
Perform Manual Hardening for Versa Analytics

 For supported software information, click [here](#).

This article describes the recommended manual hardening for the Versa Analytics Releases 20.2 and later. System hardening ensures that Versa Networks products are secure when running in customer networks.

Use Signed SSL Certificates

By default, Analytics nodes work with autogenerated, self-signed certificates. Production equipment must have a valid signed certificate so that devices accessing the infrastructure do not trigger certificate errors.

To enable secure mode, you must have installed all Versa Director and Analytics devices with production certificates and verified their functionality.

Note: Enabling secure mode has consequences for the procedures described in this article. It is recommended that you verify working condition of all system functions before you enable secure mode.

To generate a certificate signing request (CSR), you use the `van-csr-gen.sh` script. Depending on the version of Analytics software, the `van-csr-gen.sh` script may not be present on the Analytics node. If it is not present, upload it to the `/opt/versa/scripts/van-scripts` directory.

Enable SSL Certificates

1. Generate a CSR by running the `van-csr-gen.sh` script. For example:

```
$ cd /opt/versa/scripts/van-scripts
$ ./van-csr-gen.sh --domain analytics1.versa-networks.com \
--country US --state CA \
--organizationalunit IT --locality "San Jose" \
--email lab@versa-networks.com \
--organization Versa Networks \
--keypass versa123
```

2. Copy the certificate to the Certificate Authority (CA) and sign it. Note that the signed certificate must be in PEM file format.
3. In the versa user's home directory, create a temporary directory for the signed certificate, private key, and CA certificate, and assign the directory 700 permission:

```
$ mkdir certs
$ chmod 700 cert
```

4. Install the SSL certificate. Note that the private key is stored in the `/var/versa/vnms/data/certs/certificate-name.key` file.

```
$ sudo /opt/versa/scripts/van-scripts/van-import-cert.sh \
--key path-to-private-key-file \
--cert path-to-signed-certificate-file \
--keypass certificate-password \
--cafile path-to-CA-certificate-file
```

5. Securely back up and store the certificate and private key files generated in Steps 1 and 3 to a secure location using the `scp` command.
6. Delete the certificate and private key files generated in Steps 1 and 3 so that the private key is not left for anyone to read.
7. Repeat Steps 1 through 6 for all Analytics nodes in the cluster.

Enable SSH Banners

1. Create banner text in the `/opt/versa/etc/banner.net` file using a file editor (for example, Vi or Nano) and save the file.
2. Change the file ownership to `versa:versa`:

```
$ sudo chown versa:versa /opt/versa/etc/banner.net
```

3. Modify the SSH banner entry in the `sshd_config` file to use the `banner.net` file from Step 1:

```
$ sudo sed -i -e 's/#Banner.*/Banner /opt/versa/etc/banner.net/' /etc/ssh/sshd_config
```

4. Restart the SSH service:

```
$ sudo service ssh restart
```

Update OS Security Package

To harden the Analytics security, regularly update the Analytics nodes to the latest OS security pack (OS SPack). For more information, see [Use OS Security Packages](#).

Configure NTP

You configure the Network Time Protocol (NTP) and the timezone to use in the network so that all devices in the network operate on the same time. Time synchronization is important so that the timestamps in log files match across all devices. Also, there are cryptographic requirements for time synchronization. NTP and timezone services on the Analytics platform are provided by the Ubuntu core operating system.

To modify the NTP servers:

1. Log into the Versa Analytics node.
2. Edit the `/etc/ntp.conf` file to update the servers.
3. Restart the NTP daemon:

```
| admin@Analytics$ sudo service ntp restart
```

To configure system timezone:

1. Identify the desired timezone. For example:

```
| admin@Analytics$ timedatectl list-timezones | grep -i chicago  
America/Chicago
```

2. Unlink the current timezone:

```
| admin@Analytics$ sudo unlink /etc/localtime
```

3. Reboot the Analytics node.

Configure DNS

DNS services on the Analytics platform are provided by the Ubuntu core operating system.

