VMware Smart Assurance Network Configuration Manager Security Configuration Guide

VMware Smart Assurance 10.1.4

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Overview

1

This document describes the user authorization security policy for VMware Smart Assurance Network Configuration Manager and introduces concepts and principles used in the implementation of the authorization features.

Terminology

2

To clarify the terminology used within this document, a Principal represents both a User and a Group.

A Group is a container or a composite entity comprised of Principals as its members. For example, a group can be comprised of users and groups, with the exception of recursive group membership.

A Principal can be a member of multiple groups, at the same time.

Security enhancements

3

This chapters provides information on security enhancments in Network Communication Manager.

The following 3rd party components are upgraded for Network Communication Manager 10.1.4, to address multiple security vulnerabilities:

- Postgress is upgraded to 13.1.
- Spring-framework is upgraded to 5.3.1.
- Spring-Security is upgraded to 5.4.1.
- BouncyCastle is upgraded to 1.68.
- Jackson-databind is upgraded to 2.11.4.

Following Security Enhancements and Hardening issues has been addressed as part of NCM 10.1.4 release:

- Cross-site scripting issue is reported in setupmgr.

Following Security Enhancements and Hardening issues has been addressed as part of NCM 10.1.3 release:

- Cross-Frame scripting issue is reported for setupmgr in Device Server.
- Cross-Frame scripting issue in Report Advisor web page when launched using port 8443
- Cross-Site Scripting is reported in SysAdmin for the ServerPath field

Following Security Enhancements and Hardening issues has been addressed as part of NCM 10.1.1 release:

- Cross Site Scripting issues addressed for the following URLs in SysAdmin Console web page:

  `/SysAdmin/console/ServerUtilization.jsp?serverName=<ServerName>`

  `/SysAdmin/console/ServiceDetails.jsp?serverName=<ServerName>&serviceName=<ServiceName>`

  `/SysAdmin/console/SaveNotificationSetup.jsp [emails parameter]`
- NCM 10.1.1.0 enforces an additional security constraint to use a minimum of 15-character password length (STIG V-69555).

- PostgreSQL STIG hardening issues has been addressed in NCM. For more information refer, PostgreSQL STIG Hardening Fixed Issues in 10.1.1.

Following Security Enhancements and Hardening issues has been addressed as part of 10.1.0 release:

- TLS 1.1 and TLS 1.0 protocols has been disabled and only TLS 1.2 protocol has been enabled in NCM. Also all the Low cipher suites including RC4, DES and 3DES has been disabled.

```
SSLProtocol="-TLSv1-TLSv1.1+TLSv1.2"
SSLCipherSuite="RSA:!EXP:!NULL:+HIGH:+MEDIUM:-LOW:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!
KRB5:!aECDH:!EDH:!3DES"
```

- The http access to SysAdmin Console has been disabled and all the http requests are redirected to https.

```
http://<NCM_IP>:8080/SysAdmin URL is redirected to https://<NCM_IP>:8443/SysAdmin
```

- Apache Tomcat and Apache http server has been hardened to address some of the security issues related to Cross Site scripting, Cross Frame scripting and Strict transport security in NCM.
- The directory listing has been disabled for the following URLs:

  https://<NCM_IP>:443/cgi-bin/

  https://<NCM_IP>:443/icons/

  https://<NCM_IP>:443/tmp/

  https://<NCM_IP>:443/images/

  https://<NCM_IP>:443/web/

  https://<NCM_IP>:443/lib/

  https://<NCM_IP>:443/icons/small/

  https://<NCM_IP>:443/WEB-INF/lib/

  https://<NCM_IP>:443/WEB-INF/

  https://<NCM_IP>:443/app/

  https://<NCM_IP>:443/help/

- Apache STIG hardening issues has been addressed in NCM. For more information refer, Apache STIG Hardening Fixed Issues in 10.1.1.

Access control settings

4

Access control settings enable the protection of resources against unauthorized access. The default user account and passwords are provided in this topic.

Table 4-1. Default accounts

User account	Password	Description
sysadmin	sysadmin	Default system administrator account for Network Configuration Manager.
smc-user	sysadmin	Network Configuration Manager System Management Console user account.
jmx-user	sysadmin	JMiniX JMX console user account.
msa-user	sysadmin	Account to access msa

This chapter includes the following topics:

Authentication configuration

Network Configuration Manager supports various methods of external authentication.

