

vRealize Automation の管理

2020 年 12 月 21 日

vRealize Automation 8.1

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

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

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

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

目次

- 1 vRealize Automation の管理 4**
- 2 ユーザーの管理 5**
 - [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 6](#)
 - [vRealize Automation でユーザーを削除する方法 7](#)
 - [vRealize Automation でユーザー ロールを編集する方法 7](#)
 - [vRealize Automation でグループ ロールの割り当てを編集する方法 8](#)
 - [vRealize Automation のユーザー ロールについて 8](#)
- 3 アプライアンスの保守 18**
 - [vRealize Automation の起動と停止 18](#)
 - [vRealize Automation の DNS 割り当ての更新 20](#)
 - [時刻同期を有効にする方法 21](#)
 - [時刻同期を無効にする方法 22](#)
 - [root パスワードをリセットする方法 22](#)
- 4 vRealize Automation でのマルチ組織テナント構成の使用 24**
 - [vRealize Automation のマルチ組織テナントの設定 26](#)
 - [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 28](#)
 - [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 29](#)
 - [テナントへのログインおよび vRealize Automation へのユーザーの追加 32](#)
 - [vRealize Orchestrator と vRealize Automation マルチ組織展開の使用 32](#)
- 5 ログの操作 34**
 - [ログおよびログ バンドルを操作する方法 34](#)
 - [vRealize Log Insight へのログ転送を設定する方法 36](#)
 - [Syslog 統合を作成または更新する方法 39](#)
 - [ログインのための Syslog 統合を削除する方法 40](#)
- 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 41**
 - [プログラムに参加または離脱する方法 41](#)
 - [プログラムのデータ収集時間を設定する方法 42](#)

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。vRealize Automation 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。

LCM と Workspace ONE Access の使用方法の詳細については、[VMware Identity Manager を使用したユーザー管理](#)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](#)

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

vRealize Automation Cloud Assembly サービス ロールによって、vRealize Automation 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. vRealize Automation 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が必要です。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。 vRealize Automation 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。これらの 2 つのロールの権限は、以下で定義されています。
Cloud Assembly 閲覧者	情報は表示できるが、作成、更新、削除はできないユーザー。読み取り専用のロールです。

サービス ロールに加えて、vRealize Automation Cloud Assembly にはプロジェクト ロールがあります。

プロジェクト ロールは vRealize Automation 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、ブループリン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。
- 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、ブループリン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。

表 2-2. vRealize Automation 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
[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、ユーザー、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		はい。自分のプロジェクト			
	プロジェクトでユーザーを追加し、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	
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				
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					

表 2-2. vRealize Automation 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
	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				
	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 - マシン	マシンの追加と削除	はい				
	マシンの表示	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 - ボリューム	検出されたストレージ ボリュームの削除	はい				
	検出されたストレージ 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。
リソース - Kubernetes	Kubernetes クラスターの展開または追加、および名前空間の作成または追加	はい				
	Kubernetes クラスターと名前空間の表示	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				

表 2-2. vRealize Automation 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 関 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
	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 プランの作成、更新、ま たは削除	はい				
	オンボード プランの表示	はい	はい			はい。自 分のプロ ジェクト
[マーケットプレイス]						
	[マーケットプレイス] タブを表示して開 く	はい	はい			
	ダウンロードしたブループリントを [デザ イン] タブで使用する	はい		はい。プ ロジェク トに関連 付けられ ている場 合。	はい。プ ロジェク トに関連 付けられ ている場 合。	
マーケットプレイス - ブループリント	ブループリントのダウンロード	はい				
	ブループリントの表示	はい	はい			
マーケットプレイス - イメージ	イメージのダウンロード	はい				
	イメージの表示	はい	はい			
マーケットプレイス - ダウンロード	ダウンロードしたすべてのアイテムのロ グの表示	はい	はい			
[拡張性]						
	[拡張性] タブを表示して開く	はい	はい			はい

表 2-2. vRealize Automation 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 関 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
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] タブを開き、ブループリントの リストを表示	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
ブループリント	ブループリントの作成、更新、および削除	はい		はい。自 分のプロ ジェクト	はい。自 分のプロ ジェクト	
	ブループリントの表示	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
	ブループリントのダウンロード	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
	ブループリントのアップロード	はい		はい。自 分のプロ ジェクト	はい。自 分のプロ ジェクト	

