

EMC® vRealize Data Protection Extension®

Version 3.1.x

Installation and Administration Guide

302-003-027

REV 02

Copyright © 2014-2017 Dell Inc. and its subsidiaries. All rights reserved.

Published March 2017

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners.
Published in the USA.

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.EMC.com

CONTENTS

Figures		7
Tables		9
Preface		11
Chapter 1	Introduction	15
	vRealize Data Protection Extension.....	16
	Key concepts and components.....	16
	Users.....	16
	Blueprints.....	16
	Catalog services.....	17
	Advanced services.....	17
	Property groups.....	17
	Data protection policies.....	17
	Data protection policy definitions and descriptions.....	17
	vRealize Automation and vRealize Orchestrator integration.....	18
	vRealize Automation endpoints.....	18
	vRealize Automation tasks.....	19
	vCloud Automation vs. vRealize Automation.....	20
	Avamar limitations.....	20
Chapter 2	Installation and Upgrade	21
	Compatibility.....	22
	Required components.....	22
	Supported product versions.....	22
	Pre-installation.....	22
	Verify the configuration of the vRealize Automation installation....	22
	Install the VMware vCenter Orchestrator Plug-in for vCloud Automation Center.....	23
	Configuring XaaS to recognize vRealize Orchestrator.....	23
	Check for the default tenant.....	24
	Add a vRealize Automation host.....	25
	Adding an IaaS host.....	28
	Verify vCenter endpoints.....	32
	Install the EMC Data Protection Restore Client for Avamar systems	32
	Installing the EMC vRealize Data Protection Extension.....	33
	Installing the vmoapp using vRealize Orchestrator.....	34
	Installing the vmoapp from the command line.....	34
	Installing data protection admin services into a specific tenant.....	35
	Licensing.....	42
	Linux-based vRealize Orchestrator server.....	42
	Verifying the licensing validation check.....	43
	Upgrading the EMC vRealize Data Protection Extension.....	44
	Install the EMC vRealize Data Protection Extension vmoapp.....	44

	Update the default setup in each vRealize Automation tenant.....	44
	Update custom workflows and actions.....	47
	Verifying the new version.....	47
	Run cleanup script after upgrading.....	47
	Uninstalling the EMC vRealize Data Protection Extension.....	48
	Uninstall EMC data protection from a single tenant.....	48
	Uninstall the plug-in from vRealize Orchestrator.....	49
Chapter 3	Administration	51
	Data protection configuration for the tenant.....	52
	Clustered vRealize Orchestrator environment.....	52
	Avamar domains for tenant data protection policies.....	53
	Adding a second vCenter endpoint.....	53
	Managing multiple vCenters with Avamar.....	54
	Tenant and EMC vRealize Data Protection Extension configurations	54
	Data protection administration.....	55
	Service blueprints.....	55
	Configuring an Avamar data protection system.....	56
	Configuring application-consistent data protection.....	58
	Restoring a virtual machine to a new location using advanced options.....	60
	Restoring a deleted virtual machine.....	62
Chapter 4	Business Group User Operations	65
	Provisioning a protected virtual machine.....	66
	Data protection actions.....	67
	Adding data protection to a virtual machine.....	67
	Running data protection on a virtual machine.....	67
	Viewing the protection status of a virtual machine.....	68
	Removing data protection from a virtual machine.....	68
	Restore actions.....	69
	Restoring a virtual machine to its original location.....	69
	Restoring a virtual machine to a new location.....	69
	File-level restore.....	70
	Expiring or destroying a virtual machine.....	72
Chapter 5	Logging and Supportability	73
	Monitoring status.....	74
	Event and error message codes.....	75
	Avamar Client activity window.....	76
	Single-click log capturing and packaging.....	76
	vRealize Automation log bundling.....	76
	vRealize Orchestrator log bundling.....	77
	Log locations.....	77
Chapter 6	Troubleshooting	79
	General Troubleshooting.....	80
	Items to investigate when data protection is not added.....	80
	Troubleshooting the EMC vRealize Data Protection Extension.....	80
	Avamar policies do not display when running Setup a Data Protection Property Group or Add Data Protection workflows.....	80
	Null error when provisioning from blueprint with deleted policy.....	81

No available policy found from virtual machine properties when there is no EDP system.....	81
vRealize Automation event subscriptions.....	82
Virtual machine is not added to application policy if agent in virtual machine is not activated.....	82
Exchange plug-in re-added in Avamar when client deleted using Avamar Administrator	82
Checking the EMC vRealize Data Protection Extension configuration.....	83
Configuration checks performed by the EMC data protection configuration workflow.....	83
Error and warning messages.....	84

CONTENTS

FIGURES

1	Inventory tab in vRealize Orchestrator.....	24
2	Existing tenants in vRealize Orchestrator.....	24
3	Workflows tab in vRealize Orchestrator.....	25
4	Start Workflow in vRealize Orchestrator.....	26
5	Start Workflow: Add a vRA host.....	27
6	Host Authentication in Start Workflow wizard.....	28
7	Start workflow in vRealize Orchestrator.....	29
8	Add an IaaS host in Start workflow wizard.....	29
9	Host Authentication in Start workflow wizard.....	30
10	Host Authentication in Start workflow wizard.....	31
11	Valid provisioning groups under vRealize Automation Infrastructure	32
12	Start Workflow in vRealize Orchestrator.....	36
13	Start Workflow wizard.....	36
14	Select vCACCAFE Host dialog.....	37
15	Catalog Service in Start Workflow wizard.....	38
16	Administrator Entitlement in Start Workflow wizard.....	39
17	user Entitlement in Start Workflow wizard.....	40
18	Data Protection in Start Workflow wizard.....	41
19	Workflow interaction form.....	45
20	Start Workflow : Update default setup for tenant.....	46
21	Select policy for the blueprint.....	66
22	Select policy to run data protection.....	68
23	Successful request in vRA.....	74
24	Failed request in vRA.....	74
25	Avamar Client activity window.....	76

FIGURES

TABLES

1	Revision history.....	11
2	Style conventions.....	12
3	vRealize Automation tasks.....	19
4	Supported product versions.....	22
5	Service catalog blueprints.....	55
6	Avamar plug-ins supported for application-consistent data protection.....	58
7	Event and error codes.....	75
8	Default log locations.....	77
9	Error and warning messages.....	84

TABLES

PREFACE

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

If a product does not function correctly or does not function as described in this document contact an EMC technical support professional.

Note

This document was accurate at publication time. Go to EMC Online Support (<https://support.EMC.com>) to find the latest version of this document.

Purpose

This document describes how to install, configure, and use the EMC vRealize Data Protection Extension.

Audience

This document is intended for system administrators who will be installing, configuring, and using the EMC vRealize Data Protection Extension. A high degree of knowledge regarding EMC Avamar and VMware vRealize Automation administration is required.

Revision history

The following table presents the revision history of this document.

Table 1 Revision history

Revision	Date	Description
02	March 31, 2017	Added note to "Installing data protection admin services into a specific tenant" to indicate that fields in the Data Protection screen are optional, but if not entered during the install, you must run the Add a tenant data protection system Catalog Item from vRA after the install.
01	October 14, 2016	First release of this document for version 3.1 of the EMC vRealize Data Protection Extension

Related documentation

The following EMC publications available at <https://support.emc.com> provide additional information:

- *EMC vRealize Data Protection Extension Release Notes*
- *EMC Avamar Administration Guide*

The following VMware publications available at <https://www.vmware.com/support/pubs/> provide additional information:

- vRealize Automation documentation:

- *Foundations and Concepts*
- *Installation and Configuration*
- *System Administration*
- *IaaS Configuration*
- *Tenant Administration*
- vRealize Orchestrator documentation:
 - *Using the vRealize Orchestrator plugin for vRealize Automation*

Typographical conventions

EMC uses the following type style conventions in this document:

Table 2 Style conventions

Bold	Used for names of interface elements, such as names of buttons, fields, tab names, and menu paths (what the user specifically selects or clicks)
<i>Italic</i>	Used for full titles of publications that are referenced in text
Monospace	Used for: <ul style="list-style-type: none"> • System code • System output, such as an error message or script • Pathnames, file names, prompts, and syntax • Commands and options
<i>Monospace italic</i>	Used for variables
Monospace bold	Used for user input
[]	Square brackets enclose optional values
	Vertical bar indicates alternate selections - the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate non-essential information that is omitted from the example

Where to get help

EMC support, product, and licensing information can be obtained as follows:

Product information

For documentation, release notes, software updates, or information about EMC products, go to EMC Online Support at <https://support.emc.com>.

Technical support

Go to EMC Online Support and click Service Center. Several options for contacting EMC Technical Support appear on the site. Note that to open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Online communities

Go to EMC Community Network at <https://community.emc.com> for peer contacts, conversations, and content on product support and solutions. Interactively engage online with customers, partners, and certified professionals for all EMC products.

Your comments

Your suggestions help to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to DPAD.Doc.Feedback@emc.com.

CHAPTER 1

Introduction

This chapter includes the following topics:

- [vRealize Data Protection Extension](#)..... 16
- [Key concepts and components](#)..... 16
- [Data protection policy definitions and descriptions](#)..... 17
- [vRealize Automation and vRealize Orchestrator integration](#)..... 18
- [vRealize Automation endpoints](#)..... 18
- [vRealize Automation tasks](#)..... 19
- [vCloud Automation vs. vRealize Automation](#)..... 20
- [Avamar limitations](#).....20

vRealize Data Protection Extension

VMware vRealize Automation™ allows authorized administrators, developers, and business users to request new IT services and manage specific cloud and IT resources based on their roles and privileges. The vRealize Data Protection Extension adds data protection to the services available during self-provisioning.

Data protection can be performed to an Avamar system, and consists of two types:

- Image level data protection, which protects virtual machines at the disk level.
- Application Consistent data protection, which uses Avamar's Application Data Protection feature to protect VMs at an application level such that application-specific data is not lost.

With the vRealize Data Protection Extension, the management of data protection is integrated into the standard vRealize Automation workflow. Service Level Agreements (SLAs) seamlessly enable data protection in the cloud. The applications are protected automatically when you enable EMC data protection.

Key concepts and components

The following sections define the key components of the EMC vRealize Data Protection Extension.

Users

The EMC vRealize Data Protection Extension has two primary intended users. The first user is the data protection administrator. This user most likely has the tenant administrator role in vRealize Automation and should be added to the Administrator Entitlement that is created when running the **Install default setup for tenant** workflow. This user is responsible for the administration of the EMC vRealize Data Protection Extension. The responsibilities of the user include tenant administration, setting up blueprints with data protection, adding or removing data protection systems, deleting build profiles, and performing any advanced restore requests. For further information regarding these administrative responsibilities, see [Administration](#) on page 51.

The second user is the end user. This user most likely has the Business Group User role in vRealize Automation and should be added to the User Entitlement that is created when running the **Install default setup for tenant** workflow. This end user will provision virtual machines with data protection by using the blueprints that the data protection administrator creates. End users can also perform additional data protection actions on their provisioned virtual machines.

Blueprints

vRealize Automation enforces business rules around the self-provisioning of virtual machines using blueprints. A blueprint is the complete specification used to determine one or more virtual machine's attributes, the manner in which they are provisioned, and their policy and management settings.

Individual machines or all the machines in the blueprint can be protected using the EMC vRealize Data Protection Extension.

Catalog services

Self-provisioners select services from a catalog of services to which they are entitled.

Catalog services are backed by one of two types of blueprints:

- Blueprints define the rules about provisioning a virtual machine.
- Service blueprints define rules about self-provisioning custom services created with the Advanced Services mechanism, which is backed by the vRealize Orchestrator component.

Advanced services

Advanced Services, also known as XaaS (Anything as a Service), is vRealize Automation's extensible service construct.

The EMC vRealize Data Protection Extension delivers its data protection services as Advanced Services.

- If a service level agreement is assigned to the blueprint, the virtual machine will be added to a data protection policy at provisioning time.
- Blueprints can be configured with or without data protection policies assigned to them.

Property groups

A property group is a set of properties to be applied to a machine when it is provisioned.

These properties may determine the specification of the machine, the manner in which it is provisioned, operations to be performed after it is provisioned, or management information about the machine maintained within vRealize Automation. The EMC vRealize Data Protection Extension uses these property groups to add the data protection policy to blueprints.

Data protection policies

Data protection policies allow data protection administrators to control backup schedules and retention periods.

Policies map to the underlying data protection provider from which the policy originated, and adhere to the service level agreement (SLA) that the data protection provider supports. For example, an Avamar data protection system uses Groups.

Data protection policy definitions and descriptions

Backup policies are created and stored within the data protection system. The EMC vRealize Data Protection Extension does not hold copies of policy definitions but keeps references to the original policy. This allows the backup administrator to modify the policy definition as needed without affecting the vRealize Data Protection Extension's loosely coupled reference.

Note

The policy name references the policy objects. EMC recommends that you do not change the policy name after creating it. If you do change the policy name in the data protection system, then associated property groups that reference the policy must either be updated manually or the **Setup data protection property group** service must be requested again to update the property group with the new policy.

Since policies are referenced by name, EMC recommends using a unique name for each policy across all the data protection providers. For example, if two Avamar systems contain a policy group that is named Gold, two Gold policies appear in some of the workflows in vRA, making it difficult to determine which Gold policy applies to which specific Avamar system.

Note

The EMC vRealize Data Protection Extension uses the term "policy" or "policy group" to refer to Avamar groups.

For blueprints with multiple components, you can either apply a configured Property Group to the root blueprint properties, which each component will then inherit, or apply to individual components as desired.

vRealize Automation and vRealize Orchestrator integration

vRealize Orchestrator is the workflow engine integrated with vRealize Automation. The vRealize Orchestrator server that is distributed with vRealize Automation is pre-configured, and therefore, when the Virtualization Administrator deploys the vRealize Automation Appliance, the vRealize Orchestrator server is up and running.

The vRealize Orchestrator product already offers hundreds of reusable workflows that vRealize Automation workflows can leverage. vRealize Automation workflows can run vRealize Orchestrator workflows, immediately extending the vSphere-oriented use cases for vRealize Automation. With the EMC vRealize Data Protection Extension installed, data protection features are accessible from the vRealize Automation and the vRealize Orchestrator user interfaces.

The vRealize Data Protection Extension includes both vRealize Automation services and public vRealize Orchestrator workflows and actions. General vRealize Orchestrator conventions for versioning and logging of workflows are followed.

Note

vRealize Orchestrator workflows and vRealize Automation services are not used during scheduled protection operations.

vRealize Automation endpoints

In vRealize Automation, an endpoint represents an external resource that is assigned to vRealize Automation to manage and allocate on behalf of tenants. In essence, this endpoint is the infrastructure fabric that vRealize Automation manages and makes available via reservations to one or more tenants.

Typically, IaaS administrators are responsible for creating endpoints while setting up the vRealize Automation infrastructure.

The EMC vRealize Data Protection Extension supports vCenter Server endpoints. For information on configuring the vCenter Server as the endpoint, refer to vRealize Automation documentation, which is available on the VMware website.

vRealize Automation tasks

The tasks in the following table encompass a typical end-to-end workflow using all required systems: vRealize Automation, vRealize Orchestrator, and the Data Protection System. The components must be configured and running with the EMC vRealize Data Protection Extension.

Table 3 vRealize Automation tasks

Task	Typical User	For more information
Install the EMC vRealize Data Protection Extension	System administrator	Installing the EMC Plug-in for vRealize Automation
Install the data protection service blueprints and resource actions into a tenant	Tenant administrator or XaaS architect	Installing data protection admin services into a specific tenant or the following link
Configure and entitle access to data protection functionality	Tenant administrator	Installing data protection admin services into a specific tenant
Create a virtual vSphere blueprint	Tenant administrator	Refer to vRealize Automation documentation for instructions on creating blueprints
To enforce data protection rules during provisioning, add data protection to a blueprint	Tenant administrator	Setting up data protection on a blueprint
Use advanced options to restore a virtual machine to a new location	Tenant administrator	Advanced restore to new for administrators
Restore a deleted virtual machine	Tenant administrator	Restoring a deleted virtual machine
Provision virtual machines from a protected blueprint	Business group user	Provisioning a protected virtual machine
Use actions to manage protection on provisioned virtual machines: <ul style="list-style-type: none"> • Add data protection to a virtual machine • Run data protection on a virtual machine • View protection status and backup inventory • Remove data protection from a virtual machine • Restore a virtual machine to its original location 	Business group user	Data protection actions Restore actions

Table 3 vRealize Automation tasks (continued)

Task	Typical User	For more information
<ul style="list-style-type: none"> Restore a virtual machine to a new location File-level restore (restore individual files or a directory of files to the same or different location on the virtual machine) 		
View error logs	Any user	Event and error message codes

vCloud Automation vs. vRealize Automation

vRealize Automation is the new brand name to replace VMware vCloud Automation Center (vCAC). Throughout this document, the product is referred to as vRealize Automation. However, sometimes, the vCAC name still exists within the product. The same is true for vRealize Orchestrator, previously referred to as vCenter Orchestrator.