- TACACS+
- RADIUS
- LDAP
- SAML

The *VMware Smart Assurance Network Configuration Manager Online User Guide*, accessed from the Network Configuration Manager client, contains more information on authentication configuration. To access the guide, click **Help > Help Contents**. Use the Search function to find more information about Authentication.

User actions performed without authentication

The user actions that can be performed without authentication are described in this topic.

Table 4-2. User actions available without authentication

User action	Description of component
View online documentation	The *VMware Smart Assurance Network Configuration Manager Online User Guide* is hosted on the Network Configuration Manager Application Server.
View API Javadoc and samples	The *Network Configuration Manager API Javadoc* and samples are hosted on the Network Configuration Manager Application Server.

User authorization

User authorization settings control rights or permissions that are granted to enable a user to access a resource managed by the product.

Only authenticated users are allowed access to Network Configuration Manager. These authenticated users must be granted the appropriate permissions (or privileges) for authorization to access the application's features and functions. Access to the application is by the user interface (UI) or a public application programming interface (API).

Note The **Remember me** checkbox is available in the **SysAdmin Login** screen. If this checkbox is selected, the application remembers the last successful login username. If the application is launched again, the username is automatically available. By default, the **Remember me** checkbox is selected. Clear the selection to overcome this behavior.

Database component access

The Network Configuration Manager database (PostgreSQL) uses an access list to limit access to the database. The access list is automatically generated based on the user's selections during the installation process.

If the product is configured so that the application server and database reside on the same server, the database access list only allows local connections over the loopback address. If the application server is remote from the database, the installer adds an entry in the access list for the remote servers and modifies the PostgreSQL configuration so that it listens on the external network interface.

Editing PostgreSQL access list

The PostgreSQL access list is automatically configured by the Network Configuration Manager installer. Use this procedure to manually edit the access list.

Procedure

1. Open the `[Product_Directory]/db/controldb/data/pg_hba.conf`.

   Scroll to the bottom of the file and locate the md5 entries.

2. Add a new trusted IP address by inserting a new line. For example, **`host all all <IP address>/32 md5`**

   Replace **`<IP address>`** with the IP address you are giving access to.

3. Save and then Close the file.
4. Stop the Sysadmin service (Linux): **`service sysadmin stop`**
5. Stop the ncm-as service (Linux):
   - Linux: **`service ncm_as stop`**
6. Start the Sysadmin service (Linux): **`service sysadmin start`**
7. Restart the controldb service (Linux):
   - Linux: **`service controldb restart`**
8. Start the ncm-as service (Linux):
   - Linux: **`service ncm_as start`**

What to do next

Additional information about `pg_hba.conf` can be found at: http://www.postgresql.org.

Editing PostgreSQL listen addresses

The PostgreSQL listen addresses are automatically configured by the Network Configuration Manager installer. Use this procedure to manually edit the addresses.

Procedure

1. Edit `[Product_Directory]/db/controldb/data/postgresql.conf`
2. Locate the line that begins with `listen_addresses =` (near line 56).

   Remove the leading pound sign, **#**, to uncomment the line. If the line is commented out, it defaults to listen only on the local loopback address. For example,

   ```
   listen_addresses = 'localhost, 192.168.0.1' # Listen on localhost and 192.168.0.1
   listen_addresses = '*' # Listen on all addresses
   ```

   The list of listen addresses is comma delimited, and it must contain the 'localhost' address at a minimum. The list must be surrounded by single quotes. For example, to listen on all addresses, you can use an asterisk, **`'*'`**

3. Save, and then Close the file.

4 Stop the Sysadmin service (Linux): **`service sysadmin stop`**

5 Stop the ncm-as service (Linux):

- Linux: **`service ncm_as stop`**

6 Start the Sysadmin service (Linux): **`service sysadmin start`**

7 Restart the controldb service (Linux):

- Linux: **`service controldb restart`**

8 Start the ncm-as service (Linux):

- Linux: **`service ncm_as start`**

What to do next

Additional information on the `postgresql.conf` file can be found at: http://www.postgresql.org.

Log management and retrieval

Log files can only be accessed directly from the server. If remote access is required, the files may be exported through a file share.

