

Software Vulnerability Manager 2019 Virtual Appliance

Installation Guide

Legal Information

Book Name: Part Number: Software Vulnerability Manager 2019 Virtual Appliance Installation Guide

Product Release Date:

SVM-7300-VAIG02 July 2019

Copyright Notice

Copyright © 2019 Flexera

This publication contains proprietary and confidential information and creative works owned by Flexera and its licensors, if any. Any use, copying, publication, distribution, display, modification, or transmission of such publication in whole or in part in any form or by any means without the prior express written permission of Flexera is strictly prohibited. Except where expressly provided by Flexera in writing, possession of this publication shall not be construed to confer any license or rights under any Flexera intellectual property rights, whether by estoppel, implication, or otherwise.

All copies of the technology and related information, if allowed by Flexera, must display this notice of copyright and ownership in full.

Intellectual Property

For a list of trademarks and patents that are owned by Flexera, see https://www.flexera.com/producer/company/about/intellectual-property/. All other brand and product names mentioned in Flexera products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

Restricted Rights Legend

The Software is commercial computer software. If the user or licensee of the Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Software was developed fully at private expense. All other use is prohibited.

1 Contents

2	Software Vulnerability Manager 2019 Virtual Appliance Installation Guide	5
	Legal Information	7
	Using Help	8
	Contacting Us	8
3	Installing Software Vulnerability Manager Ubuntu OS	9
	Initial Configuration	10
	Configure Your Console Data	11
	Configure Your Time Zone Data	11
	Change Your Administrator Password	12
	Network Configuration	12
	Automatic (DHCP) Network Configuration	13
	Manual (Static) Network Connection	13
	Do Nothing	14
	Customer Information	14
	Server Configuration	14
	Create Server Certificate	15
	Disk Initialization	16
	Database Configuration	16
	Configure Your Maria DB Server (Optional)	17
	Proxy Configuration	17
	Email and SMS Settings	18
	Software Updates	18
	LDAP Configuration	19
4	Installing Software Vulnerability Manager CentOS	21
	Initial Configuration	22
	Configure Your Time Zone	22

Α

Configure Your keyboard Layout	
Configure Your System Language	
Change Your Administrator Password	
Network Configuration	
Automatic (DHCP) Network Configuration	
Manual (Static) Network Connection	
Do Nothing	
Customer Information	27
Server Configuration	
Create Server Certificate	
Disk Initialization	29
Database Configuration	29
Proxy Configuration	
Email and SMS Settings	
Software Updates	
LDAP Configuration	32
Appendix A - CentOS VA migration from Ubuntu VA	33
Actions on Ubuntu Vitrual Appliance	
Actions on ContOS Virtual Appliance	
Actions on Centos virtual Appliance	
Migration Steps	

Software Vulnerability Manager 2019 Virtual Appliance Installation Guide

Software Vulnerability Manager 2019 Virtual Appliance

Software Vulnerability Manager is a revolutionary tool that simplifies the troublesome area of identifying vulnerable programs and patching them.

Software Vulnerability Manager Virtual Appliance provides you with an easy way to deploy and configure Software Vulnerability Manager without the need install and configure a Linux server from scratch. The VA is designed to be easy to deploy and require minimal maintenance.

If the appliance is based on Ubuntu Server LTS 14.04 then requires VMware vSphere 5.0+ with vSphere Client to deploy and run the Virtual Appliance. Deployment on VMWare and ESX is also supported.

If the appliance is based on CentOS, deployment on VMWare and HyperV virtualization platforms is also supported.

