

VMware Aria Suite Lifecycle Installation, Upgrade, and Management Guide

October 2023

VMware Aria Suite Lifecycle 8.14

You can find the most up-to-date technical documentation on the VMware by Broadcom website at:

<https://docs.vmware.com/>

VMware by Broadcom

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

Copyright © 2023 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to <https://www.broadcom.com>. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies. [Copyright and trademark information](#).

Contents

What is VMware Aria Suite Lifecycle 9

1 Installing VMware Aria Suite Lifecycle 10

System requirements for VMware Aria Suite Lifecycle 10

VMware Aria Suite Lifecycle ports 12

Installing VMware Aria Suite Lifecycle and VMware Aria Suite applications 14

How to run the VMware Aria Suite Lifecycle Easy Installer for VMware Aria Automation and VMware Workspace ONE Access 14

Install and configure VMware Identity Manager 15

Install applications using the Lifecycle Operations service 17

Prepare to install and deploy products 18

Installing VMware Aria Suite Lifecycle with Easy Installer for VMware Aria Automation and Workspace ONE Access 19

Install VMware Workspace ONE Access 20

Install VMware Aria Automation 22

Migrate applications using the Lifecycle Operations service 23

Migrate from an earlier version of VMware Aria Suite Lifecycle to the current version 23

Download and run the Easy Installer 24

Install VMware Aria Suite Lifecycle 25

Migrate to the current version of VMware Aria Suite Lifecycle 26

Log in to VMware Aria Suite Lifecycle 27

Overview My Services dashboard 27

Displaying notifications 29

Configuring SMTP for email outbound notifications 29

Creating incoming webhooks for Slack and Teams channels in VMware Aria Suite Lifecycle 30

Configuring outbound notifications 31

Participating in the Customer Experience Improvement Program 31

2 Configuring VMware Aria Suite Lifecycle 33

Configure settings 33

Configuring an authentication provider in VMware Aria Suite Lifecycle 35

Configure a network proxy 35

Configure Your System 36

Activate or deactivate SSH on VMware Aria Suite Lifecycle 36

Working with VMware Aria Suite Lifecycle logs 37

Setting your VMware Aria Suite Lifecycle time 41

Federal Information Processing Standard (FIPS) 140-2 support 41

- Configure NTP servers 42
 - Configure NTP settings post-deployment 42
- Configure DNS servers in VMware Aria Suite Lifecycle 43
- Data source using SNMP configurations for VMware Aria Operations for Networks 43
 - Add SNMP Configuration 44
- Working with product support 44
 - Configure product binaries 44
 - Patching products by using VMware Aria Suite Lifecycle 46
 - Configure your patched product binaries 46
 - Run a script to address issues in your environment 47
 - Register with My VMware 49
- Manage certificates 51
 - Assign the certificate administrator role 53
 - Replace your VMware Identity Manager certificate 53
 - Replace your self-signed certificate 71
 - Replace your custom certificate 71
- Manage licenses 72
- Manage passwords 73
- Add and manage data center associations 75
 - Assign a user role in a vCenter 75
 - Add a vCenter to a data center 77
 - Remove a vCenter from a data center 78
 - Install and configure on VMware Cloud on AWS 78
- Add an NSX load balancer 79
- Working with the Identity and Tenant Management service 80
 - Manage directories for VMware Identity Manager 82
 - Assign user roles and manage users 83
 - Add Active Directory over LDAP 84
 - Add Active Directory with integrated Windows authentication 87
- Tenant management 89
 - Multi-tenancy overview 90
 - Multi-tenancy model 92
 - Enable multi-tenancy 98
 - Manage tenants 99
- Tenant migration 103
 - Migrating VMware Workspace ONE Access tenants 103
 - Merging VMware Aria Automation tenants and directories 105
- 3 Creating a VMware Identity Manager environment 107**
 - Create a new private cloud environment using the installation wizard 107
 - Install VMware Identity Manager 110

Configure environment settings for a new private cloud	111
Install VMware Aria Suite products	111
Accept EULA and license selection	112
Configure certificate details	113
Configure infrastructure details	114
Configure binary mapping details	115
Configure network details	116
Configure product details	117
Configure VMware Aria Suite products for installation	119
Considerations for configuring VMware Aria Automation	121
Continuous availability for VMware Aria Operations	122
Allow continuous availability for VMware Aria Operations	122
Validate private cloud environment details	123
Pre-check validation	123
Replace VMware Aria Automation certificates	125
Confirm environment and installation settings	125
Import an existing environment using an installation wizard	126
Import a VMware Workspace ONE Access environment	127
Import a VMware Aria Automation environment	128
Import VMware Aria Automation Config	129
Import a VMware Aria Operations for Networks environment	129
Import a VMware Aria Operations environment	130
Import a VMware Aria Automation Orchestrator environment	131
Import a VMware Aria Operations for Logs environment	132
Create a private cloud environment using a configuration file	132
Create a hybrid environment using a cloud proxy	134
Configuring environment settings for a new cloud proxy	134
Installing cloud proxy products	135
Configuring cloud proxy product details	135
Upgrade your cloud extensibility proxy	136
Onboarding VMware Aria Universal Suite subscriptions	138
4 Managing environments	139
Day 2 operations for global environment in VMware Aria Suite Lifecycle	139
Resize hardware resources deployed for VMware Lifecycle Manager	141
Day 2 operations with other products in VMware Aria Suite Lifecycle	142
Reconfigure internal pods and service subnets	143
Add a product to an existing private cloud environment	144
Add a data source to an existing private cloud environment	144
Data operations supported by VMware Aria Operations for Networks	145
Import data sources in VMware Aria Suite Lifecycle	145

- Manage a data source in an existing private cloud environment 145
- Update bulk passwords for data sources 146
- Scale out VMware Identity Manager for high availability 147
 - Scheduled health checks 149
 - Scale out tenant-enabled Workspace ONE Access 149
 - Scaling a Windows connector 150
- Scale out VMware Aria Suite products 151
 - Scale out a tenant-enabled VMware Aria Automation environment 152
- Scale up VMware Aria Suite products 153
- Export a private cloud environment configuration file 154
- Download private cloud product logs 154
- Delete an environment 155
- Managing VMware Aria Suite products in a private cloud 156
 - Create and manage a product snapshot 157
 - Inventory synchronization in VMware Aria Suite Lifecycle 158
 - Product references for VMware Aria Suite Lifecycle 159
 - Change your password for products 159
 - Delete a product from an environment 160
 - Replace product certificates 161
 - Configure and replace product licenses 162
- Configure health monitoring for the VMware Aria Suite management stack 163
 - Monitoring content health status in VMware Aria Suite Lifecycle 164
 - View the SDDC Health Overview dashboard in VMware Aria Operations 164
 - Activate or deactivate product health checkin in VMware Aria Suite Lifecycle 165
- Adding and managing content from Marketplace 165
 - Find and download content from VMware Marketplace 165
 - View and upgrade your Marketplace content 166
 - Install a downloaded Marketplace content 167
 - Delete content downloaded from VMware Marketplace 167

5 Working with the Content Management service 169

- Working with content endpoints 171
 - Add a VMware Aria Automation Orchestrator content endpoint 173
 - Add a VMware Aria Automation content endpoint 175
 - Add a VMware Aria Automation cloud endpoint 176
 - Add a source control endpoint 177
 - Add a vCenter content endpoint in VMware Aria Suite Lifecycle 178
 - Add a VMware Aria Operations endpoint 179
 - Create an SSH user in VMware Aria Operations 180
 - Delete a content endpoint 180
 - Edit a content endpoint 180

- Managing VMware Aria Suite Lifecycle content 181
 - Add content 182
 - Delete multiple content names or versions 184
 - Working with captured content 184
 - Content actions 185
 - Available content types 185
 - Searching content 188
 - Test Content 188
 - Performing Unit Tests 188
 - Using content source control within VMware Aria Suite Lifecycle 191
 - Check in content to a source control endpoint 193
 - Check Out Content from a Source Control Endpoint 195
 - Deploy a content package 197
 - Managing multiple releases of a content package 197
 - Delete a content package 199
 - Recognizing potential content issues 199
- Access source control 199
- Managing source control server endpoints 200
 - Add a source control server endpoint 200
 - Delete a source control server endpoint 201
- Working with content settings 202
 - Configure pipeline stub 203
 - Map proxy setting 204
 - Content pipeline settings 205
- Content pipelines 206

6 Upgrading product versions in the Lifecycle Operations service 208

- Upgrade VMware Aria Suite Lifecycle 208
 - Support for additional product versions 210
- Upgrade your VMware Identity Manager 210
 - Migrating a Microsoft Windows connector 212
- Upgrade vRealize Automation 8.x or VMware Aria Automation by using VMware Aria Suite Lifecycle 213
 - VMware Aria Automation stages in VMware Aria Suite Lifecycle workflow 215
- Upgrade a VMware Aria Suite Product 216
 - Upgrade existing products using the pre-upgrade checker 218
 - Upgrade VMware Aria Operations 219
 - Upgrade VMware Aria Operations for Networks 221
 - Upgrade VMware Aria Operations for Logs 221
 - Upgrade VMware Aria Automation Config 222

7 Performing disaster recovery 224

8 Managing product licenses in the Locker 225

- Managing VMware Aria Universal Suite licenses in the Locker 225
 - Downloading usage report for VMware Aria Universal Suite licenses 227
- Activating VMware Aria Universal Suite licenses 227
- Day 2 operations for VMware Aria Universal Suite 228
- Day 2 operations for VMware Aria Universal Suite licenses 228

9 Troubleshooting 230

- Large VMware Aria Operations machine fails to power on 231
- Deployment fails during VMware Aria Operations for Logs clustering and VMware Workspace ONE Access registration 232
- Change in DNS server 233
- Wrong IP details specified during VMware Aria Suite Lifecycle deployment 233
- Binary mappings are not populated 234
- Content capture fails with secure field 234
- Fix errors using log files 234
- Cloud template capture fails 235
- Component profile deployment fails 235
- Update VMware Aria Suite Lifecycle host name 235
- Resource not found in directory management 236
- Capture, test, or release fails in VMware Aria Automation Orchestrator content 237
- Import or inventory sync of VMware Aria Suite fails 237
- Workspace ONE Access Day 2 operations fail when the root password expires 238
- Enable log rotation for pgpool logs on postgres clustered VMware Workspace ONE Access 238
- VMware Workspace ONE Access postgres cluster outage due to loss of delegate IP 239
- Importing VMware Aria Automation in VMware Aria Suite Lifecycle fails 240
- VMware Aria Suite Lifecycle displays older version after upgrade 241
- Disconnected licenses are not listed for reconnect 241

What is VMware Aria Suite Lifecycle

VMware Aria Suite Lifecycle provides a comprehensive solution for deploying, configuring, managing, and upgrading VMware Aria Suite products.

These products include VMware Aria Operations, VMware Aria Automation, VMware Aria Automation Orchestrator, VMware Aria Operations for Networks, and VMware Aria Operations for Logs.

VMware Aria Suite Lifecycle provides product installation and content lifecycle management capabilities to automate the deployment of VMware Aria Suite content across different environments.

As a VM administrator who is familiar with enterprise management applications and data center operations, you can install and manage VMware Aria Suite products by using VMware Aria Suite Lifecycle.

Use the VMware Aria Suite Lifecycle [Easy Installer](#) to install VMware Aria Suite Lifecycle, VMware Aria Automation, and Workspace ONE Access and then install other available VMware Aria Suite products.

Note While VMware Identity Manager has been officially renamed VMware Workspace ONE Access, VMware Aria Suite Lifecycle uses the VMware Identity Manager 3.3 clustered environment. VMware Aria Suite Lifecycle does not support VMware Workspace ONE Access 20.x and later.

You can find *VMware Identity Manager 3.3* product documentation on the [VMware Workspace ONE Access Documentation](#) landing page.

You can find VMware Aria Suite product documentation on the [VMware Cloud Management Suites Documentation](#) landing page.

Installing VMware Aria Suite Lifecycle

1

VMware Aria Suite Lifecycle helps you to install the VMware Aria Suite products in a shorter period than installing individual products. You can also manage and upgrade your VMware Aria Suite products by using VMware Aria Suite Lifecycle.

- [System requirements for VMware Aria Suite Lifecycle](#)

The following hardware and operating system requirements are required for VMware Aria Suite Lifecycle.

- [VMware Aria Suite Lifecycle ports](#)

This section provides a list of ports used by VMware Aria Suite Lifecycle for product and integration communication.

- [Installing VMware Aria Suite Lifecycle and VMware Aria Suite applications](#)

You can use one of the VMware Aria Suite Lifecycle installers to install the required VMware Aria Suite products.

- [Log in to VMware Aria Suite Lifecycle](#)

Log in to VMware Aria Suite Lifecycle to create and manage cloud environments with VMware Aria Suite Lifecycle.

- [Overview of the VMware Aria Suite Lifecycle My Services dashboard](#)

Access VMware Aria Suite Lifecycle services from the My Services dashboard.

- [Display notifications in VMware Aria Suite Lifecycle](#)

You can view VMware Aria Suite Lifecycle notifications for product updates and related information.

- [Participating in the Customer Experience Improvement Program for VMware Aria Suite Lifecycle](#)

This product participates in VMware's Customer Experience Improvement Program (CEIP).

System requirements for VMware Aria Suite Lifecycle

The following hardware and operating system requirements are required for VMware Aria Suite Lifecycle.

Requirements	VMware Aria Suite Lifecycle
Minimum software requirements	<ul style="list-style-type: none"> ■ vCenter 6.0 ■ ESXi version 6.0
Minimum hardware requirements	<ul style="list-style-type: none"> ■ 6 GB memory ■ 78 GB storage - Thick provision
Virtual CPU	2

Supported VMware Aria Suite products for installation, scale out, and upgrade

VMware Aria Suite Lifecycle supports the following VMware Aria Suite products:

- VMware Aria Automation
- VMware Aria Automation Config
- VMware Aria Operations
- VMware Aria Automation Orchestrator
- VMware Workspace ONE Access (VMware Identity Manager)
- VMware Aria Operations for Logs
- VMware Aria Operations for Networks

For related information about product and version support, see the [VMware Product Interoperability Matrix](#). The interoperability matrix provides details about supported product versions and their compatibility with VMware Aria Suite Lifecycle and with one another.

For more information about VMware Aria Suite, see [VMware Aria Suite Overview product documentation](#).

You can onboard a supported VMware Aria Suite product version in VMware Aria Suite Lifecycle and then upgrade that product by using VMware Aria Suite Lifecycle.

Supported VMware Aria Suite versions for imported products in VMware Aria Suite Lifecycle

VMware Aria Suite Lifecycle supports the following VMware Aria Suite products and product versions.

Also see the [VMware Product Interoperability Matrix](#).

- VMware Aria Automation
 - For older product versions, see earlier versions of this topic.
- VMware Aria Automation Config
 - For older product versions, see earlier versions of this topic.
- VMware Aria Operations

For older product versions, see earlier versions of this topic.

- VMware Aria Operations for Logs

For older product versions, see earlier versions of this topic.

- VMware Workspace ONE Access

VMware Identity Manager 3.3.x

While VMware Identity Manager has been officially renamed VMware Workspace ONE Access, VMware Aria Suite Lifecycle uses the VMware Identity Manager 3.3 clustered environment. VMware Aria Suite Lifecycle supports VMware Identity Manager 3.3 and later. VMware Aria Suite Lifecycle does not support VMware Workspace ONE Access 20.x and later. For more information, see *VMware Identity Manager 3.3* documentation at [VMware Workspace ONE Access Documentation](#).

- VMware Aria Operations for Networks

For older product versions, see earlier versions of this topic.

- VMware Aria Automation Orchestrator

For older product versions, see earlier versions of this topic.

For more information about product and version interoperability, see [VMware Product Interoperability Matrix](#). For more information, see VMware Aria Suite [product documentation](#).

VMware Aria Suite Lifecycle ports

This section provides a list of ports used by VMware Aria Suite Lifecycle for product and integration communication.

Note All the appliances require NTP and DNS access, therefore, you must open the NTP and DNS ports of each respective NTP and DNS server.

Note VMware Aria Suite Lifecycle is empowered with Common Appliance Platform (CAP), which replaces the VMware Appliance Management Interface (VAMI) for product installations and upgrades. CAP is an approach to standardize appliance management for all VMware appliances. CAP uses port 8000.

Table 1-1. Required ports and allowed endpoints for integration and communication with VMware services in Cloud

Service	TCP Port	Required allowed URL
My VMware	443	https://apigw.vmware.com
Marketplace	443	https://gtw.marketplace.cloud.vmware.com
Updates	443	https://vapp-updates.vmware.com
Compatibility	443	https://simsservice.vmware.com

Table 1-1. Required ports and allowed endpoints for integration and communication with VMware services in Cloud (continued)

Service	TCP Port	Required allowed URL
Patch and policy refresh repository	443	https://vrealize-updates.vmware.com
VMware Cloud	443	https://console.cloud.vmware.com
VMware Cloud API	443	https://api.mgmt.cloud.vmware.com
Subscriptions API	443	https://vconnect.vmware.com

Additional and required allowed URLs are listed in the following table.

My VMware API host names	Marketplace API host names	Marketplace API host URLs
apigw.vmware.com	marketplace.vmware.com	https://gtw.marketplace.cloud.vmware.com
download2.vmware.com download3.vmware.com	drd6c1w7be.execute-api.us-west-1.amazonaws.com (* .amazonaws.com)	https://cspmarketplacemainbuck.s3.us-west-2.amazonaws.com https://cspmarketplaceproductiondownloadable.s3.us-west-2.amazonaws.com and https://cspmarketplacemainbuck.s3.us-west-2.amazonaws.com
*.akamaiedge.net		

Note VMware Aria Suite Lifecycle always initiates the communication to retrieve or to send data to the VMware services. You can configure your network to permit outbound traffic and block inbound traffic to the specified port without impacting the VMware Aria Suite Lifecycle features that integrate with the VMware services.

Ensure that any downloads or API host URLs that are redirected from [VMware Marketplace](#) are allowed.

Table 1-2. Required ports for integration and communication with VMware on-premises products

Product or Integration	TCP Port Number
VMware Aria Automation appliance	8008, 443, 22
VMware Aria Operations analytics cluster appliances	443, 22
VMware Aria Operations remote collector appliances	443, 22
VMware Aria Operations for Logs appliances	443, 9543, 16520, 22
VMware Aria Operations for Networks	443, 22
Workspace ONE Access appliances	8443, 443, 22 5432, 9999, 9898, 9000, 9694 (Use these for a cluster) For related information, see KB 79163 .
VMware Aria Automation Orchestrator appliances	443
vCenter server instances	443

Table 1-2. Required ports for integration and communication with VMware on-premises products (continued)

Product or Integration	TCP Port Number
ESXi host instances	443
Content management host (GitLab)	443

Note ICMP protocol must be enabled between VMware Aria Suite Lifecycle and the products that are being managed.

For more information about ports, see the VMware Aria Suite Lifecycle [Security Hardening Guide](#) and the [VMware Ports and Protocol](#) tool. Also see the VMware [Product Interoperability Matrix](#).

Installing VMware Aria Suite Lifecycle and VMware Aria Suite applications

You can use one of the VMware Aria Suite Lifecycle installers to install the required VMware Aria Suite products.

- VMware Aria Suite Lifecycle VMware Aria Automation Easy Installer for VMware Aria Automation and VMware Workspace ONE Access: This installer helps to install VMware Aria Suite Lifecycle, VMware Aria Automation, and VMware Workspace ONE Access. The OVA bundle of this package contains the binaries for VMware Aria Suite Lifecycle, VMware Aria Automation, and VMware Workspace ONE Access.
- VMware Aria Suite Lifecycle VMware Aria Automation Easy Installer: This installer helps to install only VMware Aria Suite Lifecycle. This package contains the OVA bundle for only VMware Aria Suite Lifecycle.

You can download the executable file of one of these installers from the [VMware Customer Connect](#) download page.

How to run the VMware Aria Suite Lifecycle Easy Installer for VMware Aria Automation and VMware Workspace ONE Access

The VMware Aria Suite Lifecycle VMware Aria Automation Easy Installer for VMware Aria Automation and VMware Workspace ONE Access is downloadable from the VMware Customer Connect download page.

Procedure

- 1 Download the VMware Aria Suite Lifecycle VMware Aria Automation Easy Installer for VMware Aria Automation and VMware Workspace ONE Access executable file from the [VMware Customer Connect](#) download page.
- 2 After you download the file, mount the `vra-lcm-installer.iso` file.
- 3 Browse to the folder `vrlcm-ui-installer` inside the CD-ROM.

- 4 The folder contains three subfolders for three operating systems. Based on your operating system, browse to the corresponding operating system folder inside the `vrlcm-ui-installer` folder.
- 5 Click the installer file in the folder.

Operating System	File Path
Windows	<code>lcm-installer\vrlcm-ui-installer\win32</code>
Linux	<ol style="list-style-type: none"> a Log in to Linux VM. b Run <code>apt-get install p7zip-full</code>. c Run <code>7z x vra-lcm-installer.iso</code>. d Run <code>chmod +x vrlcm-ui-installer/lin64/installer</code> e Run <code>chmod +x ./vrlcm/ovftool/lin64/ovftool*</code> f Run <code>apt install libnss3</code> (required only if the libnss3 component is not installed.) g Run <code>vrlcm-ui-installer/lin64/installer</code>.
Mac	<code>vrlcm-ui-installer/mac/Installer</code>

The VMware Aria Suite Lifecycle VMware Aria Automation Easy Installer for VMware Aria Automation and VMware Workspace ONE Access is specific to the operating system. Ensure that you are using the valid UI folder path to run the installer.

Results

You can now install your applications using the VMware Aria Suite Lifecycle VMware Aria Automation Easy Installer for VMware Aria Automation and VMware Workspace ONE Access.

If the VMware Aria Suite Lifecycle VMware Aria Automation Easy Installer for VMware Aria Automation and VMware Workspace ONE Access fails to launch, and you see this error message `A problem occurred during installation`. Check the installer logs and retry, it is because:

- A host rebooted during installation. Select the host to return to a healthy state.
- The datastore was 100% full during installation. Clear the datastore memory and retry launching the VMware Aria Automation Easy Installer.
- The VMware Aria Suite Lifecycle VMware Aria Automation Easy Installer for VMware Aria Automation and VMware Workspace ONE Access could not connect to the ESXI host. Add the target vCenter and all cluster associated ESXI servers DNS FQDN entries to the system host file: `C:\Windows\System32\drivers\etc\hosts`. For Linux and Mac, use `/etc/hosts`.

Install and configure VMware Identity Manager in VMware Aria Suite Lifecycle

You can install a new instance of VMware Workspace ONE Access or import an existing instance when you are configuring VMware Aria Suite Lifecycle VMware Aria Automation Easy Installer for VMware Aria Automation and VMware Workspace ONE Access.

If you want to customize your VMware Workspace ONE Access configuration, which can include deployment of VMware Workspace ONE Access in a standard or a cluster mode, customized mode of network, storage, you can skip the installation of VMware Workspace ONE Access. If you have skipped, you are still prompted to configure the VMware Workspace ONE Access on the VMware Aria Suite Lifecycle UI. With VMware Aria Suite Lifecycle VMware Aria Automation Easy Installer for VMware Aria Automation and VMware Workspace ONE Access, you either import an existing VMware Workspace ONE Access into VMware Aria Suite Lifecycle or a new instance of VMware Workspace ONE Access can be deployed. For more information on hardware re-sizing for VMware Workspace ONE Access, see [Resize hardware resource for VMware Lifecycle Manager in VMware Aria Suite Lifecycle](#).

For information about product and version compatibility, see the [VMware Interoperability Matrix](#), such as this [sample page](#).

Prerequisites

Verify that you have a static IP address before you begin your configuration.

The terms VMware Identity Manager and VMware Workspace ONE Access are used interchangeably in VMware Aria Suite Lifecycle.

Procedure

- 1 To install a new instance, select the **Install new** VMware Workspace ONE Access option.
- 2 Enter the required text boxes under **Virtual Machine Name**, **IP Address**, **Hostname**, and **Default Configuration Admin**.

Note The VMware Aria Suite Lifecycle VMware Aria Automation Easy Installer for VMware Aria Automation and VMware Workspace ONE Access creates the default configuration admin user as a local user in VMware Workspace ONE Access and the same user is used to integrate products with VMware Workspace ONE Access.

- 3 To import an existing instance, select **Import Existing vIDM**.
 - a Enter the **Hostname**, **Admin Password**, **System Admin Password**, **SSH User Password**, **Root Password**, **Default Configuration Admin**, and **Default Configuration Password**.
 - b Select the **Sync group members to the Directory when user want to sync group member** while adding a group for the global configuration of VMware Workspace ONE Access.

With VMware Aria Automation Easy Installer for VMware Aria Automation and VMware Workspace ONE Access	VMware Workspace ONE Access supported version
New installation of VMware Aria Suite Lifecycle	3.3.7
Import VMware Aria Suite Lifecycle	3.3.7
Deploy VMware Aria Automation	3.3.7

Note VMware Workspace ONE Access is supported for single or cluster instance with embedded Postgres database.

Note VMware Workspace ONE Access is not supported for the following scenarios:

- Single or cluster instance having external database (Postgres/MSSQL and so on).
- Single or cluster instance with additional connectors (Windows and external connectors) other than the embedded ones.
- VMware Workspace ONE Access version 3.3.0 and earlier.

Note If the older version of VMware Aria Suite Lifecycle does not have VMware Workspace ONE Access, it can either be installed or imported. VMware Workspace ONE Access and extended day-2 functionalities are not supported from the VMware Aria Suite Lifecycle and extended day-2 functionalities are not supported from the VMware Aria Suite Lifecycle if the imported VMware Workspace ONE Access not in supported form factor.

Upgrade support from an older VMware Workspace ONE Access version (3.3.0 and earlier) to the latest is only available if it is a single instance or a node VMware Workspace ONE Access with embedded postgres database. Otherwise, you can upgrade outside VMware Aria Suite Lifecycle. After upgrade, it can be reimported by starting an Inventory Sync in VMware Aria Suite Lifecycle.

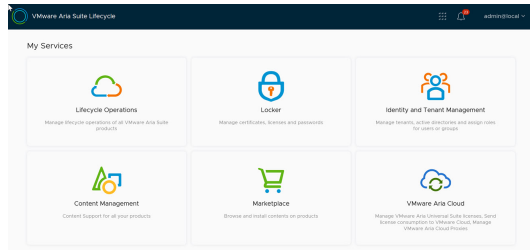
4 Click **Next**.

If you cannot deploy VMware Aria Suite Lifecycle, VMware Workspace ONE Access, or VMware Aria Automation in VMware Cloud on AWS vCenter by using VMware Aria Suite Lifecycle VMware Aria Automation Easy Installer for VMware Aria Automation and VMware Workspace ONE Access, then use the vCenter that has an administrator privilege to deploy products.

Install applications using the Lifecycle Operations service in VMware Aria Suite Lifecycle

You can install VMware Aria Suite Lifecycle, VMware Workspace ONE Access, and VMware Aria Automation applications by using the Lifecycle Operations service.

You install applications in VMware Aria Suite Lifecycle by using the **Lifecycle Operations** service.



Prepare to install and deploy products with VMware Aria Suite Lifecycle

Prepare to install VMware Aria Suite Lifecycle applications by using the VMware Aria Automation Easy Installer for VMware Aria Automation and VMware Workspace ONE Access.

You can install and configure VMware Aria Suite Lifecycle by using VMware Aria Automation Easy Installer for VMware Aria Automation and VMware Workspace ONE Access. Refer to *Installing VMware Aria Automation with Easy Installer* on the [VMware Aria Automation Documentation](#) page for your release.

Prerequisites

- Verify if a vCenter is available for deploying VMware Aria Suite Lifecycle and products.
- A static IPv4 with accurate FQDN is used for a VMware Aria Suite Lifecycle deployment.
- To prevent unwanted internal ports outside after VMware Aria Suite Lifecycle virtual appliance reboot, log in to VMware Aria Suite Lifecycle virtual appliance through SSH and run the command `rm -rf /etc/bootstrap/everyboot.d/10-start-services`, after deploying VMware Aria Suite Lifecycle virtual appliance from the Easy Installer.

Procedure

- 1 Deploy VMware Aria Suite Lifecycle by using VMware Aria Automation Easy Installer for VMware Aria Automation and VMware Workspace ONE Access.

By default, you can find the following information:

- `default_datacenter` (data center name provided in the VMware Aria Automation Easy Installer)
- `default_vCenter` (vCenter name provided in Easy Installer)
- DNS servers and NTP servers
- Data Disk Extended (Disk size provided in VMware Aria Automation Easy Installer)
- `globalenvironment` (VMware Workspace ONE Access - Based on product selection)
- VMware Aria Automation environment (Based on product selection)
- VMware Workspace ONE Access and VMware Aria Automation passwords in the VMware Aria Suite Lifecycle Locker
- Source mapping for VMware Aria Automation and VMware Workspace ONE Access

- 2 To deploy a new product, after you log in to VMware Aria Suite Lifecycle, click **Lifecycle Operations** on the **My Services** page.
- 3 Click **Datacenters > ADD DATACENTER**.
- 4 Add a vCenter to the data center.
- 5 Create a valid certificate in the VMware Aria Suite Lifecycle locker.
- 6 Add the required license keys for future use in the VMware Aria Suite Lifecycle locker.
- 7 Extend the VMware Aria Suite Lifecycle appliance disk space to accommodate product binaries and other necessary components to be used in future.
- 8 (Optional) Configure the proxy settings in VMware Aria Suite Lifecycle for an internal network connectivity.

Installing VMware Aria Suite Lifecycle with Easy Installer for VMware Aria Automation and Workspace ONE Access

You can install VMware Aria Suite Lifecycle using VMware Aria Suite Lifecycle Easy Installer for VMware Aria Automation and Workspace ONE Access.



Watch the VMware Aria Suite Lifecycle [Installation with Easy Installer video](#).

Prerequisites

You must meet these prerequisites before you can install VMware Aria Suite Lifecycle:

- Ensure you have a vCenter set up and access to the credentials.
- Ensure you have the network configuration details for VMware Aria Automation
- Ensure you know the VMware Aria Suite Lifecycle VA deployment details

Procedure

- 1 Click **Install** on the **Easy Installer** window.
- 2 Click **Next** after reading the introduction.
- 3 Accept the License Agreement and click **Next**. Read the **Customer Experience Improvement Program** and select the checkbox to join the program.
- 4 To specify vCenter details, enter these details on the Appliance Deployment Target tab.
 - a Enter the **vCenter Server Hostname**.
 - b Enter the **HTTPs Port** number.
 - c Enter the **vCenter Server Username**, and **Password**.
- 5 Click **Next** and you are prompted with a certificate warning, click **Accept** to proceed.

- 6 You must specify a location to deploy virtual appliances.
 - a Expand the vCenter tree.
 - b Expand to any data center and map your deployment to a specific VM folder.
- 7 Specify a resource cluster on the **Select a Compute Resource** tab.
 - a Expand the data center tree to an appropriate resource location and click **Next**.
- 8 On the **Select a Storage Location** tab, select a datastore to store your deployment and click **Next**.
- 9 On the **Network Configuration** and **Password Configuration** tabs, set up your **Network** and **Password configuration** by entering the required fields, and clicking **Next**.
 - a For a VMware Aria Suite Lifecycle VM, enter the **NTP Server** for the appliance and click **Next**.

The network configurations provided for all products are a one time entry for your configuration settings. The password provided is also common for all products and you need not enter the password again while you are installing the products.

Password should have minimum one upper case, one lower case, one number and one special character. Special characters can be !@#\$%^&*().

- 10 Set up VMware Aria Suite Lifecycle configuration settings,
 - a Enter a **Virtual Machine Name, IP Address, and Hostname**.
 - b Provide configuration information. Enter the **Data Center Name, vCenter Name** and **Increase the Disk Space** fields.
 - c Enable or disable the **FIPS Mode Compliance**, as required.
 - d Click **Next**.

What to do next

You can now start installing VMware Aria Suite Lifecycle.

Install VMware Workspace ONE Access

You can install a new instance of VMware Workspace ONE Access or import an existing instance when you are configuring VMware Aria Suite Lifecycle VMware Aria Automation Easy Installer for VMware Aria Automation and VMware Workspace ONE Access.

- Without installing or importing a VMware Workspace ONE Access, you cannot access any other environment from VMware Aria Suite Lifecycle.
- If you are installing VMware Aria Automation, ensure that you deploy VMware Workspace ONE Access with the recommended size for VMware Aria Automation.
- Refer to *Installing VMware Aria Automation with Easy Installer* on the [VMware Aria Automation Documentation](#) page.

Prerequisites

- Verify that you have a static IP address and Active Directory details before you begin your configuration.
- Verify that an external load balancer is installed with a valid certificate and the requirements are met. For load-balancing specific information for VMware Workspace ONE Access, see the *VMware Aria Automation Load Balancing Guide* on the [VMware Aria Automation Documentation](#) page.

Procedure

- 1 To install a new instance, select **Install** VMware Workspace ONE Access.
 - a Enter the required content for **Virtual Machine Name**, **IP Address**, **Hostname**, and **Default Configuration Admin**.
- 2 To import an existing instance, click **Import Existing vIDM**.
 - a Enter the **Hostname**, **Admin Password**, **System Admin Password**, **SSH User Password**, **Root Password**, **Default Configuration Admin**, and **Default Configuration Admin Password**.

Note This is a local user that you create on the default tenant in VMware Workspace ONE Access and provide the admin access in the default tenant. The same user is used for all product integration with VMware Workspace ONE Access and the admin role is assigned in the corresponding product. For example, when VMware Aria Automation is registered with VMware Workspace ONE Access, this default configuration user is made the organization admin and is given with appropriate roles. After VMware Aria Automation is deployed, the configuration user is the initial user to log in with. With other products, when they are integrated with VMware Workspace ONE Access, the same user is assigned an admin role in the product. More of SSO use-case where the default configuration admin has access to all deployed products.

- 3 Click **Next**.

Creating catalog applications for VMware Aria Suite products

You can deploy a catalog application to access VMware Aria Suite products that are managed in VMware Workspace ONE Access).

When you install VMware Aria Suite products in VMware Aria Suite Lifecycle, you can integrate with VMware Workspace ONE Access to create a catalog application in VMware Workspace ONE Access.

The VMware Aria Suite products that support the use of catalog applications are VMware Aria Automation, VMware Aria Operations for Logs, VMware Aria Operations for Networks, VMware Aria Operations, and VMware Aria Suite Lifecycle.

For related information about VMware Aria Suite products, see [VMware Cloud Management Suites Documentation](#).

Install VMware Aria Automation by using VMware Aria Suite Lifecycle Easy Installer

The VMware Aria Suite Lifecycle Easy Installer for VMware Aria Automation and VMware Workspace ONE Access provides you with a functionality to install VMware Aria Automation with minimum steps.

The installer provides you with minimal or a clustered deployment options before you start your VMware Aria Automation configuration. Manual installation of VMware Aria Automation through OVA or ISO is not supported.

Prerequisites

- Verify that you have the primary VMware Aria Automation credentials before installing VMware Aria Automation. VMware Aria Automation an external VMware Workspace ONE Access.
- Verify that an external load balancer is installed and the requirements are met. For more information, see the *Load Balancing Guide* on the [VMware Aria Automation Documentation](#) page.

Procedure

- 1 Enter the VMware Aria Automation **Environment Name**.
- 2 Under VMware Aria Automation license, enter the license key.
- 3 After configuring your VMware Workspace ONE Access settings, you can opt to install VMware Aria Automation.
- 4 For a standard deployment with a primary node, perform the following steps:
 - a Enter the **Virtual Machine Name**, **IP Address**, and **FQDN Hostname** of VMware Aria Automation.
 - b Provide configuration information. Enter the **Data Center Name**, **Name** and **Increase the Disk Space** fields. For more information, refer to *Installing VMware Aria Automation with Easy Installer* on the [VMware Aria Automation Documentation](#) page.
 - c Activate or deactivate the **FIPS Mode Compliance** setting, as required.
 - d Skip to Step 6.
- 5 For a cluster deployment with three nodes, enter the **Load Balancer IP address** and **Hostname**.
- 6 For a cluster deployment, create a primary node by using step 4 as a guideline.
- 7 For a cluster deployment, create secondary nodes, enter the required text boxes, and proceed.

- 8 Under **Advanced Configuration** for VMware Aria Automation, you can either choose the **Use Default option** to enable the default values for internal pods and services configuration in CIDR format, or use the **Use Custom** option to enter the values for K8S Cluster IP Range and K8S Service IP Range in CIDR format.
- 9 Click **Next**.
- 10 Read the **Summary** page with the entered data and click **Submit**.

After submitting your details, the installer takes about 30 minutes to install the VMware Aria Suite Lifecycle, copy binaries and then start the installation process. You can enable multi-tenancy for VMware Aria Automation, refer to [Tenant management in VMware Aria Suite Lifecycle](#).

Migrate applications using the Lifecycle Operations service in VMware Aria Suite Lifecycle

You can use VMware Aria Suite Lifecycle VMware Aria Automation Easy Installer for VMware Aria Automation and VMware Workspace ONE Access to migrate older versions of VMware Aria Suite Lifecycle applications to the latest versions.

You migrate applications in VMware Aria Suite Lifecycle by using the **Lifecycle Operations** service.

Migrate from an earlier version of VMware Aria Suite Lifecycle to the current version

You can migrate from an earlier version of VMware Aria Suite Lifecycle to the current VMware Aria Suite Lifecycle version.

You cannot directly migrate or upgrade a VMware vRealize Suite Lifecycle Manager 2.x environment to VMware Aria Suite Lifecycle 8.12. To upgrade to VMware Aria Suite Lifecycle version 8.12, first migrate your 2.x environment to VMware vRealize Suite Lifecycle Manager 8.8.x to 8.10 and then upgrade to VMware Aria Suite Lifecycle 8.12.

The VMware Aria Suite Lifecycle migration requires inputs, such as legacy VMware Aria Suite Lifecycle hostname, user name, password, and SSH password.

Prerequisites

- Verify that latest version of VMware Aria Suite Lifecycle is installed.
- Verify that the legacy VMware Aria Suite Lifecycle has SSH enabled for the root user.
- Some legacy versions of vRealize Suite Lifecycle Manager cannot be directly upgraded to VMware Aria Suite Lifecycle. For information about upgrading legacy versions of the product, refer to the VMware Aria Suite Lifecycle release notes.

Procedure

- 1 From the **Easy Installer** wizard, click **Migrate**.
- 2 Enter the vCenter details where the new VMware Aria Suite Lifecycle is installed.

- 3 Select the datacenter in the vCenter **Server**, **Compute Resource**, and **Storage** settings.
- 4 Enter the network configuration details.
- 5 In the **Password configuration**, enter the password for the VMware Aria Suite Lifecycle root and admin password.
- 6 If you want to deploy Workspace ONE Access, then enter the password for **admin**, **sshuser**, and **root credential**.
- 7 Enter the VMware Aria Suite Lifecycle **VMname**, **Hostname**, and the **IP details**.
- 8 Enter the legacy VMware Aria Suite Lifecycle **Hostname**, **Username**, and **Password**.
- 9 Select **New Identity Manager Installation** or **Import Existing Identity Manager**.
If you have selected **New Identity Manager Installation**, then it is deployed in the same vCenter mentioned in step 2. If you selected **Import Existing Identity Manager**, verify that the identity manager is already registered in the VMware Aria Suite Lifecycle legacy VM and identity manager SSH is enabled for the root user.
- 10 Click **Submit**.
- 11 When the migration is successful, click the VMware Aria Suite Lifecycle URL or the migration request to view the progress by logging in with `admin@local` with the password given in step 5.
- 12 All the environments with data centers, vCenter instances, settings (such as NTP, DNS, and so on), content endpoints that are managed by VMware Aria Suite Lifecycle are migrated and the environments are imported to the latest version.

Results

As part of migration, create a global environment based on installation or import when you import legacy VMware Aria Suite Lifecycle VMware Workspace ONE Access to VMware Aria Suite Lifecycle. If there is a failure in the global environment, it can be due to the missing SSH user password in the legacy VMware Aria Suite Lifecycle. Enter the SSH password details by selecting the correct password on retry and submit the changes to create a global environment. After a global environment is created, you can resume the migration operation.

With migration you can create environments, settings, certificate and so on. You can check the status of migration on the Request status.

Note If you import an existing VMware Workspace ONE Access and if the admin password is different from the SSH user for the VMware Workspace ONE Access, then the global environment request fails. In this case, add the SSH password in the VMware Aria Suite Lifecycle locker manually and retry the request with this password.

Download and run the VMware Aria Suite Lifecycle Easy Installer

You can download the executable file from the Customer Connect download page.

Procedure

- 1 Download the VMware Aria Suite Lifecycle VMware Aria Automation Easy Installer executable file from the [VMware Customer Connect](#) download page.
- 2 After you download the file, mount the `lcm-installer.iso` file.
- 3 Browse to the folder `vrlcm-ui-installer` inside the CD-ROM.
- 4 The folder contains three subfolders for three operating systems. Based on your operating system, browse to the corresponding operating system folder inside the `vrlcm-ui-installer` folder.
- 5 Click the installer file in the folder.

Operating System	File Path
Windows	<code>lcm-installer\vrlcm-ui-installer\win32</code>
Linux	<ol style="list-style-type: none"> a Log in to Linux VM. b Run <code>apt-get install p7zip-full</code>. c Run <code>7z x vra-lcm-installer.iso</code>. d Run <code>chmod +x vrlcm-ui-installer/lin64/installer</code> e Run <code>apt install libnss3</code> (required only if the libnss3 component is not installed.) f Run <code>vrlcm-ui-installer/lin64/installer</code>.
Mac	<code>vrlcm-ui-installer/mac/Installer</code>

- 6 The VMware Aria Suite Lifecycle VMware Aria Automation Easy Installer UI is specific to the operating system. Ensure that you are using the valid UI folder path to run the installer.

Results

You can now install VMware Aria Suite Lifecycle using the VMware Aria Suite Lifecycle VMware Aria Automation Easy Installer.

Install VMware Aria Suite Lifecycle

You can install VMware Aria Suite Lifecycle by using the VMware Aria Suite Lifecycle VMware Aria Automation Easy Installer.

Prerequisites

- Ensure you have a vCenter set up and access to the credentials.
- Ensure you know the Workspace ONE Access VA deployment details.

Procedure

- 1 Click **Install** on the VMware Aria Suite Lifecycle Easy Installer window.
- 2 Click **Next** after reading the introduction.

- 3 Accept the End User License Agreement and click **Next**. Read the Customer Experience Improvement Program and select the check box to join the program.
- 4 To specify vCenter details, enter these details on the **Appliance Deployment Target** tab.
 - a Enter the vCenter **Server Hostname**.
 - b Enter the **HTTPs Port number**.
 - c Enter the vCenter **Server Username** and **Password**.
- 5 Click **Next** and you are prompted with a certificate warning, click **Accept** to proceed.
- 6 Specify a storage location to deploy virtual appliances.
 - a Expand the vCenter tree.
 - b Expand to any data center and map your deployment to a specific VM folder.
- 7 Specify a resource cluster on the **Select a Compute Resource** tab.
 - a Expand the data center tree to an appropriate resource location and click **Next**.
- 8 On the **Select a Storage Location** tab, select a data store to store your deployment and click **Next**.
- 9 On the **Network Configuration** and **Password Configuration** tabs, set up your network and password configuration by entering the required fields, and then click **Next**.
 - a For a VMware Aria Suite Lifecycle VM, enter the **NTP Server** for the appliance and click **Next**.

The network configurations provided for all products are a one-time entry for your configuration settings. The password provided is also common for all products and you need not enter the password again while you are installing the products.

Password should have minimum one upper case, one lower case, one number and one special character. Special characters can be !@#\$%^&*(). A colon(:) is not supported in the password.
- 10 Set up VMware Aria Suite Lifecycle configuration settings.
 - a Enter a **Virtual Machine Name**, **IP Address**, and **Hostname**.
 - b Provide configuration information. Enter the **Data Center Name**, vCenter **Name** and **Increase the Disk Space** fields.
 - c Enable or disable the FIPS Mode Compliance, as required.
 - d Click **Next**.
 - e Verify the details in the **Summary** page and then click **Submit**.

Migrate to the current version of VMware Aria Suite Lifecycle

To migrate from older versions of VMware Aria Suite Lifecycle, use VMware Aria Automation Easy Installer.

You cannot directly migrate or upgrade a VMware vRealize Suite Lifecycle Manager 2.x environment to VMware Aria Suite Lifecycle 8.12. To upgrade to VMware Aria Suite Lifecycle version 8.12, first migrate your 2.x environment to VMware vRealize Suite Lifecycle Manager 8.8.x to 8.10 and then upgrade to VMware Aria Suite Lifecycle 8.12.

Log in to VMware Aria Suite Lifecycle

Log in to VMware Aria Suite Lifecycle to create and manage cloud environments with VMware Aria Suite Lifecycle.

Prerequisites

Deploy the VMware Aria Suite Lifecycle appliance.

Procedure

- 1 Use a supported web browser (Chrome, IE or Mozilla FireFox) to connect to your VMware Aria Suite Lifecycle appliance by using the appliance's IP address or host name.

https://IP address/vr1cm

Note You can also access VMware Aria Suite Lifecycle using the URL `https://IP address`. The URL `http://IP address` does not successfully redirect to VMware Aria Suite Lifecycle.

- 2 Enter the administrator user name.

admin@local

- 3 Enter the default administrator password.

Admin password will be the default password given in the VMware Aria Automation Easy Installer while deploying VMware Aria Suite Lifecycle.

- 4 Click **Log In**.

What to do next

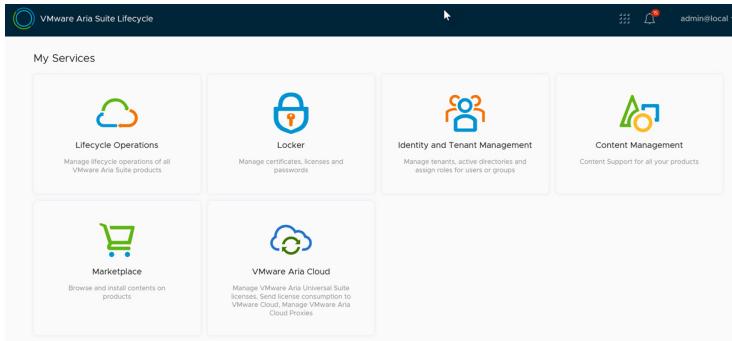
If you are logging in to VMware Aria Suite Lifecycle for the first time, set the VMware Aria Suite Lifecycle `root` password. If you want to reset the password, use the **Settings** tab to make the change.

Configure a new administrator password and other VMware Aria Suite Lifecycle settings, such as SSH settings.

Overview of the VMware Aria Suite Lifecycle My Services dashboard

Access VMware Aria Suite Lifecycle services from the My Services dashboard.

The services provided by VMware Aria Suite Lifecycle are available on the **My Services** dashboard.



The **My Services** dashboard consists of the following services:

Lifecycle Operations

Use this service to manage the Day 0 to Day N operations of the VMware Aria Suite products such as VMware Aria Automation and VMware Aria Operations for Networks.

Locker

Use this service to manage certificates, licenses, and passwords. You can create and import certificates and initiate a certificate signing request (CSR). You can also validate a certificate before applying or replacing it.

Identity and Tenant Management

Use this service to manage active directories and tenants, and assign roles to users or groups.

Content Management

Use this service to manage content and content settings, including software-defined data center (SDDC) content. You can also capture, test, and release content to various environments, and access source control capabilities through GitLab or bit bucket integration.

Marketplace

Use this option to the [VMware Marketplace](#).


VMware Aria Cloud

Use this option to manage suite licenses, subscriptions, and cloud proxies.

Note For information about installing and configuring a cloud proxy, see [Configuring environment settings for a new cloud proxy](#). If you are installing and configuring a cloud proxy for VMware Aria Automation, also see cloud proxy information in *Using VMware Aria Automation Assembler* at the VMware Aria Automation [product documentation page](#).

Display notifications in VMware Aria Suite Lifecycle

You can view VMware Aria Suite Lifecycle notifications for product updates and related information.

To view available notifications, navigate to the **My Services** dashboard and click the bell icon  in the upper right of the page. To list all notifications, click **See All Notifications** on the resultant Notifications menu.

The following types of notifications are available in VMware Aria Suite Lifecycle.

- License Health: Provides notifications about the expired licenses and proactive notifications about the licenses that will expire in the next three months.
- Certificate Health: Provides notifications about the expired certificates and proactive notifications about the certificates that will expire in the next one month.
- Product Upgrade: Provides notifications about the upgrade availability of VMware Aria Suite products.
- Product Patch: Provides notifications about the patch availability of VMware Aria Suite products.
- VMware Aria Suite Lifecycle Self Upgrade: Provides notifications about the upgrade availability of VMware Aria Suite Lifecycle.
- VMware Aria Suite Lifecycle Self Patch: Provides notifications about the patch availability of VMware Aria Suite Lifecycle.
- VMware Aria Suite Lifecycle Product Support Pack: Provides notifications about the product support pack availability of VMware Aria Suite Lifecycle.
- VCF notifications (VMware Aria Suite Lifecycle-SDDC Manager FIPS status): Provides notifications to verify if VMware Aria Suite Lifecycle and SDDC Manager are in sync.
- Health Notifications for VMware Aria Suite Products: Provides notifications about the health of VMware Aria Suite products.
- Identity Manager Health Notification: Provides notifications about the health of VMware Workspace ONE Access, including system health and Postgres Database Cluster health.

Configuring SMTP for email outbound notifications

SMTP server is required to send emails, so you must configure SMTP server prior to configuring outbound notifications in VMware Aria Suite Lifecycle.

Procedure

- 1 Navigate to **Settings** from the Lifecycle Operations dashboard.
- 2 Select **SMTP** from Server & Accounts.
- 3 Enter the sender's email ID under SMTP Configuration Details.
- 4 Enter the **SMTP Hostname/IP Address**, and then select **Encryption** from the list.
- 5 Select the **SMTP Port Number**.
- 6 If you select the **Requires Authentication** toggle, you must provide the authentication details. Select the plus (+) sign or the key symbol to add the password details.
- 7 Select an option from the available SMTP Credentials.
- 8 Click **Save**.
- 9 After a successful SMTP configuration, click **SEND TEST EMAIL** to validate if the configured SMTP server is correct. Enter your email ID to start receiving email notifications.

What to do next

You can configure email outbound notifications.

Creating incoming webhooks for Slack and Teams channels in VMware Aria Suite Lifecycle

When you create an Incoming Webhook, you receive a unique URL. You must add this unique URL in the Outbound Notifications page to receive alerts and outbound notifications.

Procedure

- 1 To create an Incoming Webhook on Teams, go to the channel where you want to add the webhook and select the **More Options** ellipsis (...).
- 2 Click **Connectors** from the drop-down menu.
- 3 Search for Incoming Webhook, and then select **Add**.
- 4 Select **Configure**, and provide a name. You can also upload an image for the webhook, if required.
- 5 A unique URL is generated that maps to the channel. Copy and save the webhook URL, and then click **Done**.
- 6 To create an Incoming Webhook on Slack, create your Slack app, and then select the **Incoming Webhooks** feature.
- 7 Select the **Activate Incoming Webhooks** toggle.
- 8 Click **Add New Webhook to Workspace**, and then click **Authorize**.
- 9 A unique Webhook URL is generated for your use.

Configuring outbound notifications in VMware Aria Suite Lifecycle

Outbound notifications allow you to configure your email ID, Slack, and Teams channels. After you configure outbound notifications in VMware Aria Suite Lifecycle, you should start receiving notifications in your registered email ID or supported media integrations such as Slack or Microsoft Teams.

You can also view the health status of your VMware Aria Suite products and license details. Outbound notifications are critical or consolidated. You would receive instant alerts for critical notifications. You can choose daily, weekly, or monthly alerts for consolidated notifications. Consolidated notifications provide a list of critical, moderate, and other relevant updates.

Note Sending outbound notifications by way of a proxy server is supported if you add the SMTP server to the exclusion list for your network proxy. See [Configure a network proxy in VMware Aria Suite Lifecycle](#).

Prerequisites

- Ensure that SMTP server is configured prior to configuring email outbound notifications.
- Create incoming web hooks for supported media integrations such as Slack or Microsoft Teams.

Procedure

- 1 Log in to VMware Aria Suite Lifecycle.
- 2 On the **My Services** page., click **Lifecycle Operations**.
- 3 In the navigation list on the left, select **Settings**.
- 4 On the **System Administration** page, click **Outbound Notifications**.
- 5 Enter the **Integration Name**, and then select the **Frequency**.
- 6 Enter the **Webhooks** URL that you created for the Slack and/or Teams channels, and then click **VALIDATE AND ADD**.
- 7 After a successful validation, enter the email IDs of the required **Recipients**.
- 8 Select the applicable check boxes for **Notification Triggers**.
- 9 Click **Save**.

Participating in the Customer Experience Improvement Program for VMware Aria Suite Lifecycle

This product participates in VMware's Customer Experience Improvement Program (CEIP).

The Customer Experience Improvement Program (CEIP) provides VMware with information that enables designers and engineers to improve products and services, fix problems, and advise you on how best to deploy and use VMware products and services. It collects usage and runtime data to help gauge system stability and the consumption levels of different features. This information also helps VMware designers and engineers determine what to build next based on which use-cases and features are being used or not used. You can join or leave the Customer Experience Improvement Program in VMware Aria Suite Lifecycle.