Log settings

A log is a chronological record of system activities sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction, from inception to final results.

Table 4-3. Log description

Log component	Location
AutoDisc	[Product_Directory]/logs/autodisc.log
CF List	[Product_Directory]/logs/cflist.log
CF Write	[Product_Directory]/logs/cfwrite.log
CommMgr	[Product_Directory]/logs/commmgr.log
Controldaemon	[Product_Directory]/logs/daemon.log
Cut Thru Master	[Product_Directory]/logs/cutthrum.log
Cut Thru Server	[Product_Directory]/logs/cutthrus.log
DASL Compile	[Product_Directory]/logs/daslcompile.log
Device Driver Install Log	[Product_Directory]/logs/device_driver_install.log
Device Services AutoDiscovery Log	[Product_Directory]/logs/autodisc.log
Device Services CommMgr	[Product_Directory]/logs/commmgr.log
Device Services Cut Thru (Application Server) Activity Log	[Product_Directory]/logs/cutthrum.log
Device Services Cut Thru (Device Server)	[Product_Directory]/logs/cutthrus.log

Table 4-3. Log description (continued)

Log component	Location
Device Services Event Dispatch	[Product_Directory]/logs/eventdispatch.log
Device Services SysSync (Application Server)	[Product_Directory]/logs/syssyncm.log
Device Services SysSync Server (Device Server)	[Product_Directory]/logs/syssyncs.log
Device Services SysSync Transfer Log	[Product_Directory]/logs/ssxfrcgi.log
Documentation Install Log	[Product_Directory]/logs/documentation_install.log
Event Dispatch	[Product_Directory]/logs/eventdispatch.log
Event Handler	[Product_Directory]/logs/event.log
NCM Application Server Log	[Product_Directory]/ncmcore/logs/server.log
NCM Application Server Compliance Audit	[Product_Directory]/ncmcore/logs/compliance-audit.log
NCM Application Server Credential Rollout	[Product_Directory]/ncmcore/logs/credential-rollout.log
NCM Application Server General Log	[Product_Directory]/ncmcore/logs/server.log
NCM Application Server Powerup Events	[Product_Directory]/ncmcore/logs/powerup-events.log
NCM Application Server SAML	[Product_Directory]/ncmcore/logs/saml.log
NCM Application Server Voyence Audit	[Product_Directory]/ncmcore/logs/voyence-audit.log
NCM Application Server Voyence Log	[Product_Directory]/ncmcore/logs/powerup.log
NCM Application Server Compliance Audit Log	[Product_Directory]/ncmcore/logs/compliance-audit.log
Network Configuration Manager Controldaemon	[Product_Directory]/logs/daemon.log
NCM Application Server Credential Rollout Activity Log	[Product_Directory]/ncmcore/logs/credential-rollout.log
Network Configuration Manager Events Log	[Product_Directory]/ncmcore/logs/powerup-events.log
Network Configuration Manager SAMLActivity Log	[Product_Directory]/ncmcore/logs/saml.log
Network Configuration Manager Security Audit Log	[Product_Directory]/ncmcore/logs/voyence-audit.log
Network Configuration Manager Server Debug Log	[Product_Directory]/ncmcore/logs/powerup.log
Network Configuration Manager Server Information Log	[Product_Directory]/ncmcore/logs/server.log
Package Validate	[Product_Directory]/logs/pkgvalidate.log
PostgreSQL	[Product_Directory]/db/controldb/logs/server.postmaster
Setup Manager	[Product_Directory]/logs/setupmgr.log
SSH Daemon	[Product_Directory]/logs/sshdaemon.log
SysSync Master	[Product_Directory]/logs/syssyncm.log
SysSync Server	[Product_Directory]/logs/syssyncs.log
SysSync Transfer (ssxfrcgi)	[Product_Directory]/logs/ssxfrcgi.log
System Monitor (Application Server)	[Product_Directory]/logs/sysmonm.log
System Monitor Master	[Product_Directory]/logs/sysmonm.log
System Monitor Server	[Product_Directory]/logs/sysmons.log

Table 4-3. Log description (continued)

Log component	Location
Tomcat	[Tomcat Directory]/logs/catalina.out
Transformer service	[Product_Directory]/Transformation/logs/transformer.log

Enabling log file debugging

By default, debug logging is disabled (turned Off). When enabled, debug logging can consume a significantly large amount of disk space. Turn On debug logging only when needed.