By scanning the network, organizations can effectively protect their corporate IT infrastructure against the threat posed by unpatched vulnerabilities:

- Non-intrusive authenticated vulnerability and patch scanning
- Covers programs and plug-ins from thousands of vendors
- Unprecedented accuracy, no more false positives
- Reports security status for each program
- Reports criticality rating for each insecure program
- Reports end-of-life programs
- Identifies missing patches
- Automated patch repackaging
- Integration with WSUS for easy patch distribution

• Integration with System Center Configuration Manager for extensive patch management

Table 2-1 • Software Vulnerability Manager On-Premises Edition Virtual Appliance Installation Guide

Торіс	Content
Installing Software	The following topics appear in the order that they appear in the installation procedure.
Vulnerability Manager Ubuntu OS	Initial Configuration
	Network Configuration
	Customer Information
	Server Configuration
	Disk Initialization
	Database Configuration
	Configure Your Maria DB Server (Optional)
	Proxy Configuration
	Email and SMS Settings
	Software Updates
	LDAP Configuration
Installing Software	The following topics appear in the order that they appear in the installation procedure.
Vulnerability Manager	Initial Configuration
	Network Configuration
	Customer Information
	Server Configuration
	Disk Initialization
	Database Configuration
	Proxy Configuration
	Email and SMS Settings
	Software Updates
	LDAP Configuration

Table 2-1 • Software Vulnerability	Manager On-Premises Edition	Virtual Appliance Installation Guide
------------------------------------	-----------------------------	--------------------------------------

Software Vulnerability Manager.

Торіс	Content
Appendix A - CentOS VA	Explains Migration from Ubuntu Virtual Appliance to CentOS Virtual Appliance
migration from Ubuntu VA	Actions on Ubuntu Vitrual Appliance
	Actions on CentOS Virtual Appliance
	Migration Steps
	Note • Flexera highly recommends to use the CentOS Virtual Appliance to deploy the

Legal Information

Software Vulnerability Manager 2019 Virtual Appliance

Copyright Notice

Copyright © 2019 Flexera.

This publication contains proprietary and confidential information and creative works owned by Flexera and its licensors, if any. Any use, copying, publication, distribution, display, modification, or transmission of such publication in whole or in part in any form or by any means without the prior express written permission of Flexera is strictly prohibited. Except where expressly provided by Flexera in writing, possession of this publication shall not be construed to confer any license or rights under any Flexera intellectual property rights, whether by estoppel, implication, or otherwise.

All copies of the technology and related information, if allowed by Flexera, must display this notice of copyright and ownership in full.

Intellectual Property

For a list of trademarks and patents that are owned by Flexera, see https://www.flexera.com/producer/company/about/ intellectual-property. All other brand and product names mentioned in Flexera products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

Restricted Rights Legend

The Software is commercial computer software. If the user or licensee of the Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Software was developed fully at private expense. All other use is prohibited.

Using Help

Help is available from the [ProductName] interface help icon located at the top right of the screen or click the fields labeled with a "(?)" to access the contextual help.

Online Help

For online help, see https://helpnet.flexerasoftware.com/csionprem/Default.htm

Release Notes

For the latest product release notes, see https://helpnet.flexerasoftware.com/ ?product=Software%20Vulnerability%20Manager%202018%20On-Premises%20Edition&version=2018

For earlier product release notes, see https://helpnet.flexerasoftware.com/ ?product=Software%20Vulnerability%20Manager%202018%20On-Premises%20Edition&version=Previous

Contacting Us

Software Vulnerability Manager 2019 Virtual Appliance

Flexera is headquartered in Itasca, Illinois, and has offices worldwide. To contact us or to learn more about our products, visit our website at: https://www.flexera.com/

Product Feedback

Have a suggestion for how we can improve this product? Please come share direct feedback with the product team and vote on ideas submitted by other users in our online community at: Customer Community feedback page for Software Vulnerability Manager.

Installing Software Vulnerability Manager Ubuntu OS

Software Vulnerability Manager 2019 Virtual Appliance

The following steps appear in the order that they appear in the installation procedure. You can use the arrow and Page Up/ Down keys to navigate, press ESC to go back or F2 to open an administrator shell.

