Deploy Passive Authentication

For supported software information, click here.

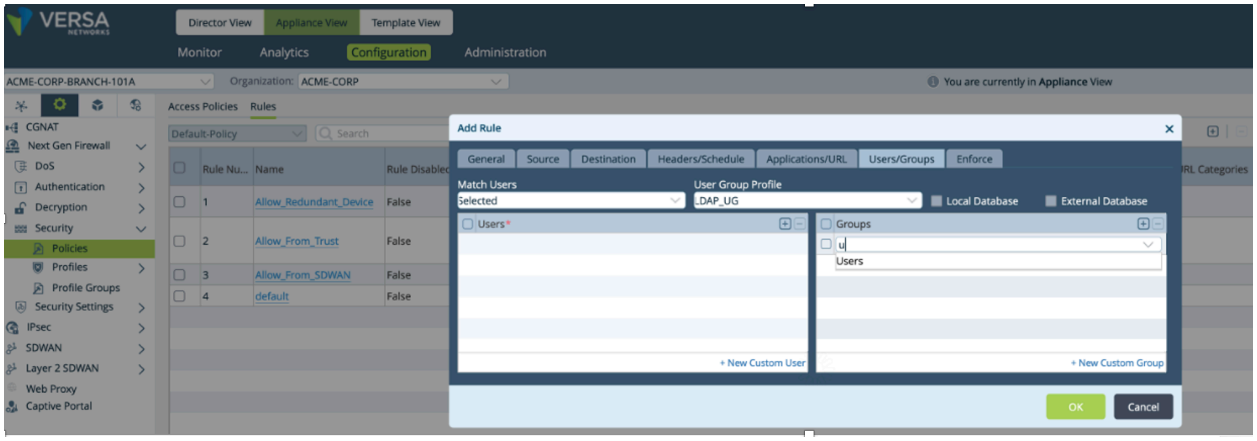
Passive authentication checks and confirms user identity without requiring any authentication action. Secure SD-WAN CPEs use Versa Messaging Service (VMS) for passive authentication and users do not have to authenticate themselves using a captive portal. This improves user experience by avoiding opening a web browser to enter their details.

VMS functions alongside the Active Directory of customers and when Active Directory authenticates a user, VMS receives a notification from the Windows WMI agent for user login or logoff events. This notification also contains the end user IP address details and VMS disseminates this information to all secure SD-WAN devices in the network.

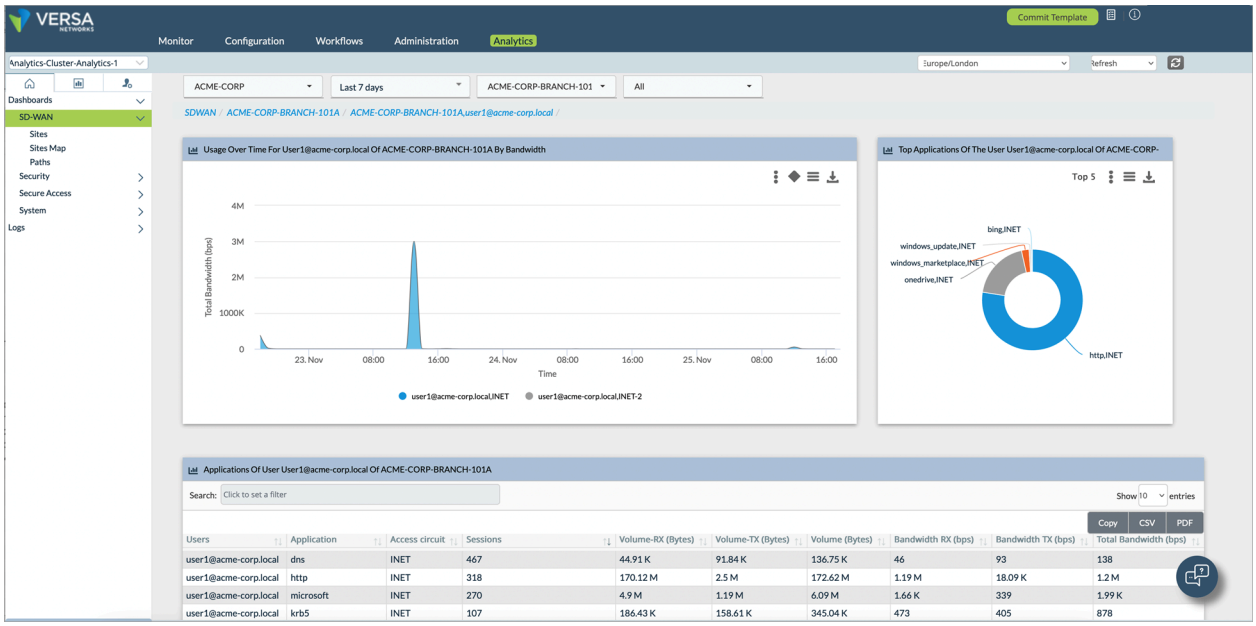
This article provides an overview of VMS and of VMS deployment architectures, and then describes the procedures for deploying passive authentication.

Overview of VMS and the WMI Agent

Passive authentication improves metadata accuracy, because it disseminates changes to user–IP address mappings in near real time to the secure SD-WAN CPE. Secure SD-WAN administrators can use this information to configure user- or user group-based rules such as firewall and SD-WAN policy. The following screenshot shows a firewall policy based on user group and user match criteria. These group details are sourced from the customer's Active Directory (AD) server and are not configured on the secure SD-WAN CPE. After you apply the rules to the secure SD-WAN CPE, VMS shares the user-to-IP-address mappings, which allows the CPE to apply the exact policy to each end user.



Passive authentication also allows you to view usernames and statistics in Analytics logs. The following example screenshot displays usernames instead of IP addresses and shows that user1, user2, and user4 have been accessing the network over the last 7 days. The screenshot does not show that these users used the same IP address (192.168.101.100) at different times. Passive authentication associates a user with an IP address when the user uses it, which improves the accuracy of information and provides better end user control.



VMS circulates user-to-IP address mappings to secure SD-WAN CPEs using the following channels:

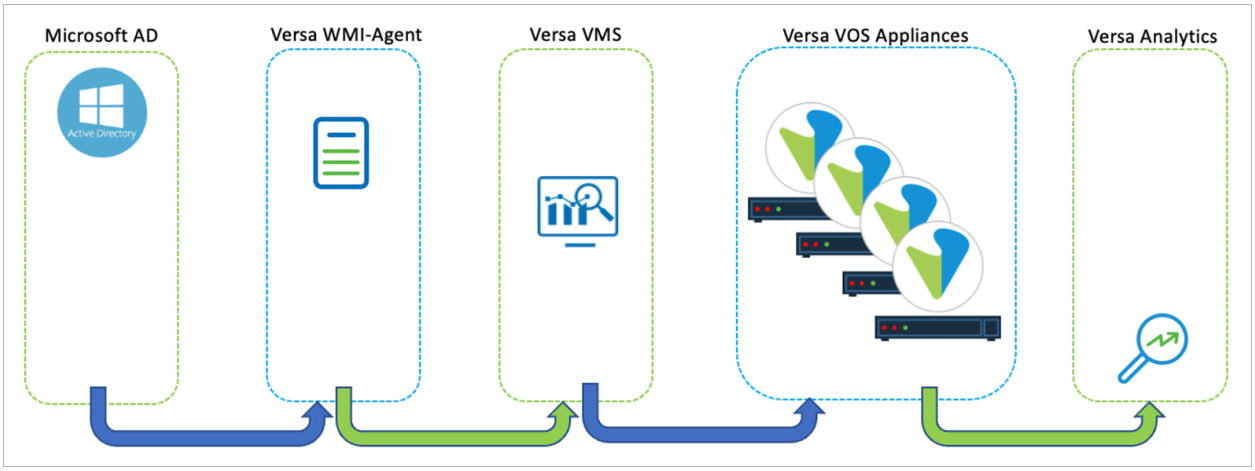
- Real-time channel—Stream data in near real time from VMS servers to secure SD-WAN CPEs that are configured to receive the user–IP address mappings.
- Bulk update channel—Create a snapshot of the user–IP address mappings available to the secure SD-WAN CPE at a configurable interval. Secure SD-WAN CPEs use this channel to synchronize user–IP mappings when the real-time channel is not available.

Alongside VMS is the Versa Windows Management Instrumentation (WMI) agent. Microsoft describes WMI as follows:

> WMI is the Microsoft implementation of Web-Based Enterprise Management (WBEM). This is an industry initiative to develop a standard technology for accessing management information in an enterprise environment. WMI uses the Common Information Model (CIM) industry standard to represent systems, applications, networks, devices, and other managed components. CIM is developed and maintained by the Distributed Management Task Force (DMTF). The ability to obtain management data from remote computers is what makes WMI useful.

The Versa WMI agent leverages this framework by obtaining login and logout events from the users' Active Directory server and sharing this data with the VMS server over a TLS channel. Figure 1 summarizes these components and shows the flow of information from Active Directory to Versa Analytics through Versa Operating System™ (VOS™) devices. Note that this example only shows real-time channel flow.

Figure 1: Flow of Information from Microsoft Active Directory to Versa Analytics



Deployment Architectures

There are two reference architectures for deploying passive authentication:

- VMS deployment in the Versa headend. This deployment architecture can be called either on-premises or off-premises depending on whether the headend is owned by a customer, a service provider, or Versa Networks.
- VMS deployment at customer site, that is, on-premises. This is the architecture discussed in this article

Figure 2 shows a VMS deployment in the Versa headend. Here, VMS is deployed in the Versa headend and the WMI agent is installed at the customer site.

Figure 2: VMS Versa Headend Deployment

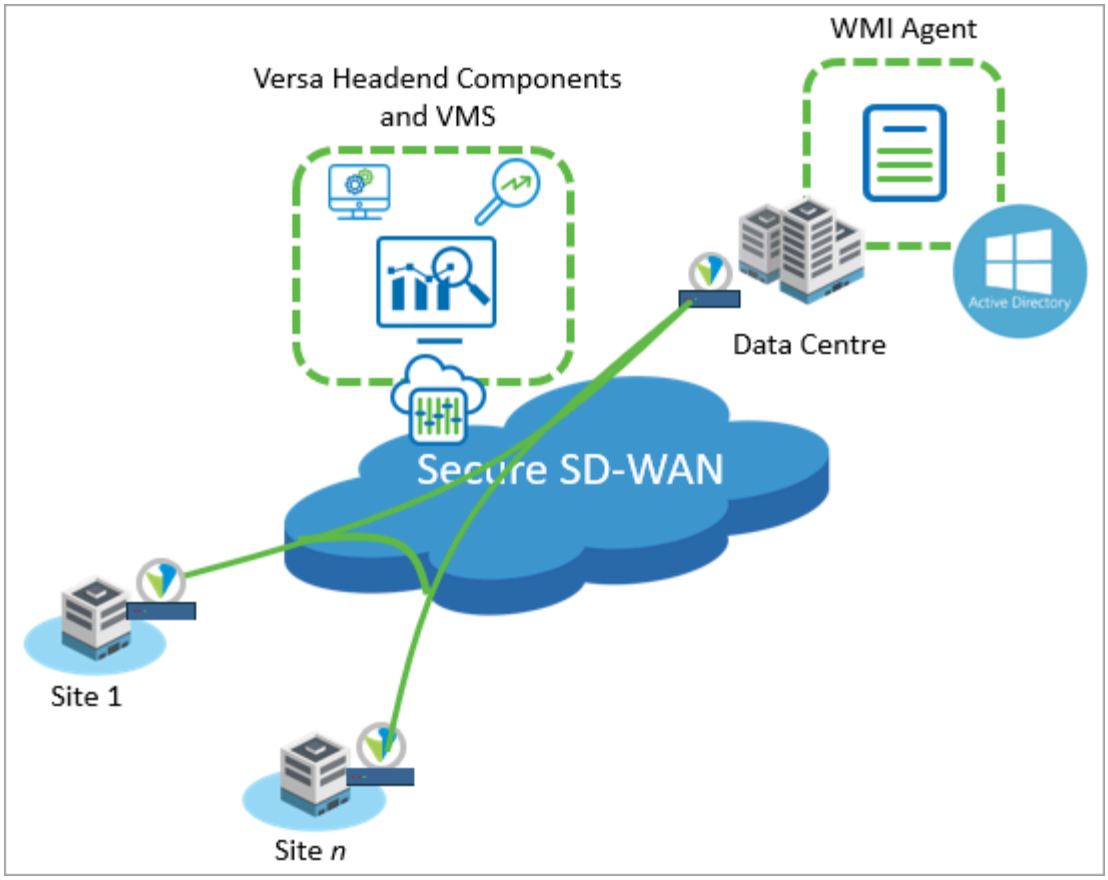
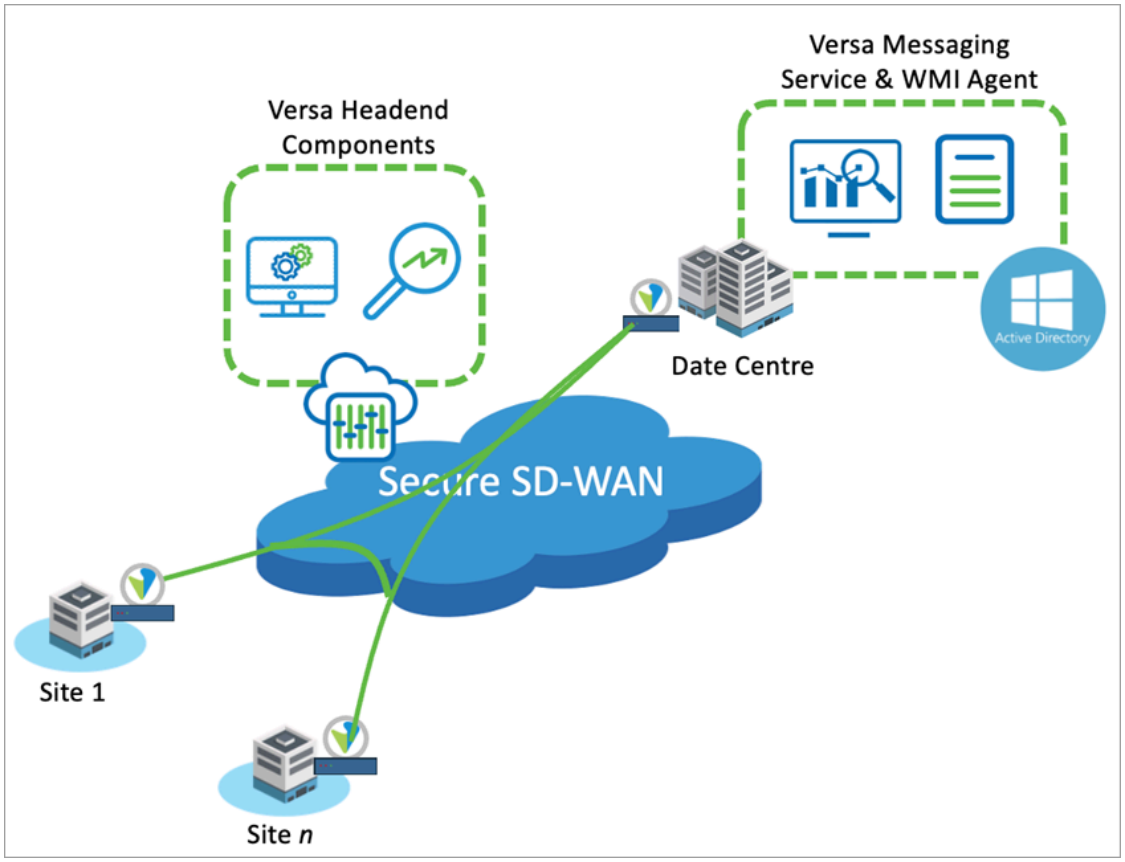


Figure 3 shows a VMS deployment at a customer site. Here, both VMS and the WMI agent are deployed in the customer data center, which may also host the customer's Active Directory.

Figure 3: VMS On-Premises Deployment



As an example scenario for resilient VMS deployment, we deploy two VMS servers in the customer network. The servers sit behind a VOS ADC load balancer. (For more information, see Configure an Application Delivery Controller.) Additionally, we deploy two Versa WMI agents. Unlike VMS, these are not behind the load balancer. Figure 4 shows the high-level overview of this architecture.

Figure 4: Resilient VMS Deployment

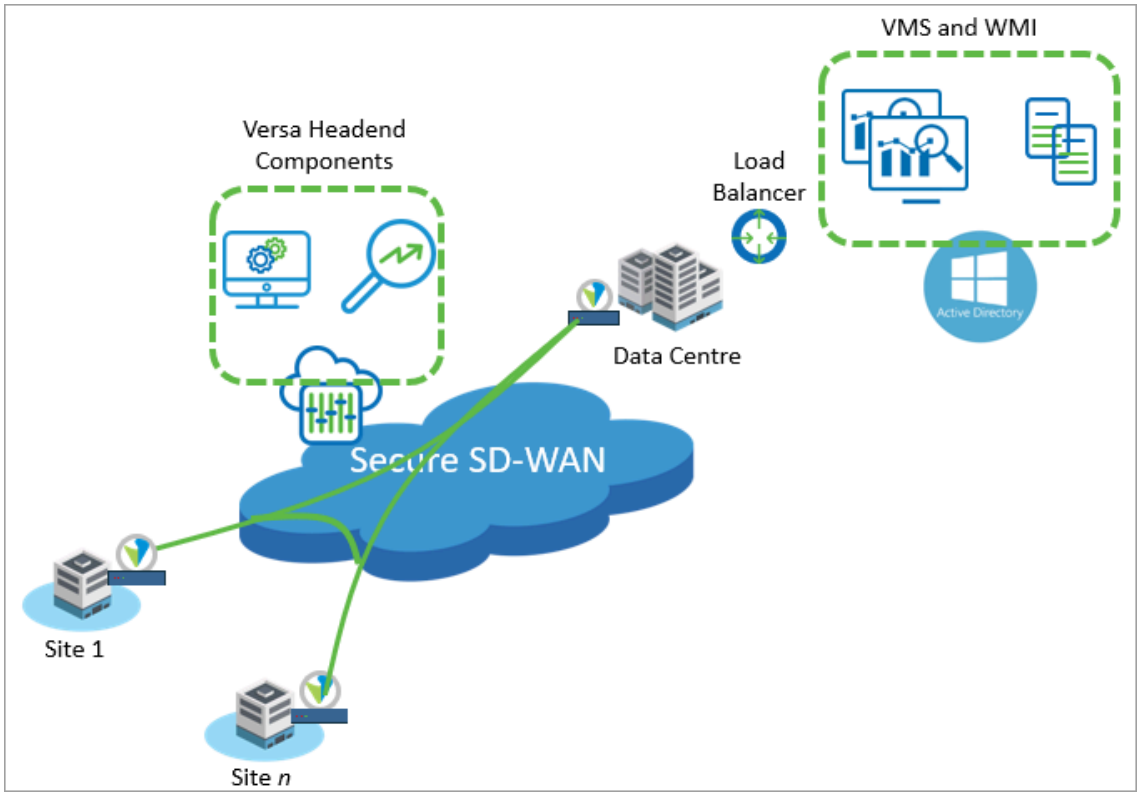


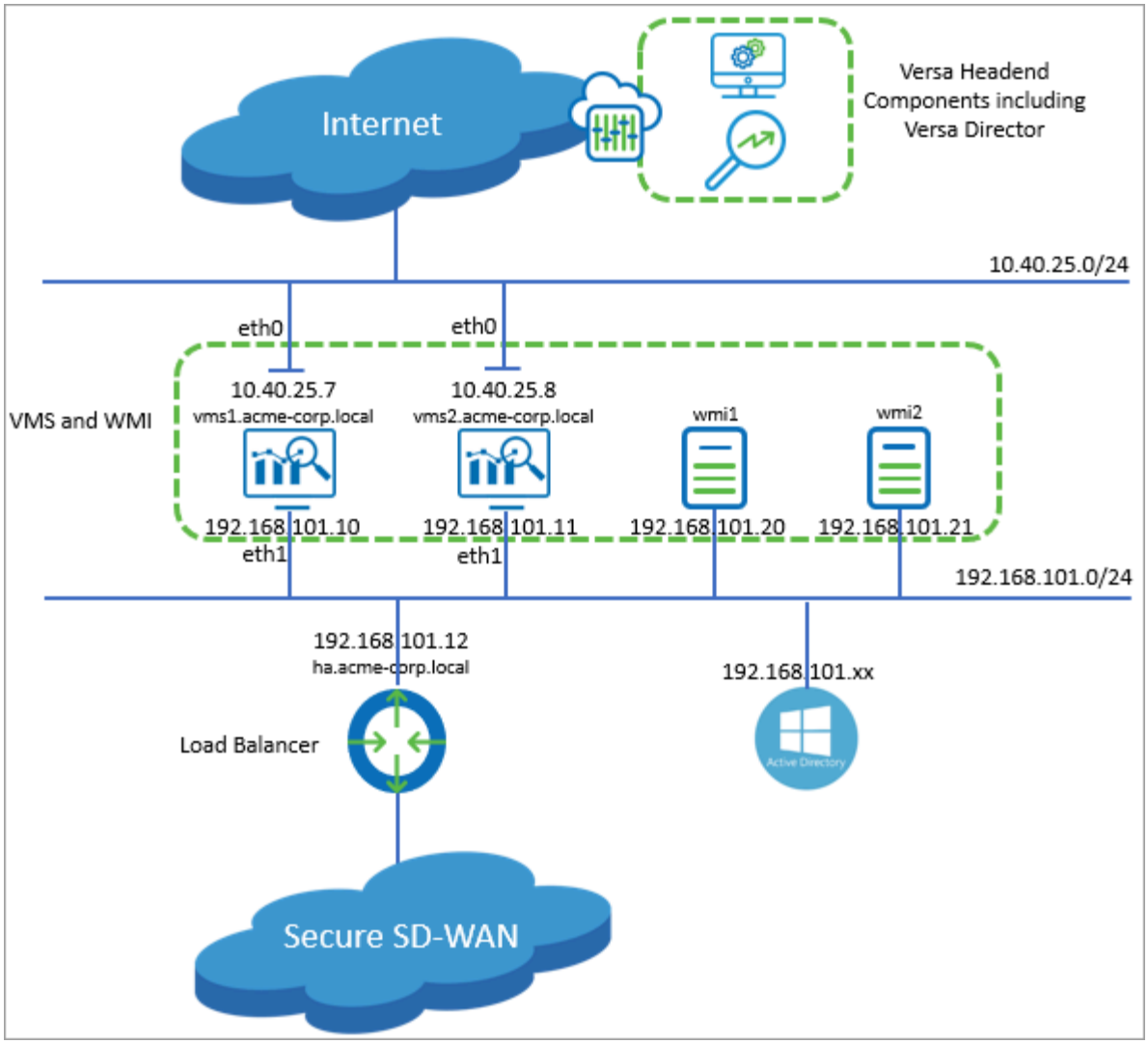
Figure 5 shows that VMS, the WMI agent, and the load balancer are located on 192.168.101.0/24. On the VMS server, this is interface eth1, which is used for bidirectional data flows between the following:

- Active Directory and WMI agent
- WMI agent and VMS
- VMS and LAN interface of secure SD-WAN CPE
- Versa Director and Active Directory (optional), through a secure SD-WAN CPE acting as a proxy appliance when communicating to Active Directory

Additionally, VMS servers have a second interface located on 10.40.25.0/24 (eth0). This interface is used for bidirectional data flows between the following:

- Management network and VMS
- VMS and Director

Figure 5: Details of Resilient VMS Deployment



As an alternate design, you can use eth0 on the VMS server for all communication. You can choose either design.

Best Practices

The following are general best practices guidelines to supplement the step-by-step configuration guidelines:

- You must configure a messaging server on all secure SD-WAN CPE at all sites. Otherwise, these CPEs cannot connect to the VMS server to collect live user data, and without this data, VMS cannot populate Analytics with username information and cannot apply policy to users or user groups.
- It is not mandatory configure LDAP server profiles and user and user group profiles on all secure SD-WAN devices. These configurations are mandatory only on the device closest to the LDAP server, if you are creating policies, such as firewall or SD-WAN–based, for users or user groups. If you are not creating such policies and use VMS to populate Analytics, you do not need to configure an LDAP server and user and user group profiles. Note that, although the Versa Director UI appears to support only a single CPE for proxy devices, you can use multiple proxies for an organization.
- To save time, use a service template for the configuration's messaging service elements rather than configuring

each device individually. Associate a preconfigured service template with the device template using a device group. For more information, see Associate a Service Template with a Device Group. The configurations in this article use a device template. If required, you can apply the same configuration using a service template.

- Connections between a secure SD-WAN branch and VMS use TLSv1.2 to encrypt username-to-IP-address mappings. For more information, see Verify Packets between the Secure SD-WAN Branch and the VMS Server, below.
- Connections between the WMI agent and VMS use TLSv1.2 to encrypt username-to-IP-address mappings. For more information, see Verify Packets between the WMI Agent and the VMS Server, below.
- VMS supports multiple LAN VRFs. Although VMS is configured on the secure SD-WAN device to connect to the VMS service on the customer LAN, the SD-WAN device needs to connect to only one VRF. However, because VMS monitors all end user login and logout events through the WMI agent, as long as these events are logged to the Active Directory server that the WMI agent monitors, it does not matter which VRFs the end users use, because the events are still captured by the VMS service.
- In VMS Release 21.2.2, the eth0 interfaces connects to the internet to complete the installation, and so this interface also connects to Versa Director. To verify this, ping the internet from the VMS server before you configure VMS.
- For the secure SD-WAN and application delivery controller (ADC) functions, use a different physical VOS device for each function. Although the same VOS device can support both functions, the secure SD-WAN CPE element of the VOS device cannot connect to the VMS service. Other secure SD-WAN devices can connect, but VOS devices that combine secure SD-WAN and ADC features are unable to connect to VMS. By separating these features onto different devices, all secure SD-WAN devices can connect to the VMS service. If you use a third-party load balancer and do not a VOS ADC, you can ignore this point.
- It is recommended that you create a user account specifically for VMS to query Versa Director. Also, set the password so that it does not need to be changed at first login and so that it never expires. Set the account permissions to TenantSuperAdmin. The examples in this article use an account named acme-corp-admin.
- It is recommended that you create a non-administrator user account on the customer's Active Directory. The WMI agent uses this account to access event logs on Active Directory. Although the steps in this article use an Administrator account, Configure Active Directory, below, describes how to create a non-administrator account.
- Configure the recommended firewall rules to permit the WMI agent to query Active Directory. For more information, see Configure Active Directory, below.

Summary of Passive Authentication Configuration

This section summarizes the procedures for configuring passive authentication. The remainder of the sections in this article provide the details for configuring the customer's DNS server, VMS servers, Active Directory, the WMI agent, Versa Director, and an application delivery controller (ADC), and they describe how to verify the configuration.

The screenshots in these procedures are from the following releases:

- Versa Director Release 21.2.3
- VOS Release 21.2.3
- VMS Release 21.2.2

The following are the high-level steps to configure and deploy passive authentication:

1. Configure the customer's DNS server. For more information, see Configure the DNS Server, below.

2. Configure VMS servers:
    a. Configure IP addressing or routing on the VMS servers.
    b. Configure the primary VMS server. (You copy the configuration to the secondary server later.)
        i. Create the root certificate.
        ii. Issue the **vsh configure-passive-auth** CLI command for the first configuration pass. Note that the organization name, Versa Director username, and password that you enter in this and all the other **vsh configure-passive-auth** commands are case-sensitive.
        iii. Issue the **vsh configure-passive-auth** CLI command for the second configuration pass.
        iv. Issue the **vsh initialize-passive-auth** CLI command to enable the VMS service.
        v. Update the permissions for the client-cert.pfx and root-ca-cert.pem certificate files.
    c. Configure the secondary VMS server:
        i. Copy all the certificates from the /opt/versa/vms/certs directory on the primary server to the same directory on the secondary server.
        ii. Update the permissions for the client-cert.pfx and root-ca-cert.pem certificate files.
        iii. Issue the **vsh configure-passive-auth** CLI command for the first configuration pass. When prompted, do not regenerate the certifications.
        iv. Issue the **vsh configure-passive-auth** CLI command for the second configuration pass. When prompted, do not regenerate the certifications.
        v. Issue the **vsh initialize-passive-auth** CLI command to enable the VMS service.

    For more information, see Configure VMS, below.

3. Configure Active Directory:
    a. Update firewall rules.
    b. Configure a non-administrator user.

    For more information, see Configure Active Directory, below.

4. Configure the WMI agent:
    a. Copy the client-cert.pfx and root-ca-cert.pem files from the VMS server to the WMI agent.
    b. Install the root-ca-cert.pem certificate in the Trusted Root Certificate Authority folder using certlm.msc.
    c. Install the WMI agent software.
    d. Configure the WMI agent software:
        i. Configure Active Directory:
            a. For resilience, add two or more LDAP servers.
        ii. Configure the VMS server:
            a. Add both VMS servers. The WMI agent communicates with both VMS servers directly and does not use load balancer.
            b. Import the client-cert.pfx certificate.

    For more information, see Configure the WMI Agent, below.

5. Configure the secure SD-WAN CPE using Versa Director:

a. On Versa Director, upload the root-ca-cert.pem certificate from VMS to the CA certificates.
b. Configure the secure SD-WAN CPE:
    i. Configure DNS settings.
    ii. Configure the messaging service.
    iii. Configure the passive authentication profile.
    iv. Optionally, configure the LDAP server profile and user or group profile. For more information, see Best Practices, above.
c. Optional, configure firewall policy or SD-WAN policy based on users or user groups.

For more information, see Configure Passive Authentication on the Versa Director, below.

6. Configure an ADC. Secure SD-WAN CPEs connect to VMS servers through an ADC load balancer that is hosted in front of the VMS servers. You can use any load balancer for this function, including a VOS device. If you use a VOS device, perform the following high-level steps to configure ADC:
    a. Configure a VIP interface on the VOS device.
    b. Add the ADC service.
    c. Configure the ADC service.

    For more information, see Configure an Application Delivery Controller, below.

7. Verify the passive authentication configurations. For more information, see Verify the Passive Authentication Deployment, below.

Configure the DNS Server

You must configure the customer's DNS server. To do this, you create the following DNS records on the customer's DNS server:

- VMS Server 1—For example, 192.168.101.10, vms1.acme-corp.local
- VMS Server 2—For example,192.168.101.11, vms2.acme-corp.local
- VMS VIP—For example, 192.168.101.12, ha.acme-corp.local

Configure VMS

The following sections describe how to install and configure VMS service on VMS server. To configure VMS, you do the following:

1. Configure the Ethernet interfaces on the VMS servers.
2. Install and configure the primary VMS server.
3. Configure the standby VMS server.

Note that the following are the default login credentials for VMS:

- Username—admin
- Password—versa123

Configure the Ethernet Interfaces on the VMS Servers

To configure the Ethernet interfaces on the VMS servers, you edit the /etc/network/interfaces file. To edit this file, you must have sudo privileges.

To configure the Ethernet interfaces:

1. Log in to the primary VMS server.
2. Edit the /etc/network/interfaces file:

```
[admin@vms1: ~] $ sudo cat /etc/network/interfaces
[sudo] password for admin:
```

3. Enter the password. The default password is versa123.
4. In the interfaces file, configure the correct IP addresses on the eth0 and eth1 interfaces. eth0 is typically the management interface, and eth0 connects to the network on which the secure SD-WAN CPE and the WMI agent server are located. In our example here, this network is vms1.acme-corp.local, and its IP address is 192.168.101.10.

```
[admin@vms1: ~] $ sudo cat /etc/network/interfaces
[sudo] password for admin:
# interfaces(5) file used by ifup(8) and ifdown(8)
# Include files from /etc/network/interfaces.d:
# ETH0 is the management interface. It is also used to access Versa Director (hosted on the internet).
auto eth0
iface eth0 inet static
address 10.40.25.7
netmask 255.255.0.0
gateway 10.40.0.1

# ETH1 is used to push user-mapping information to the secure SD-WAN CPE and to connect with the WMI agent.
auto eth1
iface eth1 inet static
address 192.168.101.10
netmask 255.255.255.0

# Static routes to the LAN address ranges connected to the secure SD-WAN CPE are required on VMS. When the secure
# SD-WAN CPE requests user-IP mapping information from VMS, the secure SD-WAN CPE uses the LAN interface to
# make this request. Therefore, a route must exist on VMS to route traffic back to the CPE using ETH1; otherwise,
# it follows the default route using ETH0). If WMI agent is in another address range than VMS, a route for the
# WMI agent is also required for routing using ETH1.
post-up route add -net 192.168.0.0 netmask 255.255.0.0 gw 192.168.101.1
```

5. Save the changes to the /etc/network/interfaces file.
6. Repeat Steps 1 through 5 for the secondary VMS server. In our example, this network is vms2.acme-corp.local, its eth0 interface address is 10.40.25.8, and its eth1 address is 192.168.101.11.

Install and Configure the Primary VMS Server

1. Generate a root certificate by issuing a CLI command in the following format. Type the command on a single. Replace all variables indicated in italicized text with the appropriate values. Note that you cannot continue the installation without generating a root certificate. Currently, Versa does not support the use of the customer's own root certificates. This phase of configuration may take up to 10 minutes.

   > [admin@vms1: ~] **sudo /opt/versa/vms/certs/vms_cert_gen.sh --domain** *domain-name* **--country** *country*
   > **--state** *state* **--locality** *location* **--organization** *organization-name* **--organizationalunit** *unit-name*
   > **--email** *email-address* **--keypass** *password* **--validity** *validity* **--san** *san*,**DNS:***dns-name*

   For example:

   > [admin@vms1: ~] **sudo /opt/versa/vms/certs/vms_cert_gen.sh --domain ha --country US --state CA --locality SC --organization acme-corp.local --organizationalunit SE --email admin@acme-corp.local --keypass versa123 --validity 700 --san ha.acme-corp.local,DNS:ha**

2. To execute the first phase of the configuration of the active VMS server, issue the **vsh configure-passive-auth** CLI command. For example:

   > [admin@versa-msgservice: ~] $ **vsh configure-passive-auth**
   >
   > First-time configuration!
   >
   > Is the primary interface configuration finalized? (y/N) : **y**
   >
   > Management Interface IP of this VMS server
   > Please Enter this VMS Server Management/Primary Interface IP Address: **10.40.25.7**
   > # This is the management interface of the VMS server. In this example, it is ETH0.
   >
   > FQDN of this VMS server
   > Please enter the FQDN of this VMS Server: **vms1.acme-corp.local**
   > # This is the FQDN of the active VMS server.
   >
   > It may take up to 10 minutes to complete initialization.
   >
   > Adding new hosts entry.
   > It may take up to 10 minutes to complete initialization.
   >
   > Info: Installing Kubernetes ...
   > Info: Creating auto completions for kubectl
   > Info: Disabling Swap ...
   > Info: Creating Docker overlay ....
   > Enable and restart Docker
   > Info: Enable and restart Docker
   > total 963988

```
-rw-rw-r-- 1 versa versa  15131067 Jul 20 12:52 flannel.tar.bz2
-rw-rw-r-- 1 versa versa  78435054 Jul 20 12:52 etcd.tar.bz2
-rw-rw-r-- 1 versa versa  12502350 Jul 20 12:52 coredns.tar.bz2
-rw-rw-r-- 1 versa versa 231355183 Jul 20 12:52 concentrator.tar.bz2
-rw-rw-r-- 1 versa versa  26220780 Jul 20 12:52 kube-apiserver.tar.bz2
-rw-rw-r-- 1 versa versa 223233125 Jul 20 12:52 ise-agent.tar.bz2
-rw-rw-r-- 1 versa versa   3904253 Jul 20 12:52 message-server.tar.bz2
-rw-rw-r-- 1 versa versa  12427735 Jul 20 12:52 kube-scheduler.tar.bz2
-rw-rw-r-- 1 versa versa  42734652 Jul 20 12:52 kube-proxy.tar.bz2
-rw-rw-r-- 1 versa versa  25608143 Jul 20 12:52 kube-controller-manager.tar.bz2
-rw-rw-r-- 1 versa versa    284858 Jul 20 12:52 pause.tar.bz2
-rw-rw-r-- 1 versa versa  34510568 Jul 20 12:52 nginx.tar.bz2
-rw-rw-r-- 1 versa versa  33491344 Jul 20 12:52 redis.tar.bz2
-rw-rw-r-- 1 versa versa 209158609 Jul 20 12:52 pkg-builder.tar.bz2
-rw-rw-r-- 1 versa versa  21255565 Jul 20 12:52 vxdev.tar.bz2
-rw-rw-r-- 1 versa versa   3814471 Jul 20 12:52 uipmap.tar.bz2
-rw-rw-r-- 1 versa versa   3844141 Jul 20 12:52 sgt-server.tar.bz2
-rw-rw-r-- 1 versa versa   9155314 Jul 20 12:52 registry.tar.bz2
drwxrwxr-x 4 versa versa      4096 Aug  2 11:32 ..
drwxrwxr-x 2 versa versa      4096 Aug  2 11:32 .
Extracting concentrator.tar.bz2...
Loading concentrator.tar ...
Loaded image: concentrator:1.0.0
Extracting coredns.tar.bz2...
Loading coredns.tar ...
Loaded image: k8s.gcr.io/coredns:1.7.0
Extracting etcd.tar.bz2...
Loading etcd.tar ...
Loaded image: k8s.gcr.io/etcd:3.4.13-0
Extracting flannel.tar.bz2...
Loading flannel.tar ...
Loaded image: quay.io/coreos/flannel:v0.11.0-amd64
Extracting ise-agent.tar.bz2...
Loading ise-agent.tar ...
Loaded image: ise-agent:1.0.0
Extracting kube-apiserver.tar.bz2...
Loading kube-apiserver.tar ...
Loaded image: k8s.gcr.io/kube-apiserver:v1.20.4
Extracting kube-controller-manager.tar.bz2...
Loading kube-controller-manager.tar ...
Loaded image: k8s.gcr.io/kube-controller-manager:v1.20.4
Extracting kube-proxy.tar.bz2...
Loading kube-proxy.tar ...
Loaded image: k8s.gcr.io/kube-proxy:v1.20.4
Extracting kube-scheduler.tar.bz2...
Loading kube-scheduler.tar ...
Loaded image: k8s.gcr.io/kube-scheduler:v1.20.4
Extracting message-server.tar.bz2...
Loading message-server.tar ...
Loaded image: message-server:1.0.0
Extracting nginx.tar.bz2...
Loading nginx.tar ...
Loaded image: nginx:1.7.9
Extracting pause.tar.bz2...
```

```
Loading pause.tar ...
Loaded image: k8s.gcr.io/pause:3.2
Extracting pkg-builder.tar.bz2...
Loading pkg-builder.tar ...
Loaded image: pkg-builder:1.0.0
Extracting redis.tar.bz2...
Loading redis.tar ...
Loaded image: redis:1.0.0
Extracting registry.tar.bz2...
Loading registry.tar ...
Loaded image: registry:2
Extracting sgt-server.tar.bz2...
Loading sgt-server.tar ...
Loaded image: sgt-server:1.0.0
Extracting uipmap.tar.bz2...
Loading uipmap.tar ...
Loaded image: uipmap:1.0.0
Extracting vxdev.tar.bz2...
Loading vxdev.tar ...
Loaded image: vxdev:1.0.0
REPOSITORY                      TAG           IMAGE ID       CREATED         SIZE
ise-agent                       1.0.0         2141ac3cc15a   4 months ago    583MB
redis                           1.0.0         f90a716ad2d5   4 months ago    106MB
concentrator                    1.0.0         adac8a6cc21f   4 months ago    603MB
message-server                  1.0.0         694409633c8e   4 months ago    11.6MB
uipmap                          1.0.0         f70397c65c49   4 months ago    11.2MB
pkg-builder                     1.0.0         2cdf8332ff38   4 months ago    536MB
vxdev                           1.0.0         1048f85397f0   7 months ago    61.4MB
sgt-server                      1.0.0         646ed51aa809   14 months ago   11.3MB
k8s.gcr.io/kube-proxy           v1.20.4       c29e6c583067   21 months ago   118MB
k8s.gcr.io/kube-apiserver       v1.20.4       ae5eb22e4a9d   21 months ago   122MB
k8s.gcr.io/kube-controller-manager   v1.20.4       0a41a1414c53   21 months ago   116MB
k8s.gcr.io/kube-scheduler       v1.20.4       5f8cb769bd73   21 months ago   47.3MB
k8s.gcr.io/etcd                 3.4.13-0      0369cf4303ff   2 years ago     253MB
registry                        2             2d4f4b5309b1   2 years ago     26.2MB
k8s.gcr.io/coredns              1.7.0         bfe3a36ebd25   2 years ago     45.2MB
k8s.gcr.io/pause                3.2           80d28bedfe5d   2 years ago     683kB
quay.io/coreos/flannel          v0.11.0-amd64   ff281650a721   3 years ago     52.6MB
nginx                           1.7.9         84581e99d807   7 years ago     91.7MB
Info: Initialize Kubernetes; this will take a few mins
Info: Kube Init successful
Info: Init Flannel
podsecuritypolicy.policy/psp.flannel.unprivileged created
Warning: rbac.authorization.k8s.io/v1beta1 ClusterRole is deprecated in v1.17+, unavailable in v1.22+;
use rbac.authorization.k8s.io/v1 ClusterRole
clusterrole.rbac.authorization.k8s.io/flannel created
Warning: rbac.authorization.k8s.io/v1beta1 ClusterRoleBinding is deprecated in v1.17+, unavailable in v1.
22+; use rbac.authorization.k8s.io/v1 ClusterRoleBinding
clusterrolebinding.rbac.authorization.k8s.io/flannel created
serviceaccount/flannel created
configmap/kube-flannel-cfg created
daemonset.apps/kube-flannel-ds-amd64 created
daemonset.apps/kube-flannel-ds-arm64 created
daemonset.apps/kube-flannel-ds-arm created
```

```
daemonset.apps/kube-flannel-ds-ppc64le created
daemonset.apps/kube-flannel-ds-s390x created
Info: Kubernetes: All-In-One
node/vms1.acme-corp.local untainted
Info: Create local registry
8e5640b62e6bee1f9a41cb7b049bebd90b5024cafc5b57ab297c8d023640accb
REPOSITORY                      TAG           IMAGE ID       CREATED         SIZE
ise-agent                       1.0.0         2141ac3cc15a   4 months ago    583MB
redis                           1.0.0         f90a716ad2d5   4 months ago    106MB
concentrator                    1.0.0         adac8a6cc21f   4 months ago    603MB
message-server                  1.0.0         694409633c8e   4 months ago    11.6MB
uipmap                          1.0.0         f70397c65c49   4 months ago    11.2MB
pkg-builder                     1.0.0         2cdf8332ff38   4 months ago    536MB
vxdev                           1.0.0         1048f85397f0   7 months ago    61.4MB
sgt-server                      1.0.0         646ed51aa809   14 months ago   11.3MB
k8s.gcr.io/kube-proxy           v1.20.4       c29e6c583067   21 months ago   118MB
k8s.gcr.io/kube-controller-manager   v1.20.4       0a41a1414c53   21 months ago   116MB
k8s.gcr.io/kube-apiserver       v1.20.4       ae5eb22e4a9d   21 months ago   122MB
k8s.gcr.io/kube-scheduler       v1.20.4       5f8cb769bd73   21 months ago   47.3MB
k8s.gcr.io/etcd                 3.4.13-0      0369cf4303ff   2 years ago     253MB
registry                        2             2d4f4b5309b1   2 years ago     26.2MB
k8s.gcr.io/coredns              1.7.0         bfe3a36ebd25   2 years ago     45.2MB
k8s.gcr.io/pause                3.2           80d28bedfe5d   2 years ago     683kB
quay.io/coreos/flannel          v0.11.0-amd64 ff281650a721   3 years ago     52.6MB
nginx                           1.7.9         84581e99d807   7 years ago     91.7MB
The push refers to repository [localhost:5000/message-server]
24613632e82e: Preparing
24613632e82e: Pushed
1.0.0: digest: sha256:52457938af81f3708a49292437df8490824de1906b8e5b18618ae254b0142ed0 size:
528
The push refers to repository [localhost:5000/redis]
94dd67a59053: Preparing
258a1ab6dab5: Preparing
35613d8e624a: Preparing
0302cabf4dde: Preparing
6eeff2593e88: Preparing
9eef6e3cc293: Preparing
89ce1a07a7e4: Preparing
7e718b9c0c8c: Preparing
9eef6e3cc293: Waiting
89ce1a07a7e4: Waiting
7e718b9c0c8c: Waiting
258a1ab6dab5: Pushed
0302cabf4dde: Pushed
35613d8e624a: Pushed
94dd67a59053: Pushed
89ce1a07a7e4: Pushed
9eef6e3cc293: Pushed
6eeff2593e88: Pushed
7e718b9c0c8c: Pushed
1.0.0: digest: sha256:2f9e3dea6c1896b20fea2c09105269c01b5b78b6c9a6c51324c3352ab4ea6a3a size:
1992
The push refers to repository [localhost:5000/vxdev]
e16707a6a3f2: Preparing
```

```
fb05eb894d9b: Preparing
c3c8752efcba: Preparing
55eb4e5bef72: Preparing
6dae8915d345: Preparing
02130b505ed2: Preparing
99496a4bc26e: Preparing
9e5f7f0191e2: Preparing
cb381a32b229: Preparing
02130b505ed2: Waiting
99496a4bc26e: Waiting
9e5f7f0191e2: Waiting
cb381a32b229: Waiting
55eb4e5bef72: Pushed
c3c8752efcba: Pushed
e16707a6a3f2: Pushed
6dae8915d345: Pushed
02130b505ed2: Pushed
fb05eb894d9b: Pushed
9e5f7f0191e2: Pushed
cb381a32b229: Pushed
99496a4bc26e: Pushed
1.0.0: digest: sha256:139c9af272bcfc2ddd5cc4ac1d593141ec88a785d96977a1b798c559c01199e0 size:
2202
The push refers to repository [localhost:5000/concentrator]
15d2dcf2da64: Preparing
9b98a31e6cf4: Preparing
0554dc362645: Preparing
40a07d74f60b: Preparing
a404f63be022: Preparing
badb85343016: Preparing
6f15325cc380: Preparing
1e77dd81f9fa: Preparing
030309cad0ba: Preparing
badb85343016: Waiting
6f15325cc380: Waiting
1e77dd81f9fa: Waiting
030309cad0ba: Waiting
9b98a31e6cf4: Pushed
40a07d74f60b: Pushed
0554dc362645: Pushed
15d2dcf2da64: Pushed
6f15325cc380: Pushed
1e77dd81f9fa: Pushed
a404f63be022: Pushed
030309cad0ba: Pushed
badb85343016: Pushed
1.0.0: digest: sha256:8f1addecf664181ef42f542e9e92e2e76b8478778f17aa7a6deb647982beacce size:
2198
The push refers to repository [localhost:5000/uipmap]
94178e95f838: Preparing
94178e95f838: Pushed
1.0.0: digest: sha256:e7746eca1995900e4d643a2edae055740046da6338595ef009e478b871bd22c7 size:
528
The push refers to repository [localhost:5000/pkg-builder]
```

```
da3f6ab864b6: Preparing
f690be4f6cdd: Preparing
2719c9c4257e: Preparing
0a83fc3d286e: Preparing
7b2781c31a7a: Preparing
ec60cb431167: Preparing
e6d9d10bab7e: Preparing
a9ae8da98746: Preparing
22f708c101a3: Preparing
90b04e3f5fa7: Preparing
454f4316781b: Preparing
28d6f0f37200: Preparing
9e6ae86b45a6: Preparing
d10e36763753: Preparing
6f15325cc380: Preparing
1e77dd81f9fa: Preparing
030309cad0ba: Preparing
ec60cb431167: Waiting
e6d9d10bab7e: Waiting
a9ae8da98746: Waiting
28d6f0f37200: Waiting
9e6ae86b45a6: Waiting
d10e36763753: Waiting
22f708c101a3: Waiting
90b04e3f5fa7: Waiting
454f4316781b: Waiting
6f15325cc380: Waiting
1e77dd81f9fa: Waiting
030309cad0ba: Waiting
0a83fc3d286e: Pushed
f690be4f6cdd: Pushed
7b2781c31a7a: Pushed
da3f6ab864b6: Pushed
2719c9c4257e: Pushed
ec60cb431167: Pushed
e6d9d10bab7e: Pushed
a9ae8da98746: Pushed
22f708c101a3: Pushed
90b04e3f5fa7: Pushed
6f15325cc380: Mounted from concentrator
1e77dd81f9fa: Mounted from concentrator
9e6ae86b45a6: Pushed
030309cad0ba: Mounted from concentrator
454f4316781b: Pushed
28d6f0f37200: Pushed
d10e36763753: Pushed
1.0.0: digest: sha256:841fd868da899661de486a38a0f2ada7ecf8b96eb2e033909f487e46295883eb size:
3860
The push refers to repository [localhost:5000/ise-agent]
77f26c1e8a52: Preparing
372336e7e177: Preparing
4b43f9e40e2a: Preparing
c07cd577fd36: Preparing
1896bb642302: Preparing
```

```
6f15325cc380: Preparing
1e77dd81f9fa: Preparing
030309cad0ba: Preparing
6f15325cc380: Waiting
1e77dd81f9fa: Waiting
030309cad0ba: Waiting
c07cd577fd36: Pushed
372336e7e177: Pushed
6f15325cc380: Mounted from pkg-builder
77f26c1e8a52: Pushed
4b43f9e40e2a: Pushed
1e77dd81f9fa: Mounted from pkg-builder
030309cad0ba: Mounted from pkg-builder
1896bb642302: Pushed
1.0.0: digest: sha256:263ee5a11c9c15902af068915f232428b39efc51ee69e2ef9a726e7a30fd4279 size:
1989
The push refers to repository [localhost:5000/sgt-server]
20f8baca1e24: Preparing
20f8baca1e24: Pushed
1.0.0: digest: sha256:eefea21a6587cafb66476de7bfda66687c8caa8a4097b5f2b11ea6aaaf57453f size:
528
NAME                  STATUS   ROLES                  AGE     VERSION
vms1.acme-corp.local   Ready    control-plane,master   5m16s   v1.20.4
Name:               vms1.acme-corp.local
Roles:              control-plane,master
Labels:             beta.kubernetes.io/arch=amd64
                    beta.kubernetes.io/os=linux
                    kubernetes.io/arch=amd64
                    kubernetes.io/hostname=vms1.acme-corp.local
                    kubernetes.io/os=linux
                    node-role.kubernetes.io/control-plane=
                    node-role.kubernetes.io/master=
Annotations:        flannel.alpha.coreos.com/backend-data: {"VtepMAC":"ae:c8:02:6b:a0:83"}
                    flannel.alpha.coreos.com/backend-type: vxlan
                    flannel.alpha.coreos.com/kube-subnet-manager: true
                    flannel.alpha.coreos.com/public-ip: 10.40.25.7
                    kubeadm.alpha.kubernetes.io/cri-socket: /var/run/dockershim.sock
                    node.alpha.kubernetes.io/ttl: 0
                    volumes.kubernetes.io/controller-managed-attach-detach: true
CreationTimestamp:  Mon, 05 Dec 2022 03:03:00 -0800
Taints:             <none>
Unschedulable:      false
Lease:
  HolderIdentity:  vms1.acme-corp.local
  AcquireTime:     <unset>
  RenewTime:       Mon, 05 Dec 2022 03:08:13 -0800
Conditions:
  Type             Status  LastHeartbeatTime                 LastTransitionTime                Reason
Message
  ----             ------  -----------------                 ------------------                ------
  -------
  MemoryPressure   False   Mon, 05 Dec 2022 03:07:54 -0800   Mon, 05 Dec 2022 03:02:55 -0800
KubeletHasSufficientMemory   kubelet has sufficient memory available
  DiskPressure     False   Mon, 05 Dec 2022 03:07:54 -0800   Mon, 05 Dec 2022 03:02:55 -0800
KubeletHasNoDiskPressure     kubelet has no disk pressure
```

```
  PIDPressure      False   Mon, 05 Dec 2022 03:07:54 -0800   Mon, 05 Dec 2022 03:02:55 -0800
KubeletHasSufficientPID      kubelet has sufficient PID available
  Ready            True    Mon, 05 Dec 2022 03:07:54 -0800   Mon, 05 Dec 2022 03:03:32 -0800
KubeletReady                 kubelet is posting ready status. AppArmor enabled
Addresses:
  InternalIP:  10.40.25.7
  Hostname:    vms1.acme-corp.local
Capacity:
  cpu:                4
  ephemeral-storage:  255959548Ki
  hugepages-2Mi:      0
  memory:             4038796Ki
  pods:               110
Allocatable:
  cpu:                4
  ephemeral-storage:  235892319047
  hugepages-2Mi:      0
  memory:             3936396Ki
  pods:               110
System Info:
  Machine ID:                 d7663e735f3241518255e013c9340f06
  System UUID:                C1A23613-2D33-4308-848D-20D3BFF0DAF7
  Boot ID:                    39f5dbce-e7a5-4cfc-ac9c-749c05677fc1
  Kernel Version:             4.15.0-112-generic
  OS Image:                   Ubuntu 18.04.5 LTS
  Operating System:           linux
  Architecture:               amd64
  Container Runtime Version:  docker://20.10.7
  Kubelet Version:            v1.20.4
  Kube-Proxy Version:         v1.20.4
PodCIDR:                      10.244.0.0/24
PodCIDRs:                     10.244.0.0/24
Non-terminated Pods:          (8 in total)
  Namespace                   Name                                       CPU Requests  CPU Limits  Memory Requests
Memory Limits  AGE
  ---------                   ----                                       ------------  ----------  ---------------  -------------  ---
  kube-system                 coredns-74ff55c5b-l8jwd                    100m (2%)     0 (0%)      70Mi (1%)
170Mi (4%)     4m57s
  kube-system                 coredns-74ff55c5b-vvwcj                    100m (2%)     0 (0%)      70Mi (1%)
170Mi (4%)     4m57s
  kube-system                 etcd-vms1.acme-corp.local                  100m (2%)     0 (0%)      100Mi (2%)
0 (0%)         4m55s
  kube-system                 kube-apiserver-vms1.acme-corp.local        250m (6%)     0 (0%)      0
(0%)           0 (0%)         4m55s
  kube-system                 kube-controller-manager-vms1.acme-corp.local  200m (5%)     0 (0%)      0
(0%)           0 (0%)         4m55s
  kube-system                 kube-flannel-ds-amd64-bw89w                100m (2%)     100m (2%)   50Mi
(1%)       50Mi (1%)      4m57s
  kube-system                 kube-proxy-rns5j                           0 (0%)        0 (0%)      0 (0%)           0
(0%)         4m57s
  kube-system                 kube-scheduler-vms1.acme-corp.local        100m (2%)     0 (0%)      0
(0%)           0 (0%)         4m55s
Allocated resources:
  (Total limits may be over 100 percent, that is, overcommitted.)
```

```
  Resource           Requests    Limits
  --------           --------    ------
  cpu                950m (23%)  100m (2%)
  memory             290Mi (7%)  390Mi (10%)
  ephemeral-storage  100Mi (0%)  0 (0%)
  hugepages-2Mi      0 (0%)      0 (0%)
Events:
  Type    Reason                   Age                From        Message
  ----    ------                   ----               ----        -------
  Normal  NodeHasSufficientPID     6m30s (x7 over 6m40s)  kubelet     Node vms1.acme-corp.local status
is now: NodeHasSufficientPID
  Normal  NodeAllocatableEnforced  6m29s                  kubelet     Updated Node Allocatable limit across
pods
  Normal  NodeHasSufficientMemory  6m26s (x8 over 6m40s)  kubelet     Node vms1.acme-corp.local
status is now: NodeHasSufficientMemory
  Normal  NodeHasNoDiskPressure    6m26s (x8 over 6m40s)  kubelet     Node vms1.acme-corp.local
status is now: NodeHasNoDiskPressure
  Normal  Starting                 4m56s                  kubelet     Starting kubelet.
  Normal  NodeHasSufficientMemory  4m56s                  kubelet     Node vms1.acme-corp.local status is
now: NodeHasSufficientMemory
  Normal  NodeHasNoDiskPressure    4m56s                  kubelet     Node vms1.acme-corp.local status is
now: NodeHasNoDiskPressure
  Normal  NodeHasSufficientPID     4m56s                  kubelet     Node vms1.acme-corp.local status is now:
NodeHasSufficientPID
  Normal  NodeAllocatableEnforced  4m55s                  kubelet     Updated Node Allocatable limit across
pods
  Normal  Starting                 4m48s                  kube-proxy  Starting kube-proxy.
  Normal  NodeReady                4m45s                  kubelet     Node vms1.acme-corp.local status is now:
NodeReady
Mon Dec  5 03:08:17 PST 2022 File /opt/versa/etc/initial_install is deleted by /opt/versa/scripts/install/vms_
install_helper.sh
Info: Initial Installation is completed
Initial setup completed
Please run "vsh configure-SERVICE_NAME" to begin your configuration.
```

3. To execute the second phase of the configuration of the active VMS server, issue the **vsh configure-passive-auth** CLI command again. For example:

```
[admin@versa-msgservice: ~] $ vsh configure-passive-auth
[sudo] password for admin:

Please provide the VMS server's network information
This Information is needed for connectivity with VOS devices
IP Address of interface connecting to VOS devices
Please Enter VMS node IP connecting to VOS Devices           : 192.168.101.10
# This is the VMS interface that connects to the secure SD-WAN. In this example, it is ETH1.

Please provide the VMS server's network information
This Information is needed for connectivity with External Agent
IP Address of interface connecting to External Agent
Please Enter VMS node IP  Address connecting External Agent    : 192.168.101.10
# This is the VMS interface that connects to the WMI agent. In this example, it is ETH1.

Info: PA_VMS_EXTERNAL_IP: 192.168.101.10
```

==========CONFIGURING-PASSIVE-AUTH-PARAMETERS==========
==========PASSIVE-AUTH-PARAMETERS-CONFIGURATION-COMPLETED==========
==========CONFIGURING-COMMON-PARAMETERS==========

Please provide the below information; typed response will not be displayed.
This Information is needed for connectivity with Versa Director

Primary Versa Director's IP Address
Please Enter Primary Versa Director's IP Address : **3.10.66.223**
This is the IP address that Versa Director administrators connect to, to configure the secure SD-WAN CPE. It is also known
as the northbound interface.

Please Enter Secondary Versa Director's IP Address: **3.10.66.223**
Because this test platform has no resilience, the same IP address is used twice. For production, ensure that you use the
correct northbound IP address.

Enter the Versa Director GUI username with Admin privileges : USERNAME : **acme-corp-admin**
This is the user account configured on Versa Director so VMS can query Versa Director.

Versa Director User is not a known Admin account .
Do you want to proceed with the user: acme-corp-admin (y/N): **y**

Primary Versa Director's Credentials
Enter Password for Versa Director User: 'acme-corp-admin': ***enter-user-account-password***
Re-enter Password for Versa Director User: 'acme-corp-admin': ***enter-user-account-password***

Versa Tenant Details
Please enter tenant name for this service : : **ACME-CORP**
This is the organization name as configured on Versa Director. It is case-sensitive.
Configuring for tenant: ACME-CORP

VMS Intermediate Server-Client Certificate Generation
Please provide the below information for the VMS node
This Information is needed for Client Certificate Generation and Validation

When prompted, please enter the password used for root/intermediate certificate generation
FQDN of Versa Message Service's
Please Enter FQDN used in Versa Message Service : **ha.acme-corp.local**
Please Enter Subject ALT Name 1 used in Versa Message Service certificate file : **vms1.acme-corp.local**
Please Enter Subject ALT Name 2 used in Versa Message Service certificate file : **vms2.acme-corp.local**

Certificate Regeneration
Existing Certificates FQDN:
Do you want to regerate the certificates with new FQDN: ha.acme-corp.local ? (y/N) : **y**
[2022-12-05 03:13:28-08:00]: Started generating certificates...
[2022-12-05 03:13:29-08:00]: Server private key and csr created successfully
[2022-12-05 03:13:29-08:00]: Creating server certificate...

```
Enter pass phrase for /opt/versa/vms/certs/ca-key.pem:
[2022-12-05 03:13:32-08:00]: Server certificate created successfully
[2022-12-05 03:13:32-08:00]: Server certificate bundle created successfully
[2022-12-05 03:13:32-08:00]: Creating client private key and csr...
[2022-12-05 03:13:32-08:00]: Client private key and csr created successfully
[2022-12-05 03:13:32-08:00]: Creating client certificate...
Enter pass phrase for /opt/versa/vms/certs/ca-key.pem:
[2022-12-05 03:13:36-08:00]: Client certificate created successfully
[2022-12-05 03:13:36-08:00]: Creating client certificate (pfx format)...
[2022-12-05 03:13:36-08:00]: Client certificate (pfx format) created successfully
[2022-12-05 03:13:36-08:00]: All certificates and keys are successfully created.
[2022-12-05 03:13:36-08:00]: Validating CA certificate...
/opt/versa/vms/certs/ca-cert.pem: OK
[2022-12-05 03:13:36-08:00]: Validation for CA certificate succeeded
[2022-12-05 03:13:36-08:00]: Validating server certificate...
/opt/versa/vms/certs/server-cert.pem: OK
[2022-12-05 03:13:36-08:00]: Validation for server certificate succeeded
[2022-12-05 03:13:36-08:00]: Validating client certificate...
/opt/versa/vms/certs/client-cert.pem: OK
[2022-12-05 03:13:36-08:00]: Validation for client certificate succeeded
[2022-12-05 03:13:36-08:00]: Exiting...
Certificate Regenerated with SAN: ha.acme-corp.local, vms1.acme-corp.local, vms2.acme-corp.local
Establishing connectivity with Director

Please provide the following server identification information
This Information is needed for HA failover
Please Enter a unique name for this VMS node     : vms1-acme-corp

VMS configuration completed

Please run "vsh initialize-SERVICE_NAME" to complete setup

==========================COMMON-PARAMETERS-CONFIGURATION-
COMPLETED==========================

Run "vsh initialize-passive-auth" to complete deployment

=====================================CONFIGURATION-
COMPLETED================================
```

4. To start VMS services, issue the **vsh initialize-passive-auth** CLI command. For example:

```
[admin@versa-msgservice: ~] $ vsh initialize-passive-auth

---------- Starting Deployment of Passive Authentication ----------

Info: start-passive-auth
NAME                STATUS   ROLES                AGE   VERSION
vms1.acme-corp.local   Ready    control-plane,master   11m   v1.20.4

Info: ============================================================
persistentvolume/pkg-mgr-pv-volume created

Info: Successfully created persistent volume package manager
```

```
persistentvolumeclaim/pkg-mgr-pv-claim created

Info: Successfully created pv claim for package manager
pkg-mgr-pv-volume   60Gi       RWX            Retain           Bound    default/pkg-mgr-pv-claim
manual                  3s

Info: ============================================================
persistentvolume/app-logs-volume created

Info: Successfully created persistent volume for logs
persistentvolumeclaim/app-logs-volume-claim created

Info: Successfully created claim for logs volume
app-logs-volume   15Gi       RWX            Retain           Bound    default/app-logs-volume-claim
manual                  3s

Info: ============================================================
persistentvolume/apps-volume created

Info: Successfully created persistent volume for apps
persistentvolumeclaim/apps-volume-claim created

Info: Successfully created claim for apps volume
apps-volume   15Gi       RWX            Retain           Bound    default/apps-volume-claim    manual
2s

Info: ---------- Persistent Volumes ----------

NAME               CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM
STORAGECLASS   REASON   AGE
app-logs-volume    15Gi       RWX            Retain           Bound    default/app-logs-volume-claim
manual                  10s
apps-volume        15Gi       RWX            Retain           Bound    default/apps-volume-claim
manual                  5s
pkg-mgr-pv-volume   60Gi       RWX            Retain           Bound    default/pkg-mgr-pv-claim
manual                  14s

Info: ---------- Volume Claims ----------
                                                NAME                  STATUS   VOLUME             CAPACITY
ACCESS MODES   STORAGECLASS   AGE
app-logs-volume-claim   Bound    app-logs-volume     15Gi       RWX            manual         10s
apps-volume-claim       Bound    apps-volume         15Gi       RWX            manual         6s
pkg-mgr-pv-claim        Bound    pkg-mgr-pv-volume   60Gi       RWX            manual         15s

Info: ---------- Redis UIPMAP ----------
deployment.apps/redis-uipmap created

Info: Successfully created redis-uipmap deployment
service/redis-uipmap created

Info: Successfully created redis-uipmap service

Info: ---------- VxDEV ----------
deployment.apps/vxdev created
```

```
Info: Successfully created vxdev deployment
service/vxdev created

Info: Successfully created vxdev service

Info: ----------------------- Message-Server ------------------
deployment.apps/message-server created

Info: Successfully created message-server deployment
service/message-server created

Info: Successfully created message-server service

Info: -------------------- Pkg-Builder -------------------------
deployment.apps/pkg-builder created

Info: Successfully created pkg-builder deployment

Info: -------------------- Pkg-Server -------------------------
configmap/nginx-config created

Info: Successfully created pkg-server configMap
service/nginx created

Info: Successfully created pkg-server service
deployment.apps/nginx created

Info: Successfully created pkg-server-deployment

Waiting for deployments to start before starting uip ...

Info: ----------------------- UIPMAP ---------------------------
deployment.apps/uipmap created

Info: Successfully created uipmap deployment
service/uipmap created

Info: Successfully created uipmap service

Info: --------------------- Concentrator ----------------------
deployment.apps/concentrator created

Info: Successfully created concentrator deployment
service/concentrator created

Info: Successfully created concentrator service
PODS
NAME                          READY   STATUS              RESTARTS   AGE
concentrator-5fdf6cfcb8-gn5rl     0/1     ContainerCreating   0          3s
message-server-7b6db77b94-cl2v9   1/1     Running             0          47s
nginx-56799c4fd6-lw7k6            1/1     Running             0          33s
pkg-builder-bbdf5c558-nptzl       1/1     Running             0          41s
redis-uipmap-687c77bd74-z97gg     1/1     Running             0          59s
```

```
uipmap-bd565f987-4jfdf          1/1     Running           0         9s
vxdev-764d8cc4b9-cqkmt          1/1     Running           0         52s

================================================================================================

SERVICES
NAME             TYPE        CLUSTER-IP       EXTERNAL-IP      PORT(S)                    AGE
concentrator     ClusterIP   10.106.99.7      192.168.101.10   3092/TCP                   2s
kubernetes       ClusterIP   10.96.0.1        <none>           443/TCP                    12m
message-server   ClusterIP   10.102.231.20    192.168.101.10   3074/TCP,3101/TCP,3102/TCP   46s
nginx            ClusterIP   10.101.150.200   192.168.101.10   443/TCP                    36s
redis-uipmap     ClusterIP   10.110.132.36    <none>           6379/TCP                   58s
uipmap           ClusterIP   10.99.19.213     <none>           7000/TCP                   8s
vxdev            ClusterIP   10.100.100.21    <none>           8080/TCP                   52s

================================================================================================

Pods may take up to 5 minutes to complete deployment

================================================================================================

Monitor status of deployment using vsh status

================================================================================================

Versa Package Info: versa-msgservice-20220720-194500-b85e521-21.2.2

================================================================================================

Info: SYSTEM-SERVICES-STATUS
kubelet:active (6779)
docker:active (2064)

================================================================================================

PODS-STATUS
NAME                           READY   STATUS    RESTARTS   AGE
concentrator-5fdf6cfcb8-gn5rl  1/1     Running   0          15s
message-server-7b6db77b94-cl2v9   1/1     Running   0          59s
nginx-56799c4fd6-lw7k6            1/1     Running   0          45s
pkg-builder-bbdf5c558-nptzl       1/1     Running   0          53s
redis-uipmap-687c77bd74-z97gg     1/1     Running   0          71s
uipmap-bd565f987-4jfdf            1/1     Running   0          21s
vxdev-764d8cc4b9-cqkmt            1/1     Running   0          64s

================================================================================================

SERVICES-STATUS
NAME             TYPE        CLUSTER-IP       EXTERNAL-IP      PORT(S)                    AGE
concentrator     ClusterIP   10.106.99.7      192.168.101.10   3092/TCP                   13s
kubernetes       ClusterIP   10.96.0.1        <none>           443/TCP                    12m
message-server   ClusterIP   10.102.231.20    192.168.101.10   3074/TCP,3101/TCP,3102/TCP   57s
nginx            ClusterIP   10.101.150.200   192.168.101.10   443/TCP                    47s
redis-uipmap     ClusterIP   10.110.132.36    <none>           6379/TCP                   69s
```

```
uipmap          ClusterIP   10.99.19.213    <none>          7000/TCP                19s
vxdev           ClusterIP   10.100.100.21   <none>          8080/TCP                63s

================================================================================================

---------- Deployment of Passive Authentication completed----------
```

5. To check whether the VMS service started, issue the **vsh status** CLI command. For example:

```
[admin@versa-msgservice: ~] $ vsh status

================================================================================================

Versa Package Info: versa-msgservice-20220720-194500-b85e521-21.2.2

================================================================================================

Info: SYSTEM-SERVICES-STATUS
kubelet:active (6779)
docker:active (2064)

================================================================================================

PODS-STATUS
NAME                          READY   STATUS    RESTARTS   AGE
concentrator-5fdf6cfcb8-gn5rl     1/1     Running   0          11m
message-server-7b6db77b94-cl2v9   1/1     Running   0          12m
nginx-56799c4fd6-lw7k6            1/1     Running   0          12m
pkg-builder-bbdf5c558-nptzl       1/1     Running   0          12m
redis-uipmap-687c77bd74-z97gg     1/1     Running   0          12m
uipmap-bd565f987-4jfdf            1/1     Running   0          11m
vxdev-764d8cc4b9-cqkmt            1/1     Running   0          12m

================================================================================================

SERVICES-STATUS
NAME            TYPE        CLUSTER-IP       EXTERNAL-IP      PORT(S)                  AGE
concentrator    ClusterIP   10.106.99.7      192.168.101.10   3092/TCP                 11m
kubernetes      ClusterIP   10.96.0.1        <none>           443/TCP                  24m
message-server  ClusterIP   10.102.231.20    192.168.101.10   3074/TCP,3101/TCP,3102/TCP   12m
nginx           ClusterIP   10.101.150.200   192.168.101.10   443/TCP                  12m
redis-uipmap    ClusterIP   10.110.132.36    <none>           6379/TCP                 12m
uipmap          ClusterIP   10.99.19.213     <none>           7000/TCP                 11m
vxdev           ClusterIP   10.100.100.21    <none>           8080/TCP                 12m

================================================================================================
```

6. Update the certificate permissions on the active VMS server:

```
[admin@versa-msgservice: ~] $ cd /opt/versa/vms/certs/
[admin@versa-msgservice: certs] $ sudo chmod 777 root-ca-cert.pem
[admin@versa-msgservice: certs] $ sudo chmod 777 client-cert.pfx
```

Configure the Standby VMS Server

Before you configure the standby VMS server, you must copy the certificates from the active VMS server to the standby VMS server. To copy the certificates:

1. Check that no certificates are present on the standby VMS server. The following output confirms that no certificates exist:

```
[admin@versa-msgservice: ~] $ cd /opt/versa/vms/certs/
[admin@versa-msgservice: certs] $ ls -lh
total 28K
-rw-rw-r-- 1 versa versa 4.2K Jul 20 12:45 intermediate.cnf
-rw-rw-r-- 1 versa versa 4.3K Jul 20 12:45 openssl.cnf
-rwxrwxr-x 1 versa versa 12K Jul 20 12:45 vms_cert_gen.sh
```

2. Create a temporary folder to use for copying the certificates from the active server:

```
[admin@versa-msgservice: ~] $ mkdir /home/admin/ha-certs
[admin@versa-msgservice: ~] $ chmod a+x /home/admin/ha-certs
```

3. Copy the certificates from the active VMS server to the temporary folder on the standby server:

```
[admin@vms1: certs] $ sudo scp /opt/versa/vms/certs/ * admin@10.40.25.8:/home/admin/ha-certs
[sudo] password for admin:
The authenticity of host '10.40.25.8 (10.40.25.8)' can't be established.
ECDSA key fingerprint is SHA256:Mi2Bi90EEjetH0qR7NOqcBUvZh/T48f4+ig55kZ+M18.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.40.25.8' (ECDSA) to the list of known hosts.
================================================================================
WARNING!
This is a Proprietary System
You have accessed a Proprietary System

If you are not authorized to use this computer system, you MUST log off now.
Unauthorized use of this computer system, including unauthorized attempts or
acts to deny service on, upload information to download information from,
change information on, or access a non-public site from, this computer system,
are strictly prohibited and may be punishable under federal and state criminal
and civil laws. All data contained on this computer systems may be monitored,
intercepted, recorded, read, copied, or captured in any manner by authorized
System personnel. System personnel may use or transfer this data as required or
permitted under applicable law. Without limiting the previous sentence, system
personnel may give to law enforcement officials any potential evidence of crime
found on this computer system. Use of this system by any user, authorized or
unauthorized, constitutes EXPRESS CONSENT to this monitoring, interception,
recording, reading, copying, or capturing, and use and transfer. Please verify
if this is the current version of the banner when deploying to the system.
================================================================================

admin@10.40.25.8's password:
/opt/versa/vms/certs: not a regular file
1000.pem
100% 2159    97.0KB/s   00:00
```

```
7E84B9ED1B03D43FF1C27A4013813E1F2CD77BAF.
pem                                                100% 5754   342.4KB/s   00:00
7E84B9ED1B03D43FF1C27A4013813E1F2CD77BB0.
pem                                                100% 6253     4.2MB/s   00:00
backup: not a regular file
ca-cert-bundle.pem
100% 4354     2.7MB/s   00:00
ca-cert.pem
100% 2159     1.7MB/s   00:00
ca-csr.pem
100% 1769   221.9KB/s   00:00
ca-index
100%  224   262.1KB/s   00:00
ca-index.attr
100%   21    24.5KB/s   00:00
ca-index.attr.old
100%   21     2.6KB/s   00:00
ca-index.old
100%  116    89.5KB/s   00:00
ca-key.pem
100% 3326   319.7KB/s   00:00
ca-serial
100%   41    42.9KB/s   00:00
ca-serial.old
100%   41    39.1KB/s   00:00
client-cert.pem
100% 6253     5.1MB/s   00:00
client-cert.pfx
100% 6141   998.5KB/s   00:00
client.csr                                                              100%
1005   661.6KB/s   00:00
client-key.pem
100% 1704   340.0KB/s   00:00
crl: not a regular file
crlnumber
100%    5     0.5KB/s   00:00
intermediate.cnf
100% 4270     2.5MB/s   00:00
intermediate_index.txt
100%  133    82.9KB/s   00:00
intermediate_index.txt.attr
100%   21    14.2KB/s   00:00
intermediate_index.txt.attr.
old                                                    100%    0     0.0KB/s
00:00
intermediate_index.txt.old
100%    0     0.0KB/s   00:00
openssl.cnf
100% 4333   922.4KB/s   00:00
root-ca-cert.pem
100% 2195   164.6KB/s   00:00
root-ca-key.pem
100% 3326   493.7KB/s   00:00
serial                                                                  100%
```

```
5     1.5KB/s   00:00
serial.old
100%    5     0.8KB/s   00:00
server-cert-bundle.pem
100%   10KB   8.4MB/s   00:00
server-cert.pem
100% 5754     5.2MB/s   00:00
server.csr
100% 1115   747.1KB/s   00:00
server-key.pem
100% 1704     1.7MB/s   00:00
vms_cert_gen.sh
100%   11KB  11.4MB/s   00:00
vms-encrypt.key
100%   44    43.0KB/s   00:00
```

4. Copy the certificates from the temporary folder to the correct folder on the standby VMS server:

```
[admin@versa-msgservice: ha-certs] $ sudo cp /home/admin/ha-certs/* /opt/versa/vms/certs/
[admin@versa-msgservice: ha-certs] $ cd /opt/versa/vms/certs/
[admin@versa-msgservice: certs] $ ls -lh
total 176K
-rw-r----- 1 root  root  2.2K Oct  3 08:29 1000.pem
-rw-r----- 1 root  root  5.7K Oct  3 08:29 7E84B9ED1B03D43FF1C27A4013813E1F2CD77BAF.pem
-rw-r----- 1 root  root  6.2K Oct  3 08:29 7E84B9ED1B03D43FF1C27A4013813E1F2CD77BB0.pem
-r--r----- 1 root  root  4.3K Oct  3 08:29 ca-cert-bundle.pem
-r--r----- 1 root  root  2.2K Oct  3 08:29 ca-cert.pem
-rw-r----- 1 root  root  1.8K Oct  3 08:29 ca-csr.pem
-rw-r----- 1 root  root   224 Oct  3 08:29 ca-index
-rw-r----- 1 root  root    21 Oct  3 08:29 ca-index.attr
-rw-r----- 1 root  root    21 Oct  3 08:29 ca-index.attr.old
-rw-r----- 1 root  root   116 Oct  3 08:29 ca-index.old
-r-------- 1 root  root  3.3K Oct  3 08:29 ca-key.pem
-rw-r----- 1 root  root    41 Oct  3 08:29 ca-serial
-rw-r----- 1 root  root    41 Oct  3 08:29 ca-serial.old
-rw-r----- 1 root  root  6.2K Oct  3 08:29 client-cert.pem
-rwxr-x--- 1 root  root  6.0K Oct  3 08:29 client-cert.pfx
-rw-r----- 1 root  root  1005 Oct  3 08:29 client.csr
-rw------- 1 root  root  1.7K Oct  3 08:29 client-key.pem
-rw-r----- 1 root  root     5 Oct  3 08:29 crlnumber
-rw-rw-r-- 1 versa versa 4.2K Oct  3 08:29 intermediate.cnf
-rw-r----- 1 root  root   133 Oct  3 08:29 intermediate_index.txt
-rw-r----- 1 root  root    21 Oct  3 08:29 intermediate_index.txt.attr
-rw-r----- 1 root  root     0 Oct  3 08:29 intermediate_index.txt.attr.old
-rw-r----- 1 root  root     0 Oct  3 08:29 intermediate_index.txt.old
-rw-rw-r-- 1 versa versa 4.3K Oct  3 08:29 openssl.cnf
-rwxr-x--- 1 root  root  2.2K Oct  3 08:29 root-ca-cert.pem
-r-------- 1 root  root  3.3K Oct  3 08:29 root-ca-key.pem
-rw-r----- 1 root  root     5 Oct  3 08:29 serial
-rw-r----- 1 root  root     5 Oct  3 08:29 serial.old
-rw-r----- 1 root  root  9.9K Oct  3 08:29 server-cert-bundle.pem
-rw-r----- 1 root  root  5.7K Oct  3 08:29 server-cert.pem
-rw-r----- 1 root  root  1.1K Oct  3 08:29 server.csr
-rw------- 1 root  root  1.7K Oct  3 08:29 server-key.pem
```

```
-rwxrwxr-x 1 versa versa  12K Oct  3 08:29 vms_cert_gen.sh
-rw-r----- 1 root  root    44 Oct  3 08:29 vms-encrypt.key
```

5. Delete the temporary folder:

```
[admin@versa-msgservice: certs] $ sudo rm -rf /home/admin/ha-certs/
```

6. Update permissions for the client-cert.pfx and root-ca-cert.pem certificates on the standby VMS server

```
[admin@versa-msgservice: certs] $ sudo chmod 777 client-cert.pfx
[admin@versa-msgservice: certs] $ sudo chmod 777 root-ca-cert.pem
```

Next, configure the standby VMS server:

1. To execute the first phase of the configuration of the standby VMS server, issue the **vsh configure-passive-auth** CLI command. For example:

```
[admin@versa-msgservice: certs] $ vsh configure-passive-auth

================================================================================================

            First-time configuration!

Is the primary interface configuration finalized?  (y/N) :  y
Management Interface IP of this VMS server
Please Enter this VMS Server Management/Primary Interface IP Address   : 10.40.25.8
# This is the management interface of the VMS server. In this example, it is ETH0.

================================================================================================

FQDN of this VMS server
Please enter the FQDN of this VMS Server:  vms2.acme-corp.local
# This is the FQDN of the standby VMS server.

It may take up to 10 minutes to complete initialization.

================================================================================================

Adding new hosts entry.
It may take up to 10 minutes to complete initialization.

================================================================================================

Info: Installing Kubernetes ...
Info: Creating auto completions for kubectl
Info: Disabling Swap ...
Info: Creating Docker overlay ....
Enable and restart Docker
Info: Enable and restart Docker
total 963988
-rw-rw-r-- 1 versa versa  15131067 Jul 20 12:52 flannel.tar.bz2
-rw-rw-r-- 1 versa versa  78435054 Jul 20 12:52 etcd.tar.bz2
-rw-rw-r-- 1 versa versa  12502350 Jul 20 12:52 coredns.tar.bz2
-rw-rw-r-- 1 versa versa 231355183 Jul 20 12:52 concentrator.tar.bz2
```

```
-rw-rw-r-- 1 versa versa  26220780 Jul 20 12:52 kube-apiserver.tar.bz2
-rw-rw-r-- 1 versa versa 223233125 Jul 20 12:52 ise-agent.tar.bz2
-rw-rw-r-- 1 versa versa   3904253 Jul 20 12:52 message-server.tar.bz2
-rw-rw-r-- 1 versa versa  12427735 Jul 20 12:52 kube-scheduler.tar.bz2
-rw-rw-r-- 1 versa versa  42734652 Jul 20 12:52 kube-proxy.tar.bz2
-rw-rw-r-- 1 versa versa  25608143 Jul 20 12:52 kube-controller-manager.tar.bz2
-rw-rw-r-- 1 versa versa    284858 Jul 20 12:52 pause.tar.bz2
-rw-rw-r-- 1 versa versa  34510568 Jul 20 12:52 nginx.tar.bz2
-rw-rw-r-- 1 versa versa  33491344 Jul 20 12:52 redis.tar.bz2
-rw-rw-r-- 1 versa versa 209158609 Jul 20 12:52 pkg-builder.tar.bz2
-rw-rw-r-- 1 versa versa  21255565 Jul 20 12:52 vxdev.tar.bz2
-rw-rw-r-- 1 versa versa   3814471 Jul 20 12:52 uipmap.tar.bz2
-rw-rw-r-- 1 versa versa   3844141 Jul 20 12:52 sgt-server.tar.bz2
-rw-rw-r-- 1 versa versa   9155314 Jul 20 12:52 registry.tar.bz2
drwxrwxr-x 4 versa versa      4096 Aug  2 11:32 ..
drwxrwxr-x 2 versa versa      4096 Aug  2 11:32 .
Extracting concentrator.tar.bz2...
Loading concentrator.tar ...
Loaded image: concentrator:1.0.0
Extracting coredns.tar.bz2...
Loading coredns.tar ...
Loaded image: k8s.gcr.io/coredns:1.7.0
Extracting etcd.tar.bz2...
Loading etcd.tar ...
Loaded image: k8s.gcr.io/etcd:3.4.13-0
Extracting flannel.tar.bz2...
Loading flannel.tar ...
Loaded image: quay.io/coreos/flannel:v0.11.0-amd64
Extracting ise-agent.tar.bz2...
Loading ise-agent.tar ...
Loaded image: ise-agent:1.0.0
Extracting kube-apiserver.tar.bz2...
Loading kube-apiserver.tar ...
Loaded image: k8s.gcr.io/kube-apiserver:v1.20.4
Extracting kube-controller-manager.tar.bz2...
Loading kube-controller-manager.tar ...
Loaded image: k8s.gcr.io/kube-controller-manager:v1.20.4
Extracting kube-proxy.tar.bz2...
Loading kube-proxy.tar ...
Loaded image: k8s.gcr.io/kube-proxy:v1.20.4
Extracting kube-scheduler.tar.bz2...
Loading kube-scheduler.tar ...
Loaded image: k8s.gcr.io/kube-scheduler:v1.20.4
Extracting message-server.tar.bz2...
Loading message-server.tar ...
Loaded image: message-server:1.0.0
Extracting nginx.tar.bz2...
Loading nginx.tar ...
Loaded image: nginx:1.7.9
Extracting pause.tar.bz2...
Loading pause.tar ...
Loaded image: k8s.gcr.io/pause:3.2
Extracting pkg-builder.tar.bz2...
Loading pkg-builder.tar ...
```

```
Loaded image: pkg-builder:1.0.0
Extracting redis.tar.bz2...
Loading redis.tar ...
Loaded image: redis:1.0.0
Extracting registry.tar.bz2...
Loading registry.tar ...
Loaded image: registry:2
Extracting sgt-server.tar.bz2...
Loading sgt-server.tar ...
Loaded image: sgt-server:1.0.0
Extracting uipmap.tar.bz2...
Loading uipmap.tar ...
Loaded image: uipmap:1.0.0
Extracting vxdev.tar.bz2...
Loading vxdev.tar ...
Loaded image: vxdev:1.0.0
REPOSITORY                      TAG           IMAGE ID       CREATED         SIZE
ise-agent                       1.0.0         2141ac3cc15a   4 months ago    583MB
redis                           1.0.0         f90a716ad2d5   4 months ago    106MB
concentrator                    1.0.0         adac8a6cc21f   4 months ago    603MB
message-server                  1.0.0         694409633c8e   4 months ago    11.6MB
uipmap                          1.0.0         f70397c65c49   4 months ago    11.2MB
pkg-builder                     1.0.0         2cdf8332ff38   4 months ago    536MB
vxdev                           1.0.0         1048f85397f0   7 months ago    61.4MB
sgt-server                      1.0.0         646ed51aa809   14 months ago   11.3MB
k8s.gcr.io/kube-proxy           v1.20.4       c29e6c583067   21 months ago   118MB
k8s.gcr.io/kube-controller-manager   v1.20.4       0a41a1414c53   21 months ago   116MB
k8s.gcr.io/kube-apiserver       v1.20.4       ae5eb22e4a9d   21 months ago   122MB
k8s.gcr.io/kube-scheduler       v1.20.4       5f8cb769bd73   21 months ago   47.3MB
k8s.gcr.io/etcd                 3.4.13-0      0369cf4303ff   2 years ago     253MB
registry                        2             2d4f4b5309b1   2 years ago     26.2MB
k8s.gcr.io/coredns              1.7.0         bfe3a36ebd25   2 years ago     45.2MB
k8s.gcr.io/pause                3.2           80d28bedfe5d   2 years ago     683kB
quay.io/coreos/flannel          v0.11.0-amd64 ff281650a721   3 years ago     52.6MB
nginx                           1.7.9         84581e99d807   7 years ago     91.7MB
Info: Initialize Kubernetes; this will take a few minutes
Info: Kube Init successful
Info: Init Flannel
podsecuritypolicy.policy/psp.flannel.unprivileged created
Warning: rbac.authorization.k8s.io/v1beta1 ClusterRole is deprecated in v1.17+, unavailable in v1.22+;
use rbac.authorization.k8s.io/v1 ClusterRole
clusterrole.rbac.authorization.k8s.io/flannel created
Warning: rbac.authorization.k8s.io/v1beta1 ClusterRoleBinding is deprecated in v1.17+, unavailable in v1.
22+; use rbac.authorization.k8s.io/v1 ClusterRoleBinding
clusterrolebinding.rbac.authorization.k8s.io/flannel created
serviceaccount/flannel created
configmap/kube-flannel-cfg created
daemonset.apps/kube-flannel-ds-amd64 created
daemonset.apps/kube-flannel-ds-arm64 created
daemonset.apps/kube-flannel-ds-arm created
daemonset.apps/kube-flannel-ds-ppc64le created
daemonset.apps/kube-flannel-ds-s390x created
Info: Kubernetes: All-In-One
node/vms2.acme-corp.local untainted
```

```
Info: Create local registry
4babbc19b2caa5ba70c1f0b82ac23ef036d7c7f5e8ca2cf8872f22f76a5e0a66
REPOSITORY                      TAG           IMAGE ID       CREATED         SIZE
ise-agent                       1.0.0         2141ac3cc15a   4 months ago    583MB
redis                           1.0.0         f90a716ad2d5   4 months ago    106MB
concentrator                    1.0.0         adac8a6cc21f   4 months ago    603MB
message-server                  1.0.0         694409633c8e   4 months ago    11.6MB
uipmap                          1.0.0         f70397c65c49   4 months ago    11.2MB
pkg-builder                     1.0.0         2cdf8332ff38   4 months ago    536MB
vxdev                           1.0.0         1048f85397f0   7 months ago    61.4MB
sgt-server                      1.0.0         646ed51aa809   14 months ago   11.3MB
k8s.gcr.io/kube-proxy           v1.20.4       c29e6c583067   21 months ago   118MB
k8s.gcr.io/kube-controller-manager   v1.20.4       0a41a1414c53   21 months ago   116MB
k8s.gcr.io/kube-apiserver       v1.20.4       ae5eb22e4a9d   21 months ago   122MB
k8s.gcr.io/kube-scheduler       v1.20.4       5f8cb769bd73   21 months ago   47.3MB
k8s.gcr.io/etcd                 3.4.13-0      0369cf4303ff   2 years ago     253MB
registry                        2             2d4f4b5309b1   2 years ago     26.2MB
k8s.gcr.io/coredns              1.7.0         bfe3a36ebd25   2 years ago     45.2MB
k8s.gcr.io/pause                3.2           80d28bedfe5d   2 years ago     683kB
quay.io/coreos/flannel          v0.11.0-amd64 ff281650a721   3 years ago     52.6MB
nginx                           1.7.9         84581e99d807   7 years ago     91.7MB
The push refers to repository [localhost:5000/message-server]
24613632e82e: Preparing
24613632e82e: Pushed
1.0.0: digest: sha256:52457938af81f3708a49292437df8490824de1906b8e5b18618ae254b0142ed0 size:
528
The push refers to repository [localhost:5000/redis]
94dd67a59053: Preparing
258a1ab6dab5: Preparing
35613d8e624a: Preparing
0302cabf4dde: Preparing
6eeff2593e88: Preparing
9eef6e3cc293: Preparing
89ce1a07a7e4: Preparing
7e718b9c0c8c: Preparing
9eef6e3cc293: Waiting
89ce1a07a7e4: Waiting
7e718b9c0c8c: Waiting
258a1ab6dab5: Pushed
0302cabf4dde: Pushed
35613d8e624a: Pushed
94dd67a59053: Pushed
89ce1a07a7e4: Pushed
9eef6e3cc293: Pushed
6eeff2593e88: Pushed
7e718b9c0c8c: Pushed
1.0.0: digest: sha256:2f9e3dea6c1896b20fea2c09105269c01b5b78b6c9a6c51324c3352ab4ea6a3a size:
1992
The push refers to repository [localhost:5000/vxdev]
e16707a6a3f2: Preparing
fb05eb894d9b: Preparing
c3c8752efcba: Preparing
55eb4e5bef72: Preparing
6dae8915d345: Preparing
```

```
02130b505ed2: Preparing
99496a4bc26e: Preparing
9e5f7f0191e2: Preparing
cb381a32b229: Preparing
99496a4bc26e: Waiting
9e5f7f0191e2: Waiting
cb381a32b229: Waiting
02130b505ed2: Waiting
55eb4e5bef72: Pushed
c3c8752efcba: Pushed
6dae8915d345: Pushed
e16707a6a3f2: Pushed
02130b505ed2: Pushed
fb05eb894d9b: Pushed
9e5f7f0191e2: Pushed
cb381a32b229: Pushed
99496a4bc26e: Pushed
1.0.0: digest: sha256:139c9af272bcfc2ddd5cc4ac1d593141ec88a785d96977a1b798c559c01199e0 size:
2202
The push refers to repository [localhost:5000/concentrator]
15d2dcf2da64: Preparing
9b98a31e6cf4: Preparing
0554dc362645: Preparing
40a07d74f60b: Preparing
a404f63be022: Preparing
badb85343016: Preparing
6f15325cc380: Preparing
1e77dd81f9fa: Preparing
030309cad0ba: Preparing
badb85343016: Waiting
6f15325cc380: Waiting
1e77dd81f9fa: Waiting
030309cad0ba: Waiting
0554dc362645: Pushed
40a07d74f60b: Pushed
9b98a31e6cf4: Pushed
15d2dcf2da64: Pushed
6f15325cc380: Pushed
1e77dd81f9fa: Pushed
a404f63be022: Pushed
030309cad0ba: Pushed
badb85343016: Pushed
1.0.0: digest: sha256:8f1addecf664181ef42f542e9e92e2e76b8478778f17aa7a6deb647982beacce size:
2198
The push refers to repository [localhost:5000/uipmap]
94178e95f838: Preparing
94178e95f838: Pushed
1.0.0: digest: sha256:e7746eca1995900e4d643a2edae055740046da6338595ef009e478b871bd22c7 size:
528
The push refers to repository [localhost:5000/pkg-builder]
da3f6ab864b6: Preparing
f690be4f6cdd: Preparing
2719c9c4257e: Preparing
0a83fc3d286e: Preparing
```

```
7b2781c31a7a: Preparing
ec60cb431167: Preparing
e6d9d10bab7e: Preparing
a9ae8da98746: Preparing
22f708c101a3: Preparing
90b04e3f5fa7: Preparing
454f4316781b: Preparing
28d6f0f37200: Preparing
9e6ae86b45a6: Preparing
d10e36763753: Preparing
6f15325cc380: Preparing
1e77dd81f9fa: Preparing
030309cad0ba: Preparing
ec60cb431167: Waiting
e6d9d10bab7e: Waiting
a9ae8da98746: Waiting
22f708c101a3: Waiting
90b04e3f5fa7: Waiting
454f4316781b: Waiting
28d6f0f37200: Waiting
9e6ae86b45a6: Waiting
d10e36763753: Waiting
6f15325cc380: Waiting
1e77dd81f9fa: Waiting
030309cad0ba: Waiting
f690be4f6cdd: Pushed
0a83fc3d286e: Pushed
2719c9c4257e: Pushed
7b2781c31a7a: Pushed
da3f6ab864b6: Pushed
ec60cb431167: Pushed
a9ae8da98746: Pushed
e6d9d10bab7e: Pushed
22f708c101a3: Pushed
90b04e3f5fa7: Pushed
6f15325cc380: Mounted from concentrator
1e77dd81f9fa: Mounted from concentrator
9e6ae86b45a6: Pushed
030309cad0ba: Mounted from concentrator
454f4316781b: Pushed
28d6f0f37200: Pushed
d10e36763753: Pushed
1.0.0: digest: sha256:841fd868da899661de486a38a0f2ada7ecf8b96eb2e033909f487e46295883eb size:
3860
The push refers to repository [localhost:5000/ise-agent]
77f26c1e8a52: Preparing
372336e7e177: Preparing
4b43f9e40e2a: Preparing
c07cd577fd36: Preparing
1896bb642302: Preparing
6f15325cc380: Preparing
1e77dd81f9fa: Preparing
030309cad0ba: Preparing
6f15325cc380: Waiting
```

```
1e77dd81f9fa: Waiting
030309cad0ba: Waiting
372336e7e177: Pushed
c07cd577fd36: Pushed
6f15325cc380: Mounted from pkg-builder
4b43f9e40e2a: Pushed
1e77dd81f9fa: Mounted from pkg-builder
77f26c1e8a52: Pushed
030309cad0ba: Mounted from pkg-builder
1896bb642302: Pushed
1.0.0: digest: sha256:263ee5a11c9c15902af068915f232428b39efc51ee69e2ef9a726e7a30fd4279 size:
1989
The push refers to repository [localhost:5000/sgt-server]
20f8baca1e24: Preparing
20f8baca1e24: Pushed
1.0.0: digest: sha256:eefea21a6587cafb66476de7bfda66687c8caa8a4097b5f2b11ea6aaaf57453f size:
528
NAME                  STATUS   ROLES                  AGE     VERSION
vms2.acme-corp.local   Ready    control-plane,master   5m30s   v1.20.4
Name:               vms2.acme-corp.local
Roles:              control-plane,master
Labels:             beta.kubernetes.io/arch=amd64
                    beta.kubernetes.io/os=linux
                    kubernetes.io/arch=amd64
                    kubernetes.io/hostname=vms2.acme-corp.local
                    kubernetes.io/os=linux
                    node-role.kubernetes.io/control-plane=
                    node-role.kubernetes.io/master=
Annotations:        flannel.alpha.coreos.com/backend-data: {"VtepMAC":"ca:19:1e:4c:7c:4a"}
                    flannel.alpha.coreos.com/backend-type: vxlan
                    flannel.alpha.coreos.com/kube-subnet-manager: true
                    flannel.alpha.coreos.com/public-ip: 10.40.25.8
                    kubeadm.alpha.kubernetes.io/cri-socket: /var/run/dockershim.sock
                    node.alpha.kubernetes.io/ttl: 0
                    volumes.kubernetes.io/controller-managed-attach-detach: true
CreationTimestamp:  Fri, 02 Dec 2022 06:42:31 -0800
Taints:             <none>
Unschedulable:      false
Lease:
  HolderIdentity:  vms2.acme-corp.local
  AcquireTime:     <unset>
  RenewTime:       Fri, 02 Dec 2022 06:47:57 -0800
Conditions:
  Type             Status  LastHeartbeatTime                 LastTransitionTime                Reason
Message
  ----             ------  -----------------                 ------------------                ------
  -------
  MemoryPressure   False   Fri, 02 Dec 2022 06:47:59 -0800   Fri, 02 Dec 2022 06:42:27 -0800
KubeletHasSufficientMemory   kubelet has sufficient memory available
  DiskPressure     False   Fri, 02 Dec 2022 06:47:59 -0800   Fri, 02 Dec 2022 06:42:27 -0800
KubeletHasNoDiskPressure     kubelet has no disk pressure
  PIDPressure      False   Fri, 02 Dec 2022 06:47:59 -0800   Fri, 02 Dec 2022 06:42:27 -0800
KubeletHasSufficientPID      kubelet has sufficient PID available
  Ready            True    Fri, 02 Dec 2022 06:47:59 -0800   Fri, 02 Dec 2022 06:43:36 -0800
KubeletReady                 kubelet is posting ready status. AppArmor enabled
```

```
Addresses:
  InternalIP:  10.40.25.8
  Hostname:    vms2.acme-corp.local
Capacity:
  cpu:                4
  ephemeral-storage:  255959548Ki
  hugepages-2Mi:      0
  memory:             4038796Ki
  pods:               110
Allocatable:
  cpu:                4
  ephemeral-storage:  235892319047
  hugepages-2Mi:      0
  memory:             3936396Ki
  pods:               110
System Info:
  Machine ID:                 d7663e735f3241518255e013c9340f06
  System UUID:                ED7C1257-A577-43EB-80FE-6B8CB60D58CA
  Boot ID:                    e816bf18-0293-418e-b47d-35fb1d425bec
  Kernel Version:             4.15.0-112-generic
  OS Image:                   Ubuntu 18.04.5 LTS
  Operating System:           linux
  Architecture:               amd64
  Container Runtime Version:  docker://20.10.7
  Kubelet Version:            v1.20.4
  Kube-Proxy Version:         v1.20.4
PodCIDR:                      10.244.0.0/24
PodCIDRs:                     10.244.0.0/24
Non-terminated Pods:          (8 in total)
  Namespace                   Name                                        CPU Requests  CPU Limits  Memory Requests
Memory Limits  AGE
  ---------                   ----                                        ------------  ----------  ---------------  -------------  ---
  kube-system                 coredns-74ff55c5b-fb8gb                     100m (2%)     0 (0%)      70Mi (1%)
170Mi (4%)     5m8s
  kube-system                 coredns-74ff55c5b-kqhwj                     100m (2%)     0 (0%)      70Mi (1%)
170Mi (4%)     5m8s
  kube-system                 etcd-vms2.acme-corp.local                   100m (2%)     0 (0%)      100Mi (2%)
0 (0%)         5m28s
  kube-system                 kube-apiserver-vms2.acme-corp.local         250m (6%)     0 (0%)      0
(0%)           0 (0%)         5m28s
  kube-system                 kube-controller-manager-vms2.acme-corp.local  200m (5%)     0 (0%)      0
(0%)           0 (0%)         5m27s
  kube-system                 kube-flannel-ds-amd64-9nbn2                 100m (2%)     100m (2%)   50Mi
(1%)       50Mi (1%)      5m9s
  kube-system                 kube-proxy-bbr5r                            0 (0%)        0 (0%)      0 (0%)           0
(0%)         5m8s
  kube-system                 kube-scheduler-vms2.acme-corp.local         100m (2%)     0 (0%)      0
(0%)           0 (0%)         5m28s
Allocated resources:
  (Total limits may be over 100 percent, that is, overcommitted.)
  Resource           Requests    Limits
  --------           --------    ------
  cpu                950m (23%)  100m (2%)
  memory             290Mi (7%)  390Mi (10%)
```

```
  ephemeral-storage  100Mi (0%)  0 (0%)
  hugepages-2Mi      0 (0%)      0 (0%)
Events:
  Type    Reason                   Age                From        Message
  ----    ------                   ----               ----        -------
  Normal  NodeHasSufficientMemory  7m7s (x5 over 7m11s)  kubelet     Node vms2.acme-corp.local
status is now: NodeHasSufficientMemory
  Normal  NodeHasNoDiskPressure    7m7s (x5 over 7m11s)  kubelet     Node vms2.acme-corp.local
status is now: NodeHasNoDiskPressure
  Normal  NodeHasSufficientPID     7m7s (x5 over 7m11s)  kubelet     Node vms2.acme-corp.local status is
now: NodeHasSufficientPID
  Normal  Starting                 5m17s              kubelet     Starting kubelet.
  Normal  NodeHasSufficientMemory  5m17s              kubelet     Node vms2.acme-corp.local status is
now: NodeHasSufficientMemory
  Normal  NodeHasNoDiskPressure    5m17s              kubelet     Node vms2.acme-corp.local status is
now: NodeHasNoDiskPressure
  Normal  NodeHasSufficientPID     5m17s              kubelet     Node vms2.acme-corp.local status is now:
NodeHasSufficientPID
  Normal  NodeAllocatableEnforced  5m16s              kubelet     Updated Node Allocatable limit across
pods
  Normal  Starting                 5m7s               kubelet     Starting kubelet.
  Normal  NodeHasSufficientMemory  5m7s               kubelet     Node vms2.acme-corp.local status is
now: NodeHasSufficientMemory
  Normal  NodeHasNoDiskPressure    5m7s               kubelet     Node vms2.acme-corp.local status is
now: NodeHasNoDiskPressure
  Normal  NodeHasSufficientPID     5m7s               kubelet     Node vms2.acme-corp.local status is now:
NodeHasSufficientPID
  Normal  NodeAllocatableEnforced  5m6s               kubelet     Updated Node Allocatable limit across
pods
  Normal  Starting                 4m33s              kube-proxy  Starting kube-proxy.
  Normal  NodeReady                4m26s              kubelet     Node vms2.acme-corp.local status is now:
NodeReady
Fri Dec  2 06:48:02 PST 2022 File /opt/versa/etc/initial_install is deleted by /opt/versa/scripts/install/vms_
install_helper.sh

Info: Initial Installation is completed
Initial setup completed
Please run "vsh configure-SERVICE_NAME" to begin your configuration.
```

2. To execute the second phase of the configuration, issue the **vsh configure-passive-auth** CLI command again. Note that you must not regenerate certificates when you are prompted. For example:

```
[admin@versa-msgservice: certs] $ vsh configure-passive-auth
[sudo] password for admin:

================================================================================

Please provide the VMS server's network information

This Information is needed for connectivity with VersaOS Devices
IP Address of interface connecting to VOS devices
Please Enter VMS node IP connecting to VOS Devices          : 192.168.101.11
# This is the VMS interface that connects to the secure SD-WAN CPE, which here is ETH1.
```

```
================================================================================

Please provide the VMS server's network information

This Information is needed for connectivity with External Agent
IP Address of interface connecting to External Agent
Please Enter VMS node IP  Address connecting External Agent    : 192.168.101.11
# This is the VMS interface that connects to the secure SD-WAN CPE, which here is ETH1.

Info: PA_VMS_EXTERNAL_IP: 192.168.101.11

==========================CONFIGURING-PASSIVE-AUTH-
PARAMETERS==================================

======================PASSIVE-AUTH-PARAMETERS-CONFIGURATION-
COMPLETED=========================

==============================CONFIGURING-COMMON-
PARAMETERS==================================

Please provide the following information; typed response will not be displayed

This Information is needed for connectivity with Versa Director

================================================================================

Primary Versa Director's IP Address

Please Enter Primary Versa Director's IP Address   : 3.10.66.223
# This is the IP address Versa Director administrators connect to configure secure SD-WAN CPE. This is
also known as the
# northbound interface.

Please Enter Secondary Versa Director's IP Address: 3.10.66.223
# Because this test platform has no resilience, the same IP address was used twice. Ensure that for
production, the correct
#northbound IP address is used.

================================================================================

Enter the Versa Director GUI UserName with Admin privileges : USERNAME : acme-corp-admin
# This is the user account configured on Versa Director for VMS to query the Director.

Versa Director User is not a known Admin account
Do you want to proceed with the user: acme-corp-admin (y/N): y

Primary Versa Director's Credentials

Enter Password for Versa Director User: 'acme-corp-admin'      :  user-account-password
RE-Enter Password for Versa Director User: 'acme-corp-admin'   :  user-account-password
================================================================================

Versa Tenant Details
```

```
Please enter Tenant Name for this Service :                    : ACME-CORP
# This is the organization name as configured on Director. It is case-sensitive.

Configuring for Tenant: ACME-CORP

================================================================================

VMS Intermediate Server-Client Certificate Generation

Please provide the below information for the VMS node
This Information is needed for Client Certificate Generation and Validation
When prompted, please enter the password used for root/intermediate certificate generation

================================================================================

FQDN of Versa Message Service's
Please Enter FQDN used in Versa Message Service                    : ha.acme-corp.local
Please Enter Subject ALT Name 1 used in Versa Message Service certificate file   : vms1.acme-corp.
local
Please Enter Subject ALT Name 2 used in Versa Message Service certificate file   : vms2.acme-corp.
local

Certificate Regeneration
Existing Certificates FQDN:
Do you want to regenerate the certificates with new FQDN: ha.acme-corp.local ?  (y/N) :  n
# Note: Do not regenerate the certificate.

Establishing connectivity with Director

Establishing connectivity with Director

================================================================================

Please provide the below server identification information

This Information is needed for HA fail-over
Please Enter a unique name for this VMS node     : acme-corp-vms2

================================================================================

VMS configuration completed

Please run "vsh initialize-SERVICE_NAME" to complete setup.

============================COMMON-PARAMETERS-CONFIGURATION-
COMPLETED============================

Run "vsh initialize-passive-auth" to complete deployment.


=====================================CONFIGURATION-
COMPLETED================================
```

3. To start the VMS services, issue the **vsh initialize-passive-auth** CLI command. For example:

```
[admin@versa-msgservice: certs] $ vsh initialize-passive-auth

---------- Starting Deployment of Passive Authentication ----------

Info: start-passive-auth
NAME                 STATUS   ROLES                  AGE   VERSION
vms2.acme-corp.local   Ready    control-plane,master   22m   v1.20.4

Info: ============================================================
persistentvolume/pkg-mgr-pv-volume created

Info: Successfully created persistent volume package manager
persistentvolumeclaim/pkg-mgr-pv-claim created

Info: Successfully created pv claim for package manager
pkg-mgr-pv-volume   60Gi       RWX            Retain           Bound    default/pkg-mgr-pv-claim
manual                 3s

Info: ============================================================
persistentvolume/app-logs-volume created
Info: Successfully created persistent volume for logs

persistentvolumeclaim/app-logs-volume-claim created
Info: Successfully created claim for logs volume

app-logs-volume   15Gi       RWX            Retain           Bound    default/app-logs-volume-claim
manual                 3s

Info: ============================================================

persistentvolume/apps-volume created

persistentvolumeclaim/apps-volume-claim created

apps-volume   15Gi       RWX            Retain           Bound    default/apps-volume-claim   manual
3s

Info: ---------- Persistent Volumes ----------

NAME                 CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM
STORAGECLASS   REASON   AGE
app-logs-volume     15Gi       RWX            Retain           Bound    default/app-logs-volume-claim
manual                 10s
apps-volume         15Gi       RWX            Retain           Bound    default/apps-volume-claim
manual                 5s
pkg-mgr-pv-volume   60Gi       RWX            Retain           Bound    default/pkg-mgr-pv-claim
manual                 14s

Info: ---------- Volume Claims ----------

NAME                   STATUS   VOLUME             CAPACITY   ACCESS MODES   STORAGE CLASS   AGE
app-logs-volume-claim   Bound    app-logs-volume     15Gi       RWX            manual          10s
apps-volume-claim       Bound    apps-volume         15Gi       RWX            manual          5s
pkg-mgr-pv-claim        Bound    pkg-mgr-pv-volume   60Gi       RWX            manual          15s
```

```
Info: ----------------- Redis UIPMAP ---------------------------

deployment.apps/redis-uipmap created
Info: Successfully created redis-uipmap deployment

service/redis-uipmap created
Info: Successfully created redis-uipmap service

Info: ---------------------- VxDEV ---------------------------

deployment.apps/vxdev created
Info: Successfully created vxdev deployment

service/vxdev created
Info: Successfully created vxdev service

Info: ---------------------- Message-Server ------------------

deployment.apps/message-server created
Info: Successfully created message-server deployment

service/message-server created
Info: Successfully created message-server service

Info: -------------------- Pkg-Builder -----------------------

deployment.apps/pkg-builder created
Info: Successfully created pkg-builder deployment

Info: -------------------- PkG-Server ------------------------

configmap/nginx-config created
Info: Successfully created pkg-server configMap

service/nginx created
Info: Successfully created pkg-server service

deployment.apps/nginx created
Info: Successfully created pkg-server-deployment

Waiting for deployments to start before starting uip ...

Info: ---------------------- UIPMAP ---------------------------

deployment.apps/uipmap created
Info: Successfully created uipmap deployment

service/uipmap created
Info: Successfully created uipmap service

Info: --------------------- Concentrator ----------------------

deployment.apps/concentrator created
```

```
Info: Successfully created concentrator deployment

service/concentrator created
Info: Successfully created concentrator service

PODS
NAME                          READY   STATUS              RESTARTS   AGE
concentrator-5fdf6cfcb8-s7g8l     0/1     ContainerCreating   0          3s
message-server-7b6db77b94-4vjvp   1/1     Running             0          49s
nginx-56799c4fd6-4k2cr            1/1     Running             0          34s
pkg-builder-bbdf5c558-c4vhw       1/1     Running             0          42s
redis-uipmap-687c77bd74-nblxg     1/1     Running             0          62s
uipmap-bd565f987-n6c8h            1/1     Running             0          10s
vxdev-764d8cc4b9-hbrs9            1/1     Running             0          56s

================================================================================

SERVICES
NAME             TYPE        CLUSTER-IP       EXTERNAL-IP      PORT(S)                  AGE
concentrator     ClusterIP   10.107.81.121    192.168.101.11   3092/TCP                 2s
kubernetes       ClusterIP   10.96.0.1        <none>           443/TCP                  24m
message-server   ClusterIP   10.102.216.58    192.168.101.11   3074/TCP,3101/TCP,3102/TCP   48s
nginx            ClusterIP   10.96.19.242     192.168.101.11   443/TCP                  37s
redis-uipmap     ClusterIP   10.110.74.126    <none>           6379/TCP                 61s
uipmap           ClusterIP   10.107.230.102   <none>           7000/TCP                 9s
vxdev            ClusterIP   10.101.126.157   <none>           8080/TCP                 55s

================================================================================

Pods may take up to 5 minutes to complete deployment

Monitor status of deployment using vsh status

Versa Package Info: versa-msgservice-20220720-194500-b85e521-21.2.2

================================================================================

Info: SYSTEM-SERVICES-STATUS

kubelet:active (9361)
docker:active (4244)

================================================================================

PODS-STATUS
NAME                          READY   STATUS    RESTARTS   AGE
concentrator-5fdf6cfcb8-s7g8l     1/1     Running   0          15s
message-server-7b6db77b94-4vjvp   1/1     Running   0          61s
nginx-56799c4fd6-4k2cr            1/1     Running   0          46s
pkg-builder-bbdf5c558-c4vhw       1/1     Running   0          54s
redis-uipmap-687c77bd74-nblxg     1/1     Running   0          74s
uipmap-bd565f987-n6c8h            1/1     Running   0          22s
vxdev-764d8cc4b9-hbrs9            1/1     Running   0          68s
```

```
================================================================================================

SERVICES-STATUS
NAME            TYPE       CLUSTER-IP       EXTERNAL-IP      PORT(S)                 AGE
concentrator    ClusterIP  10.107.81.121    192.168.101.11   3092/TCP                13s
kubernetes      ClusterIP  10.96.0.1        <none>           443/TCP                 24m
message-server  ClusterIP  10.102.216.58    192.168.101.11   3074/TCP,3101/TCP,3102/TCP  59s
nginx           ClusterIP  10.96.19.242     192.168.101.11   443/TCP                 48s
redis-uipmap    ClusterIP  10.110.74.126    <none>           6379/TCP                72s
uipmap          ClusterIP  10.107.230.102   <none>           7000/TCP                20s
vxdev           ClusterIP  10.101.126.157   <none>           8080/TCP                66s

================================================================================================

---------- Deployment of Passive Authentication completed----------
```

4. To verify that the VMS service started, issue the **vsh status** CLI command. For example:

```
[admin@vms2: ~] $ vsh status
[sudo] password for admin:

================================================================================================

Versa Package Info: versa-msgservice-20220720-194500-b85e521-21.2.2

================================================================================================

Info: SYSTEM-SERVICES-STATUS
kubelet:active (978)
docker:active (1167)

================================================================================================

PODS-STATUS
NAME                          READY   STATUS    RESTARTS   AGE
concentrator-5fdf6cfcb8-kbhjk     1/1     Running   1          5m52s
message-server-7b6db77b94-xwmc5   1/1     Running   1          6m34s
nginx-56799c4fd6-6lqnz            1/1     Running   1          6m21s
pkg-builder-bbdf5c558-pfvwx       1/1     Running   1          6m28s
redis-uipmap-687c77bd74-t7ssw     1/1     Running   1          6m50s
uipmap-bd565f987-qgvhw            1/1     Running   2          5m57s
vxdev-54599d5f8b-l7bdv            1/1     Running   1          6m43s

================================================================================================

SERVICES-STATUS
NAME            TYPE       CLUSTER-IP       EXTERNAL-IP      PORT(S)                 AGE
concentrator    ClusterIP  10.109.127.231   10.40.25.8       3092/TCP                5m50s
kubernetes      ClusterIP  10.96.0.1        <none>           443/TCP                 19m
message-server  ClusterIP  10.102.52.122    192.168.60.173   3074/TCP,3101/TCP,3102/TCP  6m33s
nginx           ClusterIP  10.100.143.202   192.168.60.173   443/TCP                 6m23s
redis-uipmap    ClusterIP  10.102.17.210    <none>           6379/TCP                6m48s
uipmap          ClusterIP  10.109.240.33    <none>           7000/TCP                5m56s
```

```
vxdev        ClusterIP   10.96.241.2     <none>        8080/TCP              6m39s
================================================================================
```

Configure Active Directory

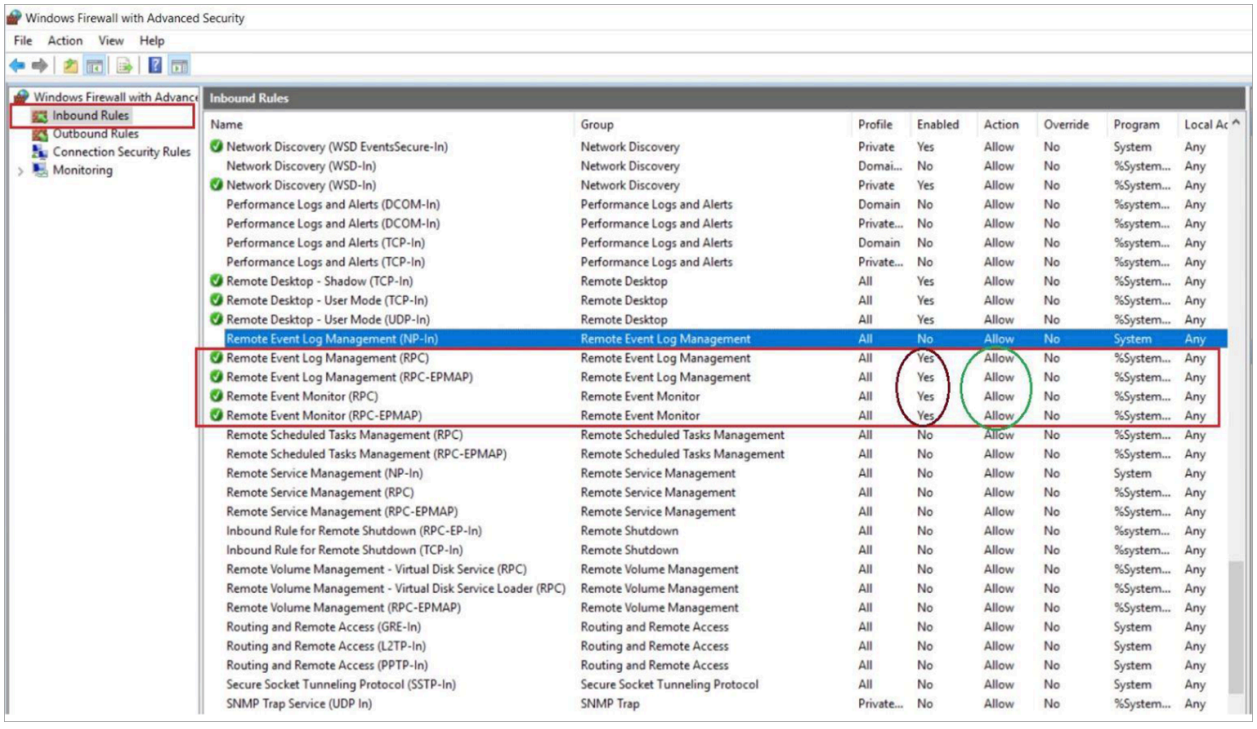
On Active Directory, you need to update firewall rules and configure a non-administrator user.

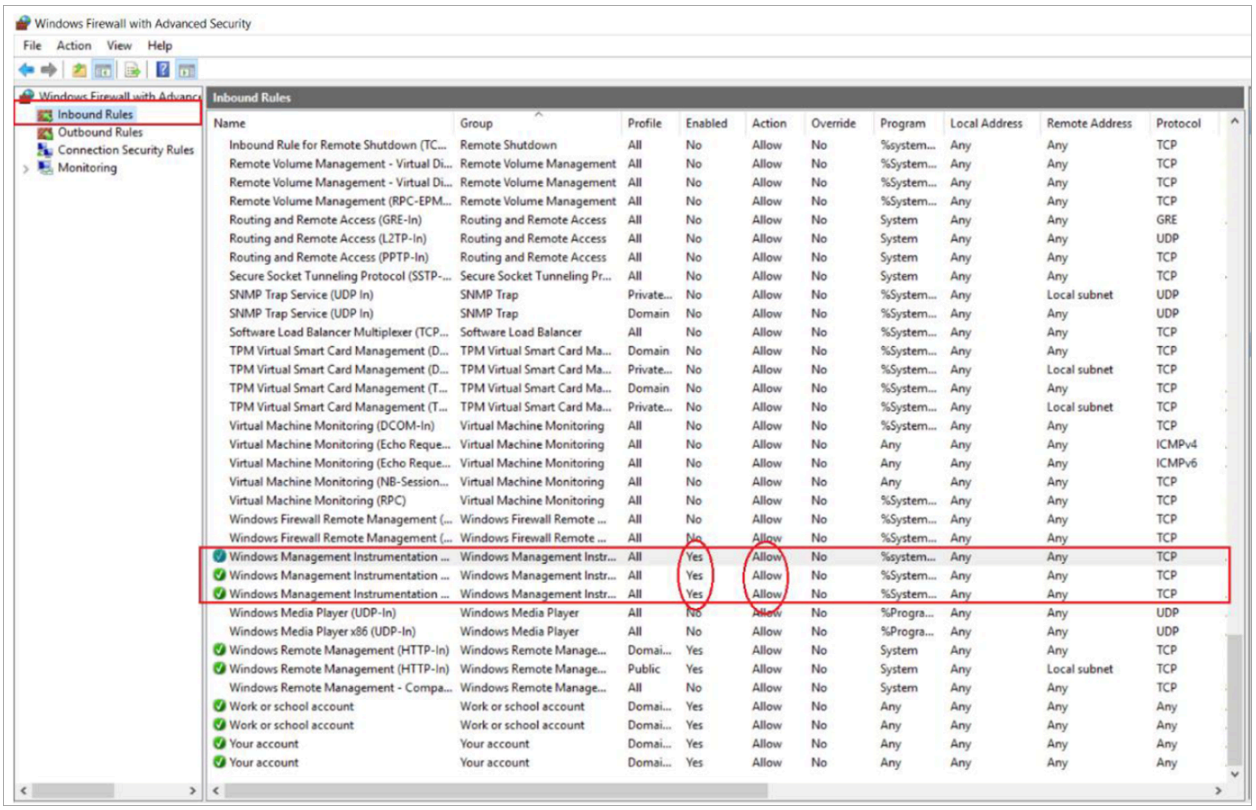
Update Firewall Rules

On Active Directory, go to the Windows Firewall and enable the following inbound rules:

- Remote Event Log Management (RPC)
- Remote Event Log Management (RPC-EPMAP)
- Remote Event Monitor (RPC)
- Remote Event Monitor (RPC-EPMAP)
- Windows Management Instrumentation (Async-In)
- Windows Management Instrumentation (DCOM-In)
- Windows Management Instrumentation (WMI-In)

The following sample screenshots show that these rules are enabled. The Enabled column shows Yes, and the Action column shows Allow.