Avamar limitations

The following limitation exists in the Avamar Data Protection system:

- Domain names within Avamar Data Protection systems can be a maximum of 63 characters in length. The vRealize Automation hostname forms the tenant domain name in Avamar Data Protection systems. If the hostname is very long, the tenant URL name might need to be shorter so that it does not exceed the limit.
For example: `MyTenant_MyDomainIsLong.VeryLong.com`
In this example, `_MyDomainIsLong.VeryLong.com` contains 28 characters, which means that the tenant URL name (`MyTenant`) cannot be longer than 35 characters.
- Avamar does not allow the use of tildes (~) in tenant names.

CHAPTER 2

Installation and Upgrade

This chapter includes the following topics:

- [Compatibility](#)..... 22
- [Pre-installation](#)..... 22
- [Installing the EMC vRealize Data Protection Extension](#)..... 33
- [Installing data protection admin services into a specific tenant](#)..... 35
- [Licensing](#)..... 42
- [Upgrading the EMC vRealize Data Protection Extension](#)..... 44
- [Uninstalling the EMC vRealize Data Protection Extension](#)..... 48

Compatibility

This section describes the components that are required for using the EMC vRealize Data Protection Extension, and the versions of the products that the vRealize Data Protection Extension supports.

Required components

Operation of the EMC vRealize Data Protection Extension requires the following products:

- VMware vRealize Automation, including the latest IaaS server
- VMware vRealize Orchestrator
- VMware vSphere
- VMware ESXi Host
- Avamar Server with Avamar Image Proxy client(s)

Supported product versions

The following table lists the versions of vRealize Automation and Avamar that the vRealize Data Protection Extension supports.

Table 4 Supported product versions

vRealize Automation	Avamar
7.1	7.2.x, 7.3
7.0.1	7.2.x, 7.3

Note

The vRealize Data Protection Extension is not supported on the vCenter Orchestrator component that is installed with vSphere 5.5.x.

Pre-installation

Before you install the EMC vRealize Data Protection Extension, perform the following tasks.

Verify the configuration of the vRealize Automation installation

Before installing the EMC vRealize Data Protection Extension, verify the following in the base vRealize Automation installation configuration:

- The vRealize Automation Appliance has been deployed and configured
- IaaS components have been installed
- Tenants have been configured
- Agents, endpoints, and groups have been configured
- Blueprints have been created and published

- XaaS services have been set up
- A vRealize Automation (vCAC CAFE endpoint) exists for the default tenant (`vsphere.local`).
- A vRealize Automation Infrastructure Administration endpoint exists for the IaaS component. There is only one endpoint.

Install the VMware vCenter Orchestrator Plug-in for vCloud Automation Center

The VMware vCenter Orchestrator Plug-in for vCloud Automation Center allows interaction between vRealize Orchestrator and vRealize Automation. The plug-in is a `.vmoapp` file name extension, which is a VMware vCenter Orchestrator application file that you must install in the vRealize Orchestrator Client.

Note

This step is not required when using the vRealize Automation Appliance with the internal vRealize Orchestrator server.

The VMware vCenter Orchestrator Plug-in for vRealize Automation contains the following two plug-ins:

- vCloud Automation Center plug-in for vCenter Orchestrator
- vCloud Automation Center Infrastructure Administration plug-in for vCenter Orchestrator

Refer to the *VMware vCenter Orchestrator Plug-in for vCloud Automation Center Release Notes*, and download the vCloud Automation Center Plug-in that is specific to the version of vRealize Automation.

Configuring XaaS to recognize vRealize Orchestrator

vRealize Automation's XaaS (Advanced Services) depend on an underlying vRealize Orchestrator. If you are using an external vRealize Orchestrator, configure that instance as an endpoint.

Note

If you are using the vRealize Orchestrator instance that is bundled with the vRealize Automation Appliance, and you have turned on the vRealize Orchestrator service during the general vRealize Automation installation, verify that vRealize Automation automatically points at the internal vRealize Orchestrator instance.

The following procedure configures the external vRealize Orchestrator instance that backs the XaaS/ASD mechanisms.

Procedure

1. Open a browser window, and access vRealize Automation.
2. Log in using the system administrator or tenant administrator credentials.
3. For the system administrator, select **Administration > Advanced Services > Server Configuration**. For the tenant administrator, select **Administration > vRO Configuration > Server Configuration**.
4. Point the server to the vRealize Orchestrator. By default, vRealize Automation points to the internal vRealize Orchestrator.

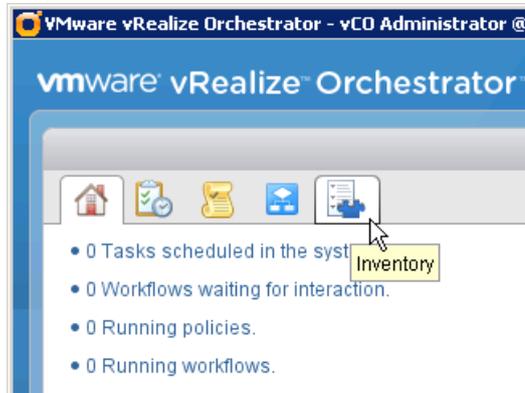
Check for the default tenant

This section describes how to determine whether you have configured a default tenant and the other required tenants for the EMC vRealize Data Protection Extension system. If not, add a vRealize Automation host for each tenant.

Procedure

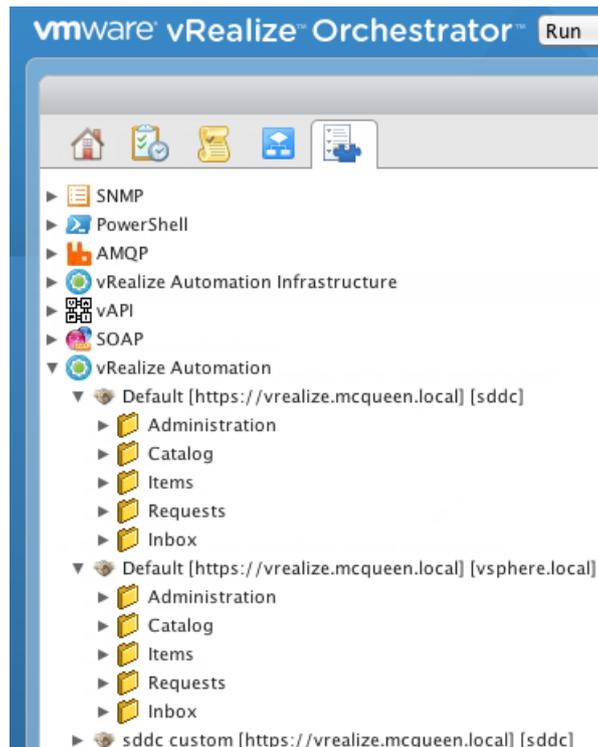
1. In vRealize Orchestrator Client, select the **Inventory** tab.

Figure 1 Inventory tab in vRealize Orchestrator



2. Expand **vRealize Automation**, as shown in the following figure. Existing tenants are listed.

Figure 2 Existing tenants in vRealize Orchestrator



If one or more of the tenants are missing, add a vRealize Automation host for each of those tenants as described in the following section.

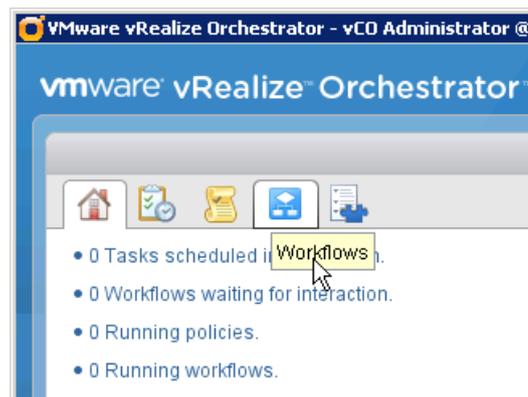
Add a vRealize Automation host

This section describes how to run the **Add a vRA host** workflow, which adds and configures a vRealize Automation host. If you have already done this task, you can skip this section.

Procedure

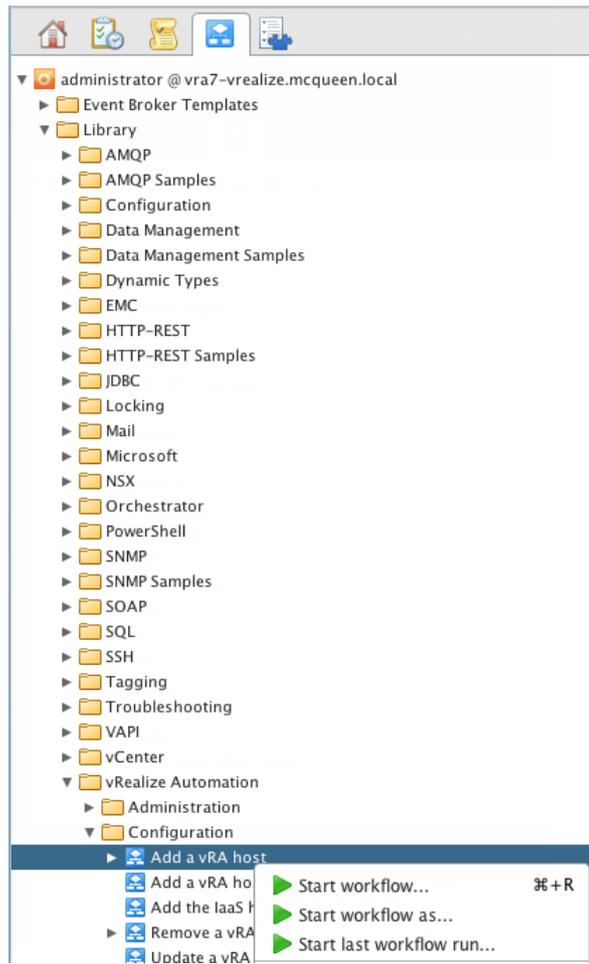
1. In the vRealize Orchestrator Client, select the **Workflows** tab.

Figure 3 Workflows tab in vRealize Orchestrator



2. Browse to `/Library/vRealize Automation/Configuration`.
3. Right-click **Add a vRA host**, and select **Start Workflow**.

Figure 4 Start Workflow in vRealize Orchestrator



The workflow wizard opens on the **Add a vRA host** screen.

Figure 5 Start Workflow: Add a vRA host

Start Workflow : Add a vRA host

1 Add a vCAC host

- 1a Host Properties
- 2 Host Authentication
 - 2a User credentials

Properties to create a new host. The name is the host's unique identifier.

* Host Name

* Host URL

Automatically install SSL certificates

Yes No

Connection timeout (seconds)

30.0

Operation timeout (seconds)

60.0

Cancel Back Next Submit

- In the **Add a vRA host** screen, supply the following information:
 - Host Name:** Type the tenant, "default tenant" or the actual tenant name.
 - Host URL:** Type the vCloud Automation Center/vRealize Automation Appliance URL.
 - Automatically install SSL certificates:** Select **Yes**.
- Click **Next**.
The **Host Authentication** screen displays.

Figure 6 Host Authentication in Start Workflow wizard

6. In the **Host Authentication** screen, type the tenant name and the tenant administrator credentials.
7. Click **Submit**.
8. Repeat this procedure for each tenant that you are configuring.

Adding an IaaS host

This section describes how to add an IaaS (Infrastructure-as-a-Service) host.

Procedure

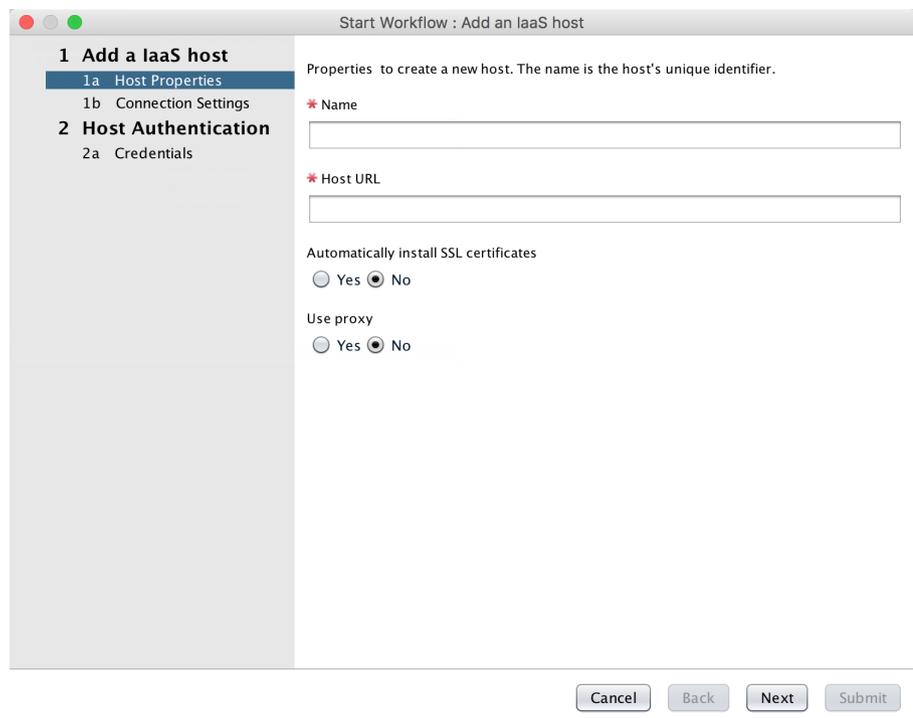
1. In the vRealize Orchestrator Client, select the **Workflows** tab.
2. Browse to `/Library/vRealize Automation/Infrastructure Administration/Configuration`.
3. Right-click **Add an IaaS host**, and select **Start workflow**.

Figure 7 Start workflow in vRealize Orchestrator



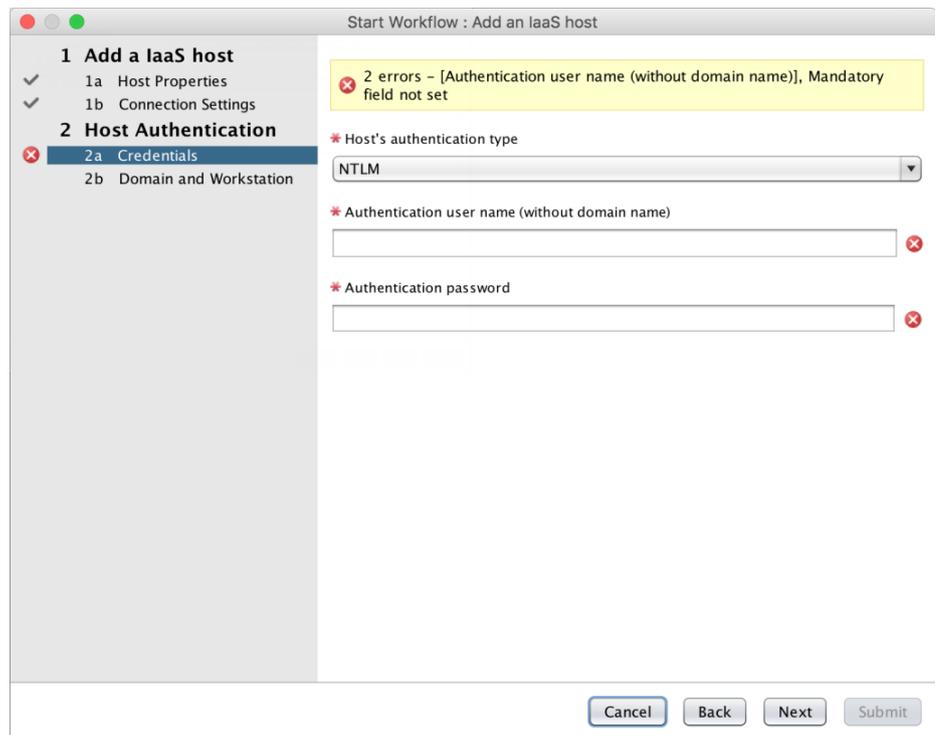
The workflow wizard opens to the **Add an IaaS host** screen.