- Initial Configuration
- Network Configuration
- Customer Information
- Server Configuration
- Disk Initialization
- Database Configuration
- Configure Your Maria DB Server (Optional)
- Proxy Configuration
- Email and SMS Settings
- Software Updates
- LDAP Configuration



0

Important • Note the below following recommendations on Virtual Appliance:

- Flexera highly recommends to use the CentOS Virtual Appliance to deploy the Software Vulnerability Manager.
- To migrate from the Ubuntu Virtual Applicance to the CentOS Virtual Appliance, see Appendix A CentOS VA migration from Ubuntu VA

Initial Configuration

Software Vulnerability Manager 2019 Virtual Appliance

To start the configuration, login to your Software Vulnerability Manager server as root and enter the default password (flexera).



The Initial Configuration screen will appear. Click **Begin** to start configuring the Software Vulnerability Manager Virtual Appliance for the following.

- Configure Your Console Data
- Configure Your Time Zone Data
- Change Your Administrator Password



Configure Your Console Data

Software Vulnerability Manager 2019 Virtual Appliance

Select the policy you want to use for handling keymaps and click **OK**.



Configure Your Time Zone Data

Software Vulnerability Manager 2019 Virtual Appliance

Select you geographic area from the list and click **OK**. You will then be presented with a list of cities representing the time zones in which they are located.

Please select the geographic area in narrow this down by presenting a lis are located. Geographic area:	Configuring tzdata n which you live. Subsequent configuration questions will st of cities, representing the time zones in which they
	Africa America Antarctica Australia Arctic Ocean Asia Atlantic Ocean Europe Indian Ocean Pacific Ocean System V timezones US Nome of the above
<0k>	<cancel></cancel>

Change Your Administrator Password

Software Vulnerability Manager 2019 Virtual Appliance

Enter and confirm a new root account password for the Ubuntu Linux install on the VA and click Next.

Change Administrator	r Password
New password: <mark>********</mark> Confirm password: <mark>********</mark>	
Previous	Next

Network Configuration

Software Vulnerability Manager 2019 Virtual Appliance

Choose the network configuration method to use and click **Next** to configure the following.

- Automatic (DHCP) Network Configuration
- Manual (Static) Network Connection
- Do Nothing



Automatic (DHCP) Network Configuration

Software Vulnerability Manager 2019 Virtual Appliance

If you selected Automatic (DCHP) in the previous step no further action is required.

Manual (Static) Network Connection

Software Vulnerability Manager 2019 Virtual Appliance

If you selected Manual (static) in the previous step you must enter the required details and click Save.



Do Nothing

Software Vulnerability Manager 2019 Virtual Appliance

If you selected **Do nothing** in the previous step no further action is required.

Customer Information

Software Vulnerability Manager 2019 Virtual Appliance

Enter the name of your company, your Customer ID number that was supplied by Flexera and click Save.

Customer Information Company name: Customer ID: 1	
Previous	

Server Configuration

Software Vulnerability Manager 2019 Virtual Appliance

Enter your Server Address, which can be a fully qualified domain name or an IP address, and click **Next** to Create Server Certificate.

Г			Ъ
ŀ	-	-	-
Ľ			
L			

Note • This needs to match the URL that will be used to access the server via HTTP/HTTPS.



Create Server Certificate

Software Vulnerability Manager 2019 Virtual Appliance

Enter your Domain Name, Company Name, Administration Email and Certificate Validity (years) and click **Create Certificate**.

This generates a self-signed certificate. It is necessary to distribute the certificate to all hosts running the UI, System Center Plugin, Daemon and agents. Currently the public certificate can be recovered either by copying it from inside the VA (it is saved as /etc/csi/) or by exporting it from Internet Explorer.



Disk Initialization

Software Vulnerability Manager 2019 Virtual Appliance

Click **Initialize Disks** to partition your drives to ensure that you have enough disk space for the Software Vulnerability Manager Virtual Appliance.

When completed, click **Next**.