Configure a Non-Administrator User

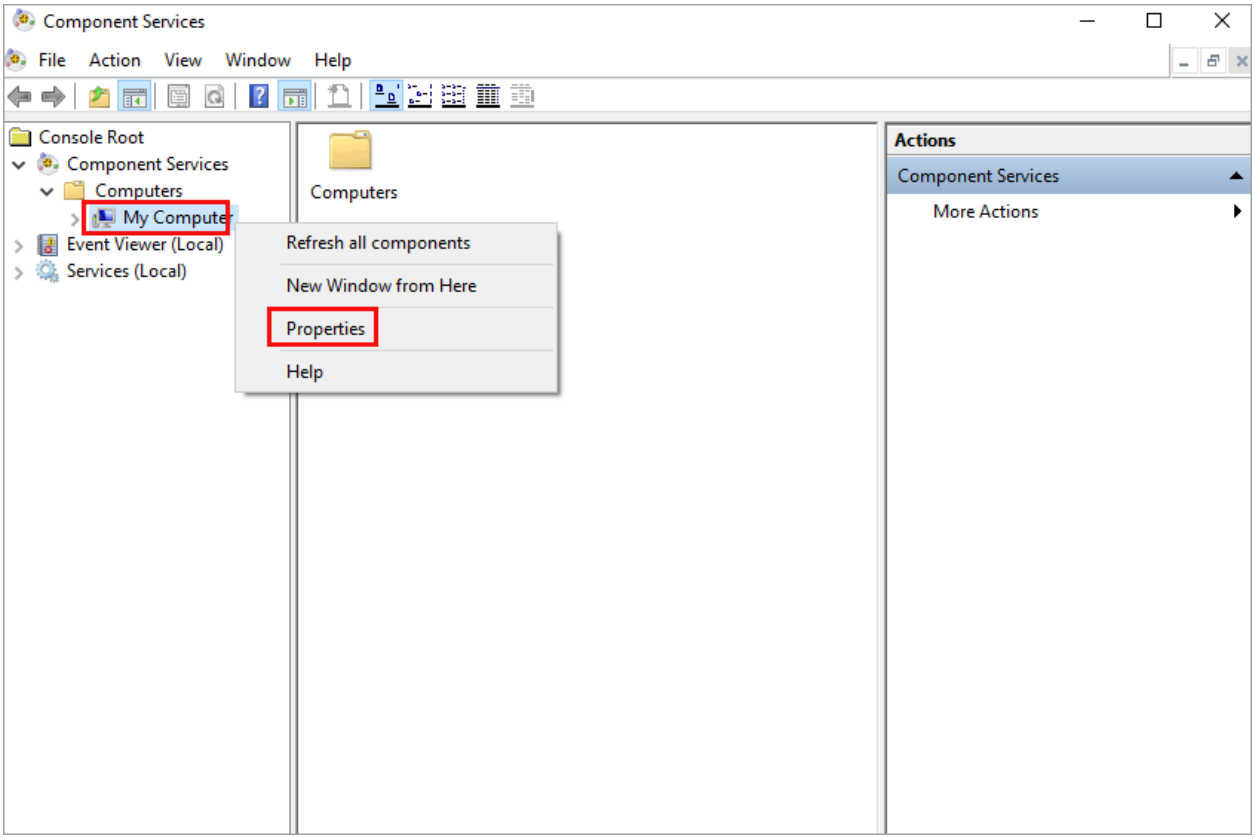
To allow a non-administrator user to access event logs and group filters on Active Directory:

1. Create a new user and add the user to the relevant Active Directory built-in groups so that they can access event logs.
    a. On the Active Directory Server, add a new user (for example, event-auditor). For this user, select the User Cannot Change the Password and Password Never Expires options, to ensure that the password cannot be changed at the next login.
    b. Add the user to a group (for example, event-auditors).
    c. Select the Active Directory domain (for example, acme-corp.local) > Builtin, and then select Event Log Readers in right side panel.
    d. Right-click on Event Log Readers, and select Add to a Group.
    e. Under Enter the Object Names To Select, enter the name of the group you created above (here, event-auditors).
    f. Click Check Names, and then click OK.
    g. Repeat Steps 1b through 1d for Builtin Distributed COM Users.
    h. Repeat Steps 1b through 1d for Builtin Performance Monitor Users.
2. Configuring the DCOM Security Settings to allow the groups to access the system remotely.
    a. Click Start and then select Run.

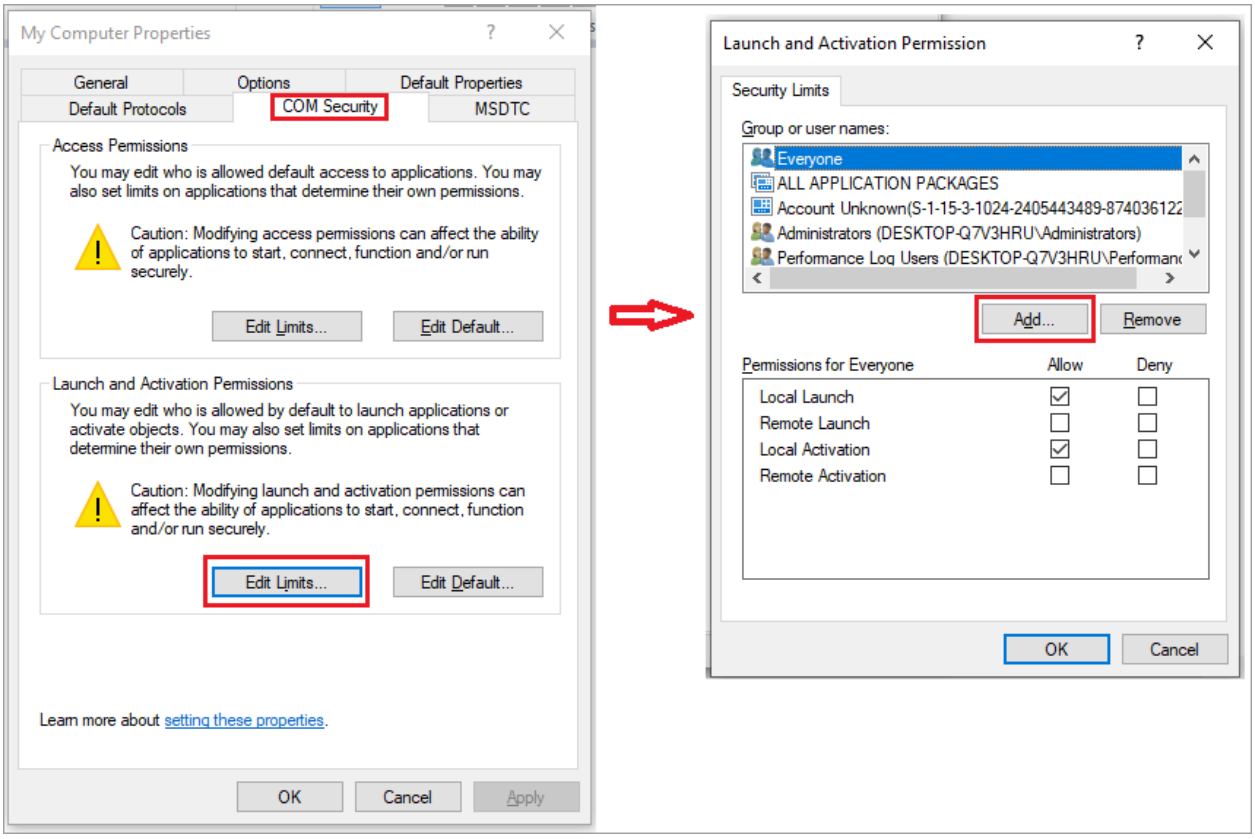
b. Type **dcomcnfg**, and then click OK.

c. Drill down to the Component Services tree until you find My Computer.

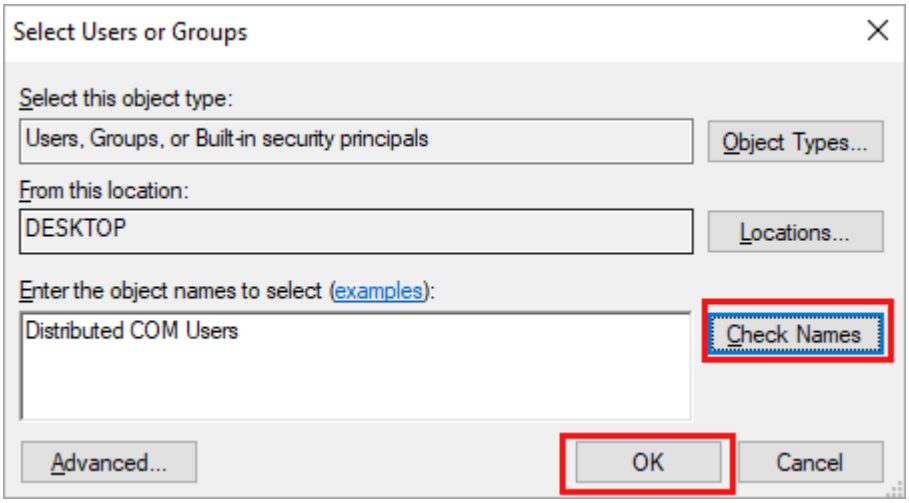
d. Right-click My Computer, and then in the menu, select Properties.



e. In the My Computer Properties screen, select the COM Security tab, and then in the Launch and Activation Permissions section, click Edit Limits. Then click Add.



f. In the Select Users or Groups window, type Distributed COM Users in the Enter the Object Names To Select field.



g. Click Check Names, and then click OK.

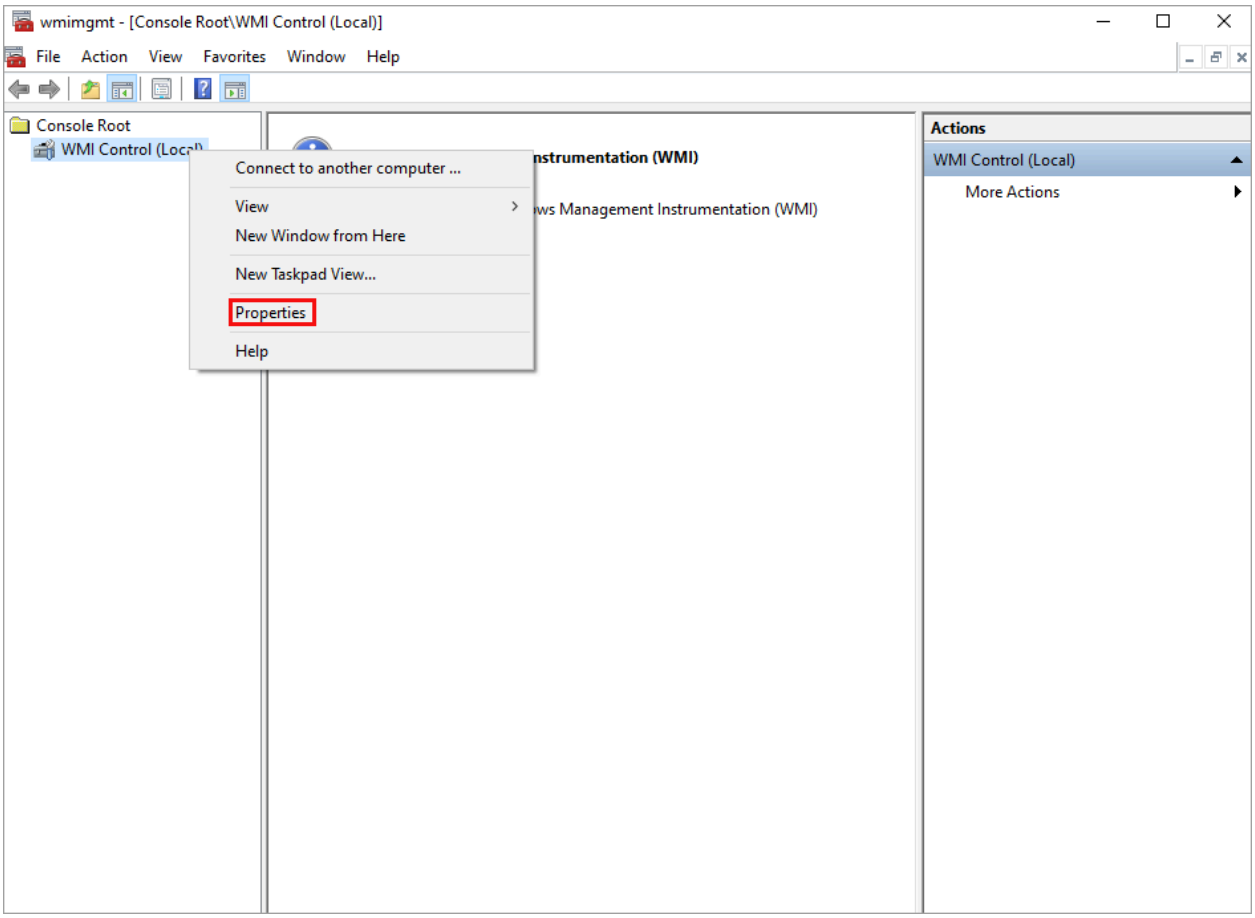
h. Click Add.

i. Repeat Steps 2c through 2h for the Performance Monitor Users group.

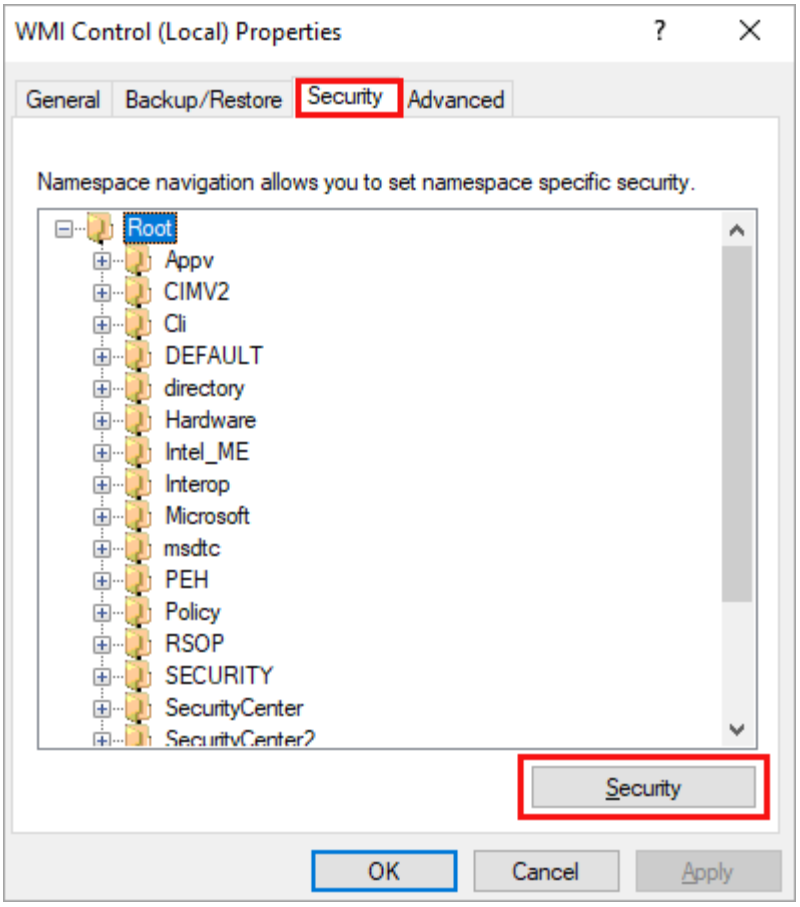
j. Check Allow for the permissions for each of these groups—Local Launch, Remote Launch, Local Activation, Remote Activation.

k. Click OK.

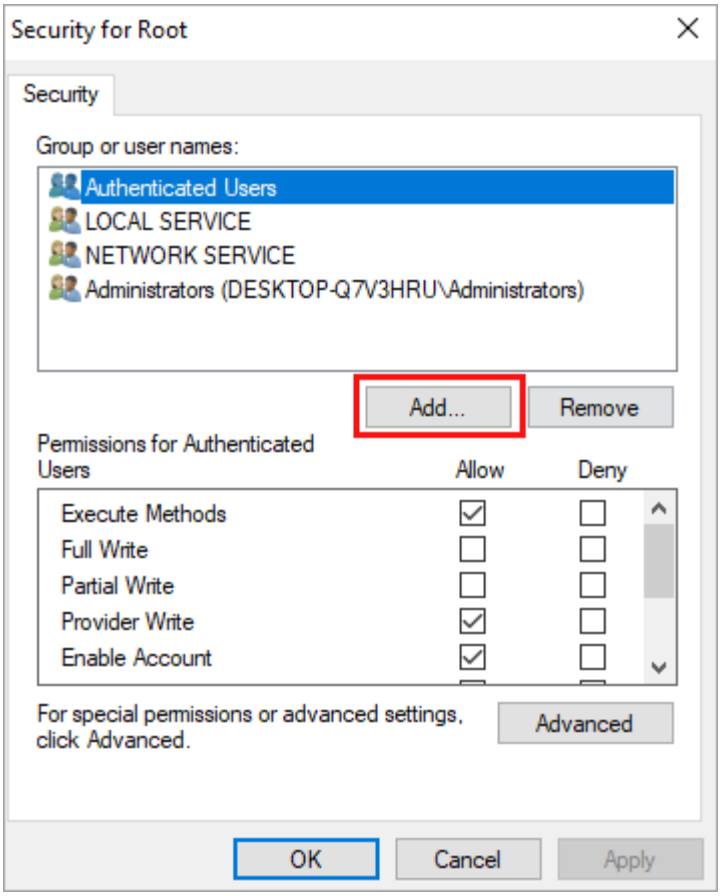
3. Set the WMI control security settings that you want to apply to all name spaces, to ensure that all classes in all name spaces receive access for both user groups. You do this so that the OpManager can fetch this data using WMI.
   a. Click Start and then select Run.
   b. Type **wmimgmt.msc**, and then click OK.
   c. In the wmimgmt window, right-click WMI Control (Local) and then click Properties.



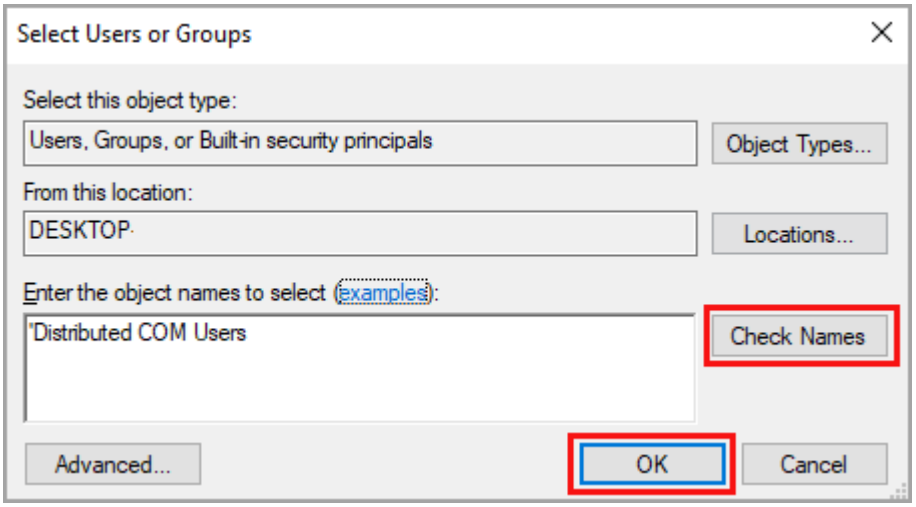
   d. In the WMI Control (Local) Properties window, select the Security tab.
   e. Select Root and then click Security.



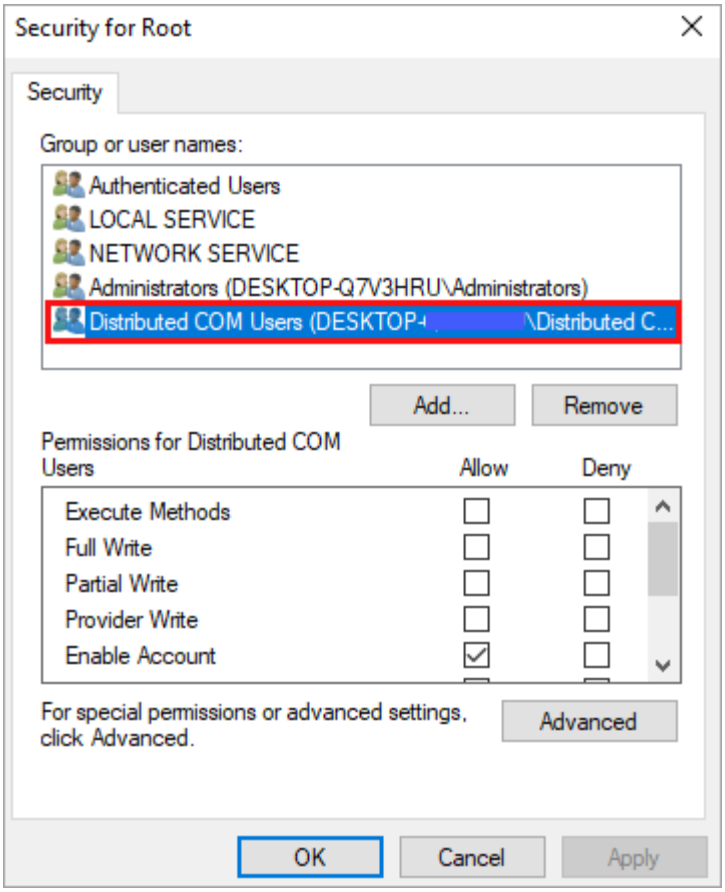
f. In the Security for Root window, click Add.



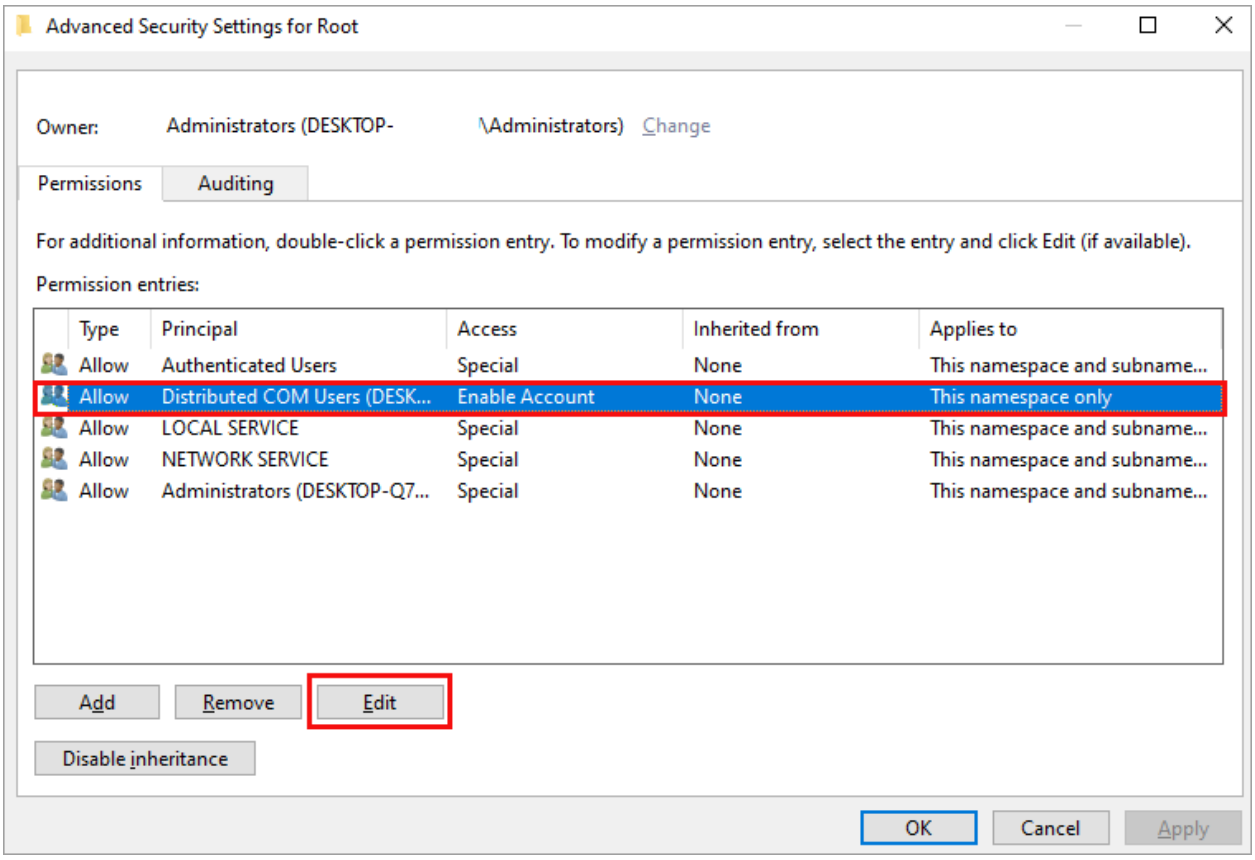
g. In the Select Users or Groups window, type Distributed COM Users in the Enter the Object Names To Select field.



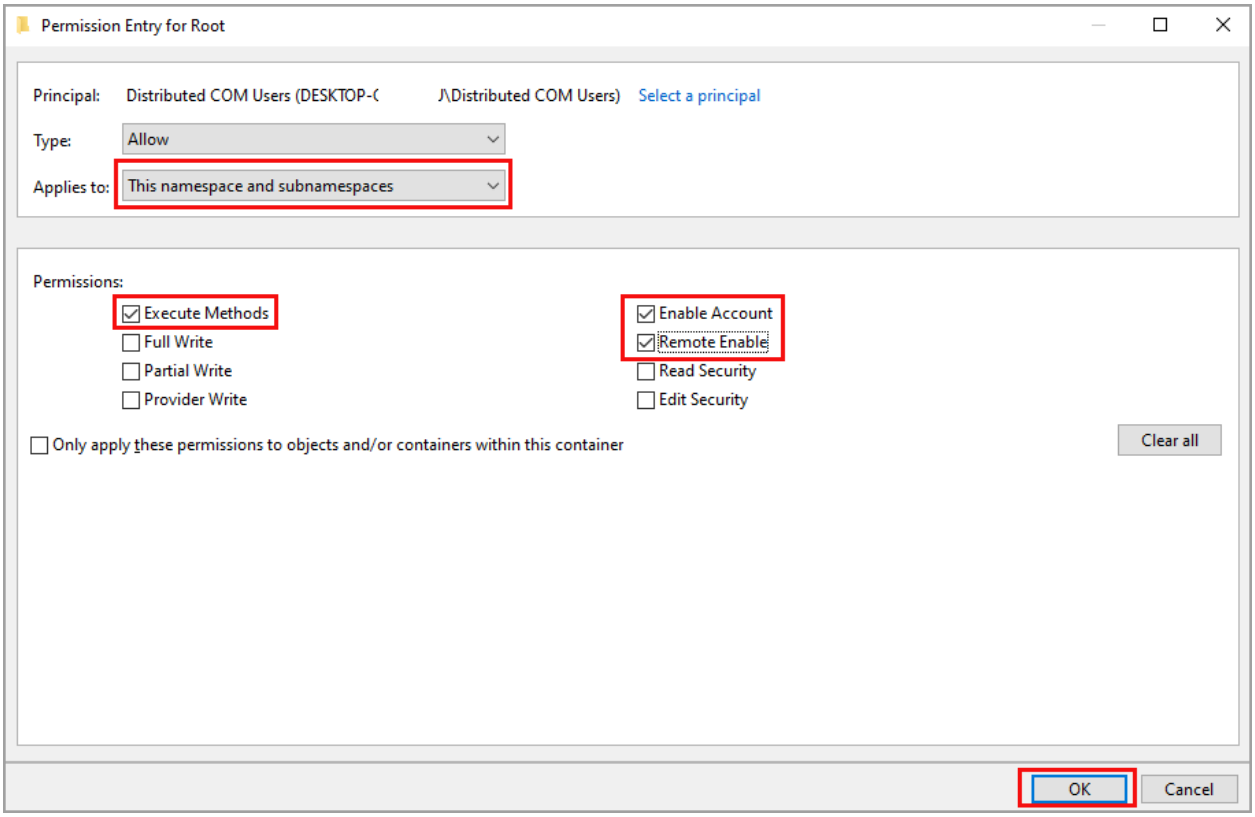
h. Click Check Names and then click OK.



i. In the Security for Root window, select the Distributed COM Users, and then click Advanced.



j. In the Advanced Security Settings for Root window, select Distributed COM Users, and then click Edit.



k. In the Permission Entry for Root window, select This Name Space and Sub-Name Spaces in the Applies To field.
l. Under Permissions, check Execute Methods, Enable Account, and Remote Enable.
m. Click OK
n. Repeat Steps 3d through 3m for the Performance Monitor Users group.
o. Click OK.

Configure the WMI Agent

This section describes how to install and configure the WMI agent.

Before You Begin

Before you install the WMI agent:

- Copy the root-ca-cert.pem and client-cert.pfx certificate files from the VMS server to the WMI agent device. These files are in the /opt/versa/vms/certs/ directory on the VMS server. Because these files are the same on the active and standby VMS servers, you can copy them from any VMS server. Note that you cannot copy the files without changing file permissions. For more information, see Configure the Standby VMS Server, above.
- Although not mandatory, it is recommended that you configure a static IP address for the WMI agent. Doing this simplifies management of the WMI agent because the address is not allocated dynamically. In any case, you must ensure that the WMI agent resolves DNS lookups using the DNS server that was updated with FQDNs for the VMS

servers, as described in Configure the Standby VMS Server, above. The WMI agent is configured to connect to VMS servers using the FQDN, so to resolve these names, the WMI agent must point to the correct DNS server or servers.

Install the WMI Agent

You can install the Versa WMI agent as a standalone component or as a software package installed on a Windows server. The standalone installation is supported on the Windows 10 Client or Windows Server 2016. For hardware requirements, see the Windows 10 Client or Windows Server 2016 documentation.

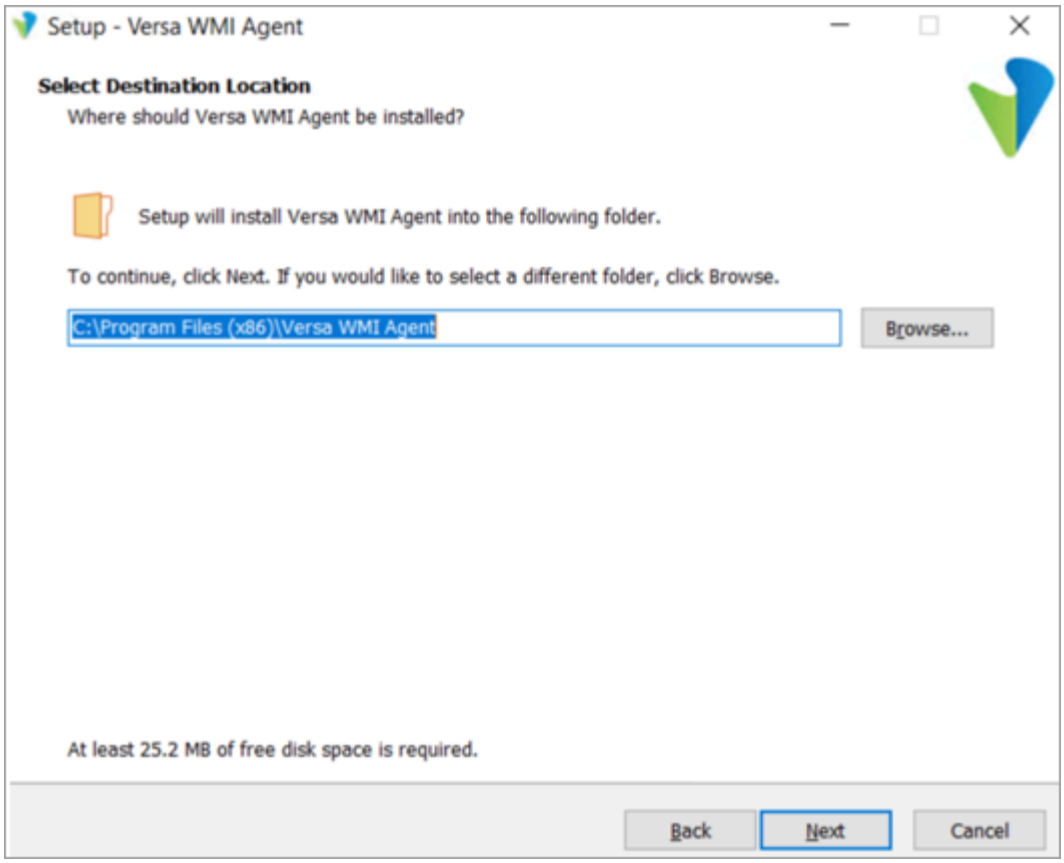
Before you install the WMI agent:

- Download the WinSCP or Wireshark application to the Windows device so that you can use it for debugging.
- After you install Windows, copy the VersaWmiAgentInstaller.exe file to the Windows device from the following link: https://versanetworks.app.box.com/s/d7jh1z6y3kaijd3yfwil0uxchr1w9ton

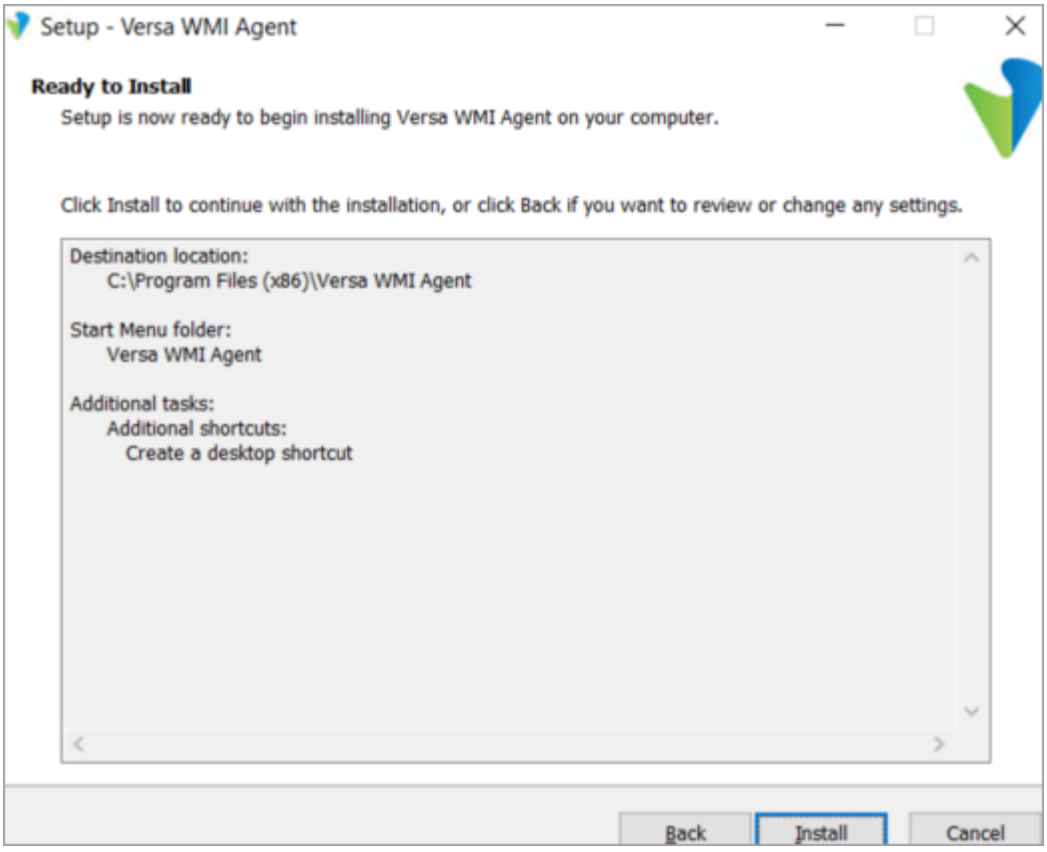
To install the WMI agent:

1. Double-click the VersaWmiAgentInstaller.exe file to initiate the installation wizard.

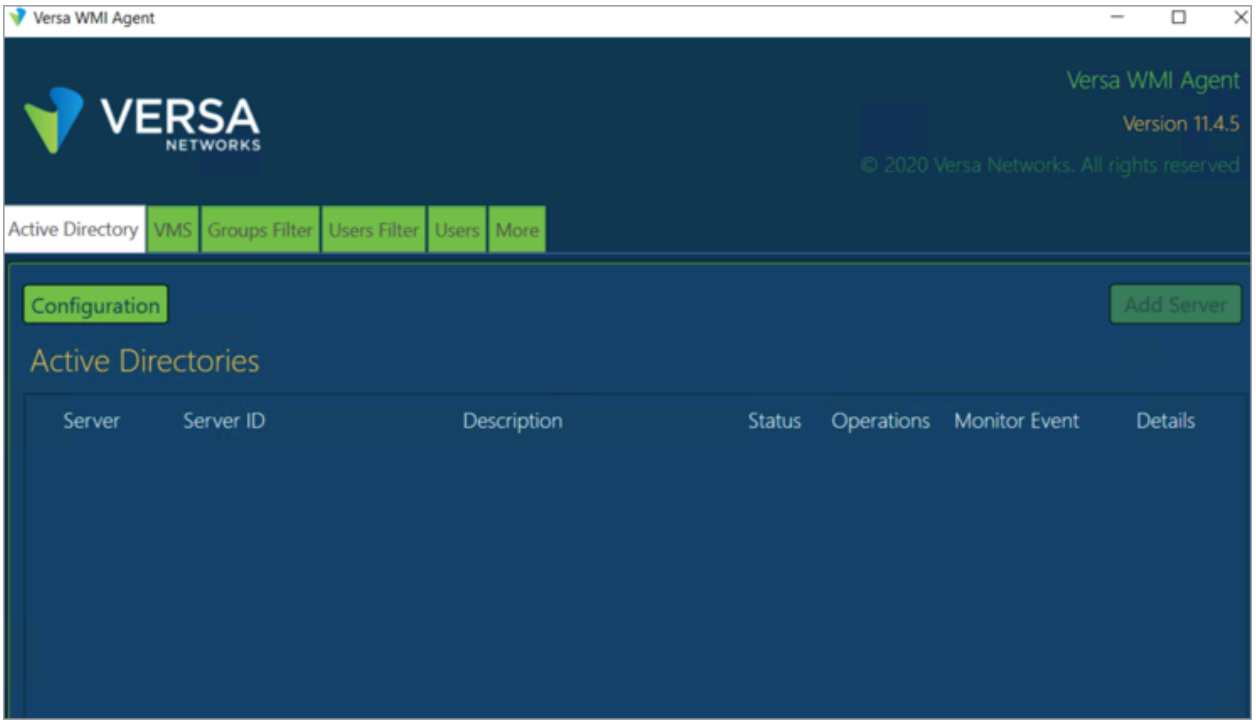
2. Click Next in all the windows of the WMI agent installation wizard until you finish the installation.



3. In the Ready to Install window, click Install, and then, in the last wizard window, click Finish to complete the installation.



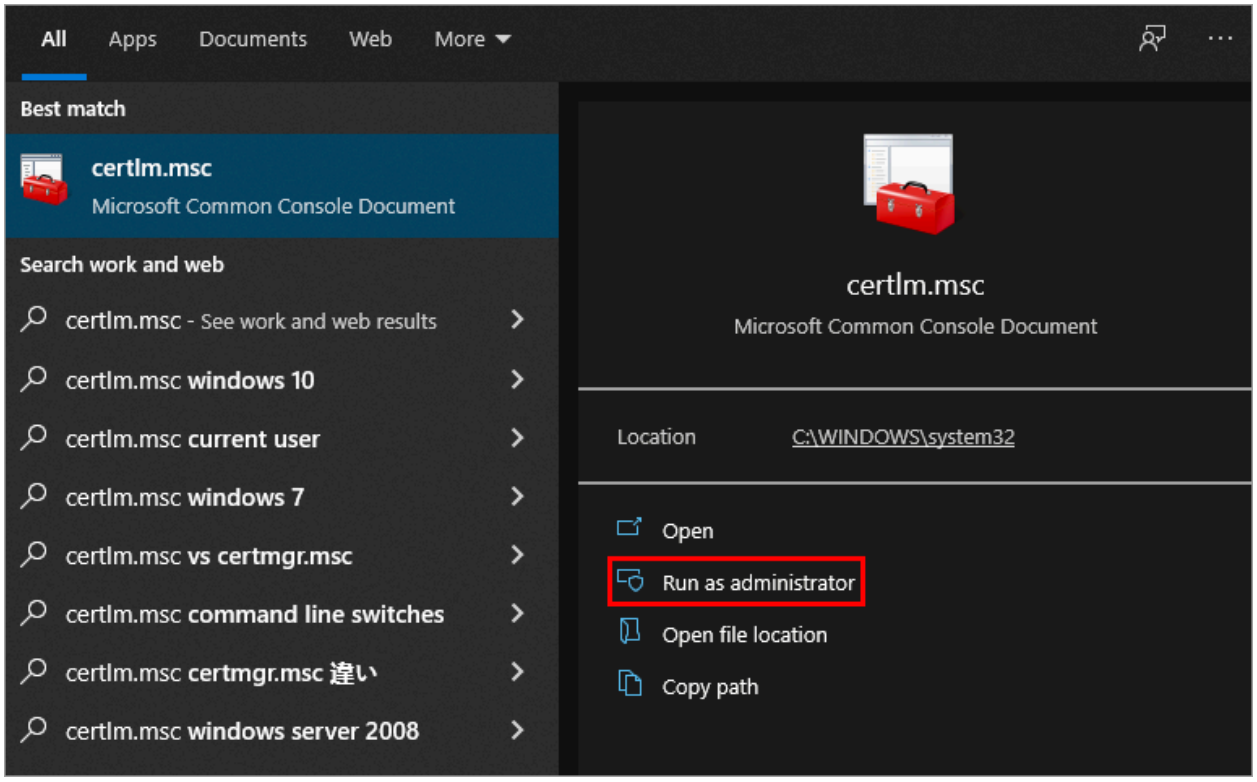
After you click Finish, the WMI agent launches.