To configure system DNS:

1. Edit the `/etc/network/interfaces` file as required.
2. Restart the interface:

```
| $ ifdown  
$ ifup
```

Verify the Software Version

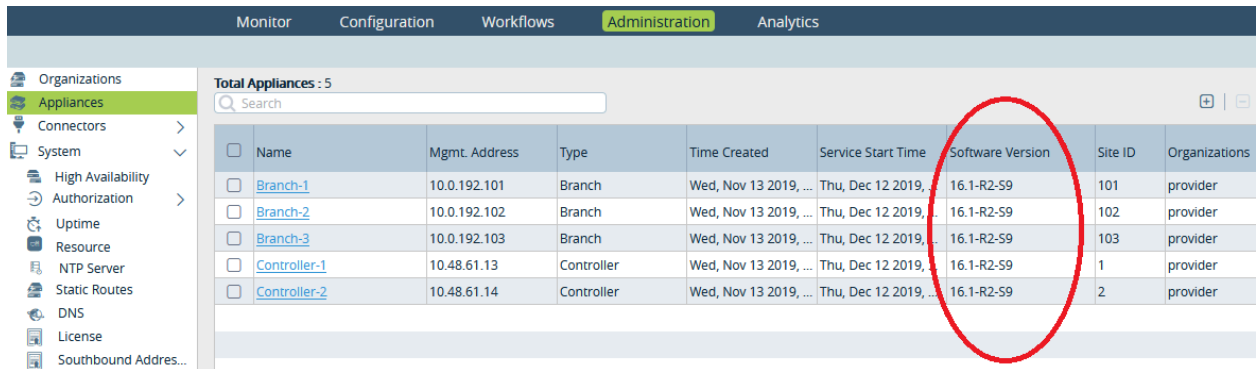
For the best performance of all SD-WAN components, Versa Networks requires that all components run the same software version.

1. To verify the software version of Versa Director or Analytics, log in to the CLI and issue the **show system package-info** CLI command. For example:

```
| Administrator@analytics1> show system package-info  
Package      Versa Analytics Software  
Release      16.1R2  
Build        S9  
Release date  20190628  
Package id   a454c1d
```

UI Package id 3580b52
Package name versa-analytics-20190628-150633-a454c1d-16.1R2S9
Branch 16.1R2

2. To verify the software version running on VOS devices:
 - a. In Director view, select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar. The Software Version column displays the version.



The screenshot shows the Versa Director interface with the 'Administration' tab selected. In the left-hand menu, 'Appliances' is highlighted. The main area displays a table of appliances. The 'Software Version' column is circled in red. The table has 9 columns: Name, Mgmt. Address, Type, Time Created, Service Start Time, Software Version, Site ID, and Organizations. There are 5 appliances listed: Branch-1, Branch-2, Branch-3, Controller-1, and Controller-2. All have a software version of 16.1-R2-S9.

Name	Mgmt. Address	Type	Time Created	Service Start Time	Software Version	Site ID	Organizations
Branch-1	10.0.192.101	Branch	Wed, Nov 13 2019, ...	Thu, Dec 12 2019, ...	16.1-R2-S9	101	provider
Branch-2	10.0.192.102	Branch	Wed, Nov 13 2019, ...	Thu, Dec 12 2019, ...	16.1-R2-S9	102	provider
Branch-3	10.0.192.103	Branch	Wed, Nov 13 2019, ...	Thu, Dec 12 2019, ...	16.1-R2-S9	103	provider
Controller-1	10.48.61.13	Controller	Wed, Nov 13 2019, ...	Thu, Dec 12 2019, ...	16.1-R2-S9	1	provider
Controller-2	10.48.61.14	Controller	Wed, Nov 13 2019, ...	Thu, Dec 12 2019, ...	16.1-R2-S9	2	provider

Enable Centralized Authentication

For Releases 20.2.2 and later.