Device Size Mount Point Status Noot /dev/sda 100.0 GiB / Mounted Database /dev/sdc 50.0 GiB /var/lib/mysql Uninitialized Spool /dev/sdd 50.0 GiB /var/spool/csi Uninitialized Suap /dev/sdb 4.0 GiB none Uninitialized. System disks need to be initialized. This operation will be performed only once. Initialize Disks			Di	sk Initialization		
System disks need to be initialized. This operation will be performed only once. Previous	Root Database Spool Swap	Device /dev/sda /dev/sdc /dev/sdd /dev/sdb	Size 100.0 GiB 50.0 GiB 50.0 GiB 4.0 GiB	Mount Point / /var/lib/mysql /var/spool/csi none	<mark>Status</mark> Mounted Uninitialized Uninitialized Uninitialized	
Previous Initialize Disks		Syst This	tem disks ne s operation	ed to be initiali: will be performed	zed. only once.	
		Previous			Initialize Disks	

Database Configuration

Software Vulnerability Manager 2019 Virtual Appliance

Enter the Host, Username and Password details and then click Next.

Database Configuration	
Host: localhost Username: root Password: *******	
Back	

Configure Your Maria DB Server (Optional)

Software Vulnerability Manager 2019 Virtual Appliance

Enter a new password for your MariaDB administrative root server (optional) and click **OK**. You will be asked to repeat the password.

When completed, click **Ok**.

Configuring mariadb-server-5.5 While not mandatory, it is highly recommended that you set a password for the MariaDB administrative "root" user. If this field is left blank, the password will not be changed. New password for the MariaDB "root" user:
<0k>

Proxy Configuration

Software Vulnerability Manager 2019 Virtual Appliance

If your network uses a proxy to connect to the Internet, you can select **Use Proxy**, enter the Host, Port, Username and Password details and then click **Next**.

Proxy Configuration
Use Proxy: []
Host: Port: Username: Password:
Previous

Email and SMS Settings

Software Vulnerability Manager 2019 Virtual Appliance

Enter the Email and SMS notification details and click Next.

Email	and SMS Settings
Reply Email: No-reply Email: SMTP Relay Server:	admin@192.168.36.231 no-reply@192.168.36.231
SMS Notifications:	
Previous	Next

Software Updates

Software Vulnerability Manager 2019 Virtual Appliance

Enable automatic software updates to check for, and install, security updates on a daily basis.



You will be informed of all available security updates and given the option to Update now or Skip them.



LDAP Configuration

Software Vulnerability Manager 2019 Virtual Appliance

Before configuring LDAP support you will need the following:

- The LDAP URL for your LDAP server
- The Base DN for the point in the directory where user-lookups will be made (the Base DN must contain at least one user account)
- The LDAP UID attribute that the usernames will be compared to
- The Bind DN for user-lookups or, alternatively, existing support for anonymous bind lookups

Select Use LDAP, enter the LDAP Host URL, LDAP Base DN, UID Attribute, and Bind details and then click Save.

LDAP Configuration	
Use LDAP: []]	
LDAP Host URL: LDAP Base DN: UID Attribute:	
Anonymous Bind: [*] Bind DN: Bind Password:	
Back	

Chapter 3 Installing Software Vulnerability Manager Ubuntu OS

LDAP Configuration

Installing Software Vulnerability Manager CentOS

Software Vulnerability Manager 2019 Virtual Appliance

The following steps appear in the order that they appear in the installation procedure. You can use the arrow and Page Up/ Down keys to navigate, press ESC to go back or F2 to open an administrator shell.

- Initial Configuration
- Network Configuration
- Customer Information
- Server Configuration
- Disk Initialization
- Database Configuration
- Proxy Configuration
- Email and SMS Settings
- Software Updates
- LDAP Configuration

Software Vulnerability Manager

Network Configuration Customer Information Server Configuration Proxy Settings Database Settings Email and SMS Settings LDAP Settings

Change Time Zone Change Keyboard Layout Change System Language Change Administrator Password Disk Management Software Updates Open Administrator Shell

Exit

Initial Configuration

Software Vulnerability Manager 2019 Virtual Appliance

To start the configuration, login to your Software Vulnerability Manager 2019 server as root and enter the default password (flexera).



