Install the Versa Messaging Service

For supported software information, click here.

Versa Messaging Service (VMS) is a services platform that enhances the scalability of Versa services and applications. VMS is built by leveraging state-of-the-art open source technologies such as Kubernetes and Docker.

The following are some of the main features of VMS:

- Handles data such as critical network performance information, security updates, and passive authentication data such as user-to-IP address mapping
- Manages highly dynamic data that is streamed to each Versa Operating System™ (VOS™) device to keep it updated
- Processes a high volume and a large scale of data

To create a VMS message-streaming server, you install the VMS software on an bare-metal platform. This article describes how to install the software.

Before You Begin

Before you install the VMS software on a bare-metal platform, ensure that the bare-metal platform meets the following minimum hardware requirements:

- 8 cores
- 16-GB RAM
- 250-GB solid state drive (SSD)

Ensure that you have downloaded the VMS ISO image from https://versanetworks.app.box.com/s/d7jh1z6y3kaijd3yfwil0uxchr1w9ton/folder/164723287877

Ensure that the ports necessary for VMS control and worker nodes are available for communication. For more information see, Firewall Requirements.

Install the VMS Software on a Bare-Metal Platform

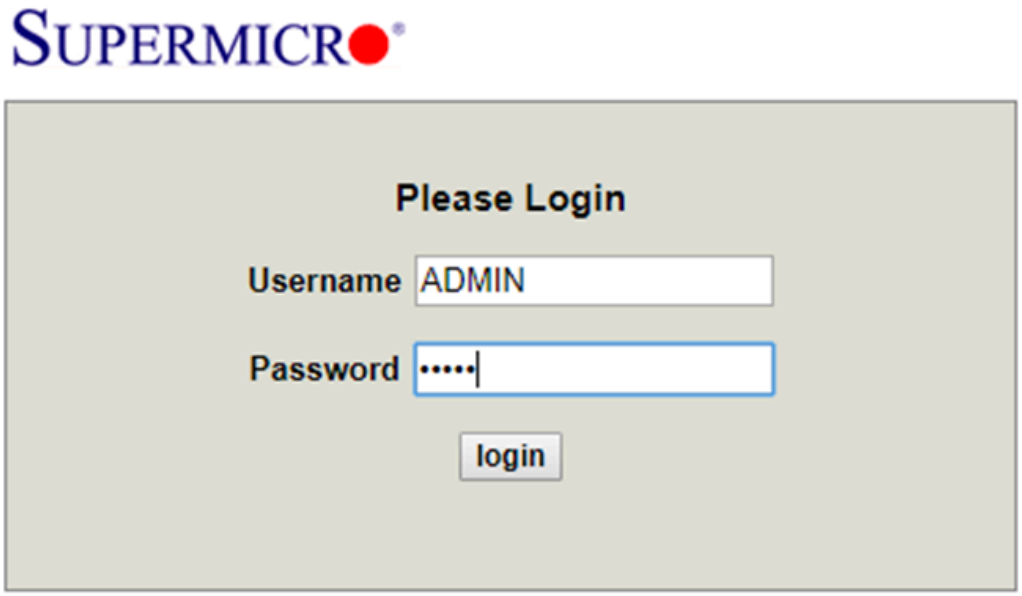
This section describes how to install the VMS software on a bare-metal platform.

The figures in this procedure are created using a Supermicro server. The actual screens you see may differ, depending on your server.

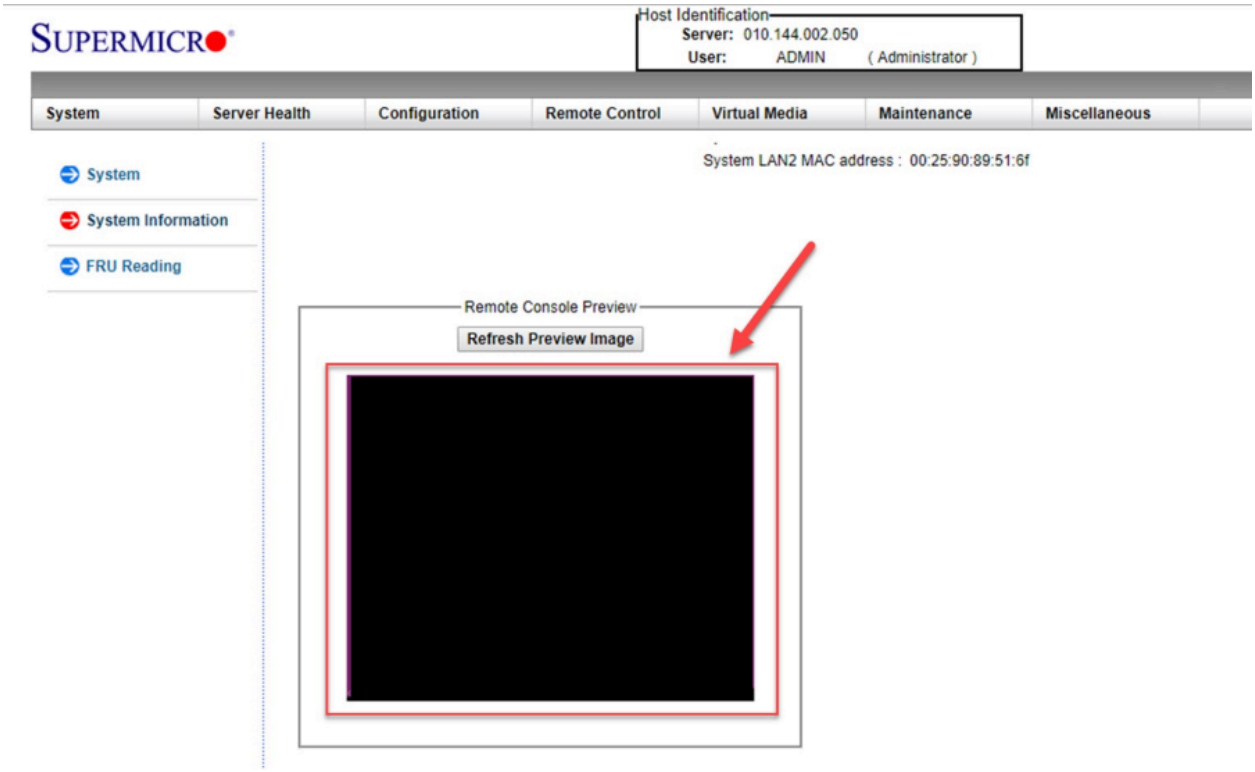
To access the bare-metal platform remotely, configure the Intelligent Platform Management Interface (IPMI) on the bare-metal server.