Figure 8 Add an IaaS host in Start workflow wizard



4. In the **Add an IaaS host Host Properties** screen:
 - Type the IaaS hostname in both the **Name** and the **Host** fields.
 - Select **Yes** for **Automatically install SSL certificates**.
5. In the **Add an IaaS host Connection Settings** screen, select **Yes** for default connection settings.
6. Click **Next**.
The **Host Authentication - User credentials** screen displays.

Figure 9 Host Authentication in Start workflow wizard



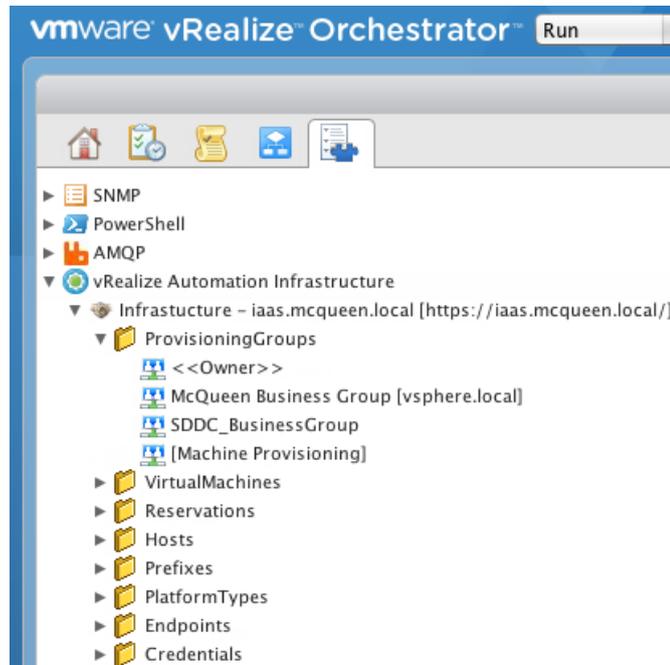
7. In the **Host Authentication - User credentials** screen, type the vRealize Automation service account name (without the domain) and password, and click **Next**.
The **Host Authentication - Domain and Workstation** screen displays.

Figure 10 Host Authentication in Start workflow wizard

The screenshot shows a window titled "Start Workflow : Add an IaaS host". On the left, a sidebar contains a tree view with the following items: "1 Add a IaaS host" (checked), "1a Host Properties" (checked), "1b Connection Settings" (checked), "2 Host Authentication" (checked), "2a Credentials" (checked), and "2b Domain and Workstation" (selected and highlighted in blue). The main content area contains two text input fields. The first is labeled "Workstation for NTLM authentication" and is empty. The second is labeled "* Domain for NTLM authentication" and is also empty. At the bottom right of the window, there are four buttons: "Cancel", "Back", "Next", and "Submit".

8. In the **Host Authentication - Domain and Workstation** screen, type the domain name in the **Domain for NTLM authentication** field, and click **Submit**.
9. To verify that the new IaaS host has been created, select the **Inventory** tab.
10. Expand **vRealize Automation Infrastructure > host > Provisioning Groups**.

If valid provisioning groups are listed as shown in the following figure, the connection was successful.

Figure 11 Valid provisioning groups under vRealize Automation Infrastructure

Verify vCenter endpoints

vRealize Orchestrator is bundled with a vCenter plug-in. If you configured an external vRealize Orchestrator in the previous section, you must re-add the vCenter endpoint. A vCenter endpoint must exist, since this endpoint enables the provisioning of virtual machines in vRealize Automation.

You can create the endpoint by running the vRealize Orchestrator **Add a vCenter Server instance** workflow (located in `/Library/vCenter/Configuration`) or from the **Administration > vRO Configuration > Endpoints** tab in vRealize Automation.

Note

In order for Avamar to create tenant domains for a new vCenter, the user must either perform a reload operation in vRealize Orchestrator, or restart the `vco-server` service after creating the vCenter endpoint.

Install the EMC Data Protection Restore Client for Avamar systems

The **EMC Data Protection Restore Client** is an application for Avamar systems that allows business group users to restore individual files, or a directory of files, from a virtual machine backup. This section describes how to install the `EDP-FLR.rpm` to use the **EMC Data Protection Restore Client**. This rpm must be installed on all Avamar servers being used for data protection by the EMC vRealize Data Protection Extension.

Before you begin

- All vCenters used by vRealize Automation must be added to the Avamar servers being used by the EMC vRealize Data Protection Extension.
- Image proxies must be deployed in each vCenter and registered with the Avamar servers.

Procedure

1. Log in via SSH as the root or admin user on the Avamar server you plan to install the `EDP-FLR.rpm`.
2. To stop Apache Tomcat, type the following command:
`emwebapp.sh --stop`
3. To install the `EDP-FLR.rpm`, type the following command:
`rpm -ivh <flr-rpm>`
4. To restart Apache Tomcat, type the following command:
`emwebapp.sh --start`

In case the EBR server is running

If the EBR server is running on the Avamar server, use the following procedure to install the `EDP-FLR.rpm`.

Procedure

1. If the `EDP-FLR.rpm` is installed, uninstall it.
2. Type the following command to install the `EDP-FLR.rpm`:
`rpm -ivh <flr-rpm>`
3. Type the following command to stop and restart Apache Tomcat:
`emwebapp.sh --stop && emwebapp.sh --start`

In case an Avamar upgrade is required

If the Avamar server must be upgraded to a different version, use the following procedure to re-install `EDP-FLR` after the upgrade has been done.

Procedure

1. If the `EDP-FLR rpm` is installed, uninstall the rpm:
`rpm -e <edp-flr>`
2. To install the `EDP-FLR rpm`, type the following command:
`rpm -ivh <flr-rpm>`
3. To stop and restart Apache Tomcat, type the following command:
`emwebapp.sh --stop && emwebapp.sh --start`

Installing the EMC vRealize Data Protection Extension

The EMC vRealize Data Protection Extension is packaged as a vRealize Orchestrator `vmoapp`. The `vmoapp` contains a vRealize Orchestrator plug-in and a package of workflows and actions.

The EMC vRealize Data Protection Extension is designed so that it can be consumed as Advanced Services and Resource Actions within vRealize Automation. Organizations that are accustomed to using workflows from the vRealize Orchestrator level can leverage the workflows in that context as well.

You can install the `vmoapp` either from the **vRealize Orchestrator Control Center**, or from the command line, as described in the following two sections.

Installing the vmoapp using vRealize Orchestrator

If you are using multiple vRealize Orchestrator nodes in a cluster, install the vmoapp on each vRealize Orchestrator node.

Note

If you are installing in a Windows environment, it is recommended that you use Microsoft Internet Explorer or Mozilla Firefox. If you are installing in a MacOS, it is recommended that you use Mozilla Firefox.

Procedure

1. Open the browser to the **vRealize Orchestrator Control Center**.
If you are using the local vRealize Orchestrator server, this system is the vRealize Automation server. If not, the system is the external vRealize Orchestrator server.
2. Click **Manage Plug-ins** on the main window.
3. Click **Browse...**, select the `.vmoapp` file that you want to install, and click **Install**.
4. Read and accept the license agreement, and then click **Install**.
The installation should complete quickly.
5. In the main window, select **Startup Options**, and restart the vRealize Orchestrator server.
6. Check the vRealize Automation configuration by running the **Check EMC data protection configuration** workflow. Instructions are provided in [Checking the EMC Plug-in for vRealize Automation configuration](#).

Installing the vmoapp from the command line

If you prefer, you can install the vmoapp from the command line rather than using vRealize Orchestrator Configuration web application.

Procedure

1. Use an http client, such as curl, to upload the `.vmoapp` file to the vRealize Orchestrator server. For example:

```
$ curl --insecure --user 'user:password' --form file=@/path/to/.vmoapp --form format=vmoapp https://vro.server:8281/vco/api/plugins
```

Note

The port on vRealize Orchestrator bundled with vRealize Automation is now port 443. However, you should continue to use port 8281 if using a standalone vRealize Orchestrator appliance.

2. Restart the vco-server service on the vRealize Orchestrator server. The following example illustrates how to do this using the `ssh` command:

```
$ ssh user@vro.server service vco-server restart
```

3. Check the vRealize Automation configuration by running the **Check EMC data protection configuration** workflow. Instructions are provided in [Checking the EMC Plug-in for vRealize Automation configuration](#).

Installing data protection admin services into a specific tenant

This section describes how to use the vRealize Orchestrator **Install default setup for tenant** workflow to automate some of the Advanced Services configuration steps.

Before you begin

- For the tenant you are setting up, there must be a user configured with credentials having Infrastructure Architect, Tenant Administrator and XaaS Architect roles. When adding the vRealize Automation host, a user with these roles is required.

Note

For a secondary tenant, you must have both the `vsphere.local` default tenant and the secondary tenant added as vRealize Automation (vCAC CAFE) hosts.

- A business group must exist, to which the data protection admin services are entitled.
- Data protection systems such as Avamar or Avamar Virtual Edition (AVE) must be installed, and the versions must be supported as described in the compatibility and interoperability matrix documents for the respective systems.
- If using Avamar, vRealize Automation vCenter endpoints must be registered with the Avamar systems using the fully qualified domain name (FQDN).
- If using Avamar for image-level backups, Image proxies compliant with the server version must be deployed within the vCenter endpoints and registered with their respective Avamar systems.

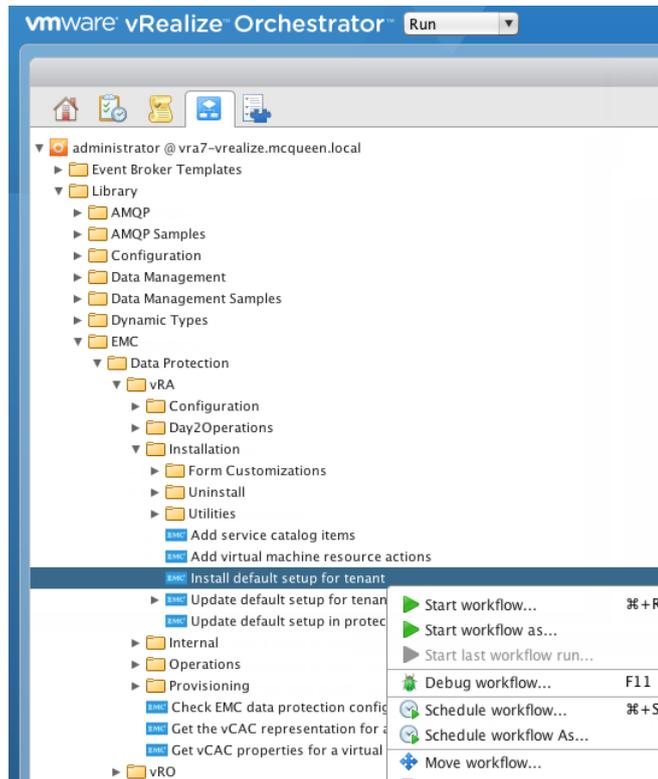
WARNING

The data protection admin services should not be exposed to any user who does not qualify as an administrator of the data protection services.

Procedure

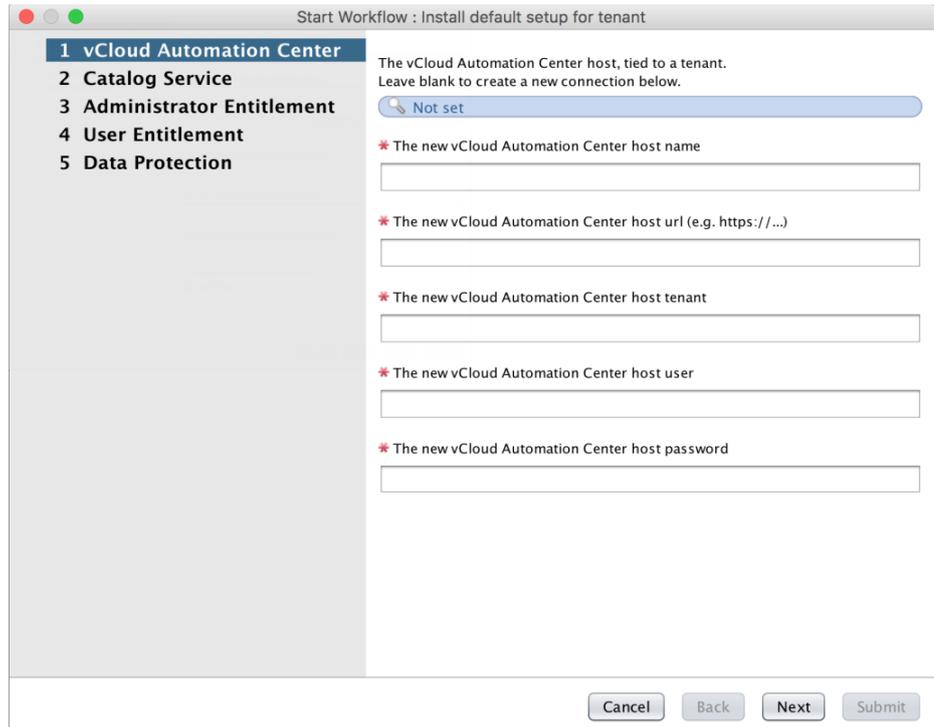
1. Log in to the vRealize Orchestrator client.
2. Select the **Workflows** tab.
3. Browse to `/Library/EMC/Data Protection/vRA/Installation`.
4. Right-click the **Install default setup for tenant** workflow and select **Start Workflow** as shown in the following figure.

Figure 12 Start Workflow in vRealize Orchestrator



The workflow wizard opens on the **vCloud Automation Center** screen.

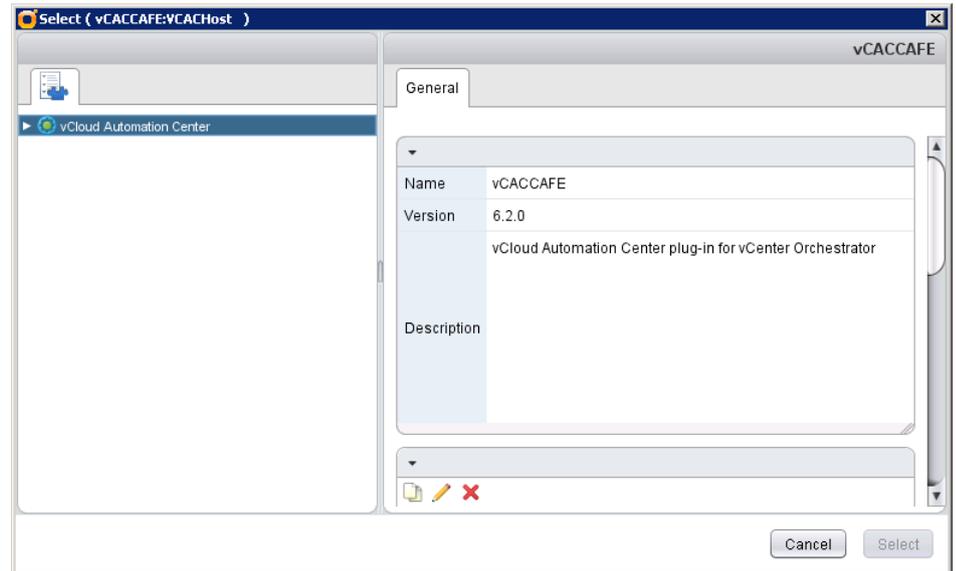
Figure 13 Start Workflow wizard



5. If you have already created the tenant-specific vCloud Automation Center host (as described in [Adding a vCloud Automation Center host](#), perform the following three steps. If you have not created the host, continue to step 6.
 - a. Click the **Not set** link in the top-most field.

The **vCACCAFE Host** dialog box opens.

Figure 14 Select vCACCAFE Host dialog



- b. In the left pane, expand the **vCloud Automation Center** list.
 - c. Select the tenant-specific vCAC host, and then click **Select**.

You are returned to the workflow wizard. Continue to step 7.

6. If you have not created a tenant-specific vCloud Automation Center host (as described in [Adding a vCloud Automation Center host](#), supply the following information in the **vCloud Automation Center** screen to create the host.

Note

When you enter this information manually, the workflow creates the vCenter Automation Center host for you. However, you cannot use the **Chooser** dialog boxes to select existing vRealize Automation Catalogs and Entitlements in the following screens. You must specify them manually.

