You can find the most up-to-date technical documentation on the VMware by Broadcom website at:
https://docs.vmware.com/
Contents

About the Getting Started with VMware Aria Operations Guide 5

1 About Installing 6
   Workflow of VMware Aria Operations Installation 6
   Sizing the Cluster 8
      Add Data Disk Space to a vApp Node 9
   Complexity of Your Environment 9
   Cluster Nodes 11
   About Remote Collector Nodes 13
   About High Availability 15
   About VMware Aria Operations Continuous Availability 17

2 Preparing for Installation 19
   Requirements 19
      Requirements for IPv6 19
      Cluster Requirements 20
      Sizing and Scaling Requirements 23

3 Installing VMware Aria Operations 24
   Deployment of VMware Aria Operations 24
      Create a Node by Deploying an OVF 24
   Installation Types 27
      Installing VMware Aria Operations for a New User 27
      Installing VMware Aria Operations as an Administrator 30
      Expand an Existing Installation of VMware Aria Operations 31
   Using VMware Aria Operations on-premises to Monitor VMware Cloud 33

4 Resize your Cluster by Adding Nodes 39
   Adding High Availability 40
      Run the Setup Wizard to Add a Primary Replica Node 40
   Adding Continuous Availability 41
      Activate Continuous Availability in VMware Aria Operations 41
   Cluster and Node Maintenance 42
      Cluster Management 45
   Troubleshooting 47
      Troubleshooting Cluster Problems 47

5 Post-Installation Considerations 49
About Logging In 49
Log In and Continue with a New Installation 50
After You Log In 51
Installing Cloud Proxy 55
Monitoring Multiple Cloud Accounts in VMware Aria Operations 55
Secure the Console 57
Log in to a Remote Console Session 58

6 Upgrade, Backup and Restore 59
Obtain the Software Update PAK File 59
Create a Snapshot as Part of an Update 60
How To Preserve Customized Content 61
Back Up and Restore 62
Software Updates 62
   Install a Software Update 64
Before Upgrading to VMware Aria Operations 8.12 66
   Running the VMware Aria Operations 8.12 Pre-Upgrade Readiness Assessment Tool 66
About the Getting Started with VMware Aria Operations Guide

The *Getting Started with VMware Aria Operations Guide* provides information about deploying the VMware® VMware Aria Operations virtual appliance, including how to create and configure the VMware Aria Operations cluster.

The VMware Aria Operations installation process consists of deploying the VMware Aria Operations virtual appliance once for each cluster node, and accessing the product to finish setting up the application.

Intended Audience

This information is intended for anyone who wants to install and configure VMware Aria Operations by using a virtual appliance deployment. The information is written for experienced virtual machine administrators who are familiar with enterprise management applications and data center operations.

For administrators who want to deploy the VMware Aria Operations virtual appliance programmatically, the VMware Aria Operations CaSA API documentation is available in HTML format and is installed with your VMware Aria Operations instance. For example, if the URL of your instance is `https://operations.example.com`, the API reference is available from `https://operations.example.com/casa/api-guide.html`.
About Installing

You prepare for VMware Aria Operations installation by evaluating your environment and deploying enough VMware Aria Operations cluster nodes to support how you want to use the product.

Read the following topics next:

- Workflow of VMware Aria Operations Installation
- Sizing the VMware Aria Operations Cluster
- Complexity of Your Environment
- About VMware Aria Operations Cluster Nodes
- About VMware Aria Operations Remote Collector Nodes
- About VMware Aria Operations High Availability
- About VMware Aria Operations Continuous Availability

Workflow of VMware Aria Operations Installation

The VMware Aria Operations virtual appliance installation process consists of deploying the VMware Aria Operations OVA, once for each cluster node, accessing the product to set up cluster nodes according to their role, and logging in to configure the installation.
To automate installation, configuration, upgrade, patch, configuration management, drift remediation and health from within a single pane of glass, you can use VMware Aria Suite Lifecycle Manager. If you are a new user, click here to install VMware Aria Suite Lifecycle Manager. This provides the IT Managers of Cloud admin resources to focus on business-critical initiatives, while improving time to value (TTV), reliability, and consistency.
You can also install upgrade VMware Aria Operations by using VMware Aria Suite Lifecycle Manager. For more information, see Create a new private cloud environment.

Sizing the VMware Aria Operations Cluster

The resources needed for VMware Aria Operations depend on how large of an environment you expect to monitor and analyze, how many metrics you plan to collect, and how long you need to store the data.

It is difficult to broadly predict the CPU, memory, and disk requirements that will meet the needs of a particular environment. There are many variables, such as the number and type of objects collected, which includes the number and type of adapters installed, the presence of HA, the duration of data retention, and the quantity of specific data points of interest, such as symptoms, changes, and so on.

VMware expects VMware Aria Operations sizing information to evolve, and maintains Knowledge Base articles so that sizing calculations can be adjusted to adapt to usage data and changes in versions of VMware Aria Operations.

Knowledge Base article 2093783

The Knowledge Base articles include overall maximums, plus spreadsheet calculators in which you enter the number of objects and metrics that you expect to monitor. To obtain the numbers, some users take the following high-level approach, which uses VMware Aria Operations itself.

1. Review this guide to understand how to deploy and configure a VMware Aria Operations node.
2. Deploy a temporary VMware Aria Operations node.
3. Configure one or more adapters, and allow the temporary node to collect overnight.
4. Access the Cluster Management page on the temporary node.
5. Using the Adapter Instances list in the lower portion of the display as a reference, enter object and metric totals of the different adapter types into the appropriate sizing spreadsheet from Knowledge Base article 2093783.
6. Deploy the VMware Aria Operations cluster based on the spreadsheet sizing recommendation. You can build the cluster by adding resources and data nodes to the temporary node or by starting over.

If you have a large number of adapters, you might need to reset and repeat the process on the temporary node until you have all the totals you need. The temporary node will not have enough capacity to simultaneously run every connection from a large enterprise.

Another approach to sizing is through self monitoring. Deploy the cluster based on your best estimate, but create an alert for when capacity falls below a threshold, one that allows enough time to add nodes or disk to the cluster. You also have the option to create an email notification when thresholds are passed.
During internal testing, a single-node vApp deployment of VMware Aria Operations that monitored 8,000 virtual machines ran out of disk storage within one week.

**Add Data Disk Space to a VMware Aria Operations vApp Node**

You add to the data disk of VMware Aria Operations vApp nodes when space for storing the collected data runs low.

**Prerequisites**

- Note the disk size of the analytics cluster nodes. When adding disk, you must maintain uniform size across analytics cluster nodes.
- Use the VMware Aria Operations administration interface to take the node offline.
- Verify that you are connected to a vCenter Server system with a vSphere Client, and log in to the vSphere Client.

**Procedure**

1. Shut down the virtual machine for the node.
2. Edit the hardware settings of the virtual machine, and add another disk.
   - **Note** Do not expand disks. VMware Aria Operations does not support expanding disks.
3. Power on the virtual machine for the node.

**Results**

During the power-on process, the virtual machine expands the VMware Aria Operations data partition.

**Complexity of Your Environment**

When you deploy VMware Aria Operations, the number and nature of the objects that you want to monitor might be complex enough to recommend a Professional Services engagement.

**Complexity Levels**

Every enterprise is different in terms of the systems that are present and the level of experience of deployment personnel. The following table presents a color-coded guide to help you determine where you are on the complexity scale.

- **Green**
  - Your installation only includes conditions that most users can understand and work with, without assistance. Continue your deployment.
- **Yellow**
Your installation includes conditions that might justify help with your deployment, depending on your level of experience. Consult your account representative before proceeding, and discuss using Professional Services.

- **Red**

Your installation includes conditions that strongly recommend a Professional Services engagement. Consult your account representative before proceeding, and discuss using Professional Services.

Note that these color-coded levels are not firm rules. Your product experience, which increases as you work with VMware Aria Operations and in partnership with Professional Services, must be taken into account when deploying VMware Aria Operations.

### Table 1-1. Effect of Deployment Conditions on Complexity

<table>
<thead>
<tr>
<th>Complexity Level</th>
<th>Current or New Deployment Condition</th>
<th>Additional Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Green</strong></td>
<td>You run only one VMware Aria Operations deployment.</td>
<td>Lone instances are usually easy to create in VMware Aria Operations.</td>
</tr>
<tr>
<td><strong>Green</strong></td>
<td>Your deployment includes a management pack that is listed as Green according to the compatibility guide on the VMware Solutions Exchange Web site.</td>
<td>The compatibility guide indicates whether the supported management pack for VMware Aria Operations is a compatible 5.x one or a new one designed for this release. In some cases, both might work but produce different results. Regardless, users might need help in adjusting their configuration so that associated data, dashboards, alerts, and so on appear as expected. Note that the terms solution, management pack, adapter, and plug-in are used somewhat interchangeably.</td>
</tr>
<tr>
<td><strong>Yellow</strong></td>
<td>You run multiple instances of VMware Aria Operations.</td>
<td>Multiple instances are typically used to address scaling or operator use patterns.</td>
</tr>
<tr>
<td><strong>Yellow</strong></td>
<td>Your deployment includes a management pack that is listed as Yellow according to the compatibility guide on the VMware Solutions Exchange Web site.</td>
<td>The compatibility guide indicates whether the supported management pack for VMware Aria Operations is a compatible 5.x one or a new one designed for this release. In some cases, both might work but produce different results. Regardless, users might need help in adjusting their configuration so that associated data, dashboards, alerts, and so on appear as expected.</td>
</tr>
<tr>
<td><strong>Yellow</strong></td>
<td>You are deploying a multiple-node VMware Aria Operations cluster.</td>
<td>Multiple nodes are typically used for scaling out the monitoring capability of VMware Aria Operations.</td>
</tr>
<tr>
<td><strong>Yellow</strong></td>
<td>Your new VMware Aria Operations instance will include a Linux based deployment.</td>
<td>Linux deployments are not as common as vApp deployments and often need special consideration.</td>
</tr>
<tr>
<td>Complexity Level</td>
<td>Current or New Deployment Condition</td>
<td>Additional Notes</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Yellow</td>
<td>Your VMware Aria Operations instance will use high availability (HA).</td>
<td>High availability and its node failover capability is a unique multiple-node feature that you might want additional help in understanding.</td>
</tr>
<tr>
<td>Yellow</td>
<td>You want help in understanding the new or changed features in VMware Aria Operations and how to use them in your environment.</td>
<td>VMware Aria Operations is different than vCenter Operations Manager in areas such as policies, alerts, compliance, custom reporting, or badges. In addition, VMware Aria Operations uses one consolidated interface.</td>
</tr>
<tr>
<td>Red</td>
<td>You run multiple instances of VMware Aria Operations, where at least one includes virtual desktop infrastructure (VDI).</td>
<td>Multiple instances are typically used to address scaling, operator use patterns, or because separate VDI (V4V monitoring) and non-VDI instances are needed.</td>
</tr>
<tr>
<td>Red</td>
<td>Your deployment includes a management pack that is listed as Red according to the compatibility guide on the VMware Solutions Exchange Web site.</td>
<td>The compatibility guide indicates whether the supported management pack for VMware Aria Operations is a compatible 5.x one or a new one designed for this release. In some cases, both might work but produce different results. Regardless, users might need help in adjusting their configuration so that associated data, dashboards, alerts, and so on appear as expected.</td>
</tr>
<tr>
<td>Red</td>
<td>You are deploying multiple VMware Aria Operations clusters.</td>
<td>Multiple clusters are typically used to isolate business operations or functions.</td>
</tr>
<tr>
<td>Red</td>
<td>Your current VMware Aria Operations deployment required a Professional Services engagement to install it.</td>
<td>If your environment was complex enough to justify a Professional Services engagement in the previous version, it is possible that the same conditions still apply and might warrant a similar engagement for this version.</td>
</tr>
<tr>
<td>Red</td>
<td>Professional Services customized your VMware Aria Operations deployment. Examples of customization include special integrations, scripting, nonstandard configurations, multiple level alerting, or custom reporting.</td>
<td>If your environment was complex enough to justify a Professional Services engagement in the previous version, it is possible that the same conditions still apply and might warrant a similar engagement for this version.</td>
</tr>
</tbody>
</table>

**About VMware Aria Operations Cluster Nodes**

All VMware Aria Operations clusters consist of a primary node, an optional replica node for high availability or continuously availability, and optional data nodes.