To install the VMS software on a bare-metal platform:

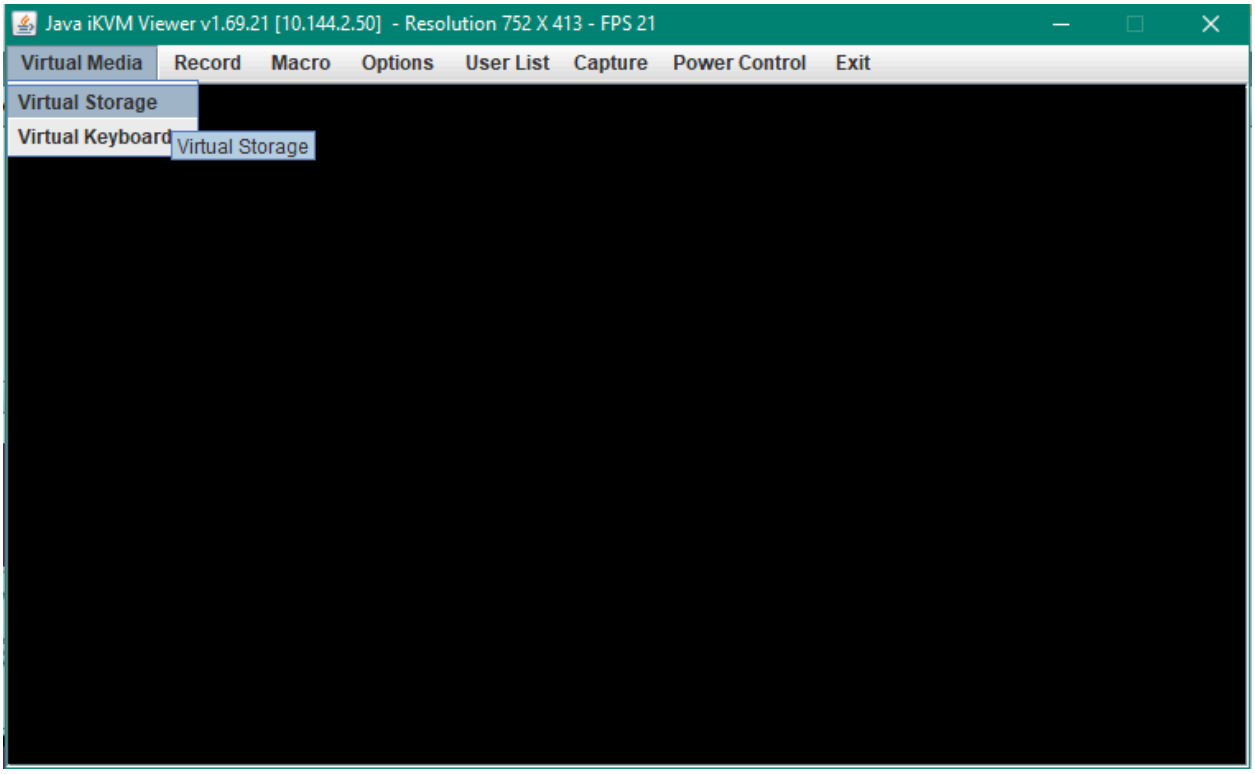
1. Log in to the remote console.



2. Click anywhere in the Remote Console Preview window to launch the remote console. If the Java SE Development Kit is installed on the server, you can launch the remote console from the development kit.