The Initial Configuration screen will appear. Click **Begin** to start configuring the Software Vulnerability Manager 2019 Virtual Appliance for the following.

- Configure Your Time Zone
- Configure Your keyboard Layout
- Configure Your System Language



Configure Your Time Zone

Software Vulnerability Manager 2019 Virtual Appliance

Select your time zone from the list and click Save

Time Zone Locale
Pacific/Majuro
Pacific/Marquesas
Pacific/Midway
Pacific/Nauru
Pacif ic/Niue
Pacific/Norfolk
Pacific/Noumea
Pacific/Pago_Pago
Pacif ic/Palau
Pacific/Pitcairn
Pacif ic/Pohnpei
Pacific/Port_Moresby
Pacific/Rarotonga
Pacif ic/Saipan
Pacific/Tahiti
Pacific/Tarawa
Pacif ic/Tongatapu
Pacific/Wake
Pacific/Wallis
UTC
Save Back

Configure Your keyboard Layout

Software Vulnerability Manager 2019 Virtual Appliance

Select your keyboard layout from the list and click Save.

Keyboard Layout	
<pre>tr_q-latin5 tralt trf trf trf-fgGIod trq ttwin_alt-UTF-8 ttwin_cplk-UTF-8 ttwin_ct_sh-UTF-8 ttwin_ctrl-UTF-8 tw tw-indigenous tw-saisiyat ua ua-cp1251 ua-utf ua-utf ua-utf-ws ua-ws uk unicode</pre>	
Bau	ck

Configure Your System Language

Software Vulnerability Manager 2019 Virtual Appliance

Select your system language from the list and click Save.

	System	Language	
17. 000	0450		
en_IE.180885	915@eur	' 0	
en_IL.utf8			
en_ILveuro			
en_In.utro			
en_NG utf8			
en_{NZ}			
$m_{\rm NZ} = 12088$	91		
en N7 utf8	,,,,		
en PH			
en PH, iso885	591		
en PH.utf8			
en SG			
en SG.iso885	591		
en_SG.utf8			
en_US			
en_US.iso885	591		
en_US.iso885	i915		
en_US.utf8			
Save		Be	ack
	-		

Change Your Administrator Password

Software Vulnerability Manager 2019 Virtual Appliance

Enter and confirm a new root account password for the CentOS Linux install on the Virtual Appliance and click Next.



Network Configuration

Software Vulnerability Manager 2019 Virtual Appliance

Choose the network configuration method to use and click Next to configure the following.

- Automatic (DHCP) Network Configuration
- Manual (Static) Network Connection
- Do Nothing



Note • To select any network configuration method, use Space Bar in the key board

Automatic (DHCP) Network Configuration

Software Vulnerability Manager 2019 Virtual Appliance

If you selected Automatic (DCHP) in the previous step no further action is required.

Manual (Static) Network Connection

Software Vulnerability Manager 2019 Virtual Appliance

If you selected Manual (static) in the previous step you must enter the required details and click Save.

Static Netwo	rk Configuration
IP address: Netmask: Gateway: Search domain(s): Nameserver(s):	
Back	Save

Do Nothing

Software Vulnerability Manager 2019 Virtual Appliance

If you selected **Do nothing** in the previous step no further action is required.

Customer Information

Software Vulnerability Manager 2019 Virtual Appliance

Enter the name of your company, your Customer ID number that was supplied by Flexera and click Save.

	Customer Information Company name: Customer ID: 1
Previous	Previous Next

Server Configuration

Software Vulnerability Manager 2019 Virtual Appliance

Enter your Server Address, which can be a fully qualified domain name or an IP address, and click **Next** to Create Server Certificate.

Note • This needs to match the URL that will be used to access the server via HTTP/HTTPS.

