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

1 Getting Started with VMware Aria Operations for Networks 4
   Start VMware Aria Operations for Networks Trial 6
   Setting up VMware Aria Operations for Networks Collector (OVA) 8
      Collector Recommendation and Other Requirements 11
   Setting up Operations for Networks Collector (AMI) in AWS for VMware SD-WAN 13
Getting Started with VMware Aria Operations for Networks

VMware Aria Operations for Networks provides end-to-end network visibility across VMware NSX-T, VMware SD-WAN, VMware Cloud, public cloud, and other multi-cloud deployments. Cloud, network, and security administrators can use VMware Aria Operations for Networks to view usage details across all their clouds, both public and private. This document introduces you to the VMware Aria Operations for Networks service.

VMware Aria Operations for Networks provides you visibility into the network flows and security of your on-premise and cloud applications, and helps you administer your NSX-based Software-Defined Data Center (SDDC). Use VMware Aria Operations for Networks to monitor and diagnose problems with your network resources.

For example, you can check your network flows, your virtual machine and NSX security rules, plan for optimal micro segmentation, and take other network management actions.

To successfully on-boarded with VMware Aria Operations for Networks, you must do the following:

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Sign-up for VMware Cloud Services and request for VMware Aria Operations for Networks trial | Sign up to VMware Aria Operations for Networks  
   **Note**  
   - Ensure you are familiar with the trial limits. See Trial limits. |
<p>| Log in to VMware Aria Operations for Networks | Start VMware Aria Operations for Networks Trial     |</p>
<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy Collector and connect to Cloud Platform</td>
<td>Setting up VMware Aria Operations for Networks Collector (OVA)</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Ensure you allow the HTTPS port 443 in the firewall to communicate between the Collector and the following domain:</td>
</tr>
<tr>
<td></td>
<td>us.pd.ni-onsaas.com (US region)</td>
</tr>
<tr>
<td></td>
<td>uk.pd.ni-onsaas.com (UK region)</td>
</tr>
<tr>
<td></td>
<td>de.pd.ni-onsaas.com (Frankfurt region)</td>
</tr>
<tr>
<td></td>
<td>au.pd.ni-onsaas.com (Sydney region)</td>
</tr>
<tr>
<td></td>
<td>jp.pd.ni-onsaas.com (Tokyo region)</td>
</tr>
<tr>
<td></td>
<td>ca.pd.ni-onsaas.com (Canada region)</td>
</tr>
<tr>
<td></td>
<td>in.pd.ni-onsaas.com (India region)</td>
</tr>
<tr>
<td></td>
<td>You can locate a region from the browser URL that you use to access the service. For example, in the URL <a href="https://ca.www.mgmt.cloud.vmware.com/ni">https://ca.www.mgmt.cloud.vmware.com/ni</a>, ca indicates CA (Canada) region. Similarly in the URL <a href="https://uk.www.mgmt.cloud.vmware.com/ni">https://uk.www.mgmt.cloud.vmware.com/ni</a>, us indicates the UK region.</td>
</tr>
<tr>
<td></td>
<td>For details about other ports and protocols required for VMware Aria Operations for Networks, see VMware Ports and Protocols.</td>
</tr>
<tr>
<td>(Optional) Deploy Collector for VMware SD-WAN</td>
<td>Setting up Operations for Networks Collector (AMI) in AWS for VMware SD-WAN</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If your environment does not have a vCenter server, and you want to deploy your collector in a cloud environment then you can deploy your collector in AWS.</td>
</tr>
<tr>
<td>Add data sources in VMware Aria Operations for Networks</td>
<td>Adding a Data Source in VMware Aria Operations for Networks</td>
</tr>
</tbody>
</table>

After you successfully on-board with VMware Aria Operations for Networks, you can view the data source related information, do micro-segmentation plannings, plan application security and migration, and many more. To know more, see Using VMware Aria Operations for Networks (SaaS).