Procedure

1. Edit `[Product_Directory]/conf/logs.cfg`
2. Locate, and then uncomment the following line by removing the number sign (#) character at the beginning of the line: **`#*:log(0-9):file(10x1000000)`**
3. Save changes to the file.
4. Restart the Network Configuration Manager service using the following:
   - Linux: **`/etc/init.d/voyence restart`**

Disabling log file debugging for the ncm-as service

By default, log file debugging for the ncm-as service is enabled (turned On). When debug logging for the ncm-as service is enabled, the log file size grows quickly. To disable log file debugging for the ncm-as service, follow this procedure.

Procedure

1. Edit `[Product-Directory]/ncmcore/webapps/ncm-webapp/WEB-INF/classes/log4j.xml`
2. Go to the section that begins on line 381, and change the priority value from `DEBUG` to `INFO`. For example:

```
<category name="com.powerup">
<priority value="INFO" />
<appender-ref ref="POWERUP"/>
</category>
```

3. Save the changes.
4. Restart the ncm-as service:
   - Linux: **`service ncm-as restart`**

Communication security settings

5

Communication security settings enable the establishment of secure communication channels between the product components, as well as between product components and external systems or components.

Table 5-1. Port usage

Service	Protocol	Destination Port	Application server (AS)/ Direction	Device server (DS)/ Direction	Combination server (CS)/ Direction	Database server (DB)/ Direction
Apache	TCP	80	Client to AS	N/A	Client to CS	N/A
NCM AS	TCP	8881	Client to AS	DS to AS, DS to CS	Client to CS	N/A
NCM AS SSL	TCP	8880	Client to AS	N/A	Client to CS	N/A
Apache SSL	TCP	443	Client to AS, DS to AS	AS to DS, CS to DS	Client to CS, DS to CS	N/A
SNMP	UDP	161	N/A	DS to Device	CS to Device	N/A
Telnet	TCP	23	N/A	DS to Device	CS to Device	N/A
SSH	TCP	22	N/A	DS to Device	CS to Device	N/A
SCP	TCP	22	N/A	DS to Device	CS to Device	N/A
TFTP	UDP	69, >1023	N/A	DS to Device, Device to DS	CS to Device, Device to CS	N/A
FTP	TCP	21	N/A	DS to Device	CS to Device	N/A
SNMP Traps	UDP	162	N/A	Device to DS	Device to CS	N/A
Syslog	UDP	514	N/A	Device to DS	Device to CS	N/A
Cut-Through	TCP	11965	Client to AS	N/A	Client to CS	N/A
Cut-Through	TCP	11966	AS to DS	CS to DS	N/A	N/A
TACACS+	TCP	49	AS to TACACS+ Server	N/A	CS to TACACS+ Server	N/A
Radius	TCP	1645, 1646, 1812, 1813	AS to Radius Server	N/A	CS to Radius Server	N/A
LDAP	TCP	389	AS to LDAP Server	N/A	CS to LDAP Server	N/A

Table 5-1. Port usage (continued)

Service	Protocol	Destination Port	Application server (AS)/ Direction	Device server (DS)/ Direction	Combination server (CS)/ Direction	Database server (DB)/ Direction
Telnet Cut-Through Proxy	TCP	1029	Client to AS	N/A	Client to CS	N/A
SSH Cut-Through Proxy	TCP	1031	Client to AS	N/A	Client to CS	N/A
SMTP	TCP	25	AS to SMTP Server	N/A	CS to SMTP Server	N/A
DNS	TCP	53	N/A	DS to DNS Server	CS to DNS Server	N/A
Tomcat SSL	TCP	8443	Client to AS	N/A	N/A	N/A
PostgreSQL	TCP	5435	AS to DB	N/A	CS to DB	AS to DB, CS to DB
NCM AS	TCP	1099	Registry port	N/A	Internal bean registration	N/A
NCMMSA Tomcat	TCP	9443	N/A	N/A	N/A	N/A
NCMMSA	TCP	9005	N/A	N/A	N/A	N/A
Tomcat	TCP	8005	N/A	N/A	N/A	N/A
Voyenced	TCP	9991	AS to DS	AS to DS	CS to DS	N/A
Voyenced	TCP	9992	DS to AS	DS to AS	DS to CS	N/A
Active MQ broker	TCP	61616	Client to AS	N/A	Client to CS	N/A
Commgrd	TCP	9995	AS to DS DS to AS	AS to DS DS to AS	CS to DS DS to CS	N/A
Autodiscd	TCP	9996	AS to DS DS to AS	AS to DS DS to AS	CS to DS DS to CS	N/A
Syssyncd Master	TCP	9997	AS to DS	AS to DS CS to DS	CS to DS	N/A
Syssyncd Server	TCP	9998	DS to AS	DS to AS	DS to CS	N/A
Smarts Adapter	TCP	11805	Client to Adapter	N/A	Client to Adapter	N/A
Smarts Adapter	TCP	11880	Client to Adapter	N/A	Client to Adapter	N/A
Smarts Adapter	TCP	11843	Client to Adapter	N/A	Client to Adapter	N/A