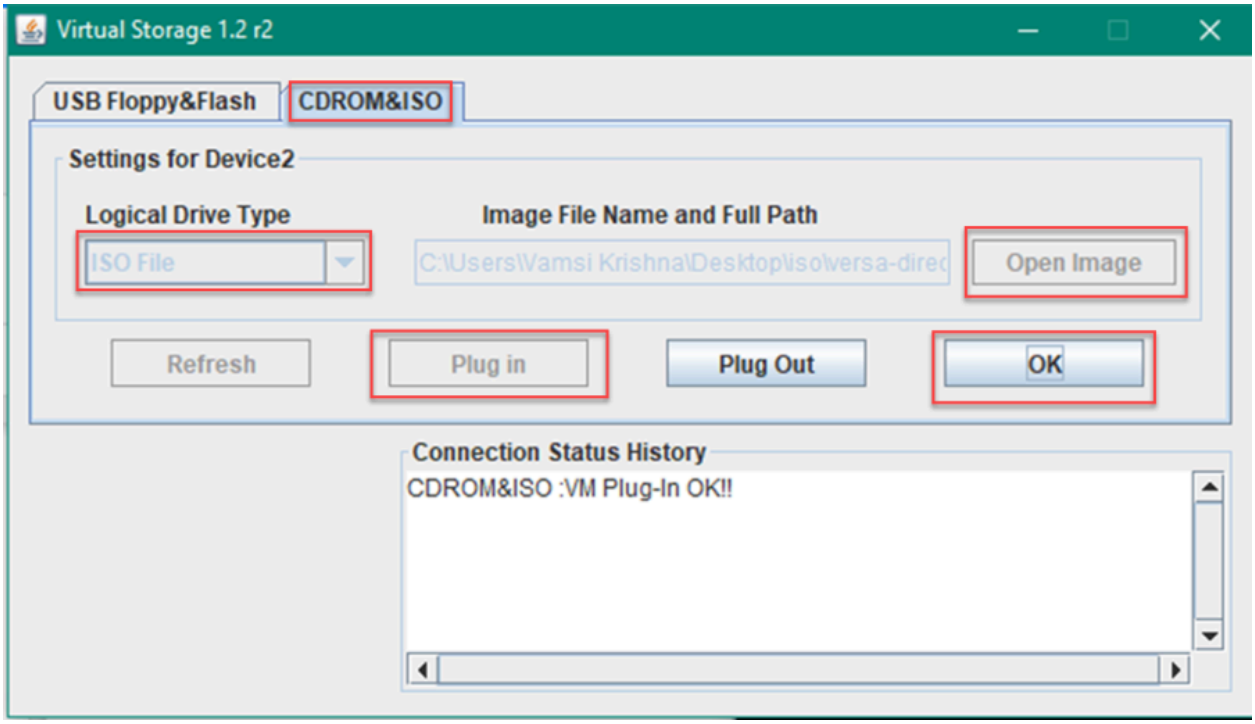


3. In the Virtual Media tab, click Virtual Storage.

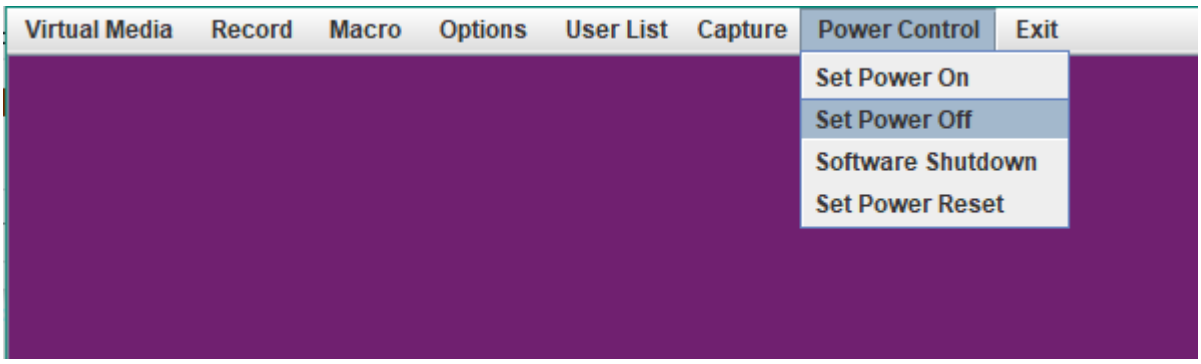


4. In the Virtual Storage window, select the CDROM & ISO tab. The Settings for Device2 window displays.

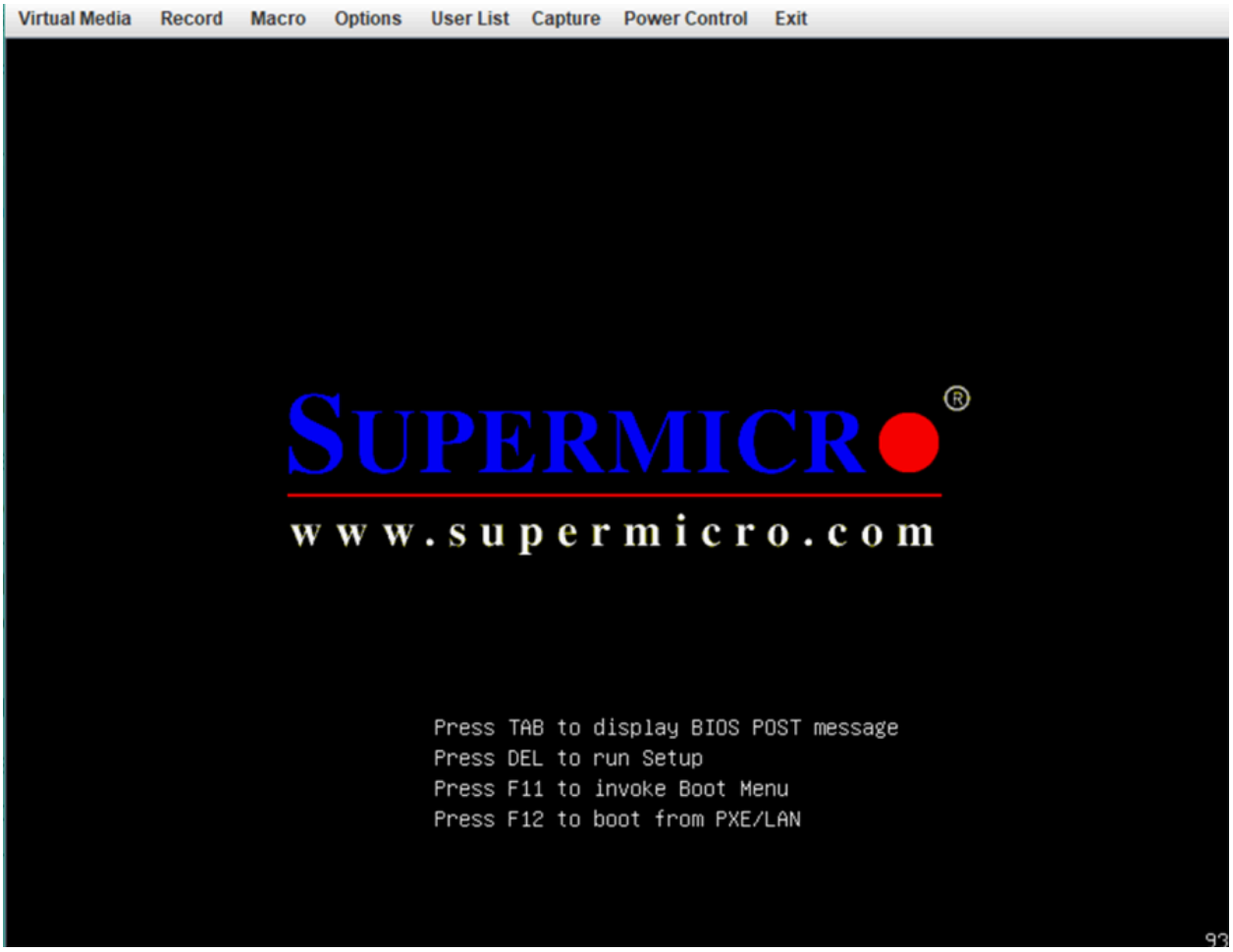
a. In the Logical Drive Type field, select ISO File.
b. Click Open Image, and type the full path name of the software image. You can find the image at https://versanetworks.app.box.com/s/d7jh1z6y3kaijd3yfwil0uxchr1w9ton/folder/164723287877
c. Click Plug In.
d. Click OK.