表 2-2. vRealize Automation 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
	ブループリントの展開	はい		はい。自分のプロジェクト	はい。自分のプロジェクト	
	ブループリントのバージョンとリストア	はい		はい。自分のプロジェクト	はい。自分のプロジェクト	
	カタログへのブループリントのリリース	はい		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
[展開]						
	[展開] タブを表示して開く	はい	はい	はい	はい	はい
	展開の詳細、展開履歴、トラブルシューティング情報などを含め、展開を表示する。	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	

Service Broker サービス ロール

vRealize Automation Service Broker サービス ロールによって、vRealize Automation 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	vRealize Automation Service Broker 管理者ロールを持たないすべてのユーザー。 vRealize Automation 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。これらの 2 つのロールの権限は、以下で定義されています。
Service Broker 閲覧者	読み取り専用の権限を持つユーザーで、情報を表示することはできますが、値の作成、更新、削除はできません。

サービス ロールに加えて、vRealize Automation Service Broker にはプロジェクト ロールがあります。

プロジェクト ロールは vRealize Automation 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、ブループリン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。
- 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。

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
[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				

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
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、ユーザー、プロビジョニング、Kubernetes、および統合の値の更新または削除	はい				
	プロジェクトの表示	はい	はい			
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				
	コンテンツの表示	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
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
	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	
[展開]						
	[展開] タブを表示して開く	はい	はい	はい。	はい	はい
	展開の詳細、展開履歴、トラブルシ ュエーティング情報などを含め、展開 を表示する。	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
	承認申請への応答	はい		Service Broker ユー ザー ロールの み	Service Broker ユーザ ー ロールのみ	Service Broker ユー ザー ロー ルのみ

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](#)
- [vRealize Automation の DNS 割り当ての更新](#)
- [vRealize Automation の時刻同期を有効にする方法](#)
- [時刻同期を無効にする方法](#)
- [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。

注： 可能であれば、`vraccli 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。

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

- 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。

- 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。
- 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
```

- 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
```

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 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
```

- 3 vCenter Server にログインし、Shut Down Guest OS コマンドを使用して、すべての vRealize Automation ノードをシャットダウンします。
- 4 各 vRealize Automation ノードの OVF DNS プロパティを更新します。
 - a vCenter Server のインベントリから vRealize Automation ノードに移動します。
 - b [構成] タブを選択し、[設定] を展開します。
 - c [vApp オプション] を選択します。
 - d OVF プロパティのリストで、vami.DNS.vRealize_Automation を探して選択します。
 - e [値の設定] をクリックし、[プロパティ値] テキスト ボックスに新しい DNS エントリを入力します。
 - f [OK] をクリックします。
- 5 すべての vRealize Automation ノードを起動し、完全に起動するまで待機します。完全に起動すると、コンソールが青い画面になります。
- 6 再度 vRealize Automation ノードを再起動し、完全に起動するまで待機します。
- 7 SSH を使用して各 vRealize Automation ノードにログインし、/etc/resolve.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。
- 8 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 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 アプライアンスをホストしている 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。</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> <p>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>
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 `vracli ntp apply` コマンドを実行します。

ESXi の NTP 構成が vRealize Automation 環境に適用されます。

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。

- b `vracli ntp apply` コマンドを実行します。

systemd の NTP 構成が vRealize Automation 環境に適用されます。

4 (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。

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、NTP サーバと同期されている vRealize Automation アプライアンスを再起動します。

時刻同期を無効にする方法

vRealize Automation 環境で NTP (Network Time Protocol) 時刻同期を無効にするには、vRealize Automation アプライアンスのコマンド ラインを使用します。

また、`vracli ntp reset` コマンドを実行し、`vracli ntp apply` コマンドを実行して新しい構成を適用することにより、vRealize Automation アプライアンスの NTP 構成をリセットすることもできます。

前提条件

ESXi または systemd との時刻同期が構成されていることを確認します。[vRealize Automation の時刻同期を有効にする方法](#)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 ESXi または systemd との時刻同期を無効にするには、`vracli ntp disable` コマンドを実行します。
- 3 `vracli ntp apply` コマンドを実行します。
- 4 (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。

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。

```

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 [/]#` プロンプトで `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 [/]#` プロンプトで、`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。

LCM と Workspace ONE Access の使用方法の詳細については、[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。

マルチテナント用に vRealize Automation を構成する場合は、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を構成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。

マルチテナントが最初に構成される際、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。

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 3.3.2 をインストールして構成します。
- vRealize Suite Lifecycle Manager バージョン 8.1 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 3.3.2 と vRA 8.1 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 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 8.1 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 :

- vra1.example.local
- vra2.example.local
- vra3.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