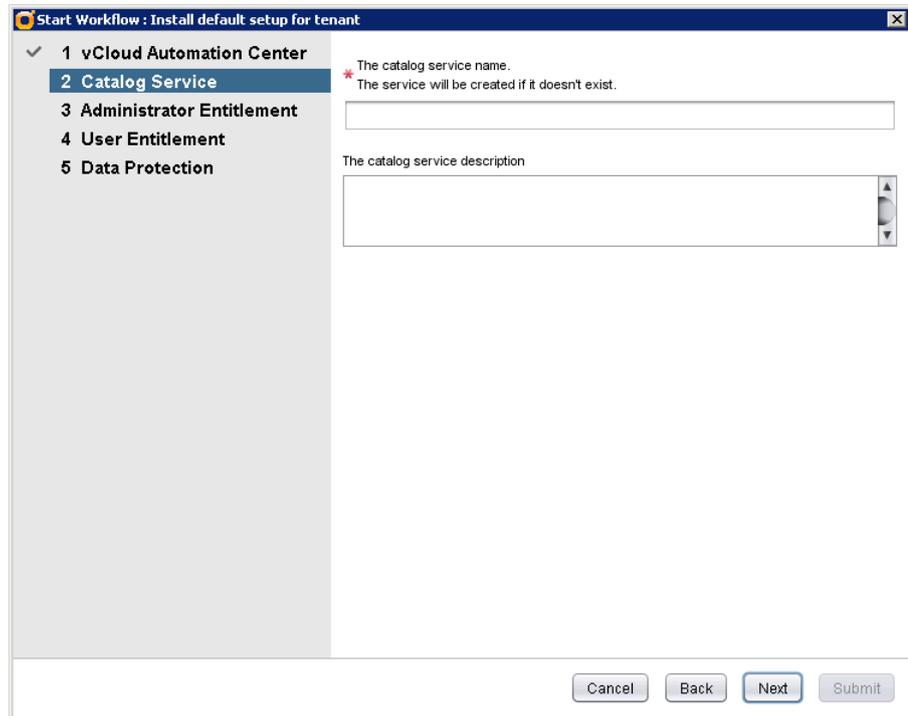
- **The new vCloud Automation Center host name:** Type a hostname for the vRealize Automation host. You can choose any name, but best practice is to provide the name of the tenant.
- **The new vCloud Automation Center host url:** Type the base URL for the vRealize Automation host (for example, `https:// ...`).
- **The new vCloud Automation Center host tenant:** Type the tenant URL name (for example, `vsphere.local`).
- **The new vCloud Automation Center host user:** Type the username for a user who has both the tenant administrator and the service architect roles for the tenant.

- **The new vCloud Automation Center host password:** Type the password for the user specified in the previous field.

7. Click **Next**.

The **Catalog Service** screen displays. Data protection admin services are published in the catalog service.

Figure 15 Catalog Service in Start Workflow wizard



8. On the **Catalog Service** screen, click **Not set** to select an existing catalog service, or type a name to create one.

9. Click **Next**.

The **Administrator Entitlement** screen displays. On this screen, you can entitle the data protection admin services to data protection admin users.

Figure 16 Administrator Entitlement in Start Workflow wizard

10. On the **Administrator Entitlement** screen, do the following:

- **The administrator entitlement name:** To select an existing administrator entitlement name, or type a new entitlement name, Click **Not set**.

Note

If you type the entitlement name, the system automatically creates the entitlement. However, a newly created entitlement does not have any users. Users must be added manually to the entitlement in vRealize Automation after the installation completes.

- **The administrator entitlement description:** Optionally, type a description for the entitlement.
- **The administrator entitlement business group name:** To select an existing business group name, or type the name of an existing business group, click **Not set**.

11. Click **Next**.

The **User Entitlement** screen displays.

Figure 17 user Entitlement in Start Workflow wizard

12. On the **User Entitlement** screen, do the following:

- **The user entitlement name:** To select an existing entitlement name, or type a user entitlement name, click **Not set**.

Note

If you type the entitlement name, the system automatically creates the entitlement. However, a newly created entitlement does not have any users. Users must be added manually to the entitlement in vRealize Automation after the installation completes.

- **The user entitlement description:** Optionally, type a description for the entitlement.
- **The user entitlement business group name:** To select an existing business group name, or type the name of an existing business group, click **Not set**.

13. Click **Next**.

The **Data Protection** screen displays.

Figure 18 Data Protection in Start Workflow wizard

14. On the **Data Protection** screen, do the following:
- **The data protection type to configure:** Select the data protection system (Avamar) used to protect the tenant.
 - **The data protection system hostname:** Type the data protection system's FQDN.
 - **The data protection system port:** Leave the data protection system port field blank unless the data protection system has been configured to listen on a non-standard port.
 - **The data protection system username:** Type the username required to log in to the data protection system.
 - **The data protection system password:** Type the password required to log in to the data protection system.
 - **The data protection system custom connection properties:** Leave this field blank.

Note

The fields on this page are optional. However, if the data protection system is not added during the install, you must run the **Add a tenant data protection system** Catalog Item from vRA after the install.

15. To run the workflow, click **Submit**.
16. Verify that the workflow ran successfully as follows:
- After the workflow has finished running, watch for `State - completed` in the workflow output.
 - View the data protection endpoint by selecting the **Inventory** tab, and clicking **EMC Data Protection**.

- c. If the vRealize Automation tenant-specific host was created by the workflow, verify that it exists for the tenant.
 - d. Log in to vRealize Automation as a tenant administrator (any user who was entitled to the data protection admin services published above).
 - e. On the **Catalog** tab, select the service that you created or selected.
 - f. Verify that you see the data protection service blueprints.
 You use the services to add data protection to the business rules incorporated in a blueprint.
17. Optionally, check the vRealize Data Protection Extension configuration as described in [Checking the EMC Plug-in for vRealize Automation configuration](#).

Licensing

Currently, you can order the EMC vRealize Data Protection Extension at no cost through the EMC DirectXpress (DXP) or ChannelXpress (CXP) ordering process. A License Authorization Code (LAC) letter is emailed or physically delivered to customers and partners during order processing and fulfillment. The LAC letter contains instructions for downloading software binaries as well as activating the license, entitlement, and generating the licensing key and/or file via the licensing website. The vRealize Data Protection Extension requires this licensing file, which you must place on the vRealize Orchestrator server.

The following sections describe where to put the licensing file on the Orchestrator server, and how to verify the validation check that is performed by the licensing.

Linux-based vRealize Orchestrator server

Procedure

1. Log in as `root` to the Linux system where the vRealize Orchestrator server is installed.
2. Browse to the following directory:
`/var/lib/vco/app-server/conf/plugins/`
3. In this directory, create a folder named `edplicense`.
4. Secure FTP the license file from the download location to the `edplicense` directory.
5. To change the owner of the `edplicense` directory and of the license file to the vCO user, type the following commands:

```
chown vco:vco /var/lib/vco/app-server/conf/plugins/edplicense
chown vco:vco <edplicenseFileName>
```

6. Open the browser to the vRealize Orchestrator Configuration web application for the vRealize Automation system, and in the left-hand pane, select **Startup Options**, and restart the vRealize Orchestrator server.

Results

The license file will now reside in `/var/lib/vco/app-server/conf/plugins/edplicense`. The EMC vRealize Data Protection Extension will look in this directory

to find the file and to validate its contents after any EMC plug-in operation is performed.

Verifying the licensing validation check

This section describes where to look in the log files to verify that the validation check performed by the plug-in licensing was successful.

The log files and their locations are listed as follows:

- **Linux** – /var/lib/vco/app-server/logs, which is sym-link'ed to /var/log/vmware/vco/app-server/
- **Windows** – C:\Program Files\VMware\Infrastructure\Orchestrator\app-server\logs
- **Files:**
 - catalina.out log file may or may not have an entry, depending on platform
 - edp_4_vcac.log file has an entry
 - server.log file has an entry

The following example shows a successful validation:

```
2015-03-06 17:01:48.992-0700 [http-bio-0.0.0.0-8281-exec-7]
[initEdpLicense] INFO {} [EdpRepository] Beginning to initialize
the EMC license check.
2015-03-06 17:01:49.015-0700 [http-bio-0.0.0.0-8281-exec-7]
[initEdpLicense] INFO {} [EdpRepository] (Set license policy:
PERMANENT licenses allowed.)
2015-03-06 17:01:49.015-0700 [http-bio-0.0.0.0-8281-exec-7]
[initEdpLicense] INFO {} [EdpRepository] (Set license policy: NO
LIC FILES allowed.)
2015-03-06 17:01:49.304-0700 [http-bio-0.0.0.0-8281-exec-7]
[setFeatures] INFO {} [EdpRepository] Feature: vra_edp_plugin
Valid: true
2015-03-06 17:01:49.305-0700 [http-bio-0.0.0.0-8281-exec-7]
[initEdpLicense] INFO {} [EdpRepository] Done initializing the
license processing.
```

The following example shows a validation that failed with valid file in place:

```
2015-03-06 17:01:48.992-0700 [http-bio-0.0.0.0-8281-exec-7]
[initEdpLicense] INFO {} [EdpRepository] Beginning to initialize
the EMC license check.
2015-03-06 17:01:49.015-0700 [http-bio-0.0.0.0-8281-exec-7]
[initEdpLicense] INFO {} [EdpRepository] (Set license policy:
PERMANENT licenses allowed.)
2015-03-06 17:01:49.015-0700 [http-bio-0.0.0.0-8281-exec-7]
[initEdpLicense] INFO {} [EdpRepository] (Set license policy: NO
LIC FILES allowed.)
2015-03-06 17:01:49.304-0700 [http-bio-0.0.0.0-8281-exec-7]
[setFeatures] INFO {} [EdpRepository] Feature: vra_edp_plugin
Valid: false
2015-03-06 17:01:49.305-0700 [http-bio-0.0.0.0-8281-exec-7]
[initEdpLicense] INFO {} [EdpRepository] Done initializing the
license processing.
```

Upgrading the EMC vRealize Data Protection Extension

This section describes how to upgrade an existing EMC vRealize Data Protection Extension installation to the latest version. It assumes that you have already downloaded the `edp4vcac-3.1.0.n.vmoapp` file.

While upgrading the EMC vRealize Data Protection Extension, you can continue to perform data protection system operations, including scheduled backups. You cannot, however, perform the following:

- During the upgrade, you are not able to:
 - Run data protection
 - Restore data
 - View protection status
 - Add/remove data protection
 - Perform property group operations
 - Add/remove data protection systems
 - Set up a data protection property group
- During restart of the vRealize Orchestrator server(s), you are not able to:
 - Assign data protection during virtual machine provisioning
 - Retire the protection client during virtual machine destroy

After the upgrade completes, the existing EMC data protection systems will be available, and all policies, clients, and backups will still be available.

Note

Before upgrading, EMC recommends that you backup or take snapshots of the vRealize infrastructure, including:

- the vRealize Automation server
 - the vRealize Automation database
 - the vRealize Orchestrator server(s) (if using external servers).
-

Install the EMC vRealize Data Protection Extension vmoapp

Install the vRealize Data Protection Extension `vmoapp` and verify the installation as described in [Installing the EMC Plug-in for vRealize Automation](#).

Note

If using multiple vRealize Orchestrator nodes in a cluster, perform this step on each vRealize Orchestrator node.

Update the default setup in each vRealize Automation tenant

This procedure deletes and re-creates the catalog items and resource actions (and their forms) that were added to the vRealize Automation service catalog in the previous release.

If you previously applied form customizations to the catalog items or resource actions, or changed the icon, those changes are lost and must be reapplied in vRealize

Automation. The update process maintains the previous entitlements and approval policies, if any. After performing this update, verify the entitlement(s) on each catalog item and resource action.

You can run the update workflow to update all tenants, or to update individual tenants.

Note

If you are using multiple vRealize Orchestrator nodes in a cluster, this update only must be run on one of them against the vRealize Automation server.

Running the update workflow for all tenants

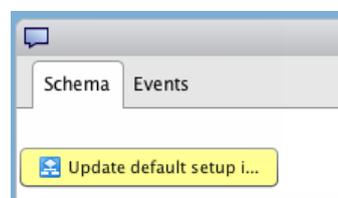
This section describes how to run the workflow that updates all the vRealize Automation tenants.

Procedure

1. In the vRealize Orchestrator client, select the **Workflows** tab.
2. Browse to the following workflow:
Library/EMC/Data Protection/vRA/Installation/
3. Select the **Update default setup for protected tenants** workflow, and click the green arrow (▶) in the upper-left corner of the right-hand pane to start the workflow.

Figure 19 Workflow interaction form

If the **Workflow interaction form** does not open automatically, select the icon at the top of the workflow editor.



Note

You are prompted with a workflow interaction form for each vRealize Automation tenant in the system that has been configured with the vRealize Data Protection Extension. If you want to skip updating a particular tenant, select **No** for the **Update setup for tenant?** option, and then click **Submit** (do not click **Cancel**).

4. In the **Workflow interaction form**, click **Not set** for each of the parameters (catalog service, entitlement for tenant administrators, and entitlement for tenant users), and select the appropriate options in the **Chooser** dialog box.
5. When you have set the parameters, click **Submit**.

Running the update workflow for individual tenants

This section describes how to run the workflow that lets you select a vRealize Automation tenant to update.

Procedure

1. In the vRealize Automation client, select the **Workflows** tab.
2. Browse to the following workflow:
Library/EMC/Data Protection/vRA/Installation/
3. Select the **Update default setup for tenant** workflow, and click the green arrow (▶) in the upper-left corner of the right-hand pane to start the workflow.

The **Start Workflow : Update default setup for tenant** form opens.

Figure 20 Start Workflow : Update default setup for tenant

4. For **The vRealize Automation center host, tied to a tenant** parameter, Click **Not set**, and select the vRealize Automation tenant that you want to update in the **Chooser** dialog box.
5. An additional upgrade option will remove the old ExternalWfStub.* properties from upgraded blueprints, now referred to as property groups. Prior to selecting **Yes** to remove these properties, EMC recommends that you back up your blueprints by using the instructions at the following [link](#).
6. Click **Not set** for each of the remaining three parameters (catalog service, entitlement for tenant administrators, and entitlement for tenant users), and select the appropriate options in the **Chooser** dialog box.
7. When you have set the parameters, click **Submit**.

Update custom workflows and actions

In vRealize Orchestrator, if you have written custom workflows or actions that use the EMC vRealize Data Protection Extension's workflows, actions, or scripting objects, you must verify the code against the new version in the vRealize Orchestrator client.

Verifying the new version

After upgrading the EMC vRealize Data Protection Extension and restarting the vRealize Orchestrator server, use one of the following methods to verify that the system has the correct new version:

- Select **Help > Installed Plug-ins** in the vRealize Orchestrator Control Center.
- Select **Manage Plug-ins** in the left-hand pane of vRealize Orchestrator Configuration UI.

Note

If you deployed the `.vmoapp` file using an http client, restart the vRealize Orchestrator Configuration server to see the updated version here.

- View the contents of the **Workflows** and **Actions** tabs for the `com.emc.edp4vcac` package in the vRealize Orchestrator client. All the workflows and actions should have a new version number.

Run cleanup script after upgrading

After upgrading to 3.1.0, some unnecessary workflows and actions may remain in the vRealize Orchestrator server from version 3.0.0.

You can remove these entries manually in the vRealize Orchestrator client of each vRealize Orchestrator server, or you can run a cleanup script.

The cleanup script `cleanup-pkg-after-upgrade.sh` is located in the `docs/` folder of the `edp4vcac-3.1.0.N.zip` file. You can run the script on the following:

- vRealize Automation Linux appliance
- vRealize Orchestrator Linux appliance
- Any Mac OS, Linux, or Windows (with cygwin, MKS or similar installed) machine which has `curl` and `xmlint` or `xpath` (from `perl`) installed.

To run the script, unzip or copy the script to a system where you can run it from, and then run one of the following commands. If you are using a vRO cluster, run the command against each vRealize Orchestrator server.

- `$ sh cleanup-pkg-after-upgrade.sh --prompt`. This command prompts you to type values.
- `$ sh cleanup-pkg-after-upgrade.sh --host <vrohost> --user <user@vsphere.local> -- port <443 or 8281> --pass <password>`

Note

Specify port 443 for when using the internal vRealize Orchestrator appliance, or port 8281 when using a stand-alone vRealize Orchestrator appliance.

Changes to workflow and actions directory locations from release 2.0 to 3.0 and later

If upgrading from the 2.0 release, workflow IDs remain the same, however, the location of the workflows changed in release 3.0.0. The folder `Library/EMC/Data Protection/vRA` contains most of the workflows originally under `Library/EMC/Data Protection/vCAC`. The folder `Library/EMC/Data Protection/vRO` contains the remaining workflows.