When you install VMware Aria Operations, you use a VMware Aria Operations vApp deployment to create role-less nodes. After the nodes are created and have their names and IP addresses, you use an administration interface to configure them according to their role.
You can create role-less nodes all at once or as needed. A common as-needed practice might be to add nodes to scale out VMware Aria Operations to monitor an environment as the environment extends larger.

The following node types make up the VMware Aria Operations analytics cluster:

**Primary Node**

The primary node is the initial, required node in VMware Aria Operations. All other nodes are managed by the primary node.

In a single-node installation, the primary node manages itself, has adapters installed on it, and performs all data collection and analysis.

**Data Node**

In larger deployments, additional data nodes have adapters installed and perform collection and analysis.

Larger deployments usually include adapters only on the data nodes so that primary and replica node resources can be dedicated to cluster management.

**Replica Node**

To use VMware Aria Operations high availability (HA) and continuous availability (CA) the cluster requires that you convert a data node into a replica of the primary node.

The following node types are a member of the VMware Aria Operations cluster but not part of the analytics cluster:

**Remote Collector Node/**

Distributed deployments might require a remote collector node that can navigate firewalls, interface with a remote data source, reduce the bandwidth across data centers, or reduce the load on the VMware Aria Operations analytics cluster. Remote collectors only gather objects for the inventory, without storing data or performing analysis. In addition, remote collector nodes might be installed on a different operating system than the rest of the cluster.

**Witness Node**

To use VMware Aria Operations continuous availability (CA), the cluster requires that you have a witness node. Each VMware Aria Operations cluster can have only one witness node. If the network connection between the two fault domains is lost, the witness node acts as a decision maker regarding the availability of VMware Aria Operations.

**Note** Starting with version 8.10 of VMware Aria Operations, you cannot deploy new remote collectors. If you require a new agent to collect data, you must deploy a cloud proxy. For more information on how to deploy a cloud proxy, see Installing Cloud Proxy.
About VMware Aria Operations Remote Collector Nodes

A remote collector node is an additional cluster node that allows VMware Aria Operations to gather more objects into its inventory for monitoring purposes. Unlike the data nodes, the remote collector nodes only perform the collector role of VMware Aria Operations. These remote collectors do not store data or process any analytics functions. Remote collectors collect data from integrated objects and then forward the data back to the cluster nodes. The primary node then processes the data which you then view as reports and analytics.

A remote collector node is usually used to navigate firewalls, reduce bandwidth across data centers, connect to remote data sources, or reduce the load on the VMware Aria Operations analytics cluster.

Remote collectors do not buffer data while the network is experiencing a problem. If the connection between the remote collector and the analytics cluster is lost, the remote collector does not store data points that occur during that time. In turn, and after the connection is restored, VMware Aria Operations does not retroactively incorporate associated events from that time into any monitoring or analysis.

Note You cannot deploy new remote collectors VMware Aria Operations. If you require a new agent to collect data, you must deploy a cloud proxy. For more information on how to deploy a cloud proxy, see Installing Cloud Proxy.

Note Remote collectors are not supported by the Application Monitoring management pack.

Ports information for VMware Aria Operations is available on Ports and Protocol.

Monitoring the Health of Remote Collectors

After you upgrade your VMware Aria Operations cluster to version 8.10, you can view the status and health of your remote collectors from the Cloud Proxy page.

1 Log in to VMware Aria Operations.
2 From the left menu, click Data Sources > Cloud Proxy.

You can view the health of the remote collectors.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the remote collector.</td>
</tr>
<tr>
<td>IP</td>
<td>The IP address of the remote collector.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the remote collector. Once the remote collector is connected to VMware Aria Operations, the status shows as Online. If the remote collector is not connected to VMware Aria Operations the Offline status is displayed.</td>
</tr>
<tr>
<td>Version</td>
<td>The version used to install the cloud proxy.</td>
</tr>
</tbody>
</table>
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounts</td>
<td>The number of accounts that are created and associated with the remote collector.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays whether it's a remote collector or a cloud proxy.</td>
</tr>
<tr>
<td>Network Proxy Address</td>
<td>Not applicable for the remote collectors.</td>
</tr>
<tr>
<td>Network Proxy Port</td>
<td>Not applicable for the remote collectors.</td>
</tr>
<tr>
<td>Target</td>
<td>Displays the target location on which the remote collector is deployed.</td>
</tr>
<tr>
<td>Data Persistence</td>
<td>Not applicable for the remote collectors.</td>
</tr>
<tr>
<td>Time Estimation</td>
<td>Not applicable for the remote collectors.</td>
</tr>
</tbody>
</table>

#### Filter
Filters the list of remote collectors according to the following criteria:
- Name
- IP
- Version
- Accounts
- Network Proxy Address
- Network Proxy Port
- Target Location
- Data Persistence

### Table 1-2. Cloud Proxy Page Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy ID</td>
<td>ID of the remote collectors.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the remote collectors.</td>
</tr>
<tr>
<td>OVA Version</td>
<td>The OVA file version used to install the remote collectors.</td>
</tr>
<tr>
<td>Creation Date</td>
<td>Date of creation of the remote collectors.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the remote collectors.</td>
</tr>
<tr>
<td>Last Heartbeat</td>
<td>Last time stamp when VMware Aria Operations ran a Health Check for this remote collector. When you click a remote collector to view its details, VMware Aria Operations sends a heartbeat to check if the remote collector is still reachable.</td>
</tr>
<tr>
<td>CPU</td>
<td>CPU usage.</td>
</tr>
<tr>
<td>Memory</td>
<td>Memory usage.</td>
</tr>
</tbody>
</table>
4 Click the vertical ellipsis to rename or remove the remote collector.

5 View and monitor the health of the adapters using the remote collector.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The adapter type.</td>
</tr>
<tr>
<td>Creation Date</td>
<td>Date of creation of the adapters.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays if the adapter is sending data or not.</td>
</tr>
<tr>
<td>Last Sent Time</td>
<td>Last time stamp when the adapter sent data using the remote collectors.</td>
</tr>
<tr>
<td>Objects Collected</td>
<td>Total number of objects collected.</td>
</tr>
<tr>
<td>Metrics Collected</td>
<td>Total number of metrics collected.</td>
</tr>
</tbody>
</table>

About VMware Aria Operations High Availability

VMware Aria Operations supports high availability (HA). HA creates a replica for the VMware Aria Operations primary node and protects the analytics cluster against the loss of a node.

With HA, data stored in the primary node is always 100% backed up on the replica node. To activate HA, you must have at least one data node deployed, in addition to the primary node. If you have more than one data node, the data stored in the primary node can be stored and replicated in any of the other nodes. But in case the primary node fails, only the replica node can function as the replacement of the primary node.

- HA is not a disaster recovery mechanism. HA protects the analytics cluster against the loss of only one node, and because only one loss is supported, you cannot stretch nodes across vSphere clusters in an attempt to isolate nodes or build failure zones.

- When HA is activated, the replica can take over all functions that the primary provides, were the primary to fail for any reason. If the primary fails, failover to the replica is automatic and requires only two to three minutes of VMware Aria Operations downtime to resume operations and restart data collection.

When a primary node problem causes failover, the replica node becomes the primary node, and the cluster runs in degraded mode. To get out of degraded mode, take one of the following steps.

- Return to HA mode by correcting the problem with the primary node. When a primary node exits an HA-activated cluster, primary node does not rejoin with the cluster without manual intervention. Therefore, restart the VMware Aria Operations Analytics process on the downed node to change its role to replica and rejoin the cluster.

- Remove the failed primary node then re-activate HA by converting a data node into replica. Removed primary nodes cannot be repaired and readded to VMware Aria Operations.
Remove the old, failed primary node and then change to non-HA operation by deactivating HA. Removed primary nodes cannot be repaired and readded to VMware Aria Operations.

In the administration interface, after an HA replica node takes over and becomes the new primary node, you cannot remove the previous, offline primary node from the cluster. In addition, the previous node remains listed as a primary node. To refresh the display and activate removal of the node, refresh the browser.

When HA is activated, the cluster can survive the loss of one data node without losing any data. However, HA protects against the loss of only one node at a time, of any kind, so simultaneously losing data and primary/replica nodes, or two or more data nodes, is not supported. Instead, VMware Aria Operations HA provides additional application level data protection to ensure application level availability.

When HA is activated, it lowers VMware Aria Operations capacity and processing by half, because HA creates a redundant copy of data throughout the cluster, and the replica backup of the primary node. Consider your potential use of HA when planning the number and size of your VMware Aria Operations cluster nodes. See Sizing the VMware Aria Operations Cluster.

When HA is activated, deploy analytics cluster nodes on separate hosts for redundancy and isolation. One option is to use anti-affinity rules that keep nodes on specific hosts in the vSphere cluster.

If you cannot keep the nodes separate, you should not activate HA. A host fault might cause the loss of more than one node, which is not supported, and all of VMware Aria Operations can become unavailable.

The opposite is also true. Without HA, you can keep nodes on the same host, and it will not make a difference. Without HA, the loss of even one node can make all of VMware Aria Operations unavailable.

When you power off the data node and change the network settings of the VM, this affects the IP address of the data node. After this point, the HA cluster is no longer accessible and all the nodes have a status of "Waiting for analytics". Verify that you have used a static IP address.

When you remove a node that has one or more vCenter adapters configured to collect data from a HA-activated cluster, one or more vCenter adapters associated with that node stops collecting. You change the adapter configuration to pin them to another node before removing the node.

Administration UI shows the resource cache count, which is created for active objects only, but the Inventory displays all objects. Therefore, when you remove a node from a HA-activated cluster allowing the vCenter adapters collect data and rebalance each node, the Inventory displays a different quantity of objects from that shown in the Administration UI.
About VMware Aria Operations Continuous Availability

VMware Aria Operations supports continuous availability (CA). CA separates 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.

You can configure the analytics cluster with Continuous Availability. This allows the cluster nodes to be stretch across two fault-domains. A fault domain consists of one or more analytics nodes grouped according to their physical location in the data center. With CA, the two fault domains permit VMware Aria Operations to tolerate failures of an entire physical location and failures from resources dedicated to a single fault domain.

To activate continuous availability within VMware Aria Operations, the witness node must be deployed in the cluster. The VMware Aria Operations cluster can have only one witness node. The witness node does not collect nor store data. In a situation where network connectivity the two fault-domains is lost, the cluster would go into a split-brain situation. This situation is detected by the Witness Node and one of the fault domains will go offline to avoid data inconsistency issues. You will see a Bring Online button on the admin UI of the nodes which are made offline by the witness node. Before using this option to bring the fault domain online, ensure that the network connectivity between the nodes across the two fault domains is restored and stable. Once confirmed you can bring the fault domain online.

With CA, the data stored in the primary node and data nodes grouped in fault domain 1 is always 100% synced to the replica node and data nodes paired in fault domain 2. To activate CA, you must have at least one data node deployed, in addition to the primary node. If you have more than one data node, there must be an even number of data nodes including the primary node. For example, the cluster must have 2, 4, 6, 8, 10, 12, 14 or 16 nodes based on the appropriate sizing requirements. The data stored in the primary node in fault domain 1 is stored and replicated in the replica node in fault domain 2. The data stored in the data nodes in fault domain 1 is stored and replicated in the paired data nodes in fault domain 2. But in case the primary node fails, only the replica node can function as the replacement of the primary node.

- CA protects the analytics cluster against the loss of half the analytics nodes specific to one fault domain. You can stretch nodes across vSphere clusters in an attempt to isolate nodes or build failure zones.
- When CA is activated, the replica node can take over all functions that the primary node provides, in case of a primary node failure. The failover to the replica is automatic and requires only two to three minutes of VMware Aria Operations downtime to resume operations and restart data collection.

Note: In case of a primary node failure, the replica node becomes the primary node, and the cluster runs in degraded mode. To fix this, perform any one of the following actions.

- Correct the primary node failure manually.
- Return to CA mode by replacing the primary node. Replacement nodes do not repair the node failure, instead a new node assumes the primary node role.
In the administration interface, after a CA replica node takes over and becomes the new primary node, you cannot remove the previous, offline primary node from the cluster. In addition, the previous node remains listed as a primary node. To refresh the display and activate the removal of the node, refresh the browser.