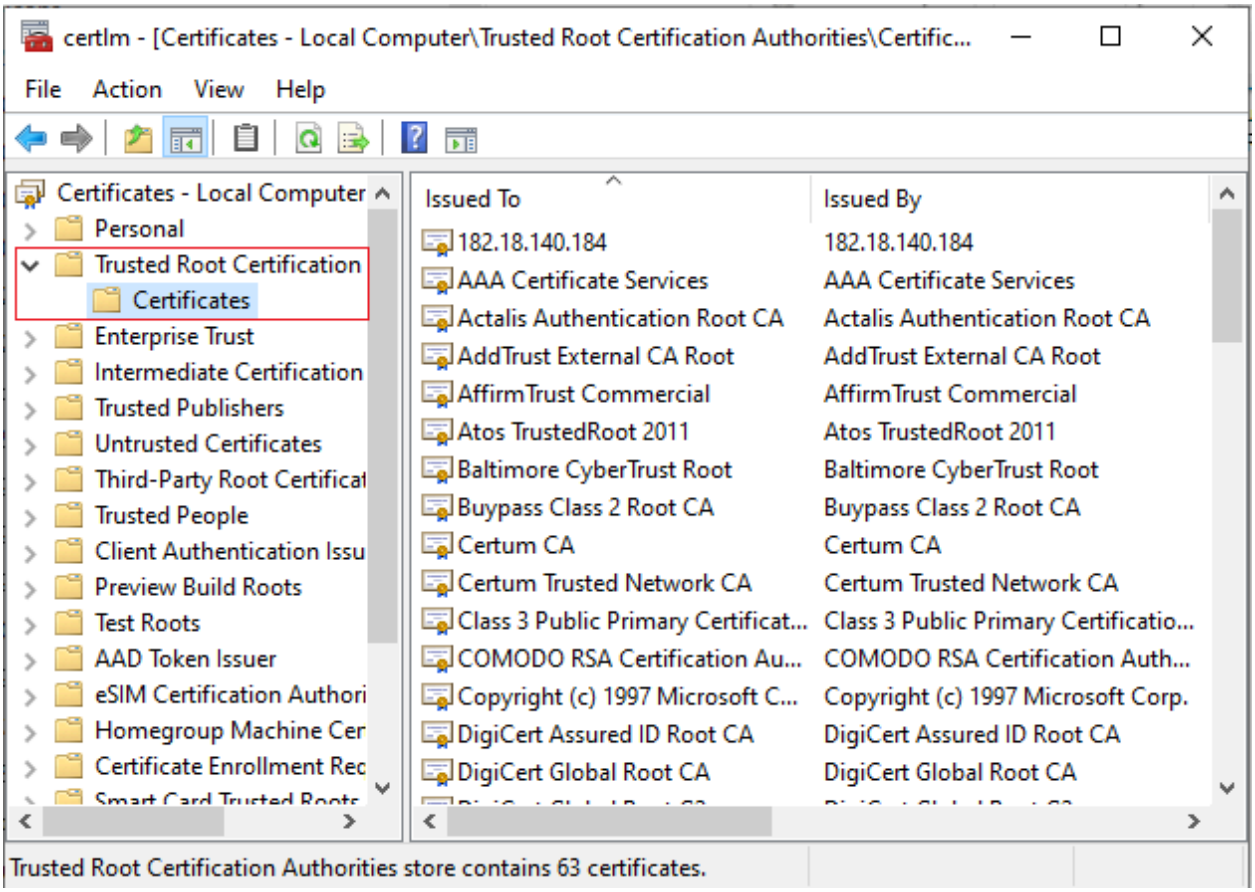
Install the Root CA Certificate

To install the root-ca-cert.pem certificate file in the Windows client Certificate Store:

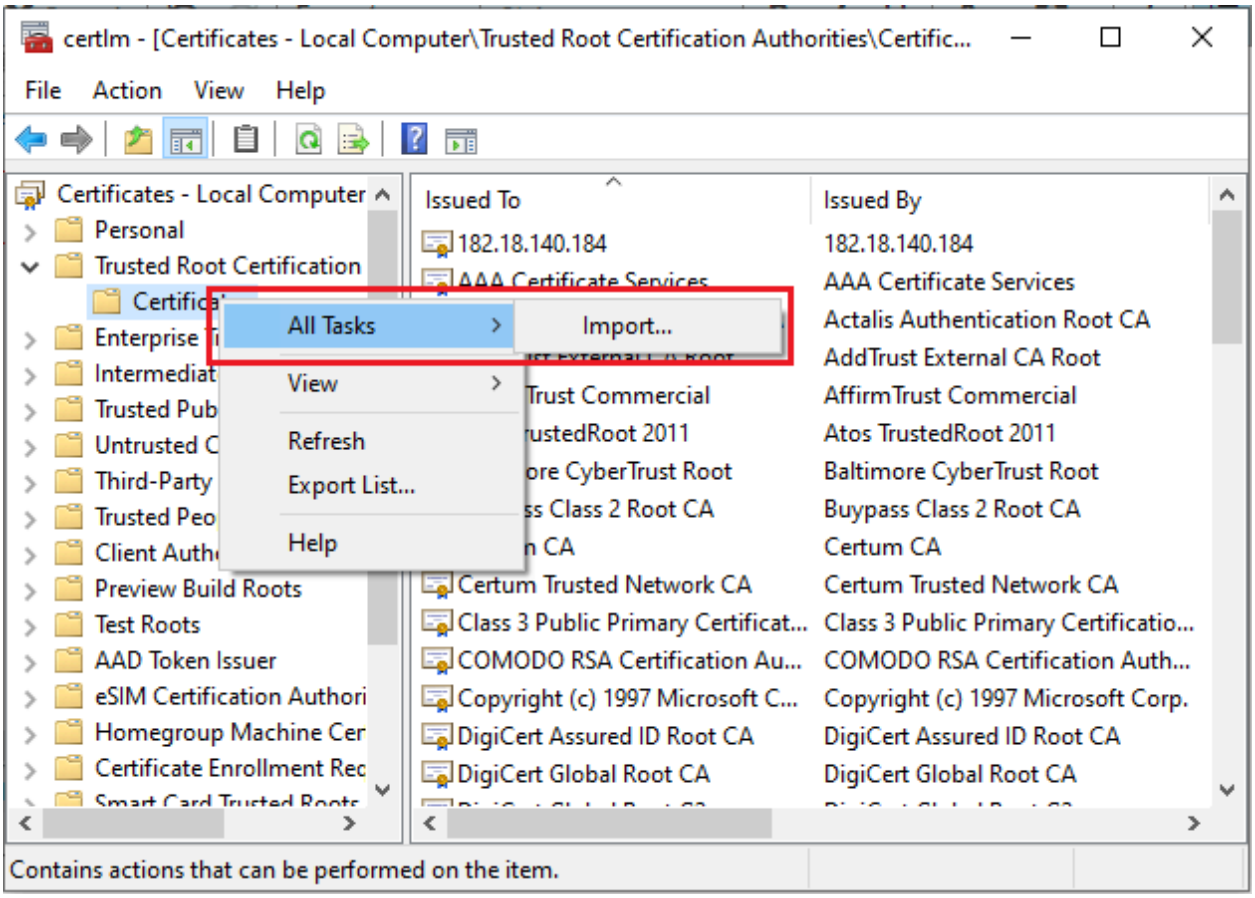
1. On the Windows device with the WMI agent, open certlm.msc and then select Run as Administrator.



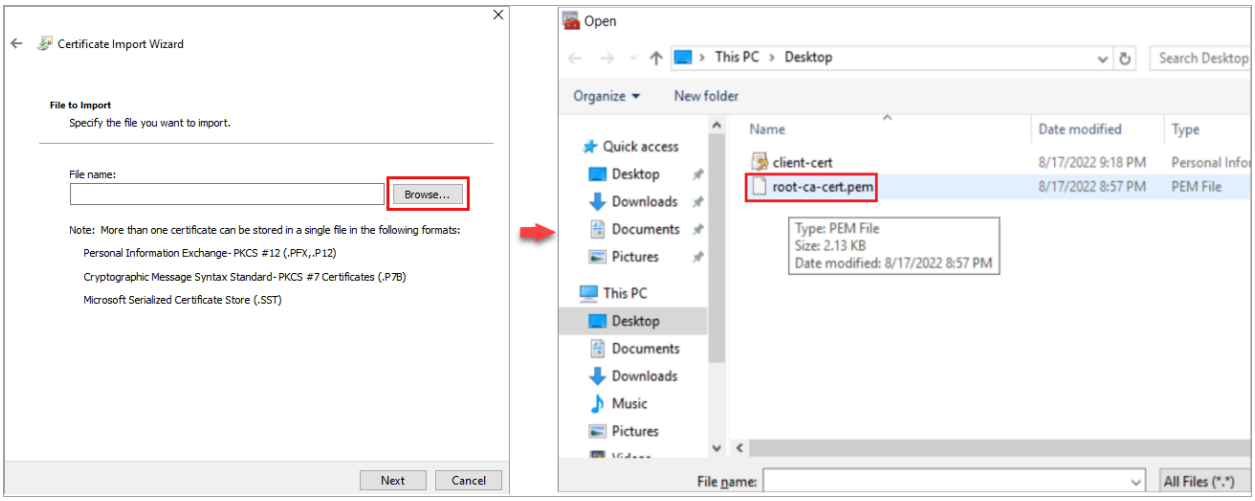
2. In the certlm popup window, select Trusted Root Certification Authorities > Certificates.



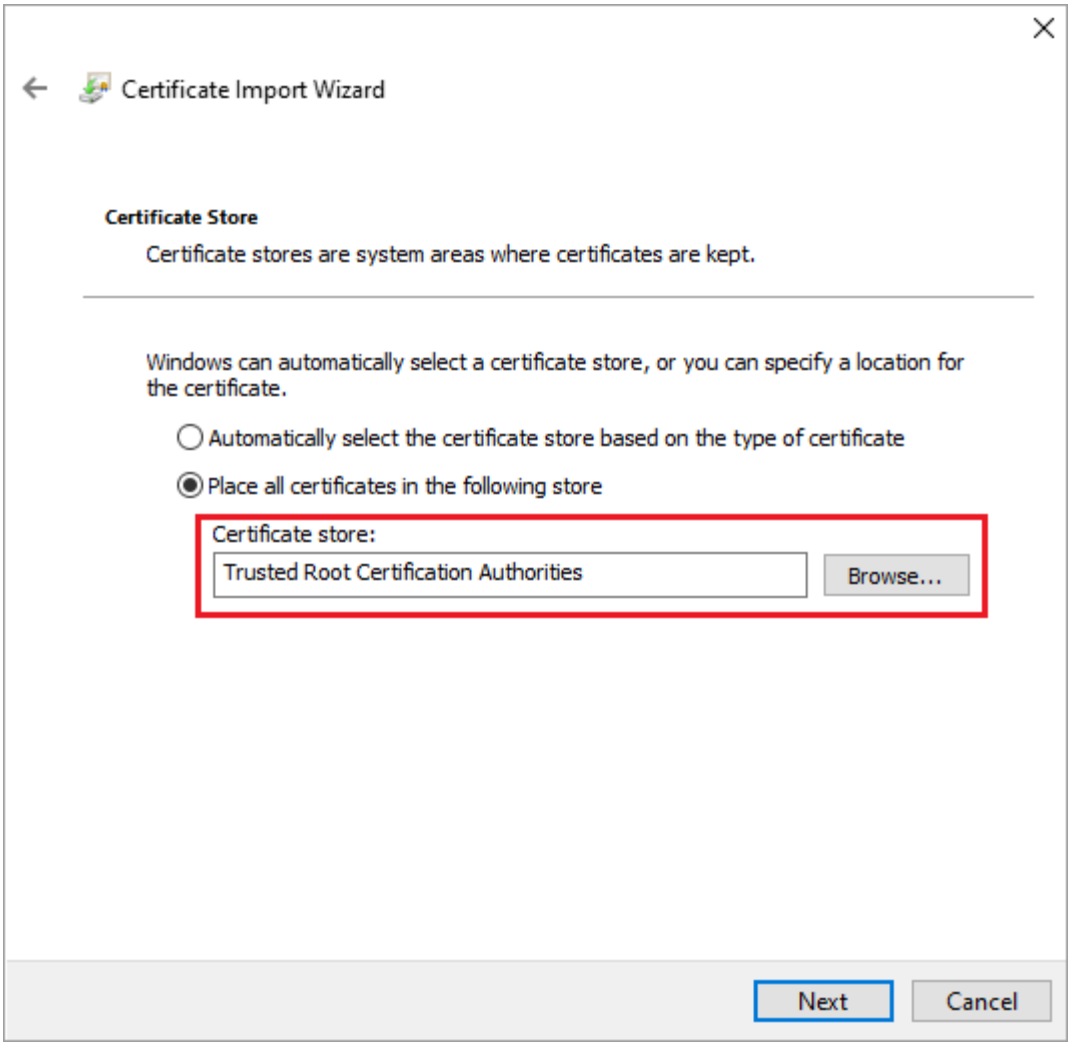
3. Right-click Certificates, select All Tasks, and then click Import.



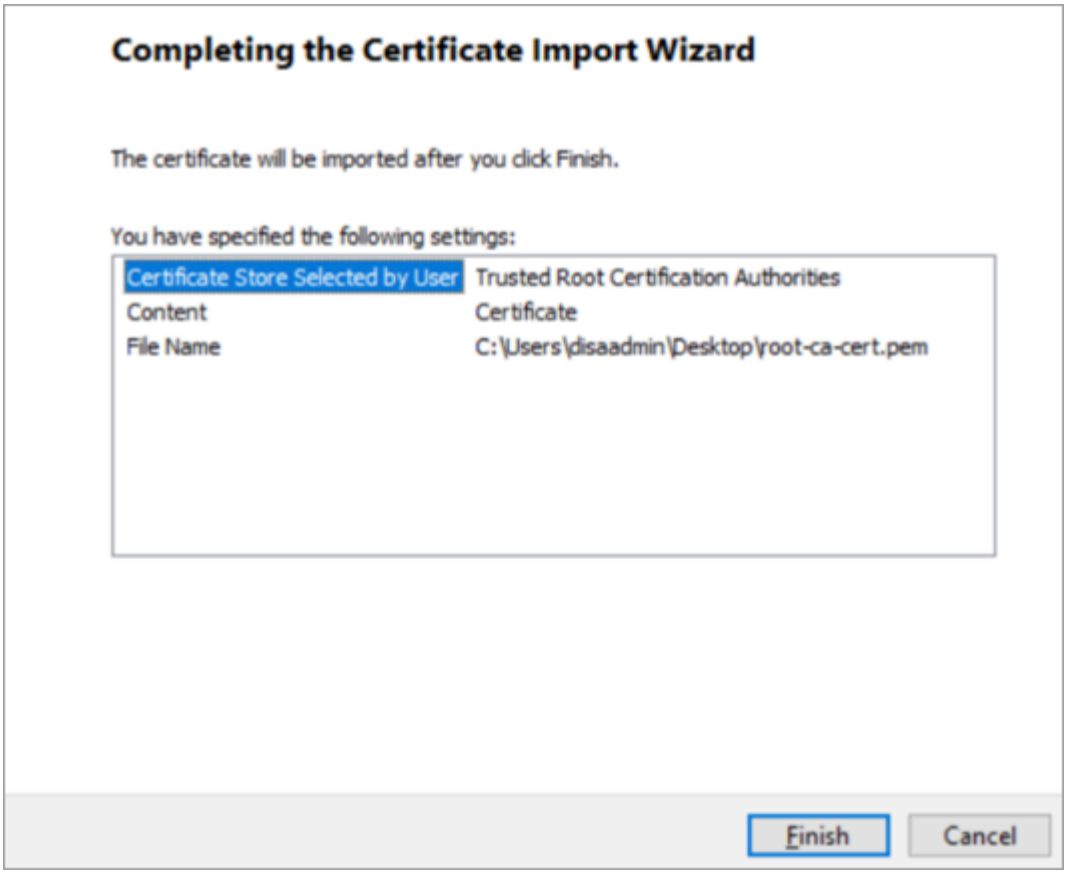
4. In the File to Import window, click Browse and select the root-ca-cert.pem certificate file from the location where you saved it.



5. Click Next.
6. In the Certificate Store window, click Place All Certificates in the Following Store (which is the default), and then select Trusted Root Certification Authorities (which is the default).



7. Click Next, and then click Finish in the final window of the wizard.

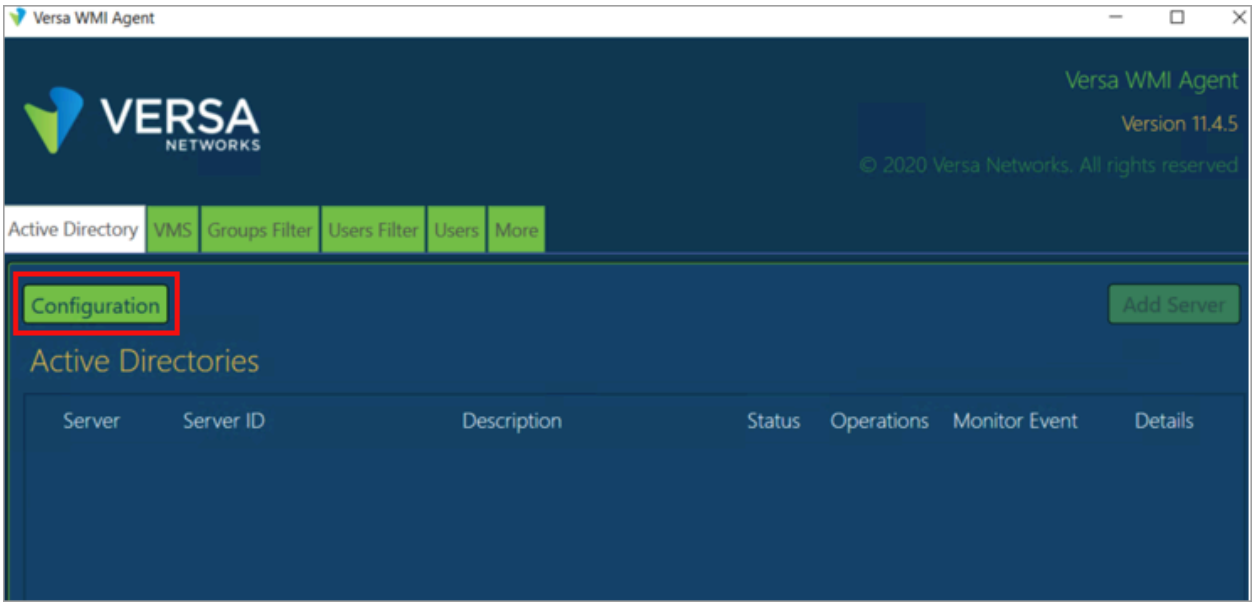


Configure Active Directory Servers

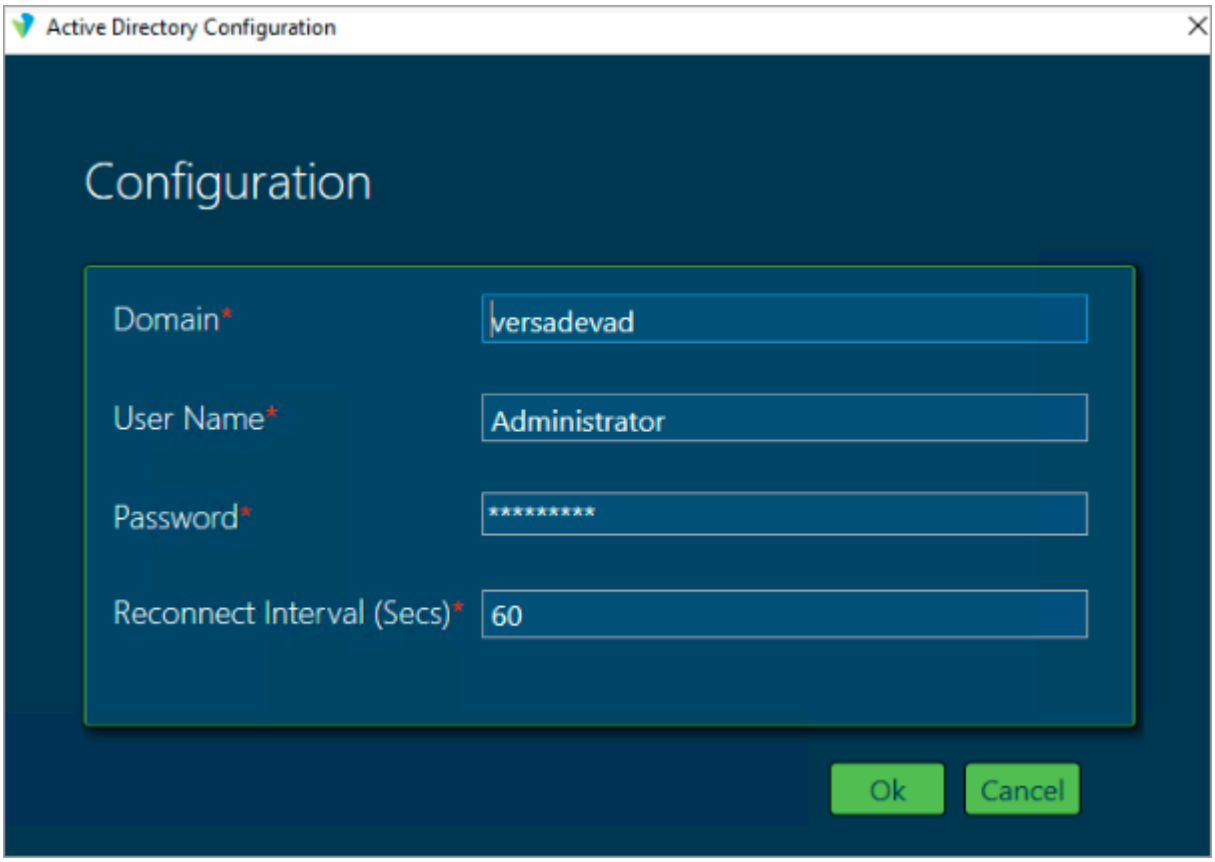
After you install the WMI agent, you configure Active Directory server information for the WMI agent so that it can receive information from Active Directory.

To configure an Active Directory server on the WMI agent:

1. To start the WMI agent, double-click the  WMI agent shortcut on the desktop. The Active Directory tab displays.

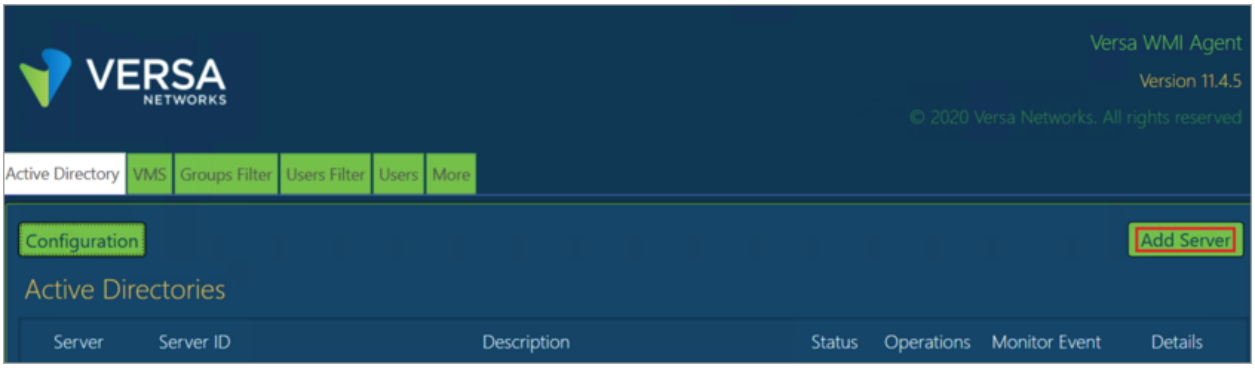


2. To configure authentication information for Active Directory, in the Active Directory tab, click Configuration. The Active Directory Configuration popup window displays. In the following example, the domain is acme-corp.local, the username to connect to Active Directory is Administrator, and the Administrator password is also provided.

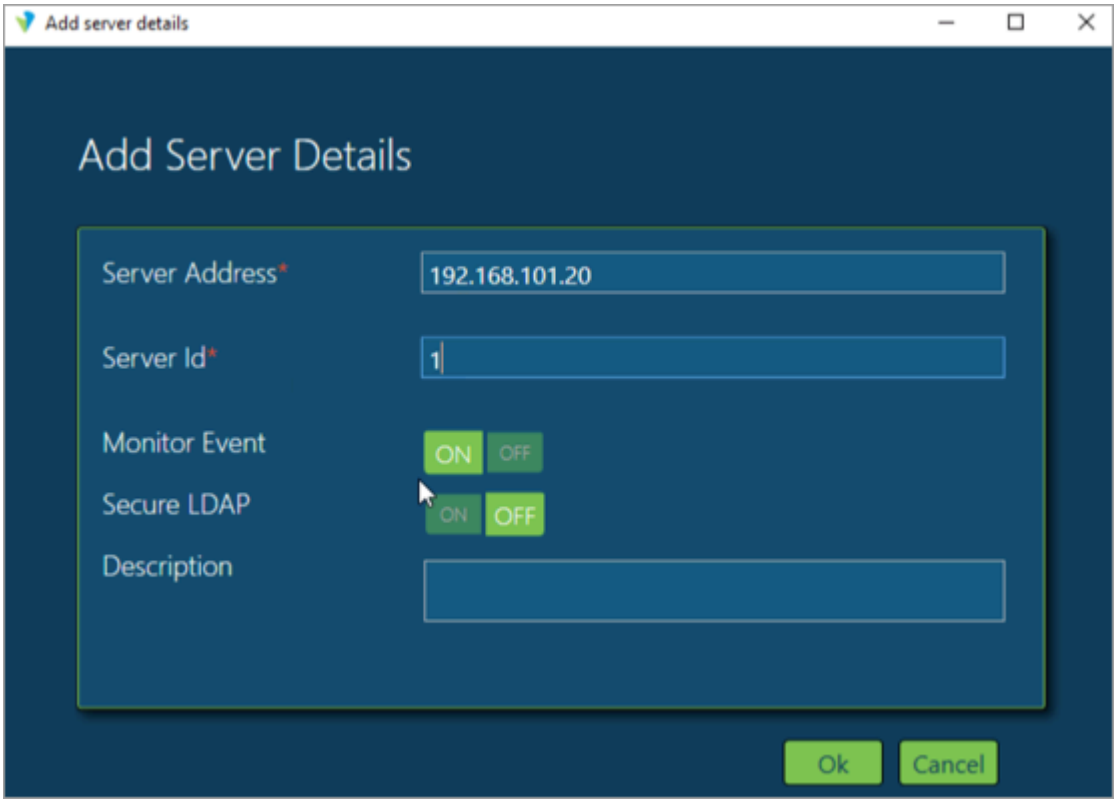


3. Click OK.

4. To enter Active Directory server information, click Add Server.

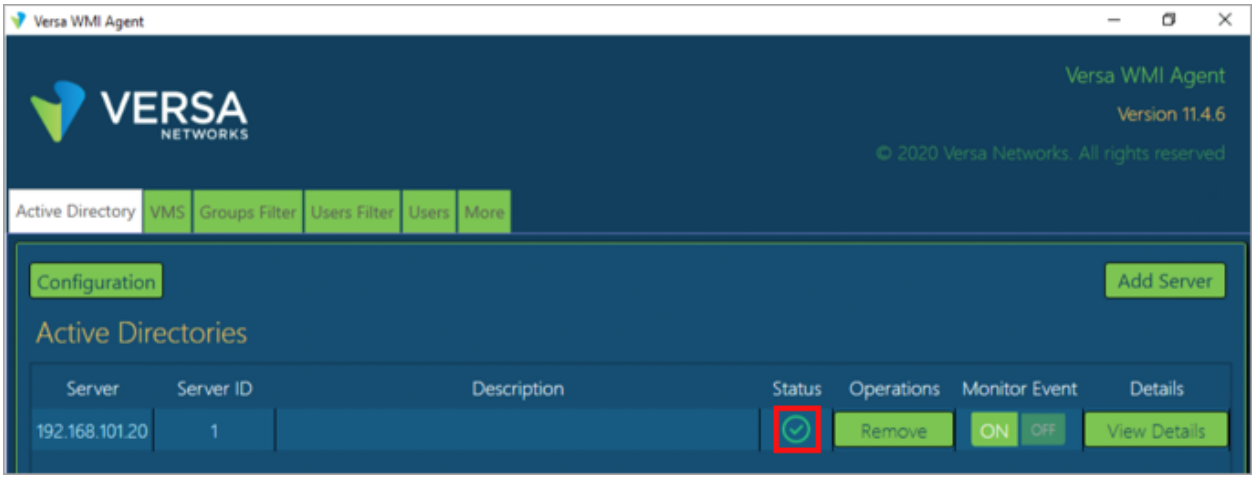


5. In the Add Server Details popup window, enter the following information.



   a. Enter the IP address of the server (here,192.168.101.20).
   b. Enter the identifier of the server (here, 1). You can use any value for the identifier, because the server ID is local to the WMI agent.
   c. Click OK.

6. Check the status under Active Directories. A green checkmark indicates that the WMI agent is successfully connected to the Active Directory server, as shown in the following screenshot. If you configure the IP address or credentials of the Active Directory server incorrectly, the status displays red.



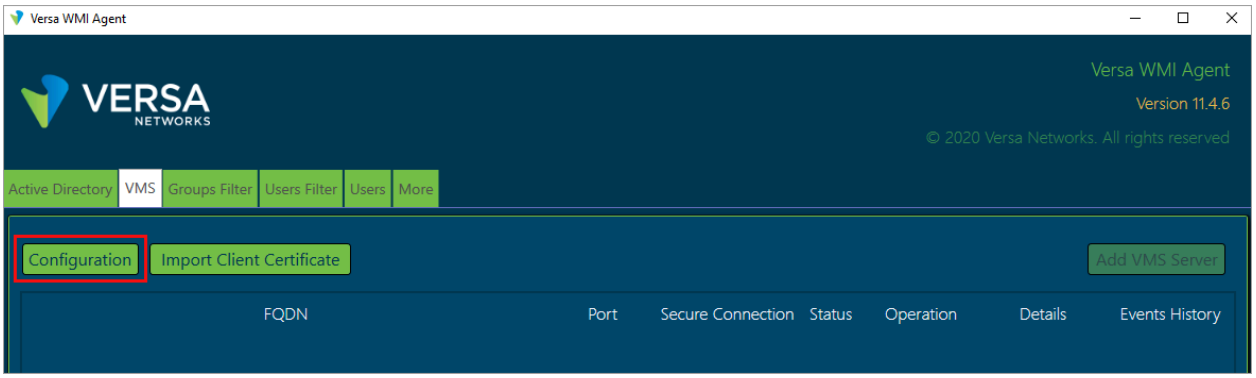
7. Repeat Steps 1 through 5 to configure other Active Directory servers in the domain.

Configure VMS Servers

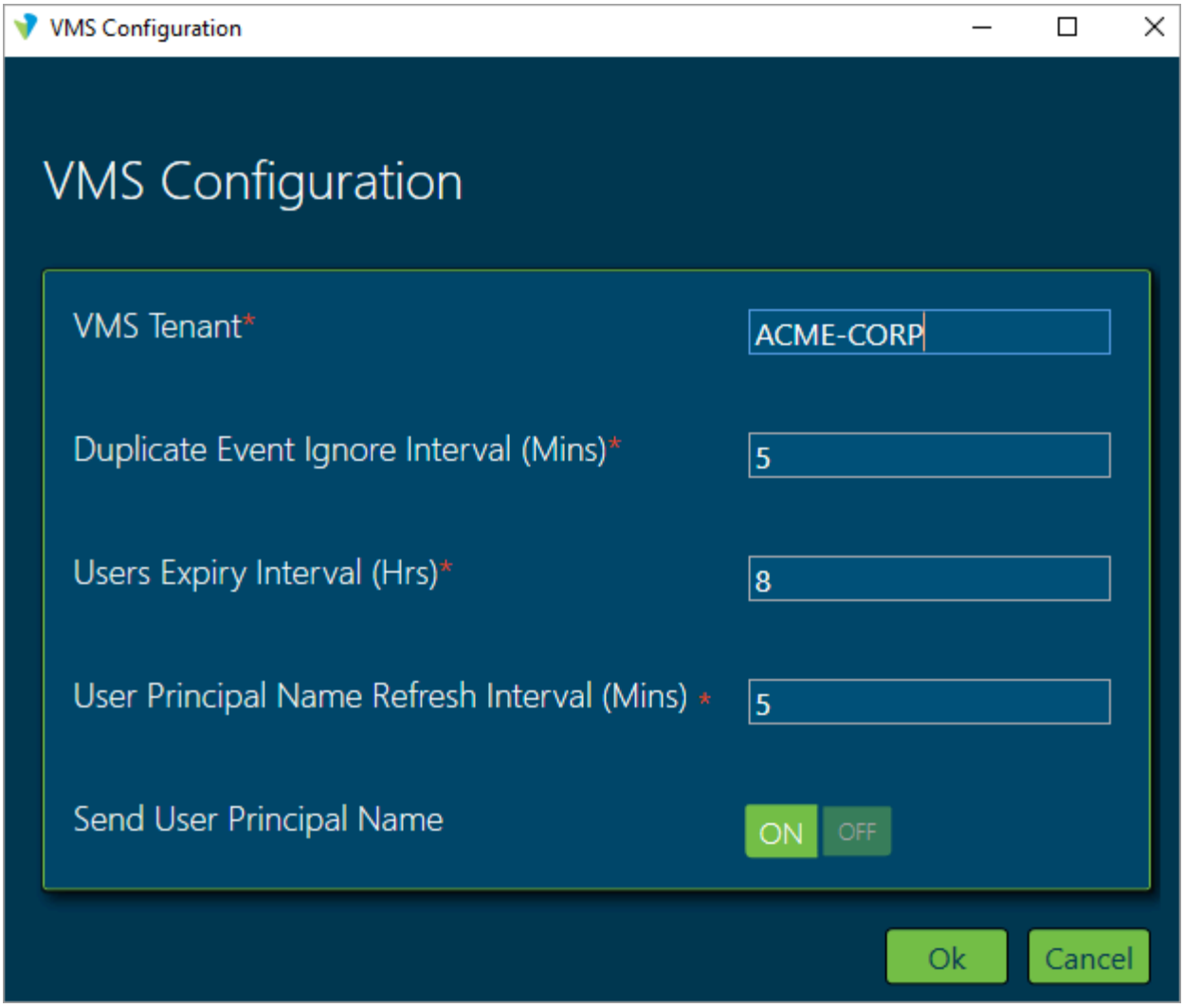
You configure VMS server information for the WMI agent so that it can receive information from Active Directory and pass it to the VMS server.

To configure a VMS server:

1. In the WMI agent main window, select the VMS tab.



2. Click Configuration. In the VMS Configuration popup window, enter the following information.



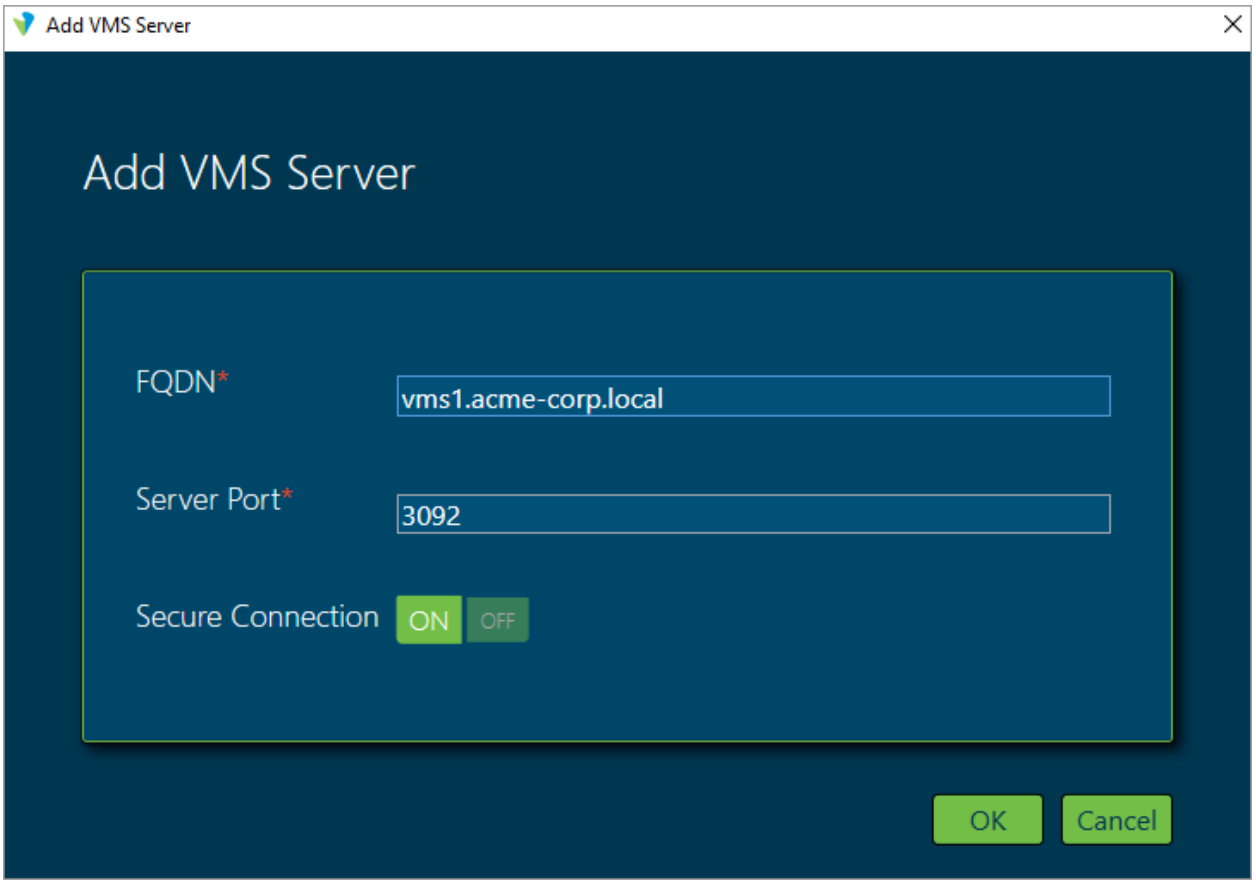
a. Enter the VMS tenant name (here, ACME-CORP). The VMS tenant is the name of the organization as configured on Versa Director. This field is case-sensitive, so enter the organization name exactly as it appears in Versa Director.

b. Enter values for the other required fields. The values shown in the screenshot are the default values.

c. If Active Directory is not configured with a user principal name, toggle the Send User Principal Name to Off. If you do this, sAMAccountName is populated instead. (The sAMAccountName attribute is a login name that supports clients and servers from previous Windows versions, for backwards compatibility, such as Windows NT 4.0, Windows 95, Windows 98, and LAN Manager.)

d. Click OK.

3. In the VMS tab, click Add VMS Server. In the Add VMS Servers popup window, enter the following information.

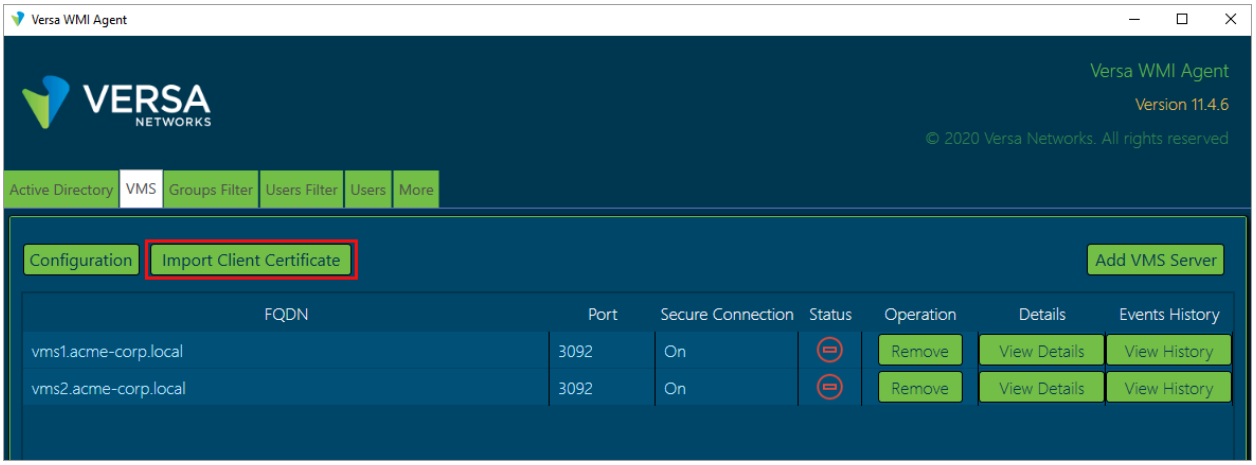


a. Enter the FQDN of the VMS server to which to connect the WMI agent (here, vms1.acme-corp.local). The FQDNs must the same as those configured on the DNS server and during VMS installation. For more information, see Configure VMS, above.