Also, all the actions that are originally located under the `com.emc.edp4vcac*` action modules are now located under `com.emc.edp*` action modules.

Uninstalling the EMC vRealize Data Protection Extension

The following sections describe how to uninstall the EMC vRealize Data Protection Extension. The tasks include removing EMC data protection from each tenant, and uninstalling the extension from vRealize Orchestrator.

Uninstall EMC data protection from a single tenant

The following two sections describe how to remove default setup items, and how to reconfigure vRealize Automation blueprints for a single tenant. These procedures must be performed on each vRealize Automation tenant.

Remove default setup items

This procedure describes how to remove the catalog items and resource actions.

You can also remove the EMC data protection system configured for the vRealize Automation tenant.

1. Open the vRealize Orchestrator client.
2. In the **Workflows** tab, browse to `/Library/EMC/Data Protection/vRA/Installation/Uninstall`, and run the **Remove default setup for tenant** workflow.
3. Select the vRealize Automation host connection for the tenant.
4. Select if you want to remove the EMC data protection system(s) configured for the tenant.
If you do not remove the configured systems for the tenant, you can still perform protection operations through vRealize Orchestrator.
5. To remove any **ExternalWFStubs.MachineDisposing** properties left over from previous versions of the EMC vRealize Data Protection Extension, browse to **Infrastructure > Managed Machines**, and update any existing machines available to the tenant. If you retained the EMC data protection system(s) for the tenant and are not removing the entire EMC vRealize Data Protection Extension, you can leave this property to have the client in Avamar still be retired when the machine is

disposed in vRealize Automation. If you are using custom machine lifecycle workflows that use the EMC data protection workflows, modify the custom workflows instead.

Alternate Procedure

If preferred, you can uninstall the plug-in from a tenant using the following steps.

1. In vRealize Automation, delete the catalog items and resource actions manually.
2. In the vRealize Orchestrator client's **Workflows** tab, browse to `/Library/EMC/Data Protection/vRO/Configuration`, and run the **Remove a data protection system** workflow to remove the systems configured for the tenant.

Reconfigure vRealize Automation blueprints

After removing the default setup items, reconfigure the blueprints.

Procedure

1. Open vRealize Automation.
2. Browse to **Design > Blueprints**, and update any Blueprints available to the tenant that you had previously configured for data protection during provisioning and retiring.
3. Remove from the blueprint any property groups that were created and/or configured for data protection.
4. Browse to **Administration > Property Dictionary**, and remove any property groups that were created and/or configured for data protection (generally, by using the **Setup data protection property group**), and remove their associated property definitions.

Uninstall the plug-in from vRealize Orchestrator

This section describes how to uninstall the EMC vRealize Data Protection Extension from vRealize Orchestrator.

Before you begin

The EMC vRealize Data Protection Extension must have been uninstalled from each tenant in vRealize Automation.

Procedure

1. Open the vRealize Orchestrator client.
2. In the **Inventory** tab under the **EMC Data Protection** branch, verify that all the data protection systems were removed. If they were not, right-click each one, select **Run Workflow... > Remove a data protection system**, and run that workflow.
3. Use the instructions that are provided in the following VMware Knowledge Base article to remove all custom workflows, actions, policies, web view, configurations, settings, and resources that the plug-in contains:

<http://kb.vmware.com/kb/2064575>

Have a backup or snapshot of the vRealize Orchestrator virtual machine in case you must revert the changes.

Use the following information when performing the steps in the KB article:

- The dar file is `edp4vcac.dar`

- The configuration file is `EDP.xml`
 - The package to remove in the vRealize Orchestrator client is `com.emc.edp4vcac`
4. Verify that all the `com.emc.edp` action modules are deleted; if not, delete them in the vRealize Orchestrator client.
 5. Verify that the `/Library/EMC/Data Protection workflow` folder is empty and/or delete it in the vRealize Orchestrator client.

CHAPTER 3

Administration

This chapter includes the following topics:

- [Data protection configuration for the tenant](#)..... 52
- [Data protection administration](#).....55

Data protection configuration for the tenant

The EMC vRealize Data Protection Extension provides the ability to perform data protection operations within vRealize Automation.

These operations are configured at a per-tenant level and consist of two main components:

- A set of data protection XaaS Blueprints which are made available to data protection administrators.
- A set of XaaS Resource Actions which are made available so that owners of virtual machines can manage their own data protection needs on a per-virtual machine basis.

Clustered vRealize Orchestrator environment

The EMC vRealize Data Protection Extension supports a clustered vRealize Orchestrator (vRO) environment. However, the Data Protection system information is stored locally on each vRO appliance. Therefore, in a clustered vRealize Orchestrator environment, you must run the **Install default setup for tenant** workflow per tenant on one of the vRO appliances.

Additionally, if you want to replicate the configuration information among the other nodes in the cluster, you must synchronize this vRO appliance with the other nodes. For example, if the vRO appliance that you run the **Install default setup for tenant** workflow on is node A, to synchronize the other nodes in the cluster with node A:

1. Log in to the **vRO Control Center** of each of the other nodes.
2. Invoke **Join Node to Cluster**.
3. Specify the Remote Orchestrator Server as Node A (IP address or hostname).
4. Provide the Remote Orchestrator Server's **vRO Control Center** credentials.

This replicates the configuration information of node A into the current node. Even if the cluster was formed previously, you must repeat this step and specify the number of active nodes for any configuration changes to occur.

Note that in an environment with clustered vRO appliances, you may need to perform the steps above for the following workflows as well:

- **Remove a data protection system**—If you want to remove a tenant data protection system, run the **Remove a data protection system** workflow from the vRealize Orchestrator client of each vRO in the cluster, or from the vRealize service catalog, per tenant on one of the vRO appliances. This removes the EDP system from one of the nodes in the cluster. You must then perform the steps above to replicate this removal on the other nodes.
- **Add a tenant data protection system**—If you want to add a tenant data protection system, run the **Install default setup for tenant** or **Add a tenant data protection system** workflow per tenant on one of the vRO appliances. You must then perform the steps above to replicate this addition on the other nodes.
- **Update a tenant data protection system**—This is a vCO workflow that is not currently available in vRA, and is located under `Library/EMC/Data Protection/vRO/Configuration`. After running this workflow, you must then perform the steps above to replicate the update on the other nodes.

Note

In a clustered vRealize Orchestrator environment with load balancing of vRA traffic across two vRO systems, the EdpSystem ID on both vRO systems must match. If the IDs do not match, and you run the vRA request for findAll on one vRO and then send a findById using that list to the other vRO, the unique ID created for clients, policies, and so on, do not match and result in some empty select boxes in vRA. To ensure that both systems have the same EdpSystem ID, log in to the **vRO Control Center** and invoke **Join Node to Cluster**. This joins the vRealize Orchestrator server to another vRealize Orchestrator server to form or expand a cluster. The current server automatically replicates the configuration of the remote server. You can then restart the vRO services on the updated systems by using **Startup Options** in the **vRO Control Center**.

Avamar domains for tenant data protection policies

When you add a data protection system for a tenant, tenant domains are created in Avamar. One tenant domain is created per vCenter domain, and one tenant domain is created under the EDP domain that you create when configuring Avamar for application-consistent backup. If the domains exist, these existing domains are used.

If you create a domain manually, ensure that you create it as a direct sub-domain of the vCenter domain for VMware image backup, or EDP domain for application-consistent backup, with the vCenter domain representing the provisioning infrastructure for the tenant, and use the following naming convention:

```
tenantUrlName_vRAServerFQDN. For example,  
vsphere.local_vraserver.domain.com.
```

Note

Policies consist of two types — the policies for VMware image backups created in the vCenter domain under the tenant domain, and the policies for application consistent backups created in the EDP domain under the tenant domain.

Adding a second vCenter endpoint

When you add a vCenter endpoint to vRealize Automation, the data protection system administrator must manually add the vCenter client to the data protection system. Once that has been accomplished, the EMC vRealize Data Protection Extension is used to add tenant domains.

You can add tenant domains using either of the following options:

- Restart the vRealize Orchestrator service.
- Log in to vRealize Orchestrator client and refresh using the following steps.
 1. Select the **Inventory** tab.
 2. Select the **EMC Data Protection** top node.
 3. Click the **Refresh** button at the top right corner.

Managing multiple vCenters with Avamar

The EMC vRealize Data Protection Extension handles a policy similar to a service level agreement (SLA). Only one SLA is allowed per policy name (Avamar Group) per policy type (Image or Application Consistent).

To fulfill this SLA across vCenters, an administrator must create an Avamar Group in each vCenter by using the Avamar Administration GUI.

Example 1 SLA named Gold where data center contains two vCenter servers

For an SLA named Gold that requires daily backups, where the data center contains two vCenters: The virtual machine can now belong to either vCenter, and Avamar can successfully perform the backup.

1. Create the Avamar Group for the Gold SLA under the domain `/vCenter1/tenant domain` with the desired settings.
2. Copy the group into the domain `/vCenter2/tenant domain`.

Tenant and EMC vRealize Data Protection Extension configurations

There are a number of different ways to configure data protection systems across tenants. The tenant administrator can choose between the following Avamar configurations based on their environment.

Avamar tenant configurations

A tenant administrator can choose between the following options to configure the Avamar data protection systems across tenants.

One tenant and one data protection system

The tenant administrator runs either the **Install default setup tenant** workflow from vRealize Orchestrator or the **Add a tenant data protection system** workflow from the vRealize Automation tenant. The section [Avamar domains for tenant data protection policies](#) provides information about how domains are added to the Avamar data protection system across tenants.

One tenant and multiple data protection systems

The tenant administrator runs either the **Install default setup tenant** workflow from vRealize Orchestrator or the **Add a tenant data protection system** workflow from the vRealize Automation tenant to add the first data protection system. The administrator then runs the **Add a tenant data protection system** workflow again from the same tenant to add a different data protection system. The section [Configuring an Avamar data protection system](#) provides more information.

Multiple tenants and one data protection system

The tenant administrator runs either the **Install default setup tenant workflow** from vRealize Orchestrator or the **Add a tenant data protection system** workflow from the vRealize Automation tenant for all tenants, specifying the same data protection system.

Multiple tenants with each tenant pointing to different data protection systems

The tenant administrator runs either the **Install default setup tenant workflow** from vRealize Orchestrator or the **Add a tenant data protection system** workflow from

the vRealize Automation tenant for all tenants, specifying a different data protection system.

Avamar multi-tenant configuration considerations

Note the following information with regard to Avamar multi-tenant configurations:

- The backup administrator can add a data protection policy to a tenant domain, or remove a data protection policy from a tenant domain, and can manually add domains in Avamar. If you configure multiple tenants, create a policy in each tenant domain by using the Avamar system's user interface or command line interface.
- After the Avamar server node has been added as the EMC data protection system, the tenants can be configured through requests from the vRealize Automation Service Catalog.
- Moving tenants from one Avamar system to another Avamar system is not supported.
- When you add protection using data protection actions rather than through a policy-protected blueprint, re-add data protection if the virtual machine is re-provisioned. Virtual machines that are provisioned from blueprints with policy protection do not have this limitation.

Data protection administration

After the one-time configuration of the data protection system connection information, the tenant administrator must assign available data protection policies to virtual machine blueprints.

Service blueprints

The following table lists the EMC vRealize Data Protection Extension XaaS blueprint names and descriptions. These XaaS blueprints are added to the service catalog for the data protection administrator user with the Administrator Entitlement, which you create by running the **Install default setup for tenant** workflow in vRealize Orchestrator.

Table 5 Service catalog blueprints

Service blueprint name	Description
Add a tenant data protection system	Configures and adds an EMC Data Protection system to the vCenter Orchestrator inventory. EMC's Data Protection Suite consists of various software offerings for data backup, recovery, and archiving. Currently, you can add Avamar data protection systems using this workflow.
Remove a tenant data protection system	Removes an EMC vRealize Data Protection system from the vRealize Orchestration inventory. Typically, this service blueprint is only required if the user wants to change the data protection system.
Set up a data protection property group	Allows you to add or modify data protection on a new or existing property group. For Avamar, both image-level and application-consistent protection policies are available. If you select an application-consistent protection policy, an optional

Table 5 Service catalog blueprints (continued)

Service blueprint name	Description
	configuration field allows you to specify a time in minutes that the custom workflow should wait to discover a configured hostname of the virtual machine.
Restore deleted machine from backup	Restores a deleted virtual machine that had data protection and backups on an Avamar server. The machine is restored as a new virtual machine.

Configuring an Avamar data protection system

This topic describes how to configure an Avamar data protection system by using vRealize Automation. After you have configured the system, you can verify that it has been added by logging in to the vRealize Orchestrator Client.

Before you begin

You must be logged in to vRealize Automation as a user with the administrator entitlement, as defined in the **Install default setup for tenant** workflow.

Procedure

1. In vRealize Automation, select the **Catalog** tab.
2. In the left pane, click the data protection service.
3. In the **Services** pane, click **Request** for **Add a tenant data protection system**.
The **Add a tenant data protection system** page displays, open on the **System Information** tab.
4. In the **System Information** tab:
 - a. Select **Avamar** from the drop-down list.
 - b. Type the FQDN of the system that you are adding.
 - c. Optionally, select a port, and type custom properties.
 - d. To display the **Credentials** tab, click **Next**.
5. In the **Credentials** tab:
 - a. Type the username and password that is required to access the data protection system.
 - b. Click **Submit**.
6. To close the request configuration message, click **OK**.
7. Select the **Requests** tab, and view the progress of the second Avamar addition until it completes successfully.
8. To verify that the data protection system has been successfully added, log in to the VMware vRealize Orchestrator Client.
The client opens on the **My Orchestrator** tab.
9. Select the **Inventory** tab.
10. In the **Inventory** tab, click the arrow beside **EMC Data Protection** to expand its list.

You should see both Avamar systems.

Note

The Avamar system does not display any policies if the policies were incorrectly added to `/vCenter/tenant domain` in the **Avamar Administration** GUI.

Setting up data protection on a blueprint

To add data protection to a blueprint in vRealize Automation, perform the following steps. Once the data protection has been added to the blueprint, the business group user can apply data protection to a virtual machine at the time of provisioning.

During this procedure, you create a property group that contains either a list of user-selectable policies, or a single, non-selectable policy. A selectable-policy property group allows the business group user to choose a policy when requesting a blueprint. A non-selectable-policy property group contains a single policy that is applied automatically when the business group user requests a blueprint.

Procedure

1. In vRealize Automation, browse to **Catalog > Setup data protection property group**, and click **Request**.

The **Setup a data protection property group** page displays.

2. Create a property group or select an existing one.
 - To create a property group:
 - a. Select **[New Property Group]** from the drop-down list.
 - b. Specify a name, a unique ID, and an optional description.

Note

The property group created will only be visible by the current tenant.

- c. To display the **Data Protection** tab, click **Next**.
- To use an existing property group, select the property group from the drop-down list, and click **Next** to display the **Data Protection** tab.
-

Note

You can use existing property groups that do not have data protection. Any required data protection properties will be added to the property group. If the property group already has data protection properties, you can select one or more policies to add to the existing policy for the property group.

3. In the **Data Protection** tab, you can decide whether the business group user can select one or more protection policies when the blueprint is requested. Also, you can select the policy or policies that the property group uses.

The property group can contain either a list of selectable policies or a single, non-selectable policy that is applied automatically to the virtual machine at provisioning time.

- To create or update a property group with selectable policies:
 - a. In the **Allow user to select data protection policy when blueprint is run?** drop-down, select **Yes**.
 - b. If the VM is a database server (for example, if the VM is an Oracle database), EMC recommends protecting the virtual machine with both

the Application consistent data protection policy and an Image level data protection policy.

- c. Select the checkbox next to one or more policies in the list.
 - d. If you select an Application Consistent Data Protection policy, specify a time in minutes that the custom workflow should wait to discover a configured hostname of the virtual machine. The default is 10 minutes.
 - To create or update a property group with a non-selectable policy that is applied automatically to the virtual machine at provisioning time:
 - a. In the **Allow user to select data protection policy when blueprint is run?** drop-down, select **No**.
 - b. If the VM is a database server (for example, if the VM is an Oracle database), EMC recommends protecting the virtual machine with both the Application consistent data protection policy and an Image level data protection policy.
 - c. Select one policy in the list.
 - d. If you select an Application Consistent Data Protection policy, specify a time in minutes that the custom workflow should wait to discover a configured hostname of the virtual machine. The default is 10 minutes.
4. Click **Submit**.