To enable centralized authentication (TACACS+) on Analytics nodes:

1. SSH to the Analytics Node.
2. Start the CLI:

```
| $ cli
```

3. Enter configuration mode:

```
| > configure
```

4. Set the authentication order to be remote first, then local:

```
| % set system external-aaa auth-order remote-then-local
```

5. Set the IP address of the TACACS+ server:

```
| % set system external-aaa tacacs-plus server ip-address key key-value
```

6. Set the functions for which you want to use the TACACS+ server. For example, to use the TACACS+ server for authentication:

```
| % set system external-aaa tacacs-plus action authentication
```

To use the server for accounting:

```
| % set system external-aaa tacacs-plus action accounting
```

7. Save the changes:

```
| % commit
```

TACACS+ Server Configuration

Users logging in from the TACACS+ server can have administrative permissions or operator permissions. To configure this, the TACACS+ server return must return the following versa-user-group attributes:

- admin—Users have administrative access to the Analytics node.
- oper—Users have operator access to the Analytics node.

Enable Secure Mode

You enable secure mode to harden the Linux core OS components to meet the Linux CIS benchmarks.

Before you enable secure mode, you must enable centralized authentication. For more information, see [Enable Centralized Authentication](#), above.

To enable secure mode:

1. From the CLI, execute the secure mode script:

```
| versa@analytics1$ cli  
| versa@analytics1> request system secure-mode enable
```

For example:

```
| versa@analytics1> request system secure-mode enable  
Will enable secure mode. Are you sure? [no,yes] : yes  
status success  
result Enabling Versa OS secure mode  
result Hardening SSH service  
result Hardening password scheme  
result Disabling USB storage  
result Hardening permissions on system executables  
result Hardening permissions on sensitive files  
result Hardening: Disabling FileSystem knobs  
result Hardening: Restricting the use of the job-scheduling privilege  
result Hardening: System knobs and TCP settings  
result Hardening console login permissions  
result Hardening port permissions
```

2. Exit the CLI and restart Versa services for the changes to take effect:

```
versa@analytics1: $ vsh restart
```

3. Change the Linux user passwords on the local device so that they all meet the complexity criteria.

To verify that secure mode is operating:

1. Issue the **request system secure-mode test brief** CLI command
2. Check the results in the `/var/log/versa/versa-security-test-date.log` file. The following is a sample of the log file contents that indicate that secure mode is operating properly:

```
[admin@director1: ~] $ sudo cat /var/log/versa/versa-security-test-20190411-092258.log
[sudo] password for admin:
[INFO] sshd config check complete - error count = 0
[INFO] login.defs config check complete - error count = 0
[INFO] pam passwd config check complete - error count = 0
[INFO] blacklist config check complete - error count = 0
[ERROR] Default password found in file (/opt/versa/scripts/strongswan/get_ipsec_params.lua)
[INFO] Default password check complete - error count = 1
```

Change Analytics Passwords

You must change the default passwords for the following predefined accounts and service on the Analytics platform:

- Shell accounts—admin, versa
- Analytics UI accounts—admin, Administrator
- Tomcat service

Change Shell Account Passwords

The default configuration for Analytics nodes includes two shell accounts: admin and versa. The default password for both accounts is versa123. To harden Analytics nodes, you must change the passwords for these accounts on every search-type and analytics-type Analytics node.