When CA is activated, the cluster can survive the loss of half the data nodes, all in one fault domain, without losing any data. CA protects against the loss of only one fault domain at a time. Simultaneously losing data and primary/replica nodes, or two or more data nodes in both fault domains, is not supported.

A CA activated cluster will be non-functional if you power off the primary node or the primary node replica while one of the fault domains is down.

When CA is activated, it lowers the VMware Aria Operations capacity and processing by half, because CA creates a redundant copy of data throughout the cluster, and the replica backup of the primary node. Consider your potential use of CA when planning the number and size of your VMware Aria Operations cluster nodes. See Sizing the VMware Aria Operations Cluster.

When CA is activated, deploy analytics cluster nodes, in each fault domain, on separate hosts for redundancy and isolation. You can also use anti-affinity rules that keep nodes on specific hosts in the vSphere clusters.

If you cannot keep the nodes separate in each fault domain, you can still activate CA. A host fault might cause the loss of the data nodes in the fault domain, and VMware Aria Operations can still be available in the other fault domain.

If you cannot split the data nodes into different vSphere clusters, do not activate CA. A cluster failure can cause the loss of more than half of the data nodes, which is not supported, and all of vSphere might become unavailable.

Without CA, you can keep nodes on the same host in the same vSphere. Without CA, the loss of even one node might make all of VMware Aria Operations unavailable.

When you power off data nodes in both fault domains and change the network settings of the VMs, it affects the IP address of the data nodes. After this point, the CA cluster is no longer accessible and all the nodes status change to "Waiting for analytics". Verify that you have used a static IP address.

When you remove a node that has one or more vCenter adapters configured to collect data from a CA-activated cluster, one or more vCenter adapters associated with that node stops collecting. You must change the adapter configuration to pin them to another node before removing the node.

The administration interface displays the resource cache count, which is created for active objects only, but the inventory displays all objects. When you remove a node from a CA-activated cluster allowing the vCenter adapters to collect data and rebalance each node, the inventory displays a different quantity of objects from that shown in the administration interface.
Preparing for Installation

When you prepare for your installation, consider some of these best practices, cluster, sizing and scaling requirements.

Read the following topics next:

- **Requirements**

**Requirements**

You have to consider important requirements while creating nodes in a VMware Aria Operations.

**Using IPv6 with VMware Aria Operations**

VMware Aria Operations supports both, Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). All nodes in the cluster must follow the same protocol. For endpoint communications, you can use IPv4 or IPv6. If the environment only supports the IPv6 protocol, the **Prefer IPv6** flag must be activated during the OVF deployment for each node. If you set the **Prefer IPv6** flag, then VMware Aria Operations uses IPv6 for all communications.

**Considerations While Using IPv6**

- If any nodes use DHCP, your DHCP server must be configured to support IPv6.
- IPv6 DHCP or Static configuration must have Global Scope.
- DHCP is only supported on data nodes and remote collectors. Primary nodes and replica nodes require static addresses.
- Your DNS server must be configured to support IPv6.
- When adding nodes to the cluster, enter the IPv6 address of the primary node.
- When registering a VMware vCenter® instance within VMware Aria Operations, place square brackets around the IPv6 address of your VMware vCenter Server® system if vCenter is also using IPv6.

For example: [2015:0db8:85a3:0042:1000:8a2e:0360:7334]

**Note** When VMware Aria Operations is using IPv6, vCenter Server might still have an IPv4 address. In that case, VMware Aria Operations does not need the square brackets.
Cluster Requirements

When you create the cluster nodes that make up VMware Aria Operations, you have general requirements that you must meet.

General VMware Aria Operations Cluster Node Requirements

You have to follow some general requirements to create a node on your environment.

General Requirements

- **VMware Aria Operations version.** All nodes must run the same VMware Aria Operations version.
  
  For example, do not add a version 6.1 data node to a cluster of VMware Aria Operations 6.2 nodes.

- **Analytics Cluster Deployment Type.** In the analytics cluster, all nodes must be the same kind of deployment: vApp.

- **Witness Node Deployment Type.** The witness node must be the same vApp deployment.

- **Analytics Cluster Node Sizing.** In the analytics cluster, CPU, memory, and disk size must be identical for all nodes.
  
  Primary, replica, and data nodes must be uniform in sizing.

- **Witness Node Sizing.** The witness node has only one size and may be of different sizes from the uniform analytics cluster node size.

- **Geographical Proximity.** You may place analytics cluster nodes in different vSphere clusters, but the nodes must reside in the same geographical location.
  
  Different geographical locations are not supported.

- **Witness Node Placement.** You may place the witness node in a different vSphere cluster separate from the analytics nodes.

  **Note** A VMware Aria Operations cluster can have only one witness node.

- **Virtual Machine Maintenance.** When any node is a virtual machine, you may only update the virtual machine software by directly updating the VMware Aria Operations software.
  
  For example, going outside of VMware Aria Operations to access vSphere to update VMware Tools is not supported.

- **Redundancy and Isolation.** If you expect to activate HA, place analytics cluster nodes on separate hosts. See About VMware Aria Operations High Availability.

- **If you expect to activate CA, place analytics cluster nodes on separate hosts in fault domains, stretched across vSphere clusters.** See About VMware Aria Operations Continuous Availability.
Requirements for Solutions

Be aware that solutions might have requirements beyond those for VMware Aria Operations itself.

See your solution documentation, and verify any additional requirements before installing solutions. Note that the terms solution, management pack, adapter, and plug-in are used interchangeably.

VMware Aria Operations Cluster Node Networking Requirements

When you create the cluster nodes that make up VMware Aria Operations, the associated setup within your network environment is critical to the inter-node communication and proper operation.

Networking Requirements

Important VMware Aria Operations analytics cluster nodes need frequent communication with one another. In general, your underlying vSphere architecture might create conditions where some vSphere actions affect that communication. Examples include, but are not limited to, vMotions, storage vMotions, HA events, and DRS events.

- The primary and replica nodes must use a static IP address, or fully qualified domain name (FQDN) with a static IP address.
  Data and remote collector nodes can use dynamic host control protocol (DHCP).
- You can successfully reverse-DNS all nodes, including remote collectors, to their FQDN, currently the node hostname.
  Nodes deployed by OVF have their hostnames set to the retrieved FQDN by default.
- All nodes, including remote collectors, must be bidirectionally routable by IP address or FQDN.
- Do not separate analytics cluster nodes with network address translation (NAT), load balancer, firewall, or a proxy that inhibits bidirectional communication by IP address or FQDN.
- Analytics cluster nodes must not have the same hostname.
- Place analytics cluster nodes within the same data center and connect them to the same local area network (LAN).
- Place analytics cluster nodes on same Layer 2 network and IP subnet.
  A stretched Layer 2 or routed Layer 3 network is not supported.
- Do not span the Layer 2 network across sites, which might create network partitions or network performance issues.
- With Continuous Availability activated, separate analytics cluster nodes into fault domains, stretched across vSphere clusters.
- Packet Round Trip Time between the analytics cluster nodes must be 5 ms or lower.
- Network bandwidth between the analytics cluster nodes must be one gbps or higher.
- Do not distribute analytics cluster nodes over a wide area network (WAN).
  
  To collect data from a WAN, a remote or separate data center, or a different geographic location, use remote collectors.
- Remote collectors are supported through a routed network but not through NAT.
- Do not include an underscore in the hostname of any cluster node.
- Cloud proxies must have a proper DNS resolution to the VMware Aria Operations nodes when using short/long FQDN names. This is applicable to on-prem cloud proxy.

**VMware Aria Operations Cluster Node Best Practices**

When you create the cluster nodes that make up VMware Aria Operations, additional best practices improve performance and reliability in VMware Aria Operations.

**Best Practices**

- Deploy VMware Aria Operations analytics cluster nodes in the same vSphere cluster in a single data center and add only one node at a time to a cluster allowing it to complete before adding another node.
- If you deploy analytics cluster nodes in a highly consolidated vSphere cluster, you might need resource reservations for optimal performance.
  
  Determine whether the virtual to physical CPU ratio is affecting performance by reviewing CPU ready time and co-stop.
- Deploy analytics cluster nodes on the same type of storage tier.
- To continue to meet analytics cluster node size and performance requirements, apply storage DRS anti-affinity rules so that nodes are on separate datastores.
- To prevent unintentional migration of nodes, set storage DRS to manual.
- To ensure balanced performance from analytics cluster nodes, use ESXi hosts with the same processor frequencies. Mixed frequencies and physical core counts might affect analytics cluster performance.
- To avoid a performance decrease, VMware Aria Operations analytics cluster nodes need guaranteed resources when running at scale. The VMware Aria Operations Knowledge Base includes sizing spreadsheets that calculate resources based on the number of objects and metrics that you expect to monitor, use of HA, and so on. When sizing, it is better to over-allocate than under-allocate resources.
  
  See Knowledge Base article 2093783.
- Because nodes might change roles, avoid machine names such as Primary, Data, Replica, and so on. Examples of changed roles might include making a data node into a replica for HA, or having a replica take over the primary node role.
The NUMA placement is removed in the VMware Aria Operations 6.3 and later. Procedures related to NUMA settings from the OVA file follow:

Table 2-1. NUMA Setting

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Set the VMware Aria Operations cluster status to offline | 1 Shut down the VMware Aria Operations cluster.  
2 Right-click the cluster and click Edit Settings > Options > Advanced General.  
3 Click Configuration Parameters. In the vSphere Client, repeat these steps for each VM. |
| Remove the NUMA setting | 1 From the Configuration Parameters, remove the setting numa.vcpu.preferHT and click OK.  
2 Click OK.  
3 Repeat these steps for all the VMs in the VMware Aria Operations cluster.  
4 Power on the cluster. |

Note To ensure the availability of adequate resources and continued product performance, monitor VMware Aria Operations performance by checking its CPU usage, CPU ready and CPU contention time.

Sizing and Scaling Requirements

The CPU, memory, and disk requirements that meet the needs of a particular environment depend on the number and type of objects in your environment and the data collected. This includes the number and type of adapters installed, the use of HA (High Availability) or CA (Continuous Availability), the duration of data retention, and the quantity of specific data points of interest.

VMware updates Knowledge Base article 2093783 with the most current information about sizing and scaling. The Knowledge Base article includes overall maximums and spreadsheet calculations that provide a recommendation based on the number of objects and metrics you expect to monitor.
Installing VMware Aria Operations

VMware Aria Operations nodes are virtual appliance (vApp) based systems.

Read the following topics next:

- Deployment of VMware Aria Operations
- Installation Types
- Using VMware Aria Operations on-premises to Monitor VMware Cloud

Deployment of VMware Aria Operations

VMware Aria Operations consists of one or more nodes in a cluster. To create these nodes, you have to download and install the VMware Aria Operations suitable to your environment.

Create a Node by Deploying an OVF

VMware Aria Operations consists of one or more nodes, in a cluster. To create nodes, you use the vSphere client to download and deploy the VMware Aria Operations virtual machine, once for each cluster node.

Prerequisites

- Verify that you have permissions to deploy OVF templates to the inventory.
- If the ESXi host is part of a cluster, activate DRS in the cluster. If an ESXi host belongs to a non-DRS cluster, all resource pool functions are deactivated.
- If this node is to be the primary node, reserve a static IP address for the virtual machine, and know the associated domain name, domain search path, domain name servers, default gateway, and network mask values.
  
  Plan to keep the IP address because it is difficult to change the address after installation.
- If this node is to be a data node that will become the HA/CA replica node, reserve a static IP address for the virtual machine, and store the associated domain name, domain search path, domain name servers, default gateway, and network mask values for later use.
  
  In addition, familiarize yourself with HA node placement as described in About VMware Aria Operations High Availability and CA node allocation as described in About VMware Aria Operations Continuous Availability.
Plan your domain and machine naming so that the deployed virtual machine name begins and ends with an alphabet (a–z) or digit (0–9) characters, and will only contain alphabet, digit, or hyphen (-) characters. The underscore character (_) must not appear in the host name or anywhere in the fully qualified domain name (FQDN).

Plan to keep the name because it is difficult to change the name after installation.

For more information, review the host name specifications from the Internet Engineering Task Force. See www.ietf.org.

Plan node placement and networking to meet the requirements described in General VMware Aria Operations Cluster Node Requirements and VMware Aria Operations Cluster Node Networking Requirements.

If you expect the VMware Aria Operations cluster to use IPv6 addresses, review the IPv6 limitations described in Using IPv6 with VMware Aria Operations.