Edit the blueprint by navigating to the **Design > Blueprints** tab, and adding the property group to either the blueprint directly or to one or more components of the blueprint. The vRealize Automation documentation available at the following [link](#) provides more information.

Configuring application-consistent data protection

Application consistent data protection allows you to use Avamar plug-ins for applications to protect the application data. This is only supported for stand-alone or simplex configuration of the application.

File system backup is also supported. This feature is available with the File System plug-in which is part of the Avamar client. Avamar plug-ins are installed after the client install. You can protect file system data when it is specified in the Dataset that is part of the Avamar Group for data protection. The *Avamar Backup Clients User Guide* provides more information.

Versions 7.2.x and 7.3.x of the Avamar plug-ins that are listed in the following table are supported by the current release of the vRealize Data Protection Extension.

Table 6 Avamar plug-ins supported for application-consistent data protection

Plug-in	Related Documentation
EMC Avamar for Oracle	EMC Avamar for Oracle User Guide
EMC Avamar for SQL Server	EMC Avamar for SQL Server User Guide
EMC Avamar for Exchange VSS	EMC Avamar for Exchange VSS User Guide
EMC Avamar for SharePoint VSS	EMC Avamar for SharePoint VSS User Guide

Note

At this time, only stand-alone implementations of these applications are supported. The related documentation is available on <https://support.emc.com/products/>.

Procedure

1. Using VMware vCenter Server, create a virtual machine.
 2. Install the application (Oracle, SQL Server, SharePoint VSS, or Exchange VSS) on the virtual machine.
 3. Using the instructions that are provided in the related Avamar plug-in documentation, install the appropriate Avamar plug-in on the virtual machine, and perform any desired actions to prepare the application for data protection.
-

Note

Any changes to the application at this point are applied to all provisioned virtual machines.

4. Using vCenter, create a virtual machine template.
5. Use this virtual machine template to create the blueprint in vRA.
6. Using Avamar Administrator, create policies for the application under the EMC Data Protection (EDP) domain.
7. Using the vRealize Data Protection Extension, follow the instructions that are provided in [Setting up data protection on a blueprint](#) on page 57 to configure data protection for a new or existing blueprint.
8. Set up DHCP/VMware/Other customization to provide an IP address and hostname to the virtual machine during vRA provisioning. During provisioning, the vRealize Data Protection Extension reads the hostname of the virtual machine and activate the Avamar client to set up data protection. Ensure that the DNS configured in the Avamar server can resolve the hostname.
9. After a virtual machine is provisioned, ensure that the Avamar dataset that is used in the Avamar Group includes the databases that require protection. Follow the instructions provided in the related Avamar plug-in documentation.

Restoring application backups

You can perform restores of application backups by using the **Avamar** user interface.

The Avamar (versions 7.2.x and 7.3.x) Plug-in user guides, available at <http://support.emc.com>, provide instructions.

Supported Advanced Services actions for application-consistent data protection

The vRealize Data Protection Extension supports the following Advanced Services actions for application-consistent data protection.

Add data protection

This operation adds an application policy to a virtual machine for data protection. It activates a client if it has not already been activated.

Remove data protection

This operation removes an application policy from a virtual machine to remove data protection.

Note

Even if all data protection is removed from the virtual machine, the client is still activated.

View protection status

This operation displays the policies that protect the virtual machine, and also a list of backups of the virtual machine, including application backups.

Run data protection

This operation runs data protection for a virtual machine protected by an EMC data protection policy. Application data protection policies are also supported.

Destroy

When you run this operation, vRA shuts down and deletes the virtual machine. Before shutdown, vRA invokes a custom workflow which tries to backup the virtual machine. If the virtual machine is associated with one or more image policies and/or application policies, the workflow tries the backup using at least one of each policy type. This action provides you with an image backup and an application backup before the client is retired.

Restoring a virtual machine to a new location using advanced options

Tenant administrators can use advanced options to restore a virtual machine backed up with Avamar to a new location. These options are additional to the options available to a business group user when restoring a virtual machine to a new location.

Before you begin

- You must be logged in to vRealize Automation as a user with the administrator entitlement, as defined in the **Install default setup for tenant** workflow.
- The virtual machine that you plan to restore must have one or more existing image level backups to Avamar. Restores of virtual machines that are backed up using an Avamar application-consistent policy are not available.

Procedure

1. In vRealize Automation, select the **Items** tab.
2. In the left pane, click **Machines**.

The **Machines** list displays in the right pane.

3. In the **Owned by** list, select the group that owns the virtual machine that you plan to restore.

Only the machines that are owned by that group are displayed in the **Machines** list.

4. Click the row of the machine that you want to restore.

The row is highlighted.

Note

If you are unsure if a machine has been backed up, select **View protection status** from the **Actions** menu. Existing image-level backups are listed in the scrolling status field.

5. From the **Actions** menu, select **Advanced restore to new**.

The **Advanced restore to new** page opens on the **Restore Options** tab.

6. In the **Restore Options** tab, select a backup from the drop-down list or search for backups by date range. You can also limit the number of backups that are listed.
 - a. If you want to filter the backups by date range, select **Yes**, and select the **Start Date** and time and the **End Date** and time.
 - b. Select the maximum number of backups that you want to view.
 - c. To display the backups that match the filter criteria, click the **Backup** drop-down list.
 - d. Select the backup that you want to restore.

When you select a backup, the new name for the virtual machine is populated automatically. You can change the name if preferred.

7. To display the **Advanced Options** tab, click **Next**.

The advanced options on this tab are described in the following list.

- **Reservation:** Where to create the virtual machine. The reservation the original virtual machine was in is selected by default. Only the reservations available for the original virtual machine's owner are visible based on the business groups they belong to.
 - **Datastore:** Which datastore within the reservation to put the virtual machine in. The list of available datastores is based on the datastores that have been configured for the selected reservation. The datastore that is used for the original virtual machine's first disk is selected by default if the datastore has been added to the selected reservation. If the restored virtual machine has multiple disks, then all these disks are created in the selected datastore.
 - **Destination Resource Pool Path:** The Resource Pool to put the virtual machine in. The pool from the original virtual machine is selected by default. You can select a different pool if preferred.
 - **New VM folder:** The folder from the original virtual machine is selected by default. You can select a different folder if preferred.
8. Select the advanced options that you want to use to restore the virtual machine, and then click **Next**.
 9. Review the warning:

```
vRealize Automation 7.0.1 does not have the ability to do an automated import. Submitting this request will create a new Virtual Machine in the vCenter, however an administrator will need to use the bulk import capability to manually import this machine.
```

10. If you accept the warning, click **Submit**.
11. To close the request confirmation message, click **OK**.
12. To view the progress of the restore, select the **Requests** tab.
13. When the workflow completes, you can perform one or both of the following:
 - a. Open vCenter to verify that the machine was created in the expected location.
 - b. Bulk Import the restore into vRealize Automation. The VMware documentation at the following [link](#) provides more information.

Restoring a deleted virtual machine

Deleted virtual machines that had data protection and backups on an Avamar server retain these backups until the retention period expires. Backups are retained even when the virtual machine is deleted from the VMware infrastructure. As a tenant administrator, you can restore one of these backups as a new virtual machine.

Before you begin

- You must be logged in to vRealize Automation as a user with the administrator entitlement, as defined in the **Install default setup for tenant** workflow.
- The virtual machine that you plan to restore must have one or more existing image level backups to Avamar. Restores of virtual machines that are backed up using an Avamar application-consistent policy are not available.

Note

This feature does not provide a filter by tenant. Therefore, when restoring a deleted VM, you, as a tenant administrator, can see every deleted machine on the Avamar server. If security concerns exist regarding a multi-tenant system, EMC recommends that each tenant have its own unique Avamar server for storing backups. Alternatively, you can add entitlement for this catalog item to only appropriate users.

Procedure

1. In vRealize Automation, select the **Catalog** tab.
2. In the left pane, click the data protection service.
3. In the right pane, click **Request** for the **Restore deleted machine from backup** catalog item.

The **Restore deleted machine from backup** page opens on the **Select VM** tab.

4. On the **Select VM** tab, select which VM to restore. The **Filter By Name?** option is set to **Yes** by default. If you select **No**, the **Name Filter** option is no longer visible.
 - a. If you want to filter the results by VM name, leave the **Filter By Name?** option set to **Yes**, and type the filter criteria in the **Name Filter** field.
 You can filter by partial or full VM name, and/or by the date the machine was deleted. The date was added by Avamar when the deletion occurred, and is in the format `yyyy.mm.dd`. For example, 2015.08.31.
 - b. To display the list of machines that match the filter criteria, click the **Deleted Machine** drop-down list.

Note

This list includes all machines that match the filter criteria, including machines that do not have backups.

- c. Select the machine that you want to restore, and click **Next** to display the **Select backup** tab.
5. In the **Select backup** tab, select a backup from the drop-down list or search for backups by date range. You can also limit the number of backups that are listed.
 - a. If you want to filter the backups by date range, select **Yes**, and select the **Start Date** and time and the **End Date** and time.

- b. Select the maximum number of backups that you want to view.
 - c. To display the backups that match the filter criteria, click the **Backup** drop-down list.
 - d. Select the backup that you want to restore.
6. In the **Import Information** tab, specify the new owner's vRA username, and select the business group, reservation, and blueprint that the new VM has when it is restored.

The username is contained in the **Owner** field by default.

- a. In the **Owner** field, type the username of the owner. For example, `Annie@machine.local`.

The **Business Group** list is populated with the business groups that are common to you (as the tenant administrator) and to the owner that you specified. If the username of the new owner is invalid, or if there are no common business groups between you and the owner, the list is empty.

- b. Select the **Business Group** for the new owner.
- c. Select the **Reservation** that you want to use to determine what resources are available on the new VM. Only the reservations that are available for the selected business group are contained in the **Reservation** list.
- d. Click **Next**, or select the **Restore Location** tab.

Note

The field names appear differently depending on whether you are using vCloud Automation Center 6.1 or vRealize Automation 6.2. The names are referred to generically here.

7. In the **Restore Information** tab, you specify details about the physical hardware for the new VM based on the reservation.
- a. In the **New Virtual Machine Name** field, type a name for the new machine, or accept the default name, which is the original name plus a current timestamp.

During the restore, the system prevents the new VM name from overwriting an existing VM.
 - b. Select a **Host**.

The hosts that are contained in the list are the ESX hosts that are available in the selected reservation.
 - c. Select a **Datastore**.

The datastores that are contained in the list have been enabled in the selected reservation and that are visible to the selected ESX host.
 - d. Select a **Resource Pool**.

The resource pools that are contained in the list have been filtered based on the selected datastore.
 - e. Select a **Virtual Machine Folder**.

The folders that are contained in the list have been filtered based on the selected datastore.

f. Review the warning:

```
vRealize Automation 7.0.1 does not have the ability to do an automated import. Submitting this request will create a new Virtual Machine in the vCenter, however an administrator will need to use the bulk import capability to manually import this machine.
```

g. If you accept the warning, click **Submit.**

The size of the deleted virtual machine that you are restoring directly affects the length of time that is required to complete the restore. The larger the machine, the more time it takes.

8. When the workflow completes, you can perform one or both of the following:
 - a. Open vCenter to verify that the machine was created in the expected location.
 - b. Bulk Import the restore into vRealize Automation. The VMware documentation at the following [link](#) provides more information.

CHAPTER 4

Business Group User Operations

This chapter includes the following topics:

- [Provisioning a protected virtual machine](#)..... 66
- [Data protection actions](#)..... 67
- [Restore actions](#)..... 69
- [Expiring or destroying a virtual machine](#)..... 72

Provisioning a protected virtual machine

You can provision a protected virtual machine by requesting a blueprint that has a data protection policy assigned to it. Depending on how the tenant administrator configured the blueprint, a policy that is used to protect the machine may or may not be selectable. If the policy is not selectable during provisioning, a policy that is pre-selected by the administrator is applied to the virtual machine by default.

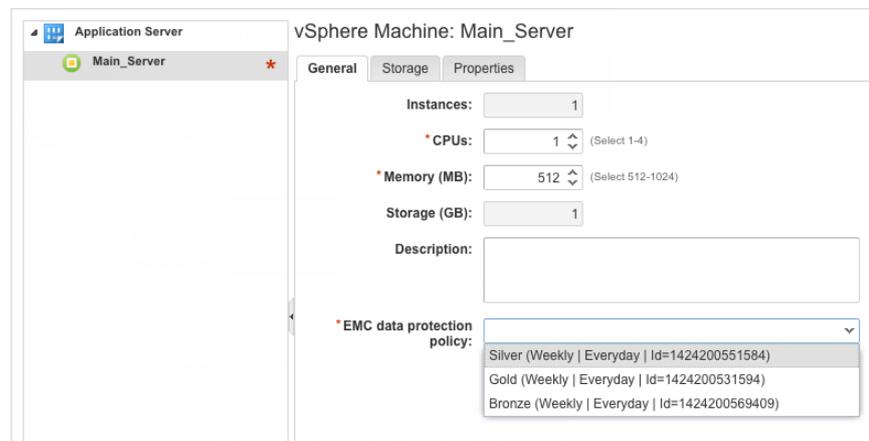
Procedure

1. In vRealize Automation, select the **Catalog** tab.
2. In the list of service catalogs, locate a blueprint that contains data protection, and click the blueprint's **Request** button.

The **New Request** page for the blueprint displays.

If the blueprint contains selectable policies, you can select one from the **EMC data protection policy** drop-down list as shown in the following figure.

Figure 21 Select policy for the blueprint



If a policy is not selectable on this page, that means that a policy has already been configured for the blueprint and is applied by default to the virtual machine that you are provisioning.

3. Optionally, change any of the remaining values on the **New Request** page as needed.
4. Click **Submit**.
5. To close the request confirmation message, click **OK**.
6. If you want to monitor the status of the provisioning request, select the **Requests** tab.

To refresh the page, click the **Refresh** button at the bottom of the page.

Results

After the virtual machine has been provisioned successfully, it will be listed in the **Machines** list on the **Items** tab. The remaining sections in this chapter describe the data protection and restore actions that you can perform on the virtual machine.

Data protection actions

This section describes the EMC vRealize Data Protection Extension actions that the business group user can perform. These tasks include:

- Adding data protection to a virtual machine
- Running data protection on a virtual machine
- Viewing the protection status of a virtual machine
- Removing data protection from a virtual machine

Adding data protection to a virtual machine

The steps in the following procedure describe how to add data protection to an existing, unprotected virtual machine by adding one, or more protection policies.

Before you begin

Procedure

1. In vRealize Automation, select the **Items** tab.
2. In the **Machines** list, click the row of the virtual machine to which you want to add data protection.

The row is highlighted.

3. Click **Actions**, and select **Add data protection** from the menu.

The **Add data protection** page displays.

4. Select a policy from the list of policies, and click **Submit**.
5. To close the request confirmation message, click **OK**.
6. If you want to monitor the status of the request, select the **Requests** tab.

To refresh the information, click the **Refresh** button at the bottom of the page.

Running data protection on a virtual machine

The steps in the following procedure describe how to perform an immediate backup of a virtual machine that has been provisioned.

Before you begin

The virtual machine must have a policy assigned to it.

Procedure

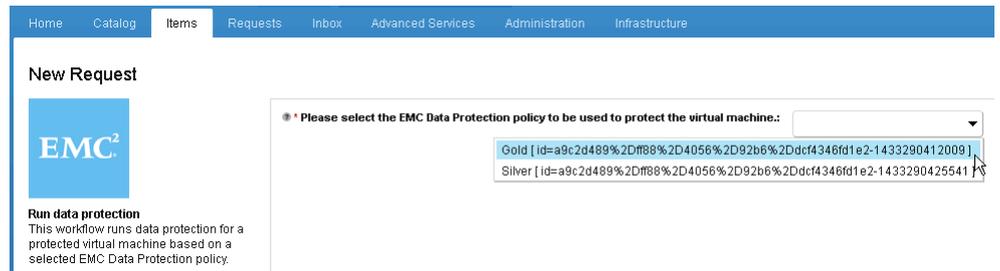
1. In vRealize Automation, select the **Items** tab.
2. In the **Machines** list, click the row of the virtual machine that you want to back up.

The row is highlighted.

3. Click **Actions**, and select **Run data protection** from the menu.

The **Run data protection** page displays.

4. Select a policy from the list, and click **Submit**.

Figure 22 Select policy to run data protection

5. To close the request configuration message, click **OK**.
6. If you want to monitor the status of the request, select the **Requests** tab.
To refresh the status, click the **Refresh** button.

Viewing the protection status of a virtual machine

The steps in the following procedure describe how to view the protection status of a virtual machine.