To change passwords for the versa and admin accounts:

1. Login to the shell on the node.
2. Issue the commands shown below.

```
admin@Analytics$ cd /opt/versa/scripts/van-security

admin@Analytics$ sudo ./analytics_securemode.sh -s
Do you want to change the shell login system password (y/N) : y
Please enter username: versa
versa exists... changing password.
New password: new-password
Retype new password: new-password
passwd: password updated successfully
```

```
Password is successfully changed for user: versa
```

```
admin@Analytics$ sudo ./analytics_securemode.sh -s
Do you want to change the shell login system password (y/N) : y
Please enter username:admin
admin exists... changing password.
New password: new-password
Retype new password: new-password
passwd: password updated successfully
Password is successfully changed for user: admin
```

Change Analytics Application UI Passwords

The default configuration for Analytics nodes includes two Analytics application accounts: admin and Administrator. To harden Analytics nodes, you must change the default passwords for these accounts on each of the analytics-type and search-type Analytics nodes. This protects the nodes from unauthorized user access, and is critical if Analytics nodes have public internet access.

If the user logs in as user Administrator to Analytics directly, and if Director is registered for authentication, then the login request is sent to Director. If Director fails, then the local database is used for authentication. If there is no Director registered, the local database is only used for authentication.

Note that you can find the default passwords in the `/opt/versa/var/van-app/properties/application.properties` file. You need root access to view this file.

To change the default passwords for the admin and Administrator accounts, perform the following procedure on each Analytics node:

1. Login to the shell.
2. Run the AdminManager.sh script, as follows:

```
admin@Analytics$ sudo /opt/versa/scripts/van-scripts/AdminManager.sh
Versa Analytics Admin Users Manager
Passwords for all local UI users need to be changed
Please enter password for user:admin
Password ?
Re-enter password ?
Please enter password for user:Administrator
Password ?
Re-enter password ?
Login credentials for all users have been changed, please do vsh restart for change to take effect.
```

3. Restart Analytics services.

```
admin@Analytics$ vsh restart
```

Change Tomcat Passwords

As part of Analytics hardening, you must change the Tomcat password and update certificates on each of the analytics-type and search-type Analytics nodes.

To change the Tomcat password and update certificates:

1. On the Analytics node, change to the `/opt/versa/scripts/van-security` directory:

```
| admin@Analytics$ cd /opt/versa/scripts/van-security
```

2. Run the `analytics_securemode.sh` script as shown below to modify the Tomcat password.

Note: When the script prompts "Do you want to change the Analytics UI local authentication administration password (y/N):", enter N if you changed the Analytics UI password in the [Change the Analytics Application UI Passwords](#) section, above. Otherwise, enter y to change the Analytics UI passwords now.

```
| admin@Analytics$ sudo ./analytics_securemode.sh -a
```

```
Info: Parsing van-security arguments
```

```
Info: modify-application-password
```

```
Do you want to change the Analytics UI local authentication administration password (y/N): N
```

```
Do you want to change the SSL and Tomcat Certificate passwords (y/N): y
```

```
Modifying Tomcat passwords ...
```

```
Change the Tomcat Password if your certificate passwords have changed
```

```
Please re-confirm (y/N): y
```

```
Enter NEW Password: new-password
```

```
ReEnter NEW Password: new-password
```

```
Modifying self-signed certificate passwords ...
```

```
Modifying Analytics-Director certificate passwords ...
```

```
This password should match the password in Director's vd-van-import-cert.sh file
```

```
Do you want to change the Analytics-Director certificate password (y/N): y
```

```
Enter NEW Password: new-password
```

```
ReEnter NEW Password: new-password
```

```
Please regenerate the certificates for this change to take effect
```

```
Regenerate certificate file using: van-import-cert.sh script
```

```
You will need to re-import certificates to Versa Director and re-register Director in Analytics
```

```
To ensure Analytics-Director communication certificates are changed with non-default passwords
```

```
Delete the TrustStore at: /opt/versa/var/van-app/certificates/versa_director_truststore.ts
```

```
Re-import by running: /opt/versa/scripts/van-scripts/van-vd-cert-install.sh
```

3. Delete the Analytics Java keystore file:

```
| admin@Analytics$ sudo rm /opt/versa/var/van-app/certificates/versa_analytics.jks
```

