

vRealize Automation の管理

2022 年 10 月

vRealize Automation 8.7

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

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

ヴィエムウェア株式会社
〒108-0023 東京都港区芝浦 3-1-1
田町ステーションタワー N 18 階
www.vmware.com/jp

Copyright © 2022 VMware, Inc. All rights reserved. 著作権および商標情報。

目次

1 vRealize Automation の管理 5

2 ユーザーの管理 6

Active Directory グループをプロジェクトに対して有効にする方法 7

vRealize Automation でユーザーを削除する方法 8

vRealize Automation でユーザー ロールを編集する方法 8

vRealize Automation でグループ ロールの割り当てを編集する方法 9

vRealize Automation のユーザー ロールについて 9

米国防総省の通知および同意バナーを有効にする 23

3 アプライアンスの保守 25

vRealize Automation の起動と停止 25

単一ノードから 3 ノードへの vRealize Automation のスケール アウト 27

クラスタ化された Workspace ONE Access インスタンスの非アフィニティ ルールと仮想マシン グループの構成 28

アプライアンス ノードの置き換え 29

vRealize Automation アプライアンスのディスク容量の拡張 30

vRealize Automation の DNS 割り当ての更新 31

ノードまたはクラスタの IP アドレスの変更 31

時刻同期を有効にする方法 33

root パスワードをリセットする方法 34

4 vRealize Automation でのマルチ組織テナント構成の使用 36

vRealize Automation のマルチ組織テナントの設定 38

単一ノードのマルチ組織環境での証明書および DNS 構成の管理 40

クラスタ化された vRealize Automation 展開での証明書および DNS 構成の管理 42

テナントへのログインおよび vRealize Automation へのユーザーの追加 44

vRealize Orchestrator と vRealize Automation マルチ組織展開の使用 45

5 ログの操作 46

ログおよびログ バンドルを操作する方法 46

vRealize Log Insight へのログ転送を設定する方法 50

Syslog 統合を作成または更新する方法 54

ログインのための Syslog 統合を削除する方法 55

コンテンツ バックの使用方法 56

6 カスタマー エクスペリエンス向上プログラムへの参加 59

プログラムに参加または離脱する方法 59

プログラムのデータ収集時間を設定する方法 60

7 製品内フィードバック フォームの有効化 61

vRealize Automation の管理

1

このガイドでは、vRealize Automation 環境の重要なインフラストラクチャとユーザー管理の面を監視および管理する方法について説明します。

ここに記載されているタスクは、vRealize Automation の展開を適切に運用するために不可欠です。これらのタスクには、ユーザーとグループの管理、システム ログの監視などがあります。

また、マルチ組織展開を構成および管理する方法についても説明します。

vRealize Automation の一部の管理タスクは vRealize Automation 内で完結しますが、他のタスクは vRealize Suite Lifecycle Manager や Workspace ONE Access などの関連製品を使用する必要があります。ユーザーは、該当するタスクを完了する前に、これらの製品とその機能について理解しておく必要があります。

たとえば、バックアップ、リストア、およびディザスタ リカバリの詳細については、[vRealize Suite 製品ドキュメント](#)の「[[Backup and Restore, and Disaster Recovery > 2019]]」セクションを参照してください。

注： ディザスタ リカバリは、vRealize Automation 8.0.1 以降でサポートされています。

vRealize Suite Lifecycle Manager のインストール、アップグレード、管理の操作の詳細については、[Lifecycle Manager 製品ドキュメント](#)を参照してください。

vRealize Automation でのユーザーとグループの管理

2

vRealize Automation では、VMware が提供する ID 管理アプリケーションである VMware Workspace ONE Access を使用して、ユーザーとグループをインポートおよび管理します。ユーザーとグループをインポートまたは作成すると、[ID およびアクセス権の管理] 画面を使用して、単一テナント展開のロール割り当てを管理できます。

vRealize Automation のインストールには、VMware Lifecycle Manager (vRSLCM または LCM) を使用します。vRealize Automation をインストールするときは、ID 管理をサポートするために、既存の Workspace ONE Access インスタンスをインポートするか、新しい Workspace ONE Access インスタンスを展開する必要があります。この 2 つのシナリオにより、管理オプションが定義されます。

- 新しい Workspace ONE Access インスタンスを展開する場合は、LCM を介してユーザーとグループを管理できます。インストール時に、Workspace ONE Access を使用して Active Directory 接続を設定できます。または、以下で説明する [ID およびアクセス権の管理] ページを使用して、vRealize Automation 内でユーザーおよびグループのいくつかの側面を表示および編集できます。
- 既存の Workspace ONE Access インスタンスを使用する場合は、インストール時に LCM を介して、vRealize Automation で使用するインスタンスをインポートします。この場合、ユーザーとグループの管理用に引き続き Workspace ONE Access を使用することも、LCM の管理機能を使用することもできます。

マルチ組織展開でのユーザー管理の詳細については、[テナントへのログインおよび vRealize Automation へのユーザーの追加](#)を参照してください。

vRealize Automation ユーザーにはロールを割り当てる必要があります。ロールは、アプリケーション内の機能へのアクセスを定義します。Workspace ONE Access インスタンスを使用して vRealize Automation をインストールする場合は、デフォルトの組織が作成され、インストーラには「組織の所有者」ロールが割り当てられます。他のすべての vRealize Automation ロールは、組織の所有者によって割り当てられます。

vRealize Automation には、組織ロール、サービス ロール、プロジェクト ロールという 3 つのタイプのロールがあります。Cloud Assembly、Service Broker、および Code Stream では、通常、ユーザー レベルのロールでリソースを使用できますが、リソースを作成および構成するには管理者レベルのロールが必要です。組織ロールは、テナント内の権限を定義するものです。組織の所有者は管理者レベルの権限を持ち、組織のメンバーはユーザー レベルの権限を持ちます。組織の所有者は、他のユーザーを追加および管理できます。

組織ロール	サービス ロール
■ 組織の所有者	■ Cloud Assembly 管理者
■ 組織のメンバー	■ Cloud Assembly ユーザー
	■ Cloud Assembly 閲覧者
	■ Service Broker 管理者
	■ Service Broker ユーザー
	■ Service Broker 閲覧者
	■ Code Stream 管理者
	■ Code Stream ユーザー
	■ Code Stream ビューア

表に示したロールに加えて、さらにプロジェクト管理者、プロジェクト ユーザーという 2 つの主なプロジェクト レベルのロールがあります。これらのロールは、Cloud Assembly でプロジェクトごとに個別に割り当てられます。これらはやや流動的なロールです。あるプロジェクトの管理者を別のプロジェクトのユーザーにすることもできます。詳細については、[vRealize Automation のユーザー ロールについて](#)を参照してください。

vRealize Suite Lifecycle Manager および Workspace ONE Access の操作の詳細については、以下を参照してください。

この章には、次のトピックが含まれています。

- [vRealize Automation で Active Directory グループをプロジェクトに対して有効にする方法](#)
- [vRealize Automation でユーザーを削除する方法](#)
- [vRealize Automation でユーザー ロールを編集する方法](#)
- [vRealize Automation でグループ ロールの割り当てを編集する方法](#)
- [vRealize Automation のユーザー ロールについて](#)
- [米国国防総省の通知および同意バナーを有効にする](#)

vRealize Automation で Active Directory グループをプロジェクトに対して有効にする方法

ユーザーをプロジェクトに追加するときに [グループの追加] ページにグループがない場合には、[ID およびアクセス権の管理] ページを確認して、グループがあればそれを追加します。グループが vRealize Automation の [ID およびアクセス権の管理] 画面に表示されない場合、そのグループは Workspace ONE Access インスタンスで同期されていない可能性があります。同期されていることを確認してから、この手順を使用して、次に示すようにグループを追加します。

Active Directory グループのメンバーをプロジェクトに追加するには、そのグループが Workspace ONE Access インスタンスと同期され、組織に追加されていることを確認する必要があります。

前提条件

同期されていないグループはプロジェクトに追加できません。Active Directory グループが Lifecycle Manager インスタンスと同期していることを確認します。

手順

- 1 追加する同じ Active Directory ドメインから、ユーザーとして vRealize Automation にログインします。
例：@mycompany.com
- 2 Cloud Assembly で、ヘッダーの右ナビゲーションにある [ID およびアクセス権の管理] をクリックします。
- 3 [エンタープライズグループ] をクリックし、[ロールの割り当て] をクリックします。
- 4 追加するグループを検索機能によって検索し、選択します。
- 5 組織ロールを割り当てます。

グループには、少なくとも組織メンバーのロールが必要です。詳細については、[vRealize Automation Cloud Assembly のユーザー ロールについて](#)を参照してください。

- 6 [サービスへのアクセス権の追加] をクリックし、1 つ以上のサービスを追加して、それぞれについてロールを選択します。
- 7 [割り当て] をクリックします。

結果

これで、Active Directory グループをプロジェクトに追加できるようになりました。

vRealize Automation でユーザーを削除する方法

vRealize Automation では、ユーザーを必要に応じて削除できます。

デフォルトではすべてのユーザーが表示されます。[ID およびアクセス権の管理] 画面では、ユーザーを追加することはできません。ユーザーを削除することはできます。

手順

- 1 [ID およびアクセス権の管理] 画面で [アクティブなユーザー] タブを選択します。
- 2 削除するユーザーを選択します。
- 3 [ユーザーの削除] をクリックします。

結果

選択したユーザーが削除されます。

vRealize Automation でユーザー ロールを編集する方法

vRealize Automation にインポート済みの Workspace ONE Access ユーザーに割り当てるロールを編集できます。

前提条件

手順

- 1 Cloud Assembly で、ヘッダーの右ナビゲーションにある [ID およびアクセス権の管理] をクリックします。

- 2 [アクティブなユーザー] タブで目的のユーザーを選択し、[ロールの編集] をクリックします。
- 3 ユーザーの組織およびサービス ロールを編集できます。
 - [組織ロールの割り当て] という見出しの横にあるドロップダウンを選択して、ユーザーと組織の関係を変更します。
 - ユーザーに新しいサービス ロールを追加するには、[サービスへのアクセス権の追加] をクリックします。
 - ユーザー ロールを削除するには、該当するサービスの横にある [X] をクリックします。
- 4 [保存] をクリックします。

結果

指定したとおりにユーザー ロールの割り当てが更新されます。

vRealize Automation でグループ ロールの割り当てを編集する方法

vRealize Automation でグループへのロールの割り当てを編集できます。

前提条件

vRealize Automation の展開に関連付けられている有効な vIDM インスタンスからユーザーとグループがインポートされていること。

手順

- 1 Cloud Assembly で、ヘッダーの右ナビゲーションにある [ID およびアクセス権の管理] をクリックします。
- 2 [エンタープライズ グループ] タブを選択します。
- 3 検索フィールドに、ロールの割り当てを編集するグループの名前を入力します。
- 4 選択されたグループのロールの割り当てを編集します。これには、次の 2 つの方法があります。
 - 組織ロールの割り当て
 - サービス ロールの割り当て
- 5 [割り当て] をクリックします。

結果

指定したとおりにロールの割り当てが更新されます。

vRealize Automation のユーザー ロールについて

組織の所有者は、ユーザーに組織ロールおよびサービス ロールを割り当てることができます。ロールによって、ユーザーが実行または表示できる内容が決まります。次に、サービス管理者は、サービスの中でプロジェクト ロールを割り当てることができます。割り当てるロールを決定するには、次の表でタスクを検討します。

Cloud Assembly サービス ロール

Cloud Assembly サービス ロールによって、Cloud Assembly で表示および実行できる内容が決まります。これらのサービス ロールは、組織の所有者がコンソールで定義します。

表 2-1. Cloud Assembly サービス ロールの説明

ロール	説明
Cloud Assembly 管理者	ユーザー インターフェイスと API リソース全体に対する読み取りおよび書き込みアクセス権を持っているユーザー。これは、クラウド アカウ ントの追加、新しいプロジェクトの作成、プロジェクト管理者の割り当 てなど、すべてを表示および操作できる唯一のユーザー ロールです。
Cloud Assembly ユーザー	Cloud Assembly 管理者ロールを持たないユーザー。 Cloud Assembly プロジェクトでは、管理者がユーザーをプロジェク ト メンバー、管理者、または閲覧者としてプロジェクトに追加します。 管理者は、プロジェクト管理者を追加することもできます。
Cloud Assembly 閲覧者	情報を表示するための読み取りアクセス権は持っているが、作成、更新、 削除はできないユーザー。これは、すべてのプロジェクトに対する読み 取り専用のロールです。 閲覧者ロールを持つユーザーは、管理者が使用できるすべての情報を表 示できます。これらのユーザーは、プロジェクト管理者またはプロジェ クト メンバーにされない限り、アクションを実行することはできませ ん。プロジェクトに関連しているユーザーは、そのロールに関連する権 限を持ちます。プロジェクト閲覧者は、管理者ロールまたはメンバー ロ ールとは異なり、権限が拡張されることはありません。

サービス ロールに加えて、Cloud Assembly にはプロジェクト ロールがあります。どのプロジェクトもすべてのサ
ービスで使用できます。

プロジェクト ロールは Cloud Assembly で定義され、プロジェクトごとに変えることができます。

次の表に、さまざまなサービス ロールおよびプロジェクト ロールで何を表示および実行できるかを示します。サ
ービス管理者にはユーザー インターフェイスのすべての領域に対する完全な権限が付与されていることに注意してく
ださい。

プロジェクト ロールに関する説明を参考にして、ユーザーに付与する権限を決定できます。

- プロジェクト管理者は、サービス管理者が作成したインフラストラクチャを活用して、プロジェクト メンバーが
開発作業に必要なリソースを確実に使用できるようにします。
- プロジェクト メンバーは、クラウド テンプレートを設計および展開するためにプロジェクト内で作業します。
次の表で、プロジェクトに含めることができるリソースは、自分が所有しているか、他のプロジェクト メンバー
と共有しているリソースのみです。
- プロジェクト閲覧者は、読み取り専用アクセスに制限されていますが、クラウド テンプレートのダウンロードな
どの非破壊的な操作を実行できる場合もあります。
- プロジェクト スーパーバイザーは、プロジェクト スーパーバイザー承認者を使用して承認ポリシーが定義され
ているプロジェクトについて、Service Broker における承認者です。スーパーバイザーに承認のコンテキスト
を提供するために、プロジェクト メンバー ロールまたはプロジェクト閲覧者ロールも付与することを検討して
ください。

表 2-2. Cloud Assembly サービス ロールとプロジェクト ロール

ユーザー インターフェイスのコンテキスト	タスク	Cloud Assembly 管理者	Cloud Assembly 閲覧者	Cloud Assembly ユーザー			
				ユーザーがプロジェクト関連のタスクを表示および実行するには、プロジェクト管理者またはプロジェクトメンバーである必要があります。			
				プロジェクト管理者	プロジェクトメンバー	プロジェクト閲覧者	プロジェクトスーパーバイザー
[Cloud Assembly へのアクセス]							
コンソール	vRA コンソールで Cloud Assembly を表示して開くことができます	はい	はい	はい	はい	はい	はい
[インフラストラクチャ]							
	[インフラストラクチャ] タブを表示して開く	はい	はい	はい	はい	はい	はい
構成 - プロジェクト	プロジェクトの作成	はい					
	プロジェクトのサマリ、プロビジョニング、Kubernetes、統合、およびテストプロジェクトの構成から値を更新または削除します。	はい					
	プロジェクトでユーザーおよびグループを追加し、ロールを割り当てます。	はい		はい。自分のプロジェクト。			
	プロジェクトの表示	はい	はい	はい。自分のプロジェクト	はい。自分のプロジェクト	はい。自分のプロジェクト	はい。自分のプロジェクト
構成 - クラウド ゾーン	クラウド ゾーンの作成、更新、または削除	はい					
	クラウド ゾーンの表示	はい	はい				
	クラウド ゾーンの [情報] ダッシュボードの表示	はい	はい				
	クラウド ゾーンのアラートの表示	はい	はい				
構成 - Kubernetes ゾーン	Kubernetes ゾーンの作成、更新、または削除	はい					
	Kubernetes ゾーンの表示	はい	はい				