次の表に、クラスタ化された Workspace ONE Access とクラスタ化された vRealize Automation のマルチ組織展開のための DNS および証明書の要件を示します。

DNS 要件	SAN 証明書の要件
Main A Type Records lcm.example.local WorkspaceOne-1.example.local WorkspaceOne-2.example.local WorkspaceOne-3.example.local vra.example-1.local vra.example-2.local vra.example-3.local	Workspace One Certificate ホスト名 : WorkspaceOne.example.local, default-tenant, example.local, tenant-1.example.local, tenant-2.example.local
Multi-Tenancy A Type Records default-tenant.example.local tenant-1.vra.example.local tenant-2.vra.example.local	Workspace One LB Certificate (LB Terminated) ホスト名 : WorkSpaceOne-lb.example.local, default-tenant.example.local, vra.example.local, tenant-1.example.local, tenant-2.example.local
Multi-Tenancy CNAME Type Records tenant-1.vra-lb.example.local - vra-lb.example.local tenant-2.vra-lb.example.local - vra.lb.exmple.local	vRealize Automation Certificate ホスト名 : vra-1.example.local, vra-2.example.local, vra-3.example.local, vra-lb.example.local, tenant-1.example.local, tenant-2.example.local 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。

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場合の詳細については、<https://docs.vmware.com/jp/VMware-Workspace-ONE-Access/3.3/idm-administrator.pdf> 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 [統合] ページで事前構成済みで利用できます。サブテナントには、事前登録済みの vRealize Orchestrator 統合はありません。サブテナントには、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。

- 組み込みの vRealize Orchestrator との統合を追加するには、vRealize Orchestrator の認証プロバイダの構成に移動し、該当する vRealize Automation テナントのホスト アドレスを使用して接続します。次に [インフラストラクチャ] - [接続] - [統合] の順に選択し、組み込みの vRO を統合として追加できます。
- マルチ組織 vRealize Automation を認証プロバイダとして使用する外部 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 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](#)

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 Automation ログとログ バンドルを作成して使用できます。

または、ログを vRealize Log Insight に自動的に転送することもできます。ログを vRealize Log Insight に転送する方法については、[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。

`vraccli` コマンドライン ユーティリティの使用法については、`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 log-bundle --help`

ログ バンドル コマンド

単純なログ バンドル、またはすべてのサービスの集約された（コールド ストレージ）ログを作成できます。どちらのログ バンドルにもサービスのすべてのログが含まれますが、コールド ストレージ バンドルにはサービス ログの過去バージョンの集約ストリームのコピーが含まれ、トラブルシューティングに利用できます。コールド ストレージ エージェントは、サービスのログを継続的に集約してローカルのファイル システムに保存します。通常、トラブルシューティングに必要なものは単純なログ バンドルだけです。

各ノードからログを収集するときのデフォルトのタイムアウト値を変更することもできます。

クラスタ化された環境では、1つのノードで `vraccli log-bundle` コマンドを実行するだけで十分です。

- ログ バンドル コマンドのヘルプの表示

```
vraccli log-bundle --help
```

- 単純なログ バンドルの作成

```
vracli log-bundle
```

- コールド ストレージ ログ バンドルの作成

```
vracli log-bundle --include-cold-storage
```

- 各ノードからログを収集するときのタイムアウト値の変更。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、CPU 使用率が高いなどの場合は、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必要がある可能性があります。

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

ログ バンドルの構造

vRealize Automation サービスは Kubernetes ポッド内にコンテナ化されています。生成されたログ バンドルは、log-bundle-`{TIMESTAMP}`.tar.xz 名前形式を使用する tar.xz アーカイブです。TIMESTAMP は、秒単位のエPOCH タイムスタンプです。通常のログ 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。何らかの理由でログ バンドルを生成できない場合は、代わりにフォールバック バンドルが作成されます。フォールバック バンドルには、現在のノードのログのみが含まれています。2 つのログ バンドル タイプの構造には若干の違いがあります。

- 通常のログ バンドル

通常のログ バンドルは、次のカテゴリに分類されます。

- ホスト ログと設定

各ホストとそのホスト固有のログの設定は、クラスタ ノード（ホスト）ごとに 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。ディレクトリの内容はホストのファイル システムと一致します。ディレクトリ数はクラスタ ノードの数と一致します。

コールド ストレージ ログは、構造化された JSON ログに `/hostname/services-logs/all/aggregated.log` として格納されます。