This chapter includes the following topics:

SSLv3 POODLE vulnerability mitigation

NCM 9.4.x includes the fix to disable SSLv3 connections. NCM components are not vulnerable to POODLE attack. For details on this vulnerability, refer to:

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566

As a fix, the SSL connections to NCM components (Application server, MSA, Apache) are disabled and only TLS connections are allowed.

The SA Suite Security KnowledgeBase (KB) reference at https://docs.vmware.com/en/VMware-Smart-Assurance/9.4.2/302-003-132_01_NCM_942_ReleaseNotes.pdf provides more information.

Network encryption

In Network Configuration Manager a few clients are configured to communicate over HTTPS and others over HTTP. You may want to change the default protocols depending upon network performance or security requirements.

Here are the default protocols used by the clients when communicating with the Application Server:

Table 5-2. Default client protocols

Clients	Protocol
NCM thick client	HTTP
J2EE API calls	HTTP
NCM Smarts Adapter	HTTPS
NCM EDAA (NCM MSA)	HTTPS

Configuring NCM thick client to use HTTPS

The NCM thick client is configured to use HTTP by default. Change it to HTTPS to make the NCM thick client secure.

The client protocol is controlled by the HTML landing page from which the client is launched.

In addition to using HTTPS, you can block the non-SSL ports through the use of a firewall between the client and the server. The ports to block are TCP port 80 and TCP port 8881.

Note Port 80 must not be blocked on the loop back.

Procedure

1 Open <VOYENCE_HOME>/ncmcore/webapps/voyence/powerup.jnlp

2 Modify this line,

```
<property name="jnlp.cc.remoting.servlet.base" value="http://$$hostname:8881/ncm-webapp/
remoting/"/>
```

Change it to

```
<property name="jnlp.cc.remoting.servlet.base" value="https://$$hostname:8880/ncm-webapp/
remoting/"/>
```

Configuring J2EE API calls to use HTTPS

The cc.remoting.servlet.base URL in the J2EE samples folder is changed from HTTPS (secure) to HTTP by default to improve performance of the J2EE API calls. To change back to HTTPS, follow these steps

Procedure

1 Open <VOYENCE_HOME>/ncmcore/webapps/ncm-webapp/samples/J2EE/conf/config.properties

2 Modify this portion of the line,

```
cc.remoting.servlet.base=http://<server-ip>:8881/ncm-webapp/remoting/
```

Change it to

```
cc.remoting.servlet.base=https://<server-ip>8880/ncm-webapp/remoting/
```

Changing NCM EDAA (MSA) or Smarts Adapter clients to use HTTP

NCM EDAA (MSA) and NCM Smarts Adapter communicate with the Application Server using HTTPS by default. Use these steps to change to HTTP.

Procedure

1 Open these files:

- $VOYENCE_HOME/ncmmsa/webapps/ncm-msa/WEB-INF/classes/config.properties
- $VOYENCE_HOME/NCMSmartsAdapter/lib/config.properties
- $TOMCAT_HOME/webapps/web/WEB-INF/classes/config.properties

2 Modify this line,

```
cc.remoting.servlet.base=https://<server-ip>:8880/ncm-webapp/remoting/
```

Change it to

```
cc.remoting.servlet.base=http://<server-ip>:8881/ncm-webapp/remoting/
```

Data security settings

Data security settings enable definition of controls to prevent data permanently stored by the product to be disclosed in an unauthorized manner.