表 2-2. Cloud Assembly サービス ロールとプロジェクト ロール (続き)

ユーザー インターフェイスのコンテキスト	タスク	Cloud Assembly 管理者	Cloud Assembly 閲覧者	Cloud Assembly ユーザー ユーザーがプロジェクト関連のタスクを表示および実行するには、プロジェクト管理者またはプロジェクト メンバーである必要があります。			
				プロジェクト管理者	プロジェクトメンバー	プロジェクト閲覧者	プロジェクトスーパーバイザー
構成 - フレーバー	フレーバーの作成、更新、または削除	はい					
	フレーバーの表示	はい	はい				
構成 - イメージ マッピング	イメージ マッピングの作成、更新、または削除	はい					
	イメージ マッピングの表示	はい	はい				
構成 - ネットワーク プロファイル	ネットワーク プロファイルの作成、更新、または削除	はい					
	イメージ ネットワーク プロファイルの表示	はい	はい				
構成 - ストレージ プロファイル	ストレージ プロファイルの作成、更新、または削除	はい					
	イメージ ストレージ プロファイルの表示	はい	はい				
構成 - 価格設定カード	価格設定カードの作成、更新、または削除	はい					
	価格設定カードの表示	はい	はい				
構成 - タグ	タグの作成、更新、または削除	はい					
	タグの表示	はい	はい				
リソース - コンピューティング	検出されたコンピューティング リソースへのタグの追加	はい					
	検出されたコンピューティング リソースの表示	はい	はい				
リソース - ネットワーク	ネットワーク タグ、IP アドレス範囲、IP アドレスの変更	はい					
	検出されたネットワーク リソースの表示	はい	はい				
リソース - セキュリティ	検出されたセキュリティ グループへのタグの追加	はい					

表 2-2. Cloud Assembly サービス ロールとプロジェクト ロール (続き)

ユーザー インターフ ェイスのコンテキス ト	タスク	Cloud Assembly 管 理者	Cloud Assembly 閲覧者	Cloud Assembly ユーザー ユーザーがプロジェクト関連のタスクを 表示および実行するには、プロジェクト管 理者またはプロジェクト メンバーである 必要があります。			
				プロジェ クト管理 者	プロジェ クト メ ンバー	プロジ ェクト 閲覧者	プロ ジェ クト スー パー バイ ザー
	検出されたセキュリティ グループの表 示	はい	はい				
リソース - ストレージ	検出されたストレージへのタグの追加	はい					
	ストレージの表示	はい	はい				
リソース - Kubernetes	Kubernetes クラスタの展開または追 加、および名前空間の作成または追加	はい					
	Kubernetes クラスタと名前空間の表 示	はい	はい	はい。自 分のプロ ジェクト	はい。自 分のプロ ジェクト	はい。 自分の プロジ ェクト	
アクティビティ - 申 請	展開申請レコードの削除	はい					
	展開申請レコードの表示	はい	はい	はい。自 分のプロ ジェクト	はい。自 分のプロ ジェクト	はい。 自分の プロジ ェクト	
アクティビティ - イ ベント ログ	イベント ログの表示	はい	はい	はい。自 分のプロ ジェクト	はい。自 分のプロ ジェクト	はい。 自分の プロジ ェクト	
接続 - クラウド アカ ウント	クラウド アカウントの作成、更新、また は削除	はい					
	クラウド アカウントの表示	はい	はい				
接続 - 統合	統合の作成、更新、または削除	はい					
	統合の表示	はい	はい				
オンボーディング	オンボーディング ブランの作成、更新、 または削除	はい					
	オンボーディング ブランの表示	はい	はい			はい。 自分の プロジ ェクト	

表 2-2. Cloud Assembly サービス ロールとプロジェクト ロール (続き)

ユーザー インターフェイスのコンテキスト	タスク	Cloud Assembly 管理者	Cloud Assembly 閲覧者	Cloud Assembly ユーザー			
				ユーザーがプロジェクト関連のタスクを表示および実行するには、プロジェクト管理者またはプロジェクトメンバーである必要があります。			
				プロジェクト管理者	プロジェクトメンバー	プロジェクト閲覧者	プロジェクトスーパーバイザー
[拡張性]							
	[拡張性] タブを表示して開く	はい	はい			はい	
イベント	拡張性イベントの表示	はい	はい				
サブスクリプション	拡張性サブスクリプションの作成、更新、または削除	はい					
	サブスクリプションの無効化	はい					
	サブスクリプションの表示	はい	はい				
ライブラリ - イベント トピック	イベント トピックの表示	はい	はい				
ライブラリ - アクション	拡張性アクションの作成、更新、または削除	はい					
	拡張性アクションの表示	はい	はい				
ライブラリ - ワークフロー	拡張性ワークフローの表示	はい	はい				
アクティビティ - アクションの実行	拡張性アクションの実行のキャンセルまたは削除	はい					
	拡張性アクションの実行の表示	はい	はい			はい。 自分のプロジェクト	
アクティビティ - ワークフローの実行	拡張性ワークフローの実行の表示	はい	はい				
[デザイン]							
デザイン	[デザイン] タブを開く	はい	はい	はい。	はい。	はい。	はい
クラウド テンプレート	クラウド テンプレートの作成、更新、削除	はい		はい。自分のプロジェクト	はい。自分のプロジェクト		

表 2-2. Cloud Assembly サービス ロールとプロジェクト ロール (続き)

ユーザー インターフェイスのコンテキスト	タスク	Cloud Assembly 管理者	Cloud Assembly 閲覧者	Cloud Assembly ユーザー ユーザーがプロジェクト関連のタスクを表示および実行するには、プロジェクト管理者またはプロジェクトメンバーである必要があります。			
				プロジェクト管理者	プロジェクトメンバー	プロジェクト閲覧者	プロジェクトスーパーバイザー
	クラウド テンプレートの表示	はい	はい	はい。自分のプロジェクト	はい。自分のプロジェクト	はい。自分のプロジェクト	
	クラウド テンプレートのダウンロード	はい	はい	はい。自分のプロジェクト	はい。自分のプロジェクト	はい。自分のプロジェクト	
	クラウド テンプレートのアップロード	はい		はい。自分のプロジェクト	はい。自分のプロジェクト		
	クラウド テンプレートの展開	はい		はい。自分のプロジェクト	はい。自分のプロジェクト		
	クラウド テンプレートのバージョン管理とリストア	はい		はい。自分のプロジェクト	はい。自分のプロジェクト		
	クラウド テンプレートのカタログへのリリース	はい		はい。自分のプロジェクト	はい。自分のプロジェクト		
カスタム リソース	カスタム リソースの作成、更新、または削除	はい					
	カスタム リソースの表示	はい	はい	はい。自分のプロジェクト	はい。自分のプロジェクト	はい。自分のプロジェクト	
カスタム アクション	カスタム アクションの作成、更新、または削除	はい					
	カスタム アクションの表示	はい	はい	はい。自分のプロジェクト	はい。自分のプロジェクト	はい。自分のプロジェクト	
[リソース]							
	[リソース] タブを表示、および開く	はい	はい	はい	はい	はい	はい

表 2-2. Cloud Assembly サービス ロールとプロジェクト ロール (続き)

ユーザー インターフ ェイスのコンテキス ト	タスク	Cloud Assembly 管 理者	Cloud Assembly 閲覧者	Cloud Assembly ユーザー ユーザーがプロジェクト関連のタスクを 表示および実行するには、プロジェクト管 理者またはプロジェクト メンバーである 必要があります。			
				プロジェ クト管理 者	プロジェ クト メ ンバー	プロジ ェクト 閲覧者	プロ ジェ クト スー パー バイ ザー
展開	展開の詳細、展開履歴、価格、監視、アラート、最適化、トラブルシューティング情報を含む展開の表示	はい	はい	はい。自 分のプロ ジェクト	はい。自 分のプロ ジェクト	はい。 自分の プロジ ェクト	
	アラートの管理	はい		はい。自 分のプロ ジェクト	はい。自 分のプロ ジェクト		
	ポリシーに基づいて展開に対して Day 2 アクションを実行	はい		はい。自 分のプロ ジェクト	はい。自 分のプロ ジェクト		
リソース - すべての リソース	検出されたすべてのリソースの表示	はい	はい				
	検出されたリソースに対して Day 2 アクションを実行。 アクションはマシンでのみ使用でき、すべてのマシンのパワーオンとパワーオフ、および vSphere マシンのリモートコンソールに限定。	はい					
リソース - すべての リソース	展開済み、オンボーディング済み、移行済みリソースの表示	はい	はい	はい。自 分のプロ ジェク ト。	はい。自 分のプロ ジェク ト。	はい。 自分の プロジ ェクト。	
	ポリシーに基づいて展開済み、オンボーディング済み、移行済みリソースに対して Day 2 アクションを実行	はい	はい	はい。自 分のプロ ジェク ト。	はい。自 分のプロ ジェク ト。		
リソース - 仮想マシ ン	検出されたマシンの表示	はい	はい				
	検出されたマシンで Day 2 アクションを実行。 アクションは、パワーオンとパワーオフ、および vSphere マシンのリモートコンソールに限定。	はい					
	VM の新規作成	はい					

表 2-2. Cloud Assembly サービス ロールとプロジェクト ロール (続き)

ユーザー インターフ ェイスのコンテキス ト	タスク	Cloud Assembly 管 理者	Cloud Assembly 閲覧者	Cloud Assembly ユーザー ユーザーがプロジェクト関連のタスクを 表示および実行するには、プロジェクト管 理者またはプロジェクト メンバーである 必要があります。			
				プロジェ クト管理 者	プロジェ クト メ ンバー	プロジ ェクト 閲覧者	プロ ジェ クト スー パー バイ ザー
	展開済み、オンボーディング済み、移行 済みリソースの表示。	はい		はい。自 分のプロ ジェク ト。	はい。自 分のプロ ジェク ト。	はい。 自分の プロジ ェクト。	
	ポリシーに基づいて展開済み、オンボー ディング済み、移行済みリソースに対し て Day 2 アクションを実行	はい		はい。自 分のプロ ジェク ト。	はい。自 分のプロ ジェク ト。		
リソース - ポリユー ム	検出されたポリュームの表示	はい	はい				
	利用可能な Day 2 アクションなし						
	展開済み、オンボーディング済み、移行 済みポリュームの表示	はい	はい	はい。自 分のプロ ジェク ト。	はい。自 分のプロ ジェク ト。	はい。 自分の プロジ ェクト。	
	ポリシーに基づいて展開済み、オンボー ディング済み、移行済みポリュームに対 して Day 2 アクションを実行	はい		はい。自 分のプロ ジェク ト。	はい。自 分のプロ ジェク ト。		
リソース - ネットワ ークとセキュリティ	検出されたネットワーク、ロード バラン サ、およびセキュリティ グループの表示	はい	はい				
	利用可能な Day 2 アクションなし						
	展開済み、オンボーディング済み、移行 済みのネットワーク、ロード バランサ、 セキュリティ グループの表示	はい	はい	はい。自 分のプロ ジェク ト。	はい。自 分のプロ ジェク ト。	はい。 自分の プロジ ェクト。	
	ポリシーに基づいて展開済み、オンボー ディング済み、移行済みのネットワー ク、ロード バランサ、セキュリティ グ ループに対して Day 2 アクションを実 行	はい		はい。自 分のプロ ジェク ト。	はい。自 分のプロ ジェク ト。		
[アラート]							
	[アラート] タブを表示して開く	はい	はい	はい	はい	はい	

表 2-2. Cloud Assembly サービス ロールとプロジェクト ロール（続き）

ユーザー インターフェイスのコンテキスト	タスク	Cloud Assembly 管理者	Cloud Assembly 閲覧者	Cloud Assembly ユーザー ユーザーがプロジェクト関連のタスクを表示および実行するには、プロジェクト管理者またはプロジェクト メンバーである必要があります。			
				プロジェクト管理者	プロジェクトメンバー	プロジェクト閲覧者	プロジェクトスーパーバイザー
	アラートの管理	はい		はい。自分のプロジェクト	はい。自分のプロジェクト		
	アラートの表示	はい	はい	はい。自分のプロジェクト	はい。自分のプロジェクト	はい。自分のプロジェクト	

Service Broker サービス ロール

Service Broker サービス ロールによって、Service Broker で表示および実行できる内容が決まります。これらのサービス ロールは、組織の所有者がコンソールで定義します。

表 2-3. Service Broker サービス ロールの説明

ロール	説明
Service Broker 管理者	ユーザー インターフェイスと API リソース全体に対する読み取りおよび書き込みアクセス権が必要です。これは、新しいプロジェクトの作成やプロジェクト管理者の割り当てなど、すべてのタスクを実行できる唯一のユーザー ロールです。
Service Broker ユーザー	Service Broker 管理者ロールを持たないすべてのユーザー。 Service Broker プロジェクトでは、管理者がユーザーをプロジェクトメンバー、管理者、または閲覧者としてプロジェクトに追加します。管理者は、プロジェクト管理者を追加することもできます。
Service Broker 閲覧者	情報を表示するための読み取りアクセス権は持っているが、作成、更新、削除はできないユーザー。 閲覧者ロールを持つユーザーは、管理者が使用できるすべての情報を表示できます。これらのユーザーは、プロジェクト管理者またはプロジェクトメンバーにされない限り、アクションを実行することはできません。プロジェクトに関連しているユーザーは、そのロールに関連する権限を持ちます。プロジェクト閲覧者は、管理者ロールまたはメンバーロールとは異なり、権限が拡張されることはありません。

サービス ロールに加えて、Service Broker にはプロジェクト ロールがあります。どのプロジェクトもすべてのサービスで使用できます。

プロジェクト ロールは Service Broker で定義され、プロジェクトごとに変えることができます。

次の表に、さまざまなサービス ロールおよびプロジェクト ロールで何を表示および実行できるかを示します。サービス管理者にはユーザー インターフェイスのすべての領域に対する完全な権限が付与されていることに注意してください。

プロジェクト ロールに関する次の説明を利用して、ユーザーに付与する権限を決定します。

- プロジェクト管理者は、サービス管理者が作成したインフラストラクチャを活用して、プロジェクト メンバーが開発作業に必要なリソースを確実に使用できるようにします。
- プロジェクト メンバーは、クラウド テンプレートを設計および展開するためにプロジェクト内で作業します。次の表で、プロジェクトに含めることができるリソースは、自分が所有しているか、他のプロジェクト メンバーと共有しているリソースのみです。
- プロジェクト閲覧者は、読み取り専用アクセスに制限されています。
- プロジェクト スーパーバイザーは、プロジェクト スーパーバイザー承認者を使用して承認ポリシーが定義されているプロジェクトについて、Service Broker における承認者です。スーパーバイザーに承認のコンテキストを提供するために、プロジェクト メンバー ロールまたはプロジェクト閲覧者ロールも付与することを検討してください。