Read the following topics next:

- Start VMware Aria Operations for Networks Trial
- Setting up VMware Aria Operations for Networks Collector (OVA)
- Setting up Operations for Networks Collector (AMI) in AWS for VMware SD-WAN
Start VMware Aria Operations for Networks Trial

To start your VMware Aria Operations for Networks trial, you must sign up for VMware Cloud Services with your VMware ID.

Sign up to VMware Aria Operations for Networks

When you sign up for a VMware Cloud service, or when someone invites you to join a service, you receive an email invitation containing a link that you use to sign up.

Procedure

1. Use the following link to sign up for the VMware Aria Operations for Networks trial service:
   
   - **Sign up** for VMware Aria Operations for Networks trial service.
     
     You sign up for VMware Cloud services with your VMware ID. If you do not have a My VMware account, you create one as you sign up.
     
     You will receive the service activation link to log in to VMware Aria Operations for Networks through email within one hour.

   **Note**
   
   - To request for the trial service, you must use the same email ID that you entered at the time of creating VMware ID.
   
   - Ensure that you are not opted-out of VMware marketing emails and check your junk folder for any email communications from VMware. If you don't receive any activation links within one or two days, contact help-vni@vmware.com to get the manual link from the Cloud services.

2. Click the link in your invitation email.

3. Sign up for VMware Cloud:
   
   a. If you have a VMware ID, follow the steps to sign up to VMware Cloud with your VMware ID credentials.
   
   b. If you do not have a VMware ID, follow the steps to create your My VMware account, and sign up to VMware Cloud.

4. Log in to VMware Cloud with your VMware ID. If you are not redirected to the VMware Aria Operations for Networks page, go to https://www.mgmt.cloud.vmware.com/.

Start VMware Aria Operations for Networks Trial

VMware offers a full-featured 30 days VMware Aria Operations for Networks free trial to all the new organizations. Any new tenant or organization can register for the VMware Aria Operations for Networks trial offer.
VMware Aria Operations for Networks is available for purchase globally and hosted in US West (Oregon), Canada Central (Montreal), Europe (London), Europe(Frankfurt), Asia Pacific (Tokyo), Asia Pacific (Sydney), Asia Pacific (Mumbai).

During the free trial, you can use all the features of VMware Aria Operations for Networks with the following limitation:

<table>
<thead>
<tr>
<th>Entities</th>
<th>Maximum Trial Limits</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMs</td>
<td>2,000</td>
</tr>
<tr>
<td>Flows</td>
<td>500,000</td>
</tr>
<tr>
<td>Physical Devices</td>
<td>30</td>
</tr>
<tr>
<td>Network Assurance and Verification Rules</td>
<td>15,000</td>
</tr>
<tr>
<td>VMware SD-WAN Edges</td>
<td>15</td>
</tr>
</tbody>
</table>

Reach out to VMware Sales, if you need to extend the trial scale limits.

**Note**  You also get an additional 15 days grace period before the permanent termination of the trial period. Contact VMware Sales to extend the trial period beyond 45 days.

Service terminates after 45 days, which result in the deletion of the service data. Any reactivation post service termination requires a new collector deployment and configuration.

**Note**  VMware Aria Operations for Networks trial offer is not applicable for existing organizations or new users to the existing organizations that have already used the trial offer.

**Prerequisites**

**Sign up to VMware Aria Operations for Networks**

**Procedure**

1  Log in to VMware Cloud services with your VMware ID.
2  Select VMware Aria Operations for Networks.
3  To start the trial, from the Select region drop-down menu, select a hosting region.

   **Note**  Select the hosting region carefully. After you start the trial, you cannot change the hosting region.

4  Click CONTINUE.

   **Note**  If a valid subscription for VMware Aria Operations for Networks exists, then you are on-boarded as a license user and not as a trial user.
Become a Customer
You can purchase a service plan at any moment during the trial period. VMware service billing starts right after you purchase the service plan.

Procedure
1. Log in to VMware Aria Operations for Networks.
2. Click BUY NOW on the Green banner on the Welcome page.
3. Click BUY SUBSCRIPTION and follow the instruction to complete the purchase.
4. Refresh the VMware Aria Operations for Networks UI to update the subscription changes.