To join or leave the Customer Experience Program, select **Lifecycle Operations > Settings > System Details**. Scroll down to the **Customer Experience Improvement Program** section and select **JOIN** or **QUIT**.

Details regarding the data collected by the Customer Experience Program, and the purposes for which that data is used by VMware, is available at <http://www.vmware.com/trustvmware/ceip.html>.

Configuring VMware Aria Suite Lifecycle

2

After you install VMware Aria Suite Lifecycle, you can perform certain post-installation tasks, such as configuring your settings, licenses, and passwords in the VMware Aria Suite Lifecycle UI.

Read the following topics next:

- [Configure VMware Aria Suite Lifecycle settings](#)
- [Manage certificates for VMware Aria Suite Lifecycle products](#)
- [Manage licenses for a VMware Aria Suite Lifecycle products](#)
- [Manage passwords for VMware Aria Suite Lifecycle products](#)
- [Add and manage data center associations for VMware Aria Suite Lifecycle](#)
- [Add an NSX load balancer](#)
- [Working with the Identity and Tenant Management service in VMware Aria Suite Lifecycle](#)

Configure VMware Aria Suite Lifecycle settings

To configure VMware Aria Suite Lifecycle settings such as passwords, and SSH settings, use the Lifecycle Operations service.

To display and edit settings, click **Lifecycle Operations** from the VMware Aria Suite Lifecycle My Services dashboard and then click **Settings**.

The first time you view the Settings page, you must provide data for all available settings to save any settings. Only a user admin has access to the System Admin applications. The settings page contains the following applications.

System Administration	Servers & Accounts
System Details	NTP Servers
Logs	SNMP
System Patches	DNS
Product Support Pack	My VMware
System Upgrade	Binary Mapping

System Administration	Servers & Accounts
Time Settings	SMTP
Change Password	
Proxy	
Change Certificate	
Authentication Provider	
Outbound Notifications	

Note The UI session inactivity timeout value is now configurable. If you are inactive for a certain period, you can select the time out in minutes before getting logged out of the session.

What to read next

- [Configuring an authentication provider in VMware Aria Suite Lifecycle](#)
You can view the authentication provider details by using the **Settings** tab in VMware Aria Suite Lifecycle.
- [Configure a network proxy in VMware Aria Suite Lifecycle](#)
As an admin, you can configure VMware Aria Suite Lifecycle with a network proxy that acts as a security barrier between your internal network and external resources, such as the internet. The network proxy inspects incoming and outgoing traffic to filter out malicious content and protect your internal network from threats.
- [Configure Your System](#)
Configure your system after installing the VMware Aria Suite Lifecycle appliance.
- [Configure NTP servers](#)
Add the NTP servers in VMware Aria Suite Lifecycle so that they can be referred while deploying VMware Aria Suite products.
- [Configure DNS servers in VMware Aria Suite Lifecycle](#)
Configure your DNS servers for configuring a VMware Aria Suite Lifecycle appliance to resolve host names and IPs from the domain name server.
- [Data source using SNMP configurations for VMware Aria Operations for Networks](#)
The VMware Aria Suite Lifecycle supports VMware Aria Operations for Networks. VMware Aria Operations for Networks consists of data sources and are recognized by the VMware Aria Suite Lifecycle appliance.
- [Working with product support](#)
After configuring your VMware Aria Suite Lifecycle system information, you can check and apply updates or patches that are available in your existing environment.

Configuring an authentication provider in VMware Aria Suite Lifecycle

You can view the authentication provider details by using the **Settings** tab in VMware Aria Suite Lifecycle.

The **Authentication Provider Information** section displays the type of the existing authentication provider, the authentication provider endpoint, the registered FQDN of the application, client ID, and the name of the catalog application.

The **Authentication Provider Action** section offers syncing and re-registering capabilities. When you change or update the host name or FQDN of VMware Aria Suite Lifecycle, the authentication provider must sync with the host name. The **Sync** button ensures that the current host name or FQDN of VMware Aria Suite Lifecycle is synced with VMware Workspace ONE Access. After syncing, you can verify the target URL and the redirect URI in the **Catalog** tab of VMware Workspace ONE Access.

The **RE-REGISTER** button allows re-registering of VMware Aria Suite Lifecycle with VMware Workspace ONE Access by creating new `oAuth` clients and catalog applications. The re-registering action occurs when VMware Workspace ONE Access is present in `globalenvironment` of VMware Aria Suite Lifecycle.

When upgrading VMware Aria Suite Lifecycle 8.1 and earlier releases, the catalog application ID for updating the existing catalog application is not saved, so a duplicate catalog application is created. The new host name and catalog application ID is saved in the inventory which is used for the subsequent operations.

Configure a network proxy in VMware Aria Suite Lifecycle

As an admin, you can configure VMware Aria Suite Lifecycle with a network proxy that acts as a security barrier between your internal network and external resources, such as the internet. The network proxy inspects incoming and outgoing traffic to filter out malicious content and protect your internal network from threats.

The following procedure shows how to configure a network proxy that filters for

Prerequisites

- Verify that you have the name of the proxy server and proxy port.

Procedure

- 1 Log in to VMware Aria Suite Lifecycle.
- 2 On the **My Services** dashboard, click **Lifecycle Operations**.
- 3 In the navigation list at the left, select **Settings**.
- 4 On the **System Administration** page, click **Proxy**.

5 The **Network Proxy Details** page appears.

- a Check the **Configure Network Proxy** box.
- b Provide the information for:
 - **Server.** Proxy server name, such as `proxy.example.com`.
 - **Port.** Proxy server port., such as `1234`.
 - **Credential.** (optional) Click **Select Credential** to select a password from the locker or click the plus sign to create a new password. See [Manage passwords for VMware Aria Suite Lifecycle products](#).
 - **Exclusion List.** A list of hostnames, domains, or IP addresses that should not be accessed through the proxy server. Traffic to destinations on the exclusion list bypasses the proxy and connects directly to target servers. For example, if your list includes `example1.domain.com`, the network proxy does not screen internet traffic between that hostname and your internal network.

Note Adding destinations to exclude ensures that outbound notifications are triggered correctly.

6 Click **Save**.

Configure Your System

Configure your system after installing the VMware Aria Suite Lifecycle appliance.

Procedure

- 1 In the My Services dashboard, click **Lifecycle Operations**, and then click **Settings**.
- 2 To extend the disk space for VMware Aria Suite Lifecycle, navigate to **System Details**, click **Extend Storage**.
 - a Enter the **vCenter Host Name**, **User Name**, and **Password** for the first time.
 - b Enter the Disk Size in GB and click **Extend**.

You cannot edit the Network Information fields.
- 3 To reboot the server, click **Reboot System**.
 - a To schedule a weekly server restart, toggle the **Schedule a restart** and select the day of the week, and time for the weekly restart.
- 4 Click **Save**.

Activate or deactivate SSH on VMware Aria Suite Lifecycle

You can enable SSH for troubleshooting purposes.

As a best practice, disable SSH in a production environment, and activate it only to troubleshoot problems that you cannot resolve by other means. Leave it enabled only while needed for a specific purpose and in accordance with your organization's security policies. If content management is enabled, then SSH is enabled automatically and it cannot be disabled. Force disablement of SSH causes failure of VMware Aria Suite Lifecycle functionality.

Procedure

- 1 From the VMware Aria Suite Lifecycle dashboard, click Lifecycle Operations and click **Settings**.
- 2 Click **System Details**, under Network Information, enter the **Host Name, IP Address, IP Address Type, Netmask** and **Gateway fields**.
- 3 Enter the **Preferred DNS** and **Alternate DNS address**.

Note SSH is enabled by default.

- 4 Click **SAVE**.

Working with VMware Aria Suite Lifecycle logs

To configure log files and download log files for troubleshooting purposes, VMware Aria Suite Lifecycle.

VMware Aria Suite Lifecycle log content is entered in `vmware_vrlcm.log` and `/blackstone-spring.log`.

Generate a log bundle in VMware Aria Suite Lifecycle

You can configure the level of information VMware Aria Suite Lifecycle collects in log files and the number of log files for VMware Aria Suite Lifecycle.

In the VMware Aria Suite Lifecycle user interface, perform the following steps.

- 1 Select **Lifecycle Operations**, and then select **Settings**, and navigate to **System Administration > Logs**.
- 2 To create a VMware Aria Suite Lifecycle log bundle, click **GENERATE LOG BUNDLE**.
- 3 To download logs, click **DOWNLOAD THE LOGS**.

In the command line interface, perform the following steps:

- 1 Connect Secure Shell (SSH) to VMware Aria Suite Lifecycle VA using root credentials.
- 2 Create a VMware Aria Suite Lifecycle log bundle directory using the command `mkdir -p /data/lcm-logbundle`.
- 3 Generate a VMware Aria Suite Lifecycle log bundle directory using the command `/var/lib/vlcm-common/vlcm-support -w /data/lcm-logbundle`.
- 4 Download `/data/lcm-logbundle/filename` with secure copy.

Configure VMware Aria Operations for Logs agents

VMware Aria Suite Lifecycle supports VMware Aria Operations for Logs for log analysis.

The content pack in VMware Aria Operations for Logs for VMware Aria Suite Lifecycle agent is pre-installed on the VMware Aria Suite Lifecycle virtual appliance. You can configure the VMware Aria Suite Lifecycle appliance to forward `cfapi` or system logs, and events to the VMware Aria Operations for Logs instance. To use the VMware Aria Suite Lifecycle content pack dashboards and widgets, the configuration should be done on `cfapi` only.

Prerequisites

Verify that you already have the VMware Aria Operations for Logs server details before you set the properties of the Log Insight agent.

Procedure

- 1 Log in to the VMware Aria Suite Lifecycle virtual appliance.
 - a Open a Web browser and go to `https://vRSLCMIP/vr1cm` and log in with your user credentials.
 - b Click **Lifecycle Operations** from the **Home** page, and then click **Settings > Logs > Logs Insight Agent Configuration**.
 - c Update the following parameters in the VMware Aria Suite Lifecycle UI section and save your changes.

```
[server]
hostname= vRealize Log Insight hostname proto=cfapi port=9000 SSL=no
```

When VMware Aria Operations for Logs server is not configured to accept an SSL connection, enabling SSL for VMware Aria Operations for Logs agents in VMware Aria Suite Lifecycle is optional.

Or

```
hostname=vRealize Log Insight hostname proto=cfapi port=9543 SSL=yes
```

When the VMware Aria Operations for Logs is configured to accept an SSL connection, VMware Aria Operations for Logs agents must be configured to use the SSL connection in VMware Aria Suite Lifecycle.

Or

```
hostname=vRealize Log Insight hostname proto=syslog port=514
SSL Server Certificates
```

Set the rules for how the VMware Aria Operations for Logs client handles the validation of the VMware Aria Operations for Logs server certificate. Certificates received by the VMware Aria Operations for Logs agent are stored locally on the agent host machine.

```
Accept Any
Accept Any Trusted
Common Name: (Self-signed server certificate is accepted if its Common Name matches
this value)
Certificates acceptance rules:
```

Note VMware Aria Operations for Logs agents that receive a new self-signed certificate with the same public key as the existing locally stored self-signed certificate will accept the new certificate. For instance, a self-signed certificate may be regenerated with an existing private key but with a new expiration date.

If the Agent has a locally stored self-signed certificate and receives a valid CA-signed certificate, the Agent silently accepts the CA-signed certificate.

Agents that have a CA-signed certificate will reject self-signed certificates. The agent accepts self-signed certificates only when it initially connects to the Log Insight server.

If an agent with a locally stored CA-signed certificate receives a valid certificate signed by another trusted CA, it is rejected by default. You can select Accept Any Trusted to accept the certificate.

Reconnection Time: 30 min (Time in minutes to force reconnection to the server. This option mitigates the imbalances caused by long-lived TCP connections).

Max Buffer Size: 200 (Max local storage usage limit(data+logs) in MBs. Valid range: 100-2000 MB. Default: 200 MB).

- 2 Perform the following steps to properly configure the required liagent.ini file so that logs can be sent to VMware Aria Operations for Logs.
 - a SSH to VMware Aria Suite Lifecycle and navigate to the `/var/lib/loginsight-agent/` folder.
 - b Edit the `liagent.ini` file and uncomment `[filelog|syslog]`. Use the following excerpt as reference:

```
# Uncomment the appropriate section to collect system logs
# The recommended way is to enable the Linux content pack from LI server
[filelog|syslog]
directory=/var/log/*
```

- c Restart the `liagent`. Use the following command line as reference:

```
/etc/init.d/liagentd restart
```

- 3 Configure the Linux Agent Group on the VMware Aria Operations for Logs Administration UI.
 - a Open a Web browser and go to `https://vRealize Log Insight hostname/IP`.
 - b Log in with the credentials - **User name** as `admin` and **Password** as `vrli_admin_password`.
 - c Click the configuration drop-down menu icon and select **Administration**.

Note The content pack is not pre-installed in VMware Aria Operations for Logs. You must install the pack by downloading it from the Marketplace and then configure the agents.

- d Under **Management**, click **Agents**.

- e From the drop-down menu on the top, select VMware Aria Suite Lifecycle from the **Available Templates** section.
- f Click **Copy Template**.
- g After copying the template provide VMware Aria Suite Lifecycle Ipv4 or FQDN, and save the configuration.
- h Once the configuration is complete, the VMware Aria Suite Lifecycle events or logs start to flow into VMware Aria Operations for Logs and the relevant widgets displays the data.

Setting your VMware Aria Suite Lifecycle time

You can configure time settings and add NTP server or use a host time for VMware Aria Suite Lifecycle.

- 1 To change the time settings, navigate to My services dashboard, click **Lifecycle Operations** and click **Settings**.
- 2 Click **Time Settings**.
- 3 For Applicable Time Sync Mode, select **Use Time Server (NTP)** or **Use Host Time**.
 - a To add a server, click **Add New Server** and enter the name, and FQDN address of the server.
 - b To edit, click the edit icon on the list of NTP servers. You cannot edit the FQDN/ IP Address, you can only edit the name of the NTP server.

For more information on adding NTP server, see [Configure NTP servers](#).

Federal Information Processing Standard (FIPS) 140-2 support

FIPS 140-2 is a United States and Canadian government standard that specifies security requirements for cryptographic modules. VMware Aria Suite Lifecycle supports FIPS 140-2.

FIPS compliance is a new and secured opt-in mode adhering to the Enterprise Readiness Initiatives (ERI) in VMware Aria Suite Lifecycle. To learn more about support for FIPS 140-2 in VMware products, see [FIPS Security Policies and Certifications](#).

Activate or deactivate FIPS Mode Compliance in VMware Aria Suite Lifecycle

You can enable FIPS Mode Compliance by using VMware Aria Automation Easy Installer during VMware Aria Suite Lifecycle installation or by selecting the option as a Day-2 operation in the Settings page.

To learn more about FIPS Mode Compliance see *Installing VMware Aria Automation with Easy Installer* on the [VMware Aria Automation Documentation](#) page.

Procedure

- 1 From My Service dashboard, select **Lifecycle Operations** and then select **Settings**.
- 2 On the System Administration page, click **System Details**.

- 3 Activate or deactivate the **FIPS Mode Compliance** check box and then click **UPDATE**.

Note VMware Aria Suite Lifecycle restarts when you activate or deactivate FIPS Mode Compliance.

When you activate FIPS Mode Compliance, VMware Aria Suite Lifecycle does not upgrade to the next version. You must deactivate the FIPS Mode Compliance, upgrade VMware Aria Suite Lifecycle, and then activate FIPS Mode Compliance.

Configure NTP servers

Add the NTP servers in VMware Aria Suite Lifecycle so that they can be referred while deploying VMware Aria Suite products.

You can use NTP servers in VMware Aria Suite product deployment schemas.

Prerequisites

Verify that the NTP servers are functioning. Use NTP servers in VMware Aria Suite product deployments.

Procedure

- 1 On the VMware Aria Suite Lifecycle dashboard and navigate to **Settings > NTP Servers**.
- 2 To add an NTP server, click **Add NTP Server**.
- 3 Enter a valid **Name** and **FQDN/ IP Address** of the NTP server.
- 4 Click **ADD**.

Note NTP servers can be set for VMware Aria Automation.

Configure NTP settings post-deployment

VMware Aria Suite Lifecycle does not allow you to configure NTP settings for the virtual appliance during the OVA deployment. This section covers information on accurate time synchronization with the infrastructure and the suite products it deploys and manages.

Prerequisites

Verify that the SSH service on the VMware Aria Suite Lifecycle appliance is enabled.

Procedure

- 1 Log in to VMware Aria Suite Lifecycle by using the Secure Shell (SSH) client.
 - a Open an SSH connection to the FQDN or IP address of the virtual appliance.
 - b Log in using following credentials, with **Setting** as value, **User Name** as root and **Password** as root_password for the user.

- 2 Configure the NTP source for the virtual appliance.
 - a Open the `/etc/systemd/timesyncd.conf` file to edit, such as `vi`.
 - b Remove the comment for the NTP configuration, add the NTP settings, and save the changes. For example, `NTP=ntp.sfo01.rainpole.local ntp.lax01.rainpole.local`
- 3 Enable the `systemd-timesyncd` service and verify the status.
 - a Run the `timedatectl set-ntp true` command to enable the network time synchronization.
 - b Run the `systemctl restart systemd-timesyncd` to enable the NTP synchronization
 - c Run the `timedatectl status` to verify the status of the service.
- 4 Logout of the session by entering **Logout**.

Configure DNS servers in VMware Aria Suite Lifecycle

Configure your DNS servers for configuring a VMware Aria Suite Lifecycle appliance to resolve host names and IPs from the domain name server.

Prerequisites

Verify that you have an existing DNS servers.

Procedure

- 1 On the My Services dashboard, click **Lifecycle Operations**.
- 2 Click **Settings** and navigate to **Servers and Protocols > DNS**.
- 3 Click **Add DNS Server**.
- 4 Enter a **DNS Server Name** and **IP Address**.
- 5 Click **Add**.

Data source using SNMP configurations for VMware Aria Operations for Networks

The VMware Aria Suite Lifecycle supports VMware Aria Operations for Networks. VMware Aria Operations for Networks consists of data sources and are recognized by the VMware Aria Suite Lifecycle appliance.

You can record SNMP configurations, that are relevant to VMware Aria Operations for Networks. Click **Add Configuration** to add SNMP for both 2c and 3 SNMP type. The configured SNMP is then used while you are adding VMware Aria Operations for Networks data source for Routers and Switches.

Note From VMware Aria Operations for Networks 4.0 and later, a new brick size is introduced in VMware Aria Suite Lifecycle, extra large for both platform and collector node. When you have three nodes in a clustered environment, the brick size should be extra large. All platform nodes in a clustered environment should be of same brick size either large or extra large. But you cannot have both large and extra large in the same cluster.

If a clustered environment is deployed with large brick size and if you want to add one more platform nodes, then you have to manually increase the CPU and the RAM size from vCenter. You can then import the environment and scale out with an extra large brick size.

Add SNMP Configuration

You can add SNMP configuration in VMware Aria Suite Lifecycle.

Procedure

- 1 Navigate to **Lifecycle Operations** dashboard and navigate to **Settings > SNMP**.
- 2 Click **Add Configuration**.
- 3 To select the **SNMP Version**, select **v2C** or **v3**.
 - a If you have selected **v3**, enter the **Username** and **Context Name**.
 - b When you select the **Authentication type**, you are then prompted to enter to the **Auth Password** and **Privacy Type**.
- 4 Click **Add**.

Working with product support

After configuring your VMware Aria Suite Lifecycle system information, you can check and apply updates or patches that are available in your existing environment.

Configure product binaries

Using VMware Aria Suite Lifecycle, you can select a product binary to use each VMware Aria Suite product.

You can download binaries outside of VMware Aria Suite Lifecycle and make them available on the NFS path.

Prerequisites

To use a product binary downloaded from [VMware Customer Connect](#), verify that you have registered with VMware Customer Connect and registered VMware Customer Connect services with VMware Aria Suite Lifecycle. See [Register with My VMware](#).

Procedure

- 1 From the **My Services**, navigate to VMware Aria Suite Lifecycle Lifecycle Operations.
- 2 Click **Settings** and navigate to **Binary Mapping > Product Binaries**.
- 3 Click **Add Binaries**.
- 4 Select the location type.
 - Local - You can map the binaries to the VMware Aria Suite Lifecycle locally downloaded copy.
 - NFS - You can map to a downloaded product binary with products dependent on the product binary location.
 - VMware Customer Connect Downloads - You can map to product binary downloaded from VMware Customer Connect.

Note The automatic product OVA mappings are mapped based on the check sum of the binary files. When you select all the OVA files in the NFS share and try to map the product binaries, then it takes long time to map and the data disk might fill faster. NFS represents the local where the OVA files are copied in the NFS shared drive, user should provide the NFS location in the format, NFS-IP:<nfs hostname/ip>:<folder path>/x/y/z. For example, 10.11.12.134:/path/to/folder.

- 5 Enter the location of the Product Binary to use in the **Base Location** text box, and click **Discover**.
- 6 Select the Product Binary file from the **Product Binary** list.

Note By default, all the VMware Customer Connect downloads from VMware Aria Suite are automatically mapped with no user intervention. If you have already downloaded the product binaries using VMware Aria Suite VMware Customer Connect integration but the mapping does not exist in the list under Product Binary then you can select VMware Customer Connect downloads option under the **Add Product Binaries** window. To manually copy the OVA files from the VMware Aria Suite virtual appliance, you can select **Local** option from the **Add Product Binaries** window and provide the location that is residing within VMware Aria Suite appliance itself. For either of the scenarios, when you click **Discover**, the relevant binaries is listed in the table within the window.

- 7 Click **Add**.
- 8 You can also view the list of **Patches** available for the products.
 - a Click **Check Patches Online**.
 - b To upload patches, click **UPLOAD**.

Note You can now delete the unsupported product binaries which are not in use. To delete the binaries, click **Delete Unsupported Binaries**, select the binaries, and then click **Delete All**.

Patching products by using VMware Aria Suite Lifecycle

You can search for and download available patches for supported products within VMware Aria Suite Lifecycle.

You can perform following actions using patches from the notifications icon:

- View product deployments that have the patches.
- View patch logs.
- View patch application status.

If you select VMware Aria Automation for patching, a pre-check option is available for validation.

Install a patch for products by using VMware Aria Suite Lifecycle

You can view and click the related patch from the notification service. You are then directed to the environment page where you can view a detailed set of information pertaining to all the patches.

Procedure

- 1 Click **Lifecycle Operations**, navigate to **Settings > Binary Mappings**.
- 2 Click **Patch Binaries**.
- 3 To map a patch offline, download the patch from the [My VMware](#) portal and place it in the data folder in VMware Aria Suite Lifecycle appliance, and then map the offline patch using the local folder option in VMware Aria Suite Lifecycle UI.
- 4 To check if there are patches available on the internet, click **CHECK PATCHES ONLINE**.
- 5 Trigger the patch install from the product card in the environment page.
- 6 Select the patch from the list of downloaded patches.

The patches must be downloaded from the **Product Binaries** page. Only the downloaded patches are listed here.
- 7 Click **Next**.
- 8 **Review and Install** the available patch and click **Finish**.

The patch install request progress can be tracked under **Requests**.
- 9 To view the history of patches, click **Patches > History**.
- 10 To view patch history from the **Environment** page, click **Patch History**.

Configure your patched product binaries

You can download and map the OVA bundle that is already patched in a VMware Aria Automation environment by using VMware Aria Suite Lifecycle. This operation is useful when you want to scale out a patched environment. VMware Aria Operations for Logs patch binaries are also supported.

Prerequisites

Ensure the OVA bundle corresponding to the patched product is downloaded from My VMware Portal to VMware Aria Suite Lifecycle appliance and is placed in the data folder. For example: /data/patchovabundles/. For more information on downloading the OVA bundles, click [My VMware](#) portal. You can also see the detailed procedure for VMware Aria Automation at [KB 79105](#).

Procedure

1 Click Lifecycle Operations and navigate to **Settings > Binary Mappings**.

2 Click **Patched Product Binaries**.

3 To download patches, click the link provided on the UI.

You are directed to My VMware page where you can download the required patch or a OVA bundle.

4 Click **ADD PATCHED BINARY**.

a Enter the **Source Location** and click **Discover**.

Source location is the directory path in the VMware Aria Suite Lifecycle appliance where the OVA bundle files are retrieved.

b Select the required OVA bundle from the list and click **ADD**.

5 To delete a product patch, click **Delete** on the selected patch.

Run a script to address issues in your environment

To implement a fix or remediate a vulnerability in a VMware Aria Suite product, you can download a script and run it in your VMware Aria Suite Lifecycle environment.

The feature supports updates to:

- VMware Aria Automation
- VMware Aria Operations
- Workspace ONE Access, formerly VMware Identity Manager
- VMware Aria Automation Orchestrator
- VMware Aria Automation Config
- VMware Aria Operations for Logs
- VMware Aria Operations for Networks

You run the script in offline mode and can use it to update both standalone and clustered node deployments.

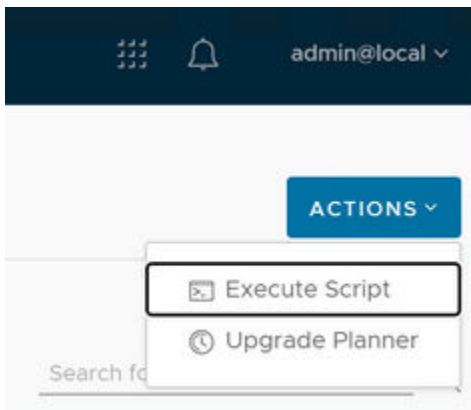
Note You can only run scripts that the VMware team shares specifically for running in VMware Aria Suite Lifecycle.

Prerequisites

- Verify that you are running VMware Aria Suite Lifecycle 8.14 or later.
- Obtain the script that you want to run from a VMware KB or from the VMware product engineering team.
- Upload the script bundle as a zip archive with a supported directory and file structure to your VMware Aria Suite Lifecycle appliance.

Procedure

- 1 Log in to VMware Aria Suite Lifecycle.
- 2 On the **My Services** dashboard, click **Lifecycle Operations**.
- 3 In the navigation list at the left, select **Environment**.
- 4 Choose how you want to run the script.
 - To run the script at the environment level, click **Actions > Execute Script** at the upper right.
 - To run the script at the product level, select a product from the environment, then click **Actions > Execute Script** at the upper right.

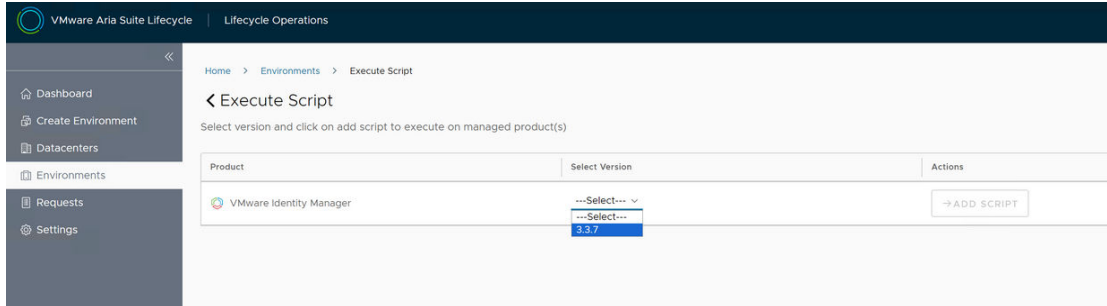


Note Running the script at the product level is a Day 2 action.

- 5 In the **Proceed to Execute Script** window that appears, click **Trigger Inventory Sync**. Then click **Proceed**.

6 In the **Execute Script** window that appears:

- a Select the product name and version.
 - If you are running the script from the environment level, select the version of the products that you are updating then click **Add Script** in the Actions column.



- If you are running the script from the product level, the product name and version are selected.
- b Select the environment for the product and click **Save & Proceed**.
 - c To provide the location of the uploaded script bundle, enter the directory where the zip archive is stored such as `/uploaded_data` and click **Display files**. Select the file you want to run and click **Save & Proceed**.
 - d When initiating script validation, a best practice is to select both:
 - Take Product Snapshot
 - Retain Product Snapshot

Then click **Validate**.

The script validation process might take some time because appliances are powered on and off when snapshots are taken. The log for the validation steps is `/var/log/vrlcm/vmware_vrlcm.log`.

- e If the validation completes successfully, click **Submit**.

Results

The **Request Details** page appears and shows how each script execution stage is progressing.

Register with My VMware

You can register with My VMware to access licenses, download product binaries and consume Marketplace content.

Enter your My VMware user name and password to enable VMware Aria Suite Lifecycle to download product Binary through My VMware. You can also enter using the proxy server under My VMware Settings. Configuring My VMware Settings is optional if you do not have internet connectivity.

Prerequisites

Verify the account details being entered has the following entitlements.

- VMware Aria Suite entitlement with download and view license permissions to download VMware Aria Suite products.
- VMware Aria Operations for Networks or NSX Data Center Enterprise Plus entitlement with download and view license permissions to download VMware Aria Operations for Networks.

The configured My VMware user must have permissions to download and view licenses.

Download the support pack from the *VMware Solution Marketplace*.

Procedure

- 1 Navigate to **Servers and Accounts**, click **My VMware**.
- 2 Click **ADD MY VMWARE ACCOUNT**.
- 3 Enter your My VMware user name and password, and click **Submit**.

After registration, you can download all the required binaries.

Note To download Product Binary, click the download arrow under **Actions** for the Product Binary to download. If your network requires proxy settings to access external Websites, you can provide those details in the Configure Proxy section. For more information on configuring proxy settings, see [Configure your proxy settings](#).

Configure your proxy settings

If you are using a proxy server in your network, you must configure the proxy server in VMware Aria Suite Lifecycle.

Normal Proxy (with or without Credential) and Proxy with AD configuration, are supported by VMware Aria Suite Lifecycle.

Prerequisites

You must have installed and configured a proxy server in your network before using it in VMware Aria Suite Lifecycle and the proxy server IP should have a host name that is resolvable from VMware Aria Suite Lifecycle appliance console.

Note

- If you are unable to configure proxy in VMware Aria Suite Lifecycle, ensure that ICMP is allowed from VMware Aria Suite Lifecycle to the Proxy host and that there are forward and reverse DNS entries for the Proxy host.
 - If the proxy server does not have a resolvable host name, then the procedure to add proxy fails.
-

Procedure

- 1 Navigate to Lifecycle Operations and click **Settings**.

2 Click **Proxy**.

3 Toggle **Configure Proxy** to use a proxy server for VMware Aria Suite Lifecycle, or deselect it to remove an existing proxy server.

VMware Aria Suite Lifecycle does not save proxy server settings when you disable proxy.

4 If you are enabling proxy, enter the **Server**, **Port**, **User name**, and **Credential**.

5 Click **Save**.

If VMware Aria Suite Lifecycle is already configured to use a proxy server, those proxy details are displayed.

Manage certificates for VMware Aria Suite Lifecycle products

The VMware Aria Suite Lifecycle Locker allows you to manage certificates for the various suite products. You can manage certificates, including generate a new certificate, for products that are deployed by VMware Aria Suite Lifecycle.

Prerequisites

- Certificates that are about to expire in less than 15 days cannot be imported.
- To manage the certificate for an imported environment, add the certificate in the VMware Aria Suite Lifecycle and perform inventory sync so that the certificate is mapped to the imported environment, after which replace certificate and scale-out wizards will be aware of the existing certificate.

Procedure

1 From the VMware Aria Suite Lifecycle My Services dashboard, click **Locker**.

2 You can either select **Generate**, **Import**, or **Generate CSR**.

Option	Description
Generate	<ul style="list-style-type: none"> a Enter the required text boxes. b Select the length of the Key. c Enter the valid Server Domain/Hostname. You can also include the wildcard certificate. For example, you can enter <code>*.sql.local</code>. d Enter the FQDN or IP Address. e Click Generate.
Import	<ul style="list-style-type: none"> a Enter a valid certificate name. b In the Passphrase text box, enter <i>Cert-Password</i> (if applicable). c Click Browse File and browse to the saved PEM file. d When you upload a PEM file, the private key and certificate chain details are populated automatically. e Enter the private key and certificate chain details manually. f Click Import. <p>The requirements for PEM file are:</p> <ul style="list-style-type: none"> ■ Both certificate chain and key must be in the same file. ■ The PEM file that are imported can have 2048 bits key or 4096 bits key. ■ If the PEM file certificate is encrypted then the passphrase must be provided while importing the certificate into VMware Aria Suite Lifecycle.
Generate CSR	<ul style="list-style-type: none"> a Enter the required text boxes. b Select the length of the key. c Enter a valid domain name. You can also include the wildcard certificate. For example, you can enter <code>*.sql.local</code>. d Enter the IP address in which you are assigning the certificate. <p>Note Generate CSR downloads a PEM file. This file can be taken to the certificate authority for signing and can be made as a trusted certificate. The pem file downloaded will have the private key and certificate request chain. You must be cautious and share only the CSR part of the pem file but not the key for the certificate signing.</p>

3 Click **Generate**.

4 You can click the certificate from the inventory to view the details and its associated environments with their products.

5 To download or replace the certificate, click the vertical ellipses on the certificate.

Results

VMware Aria Suite Lifecycle generates a new certificate for the specific domain provided by the user.

Assign the certificate administrator role in VMware Aria Suite Lifecycle

Using VMware Aria Suite Lifecycle, you can create a certificate admin who is a user or a group with a specific role assigned. These users or group of users can have certain privileges to access the certificate for any VMware Aria Suite product.

In VMware Aria Suite Lifecycle, you can delegate the certificate replacement operations to any users in a consistent manner across products. You can also allow non-admin users to perform actions such as replacing the certificate.

Prerequisites

- Verify that there are users or group of users available and such users should not have any prior roles mapped.

Procedure

- 1 On the **Lifecycle Operations** page, click **User Management**.
- 2 Navigate to **User Management** and click **ADD USER/GROUP**.
- 3 Enter a user or a group name and the user list is auto-populated.
If a user already has a role mapped from the selected user, then select another user.
- 4 Click **Next**.
- 5 Select the **Certificate Administrator** role and click **Next**.
- 6 Click **Submit**.
- 7 Log out from VMware Aria Suite Lifecycle and log in as VMware Workspace ONE Access user to access the services as an assigned admin.

Replace your Workspace ONE Access certificate by using VMware Aria Suite Lifecycle

Use this procedure to replace the VMware Identity Manager certificate or the globalenvironment setting in your VMware Aria Suite Lifecycle environment.

Note The VMware Identity Manager and Workspace ONE Access terms are used interchangeably in VMware Aria Suite Lifecycle product documentation.

For related information about replacing certificates for VMware Aria Suite Lifecycle, see [Replace certificate for VMware Aria Suite Lifecycle products](#).

Note To replace a certificate on a clustered deployment, you must manually replace the certificate on the load balancer. If you encounter an error while replacing the certificate and you are running Workspace ONE Access version 3.3.7, see <https://ikb.vmware.com/s/article/94095>.

Generate a self-signed certificate

Use the Locker service to generate a Certificate Signing Request (CSR) and create a .pem file. With information from the .pem file, you import the certificate into the VMware Aria Suite Lifecycle locker .

- 1 From the My Services dashboard, click **Locker**.
- 2 Click **Generate CSR** and enter the name `globalenvironment`.
- 3 Enter customer-specific values for all required fields on the Generate CSR form and click **Generate** to generate the .pem file.

A sample form is shown below.

The screenshot shows the 'Generate CSR' form in the VMware Aria Suite Lifecycle Locker interface. The form is titled 'Generate CSR' and is located under the 'Certificates' section. The breadcrumb navigation is 'Home > Certificates > Generate CSR'. The form contains the following fields and options:

- Name ***: globalenvironment
- Common Name (CN) ***: vidm.cap.org
- Organization (O) ***: CAP
- Organization Unit (OU) ***: CAP
- Country Code (C) ***: SG
- Locality (L)**: SG
- State (ST)**: SG
- Key Length**: 2,048 bits 4,096 bits
- Server Domain/ Hostname**: vidm.cap.org
Either server domain/FQDN or IP address is required.
- IP Address**: 10.109.44.191
Either server domain/FQDN or IP address is required.

At the bottom of the form, there are two buttons: **GENERATE** and **CANCEL**.

Note To replace your certificate in a clustered environment, enter multiple domain names and IP addresses, separated by commas.

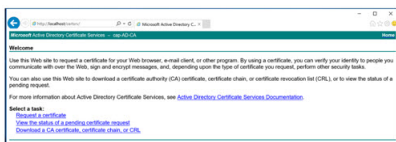
A .pem file contains a certificate signing request and a private key as in the example below with certificate and key details removed.

```
-----BEGIN CERTIFICATE REQUEST-----
...
-----END CERTIFICATE REQUEST-----
-----BEGIN PRIVATE KEY-----
...
-----END PRIVATE KEY-----
```

- 4 Submit the .pem file to a signing authority to request that it be signed. If you do not have a configured signing authority, perform the following steps.

In this example, the signing authority is the Microsoft Active Directory Certificate Service and it is configured for <http://localhost/certsrv/>.

- a Open <http://localhost/certsrv/>.
- b Click **Request a Certificate > Advance Certificate Request**.
- c For this example, click **Request a certificate**.



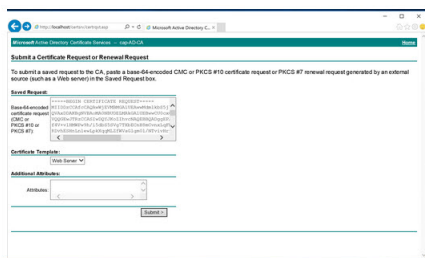
- d Click **Advanced certificate request**.



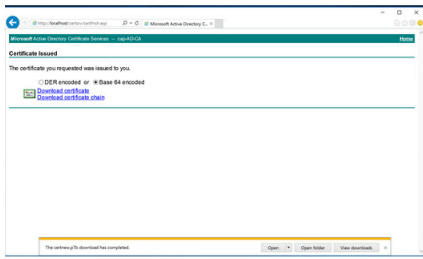
- e Click the **Submit a certificate request using base64 encoded ...** option.



- f Paste the certificate .pem file content from your certificate request and click Submit.



- 5 After the .pem is submitted, you are prompted to download a certificate. Select the **Base64 encoded** certificate format and select both the **Download certificate** and the **Download certificate chain** options.



This actions downloads `certnew.cer` for the certificate and `certnew.p7b` for the certificate chain. In this example, they are downloaded to a user downloads folder of `C:\USERS\ARUN\DOWNLOADS`. An example of both are provided below:

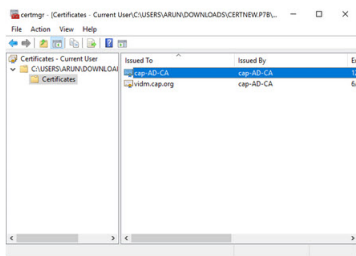
- `certnew.cer` - certificate

```
Reference: certnew.cer
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
```

- `certnew.p7b` - certificate chain

```
Reference: certnew.p7b
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
```

6 The root certificate is needed. In this example, an existing server certificate named `cap-AD-CA` exists and an existing root certificate of `vidm.cap.org` exists and both were issued by a signing authority of `cap-AD-CA`.



7 Split this into the `globalenvironment` certificate and the root certificate by using the *Copy To File* function. The certificates involved are `certnew.cert`, `globalenvironmentcert.cert`, `rootcert.cert` and the `certnew.p7b` certificate chain.

certnew	6/21/2023 4:16 PM	Security Certificate
certnew	6/21/2023 4:16 PM	PKCS #7 Certificat...
globalenvironmentcert	6/21/2023 4:18 PM	Security Certificate
rootcert	6/21/2023 4:18 PM	Security Certificate

8 Import the `globalenvironment` certificate into the VMware Aria Suite Lifecycle Locker service:

- Click **Locker** from the VMware Aria Suite Lifecycle My Services page
- Click **Certificates > Import**.

- c The Import Certificate page appears. In the **Name** field, enter `globalenvironment`.
- 9 Using the extracted `globalenvironment` and root certificate as source, open Notepad ++ or any other text editor and create a certificate chain with two certificate sections: the server certificate content at the top followed by the root certificate content . The example below shows the two sections with details removed.

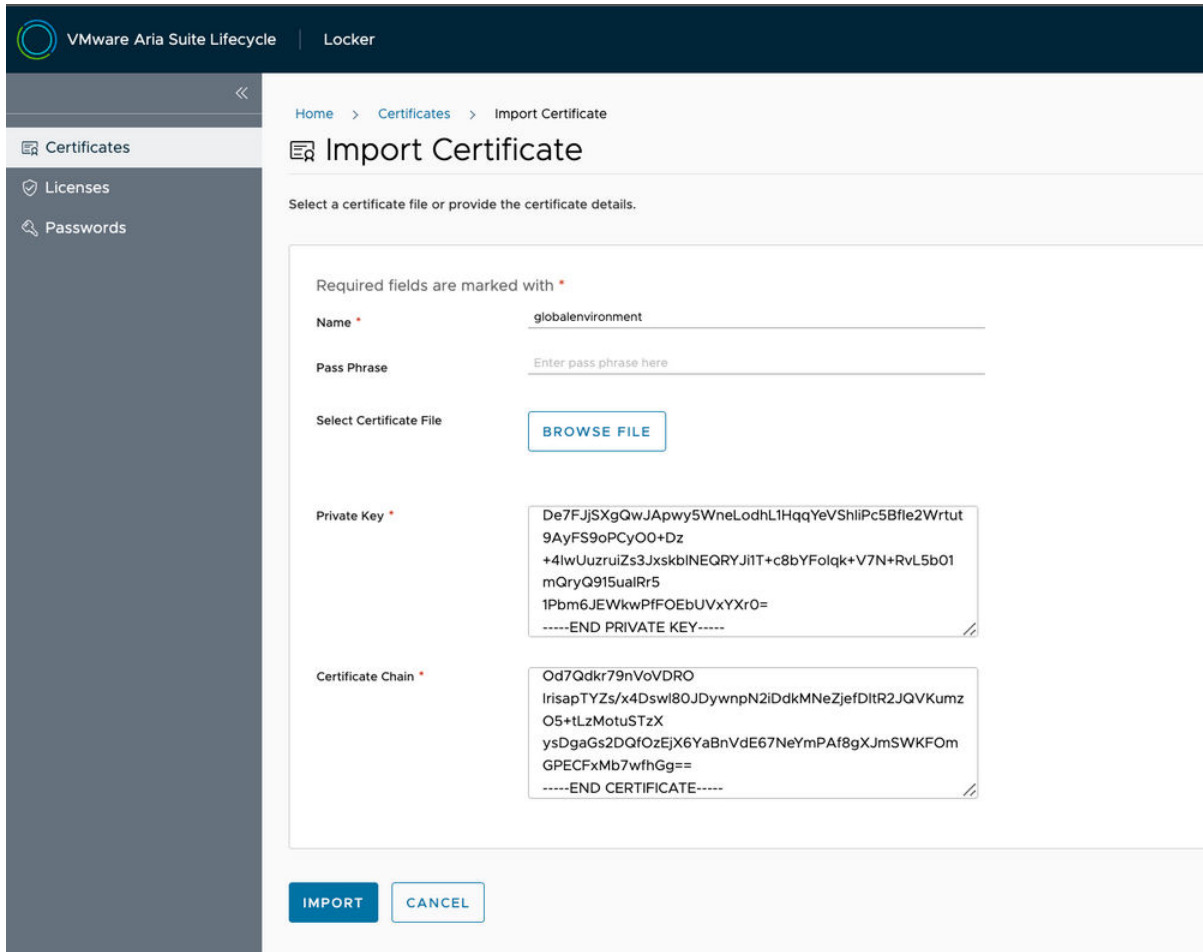
```

-----BEGIN CERTIFICATE-----
...
###server certificate content###
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
...
###root certificate content###
...
-----END CERTIFICATE-----

```

- Copy and paste the private key content from the `.pem` file created by the generated CSR into the **Private Key** section of the Import Certificate form.
 - Copy and paste the content with the two certificate sections into the **Certificate Chain** section of the Import Certificate form.
- 10 Verify the certificate chain by using a verification tool such <https://tools.keycdn.com/ssl>.
- 11 Click **Import** to import the new `globalenvironment` certificate into VMware Aria Suite Lifecycle.

A sample populated Import Certificate form is shown below.



When the import is successful, the **Certificate successfully added.** statement appears, as shown below.



12 You can display details about the successfully imported new certificate. A sample is shown below.

The screenshot displays the VMware Aria Suite Lifecycle interface. The top navigation bar includes the VMware logo and the text 'VMware Aria Suite Lifecycle | Locker'. Below this, a breadcrumb trail shows 'Home > Certificates > globalenvironment'. The main content area is titled 'globalenvironment' and has two tabs: 'Details' (selected) and 'References'. Under the 'Details' tab, the 'Certificate Details' section is visible, showing the following information:

Validity Period	
Expires In:	1 year, 11 months and 29 days
Expires On:	Friday, June 20, 2025 at 9:35:58 PM GMT+05:30
Issued On:	Wednesday, June 21, 2023 at 9:35:58 PM GMT+05:30
Healthy:	✔

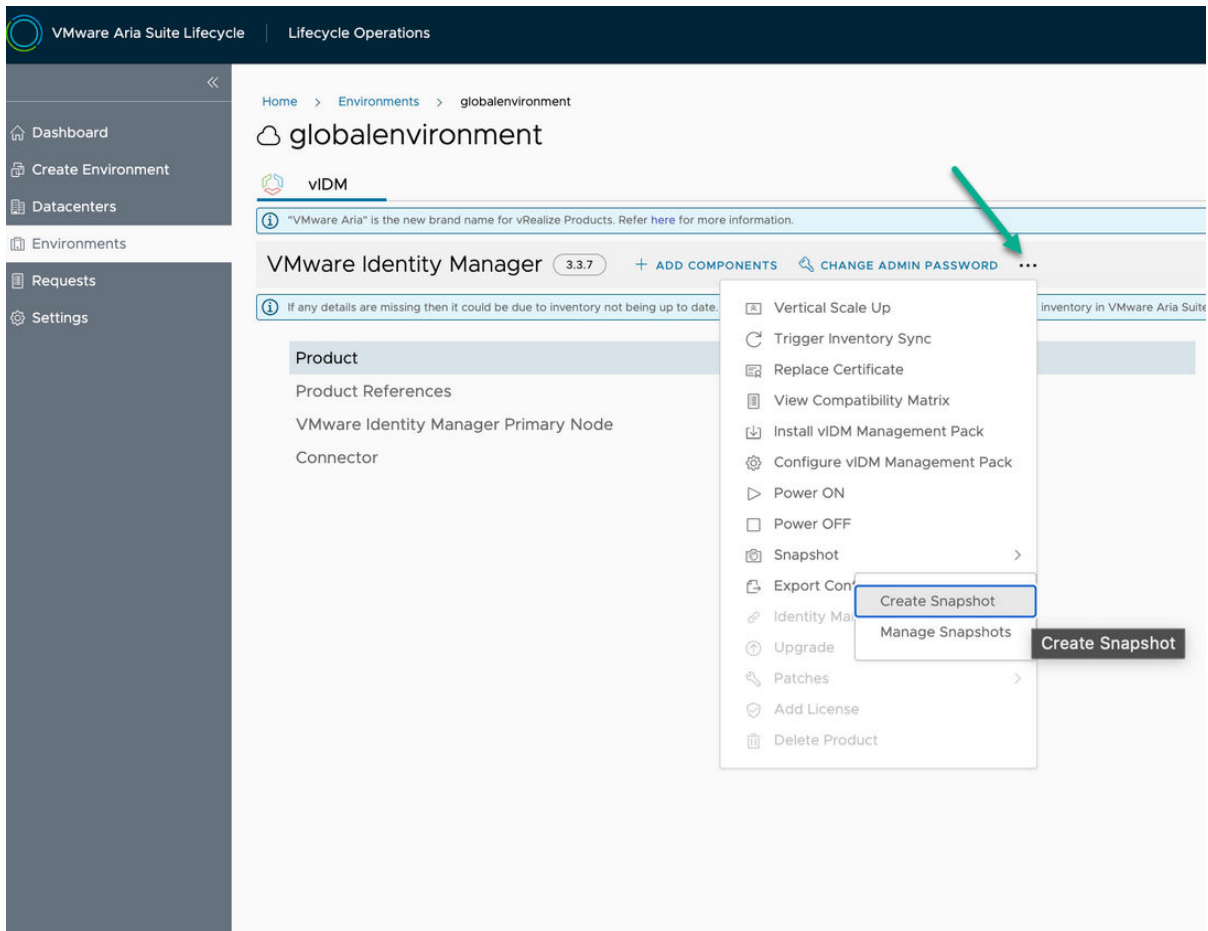
Below the validity period, the 'Certificate Information' section provides the following details:

Subject:	C=SG,ST=SG,L=SG,O=CAP,OU=CAP,CN=vidm.cap.org
Issuer:	DC=org,DC=cap,CN=cap-AD-CA
Subject Alternative Names:	IP: 10.109.44.191, DNS: vidm.cap.org
Algorithm:	SHA256WITHRSA
Key Algorithm:	RSA
Key Length:	2048
SHA256:	ca6096aee3d6907b67f8c9039a83a3ccc173b0550332a08fc58f3128e2b2dc6c
SHA1:	b54723fb26294fb50c1a9db416623b88ed4996d8

Create a snapshot of the environment

Before replacing your existing globalenvironment certificate with the new certificate, take a snapshot in the Lifecycle Operations service.

- 1 From the VMware Aria Suite Lifecycle dashboard, click **Lifecycle Operations**.
- 2 Click **Environments** and then click **View Details** on the globalenvironment tile.
- 3 Click the 3 dot ellipse (...) following the Change Admin Password option and select **Snapshot > Create Snapshot** from the drop-down menu.



- 4 For this example, enter `Snapshot Before Cert Replacement` in the **Snapshot Prefix** field **Description** fields.
- 5 Switch the **Shutdown before taking snapshot** option to the on position and click **Next**.

Create Snapshot

Snapshot Details

Precheck

Snapshot Details

Ensure that the appliances are in a consistent state before triggering snapshots

Downtime Alert: During shutdown before snapshot, VMware Identity Manager and Single Sign-On for products integrated with VMware Identity Manager will not be available.

Required fields are marked with *

Snapshot Prefix * Snapshot Before Cert Replacement

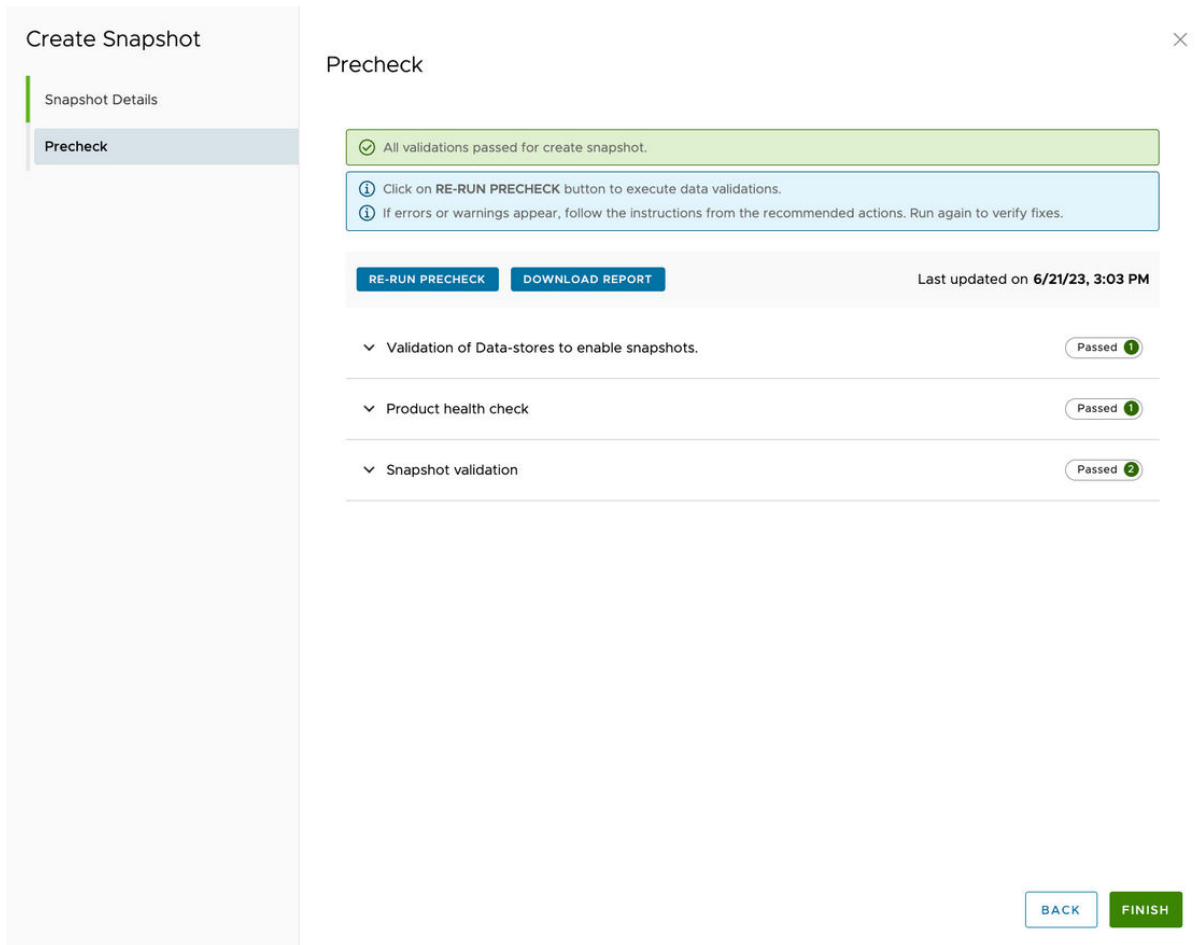
Snapshot Description Snapshot Before Cert Replacement

Snapshot With Memory

Shutdown before taking snapshot

NEXT

- 6 When prompted, click **Run Precheck**.
- 7 When the precheck result is returned, click **Finish**.