Procedure

1. In vRealize Automation, select the **Items** tab.
2. In the **Machines** list, click the row of the virtual machine for which you want to view protection status.
The row is highlighted.
3. Click **Actions**, and select **View protection status** in the menu.
The **View protection status** page displays with the machine's protection status.

Removing data protection from a virtual machine

The steps in the following procedure describe how to remove data protection from a virtual machine that has already been provisioned.

Procedure

1. In vRealize Automation, select the **Items** tab.
2. In the **Machines** list, click the row of the virtual machine from which you want to remove data protection.
The row is highlighted.
3. Click **Actions**, and select **Remove data protection** from the menu.
The **Remove data protection** page displays.
4. Click the checkbox beside one or more of the policies that you want to remove from the virtual machine.
5. Click **Submit**.
6. To close the request confirmation message, click **OK**.

Restore actions

This section describes the restore operations that the business group user can perform. These actions include restoring a virtual machine to its original location or to a new location, and restoring individual files.

Restoring a virtual machine to its original location

The steps in the following procedure describe how to restore a backup of a virtual machine to its original location.

Before you begin

The virtual machine that you plan to restore must have an existing image-level backup to Avamar. Virtual machines that are backed up using an Avamar application-consistent policy are not available and must be restored by using the Avamar data protection system.

Procedure

1. In vRealize Automation, select the **Items** tab.
2. Click the row of the machine whose backup you want to restore.
The row is highlighted.
3. From the **Actions** menu, select **Restore data**.
The **Restore data** page displays.
4. In the **Restore data** page, you can search for backups by date range, and you can limit the number of backups that are listed.
 - a. If you want to filter the backups by date range, select **Yes**, and select the **Start Date** and time and the **End Date** and time.
 - b. Select the maximum number of backups that you want to view.
 - c. To display the backups that match the filter criteria, click the **Backup** drop-down list.
 - d. Select the backup that you want to restore.
5. Accept **Yes** or select **No** as needed for the power off and power on options.
6. Click **Submit**.
7. To close the request confirmation message, click **OK**.
8. Select the **Requests** tab, and monitor the restore progress until it completes successfully.

Restoring a virtual machine to a new location

The steps in the following procedure describe how to restore a backup of a virtual machine to a location that is different from the location of the original machine. When you restore a backup to a new location, a new virtual machine is created on the vCenter and then imported back into vRealize Automation. When the restore completes, you can view the new virtual machine in the **Items** tab in vRealize Automation.

Before you begin

The virtual machine that you plan to restore must have one or more existing image level backups to Avamar. Virtual machines that are backed up using an Avamar application-consistent policy, are not available.

Procedure

1. In vRealize Automation, select the **Items** tab.
2. Click the row of the machine whose backup you want to restore.
The row is highlighted.
3. From the **ACTIONS** menu, select **Restore to new**.
The **Restore to New** page displays.
4. In the **Restore to New** page, you can search for backups by date range, and you can limit the number of backups that are listed.
 - a. If you want to filter the backups by date range, select **Yes**, and select the **Start Date** and time and the **End Date** and time.
 - b. Select the maximum number of backups that you want to view.
 - c. To display the backups that match the filter criteria, click the **Backup** drop-down list.
 - d. Select the backup that you want to restore.
When you select a backup, the new virtual machine name is provided automatically. If you prefer, you can change the name.
5. Click **Next** and review the warning message:

```
vRealize Automation 7.0.1 does not have the ability to do an automated import. Submitting this request will create a new Virtual Machine in the vCenter, however an administrator will need to use the bulk import capability to manually import this machine.
```

6. If you accept the warning, click **Submit**.
7. To close the request confirmation message, click **OK**.
8. To view the progress of the restore, select the **Requests** tab.
9. When the restore completes successfully, an administrator can perform one or both of the following:
 - a. Open vCenter to verify that the machine was created in the expected location.
 - b. Bulk Import the restore into vRealize Automation. The VMware documentation at the following [link](#) provides more information.

File-level restore

You can restore individual files or a directory from a virtual machine backup by using the **EMC Data Protection Restore Client**.

Before you begin

The virtual machine that you plan to restore must have one or more existing image level backups to Avamar. Virtual machines that are backed up using an Avamar application-consistent policy, are not available.

Procedure

1. In vRealize Automation, select the **Items** tab.
2. In the **Machines** list, click the row of the virtual machine from whose backup you want to restore a file.
The row is highlighted.
3. From the **Actions** menu, select **File level restore**.
The **File level restore** page displays, open on the **Select Backup** tab.
4. In the **Select Backup** tab, you can search for backups by date range, and you can limit the number of backups that are listed.
 - a. If you want to filter the backups by date range, select **Yes**, and select the **Start Date** and time and the **End Date** and time.
 - b. Select the maximum number of backups that you want to view.
 - c. To display the backups that match the filter criteria, click the **Backup** drop-down list.
 - d. Select the backup that you want to restore.

When you click **Next**, the **Browse FLR** tab displays with a URL to open the **EMC Data Protection Restore Client**.

5. To open the **EMC Data Protection Restore Client** in a new tab or window, right-click the URL.
6. Log in as one of the following:
 - If you are using a Microsoft Windows system, log in as Administrator.
 - If you are using a Linux system, log in as root.

The **Select items to restore** panel opens. It contains the selected backup.

7. To display its top-level item in the right-hand pane, click the backup
8. In the right-hand pane, browse to the file or directory that you want to restore, and double-click the item.

The file or directory name turns green, and the **Next** button becomes active.

9. Click **Next**.

The **Restore options** panel opens.

10. Select the client in the left pane, and then browse to the location to which you want to restore the file or directory.

11. Click **Finish**.

Click **Yes** in the **Restore Confirmation** message box.

12. To display the **Restore Monitor**, click the arrow that is located in the lower right-hand corner of the **EMC Data Protection Restore Client** window.

The **Restore Monitor** expands up from the bottom. Click the **Refresh** button on the right side of the monitor as needed.

Expiring or destroying a virtual machine

The steps in this procedure describe how to expire or destroy a virtual machine. To perform these standard vRA machine actions, you must have the appropriate entitlements. Otherwise, these actions do not display in the **Items** tab.

Procedure

1. In vRealize Automation, select the **Items** tab.
2. In the **Machines** list, click the row of the virtual machine that you want to expire or destroy.

The row is highlighted.

3. Click **Actions**, and select either **Expire** or **Destroy** from the menu.

A confirmation message displays.

4. Select the **Deployments** tab to view a tree structure of the machine(s) in each executed blueprint. You can select a deployment and click the **Destroy** action to delete all the machines in the deployment, or you can select individual machine(s) of the deployment and click the **Destroy** action.
5. Click **Submit**.
6. To close the request confirmation dialog box, click **OK**.

Results

Data protection is not removed when the virtual machine is expired. It is removed when the virtual machine is destroyed. The virtual machine can expire and be archived before it is destroyed, but the EMC vRealize Data Protection Extension retires the client and removes the policy only when the machine is destroyed.

CHAPTER 5

Logging and Supportability

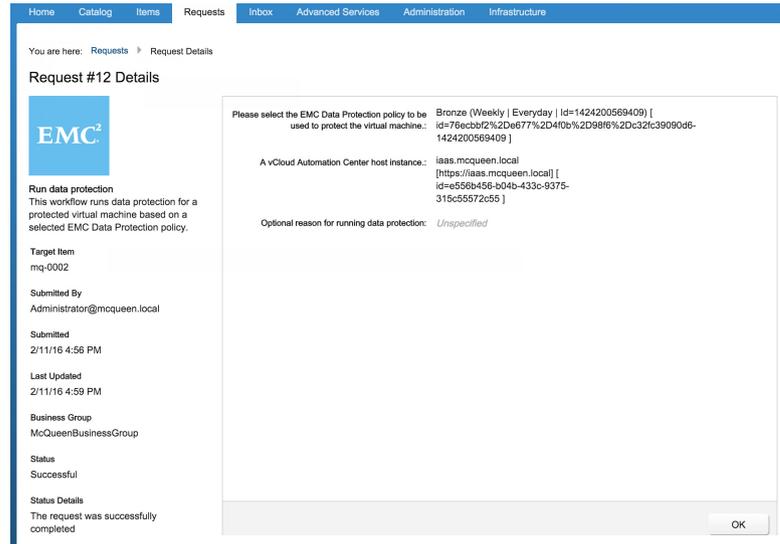
This chapter includes the following topics:

- [Monitoring status](#)..... 74
- [Event and error message codes](#)..... 75
- [Avamar Client activity window](#)..... 76
- [Single-click log capturing and packaging](#)..... 76
- [Log locations](#)..... 77

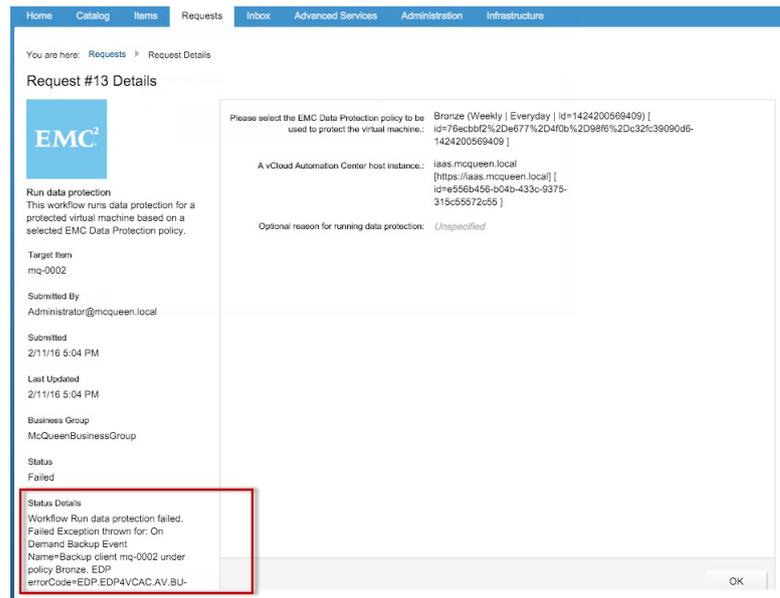
Monitoring status

You can monitor the status of the requests and view request details from the **Requests** tab in vRealize Automation Center.

The following figure shows status details for a successful request.
Figure 23 Successful request in vRA



The following figure shows status details for a request failure.
Figure 24 Failed request in vRA



Check the status details shown in the text area that is highlighted in the figure above to determine the meaning of the error and use the information for troubleshooting.

Event and error message codes

The following table lists the events and error codes that exist for the EMC vRealize Data Protection Extension.

Note

in the following error codes, {provider} indicates the data protection system (Avamar).

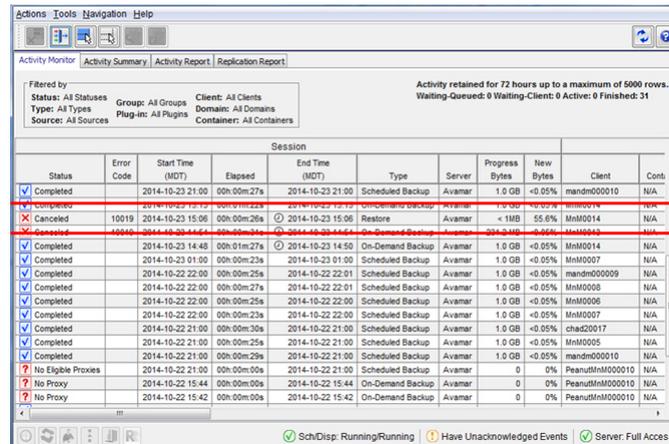
Table 7 Event and error codes

Error code	Description
EDP.EDP4VCAC. {provider}.BU-000005	EDP: General error from the EMC vRealize Data Protection Extension. Please check data protection for details.
EDP.EDP4VCAC. {provider}.BU-000010	EDP: Backup cancelled and failed to backup client.
EDP.EDP4VCAC. {provider}.BU-000030	EDP: Backup failed with backup operation error.
EDP.EDP4VCAC. {provider}.BU-000040	EDP: One or more disks protected by backup policy may have been migrated to new datastores. Please edit the backup job and verify the correct disks are still protected.
EDP.EDP4VCAC. {provider}.BU-000050	EDP: Backup failed because policy was disabled.
EDP.EDP4VCAC. {provider}.RST-000200	EDP: Restore cancelled, check data protection provider for underlying reason.
EDP.EDP4VCAC. {provider}.RST-000210	EDP: Restore failed, check data protection provider for underlying reason.
EDP.EDP4VCAC. {provider}.RST-000220	EDP: Restore failed because client is running.
EDP.EDP4VCAC.{provider}. RST-000230	EDP: Restore failed because disk restore step failed. Please verify disks in backup and try again.

Avamar Client activity window

In addition to monitoring the status through the vRealize Automation Requests details, you can log in to the Avamar UI and view status details from the Activity Monitor.

Figure 25 Avamar Client activity window



Single-click log capturing and packaging

Log bundling occurs in two areas of the product: vRealize Automation and Avamar. The EMC vRealize Data Protection Extension logs are included in the bundling facility of vRealize Automation.

vRealize Automation log bundling

vRealize Automation has a log bundle facility separate from Avamar log bundling.

You can export vRealize Orchestrator log and configuration settings using the **Export logs and application settings** vRealize Orchestrator workflow, which is located in / Library/Troubleshooting.

Please reference vRealize Automation documentation for log bundling specifics.

The following procedure describes how to collect the log bundle manually when using a vRealize Automation appliance.

Procedure

1. Log in to the vRealize Automation appliance management site.
2. Click the **Admin** tab on the menu bar.
3. Click the **Logs** tab.
4. Click **Save log files**.
5. Click **Download** and save the file to the system.

vRealize Orchestrator log bundling

You can collect the vRealize Orchestrator log files from vRealize Orchestrator Configuration.

Procedure

1. Log in to vRealize Orchestrator Control Center at:

```
http://<orchestrator_server_ip_address>:8283/vco-controlcenter
```

2. Click **Export logs**.

The system generates a .zip file bundle that you can download and save locally.

Log locations

The following table contains log descriptions and locations for the EMC vRealize Data Protection Extension and the Avamar system.

The most up-to-date log information is provided at the following links:

- [Default log locations](#)
- [Log locations for VMware vRealize Automation 7.x](#)

Table 8 Default log locations

vRealize Automation component log description	Default log location
laaS installation configuration logs	C:\Program Files (x86)\VMware\VCAC\Server\ConfigTool\Log
laaS Manager Server logs	C:\Program Files (x86)\VMware\VCAC\Server\Logs
laaS Model Manager Web (Repository) logs	C:\Program Files (x86)\VMware\VCAC\Server\Model Manager Web\Logs
laaS Distributed Execution Manager (DEM) Orchestrator and Worker logs	C:\Program Files (x86)\VMware\VCAC\Distributed Execution Manager\atdh1-ms1-70.sqa.local DEO\Logs
laaS Proxy Agent logs	C:\Program Files (x86)\VMware\VCAC\Agents\Agent_Name\Logs
vRealize Automation Identity Appliance logs	/var/log/vmware/sso/
vRealize Automation Appliance logs	/var/log/vmware/vcac/
vRealize Automation Appliance Apache error log	/var/log/apache2/error_log
vRealize Automation Appliance Upgrade logs	/opt/vmware/var/log/vami/
vRealize Orchestrator Appliance	In the vRealize Orchestrator Appliance (and the vRealize Orchestrator in the vRealize Automation Appliance),

Table 8 Default log locations (continued)

vRealize Automation component log description	Default log location
	<p>both the vRealize Orchestrator server and configuration server use tomcat logging, so the logs are in:</p> <ul style="list-style-type: none"> • /var/lib/vco/app-server/logs, which is sym-linked to /var/log/vmware/vco/app-server/ • /var/lib/vco/configuration/logs, which is sym-linked to {{/var/log/vmware/vco/configuration/}}. Mostly you will look in catalina.out. • vRealize Automation is similar: /var/lib/vcac/logs, which is sym-link'ed to /var/log/vmware/vcac.
Avamar log description	Avamar log location
Avamar MCS	/usr/local/avamar/var/mc/server_log/mcserver.log.x
Avamar GSAN	/data01/cur/gsan.log
Avamar documentation	https://support.emc.com/products/759_Avamar-Server/Documentation

CHAPTER 6

Troubleshooting

This chapter includes the following topics:

- [General Troubleshooting](#)..... 80
- [Items to investigate when data protection is not added](#)..... 80
- [Troubleshooting the EMC vRealize Data Protection Extension](#)..... 80
- [Checking the EMC vRealize Data Protection Extension configuration](#)..... 83

General Troubleshooting

Infrastructure administrators can obtain detailed failure status in the following locations in vRealize Automation:

- **Infrastructure > Recent Events**
- **Infrastructure > Monitoring > Logs**

Note

Non-Infrastructure administrators can use the **View protection status** action to see if the assignment occurred, but cannot see the logs.