Setting up VMware Aria Operations for Networks Collector (OVA)
You can set up VMware Aria Operations for Networks collector by importing OVA to your VMware vCenter server.

To add a Collector VM, you must do the following:
1. Download the Collector VM OVA.
2. Generate a Shared Secret.
3. Deployment Using vSphere Web Client

Note Before you add a Collector VM, ensure that you review and meet Recommendation for the Collector Deployment for optimum performance. To know about the Collector deployment requirement, see the System Recommendations and Requirements topic.

Generate a Shared Secret
You can generate and import the VMware Aria Operations for Networks collector virtual appliance.

Generate a shared secret and import the VMware Aria Operations for Networks collector virtual appliance:

Procedure
1. Log into the VMware Aria Operations for Networks UI.
2. Click one of the following accounts:
   - VMware vCenter
   - VMware Cloud (VMC)
VMware SD-WAN by VeloCloud

**Note**: You do not have to add any collector for public cloud accounts such as Amazon AWS and Microsoft Azure.

3 Click **ADD COLLECTOR VM**.

4 Click **DOWNLOAD** if you haven’t already downloaded the Collector.

5 Click **COPY** to copy the shared secret, and click **CLOSE**.

You need this shared secret during the deployment of VMware Aria Operations for Networks Collector OVA.

**Deployment Using vSphere Web Client**

You can import the VMware Aria Operations for Networks Collector OVA using vSphere Web Client.

**Procedure**

1 Right-click the **Datacenter** where you want to install the appliance and select **Deploy OVF Template**.

2 Enter the URL to download and install the OVA package from the internet. Or, browse your computer to select the source location of the OVA package.

3 Provide a name and specify a location where you want to save the deployed template. Click **Next**.

4 Select a resource (host or a cluster) where you want to run the deployed template. Click **Next**.

5 Verify all the details of the template. Click **Next**.

6 Read the **End-User License Agreement** and click **Accept**. Click **Next**.

7 Select a deployment configuration. Click **Next**.

8 Select the location where you want to store the files for the deployed template.
   a Select **Thin Provision** as the virtual disk format.
   b Specify the format in which you want to store the virtual disks.
   c Select the datastore in which you want to install the files.
   d Click **Next**.

9 Specify the destination network for the source network. Click **Next**.

10 Customize the template for the deployment. Provide the shared secret that is generated on the UI. You will have to manually configure the appliance using the VM console. Click **Next**.

11 Verify all the configuration data. Click **Finish**.

12 Once the Collector OVA is installed, start the VM and launch the console.
13 Log in with the console credential that you see on the screen and run the *setup* command.

14 Create the password for the *support* login and change the password for the *consoleuser*.

**Note**
- Your password must contain a minimum of 6 characters. A single quote (') is not allowed.
- You must change the *support* and *consoleuser* password periodically to comply with your organization policy.

15 **Network Configuration**: Enter the IP family to be associated with the network.
- Enter *ipv4* to configure your network with IPv4 capabilities.
- Enter *ipv6* to configure your network with IPv6 capabilities.
- Enter *dual-stack* to configure your network with both IPv4 and IPv6 capabilities.