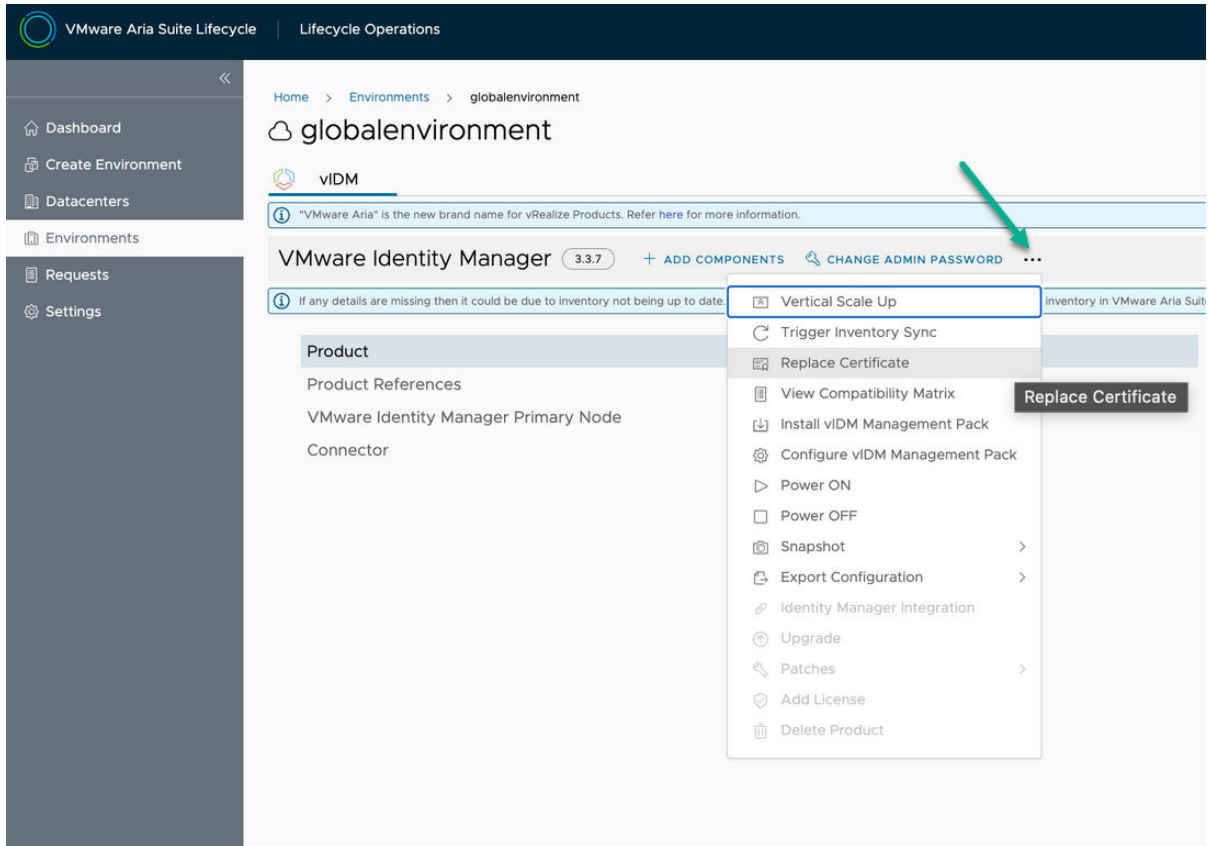


- 8 After you click **Finish**, the **Request Details** page automatically appears and displays the progression of each stage of the pre-check process.
- 9 When the snapshot request is complete, you can proceed to make the certificate replacement request.

Create the certificate replacement request

After you create the snapshot, you're ready to initiate the certificate replacement request and replace the existing standalone globalenvironment certificate with the new self-signed certificate.

- 1 On the VMware Aria Suite Lifecycle My Services page, click **Lifecycle Operations** and then click **Environments**.
- 2 Click **View Details** on the globalenvironment tile.
- 3 Click the three dot icon (...) in the VMware Identity Manager row and click **Replace Certificate** from the drop-down menu.

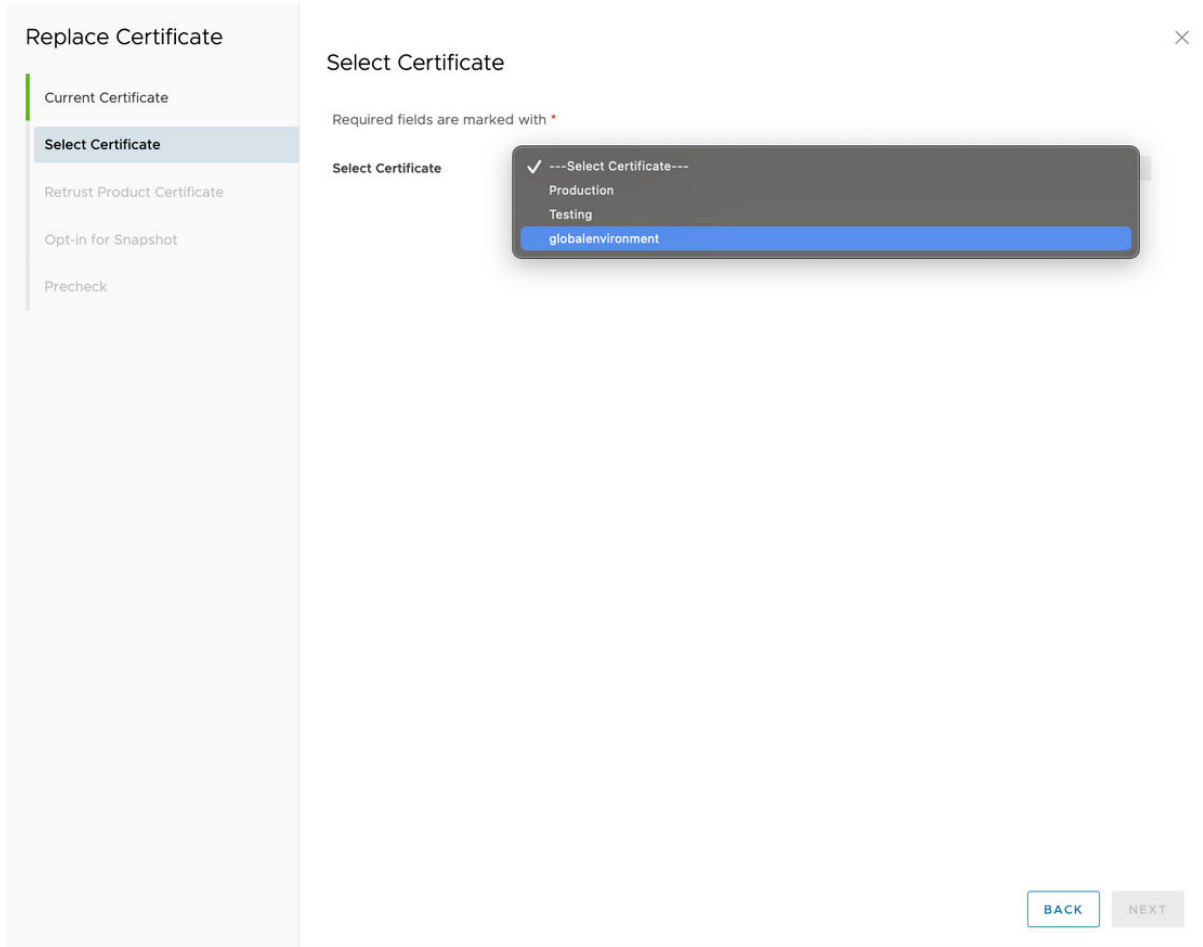


The **Current Certificate** details page appears. If you've never replaced the certificate, then this is the default certificate that was used during installation of the product.

- 4 On the resultant **Current Certificate** details page, click **Next**.

The **Select Certificate** page appears.

- 5 On the **Select Certificate** page, select **globalenvironment** from the drop-down menu.

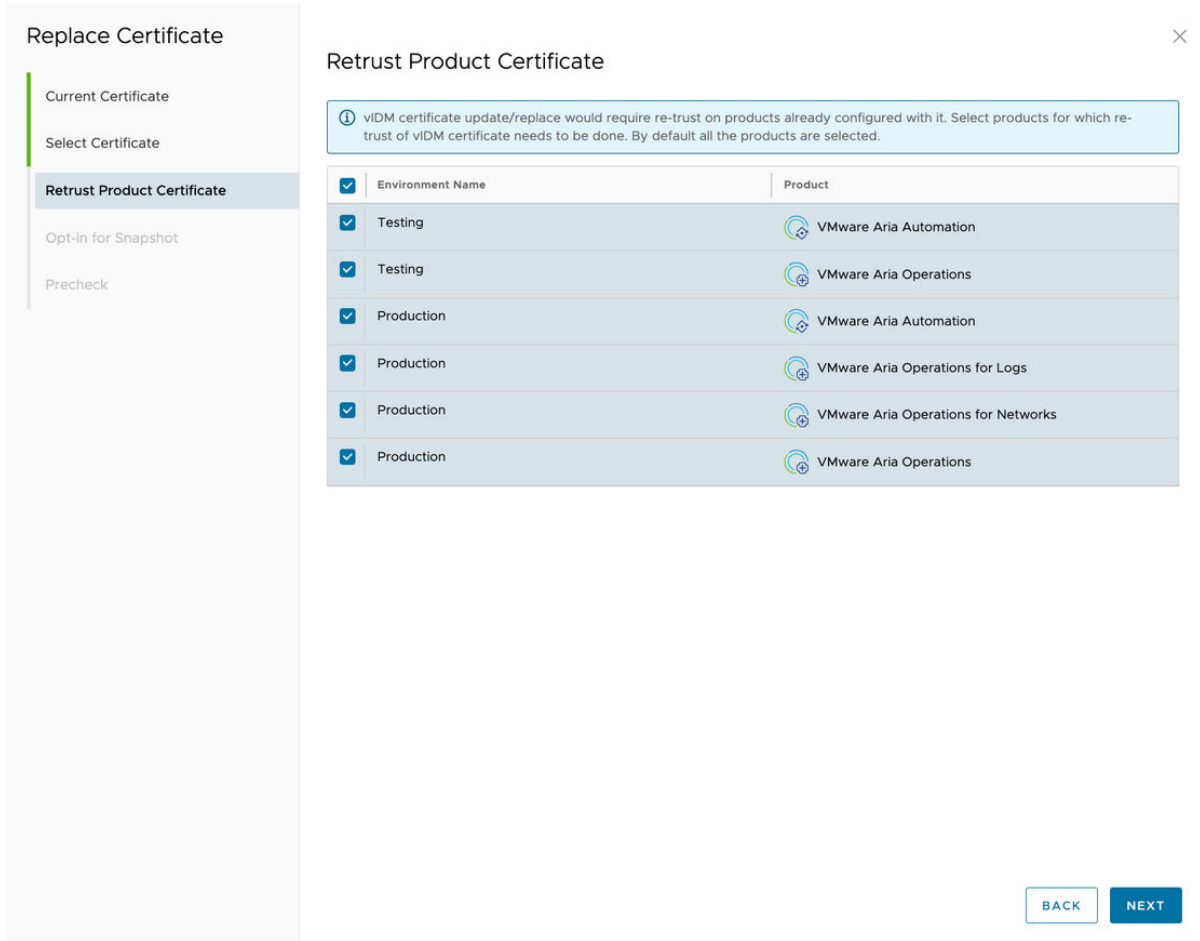


The **Select Certificate** details page appears.

- 6 On the resultant **Select Certificate** details page, click **Next**.

The **Retrust Product Certificate** page appears.

- 7 On the **Retrust Product Certificate** page, select all the products to be impacted by the retrust certificate action and then click **Next**.



The **Opt-in for Snapshot** page appears.

- 8 Click the **Opt-in for Snapshot** check box to enable the option and then click **Next**.

The **Precheck** page appears.

- 9 On the **Precheck** page, click **Run Precheck**.
- 10 If you are prompted to consent to a validation request, click **Re-run Precheck**.

Review the pre-check results and take any further actions that are needed as prompted on-screen.

Replace Certificate
✕

Current Certificate

Select Certificate

Retrust Product Certificate

Opt-in for Snapshot

Precheck

Precheck

		Resource	
✔ Passed	Validation of Datastores to enable snapshots for rollback.	Validation of Datastores to enable snapshots for rollback.	Datastore validation succeeded.

1 - 1 of 1 results | < < 1 / 1 > >

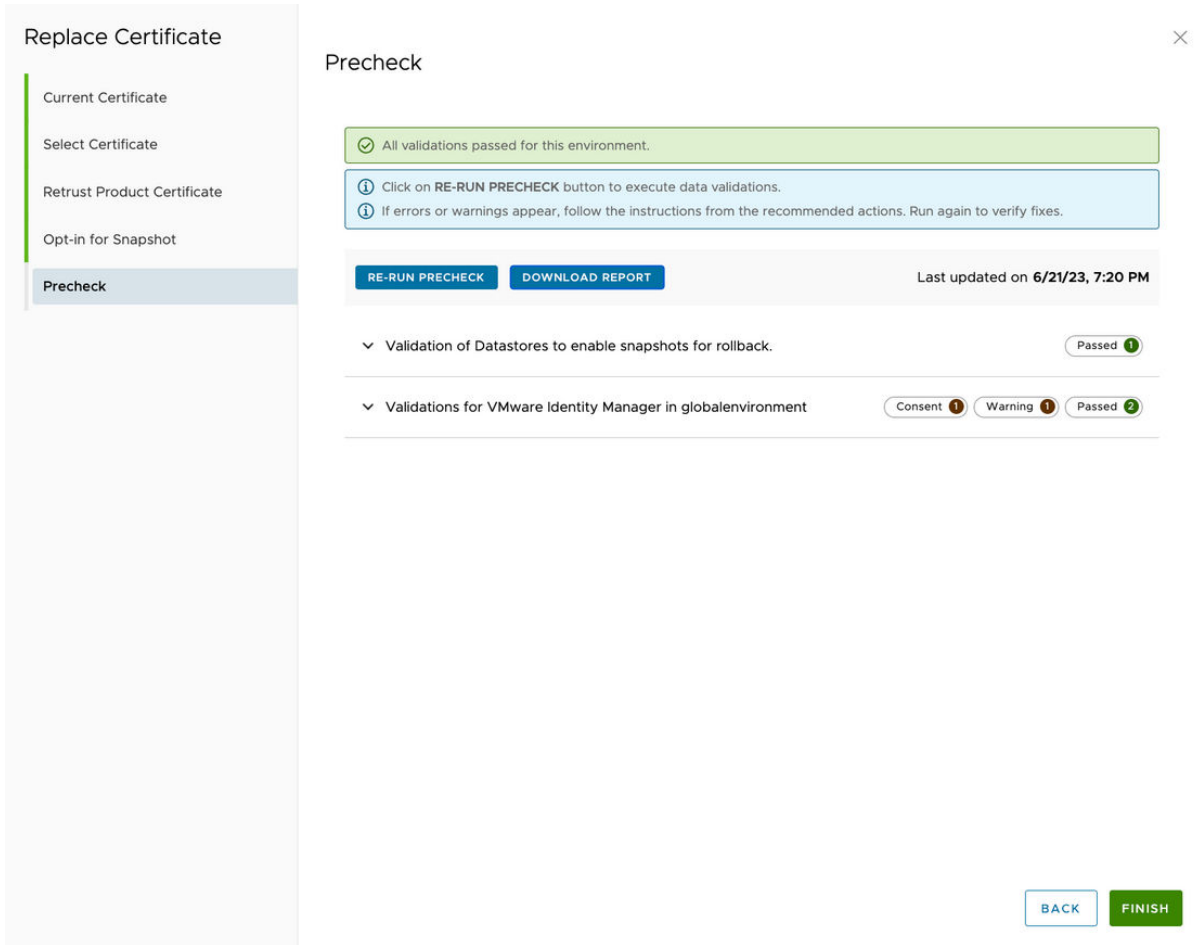
⤴ Validations for VMware Identity Manager in globaleenvironment Consent 1 Warning 1 Passed 2

Status	Check	Component / Resource	Result Description	Consent	Recommendations
👤 Consent	Validations for VMware Identity Manager in globaleenvironment	Validations for VMware Identity Manager in globaleenvironment	Product will be shutdown to take snapshots before applying new certificate. Please confirm if you want to proceed.	ACCEPT	
⚠ Warning	Validations for VMware Identity Manager in globaleenvironment	Validations for VMware Identity Manager in globaleenvironment	Re-establish trust between suite products.		
✔ Passed	certificate validation check	certificate validation check	Success. All the certificate validation passed		
✔ Passed	viDM health check	viDM health check	viDM health check validations passed		

1 - 4 of 4 results | < < 1 / 1 > >

BACK
FINISH

11 When all pre-check validations are complete, click **Finish** to submit the request.



12 You can monitor the request details status by selecting **Requests** in the Lifecycle Operations left pane menu. The stages of the replace certificate action are detailed below.

```

Stage-1
Gracefully Shut Down VMware Identity Manager
Start
Validate VMware Identity Manager Certificate
Start graceful shutdown of VMware Identity Manager
Prepare graceful shutdown of VMware Identity Manager nodes
Check power states of VMware Identity Manager nodes
Validate SSH credentials of VMware Identity Manager nodes
Update VMware Identity Manager node types
Extract vMoid of VMware Identity Manager nodes
Verify Identity Manager Appliance Health Check
Verify Identity Manager Postgres Health Check
Validate VMware Identity Manager node types
VMware Identity Manager stop horizon service
VMware Identity Manager stop Elasticsearch / Opensearch service
VMware Identity Manager stop pgpool service
VMware Identity Manager stop postgres service
Shutdown VMware Identity Manager nodes
Final

Stage-2
    
```

Create Node Snapshot

Start
Get vMoid using Virtual Machine
Virtual Machine Snapshot using vMoid
Final

Stage-3

Power on VMware Identity Manager Node(s)

Start
Validate VMware Identity Manager Certificate
Start Power On of VMware Identity Manager nodes
Prepare required inputs to power on VMware Identity Manager Node(s)
Extract vMoid
Power On VMware Identity Manager Node
Check Hostname/IP status of VMware Identity Manager
Get node endpoint of VMware Identity Manager
Final

Stage-4

Remediate VMware Identity Manager

Start
Start remediation of VMware Identity Manager
Prepare required inputs to remediate VMware Identity Manager
Validate ssh credentials of VMware Identity Manager
VMware Identity Manager start pgpool service
Update VMware Identity Manager node types
Check primary node status of VMware Identity Manager
VMware Identity Manager Appliance Health Check
Update VMware Identity Manager node details with VMware Aria Suite Lifecycle's
inventory
Final

Stage-5

Product Health Check

Start
Product Health Check prepare
vIDM health pre-Check
Final

Stage-6

Update Certificate on VMware Identity Manager

Start
Validate VMware Identity Manager Certificate
Start update of Certificate on VMware Identity Manager nodes
Update Certificate on VMware Identity Manager nodes
Final

Stage-7

Trust vIDM Certificate in LCM

Start
Add vIDM certificate to VMware Aria Suite Lifecycle trust store
Final

Stage-8

Revert to Node Snapshot

```
Start
Get vMoid
Final
```

Stage-9

```
Power On VMware Identity Manager Nodes
Start
Validate VMware Identity Manager Certificate
Final
```

Stage-10

```
Remediate VMware Identity Manager Nodes
Start
Start remediation of VMware Identity Manager
Prepare required inputs to remediate VMware Identity Manager
Validate ssh credentials of VMware Identity Manager
VMware Identity Manager start pgpool service
Update VMware Identity Manager node types
Check primary node status of VMware Identity Manager
VMware Identity Manager Appliance Health Check
Update VMware Identity Manager node details with VMware Aria Suite Lifecycle's
inventory
Final
```

Stage-11

```
Product Health Check
Start
Product Health Check prepare
Final
```

Stage-12

```
Delete Node Snapshot
Start
Get vMoid Delete Snapshot
Delete Node Snapshot
Final
```

Stage-13

```
Locker Reference Update
Start
Locker reference update init
Locker reference inventory update
Final
```

Stage-14

```
Product Replace Update Notification
Start
Start replace update notification
Replace certificate notification
Final
```

Stage-15

```
Validate if VMware Identity Manager re-trust is required on products
Start
Start Validate if VMware Identity Manager re-trust is required on products
```

```
Validate if VMware Identity Manager re-trust is required on products  
Final
```

Stage-16

```
Update VMware Identity Manager Auth provider hostname  
Start  
Start update auth provider hostname  
Trust VMware Identity Manager Certificate in VMware Aria Suite Lifecycle  
Update VMware Identity Manager Auth provider hostname  
Final
```

Stage-17

```
Retrust VMware Identity Manager on VMware Aria Automation  
Start  
Start VMware Identity Manager flow  
Check if vIDM root certificate is present on VMware Aria Automation  
Check for VMware Identity Manager availability  
Check for VMware Identity Manager Login Token  
Check for VMware Identity Manager Default Configuration User availability  
Configure VMware Identity Manager for VMware Aria Automation  
Configure Load Balancer for VMware Aria Automation  
Initialize VMware Aria Automation  
Update VMware Identity Manager allowed redirects  
Final
```

VMware Aria Operations reconfigure vidm

```
Start  
Start VMware Aria Operations - VMware Identity Manager reconfigure  
Reconfigure VMware Identity Manager  
Prepare Identity Manager catalog task  
Final
```

VMware Aria Operations for Logs retrust vidm

```
Start  
Start VMware Aria Operations for logs retrust vIDM  
Prepare Nodes  
Final
```

VMware Aria Operations for Networks Reconfigure vidm

```
Start  
Start VMware Aria Operations for Networks generic  
Validate and fetch VMware Aria Operations for Networks vidm client details  
vIDM get O Auth client details  
Reconfigure vIDM hostname  
Final
```

Stage-18

```
Re-trust VMware Identity Manager on VMware Aria Automation  
Start  
Start VMware Identity Manager flow  
Check if vIDM root certificate is present on VMware Aria Automation  
Check for VMware Identity Manager availability  
Check for VMware Identity Manager Login Token  
Check for VMware Identity Manager Default Configuration User availability  
Configure VMware Identity Manager for VMware Aria Automation
```

```

Configure Load Balancer for VMware Aria Automation
Initialize VMware Aria Automation
Update VMware Identity Manager allowed redirects
Final

```

```

VMware Aria Operations reconfigure vidm
Start
Start VMware Aria Operations - VMware Identity Manager reconfigure
Reconfigure VMware Identity Manager
Prepare Identity Manager catalog task
Final

```

- 13 When complete, confirm that the certificate is in use by clicking **Locker** from the **My Services** page of VMware Aria Suite Lifecycle and then select **Certificates > globalenvironment**.



You can also view VMware Aria Suite Lifecycle and VMware Identity Manager logs. The log statement `Applied certificate to vIDM..` indicates that the VMware Identity Manager services are being restarted.

Replace your self-signed VMware Aria Suite Lifecycle certificate

As an VMware Aria Suite Lifecycle admin, you can change the certificate for your VMware Aria Suite Lifecycle instance.

Prerequisites

Verify that you have an existing VMware Aria Suite Lifecycle certificate available.

Procedure

- 1 On the My Services dashboard, click **Lifecycle Operations**.
- 2 Navigate to **Settings** and click **Change Certificate**.
You can view the certificate details that are used by the VMware Aria Suite Lifecycle.
- 3 To replace the certificate, click **REPLACE CERTIFICATE**.
 - a Read the summary of the current certificate and click **Next**.
 - b Select a certificate from the drop-down menu and click **Next**.
 - c Click **Run Precheck** to validate your certificate details and click **Finish**.
- 4 After you click **Finish**, you can view the progress of the certificate changing on the **Request Details** page.

Replace your VMware Aria Suite Lifecycle custom certificate

If you use a custom certificate for VMware Aria Suite Lifecycle instead of default self-signed certificate, you can replace the VMware Aria Suite Lifecycle certificate.

Prerequisites

- A X509 PEM base-64 encoded certificate and private key. Verify that the private key is not encrypted.
- A machine with an SSH access to VMware Aria Suite Lifecycle, and software such as PuTTY and an SCP software such as WinSCP installed on it.

Procedure

- 1 Rename the certificate to `server.crt` and private key to `server.key`.
- 2 Open a Secure Shell connection VMware Aria Suite Lifecycle appliance as root user.
- 3 Copy the certificate files `server.crt` and `server.key` to the `/opt/vmware/vlcm/cert` folder. You can use an SCP software like WinSCP on Windows. Make sure to backup the original files before copying.
- 4 After copying the certificates, restart the VMware Aria Suite Lifecycle proxy services to update the appliance certificate.
 - a Restart the system services by executing the following command in the SSH session:


```
systemctl restart nginx.
```
 - b Check the status of the system services by executing the following command in the SSH session: `systemctl status nginx.`
- 5 After restarting the services, verify that the certificate is updated on the appliance, open a browser and go to `https://lcm-server-host`.
- 6 Verify that you see the new certificate in the browser.

Manage licenses for a VMware Aria Suite Lifecycle products

The VMware Aria Suite Lifecycle Locker allows you to manage licenses for the various suite products.

Prerequisites

Verify that a license is already available.

Procedure

- 1 From the VMware Aria Suite Lifecycle My Services dashboard, click **Locker**.
- 2 Click **Licenses**.

Existing licenses are listed, along with the their health status, expiry value, account, type, and description.
- 3 To add a license, click **Add License Manually**.
- 4 Enter the alias in the **License Alias** text box.
- 5 Enter the **License Key** and click **Validate**.

- 6 After you validate the accuracy of the license, click **Add**.
- 7 To display license details, click on the License Alias name or click the vertical ellipses in the specific license row and then click **Details** from the drop-down menu.
- 8 To update an existing license, click the vertical ellipses in the specific license row and then click **Update License** from the drop-down menu.
 - a Review the current license summary page and click **Next**.
 - b Select an environment from the references table and click **Next**.
 - c Select a license from the drop-down menu and click **Finish**.
- 9 To delete a license, click the vertical ellipses in the specific license row, and click **Delete** from the drop-down menu.
 - a If VMware Aria Suite Lifecycle has one or more My VMware accounts configured, then the corresponding license keys are automatically synced. To sync licenses from My VMware account, click **Retrieve Licenses**. However, if you have manually added the same license key to the locker then the corresponding entry from My VMware account cannot be captured.
 - b When any product is imported into VMware Aria Suite Lifecycle, the license keys present in the product are also captured and stored in the Locker under **Licenses**. If the same license key is already present, then it cannot be imported.
 - c If any product is associated to a license in VMware Aria Suite Lifecycle then the license entry cannot be deleted from the Locker.
 - d VMware Aria Suite Lifecycle does not restrict applying multiple licenses to any product, however, the product behavior does allow to set only one license key as active at anytime.
 - e Deleting a license from VMware Aria Suite Lifecycle Locker does not remove the license key from the product itself.
- 10 License keys can be applied to products managed by VMware Aria Suite Lifecycle from **Home > Environments** under **Lifecycle Operations**. Select a product from any managed environment, click the horizontal ellipses on the product name, select **Add License**, and follow the steps.

Manage passwords for VMware Aria Suite Lifecycle products

The VMware Aria Suite Lifecycle Locker allows you to manage passwords for VMware Aria Suite Lifecycle products.

The VMware Aria Suite Lifecycle Locker stores all the passwords that are used across the VMware Aria Suite Lifecycle products.

Add the passwords for adding vCenter, product deployments, products import, My VMware, and product password update. You can configure a password at the locker level and are retrieved from the UI.

Procedure

- 1 From the VMware Aria Suite Lifecycle My Services dashboard, click **Locker**.
- 2 Click **Passwords**.
- 3 To add a password, click **Add**.
 - a Enter the **Password Alias** and **Password**.
 - b To confirm, re-enter the Password and enter **Password Description**, and a valid **User Name**.

Note The user name text box is mandatory for adding the vCenter into VMware Aria Suite Lifecycle.

- c Click **Add**.
- 4 To view, copy an ID, edit, or delete a specific password, use the vertical ellipse drop-down menu at the right of each password row as described in the following table.

Function	Description
View Password	You can view the selected password in plain text if you are an Admin user, after you authenticate the VMware Aria Suite Lifecycle SSH root password. This option is not available for Workspace ONE Access users.
Copy ID	You can copy the password ID and reuse it. For example, when exporting JSON for product deployment, you can copy and reuse the existing password ID.
Edit Password	You can edit a password that does not reference an existing password.
Delete Password	You can delete a password that is no longer used and does not have any references.

If you select an existing password, you can view its details and references. The **Details** tab displays the password identifier, user name, description, creation date, and last updated date. The **References** tab displays referenced environments at the product and node level, vCenter passwords in data centers, and other passwords that are used in the **Settings** tab.

You can also update a password for products, nodes, MyVMware ([VMware Customer Connect](#)), proxy, and vCenter instances. To update the password, click the vertical ellipses (⋮) for the selected password.

Note

- When you update a password that is managed by VMware Aria Suite Lifecycle, the password is updated on the **Passwords** page and in the VMware Aria Suite Lifecycle inventory.
 - When you update a password for vCenter, MyVMware ([VMware Customer Connect](#)), proxy, or VMware Workspace ONE Access configuration administrators, the password is updated only in the VMware Aria Suite Lifecycle inventory.
-

Add and manage data center associations for VMware Aria Suite Lifecycle

To back up your private cloud environments, add a data center to VMware Aria Suite Lifecycle.

Procedure

- 1 From the VMware Aria Suite Lifecycle My Services page, click **Lifecycle Operations**.
- 2 Click **Datacenters** to display the list of data centers that are configured for your environment.
- 3 To add a new data center, click **Add Datacenter**.
 - a Enter the **Datacenter Name** and provide a **Location**.
 - b Click **Save**.
- 4 To delete a datacenter, select the **Delete** icon in the datacenter row that you want to delete.

Note If there are any INITIATED, IN PROGRESS or COMPLETED requests for an environment, then you cannot delete a data center. If it has a FAILED request, or request related to vCenter, such requests are archived.

- 5 Other options include editing and adding a vCenter, importing a datacenter, and viewing and discovering environments and products.

What to do next

To add a vCenter to the data center, see [Add a vCenter to a Data Center](#).

Assign a user role in a vCenter for VMware Aria Suite Lifecycle

Create a user role in the vSphere client with privileges that are required for VMware Aria Suite Lifecycle. The same role can be assigned to the user who can add a vCenter in VMware Aria Suite Lifecycle.

Prerequisites

Verify that you have administrative privileges to add a role to a user or a user group. You must have administrative privileges to use vCenter.

If you are using vCenter deployed on VMware Cloud on AWS SDDC, then you must use the available CloudAdmin role. For more information about VMware Cloud on AWS on vCenter, refer to the [VMware Cloud on AWS](#) product documentation.

When you deploy a VMware Cloud on AWS on vCenter, you can use the default CloudAdmin role. To learn more about cloud administrator privileges, refer to [CloudAdmin Privileges](#) documentation.

Procedure

- 1 Log in to vCenter by using the vSphere client.
- 2 On the home page of vSphere client, click **Roles** under **Administration**.
- 3 Create a role for all system interactions between VMware Aria Suite Lifecycle and vCenter.
- 4 Clone **Read-only** and provide a name to the role.
- 5 In the **Create Role** dialog box, configure the role using the following configuration settings, and click **Next**.

Setting	Value
Role Name	VMware Aria Suite Lifecycle
Privilege	<ul style="list-style-type: none"> ■ Datastore <ul style="list-style-type: none"> ■ You can select All privileges. ■ Host.Local <ul style="list-style-type: none"> ■ Operations- Add Host to vCenter ■ Operations - Create Virtual Machine ■ Operations - Delete Virtual Machine ■ Operations - Reconfigure Virtual Machine ■ Inventory - Modify - Cluster ■ Network <ul style="list-style-type: none"> ■ Assign Network ■ Resource <ul style="list-style-type: none"> ■ Assign vApp to Resource Pool ■ Assign Virtual Machine to Resource Pool ■ vApp <ul style="list-style-type: none"> ■ You can select All privileges. ■ Virtual Machines <ul style="list-style-type: none"> ■ You can select All privileges. ■ Content Library <ul style="list-style-type: none"> ■ You can select All privileges.

This role inherits the System Anonymous, System View, and System Read privileges.

Note You should have permissions to create a content library. The content library uses a datastore to store all templates, so you require permission to access, read, and write on the same datastore. All privileges under datastore and content library are needed.

- 6 Provide a name to the new role and click **Finish**.
- 7 Select **Global Permissions** under **Administration** and click **Manage**.
- 8 To add permissions, click the plus sign.
- 9 Select the user and role that you have created, and click **OK**.

Add a vCenter to a VMware Aria Suite Lifecycle data center

Add a vCenter to a data center before using the vCenter to create a private cloud environment in VMware Aria Suite Lifecycle.

Prerequisites

Ensure that you have the vCenter fully qualified domain name, user name, and password.

Procedure

- 1 On the left pane, click **Datacenters**.
- 2 To add a vCenter, on the **Datacenters** page, click **+ Add** for the vCenter.
- 3 Enter the vCenter **Name** and **vCenter FQDN**.
- 4 Click **Select Credentials** for the vCenter.
 - a You can either search for an existing vCenter credentials or add new credentials using the + sign .
 - b Click the + sign on the right corner to assign a password for the selected vCenter credential.
 - c Enter the Password details and click **Add**.
- 5 Enter the vCenter **User Name** for the vCenter.
You should have the required vCenter privileges.
- 6 Select the vCenter **Type**.
 - Management: All VMware SDDC Suite products are managed by this vCenter type.
 - Workload: All the payload or business related VMs are managed by this vCenter type.
 - Consolidated Management and Workload: Is a vCenter type, where both VMware SDDC Suite products and payload VMs are managed together.

The vCenter type selection is used only for classification; the setting has no associated product functionality.

- 7 Click **Validate** and **Save** the changes.
- 8 To import vCenter instances, click **Import**.
 - a Select the .CSV file and click **Import**. You can upload only one file at a time for a bulk import of vCenter instances in a selected data center.
 - b Click **Submit**.

What to do next

Go to the **Requests** page to see the status of this request. When the status is **Completed**, you can use this vCenter to create environments.

Remove a vCenter from a VMware Aria Suite Lifecycle data center

You can delete a vCenter from the VMware Aria Suite Lifecycle data center that is not used by the environment.

Prerequisites

Verify that the vCenter does not have a reference, such as a fully qualified domain name or a user name associated with an environment. If vCenter is associated with an environment, the delete option is not available for the vCenter.

Procedure

- 1 On the **Data Center** page, select the vCenter, and click **Delete** vCenter.
- 2 Click **Delete** to remove the selected vCenter.

Install and configure VMware Aria Suite Lifecycle on VMware Cloud on AWS

VMware Aria Suite Lifecycle supports a VMware Cloud on AWS environment. VMware Cloud on AWS is an integrated private cloud offering developed by VMware and Amazon Web Services (AWS).

You can install VMware Aria Suite Lifecycle in a VMware Cloud on AWS environment by using the using the VMware Aria Suite Lifecycle VMware Aria Automation Easy Installer. For more information, refer to the [Easy Installer](#) product documentation. Configure a virtual machine on the vCenter of a VMware Cloud on AWS software-defined data center (SDDC) to launch the VMware Aria Automation Easy Installer.

To create a cloud SDDC by using VMware Cloud on AWS and to connect the SDDC to the data center of your product, refer to [Getting Started with VMware Cloud on AWS](#) documentation. After you have successfully deployed VMware Aria Suite Lifecycle on VMware Cloud on AWS, you can also install other VMware Aria Suite products for use with VMware Cloud on AWS, such as VMware Workspace ONE Access and VMware Aria Automation.

On a VMware Cloud on AWS environment, you must add the SDDC vCenter as an endpoint only. Adding a vCenter that is external to the SDDC is not recommended. When you deploy a VMware Cloud on AWS vCenter, ensure that you have cloud administrator privileges. To learn more about cloud administrator privileges, refer to the [CloudAdmin Privileges](#) documentation.

Add an NSX load balancer

When using VMware Aria Suite Lifecycle or other VMware Aria Suite products that are deployed with VMware Cloud Foundation in a clustered environment, you can add one of the following NSX load balancer types:

- VCF managed NSX-T
- NSX Advanced load balancer, previously named Avi Networks load balancer and used by VMware Aria Automation, VMware Aria Operations, and VMware Identity Manager, VMware Aria Suite Lifecycle.
- Others

Before deploying the VMware Aria Suite product, add a load balancer to your VMware Aria Suite Lifecycle configuration as described in the following procedure.

Prerequisites

- Verify that you have the FQDN for the load balancer.
- To deploy an NSX Advanced load balancer:
 - Verify that you have deployed an NSX Advanced Load Balancer outside of VMware Aria Suite Lifecycle.
 - Verify that the NSX Advanced Load Balancer controller is configured with an NSX-T cloud account.

Procedure

- 1 Log in to VMware Aria Suite Lifecycle.
- 2 On the **My Services** dashboard, click **Lifecycle Operations**.
- 3 In the navigation list at the left, select **Settings**.
- 4 On the **System Administration** page, click **Load Balancer**.

- 5 The **Configure Load Balancer** page appears.
- a Click **Add Load Balancer**.
 - b Select the **Controller Type** and specify the controller type settings.
 - If adding a **NSX Advanced Load Balancer**, specify:

Field	Description
Controller FQDN	FQDN of the NSX Advanced Load Balancer Controller
Controller IP	IP Address of the NSX Advanced Load Balancer Controller
Username	Username for the NSX Advanced Load Balancer Controller
Password	Password for the NSX Advanced Load Balancer Controller Note Select a password from the VMware Aria Suite Lifecycle locker. If it is not listed, then use click here to create the password object and make the selection.
NSX Cloud Account	NSX-T Cloud account
Load Balancer IP	IP address that will be used to create the virtual service on the NSX Advanced Load Balancer Controller
Load Balancer FQDN	Load balancer FQDN that will be used to deploy the product

- If adding a **VMware Cloud Foundation managed NSX-T** or **Others**, specify the load balancer FQDN.
- c Click **Add**.

Results

You have created a load balancer configuration that you can use to install a product in a clustered deployment. See [Create a new private cloud environment using the installation wizard in VMware Aria Suite Lifecycle](#).

Working with the Identity and Tenant Management service in VMware Aria Suite Lifecycle

Use user and identity management options to map users in VMware Workspace ONE Access to roles that are available in VMware Aria Suite Lifecycle.

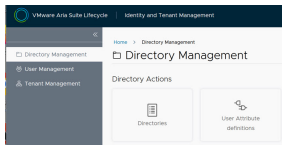
Note that the VMware Identity Manager and Workspace ONE Access terms are used interchangeably in VMware Aria Suite Lifecycle product documentation.

Configuring VMware Workspace ONE Access is a mandatory process before you install any VMware Aria Suite products. If you have not installed VMware Workspace ONE Access when installing VMware Aria Suite Lifecycle, you are prompted to configure and proceed.

Deployment of an identity manager through VMware Aria Suite Lifecycle is performed either through a single node or a cluster with an internal PostgreSQL database embedded in the appliance and does not support an external database like Microsoft SQL. VMware Aria Suite Lifecycle supports scale-out of VMware Workspace ONE Access. For more information, see [Scale out Workspace ONE Access for high availability in VMware Aria Suite Lifecycle](#).

After you deploy a global environment successfully, you can view the following options in the **VMware Aria Suite Lifecycle > Identity and Tenant Management** service.

- Directory Management
- User Management
- Tenant Management



The following roles are available and visible on the **User Management** page:

- LCM Cloud Admin
- Content Developer
- Content Release Manager
- Certificate Administrator

Although the VMware Aria Suite Lifecycle Cloud Admin has access to the VMware Workspace ONE Access service, only a few services in the **VMware Aria Suite Lifecycle > Lifecycle Operations > Settings** tab (for example, **NTP Server Setting**, **SNMP**, **DNS**, **My VMware**, and **Binary Mapping**) are accessed.

Only the **LCM Cloud Admin** role and the `admin@local` user have access rights to all the settings in the **Identity and Tenant Management** service. The default `admin@local` user is the only application administrator who can modify the **User Management** service, which in turn handles the **Directory Management** and **Identity Management** services.

Note With migration from earlier versions of VMware Aria Suite Lifecycle to the current VMware Aria Suite Lifecycle version, the VMware Workspace ONE Access Admin and VMware Workspace ONE Access Cloud Admin roles are converged into VMware Workspace ONE Access Cloud Admin. All users who were part of VMware Workspace ONE Access Admin in the previous versions of VMware Aria Suite Lifecycle would now become VMware Workspace ONE Access Cloud Admin in VMware Aria Suite Lifecycle.

Adding VMware Workspace ONE Access is an optional step and by configuring VMware Workspace ONE Access with single sign-on across VMware Aria Suite Lifecycle and products can be achieved.

Note When VMware Workspace ONE Access is used with VMware Aria Suite Lifecycle, only **Active Directory over LDAP** and **Active Directory with IWA** are used to sync users and groups to the VMware Workspace ONE Access service. Active Directory over LDAP and Active Directory with IWA are the only supported directory integration.

Manage directories for VMware Identity Manager in VMware Aria Suite Lifecycle

You can integrate your enterprise directory with VMware Identity Manager to sync users and groups to the VMware Workspace ONE Access service. Updates made in the directory configuration from VMware Aria Suite Lifecycle are reflected in VMware Workspace ONE Access.

You can create, read, update, and delete directories in VMware Workspace ONE Access.

VMware Aria Suite Lifecycle uses the terms VMware Workspace ONE Access and VMware Identity Manager interchangeably.

Options available under the directory management include the following.

- **Directories** - You can create and manage Active Directories on VMware Aria Suite Lifecycle. You can create one or more directories and sync them with their enterprise directories. With view directory, you can check sync logs and sync alerts apart from showing basic directory metadata. The directory edit allows an update for the mapped attributes, user, and group DNs. You can delete a directory configuration from VMware Aria Suite Lifecycle.
- **User Attribute Definitions** - The user attributes lists the default user attributes that sync in the directory and you can add other attributes that you can map to Active Directory attributes.

Note Directory Management is managed by the default VMware Aria Suite Lifecycle admin user - admin@local.

Supported directories

- Active Directory over LDAP - If you plan to connect to a single Active Directory domain environment, create this directory type
- Active Directory, Integrated Windows Authentication - Create this directory type if you plan to connect to a multi-domain or multi-forest Active Directory environment.
- Secure LDAP

Note For a FIPS-enabled VMware Workspace ONE Access, the bind password must be of fourteen characters.

To configure your enterprise directory, you perform the following tasks.

- Create a directory of the same type as your enterprise directory and specify the connection details.
- Map the VMware Workspace ONE Access attributes to attributes used in your Active Directory or LDAP directory.
- Specify the users and groups to sync.
- Sync users and groups.

After you integrate your enterprise directory and perform the initial sync, you can update the configuration and resync at any time.

Configuring user attribute definitions

When you use VMware Aria Suite Lifecycle configure a directory to sync with Active Directory, specify the user attributes.

Before you configure the directory, specify all required default attributes. You can also add and map additional attributes for the Active Directory.

Changing the default attributes from a required to non-required and marking an attribute to be required can be done only if there are no directories created. After the directories are created and synced, they cannot be changed.

You can mark the required and non-required attributes before adding any directory in the directories page. When you add new custom attributes after the directories are created, to map them you have to edit the directory and update the directory attribute mapping. The change takes effect the next time that the directory is synced to Active Directory.

Assign user roles and manage users

You can map a user role against users and groups present in VMware Workspace ONE Access by using VMware Aria Suite Lifecycle.

You can select a user or group mapping to edit. You can also delete a role mapping. If a group is assigned a role, and if you are a part of the group, and you log in to VMware Aria Suite Lifecycle, you can take the same roles that group. If you have individual mapping, then it can be consolidation of user role and the roles assigned towards the group.

Prerequisites

Verify that you have access to user groups in VMware Aria Suite Lifecycle.

Role	Role Description	Add User/ Groups URL
VMware Aria Suite Lifecycle Cloud Admin	Cloud administrator for VMware Aria Suite Lifecycle	ug-vrslcm-admins@rainpole.local
Content Release Manager	Content Release Manager	ug-vrslcm-content-admins@rainpole.local

Role	Role Description	Add User/ Groups URL
Content Developer	Content Developer	ug-vrslcm-content-developers@rainpole.local
Certificate Administrator	Developer for performing certificate operations	ug-vrslcm-certificate-admins@rainpole.local

Procedure

- 1 Click **Identity and Tenant Management** on the My Services dashboard.
- 2 On the left side, navigate and click **User Management**.
- 3 To add a user or a group, click **+ADD USER/GROUP**.
- 4 To select a user from the populated list in the table, enter an existing user or a group and click **Next**.

If a user or a group already has a mapping, then a warning appears and you are then asked to edit the role mapping rather create again.

- 5 Select a role for the newly created user and click **Next**.
- 6 Read the summary and click **Submit**.

Add Active Directory over LDAP

Using VMware Aria Suite Lifecycle, you can create an Active Directory over LDAP directory type to connect to a single Active Directory domain environment. For the Active Directory over LDAP directory type, the connector uses a simple bind authentication.

Prerequisites

- List the Active Directory groups and users to sync from Active Directory.
- Verify that you have specified the required default attributes and add additional attributes on the User Attributes definition.
- Verify that you have the required user credentials to add a directory.

Procedure

- 1 Click **Identity and Tenant Management** on the **My Services** dashboard.
- 2 On the **Directory Management** tab, click **Directories**.
- 3 Click **Add Directory** and select **Add Active Directory Over LDAP**.

4 Enter the following information by using the **Directory Detail** tab:

Fields	Description
Directory Information	Enter a valid directory name.
Directory Sync and Authentication	<p>Select the connector to sync with Active Directory. Connector is a VMware Workspace ONE Access service component that synchronizes users and group data between Active Directory and VMware Workspace ONE Access service.</p> <p>When used as an identity provider, it also authenticates users. Each VMware Workspace ONE Access appliance node contains a default connector component. When required a dedicated connector can also be deployed through a global environment scale-out.</p>
Authentication Enabled	<p>If you want the connector to perform authentication, select Yes.</p> <p>You can indicate whether the selected connector also performs authentication. If you are using a third-party identity provider to authenticate users, click No.</p>
Directory Search Attribute	Select an account attribute from the drop-down menu that contains a user name.
Server Location	<p>Select Directory supports DNS Service Location check box.</p> <ul style="list-style-type: none"> ■ If your Active Directory requires access over SSL/TLS, select the Directory requires all connections to use STARTTLS or SSL check box in the Certificates section, and copy and paste the domain controllers intermediate (if used) and root CA certificates into the SSL Certificate text box. Enter the intermediate CA certificate first, then the root CA certificate. Ensure that each certificate is in the PEM format and includes the BEGIN CERTIFICATE and END CERTIFICATE lines. If the domain controllers have certificates from multiple Intermediate and Root Certificate Authorities, enter all the Intermediate-Root CA certificate chains, one after another. If your Active Directory requires access over SSL/TLS and you do not provide the certificates, you cannot create the directory. ■ If you do not want to use DNS Service Location, verify that the Directory supports DNS Service Location check box is not selected and enter the Active Directory server host name and port number.

Fields	Description
Certificates	If your Active Directory requires access over SSL/TLS, select the Directory requires all connections to use SSL check box in the Certificates section and copy and paste the domain controller's Intermediate (if used) and Root CA certificate into the SSL Certificate text box. Enter the Intermediate CA certificate first, then the Root CA certificate. Ensure that the certificate is in the PEM format and includes the BEGIN CERTIFICATE and END CERTIFICATE lines. If your Active Directory requires access over SSL/TLS and you do not provide the certificate, you cannot create the directory.
Bind User Details	<ul style="list-style-type: none"> ■ Base DN - Enter the DN to start account searches. For example, OU=myUnit,DC=myCorp, DC=com. The Base DN is used for authentication. Only users under the Base DN can authenticate. Ensure that the group DNs and user DNs that you specify later for sync are under this Base DN. ■ Bind User DN - Enter the account details. For example, CN=binduser,OU=myUnit,DC=myCorp, DC=com. Use a Bind user account with a non-expiring password. ■ Bind Password: Click Test Connection to verify that the directory can connect to your Active Directory.

5 Click **Create and Next**.

For Active Directory over LDAP, the domains are listed with a check mark.

6 On the **Domain Selection Detail** tab, select the domain and click **Next**.

7 To map the directory attribute to the Active Directory, on the **Map Attribute** tab, select the required attribute and click **Save and Next**.

8 On the **Group Selection** tab, to sync from Active Directory to the VMware Workspace ONE Access directory specify the Group DN details and click **Next**.

You can also select all the active directory groups that are already available in the list to sync to the directory.

- a To select groups, click **Add Group Distinguished Name**, and specify one or more group DNs. Select the groups under them. Specify group DNs that are under the Base DN that you entered in the Base DN text box in the Add Directory page. If a group DN is outside the Base DN, users from that DN are synced but will not be able to log in.
- b Click **Find Groups**. The **Actions** column lists the number of groups found in the DN. To select all the groups in the DN, click **Select All**, or click the number and select the specific groups to sync. When you sync a group, any users that do not have Domain Users as their primary group in Active Directory are not synced.
- c Select the **Sync Nested Group Members** option.

9 On the **User Selection** tab, enter the User DN details and click **Next**.

Suite administrators is a user name in the Active Directory who acts as an Admin user for the deployed suite products, Logs, and AD table.

- 10 Select the **Sync Nested Group Members** option and enter the **Suite Administrators**.

When this option is enabled, all the users that belong directly to the group you select and all the users that belong to the nested groups under it are synced when the group is entitled. Note that the nested groups are not synced; only the users that belong to the nested groups are synced. In the VMware Workspace ONE Access directory, these users are members of the parent group that you selected for sync. If the **Sync nested group members** option is deactivated, when you specify a group to sync, all the users that belong directly to that group are synced. Users that belong to nested groups under it are not synced. Disabling this option is useful for large Active Directory configurations where traversing a group tree is resource and time-intensive. If you deactivate this option, ensure that you select all the groups whose users you want to sync.

- 11 Click **Save and Next**. In **User Selection** page, click **Add User** and specify the users DNs to sync. Specify user DNs that are under the Base DN that you entered in the Base DN text box in the Add Directory page. If a user DN is outside the Base DN, users from that DN are synced but will not be able to log in. Click **Save and Next**.
- 12 Review the **Dry Run Check** tab, read the summary, click **Sync and Complete** to start the sync to the directory. The connection to Active Directory are established, and users and group names are synced from the Active Directory to the VMware Workspace ONE Access directory.
- 13 Click **Submit**.
- 14 To edit, click the **Edit** icon on the specific active directory in the list of active directories. Any information added is appended to the configuration on VMware Workspace ONE Access. However, any removal through editing only removes the configuration from the VMware Aria Suite Lifecycle inventory and not from the VMware Workspace ONE Access.
- 15 To delete, click the **Delete** icon on the specific active directory in the list of active directories. The delete action deletes the active directory only from the VMware Aria Suite Lifecycle inventory and not from VMware Workspace ONE Access.

Add Active Directory with integrated Windows authentication

You can use VMware Aria Suite Lifecycle to create a Active Directory with integrated Windows authentication directory type when you plan to connect to a multi-domain Active Directory environment. The connector binds to Active Directory by using Integrated Windows Authentication.

Prerequisites

Verify that you have the required user credentials to add a directory.

Procedure

- 1 Click **Identity and Tenant Management** on the My Services dashboard.
- 2 Navigate to Directory Management tab, click **Directories**.

3 Click **+Add Directory** and click **Add Active Directory Over IWA**.

4 On the **Directory Detail** tab:

Fields	Description
Directory Information	Enter a valid Directory Name.
Directory Sync and Authentication	Select the connector to sync with Active Directory. Connector is a VMware Workspace ONE Access service component that synchronizes users and group data between Active Directory and VMware Workspace ONE Access service. It authenticates users. Each VMware Workspace ONE Access appliance node contains a default connector component. If necessary, a dedicated connector can also be deployed through a global environment scale-out.
Authentication Enabled	You can indicate whether the selected connector also performs authentication. If you are using a third-party identity provider to authenticate users, click No .
Directory Search Attribute	Select a search attribute from the drop-down menu.
Certificates	<ul style="list-style-type: none"> ■ If your Active Directory requires access over SSL/TLS, select the Directory requires all connections to use STARTTLS check box in the Certificates section, and copy and paste the domain controllers Intermediate (if used) and Root CA certificates into the SSL Certificate text box. Enter the Intermediate CA certificate first, then the Root CA certificate. Ensure that each certificate is in the PEM format and includes the BEGIN CERTIFICATE and END CERTIFICATE lines. If the domain controllers have certificates from multiple Intermediate and Root Certificate Authorities, enter all the Intermediate-Root CA certificate chains, one after the other. If your Active Directory requires access over SSL/TLS and you do not provide the certificates, you cannot create the directory.
Join Domain Details	Enter the Domain Name, Domain Admin user name, and Domain Password.
Bind User Details	<ul style="list-style-type: none"> ■ Enter the Bind Username and Bind Password of the bind user who has permission to query users and groups for the required domains. Enter the user name as <code>sAMAccountName@domain</code>, where domain is the fully qualified domain name. Using a Bind user account with a non-expiring password.