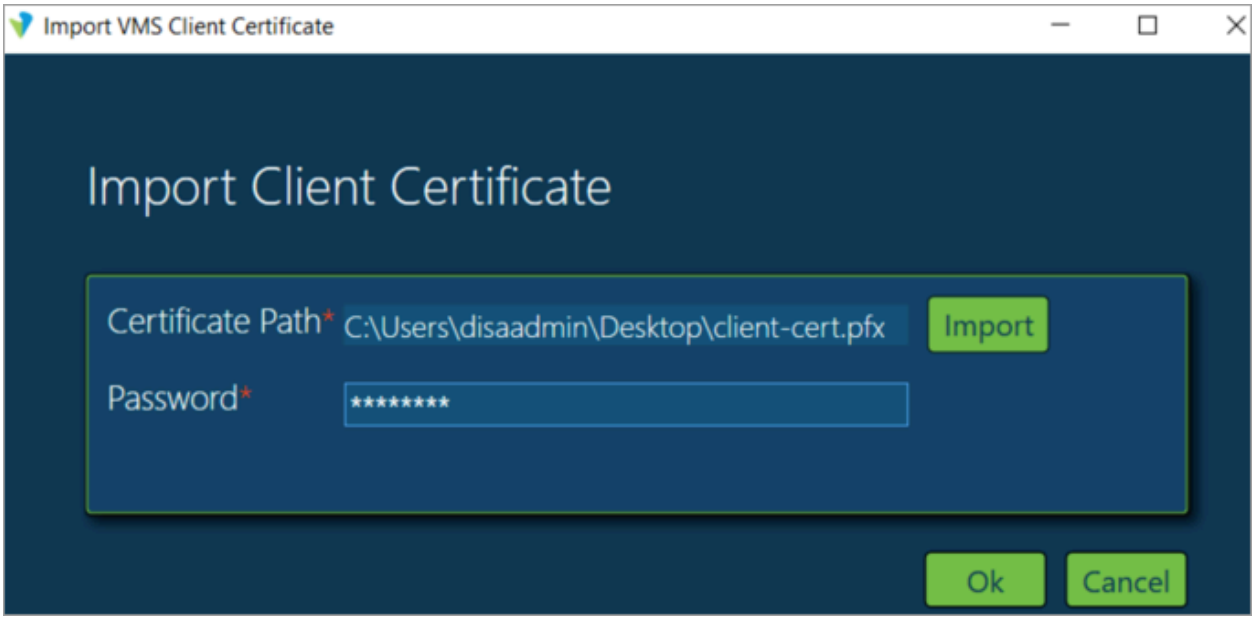
b. Enter the server port number as 3092.

c. Click OK.

4. Repeat Steps 1 through 3 for the other VMS server. The screenshot below shows that two VMS servers configured. Note that the status may display as red until you install the VMS client certificate.

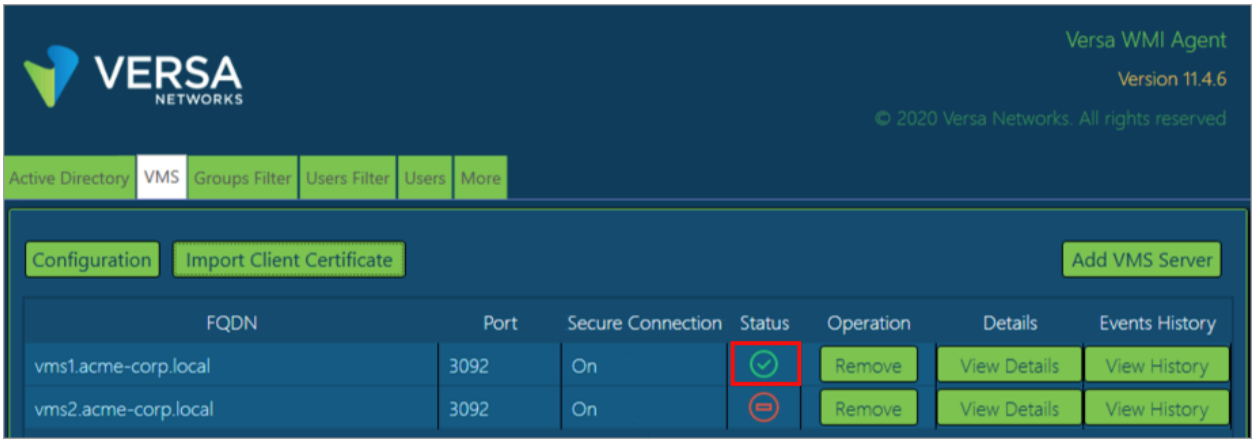


5. To install client certificate, click Import Client Certificate. The Import VMS Client Certificate popup window displays. Enter the following information.



   a. Click Import, and then select the client-cert.pfx certificate.
   b. Enter the password to create the root certificate on VMS. This example uses versa123 as the password.
   c. Click OK.

6. View the status of the VMS server for which you imported the VMS client certificate. In the sample screenshot below, the WMI agent has successfully connected to vms1.acme-corp.local and its status is green. The VMS service is not yet initialized on vms2.acme-corp.local, so the status is red.



Configure Passive Authentication on the Versa Director

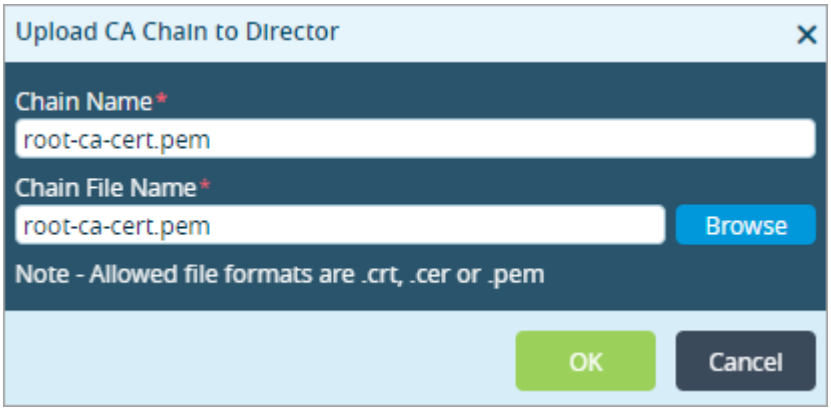
This section describes how to configure the Versa Director to support passive authentication.

Before you configure Versa Director, copy the root-ca-cert.pem file from the /opt/versa/vms/certs/ folder of the VMS server to the device that accesses Director. You can copy this certificate from any VMS server because both servers have the same file.

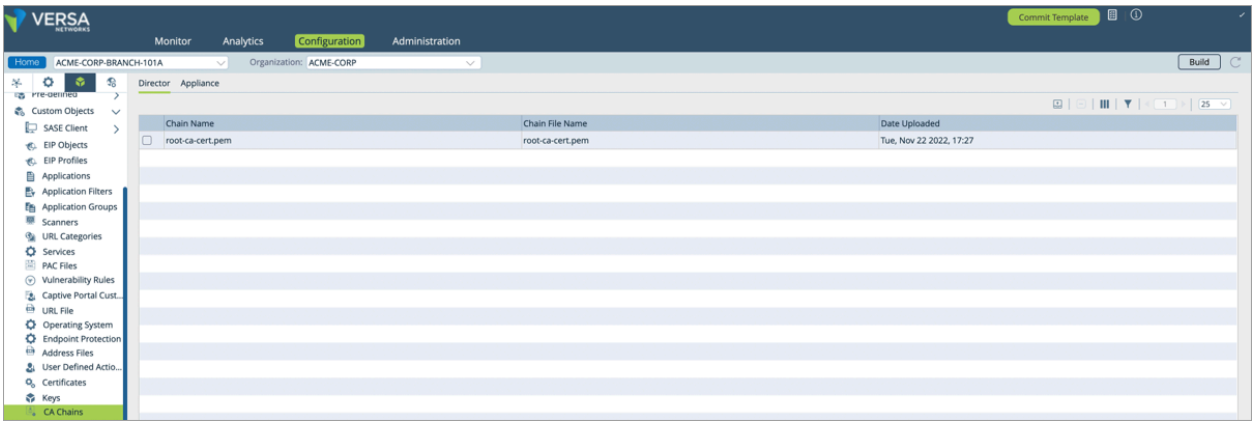
The configuration steps in this section use a device template to configure the messaging service. You can also use a general service template and then create a device group and associate all device templates with the service template. Using templates simplifies the configuration and avoids typographic errors.

Upload the CA Certificate

1. In the Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Devices > Devices in the horizontal menu bar.
   c. Select an organization in the left menu bar.
   d. Select a device in the dashboard. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Configuration > Objects & Connectors > Objects > Custom Objects > CA Chains in the left menu bar
4. Select the Director tab.
5. Click the Upload icon to upload the .crt file to the Director node. The Upload CA Chain to Director popup window displays.



6. In the Chain Name field, enter a name for the chain (here, it is the same name as the chain filename).
7. Click Browse, and then select the CA chain file to upload to the Director node
8. Click OK to upload the file. The main pane displays the uploaded file.

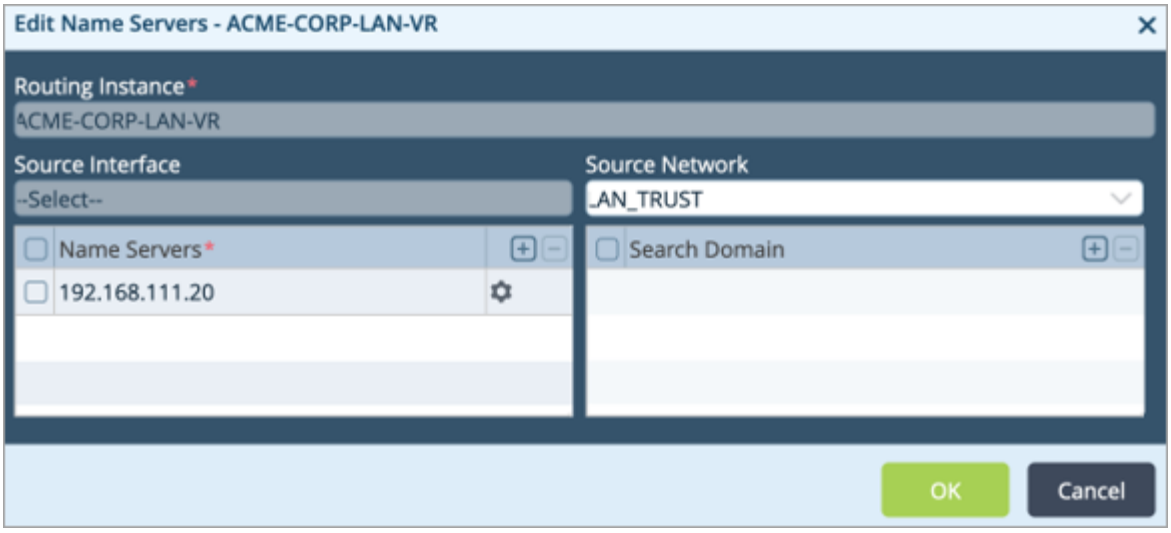


Add Customer DNS Servers

You must add at least one DNS server for the customer to resolve the FQDN of the VMS server. In this example, the FQDN is that of the VMS high availability name hosted on the ADC server. You use this FQDN when configuring the messaging service in Versa Director, as described in Configure the Messaging Service, below.

To configure a DNS server:

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the left navigation bar. This is the organization in which you are deploying the VMS server.
   d. Select a device template the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Others > System > Domain Name Servers in the left menu bar. The main pane displays the configured DNS servers.
4. Click the Add icon or select a DNS server. In the Add/Edit Name Servers popup window, enter the following information about the customer's DNS server.



a. In the Routing Instance field, select the routing instance (here, ACME-CORP-LAN-VR). This is the LAN VR that connects to the customer's DNS server

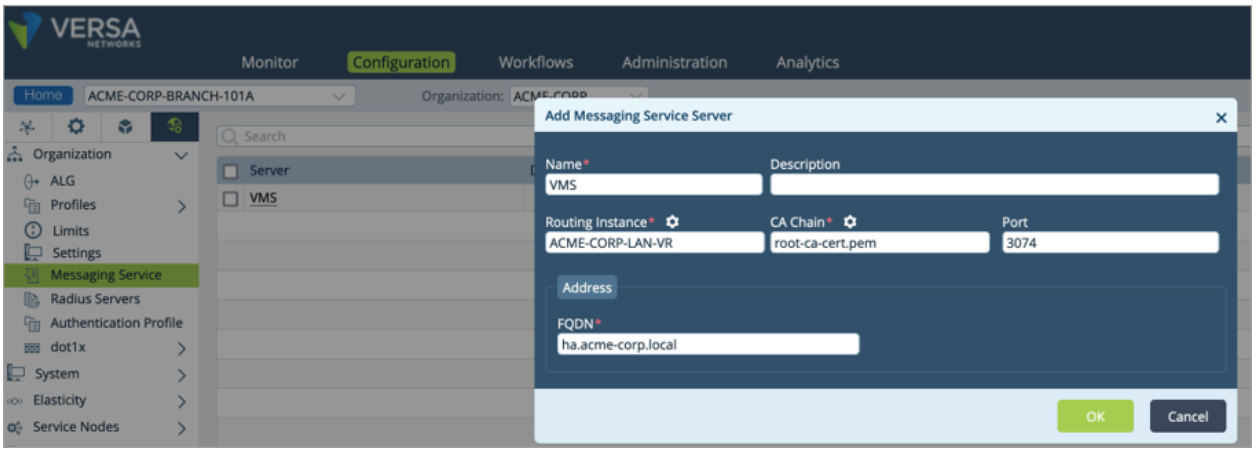
b. Select Source Network or Source Interface, as preferred. This example uses the source network (LAN_TRUST) that connects to the DNS server.

c. In the Name Servers table, click Add icon, and then enter the IP address (here,192.168.111.20) of the DNS server. For resilience, repeat this step to add more servers.

d. Click OK.

Configure the Messaging Service

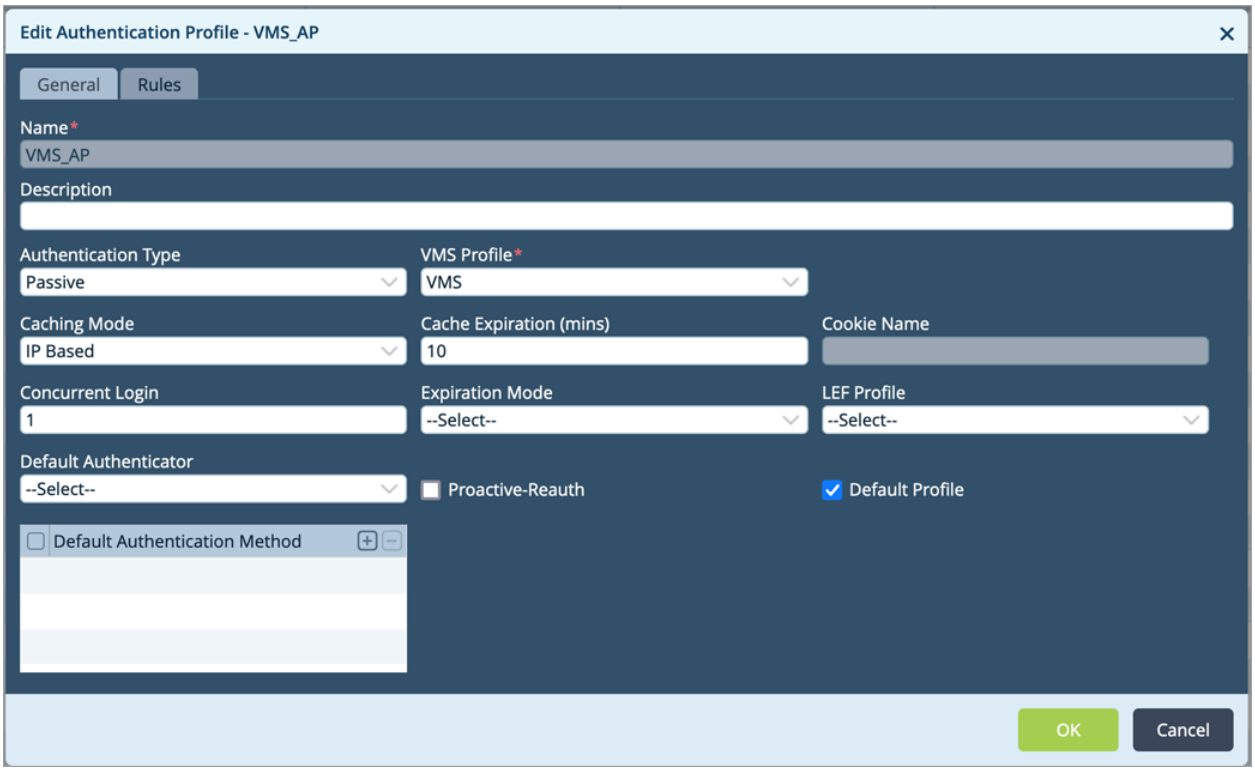
1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the left navigation bar. This is the organization in which you are deploying the VMS server.
   d. Select a device template in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Others > Organization > Messaging Service in the left menu bar.
4. Click the Add icon. In the Add Messaging Service Server popup window, enter the following information.



a. Enter a name for the messaging server (here, VMS).
b. Enter the routing instance (the organization's LAN VRF) to use to reach the VMS server or VMS load balancer. This example uses ACME-CORP-LAN-VR. This field is case-sensitive.
c. Enter the name of the CA Chain you uploaded in Upload the CA Certificate, above. This field is case-sensitive.
d. Enter 3074 (the default) as the port number.
e. Enter the FQDN associated with the VIP of the load balancer (here, ha.acme-corp.local)
f. Click OK.

Configure a Passive Authentication Profile

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the left navigation bar. This is the organization in which you are deploying the VMS server.
   d. Select a device template in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Object and Connectors > Connectors > Users/Groups > Authentication > Profiles in the left menu bar.
4. Click the Add icon or select an existing authentication profile. In the Add/Edit Authentication Profile popup window, enter the following information.



a. Enter a name for the authentication profile (here, VMS_AP)
b. In the Authentication Type field, select Passive.
c. In the VMS Profile field, select the messaging server you configured in Configure the Messaging Service, above.
d. Click OK.

Configure an LDAP Server Profile and a User and User Group Profile

To configure firewall or SD-WAN policies-based usernames or user groups, you need to configure an LDAP server profile and a user and user group profile, as described in this section. For resilience, you typically configure these profiles on the two CPEs that are closest to the Active Directory service.

As mentioned in Best Practices, above, if you are deploying VMS only to populate end usernames in Analytics, you do not need not perform these procedures, and you can skip this section.

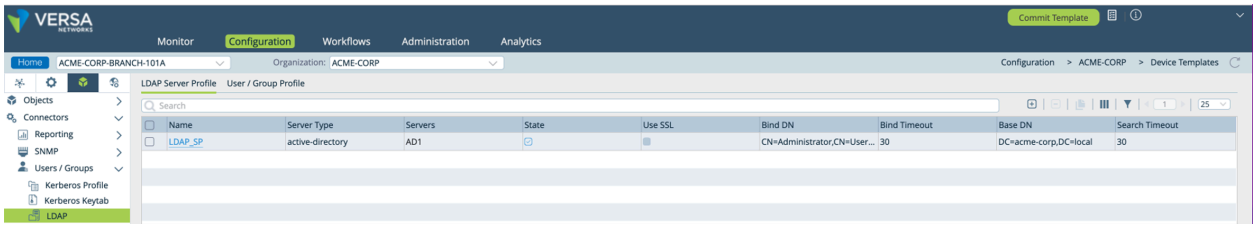
Note that the appliance proxy setting allows Versa Director to view the users and groups on the customer's Active Directory. In effect, the selected CPEs act as proxies between Versa Director and the Active Directory server. This functionality is required so that a Director administrator can build policies, such as firewall or SD-WAN, because the proxy allows the administrator to display or select Active Directory users or groups in Versa Director.

To configure an LDAP server for Active Directory authentication:

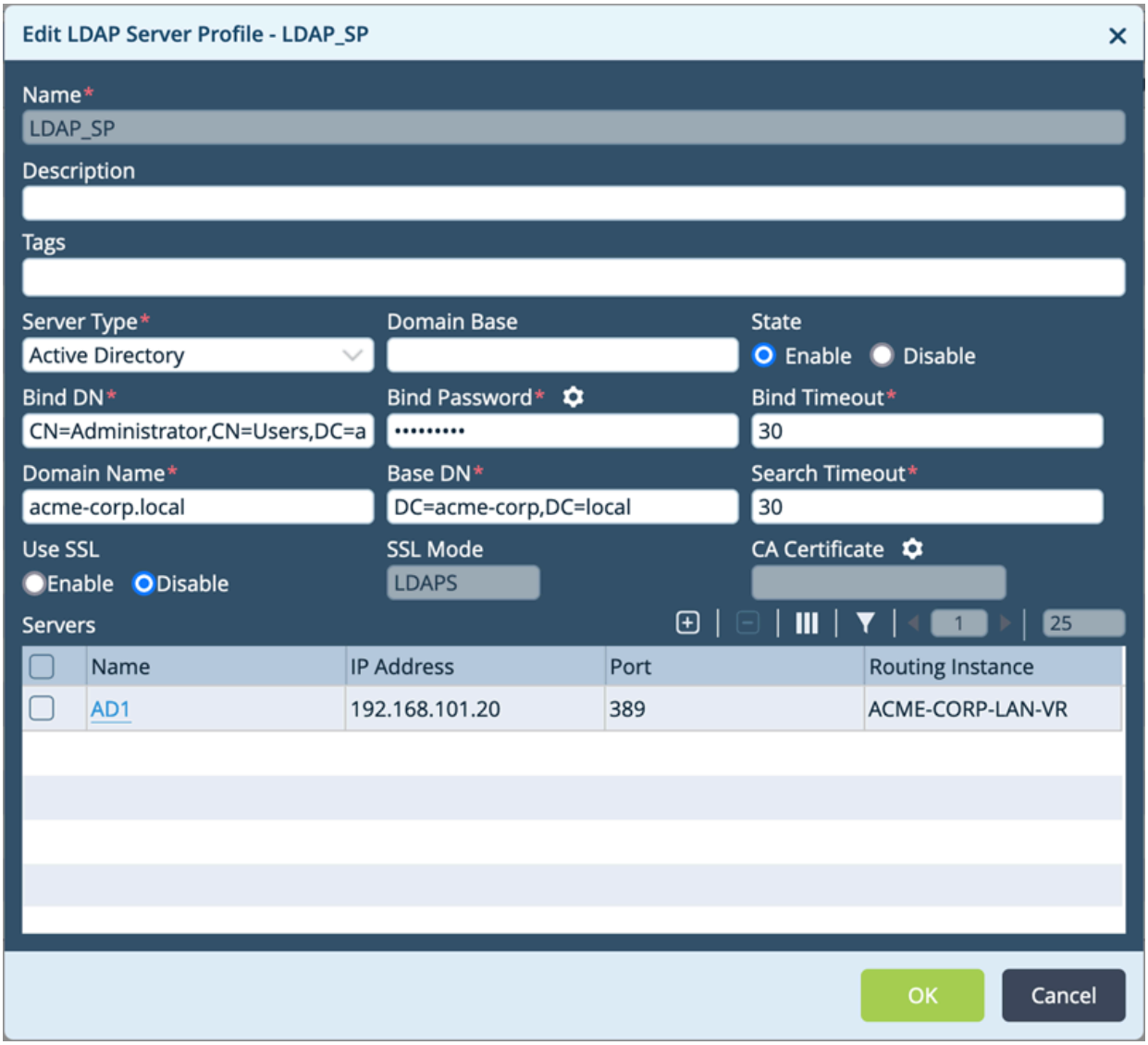
1. In Director view:

a. Select the Configuration tab in the top menu bar.
b. Select Templates > Device Templates.
c. Based on the recommendation to configure the two secure SD-WAN CPEs closest to the LDAP server, select the device template for the first Secure SD-WAN CPE. The view changes to Appliance view.

2. Select the Configuration tab in the top menu bar.
3. Select Object and Connectors > Connectors > Users/Groups > LDAP in the left menu bar.
4. Select the LDAP Server Profile tab.

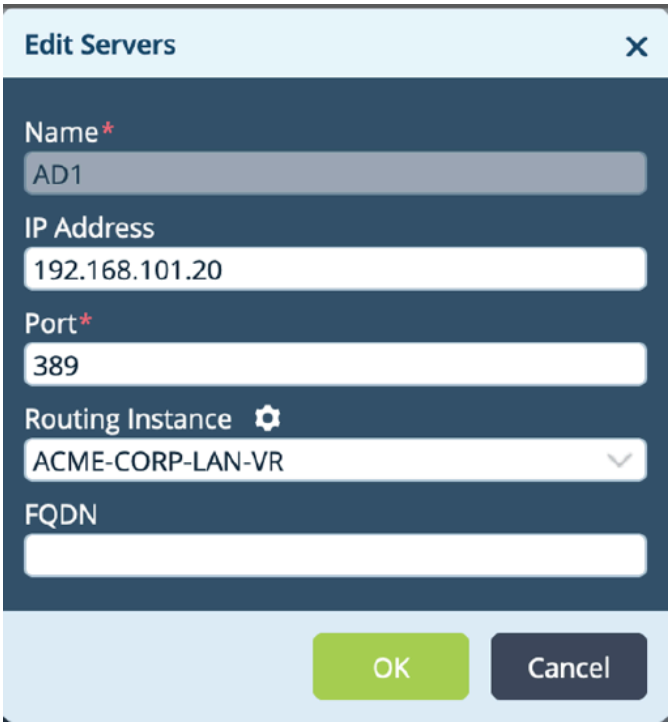


5. Click the Add icon or select an existing LDAP server profile. In the Add/Edit LDAP Server Profile popup window, enter the following information.



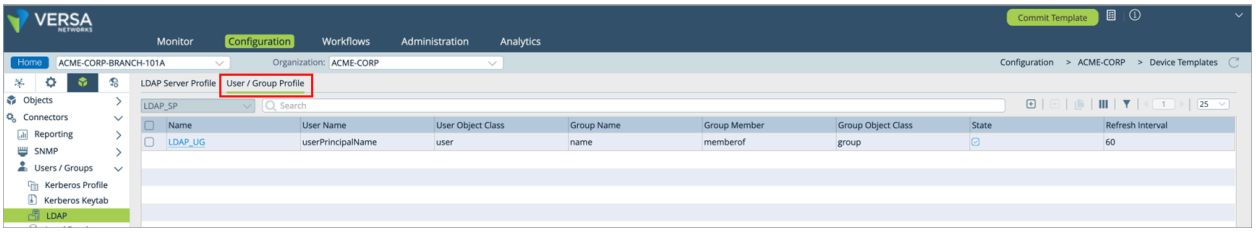
a. Enter a name for the for the LDAP server profile (here, LDAP_SP).
b. In the Server Type field, select Active Directory as the location of the LDAP server
c. In the Bind DN field, enter the bind DN (here, CN=Administrator,CN=Users,DC=acme-corp,DC=local). For more information about determining the Active Directory bind DN, see Determine the Active Directory Bind DN and Base DN, below.
d. In the Bind Password field, enter the bind password for the user defined in the DN above.
e. In the Domain Name field, enter the name of the domain in which the LDAP server resides (here, acme-corp.local).
f. In the Base DN field, enter the base DN of the LDAP directory location (here, DC=acme-corp,DC=local). For more information about determining the Active Directory base DN, see Determine the Active Directory Bind DN and Base DN, below.

6. In the Servers table, click the Add icon or select an existing LDAP server. In the Add/Edit Servers popup window, enter the following information.



a. Enter a name for the server (here, AD1).
b. Enter the IP address of the Active Directory server (here, 192.168.101.20)
c. Enter the port number of the listening port on the Active Directory server for Active Directory queries, which is usually, 389.
d. Select the Routing Instance to use to reach the Active Directory server. This is a customer LAN VR (here, ACME-CORP-LAN-VR).
e. Click OK.

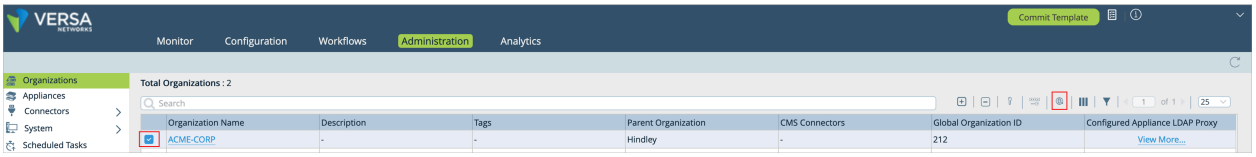
7. Click OK.
8. Repeat Steps 5 through 7 to add another Active Directory server.
9. In the LDAP screen, select the User/Group Profile tab to add a user and user group profile. Note that you can add a user and user group profile only if you add an LDAP server profile.



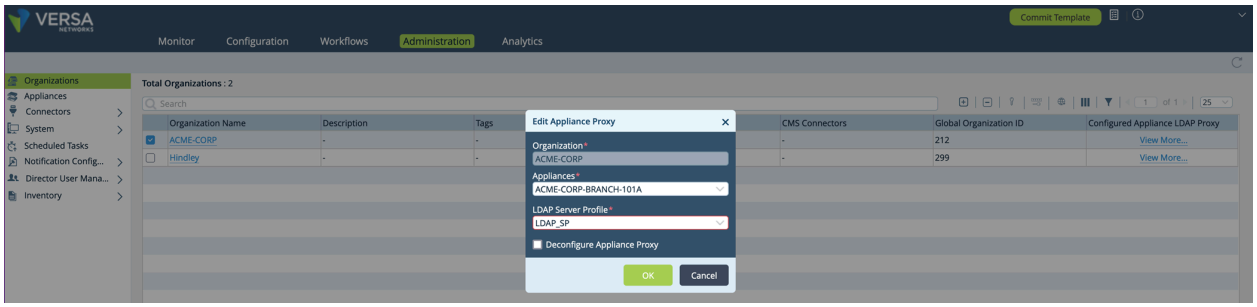
10. Click the Add icon, or select an existing LDAP server profile. In the Add/Edit LDAP Server Profile popup window, enter the following information.

a. Enter a name for the user and user group profile (here, LDAP_UG).
b. Enter the group object class (here, group).
c. Enter the group name (here, name).
d. Enter the group member (here, memberof).
e. Enter the user object class (here, user).
f. Enter the format of the username in the User Name field (here, userPrincipalName).
g. Click Ok.

11. Select the Administration tab in the top menu.
12. Select Organizations in the left menu.
13. Select the organization that you configured for the VMS service (here, ACME-CORP).



14. Click the Appliance Proxy icon. In the Edit Appliance Proxy popup window, enter the following information.



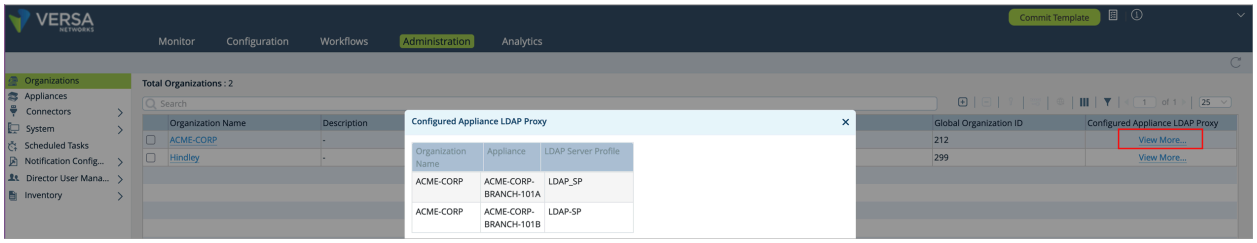
a. In the Appliance field, select one of the secure SD-WAN CPEs that is closest to the customer's Active Directory server (here, ACME-CORP-BRANCH-101A).

b. If there are multiple LDAP server profiles, select the appropriate LDAP server profile in the LDAP Server Profile field. If there is only one LDAP server profile on the secure SD-WAN CPE, the LDAP Server Profile field autopopulates with that profile. Here, the field is autopopulated with LDAP_SP, which we created in Step 5.

c. Select OK.

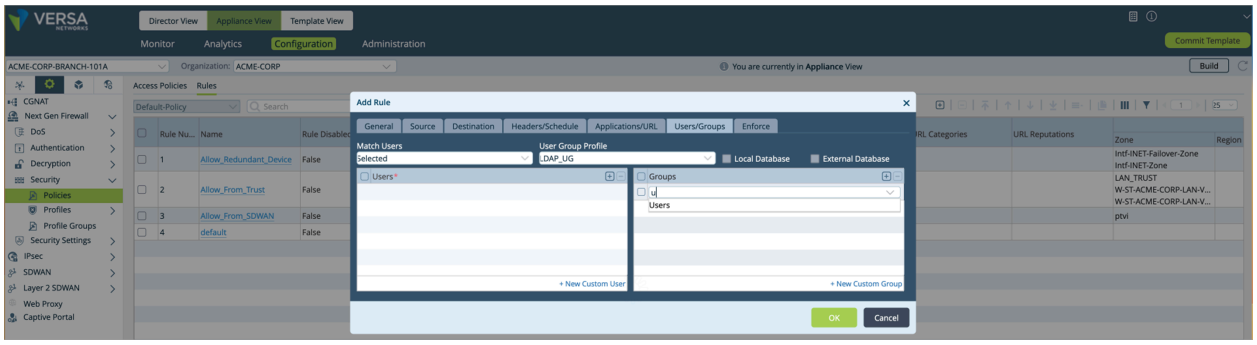
d. Repeat Steps 14a through 14c for the second secure SD-WAN CPE.

15. To view the LDAP proxy settings, in the Organizations main pane, click View More in the Configure Appliance LDAP Proxy column. The following screenshot shows the two secure SD-WAN CPEs (ACME-CORP-BRANCH-101A and ACME-CORP-BRANCH-101B) configured as proxies to interface with the LDAP server.



16. To apply the LDAP server profile configuration to the secure SD-WAN CPE, commit the template. For more information, see Commit Template Modifications.

You can now create policies that refer to the profiles in their match conditions. For example, you can configure a firewall policy whose match criteria match users or groups learned from LDAP, as shown in the following screenshot. In this example, in the Add Rules Users/Group tab, we set the Match User field to Selected, and we use the user group profile we created in the procedure above (LDAP_UG). When you type 'u' in the Groups search field, all groups that start with u display. Here, we configure the user group named Users.



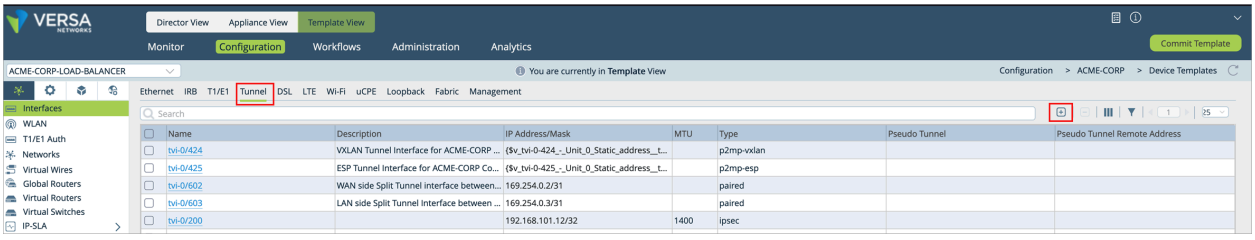
Configure an Application Delivery Controller

This section describes how to configure the application delivery controller (ADC) service on a VOS device.

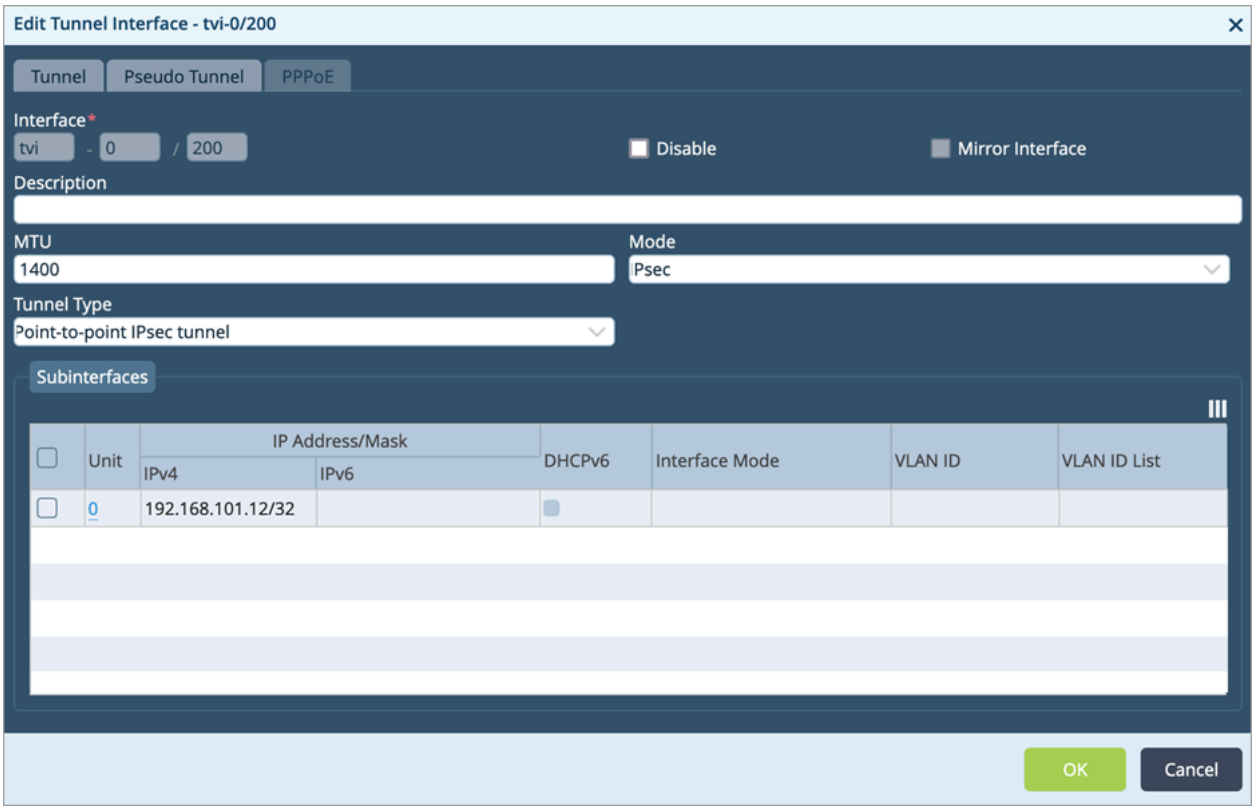
As discussed in Best Practices, above, you should not use the same VOS device for both the secure SD-WAN and ADC functions. Instead, use separate devices to perform these two functions. Although the same VOS device can support both functions, a VOS device running both secure SD-WAN and ADC cannot connect to the VMS service.

Configure a Virtual Interface

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates.
   c. Select the device template of the VOS device to perform the ADC function.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Interfaces in the left menu bar.
4. Select the Tunnel tab in the horizontal menu bar.



5. Click the Add icon, or select an existing tunnel interface. In Add/Edit Tunnel Interface popup window, enter the following information.

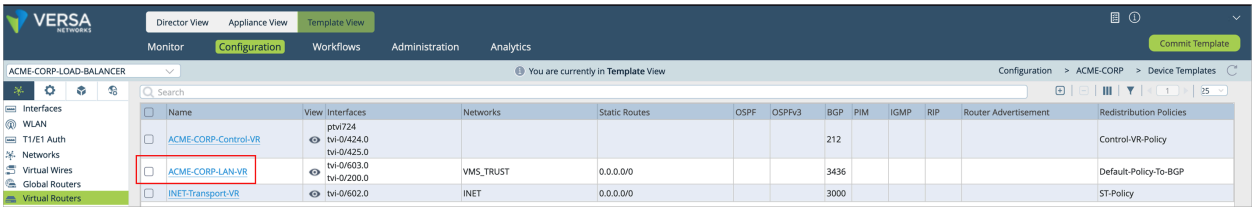


a. Enter an interface number and unit. In this example, we use 0/200.

