターゲットの vRealize Automation 環境のストレージ場所の名前または ID を入力します。	ce-san-1:custom-nfs-2
Deployment Name	ターゲットの vRealize Automation 環境で作成する展開の新しい名前を入力します。  各仮想マシンを独自の展開に移行する必要があります。1 台の仮想マシンを既存の導入単位にインポートしたり、複数の仮想マシンを 1 つの環境にインポートすることはできません。	ImportedDeployment0001
Converged Blueprint ID	仮想マシンのインポートに使用する、ターゲットの vRealize Automation 環境のブループリントの ID を入力します。  入力するのはブループリント ID だけです。ブループリント名は入力しないでください。1 つの仮想マシン コンポーネントのみを含むブループリントを選択する必要があります。そのブループリントは、公開されていて、資格に追加されている必要があります。	ImportBlueprint
Component Blueprint ID	選択したブループリントに含まれる仮想マシン コンポーネント名を入力します。複数のコンポーネントを含むブループリントに仮想マシンをインポートすることはできません。	ImportedMachine
所有者名	ターゲットの vRealize Automation 環境のユーザーを入力します。	user@tenant

適切に書式設定された完全な CSV 行の例を次に示します。Yes, MyMachine,  
a6e05812-0b06-4d4e-a84a-fed242340426, DevReservation, ce-san-1:custom-nfs-2,  
Imported Deployment 0001, ImportBlueprint, ImportedMachine, user@tenant

- b 固定 IP アドレスを持つ仮想マシンを移行する場合、次の形式のコマンドを CSV ファイルに追加します。

`,VirtualMachine.Network#.Address, w.x.y.z, HOP`

仮想マシンに適切な情報を使用して、コマンドを構成します。

- # を、この固定 IP アドレスを使用して構成するネットワーク インターフェイスの番号に変更します。たとえば、VirtualMachineNetwork0.Address のように指定します。
- w.x.y.z を、仮想マシンの固定 IP アドレスに変更します。たとえば、11.27.42.57 のように指定します。
- HOP 文字列の Hidden、Not encrypted、Not runtime は、プロパティの可視性を設定します。このデフォルトのプロパティは、インポートの成功後、仮想マシンから削除されます。

移行が成功するには、適切に構成されたアドレス プールで IP アドレスが利用できる必要があります。アドレスが見つからない、またはすでに使用されている場合、移行は固定 IP アドレスの定義をせずに実行され、エラーがログに記録されます。

- c CSV ファイルを保存します。

- 3** vRealize Automation 管理インターフェイスを使用して、仮想マシンを vRealize Automation 環境に移行します。

- a [インフラストラクチャ] - [管理] - [バルク インポート] を選択します。
- b [新規] をクリックします。
- c [名前] テキスト ボックスにこのタスクの一意の名前を入力します（例：managed migration 10）。
- d CSV ファイル名を参照して [CSV ファイル] テキスト ボックスに CSV ファイル名を入力します。

- e インポート オプションを選択します。

オプション	説明
開始時間	開始日のスケジュールを設定します。 選択される開始時間はサーバのローカル時間であり、ユーザーのワークステーションのローカル時間ではありません。
現在	移行処理を直ちに開始します。
遅延 (秒)	多数の仮想マシンを移行する場合、各仮想マシンの登録を遅延させる秒数を選択します。このオプションを選択すると、移行処理が遅くなります。遅延なしを選択する場合は空白にします。
パッチ サイズ	多数の仮想マシンを移行する場合、所定の時間に登録する仮想マシンの総数を選択します。このオプションを選択すると、移行処理が遅くなります。制限なしを選択する場合は空白にします。
管理対象のマシンを無視	選択しないままにします。
ユーザー検証をスキップ	このオプションを選択すると、ユーザーが存在するかどうかを検証せずに、CSV データ ファイルの [所有者] 列にリストされた値に仮想マシンの所有者が設定されます。このオプションを選択すると、移行時間が短くなります。
インポートのテスト	仮想マシンの移行をせずに移行プロセスをテストして、CSV ファイルのエラーを検証できます。

- f [OK] をクリックします。

処理の進行状況は、[バルク インポート] ページに表示されます。