5 Click **Create and Next**.

You can select the domains that should be associated with the Active Directory connection.

6 On the **Domain Selection Detail** tab, select the domain and click **Submit and Next**.

The Active Directory with IWA populates the list of domains and you can select or edit the domains as required.

7 To verify that the VMware Workspace ONE Access directory attribute names are mapped to the correct Active Directory attributes, on the **Map Attribute** tab, select the required attribute and click **Submit and Next**.

- 8 On the **Group Selection** tab, specify the Group DN details and click **Next**.

To select groups, click **Add Group Distinguished Name**, and specify one or more group DNs and select the groups under them. Specify group DNs that are under the Base DN that you entered in the Base DN text box in the Add Directory section. If a group DN is outside the Base DN, users from that DN will be synced but you cannot log in.

When you sync a group, any users that do not have Domain Users as their primary group in Active Directory are not synced.

- a Select the **Sync Nested Group Members** option.

- 9 On the **User Selection** tab, enter the User DN details and click **Next**.

Note When this option is enabled, all the users that belong directly to the group you select and all the users that belong to nested groups under it are synced when the group is entitled. Note that the nested groups are not synced; only the users that belong to the nested groups are synced. In the VMware Workspace ONE Access directory, these users are members of the parent group that you selected for sync. If the **Sync nested group members** option is disabled, when you specify a group to sync, all the users that belong directly to that group are synced. Users that belong to nested groups under it are not synced. Disabling this option is useful for large Active Directory configurations where traversing a group tree is resource and time intensive. If you disable this option, ensure that you select all the groups whose users you want to sync.

Suite administrators is a user name in the Active Directory who acts as an Admin user for the deployed suite products, Logs, and AD table.

- 10 On the **Dry Run Check** tab, read the Summary.
- 11 Click **Sync and Complete** to start the sync to the directory. The connection to Active Directory will be established and users and group names are synced from the Active Directory to the VMware Workspace ONE Access directory.
- 12 Click **Submit**.
- 13 To edit, click the **Edit** icon on the specific active directory in the list of active directories. New information is appended to the configuration on VMware Workspace ONE Access. However, if removed by editing you can only remove the configuration from the VMware Aria Suite Lifecycle inventory and not from the VMware Workspace ONE Access.
- 14 To delete, click the **Delete** icon on the specific active directory in the list of active directories. You can delete the active directory only from VMware Aria Suite Lifecycle inventory and not from VMware Workspace ONE Access.

Tenant management in VMware Aria Suite Lifecycle

To create and manage tenants, use VMware Workspace ONE Access and VMware Aria Suite Lifecycle.

Tenants are created in VMware Workspace ONE Access and are associated with products that are tenant-aware. Use VMware Workspace ONE Access to manage tenants.

Note that the VMware Identity Manager and Workspace ONE Access terms are used interchangeably in VMware Aria Suite Lifecycle product documentation.

Multi-tenancy overview for VMware Aria Suite Lifecycle products

This section describes multi-tenancy concepts and terminology.

- **Tenant** - It is the highest level in an organizational structure in VMware Workspace ONE Access. All objects like directories, users, groups, third party IDPs are maintained individually for each tenant. Each tenant is isolated from the rest of the tenants and they do not share any resource with each other.
- **Primary Tenant** - There is always at least one tenant (primary, default or base) present in the VMware Workspace ONE Access which is called as primary tenant.

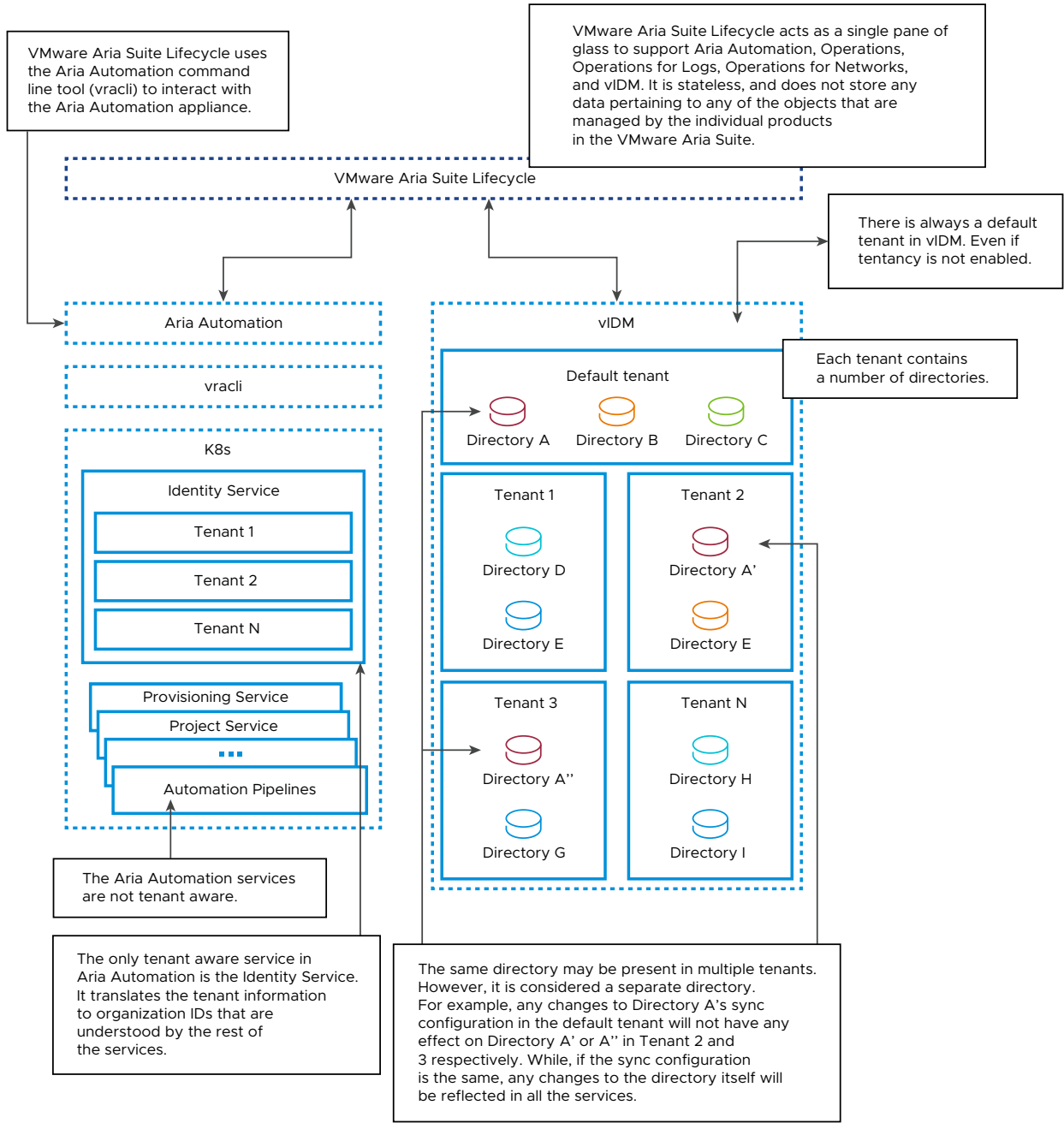
For VMware Aria Automation users, the primary tenant name is formed based on the first VMware Workspace ONE Access node that get is deployed and bootstrapped. For example, if `idm1.vmwlab.local` is the first VMware Workspace ONE Access node deployed, when you bootstrap VMware Workspace ONE Access, the primary tenant is created with name `idm1`. Nodes that are scaled out, such as `idm2.vmwlab.local` and `idm3.vmwlab.local` are not affected. The primary tenant name is formed only once and remains the same in a single or clustered instance.

- **Primary Tenant Alias** - You cannot create sub tenants in VMware Workspace ONE Access under the primary tenant until specific configurations are set and enabled. Setting an alias name for the primary tenant is required. You must create an alias on the primary tenant. The primary tenant should be accessed through the primary tenant alias FQDN on a single node or a clustered instance.
- **Provider Admin** - An admin who owns the management infrastructure, that includes VMware Workspace ONE Access, VMware Aria Automation and other products. The admin creates and manages all the tenants and associates products with tenants. The VMware Aria Suite Lifecycle admin user, `admin@local` is the only provider admin and is authorized to perform tenant management functionalities.
- **Tenant Admin** - An admin with the highest level of administrative permission in each VMware Workspace ONE Access tenant. This permission can be assigned to both local VMware Workspace ONE Access users and Active Directory users present within the VMware Workspace ONE Access tenant.
- **Tenant Aware Products** - Products that support multi-tenancy and maintains proper isolation with each logical tenant instance are tenant aware products. They have one to one mapping with VMware Workspace ONE Access tenants.
- **VMware Aria Automation Organization and Organization Owner** - In VMware Aria Automation, organization is the top-level construct and it maps 1:1 with VMware Workspace ONE Access tenant. Organization Owner has administrative permission in the VMware Aria

Automation Organization or tenant. While adding tenants and associating VMware Aria Automation with the newly added tenant, the VMware Workspace ONE Access tenant admin becomes the organization owner for the new tenant. For more information on adding tenants, see [Add tenants](#) .

- Directory - Directories are second level of objects in VMware Workspace ONE Access. It represents an external identity store or provider like Active Directory (AD) or an OpenLDAP server. There are multiple variants of directory supported in VMware Workspace ONE Access. You can add Active Directory Over LDAP and Active Directory with IWA in the Directory Management section.
- Directory Synchronization - While adding directories, configuration options are provided to filter and synchronize the required users and groups from the identity store or provider to the VMware Workspace ONE Access database. Only after a successful sync, you can integrate the users and groups with VMware Workspace ONE Access.
- Directories in tenant - Each tenant can contain several directories. The same directory configuration can be present in multiple tenants, however, it is considered a separate directory. For example: You have added Directory A in primary tenant with some directory configurations (User DNs, Group DNs, Sync configurations). And you have two sub-tenants named Tenant-1 and Tenant-2. The same directory configurations of directory A can be used on to add directories A1 and A2 on each of the sub-tenants respectively, so that the same set of users and groups are synced in sub-tenants - Tenant-1 and Tenant-2. After adding, any changes to the sync configurations of directory A in primary tenant will not affect directories A1 and A2 and its synced users and groups in Tenant-1 and Tenant-2. All three directories and its configurations are independent of each other. All three directories are affected only if the external identity store or provider changes. For example, if users or groups are getting removed directly from the Identity provider then it influences all three directories in all three tenants.

Figure 2-1. Multi-Tenancy Model



Multi-tenancy model for VMware Aria Suite Lifecycle products

This section describes multi-tenancy model explaining how tenants can be accessed through tenant FQDNs and the importance of enabling multi-tenancy along with the certificate, and DNS requirements by using VMware Aria Suite Lifecycle.

Enabling Multi-Tenancy

The master tenant is now referred to as primary tenant. Even though on day-0, the out-of-the-box VMware Workspace ONE Access includes a primary tenant already available, this is kept at a minimal configuration and further creation of tenants below the primary tenant is not possible. A sequence of configurations and API calls are to be performed on the VMware Workspace ONE Access to enable multi-tenancy. There must be an alias name created for the primary tenant when you enable multi-tenancy. For more information on enabling multi-tenancy, see [Enable multi-tenancy for VMware Aria Suite Lifecycle products](#).

For example, a VMware Workspace ONE Access with FQDN `idm1.vmwlab.local` can already have a primary tenant with name `idm1`. Before enabling multi-tenancy, you must create an alias for the primary (example, `primary-tenant`) set and use the same alias name everywhere the primary tenant is referenced.

Tenant FQDNs

By default, tenants created on VMware Workspace ONE Access are accessed through tenant URLs which are nothing but FQDNs mapped to the VMware Workspace ONE Access server. Every tenant has its own tenant FQDN. For example, on a single node VMware Workspace ONE Access with hostname `idm1.vmwlab.local`, with the primary tenant name (`idm1`) and primary tenant alias (`primary-tenant`), the primary tenant should be accessed through its FQDN `primary-tenant.vmwlab.local`. If a new tenant (`tenant1`) is created, it must be accessed only through `tenant1.vmwlab.local`.

Since every tenant requires a dedicated FQDN, creating tenants on VMware Workspace ONE Access requires a A-type DNS record mapping the tenant FQDN to the VMware Workspace ONE Access server IP address. For a clustered VMware Workspace ONE Access deployment, every tenant FQDN must have an A-type record mapping to the VMware Workspace ONE Access load balancer IP address.

The same model applies to VMware Aria Automation. When VMware Aria Automation is associated with a tenant, the VMware Aria Automation tenant must be accessed by VMware Aria Automation tenant FQDNs. For example, VMware Workspace ONE Access with FQDN `idm1.vmwlab.local` has a tenant `tenant1` accessible through `tenant1.vmwlab.local` and VMware Aria Automation `vra1.vmwlab.local` integrated with this VMware Workspace ONE

Access and associated with `tenant1`. As mentioned, the VMware Aria Automation tenant and VMware Workspace ONE Access tenant maps 1:1, so the primary tenant VMware Aria Automation can still be accessed by `vra1.vmwlab.local` and `tenant1` VMware Aria Automation must be accessed by `tenant1.vra1.vmwlab.local`.

Note There is a difference between VMware Workspace ONE Access and VMware Aria Automation tenant FQDNs. For a VMware Workspace ONE Access instance, the tenant FQDN format is tenant name (tenant1) followed by the VMware Workspace ONE Access domain name (`vmwlab.local`). For example, `tenant1.vmwlab.local`. Since it is tenant name followed by domain, it remains the same even for clustered VMware Workspace ONE Access. For a VMware Aria Automation, the VMware Aria Automation tenant FQDN format is tenant name (tenant1) followed the VMware Aria Automation server FQDN (`vra1.vmwlab.local`) For example, `tenant1.vra1.vmwlab.local`. For a clustered VMware Aria Automation behind a load-balancer `vra-lb.vmwlab.local`, `tenant1` must be accessed through `tenant1.vra-lb.vmwlab.local`.

Similar to VMware Workspace ONE Access, even VMware Aria Automation tenant FQDNs require DNS mapping. But for a VMware Aria Automation it should be CNAME type record mapping the VMware Aria Automation tenant FQDNs to the VMware Aria Automation server FQDN. For a clustered VMware Aria Automation deployment, all VMware Aria Automation tenant FQDNs must be having a CNAME type DNS record pointing to the VMware Aria Automation load balancer FQDN.

Apart from having DNS mappings as a mandatory pre-requisite, certificates are also mandatory for tenancy to work. Both VMware Workspace ONE Access, VMware Aria Automation servers and its load balancers depending on the deployment architecture should have their corresponding certificates holding all the required tenant FQDNs.

Tenant FQDNs on a single node setup

- VMware Workspace ONE Access Node: `idm1.vmwlab.local`

VMware Aria Automation Node: `vra1.vmwlab.local`

Primary tenant alias name: `primary-tenant`

Tenants: `tenant-1`, `tenant-2`

Tenant Names	VMware Workspace ONE Access Tenant FQDNs	VMware Aria Automation Tenant FQDNs
<code>primary-tenant</code>	<code>https://primary-tenant.vmwlab.local</code>	<code>https://vra1.vmwlab.local</code>
<code>tenant-1</code>	<code>https://tenant-1.vmwlab.local</code>	<code>https://tenant-1.vra1.vmwlab.local</code>
<code>tenant-2</code>	<code>https://tenant-2.vmwlab.local</code>	<code>https://tenant-2.vra1.vmwlab.local</code>

Tenant FQDNs on a clustered setup

- VMware Workspace ONE Access Load balancer: `idm-lb.vmwlab.local`

VMware Workspace ONE Access Nodes: `idm1.vmwlab.local`, `idm2.vmwlab.local`, `idm3.vmwlab.local`

VMware Aria Automation Load balancer: `vra-lb.vmwlab.local`

VMware Aria Automation Nodes: `vra1.vmwlab.local`, `vra2.vmwlab.local`,
`vra3.vmwlab.local`

Primary tenant alias name: **primary-tenant**

Tenants: tenant-1, tenant-2

Tenant Names	VMware Workspace ONE Access Tenant FQDNs	VMware Aria Automation Tenant FQDNs
primary-tenant	<i>https://primary-tenant.vmwlab.local</i>	<i>https://vra-lb.vmwlab.local</i>
tenant-1	<i>https://tenant-1.vmwlab.local</i>	<i>https://tenant-1.vra-lb.vmwlab.local</i>
tenant-2	<i>https://tenant-2.vmwlab.local</i>	<i>https://tenant-2.vra-lb.vmwlab.local</i>

Note After you enable multi-tenancy, VMware Workspace ONE Access should only be accessed through its tenant FQDNs. The old FQDNs and hostnames (`idm1.vmwlab.local`, `idm2.vmwlab.local`, `idm3.vmwlab.local` and `idm-lb.vmwlab.local`) become invalid.

Mandatory Certificate Requirements

Depending on the deployment type of VMware Workspace ONE Access and VMware Aria Automation, their corresponding server certificates should have all the tenant FQDNs present within itself. Since each tenant forms its own tenant FQDN (both VMware Workspace ONE Access tenant FQDN and VMware Aria Automation tenant FQDN), every created tenant requires

its tenant FQDN to be added as part of both VMware Workspace ONE Access and VMware Aria Automation certificates. Enabling multi-tenancy on VMware Workspace ONE Access also requires VMware Workspace ONE Access certificates updated as the primary tenant gets a new alias name and primary tenant FQDN undergoes a change.

Note

- When you change the certificates on VMware Workspace ONE Access to enable multi-tenancy or creating tenants, this brings down the service and leads to a downtime. If VMware Workspace ONE Access certificate is changed, then it goes for a service downtime. The products or services integrated with VMware Workspace ONE Access for their authentication purpose cannot use VMware Workspace ONE Access auth log-in during the downtime. Also, changing VMware Workspace ONE Access certificate requires re-trust on all product or services which again lead to a downtime for the products.

For information about changing your VMware Identity Manager certificate, see [Replace your Workspace ONE Access certificate by using VMware Aria Suite Lifecycle](#) .

For related information about replacing certificates for VMware Aria Suite Lifecycle, see [Replace certificate for VMware Aria Suite Lifecycle products](#).

- For every new tenant that is created and associated with VMware Aria Automation, even VMware Aria Automation certificates must be changed and this causes service downtime for VMware Aria Automation.
- To avoid service down-times on VMware Aria Automation, VMware Workspace ONE Access and other products or services integrated with VMware Workspace ONE Access, it is generally recommended to have wild-card certificates. For a new tenant, any change made in the VMware Workspace ONE Access certificate or VMware Aria Automation certificate, can create a downtime in VMware Aria Automation.
- If wild-card certificates are not used, then specific SAN entries are to be created for each tenant FQDN on all required certificates.
- The VMware Aria Suite Lifecycle locker service helps in managing certificates on the VMware Workspace ONE Access and VMware Aria Automation server nodes. With VMware Aria Suite Lifecycle, when you replace VMware Workspace ONE Access certificate, the re-trust of VMware Workspace ONE Access certificate on all products is performed automatically.
- Products or services external to VMware Aria Suite Lifecycle is handled manually. Locker service does not handle updating load balancer certificates. They are to be done by the user manually. Whenever load-balancer certificates are changed, the same had to be re-trusted on the products.
 - For VMware Workspace ONE Access, the VMware Workspace ONE Access Certificate update or replace operation in VMware Aria Suite Lifecycle internally makes sure the VMware Workspace ONE Access load balancer certificate is re-trusted before updating the VMware Workspace ONE Access server certificates. So, it is recommended to first change the VMware Workspace ONE Access load balancer certificate manually and then do a VMware Workspace ONE Access certificate to update or replace through VMware Aria Suite Lifecycle locker service.
 - For VMware Aria Automation, when SSL is terminated at a VMware Aria Automation load balancer and the load balancer certificate is changed manually, you must click **Re-trust Load Balancer** under the VMware Aria Automation product card to re-trust the load-balancer certificate in VMware Aria Automation. For more details, see [Day 2 operations with other products in VMware Aria Suite Lifecycle](#).

Mandatory DNS Requirements

For a single node VMware Workspace ONE Access, you require A-type DNS records highlighting the tenant FQDNs to the VMware Workspace ONE Access server IP address. And for a clustered VMware Workspace ONE Access, A-type DNS records are required pointing the tenant FQDNs to the VMware Workspace ONE Access load-balancer IP address.

For VMware Aria Automation, for a single node, CNAME type DNS records are required pointing VMware Aria Automation tenant FQDNs to the VMware Aria Automation server FQDN. And for a clustered VMware Aria Automation, CNAME type DNS records pointing VMware Aria Automation tenant FQDNs to the VMware Aria Automation load-balancer FQDN.

Requirements for multi-tenancy

Figure 2-2. Single node Workspace ONE Access and VMware Aria Automation

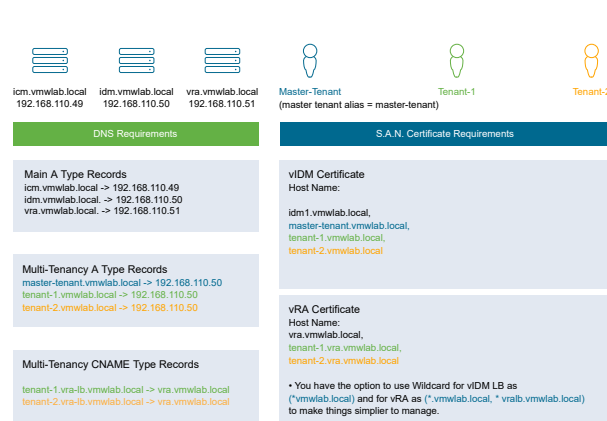


Figure 2-3. Both Workspace ONE Access and VMware Aria Automation Cluster

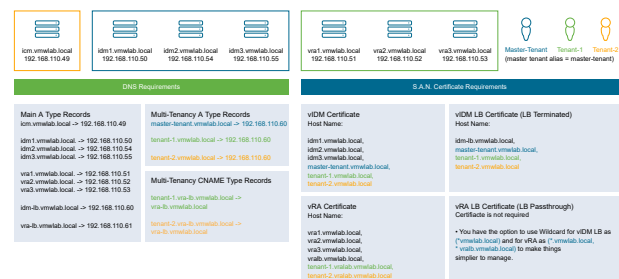


Figure 2-4. Workspace ONE Access Single and VMware Aria Automation Clustered

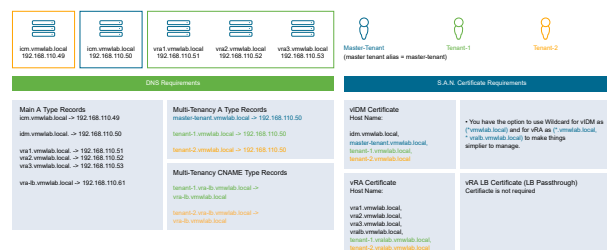
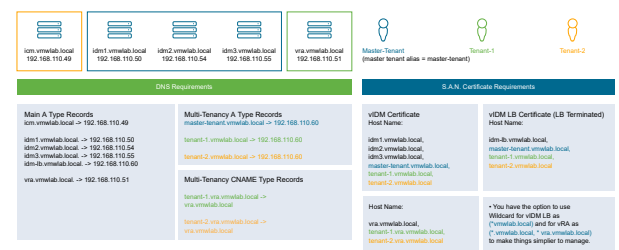


Figure 2-5. Workspace ONE Access Cluster and VMware Aria Automation Single



Enable multi-tenancy for VMware Aria Suite Lifecycle products

To configure support for multi-tenancy, use VMware Aria Suite Lifecycle.

Prerequisites

- Verify that you have a VMware Workspace ONE Access global environment.

- Verify if the inventories are synchronized for all the environments in VMware Aria Suite Lifecycle and all environments and products are up to date. This is to discover all the VMware Workspace ONE Access-product integrations required for VMware Workspace ONE Access re-register.
- Verify if the VMware Workspace ONE Access global environment certificate is managed through the VMware Aria Suite Lifecycle Locker service.
- Ensure to take a snapshot of VMware Workspace ONE Access. It is recommended, since enabling multi-tenancy transforms VMware Workspace ONE Access to be accessed through tenant FQDNs and existing VMware Workspace ONE Access URLs will not be accessible.
- For a clustered VMware Workspace ONE Access, verify VMware Workspace ONE Access cluster health status is green by triggering cluster health. For more information, [Day 2 operations with other products in VMware Aria Suite Lifecycle](#)
- Verify the VMware Workspace ONE Access certificate is updated with the primary tenant alias FQDN. Also ensure that the A-type DNS record is added mapping the primary tenant alias FQDN. For more information about Mandatory Certificate and DNS requirements, see [Multi-tenancy model for VMware Aria Suite Lifecycle products](#).

Procedure

- 1 Click **Identity and Tenant Management** and navigate to **Tenant Management**.
- 2 Read the Opt-in message and click **Enable Tenancy**.
- 3 Enter the primary tenant Alias name.

Ensure that the hostname or FQDN does not already exist. While enabling multi-tenancy, this FQDN is assigned to the primary tenant.

Ensure all products currently integrated with global environment VMware Workspace ONE Access are already listed and selected for re-registration against the new primary tenant alias FQDN in the Product Re-registration table. For more information on Product References, see [Product references for VMware Aria Suite Lifecycle](#).

- 4 Click **Submit**, after you validate the entries.

After you enable multi-tenancy on the VMware Workspace ONE Access, it can only be accessed through its tenant FQDNs, and at this point as the primary tenant is the only available tenant, primary tenant alias FQDN is the only endpoint through which VMware Workspace ONE Access can be accessed. When the VMware Aria Suite Lifecycle enable multi-tenancy request is completed, create tenants by using the **Tenant Management** tab.

Manage tenants for VMware Aria Suite Lifecycle products

To manage tenants, use VMware Aria Suite Lifecycle.

You can add, delete, search, and manage your tenants by using the Identity and Tenant Management service in VMware Aria Suite Lifecycle.

Add tenants

To add tenants to VMware Workspace ONE Access, use VMware Aria Suite Lifecycle. You can also create a tenant admin, add directories to the new tenant, and associate tenant-aware products to the tenant.

When you add a tenant, the process also contains a pre-check step which validates all the given inputs and selected environments to make sure tenant creation and product associations work seamlessly.

Prerequisites

- Verify that you have DNS configured in both VMware Aria Automation and VMware Workspace ONE Access. To access a tenant, the DNS server must be configured correctly before starting the VMware Aria Suite Lifecycle flow Add Tenant procedure.
- Ensure that the A-type DNS record is added for the new tenant FQDN. For a multi-SAN environment, ensure that VMware Workspace ONE Access certificate is updated with the new tenant FQDN that is to be created. For more details, see [Multi-tenancy model for VMware Aria Suite Lifecycle products](#). For all the VMware Aria Automation instances that are to be associated with the new tenant ensure that the CNAME type DNS records are added and certificate requirements are met.
- For all the VMware Aria Automation instances that are to be associated with the new tenant ensure that the CNAME type DNS records are added and certificate requirements are entered.

Procedure

- 1 On the My Services dashboard, click **Identity and Tenant Management**.
- 2 Navigate to Tenant Management, click **ADD TENANT**.
- 3 Enter a tenant name and under the Administrator Details, enter **Username, First Name, Last name, Email ID, and Password** of the Tenant Admin.
- 4 Click **Next**.
- 5 (Optional) On the Directory Details tab, choose the directories from primary tenant that are to be migrated to the new tenant being created.

You can find the existing directory names listed in the directory column.

- 6 You can select any directories and click **Next**.
 - a Opt-in for migrate directories lists all the existing directories from the primary tenant. Only AD Over LDAP and AD with IWA directories is listed.
 - b To migrate, select the directories.
 - c Enter the passwords that are required for validation
 - d Click **Validate**. When validation is successful, click **Save and Next**.

- 7 Select that products that are should be associated with the new tenant, such as VMware Aria Suite Lifecycle and VMware Aria Automation.

Note Verify that you have considered the recommendation given for both certificate and DNS.

- 8 Click **Save** and **Next**.
- 9 Click **Run a Precheck** to the validate the tenant details and certificate details.
 - Tenant Name validation Check – To validate the entered tenant name matches criteria.
 - Tenant Name Existence Check – To validate a tenant already exists.
 - VMware Workspace ONE Access Tenant FQDN Reachability and Resolvability Check
 - VMware Workspace ONE AccessTenant FQDN Certificate Check
 - VMware Aria Automation Tenant FQDN Reachability and Resolvability Check
 - VMware Aria Automation Tenant FQDN Certificate Check
 - a If the validations are not successful and if you want to make some changes, and resume the tenant creation operation, click **Save and Exit**. The same wizard can be opened anytime to re-run the precheck to complete and proceed.
 - b If the pre-check validations are green, click **Save and Next**. A summary of the whole selection appears.
- 10 Click **Next** and **Create Tenant** changes after reading the summary.

You can view the tenant creation under the **Request Details** page. Both VMware Workspace ONE Access and VMware Aria Automation tenants can be accessed through its tenant FQDNs. For more information, see [Tenant management in VMware Aria Suite Lifecycle](#). You can log in to both VMware Workspace ONE Access tenant FQDN and VMware Aria Automation tenant FQDN with the tenant admin credentials. The VMware Workspace ONE Access tenant admin is also made the organization owner in new tenant VMware Aria Automation.

Delete a tenant

The delete tenant operation deletes the tenant from VMware Workspace ONE Access, including all resources that have been created for that tenant.

The delete tenant operation is not available for tenants that have product associations.

Managing tenants for post-deployment operations

All operations that are available in the Add Tenant wizard are available as a Day 2 operation in VMware Aria Automation.

Manage tenant admins

When tenants are first created, only one local VMware Workspace ONE Access user is created and that user is given tenant admin permissions. You can add and manage tenants admin at later stage when required.

Manage tenant admins - Add tenant admins

This option is used to add a new local user in VMware Workspace ONE Access and assign tenant admin permission to that user.

- 1 Navigate to **Identity and Tenant Management** service and click **Tenant Management**.
- 2 To add an admin, select the tenant.
- 3 Click **ADD TENANT ADMIN**. The create tenant admin page loads
- 4 Enter the details for the new tenant admin and click **Create Tenant Admin**.

After you submit, a request is created that can be tracked for completion and user is listed in the tenant admin list.

Manage tenant admins - Search and assign

This option is used when there are users already present in the VMware Workspace ONE Access under the concerned tenant and requires tenant admin permission. The search can find both local VMware Workspace ONE Access users and Active Directory Users that are synced in the concerned tenant. Multiple users can be searched and assigned with tenant admin permission.

- 1 Navigate to **Identity and Tenant Management** service and click **Tenant Management**.
- 2 To add an admin, select the tenant.
- 3 Click **SEARCH AND ASSIGN**.
- 4 When all the users are selected, click **Assign Tenant Admin**.

After you submit, a request is created that can be tracked for completion and user is listed in the tenant admin list.

Associate products

When the tenants are created, as a day-2 operation at any point, you can associate more products. Product Associations lists the current products that are associated with the tenant. To add more association, click **Add Product Association**. Select the product and check the recommendations given. For VMware Aria Automation, ensure that the Certificate and DNS requirements are entered. Select the tenant admins from the list available. The tenant admin is made the organization owner for the new tenant VMware Aria Automation. Run pre-check to validate your entries and click **Submit**. Once the request completes, the associated product is listed under the **Product Association** list.

Migrate directories

Migrate directories day-2 is similar to the **Add Tenant** wizard. The directories tab inside the tenant view lists the current directories that are present in the tenant.

Note The directories are read-only. VMware Aria Suite Lifecycle does not allow complete directory management for subtenant directories. Directory management is only available for directories present in the primary tenant.

When you click **Add Directories**, all the directories from the primary tenant are retrieved. Select directories that are to be migrated, validate them, and then submit.

Migrating tenants in VMware Aria Suite Lifecycle

To migrate tenants and specific tenant data for VMware Workspace ONE Access, use VMware Aria Suite Lifecycle.

Tenant migration involves close coordination between VMware Workspace ONE Access, VMware Aria Suite Lifecycle, and VMware Aria Automation.

VMware Aria Suite Lifecycle migrates the following VMware Aria Automation data to the VMware Workspace ONE Access global environment:

- Tenants
- Directories
- Custom groups
- Roles and rule set
- User attributes
- Access policies
- Network ranges
- Third-party IDP configurations

Migrating VMware Workspace ONE Access tenants by using VMware Aria Suite Lifecycle

You can migrate VMware Workspace ONE Access by using VMware Aria Suite Lifecycle.

Prerequisites

- The SMTP information of the source tenant must be configured on the Global Environment of VMware Workspace ONE Access. This information is required to receive email instructions to reset the password for all local users. Prior to tenant migration, all local users in the source tenant must have valid email IDs.
- For custom group migration, you must enable remote connection from the Global Environment of VMware Workspace ONE Access to the VMware Aria Automation database. Refer to [KB 81219](#) for more information on enabling remote connection.

- Ensure that you have DNS configured in VMware Aria Automation and VMware Workspace ONE Access.
- Ensure that the source VMware Aria Automation environment is in a healthy state and directories are synced before tenant migration.

This procedure assumes tenancy has already been enabled and that you have existing tenants to migrate.

Procedure

- 1 From the VMware Aria Suite Lifecycle My Services dashboard, click **Identity and Tenant Management**.
- 2 Click **Tenant Management** and then click **Tenant Migrations**.
- 3 Read the information on VMware Workspace ONE Access tenant migration and VMware Aria Automation tenant mapping, and then click **Continue**.
- 4 On the Environment Selection tab, select the **Source Environment** and **Target Environment**.
Based on your source and the target environment selection, you can view a tabular representation of the available tenants on the source VMware Aria Automation. You can also view the status of the migrated or merged tenants on the VMware Aria Automation environment.
- 5 Click **Next**.
- 6 On the Tenant Migration Workflow page, you can view the workflow of Tenant Migration and Tenant Merge, and understand the correlation between the two operations.
- 7 Click **SAVE AND NEXT** and read the list of manual steps which must be performed to proceed with the migration. Select the check box to confirm that you have read and verified the prerequisites and limitations.
- 8 To specify the Tenant Migration Workflow, enter these details on the Tenant Details tab.
 - a Select the **Source Tenant**.
The source tenants listed are not the migrated or merged tenants.
 - b Enter the **Tenant Name**.
 - c Under Target Tenant administrator details, enter the **Target Tenant Username, First Name, Last Name**, valid **Email ID**, and **Password**.

Note To migrate a directory is a one-time operation, select all the directories which must be migrated. If the required directories are not selected during migration, you have to perform this operation manually.

 - d Click **SAVE AND NEXT**.
- 9 Click **Validate**. After a successful validation, click **SAVE AND NEXT**.

10 Click **Run Precheck** to validate the tenant details and certificate details. Click **SAVE AND NEXT**.

11 On the Summary Step tab, you can view the summary of your selections.

12 Click **SUBMIT** if your validations are successful.

If the validations are not successful and you want to make changes, and then resume the tenant migration operation, click **SAVE AND EXIT**. The same wizard can be opened anytime to rerun the precheck to proceed.

You can view the tenant migration details under the Request Details page. VMware Workspace ONE Access and VMware Aria Automation tenants can be accessed through its tenant FQDNs.

Merging VMware Aria Automation tenants and directories by using VMware Aria Suite Lifecycle

To merge VMware Aria Automation tenants and directories, use the Identity and Tenant Management service in VMware Aria Suite Lifecycle.

VMware Aria Suite Lifecycle creates the VMware Aria Automation endpoints for existing tenants in the VMware Aria Automation environment. You can also migrate other resources by using VMware Aria Suite Lifecycle.

Prerequisites

- VMware Aria Automation does not require you to accept a source certificate during migration assessment. To merge or manage the tenant using VMware Aria Suite Lifecycle, you can delete the manually added source environment from VMware Aria Automation.
- Ensure that the VMware Workspace ONE Access specific data is migrated to the target data in the Global Environment.

This procedure assumes tenancy has already been enabled and that you have existing tenants and directories to merge.

Procedure

- 1 From the VMware Aria Suite Lifecycle My Services dashboard, click **Identity and Tenant Management**.
- 2 Select **Tenant Management**, and then click **Tenant Migrations**.
- 3 Read the information on VMware Workspace ONE Access Tenant Migration and VMware Aria Automation Mapping, and then click **Continue**.
- 4 On the Environment Selection tab, select the **Source Environment** and **Target Environment**.

Based on your source and the target environment selection, you can view a tabular representation of the available tenants on the source VMware Aria Automation. You can also view the status of the migrated or merged tenants on VMware Aria Automation environment.

- 5 Click **Next** and on the Tenant Migration Workflow page, you can view the workflow of Tenant Migration and Tenant Merge.
- 6 On the Merge Details tab, you can select one or multiple tenant mappings.
If you cannot view the target tenant, perform an inventory sync, or perform a product association for the tenant.
- 7 Click **Next** and you can view the summary of your selections on the Summary Step tab.
- 8 Click **SUBMIT** if your validations are successful.

Note If the validations are not successful and you want to make changes, and then resume the tenant merge operation, click **SAVE AND EXIT**. The same wizard can be opened anytime to rerun the precheck to proceed.

Creating a VMware Identity Manager environment in VMware Aria Suite Lifecycle

3

You can create an environment and install VMware Aria Suite products in VMware Workspace ONE Access by using VMware Aria Suite Lifecycle.

For more information on the supported VMware Aria Suite products and versions, see [System requirements for VMware Aria Suite Lifecycle](#).

Note that the VMware Identity Manager and Workspace ONE Access terms are used interchangeably in VMware Aria Suite Lifecycle product documentation.

Read the following topics next:

- [Create a new private cloud environment using the installation wizard in VMware Aria Suite Lifecycle](#)
- [Import an existing environment using a VMware Aria Suite Lifecycle installation wizard](#)
- [Create a private cloud environment using a configuration file in VMware Aria Suite Lifecycle](#)
- [Create a hybrid environment using a cloud proxy in VMware Aria Suite Lifecycle](#)

Create a new private cloud environment using the installation wizard in VMware Aria Suite Lifecycle

To create a private cloud environment and install VMware Aria Suite products, use a VMware Aria Suite Lifecycle installation wizard.

Prerequisites

- Configure product binaries for the products to install. See [Configure product binaries](#) for your release.
- Ensure that you have added a vCenter to the data center with valid credentials and the request is complete.
- Generate a single SAN certificate with host names for each product to install from the Certificate tab in the UI.

- Verify that your system meets the hardware and software requirements for each of the VMware Aria Suite products you want to install. See the following product documentation for system requirements needed for your specific product release:
 - [VMware Aria Automation documentation](#)
 - [VMware Aria Automation Orchestrator documentation](#)
 - [VMware Aria Operations documentation](#)
 - [VMware Aria Operations for Logs documentation](#)
- VMware Aria Automation Orchestrator offers two setup options:
 - VMware Aria Automation Orchestrator-Integrated

This is the traditional VMware Aria Automation Orchestrator setup option, where VMware Aria Automation Orchestrator is integrated with VMware Aria Automation.

 - If VMware Aria Automation is multi-tenancy enabled, then multiple instances of VMware Aria Automation Orchestrator can be installed in VMware Aria Suite Lifecycle.
 - If VMware Aria Automation is not multi-tenancy enabled, then one instance of VMware Aria Automation Orchestrator can be installed in VMware Aria Suite Lifecycle.
 - VMware Aria Automation Orchestrator Standalone: This setup option has no dependency on VMware Aria Automation and it allows you to integrate with vSphere.
- VMware Aria Automation Config offers two setup options:
 - VMware Aria Automation Config-Integrated: This setup is part of VMware Aria Automation Config single node setup, which does not support multiple node setup or vertical scale up options. After VMware Aria Automation is installed, if multiple tenancy is not enabled, the VMware Aria Automation Config instance associates with the base tenant of VMware Aria Automation. When multi-tenancy is enabled in VMware Aria Automation, VMware Aria Automation Config is associated with the newly added tenants, and then proceeds with the installation. When VMware Aria Automation is imported, the VMware Aria Automation Config instances which are associated with VMware Aria Automation are also imported.
 - VMware Aria Automation Config Standalone: This setup has no dependency on VMware Aria Automation.

When installing VMware Aria Automation Config, you require the following licenses:

 - VMware Aria Automation Config-Integrated: VMware Aria Automation Enterprise, VMware Aria Automation Advanced or Suite license.

- VMware Aria Automation Config Standalone: VMware Aria Automation Standard Plus license.

Procedure

1 Install VMware Workspace ONE Access in VMware Aria Suite Lifecycle

For VMware Aria Suite Lifecycle, VMware Workspace ONE Access installation is optional when creating an environment. You create an environment in the **Lifecycle Operations** service.

2 Configure environment settings for a new private cloud

Configure environment settings, such as name, password, and data center for a private cloud environment by using VMware Aria Suite Lifecycle.

3 Install VMware Aria Suite products

Select which VMware Aria Suite products to install in the private cloud environment by using VMware Aria Suite Lifecycle.

4 Accept EULA and license selection

Accept the VMware end-user license agreement and enter the license key by using VMware Aria Suite Lifecycle.

5 Configure certificate details

To create an environment and specify an existing certificate for the environment, use VMware Aria Suite Lifecycle.

6 Configure infrastructure details

To configure infrastructure details when you create a product environment, use VMware Aria Suite Lifecycle.

7 Configure network details

You can configure an environment by establishing a network connection within an environment in VMware Aria Suite Lifecycle.

8 Configure product details

To view and configure products that were selected during environment creation, use VMware Aria Suite Lifecycle.

9 Configure VMware Aria Suite products for installation

To configure the product details for each VMware Aria Suite product that you are installing in the private cloud environment, use VMware Aria Suite Lifecycle.

10 Validate private cloud environment details

To configure vCenter, cluster, network, datastore, and certificate details for a new private cloud environment, use VMware Aria Suite Lifecycle.

11 Confirm environment and installation settings

To verify product environment and installation settings, use VMware Aria Suite Lifecycle.

Install VMware Workspace ONE Access in VMware Aria Suite Lifecycle

For VMware Aria Suite Lifecycle, VMware Workspace ONE Access installation is optional when creating an environment. You create an environment in the **Lifecycle Operations** service.

Federal Information Processing Standard (FIPS) and non-FIPS mode are supported during VMware Workspace ONE Access installation. However, you cannot toggle the FIPS mode after the VMware Workspace ONE Access installation.

You can allow or deactivate the VMware Workspace ONE Access toggle button.

Note that the VMware Identity Manager and Workspace ONE Access terms are used interchangeably in VMware Aria Suite Lifecycle product documentation.

Note Prior to installing or importing VMware Aria Automation, ensure that the global environment setting is installed for VMware Workspace ONE Access in VMware Aria Suite Lifecycle. If not installed, you cannot proceed with the VMware Aria Automation deployment. To install the global environment, use the toggle button in the Create Environment page.

Procedure

- 1 Navigate to **My Services** dashboard, and click **Lifecycle Operations**.
- 2 Enable the **Install Identity Manager** toggle to install VMware Workspace ONE Access. Deactivate the **Install Identity Manager** toggle button to proceed with other product installations.
- 3 Click **Create Environment**, and enter the environment details.
 - a The environment name remains as global environment by default.
 - b (Optional) Enter the environment description, which can be a maximum of 1024 characters.
 - c Add the Password details.

Note If there is no password listed, open the VMware Aria Suite Lifecycle locker and add a password.

- d Select the **Datacenter** name.
 - e Enable or deactivate the JSON Configuration toggle bar, as required. When you allow the JSON configuration, you can paste the JSON file text manually or you can import the file from your local system.
 - f Click **Next**.
- 4 If you allowed Install Identity Manager in step 2, select the **New Install** option to install VMware Workspace ONE Access. If the toggle is deactivated, select the **New Install** option for other products.
 - 5 Select the required supported version for VMware Workspace ONE Access and click **Next**.

Results

For more information on configuring VMware Workspace ONE Access, see sections under [Install VMware Aria Suite products](#).

Configure environment settings for a new private cloud

Configure environment settings, such as name, password, and data center for a private cloud environment by using VMware Aria Suite Lifecycle.

Procedure

- 1 Log in to VMware Aria Suite Lifecycle as an administrator, select the **Lifecycle Operations** from the **My Services** dashboard, and click **Create Environment**.
- 2 In the **Environment Name**, enter a descriptive name for the new private cloud environment.
This name must be unique among environments on this instance of VMware Aria Suite Lifecycle.
- 3 (Optional) Enter the **Environment Description**, which can be a maximum of 1024 characters.
- 4 Enter a **Default Admin Password** and confirm the password.
The default password must be a minimum of 8 characters.
- 5 From **Data Center**, select an existing data center for this environment, or click **+** to add a data center to VMware Aria Suite Lifecycle.

For information about adding a data center, see [Add and manage data center associations for VMware Aria Suite Lifecycle](#).
- 6 Activate or deactivate the JSON configuration toggle, as required. When you activate the JSON configuration file, you can paste the JSON file text manually or you can import the file from your local system.
- 7 (Optional) Select **Join the VMware Customer Experience Program** to join CEIP for this environment.

This product participates in the VMware Customer Experience Program (CEIP). Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at <http://www.vmware.com/trustvmware/ceip.html>.

You can join or quit the program later by selecting the **Lifecycle Operations** service and then selecting **Settings > System Details**. Select **JOIN** or **QUIT** in the **Customer Experience Program** section of the **System Details** page.
- 8 Click **Next**.

Install VMware Aria Suite products

Select which VMware Aria Suite products to install in the private cloud environment by using VMware Aria Suite Lifecycle.

Prerequisites

Verify that you have a data center and environment credentials already created.

Procedure

- 1 Select whether to install VMware Aria Suite products by product.
 - a Select which individual VMware Aria Suite products to add to the private cloud environment and whether to do a new install of each product or import an existing installation of the product. For each new install, select the product **Version** and **Size** to deploy.
- 2 Click **Next**.

Note

- VMware Aria Automation Orchestrator offers two setup options: VMware Aria Automation Orchestrator integrated and VMware Aria Automation Orchestrator standalone. For information about configuring an integrated or standalone setup, see [Configure product details](#).
 - VMware Aria Suite Lifecycle allows continuous availability (CA) for VMware Aria Operations. For more information, see [Continuous availability for VMware Aria Operations](#).
-

Accept EULA and license selection

Accept the VMware end-user license agreement and enter the license key by using VMware Aria Suite Lifecycle.

Procedure

- 1 Read the end-user license agreement, select **I agree to the terms and conditions**, and click **Next**.
- 2 Specify any additional license settings.
 - a To select the license keys from the locker, click **Select** to open the list of licenses which are applicable to the selected products and versions. If not, select all the keys available from the listing.
 - b Click **Add**, to add a new license key to the locker from within the installation flow.
 - c Click **Validate** to validate the license. If multiple license keys are available for a product then this action will suggest to choose one per product selected for the deployment.

You can now view the applicable license keys. Next steps are not available until all the products deployed have appropriate licenses.

Note Valid product licenses are displayed in VMware Aria Suite Lifecycle. License validation does not check the functionality allowed by the licenses themselves.

Configure certificate details

To create an environment and specify an existing certificate for the environment, use VMware Aria Suite Lifecycle.

Prerequisites

Verify that the imported or created certificate has all the IP addresses and domain or host names added.

Procedure

- 1 Under the **Certificate Details**, select the **Certificate** from the drop-down menu.

If you want to provide certificate details at product level, you can specify the certificate at the product properties of each product. The action can override the certificates that are selected at the infrastructure level.

- 2 To create a certificate, click the plus sign.

In the **Add Certificate** window, enter the required details.

Fields	Description
Certificate Name	Enter a valid certificate name.
Common Name	To identify the certificate, enter a common name.
Organization	Enter the Organization name.
Organizational Unit	Enter the Organization Unit.
Country Code	Enter a country code which must be in two characters only.
Locality	Enter your locality.
State	Enter the State.
Key Length	Select the length of the key. You can select 2048 or 4096 bits.
Domain Name	Enter a valid domain name.
IP Address	Enter the IP address in which you are assigning the certificate.

- 3 Click **Generate**.
- 4 To import an existing certificate, select **Import Certificate** option.

Fields	Description
Certificate Name	Enter a valid certificate name.
Select File	<ol style="list-style-type: none"> 1 Click Choose File. 2 Browse to the saved PEM file.
Passphrase	Enter the Passphrase field, enter Cert- Password (if applicable).
Enter Private Key	When you upload a PEM file, the private key details are populated automatically.
Enter Certificate Chain	When you upload a PEM file, the certificate details are populated automatically.

- 5 Click **Import**.

- 6 Click **Next**.

Configure infrastructure details

To configure infrastructure details when you create a product environment, use VMware Aria Suite Lifecycle.

Prerequisites

If the selected datacenter does not have an associated vCenter, add a vCenter.

Procedure

- 1 Select a vCenter from the drop-down menu.

Note There should be at least one vCenter associated with a datacenter.

- 2 Select a **Cluster**.
- 3 When you click **Select a Folder**, all folders that are associated in the vCenter are listed.

If folders are not displayed, refresh vCenter data collection from the VMware Aria Suite Lifecycle settings page.

- 4 To deploy your VM, click **Select a Resource Pool**.

All the resource pools that are associated with the selected cluster are listed.

Note You can select a resource pool to deploy your VM. Both folder and resource pool selection are optional. If you do not specify a resource pool, the VM is deployed in the root default resource pool of the selected cluster. If you do not specify the folder details for both vCenter and a resource pool, the VM deployment is saved in the root default VM folder of the datacenter inside the vCenter .

- 5 Select the required **Network**, **DataStore**, and **Disk Disk Mode**.

Note VMware Aria Operations deployment fails when you provide incorrect infrastructure details such as wrong DNS or gateway details without running a pre-check while you create an environment flow. If the deployment fails, you might not see the correct cause of deployment failure using the error or code message that appears in VMware Aria Suite Lifecycle UI, and you cannot proceed further with that deployment. As a result, you might have to delete the environment card from VMware Aria Suite Lifecycle with all the products or nodes that were deployed as part of that environment. You can run pre-check so that the Infrastructure-related issues are detected and can be corrected before starting the deployment.

- 6 With VMware Aria Suite Lifecycle, to integrate with VMware Workspace ONE Access, select **Integrate with Identity Manager** toggle button.

Note The default configuration admin given while installing VMware Workspace ONE Access (global environment) are made the admin for the product as well while integrating with VMware Workspace ONE Access.

VMware Workspace ONE Access acts as an identity provider and manages SSO for the VMware Aria Suite products and VMware Aria Suite Lifecycle when integrated with VMware Aria Suite Lifecycle. SSO provides a single set of credentials to access all VMware Aria Suite applications and VMware Aria Suite Lifecycle. With SSO, you are only required to log in once, and then you can seamlessly access all VMware Aria Suite applications.

- 7 Select the **Use Content Library** to use OVF's hosted on a vCenter content library, if there is a network latency from VMware Aria Suite Lifecycle to vCenter.

Copying OVF and VMDK files for deployment from VMware Aria Suite Lifecycle to vCenter might take more time and lead to a deployment failure if there is a network latency from VMware Aria Suite Lifecycle to the target vCenter. Content libraries in vCenter can be used to host OVF's. They can also be used from VMware Aria Suite Lifecycle to deploy products. You can perform the steps before you start a vCenter inventory sync operation in VMware Aria Suite Lifecycle.

- To create a content library, see [Create Library](#).
- To import a content library, see [Import Library](#).

VMware Aria Suite Lifecycle supports deployment only from publisher or local content libraries.

- 8 To configure **Binary Mapping**, click **Next**.

Configure binary mapping details

To create an environment in VMware Aria Suite Lifecycle, select one or more binaries for the products.

You can map the correct library items for the respective products deployed by VMware Aria Suite Lifecycle. If none are selected, a default binary from VMware Aria Suite Lifecycle is used to deploy that product.

Procedure

- 1 To add a content library item, click **+SELECT CONTENT LIBRARY ITEMS**.
- 2 Search for a library item or select one from the content library. You can add multiple content libraries and associate products as required.
- 3 Click **Select**.

- 4 Select a **Product** corresponding to the selected content library item.

Note VMware Aria Suite Lifecycle validates the OVF package in the specified content library item corresponding to the selected product.

- 5 Click **Next**.

Note The content library item for a particular node, if it needs to be deployed into a different vCenter, can be selected.

Results

After submitting your binaries maps, click next to configure your network settings.

Configure network details

You can configure an environment by establishing a network connection within an environment in VMware Aria Suite Lifecycle.

Prerequisites

- A static IP address set is required for any product deployment from VMware Aria Suite Lifecycle.
- Verify that you have domain name mapped for the IP addresses used for deployed products.

Procedure

- 1 Under the **Network** page, enter the **Default Gateway** address.
- 2 Enter the **Netmask** IP address.
- 3 Enter the **Domain Name** and **Domain Search Path**.
- 4 The DNS servers are automatically listed. To refresh the list, click **Add New Server** or **Edit Server Selection**.
- 5 Select the required time sync mode:

Option	Description
Use Time Server (NTP)	When you select the NTP server, you have to select the assigned time server from the NTP list. If an NTP server is not added, then to add one, click Global Settings . You are then directed to the Settings page to add an NTP server. For more information, see Configure NTP servers .
Use Host Time	When you select the host time, the environment proceeds with the system time.

- 6 To add an NTP at the infrastructure level after you add NTP servers, click **Select Servers**.
- 7 Select the NTP servers from the list.