Items to investigate when data protection is not added

Investigate the following items if a virtual machine is successfully provisioned but data protection is not added.

- Is the data protection system up and running?
- Does the policy exist in Avamar in the right tenant domain under the correct vCenter client? See [Avamar domains for tenant data protection policies](#) or [Tenant and EMC vRealize Data Protection Extension configurations](#) for more information.
- Is the environment configured correctly? In the vRealize Orchestrator client, select the **Workflows** tab, browse to `/Library/EMC/Data Protection/vRA`, and run the **Check EMC data protection configuration** workflow. To see if there are any errors or warnings, check the logs.

Troubleshooting the EMC vRealize Data Protection Extension

The following are known issues that you may encounter when working with vRealize Automation components.

Avamar policies do not display when running Setup a Data Protection Property Group or Add Data Protection workflows

A recently added, modified or deleted Avamar policy may not immediately display in the vRA policy lists when running the **Setup a Data Protection Property Group** or **Add Data Protection** workflows.

You can either wait for a few minutes or perform the following steps if you require these policies to display immediately.

Log into the vRealize Orchestrator client and refresh using the following steps:

1. Select the **Inventory** tab.
2. Select the EMC Data Protection top node.
3. Click the **Refresh** button at the top right corner.

Alternatively, you can log into the vRealize Orchestrator client and flush the cache using the following steps:

1. Select the **Workflows** tab.
2. Navigate to **EMC > Data Protection > vRO > Utilities**.
3. Run **Flush cached data** or **Flush cached data on system**.

Null error when provisioning from blueprint with deleted policy

When it is discovered that a virtual machine is not protected by the data protection system as expected, there may have been a change to the underlying data protection system itself.

The vRealize Automation user provisions a virtual machine, which uses a build profile configured with the data protection policy.

The result of the provisioning request: **Success**.

The cause of the error: A change to the underlying data protection system has removed the policy attached to the blueprint. Protection cannot be added to the virtual machine and fails.

The protection failure is NOT a hard failure for the provisioning request. At the version level of the system, there is no way to show a warning through the UI of the vRealize Automation system.

Therefore, a message is logged in the `catalina.out` log file of the vRealize Orchestrator system. The vRealize Data Protection Extension logs the following message:

```
[McsdkProtectionProvider] EDP: Backup Policy could not be found
and may have been deleted.
```

No available policy found from virtual machine properties when there is no EDP system

When it is discovered that a virtual machine is not protected by the data protection system as expected, the underlying data protection system may not be available.

The vRealize Automation user provisions a virtual machine, which uses a build profile configured with the data protection policy.

The result of the provisioning request: **Success**.

The cause of the error: The underlying data protection system has either been removed or is not functional. Protection cannot be added to the virtual machine and fails.

The protection failure is NOT a hard failure for the provisioning request. At the version level of the system, there is no way to show a warning through the UI of the vRealize Automation system.

Therefore, a message is logged in the `catalina.out` log file of the vRealize Orchestrator system. The vRealize Data Protection Extension logs the following message:

```
EDP Provider is null.
No available policy found from VM properties of <VM-name>,
skipping protection policy assignment.
```

vRealize Automation event subscriptions

The vRealize Data Protection Extension uses a new method introduced in vRealize Automation 7 called event subscriptions.

In vRealize Automation, **Administration > Events > Event Logs** lists all events in the vRealize Automation system, including machine workflows.

For Provisioning, events with descriptions of "Workflow 'Machine provisioned subscription' has started" and "Workflow 'Machine provisioned subscription' has completed" appear.

For Destroy, events with descriptions of "Workflow 'Machine unprovisioned subscription' has started" and "Workflow 'Machine unprovisioned subscription' has completed" appear.

Virtual machine is not added to application policy if agent in virtual machine is not activated

Occasionally, the virtual machine may not be added to an application policy for application data protection after provisioning, or an **Add data protection** resource action may fail to add the virtual machine to an application policy for application data protection.

This occurs when the agent in the virtual machine is not activated, due to the following reasons:

- The virtual machine may not be on the network
- The virtual machine may not have a hostname configured. The configured hostname must be on DNS (Domain Name Service) for Avamar to communicate with the agent at the hostname
- The firewall on the virtual machine may be blocking port 28002. Avamar tries to communicate with the application agent on this port in the virtual machine, as described in the *Avamar Administrator's Guide* in the section "Client paging."

Exchange plug-in re-added in Avamar when client deleted using Avamar Administrator

When you use the **Avamar Administrator** GUI to delete an Exchange client activated with Avamar, Avamar automatically restores the Exchange plug-in under the `/clients` folder. For the EMC vRealize Data Protection Extension, you may not notice that this has occurred because the Extension searches for application clients under `/EDP/tenant_name` and not `/clients`.

This issue does not occur when the client is retired. EMC recommends that you retire the client using **Avamar Administrator** instead of deleting the client.

Checking the EMC vRealize Data Protection Extension configuration

The EMC vRealize Data Protection Extension provides a utility workflow that can diagnose some of the potential configuration issues between itself and vRealize Automation, vRealize Orchestrator, vCenter, and Avamar.

Procedure

1. Log in to the **vRealize Orchestrator** client.
2. Select the **Workflows** tab, and browse to the following location:
`Library/EMC/Data Protection/vRA`
3. Select the **Check EMC data protection configuration** workflow, and click the green arrow (▶) in the upper-left corner of the right-hand pane to start the workflow.
4. While the workflow is running, select the **Logs** tab to monitor its progress.

Results

If errors are discovered, the workflow run fails and errors are logged. If warnings are discovered, the workflow run passes and warning messages are logged. All errors and warnings display in the **Logs** tab and are written to the `/var/log/vco/app-server/server.log` file on the server running the vRealize Orchestrator instance (typically the vRealize Automation server machine).

Configuration checks performed by the EMC data protection configuration workflow

The **Check EMC data protection configuration** workflow runs the following configuration checks:

- Ensures that the required plug-ins and packages are installed. If the required plug-ins are not installed, the workflow fails immediately with a validation error. To see more information regarding the error:
 1. Select **Tools > User Preferences**.
 2. Select **Workflows**.
 3. Clear the selection for **Validate a workflow before running it** checkbox.
 4. Click **Save & Close**.
 5. Re-run the **Check EMC data protection configuration** workflow, which is located in `/Library/EMC/Data Protection/vRA`.
- Ensures that the vRA Infrastructure Administration and vCloud Automation Center connections are in the vRealize Orchestrator inventory. You can typically address these issues by running the following workflows in the specified order:
 - The **Add an IaaS host** workflow, which is located in `Library/vCloud Automation Center/Infrastructure Administration/Configuration/`.
 - The **Add a vRA host** workflow, which is located in `Library/vCloud Automation Center/Configuration`.
- Ensures that the vCenter Server connection(s) are in the vRealize Orchestrator inventory, and that they match up with the vSphere endpoint(s) configured in the

vRealize Automation Infrastructure configuration. To add missing vCenter Server connections to vRealize Orchestrator, run **Add a vCenter Server instance** workflow, which is located in `Library/vCenter/Configuration`.

- Ensures the machine lifecycle event subscriptions are configured in each tenant.
- Ensures that at least one vRealize Automation host per tenant has sufficient permissions to run the Data Protection Extension installation workflow.
- Ensures that any configured EMC data protection systems are valid and connected, and have protection policies.
- If there are clients in the EMC data protection systems, ensures that the *VirtualCenter.FQDN* field in the vSphere Client under **Administration > vCenter Server Settings > Advanced Properties** matches the vCenter server configured in the EDP Protection System.

You can run the **Check EMC data protection configuration** workflow multiple times as you correct issues with the configuration.

Error and warning messages

The following table lists error and warning messages that can occur when you run the **Check EMC data protection configuration** workflow, which is located in `Library/EMC/Data Protection/vRA`. It also provides a number of possible solutions that you can use to resolve the error and warning conditions.

Table 9 Error and warning messages

Messages	Type	Possible solution(s)
Missing vCAC Infrastructure plugin.	Error	<ul style="list-style-type: none"> • In vRealize Orchestrator client, select Help > Installed Plug-ins... and verify the vCAC plug-in is installed. • Install the VMware vCenter Orchestrator Plug-In for vCloud Automation Center from VMware.com.
Missing vCAC Cafe plugin.	Error	<ul style="list-style-type: none"> • In vRealize Orchestrator client, select Help > Installed Plug-ins... and verify the vCACCAFE plug-in is installed. • Install the VMware vCenter Orchestrator Plug-In for vCloud Automation Center from vmware.com.
Missing EDP plugin.	Error	<ul style="list-style-type: none"> • In vRealize Orchestrator client, select Help > Installed Plug-ins... and verify the EDP plug-in is installed. • Install the EMC vRealize Data Protection Extension from emc.com.
Missing default IaaS host in vCO inventory.	Error	To add the host to vRealize Orchestrator, run the <code>Library/vCloud Automation Center/Infrastructure Administration/Configuration/Add an IaaS host</code> workflow.
Found <X> IaaS hosts in vCO inventory, with <Y> not connected to <vcac-	Warning	To remove the other hosts from vRealize Orchestrator, run the <code>Library/vCloud Automation Center/Infrastructure</code>

Table 9 Error and warning messages (continued)

Messages	Type	Possible solution(s)
url>. Only the '<vcac-name>' host is used, which might not be the expected one.		Administration/Configuration/Remove an IaaS host workflow.
Failed to get provisioning groups from IaaS host <vcac-url>, other operations might not work.	Error	<ul style="list-style-type: none"> Verify that the IaaS server is running and accessible. Restart, if needed. Verify that the IaaS server connection is in the Inventory tab of the vRealize Orchestrator client, under vCAC Infrastructure Administration. Check the log files on the IaaS server.
Unexpected exception checking vCAC hosts: <error>	Error	<ul style="list-style-type: none"> Verify that the IaaS server is running and accessible. Restart, if needed. Check the log files on the vRealize Orchestrator server for more information related to the error. Check the log files on the IaaS server.
Missing default vCAC cafe host in vCO inventory.	Error	To add a vsphere.local tenant host to vRealize Orchestrator, run the Library/vCloud Automation Center/Configuration/Add a vCAC host workflow.
Found <X> 'vsphere.local' tenant vCAC cafe hosts in vCO inventory, with <Y> not connected to <cafe-url>.	Error	To remove the other hosts from vRealize Orchestrator, run the Library/vCloud Automation Center/Configuration/Remove a vCAC host workflow.
Found <X> 'vsphere.local' tenant vCAC cafe hosts in vCO inventory, but they point to same vcac url which should work fine. This can occur when vCAC 6.1+ creates the 'Default' vCAC cafe host connections.	Warning	To remove the other hosts from vRealize Orchestrator, optionally run the Library/vCloud Automation Center/Configuration/Remove a vCAC host workflow.
No vCenter connections found in vCO inventory.	Error	To add the vCenter server connection(s) to vRealize Orchestrator, run the Library/vCenter/Configuration/Add a vCenter Server instance workflow.
Malformed endpoint URL '<vsphere-endpoint-url>': must be of type: https://hostname/sdk or https://IP_Address/sdk.	Warning	Verify and fix the vSphere endpoint URL in the vRealize Automation Infrastructure tab.

Table 9 Error and warning messages (continued)

Messages	Type	Possible solution(s)
Failed to find vCenter connection in vCO matching '<vsphere-endpoint-url>' vSphere endpoint in IaaS host '<vcac-name>'.	Warning	<ul style="list-style-type: none"> To add the vCenter server connection to vRealize Orchestrator, run the <code>Library/vCenter/Configuration/Add a vCenter Server instance workflow</code>. To update the vCenter server connection in vRealize Orchestrator to match what is configured in the vRealize Automation Infrastructure tab, run the <code>Library/vCenter/Configuration/Update a vCenter Server instance workflow</code>.
vCenter endpoint in IaaS host '<vcac-name>' has invalid uri '<vsphere-endpointurl>'.	Warning	Verify and fix the vSphere endpoint URL in the vRealize Automation Infrastructure tab.
Failed to find vSphere endpoints in IaaS host '<vcac-name>'.	Warning	Create the vSphere endpoint(s) in the vRealize Automation Infrastructure tab.
Unexpected exception checking IaaS vSphere connection endpoints: <error>	Error	<ul style="list-style-type: none"> Verify the IaaS server is running and accessible. Restart, if needed. Check the log files on the vRealize Orchestrator server for more information related to the error. Check the log files on the IaaS server.
Failed to find the vCenter hostname and IP information:<vcenter>	Warning	<ul style="list-style-type: none"> Verify the vCenter connection information in the vRealize Orchestrator client Inventory tab, under vCenter Server. To correct the vCenter Server information for the connection in vRealize Orchestrator, run the <code>Library/vCenter/Configuration/Update a vCenter Server instance workflow</code>.
No EdpSystems have been configured for data protection.	Warning	<ul style="list-style-type: none"> Use the Add a tenant data protection system catalog item in vRealize Automation, if you already ran the install workflow for the tenant. To configure a vRealize Automation tenant, including the data protection system, run the <code>Library/EMC/Data Protection/vRA/Installation/Install default setup for tenant workflow</code>. To configure a data protection system instance for a vRealize Automation tenant, without doing the other tenant setup steps, run the <code>Library/EMC/Data Protection/vRA/Installation/Utilities/Create or</code>

Table 9 Error and warning messages (continued)

Messages	Type	Possible solution(s)
		<p>update a tenant data protection system workflow.</p> <ul style="list-style-type: none"> To manually setup a data protection system, run the <code>Library/EMC/Data Protection/vRO/Configuration/Add a data protection system workflow</code>.
Avamar EdpSystem '<name>' (<host>) has no available policies.	Warning	Create the Backup Groups in the appropriate <tenant>_<vrealize-host> subdomain of each vCenter client domain in Avamar.
Avamar EdpSystem '<name>' (<host>) is enabled but disconnected.	Warning	<ul style="list-style-type: none"> Verify that the Avamar server, including the MCS, is running and accessible. Check the description of the connection in the vRealize Orchestrator client Inventory tab under EMC Data Protection, which shows any error that occurred at connection startup. Check the logs files on the vRealize Orchestrator server for more information related to the error.
Failed to find a matching vCenter for the vCenter configured in the EdpServer: <name>. EdpServer FQDN=<vcenter-hostname>. vCenter FQDN(s)=<vcenter-hostname>. Please check the VirtualCenter.FQDN setting in the vCenter Advanced Properties	Warning	<ul style="list-style-type: none"> To add the vCenter server connection to vRealize Orchestrator, run the <code>Library/vCenter/Configuration/Add a vCenter Server instance workflow</code>. To update the vCenter server connection in vRealize Orchestrator to match what is configured in the Avamar server, run the <code>Library/vCenter/Configuration/Update a vCenter Server instance workflow</code>. Verify or update the <code>VirtualCenter.FQDN</code> setting in the Advanced Properties of the vCenter server settings in the vSphere web client to match what is configured in the Avamar server.
Unable to get policies from Avamar EdpSystem '<name>' (<host>): <error>	Error	<ul style="list-style-type: none"> Verify that the Avamar server, including the MCS, is running and accessible. Check the logs files on the vRealize Orchestrator server for more information related to the error.
Unexpected exception checking EdpSystems: <error>	Error	Check the logs files on the vRealize Orchestrator server for more information related to the error.
Unable to find vRealize Automation machine provisioning event subscription for '<tenant>' tenant EMC data	Warning	Run the installation for the tenant, if not done already, and then update the default setup for the tenant.

Table 9 Error and warning messages (continued)

Messages	Type	Possible solution(s)
protection system(s), or Unable to find vRealize Automation machine unprovisioning event subscription for '<tenant>' tenant EMC data protection system(s).		
Unexpected exception checking vRealize Automation event subscriptions: <error>	Error	Check the log files on the vRealize Orchestrator server for more information.
None of the <n> vRealize Automation hosts for tenant '<tenant>' appear to have the Infrastructure Architect, Tenant Administrator, and XaaS Architect roles. The EMC data protection default tenant setup workflows requires a vRealize Automation host with a user configured with those roles.	Error	Verify that the Roles of the user(s) of the vRealize Automation hosts.