16 Based on your choice in Step 15, enter the details of the IP family.

<table>
<thead>
<tr>
<th>Action</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>Enter IPv4 network configuration details such as:</td>
</tr>
<tr>
<td></td>
<td>a  <em>IP_Address</em>: Second reserved static IPv4 address.</td>
</tr>
<tr>
<td></td>
<td>b  <em>Netmask</em>: Subnet mask for the static IPv4 address.</td>
</tr>
<tr>
<td></td>
<td>c  <em>Default_Gateway</em>: Default gateway of your network.</td>
</tr>
<tr>
<td></td>
<td>d  <em>DNS</em>: DNS server of your environment. To enter multiple DNS servers, use space.</td>
</tr>
<tr>
<td></td>
<td>e  <em>Domain _Search</em>: The domain that must be appended for DNS lookups.</td>
</tr>
<tr>
<td></td>
<td>f  Enter <em>y</em> to save the configuration.</td>
</tr>
<tr>
<td>ipv6</td>
<td>Enter IPv6 network configuration details such as:</td>
</tr>
<tr>
<td></td>
<td>a  <em>IPV6_Address</em>: Second reserved static IPv6 address.</td>
</tr>
<tr>
<td></td>
<td>b  <em>IPV6_Netmask</em>: Subnet mask for the static IPv6 address.</td>
</tr>
<tr>
<td></td>
<td>c  <em>IPV6_Default Gateway</em>: Default gateway of your network.</td>
</tr>
<tr>
<td></td>
<td>d  <em>IPV6_DNS</em>: DNS server of your environment. To enter multiple DNS servers, use space.</td>
</tr>
<tr>
<td></td>
<td>e  <em>Domain _Search</em>: The domain that must be appended for DNS lookups.</td>
</tr>
<tr>
<td></td>
<td>f  Enter <em>y</em> to save the configuration.</td>
</tr>
<tr>
<td>dual-stack</td>
<td>Enter both IPv4 and IPv6 network configuration details.</td>
</tr>
</tbody>
</table>

17 **Network Time Server Configuration**: Configure NTP or secure NTP servers.
- Enter *y* if network time security is supported for the NTP server. Network time security is supported only in secure NTP servers.
- Enter *n* if network time security is not supported for the NTP server.

18 Based on your choice in step 16, enter the IP address or FQDN details of a NTP or secure NTP server. Ensure that the VMs can reach these servers. If the NTP time is out of sync, the services will fail to start.

To enter multiple servers, use commas.
19 (Optional) To configure web proxy:
   a Enter y.
   b Provide the web proxy details.

20 A check is made to see if the shared secret key has been configured. The collector is paired
with the corresponding platform. This may take few minutes.

21 All the services are verified.

22 Click Finish, when you see the Proxy Detected! message displayed on the onboarding page. You
will be redirected to the Login page.

Collector Recommendation and Other Requirements

For optimum performance, you must match the minimum recommendations for the deployment.

Recommendation for the Collector Deployment

Table 1-1. Specifications for Collector Brick Size

<table>
<thead>
<tr>
<th>Brick Size</th>
<th>Cores required for 2.1 GHz CPU</th>
<th>Cores required for 2.3 GHz CPU</th>
<th>Cores required for 2.6 GHz CPU</th>
<th>RAM</th>
<th>Disk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>12 GB</td>
<td>200 GB</td>
</tr>
<tr>
<td>Large</td>
<td>10</td>
<td>9</td>
<td>8</td>
<td>16 GB</td>
<td>200 GB</td>
</tr>
<tr>
<td>Extra Large</td>
<td>10</td>
<td>9</td>
<td>8</td>
<td>24 GB</td>
<td>200 GB</td>
</tr>
<tr>
<td>2X Large</td>
<td>20</td>
<td>18</td>
<td>16</td>
<td>48 GB</td>
<td>300 GB</td>
</tr>
</tbody>
</table>

Note The reservation for the CPU speed and RAM for each node must be 100% of the value
specified above.

Table 1-2. Collector Deployment - Maximum Capacity

<table>
<thead>
<tr>
<th>Collector Size</th>
<th>Number of VMs (K = Thousand)</th>
<th>Flows per Day (M = Million)</th>
<th>Flow count in 4 days (M = Million)</th>
<th>Number of Edges for VMware SD-WAN (K = Thousand)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium</td>
<td>4K</td>
<td>2.5M</td>
<td>3.25M</td>
<td>4K</td>
</tr>
<tr>
<td>Large</td>
<td>10K</td>
<td>5M</td>
<td>6.5M</td>
<td>6K</td>
</tr>
</tbody>
</table>
Table 1-2. Collector Deployment - Maximum Capacity (continued)

<table>
<thead>
<tr>
<th>Collector Size</th>
<th>Number of VMs (K = Thousand)</th>
<th>Flows per Day (M = Million)</th>
<th>Flow count in 4 days (M = Million)</th>
<th>Number of Edges for VMware SD-WAN (K = Thousand)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extra Large</td>
<td>35K</td>
<td>10M</td>
<td>13M</td>
<td>10K</td>
</tr>
<tr>
<td>2X Large</td>
<td>45K</td>
<td>17M</td>
<td>22M</td>
<td>10K</td>
</tr>
</tbody>
</table>

**Note**
- The count of VMs and edges mentioned in the table is the maximum individual limit for a single deployment. So, if you have edges in your setup, you might have to reduce the VM count.
- The count of VMs includes the templates on the VMware vCenter as well.
- For a single deployment with more than one collector, the limitation on the total flows across collectors is based on the capacity of the platform.