When you select a VMware Aria Suite product, you can configure time servers for the selected component.

Configure product details

To view and configure products that were selected during environment creation, use VMware Aria Suite Lifecycle.

You can configure product details as part of installation or as part of subsequent configuration tasks. Under the **Product Details**, select products for a new installation.

Product	Function
VMware Aria Automation	<ol style="list-style-type: none"> To monitor health of VMware Aria Automation, select the Monitor with VMware Aria Operations check box. To manage the workload using load balancer and reclaim unused resources from the resource pool, select the Workload Placement and Reclamation check box. <p>This is only available for a new installation where in VMware Aria Operations monitors health of VMware Aria Automation. Inter-product configuration is not supported for an existing environment.</p> <p>Cross-product integration for VMware Aria Automation with VMware Aria Operations is not applicable for an import of VMware Aria Automation. This option is only applicable if there is a new installation of VMware Aria Automation.</p> <p>If VMware Aria Operations is not present, then you can integrate the products outside of VMware Aria Suite Lifecycle.</p> <p>You can also perform cross-product configuration when VMware Aria Automation is the only product and VMware Aria Operations is a part of an environment or when VMware Aria Automation is deployed with import or as new install of VMware Aria Operations.</p> <ol style="list-style-type: none"> For a newly installed VMware Aria Automation, select the Configure internal pods and service subsets checkbox, and then enter a K8 Cluster IP Range and K8 Service IP Range. Select the product certificate from the drop-down menu. (Optional) Select ON or OFF to activate or deactivate the FIPS compliance mode. Select the Applicable Time Sync mode. Select the Time Server (NTP). For more information, see Configure NTP servers. If you want to configure cluster virtual IPs, then select the Yes or No options. (Optional) Click Anti-Affinity / Affinity Rule check box to create host rules in the vCenter for each deployed VM. <p>For more information about database creation, see Create a new private cloud environment using the installation wizard in VMware Aria Suite Lifecycle.</p>
VMware Aria Automation Config	<ol style="list-style-type: none"> For VMware Aria Automation Config, select the Tenant ID from the drop-down menu under Product Properties. For vVMware Aria Automation Config, enter the VM name, FQDN and Virtual IP Address under Components. <ul style="list-style-type: none"> For VMware Aria Automation Config, you can only perform a single node VMware Aria Automation Config installation at a time. For VMware Aria Automation deployment along with VMware Aria Automation Config, the tenant ID is selected by default. Any additional VMware Aria Automation Config deployment can be performed based on the tenant as organic growth. Federal Information Processing Standard 140-2 Support (FIPS) is supported for VMware Aria Automation Config.

Product	Function
VMware Aria Operations for Logs	<p>Federal Information Processing Standard 140-2 Support (FIPS) is supported for VMware Aria Operations for Logs.</p> <ol style="list-style-type: none"> 1 Select the node size from the drop-down menu. 2 (Optional) Select ON or OFF to enable or deactivate the FIPS compliance mode. 3 Under Integrated Load Balance Configuration, if you select the Configure Cluster Virtual IPs, enter the FQDN and Virtual IP Address. 4 To add more node, click ADD NODE. 5 Select the Applicable Time Sync Mode. 6 Under components, enter the vRLI primary node details. 7 (Optional) Click Anti-Affinity / Affinity Rule check box to create host rules in the vCenter for each deployed VM. 8 (Optional) Click Add Components to configure additional settings. 9 Enter the required fields.
VMware Aria Operations	<p>Federal Information Processing Standard 140-2 Support (FIPS) is supported for VMware Aria Operations for Logs.</p> <ol style="list-style-type: none"> 1 Under Product Properties, select the Disable TLS version from the drop-down menu. 2 (Optional) Select ON or OFF to enable or deactivate the FIPS compliance mode. 3 Select the Certificate from the drop-down menu. 4 (Optional) Click Anti-Affinity / Affinity Rule check box to create host rules in the vCenter for each deployed VM. 5 Add the Product Password. 6 (Optional) Click Integrate with Identity Manager check box. 7 Select the Time Sync Mode. 8 For continuous availability-based deployment, under Components, enter the Infrastructure and Network details for the Witness Domain. 9 For Continuous Availability (CA) based deployment, enter the Infrastructure and Network details for Fault Domain 1 and Fault Domain 2. 10 If you want to add additional data nodes for a cluster, click the Add Components tab. If you select Use Global Configuration, the field data is populated based on the information provided in the Infrastructure tab. You can select this option for Witness Domain, Fault Domain 1, or Fault Domain 2. Ensure that each domain is in different physical location so that if one fault domain fails, nodes from the other fault domain remains active. 11 If you want to add remote collectors, click Add Collector Group, and then add the details for the new collector nodes.
VMware Aria Operations for Networks	<ol style="list-style-type: none"> 1 Under the Product Properties, select the node size from the drop-down menu. 2 Select the applicable Time Sync Mode. 3 Under components, enter the platform and collector details for VMware Aria Operations for Networks. 4 (Optional) Click Anti-Affinity / Affinity Rule check box to create host rules in the vCenter for each deployed VM.

Product	Function
VMware Aria Automation Orchestrator	<p>VMware Aria Automation Orchestrator offers two setup options:</p> <ul style="list-style-type: none"> ■ VMware Aria Automation Orchestrator-Integrated <p>This is the traditional VMware Aria Automation Orchestrator setup option, where VMware Aria Automation Orchestrator is integrated with VMware Aria Automation and you can install VMware Aria Automation Orchestrator after installing VMware Aria Automation</p> ■ VMware Aria Automation Orchestrator Standalone: This setup option has no dependency on VMware Aria Automation and it allows you to integrate with vSphere. <p>In addition to the configuration steps described below, the standalone setup requires the following input:</p> <ul style="list-style-type: none"> ■ vCenter Host: vCenter FQDN. ■ Admin Group: Group name. ■ Admin Group Domain: Domain that the user belongs to. <p>Note To deploy VMware Aria Automation Orchestrator with vSphere authentication using VMware Aria Suite Lifecycle, the Admin Group in vSphere must have full administrator permissions.</p> <ol style="list-style-type: none"> 1 Under the Product Properties, select ON or OFF to enable or deactivate the FIPS compliance mode. 2 Select the Certificate from the drop-down menu. 3 Add the Product Password. 4 Select the applicable Time Sync Mode. 5 For a standard deployment, enter the host name and IP address under Components. 6 Under Cluster Virtual IP, enter the load balancer host FQDN for the cluster deployment. 7 Under Components, enter the host name and IP address for the primary and secondary nodes.
VMware Workspace ONE Access	<ol style="list-style-type: none"> 1 Under the Product Properties, select the certificate from drop-down menu. 2 Select the admin password from the locker. 3 Specify the default configuration admin user name and password. This configuration is created as local user in VMware Workspace ONE Access and is used for VMware Aria Suite product integration. 4 Check Sync Group Members. When enabled, members of the groups are synced from the active directory. When this is deactivated, group names are synced to the directory, but members of the group are not synced. 5 For a cluster deployment, under Cluster Virtual IP, enter Cluster VIP FQDN. This setting is used to load balance the application. 6 For a cluster deployment, enter the database IP address that is used internally for proxy access to the primary postgres database. <p>This is not same as the address used to load-balance the application and the IP address should be free and available.</p> 7 Under Components, enter the VMware Workspace ONE Access single or cluster node details.

Configure VMware Aria Suite products for installation

To configure the product details for each VMware Aria Suite product that you are installing in the private cloud environment, use VMware Aria Suite Lifecycle.

Configuration tabs appear only for the products you selected to install. You can access advanced properties to perform tasks such adding different vCenter instances, activating or deactivating VMware Workspace ONE Access registrations, and so on.

Procedure

- 1 Click the VMware Aria Automation check box to configure installation details for VMware Aria Automation.

- a Enter the fully qualified domain name and the IP address for the VMware Aria Automation appliance.

A Windows user must have administrator rights.

For more information about the VMware Aria Automation appliance, see the KB article [55706](#).

- 2 When installing VMware Aria Automation Config, specify the following additional options:

- VMware Aria Automation Config Standalone

This configuration has no dependency on VMware Aria Automation and the installation proceeds without VMware Workspace ONE Access integration.

- VMware Aria Automation-integrated VMware Aria Automation Config

This configuration allows VMware Aria Automation Config to be installed for each tenant that is configured in VMware Aria Automation performing organic growth.

- 3 Click the VMware Aria Operations check box to configure installation details for VMware Aria Operations.

- a Enter the NTP server address.
- b (Optional) Click the plus sign to **Add components** and then select the component type.
- c Enter the host name in the form of a fully qualified domain name.
- d Enter the IP address for each component.
- e Select the **Node Count** or **Node Size** for VMware Aria Operations deployment. VMware Aria Operations recommends that the number of analytic nodes available for a selection depend on the selected node size.

The default type of deployment for VMware Aria Operations is a node size and node count.

- 4 Click the VMware Aria Operations for Logs check box to configure installation details for VMware Aria Operations for Logs.

- a (Optional) Click the plus sign to **Add components** and select the type of component to add.
- b Enter the host name in the form of a fully qualified domain name and the IP address for each component.
- c If you are adding cluster virtual IPS, optionally enter load balancer settings.
- d Click **Components + icon**, to add and enable any of the configuration during the deployment.

The deployment type available for VMware Aria Operations for Logs is standalone and cluster.

- 5 Click the VMware Aria Operations for Networks check box to configure installation details for VMware Aria Operations for Networks.
 - a (Optional) Click the plus sign to **Add components** and select the type of component to add.
 - b Select the license key if registered in My VMware or enter the license key manually.
 - c Enter the Infrastructure details and select the NTP servers.
 - d Enter the network and certificate details.
 - e Under the **Product Details**, click **Add** component to add a VMware Aria Operations for Networks platform or a collector. This option is dependant on what type of VMware Aria Operations for Networks you are selecting initially. If you have selected a cluster of VMware Aria Operations for Networks, then you can have two platforms and one collector by default.

The deployment type available for VMware Aria Operations for Networks is standard and cluster.

- 6 Click the VMware Aria Automation Orchestrator check box to configure installation details for VMware Aria Automation Orchestrator.

VMware Aria Automation Orchestrator offers two setup options:

- VMware Aria Automation Orchestrator-Integrated

This is the traditional VMware Aria Automation Orchestrator setup option, where VMware Aria Automation Orchestrator is integrated with VMware Aria Automation and you can install VMware Aria Automation Orchestrator after installing VMware Aria Automation
- VMware Aria Automation Orchestrator Standalone: This setup option has no dependency on VMware Aria Automation and it allows you to integrate with vSphere.

The deployment type available for the traditional VMware Aria Automation Orchestrator setup option, where VMware Aria Automation Orchestrator is integrated with VMware Aria Automation is standard and cluster.

- 7 Click **Next**.

Considerations for configuring VMware Aria Automation

Consider the following information when performing scale-out, deployment, replace certificate, and import brownfield operations in VMware Aria Suite Lifecycle.

- When the VMware Aria Automation replace certificate fails intermittently at initialize cluster after replacing the certificate, retry the failed VMware Aria Automation replace certificate.
- VMware Aria Automation HA replace certificate fails at the initial cluster after replacing the certificate, when SAN certificate has additional host names. At this instance, replace the VMware Aria Automation HA certificate with SAN certificate which has the required hostnames like VMware Aria Automation load balancer host name and three VMware Aria Automation hostnames.

- When VMware Aria Automation scale out fails at initialize cluster due to liquibase locks then click the retry option in the failed VMware Aria Automation scale out request to retry the initialize cluster step.
- Verify if the SAN certificate is used instead of wild card certificate for VMware Aria Automation deployment.
- Verify to provide all four host names, including three VMware Aria Automation node host names and a VMware Aria Automation load balancer host name in the SAN certificate when the custom certificate is used.

Continuous availability for VMware Aria Operations

Continuous availability (CA) for VMware Aria Operations prevents loss of data during a node failure and ensures availability of VMware Aria Operations during a physical location failure when working with VMware Aria Suite Lifecycle.

CA segregates the VMware Aria Operations cluster into two fault domains, stretching across vSphere clusters, and protects the analytics cluster against the loss of an entire fault domain. The two fault domains are **Fault Domain 1** and **Fault Domain 2**. By default, the primary node and the replica node are assigned to **Fault Domain 1** and **Fault Domain 2**. If **Fault Domain 1** fails, the functionality is not disrupted as the other pair node ensures that the incident results in no data loss.

The **Witness Node** is the third network domain that exists independently and identifies network partitioning across the two fault domains. If network connectivity between the two fault domains is lost, the cluster goes into a split-brain situation, which is detected by the **Witness Node**. Immediately, one of the fault domains goes offline to avoid data inconsistency problems.

Note A minimum of three pairs of nodes are required to enable CA. You can add a maximum of 16 data nodes, including the primary and replica nodes.

Allow continuous availability for VMware Aria Operations

You can now enable continuous availability (CA) for VMware Aria Operations in VMware Aria Suite Lifecycle.

Prerequisites

Verify that you have a data center and the required environment credentials.

Procedure

- 1 Under **Select Product**, select VMware Aria Operations and then select **New Install**.
- 2 Select the **Version** from the drop-down menu.
- 3 Select **CA** as the **Availability** option.

- 4 Select the **Deployment Type** from the drop-down menu, and based on the selection of the **Deployment Type**, select the number of nodes from the **Node Count** drop-down menu.

Note For more information about the sizing guidelines for VMware Aria Operations continuous availability, see [KB article 78495](#).

Validate private cloud environment details

To configure vCenter, cluster, network, datastore, and certificate details for a new private cloud environment, use VMware Aria Suite Lifecycle.

Procedure

- 1 Enter the details of the vCenter where you are installing the VMware Aria Suite and the names of the cluster, network, and datastore to use for this environment.

The vCenter name must be in the form of a fully qualified domain name.

- 2 Select the disk file format, and click **Next**.

Option	Description
Thin	Use for evaluation and testing.
Thick	Use for production environments.

- 3 Enter the default gateway, domain, domain search path, DNS server, and netmask details for the environment, and click **Next**.

- 4 Enter the key passphrase and private key.

- 5 Enter certificate chain for the SAN certificate to import or select the **Generated Certificate** option, and click **Next**.

For information on generating a SAN certificate, see [Manage certificates for VMware Aria Suite Lifecycle products](#).

- 6 Enter the product details for each of the VMware Aria Suite products that you have selected to install by providing its Windows hostname and IP Address.

- 7 Click the **PRE-CHECK** to run and validate the properties for each of the VMware Aria Suite products.

Note If the pre-check fails, make the recommended corrections and run pre-check again.

- 8 Review the summary information and then click **Submit**.

Pre-check validation

Based on the pre-check validation you can change your input settings and rerun the pre-validation check in VMware Aria Suite Lifecycle.

How does pre-check validation work?

When you click the **Run Pre-Check** button, a report is generated indicating whether the pre-validation is in PASS or FAIL state. Therefore, based on the report you can modify your inputs given in the previous steps and click the **RE - RUN PRE CHECK** button. The report contains the following information:

- Status of the Check
- Check Name
- Component/Resource against which the current check is run.
- Result description about the check execution
- Recommendation, if there is FAILURE or WARNING

The report also generates color coded status:

- GREEN SYMBOL - PASSED
- RED SYMBOL - FAILED
- YELLOW SYMBOL - WARNING
- GREEN FIXED SYMBOL - REMEDIATED & FIXED

You cannot proceed unless the pre-validation is successful. You can track the pre-validation request progress on the **Request** tab as the name VALIDATE_CREATE_ENVIRONMENT. When the pre-validation is finished and the NEXT button is activated, you can submit the request for deployment. When you are submitting, you can skip the pre-validation. By default, this flag is activated. This verifies pre-validations are run before deployment is started. If you skip this, then you can deselect the flag and click **Submit**. Pre-validation does not run again before the deployment begins.

If you click **Submit** with the pre-validation flag activated and a request named VALIDATE_AND_CREATE_ENVIRONMENT is created. If you click **Submit** by deselecting the pre-validation flag, a request named CREATE_ENVIRONMENT is created. You can track the progress of pre-validation requests in the VMware Aria Suite Lifecycle **Request** tab.

Before you run a pre-check on VMware Aria Automation, verify all the component VMs are communicating with VMware Aria Suite Lifecycle appliance. After you activate pre-check and submit the create environment, if pre-check fails then resume the wizard from the **Request** page with a request state as PRE_VALIDATION_FAILED. From the report, if the failure is due to the wrong IaaS credential then rerunning pre-check on updating the Windows password in the product details page still results in the wrong IaaS credential. To fix this, update the Windows password in the product details page at each node level and rerun the re-check.

If the `VALIDATE_AND_CREATE_ENVIRONMENT` request fails with a status `PRE-VALIDATION-FAILED`, then you can validate your inputs by clicking the icon under the action tab. This directs you to the wizard where you can modify your inputs and run `PRE CHECK` or click **Submit** for deployment. When deployment is complete, you can see the last run pre-validation report. This option is available from the environment page in the **Manage Environments** page. You can also view the last run report under **View Last Pre Check Result** under **Environment**.

Note The VMware Aria Suite Lifecycle pre-check operation does not consider extended storage. If the extended storage option is used to deploy VMware Aria Operations nodes by using VMware Aria Suite Lifecycle, the pre-check might succeed but the deployment can fail due to insufficient disk space. For more information, see KB article [56365](#).

Only **Automate checks** is runs a manual pre-requisite for VMware Aria Suite in VMware Aria Suite Lifecycle. You can select `DOWNLOAD SCRIPT` and run on all the Windows machine. The zip contains a readme file, which explains how to run the script. This step is mandatory if you have selected VMware Aria Automation as one of the products during an environment creation.

Replace VMware Aria Automation certificates

To update or replace VMware Aria Automation certificates if your certificate expires or if you are using a self-signed certificate and your company security policy requires you to use its SSL certificates, use VMware Aria Suite Lifecycle.

Procedure

- 1 Create a certificate signing request from VMware Aria Suite Lifecycle (or obtain a SAN) and specify a certificate that includes IP, FQDN, and load balancer VIP FQDN settings.
- 2 In VMware Aria Suite Lifecycle, navigate to the locker, and import a new certificate for VMware Aria Automation.
- 3 In the **Environments** page, select the VMware Aria Automation environment.
- 4 Select the vertical ellipses (...) and then click **Replace Certificate**.

Confirm environment and installation settings

To verify product environment and installation settings, use VMware Aria Suite Lifecycle.

Procedure

- 1 In VMware Aria Suite Lifecycle, verify that the listed environment and installation settings are accurate.
- 2 (Optional) Click **Back** or click the relevant page in the navigation pane to change any settings.

- 3 (Optional) Click **Export** to export a configuration file with all the product and user data for this private cloud.

You can use the exported configuration file to create a private cloud. See [Create a private cloud environment using a configuration file in VMware Aria Suite Lifecycle](#). Modify the exported configuration file as required before using it to create another private cloud. Private and primary key information is not included in the exported configuration file. You must manually insert those keys.

Update or modify the exported configuration file as required before using it to create another private cloud.

- 4 (Optional) Select the **Topology** tab to display the integration of available VMware Aria Suite products in VMware Aria Suite Lifecycle.
- 5 Click on a specific VMware Aria Suite product, group, or node to view the product or node properties, such as FQDN, IP address, network, DNS, and so on.
- 6 Click **Finish**.

VMware Aria Suite Lifecycle creates the private cloud environment and begins installing the selected VMware Aria Suite products.

What to do next

To monitor product installation progress, click **Home**. Installation progress appears under **Recent Requests**.

Import an existing environment using a VMware Aria Suite Lifecycle installation wizard

To import an existing private cloud environment for a VMware Aria Suite product, use the VMware Aria Suite Lifecycle installation wizard.

Prerequisites

- Verify that you have an existing VMware Aria Suite instance.
- Verify that you have an existing data center.
- Verify that you have created or imported a certificate.

Note Certificates are not required for importing an existing environment. However, it is required when you select both import and new install in one flow while creating an environment.

Procedure

- 1 Log in to VMware Aria Suite Lifecycle as a VMware Aria Suite Lifecycle Admin or VMware Aria Suite Lifecycle Cloud Admin and click **Create Environment**.

- 2 After entering the environment data fields, under each of the required VMware Aria Suite product, select **Import** and click the required VMware Aria Suite product check box for the VMware Aria Suite product name.
- 3 Click **Next**.
- 4 In the launched install wizard, on the **Products Details** page, update the details and select all the vCenter servers where all product components are installed.

If you select a combination of import and install for two or more products while creating an environment, then enter the details as a new Install of product. If you are opting for an organic growth by adding another product after creating an environment with **New Install** or combination of **Import** and **New Install**, then the details in Install wizard is already pre-populated. You can go ahead and click **Next**. If you are opting for an organic growth by adding another product after creating an Environment with **Import** only, then the installation wizard details are not pre-populated.

After you import a product for a scale out, you must add a certificate. To manage a certificate, add the certificate from the settings tab and then import during scale out.

- 5 Review the summary information and then click **Submit**.
- 6 Import product certificates.

The VMware Aria Suite Lifecycle Locker cannot import product certificates, so you must import the product certificate after you import the product.

When you import a product into a new environment, the **Product Details** view does not display a certificate entry. However, when you import a product into an existing environment that contains other products, the **Product Details** view does display the environment-level certificate. The relevant certificate is consumed and visible in the Locker Certificates view, but the certificate is not actually assigned. Regardless of where you are importing a product into a new or existing environment, you must import the product certificate after you import the product.

- 7 Perform an inventory synchronization of the imported product.

After inventory synchronization, the **Product Details** view correctly reflects the certificate references.

Import a VMware Workspace ONE Access environment

You can import a VMware Workspace ONE Access instance into VMware Aria Suite Lifecycle.

Procedure

- 1 After creating an environment on the **Create Environment** page, open the product card and select the VMware Workspace ONE Access check box.
- 2 Select **Import** and click **Next**.

3 Enter a valid FQDN address.

To import a clustered VMware Workspace ONE Access, use a load balancer host name.

4 To import with tenancy-enabled VMware Workspace ONE Access, enter the **Default Tenant Alias Host Name**.

The *System Admin*, *Admin*, *SSH User*, and *Root* passwords are listed automatically.

5 Enter the **Default Configuration Admin User name**.

6 (Optional) Select the **Sync Group Members** check box and vCenter list.

7 Click **Next** and review the summary information.

8 Click **Submit**.

Import a VMware Aria Automation environment

You can import an existing instance of VMware Aria Automation into VMware Aria Suite Lifecycle.

For creating a global environment, you are prompted to install VMware Workspace ONE Access if you skipped this step when you initially installed VMware Aria Suite Lifecycle. To install VMware Workspace ONE Access, see [Install VMware Workspace ONE Access in VMware Aria Suite Lifecycle](#). To import a VMware Aria Automation brownfield environment, verify that the VMware Workspace ONE Access in VMware Aria Suite Lifecycle matches the VMware Workspace ONE Access registered with VMware Aria Automation.

Use the same configuration admin user for both VMware Workspace ONE Access and VMware Aria Automation in VMware Aria Suite Lifecycle.

Prerequisites

Verify that you have the required IP credentials.

Procedure

1 After creating an environment on the **Create Environment** page, open the product card and select the VMware Aria Automation check box.

2 Click **Import** and then click **Next**.

3 Under **Products Details**, enter the required VMware Aria Automation fields and then select the **Import** version.

4 Specify the primary node host name and select **Primary Node root Password**.

If each node has different passwords then the import request fails. You can provide the correct password in the retry sequence of each failed request.

5 Select the vCenter where the product nodes reside.

For information about configuring VMware Aria Automation, see [Considerations for configuring VMware Aria Automation](#).

- 6 Click **Submit**.

Import VMware Aria Automation Config

You can import an instance of VMware Aria Automation Config into VMware Aria Suite Lifecycle.

Prerequisites

Ensure that you have the required IP credentials.

Procedure

- 1 After creating an environment on the **Create Environment** page, open the products card and select the VMware Aria Automation Config check box.
- 2 Select **Import** and click **Next**.
- 3 Enter the VMware Aria Automation Config **Master Node IP Address**, **Root**, and **Admin Password** values.
- 4 Under the vCenter servers section, select a vCenter instance.
- 5 Click **Next** and review the summary information.
- 6 Click **Submit** to import.

Import a VMware Aria Operations for Networks environment

You can import an existing VMware Aria Operations for Networks environment into VMware Aria Suite Lifecycle.

Prerequisites

Verify that there is an instance of VMware Aria Operations for Networks along with its user credentials available.

Procedure

- 1 After creating an environment on the **Create Environment** page, open the product card and select the VMware Aria Operations for Networks check box.
- 2 Click **Import** and then click **Next**.
- 3 On the **Product Details** page, enter the **vRNI Admin user name**.
All authorization tokens are generated using the administrator user name and password.

4 Enter the **Console Password** and **Support Password**.

With console user and support user credentials, you can run VMware Aria Operations for Networks-specific commands and debug your environment.

Note The support password for all nodes must be identical. Although, import of VMware Aria Operations for Networks can be successful, future operations such as upgrade precheck, upgrade, password update, clustering and so on fail if the passwords are not identical. You must change the support password of all nodes to one single password. Similarly, console passwords of all nodes must be identical. The console and support password can be identical for all nodes. If each node has different passwords, then the import request fails. You can provide the correct password in the retry of each failed request sequence.

5 Enter the **vRNI Admin Password** and **Platform IP** address.

6 Select the vCenter instance from the drop-down menu and click **Next**.

7 Review the summary information and then click **Submit**.

Example: Console and support password

For a standard VMware Aria Operations for Networks deployment:

- Platform: support password=VMware1! consoleuser password=Test@123
- Collector: support password=VMware1! consoleuser password=Test@123

For a 3 node cluster with 1 collector:

- Platform1: support password=VMware1! consoleuser password=Test@123
- Platform2: support password=VMware1! consoleuser password=Test@123
- Platform3: support password=VMware1! consoleuser password=Test@123
- Collector: support password=VMware1! consoleuser password=Test@123

Import a VMware Aria Operations environment

You can import an instance of VMware Aria Operations into VMware Aria Suite Lifecycle.

Prerequisites

Verify that you have the required IP credentials.

Procedure

- 1 After creating an environment on the **Create Environment** page, open the product card and select the VMware Aria Operations check box.
- 2 Select **Import** and then click **Next**.
- 3 Enter the VMware Aria Operations **Master Node IP Address**, **Root**, and **Admin Password**.

The admin password should be for a local user only, not a user with administrator permissions.

If you are importing an existing VMware Aria Operations installation, enable SSH for all the VMware Aria Operations nodes and set root passwords in all nodes.

- 4 Select a vCenter instance.
- 5 Click **Next** and review the summary information.
- 6 Click **Submit** to import.

If each node has different passwords, the import request fails. You can provide the correct password in the retry operation for each failed request.

Import a VMware Aria Automation Orchestrator environment

You can import an instance of VMware Aria Automation Orchestrator into VMware Aria Suite Lifecycle.

Prerequisites

- Verify that you have the required IP credentials.
- If you are using the traditional VMware Aria Automation Orchestrator setup option, where VMware Aria Automation Orchestrator is integrated with VMware Aria Automation , verify that you have a VMware Aria Automation environment prior to installing VMware Aria Automation Orchestrator.
 - If VMware Aria Automation is multi-tenancy enabled, you can install multiple instances of VMware Aria Automation Orchestrator in VMware Aria Suite Lifecycle.
 - If VMware Aria Automation is not multi-tenancy enabled, you can only install instance of VMware Aria Automation Orchestrator in VMware Aria Suite Lifecycle.

Note VMware Aria Automation Orchestrator offers two setup options:

- **VMware Aria Automation Orchestrator-Integrated**
This is the traditional VMware Aria Automation Orchestrator setup option, where VMware Aria Automation Orchestrator is integrated with VMware Aria Automation and you can install VMware Aria Automation Orchestrator after installing VMware Aria Automation
- **VMware Aria Automation Orchestrator Standalone:** This setup option has no dependency on VMware Aria Automation and it allows you to integrate with vSphere.

For related information, see [Configure product details](#) .

Procedure

- 1 After creating an environment on the **Create Environment** page, select the VMware Aria Automation Orchestrator check box on the product card.
- 2 Select **Import** and then click **Next**.
- 3 Enter the **vRO Hostname** and **Root Password** of VMware Aria Automation Orchestrator.

- 4 Enter the **vIDM Tenant Admin** and **vIDM Tenant Admin Password**.
- 5 Select the vCenter instances from the list.
- 6 Click **Next** and review the summary information.
- 7 Click **Submit**.

Import a VMware Aria Operations for Logs environment

You can import an instance of VMware Aria Operations for Logs into VMware Aria Suite Lifecycle.

Prerequisites

Verify that you have the required IP credentials.

Procedure

- 1 After creating an environment on the **Create Environment** page, open the product card and select the VMware Aria Operations for Logs check box.
- 2 Select **Import** and then click **Next**.
- 3 Specify the VMware Aria Operations for Logs **Master Node FQDN**, **Root**, and **Admin Password**.

Note For **Admin Password**, select the admin user password for the VMware Aria Operations for Logs local admin user (the **vRLI password**), not the VMware Aria Suite Lifecycle admin user.

Note If each node has different passwords, the import request fails. You can provide the correct password in the retry of each failed request.

- 4 Select a vCenter instance.
- 5 Click **Next** and review the summary information.
- 6 Click **Submit**.

Create a private cloud environment using a configuration file in VMware Aria Suite Lifecycle

To create a private cloud environment with a product configuration file, use VMware Aria Suite Lifecycle.

Review the [What is a Private Cloud](#) information before you configure your environment.

When you are creating an environment using a JSON specification file, if the VMware Aria Suite Lifecycle locker ID for the passwords is used, you must use the respective locker ID from the current VMware Aria Suite Lifecycle. Navigate to **Locker > Passwords** and copy the password ID, and use it in the specification file. There is no action required for a plain text password.

When using a JSON specification file, you must update all the parameters in each node's advanced settings as required. |

Prerequisites

- Configure OVA settings for the products to install. See [Configure product binaries](#).
- Ensure that you have added a vCenter to the data center with valid credentials and that the request has completed.

Procedure

- 1 Log in to VMware Aria Suite Lifecycle as administrator and click **Create Environment**.
- 2 From **Data Center**, select an existing data center for this environment, or click **+** to add a data center to VMware Aria Suite Lifecycle.

For information about adding a data center, see [Add and manage data center associations for VMware Aria Suite Lifecycle](#).

- 3 Activate or deactivate the JSON configuration toggle, as required. When you activate the JSON configuration file, you can paste the JSON file text manually or you can import the file from your local system.
- 4 (Optional) Select **Join the VMware Customer Experience Program** to join CEIP for this environment.

This product participates in the VMware Customer Experience Program (CEIP). Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at <http://www.vmware.com/trustvmware/ceip.html>.

You can join or quit the program later by selecting the **Lifecycle Operations** service and then selecting **Settings > System Details**. Select **JOIN** or **QUIT** in the **Customer Experience Program** section of the **System Details** page.

- 5 Click the **Use Configuration file** toggle feature.
- 6 Paste the text of the product configuration JSON file into the **Product Config JSON** text box, and click **Next**.

You can download the configuration file from the summary page to create a JSON file for the product or the solution with the latest inputs that were provided while configuring the environment.

The create installation wizard is launched and the JSON data is populated. You can validate the data before you click submit. For more information on getting a sample JSON file, see KB article [75255](#).

What to do next

To monitor product installation progress, click the **Home** button. VMware Aria Suite Lifecycle displays installation progress for the environment under **Recent Requests** and on the **Requests** tab.

Create a hybrid environment using a cloud proxy in VMware Aria Suite Lifecycle

When you want to create a hybrid environment, and require the software-as-a-service to manage your on-premise data, you can use the cloud proxy. The cloud proxy environment enables software-as-a-service and VMware Cloud services to communicate with on-premise services.

Configuring environment settings for a new cloud proxy

To configure environment settings, such as name, password, and data center for a new cloud proxy environment, use VMware Aria Suite Lifecycle.

Procedure

- 1 Log in to VMware Aria Suite Lifecycle as an administrator and click **VMware Aria Cloud**.
- 2 Click **Create / Deploy Cloud Proxy**.
- 3 In the **Environment Name**, enter a descriptive name for the new cloud proxy environment. This name must be unique.
- 4 Enter the **Environment Description**, which can be a maximum of 1024 characters.
- 5 Enter a **Default Admin Password** and confirm the password. The default password must be a minimum of 8 characters.
- 6 From **Data Center**, select an existing data center for this environment or click **+** to add a data center.
- 7 Activate or deactivate the **JSON Configuration** toggle, as required. When you activate the JSON configuration, you can paste the JSON file text manually or you can import the file from your local system.
- 8 Select **Join the VMware Customer Experience Program** to join CEIP for this environment. This product participates in the VMware Customer Experience Program (CEIP). Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at <http://www.vmware.com/trustvmware/ceip.html>.

Installing cloud proxy products

The available cloud proxy products are cloud extensibility proxy (ABX cloud proxy), VMware Cloud services data collector (target cloud proxy), and VMware Aria Operations for Networks cloud proxy. To select the cloud proxy products to install in the private cloud environment, use VMware Aria Suite Lifecycle.

Prerequisites

Verify that you have the required data center and environment credentials.

Procedure

- 1 Select the cloud proxy products to add to the private cloud environment, and then select the **Installation Type**.

You can perform a fresh installation of a product or import from an existing installation of the product.

- 2 Select the **Deployment Type**.
- 3 Click **Next**.

What to do next

After installing the cloud proxy products and to finish EULA and license selection, configure certificate details, and configure network details, complete the procedure at [Create a new private cloud environment using the installation wizard in VMware Aria Suite Lifecycle](#) for your product release.

Configuring cloud proxy product details

To view and configure the cloud proxy products that were selected during environment creation, use VMware Aria Suite Lifecycle.

Product	Function
Install cloud extensibility proxy	<ol style="list-style-type: none"> 1 Under Product Properties, enter the Proxy Name. 2 Select the Product Password. 3 Select the Refresh Key. 4 Under Components, enter the VM Name, FQDN, and IP Address. 5 Click Next.
Install VMware Cloud Services data collector	<ol style="list-style-type: none"> 1 Under Product Properties, enter the Proxy Name. 2 Select the VMware Aria Automation Assembler and VMware Aria Operations for Logs check boxes, as applicable. 3 Select the Product Password. 4 Select the Refresh Key. 5 Under Components, enter the VM Name, FQDN, and IP Address. 6 Click Next.
Install VMware Aria Operations for Networks cloud proxy	<ol style="list-style-type: none"> 1 Under Product Properties, enter the Proxy Name. 2 Select the Product Password. 3 Select the Refresh Key. 4 For a new server, enter the following details: <ol style="list-style-type: none"> a Add the server Name and FQDN/IP Address. b Click Submit. 5 For an existing server, enter the following details: <ol style="list-style-type: none"> a Select the NTP Servers. b Click Next. c Change Server Priority, as required. d Click Finish. 6 Under Components, enter the VM Name, FQDN, and IP Address. 7 Click Next.

What to do next

To validate details and complete installation after configuring the cloud proxy product details, complete the procedure at [Create a new private cloud environment using the installation wizard in VMware Aria Suite Lifecycle](#) for your release.

Upgrade your cloud extensibility proxy

The cloud extensibility proxy (ABX cloud proxy) is a virtual appliance that you can use to configure the on-premises extensibility action integrations with the VMware Aria Automation Orchestrator integrations in VMware Aria Automation Assembler. The following procedure shows how to upgrade an installed cloud extensibility proxy, using VMware Aria Suite Lifecycle.

Prerequisites

- Verify that you are running VMware Aria Suite Lifecycle 8.14 or later.

- Create a snapshot of the existing cloud extensibility proxy product. See [Create and manage a product snapshot](#)

Procedure

- 1 Log in to VMware Aria Suite Lifecycle.
- 2 On the **My Services** dashboard, click **VMware Aria Cloud**.
- 3 In the navigation list at the left, select **Cloud Proxies**.
- 4 On the **Cloud Environments** page, select the cloud extensibility proxy that you want to upgrade.
- 5 The **Cloud Extensibility Proxy** page appears.
 - a Click **Upgrade**.
 - b Click **Trigger Inventory Sync**.
 - c When the prompt for **Proceed to Upgrade** appears, click **Proceed**.
- 6 The **Upgrade Cloud Extensibility Proxy** page appears.

Prepare for the upgrade.

- a The URL of the repository where the upgrade is located is populated by default. Click **Next**

Note A version check ensures that the version in the upgrade repository is newer than the currently installed version. If the version check fails, a message reports that the upgrade is not available and the upgrade process ends.

- b For snapshot type, **Take product snapshot** is selected by default. Click **Next**.
- c Click **Run Precheck**.

The precheck verifies:

- SSH connectivity status
- Password compliance
- vCenter properties availability
- vCenter managed object reference ID presence
- VMware Aria Automation cloud extensibility proxy health
- Hostname resolvability
- Unique IP address resolvability

If any checks fail, click **Download Report** to see the recommended actions. Then after taking corrective action, click **Re-run Precheck**. If all checks pass, click **Next**.

- d When the upgrade summary appears, verify that the upgrade details are correct, then click **Submit**.

Results

The **Request Details** page appears and shows how each upgrade stage is progressing. The upgrade requires approximately one hour to complete.

Onboarding VMware Aria Universal Suite subscriptions

VMware Aria Universal Suite is a SaaS cloud management suite that combines automation, operations, and log analytics into one license. You can start using and managing your VMware Aria Universal Suite subscription with the help of VMware Aria Suite Lifecycle and VMware Aria Subscription.

Prerequisites

For information about activating your subscription license and starting the onboarding process, see the [vRealize Cloud Universal Onboarding guide](#). To manage your licenses in VMware Aria Suite Lifecycle, see [Chapter 8 Managing product licenses in VMware Aria Suite Lifecycle by using the Locker service](#).

Managing environments in VMware Aria Suite Lifecycle

4

You can manage data centers, vCenter servers, and VMware Aria Suite products in your private cloud environments by using VMware Aria Suite Lifecycle.

Read the following topics next:

- [Day 2 operations for global environment in VMware Aria Suite Lifecycle](#)
- [Day 2 operations with other products in VMware Aria Suite Lifecycle](#)
- [Add a product to an existing private cloud environment](#)
- [Add a data source to an existing private cloud environment](#)
- [Manage a data source in an existing private cloud environment](#)
- [Update bulk passwords for data sources](#)
- [Scale out Workspace ONE Access for high availability in VMware Aria Suite Lifecycle](#)
- [Scale out VMware Aria Suite products](#)
- [Scale up VMware Aria Suite products](#)
- [Export a private cloud environment configuration file](#)
- [Download private cloud product logs](#)
- [Delete an environment](#)
- [Managing VMware Aria Suite products in a private cloud](#)
- [Configure health monitoring for the VMware Aria Suite management stack in VMware Aria Suite Lifecycle](#)
- [Adding and managing content from Marketplace](#)

Day 2 operations for global environment in VMware Aria Suite Lifecycle

A global environment is created after an installation or a migration of VMware Aria Suite Lifecycle. A global environment displays the VMware Workspace ONE Access instance and version.

When you click the **View Details** on a created environment, you can view the lists of primary, secondary, and connector information of the VMware Workspace ONE Access that is used in the VMware Aria Suite Lifecycle. You can view the product properties for each the VMware Workspace ONE Access cluster. To view the list of inter-product configurations, click the **Product References**.

After an upgrade, all products currently integrated with global environment VMware Workspace ONE Access are shown in the **Product References** list. The global environment VMware Workspace ONE Access **View Details** page contains the Day 2 operations:

- Topology

The topology viewer displays the group and node structure, vCenter, and product integration details between VMware Workspace ONE Access and VMware Aria Suite products.

- Initiate cluster health check

This option initiates an instant health check on the VMware Workspace ONE Access cluster nodes and provides a notification in VMware Aria Suite Lifecycle.

Based on the health status of the cluster nodes, a `vIDM vPostgres Cluster Health` notification is specified as either `CRITICAL` or `OK`. For the notification to be precise, verify that VMware Workspace ONE Access can communicate with all the VMware Workspace ONE Access nodes in the cluster and that the global environment VMware Workspace ONE Access inventory is up-to-date in VMware Aria Suite Lifecycle.

The health check includes `postgres service` status check, `pgpool service` (responsible for automatic failover) status check, and `Delegate IP` (database load balancer IP) availability checks in addition to basic VMware Workspace ONE Access service availability checks.

If a status is marked `CRITICAL`, a link to the KB article [75080](#) is provided. The health check runs every hour as a scheduled job. The latest health statuses are updated in the `vIDM vPostgres Cluster Health` notification.

If VMware Workspace ONE Access is clustered through VMware Aria Suite Lifecycle, you can use the **Power ON** option to remediate the critical cluster health.

- Power ON

This option powers on the VMware Workspace ONE Access nodes and ensures that all required services are bootstrapped. It repairs any inconsistencies in a clustered instance (VMware Aria Suite Lifecycle clustered VMware Workspace ONE Access), such as fixing the Delegate IP (database load balancer IP) and any replication delays in the secondary nodes. If VMware Workspace ONE Access is clustered through VMware Aria Suite Lifecycle, use this option for any use case which involves powering on the cluster like snapshot revert, reboot, power on.

Note When performing the Power ON operation, if you activate the **Reboot vIDM nodes** checkbox, the reboot is performed as a part of the remediation. If you deactivate the checkbox, the request fails if a reboot is required to remediate the cluster.

- Power OFF

This option powers off all the VMware Workspace ONE Access services by shutting them down. It also brings down the services that are responsible for an automatic failover, and any related components in a clustered deployment. The option is available for single node and clustered node VMware Workspace ONE Access.

If VMware Workspace ONE Access is clustered through VMware Aria Suite Lifecycle, use this option for a scenario that involves bringing down the cluster, such as reboot and shut down. Creating a VMware Workspace ONE Access snapshot through VMware Aria Suite Lifecycle stores the snapshot after bringing down the VMware Workspace ONE Access services gracefully.

Note A change in VMware Workspace ONE Access certificate requires re-trusting the VMware Workspace ONE Access certificate for all products and services that are integrated with it. When updating a certificate, you can select all currently referenced products for re-trust. For more information about product references, see [Product references for VMware Aria Suite Lifecycle](#). For more information about hardware requirements based on the number of users in a directory, see [System and Network Configurations Requirements](#) for your product release.

Resize hardware resources for VMware Lifecycle Manager in VMware Aria Suite Lifecycle

To resize the hardware required for a deployed VMware Lifecycle Manager environment, use VMware Aria Suite Lifecycle.

Procedure

- 1 On the Workspace ONE Access **Global Environment** page, click the ellipses.
- 2 Click **Cluster Health**.

After the cluster health collection is complete, the health status is displayed in the VMware Aria Suite Lifecycle in the notification lists.

Note If the status is red, click **Power ON**. For related information, see KB article [75080](#).

- 3 You can scale up to the required size by performing a vertical scale up. For more information, see [Scale up VMware Aria Suite products](#).

Results

For information about hardware requirements for Workspace ONE Access when integrated with VMware Aria Automation, see the hardware requirements in the [vRealize Automation Reference Architecture](#) for your release.

To additional information about the hardware requirements based on the number of users in a directory, see [System and Network Configurations Requirements](#) for your Workspace ONE Access product release.

Day 2 operations with other products in VMware Aria Suite Lifecycle

You can perform day 2 operations for integrated products by using VMware Aria Suite Lifecycle.

Day 2 operations for all products - excluding Workspace ONE Access

The VMware Aria Suite products on the **Environments** page consist of the following capabilities:

- Topology

The **Topology** viewer displays the node structure and integrations between different VMware Aria Suite products within VMware Aria Suite Lifecycle. You can select the available VMware Aria Suite product and display the version, certificate, and license details. You can also select a primary or secondary node to view the FQDN, IP address, network, DNS, and other node properties.

- New collector group

New collector groups are available for VMware Aria Operations. You can add new collectors, group new collector nodes, and move collector nodes into new collector groups. You can also add a remote collector and cloud proxy to the collector group.

Note Do not add a cloud proxy to a collector group from a remote collector. Create a separate cloud proxies group that contains only cloud proxies.

- Re-trust with VMware Workspace ONE Access

When a VMware Workspace ONE Access certificate changes, all products and services that are integrated with VMware Workspace ONE Access must be configured to retrust the VMware Workspace ONE Access certificate. When you replace or change a VMware Workspace ONE Access certificate, all products that integrated with VMware Workspace ONE Access are available for re-trust on the **Product References** page.

Note This option applies only to products that are integrated with a VMware Workspace ONE Access global environment and that appear in the **Product References** table in the VMware Workspace ONE Access global environment.

- Re-register with VMware Workspace ONE Access

Products that are integrated with VMware Workspace ONE Access are registered with the VMware Workspace ONE Access FQDN endpoint. If the VMware Workspace ONE Access FQDN changes, products and services that are integrated with VMware Workspace ONE Access must re-register with the new VMware Workspace ONE Access FQDN.

- Enable FIPS compliance mode

The FIPS compliance mode option is available for VMware Aria Operations for Logs and VMware Aria Operations. You can activate or deactivate the FIPS mode during product deployment. Alternatively, you can select the **Enable FIPS Compliance** option for the product level operation on the **Manage Environments** page.

Note If you activate the FIPS mode for a VMware Aria Suite product, you cannot revert and run it on a non-FIPS mode.

- Update NTP configuration

After deploying a VMware Aria Suite product, you can update its NTP configuration details. Using the **Time Sync Mode** option, you can specify either the NTP server time or the EXSi host time. When you choose the NTP server, you can add new server details or you edit existing server details, such as the server name and FQDN/IP address. You can also change the priority of the servers.

Day 2 operations for VMware Aria Automation clustered deployment

If the VMware Aria Automation load-balancer is configured such that SSL is terminated at the load-balancer, then for any change of certificate in the load balancer must be re-trusted in VMware Aria Automation. In a clustered deployment of VMware Aria Automation, you can click **Re-trust Load Balancer** to re-trust the load balancer certificate in VMware Aria Automation.

Note This operation primarily checks VMware Aria Suite Lifecycle inventory of the clustered VMware Aria Automation before performing the re-trust. The inventory data for clustered VMware Aria Automation has a `vra-va-ssl_terminated_at_load-balancer` parameter under the **Cluster VIP** section of product properties. The parameter decides whether the SSL is terminated at the VMware Aria Automation load balancer. For all green text box VMware Aria Automation deployments, this option is provided as an input to be completed by the user. For an existing brown field deployment, the parameter value is automatically computed.

Note Start up and shutdown operations are also available for VMware Aria Automation, which helps to gracefully start and shut down the VMware Aria Automation services.

Reconfigure internal pods and service subnets

You can modify the VMware Aria Automation internal IP range by using VMware Aria Suite Lifecycle.

Prerequisites

Verify that a product has existing internal IP range values. For information on K8 service and cluster IP range, see [Install VMware Aria Automation by using VMware Aria Suite Lifecycle Easy Installer](#).

Procedure

- 1 From the **Environment** page, select a product card and then click the vertical ellipses.

- 2 Select **Reconfigure Internal Pods and Service Subnets**.
- 3 Enter internal IP range values for **K8 Cluster IP Range** and **K8 Service IP Range**.
- 4 Click **Next**.
- 5 To validate the IP range information, click **RUN PRECHECK** , and click **Finish**.

Add a product to an existing private cloud environment

To change your environment, add a product to an existing environment in VMware Aria Suite Lifecycle.

You can import an existing VMware Aria Suite product into an existing environment. You can also add to an existing environment by deploying a fresh product deployment.

An environment can contain only one instance of each supported VMware Aria Suite product.

Prerequisites

Verify that you have an existing private cloud environment in VMware Aria Suite Lifecycle that does not already contain the supported VMware Aria Suite products.

Procedure

- 1 Click **Manage Environments**.
- 2 To perform organic growth, click the ellipsis (...) for the environment and select **Add Products**.
- 3 Select the products to add and enter the necessary configuration information.

Add a data source to an existing private cloud environment

To collect network information by adding a data source to your environment, use VMware Aria Suite Lifecycle.

Prerequisites

Verify that you have an existing VMware Aria Operations for Networks instance in VMware Aria Suite Lifecycle.

Procedure

- 1 Click **Manage Environments**.
- 2 Click **View Details of Environments** for the environment in which to add the data source.
- 3 Click the ellipsis (...) for VMware Aria Operations for Networks, and select **Add Data Source**.
- 4 Enter the required details and click **Submit Request**.

Data operations supported by VMware Aria Operations for Networks

To add data source types that are supported by VMware Aria Operations for Networks, use VMware Aria Suite Lifecycle.

Data source	Description
vCenter	You can enter the vCenter information and proxy details in the provided fields.
NSX Manager	You can enter the NSX information and proxy details in the provided fields.
Routers and switches	You can enter the SNMP configuration details in the provided fields by clicking the Advanced Settings . Note You can add similar data sources to the VMware Aria Operations for Networks that are specific to its respective products or functionalities.

Import data sources in VMware Aria Suite Lifecycle

You can import data sources in bulk into VMware Aria Operations for Networks by using VMware Aria Suite Lifecycle.

This capability is helpful when the same SNMP or other network configuration must be used for multiple switches. Common configurations and variable parameters such as IP address must be imported in VMware Aria Suite Lifecycle and provisioned in VMware Aria Operations for Networks.

You can also import data sources when you import a VMware Aria Operations for Networks instance.

Prerequisites

Verify that you have an existing VMware Aria Operations for Networks instance.

Procedure

- 1 From a VMware Aria Operations for Networks environment card, right click on the vertical ellipses and select **Add Data Sources > Bulk**.
- 2 Select CSV or JSON format to import the data sources in a defined report format.
- 3 Click **SELECT File**, select the file, and then click **Next**.
- 4 Click **Submit Request**.
You can view requests on the **Request** page.
- 5 To update a file in the required format, click **Download Template**.

Manage a data source in an existing private cloud environment

You can edit or delete a data source in your environment by using VMware Aria Suite Lifecycle.

Prerequisites

Verify that you have created a VMware Aria Operations for Networks data source in VMware Aria Suite Lifecycle.

Procedure

- 1 In the VMware Aria Suite Lifecycle dashboard, click **Manage Environments**.
- 2 On the **Environments** page, select the VMware Aria Operations for Networks product card and then click **View Details**.
- 3 Click **EDIT DATA SOURCE** or **DELETE DATA SOURCE**, as applicable.
 - a If you click **DELETE DATA SOURCE**, the selected data source is deleted.

Note If a data source is referenced in any other data source of VMware Aria Suite Lifecycle, you cannot delete the referenced data source.

- b If you click **EDIT DATA SOURCE**, you can edit the collector (proxy) VM, data source user name, data source password, and the data source nickname.

Note By default, the data source IP address/FQDN is deactivated.

- 4 Click **SUBMIT**.

Update bulk passwords for data sources

To perform a bulk password update for data source passwords, use VMware Aria Suite Lifecycle.

Prerequisites

Verify if you have created VMware Aria Operations for Networks data source passwords in VMware Aria Suite Lifecycle.

Procedure

- 1 Under **Environments**, select the data sources that you want to update.
- 2 Select the VMware Aria Operations for Networks product card, click the vertical ellipses for the environment, and then click **Change Data Sources Password**.
- 3 Under **Select Data Sources**, select the data sources to update, and then click **Next**.
- 4 Under **Update Credentials**, click **New Password** and then click **Next**.

Note If you select multiple data sources to update passwords, the new password applies to all the selected data sources.

- 5 Under **Precheck details**, click **RUN PRECHECK** and then click **Next**.
- 6 Under **Summary**, verify the changes for the data sources.

7 Click **Finish**.

Note When you perform a bulk password update and one or more passwords fail to update, the request is marked complete. No warning appears for passwords not updated. Click the data source details for information, and then retry updating the bulk passwords.

Scale out Workspace ONE Access for high availability in VMware Aria Suite Lifecycle

To increase high availability options in Workspace ONE Access, use VMware Aria Suite Lifecycle.

- Take a snapshot of the Workspace ONE Access node and VMware Aria Suite Lifecycle before you perform the scale-out operation. Scale out allows you to go from one node to three nodes.
- Verify that there is a certificate already added in the VMware Aria Suite Lifecycle Locker. This certificate should include in the SAN field the FQDN of the three nodes and load balancer. IPs are optional.
- Verify that there is a single A and single PTR DNS record created for each of the two new nodes and the load balancer.
- The Scale Out operation requires four additional IPs - two for the secondary nodes, one for the load balancer, and one for the delegate IP. The delegate IP does not require a DNS record.
- Replace the certificate on the standalone Workspace ONE Access node. The certificate should also have the SAN entries of all the three nodes or wild-card certificate. For information on replacing certificates, see [Replace certificate for VMware Aria Suite Lifecycle products](#).
- Scale-In is not supported when you deploy Workspace ONE Access cluster through VMware Aria Suite Lifecycle.

Note If you apply [KB 87185](#) patch on a single node appliance, and then perform scale-out to cluster operations, follow [KB 87185](#) to apply the patch on the scaled out nodes.

Prerequisites

Note that the VMware Identity Manager and Workspace ONE Access terms are used interchangeably in VMware Aria Suite Lifecycle product documentation.

For a Workspace ONE Access cluster and replace certificate actions, take a snapshot of the Workspace ONE Access nodes before performing any scaling operations. For related information about replacing the VMware Identity Manager certificate, see [Replace your Workspace ONE Access certificate by using VMware Aria Suite Lifecycle](#) .