4. Delete the Director trust store file:

```
| admin@Analytics$ sudo rm /opt/versa/var/van-app/certificates/versa_director_truststore.ts
```


5. To use self-signed certificates, switch to the Director node and regenerate them (you can choose to back up the certificates):

```
admin@Director$ sudo rm /opt/versa/var/van-app/certificates/versa_analytics_client.*
admin@Director$ sudo /opt/versa/scripts/van-scripts/van-cert-install.sh
```

6. To use CA-signed certificates, re-import the certificates on the Analytics node:

```
admin@Analytics$ sudo /opt/versa/scripts/van-scripts/van-import-cert.sh \
--key path-to-private-key-file \
--cert path-to-signed-certificate-file \
--keypass certificate-password \
--cafile path-to-CA-certificate-file
```

7. On the Director node, copy the Director certificate to the Analytics cluster:

```
admin@Director$ cd /var/versa/vnms/data/certs
admin@Director$ scp versa_director_client.cer versa@analytics-node-ip:/opt/versa/var/van-app/
certificate
```

8. On the Analytics node, re-import the Director certificate:

```
admin@Analytics$ cd /opt/versa/var/van-app/certificates/
admin@Analytics$ sudo /opt/versa/scripts/van-scripts/van-vd-cert-install.sh versa_director_client.
cer director-hostname
```

Disable Analytics UI Access (Optional)

This is an optional step you can take to prevent users from directly accessing the Analytics UI. The procedure below redirects the URL normally used to access the Analytics UI so that it accesses the Director node instead.

Caution: Once you redirect the URL, it causes any attempts to login to the Analytics UI by scripts or API calls to fail.

To disable Analytics UI access:

1. Login to the shell of each of analytics-type and search-type node in the Analytics cluster.
2. Issue the following command to redirect the Analytics UI URL:

```
admin@Analytics$ sudo /opt/versa/scripts/van-security/analytics_securemode.sh -u
Info: Parsing van-security arguments
Info: enable/disable url-redirection
Do you want to enable/disable VAN UI URL redirection (y/N) : y
Do you want to enable or disable (e/d) : e
Please enter the complete director URL : https://versa-director-ip
Changed the URL to https://versa-director-ip successfully
```

3. Restart Analytics processes for the previous command to take effect.

```
admin@Analytics$ vsh restart
```

Disable Unused Kernel Modules

As part of Analytics hardening, you should disable the following unused Linux kernel modules to protect the device against the exploitation of any flaws in its implementation:

- DCCP—Datagram Congestion Control Protocol
- SCTP—Stream Control Transmission Protocol
- TDS—Tabular Data Stream protocol
- TIPC—Transparent Interprocess Communication protocol

To disable the unused kernel modules:

1. Edit the `/etc/modprobe.d/CIS.conf` file. Note that the file may not be present on the device.

```
| # sudo vi /etc/modprobe.d/CIS.conf
```

2. Add the following lines to the file. The `/bin/true` option disables the loading of the kernel module.

```
| install dccp /bin/true
| install sctp /bin/true
| install tds /bin/true
| install tipc /bin/true
```

3. Save the file.
4. Check that the modules have been disabled:

```
| # modprobe -n -v dccp
| install /bin/true
| # modprobe -n -v sctp
| install /bin/true
| # modprobe -n -v tds
| install /bin/true
| # modprobe -n -v tipc
| install /bin/true
```

Disable Promiscuous Mode

As part of Analytics hardening, you should disable promiscuous mode on the `eth0`, `eth1`, and `eth2` Ethernet interfaces.

To disable promiscuous mode:

1. Edit the `/etc/network/interfaces` file.

```
| $ sudo vi /etc/network/interfaces
```

2. Locate the line `"iface ethx inet static"`, and replace `x` with the interface number.
3. Add the line `"up ip link set ethx promisc off"` to the file, replacing `x` with the interface number.
4. Save the file.