表 2-4. Service Broker サービス ロールとプロジェクト ロール

ユーザー インターフェイスのコンテキスト	タスク	Service Broker 管理者	Service Broker 閲覧者	Service Broker ユーザー			
				ユーザーがプロジェクト関連のタスクを表示および実行するには、プロジェクト管理者である必要があります。			
				プロジェクト管理者	プロジェクトメンバー	プロジェクト閲覧者	プロジェクトスーパーバイザー
[Service Broker へのアクセス]							
コンソール	コンソールで Service Broker を表示して開くことができます	はい	はい	はい	はい	はい	はい
[インフラストラクチャ]							
	[インフラストラクチャ] タブを表示して開く	はい	はい				
構成 - プロジェクト	プロジェクトの作成	はい					
	プロジェクトのサマリ、プロビジョニング、Kubernetes、統合、およびテストプロジェクトの構成から値を更新または削除します。	はい					
	プロジェクトでユーザーおよびグループを追加し、ロールを割り当てます。	はい		はい。自分のプロジェクト。			

表 2-4. Service Broker サービス ロールとプロジェクト ロール (続き)

ユーザー インターフェイスのコンテキスト	タスク	Service Broker 管理者	Service Broker 閲覧者	Service Broker ユーザー			
				ユーザーがプロジェクト関連のタスクを表示および実行するには、プロジェクト管理者である必要があります。			
				プロジェクト管理者	プロジェクトメンバー	プロジェクト閲覧者	プロジェクトスーパーバイザー
	プロジェクトの表示	はい	はい	はい。自分のプロジェクト	はい。自分のプロジェクト	はい。自分のプロジェクト	
構成 - クラウドゾーン	クラウドゾーンの作成、更新、または削除	はい					
	クラウドゾーンの表示	はい	はい				
構成 - Kubernetesゾーン	Kubernetesゾーンの作成、更新、または削除	はい					
	Kubernetesゾーンの表示	はい	はい				
接続 - クラウドアカウント	クラウドアカウントの作成、更新、または削除	はい					
	クラウドアカウントの表示	はい	はい				
接続 - 統合	統合の作成、更新、または削除	はい					
	統合の表示	はい	はい				
アクティビティ - 申請	展開申請レコードの削除	はい					
	展開申請レコードの表示	はい					
アクティビティ - イベントログ	イベントログの表示	はい					
[コンテンツとポリシー]							
	[コンテンツとポリシー] タブを表示して開く	はい	はい				
コンテンツソース	コンテンツソースの作成、更新、または削除	はい					
	コンテンツソースの表示	はい	はい				
コンテンツの共有	共有コンテンツの追加または削除	はい					
	共有コンテンツの表示	はい	はい				
コンテンツ	フォームのカスタマイズとアイテムの構成	はい					

表 2-4. Service Broker サービス ロールとプロジェクト ロール（続き）

ユーザー インターフェイスのコンテキスト	タスク	Service Broker 管理者	Service Broker 閲覧者	Service Broker ユーザー			
				ユーザーがプロジェクト関連のタスクを表示および実行するには、プロジェクト管理者である必要があります。			
				プロジェクト管理者	プロジェクトメンバー	プロジェクト閲覧者	プロジェクトスーパーバイザー
	コンテンツの表示	はい	はい				
ポリシー - 定義	ポリシー定義の作成、更新、または削除	はい					
	ポリシー定義の表示	はい	はい				
ポリシー - 適用	適用ログの表示	はい	はい				
通知 - メール サーバ	メール サーバの設定	はい					
[カタログ]							
	[カタログ] タブを表示して開く	はい	はい	はい	はい	はい	はい
	使用可能なカタログ アイテムの表示	はい	はい	はい。自分のプロジェクト	はい。自分のプロジェクト	はい。自分のプロジェクト	
	カタログ アイテムの要求	はい		はい。自分のプロジェクト	はい。自分のプロジェクト		
[リソース]							
	[リソース] タブを表示、および開く	はい	はい	はい。	はい	はい	はい
展開	展開の詳細、展開履歴、価格、監視、アラート、最適化、トラブルシューティング情報を含む展開の表示	はい	はい	はい。自分のプロジェクト	はい。自分のプロジェクト	はい。自分のプロジェクト	
	アラートの管理	はい		はい。自分のプロジェクト	はい。自分のプロジェクト		
	ポリシーに基づいて展開に対して Day 2 アクションを実行	はい		はい。自分のプロジェクト	はい。自分のプロジェクト		
リソース - すべてのリソース	検出されたすべてのリソースの表示	はい	はい				

表 2-4. Service Broker サービス ロールとプロジェクト ロール (続き)

ユーザー インターフ ェイスのコンテキス ト	タスク	Service Broker 管 理者	Service Broker 関 覧者	Service Broker ユーザー			
				ユーザーがプロジェクト関連のタスクを表示 および実行するには、プロジェクト管理者で ある必要があります。			
				プロジェ クト管理 者	プロジェ クトメン バー	プロジ ェクト 閲覧者	プロジ ェクト スーパ ーバイ ザー
	検出されたリソースに対して Day 2 アク ションを実行。 アクションはマシンでのみ使用でき、すべ てのマシンのパワーオンとパワーオフ、お よび vSphere マシンのリモート コンソ ールに限定。	はい					
リソース - すべての リソース	展開済み、オンボーディング済み、移行済 みリソースの表示	はい	はい	はい。自 分のプロ ジェクト。	はい。自 分のプロ ジェク ト。	はい。 自分の プロジ ェクト。	
	ポリシーに基づいて展開済み、オンボーデ ィング済み、移行済みリソースに対して Day 2 アクションを実行	はい	はい	はい。自 分のプロ ジェクト。	はい。自 分のプロ ジェク ト。		
リソース - 仮想マシ ン	検出されたマシンの表示	はい	はい				
	検出されたマシンで Day 2 アクションを 実行。 アクションは、パワーオンとパワーオフ、 および vSphere マシンのリモート コン ソールに限定。	はい					
	VM の新規作成	はい					
	展開済み、オンボーディング済み、移行済 みリソースの表示。	はい		はい。自 分のプロ ジェクト。	はい。自 分のプロ ジェク ト。	はい。 自分の プロジ ェクト。	
	ポリシーに基づいて展開済み、オンボーデ ィング済み、移行済みリソースに対して Day 2 アクションを実行	はい		はい。自 分のプロ ジェクト。	はい。自 分のプロ ジェク ト。		
リソース - ボリューム	検出されたボリュームの表示	はい	はい				
	利用可能な Day 2 アクションなし						
	展開済み、オンボーディング済み、移行済 みボリュームの表示	はい	はい	はい。自 分のプロ ジェクト。	はい。自 分のプロ ジェク ト。	はい。 自分の プロジ ェクト。	

表 2-4. Service Broker サービス ロールとプロジェクト ロール（続き）

ユーザー インターフ ェイスのコンテキス ト	タスク	Service Broker 管 理者	Service Broker 関 覧者	Service Broker ユーザー			
				ユーザーがプロジェクト関連のタスクを表示 および実行するには、プロジェクト管理者で ある必要があります。			
				プロジェ クト管理 者	プロジェ クトメン バー	プロジ ェクト 閲覧者	プロジ ェクト スーパ ーバイ ザー
	ポリシーに基づいて展開済み、オンボーデ ィング済み、移行済みボリュームに対して Day 2 アクションを実行	はい		はい。自 分のプロ ジェクト。	はい。自 分のプロ ジェク ト。		
リソース - ネットワ ークとセキュリティ	検出されたネットワーク、ロード バラン サ、およびセキュリティ グループの表示	はい	はい				
	利用可能な Day 2 アクションなし						
	展開済み、オンボーディング済み、移行済 みのネットワーク、ロード バランサ、セキ ュリティ グループの表示	はい	はい	はい。自 分のプロ ジェクト。	はい。自 分のプロ ジェク ト。	はい。 自分の プロジ ェクト。	
	ポリシーに基づいて展開済み、オンボーデ ィング済み、移行済みのネットワーク、ロ ード バランサ、セキュリティ グループに 対して Day 2 アクションを実行	はい		はい。自 分のプロ ジェクト。	はい。自 分のプロ ジェク ト。		
[承認]							
	[承認] タブを表示して開く	はい	はい	はい	はい	はい	はい
	承認申請への応答	はい		はい。自 分のプロ ジェクト。 ポリシー 承認者は プロジェ クト管理 者	指定され た承認者 である場 合のみ	指定さ れた承認者で ある場合のみ	はい。 自分の プロジ ェク ト。ポ リシー 承認者 はプロ ジェク トス ーパー バイザ ー

米国国防総省の通知および同意バナーを有効にする

政府関連の一部のユーザーについて、管理者は、ユーザーが vRealize Automation にアクセスできるようにするため、標準の国防総省 (DoD) 通知および同意バナーを Workspace ONE Access で構成する必要があります。

必須標準の DoD 通知および同意バナーのテキストは、次のとおりです。

米国政府 (USG) の情報システム (IS) にアクセスしています。このシステムは、USG で認可された用途でのみ使用できます。この IS (この IS に接続されたデバイスを含む) を使用すると、次の条件に同意したことになります。

- USG は、侵入テスト、通信保全 (COMSEC) の監視、ネットワークの運用と防御、職員の違法行為 (PM)、法の執行 (LE)、対敵情報 (CI) の調査などの目的で (ただし、これらに限定されない) この IS 上の通信を定期的に傍受および監視します。
- USG は、この IS に保存されているデータをいつでも検査および取得できます。
- この IS を使用した通信、またはこの IS に保存されているデータは、非公開ではなく、定期的に監視、傍受、検索されます。また、USG が認可した目的のために開示または使用される可能性があります。

このバナーを Workspace ONE Access で構成する方法を次に示します。詳細については、Workspace ONE Access 管理コンソールのドキュメントを参照してください。

手順

- 1 Workspace ONE 管理コンソールに管理者としてログインします。
- 2 VMware Identity Manager コンソールで [ID とアクセス管理] タブをクリックします。
- 3 [セットアップ] をクリックしてから、[コネクタ] タブをクリックします。
- 4 構成する各コネクタのワーカー リンクをクリックします。
- 5 [認証アダプタ] タブをクリックしてから、CertificateAuthAdapter をクリックします。
- 6 [認証前に同意書を有効にする] チェック ボックスをクリックします。
- 7 必須標準の DoD 通知および同意バナーのテキストを [同意書の内容] ボックスに貼り付けます。
- 8 変更内容を保存します。

結果

vRealize Automation アプライアンスの保守

3

システム管理者として、インストールされている vRealize Automation アプリケーションが正常に機能するように、さまざまなタスクを実行する必要がある場合があります。

vRealize Automation を初めて使用する場合は、これらのタスクは必須ではありません。これらのタスクの実行方法を把握することは、パフォーマンスや製品の動作に関する問題を解決する必要がある場合に役立ちます。

この章には、次のトピックが含まれています。

- vRealize Automation の起動と停止
- 単一ノードから 3 ノードへの vRealize Automation のスケール アウト
- クラスタ化された Workspace ONE Access インスタンスの非アフィニティ ルールと仮想マシン グループの構成
- vRealize Automation アプライアンス ノードの置き換え
- vRealize Automation アプライアンスのディスク容量の拡張
- vRealize Automation の DNS 割り当ての更新
- vRealize Automation ノードまたはクラスタの IP アドレスの変更
- vRealize Automation の時刻同期を有効にする方法
- vRealize Automation の root パスワードをリセットする方法

vRealize Automation の起動と停止

vRealize Automation の起動またはシャットダウン時の適切な手順は次のとおりです。

vRealize Automation のコンポーネントをシャットダウンおよび起動するには、vRealize Suite Lifecycle Manager の [ライフサイクル操作] - [環境] セクションにあるパワーオフおよびパワーオン機能を使用する方法が推奨されます。次の手順では、何らかの理由で vRealize Suite Lifecycle Manager が使用できない場合に vRealize Automation をシャットダウンおよび起動する方法について説明します。

vRealize Automation のシャットダウン

データの整合性を維持するために、仮想アプライアンスをパワーオフする前に vRealize Automation サービスをシャットダウンする必要があります。SSH または VMRC を使用して、任意のアプライアンスからすべてのノードをシャットダウンまたは起動できます。

注： 可能であれば、`vracli reset vidm` コマンドは使用しないでください。このコマンドは、Workspace ONE Access のすべての設定をリセットし、ユーザーとプロビジョニング済みリソースとの間の関連付けを解除します。

- 1 SSH または VMRC を使用して、任意の vRealize Automation アプライアンスのコンソールにログインします。
- 2 すべてのクラスタ ノードで vRealize Automation サービスをシャットダウンするには、次の一連のコマンドを実行します。

注： これらのコマンドのいずれかをコピーして実行すると失敗する場合は、まずメモ帳に貼り付け、そこからコピーし直して実行します。この手順により、ドキュメント ソースに存在する可能性のある非表示の文字やその他のアーティファクトを取り除きます。

```
/opt/scripts/deploy.sh --shutdown
```

- 3 vRealize Automation アプライアンスをシャットダウンします。

これで、vRealize Automation 環境がシャットダウンされます。

vRealize Automation の起動

予定外のシャットダウン、制御されたシャットダウン、またはリカバリ手順の後には、特定の順序で vRealize Automation コンポーネントを再起動する必要があります。vRLCM は重要度の低いコンポーネントであるため、いつでも起動できます。以前は VMware Identity Management と呼ばれていた VMware Workspace ONE Access コンポーネントは、vRealize Automation を起動する前に起動する必要があります。

注： vRealize Automation コンポーネントを起動する前に、対応するロードバランサが実行されていることを確認します。

- 1 すべての vRealize Automation アプライアンスをパワーオンし、起動するまで待機します。
- 2 SSH または VMRC を使用して任意のアプライアンスのコンソールにログインし、次のコマンドを実行して、すべてのノードのサービスを復旧します。

```
/opt/scripts/deploy.sh
```

- 3 次のコマンドにより、すべてのサービスが実行されていることを確認します。

```
kubectl get pods --all-namespaces
```

注： 各サービスについて、それぞれ実行中または完了済みのいずれかの状態で 3 つのインスタンスが表示されます。

すべてのサービスが実行中または完了済みと表示されたら、vRealize Automation を使用する準備が完了しています。

vRealize Automation の再起動

すべての vRealize Automation サービスは、クラスタ内の任意のアプライアンスから一元的に再起動できます。上記の手順で vRealize Automation をシャットダウンし、指示どおりに vRealize Automation を起動します。vRealize Automation を再起動する前に、該当するすべてのロードバランサと VMware Workspace ONE Access コンポーネントが実行されていることを確認します。

すべてのサービスが実行中または完了済みと表示されたら、vRealize Automation を使用する準備が完了しています。

次のコマンドを実行して、すべてのサービスが実行されていることを確認します。

```
kubectl -n prelude get pods
```

単一ノードから 3 ノードへの vRealize Automation のスケール アウト

必要に応じて、vRealize Automation 展開を単一ノードから 3 ノードにスケール アウトできます。

この手順の多くの部分は、vRealize Suite Lifecycle Manager の機能を使用して実行する必要があります。vRealize Suite Lifecycle Manager のインストール、アップグレード、管理の操作の詳細については、[Lifecycle Manager 製品ドキュメント](#)を参照してください。

3 ノードのクラスタ化された展開を使用している場合、vRealize Automation は通常、1 台のノードに障害が発生した場合でも引き続き機能します。3 ノード クラスタ内の 2 台のノードで障害が発生すると、vRealize Automation は機能しなくなります。

前提条件

この手順は、機能している単一ノードの vRealize Automation 展開がすでにあることを前提としています。

手順

- 1 すべての vRealize Automation アプライアンスをシャットダウンします。

すべてのクラスタ ノードで vRealize Automation サービスをシャットダウンするには、次の一連のコマンドを実行します。

```
/opt/scripts/svc-stop.sh  
sleep 120  
/opt/scripts/deploy.sh --onlyClean
```

これにより、vRealize Automation アプライアンスをシャットダウンできるようになります。

2 展開のスナップショットを作成します。

vRealize Suite Lifecycle Manager の [スナップショットの作成] オプションを使用します。[ライフサイクル操作] - [環境] - [vRA] - [詳細の表示] の順に選択します。