You should configure a load balancer and add its VIP to the certificate before performing the scale-out operation. For information about configuring a load balancer, see the *VMware Aria Automation and VMware Aria Automation Orchestrator Load Balancing* product [documentation](#). For additional information, refer to the Workspace ONE Access load-balancing [documentation](#) to configure highly-available identity provider for VMware Aria Automation.

Workspace ONE Access does not support SSL passthrough. You must manually import the certificate into the load balancer before performing this scale-out operation.

Procedure

- 1 Navigate to **Environments**, on the environment page, click **Add Component** .
- 2 Enter the **Infrastructure** details and click **Next**.
- 3 Enter the **Network** details and click **Next**.

Verify that the primary node and the additional components use the same default gateway and they are connected with each other.

- 4 On the **Product Properties**, the certificate details are auto-populated.
- 5 On the **Components** tab, select **Take product snapshot** or **Retain product snapshot taken**. If the **Take product snapshot** is set to true, the snapshot is taken prior to starting scale out, and can be rolled back to its initial state during a scale out failure, the snapshot is taken with the prefix `LCM_AUTOGENERATED`. If the **Retain product snapshot taken** is set to true, it can be retained.

Note A snapshot rollback action is available for the failed scale out request on the requests page.

- 6 Enter the load balancer host name.
- 7 Enter a delegate IP address.

Note The delegate IP address is used internally as a proxy to postgres master (primary). It should be a free or an available IP address. This is not same as the IP address used to load-balance the application.

Note You can add two components of type secondary and provide an FQDN and IP address. It is recommended for a Workspace ONE Access cluster to contain of three nodes behind a load balancer.

- 8 Click and run the pre-check.
- 9 Click **Submit**.

Note If you do not restart the appliance, the scale-out procedure fails with an `unable to find root certificate error`.

Scheduled health checks

You can use VMware Aria Suite Lifecycle to schedule health checks.

For clustered instances of VMware Workspace ONE Access a health check runs every hour. You can view the cluster health status in the VMware Aria Suite Lifecycle environment card.

The following postgres cluster health checks are important and may require attention:

- 1 Workspace ONE Access nodes reachability from VMware Aria Suite Lifecycle.
- 2 DelegateIP assignment to any of the cluster nodes.
- 3 Postgres primary node existence.
- 4 Postgres nodes having replication delay.
- 5 Postgres nodes being marked as down in the cluster.
- 6 Pgpool primary node existence.
- 7 Pgpool running on all nodes.

The above checks are captured and appropriate description messages are displayed in a notification similar to the following example:

```
vIDM postgres cluster health status is critical
```

For related information, see the KB article [75080](#).

If all the health checks are validated, VMware Aria Suite Lifecycle provides a notification message such as the following:

```
vIDM postgres cluster health status is ok
```

For related information about scheduling cluster health checks for Day 2 operations, see [Day 2 operations for global environment in VMware Aria Suite Lifecycle](#).

You can pause the health notifications when troubleshooting issues, such as Workspace ONE Access password management, replacing certificates, upgrade related issues, and more.

When performing an hourly check or during a maintenance, you can click the **Pause Cluster Health Check**, and then click **Submit** to pause the health notifications. You can also use similar options to resume the health check.

Scale out tenant-enabled Workspace ONE Access

To scale out a tenant-enabled Workspace ONE Access environment, use VMware Aria Suite Lifecycle.

A tenant-enabled Workspace ONE Access can only be accessed by tenant FQDNs. Scaling out a tenant-enabled Workspace ONE Access from a single node to a three node cluster behind a load balancer requires changes to its DNS and certificate requirements.

All the Workspace ONE Access tenant FQDNs must point to the load balancer IP address instead of a single node IP address. The Workspace ONE Access load balancer certificate must hold all the tenant FQDNs. For more information on mandatory certificates and DNS requirements, see [Multi-tenancy model for VMware Aria Suite Lifecycle products](#).

The same recommendations are provided in the VMware Aria Suite Lifecycle user interface as a pre-requisite before scaling out the Workspace ONE Access global environment. For more information, see [Multi-tenancy model for VMware Aria Suite Lifecycle products](#).

Scaling a Windows connector

To scale up a Windows connector, use VMware Aria Suite Lifecycle.

Prerequisites

Follow these prerequisites for a Windows system in which the connector is to be installed.

- The supported JRE version is between 8 update 181 to 8 update 251.
- The supported .NET framework version is 4.6.0.
- The supported Windows Server versions are 2012 R2, 2016, and 2019.
- A unique Windows system is required for the migration and it must be connected to a domain server.

Procedure

- 1 Navigate to **Environments** on the environment page, and then click **Add Components**.
- 2 Enter the **Infrastructure** details and then click **Next**.
- 3 Enter the **Network** details and then click **Next**.

Verify that the primary node and the additional components use the same default gateway and they are connected with each other.

- 4 On the **Product Properties** page, verify that the certificate details are auto-populated.
- 5 On the **Components** tab, select **Windows Connector**.
 - a Enter the **Windows VM Name** value.
 - b Enter the **FQDN** value.
 - c Enter a user-defined Windows **Connector Name** value and then select **Connector Admin Password**.
 - d Enter the **Domain Admin** details.
- 6 Click and run the pre-check.
- 7 Click **Submit**.

Scale out VMware Aria Suite products

To add components to your product and form a cluster by configuring a multi node setup, use VMware Aria Suite Lifecycle.

Prerequisites

Before you add a product component, you must first perform the certificate mapping in the VMware Aria Suite Lifecycle locker. When you replace the VMware Aria Automation certificate by using the new certificate added to locker, the new certificate contains additional host entries for new components to be added during scale out. After you import or create a certificate in the locker, apply the certificate in the product. The additional components are then visible in the product.

To map the certificate for the product in the locker, import the product certificate in the locker and initiate the inventory sync for that product. This creates a reference for that product with the certificate in the locker. This is applicable for an import scenario.

Verify that the certificate is replaced in the product where the certificate contains all the product components host names including the load balancer host name and a new additional component host names that are added is also specified. For more information on replacing certificates, see [Replace certificate for VMware Aria Suite Lifecycle products](#). For more information on load balance, see Load Balancing Guide on the [VMware Aria Automation Documentation](#) page.

Procedure

- 1 On the environment card, select a product, click the vertical ellipses, and select **Add Component**.

For an imported environment, manually enter the text boxes for the selected product.

Note At times, scaling out patched products from VMware Aria Suite Lifecycle might fail. This is because joining the cluster fails due to version mismatch in the product appliances. You can download and use the OVA corresponding to the patch. When you add a component, a warning message appears indicating whether the OVA required to scale out the patched product is available or not in the VMware Aria Suite Lifecycle. The required OVA bundle can be downloaded from My VMware portal into the VMware Aria Suite Lifecycle appliance and mapped. You can download and map the patched product binaries. For more information on how to download the patch product binaries, see [Configure your patched product binaries](#).

- 2 Under the **Infra** details, select the required **vCenter**, **Cluster**, **Network**, **Datastore**, and **Disk Format** from the drop-down menus.
- 3 Select the **Applicable Time Sync** mode and click **Next**.
- 4 Under the **Network** details, if the environment is a newly created, then the text boxes are auto-populated. If the environment is imported, you have to manually enter the text boxes.
- 5 Click **Next**.

- 6 Select the **Applicable Time Sync Mode** and under the components section, select the node.

The advanced setting provides more information on configuring the selected node in a cluster. For an imported environment in which a product is scaled out, ensure that the provided certificate is primary node certificate.

- 7 On the Components tab, select **Take product snapshot** or **Retain product snapshot taken**. If the **Take product snapshot** is set to true, the snapshot is taken prior to starting scale-out, and can be rolled back to its initial state during a scale-out failure, the snapshot is taken with the prefix LCM_AUTOGENERATED. If the **Retain product snapshot taken** is set to true, it can be retained.

Note A snapshot rollback action is available for the failed scale-out request in the requests page.

- 8 Under **Component > Product properties**, select the required text boxes.

The field in this section varies for different products.

Product Name	Components
VMware Aria Automation	secondary
VMware Aria Operations	<ul style="list-style-type: none"> ■ Data ■ Cloud Proxy
VMware Aria Operations for Logs	VRLI-Worker
VMware Aria Operations for Networks	<ul style="list-style-type: none"> ■ vRNI-Platform ■ vRNI-Collector

- 9 Enter the required text boxes, click **Next**, and then click **Precheck**.
- 10 Review the summary and click **Submit**.

Scale out a tenant-enabled VMware Aria Automation environment

To scale out a multi-tenant VMware Aria Automation environment, use VMware Aria Suite Lifecycle.

Scaling out a tenant-enabled VMware Aria Automation from a single node to a three node cluster behind a load-balancer requires changes to its DNS and certificate requirements. Tenant enabled VMware Aria Automation can only be accessed through VMware Aria Automation tenant FQDNs. For more information on tenant FQDNs, see [Multi-tenancy model for VMware Aria Suite Lifecycle products](#).

After scaled-out, VMware Aria Automation tenants must be accessed through load-balancer tenant FQDNs and DNS, and certificates changes must be made accordingly. The same recommendations are shown in the VMware Aria Suite Lifecycle user interface as a pre-requisite to be performed before scaling out VMware Aria Automation 8.x.

Scale up VMware Aria Suite products

To scale up resource allocations such as RAM, disk capacity, and vCPUs in cluster nodes, use VMware Aria Suite Lifecycle.

The nodes of a single cluster are grouped. Each group consists of nodes of equal size. A product can have a single group or multiple groups. If the node sizes vary across the different groups, you can scale up to standardize the node sizes. Day 2 actions can include scaling operations to manage environments and avoid performance degradation. You can increase the storage capacity for a product by scaling up the current size and adding a disk with the required capacity.

The **Vertical Scale Up** option is supported for VMware Aria Operations for Logs, VMware Aria Automation, VMware Aria Operations for Networks, Workspace ONE Access, and VMware Aria Operations.

Prerequisites

Verify that you have an existing private cloud environment in VMware Aria Suite Lifecycle that contains supported VMware Aria Suite products.

Procedure

- 1 From the VMware Aria Suite Lifecycle dashboard, click **Manage Environments**.
- 2 Click **View Details** for either the global environment or a specific VMware Aria Suite product.
- 3 Click the ellipsis (...) for the product level operation, and then select **Vertical Scale Up**.
- 4 In the **Proceed to Vertical Scale Up** pop-up window, click **Trigger Inventory Sync**.
- 5 Click **Proceed** when the inventory sync is complete.
- 6 Select the **Node Type**, and then click **Next**.
- 7 Under **Vertical Scale-Up Details**, select **Scale Up Size** from the drop-down menu. You can select the **Additional Disk Size** (optional).
- 8 Under **Advanced Settings**, select the appropriate data store from the drop-down menus, and then click **Next**.
- 9 Click **RUN PRECHECK**.

Note If the validation is successful, a successful validation message appears. If you see an error message, follow the instructions provided in the **Recommendations** tab, and then click **RE-RUN PRECHECK**.

10 When the validation succeeds, click **Submit** to view the details of your request.

Note

- For Workspace ONE Access, the default deployment option and the VMware Aria Automation specified size of 8 CPU and 16 GB memory are supported. To increase the storage capacity, 70% can be assigned to `/db` and 30% to `/var` or `/opt`.
 - The `requiredCpuCount` and `requiredMemory` parameters are the overall CPU and memory parameters that are available for a node.
 - For VMware Aria Suite products, you provide the extra disk size to increase the capacity. The `requiredCapacity` parameter adds an extra disk to the available capacity. For VMware Aria Automation, you select the required disk for expansion and choose how much to expand the existing disk.
 - If you are installing VMware Aria Automation, ensure that you deploy Workspace ONE Access with the suggested size for VMware Aria Automation.
 - For Workspace ONE Access, you must be connected to the internet to perform the vertical scale up operation.
-

Export a private cloud environment configuration file

To export a private cloud environment configuration file for future environment deployments, use VMware Aria Suite Lifecycle.

For any data source added in a VMware Aria Operations for Networks environment, you can export its data source details in a config file. You can use the file to configure a new VMware Aria Operations for Networks environment with these same data sources.

Procedure

- 1 Click **Manage Environments**.
- 2 Click the ellipsis (...) for the environment and select **Export Configuration**.
- 3 Select the configuration file type to export from **Simple** or **Advance** section.
- 4 Click **Save File** and click **OK**.

The configuration file is downloaded to your browser's default download location.

What to do next

Use the configuration file to create new private cloud environments. See [Create a private cloud environment using a configuration file in VMware Aria Suite Lifecycle](#).

Download private cloud product logs

To download product log file bundles to share with VMware support, use VMware Aria Suite Lifecycle.

Procedure

- 1 Click **Manage Environments**.
- 2 Click the ellipsis (...) for the environment and select **Download Logs**.

Delete an environment

You can delete an existing environment from VMware Aria Suite Lifecycle. You cannot select and delete a specific product within an environment.

You can delete both successful and failed environment deployments. You can also delete initiated environments or environments that failed to deploy.

Note You can edit an existing environment that is in progress or that has failed to deploy by selecting any product under **Environments**, clicking the vertical ellipses for the product, and selecting **Edit Environment Details**. You can edit the environment name or the environment description. You cannot edit the environment name for a global environment.

You can use Workspace ONE Access to create an environment.

The following considerations exist when using Workspace ONE Access to delete an environment:

- VMware Aria Automation 8.x cannot be installed or imported.
- You cannot use Workspace ONE Access as an authentication source for VMware Aria Suite Lifecycle.
- You cannot access identity and tenant management. The user and active directory management become inaccessible. The existing roles and user mappings of Workspace ONE Access from VMware Aria Suite Lifecycle is removed.

Procedure

- 1 Click **Manage Environments** to delete a successfully installed environment, or delete a failed environment deployment listed under **Recent Requests**.
- 2 Click the three dots in the upper right corner of the environment tile and then select **Delete Environment**.
- 3 (Optional) Select **Delete related virtual machines from vCenter** to delete all virtual machines associated with this environment from vCenter.

If you do not select this option, all virtual machines associated with this environment remain in vCenter after the environment is deleted from VMware Aria Suite Lifecycle.

- 4 Select **Delete related virtual machines from vCenter** to delete virtual machines associated with the environment.

This option is available only if you have virtual machine associated with an environment in vCenter. If selected, virtual machines associated to the environment are also deleted from the vCenter. If it is not selected, records of this environment are only removed from VMware Aria Suite Lifecycle.

- 5 Click **DELETE**.
- 6 If you deleted virtual machines associate with the environment, verify that the list of virtual machines to delete is correct and then click **CONFIRM DELETE**.

IaaS virtual machine names do not appear in this list.

If the VM delete operation fails, an option is available to delete the environment from VMware Aria Suite Lifecycle. You can then delete the VMs manually from vCenter.

For a brownfield import, if you did not add a vCenter list, the delete environment confirmation dialog box does not show the VM list in vCenter and you must remove them manually.

- 7 Click **CLOSE**.

Results

The environment is removed from VMware Aria Suite Lifecycle.

What to do next

You can view the progress of the delete operation on the **Requests** page.

Managing VMware Aria Suite products in a private cloud

To upgrade and patch VMware Aria Suite products and download product logs, use VMware Aria Suite Lifecycle.

What to read next

- [Create and manage a product snapshot](#)
To create and manage a product snapshot and save the product state at a particular point in time, use VMware Aria Suite Lifecycle.
- [Inventory synchronization in VMware Aria Suite Lifecycle](#)
To initiate inventory synchronization and update the configuration of managed products, use VMware Aria Suite Lifecycle.
- [Product references for VMware Aria Suite Lifecycle](#)
Discover information about the products that are managed by VMware Aria Suite Lifecycle.
- [Change your password for products](#)
You can change the password for the installed VMware Aria Suite products by using VMware Aria Suite Lifecycle. Several types of password change options are available.
- [Delete a product from an environment](#)
You can delete a VMware Aria Suite product instance from a VMware Aria Suite Lifecycle environment.
- [Replace certificate for VMware Aria Suite Lifecycle products](#)
To replace existing product certificates, use VMware Aria Suite Lifecycle.

- [Configure and replace product licenses](#)

To configure and replace VMware Aria Suite product licenses, such as VMware Aria Automation licenses, use VMware Aria Suite Lifecycle

Create and manage a product snapshot

To create and manage a product snapshot and save the product state at a particular point in time, use VMware Aria Suite Lifecycle.

Managed snapshots are available for VMware Aria Suite Lifecycle. However, if you initiate a snapshot directly, outside of VMware Aria Suite Lifecycle, the snapshot is no longer managed in VMware Aria Suite Lifecycle.

Procedure

- 1 To create a snapshot, click **Manage Environments**.
- 2 Click **VIEW DETAILS**.
- 3 Click the ellipses icon next to the name of the product to snapshot and select **Create Snapshot**.
- 4 Under **Snapshot Details**, enter the **Snapshot Prefix** and the **Snapshot Description** details.
- 5 (optional) For certain VMware Aria Suite products, you can select the **Snapshot With Memory** toggle.
- 6 (optional) Select the **Shutdown before taking snapshot** toggle, as required.
- 7 Click **Next**.
- 8 Click **Run precheck** and then click **Finish**.

Note Day 2 operations that depend on vCenter, such as creating a snapshot, fail if the guest tools are not running or if the IP address or host name are not visible in vCenter. VMware Aria Operations configuration is not accessible after reverting a VMware Aria Operations snapshot. For more information, see KB article [56560](#).

- 9 To manage a product snapshot, click **Manage Environments**.
- 10 Click **VIEW DETAILS**.
- 11 Click the ellipses icon next to the name of the product to snapshot and select **Manage Snapshot**.

You can view the snapshot tree structure and the snapshot details.

- 12 (optional) Click **Delete** to permanently delete a snapshot.
- 13 (optional) Click **Revert** and then click **RUN PRECHECK** to revert a snapshot.

Results

Note

- The partial or inconsistent snapshot does not provide the revert option.
- You can rollback or revert a snapshot that you created during an upgrade or a scale-out in the Requests tab.
- When you deploy vRealize Suite products, a custom attribute is created on vCenter to support the snapshot inventory from VMware Aria Suite Lifecycle.

VMware Aria Suite Lifecycle saves state and configuration details for the product's virtual appliance. For more information, see KB article [56361](#).

What to do next

After you create a product snapshot, you can revert the product virtual appliance to the state of the snapshot.

Inventory synchronization in VMware Aria Suite Lifecycle

To initiate inventory synchronization and update the configuration of managed products, use VMware Aria Suite Lifecycle.

If you update managed product configurations outside of VMware Aria Suite Lifecycle, the products managed from VMware Aria Suite Lifecycle will be out of sync.

If any components of products are added or deleted outside of VMware Aria Suite Lifecycle, you can use inventory synchronization to update them.

If a product password is changed outside of VMware Aria Suite Lifecycle, it can be updated in VMware Aria Suite Lifecycle by synchronizing.

To change the root password of VMware Aria Operations, create a root password in the VMware Aria Suite Lifecycle locker and use the same to replace the VMware Aria Operations root password through VMware Aria Suite Lifecycle. You need not change the root password in the VMware Aria Operations.

If you change the password directly in the product, for example VMware Aria Operations, you can use VMware Aria Suite Lifecycle to synchronize the changed passwords with VMware Aria Suite Lifecycle.

You can synchronize your inventories for each product and for all the products across all environments.

- Instead of navigating to each product to synchronize inventories, click the horizontal ellipses on the product card and click **Trigger Inventory Sync**.
- If there are multiple environments, and multiple products within an environment, click **Trigger Inventory Sync** on the **Environment** page. This initiates the inventory sync on all the products in all environments.

- To initiate inventory synchronization for the product, click **View Details** and then click **Trigger Inventory Sync**.

Product references for VMware Aria Suite Lifecycle

Discover information about the products that are managed by VMware Aria Suite Lifecycle.

VMware Aria Suite Lifecycle product reference details are available on the **Product References** page. For example, if product A is integrated with product B, the **View Details** page of both product A and B contain an entry in the **Product References** table that reference one another.

If a product, for example VMware Aria Automation, is integrated with the global environment Workspace ONE Access and is using Workspace ONE Access as an authentication provider, then both VMware Aria Automation and the global environment Workspace ONE Access contain a reference to one another in their **View Details > Product References** table.

The product reference entries are created when you create an environment and during an inventory synchronization. If the expected product does not appear in the Workspace ONE Access global environment **Product Reference** table, then validate that the inventory synchronization for the related product is selected and is completed successfully.

For global environment Workspace ONE Access, the product references are used while performing following Day 2 operations:

- Certificate update or replace operations

A change in Workspace ONE Access certificate requires re-trust of Workspace ONE Access certificate on all products or services currently integrated with it. While updating a certificate, you can re-trust currently referenced products.

- Tenancy enablement operations

Once tenancy is enabled, Workspace ONE Access can be accessed only through tenant FQDNs. All the existing products or services currently integrated with Workspace ONE Access must go for a re-register of Workspace ONE Access against its primary tenant alias FQDN. While enabling tenancy, you can re-register currently referenced products.

The **Manage Environments** page in the VMware Aria Suite Lifecycle displays a complete inventory of each product.

The product references information is used in Day 2 operations to ensure that a life cycle operation performed on one product does not break the current integration with referenced products.

Change your password for products

You can change the password for the installed VMware Aria Suite products by using VMware Aria Suite Lifecycle. Several types of password change options are available.

To change a product password, open the product card environment and click **View Details > Change Password**.

The following password change options are available on the product details page:

Type of password change	Product name
Admin Password Change	<ul style="list-style-type: none"> ■ VMware Aria Automation ■ VMware Aria Operations ■ VMware Aria Operations for Networks ■ VMware Aria Operations for Logs ■ Workspace ONE Access
Root Password Change	<ul style="list-style-type: none"> ■ VMware Aria Automation ■ VMware Aria Operations ■ VMware Aria Operations for Logs ■ Workspace ONE Access
Support Password Change	VMware Aria Operations for Networks
Console User Password Change	VMware Aria Operations for Networks
SSH User Password Change	Workspace ONE Access

Delete a product from an environment

You can delete a VMware Aria Suite product instance from a VMware Aria Suite Lifecycle environment.

You can delete a product deployment from a vCenter. The VMware Aria Suite Lifecycle can delete product integration in a given environment for the selected product, if it is done within VMware Aria Suite Lifecycle while deploying products.

For an environment in which products are imported, VMware Aria Suite Lifecycle does not gather information about existing product integrations within products. Therefore, you can manually remove the product integration while deleting products.

Prerequisites

Verify that the product exists in your VMware Aria Suite Lifecycle environment.

Procedure

- 1 From the **Environment** page, select a product instance and right-click on the vertical ellipses.
- 2 Click **Delete Product**.

Note When there are products that are internally integrated within a product, then verify the integrations before deleting the product. However, VMware Aria Suite Lifecycle cannot remove the external integrations in the products.

- 3 To delete all associated VMs from vCenter for the selected product, select the **Delete associated VMs** check box.

- 4 To delete Windows machines, select **Delete associated Windows Machines** check box and click **Delete**.

Before you delete associated VMs from vCenter on the **Delete Product** window, review the list of VMs and then click **Confirm Delete**.

Results

The selected VMware Aria Suite product and its associated VMs from an environment are deleted.

Replace certificate for VMware Aria Suite Lifecycle products

To replace existing product certificates, use VMware Aria Suite Lifecycle.

If the product is SSL terminated, you must manually replace the certificate and CA in the load balancer first. The VMware Identity Manager requires this step.

For information about replacing a VMware Aria Suite Lifecycle VAMI/VA certificate, see [Replace your VMware Aria Suite Lifecycle custom certificate](#).

For information about replacing your VMware Identity Manager certificate, see [Replace your Workspace ONE Access certificate by using VMware Aria Suite Lifecycle](#). Note that the VMware Identity Manager and Workspace ONE Access terms are used interchangeably in VMware Aria Suite Lifecycle product documentation.

For information about identity manager trust certificates, see [Day 2 operations with other products in VMware Aria Suite Lifecycle](#).

Prerequisites

Verify that your product has an existing certificate. You can either create or import a certificate in the VMware Aria Suite Lifecycle locker. For information about creating certificates, see [Manage certificates for VMware Aria Suite Lifecycle products](#).

Procedure

- 1 From the **Environment** page, select a product and click on the vertical ellipses.
- 2 Click **Replace Certificate**.
- 3 From the **Current Certificate**, click **Next**.
- 4 Select a certificate from the drop-down menu and click **Next**.
- 5 Review the certificate summary and click **Next**.
- 6 Select the product instance and click **Next**.

To replace a Workspace ONE Access certificate, you must re-trust the configured products.

By default, all the products are listed in the **Re-Trust Product Certificate** wizard.

- 7 (Optional) Select the **Opt-in for Snapshot** check box.

Note This options allows you to take snapshots for products that do not have a built-in certificate rollback capability. You can use this option to revert the snapshot in case of a failure to replace a certificate. The option is only applicable for Workspace ONE Access and VMware Aria Operations for Networks.

If the replace certificate request fails, you can revert to the snapshot and re-submit the failed request to rollback the operation.

- 8 To validate the certificate information, click **RUN PRECHECK** and click **Finish**.
- 9 Click **Accept** and **Submit**.

Configure and replace product licenses

To configure and replace VMware Aria Suite product licenses, such as VMware Aria Automation licenses, use VMware Aria Suite Lifecycle

Prerequisites

- Verify that you have the VMware Aria Automation instance in VMware Aria Suite Lifecycle.
- Ensure that you have added a license in the VMware Aria Suite Lifecycle locker. For information about adding licenses, see [Manage licenses for a VMware Aria Suite Lifecycle products](#).

Procedure

- 1 Log in to VMware Aria Suite Lifecycle.
- 2 Select the **Environments** tab and then click **View Details** for a VMware Aria Suite product card.
- 3 Select the product options (...) icon and then click **Add License** from the drop-down list. You can view the list of current licenses.
- 4 Click **Next**.
- 5 Select a new license from the drop-down list and then verify the license details.
- 6 (Optional) In VMware Aria Automation, VMware Aria Operations, and VMware Aria Operations for Logs, you can delete the older licenses after selecting a new license. Select the licenses to be removed under **Terminate Licenses**.
- 7 Click **Finish**.

You can view license requests in VMware Aria Suite Lifecycle **Requests** tab.

What to do next

For more information on configuring the license, see [Manage licenses for a VMware Aria Suite Lifecycle products](#).

Configure health monitoring for the VMware Aria Suite management stack in VMware Aria Suite Lifecycle

To display the health status of VMware Aria Suite products when VMware Aria Operations is part of your environment, use VMware Aria Suite Lifecycle.

Health status information in VMware Aria Suite Lifecycle is available only for VMware Aria Suite Lifecycle supported products, which include VMware Aria Automation, VMware Aria Operations, and VMware Aria Operations for Logs.

Prerequisites

To display health status information for your environment, verify that VMware Aria Operations exists in the same environment as other VMware Aria Suite products. For related information, see [Add a product to an existing private cloud environment](#) . For information about creating an environment, see [Chapter 3 Creating a VMware Identity Manager environment in VMware Aria Suite Lifecycle](#).

- [Monitoring content health status in VMware Aria Suite Lifecycle](#)

You can use VMware Aria Suite Lifecycle to display private cloud environment health for individual products and for the overall environment.

- [View the SDDC Health Overview dashboard in VMware Aria Operations](#)

To view detailed health status information in VMware Aria Operations, use options in VMware Aria Suite Lifecycle.

- [Activate or deactivate product health checkin in VMware Aria Suite Lifecycle](#)

Procedure

- 1 Install the SDDC management pack in VMware Aria Operations. You can install the SDDC management pack from the Marketplace page in VMware Aria Suite Lifecycle or outside of VMware Aria Suite Lifecycle.
- 2 Configure adapter instances for VMware Aria Operations for Logs and VMware Aria Automation in VMware Aria Operations.
- 3 Verify that the VMware Aria Operations SDDC health overview dashboard displays the health status for VMware Aria Operations and other VMware Aria Suite products.
- 4 After the health status appears in the SDDC health overview dashboard, VMware Aria Suite Lifecycle runs the scheduled health status.

Results

VMware Aria Suite Lifecycle displays the health status of the SDDC management pack, and retrieves the health status information from one instance of VMware Aria Operations in a given private cloud environment.

The health status applies only to the VMware Aria Suite products configured in the target VMware Aria Operations instance within the private cloud environment. Do not configure additional VMware Aria Suite products from other private cloud environments in the same instance of VMware Aria Operations.

Monitoring content health status in VMware Aria Suite Lifecycle

You can use VMware Aria Suite Lifecycle to display private cloud environment health for individual products and for the overall environment.

Health status by color

To activate or deactivate health at the environment level, click the vertical ellipses on the environment page. The following table presents a color-coded guide to help you determine the health status of your private cloud environment.

Color	Status
Gray	<p>A gray status indicates one of the following scenarios:</p> <ul style="list-style-type: none"> ■ VMware Aria Operations is not part of your private cloud environment. ■ VMware Aria Operations is not configured for the SDDC management health solution management pack. ■ An error occurred while determining private cloud environment health. ■ Health information is not yet available.
Green	VMware Aria Operations is reporting health as green, based on its policies, for all configured products.
Yellow	VMware Aria Operations is reporting health as yellow, based on its policies, for at least one configured product.
Red	VMware Aria Operations is reporting health as orange or red, based on its policies, for at least one configured product.

Health status in VMware Aria Suite Lifecycle continues to display these colors, even when you only partially configure VMware Aria Suite products in VMware Aria Operations. VMware Aria Suite Lifecycle does not attempt to determine health status of VMware Aria Suite products that are not configured in the private cloud environment.

View the SDDC Health Overview dashboard in VMware Aria Operations

To view detailed health status information in VMware Aria Operations, use options in VMware Aria Suite Lifecycle.

Prerequisites

Verify that you have valid VMware Aria Operations credentials and access to VMware Workspace ONE Access.

Procedure

- 1 In VMware Aria Suite Lifecycle, click the health status for the private cloud environment to open the SDDC Health Overview Dashboard for the environment in VMware Aria Operations.
- 2 In VMware Aria Suite Lifecycle, click the health status for an individual product to open the summary page for that product in VMware Aria Operations.

Activate or deactivate product health checkin in VMware Aria Suite Lifecycle

You can activate the health check option to check the health of an existing environment. You can use this option to evaluate VMware Aria Suite Lifecycle environments when VMware Aria Operations for Integrations is installed with an SDDC management pack. This health check is only available for the VMware Aria Operations instance that contains a SDDC management pack to monitor the health of the entire system.

The product health check option first checks if for a supported environment to run at first place. After the health checks run, it checks if there is an SDDC management health solution available. It then verifies the last status of the health solution. A health check runs periodically on a scheduled interval. When you want to avoid resource usage in particular environments, such as development environments or production environments, deactivate the health check option for those environments.

After the health check is deactivated, environment health is no longer evaluated. When a health check has run, you can view the current status of the environment.

Adding and managing content from Marketplace

You can use VMware Aria Suite Lifecycle to add and manage content from VMware Marketplace.

The [VMware Marketplace](#) contains content plug-ins for VMware Aria Automation Orchestrator, including VMware Aria Automation cloud templates and OVAs, VMware Aria Operations management packs, and VMware Aria Operations for Logs content packs. You can download these and then deploy them in your VMware Aria Suite environments.

Find and download content from VMware Marketplace

You can use VMware Aria Suite Lifecycle to search for and download content from VMware Marketplace.

VMware Aria Suite Lifecycle supports VMware Aria Automation OVA installation. If you expect to download multiple OVAs, consider increasing the `data` folder size as the OVAs have large file sizes.

Prerequisites

Verify that you have performed an initial Marketplace sync to load [VMware Marketplace](#) content.

Procedure

- 1 Click **VMware Marketplace** and click the **All** tab.
If the tab is not available, open the [VMware Marketplace](#) web page.
- 2 (Optional) To filter the list of available content by search terms, enter search terms in the **Search** text box.
- 3 (Optional) To filter the list of available content by product, publisher, or technology, click **Filter** and select the appropriate filters.
- 4 Click **View Details** to learn more about the downloadable content, including content compatibility.
- 5 Click **Download** to download the content to VMware Aria Suite Lifecycle.

Results

Downloaded content appears on the **Download** tab of the **Marketplace** page.

What to do next

Install the content you downloaded.

View and upgrade your Marketplace content

To view information about content that you have previously downloaded from VMware Marketplace, use VMware Aria Suite Lifecycle.

Procedure

- 1 Click **Marketplace** and click the **Available** tab.
VMware Aria Suite Lifecycle displays all content downloaded to VMware Aria Suite Lifecycle from [VMware Marketplace](#).
- 2 If there is an update available, you can download a newer version of the content.
 - a Highlight the notification icon on the content tile to verify that there is an available update.
If there are no notifications for the content, the notification icon does not appear.
If newer version of the content is available, VMware Aria Suite Lifecycle displays the message `New version updates are available for the app`.
 - b Click the three dots on the upper right corner of the content tile, and select **Upgrade**.
 - c To download, select a version and click **Continue**.

If you are upgrading a VMware Aria Automation cloud template, VMware Aria Automation Orchestrator plug-in, VMware Aria Operations for Logs content pack, or a VMware Aria Operations management pack with a newer version, the new version content overwrites the old version content.

- 3 Click **View Details** to view information about the content, including related content and the date the content was last modified.

Install a downloaded Marketplace content

You can use VMware Aria Suite Lifecycle to install content that you have downloaded from VMware Marketplace.

Prerequisites

- Download the desired content from [VMware Marketplace](#). See [Find and Download Content from Marketplace](#).
- Verify that the entitlements in your environment match the entitlements of the content that you want to install.

Procedure

- 1 Click **Marketplace** and click the **Available** tab.
If the **Marketplace** tab is not present, open the [VMware Marketplace](#) site.
- 2 Locate the content to install and click **Install**.
- 3 Select the data center and environment in which to install the content and click **Next**.
VMware Aria Automation and VMware Aria Operations for Integrations content is tagged with license entitlements.
- 4 After selecting a data center and environment, select the tenant in which to install the content and click **Submit**.

What to do next

You can track installation progress on the **Requests** page.

Delete content downloaded from VMware Marketplace

You can use VMware Aria Suite Lifecycle to delete content that you downloaded from VMware Marketplace.

The delete action does not remove content from environments where the content was installed by using VMware Aria Suite Lifecycle.

Procedure

- 1 Click **Marketplace** and click the **Download** tab.
- 2 Click the vertical dots in the upper right corner of the tile for to delete and click **Delete**.
- 3 Click **Yes**.

Results

The content is deleted from VMware Aria Suite Lifecycle and no longer appears under downloaded content on the **Marketplace** page.

Working with Content Management in VMware Aria Suite Lifecycle

5

The Content Management service in VMware Aria Suite Lifecycle provides a way for release managers and content developers to manage their software-defined data center (SDDC). It includes content capturing, testing, and release to various environments, and source control capabilities through different source control endpoints that include GitHub, GitLab, and Bitbucket.

Migration of content or versions is not supported from an older instance to VMware Aria Suite Lifecycle. The latest content version can be either source controlled or deployed to an end point before moving to VMware Aria Suite Lifecycle.

Content developers cannot set a release policy on endpoints. Only release managers can set policies.

The following endpoint migrations and content settings are captured and supported:

- All the endpoints are migrated along with source control user tokens.
- Tags associated with the endpoints are migrated to new instance.
- Pipeline stub configurations are migrated.

Note When a cloud admin is granted a role of release manager or content developer, the cloud admin can only view the content management app inside the VMware Aria Suite Lifecycle. The cloud admin does not have permission to view other applications. A release manager and a content developer can view the content management app. As a workaround, you can perform all the cloud admin operations using the cloud admin role only and not provide additional permissions or role mapping.

You can use content life cycle management to replace the manual processes for managing the software-defined content. Supported content includes the following entities.

Product Name	Supported Version
VMware Aria Automation	all versions
VMware Aria Automation Orchestrator	all versions
VMware vSphere	all versions

Product Name	Supported Version
VMware Aria Operations	all versions
Source control servers	<ul style="list-style-type: none"> ■ GitHub Enterprise Server: 2.20.15, 2.19.21, 2.21.6, 3.0, and 3.10.2 ■ GitLab: 12.2.12 (Enterprise Edition), 12.7, 12..8, and 15.11,13 (Enterprise Edition) ■ GitHub Cloud ■ Bitbucket Server 6.10, 7.0, and 8.12 ■ Bitbucket Cloud: Version 2.0 ■ Microsoft Azure DevOps GIT <p>Note VMware has tested the versions listed. Unlisted intermediate versions should also be supported.</p>

Content life cycle management is one of the VMware Aria Suite Lifecycle services. It includes the capability to manage content and work with source control to support a multi-developer use case.

If there are dependencies between captured content packages, all the dependencies are captured as first class objects in VMware Aria Suite Lifecycle. Each content version shows all its dependencies associated with it. For example, if a VMware Aria Automation cloud template has a dependency on a property definition, there are two items in the content catalog, one for each content package. With independent version control for each content package, you can edit, capture, and release dependencies independently so that the content is never old. VMware Aria Automation allows you to define multiple named value sets within the size and image component profile types. You can add one or more of the value sets to machine components in a blueprint. You cannot deploy or release automation-component profiles in VMware Aria Suite Lifecycle to a target end point if the corresponding value set already exists on the end point.

- [Working with content endpoints in VMware Aria Suite Lifecycle](#)

A content endpoint is an infrastructure endpoint in the software-defined data center (SDDC), for example an instance of VMware Aria Automation, that is targeted for the capture, test, and release of managed content.

- [Managing VMware Aria Suite Lifecycle content](#)

Content is a collection of files that contain definitions that represent software defined services.

- [Access source control](#)

A VMware Aria Suite Lifecycle release manager can add a source control access.

- [Managing source control server endpoints](#)

Before you can check in or check out content, a VMware Aria Suite Lifecycle must add a GitLab or Bitbucket source control server to the system.

- [Working with content settings in VMware Aria Suite Lifecycle](#)

You can add source control server endpoint, vCenter publisher, pipeline extensibility and developer restrictions in content settings.

- [Content pipelines](#)

You can use VMware Aria Suite Lifecycle to display the content capture, test, and release status of content pipelines. You can view all content pipelines that are completed, in progress, or in failed state.

Working with content endpoints in VMware Aria Suite Lifecycle

A content endpoint is an infrastructure endpoint in the software-defined data center (SDDC), for example an instance of VMware Aria Automation, that is targeted for the capture, test, and release of managed content.

You add a content endpoint to an environment to capture, test, deploy or check-in software-defined content in the form of a content package. A content package is a file that contains definitions for software-defined services, such as cloud templates, workflows, and so on. Each content endpoint can support more than one type of content package.

You use content endpoints in VMware Aria Suite Lifecycle to perform the following actions:

- Capture one or more content packages.
- Test one or more content packages in a staging environment.
- Release one or more tested content packages to a production environment.

Content life cycle management provides the following policies for VMware Aria Automation Orchestrator, VMware Aria Automation, vCenter, and VMware Aria Operations content endpoints.

Table 5-1. Policies for VMware Aria Suite products

Policy	Description
Allow content to be captured from this endpoint	Allows you to capture content from this endpoint.
Allow unit tests to be run on this endpoint	Allows you to release content for the endpoint and run test workflows against the endpoint. A VMware Aria Automation Orchestrator marked as test endpoint also acts as unit test server.
Allow releasing content packages to this endpoint	Allows you to release content for the endpoint.
Source controlled content only	Allows you to release only source controlled content to the endpoint.

Table 5-1. Policies for VMware Aria Suite products (continued)

Policy	Description
Enable code review	This policy applies only to the source control endpoints. Allows a manual review for the developers. VMware Aria Suite Lifecycle content life cycle management creates a branch with changes that require a code review. A code reviewer accepts or rejects the merge request into the branch of the respective source control.
Enable vCenter template support	Requests you for information required for deploying templates. This option is available only when you mark a vCenter server as a production endpoint.

What to read next

- [Add a VMware Aria Automation Orchestrator content endpoint in VMware Aria Suite Lifecycle](#)

To add a VMware Aria Automation Orchestrator, use the Content Management service in VMware Aria Suite Lifecycle.
- [Add a VMware Aria Automation content endpoint in VMware Aria Suite Lifecycle](#)

You can add capture, test, deploy, or check in a content package by using the Content Management service in VMware Aria Suite Lifecycle to add a VMware Aria Automation content endpoint.
- [Add a VMware Aria Automation cloud endpoint in VMware Aria Suite Lifecycle](#)

To add a VMware Aria Automation cloud endpoint to an environment, use the Content Settings service in VMware Aria Suite Lifecycle.
- [Add a source control endpoint in VMware Aria Suite Lifecycle](#)

A source control endpoint represents a project repository and a source control server. You can add a source control endpoint by using the Content Management service in VMware Aria Suite Lifecycle.
- [Add a vCenter content endpoint in VMware Aria Suite Lifecycle](#)

To add a vCenter content endpoint to an environment to capture, test, deploy, or check in a content package, use the Content Management service in VMware Aria Suite Lifecycle.
- [Add a VMware Aria Operations endpoint in VMware Aria Suite Lifecycle](#)

To add a VMware Aria Operations content endpoint to capture, test, deploy, or check in a content package, use the Content Management service in VMware Aria Suite Lifecycle.
- [Delete a content endpoint in VMware Aria Suite Lifecycle](#)

You can delete an existing content endpoint by using the Content Management service in VMware Aria Suite Lifecycle.

- [Edit a content endpoint in VMware Aria Suite Lifecycle](#)

You can edit the settings of an existing content endpoint by using the Content Management service in VMware Aria Suite Lifecycle.

Add a VMware Aria Automation Orchestrator content endpoint in VMware Aria Suite Lifecycle

To add a VMware Aria Automation Orchestrator, use the Content Management service in VMware Aria Suite Lifecycle.

A VMware Aria Automation Orchestrator endpoint is required to create VMware Aria Automation endpoints and to capture content.

Prerequisites

If you are using a VMware Aria Automation Orchestrator endpoint for unit testing, verify that the VMware Aria Automation Orchestrator instance has been configured as a unit test server.

Procedure

- 1 On the **My Services** dashboard, click **Content Management**.
- 2 Under **Endpoints**, click **NEW ENDPOINT**.
- 3 Click **VMware Aria Automation Orchestrator**.

For **VMware Aria Automation Orchestrator** content, you can capture workflows, configuration elements, and actions individually or in the folder in which they reside.

Note If a folder is captured, a temporary folder content name is displayed. You can start a content pipeline to capture all content. Add the pipeline to the VMware Aria Automation Orchestrator package as input.

- 4 Enter the information for the VMware Aria Automation Orchestrator content endpoint.
 - a In the **Name** text box, enter a unique name for the endpoint.
 - b In the **Tags** text box, enter tags associated with the endpoint.

Using tags allow you to deploy content to multiple endpoints at the same time. When you deploy content, you can select a tag instead of individual content endpoint names, and the content deploys to all endpoints that have that tag.

To add multiple tags, press **Enter** after you enter each tag.

- c In the **Server FQDN/IP** field, enter the fully qualified server name, IP address, or host name for the content endpoint server.

If the VMware Aria Automation Orchestrator instance is not embedded in VMware Aria Automation, include the port number in the server FQDN/IP. For VMware Aria Automation Orchestrator, the port is not required.

vRO-Server-FQDN:Port

- d Enter a user name and password to use to access this content endpoint.

- 5 Press **TEST CONNECTION** to test the connection to the content endpoint.

If the connection test fails, verify that the information you entered for the content endpoint is correct and try again.

- 6 Select **vRO Package**.

The VMware Aria Automation Orchestrator package can be captured from an endpoint and is associated with the content endpoint. Mark the version as Production ready. Selection of a VMware Aria Automation Orchestrator package is a post deployment capability that imports the package once any other content has been deployed allowing maintained localized or regional settings.

- Ignore modules when listing content: A comma-separated list of VMware Aria Automation Orchestrator Actions or modules that are excluded when listing from an endpoint to reduce the number. With VMware Aria Suite Lifecycle, any module or folder with or without any dependencies can be excluded while capturing or listing the content. However, for VMware Aria Automation Orchestrator-packages these modules or folders are not ignored. VMware Aria Suite Lifecycle validates the content dependencies available in the source endpoint while capturing with dependencies. This depends on the policy specified on the endpoints.
- Ignore Workflows in these folders: A comma-separated list of VMware Aria Automation Orchestrator workflow folders that are excluded when listing from an endpoint to reduce the number.
- A VMware Aria Automation Orchestrator package name cannot contain special characters and can cause issues when you capture, release or check-in a content. If you have a VMware Aria Automation Orchestrator package name with a space in between the name, then the space is converted to an underscore (_) during a capture and fails during a test and deploy.

- 7 Select the appropriate policies for the content endpoint, and click **Next**. For more information on policies, refer to the policy table provided in [Working with content endpoints in VMware Aria Suite Lifecycle](#).
- 8 Verify that the content endpoint details are correct, and click **Submit**.

Add a VMware Aria Automation content endpoint in VMware Aria Suite Lifecycle

You can add capture, test, deploy, or check in a content package by using the Content Management service in VMware Aria Suite Lifecycle to add a VMware Aria Automation content endpoint.

Prerequisites

Verify that you have added at least one VMware Aria Automation endpoint.

Note If the VMware Aria Automation Orchestrator is embedded, there is no separate instance of VMware Aria Automation Orchestrator endpoint. VMware Aria Automation Orchestrator endpoint creation is required only if you are using an external VMware Aria Automation Orchestrator endpoint for VMware Aria Automation.

Procedure

- 1 On the **My Services** dashboard, click **Content Management**.
- 2 Under **Endpoints**, click **NEW ENDPOINT**
- 3 Click **Automation**.
- 4 Enter the information for the VMware Aria Automation content endpoint.
 - a In the **Name** field, enter a unique name for the endpoint.
 - b Select the product version of the endpoint from the **Endpoint Version** drop-down menu.
 - c In the **Tags** field, enter tags associated with the endpoint.

With tags, you can deploy content to multiple endpoints at the same time. When you deploy content, you can select a tag instead of individual content endpoint names, and the content deploys to all endpoints that have that tag.

To add multiple tags, press **Enter** after you enter each tag.

- d In the **Server FQDN/IP** field, enter the fully qualified server name, IP address, or host name for the content endpoint server.

When adding an endpoint for a particular tenant, tenant based FQDN must be used as a server. For a system-based domain, use the user FQDN without a tenant.

IP addresses are not supported for adding VMware Aria Automation 8.x endpoints.

- e Enter a tenant name, user name, and password to access the content endpoint.
- f Select an external or embedded VMware Aria Automation Orchestrator endpoint to associate from the **vRO Server Endpoint** drop-down menu.

When selecting a user account for exporting or importing content into VMware Aria Suite Lifecycle, ensure that the account has all roles. The **Secure Export Consumer** role allows VMware Aria Suite Lifecycle to export passwords. Exported passwords can be imported into other VMware Aria Automation endpoints.

- 5 Press **TEST CONNECTION** to test the connection to the content endpoint.

If the connection test fails, verify that the information you entered for the content endpoint is correct and try again.

- 6 Click **Next**.

- 7 Select the appropriate policies for the content endpoint and click **Next**.

For more information about policies, see [Working with content endpoints in VMware Aria Suite Lifecycle](#).

- 8 Verify that the content endpoint details are correct and click **Submit**.

Add a VMware Aria Automation cloud endpoint in VMware Aria Suite Lifecycle

To add a VMware Aria Automation cloud endpoint to an environment, use the Content Settings service in VMware Aria Suite Lifecycle.

- 1 On the **My Services** dashboard, click **Content Management**.

- 2 Under **Endpoints**, click **NEW ENDPOINT**.

- 3 Select the VMware Aria Automation cloud endpoint option.

- 4 Enter the endpoint details for the VMware Aria Automation cloud endpoint.

- a In the **Name** field, enter a unique name for the endpoint.

- b In the **Tags** field, enter tags associated with the endpoint.

You can use tags to deploy content to multiple endpoints at the same time. When you deploy content, you can select a tag instead of individual content endpoint names. The content deploys all endpoints that have the selected tag.

- c Enter the refresh token value.

- d For the VMware Aria Automation Orchestrator server endpoint, click **External VMware Aria Orchestrator** or **VMware Aria Automation Cloud Extensibility appliance**.

- e To associate a VMware Aria Automation Orchestrator, select a VMware Aria Automation Orchestrator endpoint from the drop-down menu.

- 5 To test the connection to the content endpoint, click **TEST CONNECTION**.

If the test fails, verify that the information you entered for the content endpoint is correct and then retry.

- 6 Click **Next**.

- 7 Under **Policy Settings**, select the appropriate VMware Aria Automation Orchestrator package policy for the content endpoint and then click **Next**.

For more information about policies, see [Working with content endpoints in VMware Aria Suite Lifecycle](#).

- 8 Verify that the content endpoint details are correct and then click **Submit**.

Prerequisites

- Create an external VMware Aria Automation Orchestrator endpoint for VMware Aria Automation.
- Generate an API refresh token. For information about generating API tokens, see [How do I generate API tokens](#) in [VMware Cloud services](#) product documentation. .

Add a source control endpoint in VMware Aria Suite Lifecycle

A source control endpoint represents a project repository and a source control server. You can add a source control endpoint by using the Content Management service in VMware Aria Suite Lifecycle.

You can have any number of source control repositories and branches added to VMware Aria Suite Lifecycle. Adding a source control branch allows you to check in and check out the SDDC content.

Prerequisites

- Verify that a VMware Aria Suite Lifecycle administrator has added a system source control server in the **Content Settings** section.
- Verify that a developer has entered the GitLab access token to the source control server to support content check-in and check-out operations.

Procedure

- 1 On the **My Services** dashboard, click **Content Management**.
- 2 Under **Endpoints**, click **NEW ENDPOINT**.
- 3 Click **Source Control**.
- 4 Select the configured **Source Control Server** (Bitbucket Server, Bitbucket cloud, GitLab, GitHub, or Azure DevOps GIT).
- 5 Enter the information for the source control content endpoint.
 - a In the **Name** text box, enter a unique name for the endpoint.
 - b Enter a **Tag** name.
 - c Enter a **Branch** and **Repository Name** value for the content endpoint in the following format:
 - For GitLab, enter *group_name/repository_name*.
 - For Bitbucket server, enter *project_name/repository_name*.
 - For Bitbucket cloud, enter *repository_name* if you are using a primary workspace or enter *workspace_name/repository_name* if you are using multiple workspaces.
 - For Azure DevOps GIT, enter *organization_name/project_name/repository_name*.

- 6 Click **Test Connection** and then click **Next**.
- 7 Select the appropriate policies for this content endpoint and then click **Next**.

You can optionally select **Enable code review** to allow a manual review between developers. VMware Aria Suite Lifecycle content life cycle management creates a branch that contains the changes that require code review. A code reviewer can accept or reject the merge request into the branch.

- 8 Verify that the content endpoint details are correct and then click **Submit**.

Add a vCenter content endpoint in VMware Aria Suite Lifecycle

To add a vCenter content endpoint to an environment to capture, test, deploy, or check in a content package, use the Content Management service in VMware Aria Suite Lifecycle.

Prerequisites

Verify that you have added at least one vCenter endpoint in the **Content Settings > vSphere Template Repository** .

Procedure

- 1 On the **My Services** dashboard, click **Content Management**.
- 2 Under **Endpoints**, click **NEW ENDPOINT**
- 3 Click **vCenter**.
- 4 Enter the information for the vCenter content endpoint.
 - a In the **Name** field, enter a unique name for the endpoint.
 - b In the **Tags** field, enter tags associated with the endpoint.

Using tags allow you to deploy a content to multiple endpoints at the same time. When you deploy a content, you can select a tag instead of individual content endpoint names, and the content deploys to all endpoints that have that tag.
- 5 In the **Server FQDN/IP** text box, enter the fully qualified server name, IP address, or host name for the content endpoint server.
- 6 To access the endpoint, enter the **User name** and **Password** values.
- 7 Click **Test Connection** and then click **Next**.
- 8 Select the appropriate policies for the content endpoint.

For more information about policies, see [Working with content endpoints in VMware Aria Suite Lifecycle](#).
- 9 Click **Next** and provide the vCenter details.
- 10 Click **Next**.

- 11 To import an existing data center, click **Import LCM Data center**.

After data collection is complete, you can add vCenter settings to VMware Aria Suite Lifecycle. The virtual machine folder path (/Templates/MyTemplates/) is not imported.

When the endpoint is created, it validates that the configuration of the local subscriber details point to the publisher as defined in `Content Settings/vSphere Template Repository` setting. If there is a problem, the endpoint is deactivated and an error is displayed.

Add a VMware Aria Operations endpoint in VMware Aria Suite Lifecycle

To add a VMware Aria Operations content endpoint to capture, test, deploy, or check in a content package, use the Content Management service in VMware Aria Suite Lifecycle.

Prerequisites

- Verify that the SSH user account is configured.
- Verify that all VMware Aria Operations instances contain the same installed management packs. Also verify that the required adapter instances are properly configured.
- Do not use dashboards that refer to vCenter VM, host or datastore objects on the release endpoint until you update the reference to a specific object.

Procedure

- 1 On the **My Services** dashboard, click **Content Management**.
- 2 Under **Endpoints**, click **NEW ENDPOINT**.
- 3 Click **VMware Aria Operations**.
- 4 Enter the information for the VMware Aria Operations content endpoint.
 - a In the **Name** field, enter a unique name for the endpoint.
 - b Enter a tag name.
 - c Enter the **Server FQDN/IP** address.
 - d Enter the **Username** and **Password** values.
 - e Enter the **SSH Username** and **SSH Password** values.
 - f Click **Test Connection**. When the connection is established, click **Next**.