5. Switch off promiscuous mode:

```
| $ sudo ip link ethx promisc off
```

The following shows an example of the modified `/etc/network/interfaces` file for the `eth1` interface:

```
auto eth1
iface eth1 inet static
up ip link set eth1 promisc off
address 192.168.0.10
netmask 255.255.255.0
mtu 1200
up route add -net 192.168.0.0 netmask 255.255.0.0 gw 192.168.0.239
up route add -net 10.0.0.0 netmask 255.255.0.0 gw 192.168.0.239
up route add -net 10.1.0.0 netmask 255.255.0.0 gw 192.168.0.239
up route add -net 10.2.0.0 netmask 255.255.0.0 gw 192.168.0.239
```

Harden SSH

Change the SSH Port

To change the default port that the SSH daemon listens on:

1. Change the default SSH port:

```
| $ sudo sed -i 's/22/1022/g' /etc/ssh/sshd_config
```

2. Restart the SSH service:

```
| $ sudo service ssh restart
```

Disable the SSH Server

As part of system hardening, you can optionally disable the SSH service on the Analytics node.

To disable the SSH server:

1. Stop the SSH daemon:

```
| $ sudo service ssh restart
```

2. Remove the SSH daemon from the `init.d` directory:

```
| $ sudo rm /etc/init.d/ssh
```

Harden the SSH Server Configuration

To have the SSH server on the Analytics node continue to run, set the following parameters:

1. Edit the `/etc/ssh/sshd_config` file and replace the following values:
 - `ClientAliveInterval`—300
 - `ClientAliveCountMax`—0
2. Save the file.
3. Restart the SSH daemon:

```
| $ sudo service ssh restart
```

Disable strongSwan

To disable the strongSwan VPN on the Analytics node:

1. Stop the StrongSwan service:

```
| $ sudo service strongswan stop > /dev/null 2>&1
```

2. Disable the service from starting when the Analytics node boots:

```
| $ update-rc.d -f strongswan remove > /dev/null 2>&1
```

Perform System Upgrades

When you perform a system upgrade, for example, if you upgrade from Release 16.1R2S9 to Release 16.1R2S10, do the following to keep the system hardened.

Before you upgrade an Analytics node:

- Back up the `/opt/versa/scripts/van-scripts/van-import-cert.sh` file.
- Back up the iptables rules:

```
| $ sudo iptables-save > iptables.rules
```

After you upgrade an Analytics node:

- Restore the `/opt/versa/scripts/van-scripts/van-import-cert.sh` file.
- If you are upgrading to Release 16.1R2SX, disable port 8080, as described in [Harden Port 4566](#).
- Reapply all the iptables rules.
- Rerun the `analytics_securemode.sh` —a script as described in [Change the Analytics Passwords](#). Note that changing the Analytics UI local authentication administration password is optional.

Configure IP Packet Filtering Rules

As part of hardening, you define IP packet filter rules for the Linux kernel firewall that allows or blocks traffic to the system. When a connection attempt is made through a port on the Analytics node, the Linux IP tables (iptables) facility searches for a match in its rule set. If no matching rule is found, the default action is taken. Configure iptables rules to block access by default, and then allow access only through required systems.

Note: The iptables rules must be configured even if an external firewall is configured.

Configure iptables Rules

To configure iptables rules:

1. Download the analytics_securemode.sh script to each of the Analytics nodes.
 - a. Backup the existing script.

```
admin@Analytics$ cd /opt/versa/scripts/van-security
admin@Analytics$ cp analytics_securemode.sh analytics_securemode.sh.bak
```
 - b. Download the latest version of analytics_securemode.sh from the following location:
<https://download.versa-networks.com/index.php/s/dVyHEx2tZIxNAGG>
 - c. Copy the downloaded script to /opt/versa/scripts/van-security/analytics_securemode.sh.
2. Configure iptables rules. The following table lists notable port numbers and the methods you use to configure rules for these ports.