Encryption of data at rest

All sensitive data within the Network Configuration Manager application is encrypted during transit (server-to-server, client-to-server) or in the database.

Enabling encryption for configuration data in the Device Server cache

By default, configuration data is not encrypted in the Device Server cache. Add the CACHE_ENCRYPT attribute to the NCM Infrastructure Database to encrypt the configuration data. Note that enabling encryption only takes effect if there is a change in the configuration data (if a new Device Configuration State is created).

To enable the encryption, follow this procedure.

Procedure

1 Go to the [*Product directory*]/bin directory.

2 For Linux only, source the voyence.conf file. Type: `source /etc/voyence.conf`

3 Go to the [*Product Directory*]/cgi-bin/ directory.

4 Run one of these commands depending on where the Device Server resides:

- Application server: **./cflist.cgi > temp.txt**
- Remote Device server: **./cflist.cgi mode=pop > temp.txt**

5 Open the temp.txt file and add the CACHE_ENCRYPT=1 attribute to the NCM Infrastructure Database.

For example:

```
POP 1000 "linbgz222.lss.vmware.com"
NetList= RsrcList= DevList= EmsList= :
ADDR="10.31.151.222" AGE_DAYS=730
CLEANUP_DAYS=90 AD_ENABLE=0
```

```
AD_ARPCACHE=0 AD_DFLTROUTE=0
AD_AUTO_RESOURCE=0
AD_DEFAULT_POLL=0
SNMP_TIMEOUT=500 SNMP_RETRY=3
CM_DEBUGSESSION=0 SORTCONFIG=1
CM_MAXMAINTASKS=20 CM_PULLTIMER=1200
CUTTHRU_PULLTIMER=10
MAX_COMM_ATTEMPTS="5"
CM_SMGR_CACHING_ENABLED=1
CM_SMGR_SESSION_TIMEOUT=60
CM_SMGR_SESSIONS_PER_DEVICE=4
AD_BATCHSIZE=1000 AD_NUMHOP=10
AD_TIMEOUT=10 AD_LOOPCNT=2
CM_NATTEDIP_LOOKUP=1
CACHE_ENCRYPT=1
CM_SYSLOGCONFIG="local1.*;local4.*;local7.*"
RECORDVER="1.0"
```

6 Run the command: **./cfwrite.cgi < temp.txt**

7 Restart the vcmaster service. Use the command appropriate for the operating system where [Product_Directory] is the directory where Network Configuration Manager is installed:

- Linux: **service vcmaster start**

Security alert system settings

Security monitoring is possible in Network Configuration Manager through the use of an optional integration adapter. The Network Configuration Manager SNMP Integration Adapter allows the user to configure SNMP traps for a wide range of events in Network Configuration Manager.

VMware Smart Assurance Network Configuration Manager Installation Guide provides more information on the SNMP module.

SSL ciphers in Tomcat

Ciphers are qualified in Network Configuration Manager by modifying the server.xml files.

- [Product–directory]/ncmcore/conf/server.xml
- <Tomcat_Home>/conf/server.xml

Ciphers qualified

The following ciphers are qualified in Network Configuration Manager for the file.

- RSA:!EXP:!NULL:+HIGH:+MEDIUM:-LOW:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!KRB5:!aECDH:!EDH:!3DES

Global device security policy

6

This policy is intended to provide exclusive access to operational devices for certain privileged Principals (users and groups). If a Principal is assigned permissions at the device level against a concrete device, the Principal (referred to as the primary Principal) automatically claims exclusive access to the device. This means that other Principals are not authorized to access this device, under any circumstances.

To assign a different set of permissions than the primary Principal, the notion of an abstract Principal called Others is introduced. The Others Principal is used to represent the rest of the Principals that are not the primary Principal, and can be used by the administrator to assign permissions (typically less effective privileges) on the device.