注: vRealize Automation ノードをシャットダウンせずに作成されるオンライン スナップショットは、8.0.1 からサポートされています。vRealize Automation 8.0 環境では、まず vRealize Automation ノードを停止する必要があります。

3 vRealize Automation アプライアンスをパワーオンし、すべてのコンテナを起動します。

4 vRealize Suite Lifecycle Manager の [LCM] - [Locker] - [証明書] にある Locker 機能を使用して、すべてのコンポーネントに対する vRealize Automation 証明書を生成またはインポートします。これには、vRealize Suite Lifecycle Manager のノード FQDN および vRealize Automation Load Balancer の完全修飾ドメイン名も含まれます。

Subject Alternative Name として、3 台のアプライアンスすべての名前を追加します。

5 新しい証明書を vRealize Suite Lifecycle Manager にインポートします。

6 LCM の [ライフサイクル操作] - [環境] - [vRA] - [詳細の表示] から [証明書の置き換え] オプションを使用して、既存の vRealize Suite Lifecycle Manager 証明書を前の手順で生成された証明書に置き換えます。

7 [LCM] - [ライフサイクル操作] - [環境] - [vRA] - [詳細の表示] の順に選択し、[コンポーネントの追加] の選択項目を使用して vRealize Automation を 3 台のノードにスケール アウトします。

結果

vRealize Automation が 3 ノードの展開に拡張されています。

クラスタ化された Workspace ONE Access インスタンスの非アフィニティ ルールと仮想マシン グループの構成

vRealize Automation 環境でクラスタ化された Workspace ONE Access インスタンスを使用している場合は、非アフィニティ ルールとマシン クラスタを作成して、vSphere High Availability ワークフローを適正化してください。

クラスタ化された Workspace ONE Access ノードをホストレベルの障害から保護するには、デフォルトの vSphere 管理クラスタ内の複数のホスト上にある仮想マシンを実行するように非アフィニティ ルールを構成します。非アフィニティ ルールを作成したら、仮想マシン グループを構成して、目的のマシン起動順序を定義します。定義したマシン起動順序を使用すると、vSphere High Availability はクラスタ化された Workspace ONE Access ノードを環境に適した順序でパワーオンできるようになります。

非アフィニティ ルールと仮想マシン グループを構成する方法の詳細については、[VMware Cloud Foundation 製品ドキュメントの「クラスタ化された Workspace ONE Access インスタンスの非アフィニティ ルールと仮想マシン グループの構成」](#)を参照してください。

vRealize Automation リリース間でアップグレードする場合のアフィニティ ルールの考慮事項

vRealize Suite Lifecycle Manager は、vRealize Automation 8.x の非アフィニティ ルールをサポートしていません。vRealize Easy Installer による vRealize Automation のアップグレード中は vRealize Suite Lifecycle Manager が使用され、アップグレード中における vRealize Automation ノードのパワーオフとパワーオンの順序が具体的に設定されていないため、マシンのパワーオフおよびパワーオンの順序を定義するアフィニティ ルールと使用する順序が一致しない場合は、問題が発生することがあります。vRealize Suite Lifecycle Manager または vRealize Easy Installer を使用して vRealize Automation リリース間でアップグレードする場合は、アップグレードを開始する前にアフィニティ ルールを無効にしてください。

vRealize Automation のリリース間でアップグレードする方法の詳細については、[vRealize Automation 製品ドキュメント](#)の「[vRealize Easy Installer による vRealize Automation のインストール](#)」を参照してください。

vRealize Automation アプライアンス ノードの置き換え

複数ノード、高可用性 (HA) 構成の vRealize Automation アプライアンスで障害が発生した場合は、障害が発生したノードの置き換えが必要になる場合があります。

注意： VMware は、実行の前に、テクニカル サポートと連携して HA の問題のトラブルシューティングを行い、問題が 1 台のノードに隔離されているのを確認することを推奨します。

ノードの交換が必要であるとテクニカル サポートが判断した場合は、次の手順を実行します。

- 1 vCenter Server で、HA 構成内にあるすべてのアプライアンスのバックアップ スナップショットを作成します。

バックアップ スナップショットには、仮想マシンのメモリを含めないようにしてください。

- 2 障害が発生したノードをシャットダウンします。
- 3 障害が発生したノードの vRealize Automation ソフトウェア ビルド番号とネットワーク設定をメモします。
FQDN、IP アドレス、ゲートウェイ、DNS サーバ、特に MAC アドレスをメモします。これらと同じ値を後で置換用のノードに割り当てます。

- 4 プライマリ データベース ノードは、いずれかの健全なノードである必要があります。次の手順に従います。

- a 健全なノードのコマンドラインに root としてログインします。
- b 次のコマンドを実行して、プライマリ データベース ノードの名前を検索します。

```
vracli status | grep primary -B 1
```

結果は次の例のようになります。ここで、postgres-1 はプライマリ データベース ノードです。

```
"Conninfo":
"host=postgres-1.postgres.prelude.svc.cluster.local
dbname=repmgr-db user=repmgr-db passfile=/scratch/repmgr-db.cred
connect_timeout=10",
"Role": "primary",
```

- c 次のコマンドを実行して、プライマリ データベース ノードが健全なことを確認します。

```
kubect1 -n prelude get pods -o wide | grep postgres
```

結果は次の例のようになります。ここで、postgres-1 は実行中で健全なノードとしてリストに表示されています。

```
postgres-1 1/1 Running 0 39h 12.123.2.14 vc-vm-224-84.company.com <none> <none>
postgres-2 1/1 Running 0 39h 12.123.1.14 vc-vm-224-85.company.com <none> <none>
```

重要： プライマリ データベース ノードに障害が発生している場合は、先に進まずにテクニカル サポートに連絡してください。

- 健全なノードの root コマンド ラインから、障害が発生したノードを削除します。

```
vrac1i cluster remove faulty-node-FQDN
```

- vCenter Server を使用して、新しい vRealize Automation 置換用のノードを展開します。

同じ vRealize Automation ソフトウェア ビルド番号を展開し、障害が発生したノードのネットワーク設定を適用します。前にメモした FQDN、IP アドレス、ゲートウェイ、DNS サーバ、特に MAC アドレスを含めます。

- 置換ノードをパワーオンします。

- 置換ノードのコマンド ラインに root としてログインします。

- 次のコマンドを実行して、初期起動シーケンスが完了したことを確認します。

```
vrac1i status first-boot
```

First boot complete メッセージを探します。

- 置換ノードから、vRealize Automation クラスタに参加します。

```
vrac1i cluster join primary-DB-node-FQDN
```

- プライマリ データベース ノードのコマンド ラインに root としてログインします。

- 次のスクリプトを実行して、修復されたクラスタを展開します。

```
/opt/scripts/deploy.sh
```

vRealize Automation アプライアンスのディスク容量の拡張

ログ ファイルの保存などの目的で vRealize Automation アプライアンスのディスク容量を増やすことが必要になる場合があります。

手順

- vSphere を使用して、vRealize Automation アプライアンスの VMDK を拡張します。
- vRealize Automation アプライアンスのコマンド ラインに root ユーザーとしてログインします。
- コマンド プロンプトで次の vRealize Automation コマンドを実行します。

```
vrac1i disk-mgr resize
```

vRealize Automation のサイズ変更に失敗する場合は、[ナレッジベースの記事 KB79925](#) を参照してください。

vRealize Automation の DNS 割り当ての更新

管理者は、vRealize Automation の DNS 割り当てを更新できます。

手順

- 1 SSH または VMRC を使用して、任意の vRealize Automation アプライアンスのコンソールにログインします。
- 2 次のコマンドを実行します。

```
vracli network dns set --servers DNS1,DNS2
```

- 3 `vracli network dns status` コマンドを使用して、新しい DNS サーバがすべての vRealize Automation ノードに適切に適用されていることを確認します。
- 4 次の一連のコマンドを実行して、すべてのクラスタ ノードの vRealize Automation サービスをシャットダウンします。

```
/opt/scripts/svc-stop.sh  
sleep 120  
/opt/scripts/deploy.sh --onlyClean
```

- 5 vRealize Automation ノードを再起動し、完全に起動するまで待機します。
- 6 SSH を使用して各 vRealize Automation ノードにログインし、`/etc/resolv.conf` に新しい DNS サーバが表示されていることを確認します。
- 7 いずれかの vRealize Automation ノードで次のコマンドを実行して、vRealize Automation サービスを開始します。`/opt/scripts/deploy.sh`

結果

vRealize Automation の DNS 設定が指定されたとおりに変更されます。

vRealize Automation ノードまたはクラスタの IP アドレスの変更

vRealize Automation ノードまたはクラスタの IP アドレスは変更することができます。

たとえば、展開された vRealize Automation 環境をより便利な vCenter Server に移行したり、vRealize Automation フェイルオーバーをサポートしたりする場合があります。

vRealize Automation 管理者は、次の手順を使用して、vRealize Automation ノードまたはクラスタに新しい IP アドレスを設定し、サービスを新しい IP アドレスに再展開できます。

注： vRealize Automation ノードまたはクラスタの IP アドレスの変更を続行する前に、ノードまたはクラスタが健全な状態であることを確認する必要があります。健全な状態でないノードまたはクラスタでこの手順を実行すると、解決が非常に困難な問題が発生する可能性があります。

この手順では、vRealize Automation を特定の連続した方法で再起動します。vRealize Automation のシャットダウンと再起動の関連情報については、[vRealize Automation の起動と停止](#)を参照してください。

- 1 次のコマンドを使用して、vRealize Automation ノードまたはクラスタが健全な状態であることを確認します。

```
vraccli service status
```

- 2 vRealize Automation が健全な状態である場合は、次のコマンドを使用して、ノードまたはクラスタ アプライアンスの代替 IP アドレスを設定します。

```
vraccli network alternative-ip set --dns DNSIPaddress1,DNSIPaddress2 IPV4_address  
Gateway_IPV4_address
```

クラスタを使用している場合は、クラスタ内の該当する各ノードの代替 IP アドレスを設定します。

- 3 次のコマンドを使用して、サービスをシャットダウンします。

```
/opt/scripts/deploy.sh -shutdown
```

- 4 必要に応じて、vRealize Automation のフェイルオーバーまたは移行操作を実行します。[VMware Site Recovery Manager](#) に関する情報と、社内での実行手順およびプラクティスを参照してください。

- 5 次のコマンドを使用して、vRealize Automation の IP アドレスを変更します。

```
vraccli network alternative-ip swap
```

vRealize Automation クラスタを使用している場合は、クラスタ内の各ノードの IP アドレスを変更する必要があります。

- 6 次のコマンドを使用して、vRealize Automation を再起動します。

```
shutdown -r now
```

vRealize Automation クラスタを使用している場合は、クラスタ内の各ノードを再起動する必要があります。

- 7 次のコマンドを使用して、vRealize Automation サービスを再展開します。

```
/opt/scripts/deploy.sh
```

vRealize Automation を再起動し、サービスの再展開が実行されたら、新しい IP アドレスで vRealize Automation を使用できるようになります。

vRealize Automation の時刻同期を有効にする方法

vRealize Automation アプライアンスのコマンドラインを使用して、vRealize Automation 環境で時刻同期を有効にすることができます。

NTP (Network Time Protocol) ネットワーク プロトコルを使用して、スタンドアロンまたはクラスタ化された vRealize Automation 環境に対して時刻同期を構成できます。vRealize Automation は、相互に排他的な 2 つの NTP 構成をサポートしています。

NTP 構成	説明
ESXi	<p>この構成は、vRealize Automation をホストしている ESXi サーバが NTP サーバと同期されている場合に使用できます。クラスタ化された環境を使用している場合は、すべての ESXi ホストを NTP サーバと同期する必要があります。ESXi 向けに NTP を構成する方法については、ナレッジベースの記事 KB57147Configuring Network Time Protocol (NTP) on an ESXi host using the vSphere Web Client を参照してください。</p> <p>注： NTP サーバと同期されていない ESXi ホストに vRealize Automation 環境を移行すると、時刻のずれが生じる場合があります。</p>
systemd	<p>この構成では systemd-timesyncd デーモンを使用して vRealize Automation 環境の時刻を同期します。</p> <p>注： デフォルトでは、systemd-timesyncd デーモンは有効になっていますが、NTP サーバなしで構成されています。動的 IP アドレス構成が使用されている vRealize Automation アプライアンスでは、DHCP プロトコルが受信する任意の NTP サーバを使用できます。</p>

手順

- 1 vRealize Automation アプライアンスのコマンドラインに root としてログインします。
- 2 ESXi で NTP モードを有効にします。
 - a `vracli ntp esxi` コマンドを実行します。
 - b (オプション) NTP 構成のステータスを確認するには、`vracli ntp status` コマンドを実行します。

`vracli ntp reset` コマンドを実行して、NTP 構成をデフォルトの状態にリセットすることもできます。
- 3 systemd で NTP モードを有効にします。
 - a `vracli ntp systemd --set FQDN_or_IP_of_systemd_server` コマンドを実行します。

注： 複数の systemd NTP サーバを追加するには、ネットワーク アドレスをカンマで区切ります。各ネットワーク アドレスは、一重引用符で囲む必要があります。たとえば、`vracli ntp systemd --set 'ntp_address_1','ntp_address_2'` とします。

 - b (オプション) NTP 構成のステータスを確認するには、`vracli ntp status` コマンドを実行します。

結果

vRealize Automation アプライアンス環境で時刻同期を有効にしました。

次のステップ

NTP サーバと vRealize Automation 環境の間に 10 分を超える時間差があると、NTP 構成は失敗する可能性があります。この問題を解決するには、vRealize Automation アプライアンスを再起動します。

vRealize Automation の root パスワードをリセットする方法

vRealize Automation root パスワードを紛失したり、忘れたりした場合は、パスワードをリセットできます。

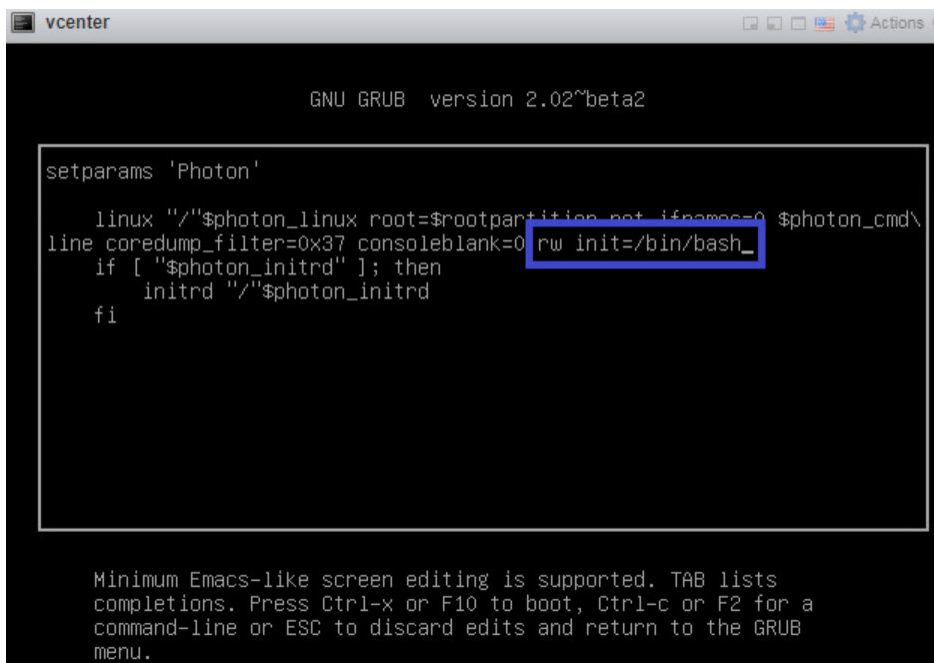
この手順では、ホスト vCenter アプライアンスのコマンドライン ウィンドウを使用して、組織の vRealize Automation root パスワードをリセットします。

前提条件

このプロセスは、vRealize Automation 管理者を対象としています。また、このプロセスでは、ホスト vCenter アプライアンスにアクセスする際に必要な認証情報を入力する必要があります。

手順

- 1 [vRealize Automation の起動と停止](#)で説明されている手順を使用して、vRealize Automation をシャットダウンして起動します。
- 2 Photon オペレーティング システムのコマンドライン ウィンドウが表示されたら、e と入力して [Enter] キーを押し、GNU GRUB ブート メニュー エディタを開きます。
- 3 GNU GRUB エディタで、次のように `linux "/" $photon_linux root=rootpartition` で始まる行の最後に `rw init=/bin/bash` と入力します。



```

vcenter
GNU GRUB version 2.02~beta2

setparams 'Photon'

linux "/"$photon_linux root=$rootpartition not ifnames=0 $photon_cmd\
line coredump_filter=0x37 consoleblank=0 rw init=/bin/bash_
if [ "$photon_initrd" ]; then
    initrd "/"$photon_initrd
fi

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
command-line or ESC to discard edits and return to the GRUB
menu.
  