Download the VMware Aria Operations .ova file to a location that is accessible to the vSphere client.

If you download the virtual machine and the file extension is .tar, change the file extension to .ova.

Verify that you are connected to a vCenter Server system with a vSphere client, and log in to the vSphere client.

Do not deploy VMware Aria Operations from an ESXi host. Deploy only from vCenter Server.

Procedure

1 Select the vSphere **Deploy OVF Template** option.

2 Enter the path to the VMware Aria Operations .ova file.

3 Follow the prompts until you are asked to enter a name for the node.

4 Enter a node name. Examples might include **Ops1**, **Ops2 Ops-A**, **Ops-B**.

   Do not include nonstandard characters such as underscores (_) in node names.
   Use a different name for each VMware Aria Operations node.

5 Follow the prompts until you are asked to select a configuration size.

6 Select the size configuration that you need. Your selection does not affect the disk size.

   Default disk space is allocated regardless of which size you select. If you need additional space to accommodate the expected data, add more disk after deploying the vApp, see Add Data Disk Space to a VMware Aria Operations vApp Node.
7 Follow the prompts until you are asked to select the disk format.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thick Provision Lazy Zeroed</td>
<td>Creates a virtual disk in a default thick format.</td>
</tr>
<tr>
<td>Thick Provision Eager Zeroed</td>
<td>Creates a type of thick virtual disk that supports clustering features such as Fault Tolerance. Thick provisioned eager-zeroed format can improve performance depending on the underlying storage subsystem. Select the thick provisioned eager-zero option when possible.</td>
</tr>
<tr>
<td>Thin Provision</td>
<td>Creates a disk in thin format. Use this format to save storage space.</td>
</tr>
</tbody>
</table>

Snapshots can negatively affect the performance of a virtual machine and typically result in a 25–30 percent degradation for the VMware Aria Operations workload. Do not use snapshots.

8 Click Next.

9 From the drop-down menu, select a Destination Network, for example, **Network 1 = TEST**, and click Next.

10 Under Networking Properties, in case of a static IP, specify the associated **Default Gateway**, **Domain Name**, **Domain Search Path**, **Domain Name Servers**, **Network 1 IP Address**, and **Network 1 Netmask** values. In case of DHCP, leave all the fields blank. The primary node and replica node require a static IP. A data node can use DHCP or a static IP.

11 In the Timezone Setting, leave the default of UTC or select a time zone.

   The preferred approach is to standardize on UTC. Alternatively, configure all nodes to the same time zone.

   **Note** You cannot configure nodes to different time zones.

12 (Optional) In Properties, under Application, select the option for IPv6.

13 (Optional) If you want to deploy a FIPS activated VMware Aria Operations setup, in the FIPS setting, select the **Activate FIPS Mode** check box.

14 Click Next.

15 Review the settings and click Finish.

16 If you are creating a multiple-node VMware Aria Operations cluster, repeat through all the steps to deploy each node.

**What to do next**

Use a Web browser client to configure a newly added node as the VMware Aria Operations primary node, a data node, or a high availability primary replica node. The primary node is required first.

**Note** For security, do not access VMware Aria Operations from untrusted or unpatched clients, or from clients using browser extensions.
Installation Types

After you have installed VMware Aria Operations product, you can either perform a new installation, an express installation, or expand an existing installation.

- Express Installation
- New installation
- Expand Installation

Figure 3-1. Getting Started Setup

Installing VMware Aria Operations for a New User

After you install VMware Aria Operations using an OVF or an installer, you are notified to the main product UI page. You can create a single node or multiple nodes depending on your environment.

Introduction to a New Installation

You can perform a new installation as a first-time user and create a single node to handle both administration and data handling.

Figure 3-2. New Installation from the Setup page

Perform a New Installation on the VMware Aria Operations Product UI

You can create a single node and configure it as a primary node or create a data node in a cluster to handle additional data. All VMware Aria Operations installations require a primary node. With a single node cluster, administration and data functions are on the same primary node. A multiple-node VMware Aria Operations cluster contains one primary node and one or more nodes for handling additional data.

Prerequisites

- Create a node by deploying the VMware Aria Operations vApp.
- After it is deployed, note the fully qualified domain name (FQDN) or IP address of the node.
If you plan to use a custom authentication certificate, verify that your certificate file meets the requirements for VMware Aria Operations.

**Procedure**

1. Navigate to the name or IP address of the node that will be the primary node of VMware Aria Operations.
   
   The setup wizard appears, and you do not need to log in to VMware Aria Operations.

2. Click **New Installation**.

3. Click **Next**.

4. Enter and confirm a password for the admin user account, and click **Next**.
   
   Passwords require a minimum of eight characters, one uppercase letter, one lowercase letter, one digit, and one special character.
   
   The user account name is admin by default and cannot be changed.

5. Select whether to use the certificate included with VMware Aria Operations or to install one of your own.
   
   a. To use your own certificate, click **Browse**, locate the certificate file, and click **Open** to load the file in the Certificate Information text box.
   
   b. Review the information detected from your certificate to verify that it meets the requirements for VMware Aria Operations.

6. Click **Next**.

7. Enter a name for the primary node.
   
   For example: **Ops-Primary**

8. Enter the URL or IP address for the Network Time Protocol (NTP) server with which the cluster synchronizes.
   
   For example: **nist.time.gov**

9. Click **Add**.
   
   Leave the NTP blank to have VMware Aria Operations manage its own synchronization by having all nodes synchronize with the primary node and replica node.

10. Click **Next**.

11. Configure the VMware Aria Operations availability. To install VMware Aria Operations with availability, activate the **Availability Mode** and select High Availability or Continuous Availability. To continue your installation on full capacity, click **Next**.

   **Note** You can activate High Availability or Continuous Availability after installation from the administrator interface.
12 Click the Add icon to add a node.
   a Enter the **Node Name** and **Node Address**.
   b Select the **Current Cluster Role**.

**Note** This step is optional if you use the default configuration. If you select High Availability for this cluster option, you can select a node from the added list of nodes to be the replica node. Although, only one node from the list can be selected as a replica node. For more information on High Availability, see [*Adding High Availability to VMware Aria Operations*](#). If you select Continuous Availability for this cluster, add at least one witness node and an even number of data nodes including the primary node and divide them across two fault domains. For more information, see [*Adding Continuous Availability*](#).

13 Click **Next**, and click **Finish**.

The administration interface appears, and it takes a moment for VMware Aria Operations to finish adding the primary node.

**Results**

You have created a primary node to which you can add more nodes.

**What to do next**

After creating the primary node, you have the following options.

- Create and add data nodes to the unstarted cluster.
- Click **Start VMware Aria Operations** to start the single-node cluster, and log in to finish configuring the product.

  The cluster might take from 10 to 30 minutes to start, depending on the size of your cluster and nodes. Do not make changes or perform any actions on cluster nodes while the cluster is starting.

  If you require a new agent to collect data, you must deploy a cloud proxy. For more information on how to deploy a cloud proxy, see [*Installing Cloud Proxy*](#).

**About the VMware Aria Operations Primary Node**

The primary node is the required, initial node in your VMware Aria Operations cluster.

The primary node performs administration for the cluster and must be online before you configure any new nodes. In addition, the primary node must be online before other nodes are brought online. If the primary node and replica node go offline together, bring them back online separately. Bring the primary node online first, and then bring the replica node online.

**Advantages of a New Installation**

You can use the new installation to create a primary node during the first installation of VMware Aria Operations. With the primary node in place, you can then start adding more nodes to form a cluster and then define an environment for your organization.
In a single-node clusters, administration and data is on the same primary node. A multiple-node cluster includes one primary node and one or more data nodes. In addition, there might be one replica node used for high availability. For continuous availability, you need a witness node and an even number of data nodes including the primary node. For more information on creating a primary node, see About the VMware Aria Operations Primary Node.

Installing VMware Aria Operations as an Administrator

As an administrator, you can install several instances of VMware Aria Operations build in your VM environment.

Introduction to Express Installation

Express installation is one possible way to create primary nodes, add data nodes, form clusters, and test your connection status. You can use express installation to save time and speed up the process of installation when compared to a new installation. Do not to use this feature unless the user is an administrator.

Figure 3-3. Express Installation from the Setup screen

Perform an Express Installation on the VMware Aria Operations product UI

Use express installation on the VMware Aria Operations cluster to create a primary node. Select express installation option when installing for the first time.

Prerequisites

Verify that you have a static IP address created from an OVF file.

Procedure

1. Navigate to the name or IP address of the node that will be the primary node of VMware Aria Operations. The setup wizard appears, and you do not need to log in to VMware Aria Operations.
2. Click Express Installation.
3. Click Next.
4. Enter and confirm a password for the admin user account, and click Next. Passwords require a minimum of 8 characters, one uppercase letter, one lowercase letter, one digit, and one special character. The user account name is admin by default and cannot be changed.
5. Click **Next**.

6. Click **Finish**.

**Results**

You have created a primary node to which you can add more nodes.

**Advantages of an Express Installation**

Express installation saves time when compared to a new installation to create a new primary node. The express installation uses the default certificates, which differ from one organization to another. This feature is mainly used by the developers or the administrators.

**Expand an Existing Installation of VMware Aria Operations**

Use this option to add a node to an existing VMware Aria Operations cluster. You can use this option if you have already configured a primary node and you want to increase the capacity by adding more nodes to your cluster.

**Introduction to Expand an Existing Installation**

You can deploy and configure additional nodes so that VMware Aria Operations can support larger environments. A primary node always requires an additional node for a cluster to monitor your environment. With expanding your installation, you can add more than one node to your cluster.

**Adding Data Nodes**

Data nodes are the additional cluster nodes that allow you to scale out VMware Aria Operations to monitor larger environments.

You can dynamically scale out VMware Aria Operations by adding data nodes without stopping the VMware Aria Operations cluster. When you scale out the cluster by 25% or more, you should restart the cluster to allow VMware Aria Operations to update its storage size, and you might notice a decrease in performance until you restart. A maintenance interval provides a good opportunity to restart the VMware Aria Operations cluster.

In addition, the product administration options include an option to re-balance the cluster, which can be done without restarting. Rebalancing adjusts the VMware Aria Operations workload across the cluster nodes.
Figure 3-4. Expand an existing installation from the Setup screen

**Note**  Do not shut down online cluster nodes externally or by using any means other than the VMware Aria Operations interface. Shut down a node externally only after taking it offline in the VMware Aria Operations interface.

Expand an Existing Installation to Add a Data Node

Larger environments with multiple-node VMware Aria Operations clusters contain one primary node and one or more data nodes for additional data collection, storage, processing, and analysis.

**Prerequisites**

- Create nodes by deploying the VMware Aria Operations vApp.
- Create and configure the primary node.
- Note the fully qualified domain name (FQDN) or IP address of the primary node.

**Procedure**

1. In a Web browser, navigate to the name or IP address of the node that will become the data node.
   
   The setup wizard appears, and you do not need to log in to VMware Aria Operations.

2. Click **Expand an Existing Installation**.

3. Click **Next**.

4. Enter a name for the node (for example, *Data-1*).

5. From the Node Type drop-down, select **Data**.

6. Enter the FQDN or IP address of the primary node and click **Validate**.

7. Select **Accept this certificate** and click **Next**.
   
   If necessary, locate the certificate on the primary node and verify the thumbprint.

8. Verify the VMware Aria Operations administrator username of admin.

9. Enter the VMware Aria Operations administrator password.

   Alternatively, instead of a password, type a pass-phrase that you were given by your VMware Aria Operations administrator.
10 Click **Next**, and click **Finish**.

The administration interface appears, and it takes a moment for VMware Aria Operations to finish adding the data node.

**What to do next**

After creating a data node, you have the following options.

- **New, unstarted clusters:**
  - Create and add more data nodes.
  - Create a high availability primary replica node.
  - In a Web browser, navigate to the primary node administration interface at `https://primary-node-name-or-ip-address/admin`. Verify that all the nodes are listed under the **Nodes in the VMware Aria Operations Cluster**. Then, click **Start VMware Aria Operations** to start the cluster and to finish configuring the product.

  The cluster might take from 10 to 30 minutes to start, depending on the size of your cluster and nodes. Do not make changes or perform any actions on cluster nodes while the cluster is starting.

- **Established, running clusters:**
  - Create and add more data nodes.
  - Create a high availability primary replica node, which requires a cluster restart.