Server Configuration
l berver com igaración
Senier Address: 10.80,130,22
001 V01 (http://doi.org/10.00.130.00
Server address can be a fully qualified
domain name or an IP address
Previous

Create Server Certificate

Software Vulnerability Manager 2019 Virtual Appliance

Enter your Domain Name, Company Name, Administration Email and Certificate Validity (years) and click **Create Certificate**.

This generates a self-signed certificate. It is necessary to distribute the certificate to all hosts running the UI, System Center Plugin, Daemon and agents. Currently the public certificate can be recovered either by copying it from inside the Virtual Appliance (it is saved as /etc/csi/) or by exporting it from Internet Explorer.

Create Server (Certificate
Domain Name: Company Name: Administrative Email: Certificate Validity (years): Certificate passphrase (optional):	10.80.130.22 Flexera admin@ 10
Back	Create Certificate

Disk Initialization

Software Vulnerability Manager 2019 Virtual Appliance

Click **Initialize Disks** to partition your drives to ensure that you have enough disk space for the Software Vulnerability Manager 2019 Virtual Appliance.

When completed, click **Next**.

Spool /dev/mappe 121.0 GiB /var/spool/csi Mounted Swap /dev/sda3 49.0 GiB none Mounted	Root Database Spool Swap	Device /dev/sda /dev/mappe /dev/mappe /dev/sda3	Size 500.0 GiB 120.0 GiB 121.0 GiB 49.0 GiB	Mount Point / /var/lib/mysql /var/spool/csi none Next	Status Mounted Mounted Mounted Mounted	
---	-----------------------------------	---	---	---	--	--

Database Configuration

Software Vulnerability Manager 2019 Virtual Appliance

Enter the Host, Username and Password details and then click Next.

Datab	ase Configuration
Host:	loca lhost
Username:	root
Password:	
Confirm Password:	
Previous	Next

Proxy Configuration

Software Vulnerability Manager 2019 Virtual Appliance

If your network uses a proxy to connect to the Internet, you can select **Use Proxy**, enter the Host, Port, Username and Password details and then click **Next**.

Proxy Configuration
Use Proxy: []]
Host: Port: Username: Password:
Previous

Email and SMS Settings

Software Vulnerability Manager 2019 Virtual Appliance

Enter the Email and SMS notification details and click Next.



Software Updates

Software Vulnerability Manager 2019 Virtual Appliance

Enable automatic software updates to check for, and install, security updates on a daily basis.



Enter the RPM Server User Name and Password, click Download and install latest RPM to install the latest updates.



LDAP Configuration

Software Vulnerability Manager 2019 Virtual Appliance

Before configuring LDAP support you will need the following:

- The LDAP URL for your LDAP server
- The Base DN for the point in the directory where user-lookups will be made (the Base DN must contain at least one user account)
- The LDAP UID attribute that the usernames will be compared to
- The Bind DN for user-lookups or, alternatively, existing support for anonymous bind lookups

Select Use LDAP, enter the LDAP Host URL, LDAP Base DN, UID Attribute, and Bind details and then click Save.

LDAP Configuration	
Use LDAP:	
LDAP Host URL: LDAP Base DN: UID Attribute:	
Anonymous Bind: Bind DN: Bind Password:	[*]
Previous	Next



Appendix A - CentOS VA migration from Ubuntu VA

Software Vulnerability Manager 2019 Virtual Appliance

Migration from Ubuntu Virtual Appliance to CentOS Virtual Appliance includes the following steps:

- Actions on Ubuntu Vitrual Appliance
- Actions on CentOS Virtual Appliance
- Migration Steps



Important • Before starting the migration, make sure the vuln_track database is synced.