```

- 4 [F10] キーをクリックして変更をプッシュし、vRealize Automation を再起動します。
- 5 vRealize Automation が再起動するまで待機します。
- 6 `root [/]# passwd` と入力し、[Enter] キーを押します。
- 7 `New password:` プロンプトで新しいパスワードを入力し、[Enter] キーを押します。
- 8 `Retype new password:` プロンプトが表示されたら、新しいパスワードを再入力して、[Enter] キーを押します。
- 9 `root [/]# reboot -f` と入力して [Enter] キーを押し、root パスワードのリセット プロセスを完了します。

```
root [ / ]# passwd
New password:
Retype new password:
passwd: password updated successfully
root [ / ]# reboot -f_
```

次のステップ

vRealize Automation 管理者として、新しい root パスワードを使用して vRealize Automation にログインできます。

vRealize Automation でのマルチ組織テナント構成の使用

4

vRealize Automation により、IT プロバイダは、各展開内で複数のテナントまたは組織を設定できます。プロバイダは、複数のテナント組織を設定し、各展開の中でインフラストラクチャを割り当てることができます。プロバイダは、テナントのユーザーを管理することもできます。各テナントは、それぞれのプロジェクト、リソース、展開を管理します。

vRealize Automation マルチ組織構成では、プロバイダは複数の組織の作成が可能で、各テナント組織は独自のプロジェクト、リソース、および展開を使用します。プロバイダはテナント インフラストラクチャをリモートで管理することはできませんが、テナントにログインして、テナント内のインフラストラクチャを管理できます。

マルチテナントは、次に示すように、3 つの異なる VMware 製品の調整と構成に依存します。

- **Workspace ONE Access**- この製品では、テナント組織内のユーザーおよびグループの管理を提供するマルチテナントおよび Active Directory ドメイン接続のインフラストラクチャ サポートを提供しています。
- **vRealize Suite Lifecycle Manager**- この製品では、vRealize Automation などのサポート対象製品のテナントの作成と構成がサポートされています。さらに、一部の証明書管理機能を提供します。
- **vRealize Automation**- プロバイダおよびユーザーは、vRealize Automation にログインして、展開を作成および管理するテナントにアクセスします。

マルチテナントを構成する場合、ユーザーはこれらの 3 つの製品のすべてと、関連するドキュメントに精通している必要があります。

vRealize Suite Lifecycle Manager および Workspace ONE Access の操作の詳細については、以下を参照してください。

- **vRealize Suite Lifecycle Manager - Lifecycle Manager 製品ドキュメント**を参照してください
- **Workspace ONE Access - VMware Identity Manager を使用したユーザー管理および VMware Workspace ONE Access の管理**を参照してください。

vRealize Suite Lifecycle Manager 権限を持つ管理者は、[ID およびテナント管理サービス] の下にある [Lifecycle Manager テナント] 画面を使用して、テナントを作成および管理します。テナントは、Active Directory IWA または LDAP 接続を使用して構築され、vRealize Automation の展開に必要な関連付けられた VMware Workspace ONE Access インスタンスによってサポートされます。Lifecycle Manager の使用方法の詳細については、関連するドキュメントを参照してください。

マルチテナントを構成するときは、基本のテナントまたはマスター テナントから開始します。このテナントは、基盤となる Workspace ONE Access アプリケーションの展開時に作成されるデフォルトのテナントです。サブテナントと呼ばれるその他のテナントは、マスター テナントに基づくことができます。vRealize Automation は現在、標準の 3 ノード展開で最大 20 のテナント組織をサポートしています。

vRealize Automation をマルチテナント用に有効にする場合は、最初にアプリケーションを単一の組織構成にインストールしてから、Lifecycle Manager を使用してマルチ組織構成を設定する必要があります。Workspace ONE Access の展開では、テナントおよび関連付けられた Active Directory ドメイン接続の管理がサポートされています。

マルチテナントを最初に設定する際には、プロバイダ管理者が Lifecycle Manager で指定されます。必要に応じて、後からこの指定を変更することも管理者を追加することもできます。マルチ組織構成では、vRealize Automation ユーザーとグループは主に Workspace ONE Access を使用して管理されます。

組織が作成されると、承認されたユーザーはアプリケーションにログインして、プロジェクトおよびリソースを作成または操作したり、展開を作成したりすることができます。管理者は、vRealize Automation でユーザー ロールを管理できます。

マルチ組織構成用の設定

vRealize Automation のインストールを完了すると、マルチ組織展開を有効にできます。マルチ組織構成を実行する場合は、マルチテナントで使用するように外部の Workspace ONE Access を構成してから、Lifecycle Manager を使用してテナントを作成および構成する必要があります。これは、新規および既存の展開の両方に適用されます。テナントを設定する最初の手順として、Lifecycle Manager を使用して、Workspace ONE Access でデフォルトで作成されたマスター テナントのエイリアスを設定する必要があります。このマスター テナントに基づいて作成するサブテナントは、このマスター テナントから Active Directory ドメイン構成を継承します。

Lifecycle Manager では、vRealize Automation などの製品や特定の環境にテナントを割り当てることができます。テナントを設定するときは、テナント管理者も指定する必要があります。マルチテナントは、テナントのホスト名に基づいてデフォルトで有効です。ユーザーは、DNS 名を使用してテナント名を手動で構成することを選択できます。この手順では、マルチテナントをサポートするためにいくつかのフラグを設定する必要があり、ロード バランサも構成する必要があります。

クラスタ化されたインスタンスを使用する場合は、Workspace ONE Access と vRealize Automation の両方のテナント ベースのホスト名がロード バランサを参照します。

クラスタ化された vRealize Automation および Workspace ONE Access のロード バランサでワイルドカード証明書を使用しない場合、ユーザーは、作成される新しいテナントごとに、証明書の SAN エントリとしてテナント ホスト名を追加する必要があります。

vRealize Automation または Lifecycle Manager でテナントを削除することはできません。テナントを既存のマルチテナント展開に追加する必要がある場合は、Lifecycle Manager を使用して実行できますが、3 ～ 4 時間のダウンタイムが必要になります。

vRealize Suite Lifecycle Manager Workspace ONE Access の使用方法の詳細については、このトピックの先頭にあるドキュメント リンクを参照してください。

ホスト名とマルチテナント

以前のバージョンの vRealize Automation では、ユーザーはディレクトリ パスに基づいて URL を使用してテナントにアクセスしました。現在のマルチテナントの実装では、ユーザーはホスト名に基づいてテナントにアクセスします。

また、vRealize Automation ユーザーがテナントへのアクセスに使用するホスト名の形式は、Workspace ONE Access 内のテナントへのアクセスに使用される形式とは異なります。たとえば、有効なホスト名は、`vidm-node1.eng.vmware.com` ではなく、`tenant1.example.eng.vmware.com` のようになります。

マルチテナントと証明書

マルチ組織構成に関連するすべてのコンポーネントについて、証明書を作成する必要があります。使用しているのが 1 つのノード構成かクラスタ化された構成かに応じて、Workspace ONE Access、Lifecycle Manager、vRealize Automation 用に 1 つまたは複数の証明書が必要になります。

証明書を構成するとき、SAN 名または特定の名前を示すワイルドカードを使用できます。証明書は、新しいテナントを追加するたびに更新する必要があるため、ワイルドカードを使用するとその管理をある程度簡素化できます。vRealize Automation および Workspace ONE Access のロード バランサでワイルドカード証明書を使用しない場合、ユーザーは、作成される新しいテナントごとに、証明書の SAN エントリとしてテナント ホスト名を追加する必要があります。また、SAN を使用している場合は、ホストを追加または削除したときや、ホスト名を変更したときに証明書を手動で更新する必要があります。また、テナントの DNS エントリも更新する必要があります。

Lifecycle Manager は、テナントごとに個別の証明書を作成しないことに注意してください。代わりに、各テナントのホスト名がリストされた単一の証明書を作成します。基本構成の場合、テナントの CNAME では次の形式が使用されます：`tenantname.vrahostname.domain`。高可用性構成の場合、名前では次の形式が使用されます：`tenantname.vraLBhostname.domain`

クラスタ化された Workspace ONE Access 構成を使用している場合は、Lifecycle Manager がロード バランサ証明書を更新できないため、手動で更新する必要があることに注意してください。また、Lifecycle Manager の外部にある製品またはサービスを再登録する必要がある場合、これは手動のプロセスです。

この章には、次のトピックが含まれています。

- [vRealize Automation のマルチ組織テナントの設定](#)
- [テナントへのログインおよび vRealize Automation へのユーザーの追加](#)
- [vRealize Orchestrator と vRealize Automation マルチ組織展開の使用](#)

vRealize Automation のマルチ組織テナントの設定

vRealize Suite Lifecycle Manager を使用して、vRealize Automation のマルチ組織テナントを設定できます。

DNS や証明書の構成など、vRealize Automation のマルチテナントを設定する手順の概要は次のとおりです。単一ノードの展開に重点を置っていますが、クラスタ化された構成に関する注意事項が含まれています。

<https://vmwarelab.org/2020/04/14/vrealize-automation-8-1-multi-tenancy-setup-with-vrealize-suite-lifecycle-manager-8-1/> で、詳細および vRealize Automation のマルチ組織構成を実行するデモのビデオを参照してください。

前提条件

- Workspace ONE Access バージョン 3.3.4 以降をインストールして構成します。
- vRealize Suite Lifecycle Manager バージョン 8.5 をインストールして構成します。

手順

1 必要な A タイプおよび CNAME タイプの DNS レコードを作成します。

- マスター テナントと各サブテナントに対して、SAN 証明書を作成して適用する必要があります。
- 単一ノードの展開では、vRealize Automation の FQDN が vRealize Automation アプライアンスを参照し、Workspace ONE Access の FQDN が Workspace ONE Access アプライアンスを参照します。
- クラスタ化された展開では、Workspace ONE Access と vRealize Automation の両方のテナントベースの FQDN が各ロード バランサを参照している必要があります。Workspace ONE Access は SSL ターミネーションを使用して構成されているため、証明書は Workspace ONE Access クラスタとロード バランサの両方に適用されます。vRealize Automation ロード バランサは SSL パススルーを使用するため、証明書は vRealize Automation クラスタにのみ適用されます。

詳細については、[単一ノードのマルチ組織環境での証明書および DNS 構成の管理](#)および[クラスタ化された vRealize Automation 展開での証明書および DNS 構成の管理](#)を参照してください。

2 Workspace ONE Access と vRealize Automation の両方に対して必要なマルチドメイン (SAN) 証明書を作成またはインポートします。

証明書のライセンスとパスワードを作成できるようにする Locker サービスを使用して Lifecycle Manager で証明書を作成できます。または、CA サーバやその他のメカニズムを使用して証明書を生成することもできます。

追加のテナントを追加または作成する必要がある場合は、vRealize Automation および Workspace ONE Access テナントを再作成して適用する必要があります。

証明書を作成したら、[ライフサイクル操作] 機能を使用して、Lifecycle Manager に適用できます。環境と製品を選択し、右側のメニューの [証明書の置き換え] オプションを選択する必要があります。その後、製品を選択できます。証明書を置き換える場合は、環境内の関連付けられているすべての製品を再信頼する必要があります。

次の手順に進む前に、証明書が適用され、すべてのサービスが再起動するまで待機する必要があります。

詳細については、[単一ノードのマルチ組織環境での証明書および DNS 構成の管理](#)および[クラスタ化された vRealize Automation 展開での証明書および DNS 構成の管理](#)を参照してください。

3 Workspace ONE Access SAN 証明書を Workspace ONE Access インスタンスまたはクラスタに適用します。

4 vRealize Suite Lifecycle Manager で、[テナントの有効化] ウィザードを実行してマルチテナントを有効にし、デフォルトのマスター テナントのエイリアスを作成します。

テナントを有効にするには、プロバイダ組織のマスター テナントまたはデフォルトのテナントのエイリアスを作成する必要があります。テナントを有効にすると、マスター テナントの FQDN を使用して Workspace ONE Access にアクセスできます。

たとえば、既存の Workspace ONE Access の FQDN が `idm.example.local` で、デフォルトのテナントのエイリアスを作成した場合、テナントを有効にすると、Workspace ONE Access の FQDN が `default-tenant.example.local` に変更され、Workspace ONE Access と通信するすべてのクライアントは `default-tenant.example.local` を介して通信するようになります。

- 5 vRealize Automation SAN 証明書を vRealize Automation インスタンスまたはクラスタに適用します。

SAN 証明書は Lifecycle Manager の Lifecycle Operations サービスを使用して適用できます。環境の詳細を表示し、右側のメニューで [証明書の置き換え] を選択する必要があります。証明書の置き換えタスクが完了するまで待ってから、テナントを追加する必要があります。証明書の置き換えの一環として、vRealize Automation サービスが再起動します。

- 6 Lifecycle Manager で、テナントの追加ウィザードを実行して、目的のテナントを構成します。

テナントを追加するには、[ID およびテナントの管理] の下にある [Lifecycle Manager テナントの管理] ページを使用します。追加できるのは、事前構成済みの証明書および DNS 設定があるテナントだけです。

テナントを作成する際には、テナント管理者を指定し、このテナントの Active Directory 接続を選択する必要があります。使用可能な接続は、デフォルトまたはマスター テナントで構成された接続に基づきます。テナントが関連付けられる製品または製品インスタンスも選択する必要があります。

次のステップ

テナントを作成した後、[ID およびテナントの管理] の下にある [Lifecycle Manager テナントの管理] ページを使用して、テナント管理者の変更や追加、Active Directory ディレクトリのテナントへの追加、テナントへの製品関連付けの変更が可能です。

Workspace ONE Access インスタンスにログインして、テナントの構成を表示および検証することもできます。

単一ノードのマルチ組織環境での証明書および DNS 構成の管理

マルチ組織テナントの vRealize Automation 構成は、複数の製品間で調整された構成に依存します。マルチ組織テナント構成を機能させるには、DNS 設定と証明書が適切に構成されていることを確認する必要があります。

このマルチ組織構成は、次のコンポーネントによる単一ノードの展開を前提にしています。

- Lifecycle Manager
- Workspace ONE Access Identity Manager
- vRealize Automation

また、プロバイダ組織であるデフォルトのテナントから開始し、tenant-1 と tenant-2 という名前の 2 つのサブテナントを作成することを前提としています。