**Advantages of an Expanding an Installation**

A data node shares the load of performing VMware Aria Operations analysis and it can also have an adapter installed to perform collection and data storage from the environment. You must have a primary node before you add data nodes to form a cluster.

**Using VMware Aria Operations on-premises to Monitor VMware Cloud**

You can use your VMware Aria Operations on-premises to manage and monitor your cloud infrastructure on VMware Clouds by simply adding a dedicated cloud account for VMware Cloud or by adding a vCenter Server account in VMware Aria Operations. You can extend the current set of monitoring, troubleshooting, optimization, and remediation processes of VMware Aria Operations on to VMware Cloud. It also provides you with a hybrid view of your environment.

**Prerequisites**

- A VPN or a direct connection to set up the bidirectional access between the nodes and cloud proxies of VMware Aria Operations on-premises and VMware Cloud.
- Scale the existing VMware Aria Operations cluster before adding the new VMware Cloud SDDC sites. To get the appropriate sizing, see [vRealize Operations Manager Online Sizer](#).
VMware Cloud on Dell EMC

The following diagram shows VMware Aria Operations on-premises collecting data from VMware Cloud on Dell EMC with cloud proxies. Configure VMware Aria Operations to monitor VMware Cloud on Dell EMC using the steps described in the topic 'Configuring a VMware Cloud on Dell EMC instance in VMware Aria Operations' in the VMware Aria Operations Configuration Guide.

VMware Cloud on AWS

The following diagram shows VMware Aria Operations on-premises collecting data from VMware Cloud on AWS with cloud proxy. Configure VMware Aria Operations to monitor VMware Cloud on AWS using the steps described in the topic 'Configuring VMware Cloud on AWS in VMware Aria Operations' in the VMware Aria Operations Configuration Guide.
Azure VMware Solution

The following diagram shows VMware Aria Operations on-premises collecting data from Azure VMware Solution with cloud proxies. Configure VMware Aria Operations to monitor Azure VMware Solution using the steps described in the topic Configuring an Azure VMware Solution Instance in VMware Aria Operations.
Oracle Cloud VMware Solution

The following diagram shows VMware Aria Operations on-premises collecting data from Oracle Cloud VMware Solution with cloud proxies. Configure VMware Aria Operations to monitor Oracle Cloud VMware Solution using the steps described in the topic Configuring an Oracle Cloud VMware Solution Instance in VMware Aria Operations.
Google Cloud VMware Engine

The following diagram shows VMware Aria Operations on-premises collecting data from Google Cloud VMware Engine with cloud proxies. Configure VMware Aria Operations to monitor Google Cloud VMware Engine using the steps described in the topic Configure a Google Cloud VMware Engine Instance in VMware Aria Operation.
Resize your Cluster by Adding Nodes

You can deploy and configure additional nodes so that VMware Aria Operations can support larger environments.

Figure 4-1. Workflow - Resize your cluster

Start

Create role-less nodes

Enable HA

Start VMware Aria Operations

Select vCenter monitoring policy goals

Add and configure more solutions

Monitor your environment

Configure the master node

Configure a data node

Configure a new installation

Configure the built-in vCenter Solution

Read the following topics next:

- Adding High Availability to VMware Aria Operations
- Adding Continuous Availability
- VMware Aria Operations Cluster and Node Maintenance
- Troubleshooting
Adding High Availability to VMware Aria Operations

You can dedicate one VMware Aria Operations cluster node to serve as a replica node for the VMware Aria Operations primary node.

Run the Setup Wizard to Add a Primary Replica Node

To activate high availability (HA) for a VMware Aria Operations cluster, specify one of the data nodes to become a replica of the primary node.

**Note**  If the cluster is running, activating HA restarts the cluster.

You can add HA to the VMware Aria Operations cluster at installation time or after VMware Aria Operations is up and running. Adding HA at installation is less intrusive because the cluster has not yet started.

**Prerequisites**

- Create nodes by deploying the VMware Aria Operations vApp.
- Create and configure the primary node.
- Create and configure a data node with a static IP address.
- Note the fully qualified domain name (FQDN) or IP address of the primary node.

**Procedure**

1. In a Web browser, navigate to the primary node administration interface.  
   https://primary-node-name-or-ip-address/admin
2. Enter the VMware Aria Operations administrator user name of admin.
3. Enter the VMware Aria Operations administrator password and click Log In.
4. Under High Availability, click Activate.
5. Select a data node to serve as the replica for the primary node.
6. Select the **Activate High Availability for this cluster** option, and click OK.
   If the cluster was online, the administration interface displays progress as VMware Aria Operations configures, synchronizes, and rebalances the cluster for HA.
7. If the primary node and replica node go offline, and the primary remains offline for any reason while the replica goes online, the replica node does not take over the primary role, take the entire cluster offline, including data nodes and log in to the replica node command-line console as a root.
8. Open $ALIVE_BASE/persistence/persistence.properties in a text editor.
9 Locate and set the following properties:

```
db.role=PRIMARY
db.driver=/data/vcops/xdb/vcops.bootstrap
```

10 Save and close `persistence.properties`.

11 In the administration interface, bring the replica node online, and verify that it becomes the primary node and bring the remaining cluster nodes online.

**What to do next**

After creating a primary replica node, you have the following options.

- New, unstarted clusters:
  - Create and add data nodes.
  - Click **Start VMware Aria Operations** to start the cluster, and log in to finish configuring the product.
    
    The cluster might take from 10 to 30 minutes to start, depending on the size of your cluster and nodes. Do not make changes or perform any actions on cluster nodes while the cluster is starting.
  - Established, running clusters:
    - Create and add data nodes.

**Adding Continuous Availability**

Continuous availability prevents data loss in the event of one or more node failures. This mode requires one witness node, one primary node, and one data node divided across two fault domains. The witness node lies outside the fault domains. By default, the primary node is assigned to **Fault Domain 1**. The data node becomes the replica node and is assigned to **Fault Domain 2**. The primary node and the replica node create a pair. The number of data nodes including the primary node should always be an even number not exceeding 16. Each data node added to **Fault Domain 1** must have a pair in **Fault Domain 2** to preserve and replicate data that is added to its peer.

**Activate Continuous Availability in VMware Aria Operations**

You can activate continuous availability (CA) for VMware Aria Operations to protect your data if there is one or more node failures.

**Note** If the cluster is running, activating CA restarts the cluster.

You can activate CA in the VMware Aria Operations cluster at the installation time or after VMware Aria Operations is up and running. Adding CA at installation is less intrusive because the cluster has not yet started.
Prerequisites

- Create nodes by deploying the VMware Aria Operations vApp.
- Create and configure the primary node.
- Create and configure the witness node.

**Note** VMware Aria Operations can have only one witness node in its cluster. While deploying an OVA file, you can select the recommended CPU/RAM configuration for the witness node.

- Create and configure one data node with a static IP address.
- Note the fully qualified domain name (FQDN) or IP address of the primary node.

Procedure

1. In a Web browser, navigate to the primary node administration interface.
   
   https://primary-node-name-or-ip-address/admin

2. Enter the VMware Aria Operations administrator user name of `admin`.

3. Enter the VMware Aria Operations administrator password and click Log In.

4. Under Continuous Availability, click **Activate CA**.

   The Continuous Availability wizard opens. The Witness node exists outside the fault domains. The primary node is already assigned to **Fault Domain 1**.

   **Note** You can enter names for each Fault Domain during installation. You can also edit the fault domain names after activating continuous availability.

5. To create a pair with the primary node, drag the data nodes to **Fault Domain 2**.

   **Note** You can add a maximum of 16 data nodes including the primary node and divide them between the fault domains to create eight pairs.

6. Click Ok.

**VMware Aria Operations Cluster and Node Maintenance**

You perform cluster and node maintenance procedures to help your VMware Aria Operations perform more efficiently. Cluster and node maintenance involves activities such as changing the online or offline state of the cluster, fault domains, or individual nodes, activating or deactivating high availability (HA) or continuous availability (CA), reviewing statistics related to the installed adapters, and rebalancing the workload for a better performance.

You perform most VMware Aria Operations cluster and node maintenance using the Cluster Management page in the product interface, or the Cluster Status and Troubleshooting page in the administration interface. The administration interface provides more options than the product interface.
Table 4-1. Cluster and Node Maintenance Procedures

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Cluster Status</td>
<td>Administration/Product</td>
<td>You can change the status of a node to online or offline. In a high availability (HA) cluster, taking the primary or replica offline causes VMware Aria Operations to run from the remaining node and for HA status to be degraded. In continuous availability (CA) cluster, taking the primary or replica offline causes VMware Aria Operations to run in a degraded status. <strong>Note</strong> You cannot convert a High Availability (HA) activated cluster to a Continuous Availability cluster and vice versa. You must first deactivate the cluster availability, so that the cluster becomes a standard cluster and then activate HA or CA as required. Any manual or system action that restarts the cluster brings all VMware Aria Operations nodes online, including any nodes that you had taken offline.</td>
</tr>
<tr>
<td>Activate or Deactivate High Availability</td>
<td>Administration</td>
<td>Activating high availability requires the cluster to have at least one data node, with all nodes online or all offline. You cannot use Remote Collector nodes. To activate high availability, see Adding High Availability to VMware Aria Operations. Deactivating high availability restarts the VMware Aria Operations cluster. After you deactivate high availability, the replica node in VMware Aria Operations converts back to a data node and restarts the cluster.</td>
</tr>
</tbody>
</table>
Table 4-1. Cluster and Node Maintenance Procedures (continued)

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate or Deactivate Continuous Availability</td>
<td>Administration</td>
<td>Activating continuous availability requires the cluster to have at least one witness node, and at least two data node, with all nodes online or all offline. You cannot use Remote Collector nodes. To activate continuous availability, see <a href="#">Adding Continuous Availability</a>. Deactivating continuous availability restarts the VMware Aria Operations cluster. When you deactivate continuous availability, you can choose to keep all your nodes or cut out one of the fault domains. <em>Click Simply Deactivate with keeping all nodes</em> to keep all your nodes when you deactivate continuous availability. <em>Note</em> You cannot deactivate continuous availability if one of your nodes is faulty. If you want to keep all your nodes, you must fix or replace the faulty node before you proceed. <em>Click Cut-Out one Fault Domain</em> and then select the fault domain you want to keep. The other fault domain and the witness node are deleted. After you deactivate continuous availability, the replica node in VMware Aria Operations converts back to a data node and restarts the cluster.</td>
</tr>
<tr>
<td>Add Nodes</td>
<td>Administration</td>
<td>You can add one or more nodes for your cluster. In a FIPS activated environment, new nodes must be FIPS compliant. In a FIPS deactivated environment, new nodes must be FIPS deactivated. Activating continuous availability requires one witness node, and an even number of data nodes including the primary node. For example, the cluster must have 2, 4, 6, 8, 10, 12, 14 or 16 nodes.</td>
</tr>
<tr>
<td>Replace Nodes</td>
<td>Administration</td>
<td>You can add nodes and replace them with a downed or non-functional node in a cluster.</td>
</tr>
<tr>
<td>Generate Passphrase</td>
<td>Administration</td>
<td>You can generate a passphrase to use instead of the administrator credentials to add a node to this cluster. The passphrase is only valid for a single use.</td>
</tr>
</tbody>
</table>
Table 4-1. Cluster and Node Maintenance Procedures (continued)

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
</table>
| Remove a Node       | Administration | When you remove a node, you lose data that the node had collected unless you are running in high availability (HA) mode. HA protects against the removal or loss of one node.  
You must not re-add nodes to VMware Aria Operations that you already removed. If your environment requires more nodes, add new nodes instead.  
When you perform maintenance and migration procedures, you should take the node offline, not remove the node. |
| Configure NTP       | Product   | The nodes in VMware Aria Operations cluster synchronize with each other by standardizing on the primary node time or by synchronizing with an external Network Time Protocol (NTP) source. |
| Rebalance the Cluster | Product   | You can rebalance adapter, disk, memory, or network load across VMware Aria Operations cluster nodes to increase the efficiency of your environment.                                                         |

Cluster Management

VMware Aria Operations includes a central page where you can monitor and manage the nodes in your VMware Aria Operations cluster and the adapters that are installed on the nodes.

How Cluster Management Works

Cluster management lets you view and change the online or offline state of the overall VMware Aria Operations cluster or the individual nodes. In addition, you can activate or deactivate high availability (HA) and view statistics related to the adapters that are installed on the nodes.