Actions on Ubuntu Vitrual Appliance

Software Vulnerability Manager 2019 Virtual Appliance

To migrate to the CentOS Virtual Appliance, follow the below preparatory steps in Ubuntu Virtual Appliance:

• Create admin migration user using the below command:

GRANT ALL PRIVILEGES ON *.* TO 'mig_admin'@'%' IDENTIFIED BY 'MIG_ADMIN' WITH GRANT OPTION;

FLUSH PRIVILEGES;

• Stop the services using the below commands:

service scandaemon stop

service sgdaemon stop

service haproxy stop

Connect to the database and truncate nsi_result table from all the private databases for fast completion:

TRUNCATE ca_<custid>.nsi_result;(delete from all partitions).

TRUNCATE ca.scan_queue; (Ideally no entries, when scan is not pending)

- Check for enough disk space, tmp space, free RAM before proceeding.
- Make sure that **Apache** service is running in both the servers.

Actions on CentOS Virtual Appliance

Software Vulnerability Manager 2019 Virtual Appliance

To migrate from the Ubuntu Virtual Appliance, follow the below preparatory steps in CentOS Virtual Appliance:

Create admin migration user using the below commands:

GRANT ALL PRIVILEGES ON *.* TO 'mig_admin'@'%' IDENTIFIED BY 'MIG_ADMIN' WITH GRANT OPTION; FLUSH PRIVILEGES;

Add the below entries in /etc/my.cnf to [mysqld] section and restart MariaDB server to apply the new settings:

net_read_timeout=1000

connect_timeout=1000

On terminal: systemctl restart mariadb.service

Using the below command, try connecting to Ubuntu VA using mig_admin user from the new CentOS VA:

mysql -umig_admin -pMIG_ADMIN -h<ubuntu VA IP>

• Using the below command, try connecting to CentOS VA from Ubuntu VA:

mysql -umig_admin -pMIG_ADMIN -h<Centos VA IP>



Note • Make sure both the servers can connect each other, if any issue found in MySQL connection then check /etc/mysql/ my.cnf file and comment # bind-address 127.0.0.0 (or) change the bind address to 0.0.0.0.

• Stop the services, using the below commands:

systemctl stop sgdaemon.service

systemctl stop scandaemon.service

systemctl stop haproxy.service

Drop the common and private databases (Centos VA) using the below commands:

DROP DATABASE ca;

DROP DATABASE ca_; (Private database starts with ca_)

Drop the private db mysql users (which starts with customer id) using the below commands:

DROP USER '<cust_id*>'@'localhost'

FLUSH PRIVILEGES;

Migration Steps

Software Vulnerability Manager 2019 Virtual Appliance

After successfully creating the **admin migration user**, follow the below migration steps:

• In CentOS VA make the following files executable:

chmod +x /usr/local/Secunia/csi/install/util/migratedb.sh

chmod +x /usr/local/Secunia/csi/install/util/dumpPDB.php

• In CentOS VA run the below script:

/usr/local/Secunia/csi/install/util/migratedb.sh

• After running the script, you can see a log folder get created at **/usr/local/Secunia/csi/install/util/** with the migration successful message. If a log folder is not created then you need to verify the permission of **dumpPDB.php**, **migratedb.sh** files. Now run the below script:

/usr/local/Secunia/csi/install/util/migratedb.sh

Script will ask for the below details of source server (Ubuntu) and destination server (CentOS):

Source IP

Source MySQL username

Source MySQL password

Destination IP

Destination MySQL username

Destination MySQL password

- In Ubuntu VA, run the below commands for permission and to copy the previously generated reports (pdf & csv):
 - On CentOS Chmod a+rwx /usr/local/Secunia/csi/reports
 - On Ubuntu scp /usr/local/Secunia/csi/reports/ root@<centos ip>:/var/spool/On centoscsi/reports/*.*
- Start services using the below commands:

systemctl start sgdaemon.service

systemctl start scandaemon.service

systemctl start haproxy.service

• After migration, remove mysql user - 'mig_admin'@'%' from both the servers using the below commands:

DROP USER 'mig_admin'@'%'; FLUSH PRIVILEGES; Chapter A Appendix A - CentOS VA migration from Ubuntu VA Migration Steps