For more information about creating an SSH user on the VMware Aria Operations instance, see [Create an SSH user in VMware Aria Operations](#).

- 5 Under **Policy Settings**, select options to capture, test, or mark as production.

For more information about policies, see [Working with content endpoints in VMware Aria Suite Lifecycle](#).
- 6 Verify that the content endpoint details are correct and then click **Submit**.

Create an SSH user in VMware Aria Operations

You can create a VMware Aria Operations endpoint in a VMware Aria Suite Lifecycle content management endpoint.

- 1 When you select `root` as an SSH user from the content endpoint, create a user on the VMware Aria Operations appliance. The user must have SSH access, belong to the user group `root`, and have a valid home directory.
- 2 Log in to the VMware Aria Operations appliance as a `root` user and create a user on the VMware Aria Operations appliance by using the following command. .

```
useradd sshuser
```

- 3 Configure user groups for the created user with `usermod -G root,wheel sshuser` settings.
- 4 Configure the correct home directory for the user by using the following commands:

```
mkdir /home/sshuser"
"chown sshuser /home/sshuser"
```

- 5 Set the password to `passwd sshuser`.
- 6 Enable the password with `sudo` capabilities by using the following commands:

```
Run command visudo

sshuser ALL = NOPASSWD: /usr/lib/vmware-vcopssuite/python/bin/python /usr/lib/vmware-vcops/
tools/opscli/ops-cli.py *
sshuser ALL = NOPASSWD: /bin/rm -rf /tmp/*
sshuser ALL = NOPASSWD: /bin/mv /tmp/*
```

Note You can use the VMware Aria Operations CLI (OPS-CLI) to export or import the content capture or release information in VMware Aria Suite Lifecycle.

Delete a content endpoint in VMware Aria Suite Lifecycle

You can delete an existing content endpoint by using the Content Management service in VMware Aria Suite Lifecycle.

Procedure

- 1 On the **My Services** dashboard, click **Content Management**.
- 2 Under **Endpoints**, click the vertical ellipses to the left of the endpoint and then click **Delete**.
You must manually delete the endpoint.
- 3 Click **OK**.

Edit a content endpoint in VMware Aria Suite Lifecycle

You can edit the settings of an existing content endpoint by using the Content Management service in VMware Aria Suite Lifecycle.

You can edit content endpoint values other than the name, which is used by various logs.

Note When VMware Aria Suite Lifecycle deploys a VMware Aria Automation instance or a VMware Aria Automation instance is imported into VMware Aria Suite Lifecycle, the content management services import content endpoints automatically through a data collection process. Because all policies are deactivated, you must edit each endpoint and assign appropriate content policies. Only certain user roles can edit content endpoints. For more information on roles, see [Content actions](#).

Procedure

- 1 On the **My Services** dashboard, click **Content Management**.
- 2 Under **Endpoints**, click the vertical ellipses to the left of the endpoint and then click **Edit**.
- 3 Edit the endpoint details you want to change and click **Next**.
- 4 Edit the endpoint policy settings you want to change and click **Next**.
- 5 Verify that the content endpoint details are correct and click **Submit**.

Managing VMware Aria Suite Lifecycle content

Content is a collection of files that contain definitions that represent software defined services.

After you add a content endpoint to one or more environments, you can manage the software-defined content that each environment contains. Use VMware Aria Suite Lifecycle to perform the following content operations:

- Capture content from an endpoint.
- Deploy to test and run unit tests.
- Check in content.
- Release content to production.

Content examples include a YAML file for a VMware Aria Automation cloud template or an XML file for a VMware Aria Automation Orchestrator workflow. Content is linked. For example, when you capture a VMware Aria Automation cloud template, all its dependencies are displayed in the content catalog. VMware Aria Suite Lifecycle displays dependency information within each content version.

The / character cannot be used in a name value or export fails.

What to read next

- [Add content](#)
You can use VMware Aria Suite Lifecycle to add content from an existing content endpoint.
- [Delete multiple content names or versions](#)
You can delete multiple content items and content versions in VMware Aria Suite Lifecycle. You can delete all the versions related to the selected content item.

- [Working with captured content](#)

You can use VMware Aria Suite Lifecycle to capture a new version of an existing content package.

- [Content actions](#)

After you capture content in VMware Aria Suite Lifecycle, you can perform and view content actions.

- [Available content types](#)

VMware Aria Suite Lifecycle supports the following content packages for each available endpoint type.

- [Searching content](#)

You can search an existing content based on certain defined entries within the UI.

- [Test Content](#)

You can test content to ensure it is ready for release.

- [Using content source control within VMware Aria Suite Lifecycle](#)

VMware Aria Suite Lifecycle content lifecycle management integrates natively into a GitLab and Bitbucket endpoint to provide content source control.

- [Deploy a content package](#)

You can use VMware Aria Suite Lifecycle to deploy a content package.

- [Managing multiple releases of a content package](#)

You can use VMware Aria Suite Lifecycle content management options to release content for multiple product types.

- [Delete a content package](#)

To delete a content package from endpoints when you no longer need the content package, use VMware Aria Suite Lifecycle .

- [Recognizing potential content issues](#)

Several common content issues may arise when using VMware Aria Suite Lifecycle.

Add content

You can use VMware Aria Suite Lifecycle to add content from an existing content endpoint.

Prerequisites

Verify that you have added a content endpoint.

Procedure

- 1 On the **My Services** dashboard, click **Content Management**.

2 Under **Content**, click **ADD CONTENT**.

If a version has already been captured, a content can be added either with the **Add Content** button or with an inline capture.

3 Select, test, or deploy the content package in addition to capturing it, and click **PROCEED**.

4 Enter the capture details for the content package.

- a From the **Select Capture Endpoint** drop-down menu, select one or multiple content types to capture.
- b Enter a tag name and select **Include all dependencies** to capture any dependencies associated with the content.

You can search for content by tag name.

- c Enter the VMware Aria Automation Orchestrator package name.

Any spaces in the name are replaced with an _ underscore character and a VMware Aria Automation Orchestrator package name.

The VMware Aria Automation Orchestrator package name is applicable only for VMware Aria Automation Orchestrator or VMware Aria Automation content having some VMware Aria Automation Orchestrator dependencies.

If you provide a new name, all the VMware Aria Automation Orchestrator contents are merged into one package. If you select an existing name from the drop-down menu, then a new version of the package is created and merges all VMware Aria Automation Orchestrator contents to the version. If a package version already exists for the endpoint, the new package version will contain old and new content.

If the VMware Aria Automation Orchestrator package is not captured prior, a new version is created but the content might not be the same as the previous version. Deploy the added VMware Aria Automation Orchestrator package to the VMware Aria Automation Orchestrator content endpoint first to append the content. If you do not enter any package name, then the name of the VMware Aria Automation Orchestrator package matches to the content that is captured with an added `-vro` as part of the name. All the discovered and captured VMware Aria Automation Orchestrator content, including individual workflows in the content files, appear in the created VMware Aria Automation Orchestrator package.

- d If the content is ready for production, select **Mark this version as production ready**.
- e Enter a description for the content version in the **Comments** field.
- f Click **Next**.

When you list the content for the first time for an endpoint, the system retrieves the content from the endpoint. After the content is captured, it is cached and the captured content is automatically refreshed every 30 minutes. You can select the **Get latest content** option to retrieve the content in between this 30 minute interval.

- 5 If prompted, enter test details for the content endpoint.
 - a Select one or more content endpoints to specify the environments to run tests on.
 - b Select **Deploy Content** to deploy the content in the endpoint before running tests.
 - c Select **Stop test deployment on first failure** to stop the test deployment when it encounters an error.
 - d Select **Run unit tests** to run available unit tests on the content.
 - e Select **Stop unit tests on first failure** to stop testing if any unit test fails.
 - f Select a server to run unit tests on from the **Select a Unit Test Server** drop-down menu.
You must have a VMware Aria Automation Orchestrator test package imported to use a unit test server.
 - g Click **Next**.
- 6 If prompted, enter the check-in details for the content package.
 - a Select one or more content endpoints from the **Select Release Endpoints** drop-down menu to specify the production environments where the system releases the content.
- 7 Click **SUBMIT**.
If you have selected a single content capture, you can view a single content pipeline. If you have selected multiple content captures, individual capture pipelines are deployed.

Delete multiple content names or versions

You can delete multiple content items and content versions in VMware Aria Suite Lifecycle. You can delete all the versions related to the selected content item.

Prerequisites

Verify that you have a content item already available in the content list.

Procedure

- 1 On the **My Services** dashboard, click **Content Management**.
- 2 Under **Content**, select the content item.
- 3 Click **Actions** and then click **Delete**.

When you delete the content item, the associated content versions are also deleted. You can perform a multi-delete operation for up to 15 content items.

Working with captured content

You can use VMware Aria Suite Lifecycle to capture a new version of an existing content package.

Procedure

- 1 On the **My Services** dashboard, click **Content Management**.
- 2 Under **Content**, click the name of the content package to capture and click **CAPTURE**.
- 3 From the **Select Capture Endpoint** drop-down menu, select the content endpoint to capture.
- 4 Select **Include all dependencies** to capture any dependencies associated with the content.
- 5 If the content is ready for production, click **Mark this version as production ready**.
- 6 Enter a description for this content version in the **Comments** field and click **CAPTURE**.

Content actions

After you capture content in VMware Aria Suite Lifecycle, you can perform and view content actions.

Deploying content

Content settings	Role	Expected behavior
Content version is production ready.	Release manager	You can view only production endpoints.
Content version is production ready.	Developer	You can test endpoints that have the test policy set, and it cannot include the production policy.
Content version is not marked as production ready.	Release manager Developer	You can view the test endpoints that have the test policy set.
Content version is not marked as source-controlled.	Release manager Developer	You can view the content endpoints that do not have the source control policy set on the content endpoint.
Content version is marked as source-controlled.	Release manager Developer	All the content endpoints are displayed based on other conditions in the table.

Using content tags

You can use tags in a specific content version to help navigate content. Tags are a useful grouping mechanism.

Available content types

VMware Aria Suite Lifecycle supports the following content packages for each available endpoint type.

Content Types

For the most current information about VMware cross product support, see the [VMware Product Interoperability Matrix](#).

Table 5-2. VMware vSphere content endpoint

Content Type	Product Support Versions	Description
vSphere-CustomSpecification	vCenter	Captures guest operating system settings saved in a specification that you can apply when cloning virtual machines or deploying from templates.
vSphere-Template	vCenter	Captures template to deploy virtual machines in the vCenter inventory.

Table 5-3. VMware Aria Automation content endpoint

Content type	Description
Automation-CloudTemplate	Captures a VMware Aria Automation cloud template to deploy virtual machines managed by VMware Aria Automation.
Automation-PolicyDefinition	Captures a VMware Aria Automation property definition for specifying custom properties.
Automation-ResourceAction	Captures a VMware Aria Automation resource action.
Automation-Subscription	Captures VMware Aria Automation subscription events that are triggered using the event broker. Captures the configured event and dependent workflows.
Automation-CustomResource	Captures VMware Aria Automation resource type.
Automation-ABXAction	Captures, tests, and releases VMware Aria Automation ABX actions.
Automation-PropertyGroup	Captures a VMware Aria Automation property group.

Table 5-4. VMware Aria Automation cloud endpoint

Content type	Description
Automation-CloudTemplate	Captures a VMware Aria Automation cloud template to deploy virtual machines managed by VMware Aria Automation.
Automation-PolicyDefinition	Captures a VMware Aria Automation property definition for specifying custom properties.
Automation-ResourceAction	Captures a VMware Aria Automation resource action.
Automation-Subscription	Captures VMware Aria Automation subscription events that are triggered using the event broker. Captures the configured event and dependent workflows.
Automation-CustomResource	Captures VMware Aria Automation resource type
Automation-ABXAction	Captures, tests, and releases VMware Aria Automation ABX actions.
Automation-PropertyGroup	Captures a VMware Aria Automation property group.

Table 5-5. VMware Aria Operations content endpoint

Content type	Description
Operations Alert	Captures VMware Aria Operations alerts containing symptom definitions and recommendations that are used to evaluate conditions and generate alerts.
Operations-Dashboard	Captures VMware Aria Operations alerts dashboard data used to determine the nature and time frame of existing and potential issues.
Operations-Report	Captures VMware Aria Operations report templates.
Operations-SuperMetric	Integrates VMware Aria Operations super metric data definition that is used to track combinations of metrics. After releasing super metric data, it assigns object types and enables super metrics in policies. All VMware Aria Operations package types support super metrics.
Operations- TextWidgetContent	Reads text from a web page or text file. You specify the URL of the web page or the name of the text file when you configure the text widget.
Operations- TopoWidgetConfig	Captures the structure of the topography around a specific resource.
Operations-View	Captures VMware Aria Operations views that help you to interpret metrics, properties, and policies of various monitored objects.
Operations- ResourceKindMetricConfig	Captures VMware Aria Operations metric configurations for particular adapter and object types so that the supported widgets are populated based on the configured metrics and selected object type.
Operations-Symptoms	Captures VMware Aria Operations operation symptoms.

Table 5-6. VMware Aria Automation Orchestratorcontent endpoint

Content Type	Description
Orchestrator-Action	Captures a VMware Aria Automation Orchestrator action.
Orchestrator-ConfigurationElement	Captures a VMware Aria Automation Orchestrator configuration element.
Orchestrator-Package	Captures a VMware Aria Automation Orchestrator package.
Orchestrator-RestHost	Captures a VMware Aria Automation Orchestrator REST host.
Orchestrator-RestOperation	Captures a VMware Aria Automation Orchestrator REST operation.
Orchestrator-Workflow	Captures a VMware Aria Automation Orchestrator workflow.

Note Ensure that Orchestrator-RestHost is available in the target vVMware Aria Automation Orchestrator prior to capturing or deploying Orchestrator-RestOperation.

Searching content

You can search an existing content based on certain defined entries within the UI.

- Content dependencies and dependency files can be seen by clicking the version and looking at the DEPENDENCIES tab.
- By clicking each file, you can download it from the content repository within VMware Aria Suite Lifecycle.

Test Content

You can test content to ensure it is ready for release.

Prerequisites

Verify that the content package has been added to VMware Aria Suite Lifecycle.

Procedure

- 1 On the **My Services** dashboard, click **Content Management**.
- 2 Under **Content**, click the name of the content package to capture.
- 3 Click the three horizontal dots to the right of the version to test and select **Test**.
- 4 Select one or more content endpoints to specify the environments to run tests on.
- 5 Select **Deploy Content** to deploy the content in the endpoint before running tests.
- 6 Select **Stop test deployment on first failure** to stop the test deployment as soon as it encounters an error.
- 7 Select **Run unit tests** to run available unit tests on the content.
- 8 Select **Stop unit tests on first failure** to stop testing if any unit test fails.
- 9 Select **Include all dependencies** to include all dependencies associated with the content package in the tests.
- 10 Select **Release Latest Dependencies** to release the latest versions of the dependencies associated with the content package.
- 11 Select a server to run unit tests on from the **Select a Unit Test Server** drop-down menu, and click **PROCEED**.

Performing Unit Tests

When you create a content endpoint, you can select **SupportTest** policy to enable the system to run unit tests after deploying a content to the test environment.

There are two servers here:

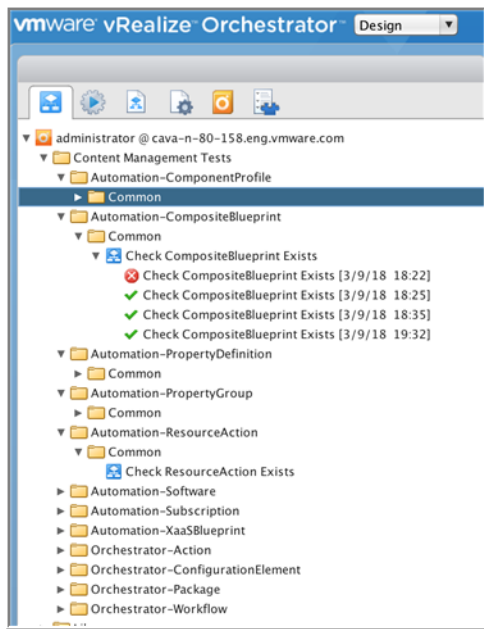
- Unit test server
- Test endpoint

The server is a staging environment in which you can deploy the contents and run unit tests against the deployed contents to the environment.

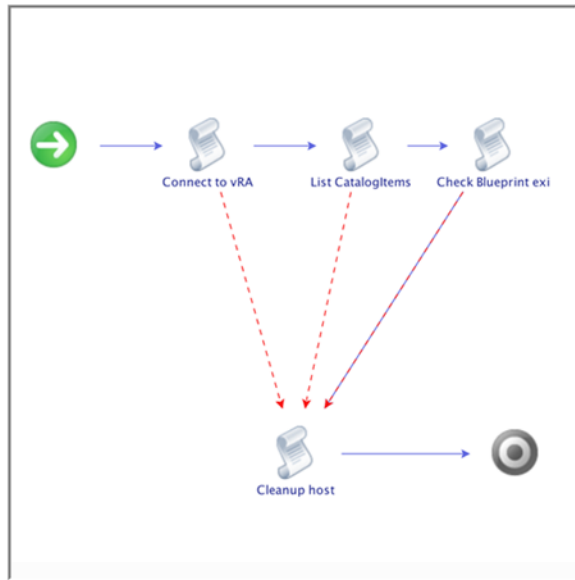
Unit Test Server

The test server is a VMware Aria Automation Orchestrator server, where you can run your unit tests against a deployed content in a test endpoint. Whenever you set an VMware Aria Automation Orchestrator endpoint as a test endpoint, it tests the VMware Aria Automation Orchestrator package and is deployed automatically to this endpoint allowing unit or integration tests. There are some basic tests already present in the package and you can extend the tests in the unit test server as well.

Menu options for Unit Test Server



Sample Unit Test Flow



Common Tests

All tests under the PackageType Common folder are run.

If you go to the unit test server (VMware Aria Automation Orchestrator), under the **Content Management Tests**, you can view separate folders for all content types. For each content type folder, there is a **common** folder present where you see all the common workflows that are run for a given content type.

Package Specific Tests

Specific tests can be run per content name. The format of tests is:

content name - test name and under the *Content-Type* folder.

When you select the unit server while testing content, the new unit tests is run against the deployed content in a test endpoint.

The following lists the overall functionality of unit tests:

- Common unit tests workflows can be written under **common** folder per content type.
- Unit test workflow for a given content can be written under `<Content Type>` and name the workflow as `<Content name> - <Tests name>`.
- If there is a test failure, then the test displays an error from a workflow.
- Checks the available inputs to test a workflow.

Sample Workflows

You can refer to the existing unit workflows available in their VMware Aria Automation Orchestrator (policy set to test). Navigate to a common folder in VMware Aria Automation Orchestrator, **Workflows > Content Management Tests > Content Type > Common**.

You can input available properties for a unit test workflow that is provided by the platform.

Property Name	Description
version	Version of content being tested.
testEndpointLink	The content endpoint link within the repository.
tenant	The tenant being connected to.
packageVersionLink	The version link to the repository.
packageType	Type of content.
packageName	Name of content.
packageId	Content Unique Identifier in the repository.
endpointUser	User name of endpoint being tested.
endpointServer	Server name of endpoint being tested.
endpointPassword	Secure password of the endpoint being tested.

Using content source control within VMware Aria Suite Lifecycle

VMware Aria Suite Lifecycle content lifecycle management integrates natively into a GitLab and Bitbucket endpoint to provide content source control.

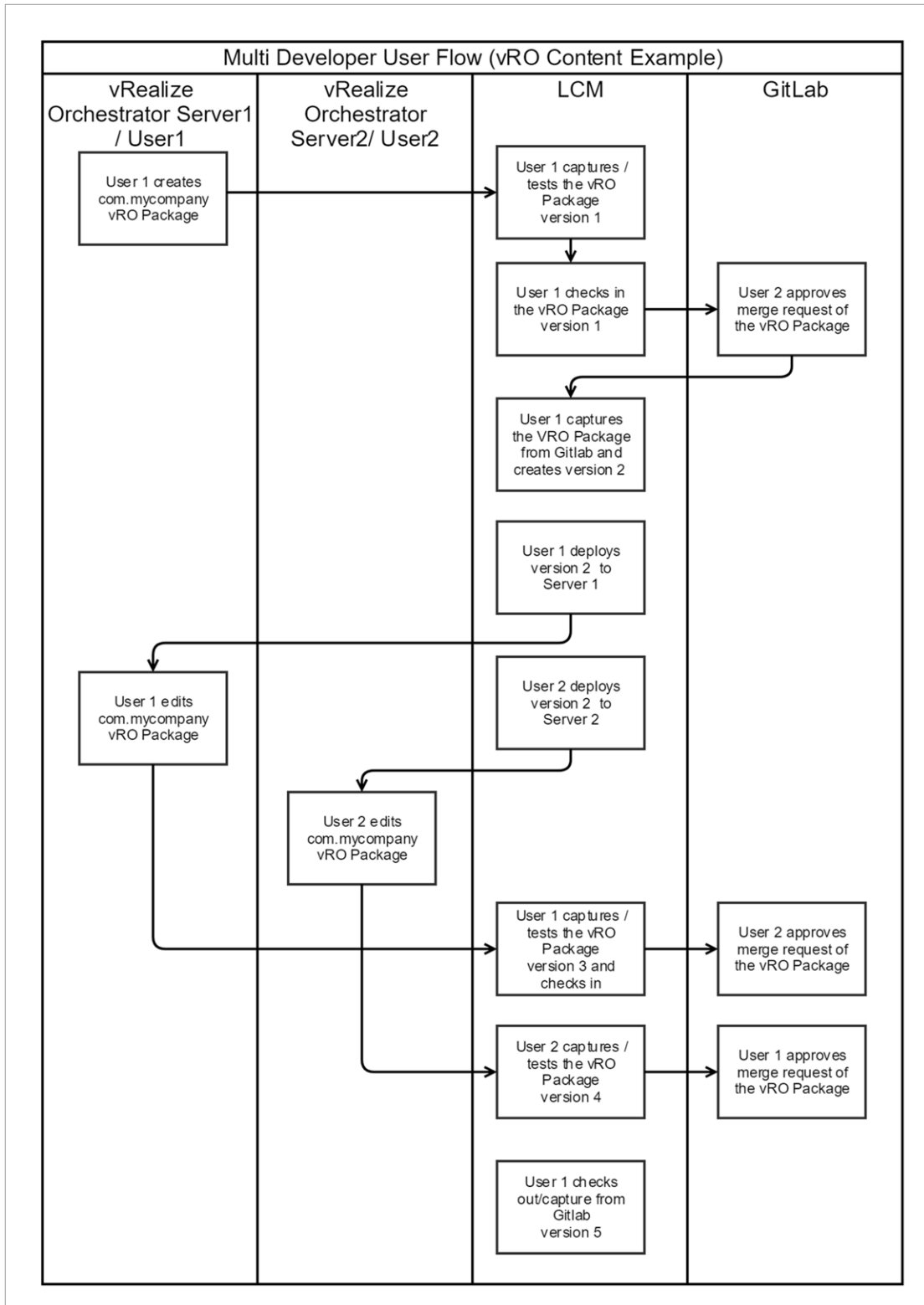
You can store content in both the VMware Aria Suite Lifecycle version-controlled repository and a GitLab or Bitbucket branch. This allows developers to work together to check in and check out content, and to code review changes prior to deploying to test or production environments.

VMware Aria Suite Lifecycle stores all source control commit hashes for the purpose of check in, so the correct state of content is known. This enables multi-developer support, which reduces the risk of overwriting content and reduces the number of merge conflicts that can occur.

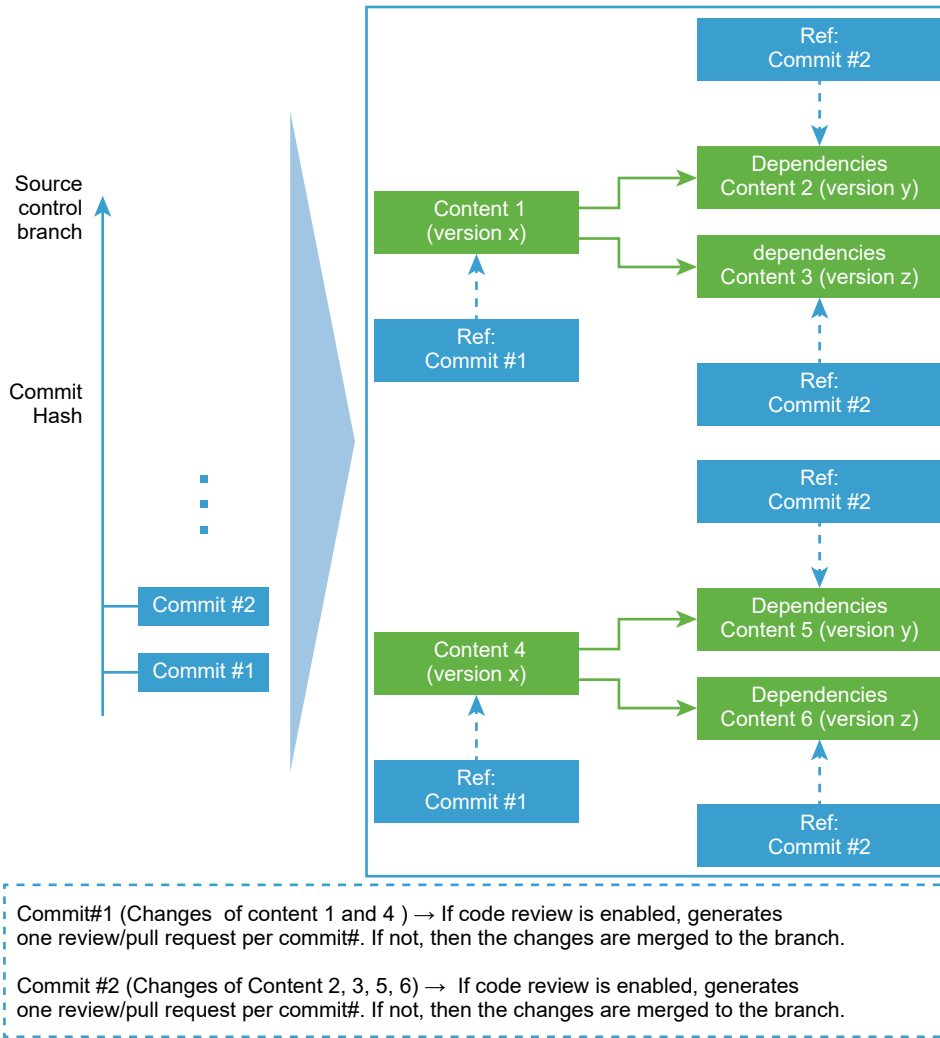
To use source control in VMware Aria Suite Lifecycle, you must meet the following prerequisites:

- Verify that you have a GitLab or Bitbucket server. If you do not have an existing GitLab server, you can use the Gitlab-CE free docker container.
- Verify that at least one VMware Aria Suite Lifecycle user has access to GitLab or Bitbucket.
- Create a branch in GitLab and apply the necessary permissions in GitLab for other developers to check in and check out content to the branch.
- The GitLab user must create an access token in GitLab and store the token against the GitLab instance under VMware Aria Suite Lifecycle **Content Settings**.

As a best practice, each time content is checked in to source control, a new version should be checked out and deployed to a content endpoint. This saves the latest changes from other developers (effective rebase of the content) and also communicates to the VMware Aria Suite Lifecycle content services which GIT Commit Hash is deployed to which content per endpoint.



Contents referring to multiple commit



hashes

Check in content to a source control endpoint

You can check-in the previously captured content to a source control endpoint by using VMware Aria Suite Lifecycle.

Prerequisites

Verify that you have added a source control endpoint to VMware Aria Suite Lifecycle. See [Using content source control within VMware Aria Suite Lifecycle](#) for source control requirements.

Note We support a single content check-in, with a maximum of 1000 files at a time.

Procedure

- 1 On the My Services dashboard, click **Content Management**.
- 2 Under **Content**, click the name of the content package to capture.
- 3 Click the name of the content package to test.

- 4 Click the three vertical dots to the right of the version to check in, and select **Check In**.
- 5 Enter the **Pipeline Name**, and then select a content endpoint from the drop-down list.
- 6 The **REPOSITORY** and **BRANCH** includes the default values.
- 7 For a VMware Aria Automation Orchestrator package merge, perform the following steps.
 - Select the **Include all dependencies** option to include all dependencies associated with the content package in the check-in.
 - Select the **Merge with delete content** option to delete content files from source control that are removed from source endpoint for VMware Aria Automation Orchestrator.
- 8 Add a descriptive comment in the **Comment** field, and click **CHECK IN**.

Results

Note Adding a check-in comment is mandatory.

When checking in a VMware Aria Automation Orchestrator package, there is an optional capability to merge with an existing VMware Aria Automation Orchestrator package that exists in the source control. This ensures that all files that are captured are checked into the path of the selected package (ultimately merged). If you do not see the package, then **Select the Source Control Endpoint > Orchestrator-Package type**, refresh the cache and check- in to view the VMware Aria Automation Orchestrator package in which it needs to be merged. You have the following new features added when you check in a VMware Aria Automation Orchestrator package:

- You can merge a custom VMware Aria Automation Orchestrator package from an endpoint to an uber package version in VMware Aria Suite Lifecycle.
- The ability to merge a custom VMware Aria Automation Orchestrator package directly to an uber package in GitLab.
- You can release a subset of contents from an VMware Aria Automation Orchestrator package while deploying to an endpoint.
- As part of the dependency management, you can remove dependency from a content version.

For a VMware Aria Automation content check-in, you can merge directly on GitLab. You can check out without dependency or check out with dependency, where you can perform the following:

- You can remove the package dependency from the latest version. For example, if you have performed a VMware Aria Automation content check in with dependency and enabled the option to merge the dependent VMware Aria Automation Orchestrator package to an uber package directly on GitLab. When you check-out the same VMware Aria Automation content with dependency from a source control.

If a code review is disabled on the source control branch, the content is auto merged.

What to do next

If a code review is enabled on the source control branch, you or another code reviewer must check the content in to GitLab manually after the code review is complete. After you check the content into GitLab, capture the latest content version from the source control server in VMware Aria Suite Lifecycle.

If you are continuing to develop on your content endpoint, capture the latest content version from source control and deploy it to your development content endpoint. This updates the content endpoint so that the content is in sync with the source control and subsequent check-ins are valid.

You can view the check in status in the **Activity Log**.

Check Out Content from a Source Control Endpoint

After a content is checked in to a source control endpoint, you can check out the content and deploy it to a content endpoint. When the content is checked out from Source Control, the content is marked with the Git Hash Code for reference.

Prerequisites

Verify that the content has been checked in to the source control endpoint. See [Check in Content to a Source Control Endpoint](#).

Procedure

- 1 On the My Services Dashboard, click **Content Management**.
- 2 Under **Content**, click **ADD CONTENT**.

Note You can check out the content inline as well.

- 3 Choose whether to test or deploy the content package in addition to capturing it, and click **PROCEED**.
- 4 Enter the capture details for the content package.
 - a From the **Select Capture Endpoint** drop-down menu, select the source control endpoint to capture content from.
 - b Select **Get the latest content** to retrieve the latest content dependencies rather than the dependencies the content was initially captured with.
 - c Select the content type and content to capture.
 - d Select **Include all dependencies** to capture any dependencies associated with the content.

Dependencies are stored in VMware Aria Suite Lifecycle, not the source control endpoint.
 - e If the content is ready for production, select **Mark this version as production ready**.

- f Enter a description for this content version in the **Comments** field.
- g Click **Next**.

5 Enter test details for the content endpoint.

This option appears only if you selected to test the content package.

- a Select one or more content endpoints to specify the environments to run tests on.
- b Select **Deploy Content** to deploy the content in the endpoint before running tests.
- c Select **Stop test deployment on first failure** to stop the test deployment as soon as it encounters an error.
- d Select **Run unit tests** to run available unit tests on the content.
- e Select **Stop unit tests on first failure** to stop testing if any unit test fails.
- f Select a server to run unit tests on from the **Select a Unit Test Server** drop-down menu.
You must have a VMware Aria Automation Orchestrator test package imported to use a unit test server.
- g Click **Next**.

6 Enter deployment details for the content package.

This option appears only if you chose to test the content package.

- a Select one or more content endpoints from the **Select Release Endpoints** drop-down menu to specify the production environments where the system releases the content.
- b Select **Stop release deployment on first failure** to stop deployment as soon as the system encounters a failure.
- c Enter a comment that explains why the content is being released in the **Release Comment** field as writing comments are mandatory.

7 Click **SUBMIT**.

Results

VMware Aria Suite Lifecycle captures the content from the source control endpoint and creates a new version of the content in the content catalog. This version is marked **SourceControl Enabled**, which tells VMware Aria Suite Lifecycle the state of the content when deploying to a content endpoint so the content is checked in against the right point in time.

What to do next

If you are using source control and have multiple capture content endpoints, only deploy content from the content catalog is marked **SourceControl Enabled**. This communicates the state of the content when deploying to a content endpoint so the content is checked in against the right point in time.

Deploy a content package

You can use VMware Aria Suite Lifecycle to deploy a content package.

Prerequisites

- Verify that the production environment has been added as a content endpoint.
- Verify that the content is ready for a production environment.

Procedure

- 1 On the **My Services** dashboard, click **Content Management**.
- 2 Click **Content** and click the name of the content package to deploy.
- 3 Click **DEPLOY** for the version to deploy.
- 4 Select one or more content endpoints from the **Select Release Endpoints** drop-down menu to specify the production environments where the system releases the content.
- 5 Select **Stop release deployment on first failure** to stop a deployment as soon as the system encounters a failure.
- 6 Select **Include all dependencies** to deploy all dependencies that are associated with the content package.
- 7 Select **Release Latest Dependencies** to release the latest versions of the dependencies associated with the content package.
- 8 In the **Release Comment** field, enter a comment that describes the content being released and then click **PROCEED**.

Managing multiple releases of a content package

You can use VMware Aria Suite Lifecycle content management options to release content for multiple product types.

Use these options to deploy releases of products such as vSphere, VMware Aria Operations, and VMware Aria Automation in a single request.

Note that failure to deploy one or more of the selected content types, does not roll back successfully deployed content that is part of the request.

Procedure

- 1 On the **My Services** dashboard, click **Content Management**.
- 2 Under **Content**, select **Content Item List**.
- 3 Expand the **Filter Applied** list.

- 4 Under the **Content Filter** section, use filters to specify to a subset of the content you want to view and deploy.

Filter type	Description
Content filters	<ul style="list-style-type: none"> ■ Production Ready ■ Development Content ■ Tested ■ Source Controlled ■ Dependencies Captured
Content types	Displays content categories based on content type.
Content endpoints	Displays associated content endpoints.

- 5 After you select a content filter, you can add a tag and then click **Apply**.
- 6 To save your filters, click **Save**.

Developers can only view their filters and release managers can view all other RM filters. The saved filters can be edited or deleted.

After you set the content filters, the default content view changes to **Content Version List**. When you provide a filter, you can locate a specific version of the content, for example, Production Ready Content with a specific tag and of a specific set of content types. For example, display only VMware Aria Automation cloud templates.

- 7 To deploy the content to a release endpoint, respond to the wizard prompts.
- 8 Click **Actions** and select **Checkin**.

Note You can check in multiple content after filtering and selecting contents. When you perform a multi-capture test and release, verify that the capture is successful because if one of the content capture fails, the entire content pipeline is marked as failed. Based on multi-capture pipeline failure, you cannot move to the next step of testing and releasing a pipeline.

- 9 To check in multiple content, use the following procedure:
- a Select an **Endpoint repository**.
 - b if you want to capture all the dependencies, select **Include all Dependencies** and merge the package, if required.
 - c Click **Check-in**.
- 10 Select an appropriate endpoint to each type of content appears.

VMware Aria Automation Orchestrator endpoints are assumed by their parent automation instance. If there are standalone VMware Aria Automation Orchestrator endpoints configured, you can also deploy them.

Delete a content package

To delete a content package from endpoints when you no longer need the content package, use VMware Aria Suite Lifecycle .

This operation cannot be undone.

Prerequisites

- Verify that one or more content endpoints are added.
- Verify that the content package is present in the deployment.

Procedure

- 1 On the **My Services** dashboard, click **Content Management**.
- 2 Click **Content** and click the name of the content package to delete.
- 3 Click the three horizontal dots to the right of the version and select **Delete**.
- 4 Click **OK**.
- 5 Refresh the page to display the results.

Recognizing potential content issues

Several common content issues may arise when using VMware Aria Suite Lifecycle.

- When transferring a customization spec between vCenter servers, the password fields cannot be decrypted by the target. This causes deployments that depend on custom specs with passwords to fail. You can manually enter the correct value in the Administrator password field after customization spec is deployed by the VMware Aria Suite Lifecycle pipeline.
- When a symptom definition is configured with `REGEX` or `NOT_REGEX`, the import fails when using the VMware Aria Operations APIs with the following error. **Error releasing Operations-Symptom message= "Invalid request... #1 violations found.", "validationFailures": [{"failureMessage": "Message Event Condition field 'operator' must be either EQ or CONTAINS.** If a symptom uses `REGEX`, the content must be imported manually by using VMware Aria Suite Lifecycle.
- A VMware Aria Suite Lifecycle pipeline execution with a large number of captures or check-ins may fail if the number of executions is higher than those supported by the endpoint type.
- When performing a multi-package capture, the entire capture fails with 409 conflict errors if there is a package with existing content.

Access source control

A VMware Aria Suite Lifecycle release manager can add a source control access.

With this privilege, a release manager can select the GitLab type or Bitbucket and enter the GitLab server name. You can supply multiple server names and assign the GitLab personal access token to the source control server.

By enabling access source control, you can add an endpoint for a source control. For information about adding a source control, see [Add a source control server endpoint in VMware Aria Suite Lifecycle](#).

To access the source control server, a developer who is logged in to VMware Aria Suite Lifecycle can associate and use their own token.

Managing source control server endpoints

Before you can check in or check out content, a VMware Aria Suite Lifecycle must add a GitLab or Bitbucket source control server to the system.

- [Add a source control server endpoint in VMware Aria Suite Lifecycle](#)

To add a source control server to the system, use the Content Management service in VMware Aria Suite Lifecycle to add a source control server endpoint.

- [Delete a source control server endpoint](#)

You can use VMware Aria Suite Lifecycle to delete a source control server endpoint that is no longer in use.

Add a source control server endpoint in VMware Aria Suite Lifecycle

To add a source control server to the system, use the Content Management service in VMware Aria Suite Lifecycle to add a source control server endpoint.

Use the following procedure to add a source control server endpoint.

Prerequisites

- Verify that you have access to a Bitbucket, GitHub, or GitLab instance that is supported for this version of VMware Aria Suite Lifecycle. For more information on the supported versions of Bitbucket, GitHub, and GitLab, see [Chapter 5 Working with Content Management in VMware Aria Suite Lifecycle](#).
- Log in to GitHub, GitLab, or Bitbucket, and generate an access token for your user that supports all scopes. Copy and save this one-time token.

- Log in to GitHub, GitLab, or Bitbucket and verify the existing group, project, and branch before adding the instance as a source control endpoint.

Note When you deactivate the file editor option, the Bitbucket API (PUT/POST) is not accessible to an administrator or developer. Do not include the `feature.file.editor` property in the property file or set the property to `true`.

Location: `base_directory\Atlassian\ApplicationData\Bitbucket\shared\bitbucket.properties`

Properties: `feature.file.editor=true`

Procedure

- 1 On the **My Services** dashboard, click **Content Management**.
- 2 Click **Content Settings**.
- 3 On the **Source Control Access** tab, click **ADD SOURCE CONTROL SERVER**.
- 4 Select the **Source Control Type**.
- 5 Enter the IP address or fully qualified domain name of the server and click **SUBMIT**.

VMware Aria Suite Lifecycle uses `https` format for any source control APIs by default. If you have not activated `https` on the GitLab instance, then specify `http://ip address:port` for the source control server on the content settings page to change the format. When you create a source control endpoint, the repository must be specified using a `GroupName/ProjectName` format. Use at least a 4 vCPU Bitbucket machine for optimal performance.

- 6 Click the **Edit** icon for the source control server.
- 7 Enter your GitLab or Bitbucket server access token in the **ACCESS KEY** text box and click **SUBMIT**.
 - a For a GitHub instance, enter the credentials for the user name and password or the access token.
 - b Click **SUBMIT**.

An access token is a unique identity for a user to perform check-in or check-out to track the GitLab or GitHub API. Create an access token for GitLab or GitHub by specifying the GitLab or GitHub server URL, for example, `gitlab.example.com` or `github.com`. For Bitbucket server and Cloud, browse to `bitbucket.org` and navigate to **App Passwords** to create a password with full permissions.

Delete a source control server endpoint

You can use VMware Aria Suite Lifecycle to delete a source control server endpoint that is no longer in use.

Prerequisites

Verify that the source control server endpoint is not being used by any content endpoints.

Procedure

- 1 On the **My Services** dashboard, click **Content Management**.
- 2 Click **Content Settings**.
- 3 On the **Source Control Access** tab, delete the source control server endpoint.
- 4 Click **OK**.

Working with content settings in VMware Aria Suite Lifecycle

You can add source control server endpoint, vCenter publisher, pipeline extensibility and developer restrictions in content settings.

Source control access

To add a source control endpoint, provide a server for that source control from GitLab. For more information, see [Add a source control server endpoint in VMware Aria Suite Lifecycle](#).

Note You can add multiple server names for a source control server endpoint and only GitLab source control is supported for this version.

vSphere template repository

You can use VMware Aria Suite Lifecycle to capture content from vCenter. The vSphere template repository is a content library within a designated vCenter instance. It stores all the templates that are captured and that can be managed by VMware Aria Suite Lifecycle.

A best practice is to have this vCenter instance close to where the templates would typically be captured, that is a development vCenter for template authoring. You can specify a vCenter instance to add as your endpoint. For more information, see [Add a vCenter content endpoint in VMware Aria Suite Lifecycle](#). The configuration model for the content library is as follows:

- 1 Create the **Content Library (Publisher)**: The vSphere template repository points to a content library that is configured for publishing. For information about configuring a publisher content library, see [vCenter Documentation](#).
- 2 Create the **Content Library Subscribers**: Each vCenter server that supports templates must support a content library that subscribes to the published library that you created in the above Step 1. The following settings are required:

Setting	Description
Automatic Synchronization	Configure this setting for automatic synchronization of the template metadata.
Subscription URL	This URL contains details about the publishers <code>lib.json</code> file. It is available when you create the publisher in Step 1.

Setting	Description
Authentication Off	Do not use this setting. You should require authentication.
Library content	<ul style="list-style-type: none"> ■ Download all library content immediately - If you don't select this option then vCenter downloads all virtual machine templates. ■ Download library content only when needed - Only the metadata is downloaded (not the disks). VMware Aria Suite Lifecycle instructs on demand and as requested to download the associated disks.

Timeout settings

You can specify time out settings for operations for various resources and endpoints. If an operation takes longer than the specified time to complete, an error message appears. The message provides details about the failed operation.

- 1 Select **Content Management** from the VMware Aria Suite Lifecycle **My Services** page and then click the **Content Settings** gear icon in the left pane navigation.
- 2 Click **Timeout Settings**.
- 3 Specify a timeout value for each of the following timeout setting categories:

Timeout type	Description
Test timeout	Time required to complete a specified VMware Aria Suite Lifecycle test operation(s).
Deploy timeout	Time required to complete a specified VMware Aria Suite Lifecycle deployment operation(s).
Content timeout	Time requirement as it pertains to the parent pipeline request, which can be a combination of capture, test, deploy, and check-in operations performed by VMware Aria Suite Lifecycle.
Capture timeout	Time requirement to fully capture specified content from the identified source(s) into VMware Aria Suite Lifecycle.
Request timeout	Time required to complete a specified VMware Aria Suite Lifecycle request operation(s).

Configure pipeline stub

You can use VMware Aria Suite Lifecycle to run pipeline stubs in a synchronous or asynchronous manner.

When running a stub in an asynchronous manner, other pipeline stages are run without waiting for the custom logic to complete. For example, a pre-capture configured to run asynchronously runs in parallel with the capture stage. However, a post-capture run is initiated only after the capture stage is run. You can schedule post-capture to run in parallel with the next scheduled stage, such as pre-test.

To associate a tag to a VMware Aria Automation Orchestrator work flow, edit the global custom tag name of the work flow to include the **vRSLCM_CUSTOM** keyword. Alternatively, you can use the */Library/Tagging/Tag* name. Migration of pre and post stub content is not supported.

Prerequisites

Verify that VMware Aria Automation Orchestrator endpoints to be used in the pre or post stub work flows are added in VMware Aria Suite Lifecycle and that they are tagged with **vRSLCM_CUSTOM** keyword.

Procedure

- 1 On the **Content Settings**, click the **Edit** icon.

The **Configure Pipeline Stub** page appears.

The **Name and Execute Pipeline** condition appears.

- 2 Select **Run in background** if the stub is to be run in an asynchronous manner.
- 3 Select the **Endpoint** from the drop-down menu.
- 4 Select a **Workflow** and click **Submit**.

Only work flows that are tagged as **vRSLCM_CUSTOM** appear in the list.

- 5 Select the **Input Param Configuration** and click **Submit**.

Map proxy setting

You can use VMware Aria Suite Lifecycle to map endpoints to REST calls.

Use the **Proxy mapping** tab to display the proxy status and configuration details such as the proxy server host name and port. You can use the proxy settings for source control endpoints only.

You can enable the proxy for a server configuration monitor (SCM) instance by selecting it from the list of servers and then clicking **Update**. Once the proxy is configured for any of the server configuration monitor (SCM) servers, the administrator cannot remove the proxy from the VMware Aria Suite Lifecycle setting page. To remove the proxy, you must remove the proxy mapping for all server configuration monitor (SCM) servers and then remove the proxy from the VMware Aria Suite Lifecycle setting page. You can remove the proxy mapping for an server configuration monitor (SCM) server by selecting it again and clicking **Update**. An administrator can confirm that the proxy is not used by any of the servers by examining the status of VMware Aria Suite Lifecycle proxy used by content management.

If the proxy is not configured, then click **Locker > Proxy** and select the **Configure Proxy** check box. For more information, see [Configure your proxy settings](#). Only a release manager and an administrator can access the proxy mapping settings in VMware Aria Suite Lifecycle.

Content pipeline settings

Use VMware Aria Suite Lifecycle to specify content pipeline settings, such as the status of the last 24 pipeline actions.

Pipeline stubs

The pipeline stubs display the status of each action. The content pipeline displays the following status types for each content run:

- Pre-capture
- Capture
- Post-capture
- Pre-test
- Test
- Post-test
- Pre-deploy/check-in
- Deploy/check-in
- Post-deploy/check-in

The *check-in* term refers to content in a source control endpoint such as Git or BitBucket. You can also view corresponding details for the associated parents pipeline.

The Run tab displays information about all the pipeline runs.

Each pipeline consists of various stages, each of which contains multiple tasks. The tasks are either parallel or sequential actions based on your custom business logic.

When you specify an action to perform on a content, a content capture can list various types of status related to such an action. Each of the content settings is related to the view displayed on the content pipeline page.

Execute pipeline conditions:

- 1 **EXECUTE_ON_SUCCESS** - The stub is executed only if the corresponding stage executes successfully. For example, Post-Capture if configured to EXECUTE_ON_SUCCESS executes only if the Capture stage is executed successfully.
- 2 **EXECUTE_ON_FAILURE** -The stub is executed only if the corresponding stage execution fails. For example, Post-Capture if configured to EXECUTE_ON_FAILURE executes only if the Capture stage is execution fails.
- 3 **EXECUTE_ON_SUCCESS_AND_FAILURE** - The stub is executed irrespective of whether the corresponding stage execution passes or fails. For example, Post-Capture if configured to EXECUTE_ON_SUCCESS_AND_FAILURE executes in both cases, whether Capture stage execution passes or fails.

Inputs parameters

The pre or post stubs support the mentioned list of parameters, the values of which can be passed to the respective VMware Aria Automation Orchestrator workflow as inputs. The value of these inputs depends on the content (been captured/tested/deployed) of the pipeline execution for which the pre or post routines are executed. Currently, all the parameters are of the type String. Therefore, the input parameters configured for the corresponding work flow in VMware Aria Automation Orchestrator should be necessarily of type String. A mismatch between the type of parameters results in an execution failure for the pipeline. For more information, see [Configure pipeline stub](#).

Post-Deploy-Pipeline	Pre-Deploy-Pipeline	Post-Test-Pipeline	Pre-Test-Pipeline	Post-Capture-Pipeline	Pre-Capture-Pipeline
■ contentName	■ contentName	■ contentEndPoint	■ contentName	■ contentName	■ contentName
■ contentEndPoint	■ contentEndPoint	■ ContentId	■ contentEndPoint	■ contentEndPoint	■ contentEndPoint
■ ContentId	■ ContentId	■ contentName	■ ContentId	■ ContentId	■ ContentId
■ contentType	■ contentType	■ contentType	■ contentType	■ contentType	■ contentType
■ ContentVersionID	■ ContentVersionID	■ ContentVersionID	■ ContentVersionID	■ ContentVersionID	■ ContentVersionID
■ requestid	■ requestid	■ requestid	■ requestid	■ requestid	■ requestid
■ requestnumber	■ requestnumber	■ requestnumber	■ requestnumber	■ requestnumber	■ requestnumber
■ status	■ requestedby	■ requestedby	■ requestedby	■ requestedby	■ requestedby
■ requestedby	■ useridentity	■ useridentity	■ useridentity	■ useridentity	■ useridentity
■ useridentity				■ status	

Content pipelines

You can use VMware Aria Suite Lifecycle to display the content capture, test, and release status of content pipelines. You can view all content pipelines that are completed, in progress, or in failed state.

If you are unable to view the complete list of pipelines, refresh the content pipelines page.

Select a content pipeline from the content pipelines list to display its status.

Content pipeline options	Description
Status Message	Displays the status summary of the selected content pipeline.
Executed by	Displays the user details when performing the execution.
Last Update	Displays the date of the selected content pipeline.
Comments	Displays additional comments entered by the user.

Content pipeline options	Description
Content Types	Displays the content type selected for the pipeline execution.
Content_pipeline <ul style="list-style-type: none">■ Capture■ Test■ Deploy	Displays the status of the selected option.

Upgrading VMware Aria Suite Lifecycle and VMware Aria Suite products

6

You can upgrade VMware Aria Suite products and VMware Aria Suite Lifecycle by using the Lifecycle Operations service.

To upgrade an older version of VMware Aria Suite Lifecycle, use the following upgrade order:

- Upgrade VMware Aria Suite Lifecycle.
- Upgrade VMware Workspace ONE Access.
- Upgrade VMware Aria Automation.

To upgrade individual VMware Aria Suite products after installing VMware Aria Suite Lifecycle, upgrade each product supported by VMware Aria Suite Lifecycle.

Read the following topics next:

- [Upgrade VMware Aria Suite Lifecycle](#)
- [Upgrade Workspace ONE Access by using VMware Aria Suite Lifecycle](#)
- [Upgrade vRealize Automation 8.x or VMware Aria Automation by using VMware Aria Suite Lifecycle](#)
- [Upgrade a VMware Aria Suite Product](#)

Upgrade VMware Aria Suite Lifecycle

You can check for and install updates to the VMware Aria Suite Lifecycle appliance.

You can also upgrade VMware Aria Suite Lifecycle by using an ISO file to install the upgrade.

Prerequisites

- Verify that you meet the system requirements. See [System requirements for VMware Aria Suite Lifecycle](#).
- Take a snapshot of the VMware Aria Suite Lifecycle virtual appliance. If you encounter any problems during upgrade, you can revert to this snapshot.
- Verify that no critical tasks are currently in progress in VMware Aria Suite Lifecycle. The upgrade process stops and starts VMware Aria Suite Lifecycle services and reboots the VMware Aria Suite Lifecycle virtual appliance, which might corrupt tasks that are in progress.

- If you are upgrading VMware Aria Suite Lifecycle through a repository URL or CD-ROM, ensure that you download the VMware Aria Suite Lifecycle upgrade binary from the MyVMware portal in advance. The file name is something like `VMware-Aria-Suite-Lifecycle-Appliance-8.X.X.XX-XXXXXXXX-updaterepo.iso`.

Note You cannot use the easy installer iso file for an VMware Aria Suite Lifecycle upgrade, you must use the VMware Aria Suite Lifecycle upgrade iso file.

Procedure

- 1 From the **My services** dashboard, click **Lifecycle Operations** and click **Settings**.
- 2 Click **System Upgrade**.

VMware Aria Suite Lifecycle displays the name, version number, and vendor of the current VMware Aria Suite Lifecycle appliance.

- 3 Select the repository type for VMware Aria Suite Lifecycle updates.

Option	Description
Check Online	You can check if the upgrades are available online. To use this option, the VMware Aria Suite Lifecycle virtual appliance must have access to <code>vapp-updates.vmware.com</code> .
URL	Enter your repository URL for updates. To use this option, extract the ISO containing the upgrade files to a private repository. Do not use a private repository that requires authentication for a file access.
CD-ROM	You can update the VMware Aria Suite Lifecycle Appliance from an ISO file that the appliance reads from the virtual CD-ROM drive.

- 4 Click **Check for Upgrade**.

After few minutes, VMware Aria Suite Lifecycle displays a message indicating if there are updates available.