証明書を作成して適用するには、vRealize Suite Lifecycle Manager の Locker サービスを使用することも、別のメカニズムを使用することもできます。また、Lifecycle Manager を使用すると、vRealize Automation または Workspace ONE Access 上で証明書を置き換えることや、再信頼することもできます。

DNS 要件

以下で説明するように、システム コンポーネントに対してメインの A タイプ レコードと CNAME タイプ レコードの両方を作成する必要があります。

- メインの A タイプ レコードを、マルチテナントを有効にするときに作成する各システム コンポーネントと各テナントの両方に対して作成します。
- 作成する各テナントのほか、マスター テナントに対して、マルチテナントの A タイプ レコードを作成します。

- マスター テナント以外の、作成する各テナントに対してマルチ テナントの CNAME タイプ レコードを作成します。

単一ノードのマルチテナント展開における証明書の要件

2 つの Subject Alternative Name (SAN) 証明書を作成する必要があります。1 つは Workspace ONE Access 用で、もう 1 つは vRealize Automation 用です。

- vRealize Automation 証明書には、vRealize Automation サーバのホスト名と、作成するテナントの名前が一覧表示されます。
- Workspace ONE Access 証明書には、作成している Workspace ONE Access サーバのホスト名とテナント名が一覧表示されます。
- 専用の SAN 名を使用している場合は、ホストを追加または削除したときや、ホスト名を変更したときに証明書を手動で更新する必要があります。また、テナントの DNS エントリも更新する必要があります。必要に応じて、構成を簡素化するために、Workspace ONE Access および vRealize Automation 証明書にワイルドカードを使用できます。たとえば、*.example.com や *.vra.example.com のようにします。

注： vRealize Automation 8.x では、<https://publicsuffix.org> にあるパブリック サフィックス リストの仕様に一致する DNS 名に対してのみ、ワイルドカード証明書をサポートしています。たとえば、*.myorg.com は有効な名前ですが、*.myorg.local は無効です。

Lifecycle Manager は、テナントごとに個別の証明書を作成しないことに注意してください。代わりに、各テナントのホスト名がリストされた単一の証明書を作成します。基本構成の場合、テナントの CNAME では次の形式が使用されます：*tenantname.vrahostname.domain* 高可用性構成の場合、名前では次の形式が使用されます：*tenantname.vraLBhostname.domain*

サマリ

次の表では、単一ノード Workspace ONE Access と単一ノード vRealize Automation の展開の DNS および証明書の要件の概要を示します。

DNS 要件	SAN 証明書の要件
Main A Type Records lcm.example.local WorkspaceOne.example.local vra.example.local	Workspace One Certificate ホスト名： WorkspaceOne.example.local、default-tenant.example.local、 tenant-1.vra.example.local、tenant-2.vra.example.local
Multi-tenancy A Type Records default-tenant.example.local tenant-1.example.local tenant-2.example.local	
Multi-Tenancy CNAME Type Records tenant-1.vra.example.local tenant-2.vra.example.local	vRealize Automation Certificate ホスト名： vra.example.local、tenant-1.vra.example.local、tenant-2.vra.example.local

クラスタ化された vRealize Automation 展開での証明書および DNS 構成の管理

マルチ組織のクラスタ化された vRealize Automation 展開を設定するには、該当するすべてのコンポーネント間で証明書と DNS の構成を調整する必要があります。

標準的なクラスタ構成には、3 台の Workspace ONE Access アプライアンスと 3 台の vRealize Automation アプライアンス、および 1 台の Lifecycle Manager アプライアンスがあります。

この構成は、次のコンポーネントによるクラスタ化された展開を前提にしています。

- Workspace ONE Access Identity Manager アプライアンス :

- idm1.example.local
- idm2.example.local
- idm3.example.local
- idm-lb.example.local

- vRealize Automation アプライアンス :

- vra-1.example.local
- vra-2.example.local
- vra-3.example.local
- vra-lb.example.local

- Lifecycle Manager アプライアンス

DNS 要件

メインの A タイプ レコードを、マルチテナントを有効にするときに作成する各コンポーネントと各テナントの両方に対して作成する必要があります。さらに、マスター テナント以外の、作成する各テナントに対してマルチ テナントの CNAME タイプ レコードを作成する必要があります。最後に、Workspace ONE Access および vRealize Automation ロード バランサに対するメインの A タイプ レコードも作成する必要があります。

- 3 台の Workspace ONE Access アプライアンスと、それぞれの FQDN を参照する vRealize Automation アプライアンスに対して、A タイプ レコードを作成します。
- また、Workspace ONE Access ロード バランサと、それぞれの FQDN を参照する vRealize Automation ロード バランサに対して、A タイプ レコードを作成します。
- デフォルトのテナントと、Workspace ONE Access ロード バランサの IP アドレスを参照する tenant-1 および tenant-2 に対して、マルチテナントの A タイプ レコードを作成します。
- vRealize Automation ロード バランサの IP アドレスを参照する tenant-1 および tenant-2 の CNAME レコードを作成します。

Subject Alternative Names (SAN) 証明書の要件

2 つの Workspace ONE Access 証明書を作成する必要があります。1 つはクラスタ アプライアンスに適用され、もう 1 つはロード バランサに適用されます。さらに、vRealize Automation アプライアンス、作成するテナント (デフォルトのテナント以外)、およびロード バランサに適用される証明書を作成します。

- Workspace ONE Access アプライアンスの証明書を作成します。この証明書には、Workspace ONE Access アプライアンスの FQDN およびデフォルトのテナントと作成した他のテナントが一覧表示されます。この証明書には、Workspace ONE Access アプライアンスの IP アドレスが含まれている必要があります。
- ベスト プラクティスとして、ロード バランサで SSL ターミネーションを作成します。このターミネーションをサポートするには、Workspace ONE Access ロード バランサの証明書を作成します。これには、Workspace ONE Access ロード バランサの FQDN、デフォルトのテナント、および作成した他のすべてのテナントが一覧表示されます。この証明書には、ロード バランサの IP アドレスが含まれている必要があります。
- 3 台の vRealize Automation アプライアンスのホスト名、および関連するロード バランサと作成しているテナントを一覧表示する vRealize Automation 用の証明書を作成する必要があります。また、3 台の vRealize Automation アプライアンスの IP アドレスを一覧表示する必要があります。
- 必要に応じて、構成を簡素化するために、Workspace ONE Access および vRealize Automation 証明書にワイルドカードを使用できます。たとえば、*.example.com、*.vra.example.com および *.vra-lb.example.com のようにします。

注： vRealize Automation 8.x では、<https://publicsuffix.org> にあるパブリック サフィックス リストの仕様に一致する DNS 名に対してのみ、ワイルドカード証明書をサポートしています。たとえば、*.myorg.com は有効な名前ですが、*.myorg.local は無効です。

クラスタ化された Workspace ONE Access 構成を使用している場合は、Lifecycle Manager がロード バランサ証明書を更新できないため、手動で更新する必要があることに注意してください。また、Lifecycle Manager の外部にある製品またはサービスを再登録する必要がある場合、これは手動のプロセスです。

クラスタ化されたマルチ組織構成の DNS エントリと証明書の概要

以下の表に、クラスタ化された Workspace ONE Access およびクラスタ化された vRealize Automation マルチ組織展開における DNS メイン A タイプ レコードおよび CNAME タイプ レコードと証明書の要件の概要を示します。

DNS 要件	SAN 証明書の要件
<p>Main A Type Records</p> <ul style="list-style-type: none"> ■ lcm.example.local ■ WorkspaceOne-1.example.local ■ WorkspaceOne-2.example.local ■ WorkspaceOne-3.example.local ■ WorkspaceOne-lb.example.local ■ vra-1.example.local ■ vra-2.example.local ■ vra-3.example.local ■ vra-lb.example.local 	<p>Workspace One Certificate</p> <p>ホスト名 :</p> <ul style="list-style-type: none"> ■ WorkspaceOne-1.example.local ■ WorkspaceOne-2.example.local ■ WorkspaceOne-3.example.local ■ default-tenant.example.local ■ tenant-1.example.local ■ tenant-2.example.local
<p>Multi-Tenancy A Type Records</p> <ul style="list-style-type: none"> ■ default-tenant.example.local ■ tenant-1.vra.example.local ■ tenant-2.vra.example.local <p>注： すべてのマルチテナント A タイプ レコードは、vIDM/WS1A ロード バランサの IP アドレスを参照する必要があります。</p>	<p>Workspace One LB Certificate (LB Terminated)</p> <p>ホスト名 :</p> <ul style="list-style-type: none"> ■ WorkspaceOne-lb.example.local ■ default-tenant.example.local ■ tenant-1.example.local ■ tenant-2.example.local
<p>Multi-Tenancy CNAME Type Records</p> <ul style="list-style-type: none"> ■ tenant-1.vra-lb.example.local - vra-lb.example.local ■ tenant-2.vra-lb.example.local - vra-lb.example.local 	<p>vRealize Automation Certificate</p> <p>ホスト名 :</p> <ul style="list-style-type: none"> ■ vra-1.example.local ■ vra-2.example.local ■ vra-3.example.local ■ vra-lb.example.local ■ tenant-1.example.local ■ tenant-2.example.local <p>SSL パススルーを使用しているため、vRealize Automation ロード バランサに証明書は必要ありません。</p>

注： 追加する各テナントは、vRealize Automation 証明書、マルチテナント CNAME レコード、マルチテナント タイプ A レコード、Workspace ONE 証明書、および Workspace ONE LB 証明書に個別に一覧表示する必要があります。

注： *.local ファイル名は、サンプル専用の名前です。多くのビジネス環境では適用できない可能性があります。

テナントへのログインおよび vRealize Automation へのユーザーの追加

Lifecycle Manager で vRealize Automation のテナントを作成した後、Workspace ONE Access にログインしてテナントを表示したり、ユーザーを追加したりできます。

関連付けされた Workspace ONE Access インスタンスにログインすることで、vRealize Automation 展開に作成されたテナントを表示できます。使用する URL は `https://default-tenant name.domainname.local` で、クラスタ化されていない展開の場合は `https://idm.domainname.local` になります。これは、デフォルトのテナント Workspace ONE Access の URL にリダイレクトします。

URL: `https://tenant-1.domainname.local` を使用して、Workspace ONE Access で特定のテナントを検証できます。この URL を指定すると、指定したテナントのユーザーが表示されるページが開きます。[ユーザーの追加] をクリックして、アドホック ベースで追加のユーザーを作成できます。

認証されたユーザーは、`https://vra.domainname.local` を使用して vRealize Automation でメイン プロバイダ組織にログインできます。このビューから、すべての vRealize Automation 関連サービスにアクセスすることができます。

認証されたユーザーは、`https://tenantname.vra.domainname.local` を使用して、vRealize Automation に該当するテナントにログインできます。

Workspace ONE Access でユーザーを管理する方法の詳細については、[ユーザーとグループの管理](#)を参照してください。

ローカル ユーザーの追加

関連付けられた Workspace ONE Access インスタンスを使用して、ローカル ユーザーを展開に追加できます。ローカル ユーザーとは、外部 ID プロバイダに保存されていないユーザーのことです。

vRealize Orchestrator と vRealize Automation マルチ組織展開の使用

vRealize Orchestrator を vRealize Automation マルチ組織テナント展開と組み合わせて使用できます。

デフォルトのテナントは、組み込みの vRealize Orchestrator 統合との間で、特別な設定を必要としない統合をサポートしています。vRealize Orchestrator は、デフォルト テナントの [統合] ページで事前構成され、利用可能です。サブテナントには事前登録された vRealize Orchestrator 統合はありません。vRealize Orchestrator の統合を追加するためのオプションがいくつかあります。

- サブテナントでは、[インフラストラクチャ] - [接続] - [統合] の順に移動して、組み込みの vRealize Orchestrator との統合を追加できます。

注： 組み込みの vRealize Orchestrator が統合として複数のテナントに追加されると、プラグイン インベントリなど、すべての vRealize Orchestrator コンテンツがこれらのテナント間で共有されます。

- サブテナントでは、マルチ組織 vRealize Automation を認証プロバイダとして使用する外部の vRealize Orchestrator インスタンスを追加できます。

vRealize Automation マルチ組織展開を認証プロバイダとして使用するすべての vRealize Orchestrator インスタンスを新しい統合を作成し、認証情報を指定せずに vRealize Orchestrator の FQDN を指定するテナントに登録できます。

vRealize Automation でのログの操作

5

提供されている `vraccli` コマンドライン ユーティリティを使用して、vRealize Automation でログを作成および使用できます。

vRealize Automation で直接ログを使用することも、すべてのログを vRealize Log Insight に転送することもできます。

この章には、次のトピックが含まれています。

- vRealize Automation でログおよびログ バンドルを操作する方法
- vRealize Automation で vRealize Log Insight へのログ転送を設定する方法
- vRealize Automation で Syslog 統合を作成または更新する方法
- コンテンツ バックの使用方法

vRealize Automation でログおよびログ バンドルを操作する方法

ログは、さまざまなサービスによって自動的に生成されます。ログ バンドルは、vRealize Automation で生成できます。ログを vRealize Log Insight に自動的に送信するように環境を設定することもできます。

`vraccli` コマンド ライン ユーティリティの詳細を確認するには、`vraccli` コマンド ラインで `--help` 引数 (`vraccli log-bundle --help` など) を使用します。

vRealize Log Insight の使用に関する関連情報については、[vRealize Automation で vRealize Log Insight へのログ転送を設定する方法](#)を参照してください。

ログ バンドル コマンド

ログ バンドルを作成して、実行するサービスから生成されるすべてのログを含めることができます。ログ バンドルには、すべてのサービス ログが含まれます。ログ バンドルはトラブルシューティングに使用できます。

クラスタ化された環境（高可用性モード）では、1 台のノードでのみ `vraccli log-bundle` コマンドを実行します。環境内のすべてのノードからログがプルされます。ただし、ネットワークや他のクラスタに問題が発生した場合は、到達可能なすべてのノードからログが取得されます。たとえば、3 ノードのクラスタで 1 台のノードが切断された場合、ログは 2 台の健全なノードからのみ収集されます。`vraccli log-bundle` コマンドからの出力には、検出された問題とその回避策の手順に関する情報が含まれています。

- ログ バンドルを作成するには、任意のノードに SSH 接続し、次の `vraccli` コマンドを実行します。

```
vraccli log-bundle
```

- 各ノードからログを収集する際のタイムアウト値を変更するには、次の `vracli` コマンドを実行します。

```
vracli log-bundle --collector-timeout $CUSTOM_TIMEOUT_IN_SECONDS
```

たとえば、環境に大きなログ ファイルが含まれている、ネットワークが遅い、または CPU 使用率が高い場合は、タイムアウトをデフォルト値の 1,000 秒よりも大きく設定することをお勧めします。

- `ebs` や `vro` などの特定のサービス ログで使用されているディスク容量を確認するには、次の `vracli` コマンドを実行してコマンド出力を調べます。

```
vracli disk-mgr
```

- アセンブリのタイムアウトやバッファの場所など、その他のオプションを設定するには、次の `vracli help` コマンドを使用します。

```
vracli log-bundle --help
```

ログ バンドルの構造

ログ バンドルは、タイムスタンプ付きの tar ファイルです。バンドルの名前は、`log-bundle-`

`<date>T<time>.tar` ファイルというパターンになります。たとえば、`log-bundle-20200629T131312.tar` です。通常、ログ バンドルには環境内のすべてのノードのログが含まれています。エラーが発生した場合は、できるだけ多くのログが記録されます。ローカル ノードからのログは最小限含まれています。

ログ バンドルは、次の内容で構成されます。

■ 環境ファイル

環境ファイルには、さまざまな Kubernetes メンテナンス コマンドの出力が含まれています。現在のリソース使用に関する情報が、ノード別およびポッド別に提供されます。また、使用可能なすべての Kubernetes エンティティのクラスタ情報と説明も含まれています。