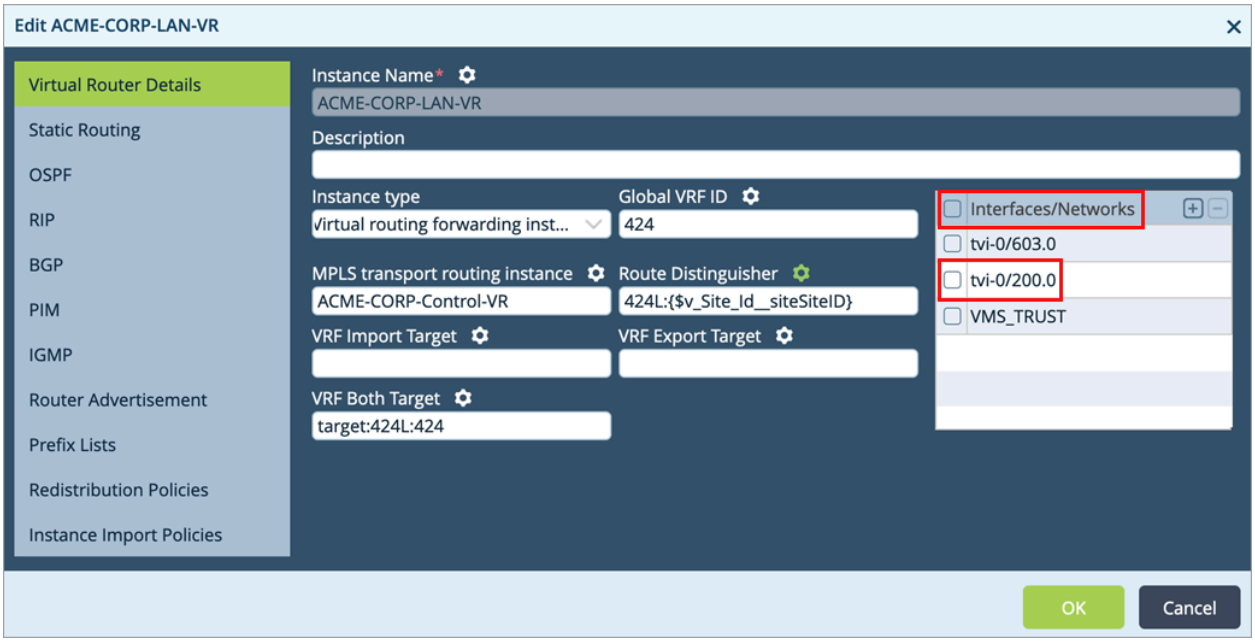
b. In the Subinterfaces table, click the unit, here, 0, and the enter the IP address of the virtual service. In this example, we use 192.168.101.12, which correlates with the FQDN ha.acme-corp.local.

c. Click OK.

6. Select Networking > Virtual Routers in the left menu bar.



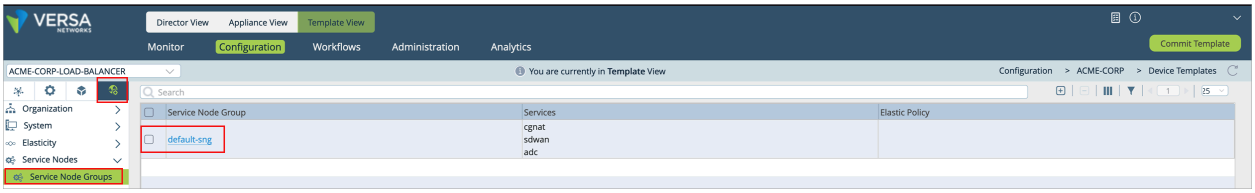
7. Select the LAN VR of the organization. In this example, we use ACME-CORP-LAN-VR. The Edit LAN-VR popup window displays.



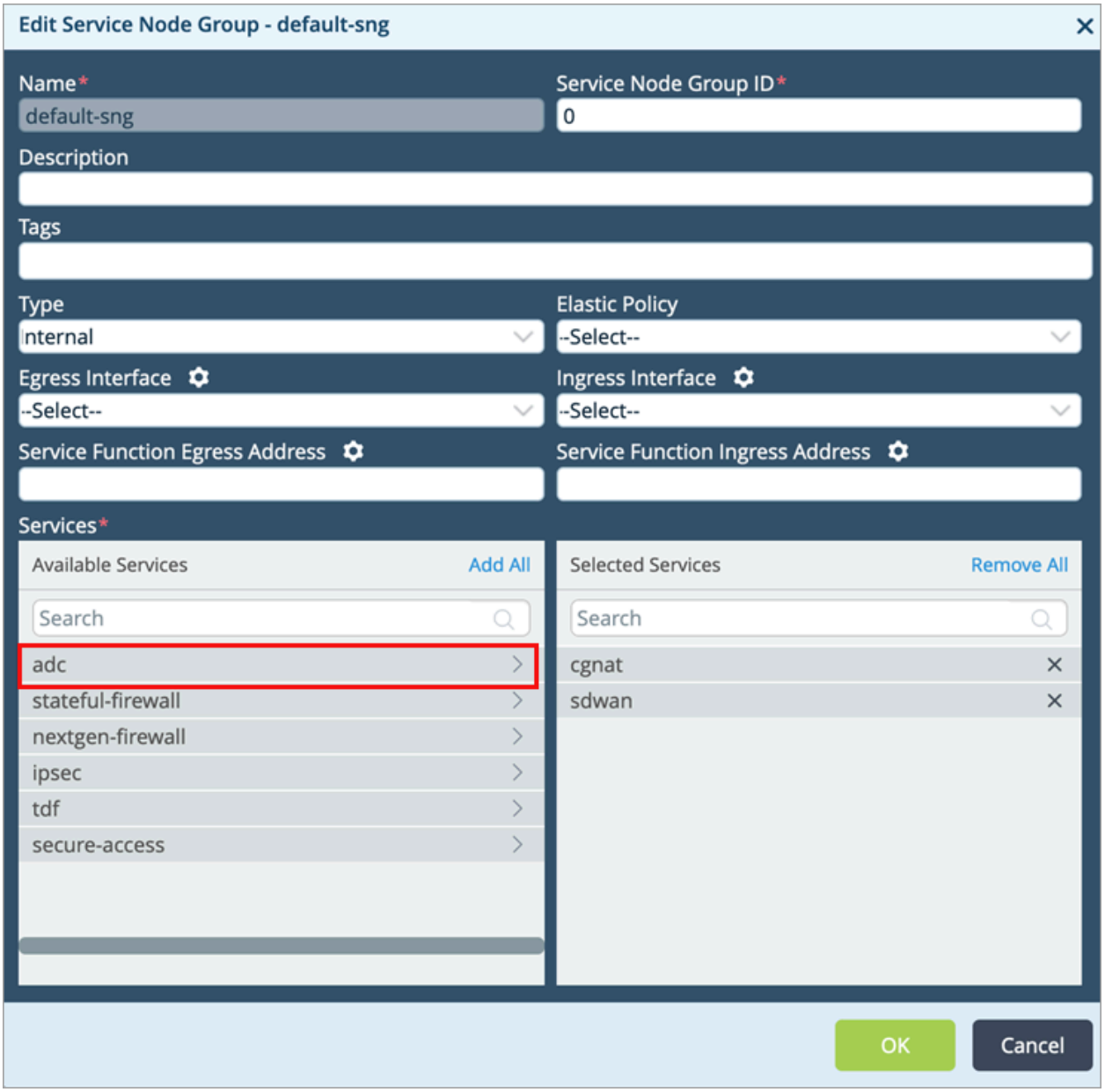
8. Select the Virtual Router Details tab.
9. In the Interfaces/Networks table, select the tunnel interface you added in Step 5 (here, tvi-0/200.0).
10. Click OK.

Add an ADC Service

1. Select the Configuration tab in the top menu bar.
2. Select Others > Service Nodes > Service Node Groups in the left menu bar.



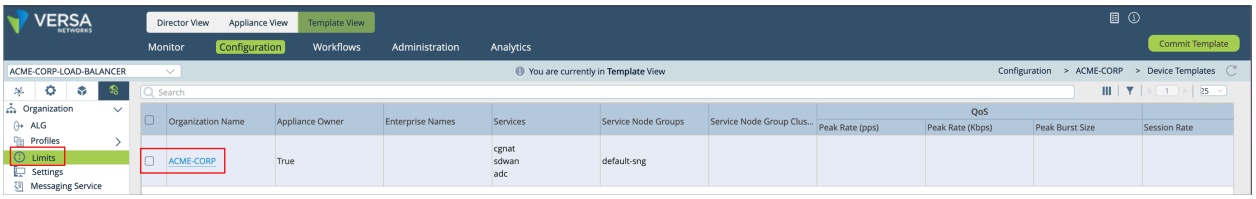
3. Select the service node group, here default-sng. The Edit Service Node Group popup window displays. Enter the following information.



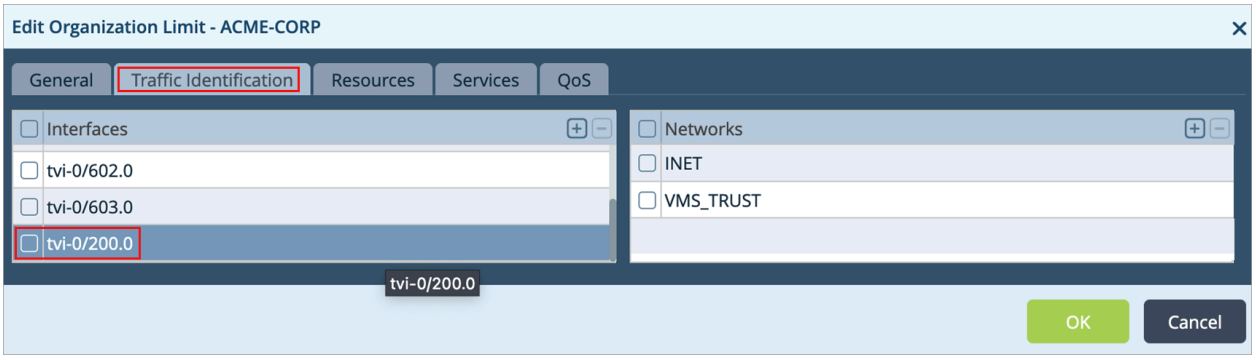
a. In the Services table, click ADC in the Available Services section to move it to Selected Services.

b. Click OK.

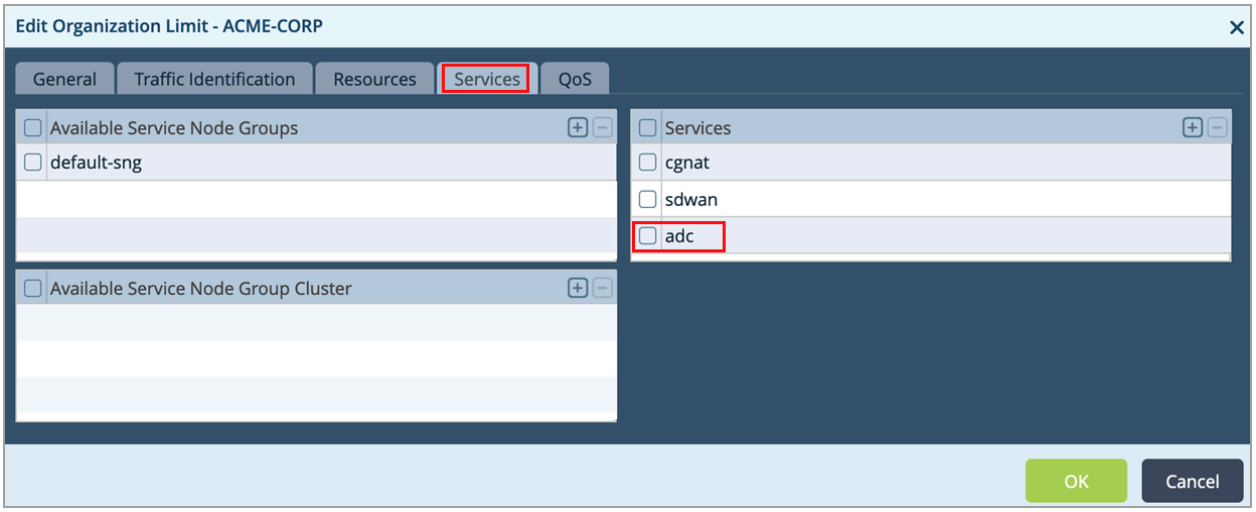
4. Select Others > Organization > Limits in the left menu bar.



5. Select the organization (here, ACME-CORP). The Edit Organization Limit popup window displays.



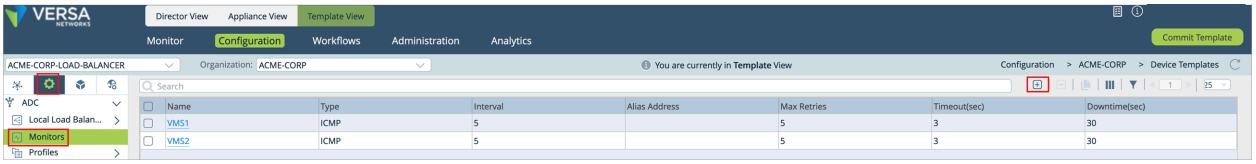
6. Select the Traffic Identification tab.
7. Select the interface you created in Step 5 of Configure a Virtual Interface, above, here, tvi-0/200.0.
8. Select the Services tab.



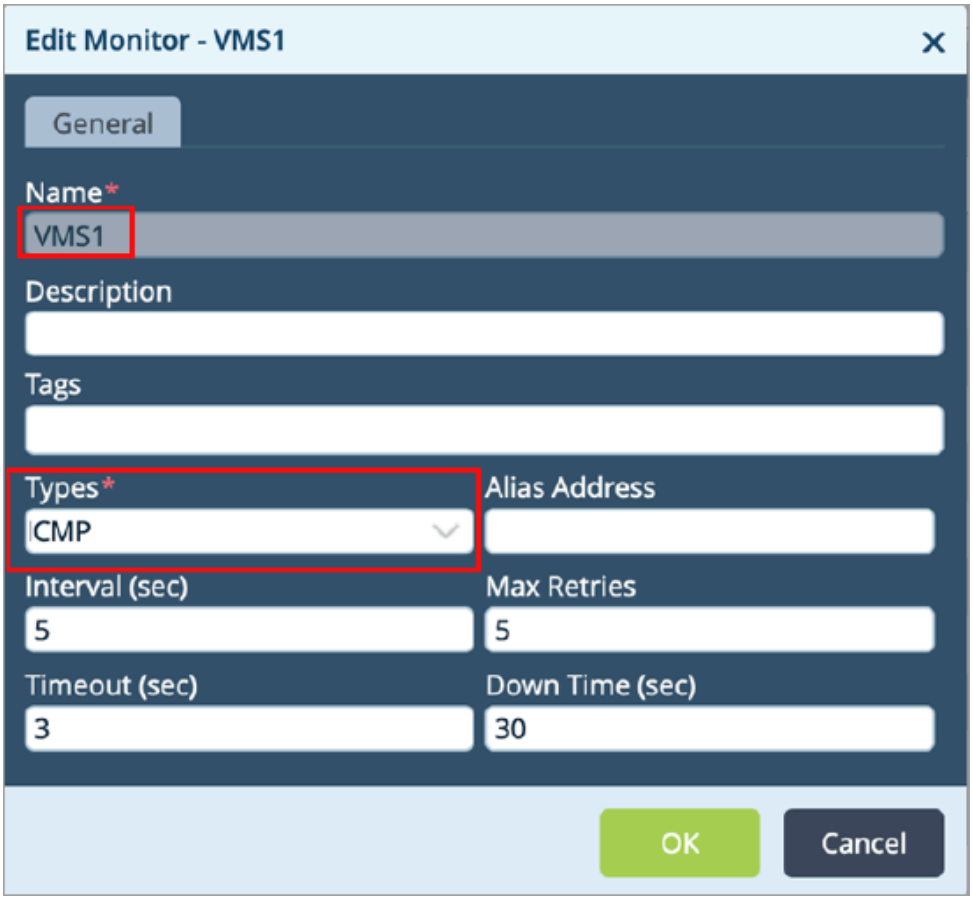
9. In the Services table, select ADC.
10. Click OK.

Configure the ADC Service

1. Select the Configuration tab in the top menu bar.
2. Select Services > ADC > Monitors in the left menu bar.

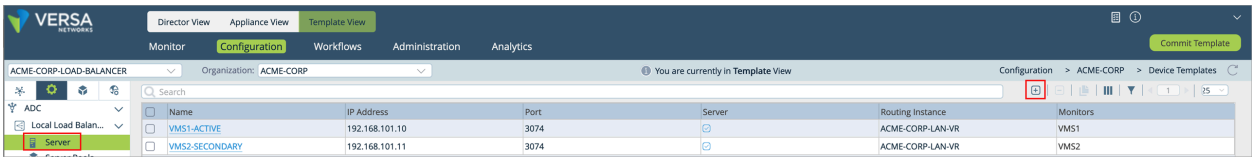


3. Click the Add icon. In the Add Monitor popup window, enter the following information. (The screenshot here shows Edit Monitor popup window.)

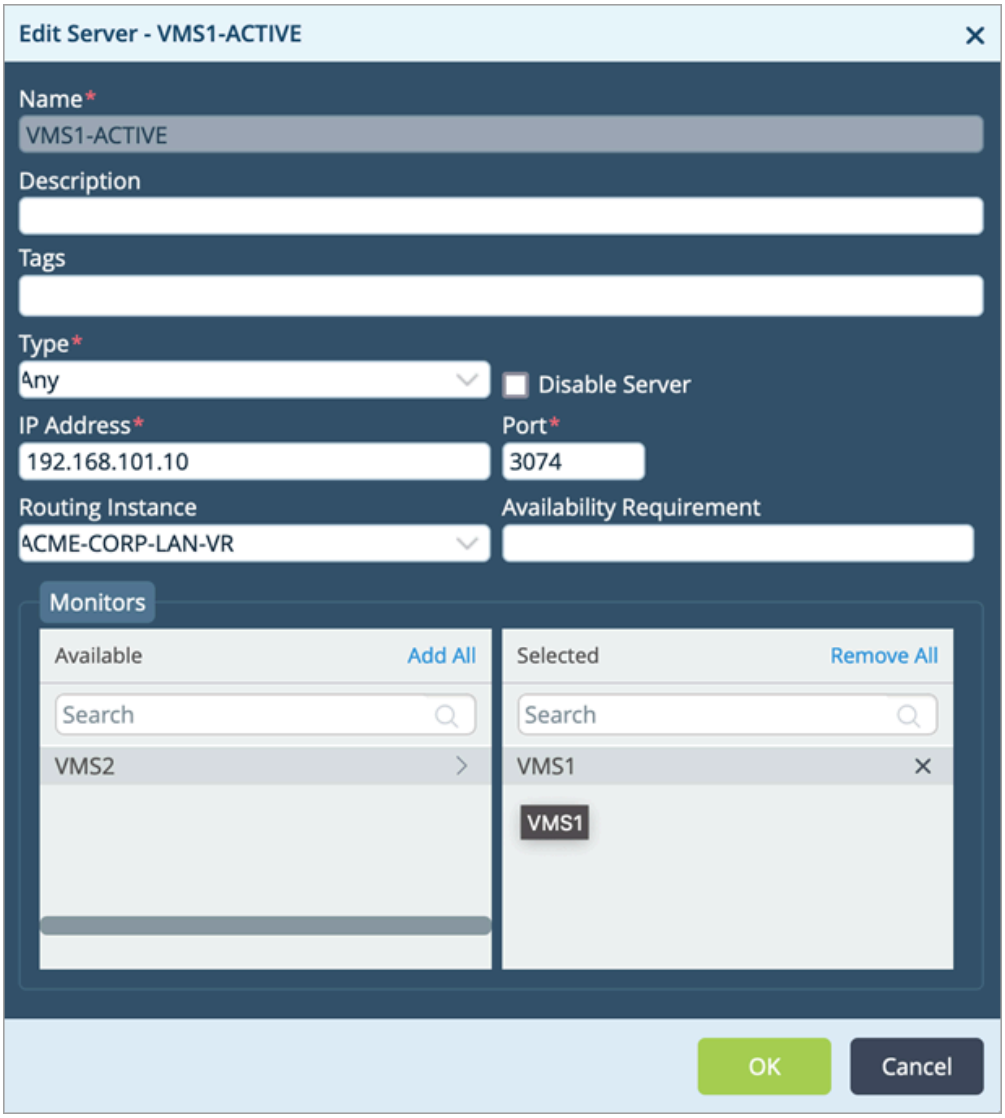


a. Enter the name of the monitor (in this example, we use VMS1).
b. In the Types field, select ICMP.
c. Click OK.
d. Repeat Steps 3a through 3c to create another monitor (here, VMS2).

4. Select Services > ADC > Local Load Balancers > Server in the left menu bar.

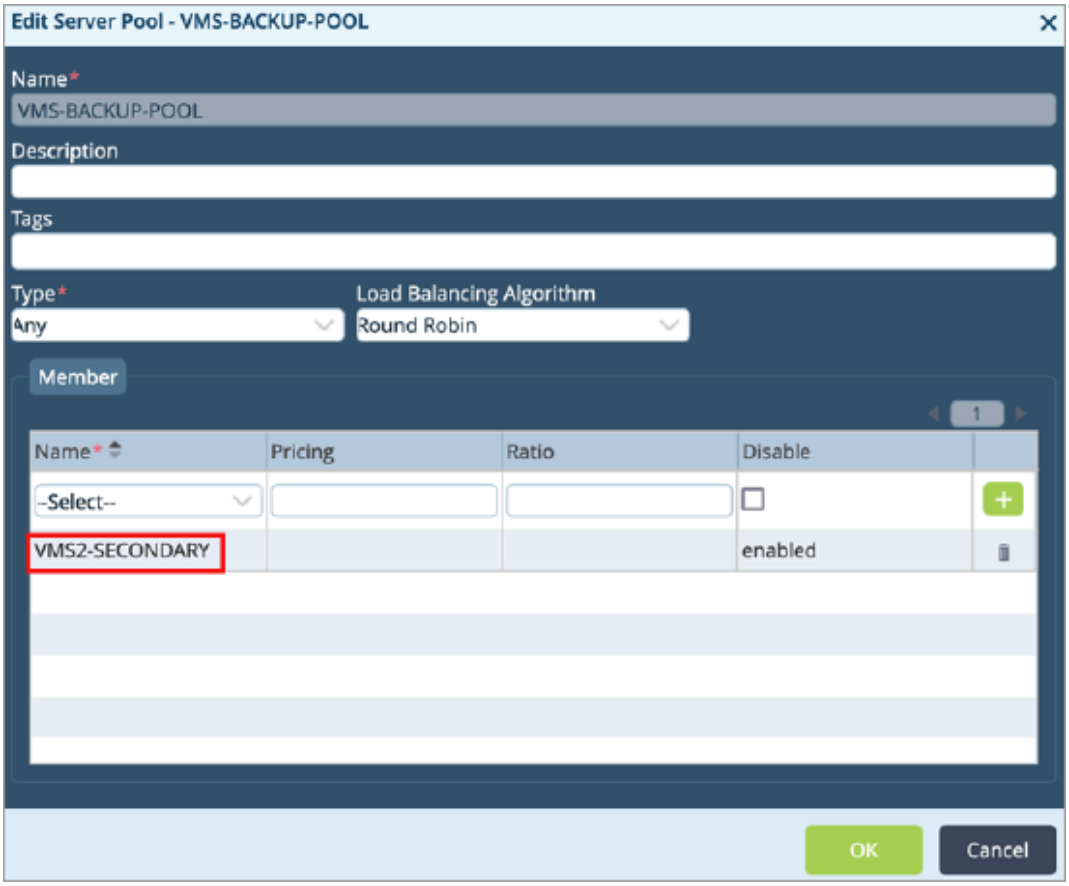


5. Click the Add icon. In the Add Server popup window, enter the following information. (The screenshot here shows the Edit Server popup window).



a. Enter a name for the monitor (here, VMS1-ACTIVE).
b. Enter the IP address of the primary VMS server (here, 192.168.101.10).
c. Enter port number 3074.
d. In the Monitors table, click on VMS1 under Available to move it to Selected.
e. Click OK.

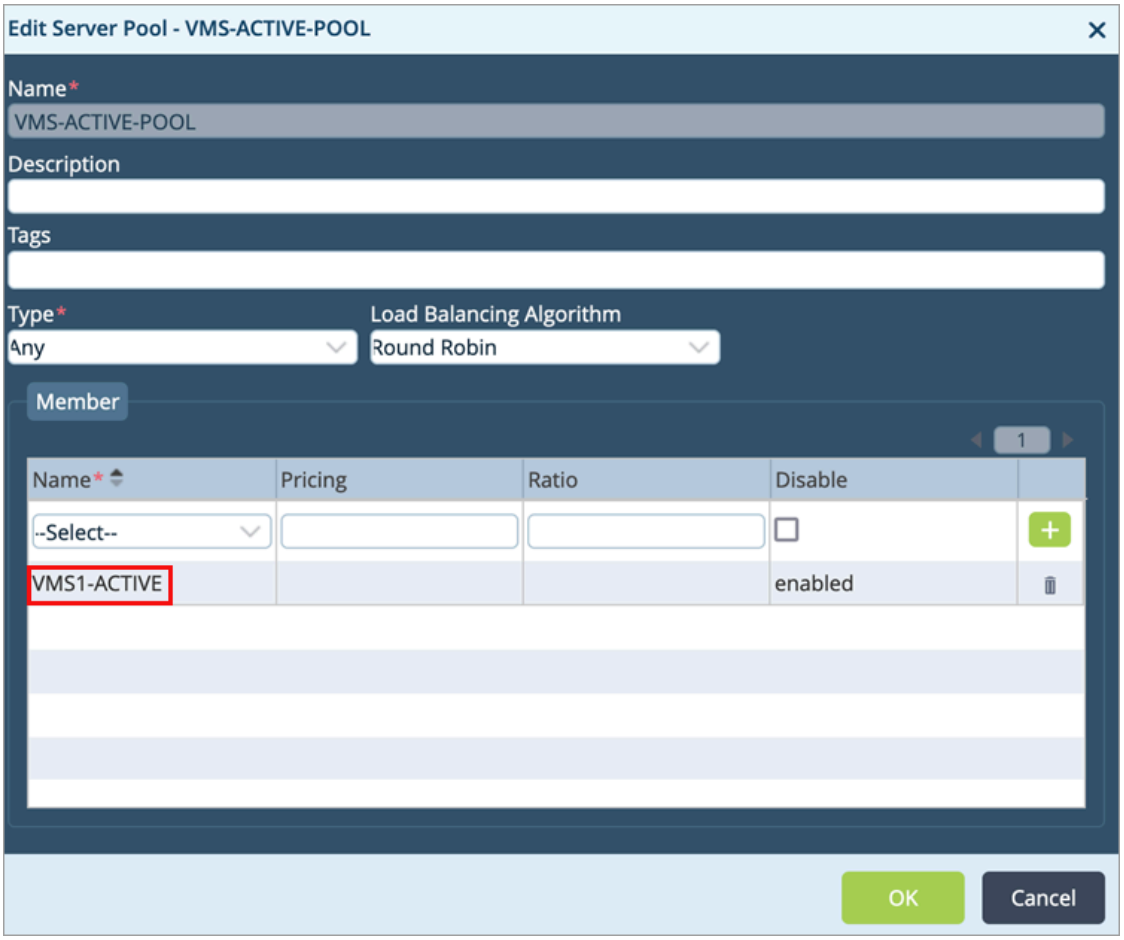
6. To add a backup VMS server, click the ⊞ Add icon again. In the Add Server popup window, enter the following information.



a. Enter a name for the monitor (here, VMS2-SECONDARY).
b. Enter the IP address of the primary VMS server (here, 192.168.101.11).
c. Enter port number 3074.
d. In the Monitor table, click on VMS2 under Available to move it to Selected.
e. Click OK.

7. Select Services > ADC > Local Load Balancers > Server Pools in the left menu bar.

8. Click the Add icon. In the Add Server Pool popup window enter the following information.

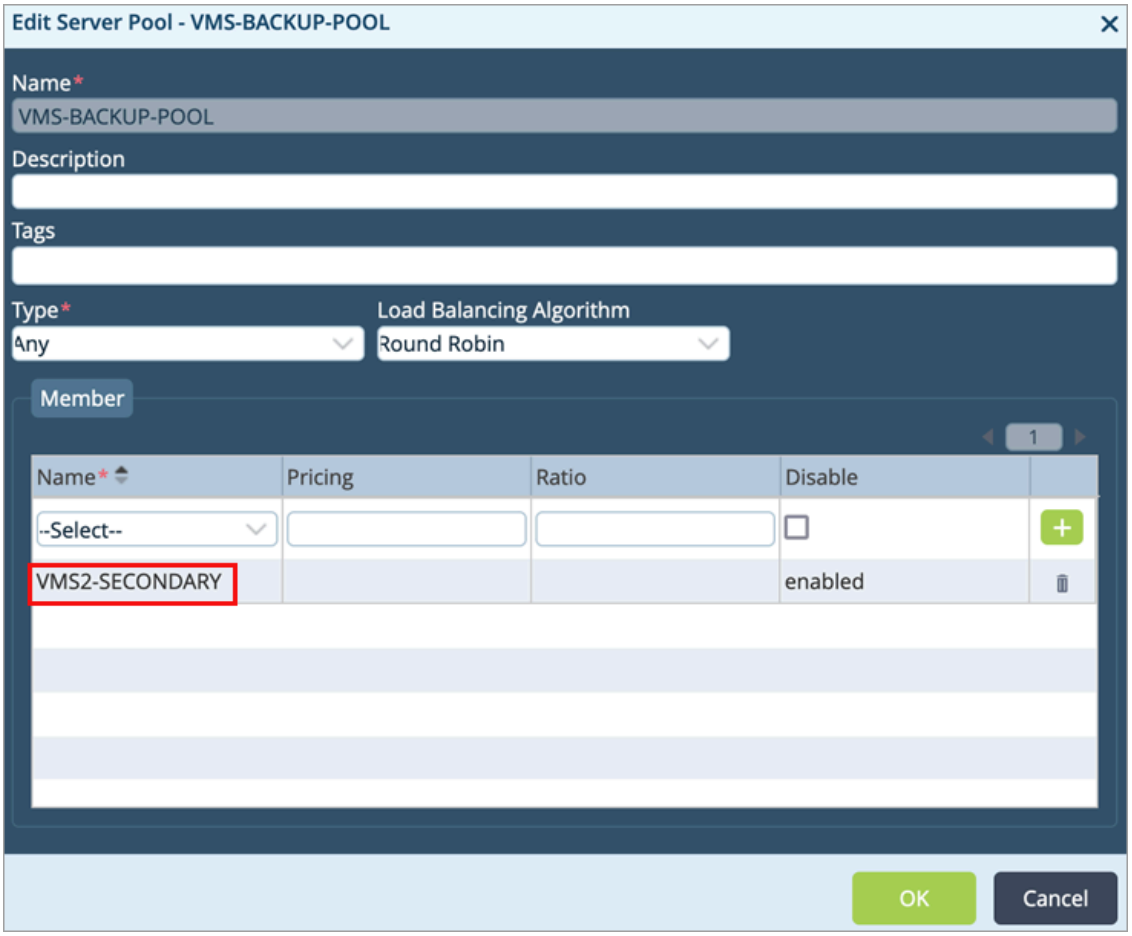


a. Enter a name for the server pool (here, VMS-ACTIVE-POOL), which we added in Step 5.

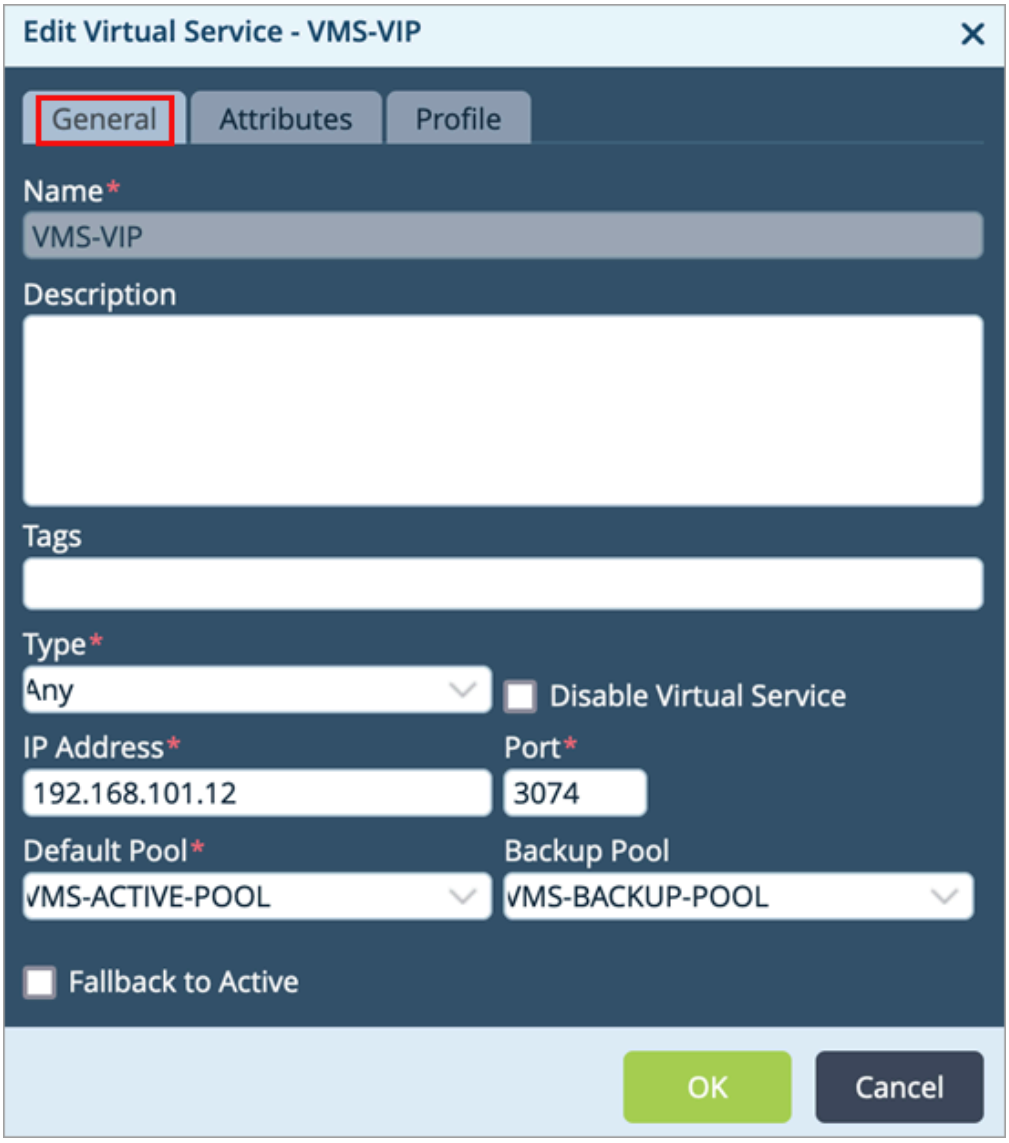
b. In the Member table, select the VMS server, VMS1-ACTIVE, under name and click the Add icon to add.

c. Click OK.

9. Repeat Steps 8a through 8c to add a backup server pool. In this example, the name of the backup pool VMS-BACKUP-POOL, and we select VMS2-SECONDARY, which we added in Step 6.



10. Select Services > ADC > Local Load Balancers > Server Pools in the left menu bar.
11. Click the ⊞ Add icon. The Add Virtual Service popup window displays.
12. Select the General tab, and enter the following information.



a. Enter a name for the virtual service (here, VMS-VIP).

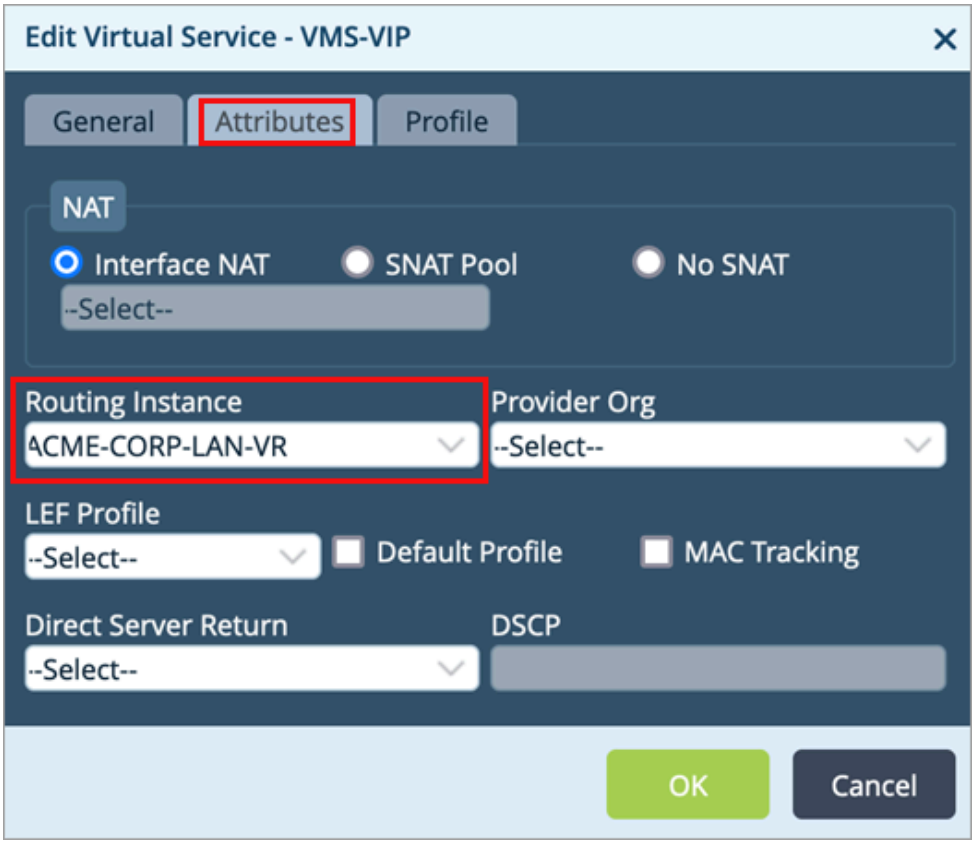
b. Enter the IP address, which is same as the tunnel interface we created in Step 5 of Configure a Virtual Interface, above (192.168.101.12). This address is also the IP address of the FQDN ha.acme-corp.local.

c. Enter 3074 as the port number.

d. In the Default Pool field, select VMS-ACTIVE-POOL, which we added in Step 8.

e. In the Backup Pool field, select VMS-BACKUP-POOL, which we added in Step 9.

13. Select the Attributes tab, and enter the following information.



a. In the Routing Instance field select ACME-CORP-LAN-VR.

b. Click OK.

14. To apply the ADC configuration to the VOS device, commit the template.

Verify the Passive Authentication Deployment

The following sections describe how to verify the passive authentication deployment.

Verify VMS

To check the status of VMS, issue the **vsh status** CLI command. Verify that all the pods are in the Running state. For example:

```
==========================================================================================
Versa Package Info: versa-msgservice-20221118-043012-873fa6b-21.2.2
==========================================================================================
Info: SYSTEM-SERVICES-STATUS
[?11


kubelet:active (2327)
docker:active (973)
```

```
================================================================================================
PODS-STATUS
NAME                                READY   STATUS    RESTARTS   AGE
concentrator-5fdf6cfcb8-tf85s       1/1     Running   9          2d20h
message-server-7b6db77b94-g8s1j     1/1     Running   9          2d20h
nginx-56799c4fd6-frjks              1/1     Running   9          2d20h
pkg-builder-bbdf5c558-obvq6         1/1     Running   9          2d20h
redis-uipnap-687c77bd74-k2gg9       1/1     Running   9          2d19h
uipmap-bd565f987-s7ddn              1/1     Running   17         2d19h
vxdev-764d8cc4b9-d5Ltf              1/1     Running   9          2d20h

================================================================================================

SERVICES-STATUS
NAME             TYPE           CLUSTER-IP       EXTERNAL-IP          PORT(S)                    AGE
concentrator     ClusterIP      10.111.88.249    192.168.101.10       3092/7CP                   2d21h
kubernetes       ClusterIP      10.96.0.1        <none>               443/TCP                    2d21h
message-server   ClusterIP      10.106.29.188    192.168.101.10       3074/TCP,3101/TCP,3102/TCP
2d21h
nginx            ClusterIP      10.103.222.79    192.168.101.10       443/TCP                    2d21h
redis-uipmap     ClusterIP      10.96.178.11     <none>               6379/TCP                   2d19h
uipmap           ClusterIP      10.106.247.136   <none                7000/TCP                   2d21h
vxdev            ClusterIP      10.107.136.113   <none>               8080/TCP                   2d21h

================================================================================================
```

To view active directory user login and logout details in real time, issue the following CLI commands. Note that using the **tail** command on the uipmap.log file displays the events sent by Active Directory to the WMI agent and then forwarded to VMS. The user events displayed in this log indicate that connectivity and credentials between these components are correct.