**Other Requirements and Considerations**
- The availability of the NTP service is critical to system operations. Ensure that you do not reboot the platform node or the collector node when the NTP service is not available.
- The recommended network latency between platform and collector VMs for optimal performance is up to 150ms. The system performance might degrade beyond this limit.
- For Network Map, the maximum supported firewall rules per VMware NSX-T Manager (including of DFW and edge rules) is 5000.

**Supported Web Browser**
- Google Chrome: The latest two versions.
- Mozilla Firefox: The latest two versions.

**Recommendations to Support High Availability for Collector**
You can customize vSphere HA options to enable vSphere high availability for the Collector.
- **Host Failure** - Restart VMs
- **Host Isolation** - Deactivated
- **Guest not heartbeat** - Deactivated
Setting up Operations for Networks Collector (AMI) in AWS for VMware SD-WAN

You can set up VMware Aria Operations for Networks collector for AWS by importing Amazon Machine Image (AMI) to your AWS environment.

If your environment does not have a VMware vCenter server, and you can deploy your collector in a cloud environment and then deploy your collector in AWS.

**Note** VMware Aria Operations for Networks supports the collector deployment in AWS using AMI only for VMware SD-WAN.

The procedure and task related to EC2 instances are documented in [https://docs.aws.amazon.com/efs/index.html](https://docs.aws.amazon.com/efs/index.html).

**Procedure**

1. Launch your EC2 instance using the VMware provided AMI in the Amazon EC2 console. For procedure details, see Create Your EC2 Resources and Launch Your EC2 Instance topic in the Amazon Elastic File System documentation.

   **Note** When you Launch your EC2 instance in AWS, you must select the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance type</td>
<td>m4.xlarge (MEDIUM BRICK)</td>
</tr>
<tr>
<td>Network</td>
<td>Select an appropriate network and subnet.</td>
</tr>
<tr>
<td>Storage</td>
<td>Default Storage.</td>
</tr>
<tr>
<td>Tags</td>
<td>As per customer Policies.</td>
</tr>
<tr>
<td>Security Group</td>
<td>Allow Outbound to 0.0.0.0/0 for port 443 (or for restricted rules, allow outbound for NI SaaS Prod FQDN for port 443).</td>
</tr>
<tr>
<td>Key</td>
<td>Select appropriate Key (SSH Login is enabled for the AMI).</td>
</tr>
</tbody>
</table>

2. When your EC2 instance is in the running state, log in to the instance.

3. Log in with the given console credentials. Run the `setup` command.
4 Create the password for the **support** login. Change the password for the **consoleuser**.

**Note**  After you change the password, the network options will be skipped during setup CLI.

Also, Proxy AMI does not support the following:

- IP change
- IPv6
- Web Proxy Configuration.

5 **Network Time Server Configuration**: Configure NTP or secure NTP servers.

- Enter *y* if network time security is supported for the NTP server. Network time security is supported only in secure NTP servers.
- Enter *n* if network time security is not supported for the NTP server.

6 Based on your choice in step 5, enter the IP address or FQDN details of a NTP or secure NTP server. Ensure that the VMs can reach these servers. If the NTP time is out of sync, the services will fail to start.

   To enter multiple servers, use commas.

7 A check is made to see if the shared secret key has been configured. The collector is paired with the corresponding platform. This process can take few minutes.

8 All the services are verified.

**What to do next**

Enable the flow collection from Edges to the collector you deployed in AWS. To enable the flow collection, do the following:

- Make the collector you deployed in AWS as a Non-VeloCloud Site. For details, contact VMware support.