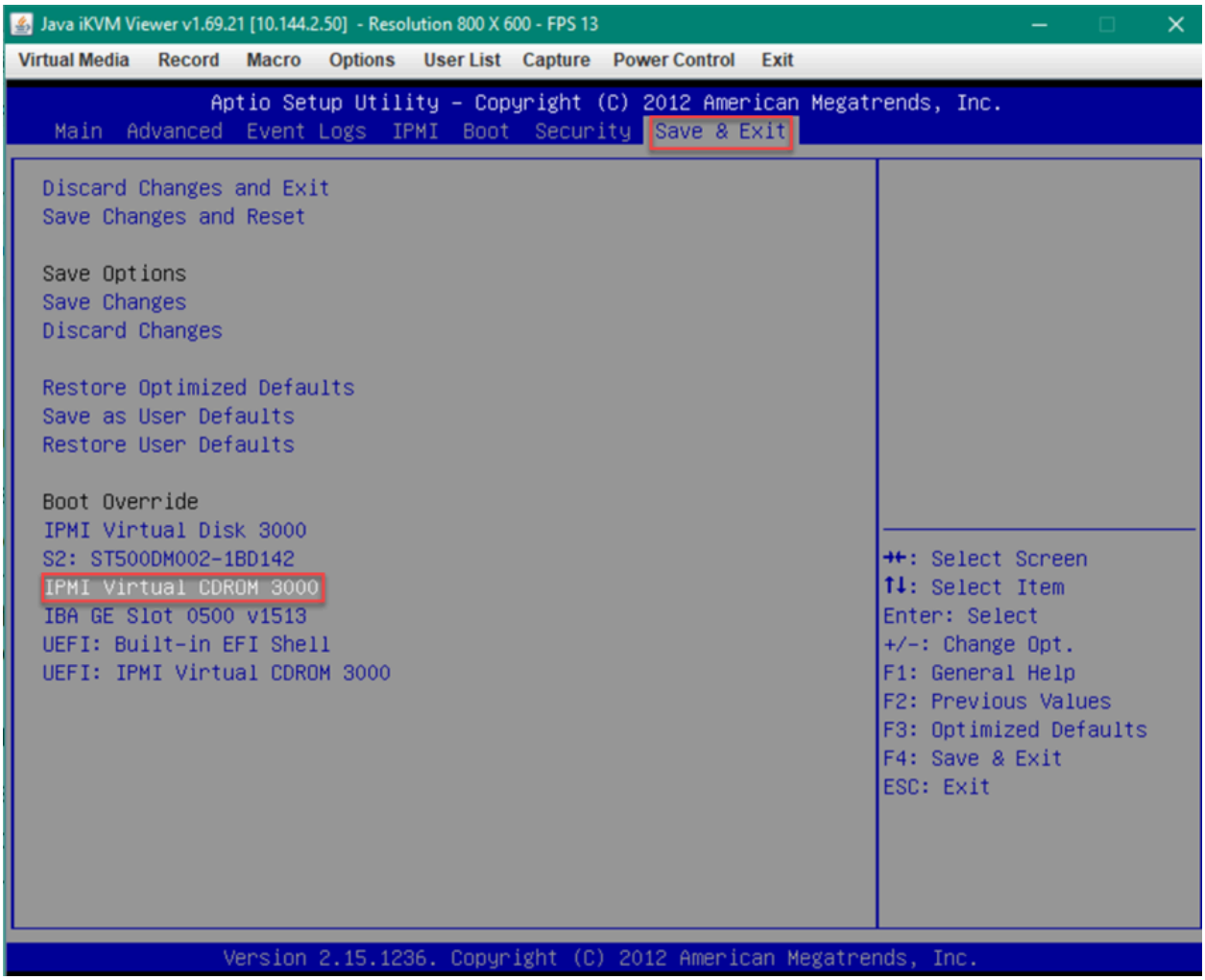
5. Select the Power Control tab.
   a. Click Set Power Off to power down the device.
   b. Click Set Power On to restart the device.