Type of Port Access	Traffic Direction	Ports	Configuration Method
Analytics port for REST Access	Inbound/HTTPS	443/8443	Configured automatically when you run the analytics_securemode.sh script. See Install iptables Rules Using a Script , below. You can add additional IP subnets by specifying the whitelist file. See Configure an iptables Whitelist , below.
Inter-cluster database and client communication	Inbound/TCP	8983, 9042, 2181	Configured automatically when you run the analytics_securemode.sh script. See Install iptables Rules Using a Script , below.
REST access port configuration and diagnostics of various	Inbound/TCP	5000, 5010, 5020, 8008	Configured automatically when you run the analytics_securemode.sh script. See Install iptables Rules Using a Script , below.

Type of Port Access	Traffic Direction	Ports	Configuration Method
services running on Analytics nodes			Rules Using a Script , below.
Log collector port where logs are received	Inbound/TCP	User configurable	<p>Configure explicitly for each of the local collector on each Analytics node that collects logs. For example, if the local collector is configured to listen on port 1234, add the following iptables command.</p> <pre>\$ sudo iptables -A INPUT -p tcp -m tcp --dport 1234 -j ACCEPT</pre>
Monitoring agent ports to retrieve health status and statistics about Analytics nodes	Inbound/HTTP	8010, 8020	<p>If headend monitoring agents nodemon and vanner are enabled on Analytics nodes, add iptables rules to allow traffic coming from their source IP addresses and ports.</p> <p>For example:</p> <pre>\$ sudo iptables -A INPUT -s <versa-monitoring-server>/32 \ -p tcp --dport 8010 -j ACCEPT \$ sudo iptables -A INPUT -s <versa-monitoring-server>/32 \ -p tcp --dport 8020 -j ACCEPT \$ sudo iptables -A INPUT -p tcp --dport 8010 -j REJECT \$ sudo iptables -A INPUT -p tcp --dport 8020 -j REJECT</pre>
Standard SSH	Inbound/TCP	22	<p>Add iptables rules to allow SSH access to the nodes. It is recommended that you allow only Versa Director IP addresses.</p> <p>For example:</p> <pre>\$ sudo iptables -A INPUT -s <versa-director-ip>/32 -p tcp \ --dport 22 -j ACCEPT \$ sudo iptables -A INPUT -p tcp --dport 22 -j REJECT</pre>

Type of Port Access	Traffic Direction	Ports	Configuration Method
Standard NTP, for time synchronization	Inbound/UDP	123	Add iptables rules to allow NTP port access to the host. For example: <pre>\$ sudo iptables -A INPUT -p udp --dport 123 -j ACCEPT</pre>
Default access (drop other access)			Issue the following commands to drop all other access to the host. default. <pre>\$ sudo iptables -A INPUT -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT \$ sudo iptables -P OUTPUT ACCEPT \$ sudo iptables -P FORWARD DROP \$ sudo iptables -P INPUT DROP</pre>

3. Issue the following command so that the rules persist when you reboot the system.

```
admin@Analytics$ vsh restart
```

4. To display the updated iptables rules, issue the following command.

```
admin@Analytics$ sudo iptables -L
```

Install iptables Rules Using a Script

You can configure many iptables rules using the `analytics_securemode.sh` script. Each time you issue the `analytics_securemode.sh -i enable` command, it sets up rules for inter-cluster access and management (UI) access. For inter-cluster access, the script determines the subnet automatically and adds it to the allow list. For management access, the script determines the subnet from the `/opt/versa/scripts/van-scripts/vansetup.conf` file. The script allows Analytics application port access to Versa Director and Analytics nodes only.

The script adds iptables entries for the following port numbers:

- 8983 (Solr)
- 9042 (Cassandra)
- 2181 (Zookeeper)
- 5000, 5010, 5020, 8008 (Versa)
- 443, 8443 (Analytics Application)

The script can also configure access for additional IP addresses and subnets. To do this, the script automatically

searches for entries in the `/opt/versa/etc/WHITELIST` file. If the file does not exist, the script prompts you to enter the IP addresses and subnets manually.