- 5 Select the **Repository Type**, and then click **Upgrade**.
 - a When VMware Aria Suite Lifecycle is not connected to the internet, you can download the VMware Aria Suite Lifecycle **Update Repository Archive** binary from My VMware portal.
 - b The downloaded ISO should be attached to VMware Aria Suite Lifecycle VM's virtual CD-ROM drive. To do this, you can either upload the ISO in a content library of the vCenter server hosting VMware Aria Suite Lifecycle or you can upload in a data store that the VMware Aria Suite Lifecycle VM can access. After uploading, you must attach the ISO to the VMware Aria Suite Lifecycle VM's CD-ROM device by editing the VM's hardware configuration from the vCenter inventory. From VMware Aria Suite Lifecycle UI, select CD-ROM based upgrade option and proceed.
- 6 In the **Prerequisites** section, click the **Product snapshots** check box and then click **Next**.

- 7 Click **Run Precheck**. When the pre-check validation is finished, download the report to view the checks and validation status.
- 8 Click **Upgrade** after a successful pre-check validation.
- 9 After a few minutes, log in to the VMware Aria Suite Lifecycle UI and click **Settings > System Upgrade** to check for the `upgrade successful` message.

When upgrade is finished, VMware Aria Suite Lifecycle displays the upgrade completion message. If you do not see this message, wait for a few minutes and refresh the UI.

What to do next

For related information about upgrading from one release to another, see [sample blog](#) articles at [VMware blogs](#).

Support for additional product versions

You can enable applicable product versions for VMware Aria Suite products while you update the VMware Aria Suite Lifecycle appliance. You can add additional policy support, enhance new product versions, and add patches to VMware Aria Suite Lifecycle.

You can check the latest available product versions on the VMware Aria Suite [product page](#). For information about which VMware products and versions are compatible with your VMware Aria Suite Lifecycle product and version, see [VMware Product Interoperability Matrix](#).

If the product version upgrade does not complete successfully, navigate to the downloaded product file. The file extension is `.pspak`. Upload and validate the file by using a supported web browser.

For information about obtaining and installing VMware Aria Suite Lifecycle Product Support Packs, see the VMware Aria Suite Lifecycle Product Support Packs release notes for your VMware Aria Suite Lifecycle version at the VMware Aria Suite Lifecycle [product documentation page](#). If there is information about VMware Aria Suite Lifecycle fix packs, that information would also reside on the VMware Aria Suite Lifecycle [product documentation page](#).

Upgrade Workspace ONE Access by using VMware Aria Suite Lifecycle

You can upgrade from earlier versions of Workspace ONE Access to the latest version if you conform to VMware Aria Suite Lifecycle supported form-factor. Otherwise, the upgrade must be

performed outside VMware Aria Suite Lifecycle. After an upgrade, you can reimport Workspace ONE Access by initiating the inventory sync operation in VMware Aria Suite Lifecycle.

Note

- If the Workspace ONE Access installation, upgrade, or scale out request is displayed as an IN PROGRESS or FAILED state in VMware Aria Suite Lifecycle, do not remediate the cluster.
- If Workspace ONE Access is clustered through VMware Aria Suite Lifecycle, use the Power ON and Power OFF options to bring down the cluster and then reboot or shut down.
- When you deploy Workspace ONE Access with VMware Aria Suite Lifecycle, do not change the Workspace ONE Access host name. For more information, refer to the [VMware Workspace ONE Access](#) documentation.

Prerequisites

Note that the VMware Identity Manager and Workspace ONE Access terms are used interchangeably in VMware Aria Suite Lifecycle product documentation.

For more information, refer to the *VMware Aria Suite Easy Installer for VMware Aria Automation and VMware Identity Manager* in VMware Aria Automation [product documentation](#).

- In a clustered environment, ensure that the **Postgres Cluster Health Status** setting is healthy by enabling the **Trigger Cluster Health** option for your product on the **Environments** page. After your request is complete, review the notifications for your product and verify that your status is healthy. If your status is unhealthy, use the **Power ON** option to remediate your cluster prior to an upgrade.
- Verify that you have taken a snapshot of Workspace ONE Access nodes.
- Verify that you have mapped your product binaries. For more information, see [Configure product binaries](#).

Procedure

- 1 On the **Lifecycle Operations** page, click **Manage Environments**.
- 2 On the **Global Environment** instance, click **View Details** and then click **Upgrade**.
- 3 Under the Product details section, you can select the following repository type.

Option	Description
Repository URL	When you select this option, you can manually add the local upgrade file location in the virtual appliance.
VMware Aria Suite Lifecycle Repository	When you select this option, you can enter the upgrade path available after mapping the binaries through VMware Aria Suite Lifecycle.
VMware Repository	Select this option and select the version. The upgrade is performed using the online source.

- 4 Click and run the pre-check.

- 5 Click **Submit**.

Migrating a Microsoft Windows connector

In connector migration, the Windows connector for Workspace ONE Access is installed on a Windows machine by providing the configuration file that is generated from an external or embedded Linux connector.

After the external or embedded Linux connector is migrated, the Integrated Windows Authentication (IWA) and LDAP directories on the Linux connector are migrated to Windows. The IWA active directories are supported only on external Windows connectors.

Prerequisites

Ensure that you adhere to the following prerequisite requirements:

- The supported JRE version is between 8 update 181 to 8 update 251.
- The supported .NET framework version is 4.6.0.
- The supported Windows Server versions are 2012 R2, 2016, and 2019.
- A unique Windows system is required for the migration and it must be connected to a domain server.

Procedure

- 1 On the **Lifecycle Operations** page, click **Manage Environment**.
- 2 Navigate to the **Global Environment** instance.
- 3 Click **View Details > Upgrade**.
- 4 Select the check box and proceed to Upgrade.
- 5 On the **Select Version** tab, select **Repository URL > Repository Type > Product Version**.
- 6 To specify the connector migration, enter the **Target Windows Connector** details in the **Migrate Linux Connector to Windows Connection** section.

Note The source connector details for the embedded connector type are populated from Workspace ONE Access. You must enter only the Linux connector SSH passwords for the external connector type.

- a Enter the target **Windows FQDN** and **Windows Domain User** values.
 - b Select the **Windows Domain Password**.
 - c Select the **Windows VM Center**.
- 7 Click and then click **RUN PREHECK**.

If the validations are not successful and you want to make changes and then resume the Workspace ONE Access upgrade operation, click **SAVE AND EXIT**.

If the validations are successful, click **Next**.

8 On the **Upgrade Summary** page, verify the details and then click **Submit**.

Upgrade vRealize Automation 8.x or VMware Aria Automation by using VMware Aria Suite Lifecycle

You can upgrade vRealize Automation 8.x or VMware Aria Automation by using VMware Aria Suite Lifecycle.

Prerequisites

- Ensure that you have upgraded the earlier versions of either vRealize Automation 8.x or VMware Aria Suite Lifecycle to the latest version of the product. For more information on upgrading your VMware Aria Suite Lifecycle, see [Upgrade VMware Aria Suite Lifecycle](#) for the target version.
- Ensure that you have upgraded VMware Workspace ONE Access. For more information on VMware Workspace ONE Access upgrade and version support, see [Upgrade Workspace ONE Access by using VMware Aria Suite Lifecycle](#).
- Perform the binary mapping of the VMware Aria Automation upgrade ISO from Local, myvmware, or NFS share. For more information on binary mapping, see [Configure product binaries](#).
- Increase the CPU, memory, and storage as per the system requirements of the target version of VMware Aria Automation. For more information, see the *Hardware Requirements* section of the *Reference Architecture* publication for the target VMware Aria Automation version. For related information, see the *System Requirements* section of the *Easy Installer* publication for the target VMware Aria Automation version. Both publications are available on the VMware Aria Automation [documentation page](#).

To enable multi-tenancy for VMware Aria Automation, see [Tenant management in VMware Aria Suite Lifecycle](#).

Procedure

- 1 On the **Lifecycle Operations** page, click **Manage Environments**.
- 2 Navigate to the source product instance.
- 3 Click **View Details** and click **Upgrade**.

A pop-up menu appears, alerting you to perform an inventory sync.

- 4 Click **Trigger Inventory Sync** of the product before you upgrade.

Note A change in the environment outside of VMware Aria Suite Lifecycle can occur. Be aware of the current state of your system and verify that the inventory to upgrade is up-to-date.

- a If the product inventory is already synced and up-to-date, click **Proceed Upgrade**.

Note: If the source version is vRealize Automation 8.0.x, use the steps given in the KB article [78325](#) before you upgrade to restore expired root accounts. Other KBs may exist for other source product versions.

- 5 After the inventory is synced, select the VMware Aria Automation version that you are upgrading to.
- 6 To specify the **Repository Type**, select **VMware Aria Suite Lifecycle Repository** if you have mapped the ISO binary map or select **Repository URL** to use a private upgrade repository URL.
- 7 If you selected **Repository URL**, enter the unauthenticated URL and then click **Next**.
- 8 Click **Pre-Check**.

Pre-check validates the following criteria:

- SSH enabled - Verifies that SSH for the root user is enabled.
- Version check - Verifies if the target version selected for upgrade is compatible with the current VMware Aria Automation version.
- Disk space on root, data, and services log partition - Verifies if the required amount of free disk space is available in the root, data, and services log partition.
- CPU and Memory Check - Verifies if the required amount say 12 CPU and 48 GB memory resources available in each VMware Aria Automation nodes before upgrade.
- vCenter property existence check - Verifies if the vCenter details are present as part of each node in the VMware Aria Suite Lifecycle inventory. Because a snapshot is taken during the upgrade process, it is important to have the right vCenter details within the VMware Aria Suite Lifecycle inventory.
- VMware Aria Automation VMs managed object reference ID retrieval check - Verifies if the managed object reference ID of the VM can be retrieved from the details available in the VMware Aria Suite Lifecycle inventory. This is required as you perform snapshot-related operations on the VMs, finding the VM using the same.

- 9 Click **Next** and **Submit**.

After you click **Submit**, you can navigate to the **Request Details** page to view the upgrade status.

You can also monitor the upgrade process by using the `vracli upgrade status --follow` command.

At various stages of the upgrade process, logs capture stage activity. The following commands can also be helpful in monitoring the upgrade progress:

- `tail -f vami.log`
- `tail -f postupdate.log`
- `tail -f deploy.log`
- `tail -f /var/log/vmware/prelude/upgrade-2022-11-06-15-22-15.log`

What to do next

To learn more about the VMware Aria Automation upgrade stages, see [VMware Aria Automation stages in VMware Aria Suite Lifecycle workflow](#).

VMware Aria Automation stages in VMware Aria Suite Lifecycle workflow

There are three stages in the upgrade process of vRealize Automation 8.x or VMware Aria Automation within the VMware Aria Suite Lifecycle workflow.

Stage of upgrade	Description
Preparation	The preparation phase verifies that the system is healthy and shuts down services to make sure that all data is persisted.
Snapshot creation	Snapshots are taken for an automated, faster recovery of failures. VMware Aria Suite Lifecycle then shuts down the VMs, takes a snapshot, turns power on, and continues to the next phase.
Upgrade	The upgrade utility is run.

For certain failure events, the VMware Aria Suite Lifecycle upgrade workflow provides options to either finish the upgrade successfully or revert to the stage before upgrade.

- The upgrade process starts with a status check task that verifies the current state of the VA. If the system already has an upgrade request due to a previous upgrade attempt, then VMware Aria Suite Lifecycle provides an option to clean the older states and start a new upgrade. You can see the status task failing with a retry parameter similar to a `cancelAndStartAfresh` statement. Setting this retry parameter to `true` cleans up older states and restarts the upgrade.
- If failures occur during the preparation phase, you can cancel the upgrade process. If a failure cannot be corrected, or if the failure is fixed manually outside of the upgrade tool, you can proceed to the next phase in the upgrade workflow. The status provided after a preparation phase failure provides two retry parameter options. If you set the `cancelAndStartAfresh` option to `true`, the upgrade process is cancelled and the system reverts to its pre-upgrade state. If you set the `proceedNext` option to `true`, the VMware Aria Suite Lifecycle upgrade proceeds to the next stage.

- The upgrade workflow consists of VM operations such as reverting or deleting a snapshot and VM shutdown, power ON, and so on. If a failure occurs, a **Skip** option can be used if the retry option in VMware Aria Suite Lifecycle does not help and when you manually perform the same operation directly in vCenter.
- The final phase of the upgrade can be successful, can succeed with warnings, or can fail.
 - Success with warnings indicates that the upgrade has completed successfully, but a minor error is detected. You can check the errors and rectify them. You can set the `succeedUpgradeRequest` retry parameter to `true` to complete the VMware Aria Suite Lifecycle upgrade workflow.
 - If upgrade fails, you can decide if you want to revert the snapshot and retry the upgrade or cancel the whole upgrade process. You can revert and delete the snapshot, cancel the current upgrade request, and move the system to a state before the upgrade started.
 - For an upgrade failure, you can see the status task after the upgrade failure with retry parameters similar to `revertSnapshotNRetryUpgrade` and `cancelUpgradeNRevertBack`. If you set `revertSnapshotNRetryUpgrade` to `true`, the upgrade utility revert the snapshot and you can retry the upgrade.
 - If you set `cancelUpgradeNRevertBack` to `true`, you can cancel the upgrade process, which can revert and delete the snapshot, cancel the current upgrade request, and move the system to a pre-upgrade state.

Note

- The VMware Aria Suite Lifecycle upgrade workflow does not support removing snapshots if there is a successful upgrade. You can keep the snapshots or remove them manually from the vCenter.
- If you cancel the upgrade process after a post preparation or upgrade phase failure, the upgrade workflow from VMware Aria Suite Lifecycle is stopped. In such situations, restart the upgrade process by using options on the **Manager Environment** page.
- You can enable the multi-tenancy for VMware Aria Automation, refer to [Tenant management in VMware Aria Suite Lifecycle](#).
- If the VMware Aria Automation upgrade fails, you must cancel upgrade or revert a snapshot, and then retry to upgrade through VMware Aria Suite Lifecycle. If you revert the snapshot manually in a vCenter, VMware Aria Automation goes into an inconsistent state.
- For VMware Aria Automation, if you cancel upgrade or revert a snapshot, and then retry upgrade, ensure that you create a support bundle that contains the log files for any future analysis and reference.

Upgrade a VMware Aria Suite Product

You can use VMware Aria Suite Lifecycle to upgrade VMware Aria Suite product installations.

Prerequisites

Verify that the VMware Aria Suite product to upgrade is part of a VMware Aria Suite Lifecycle private cloud environment, and take a snapshot of the product that you can revert to in the event that something goes wrong with the upgrade. See [Create and manage a product snapshot](#).

Procedure

- 1 On the **Lifecycle Operations** page, click **Manage Environments**.
- 2 Click **VIEW DETAILS** for the environment the product to upgrade is part of.
- 3 Click the ellipses (...) icon next to the name of the product to upgrade and select **Upgrade** from the drop-down menu.
- 4 Choose a product version to upgrade to.
- 5 If you are upgrading VMware Aria Automation or vRealize Business for Cloud, choose whether to upgrade from the **Default** repository, the VMware Aria Suite Lifecycle **Repository**, or a manually-entered **Repository URL**.
- 6 If you are upgrading VMware Aria Operations for Logs or VMware Aria Operations, choose whether to upgrade from the VMware Aria Suite Lifecycle **Repository**, or a manually-entered **Repository URL**, and then select the **Product Version**.
- 7 Click **Next**.
- 8 Select a **Snapshot** option.

- **Take product snapshot**

If the **Take product snapshot** option is set to true, and the snapshot is taken prior to an upgrade which can be rolled back to its initial state during an upgrade failure, the snapshot is taken with the prefix `LCM_AUTOGENERATED`.

- **Retain product snapshot taken**

If the **Retain product snapshot taken** option is set to true, it is retained and can be reverted back to the previous version after a successful upgrade.

Note

- When you select a snapshot, it powers off the product VMs prior to taking the snapshot. This involves a period of downtime.
 - If your upgrade fails, you can roll back by using the **Revert Snapshot** option. This is only applicable for a failed upgrade or a scale out request. If you have chosen to take snapshot as an option and your upgrade fails, the **Snapshot Rollback** action runs a new request to roll back to the initial state. Select the ellipsis (...) in the **Requests** page to access the **Snapshot Rollback** action.
-

- 9 Click **RUN PRECHECK**. After a successful pre-check, you can view the upgrade summary and click **Upgrade**.

If you have upgraded a VMware Aria Suite product outside of VMware Aria Suite Lifecycle, then VMware Aria Suite Lifecycle will not reflect the latest product version or the latest data of the upgraded product. At such instances you must delete the VMware Aria Suite product (the product that is already upgraded to the newer version outside of VMware Aria Suite Lifecycle) from VMware Aria Suite Lifecycle only, and then re-import the same product so that VMware Aria Suite Lifecycle can fetch the latest state and newer version of the product.

Note After upgrade, some requests might prevent the upgraded services to start. The VMware Aria Suite Lifecycle UI displays a maintenance mode message. If this occurs, restart the xenon server. If the issue still persists, delete the error request and restart xenon.

What to do next

You can view the progress of the upgrade on the **Requests** tab.

Upgrade existing products using the pre-upgrade checker

You can start a pre-validation check from the product UI before upgrading an existing product. You can also evaluate product upgrades and allow upgrade operations later and validate the product compatibility matrix.

For more information on upgrading VMware Aria Suite products, see [Upgrade a VMware Aria Suite Product](#).

Prerequisites

Verify that you already have an existing VMware Aria Suite product in your environment.

Procedure

- 1 On the **Lifecycle Operations** page, click **Manage Environments**.
- 2 Right-click the vertical ellipses of an existing VMware Aria Suite product and select **Upgrade**.

The compatibility matrix information is loaded with new, compatible, and incompatible versions relative to the product to be upgraded.

- 3 In the **Product details** section, select the repository type.

Repository type	Description
VMware Repository	When you select this option, the latest versions of the VMware Aria Suite products are displayed in the compatibility matrix table. You can see this option only on VMware Aria Automation. Although, the compatibility matrix information is populated at the VMware Aria Suite level, the latest versions might not be available for VMware Aria Suite Lifecycle. The Check Available Version option displays only the latest version number with its associated build number.
Repository URL	When you select this option, you can manually add the local upgrade file location in the VMware Aria Suite Lifecycle virtual appliance.
VMware Aria Suite Lifecycle Repository	When you select this option, you can select the upgrade path available after mapping the binaries through VMware Aria Suite Lifecycle.

Note The VMware Aria Operations upgrade contains a **Run Assessment** option. The **Run Assessment** option checks for VMware Aria Operations upgrade readiness. The compatibility matrix information is populated relative to the selected version of VMware Aria Operations.

- 4 Click **Next** and then click **Run Pre-check**.

When the pre-check validation is finished, download the report to view the checks and validation status.

Note If you want to run the pre-check again after evaluating the discrepancies, select the **Re-Run Pre Check**. You also re-run the pre-check operation by using the **Submit** toggle button.

- 5 Click **Next** and then click **Submit**.
- 6 If any VMware Aria Automation IaaS component upgrades fail, complete the following steps:
- Revert all the Infrastructure components back to the post-upgrade VA snapshot.
 - Revert the MS SQL database back to its pre-upgraded state.
 - Click **Retry** from VMware Aria Suite Lifecycle and set **Upgrade IaaS Using CLI** to **True**.
 - Click **Submit**.

Upgrade VMware Aria Operations

You can run a pre-validation check from the product UI before upgrading VMware Aria Operations within an environment. You can also evaluate VMware Aria Operations upgrades and run an upgrade operation later. You can also validate the product compatibility matrix.

Prerequisites

Verify that there is an older or existing version of VMware Aria Operations in the **Manage Environments** page.

Procedure

- 1 On the **Lifecycle Operations** page, click **Manage Environments**.
- 2 Right-click the vertical ellipses of an existing VMware Aria Operations product and select **Upgrade**.

The compatibility matrix information is displayed with new, compatible, and incompatible versions of products that must be upgraded.

- 3 In the **Product details** section, select the repository type.

Repository type	Description
Repository URL	When you select this option, you can manually add the local upgrade file location in a VMware Aria Suite Lifecycle virtual appliance.
VMware Aria Suite Lifecycle Repository	When you select this option, you can enter the upgrade path available after mapping the binaries through VMware Aria Suite Lifecycle.

- 4 Click **Next**.
- 5 To run the file format select **Version support from LCM** and then click **RUN PRECHECK**.

When the pre-check validation is finished, download the report to view the checks and validation status.

Note When you upgrade the VMware Aria Operations instance, you have two options.

- **Run PreCheck:** You must run to upgrade VMware Aria Operations.
- **Run Assessment Tool:** You can use this option to run a VMware Aria Operations APUAT tool.

The binary for the VMware Aria Operations APUAT tool is bundled with VMware Aria Suite Lifecycle. Once VMware Aria Suite Lifecycle is deployed, the APUAT tool is present in the VMware Aria Suite Lifecycle VA location `/data/lcmcontents/` by default.

Note If you want to run the pre-check again after evaluating the discrepancies, select **Re-Run Pre Check**. You can also re-run the pre-check by using the **Submit** toggle button.

If the OS administrator password for VMware Aria Operations expires, the VMware Aria Operations upgrade pre-check operation fails during check-in. You can change the administrator password for VMware Aria Operations within the VMware Aria Suite Lifecycle UI and then run the VMware Aria Operations pre-check option again. You can also change the VMware Aria Operations administrator password outside of VMware Aria Suite Lifecycle directly in VMware Aria Operations and then run an inventory sync for the selected VMware Aria Operations instance in the VMware Aria Suite Lifecycle UI. In either scenario, you can click **Run upgrade Precheck** for VMware Aria Operations again.

Upgrade VMware Aria Operations for Networks

You can run a pre-validation check from the product UI before upgrading VMware Aria Operations for Networks within an environment. You can also evaluate VMware Aria Operations for Networks upgrades and perform the upgrade operation later.

Procedure

- 1 On the **Lifecycle Operations** page, click **Manage Environments**.
- 2 Right-click the vertical ellipses of an existing VMware Aria Operations for Networks product and select **Upgrade**.

The compatibility matrix information is displayed with new, compatible, and incompatible versions of products that need to be upgraded.

- 3 In the **Product details** section, select the repository type.

Repository type	Description
Repository URL	When you select this option, you can manually add the local upgrade file location in the VMware Aria Suite Lifecycle virtual appliance.
VMware Aria Suite Lifecycle Repository	When you select this option, you can enter the upgrade path available after mapping the binaries through VMware Aria Suite Lifecycle.

- 4 Click **Next**.
- 5 Click **RUN PRECHECK** to run the file format and then click **Version support from VMware Aria Suite Lifecycle**.

When the pre-check validation is finished, download the report to view the checks and validation status.

Note If you want to run the pre-check again after evaluating the discrepancies, you can select the **Re-Run Pre Check**. You can also re-run the pre-check by using the **Submit** toggle button.

Upgrade VMware Aria Operations for Logs

You can run a pre-validation check from the product UI before upgrading VMware Aria Operations for Logs within an environment. You can evaluate VMware Aria Operations for Logs upgrades and allow upgrade operation later. You can also validate the product compatibility matrix.

Prerequisites

Verify that there is an older or existing version of VMware Aria Operations for Logs instance in the **Manage Environments** section on the page.

Procedure

- 1 On the **Lifecycle Operations** page, click **Manage Environments**.

- 2 Right-click the vertical ellipses of an existing VMware Aria Operations for Logs product and select **Upgrade**.

The compatibility matrix information is displayed with new, compatible and incompatible versions of the products that need to be upgraded.

- 3 In the **Product details** section, select the repository type.

Repository type	Description
Repository URL	When you select this option, you can manually add the local upgrade file location in the VMware Aria Suite Lifecycle virtual appliance.
VMware Aria Suite Lifecycle Repository	When you select this option, you can select the upgrade path available after mapping the binaries through VMware Aria Suite Lifecycle.

- 4 Click **Next**.

- 5 Click **RUN PRECHECK**.

When the pre-check validation is finished, download the report to view the checks and validation status.

Note If you want to run the pre-check again after evaluating the discrepancies, you can select **Re-Run Pre Check**. You can also re-run the pre-check by using the **Submit** toggle button.

Upgrade VMware Aria Automation Config

You can run a pre-validation check from the product UI before upgrading VMware Aria Automation Config within an environment. You can also evaluate VMware Aria Automation Config upgrades and allow upgrade operations later.

Prerequisites

Note If you have multiple tenants, you can upgrade only one tenant at a time.

Verify that there is an older or legacy or existing version of VMware Aria Automation Config in the **Manage Environments** section on the page.

Procedure

- 1 On the **Lifecycle Operations** page, click **Manage Environments**.
- 2 On the **Environments** page, select VMware Aria Automation Config, and then click **Upgrade**.
- 3 Click **Proceed** to continue with the upgrade.

- 4 In the **Select Version** section, select a repository type.

Repository type	Description
VMware Aria Suite LifecycleRepository	When you select this option, you can select the upgrade path available after mapping the binaries by using options in the VMware Aria Suite Lifecycle.
Repository URL	When you select this option, you can manually add the local upgrade file location in the VMware Aria Suite Lifecycle virtual appliance.

- 5 Click **Next**.
- 6 On the **Precheck** page, view the validation status. Click the **RE-RUN PRECHECK** button to evaluate any discrepancies.
- 7 Click **Next** to view the upgrade summary.
- 8 Click **Submit**.

What to do next

There may be additional steps required to fully complete the VMware Aria Automation Config upgrade.

Performing a disaster recovery for VMware Aria Suite Lifecycle

7

You can perform disaster recovery by running a recovery plan in VMware Aria Suite Lifecycle with re-IP by using Site Recovery Manager.

Procedure

- 1 Create a recovery plan for VMware Aria Suite Lifecycle VM and configure the recovery steps by turning off re-IP manually, and then disabling power on post recovery.
- 2 Edit the hardware setting of the recovered VMware Aria Suite Lifecycle VM in the vCenter inventory, and then assign correct network.
- 3 Power ON the VMware Aria Suite Lifecycle VM.
- 4 Access the VMware Aria Suite Lifecycle VM console from vCenter inventory as a `root` user.
- 5 Execute the following commands from the VM console.

a `/opt/vmware/share/vami/vami_set_network <Network-Interface-Name>
STATICV4+NONEV6 <New-IPv4> <SUBNETMASK> <DEFAULT-GATEWAY>`

b `/opt/vmware/share/vami/vami_set_dns <New-DNS-IP-OR-FQDN>`

c `/opt/vmware/share/vami/vami_set_hostname <New-Hostname>`

d Reboot.

- 6 Access the VMware Aria Suite Lifecycle UI with the new IPv4 or the new FQDN, and then log in. Under **Locker**, select **Home Certificates**, and then generate a new certificate, which includes the updated VMware Aria Suite Lifecycle FQDN.
- 7 On the **Lifecycle Operations** Home page, select **Settings**, and then select **Change Certificate** to update the VMware Aria Suite Lifecycle certificate that is generated in the previous step.
- 8 On the **Lifecycle Operations** Home page, select **Settings**, and then select **Authentication Provider** to perform **SYNC** and **RE-REGISTER** tasks. This upgrades the new FQDN of VMware Aria Suite Lifecycle in the VMware Workspace ONE Access catalog.

Note Perform this step only if the Workspace ONE Access is reachable to the network of the recovered VMware Aria Suite Lifecycle VM.

- 9 Perform an inventory sync with the managed products to ensure VMware Aria Suite Lifecycle is functional with the new network settings.

Managing product licenses in VMware Aria Suite Lifecycle by using the Locker service



You can centrally manage your VMware Aria Suite subscription licenses, along with other on-premises licenses, from the VMware Aria Suite Lifecycle Locker service.

For related information, see [Create a hybrid environment using a cloud proxy in VMware Aria Suite Lifecycle](#).

To learn more about VMware Aria Suite, see the [VMware Aria Suite Documentation](#) page.

Read the following topics next:

- [Managing VMware Aria Universal Suite licenses in the VMware Aria Suite Lifecycle Locker](#)
- [Activating VMware Aria Universal Suite licenses](#)
- [Day 2 operations for VMware Aria Universal Suite](#)
- [Day 2 operations for VMware Aria Universal Suite licenses](#)

Managing VMware Aria Universal Suite licenses in the VMware Aria Suite Lifecycle Locker

The Locker service within VMware Aria Suite Lifecycle helps you to manage VMware Aria Universal Suite licenses for your VMware Aria Universal Suite subscription and collect daily data usage data for associated products and services.

When you purchase VMware Aria Universal Suite subscription, you receive access to VMware Aria Subscription, which is a complimentary utility service. With VMware Aria Subscription, you can add endpoints and monitor the data usage for your VMware Aria Universal Suite subscription services.

You must create VMware Aria Universal Suite licenses at the Locker level in VMware Aria Suite Lifecycle, and then connect these licenses to VMware Aria Subscription to monitor your cloud data usage.

For more information about VMware Aria Subscription, refer to the [product documentation](#).

Prerequisites

Verify that you have registered with [VMware Customer Connect](#) (previously My VMware) to access licenses.

Procedure

- 1 If you do not have My VMware account, navigate to the VMware Aria Operations for Integrations dashboard, and then click **Settings**.
- 2 Click **My VMware** and add a VMware Aria Automation cloud account.
- 3 After your My VMware accounts are configured, then the corresponding license keys are synced.
- 4 From the VMware Aria Suite Lifecycle dashboard, click **Locker**.
- 5 Click the **License** icon. The VMware Aria Universal Suite licenses are created under My VMware account and are displayed in the licenses table.
- 6 To re-sync licenses from My VMware account, click **Retrieve Licenses**.
- 7 If you already have products deployed, then import these products in VMware Aria Suite Lifecycle, and then apply the VMware Aria Universal Suite licenses to these products captured in locker. If there are no existing products present, then you can use the VMware Aria Universal Suite licenses present in VMware Aria Suite Lifecycle locker for product deployment. For more information, see [Manage licenses for a VMware Aria Suite Lifecycle products](#) .
- 8 If you have already downloaded your license, you can add the license details in the locker.
- 9 To connect a license to VMware Aria Universal Suite subscription, select a license which is displayed in the license table, and then right-click the vertical ellipses.
 - a Click **Connect License**.
 - b Under API Token, generate an API token from your user account for VMware Aria Universal Suite subscription, and then click **Next**.
 - c Under **Match License Key**, the VMware Aria Subscription finds a correct match for the provided API token, and lists out the organization details.
 - d Under Report Frequency, you will receive a confirmation that you are connected to VMware Aria Subscription, and your data usage is reported to VMware Aria Subscription twice a day.
 - e Click **Finish**.
- 10 To disconnect a license in VMware Aria Suite Lifecycle, right-click the vertical ellipses, and then click **Disconnect License**.
- 11 To trigger the license usage for a product, select a license from the license table, and then right-click the vertical ellipses.
 - a Click **Sync Usage**.
 - b You can download the usage sync report to view the data usage for the products.

- 12 To view the data consumption report, select a license, and then right-click the vertical ellipses.
 - a Click **Generate Report**.
 - b To view a graphical representation of the report, click **GENERATE** on the **Generate Report** page.
 - c To download the report for a maximum period of 120 days, click **DOWNLOAD**.

Downloading usage report for VMware Aria Universal Suite licenses

VMware Aria Suite Lifecycle provides options for examining available VMware Aria Universal Suite licenses.

The usage report enables you to download and view your license reports. When you right-click the vertical ellipsis, you can view the usage report and the **Update Usage Key** options.

- The **General** option on the **Download Report** tab enables you to download reports for viewing, analyzing, storing, or auditing purposes.

The VMware Aria Subscription billing option enables you to download an encrypted usage data zip file and generate a usage key. For more information, see [VMware vRealize Cloud Subscription Manager](#) documentation.

You can use this usage key in VMware Aria Suite Lifecycle to update the VMware Aria Subscription usage key option. Once your usage key is updated, you can generate the license usage report for the last uploaded date to the current date.

- The **View Usage** tab displays usage details for a particular license.

Activating VMware Aria Universal Suite licenses

In the VMware Aria Universal Suite page, you must activate your VMware Aria Universal Suite subscription licenses. After you activate your licenses, you can perform the available license actions.

Procedure

- 1 To activate a VMware Aria Universal Suite subscription license, navigate to the **VMware Aria Cloud** dashboard, and then click **Cloud Universal**.
- 2 Click **Activate Subscription License**.
- 3 Select the check box to confirm that the VMware Aria Suite products are on the required patches to proceed.
- 4 Select the plus (+) sign to add the license key details, and then click **Validate**. After the license key is validated, click **ADD**. Click **Next**.

Note The license key must be a VMware Aria Universal Suite subscription. When you add a new license, you can view the license key in the VMware Aria Suite Lifecycle Locker service.

- 5 Select the **Product Type** and the **Version** values.
- 6 Enter the **FQDN/IP Address** value.
- 7 Based on the selected product, you can select **Admin Password** or **Root Password**.
- 8 Select the check box to remove all the perpetual licenses from the selected product, if required.
- 9 Click **Validate & Add**. When the validation is complete, click **Next**.
- 10 In the **Cloud Connection Details** page, you have two options.
 - Automatically send subscription license consumption from your on-premises to VMware Aria Universal Suite. This check box allows you to send subscriptions to VMware Aria Subscription. If you select this check box, enter the **API Token** details.
 - Use VMware Aria Subscription subscription licenses with perpetual licenses. If you select this check box, enter your **Associated MyVMware Account** details.
 - If you select both the check boxes, you must enter the **Network Proxy** details.
- 11 Click **Next**.
- 12 Validate the details on the **Summary** page and then click **Finish**.

What to do next

You can track the request details on the **Requests** tab.

Day 2 operations for VMware Aria Universal Suite

You can perform Day 2 operations in VMware Aria Universal Suite.

Day 2 Operations	Function
Delete	The Delete option removes the selected entry from the VMware Aria Universal Suite page, but does not delete the product.
Update Password	The Update Password option updates the VMware Aria Suite Lifecycle inventory.
Inventory Sync	The Inventory Sync option helps to sync with the product and retrieve the latest license details.
Add/Replace License	The Add/Replace License option helps to select a new license and remove existing licenses.

Day 2 operations for VMware Aria Universal Suite licenses

You can perform Day 2 operations within VMware Aria Universal Suite.

Day 2 Operations	Function
Connect License to Cloud	<ol style="list-style-type: none"> 1 Connect your VMware Aria Universal Suite subscription license to a VMware organization. 2 Add the license key and the correct API token. 3 The license key would be connected to the organization where the subscription is redeemed.
Disconnect License to Cloud	Disconnect the license key from the VMware Aria Universal Suite subscription.
Usage Bundle Download	<ol style="list-style-type: none"> 1 Select the license key and purpose. 2 Click Download.
Sync Usage	<ol style="list-style-type: none"> 1 Provide the license key and sync usage. 2 Click Sync Usage. 3 You can view the sync usage for all the products.
Update License Key	<ol style="list-style-type: none"> 1 Select the license key from the Usage Bundle Download option. 2 Select the purpose. 3 Click Download.

Troubleshooting VMware Aria Suite Lifecycle

9

VMware Aria Suite Lifecycle troubleshooting topics provide solutions to problems you might experience installing and managing VMware Aria Suite with VMware Aria Suite Lifecycle.

- [Large VMware Aria Operations machine fails to power on](#)
Large VMware Aria Operations virtual machines fails to power on due to resource limitations.
- [Deployment fails during VMware Aria Operations for Logs clustering and VMware Workspace ONE Access registration](#)
Environment deployment fails during the Adding vIDM user as vRLI Super Admin task while running vRLI Clustering and vIDM Registration.
- [Change in DNS server](#)
If there is a change in the DNS server, you can update the VMware Aria Suite Lifecycle appliance DNS settings.
- [Wrong IP details specified during VMware Aria Suite Lifecycle deployment](#)
If you have given an incorrect IP address or if you want to upgrade an existing IP address during VMware Aria Suite Lifecycle deployment, follow the steps provided in this section.
- [Binary mappings are not populated](#)
Even if the requests for each product binary are marked as completed, the binary mappings are not populated.
- [Content capture fails with secure field](#)
A VMware Aria Automation content with a secure field corrupts the field on the target environment on successful deploy.
- [Fix errors using log files](#)
VMware Aria Suite Lifecycle log files are present under the following locations for trouble shooting any issues.
- [Cloud template capture fails](#)
The captured cloud template fails after the property group is deleted.

- [Component profile deployment fails](#)

When the component profiles are released to VMware Aria Automation, the values for the text boxes **Clone from** and **Clone from snapshot** are not assigned automatically.

- [Update VMware Aria Suite Lifecycle host name](#)

If you provide an incorrect host name or if you want to change the host name of VMware Aria Suite Lifecycle after deployment, follow the steps provided in this section.

- [Resource not found in directory management](#)

The system shows an error message in Directory Management.

- [Capture, test, or release fails in VMware Aria Automation Orchestrator content](#)

Capturing, testing, or releasing VMware Aria Automation Orchestrator content may fail due to VMware Aria Automation Orchestrator database related operations.

- [Import or inventory sync of VMware Aria Suite fails](#)

The import or inventory sync of VMware Aria Suite product fails with an error message.

- [Workspace ONE Access Day 2 operations fail when the root password expires](#)

VMware Workspace ONE Access Day 2 operations such as upgrade or root password update fails when the Workspace ONE Access root password expires.

- [Enable log rotation for pgpool logs on postgres clustered VMware Workspace ONE Access](#)

You can enable log rotation for `pgpool` logs on postgres clustered VMware Workspace ONE Access installed using VMware Aria Suite Lifecycle.

- [VMware Workspace ONE Access postgres cluster outage due to loss of delegate IP](#)

Troubleshooting VMware Workspace ONE Access postgres cluster outage deployed through VMware Aria Suite Lifecycle.

- [Importing VMware Aria Automation in VMware Aria Suite Lifecycle fails](#)

When importing VMware Aria Automation in VMware Aria Suite Lifecycle, the import fails with an error message.

- [VMware Aria Suite Lifecycle displays older version after upgrade](#)

VMware Aria Suite Lifecycle displays an older version after a successful upgrade.

- [Disconnected licenses are not listed for reconnect](#)

You disconnect a connected license in VMware Aria Universal Suite and are then unable to reconnect it.

Large VMware Aria Operations machine fails to power on

Large VMware Aria Operations virtual machines fails to power on due to resource limitations.

Problem

When you deploy VMware Aria Operations in VMware Aria Suite Lifecycle, by selecting node size as large and if you have budgeted resources for a different size virtual machine, the virtual machine might fail to power on due to resource limitations.

Cause

VMware Aria Operations deployment size set in VMware Aria Suite Lifecycle is based on the number of virtual machines, catalog items, concurrent provisions, and other workload metrics for your VMware Aria Operations environment. Virtual machine size is unrelated to deployment size.

Solution

VMware Aria Operations virtual machines deployed from VMware Aria Suite Lifecycle have a large (16 vCPU and 48 GB RAM) virtual machine size, if deployed with large size, and require sufficient vCPU and RAM to power on successfully.

Deployment fails during VMware Aria Operations for Logs clustering and VMware Workspace ONE Access registration

Environment deployment fails during the Adding vIDM user as vRLI Super Admin task while running vRLI Clustering and vIDM Registration.

Problem

Even after you multiple deployment operation, environment deployment fails during the Adding vIDM user as vRLI Super Admin task while running vRLI Clustering and vIDM Registration.

The following error message appears in the logs:

```
{"errorMessage":"Unable to retrieve information about this user from VMware Identity Manager.","errorCode":"RBAC_USERS_ERROR","errorDetails":{"errorCode":"com.vmware.loginsight.api.errors.rbac.invalid_vidm_user"}}
```

Solution

- 1 Add the VMware Workspace ONE Access Suite Administrator user to VMware Aria Operations for Logs by using the VMware Aria Operations for Logs UI.
See [Create a New User Account in Aria Log Insight](#).
- 2 Remove the VMware Workspace ONE Access Suite Administrator user from VMware Aria Operations for Logs by using the VMware Aria Operations for Logs UI.
- 3 Retry the environment deployment in VMware Aria Suite Lifecycle.

Change in DNS server

If there is a change in the DNS server, you can update the VMware Aria Suite Lifecycle appliance DNS settings.

Cause

When a DNS server provided during deployment gets changed, then follow these steps to update the DNS settings of VMware Aria Suite Lifecycle.

Solution

- 1 SSH to VMware Aria Suite Lifecycle appliance using root user.
- 2 Update the DNS setting using the command:

```
/opt/vmware/share/vami/vami_set_dns
vami_set_dns [-d <domain>] [ -s <searchpath>] DNS_Server_1 [DNS_Server_2]
```

For example: `/opt/vmware/share/vami/vami_set_dns -d sqa.local -s sqa.local 10.1.1.25`

- 3 Power off the VMware Aria Suite Lifecycle virtual appliance.
- 4 Select the VMware Aria Suite Lifecycle virtual appliance from vCenter and then select **Configure**.
- 5 Select **vApp Options**.
- 6 Under Properties, specify the following command:

```
vami.DNS.VMware_vRealize_Suite_Life_Cycle_Manager_Appliance
```

- 7 Power ON the VMware Aria Suite Lifecycle virtual appliance.
- 8 Verify the new DNS entry by running the `resolvectl status`, and then verify the DNS server.

Wrong IP details specified during VMware Aria Suite Lifecycle deployment

If you have given an incorrect IP address or if you want to upgrade an existing IP address during VMware Aria Suite Lifecycle deployment, follow the steps provided in this section.

Cause

You have given an incorrect IP address while deploying VMware Aria Suite Lifecycle.

Solution

- 1 SSH to the VMware Aria Suite Lifecycle appliance using root user credentials.

2 Update the IP address by using the below command:

```
vami_set_network <interface> (STATICV4|STATICV4+DHCPV6|STATICV4+AUTOV6) <ipv4_addr>
<netmask> <gatewayv4> For example: /opt/vmware/share/vami/vami_set_network eth0
STATICV4 192.168.1.150 255.255.255.0 192.168.1.1
```

Binary mappings are not populated

Even if the requests for each product binary are marked as completed, the binary mappings are not populated.

Problem

When you navigate from **Home > Settings > Product Binaries**, the corresponding request is marked as COMPLETED in the **Requests** page but the binary mappings are not populated.

Cause

The checksum for the target product binary cannot be same as the one published by VMware.

Solution

- ◆ Ensure that the binaries are not corrupted or modified and their SHA256 checksum is the same as mentioned in MyVMware portal.

Content capture fails with secure field

A VMware Aria Automation content with a secure field corrupts the field on the target environment on successful deploy.

Cause

In VMware Aria Suite Lifecycle, the secure field is captured as encrypted from the source environment and the value cannot be decrypted when deployed.

Solution

- ◆ After you successfully deploy, log in to the target VMware Aria Automation and manually update the secure fields in the content.

Fix errors using log files

VMware Aria Suite Lifecycle log files are present under the following locations for trouble shooting any issues.

Solution

- 1 The service layer log is available at `/var/log/vr1cm`. The log file name is `vr1cm-xserver.log`.

- 2 The engine log is available at `/var/log/vrlcm`. The log file name is `vrlcm-server.log`.

Cloud template capture fails

The captured cloud template fails after the property group is deleted.

Problem

When a VMware Aria Automation composite cloud template references property definitions or property groups, if those properties are deleted, the cloud template must be updated in VMware Aria Automation or the VMware Aria Suite Lifecycle capture fails.

Solution

- 1 Edit the VMware Aria Automation cloud template.
- 2 Using the **Properties** tab, select **custom properties** tab and click **OK**.
- 3 Select each of the needed components in the cloud template and select the **Properties** tab.
- 4 Click **Save**.
- 5 Click **Finish**.

Component profile deployment fails

When the component profiles are released to VMware Aria Automation, the values for the text boxes **Clone from** and **Clone from snapshot** are not assigned automatically.

Problem

When deploying an **Image Component Profile** the **Clone From** value of the component profile is removed. The **Clone From** text boxes are empty on the target system.

Solution

- ◆ You can manually edit the component profile and the respective values from a drop-down menu.

Note When you capture and release a component profile of VMware Aria Automation using VMware Aria Suite Lifecycle, the name of component profile should start with ValueSet.

Update VMware Aria Suite Lifecycle host name

If you provide an incorrect host name or if you want to change the host name of VMware Aria Suite Lifecycle after deployment, follow the steps provided in this section.

Cause

You want to update the host name of VMware Aria Suite Lifecycle.

Solution

- 1 Use the Secure Shell (SSH) to access VMware Aria Suite Lifecycle appliance using the root user privileges.
- 2 Update the host name using the following commands:


```
rm/opt/vmware/etc/vami/flags/vami_setnetwork
/opt/vmware/share/vami/vami_set_hostname new-hostname
```
- 3 Reboot the VMware Aria Suite Lifecycle appliance.
- 4 Update the VMware Aria Suite Lifecycle certificate under **Settings** in VMware Aria Suite Lifecycle.
- 5 Close the VMware Aria Suite Lifecycle appliance.
- 6 Locate the virtual machine in vCenter.
- 7 Select Configure, and then select **vApp Options**.
- 8 Select `vami.hostname`, set the value, and then update the value to the new host name.
- 9 Power ON the virtual machine, and then change the host name using the following command:


```
/opt/vmware/share/vami/vami_config_net
```
- 10 Reboot the VMware Aria Suite Lifecycle appliance.

Resource not found in directory management

The system shows an error message in Directory Management.

Problem

When you view or edit the directory in Directory Management, the system displays an error message and cannot retrieve the required information from VMware Workspace ONE Access.

Cause

The directory is partially created or the directory configuration is incomplete.

Solution

- 1 Log in to VMware Workspace ONE Access. Verify the directory configuration, and confirm if the directory is associated with a connector. Also, validate the bind password.
- 2 If the directory configuration is incomplete, you can configure it in VMware Workspace ONE Access. You can also use VMware Aria Suite Lifecycle to remove the directory using the delete functionality, provide correct configuration details, and then add back the directory.

Solution

Note Any role assigned to the directory user in VMware Aria Suite Lifecycle must be deleted and reassigned after the directory is added back.

Capture, test, or release fails in VMware Aria Automation Orchestrator content

Capturing, testing, or releasing VMware Aria Automation Orchestrator content may fail due to VMware Aria Automation Orchestrator database related operations.

Cause

When capturing, testing, or releasing VMware Aria Automation Orchestrator content, the VMware Aria Automation Orchestrator elements may fail on the endpoint when creating content.

Solution

Inspect the VMware Aria Automation Orchestrator logs and identify the element causing the failure. Delete the respective element from VMware Aria Automation Orchestrator and retry.

Import or inventory sync of VMware Aria Suite fails

The import or inventory sync of VMware Aria Suite product fails with an error message.

Cause

When the `keyUsage` setting does not have the `digitalSignature` attribute in the HTTPS certificate of the target product, the import or inventory sync of the VMware Aria Suite product fails with an error message.

Solution

Perform the following steps:

- 1 Click the padlock icon in the address bar of a supported web browser (Chrome, Edge, or Firefox) and then click **Certificate**.
- 2 Click **Details** and then click **Key Usage**.
- 3 Verify that the `digitalSignature` attribute is present in the `keyUsage` setting. If the `digitalSignature` attribute is not present, replace the certificate on the target product with a certificate that has the `digitalSignature` attribute present in `keyUsage` setting.

Workspace ONE Access Day 2 operations fail when the root password expires

VMware Workspace ONE Access Day 2 operations such as upgrade or root password update fails when the Workspace ONE Access root password expires.

Solution

- 1 Login to the virtual appliance console of Workspace ONE Access in vCenter.
- 2 Update the root password of the Workspace ONE Access virtual appliance.
- 3 Login to VMware Aria Suite Lifecycle and run the inventory sync of Workspace ONE Access. Update the Workspace ONE Access root password when retrying a failed inventory sync request.
- 4 Initiate the Workspace ONE Access Day 2 operation.

Enable log rotation for pgpool logs on postgres clustered VMware Workspace ONE Access

You can enable log rotation for `pgpool` logs on postgres clustered VMware Workspace ONE Access installed using VMware Aria Suite Lifecycle.

Problem

The combined disk usage shown with `du -hsc /var/log/pgService/pgService*` is more than 50 percent of total disk capacity of `/dev/sda4` as indicated in the output of the command `df -h`.

Solution

- 1 When running the command `find /etc/logrotate.d -iname pgserviceLog`, if the response is `/etc/logrotate.d/pgserviceLog`, then run the following commands:
 - a `touch /etc/cron.d/rotatePgserviceLogs`
 - b `echo "*/45 * * * * root /usr/sbin/logrotate /etc/logrotate.d/pgserviceLog" > /etc/cron.d/rotatePgserviceLogs`
 - c For VMware Workspace ONE Access 3.3.2: `/etc/init.d/cron restart`
For VMware Workspace ONE Access 3.3.3 or later: `systemctl restart crond`
- 2 When running the command `find /etc/logrotate.d -iname pgserviceLog`, if there is no response, then run the following commands:
 - a `touch /etc/cron.d/rotatePgserviceLogs`
 - b `touch /etc/logrotate.d/pgserviceLog`
 - c `echo "/var/log/pgService/pgService.log {
copytruncate`

```

rotate 6

compress

missingok

size 50M

}" > /etc/logrotate.d/pgservicelog

d echo "*/45 * * * * root /usr/sbin/logrotate /etc/logrotate.d/
pgservicelog" > /etc/cron.d/rotatePgserviceLogs

e For VMware Workspace ONE Access 3.3.2: /etc/init.d/cron restart

For VMware Workspace ONE Access 3.3.3 or later: systemctl restart crond

```

VMware Workspace ONE Access postgres cluster outage due to loss of delegate IP

Troubleshooting VMware Workspace ONE Access postgres cluster outage deployed through VMware Aria Suite Lifecycle.

Problem

VMware Workspace ONE Access cluster health status displays as `CRITICAL` in VMware Aria Suite Lifecycle Health Notification due to network loss in the VMware Workspace ONE Access appliance.

Cause

Network loss on the postgres cluster primary node. For `/usr/local/bin/pcp_watchdog_info -p 9898 -h localhost -U pgpool` command, it would prompt for a password. If `/usr/local/etc/pgpool.pwd` file is present on the VMware Workspace ONE Access node, that would contain the password. If the password is not available, use the default password `password`.

Command parameters help are shown below:

`-h` : The host against which the command is run is `localhost`.

`-p` : The port on which `pgpool` accepts connections is `9898`.

`-U` : The `pgpool` health check and replication delay check user is `pgpool`.

There must be an expected response, such as one of the following:

```

3 YES <Host1>:9999 Linux <Host1> <Host1>

<Host1>:9999 Linux <Host1> <Host1> 9999 9000 4 MASTER

<Host2>:9999 Linux <Host2> <Host2> 9999 9000 7 STANDBY

<Host3>:9999 Linux <Host3> <Host3> 9999 9000 7 STANDBY

```

The response must contain a `MASTER` node and 2 `STANDBY` nodes. If any of the node's status is `SHUTDOWN` or the command execution is struck, resolve the issue as specified in the following Solutions section.

Solution

- 1 Bring down the services on VMware Workspace ONE Access nodes. Refer to KB [78815](#) for the required steps.
- 2 Power OFF the VMware Workspace ONE Access appliances in vCenter.
- 3 Power ON the VMware Workspace ONE Access nodes through VMware Aria Suite Lifecycle.

Importing VMware Aria Automation in VMware Aria Suite Lifecycle fails

When importing VMware Aria Automation in VMware Aria Suite Lifecycle, the import fails with an error message.

Problem

If the details of VMware Workspace ONE Access fails to match with VMware Aria Automation, when importing VMware Aria Automation in VMware Aria Suite Lifecycle, you may see the following error message.

```
Error Code: LCMVRAVACONFIG590026
```

```
vRealize Automation Import failed due to VMware Identity Manager details in vRealize Suite Lifecycle Manager not matching with the provided vRealize Automation. Please retry by providing vRealize Automation which has VMware Identity Manager details same as vRSLCM VMware Identity Manager details.
```

```
vRA vIDM details mismatch. vRA Import is supported only if vRSLCM vIDM is matched with vRA vIDM details.
```

Cause

The VMware Workspace ONE Access imported into VMware Aria Suite Lifecycle does not match the VMware Aria Automation host that was attempting to import.

More information about this issue is available in [KB 82234](#).

Solution

- 1 Delete `globalenvironment` from VMware Aria Suite Lifecycle.
- 2 Import VMware Workspace ONE Access which is associated with the VMware Aria Automation host.
- 3 Create a new request to import VMware Aria Automation.

VMware Aria Suite Lifecycle displays older version after upgrade

VMware Aria Suite Lifecycle displays an older version after a successful upgrade.

Problem

When you upgrade VMware Aria Suite Lifecycle from version *x* to version *y*, VMware Aria Suite Lifecycle may incorrectly display version *x* after a successful upgrade.

Cause

This behaviour occurs when the component that performs the upgrade (VAMI) fails to properly update a manifest file in VMware Aria Suite Lifecycle.

Solution

No action on your part is required. When the VAMI fails to properly update the version value in the manifest file, it automatically schedules a job that performs this operation in the next 12 hour cycle.

Disconnected licenses are not listed for reconnect

You disconnect a connected license in VMware Aria Universal Suite and are then unable to reconnect it.

Problem

If you select **License Actions > Disconnect License to Cloud** and then disconnect a connected license, you cannot connect the same license in the **License Actions > Connect License to Cloud** menu sequence. The disconnected license key does not appear as a selectable option.

Solution

- 1 From the VMware Aria Operations dashboard, navigate to **Locker** and then select **Licenses**.
- 2 Select **Connect License** from the actions for the desired license key and then follow the steps provided in the wizard to connect the license key.