■ ホスト ログと設定

各ホストの設定（`/etc` ディレクトリなど）とホスト固有のログ（`journal` など）は、1 台のクラスタ ノードまたはホストにつき 1 つのディレクトリに収集されます。ディレクトリ名は、ノードのホスト名と一致します。ディレクトリの内部コンテンツは、ホストのファイル システムと一致します。ディレクトリの数はクラスタ ノードの数と一致します。

■ サービス ログ

Kubernetes サービスのログは、次のフォルダ構造内にあります。

- `<hostname>/services-logs/<namespace>/<app-name>/file-logs/<container-name>.log`

- `<hostname>/services-logs/<namespace>/<app-name>/console-logs/<container-name>.log`

ファイル名は、たとえば `my-host-01/services-logs/prelude/vco-app/file-logs/vco-server-app.log` です。

- `hostname` は、アプリケーション コンテナが現在実行されている、または過去に実行されていたノードのホスト名です。通常は、各サービスのノードごとに 1 つのインスタンスがあります。たとえば、3 台のノードがあればインスタンスも 3 つです。

- *namespace* は、アプリケーションが展開されている Kubernetes 名前空間です。ユーザー向けのサービスの場合、この値は *prelude* です。
- *app-name* は、ログを生成した Kubernetes アプリケーションの名前（たとえば *provisioning-service-app*）です。
- *container-name* は、ログを生成したコンテナの名前です。一部のアプリケーションは複数のコンテナで構成されています。たとえば、*vco-app* コンテナには *vco-server-app* コンテナと *vco-controlcenter-app* コンテナが含まれています。
- (レガシー) ポッド ログ
vRealize Automation 8.2 でログアーキテクチャが変更されるまで、サービス ログはログバンドル内の各ポッドのディレクトリに置かれていました。 `vraccli log-bundle --include-legacy-pod-logs` コマンドを使用することによって引き続きバンドル内にポッド ログを生成できますが、すべてのログ情報はすでに各サービスのログに存在するため、これは推奨されません。ポッド ログを含めると、ログバンドルの生成に必要な時間と容量が不必要に増加する可能性があります。

ログバンドルのサイズの削減

生成されるログバンドルのサイズを削減するには、次のいずれかの `vraccli log-bundle` コマンドを使用します。

- `vraccli log-bundle --since-days n`

このコマンドを使用すると、過去 *n* 日間に生成されたログファイルのみが収集されます。それ以外の場合は、過去 2 日間のログが収集および保持されます。例：

```
vraccli log-bundle --since-days 1
```

- `vraccli log-bundle --services service_A,service_B,service_C`

このコマンドを使用すると、指定したサービスのログのみが収集されます。例：

```
vraccli log-bundle --services ebs-app,vco-app
```

- `vraccli log-bundle --skip-heap-dumps`

このコマンドを使用すると、生成されるログバンドルからすべてのヒープ ダンプが除外されます。

ログの表示

`vraccli logs <pod_name>` コマンドを使用して、サービス ポッドまたはアプリケーションのログを出力することができます。

次のコマンド オプションを使用できます。

- `--service`

単一のポッドではなく、アプリケーションのすべてのノードのログを 1 つにマージして表示します

例：`vraccli logs --service abx-service-app`

- `--tail n`

ログの最後の *n* 行を表示します。*n* のデフォルト値は 10 です。

例: `vracli logs --tail 20 abx-service-app-8598fcd4b4-tjwhk`

■ `--file`

指定したファイルのみを表示します。ファイル名が指定されていない場合は、すべてのファイルが表示されます。

例: `vracli logs --file abx-service-app.log abx-service-app-8598fcd4b4-tjwhk`

ログのローテーションについて

ログのローテーションについては、サービス ログに関する以下の事項を考慮します。

- すべてのサービスからログが生成されます。サービス ログは専用の `/var/log/services-logs` ディスクに格納されます。
- すべてのログは定期的にローテーションされます。ローテーションは、1 時間ごと、または一定のサイズ制限に達したときに発生します。
- すべての古いログのローテーションは、いずれかの時点で圧縮されます。
- ログのローテーションに対するサービス単位の割り当て容量はありません。
- システムは、可能な限り多くのログを保持します。ログのために使用されているディスク領域は、自動化によって定期的にチェックされます。ログのディスク領域が 70% に達すると、60% になるまで古いログが消去されます。
- さらに多くの領域が必要な場合は、ログ ディスクのサイズを変更します。[vRealize Automation アプライアンスのディスク容量の拡張](#)を参照してください。

ログのディスク領域を確認するには、次の `vracli` コマンドを実行します。`/dev/sdc (/var/log)` の空き容量は、各ノードで 30% 以上にする必要があります。

```
# vracli cluster exec -- bash -c 'current_node; vracli disk-mgr; exit 0'
sc1-10-182-1-103.eng.vmware.com
/dev/sda4(/):
    Total size: 47.80GiB
    Free: 34.46GiB (72.1%)
    Available (for non-superusers): 32.00GiB (66.9%)
    SCSI ID: (0:0)
/dev/sdb(/data):
    Total size: 140.68GiB
    Free: 116.68GiB (82.9%)
    Available (for non-superusers): 109.47GiB (77.8%)
    SCSI ID: (0:1)
/dev/sdc (/var/log):
    Total size: 21.48GiB
    Free: 20.76GiB (96.6%)
    Available (for non-superusers): 19.64GiB (91.4%)
    SCSI ID: (0:2)
/dev/sdd (/home):
    Total size: 29.36GiB
    Free: 29.01GiB (98.8%)
    Available (for non-superusers): 27.49GiB (93.7%)
    SCSI ID: (0:3)
```

vRealize Automation で vRealize Log Insight へのログ転送を設定する方法

ログを vRealize Automation から vRealize Log Insight に転送して、より確かなログ分析とレポート生成を利用できます。

vRealize Automation は、[fluentd ベースのログ エージェント](#)にバンドルされています。このエージェントはログを収集して保存することで、ログをログ バンドルに含めて後で検証できるようにします。vRealize Log Insight REST API を使用してログのコピーを vRealize Log Insight サーバに転送するように、エージェントを設定できます。API により、他のプログラムが vRealize Log Insight と通信できます。

vRealize Log Insight REST API のドキュメントなど、vRealize Log Insight の詳細については、[vRealize Log Insight のドキュメント](#)を参照してください。

提供されている `vraccli` コマンドライン ユーティリティを使用して、vRealize Automation ログを継続的に vRealize Log Insight に転送するようにログ エージェントを構成します。

ログのすべての行には、ホスト名と環境タグがタグ付けされています。これらの行は、vRealize Log Insight で調べることができます。高可用性 (HA) 環境の場合、ログには、ログ生成元のノードに応じて、さまざまなホスト名がタグ付けされます。環境タグは、`--environment ENV` オプションを使用して設定できます。詳細については、以下の「vRealize Log Insight の統合の設定または更新」セクションの説明を参照してください。HA 環境の場合、環境タグの値は、ログ生成元のノードに関係なく、すべてのログ行で同じになります。

`vraccli` コマンドライン ユーティリティの使用方法については、`vraccli` コマンドラインの `--help` 引数を使用して確認できます。例：`vraccli vrli --help`。ユーザー フレンドリな応答を得る場合は、コマンドを `vraccli -j vrli` で開始します。

注： 構成できるリモート ログ統合は 1 つだけです。vRealize Log Insight サーバと Syslog サーバの両方が使用可能な場合は、vRealize Log Insight が優先されます。

vRealize Log Insight の既存の構成の確認

Command

```
vraccli vrli
```

Arguments

コマンドライン引数はありません。

Output

vRealize Log Insight 統合の現在の設定が JSON 形式で出力されます。

Exit codes

終了コードは次のとおりです。

- 0 : vRealize Log Insight との統合が設定されています。
- 1 : コマンドの実行中に例外が発生しました。詳細については、エラー メッセージを確認してください。

- 61 (ENODATA) -vRealize Log Insight との統合は設定されていません。詳細については、エラー メッセージを確認してください。

Example - check integration configuration

```
$ vracli vrli
No vRLI integration configured

$ vracli vrli
{
  "agentId": "0",
  "environment": "prod",
  "host": "my-vrli.local",
  "port": 9543,
  "scheme": "https",
  "sslVerify": false
}
```

vRealize Log Insight の統合の設定または更新

Command

```
vracli vrli set [options] FQDN_OR_URL
```

注： コマンドを実行した後、指定した構成がログ エージェントによって適用されるまでに最大 2 分かかることがあります。

Arguments

■ FQDN_OR_URL

ログの送信に使用する vRealize Log Insight サーバの FQDN または URL アドレスを指定します。デフォルトでは、ポート 9543 と https が使用されます。これらの設定のいずれかを変更する必要がある場合は、代わりに URL を使用できます。

```
vracli vrli set <options> https://FQDN:9543
```

注： 次の例に示すように、ログの送信に使用するホスト スキーム（デフォルトは https）とポート（デフォルトは、https では 9543、http では 9000）には別の値を設定することもできます。

```
vracli vrli set https://HOSTNAME:9543
vracli vrli set --insecure HOSTNAME
vracli vrli set http://HOSTNAME:9000
```

vRealize Log Insight の取り込み REST API では、ポートとして https では 9543、http では 9000 が使用されます。詳細については、[vRealize Log Insight のドキュメント](#)の「vRealize Log Insight の管理」と「ポートおよび外部インターフェイス」を参照してください。

■ オプション

- --agent-id SOME_ID

このアプライアンスのログ エージェントの ID を設定します。デフォルトは 0 です。vRealize Log Insight REST API を使用してログを vRealize Log Insight に送信するときにエージェントを識別するために使用されます。

- --environment ENV

現在の環境の識別子を設定します。vRealize Log Insight ログで、各ログ エントリのタグとして使用できるようになります。デフォルトは prod です。

- --ca-file /path/to/server-ca.crt

vRealize Log Insight サーバの証明書の署名に使用された認証局 (CA) の証明書を含むファイルを指定します。指定された CA をログ エージェントが信頼するように設定し、vRealize Log Insight サーバの証明書が信頼されていない認証局によって署名されている場合に証明書を検証できるようにします。ファイルには、証明書を検証するための証明書チェーン全体を含めることができます。自己署名証明書の場合は、証明書自体を渡します。

- --ca-cert CA_CERT

定義は --ca-file の場合と同じですが、代わりに証明書（チェーン）が文字列としてインラインで渡されます。

- --insecure

サーバ証明書の SSL 検証を無効にします。ログの送信時に、ログ エージェントがすべての SSL 証明書を受け入れるように設定します。

- 詳細オプション

- --request-max-size BYTES

1 回の API 呼び出しで複数のログ イベントが取り込まれます。この引数は、各要求のペイロードの最大サイズ（バイト単位）を制御します。有効な値は 4,000 ~ 4,000,000 です。デフォルト値は 256,000 です。許容される値の関連情報については、vRealize Log Insight REST API ドキュメントで vRealize Log Insight イベントの取り込みに関する説明を参照してください。設定値が小さすぎると、許容サイズよりも大きいログ イベントがドロップされる可能性があります。

- --request-timeout SECONDS

API の呼び出しは、リモート、ネットワークの問題などのさまざまな理由からハングすることがあります。このパラメータは、接続を開く、データを書き込む、応答を待機するなどの処理が完了するのを待機する時間（秒）を表します。この時間が経過しても処理が完了しない場合、呼び出しは失敗したと見なされます。この値を 1 秒未満にすることはできません。デフォルトは 30 です。

- --request-immediate-retries RETRIES

ログは、チャンクに集約されてから vRealize Log Insight に送信されます（次の --buffer-flush-thread-count を参照）。API 要求が失敗した場合、ログは直ちに再試行されます。即時再試行のデフォルト回数は 3 です。再試行がすべて失敗した場合は、ログのチャンク全体がロールバックされ、後で再試行されます。

- --request-http-compress

ネットワーク トラフィック量を削減するために、vRealize Log Insight サーバに送信される要求に gzip 圧縮を適用できます。このパラメータを指定しない場合、圧縮は使用されません。

■ --buffer-flush-thread-count THREADS

パフォーマンス向上とネットワーク トラフィック節約のために、ログはローカルでチャンクとしてバッファリングされた後、フラッシュされてログ サーバに送信されます。各チャンクには1つのサービスのログが含まれます。環境によっては、チャンクのサイズが大きくなり、フラッシュに時間がかかることがあります。この引数は、同時にフラッシュできるチャンクの数来控制します。デフォルトは2です。

注： https を使用した統合を構成するとき、自己署名証明書や信頼されていない認証局によって署名された証明書など、信頼されていない証明書を使用するように vRealize Log Insight サーバが構成されている場合は、--ca-file、--ca-cert、--insecure の各オプションのいずれかを使用する必要があります。そうしない場合、ログ エージェントがサーバの ID を検証できず、ログが送信されません。--ca-file または --ca-cert を使用する場合、vRealize Log Insight サーバ証明書がサーバのホスト名に対して有効である必要があります。いずれの場合も、処理が終わるまで数分待った後で vRealize Log Insight がログを受信したことをチェックし、統合を確認します。

Output

出力はありません。

Exit codes

終了コードは次のとおりです。

- 0 - 設定が更新されました。
- 1 - 実行中に例外が発生しました。詳細については、エラー メッセージを確認してください。

Examples - Configure or update integration configuration

次のサンプル ステートメントは個別のコマンド ラインに分かれて表示されていますが、引数を1つのコマンド ラインにまとめることができます。たとえば、`vracli vrli set { somehost}` または `vracli vrli set --ca-file path/to/server-ca.crt` を使用してデフォルトのエージェント ID または環境の値を変更するときに、複数の引数を含めることができます。関連情報については、`vracli vrli --help` で表示されるオンライン コマンドのヘルプを参照してください。

```
$ vracli vrli set my-vrli.local
$ vracli vrli set 10.20.30.40
$ vracli vrli set --ca-file /etc/ssl/certs/ca.crt 10.20.30.40
$ vracli vrli set --ca-cert "$(cat /etc/ssl/certs/ca.crt)" 10.20.30.40
$ vracli vrli set --insecure http://my-vrli.local:8080
$ vracli vrli set --agent-id my-vrli-agent my-vrli.local
$ vracli vrli set --request-http-compress
$ vracli vrli set --environment staging my-vrli.local
$ vracli vrli set --environment staging --request-max-size 10000 --request-timeout 120 --request-immediate-retries 5 --buffer-flush-thread-count 4 my-vrli.local
```

vRealize Log Insight の統合のクリア

Command

```
vraccli vrli unset
```

注： コマンドを実行した後、指定した構成がログ エージェントによって適用されるまでに最大 2 分かかることがあります。

Arguments

コマンドライン引数はありません。

Output

確認はプレーン テキスト形式で出力されます。

Exit codes

次の終了コードが使用可能です。

- 0 - 設定がクリアされたか、設定がありませんでした。
- 1 - 実行中に例外が発生しました。詳細については、エラー メッセージを確認してください。

Examples - Clear integration

```
$ vraccli vrli unset
Clearing vRLI integration configuration

$ vraccli vrli unset
No vRLI integration configured
```

vRealize Automation で Syslog 統合を作成または更新する方法

ログ情報をリモートの Syslog サーバに送信するように、vRealize Automation を構成できます。

`vraccli remote-syslog set` コマンドは、Syslog 統合の作成、または既存の統合の上書きに使用されます。

vRealize Automation リモート Syslog 統合は、次の接続タイプをサポートしています。

- UDP 経由。
- TLS を使用しない TCP 経由。

注： TLS を使用せずに Syslog 統合を作成するには、`--disable-ssl` フラグを `vraccli remote-syslog set` コマンドに追加します。