6. After the device restarts, the remote console window displays the server banner. To perform device setup, press the Delete key.



7. In the Setup Utility window:
    a. Click the Save & Exit tab.
    b. Click IPMI Virtual CDROM 3000 to run the ISO file from a local partition.
    c. Press Enter.



8. Install the ISO and then configure the primary IP address and hostname:

```
[admin@versa-Msgservice: -] $ sudo vi /etc network/interfaces
[sudo] password for admin:
[admin@versa-msgservice: -] $ sudo vi /etc/hosts
host.conf hostname hosts hosts.allow hosts.deny
[admin@versa-msgservice: -] $ sudo vi /etc/hosts
[admin@versa-msgservice: -] $ sudo vi /etc/hostname
sudo: unable to resolve host versa-msgservice: Resource temporarily unavailable
[admin@versa-msgservice: -] $
[admin@versa-msgservice: -] $ sudo reboot
```

   VMS release details such as version, release date, and package ID are displayed after the reboot completes.
9. If a .bin file is present in the same directory as the .iso file, install the .bin file.
10. Check the status of the server by issuing the **vsh status** CLI command. For example:

```
[admin@versa-msgservice: ~] $ vsh status
[sudo] password for admin:
============================================================


Versa Package Info: versa-msgservice-20210311-102527-35de8ea-21.1.1
============================================================

SYSTEM-SERVICES-STATUS
kubelet:active (6084)
docker:active (1713)
============================================================

PODS-STATUS
============================================================

SERVICES-STATUS
NAME         TYPE        CLUSTER-IP    EXTERNAL-IP   PORT(S)   AGE
kubernetes   ClusterIP   10.96.0.1     <none>        443/TCP   72m
============================================================
```

11. To configure the server, issue the **vsh configure-passive-auth** CLI command. When prompted, configure the following information:
    a. Generate certificates if you have not already done so. For example:

```
[admin@T-VMS-S: ~] $ vsh configure-passive-auth
================================================================================

Please generate Root Certificates before config

To generate Root Certificates use: sudo /opt/versa/vms/certs/vms_cert_gen.sh

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


Operation Aborted!
GoodBye!


[admin@T-VMS-S: ~] $ sudo /opt/versa/vms/certs/vms_cert_gen.sh

Domain is mandatory

    Usage:
        vms_cert_gen

    Description:
        Generate private key and certificate signing request (CSR) for CA to sign

    Example:
        sudo /opt/versa/vms/certs/vms_cert_gen.sh --domain vms01 --country US --state CA --locality SC --organization versa-networks.com --organizationalunit IT --email admin@versa-networks.com --keypass test
123 --validity 3650 --san vms-01,DNS:vms-02

    Options:
        -h, --help            Show this help message and exit.

        --domain              <Fully qualified domain name>

        --country             <Country name>

        --state               <State name>

        --locality            <Locality name>

        --organization        <Organization name>

        --organizationalunit  <Organizationalunit Name>

        --email               <email>

        --keypass            <private key password, if you want the private key is encrypted>

        [--validity]          <certificate validity in days>

        [--san]               <Fully qualified domain name for Subject Alt-Name, please refer to example for providing multiple values>
```

```
[admin@T-VMS-S: ~] $ sudo /opt/versa/vms/certs/vms_cert_gen.sh --domain vms-test5.versa-networks.com --country US --state CA --locality SC --organization versa-networks.com --organizationalunit QA --email adm
in@versa-networks.com --keypass test123 --validity 3650 --san vms-test5.versa-networks.com,DNS:vms-test5.versa-networks.com
 => Generating Key and CSR for request domain: vms-test5.versa-networks.com, key_pass: test123
 => Request details: [/emailAddress=admin@versa-networks.com/C=US/ST=CA/L=SC/O=versa-networks.com/OU=QA/CN=vms-test5.versa-networks.com]
 => Generating Root Certificate with password encrypted keypass: test123 and Root Certificate
 => Successfully generated Key file: /opt/versa/vms/certs//root-ca-key.pem
 => Please copy the file out of the system and maintain it
 => Successfully generated ROOT CA file: /opt/versa/vms/certs//root-ca-cert.pem
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................................................................................................++++
.....................................++++
e is 65537 (0x010001)
 => Successfully generated Key file: /opt/versa/vms/certs//ca-key.pem
Ignoring -days; not generating a certificate
 => Successfully generated INTERMEDIATE_CSR_FILE: /opt/versa/vms/certs//ca-csr.pem
Using configuration from /opt/versa/vms/certs//openssl.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Sep 28 18:00:29 2021 GMT
            Not After : Sep 26 18:00:29 2031 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = CA
            organizationName          = versa-networks.com
            organizationalUnitName    = QA
            commonName                = vms-test5.versa-networks.com Intermediate Cert Authority
            emailAddress              = admin@versa-networks.com
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                C9:5C:85:DF:A5:68:C9:F0:78:D1:3D:8C:75:70:EF:35:82:83:AF:F3
            X509v3 Authority Key Identifier:
                keyid:0F:4F:B2:52:A5:12:86:70:BF:9A:53:78:DF:D1:36:78:29:94:BD:4E

            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
Certificate is to be certified until Sep 26 18:00:29 2031 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
 => Successfully generated INTERMEDIATE CA file: /opt/versa/vms/certs//ca-cert.pem
 => Successfully verified INTERMEDIATE CA file: /opt/versa/vms/certs//ca-cert.pem
 => Successfully generated the Private CA Chain
 => Please copy the /opt/versa/vms/certs//root-ca-key.pem out of this system and store it safely
 => Please use the Password "test123" during server and client cert generation for vsh configure-SERVICE
```