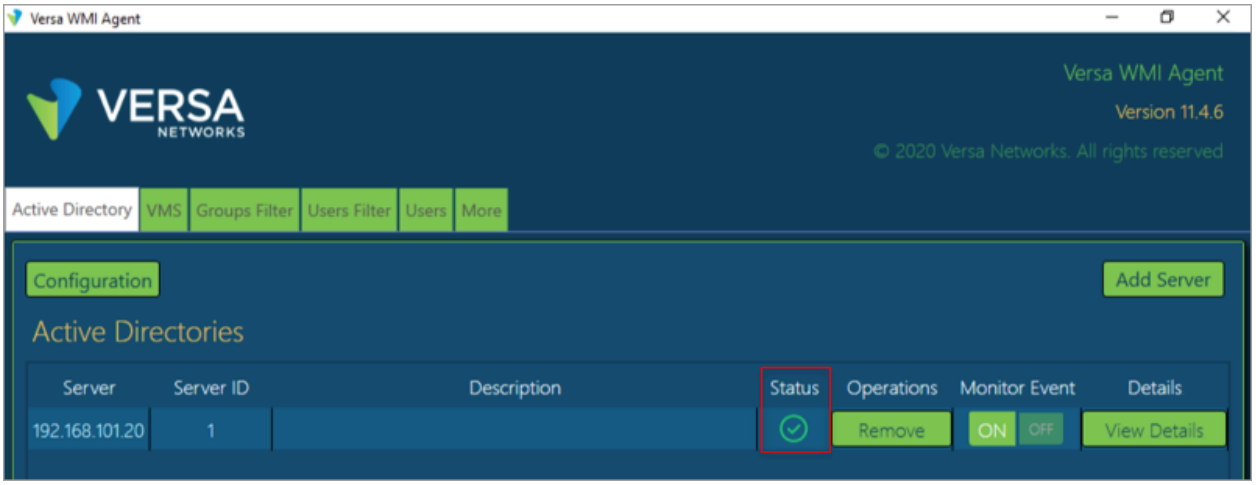
```
[admin@vms2: ~] $ sudo su
[sudo] password for admin:
root@vms2:/home/admin#
root@vms2:/var/log/versa/vms# cd /var/log/versa/vms/apps
root@vms2:/var/log/versa/vms/apps# tail -f uipmap.log
2022/08/24 12:45:33 0000219: API /uiprecord POST Userip: &{143 143 JRSS 213 { user1@versa.com
{DOMAIN : versa.com}}
{{"device-name": "DISA-MS-AD-Serv.versa.com", "type": "Regular", "address": "10.86.4.99",
"ports": "[]", "expires-at": {"text": "20220824134319", "timestamp": "1661348599"}} {}}}, SequenceNum: 143,
exists: true
2022/08/24 12:45:33 0000220: API /uiprecord POST Userip: &{144 89 JRSS 214 { user2@versa.com {DOMAIN
: versa.com}}
{{"device-name": "DISA-MS-AD-Serv.versa.com", "type": "Regular", "address": "10.86.4.99", "ports": "[]",
"expires-at": {"text": "20220824134556", "timestamp": "1661348756"}} {}}}, SequenceNum: 144, exists: true
```

Verify the WMI Agent

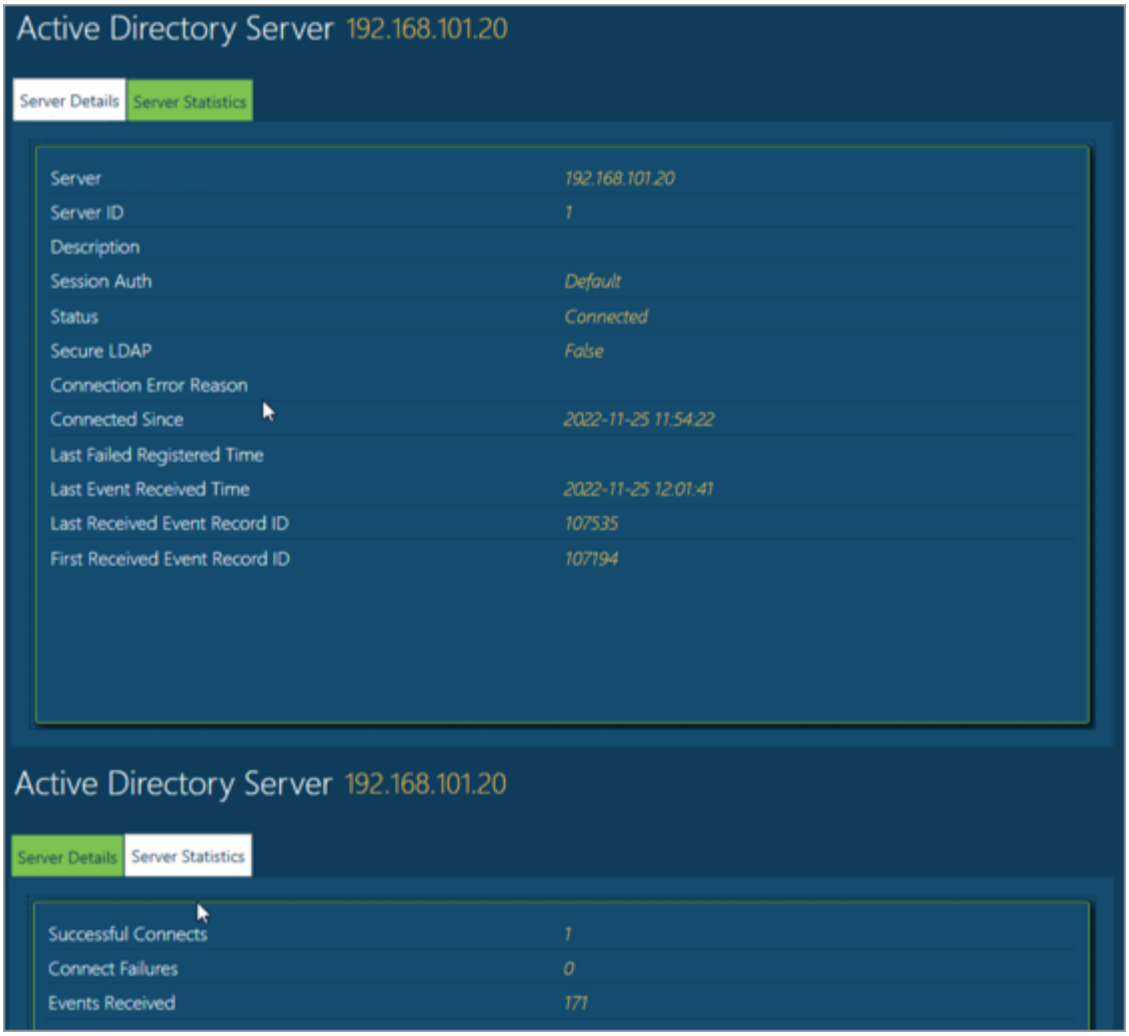
To view the status of the WMI agent and the Active Directory connection:

1. Start the WMI agent by double clicking the WMI agent shortcut. The Active Directory tab displays the status. In the

example here, the Active Directory server is 192.168.101.20. A status of green indicates that the Active Directory connection is active and that the credentials to connect to the server are correct.



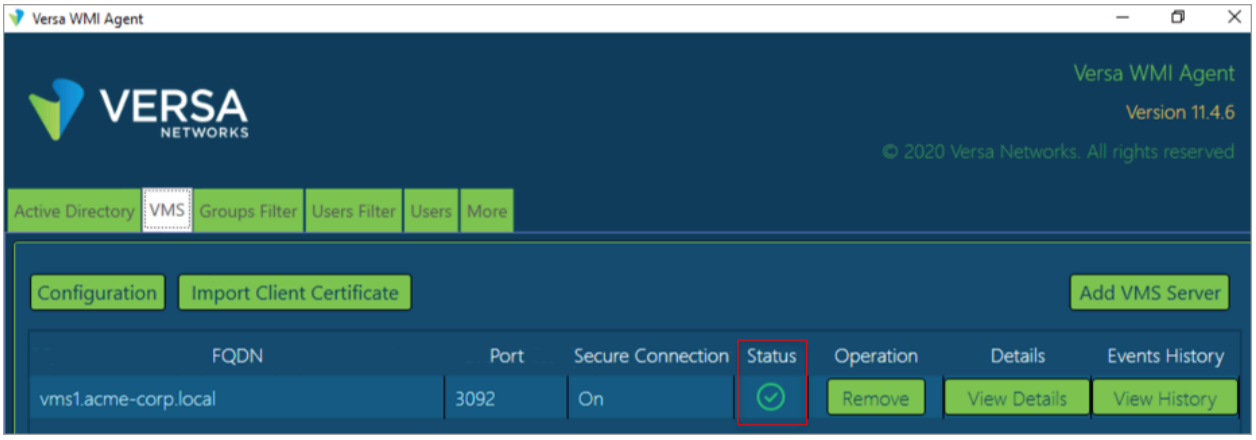
2. To view more details about the Active Directory server, click View Details. The Server Details tab displays.



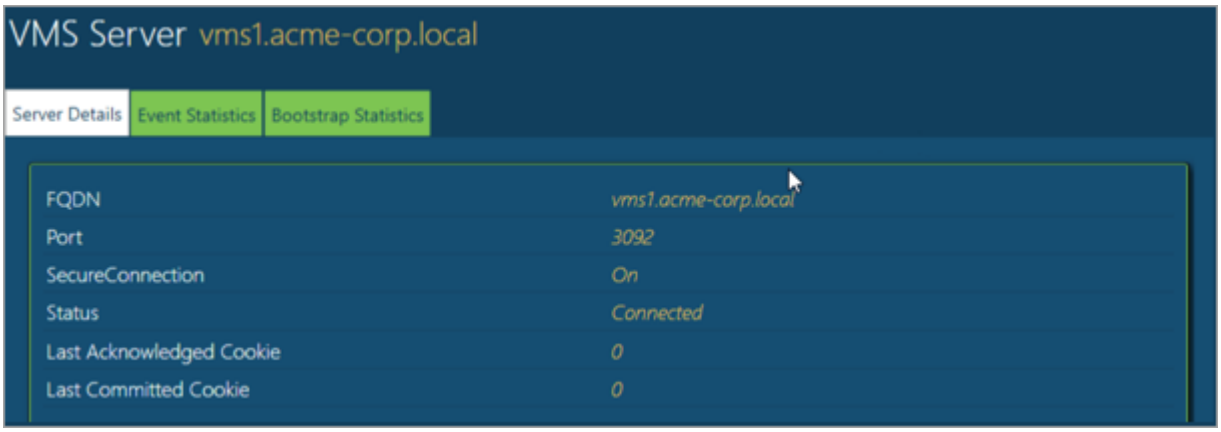
3. To view statistics, select the Server Statistics tab.

To view the status of the VMS server connection:

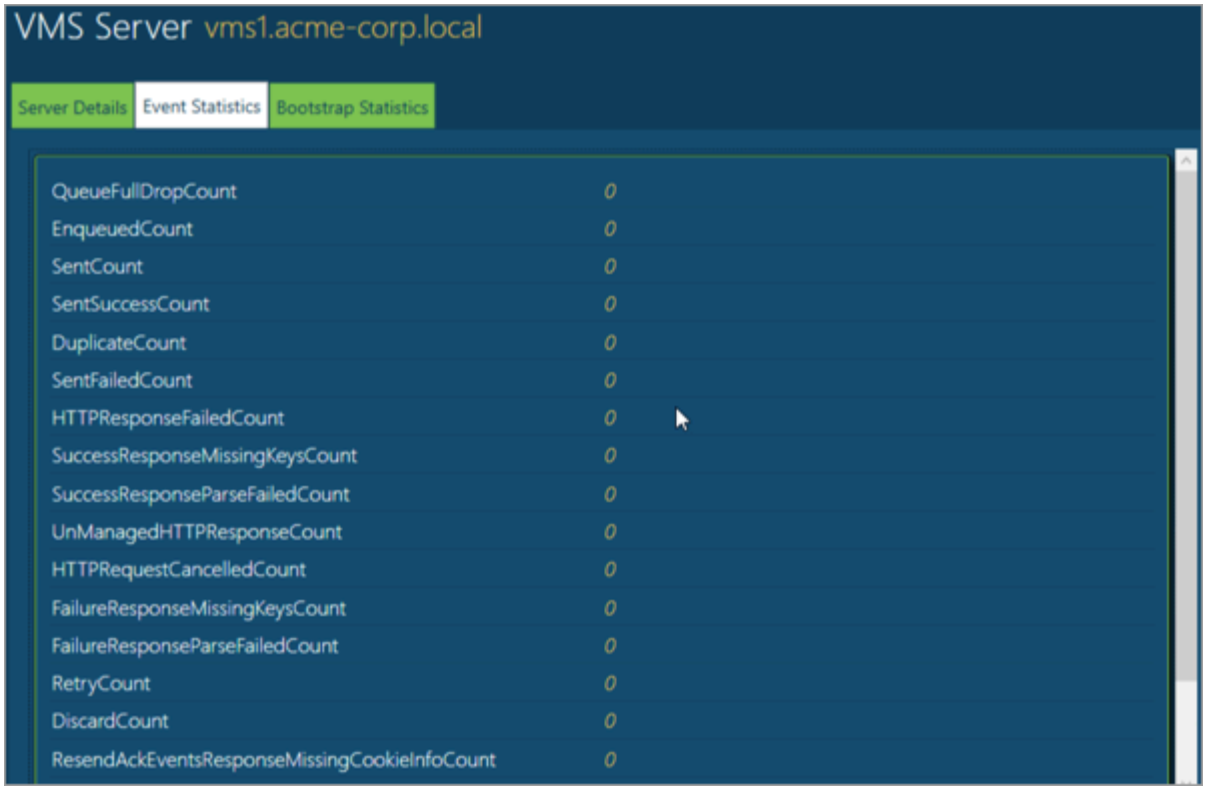
1. In the Versa WMI Agent main window, select the VMS tab. In the example here, the VMS server is vms1.acme-corp.local. A status of green indicates that the Active Directory connection is active and that the credentials to connect to the server are correct.



2. If the status is red:
   a. Ping the FQDN name of each VMS server from the WMI agent device.
   b. If the name does not resolve to the correct IP address of each server, check whether the WMI agent is resolving DNS queries to the DNS server or servers that were configured with FQDN names of the VMS service.
   c. If the name resolves, but the ping fails, check the firewall rules between the WMI agent and VMS to ensure that traffic over TCP port 3092 is permitted.
3. To view more details about the VMS server, click View Details. The Server Details tab displays.



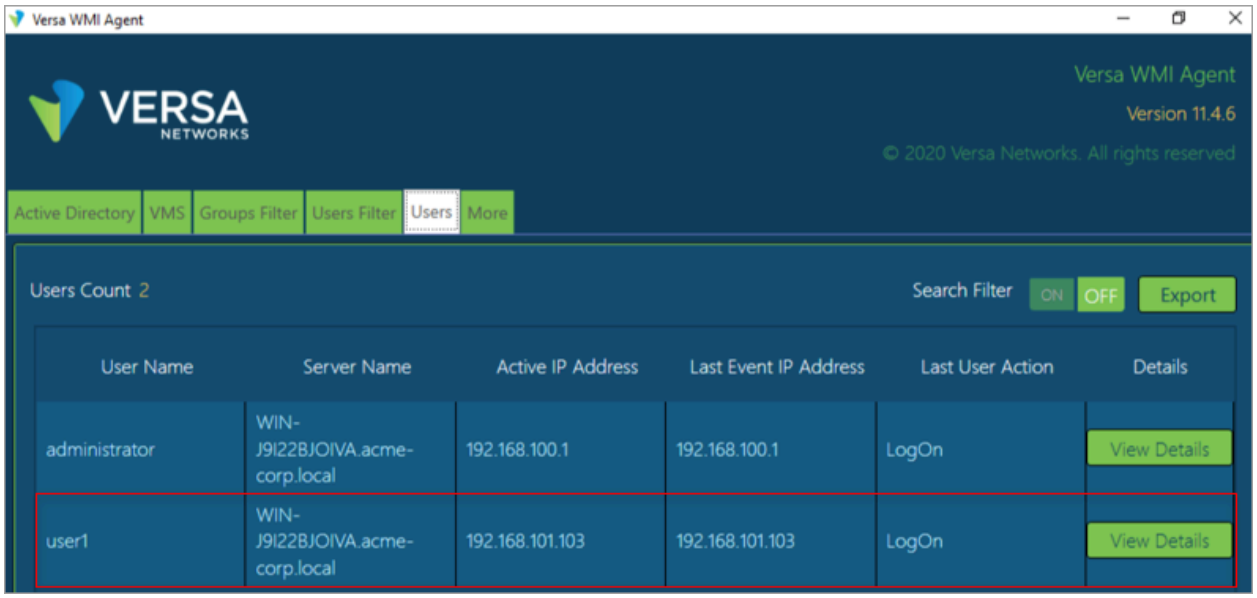
4. To view traffic events statistics, select the Event Statistics tab.



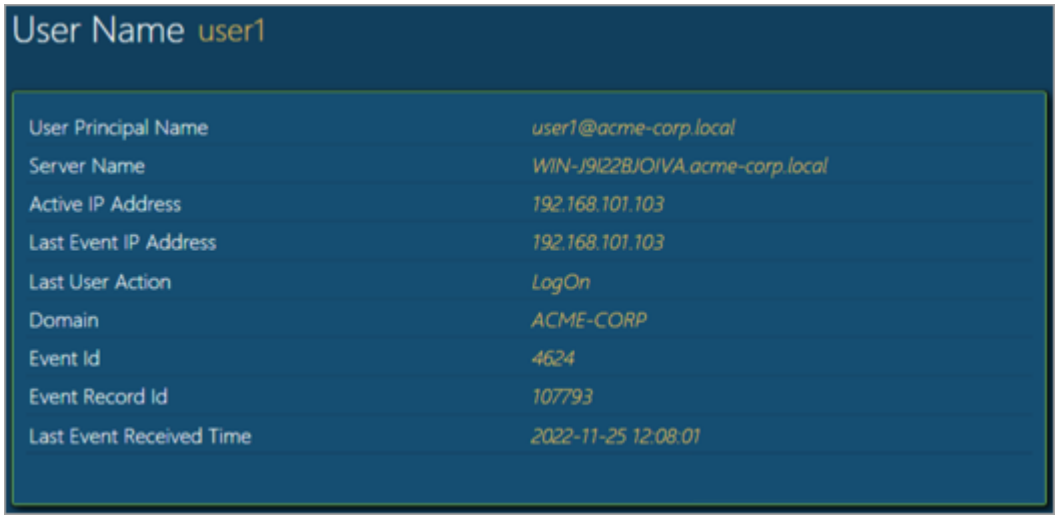
5. To view bootstrap statistics, select the Bootstrap Statistics tab.

To view end user login and logout events:

1. In the Versa WMI Agent main window, select the Users tab. The highlighted section of the screenshot below shows the end user named user1 who has logged in to a Windows device with the username user1@acme-corp.local. The entries in the columns show that user1 successfully passed authentication and that Active Directory pushed the information to the WMI agent. Receiving such events also indicates connectivity between the WMI agent and Active Directory.



2. To view more details about the user, click View Details. The Username window displays.



Verify the Secure SD-WAN CPE

1. To check the connectivity between the secure SD-WAN CPE and the FQDN of the load balancer, issue the **ping** *fqdn* **routing-instance** *LAN-VR-name* CLI command, which checks the connectivity between the LAN interface of the secure SD-WAN CPE and the VMS VIP interface on the load balancer. In the following example, the FQDN, whose resolved IP address is on the load balancer, is ha.acme-corp.local and the customer LAN routing instance is ACME-CORP-LAN-VR.

```
admin@ACME-CORP-BRANCH-101A-cli> ping ha.acme-corp.local routing-instance ACME-CORP-LAN-VR
PING ha.acme-corp.local (192.168.101.12) 56(84) bytes of data.
64 bytes from ha.acme-corp.local (192.168.101.12): icmp_seq=1 ttl=64 time=2.39 ms
64 bytes from ha.acme-corp.local (192.168.101.12): icmp_seq=2 ttl=64 time=1.16 ms
```

```
64 bytes from ha.acme-corp.local (192.168.101.12): icmp_seq=3 ttl=64 time=2.28 ms
64 bytes from ha.acme-corp.local (192.168.101.12): icmp_seq=4 ttl=64 time=1.21 ms
64 bytes from ha.acme-corp.local (192.168.101.12): icmp_seq=5 ttl=64 time=1.23 ms
--- ha.acme-corp.local ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 1.167/1.658/2.392/0.556 ms
```

Note that name resolution relies on the SD-WAN CPE performing a lookup of your DNS servers. if the name is not resolved, check the DNS configuration on the CPE. Specifically, check the IP addresses of the servers, check that the routing instance uses the same VRF that connects to the customer's DNS server, and check that the network name or interface allows connectivity to the customer's DNS server.

If the **ping** command fails but the name resolves correctly, check for routing issues and appropriate firewall rules between the secure SD-WAN CPE and the load balancer.

2. To check the application-level connectivity between the secure SD-WAN CPE and VMS, issue the **show orgs org-services vms status** command. The following example output shows that the secure SD-WAN CPE is successfully connected to the VMS server and that messages have been received from the VMS server.

```
admin@ACME-CORP-BRANCH-101A-cli> show orgs org-services ACME-CORP vms status
vms status VMS
Server profile name                          VMS
VMS fqdn                                     vmsl.acme-corp.local
Port number                                  3074
------------------
Session Statistics:
------------------
Session ID                                   5577006791947779410
Time since session was created               2022-11-25, 03:53:20
Total number of times connection has disconnected   0
gRPC channel status Connected Connect time   2022-11-25, 03:55:15
Number of reconnect attempt                  1669377315
Last reconnect attempt time                  Never Expires
Last reconnect error message                 VMSAPI_OK
-----------------------
Subscription Statistics:
-----------------------
Start time                                   2022-11-25, 03:53:20
--------
Current:
--------
Connection status                            Connected
Connect time                                 2022-11-25, 03:57:10
Last sequence number received                36
Number of messages received                  36
Number of messages dispatched                36
Number of messages dropped                   0
---------
Previous:
---------
Connection status
Connect time                                 2022-11-25, 03:55:15
```

```
Last sequence number received          0
Number of messages received            0
Number of messages dispatched          0
Number of messages dropped             0
Disconnect time                        2022-11-25, 03:57:00
Disconnect error message               VMSAPI_ERR_UNKNOWN
------
Total:
------
Number of messages received            36
Number of messages dispatched          36
Number of messages dropped             0
Number of failovers detected           0
```

If the output displays Connecting instead of Connected, check that the root-ca-cert.pem file is installed on the CPE.

Note that the sequence number, 36 in the output here, must match the sequence number in uipmap.log file on the VMS server.

3. To check that messages from the VMS server are converted to live users seen on the network, issue the **show orgs org-services user-identification live-users list** command. For example:

```
admin@ACME-CORP-BRANCH-101A-cli> show orgs org-services ACME-CORP user-identification
live-users list brief
                                        TIME
                                    SESSION  TO     EXPIRATION
IP ADDRESS      NAME                STATUS  HITS    EXPIRY  MODE
-------------------------------------------------------------------------
192.168.101.103  user1@acme-corp.local    Live    82      28098   inactivity

admin@ACME-CORP-8RANCH-101A-cli> show orgs org-services ACME-CORP user-identification
live-users list detail
                                      TIME
                                  SESSION  TO     EXPIRATION   SEQUENCE  INFORMATION
AUTHENTICATION   INTERNAL  INTERNAL
IP ADDRESS      NAME                STATUS  HITS    EXPIRY  MODE        NUMBER
SOURCE          PROFILE        ID       GROUP ID  TIME STAMP
-------------------------------------------------------------------------------------------------------------------------------
----------
192.168.101.103 user1@acme-corp.local    Live    82      28092    inactivity   36        Real time update
VMS_AP          0          -        2022-11-25 04:17:58
```

As we have already seen on the WMI agent, the user named user1@acme-corp.local is connected to the network. The information about the user has been shared from the VMS platform to the secure SD-WAN CPE. You can view the same information from the Users tab in the WMI agent UI. For more information, see Verify WMI Agent, above.

4. Optionally, to check the LDAP connectivity between secure SD-WAN CPE and customer's active directory, issue the **show orgs org-services user-identification ldap-server-data users** command. The CPE retrieves a list of all users on the LDAP platform. For example

```
admin@ACME-CORP-BRANCH-101A-cli> show orgs org-services ACME-CORP user-identification
ldap-server-data users brief
GROUP
MAPPING  LDAP                    DISPLAY
PROFILE  PROFILE  NAME           NAME    DISTINGUISHED NAME                  USER
PRINCIPAL NAME
-------------------------------------------------------------------------------------------------------
ldap_ug LDAP_SP  user4@acme-corp.local   user4    CN=user4,CN=Users,DC=acme-corp,DC=local
user4@acme-corp.local
            user3@acme-corp.local   user3    CN=user3,CN=Users,DC=acme-corp,DC=local
user3@acme-corp.local
            user2@acme-corp.local   user2    CN=user2,CN=Users,DC=acme-corp,DC=local
user2@acme-corp.local
            userl@acme-corp.local   user1    CN=user1,CN=Users,DC=acme-corp,DC=local   user1@acme-
corp.local

admin@ACME-CORP-BRANCH-101A-cli> show orgs org-services ACME-CORP user-identification
ldap-server-data users detail
GROUP                    USER                                                                SAM
MAPPING  LDAP                OBJECT
DISPLAY                                          GIVEN  ACCOUNT
PROFILE  PROFILE  NAME FORMAT      CLASS   NAME              NAME    DISTINGUISHED
NAME                 USER PRINCIPAL NAME     NAME   NAME
-------------------------------------------------------------------------------------------------------------------------------
--------------
ldap_ug  LDAP_SP  userPrincipalName  user   user4@acme-corp.local   user4
CN=user4,CN=Users,DC=acme-corp,DC=local  user4@acme-corp.local   user4  user4
                          user3@acme-corp.local   user3   CN=user3,CN=Users,DC=acme-
corp,DC=local  user3@acme-corp.local   user3  user3
                          user2@acme-corp.local   user2   CN=user2,CN=Users,DC=acme-
corp,DC=local  user2@acme-corp.local   user2  user2
                          user1@acme-corp.local   user1   CN=userl,CN=Users,DC=acme-
corp,DC=local  user1@acme-corp.local   userl  userl
```

You can use the same CLI command to view groups by replacing the keyword **users** with **groups**. For example:

```
admin@ACME-CORP-BRANCH-101A-cli> show orgs org-services ACME-CORP user-identification
ldap-server-data groups brief
GROUP
MAPPING   LDAP
PROFILE   PROFILE   NAME                          DISTINGUISHED NAME
-------------------------------------------------------------------------------------------------------------------------
ldap_ug   LDAP_SP   DnsUpdateProxy                   CN=DnsUpdateProxy,CN=Users,DC=acme-
corp,DC=local
            DnsAdmins                       CN=DnsAdmins,CN=Users,DC=acme-corp,DC=local
            Enterprise Key Admins             CN=Enterprise Key Admins,CN=Users,DC=acme-
corp,DC=local
            Key Admins                      CN=Key Admins,CN=Users,DC=acme-corp,DC=local
            Protected Users                  CN=Protected Users,CN=Users,DC=acme-corp,DC=local
            Cloneable Domain Controllers          CN=Cloneable Domain Controllers,CN=Users,DC=acme-
corp,DC=local
            Enterprise Read-only Domain Controllers  CN=Enterprise Read-only Domain
Controllers,CN=Users,DC=acme-corp,DC=local
```

```
Read-only Domain Controllers            CN=Read-only Domain
Controllers,CN=Users,DC=acme-corp,DC=local
Denied RODC Password Replication Group   CN=Denied RODC Password Replication
Group,CN=Users,DC=acme-corp,DC=local
Allowed RODC Password Replication Group  CN=Allowed RODC Password Replication
Group,CN=Users,DC=acme-corp,DC=local
Terminal Server License Servers          CN=Terminal Server License
Servers,CN=Builtin,DC=acme-corp,DC=local
Windows Authorization Access Group       CN=Windows Authorization Access
Group,CN=Builtin,DC=acme-corp,DC=local
Incoming Forest Trust Builders           CN=Incoming Forest Trust
Builders,CN=Builtin,DC=acme-corp,DC=local
Pre-Windows 2000 Compatible Access       CN=Pre-Windows 2000 Compatible
Access,CN=Builtin,DC=acme-corp,DC=local
Account Operators                        CN=Account Operators,CN=Builtin,DC=acme-corp,DC=local.
```

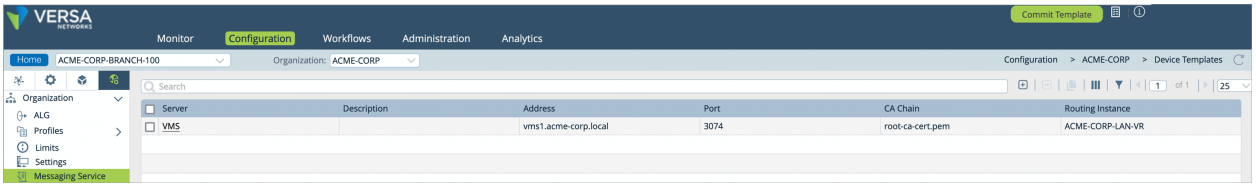
Verify Packet Capture Information

You can verify packets capture information between a secure SD-WAN server and a VMS server, and between WMI agent and VMS server for traffic-related information. In this example, we used the following IP addresses:

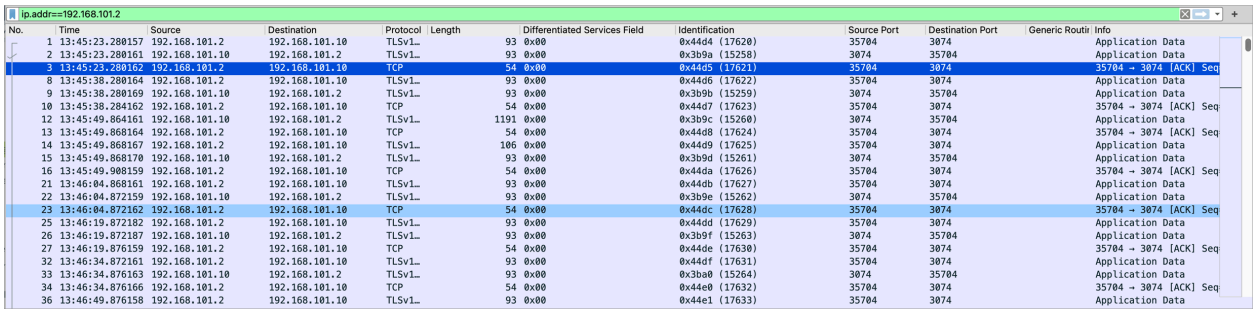
- 192.168.101.2—Local VOS branch
- 192.168.101.10—VMS

Verify Packets between the Secure SD-WAN Branch and the VMS Server

Communication between devices use TCP port 3074. You can display the communication information on the Organization > Messaging Service screen. For example:

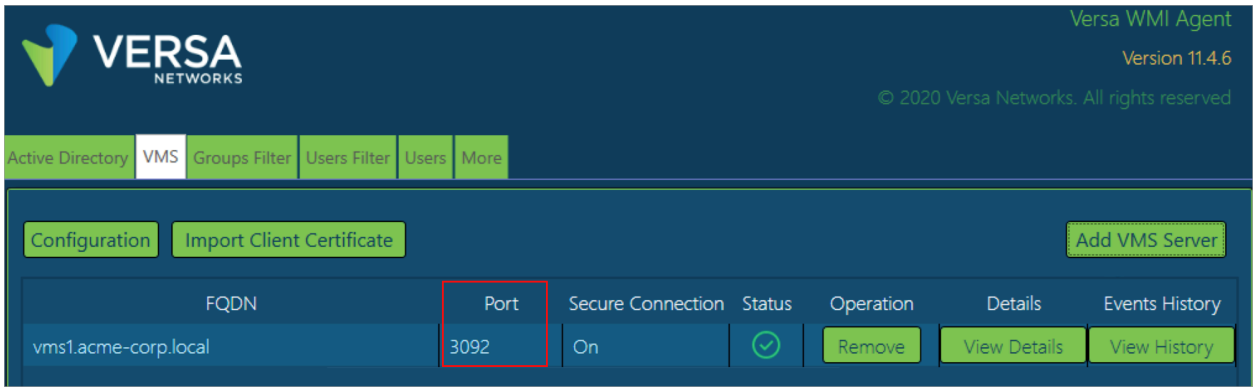


The following packet capture confirms that communication between the secure SD-WAN branch and the VMS server is using port TCP port 3074. The server is using port 3074. The client, as expected, uses an ephemeral port, here 35704. Also note that data transfer uses TLSv1.2:

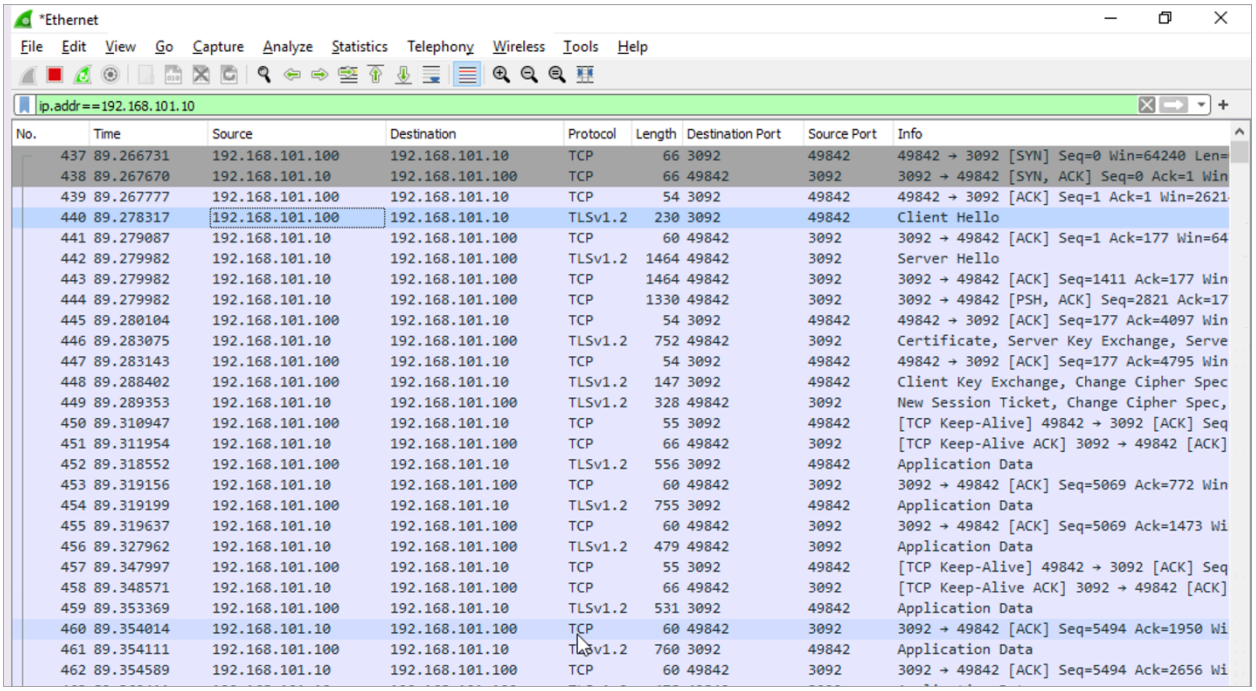


Verify Packets between the WMI Agent and the VMS Server

By default, the WMI agent is configured to connect to the VMS server on port 3092 using a secure connection:



The following packet capture confirms the connection between the WMI agent and the VMS server. It shows that packets are sent over TCP port 3092 (VMS server is 3092) and that the WMI agent uses an ephemeral port, in this case 49842. Note that data transfer uses TLSv1.2.



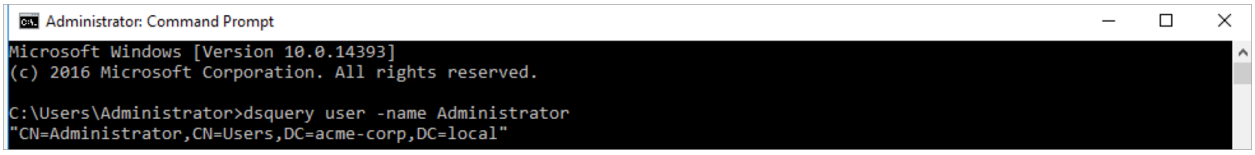
Determine the Active Directory Bind DN and Base DN

When you configure the server group profile on Versa Director, which the SD-WAN device uses to query the customer's Active Directory server, you must enter the bind distinguished name (DN) (for example, CN=Administrator,CN=Users,DC=acme-corp,DC=local) and base distinguished name (DN) (for example, DC=acme-corp,DC=local).

To determine the bind DN information on the Active Directory server, you can do one of the following:

Option 1

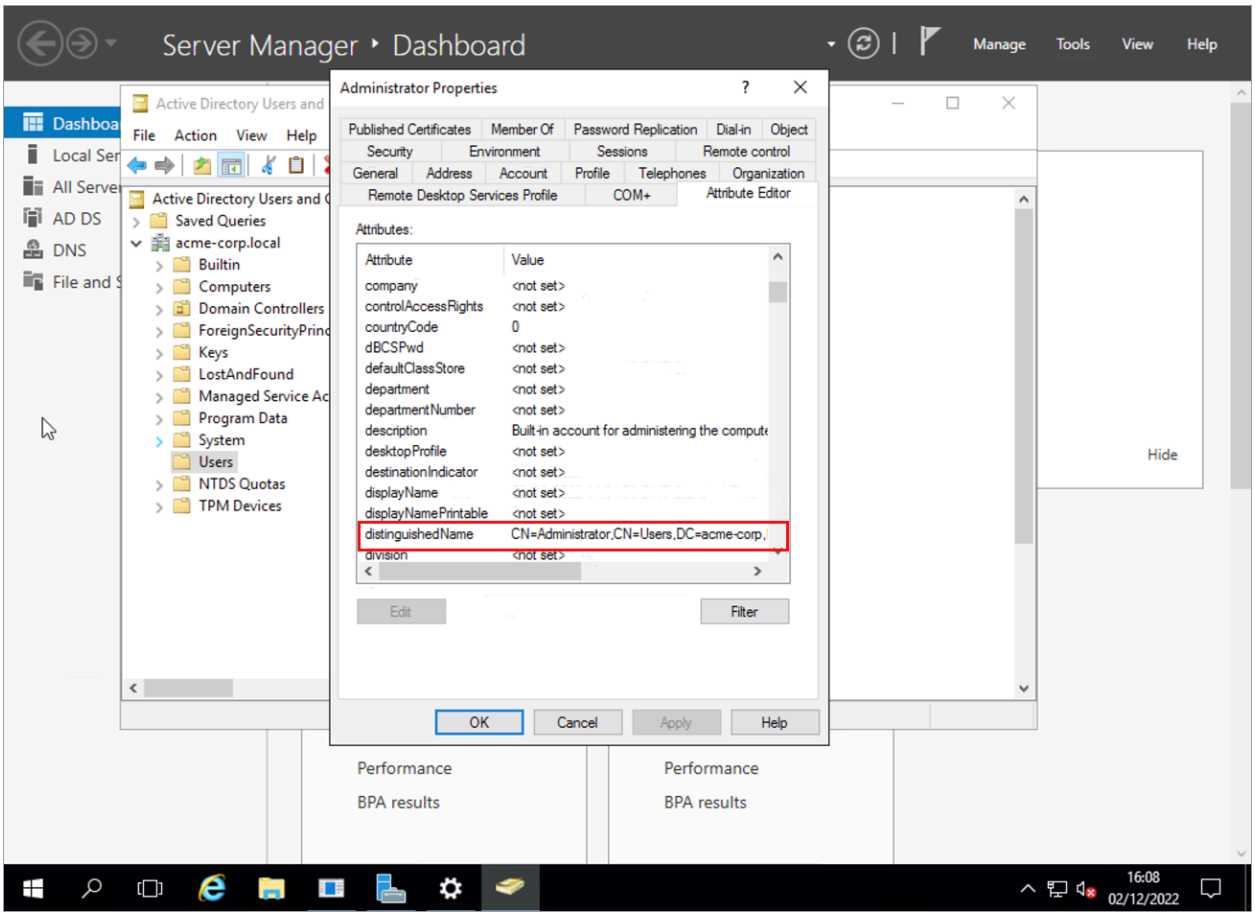
1. On the Active Directory server, in the Start menu, search for cmd or Command Prompt.
2. Right-click the Command Prompt icon and select Run as Administrator. The Command Prompt opens.
3. At the prompt, issue the **dsquery user -name** *username* command. The following shows that VMS then uses the Administrator account to query Active Directory. Here, the bind DN is CN=Administrator,CN=Users,DC=acme-corp,DC=local.



Option 2

1. On the Active Directory server, open Active Directory Users and Computers (ADUC).

2. Select View > Advanced Features.
3. Search for the username that VMS uses to access Active Directory.
4. Right-click the username and select Properties.
5. Navigate to Administrator Properties.
6. Select the Attribute Editor tab and look for "distinguished name". The following example shows that VMS uses the Administrator account to query Active Directory, and the bind DN is CN=Administrator,CN=Users,DC=acme-corp,DC=local.



To determine the base DN information on Active Directory:

1. On the Active Directory server, click Start and search for Command Prompt.
2. Right-click the Command Prompt icon and select Run as Administrator.
3. At the Administrator command prompt, type **Dsquery** and then press Enter. The base DN display in the first row (here, DC=acme-corp,DC=local).

Supported Software Information

VOS Releases 22.1.3 and earlier support all content described in this article when used with the initial release of VMS (unnumbered).

Additional Information

Commit Template Modifications
Configure an Application Delivery Controller
Configure DNS Servers
Configure Interfaces
Configure Passive Authentication for VMS
Configure User and Group Policy
Create and Manage Certificates
Install and Configure the WMI Agent
Install the Versa Messaging Service
Overview of Configuration Templates