Where You Find Cluster Management

From the left menu, click Administration, and then click the Cluster Management tile.

Cluster Management Options

The options include cluster-level monitoring and management features.
Table 4-2. Initial Setup Status Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions</td>
<td>Expand Actions and then click Network Time Protocol Settings to set the global network time protocol settings for your cluster. For more information see the 'Configuring the Global Network Time Protocol (NTP) Settings' topic in the VMware Aria Operations Configuration Guide.</td>
</tr>
<tr>
<td>Cluster Status</td>
<td>Displays the online, offline, or unknown state of the VMware Aria Operations cluster. Once CA is activated, it displays the status of the two fault domains.</td>
</tr>
<tr>
<td>High Availability</td>
<td>Indicates whether HA is activated, deactivated, or degraded.</td>
</tr>
<tr>
<td>Continuous Availability</td>
<td>Indicates whether CA is activated, deactivated, or degraded.</td>
</tr>
</tbody>
</table>

VMware Aria Operations provides node-level information and a toolbar for taking nodes online or offline.

Table 4-3. Nodes in the VMware Aria Operations Cluster

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Name</td>
<td>Machine name of the node. The node that you are logged into displays a dot next to the name.</td>
</tr>
<tr>
<td>Node Address</td>
<td>Internet protocol (IP) address of the node. Primary and replica nodes require static IP addresses. Data nodes can use DHCP or static IP.</td>
</tr>
<tr>
<td>Cluster Role</td>
<td>Type of VMware Aria Operations node: primary, data, replica, or remote collector.</td>
</tr>
<tr>
<td>Fault Domain</td>
<td>Displays the fault domain a node is associated to in a CA activated cluster.</td>
</tr>
<tr>
<td>Note</td>
<td>This column appears only if CA is activated.</td>
</tr>
<tr>
<td>Node Pair</td>
<td>Displays which pair the node belongs to. For example, in CA, nodes are added in pairs. If there are four nodes, the column displays whether the node is part of pair one or two.</td>
</tr>
<tr>
<td>Note</td>
<td>This column appears only if CA is activated.</td>
</tr>
<tr>
<td>State</td>
<td>Running, Not Running, Going Online, Going Offline, Inaccessible, Failure, Error</td>
</tr>
<tr>
<td>Status</td>
<td>Online, offline, unknown, or other condition of the node.</td>
</tr>
<tr>
<td>Objects in Process</td>
<td>Total environment objects that the node currently monitors.</td>
</tr>
<tr>
<td>Objects Being Collected</td>
<td>Total environment objects that the node collected.</td>
</tr>
</tbody>
</table>
Table 4-3. Nodes in the VMware Aria Operations Cluster (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metrics in Process</td>
<td>Total metrics that the node has discovered since being added to the cluster.</td>
</tr>
<tr>
<td>Metrics Being Collected</td>
<td>Total metrics the node has collected since being added to the cluster.</td>
</tr>
<tr>
<td>Version</td>
<td>Displays the VMware Aria Operations software version and the build number installed on the node.</td>
</tr>
</tbody>
</table>

In addition, there are adapter statistics for the selected node.

Table 4-4. Adapters on Server

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name that the installing user gave to the adapter.</td>
</tr>
<tr>
<td>Status</td>
<td>Indication of whether the adapter is collecting data or not.</td>
</tr>
<tr>
<td>Objects Being Collected</td>
<td>Total environment objects that the adapter currently monitors.</td>
</tr>
<tr>
<td>Metrics Being Collected</td>
<td>Total metrics that the adapter has collected since being installed on the node.</td>
</tr>
<tr>
<td>Last Collection Time</td>
<td>Date and time of the most recent data collection by the adapter.</td>
</tr>
<tr>
<td>Added On</td>
<td>Date and time when the adapter was installed on the node.</td>
</tr>
</tbody>
</table>

Troubleshooting

Troubleshooting Cluster Problems

A multi-node VMware Aria Operations cluster does not behave as expected.

Problem

A multi-node VMware Aria Operations cluster does not behave as expected because of general problems within the cluster or because of suspected firewall concerns.

The problems might occur because of multiple reasons:

- You may be unable to install or uninstall management packs.
- The node shows as offline in the user interface even though it is online.
You might face problems with new nodes joining the cluster.

Solution

Login to each VMware Aria Operations node in the cluster and run the following script:

```bash
$VMWARE_PYTHON_3_BIN /usr/lib/vmware-casa/bin/Netcheck.py
```

On each node, you are presented with a list of attempted connections. If a node cannot connect to the required port, it is reported in the list. Ports that do not connect must be investigated.

Note  Only one port is required within the range of 10002-10010 and 20002-20010.

For more information see KB article 82421.
VMware Aria Operations Post-Installation Considerations

After you install VMware Aria Operations, there are post-installation tasks that might need your attention.

Read the following topics next:

- About Logging In to VMware Aria Operations
- Log In and Continue with a New Installation
- After You Log In
- Installing Cloud Proxy
- Monitoring Multiple Cloud Accounts in VMware Aria Operations
- Secure the VMware Aria Operations Console
- Log in to a Remote VMware Aria Operations Console Session

About Logging In to VMware Aria Operations

Logging in to VMware Aria Operations requires that you point a Web browser to the fully qualified domain name (FQDN) or IP address of a node in the VMware Aria Operations cluster.

When you log in to VMware Aria Operations, there are a few things to keep in mind.

- After initial configuration, the product interface URL is:
  https://node-FQDN-or-IP-address
- Before initial configuration, the product URL opens the administration interface instead.
- After initial configuration, the administration interface URL is:
  https://node-FQDN-or-IP-address/admin
- The administrator account name is admin. The account name cannot be changed.
- The admin account is different from the root account used to log in to the console, and does not need to have the same password.
- When logged in to the administration interface, avoid taking the node that you are logged into offline and shutting it down. Otherwise, the interface closes.
The number of simultaneous login sessions before a performance decrease depends on factors such as the number of nodes in the analytics cluster, the size of those nodes, and the load that each user session expects to put on the system. Heavy users might engage in significant administrative activity, multiple simultaneous dashboards, cluster management tasks, and so on. Light users are more common and often require only one or two dashboards.

The sizing spreadsheet for your version of VMware Aria Operations contains further detail about simultaneous login support. See Knowledge Base article 2093783.

- You cannot log in to a VMware Aria Operations interface with user accounts that are internal to VMware Aria Operations, such as the maintenance Admin account.
- For supported Web browsers, see the VMware Aria Operations Release Notes for your version.

Log In and Continue with a New Installation

To finish a new VMware Aria Operations installation, you log in and complete a one-time process to license the product and configure solutions for the kinds of objects that you want to monitor.

Prerequisites

- Create the new cluster of VMware Aria Operations nodes.
- Verify that the cluster has enough capacity to monitor your environment. See Sizing the VMware Aria Operations Cluster.

Procedure

1. In a Web browser, navigate to the IP address or fully qualified domain name of the primary node.
2. Enter the username `admin` and the password that you defined when you configured the primary node, and click Login.
   Because this is the first time you are logging in, the administration interface appears.
3. To start the cluster, click Start VMware Aria Operations.
4. Click Yes.
   The cluster might take from 10 to 30 minutes to start, depending on your environment. Do not make changes or perform any actions on cluster nodes while the cluster is starting.
5. When the cluster finishes starting and the product login page appears, enter the admin username and password again, and click Login.
   A one-time licensing wizard appears.
6. Click Next.
7. Read and accept the End User License Agreement, and click Next.
8 Enter your product key, or select the option to run VMware Aria Operations in evaluation mode.

Your level of product license determines what solutions you may install to monitor and manage objects.

- Standard. vCenter only
- Advanced. vCenter plus other infrastructure solutions
- Enterprise. All solutions

VMware Aria Operations does not license managed objects in the same way that vSphere does, so there is no object count when you license the product.

Note: When you transition to the Standard edition, you no longer have the Advanced and Enterprise features. After the transition, delete any content that you created in the other versions to ensure that you comply with EULA and verify the license key which supports the Advanced and Enterprise features.

9 If you entered a product key, click Validate License Key.

10 Click Next.

11 Select whether or not to return usage statistics to VMware, and click Next.

12 Click Finish.

The one-time wizard finishes, and the VMware Aria Operations interface appears.

What to do next

- Use the VMware Aria Operations interface to configure the solutions that are included with the product.
- Use the VMware Aria Operations interface to add more solutions.
- Use the VMware Aria Operations interface to add monitoring policies.

After You Log In

After you log in to VMware Aria Operations from a web browser, you see the newly designed Launchpad in the Home page. You can set any dashboard to appear in the home page, beside the Launchpad. Click the Actions menu on a dashboard that you want to set as the landing page and select Set as Home landing page. To remove the dashboard as the home landing page, click the Actions menu on the relevant dashboard and select Reset from Home landing page.
Home page When You First Log In

If you have logged in using an administrative account, you must set the currency in the Global Settings page. From the left menu, click Administration, and then click the Global Settings tile. You can do so from the message that you see in the Launchpad when you log in for the first time. Optionally, you can close the message. Once you set a currency, you cannot change it. As an administrator, you must also first set up a cloud account or configure an adapter before you can start using VMware Aria Operations.

A new license key is required for VMware Aria Operations 7.0 and later versions. All license keys except vSOM Enterprise Plus and its add-ons are invalidated. The product works in evaluation mode until a new valid license key, which can be obtained from the MyVMware portal, is installed. After login, if you see the "You are using an evaluation license. Please consider applying a new license by the end of the evaluation period." message in the Launchpad you must add a new license before the end of the 60-day evaluation period in the Licensing page. To add a new license, from the message, click Actions > Go to Licensing.

Note If you added new licenses when you upgraded to VMware Aria Operations 7.0, you can skip this step.

After logging in you land on the Launchpad and if you see a message like, "VMware Aria Operations internal certificates will expire on dd/mm/yyyy. Please install a new certificate before the expiry date. For details, see KB 71018", you must upgrade your internal certificates for VMware Aria Operations using the certificate renewal PAK file from the VMware Aria Operations Administrator interface. For more information, see the KB article 71018.

Launchpad After Cloud Accounts Are Configured
Beside the Launchpad tab, you see the Multi-Cloud Overview tab. To know more about the Multi-Cloud Overview, see the topic, Monitoring Multiple Cloud Accounts in VMware Aria Operations. On top of the Home page is the search bar. The search bar is available on all pages of VMware Aria Operations. To know more about the search capabilities, see the topic, Enhanced Search Capability.

The Launchpad helps you quickly get started with configuring and using VMware Aria Operations. The Launchpad replaces the existing Quick Start page and provides unified use-case based, easy-to-follow workflows in the UI, to represent key supported capabilities of VMware Aria Operations.

The Launchpad page is divided into the following sections:

**Pillars of Operations**

Helps you start a workflow based on the key operative areas of VMware Aria Operations. Displays the following cards:

- Observability
- Capacity
- Cost
- Compliance
- Sustainability

When you click on any one of the cards, it takes you to a page that displays ways in which you can leverage that pillar of operation in VMware Aria Operations. When you are on any of these pages, click Learn More in the top banner to understand the features of the product available to you for that pillar of operation and to understand any prerequisite steps.

**Applications**

Helps you manage your business applications and applications. Displays the following cards:

- Business Applications
- Applications

**Infrastructure**

Helps you monitor and evaluate the data based on your environment type, identifying trends in object behavior, calculating possible problems, and future capacity for objects in your system based on these trends. It displays alerts when an object exhibits defined symptoms. Displays the following cards:

- vSphere
- vSAN
- NSX
- Horizon
- Kubernetes

When you click on any one of the cards, it takes you to a page that displays ways in which you configure, manage and use the adapters. When you are on any of these pages, click Learn More to understand how to configure and use the adapter.

**VMware Cloud**

Helps you monitor and evaluate the data based on your VMware Cloud environment type. It identifies trends in object behavior, calculating possible problems and future capacity for objects in your system, based on the trends. Alerts you when an object exhibits the defined symptoms. Displays the following cards:

- VMware Cloud Foundation
- VMware Cloud on AWS
- Azure VMware Solution
- Google Cloud VMware Engine
- Oracle Cloud VMware Solution
- VMware Cloud on Dell EMC

When you click on any one of the cards, it takes you to a page that displays ways in which you configure, manage and use the adapters. When you are on any of these pages, click Learn More to understand how to configure and use the cloud adapter.