b. Configure the IP address that the VMS server should use to connect to the VOS devices, the IP address that the VMS server should use to connect to the WMI agent, the primary and secondary IP addresses of the Versa Director node, and the Versa Director GUI or API login credentials of a user with administrator privileges. For example:

```
[admin@T-VMS-S: ~] $ 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   : 10.40.12.250

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

FQDN of this VMS server

Please enter the FQDN of this VMS Server:  vms-test5.versa-networks.com
This may take up to 10 minutes to complete initialization


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

Adding new hosts entry.
Warning: rbac.authorization.k8s.io/v1beta1 ClusterRole is deprecated in v1.17+, unavailable in v1.22+; use rbac.authorization.k8s.io/v1 ClusterRole
Warning: rbac.authorization.k8s.io/v1beta1 ClusterRoleBinding is deprecated in v1.17+, unavailable in v1.22+; use rbac.authorization.k8s.io/v1 ClusterRoleBinding

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


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


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


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            : 10.40.12.250

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


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

```
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    : 10.40.12.250

Info: PA_VMS_EXTERNAL_IP: 10.40.12.250

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


=========================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   : 10.40.227.102

Please Enter Secondary Versa Director's IP Address: 10.40.227.256

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



Enter the Versa Director GUI UserName with Admin privileges : USERNAME : Administrator

Primary Versa Director's Credentials

Enter Password for Versa Director User: 'Administrator'      :
RE-Enter Password for Versa Director User: 'Administrator'   :
================================================================================================
```

c. Configure the tenant name for which to enable passive authentication and the fully qualified domain name (FQDN) of the VMS server to use for certificate generation and validation. For example:

```
 Versa Tenant Details

Please enter Tenant Name for this Service :                          : Tenant2
Configuring for Teanant: Tenant2

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


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                                  : vms-test5.versa-networks.com


Please Enter Subject ALT Name 1 used in Versa Message Service certificate file   : vms-test5.versa-networks.com


Please Enter Subject ALT Name 2 used in Versa Message Service certificate file   : vms-test5.versa-networks.com
```

d. Configure the unique name for the VMS node to use during high availability (HA) switching.

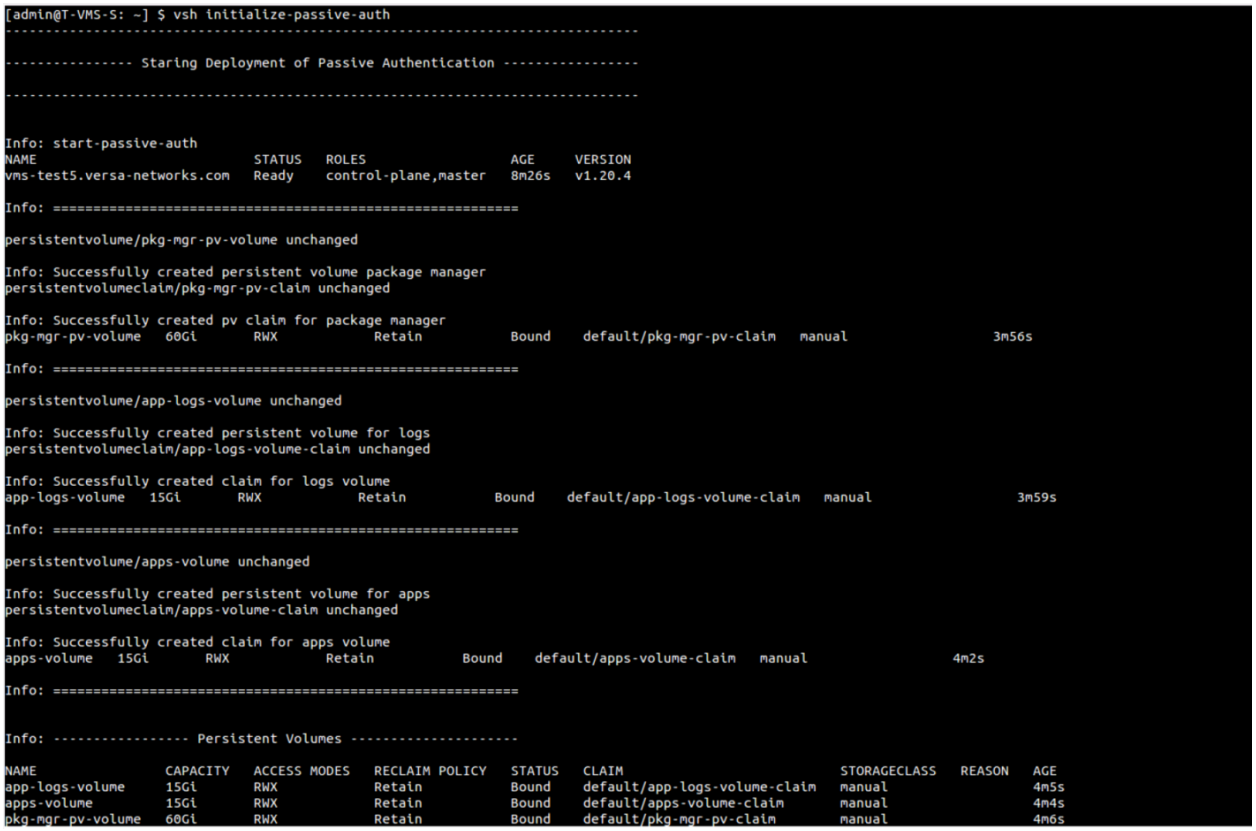
12. When prompted, enter the password to use while generating certificates. For example:

```
Certificate Regeneration

Existing Certificates FQDN:
Do you want to regerate the certificates with new FQDN: vms-test5.versa-networks.com ?  (y/N) :  y
[2021-09-28 11:15:14-07:00]: Started generating certificates...