- ポッド ログ

サービスは Kubernetes ポッド内にコンテナ化されています。サービス ログは pods ディレクトリに置かれます。このディレクトリには、名前空間ごとに 1 つ、名前空間名と同じファイル名を持つディレクトリがあります。通常、クラスタ ノードごとに各ポッドの 1 つのインスタンスが存在します。ポッド ディレクトリには、各コンテナ アプリケーションのログ ファイルがあります。

たとえば、vRealize Orchestrator コントロール センターのログは、各 `/pods/prelude/vco-app-hash/` ディレクトリの `vco-controlcenter-app.log` ファイルに格納されます。

- 環境ファイル

環境ファイルには、現在のリソース使用量の情報がノード別およびポッド別に含まれています。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。

- フォールバック ログ バンドル

vracli コマンドの終了を待機しているときにエラー メッセージが通知されると、フォールバック バンドルが生成されます。このエラーが通知された場合は、クラスタ内の各ホストまたはノードで vracli log-bundle コマンドを実行して、できるだけ多くの情報を収集する必要があります。

■ フォールバック コンテナ ログ

フォールバック ログは、/fallback-containers ディレクトリにあります。ログ ファイル名を調べることで、ポッドがどのコンテナでログを生成したかを識別できます。

```
pod-name-some-hash-container-name-other-hash.log
```

■ フォールバック コールド ストレージ

バンドルを使用してコールド ストレージ ログを収集している場合は、現在のホストのフォールバック ログが /fallback-cold-storage ディレクトリにあります。

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 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。提供されている 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 の詳細、および vRealize Log Insight API のドキュメントについては、[vRealize Log Insight のドキュメント](#)、および[/api/v1/events/ingest/{agentId}](#)ページを参照してください。

提供されている vracli コマンドライン ユーティリティを使用して、vRealize Automation ログを自動的にかつ継続的に 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。

vracli コマンドライン ユーティリティの使用方法については、vracli コマンドラインの `--help` 引数を使用して確認できます。例: `vracli vrli --help`

vRealize Log Insight の既存の構成の確認

Command

```
vracli 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": 443,
  "scheme": "https",
  "sslVerify": false
}
```

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 443）には、別の値を設定できます。

```
vracli vrli set some-host
vracli vrli set some-host:9543
vracli vrli set http://some-host:9543
```

vRealize Log Insight の取り込み API では、ポート 9543 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」トピックと「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。

vRealize Log Insight の統合の設定または更新

Command

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

Arguments

次のコマンドライン引数を使用できます。

- FQDN_OR_URL - vRealize Log Insight API 設定を使用してログを送信するときに使用する vRealize Log Insight サーバの FQDN または IP アドレス。デフォルトでは、ポート 443 と HTTPS スキームが使用されます。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。

■ 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。デフォルト値は 0 です。vRealize Log Insight API 設定を使用して vRealize Log Insight に送信されたログのログ エージェントを識別するために使用します。
- `--environment ENV` - 現在の環境の識別子を設定します。vRealize Log Insight ログで、ログ行の各イベントのタグとして使用できるようになります。デフォルト値は `prod` です。
- `--ca-file /path/to/server-ca.crt` -vRealize Log Insight サーバ証明書の署名に使用された認証局 (CA) 証明書を含むファイルを指定します。指定された CA が vRealize Log Insight サーバの証明書を検証できるように、ログ エージェントが CA を信頼するように設定します。証明書を検証するために必要な場合は、ファイルに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` - `--ca` ファイルと同じようにファイルを指定しますが、証明書（チェーン）を文字列としてインラインで渡します。
- `--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。

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

```
$ 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 --environment staging my-vrli.local
```

vRealize Log Insight の統合のクリア

Command

```
vracli vrli unset
```

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

終了コードは次のとおりです。

- 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

```
$ vracli vrli unset
Clearing vRLI integration configuration

$ vracli 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。

`vracli 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 `vracli remote-syslog set` コマンドに追加します。

- TLS を使用した TCP 経由。

vRealize Log Insight とのログ統合の構成の詳細については、[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

1 台以上のリモート 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、`vracli remote-syslog set` コマンドを実行します。

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

注： `vracli 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、`vracli 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 `vracli 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、`vracli 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

`vracli 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、`vracli 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。

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 製品およびサービスの向上、問題の解決、各製品のデプロイおよび使用に関する最適な方法をお客様に提案するために役立てられます。

CEIP を通じて収集されるデータに関する詳細と、VMware によるそのデータの使用目的については、<http://www.vmware.com/trustvmware/ceip.html> の Trust & Assurance Center に記載されています。

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 `vracli 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、`vracli 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 `vracli 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。