**Public Cloud**

Helps you monitor and evaluate the data based on your VMware Cloud environment type, identifying trends in object behavior. It calculates possible problems and future capacity for objects in your system based on the trends. Alerts you when an object exhibits defined symptoms. Displays the following cards:

- Amazon Web Services
- Microsoft Azure
- Google Cloud Provider

Click on any of the public cloud adapter cards to configure the cloud account if you already have not done so.

**Integrations**

Displays the following cards:

- Automation Central
- Outbound Plugins
- Content Repository
Installing Cloud Proxy

Install cloud proxy on your on-premise VMware Aria Operations to collect data across different geo locations.

**Note**  FIPS mode is supported in cloud proxy. To leverage this functionality, make sure your cluster is in FIPS mode.

Monitoring Multiple Cloud Accounts in VMware Aria Operations

You can now monitor all your cloud operations from the Multi-Cloud Overview page in VMware Aria Operations. This overview page provides a comprehensive understanding of your cloud accounts which includes their geo-location, top objects or services, and alerts. You can also view the capacity and time remaining, and the cost for your entire VMware Cloud Infrastructure or individual VMware clouds.

The multi-cloud overview page provides a consolidated view of all the cloud accounts on the **All Clouds** page. The different tiles provide insights into the location, health, cost, and inventory of your cloud accounts.

**World Map** tile - You use the world map to view the total number of locations and the different locations of your configured cloud accounts. The map shows numbers at different locations that signify groups of accounts. Multiple accounts in a given area, are grouped to provide a more consolidated look. You can hover over the numbers to view the area that the grouped accounts belong to or click the number to zoom in and view accounts in that specific area. You can click an account to open the account summary tab. For more information see the ‘Summary Tab’ topic in the *VMware Aria Operations User Guide*.

**Note**  If multiple accounts of the same account type use the same region, it is counted as a single location. The map also shows the total number of configured SDDCs for VMware clouds (OCVS, VMC, VMC-D, VCF, GCVE, and AVS).

**Inventory** tile - Displays the total number of configured accounts under each cloud account type. It also provides the summarized resources count (storage, compute, container, applications, and business applications) for the whole cloud infrastructure.

**VMware Cloud** tile - There are three sections under the VMware Cloud tile. You can view the capacity and the time remaining before the capacity runs out. If no data is displayed as part of the capacity and time remaining sections, check your account configuration and make sure they are collecting data.
The VMware Cloud tile also displays the total cost of ownership, potential savings, and realized savings. The cost is the aggregated value for all VMware clouds. The amount displayed is calculated from the first of the month to the current date. This value is reset at the beginning of every month.

**Public Cloud Top Services** tile - Displays the list of the top public cloud services in VMware Aria Operations.

**Alerts Volume** tile - Displays the total number of alerts that are in the critical, immediate, and warning state. The alert information is consolidated for all the cloud accounts and is represented graphically dating back a month from the current date.

**Sustainability for VMware Cloud** tile - Displays the sustainability status of your VMware Cloud that includes its green score, power consumption, carbon footprint, and overall environmental impact. To view the sustainability information in more detail, click **View Sustainability**. For more information, see the 'Sustainability' topic in the *VMware Aria Operations Configuration Guide*.

The multi-cloud overview page also provides details for the following VMware and public cloud accounts in VMware Aria Operations:

- vCenter
- VMware Cloud on Dell EMC (VMC-D)
- VMware Cloud Foundation (VCF)
- VMware Cloud on AWS (VMC on AWS)
- Google Cloud VMware Engine (GCVE)
- Oracle Cloud VMware Solution (OCVS)
- Azure VMware Solution (AVS)
- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)

All the values shown on the All Clouds page might not match with the respective metrics at the individual cloud levels. That is because the metric at the All Cloud level has values aggregated for all clouds that include VMware and public clouds.

You can select the individual VMware or public cloud to view the account details. The tiles get updated to reflect values associated with that account.

**Note**  No data is displayed for cloud accounts that do not have a configured account. To add a cloud account, click **Add Account**. For more information see the 'Adding Accounts' topic in the *VMware Aria Operations Configuration Guide*. 
VMware Cloud - Example: vCenter Cloud Account

The values displayed in the individual VMware cloud accounts like vCenter, VMware Cloud on Dell EMC, VMware Cloud on AWS, VMware Cloud Foundation, Azure VMware Solution, Oracle Cloud VMware Solution, and Google Cloud VMware Engine are based on their total number of accounts.

**Note** To view the geo location of the accounts configured for vCenter, VMware Cloud on Dell EMC, and VMware Cloud Foundation, you must assign them to a physical data center. For more information, see the 'Adding Physical Data Centers' topic in the *VMware Aria Operations Configuration Guide*.

**Top Objects** tile - Displays the top selected object types (Virtual Machine, vSphere Distributed Port Group, Host System, Datastore, vSphere Distributed Switch, vSAN Datastore, Cluster Compute Resource, Datacenter, Pods) in descending order based on object count. If an object type is not specified, it is not displayed in this tile.

**Top Objects Growth Trend** tile - Displays the growth trend of the top objects (except the vSAN Datastore) dating back a month from the current date. The vSAN Datastore growth trend data is not displayed.

Public Cloud - Example: Amazon Web Services (AWS)

The values displayed in the individual public cloud accounts like AWS, Microsoft Azure, Google Cloud Platform are based on their total number of accounts.

**Top Services** - Displays the list of top ten services for the selected cloud account. The list appears in descending order based on the count of each service.

**Top Services Growth Trend** - Displays the growth trend of the top services dating back a month from the current date.

Secure the VMware Aria Operations Console

After you install VMware Aria Operations, you secure the console of each node in the cluster by logging in for the first time.

**Procedure**

1. Locate the node console in vCenter or by direct access. In vCenter, use Alt+F1 to access the login prompt.
   
   For security, VMware Aria Operations remote terminal sessions are deactivated by default.

2. Log in as **root**.
   
   VMware Aria Operations prevents you from accessing the command prompt until you create a root password.

3. When prompted for a password, press Enter.
When prompted for the old password, press Enter.
When prompted for the new password, enter the root password that you want, and note it for future reference.
Re-enter the root password.
Log out of the console.

Log in to a Remote VMware Aria Operations Console Session

As part of managing or maintaining the nodes in your VMware Aria Operations cluster, you might need to log in to a VMware Aria Operations node through a remote console.

For security, remote login is deactivated in VMware Aria Operations by default. To activate remote login, perform the following steps.

Procedure
1. Log in to a vCenter Server system using a vSphere Web Client and select a vCenter Server instance in the vSphere Web Client navigator.
   a. Find the Virtual Machine in the hierarchy and click Launch Console.

   Note: You can also use the vSphere Client to launch the node console by direct access after activating the SSHD service.

   The virtual machine console opens in a new tab of the Web browser.
2. Locate the node console and click Launch Console.
3. In vCenter, use Alt+F1 to access the login prompt and log in as root. If this is the first time logging in, you must set a root password.
   a. When prompted for a password, press Enter.
   b. When prompted for the old password, press Enter.
   c. When prompted for the new password, enter the root password that you want, and note it for future reference.
   d. Re-enter the root password.
4. To activate remote login, enter the following command:
   
   ```
   service sshd start
   ```
Upgrade, Backup and Restore

You can update your existing VMware Aria Operations deployments to a newly released version. When you perform a software update, you need to make sure you use the correct PAK file for your cluster. A good practice is to take a snapshot of the cluster before you update the software, but you must remember to delete the snapshot once the update is complete.

**Note**  During the upgrade process, any user modifications made to the default content, including alert definitions, symptoms, recommendations, policy definitions, views, dashboards, widgets, and reports, will be overwritten. To preserve such customizations and facilitate easy restoration after the upgrade, you must clone, export or create a backup of your content.

Starting with version 8.6 of VMware Aria Operations, internal certificates are renewed when you upgrade a cluster, except when the cloud proxy version 8.4, 8.5, or earlier is present. Automatic root-CA certificate renewal will be available when cloud proxy is version 8.6 and is upgraded to higher versions. After each product upgrade, the cluster will have a new root-CA certificate with a 5-year validity period.

**Note**  Automatic certificate renewal does not affect custom certificates.

Read the following topics next:

- Obtain the Software Update PAK File
- Create a Snapshot as Part of an Update
- How To Preserve Customized Content
- Back Up and Restore
- VMware Aria Operations Software Updates
- Before Upgrading to VMware Aria Operations 8.12

**Obtain the Software Update PAK File**

Each type of cluster update requires a specific PAK file. Make sure you are using the correct one.
Download the Correct PAK files

To update your VMware Aria Operations environment, you need to download the right PAK file for the clusters you wish to upgrade. In case modifications are required, you can manually update the hosts file after completing the software update.

To download the PAK file for VMware Aria Operations, go to Download VMware Aria Operations page and select the correct version from the drop-down list.

If you are using cloud proxy, download the VMware Aria Operations Manager - Virtual Appliance upgrade .pak file with Cloud Proxy file from the Product Downloads tab, to update the VMware Aria Operations environment and your cloud proxy together.

Create a Snapshot as Part of an Update

It is mandatory to create a snapshot of each node in a cluster before you update a VMware Aria Operations cluster. Once the update is complete, you must delete the snapshot to avoid performance degradation.

For more information about snapshots, see the vSphere Virtual Machine Administration documentation.

Procedure

1. Log into the VMware Aria Operations Administrator interface at https://<primary-node-FQDN-or-IP-address>/admin.
2. Click Take Offline under the cluster status.
3. When all nodes are offline, open the vSphere client.
4. Right-click a VMware Aria Operations virtual machine.
5. Click Snapshot and then click Take Snapshot.
   a. Name the snapshot. Use a meaningful name such as "Pre-Update."
   b. Uncheck the Snapshot the Virtual Machine Memory check box.
   c. Uncheck the Ensure Quiesce Guest File System (Needs VMware Tools installed) check box.
   d. Click OK.
6. Repeat these steps for each node in the cluster.

What to do next

Start the update process as described in Install a Software Update.
How To Preserve Customized Content

When you upgrade VMware Aria Operations, it is important that you upgrade the current versions of content types that allow you to alert on and monitor the objects in your environment. With upgraded alert definitions, symptom definitions, and recommendations, you can alert on the various states of objects in your environment and identify a wider range of problem types. With upgraded views, you can create dashboards and reports to easily identify and report on problems in your environment.

You might need to perform certain steps before you upgrade the alert definitions, symptom definitions, recommendations, and views in your VMware Aria Operations environment.

- If you customized any of the alert definitions, symptom definitions, recommendations, or views that were provided with previous versions of VMware Aria Operations, and you want to retain those customized versions, perform the steps in this procedure.

- If you did not customize any of the alert definitions, symptom definitions, recommendations, or views that were provided with previous versions of VMware Aria Operations, you do not need to back them up first. Instead, you can start the upgrade, and during the upgrade select the check box named Reset out-of-the-box content.

Prerequisites

You previously customized versions of your alert definitions, symptom definitions, recommendations, or views.

Procedure

1. Before you begin the upgrade to VMware Aria Operations, back up the changes to your alert definitions, symptom definitions, recommendations, and views by cloning them.

2. Start the upgrade of VMware Aria Operations.

3. During the upgrade, select the check box named Reset out-of-the-box content.

Results

After the upgrade completes, you have preserved your customized versions of alert definitions, symptom definitions, recommendations, and views, and you have the current versions that were installed during the upgrade.

What to do next

Review the changes in the upgraded alert definitions, symptom definitions, recommendations, and views. Then, determine whether to keep your previously modified versions, or to use the upgraded versions. For more information, see Creating a Backup and Importing Content in the Managing Content chapter of the Configuration Guide.
Back Up and Restore

Back up and restore your VMware Aria Operations system regularly to avoid downtime and data loss in case of a system failure. If your system does fail, you can restore the system to the last full or incremental backup.

You can back up and restore VMware Aria Operations single or multi-node clusters by using vSphere Data Protection or other backup tools. You can perform full, differential, and incremental backups and restores of virtual machines.

To back up and restore VMware Aria Suite components by using vSphere Data Protection and NetBackup, see VMware Aria Suite Backup and Restore by Using Veritas NetBackup.

To back up and restore VMware Aria Suite single or multi-node clusters using EMC Avamar and to perform on-demand group backup, see VMware Aria Suite Backup and Restore by Using EMC Avamar.