- TLS を使用した TCP 経由。

注： 構成できるリモート ログ統合は 1 つだけです。vRealize Log Insight サーバと Syslog サーバの両方が使用可能な場合は、vRealize Log Insight が優先されます。

vRealize Log Insight とのログ統合の構成の詳細については、[vRealize Automation で vRealize Log Insight へのログ転送を設定する方法](#)を参照してください。

前提条件

リモートの Syslog サーバを構成します。

手順

- 1 vRealize Automation アプライアンスのコマンドラインに root としてログインします。
- 2 Syslog サーバとの統合を作成するには、`vraccli remote-syslog set` コマンドを実行します。

```
vraccli remote-syslog set -id name_of_integration protocol_type://
syslog_URL_or_FQDN:syslog_port
```

注： `vraccli remote-syslog set` コマンドにポートを入力しない場合、ポート値はデフォルトで 514 になります。

注： Syslog 構成に証明書を追加できます。証明書ファイルを追加するには、`--ca-file` フラグを使用します。証明書をプレーンテキストとして追加するには、`--ca-cert` フラグを使用します。

- 3 (オプション) 既存の Syslog 統合を上書きするには、`vraccli remote-syslog set` を実行して、上書きする統合の名前に `-id` フラグ値を設定します。

注： デフォルトでは、vRealize Automation アプライアンスは、Syslog 統合への上書きの確認を要求します。確認の要求をスキップするには、`-f` または `--force` フラグを `vraccli remote-syslog set` コマンドに追加します。

次のステップ

アプライアンスで現在の Syslog 統合を確認するには、`vraccli remote-syslog` コマンドを実行します。

vRealize Automation にログインするための Syslog 統合を削除する方法

`vraccli remote-syslog unset` コマンドを実行して、vRealize Automation アプライアンスから Syslog 統合を削除できます。

前提条件

vRealize Automation アプライアンスで 1 つ以上の Syslog 統合を作成します。[vRealize Automation で Syslog 統合を作成または更新する方法](#)を参照してください。

手順

- 1 vRealize Automation アプライアンスのコマンドラインに root としてログインします。
- 2 次のいずれかの方法を使用して、vRealize Automation アプライアンスから Syslog 統合を削除します。
 - 特定の Syslog 統合を削除するには、`vraccli remote-syslog unset -id Integration_name` コマンドを実行します。

- vRealize Automation アプライアンスのすべての Syslog 統合を削除するには、`-id` フラグを指定せずに `vracli remote-syslog unset` コマンドを実行します。

注： デフォルトでは、vRealize Automation アプライアンスは、すべての Syslog 統合の削除の確認を要求します。確認の要求をスキップするには、`-f` または `--force` フラグを `vracli remote-syslog unset` コマンドに追加します。

コンテンツ パックの使用方法

コンテンツ パックは、Log Insight でホストされます。また、コンテンツ パックには、特定の製品やログのセットに関連するダッシュボード、抽出されたフィールド、保存されたクエリ、アラートが含まれています。コミュニティでサポートされているコンテンツ パックは、VMware Sample Exchange からインストールでき、その他のコンテンツ パックはコンテンツ パック マーケットプレイスからインストールできます。

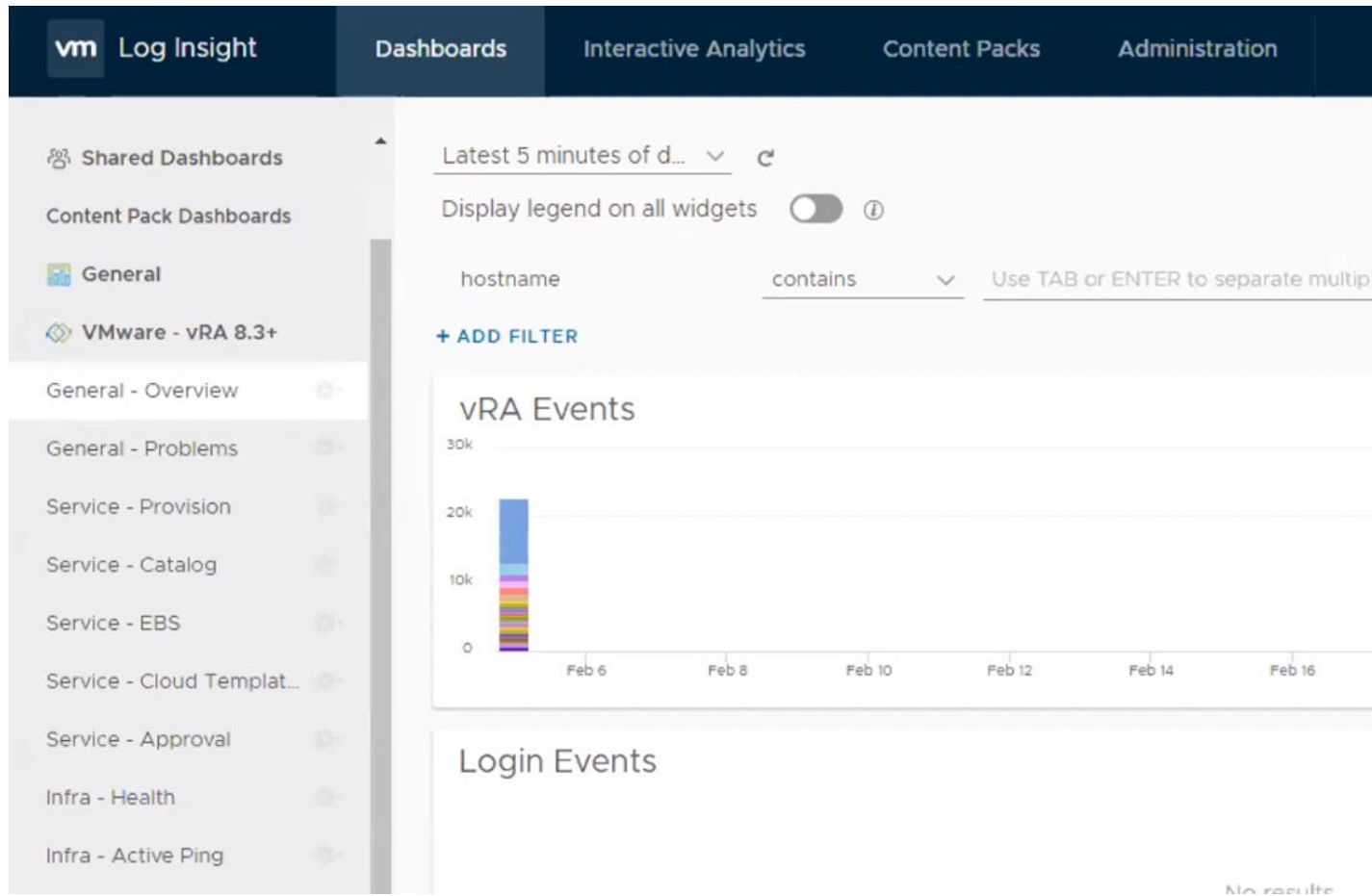
VMware vRealize Log Insight では、集約、分析、検索を通じてログ管理を自動化できます。また、動的なハイブリッド クラウド環境で運用に関する情報を得たり、企業全体の状況を把握したりできます。コンテンツ パックは、ログ メッセージなど特定のタイプのイベントに関する定義済みの情報を提供する、VMware vRealize Log Insight のプラグインです。

コンテンツ パックをダウンロードするには、Log Insight から [コンテンツ パック] - [マーケットプレイス] の順に移動します。[+ コンテンツ パックのインポート] をクリックしてコンテンツ パックをインポートすることもできます。

vRA 8.x コンテンツ パック

VMware vRealize Automation コンテンツ パックは、すべての vRA 環境コンポーネントのログ イベントのサマリーを統合された形式で提供します。組み込まれている複数のダッシュボードにより、全般的な概要、エラーや操作に関する情報、および vRA インスタンスの全体的な健全性を確認できます。これらのダッシュボードは、他のすべての Log Insight ダッシュボードと一緒に [ダッシュボード] タブに表示されます。ロードされてからダッシュボードにメトリックが入力されるまでに最大 30 秒ほどかかる場合があります。


注： vRA 7.5 以降のコンテンツ パックから vRA 8.3 コンテンツ パックにアップグレードすることはできません。vRA 8.3 コンテンツ パックをインストールする必要があります。インストール後、8.3 コンテンツ パックと 7.5 コンテンツ パックは、別々に機能します。



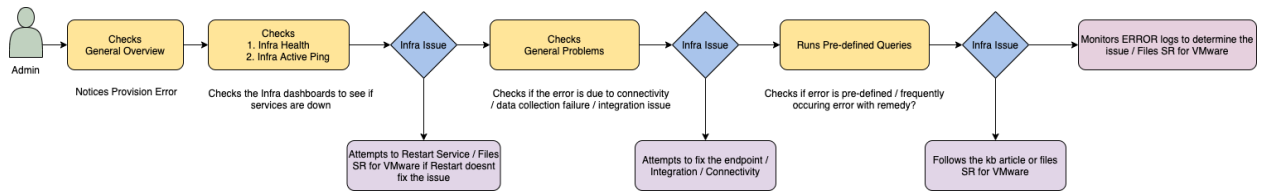
vRealize Automation コンテンツ パックには、次のダッシュボードが含まれています。

- 全般 - 概要: vRA の全体的なメトリックの概要を取得します。
- 全般 - 問題:
- サービス - プロビジョニング: プロビジョニング サービスに関連する問題を取得します。
- サービス - カタログ: カタログ サービスに関連する問題を取得します。
- サービス - EBS: イベント ブローカ サービスに関連する問題を取得します。
- サービス - クラウド テンプレート: Cloud Assembly クラウド テンプレート、カスタム リソース、およびリソース アクションに関連するエラーとメトリックを取得します。
- サービス - 承認: 承認に関連するエラーとメトリックを取得します。
- インフラストラクチャ - 健全性: 時系列の中でいつポッドが再起動されたかについての情報を取得します。このダッシュボードは、リソース制限による停止を検出するために不可欠です。
- インフラストラクチャ - アクティブな ping: 時間経過に伴う健全性チェック の URL を取得します。

各ダッシュボードには、より焦点を絞った分析を提供する個々のウィジェットが含まれています。各ウィジェットで

実行される分析のタイプを表示するには、情報  アイコンをクリックします。

通常、vRealize Automation 管理者は、次のコンテンツ バック ワークフローに従って、エラーの特定とトラブルシューティングを行います。



vRealize Automation 8.3 コンテンツ パックの詳細については、[vRealize Automation 8.3 以降の Log Insight コンテンツ パック](#)および [vRealize Log Insight](#) へのログ転送を設定する方法を参照してください。

vRealize Automation のカスタマー エクスペリエンス向上プログラムへの 参加

6

この製品は、VMware のカスタマー エクスペリエンス向上プログラム (CEIP) に参加しています。CEIP で収集される情報は、VMware の製品やサービスの向上、問題の解決に加え、各製品のデプロイおよび使用に関する最適な方法を提案するために活用されます。

CEIP を通して収集されるデータおよび VMware のその使用目的に関する詳細は、[カスタマー エクスペリエンス向上プログラム](#) ページで説明されています。

この章には、次のトピックが含まれています。

- [vRealize Automation のカスタマー エクスペリエンス向上プログラムに参加または離脱する方法](#)
- [vRealize Automation でカスタマー エクスペリエンス向上プログラムのデータ収集時間を設定する方法](#)

vRealize Automation のカスタマー エクスペリエンス向上プログラムに参加または離脱する方法

カスタマー エクスペリエンス向上プログラム (CEIP) への参加または離脱は、vRealize Automation アプライアンスのコマンド ラインから実行できます。

CEIP プログラムには、vRealize Automation のインストール時に、vRealize Lifecycle Manager (LCM) を使用して参加できます。インストール後に、コマンド ライン オプションを使用してプログラムに参加または離脱することも可能です。

コマンドライン オプションを使用してカスタマー エクスペリエンス向上プログラムに参加するには、次の手順を実行します。

- 1 vRealize Automation アプライアンスのコマンド ラインに root としてログインします。
- 2 `vraccli ceip on` コマンドを実行します。
- 3 カスタマー エクスペリエンス向上プログラムの情報を確認し、`vraccli ceip on --acknowledge-ceip` コマンドを実行します。
- 4 vRealize Automation サービスを再起動するには、`/opt/scripts/deploy.sh` コマンドを実行します。

カスタマー エクスペリエンス向上プログラムから離脱するには、次のようにコマンド ライン オプションを使用します。

- 1 vRealize Automation アプライアンスのコマンド ラインに root としてログインします。
- 2 `vraccli ceip off` コマンドを実行します。

- 3 vRealize Automation サービスを再起動するには、`/opt/scripts/deploy.sh` コマンドを実行します。

vRealize Automation でカスタマー エクスペリエンス向上プログラムのデータ収集時間を設定する方法

カスタマー エクスペリエンス向上プログラム (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マンドラインに root としてログインします。

- 2 テキスト エディタで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=<day-of-week></code>	データの収集が開始される曜日。
<code>frequency.hod=<hour-of-day></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。

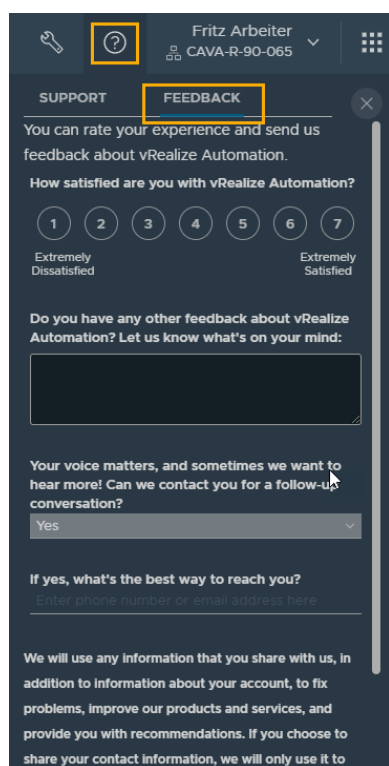
vRealize Automation での製品内フィードバック フォームの有効化

7

ユーザーから vRealize Automation 開発チームへのフィードバック送信を可能にすることができます。ユーザーからのフィードバックは開発プロセスにとって重要です。

フィードバック フォームについて

フィードバック フォームは、[フィードバック]タブのサポート パネル内にあります。このフォームを開くには、[ヘルプ] ボタンをクリックして、[フィードバック] をクリックします。



The screenshot shows a mobile application interface. At the top, there's a header with a user profile 'Fritz Arbeiter' and a device ID 'CAVA-R-90-065'. Below this, there's a navigation bar with 'SUPPORT' and 'FEEDBACK' tabs. The 'FEEDBACK' tab is active. The main content area contains a message: 'You can rate your experience and send us feedback about vRealize Automation.' followed by a rating scale from 1 to 7. Below the scale, there's a text area for additional feedback: 'Do you have any other feedback about vRealize Automation? Let us know what's on your mind:'. At the bottom, there's a dropdown menu for 'Your voice matters, and sometimes we want to hear more! Can we contact you for a follow-up conversation?' with 'Yes' selected. A note at the very bottom states: 'We will use any information that you share with us, in addition to information about your account, to fix problems, improve our products and services, and provide you with recommendations. If you choose to share your contact information, we will only use it to'.

ユーザーが [フィードバック] フォームを使用できるようにする方法

[フィードバック] フォームを使用するには、vRealize Automation ホストからインターネットにアクセスすることができ、次のベース URL がインターネット許可リストに含まれている必要があります。

- <https://lumos.vmware.com/>

- <https://feedback.esp.vmware.com/>

ホストからインターネットにアクセスできない場合は、[ヘルプ] ペインでフォームを使用できません。