To configure iptables rules:

1. Login to a shell on the Analytics node.
2. Ensure that you have download the latest version of `analytics_securemode.sh` as described in Step 1 of [Configure IP Table Rules](#).
3. Change to the `/opt/versa/scripts/van-security` directory.

```
| admin@Analytics$ cd /opt/versa/scripts/van-security
```

4. Run the `analytics_securemode.sh` script.
 - To run the script and enter additional allowed IP addresses and subnets interactively:

Ensure that no `/opt/versa/etc/WHITELIST` file exists, and then run the script as follows.

```
| admin@Analytics$ sudo ./analytics_securemode.sh -i enable

(output omitted for brevity)

Info: Please add comma separated subnets/IP eg: 1.1.1.1, 10.10.10.0/24
==> Please enter subnets/IP (or ENTER if none): 10.10.10.0, 10.20.20.0/24
Info: These are the IP ranges/IP to whitelist for inter-cluster localhost.localhost.localhost.0/24 10.10.10.0/24 10.20.20.0/24 127.0.0.1
==> Do you want to proceed? (y/N)? y

(output omitted for brevity)

Info: Please add comma separated subnets/IP eg: 1.1.1.1, 10.10.10.0/24
==> Please enter subnets/IP (hit ENTER if none): 2.2.2.2, 1.1.1.1
Info: These are the IP ranges/IP to whitelist for UI access 127.0.0.1 localhost.localhost.localhost.0/24 2.2.2.2 1.1.1.1
==> Do you want to proceed? (y/N)? y

(output omitted for brevity)

admin@Analytics$ vsh restart
```

- To run the script using a whitelist file:
 - a. Add entries to the `/opt/versa/etc/WHITELIST` file. For access between Analytics clusters, you add entries in the section labeled `INTERNAL`. For management access, you add additional IP addresses and/or subnets in the section labeled `MANAGEMENT`.

For example, the following white list file adds subnets `10.10.10.0/24` and `10.20.20.0/24` in the allowed sources list for inter-cluster access. This can be used for additional collector subnets. Additionally, `2.2.2.2` and `1.1.1.1` are added to allow source IP addresses for management access.

```
| admin@Analytics$ cat /opt/versa/etc/WHITELIST
```


INTERNAL: 10.10.10.10, 10.20.20.1/24
MANAGEMENT: 2.2.2.2, 1.1.1.1

b. Run the script as follows.

```
admin@Analytics$ sudo ./analytics_securemode.sh -i enable
Info: Parsing van-security arguments
Info: Setup iptable rules
Info: Determined 192.168.1.0/24 to be the VAN inter-cluster subnet, Will add 192.168.1.0/24 to
inter-cluster whitelistInfo: Determined 10.40.93.0/24 to be the VAN management subnet, Will
add 10.40.93.0/24 to MGMT whitelist
Info: Reading arguments from /opt/versa/etc/WHITELIST for iptables rules. If you want to make
changes, pls edit the file or
remove the file for interactive mode
Info: These are the IP ranges/IP to whitelist for inter-cluster communication 192.168.1.0/24 127.
0.0.1 10.10.10.0/24 10.20.20.0/24

(output omitted for brevity)

Info: These are the IP ranges/IP to whitelist for management communication 2.2.2.2 1.1.1.1 127.
0.0.1 192.168.1.0/24 10.40.93.0/24

(output omitted for brevity)

Info: You can check the rules by executing 'sudo iptables -L' on the shell

admin@Analytics$ vsh restart
```

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

[Perform Manual Hardening for Versa Branches, Controllers, and Hubs](#)

[Perform Manual Hardening for Versa Director](#)

[Use OS Security Packages](#)

[Use Security Packages](#)