To back up and restore VMware Aria Operations single or multi-node clusters using the Veeam Backup & Replication tool, see About Veeam Backup & Replication.

It is highly recommended to take a backup during quiet periods. Since a snapshot based backup happens at the block level, it is important that there are limited or no changes being performed by a user on the cluster configuration. This will ensure that you have a healthy backup.

It is best to take the cluster offline before you back up the VMware Aria Operations nodes. This will ensure the data consistency across the nodes and internally in the node. You can either shut down the VM before the backup or activate quiescing.

If the cluster remains online, backup your VMware Aria Operations multi-node cluster by using vSphere Data Protection or other backup tools, deactivate quiescing of the file system.

Note All nodes are backed up and restored at the same time. You cannot back up and restore individual nodes.

You can use the Site Recovery Manager to protect your VMware Aria Suite components. The VMware Aria Suite Disaster Recovery by Using Site Recovery Manager is a disaster recovery automation software that provides policy-based management, non-disruptive testing, and automated orchestration. For more information, see VMware Aria Suite Disaster Recovery by Using Site Recovery Manager.

VMware Aria Operations Software Updates

VMware Aria Operations includes a central page where you can manage updates to the product software.

How Software Updates Work

The Software Update option lets you install updates to the VMware Aria Operations product itself.
Where You Find Software Updates

Log in to the VMware Aria Operations administration interface at https://primary-node-name-or-ip-address/admin. On the left, click Software Update.

Software Update Options

The options include a wizard for locating the update PAK file and starting the installation, plus a list of updates and the VMware Aria Operations cluster nodes on which they are installed.

Table 6-1. Software Update Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install a Software Update</td>
<td>Launch a wizard that allows you to locate, accept the license, and start the installation of a VMware Aria Operations software update.</td>
</tr>
<tr>
<td>Node Name</td>
<td>Machine name of the node where the update is installed</td>
</tr>
<tr>
<td>Node IP Address</td>
<td>Internet protocol (IP) address of the node where the update is installed. Primary and replica nodes require static IP addresses. Data nodes may use DHCP or static IP.</td>
</tr>
<tr>
<td>Update Step</td>
<td>Software update progress in step x of y format</td>
</tr>
<tr>
<td>Status</td>
<td>Success, failure, in-progress, or unknown condition of the software update. For cloud proxy upgrade, every stage of the upgrade process is displayed. Hover the mouse near the status message to see more details in the pop-up window. The Cloud Proxy upgrade stages are as follows:</td>
</tr>
<tr>
<td></td>
<td>Stage 1 - Downloading</td>
</tr>
<tr>
<td></td>
<td>Stage 2: Extracting</td>
</tr>
<tr>
<td></td>
<td>Stage 3: Upgrading</td>
</tr>
<tr>
<td></td>
<td>Stage 4: Rebooting</td>
</tr>
<tr>
<td></td>
<td>Stage 5: Success</td>
</tr>
</tbody>
</table>
Install a Software Update

If you have already installed VMware Aria Operations, you can update your software when a newer version becomes available.

**Note**  Installation might take several minutes or even a couple hours depending on the size and type of your clusters and nodes.

**Note**  VMware Aria Application Remote Collector virtual appliance is deprecated and is no longer available for download from the VMware Aria Operations user interface when you upgrade to VMware Aria Operations 8.6. VMware recommends that you use cloud proxy to monitor your application services. You can migrate on-prem standalone VMware Aria Application Remote Collector to on-prem cloud proxy. For information about migrating from VMware Aria Application Remote Collector to cloud proxy, see [KB 83059](#).

**Prerequisites**

- Create a snapshot of each node in your cluster. For information about how to perform this task, see the VMware Aria Operations Information Center.

- Obtain the PAK file for your cluster. For information about which file to use, see the VMware Aria Operations Information Center.

- Before you install the PAK file, or upgrade your VMware Aria Operations instance, clone any customized content to preserve it. Customized content can include alert definitions, symptom definitions, recommendations, and views. Then, during the software update, you select the option named **Install the PAK file even if it is already installed**.

- Since version 6.2.1, VMware Aria Operations update operation has a validation process that identifies issues before you start to update your software. Although it is good practice to run the pre-update check and resolve any issues found, users who have environmental constraints can deactivate this validation check.

To deactivate the pre-update validation check, perform the following steps:

- **Edit the update file to** `/storage/db/pakRepoLocal/bypass_prechecks_VMwareAriaOperationsManagerEnterprise-buildnumberofupdate.json`

- Change the value to `TRUE` and run the update.

**Note**  If you deactivate the validation, you might encounter blocking failures during the update itself.

**Procedure**

1. Log into the primary node VMware Aria Operations administrator interface of your cluster at `https://primary-node-FQDN-or-IP-address/admin`.

2. Click **Software Update** in the left pane.

3. Click **Install a Software Update** in the main pane.
Follow the steps in the wizard to locate and install your PAK file.

This updates the OS on the virtual appliance and restarts each virtual machine.

Read the **End User License Agreement** and **Update Information**, and click **Next**.

Click **Install** to complete the installation of software update.

**Note** After you click **Install**, the installer will restart the VMware Aria Operations administrator interface, and you will be logged out. Log in once again to the VMware Aria Operations administrator interface when it is ready, and follow the update status in the software update page.

Log back into the primary node administrator interface.

The main Cluster Status page appears and cluster goes online automatically. The status page also displays the Bring Online button, but do not click it.

Clear the browser caches and if the browser page does not refresh automatically, refresh the page.

The cluster status changes to Going Online. When the cluster status changes to Online, the upgrade is complete.

**Note** If a cluster fails and the status changes to offline during the installation process of a PAK file update, then some nodes become unavailable. To fix this, you can access the administrator interface and manually take the cluster offline and click **Finish Installation** to continue the installation process.

Click **Software Update** to check that the update is done.

A message indicating that the update completed successfully appears in the main pane.

**Note** When you update VMware Aria Operations to a latest version, all nodes get upgraded by default.

If you are using cloud proxies, the cloud proxy upgrades start after the VMware Aria Operations upgrade is complete successfully. For more information, see the Monitoring the Health of Cloud Proxies from the Admin UI topic in the *VMware Aria Operations Configuration Guide*.

**What to do next**

Delete the snapshots you made before the software update.

**Note** Multiple snapshots can degrade performance, so delete your pre-update snapshots after the software update completes.
Before Upgrading to VMware Aria Operations 8.12

With every VMware Aria Operations release, many metrics are either discontinued or deactivated. These changes update the capacity analytics and improve the product scale. VMware has made many of these changes transparent or nearly so. Still, multiple changes can impact management packs that you might be using, along with the dashboards and reports that you have created. Therefore, before upgrading, run the VMware Aria Operations Pre-upgrade Readiness Assessment Tool (Assessment Tool) that helps you understand the precise impact on your environment through a detailed report.

Why Run the Assessment Tool

Various changes in VMware Aria Operations can impact the user experience. When you run the Assessment Tool, you get an HTML-formatted report identifying all the points in your system affected by the changes. Further, the Assessment Tool gives recommendations for the correct changes to be made in your content for when you upgrade from a previous release.

Note You must run the Assessment Tool on the instance of the VMware Aria Operations installation that you want to assess - typically your production system. The Assessment Tool does not alter anything in your system, and deletes itself when it has completed its run. It leaves behind only the assessment result - a support bundle that you download from the Support Bundles section of the VMware Aria Operations Administration user interface.

The Assessment tool validates your environment to ensure it is ready for the upgrade. For example, if the ESXi version does not match the product requirements, the assessment tool will identify the issue and provide you with a recommendation in the Systems Validation tab.

For detailed instructions on running the Assessment Tool, see Running the VMware Aria Operations 8.12 Pre-Upgrade Readiness Assessment Tool.

To view the upgrade path from an earlier version of VMware Aria Operations to 8.12, see VMware Aria Operations Upgrade Path.

Running the VMware Aria Operations 8.12 Pre-Upgrade Readiness Assessment Tool

Before upgrading, you can gauge the impact on your system by running the VMware Aria Operations Pre-Upgrade Readiness Assessment Tool (Assessment Tool). The tool generates a report detailing the precise impact on your environment and gives suggestions for replacement metrics.

Using the Assessment Tool consists of four distinct steps:

1. Download the corresponding version of the PAK file from Broadcom Support Portal.
2. Run the VMware Aria Operations Pre-Upgrade Readiness Assessment Tool.
3. Extract the report from the generated ZIP file.
4 Click the various items in the report to link to the solutions grid.

**Note** You must run the Assessment Tool on the instance of the VMware Aria Operations installation that you want to assess - typically your production system. The Assessment Tool does not alter anything in your system, and deletes itself when it has completed its run. It leaves behind only the assessment result - a support bundle that you download from the Support Bundles section of the VMware Aria Operations Administration user interface.

**Prerequisites**

You must have administrator privileges in your current installation of VMware Aria Operations to download and run the Assessment Tool. For more information on using the upgrade assessment tool, see the following KB article [67311](#).

**Procedure**

1 Download the corresponding version of the Assessment Tool PAK from Broadcom Support Portal to your local machine. Search for APUAT or VMware Aria Operations - Upgrade Assessment Tool.

2 Open a browser and navigate to the VMware Aria Operations administrator console: https://<primary_node_IP>/admin. Then log into the administrator user interface with the user ID **admin** and the associated password.

3 In the left pane of the administration home page, click **Software Update**.

4 Click **Install a Software Update** at the top of the screen.

5 Click the **Browse** link and navigate to the PAK file you downloaded in Step 1.

   A check mark appears next to the statement: **The selected file is ready to upload and install.** **Click UPLOAD to continue.**

6 Ensure that a check mark appears next to the statement: **Install the PAK file even if it is already installed.**

   Leave blank the check box next to Reset Default Content...

7 Click the **UPLOAD** link.

   The PAK file is uploaded from your local machine to VMware Aria Operations. Uploading may take a few minutes.

8 Once the PAK file is uploaded, click **NEXT**.

   The End User License Agreement appears.
9 Click the check box next to the statement: I accept the terms of this agreement.

Click NEXT. The Important Update and Release Information screen appears.

10 Review the release information and click NEXT. At the Install Software Update screen, click INSTALL.

The Software Update screen appears again, this time with a rotating icon and an installation in progress... bar marking the progress of the PAK file and assessment as they run on your environment. The process can take from five to 20 minutes, depending on the size of your system.

11 When the process is complete, click Support in the left pane.

The Support screen appears.

12 Select the Support Bundles option above the toolbar.

The available support bundles are listed.

13 Locate the support bundle most recently created. Click the chevron next to the bundle name to open the file and select it, then click the download link on the toolbar to save the support bundle ZIP file to your local files.

14 To review the report, extract the files from the ZIP file and open the HTML file. (Do not open the CSV file, it is for VMware use only.)

The report is a graphical depiction of your VMware Aria Operations UI components - dashboards, reports, management packs, alerts, heat maps, and so on - and includes the number of deprecated metrics impacting each component. For example, you might find that 10 of your 25 dashboards contain a total of 15 deprecated metrics.

15 Click a component.

The report details for that component are listed following the graphics, under Impacted Component Details. Taking dashboards as an example, the list provides - for each dashboard - the dashboard name, owner, widgets removed, metric-impacted views, and metric-impacted widgets. The deprecated metrics are live links.

16 Click a live metric link.

A browser window opens at URL http://partnerweb.vmware.com/programs/vrops/DeprecatedContent.html with the selected metric highlighted in a table of like metrics. If a replacement metric is available for the deprecated metric, it is listed in the same row by name and metric key. You might choose to install the new metric in place of the deprecated metric.

17 Repeat Steps 15 and 16 for all your components.

If you replace the deprecated metrics with new metrics, or update each component to provide needed information without the deprecated metrics, your system is ready for the upgrade.

18 Rerun the entire assessment process from Step 1 to confirm that your system is no longer impacted or at least mostly not impacted by the metrics changes.
Once you have upgraded to VMware Aria Operations 8.12, fix the remaining issues with replacement metrics available in the new release.

Results

Your VMware Aria Operations components are updated to work correctly in the 8.12 release.

What to do next

Once you have installed VMware Aria Operations 8.12, conduct, at a minimum, random testing to determine if system metrics are operating as you expect. Monitor the platform on an ongoing basis to confirm that you are receiving the correct data.