[2021-09-28 11:15:14-07:00]: Server private key and csr created successfully

[2021-09-28 11:15:14-07:00]: Creating server certificate...
Enter pass phrase for /opt/versa/vms/certs/ca-key.pem:
[2021-09-28 11:15:18-07:00]: Server certificate created successfully

[2021-09-28 11:15:18-07:00]: Server certificate bundle created successfully

[2021-09-28 11:15:18-07:00]: Creating client private key and csr...
[2021-09-28 11:15:18-07:00]: Client private key and csr created successfully

[2021-09-28 11:15:18-07:00]: Creating client certificate...
Enter pass phrase for /opt/versa/vms/certs/ca-key.pem:
[2021-09-28 11:15:20-07:00]: Client certificate created successfully

[2021-09-28 11:15:20-07:00]: Creating client certificate (pfx format)...
[2021-09-28 11:15:20-07:00]: Client certificate (pfx format) created successfully

[2021-09-28 11:15:21-07:00]: All certificates and keys are successfully created.
[2021-09-28 11:15:21-07:00]: Validating CA certificate...
/opt/versa/vms/certs/ca-cert.pem: OK
[2021-09-28 11:15:21-07:00]: Validation for CA certificate succeeded
[2021-09-28 11:15:21-07:00]: Validating server certificate...
/opt/versa/vms/certs/server-cert.pem: OK
[2021-09-28 11:15:21-07:00]: Validation for server certificate succeeded
[2021-09-28 11:15:21-07:00]: Validating client certificate...
/opt/versa/vms/certs/client-cert.pem: OK
[2021-09-28 11:15:21-07:00]: Validation for client certificate succeeded
[2021-09-28 11:15:21-07:00]: Exiting...


Certificate Regenerated with SAN: vms-test5.versa-networks.com, vms-test5.versa-networks.com, vms-test5.versa-networks.com




Establishing connectivity with Director


Establishing connectivity with Director

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

When the configuration process completes, a screen similar to the following displays:

```


Please provide the below server identification information

This Information is needed for HA fail-over
Please Enter a unique name for this VMS node     : vms-test5-node


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


VMS configuration completed

Please run " vsh initialize-SERVICE_NAME " to complete set-up

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

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

Run vsh initialize-passive-auth to complete Deployment

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

13. To start the deployment, **vsh initialize-passive-auth** CLI command. For, example:



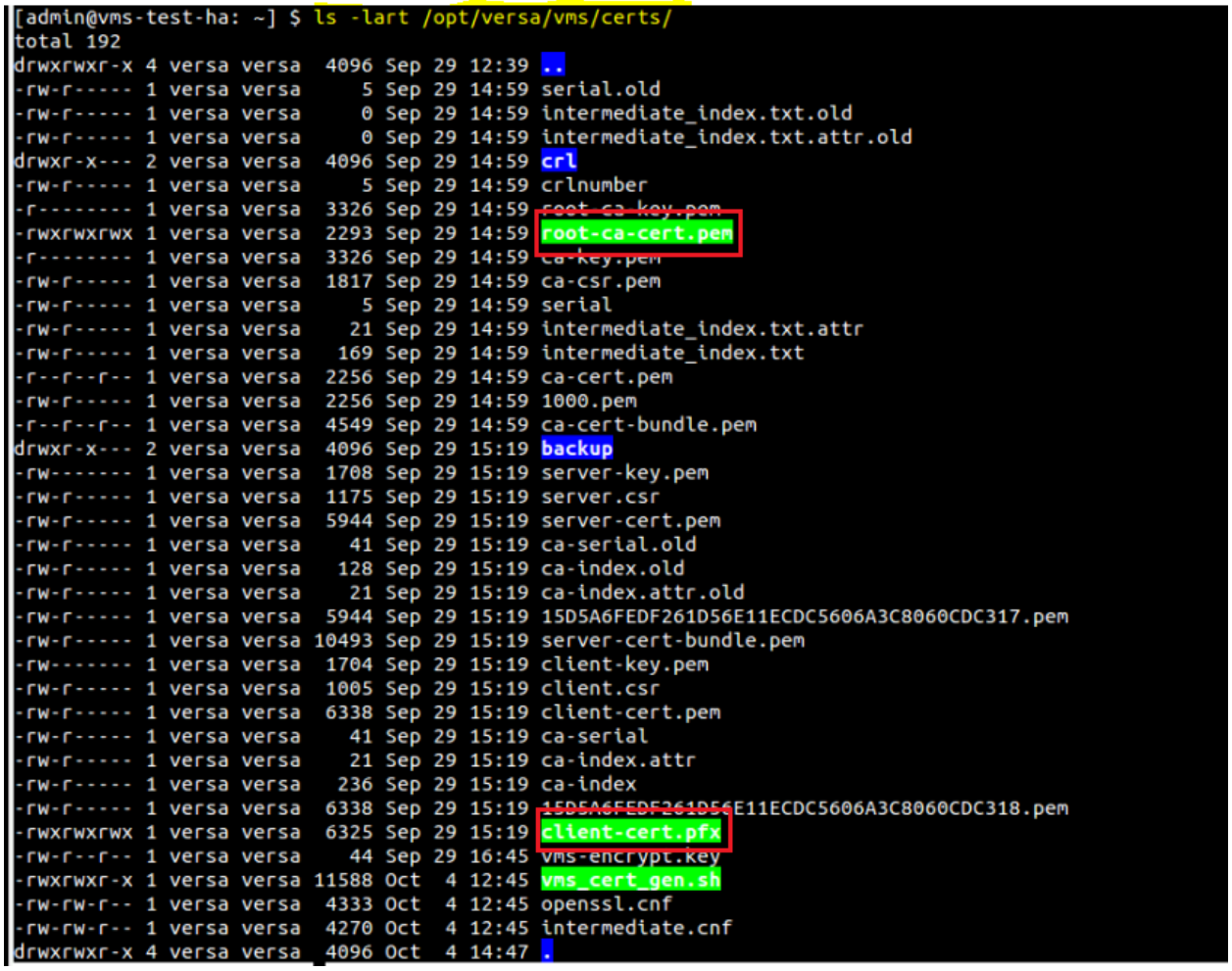
After the server is initialized, information about pods and services displays:

```
Versa Package Info: versa-msgservice-20210928-002155-3f1a754-21.2.2

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


Info: SYSTEM-SERVICES-STATUS
kubelet:active (9184)
docker:active (4252)

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

PODS-STATUS
NAME                              READY   STATUS    RESTARTS   AGE
concentrator-5fdf6cfcb8-99cqw     1/1     Running   0          14s
message-server-7b6db77b94-7xl5w   1/1     Running   0          57s
nginx-56799c4fd6-wlfhg            1/1     Running   0          43s
pkg-builder-bbdf5c558-lnksh       1/1     Running   0          51s
redis-uipmap-687c77bd74-kvr4x     1/1     Running   0          69s
uipmap-bd565f987-8x2qm            1/1     Running   0          20s
vxdev-7d56c8f5f7-w2vlb            1/1     Running   0          63s

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

SERVICES-STATUS
NAME             TYPE        CLUSTER-IP       EXTERNAL-IP    PORT(S)                      AGE
concentrator     ClusterIP   10.105.211.129   10.40.12.250   3092/TCP                     13s
kubernetes       ClusterIP   10.96.0.1        <none>         443/TCP                      9m48s
message-server   ClusterIP   10.108.220.30    10.40.12.250   3074/TCP,3101/TCP,3102/TCP   55s
nginx            ClusterIP   10.103.214.138   10.40.12.250   443/TCP                      45s
redis-uipmap     ClusterIP   10.96.145.49     <none>         6379/TCP                     66s
uipmap           ClusterIP   10.96.111.197    <none>         7000/TCP                     18s
vxdev            ClusterIP   10.102.24.192    <none>         8080/TCP                     60s

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

--------------------------------------------------------------------------------

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

--------------------------------------------------------------------------------
```

14. To check the status of the deployment, issue the **vsh status** CLI command. For example:

```
[admin@T-VMS-S: ~] $ vsh status

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

Versa Package Info: versa-msgservice-20210928-002155-3f1a754-21.2.2

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

Info: SYSTEM-SERVICES-STATUS
kubelet:active (9184)
docker:active (4252)

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

PODS-STATUS
NAME                                READY   STATUS    RESTARTS   AGE
concentrator-5fdf6cfcb8-99cqw       1/1     Running   0          3m10s
message-server-7b6db77b94-7xl5w     1/1     Running   0          3m53s
nginx-56799c4fd6-wlfhg              1/1     Running   0          3m39s
pkg-builder-bbdf5c558-lnksh         1/1     Running   0          3m47s
redis-uipmap-687c77bd74-kvr4x       1/1     Running   0          4m5s
uipmap-bd565f987-8x2qm              1/1     Running   0          3m16s
vxdev-7d56c8f5f7-w2vlb              1/1     Running   0          3m59s

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

SERVICES-STATUS
NAME             TYPE        CLUSTER-IP       EXTERNAL-IP    PORT(S)                      AGE
concentrator     ClusterIP   10.105.211.129   10.40.12.250   3092/TCP                     3m10s
kubernetes       ClusterIP   10.96.0.1        <none>         443/TCP                      12m
message-server   ClusterIP   10.108.220.30    10.40.12.250   3074/TCP,3101/TCP,3102/TCP   3m52s
nginx            ClusterIP   10.103.214.138   10.40.12.250   443/TCP                      3m42s
redis-uipmap     ClusterIP   10.96.145.49     <none>         6379/TCP                     4m3s
uipmap           ClusterIP   10.96.111.197    <none>         7000/TCP                     3m15s
vxdev            ClusterIP   10.102.24.192    <none>         8080/TCP                     3m57s

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

[admin@T-VMS-S: ~] $ date
Tue Sep 28 11:21:23 PDT 2021
```

15. Copy the certificates (root-ca-cert.pem and client-cert.pfx) to the WMI agent. For example:



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

Configure Passive Authentication for VMS
Firewall Requirements
Hardware and Software Requirements for Headend
Install and Configure the WMI Agent
Install on VMware ESXi
Upgrade the Versa Messaging Service