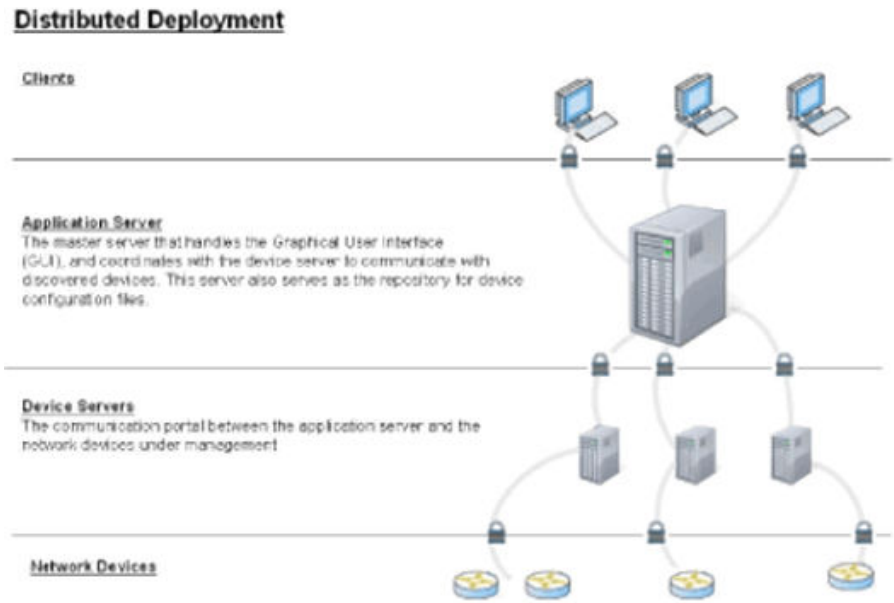
After a Principal is assigned explicit permissions on concrete devices, the permission enforcement does not fall back to the network or system.

Secure deployment and usage settings

7

This diagram illustrates the secure settings that affect the Network Configuration Manager deployment.

Figure 7-1. Distributed deployment



This chapter includes the following topics:

- Secure deployment settings
- Security patch management

Secure deployment settings

The default security settings in Network Configuration Manager and recommendations for a high security configuration are provided in this topic.

Default setting	Secure deployment setting	Pros of secure deployment setting	Cons of secure deployment setting	Instructions on how to configure secure deployment setting
Application server listens on both secure and insecure ports.	For best possible security between client and server, block access to the insecure ports through the use of a firewall.	Provides high level of protection for the communication between client and server by avoiding the tampering, spoofing, man in the middle type of attacks.	Impact on performance.	Install a firewall between the application server and the clients (or on the application server using iptables). **Note** Firewalls installed on a Network Configuration Manager server must comply with the list of standard Network Configuration Manager ports and protocols. Chapter 5 Communication security settings **Note** Port 80 must not be blocked on the loop back.
Self-signed SSL certificate is used for client connections.	Purchase or generate a trusted SSL certificate for client connections.	Client to server connections are trusted, no warnings during login.	Certificate may require additional financial cost.	Refer to the *Network Configuration Manager Installation Guide* for instructions on installing SSL certificates.
Default password is used for multiple accounts.	Change all default passwords immediately after installing the product.	Prevent access to intruders.		Change the Network Configuration Manager, System Management Console, and JMX Console passwords. Refer to the *Network Configuration Manager Installation Guide* for instructions.

Security patch management

The components that require patch management are listed in this topic.

Third-party component for which patch is needed	Frequency of patch	VMware responsibility (Y/N)	Customer responsibility (Y/N)	Reference to instructions for applying patch
Red Hat Enterprise Linux	Daily	No	Yes	Patch instructions supplied by vendor
Windows Server	Daily	No	Yes	Patch instructions supplied by vendor

Tomcat	Quarterly	Yes	Yes	Patches for this component will be supplied in a release or a service pack.
PostgreSQL	Quarterly	Yes	No	Patches for this component will be supplied in a release or a service pack.

Application security management

8

Network Configuration Manager provides administrative features to manage users, groups, and their memberships.

It is important to note that devices within the application are discovered as a part of Networks, which act as the top level containers. This approach supports Managed Service Provider environments.

Networks, in turn, can have sub-containers such as Sites, Views, and Workspaces. As a result, Network Configuration Manager defines four primary security levels, based on the scope of user access within the application. These levels play an important role in the management of permissions in relation to the Principals.

This chapter includes the following topics:

Security levels

The security levels are listed in order of increasing precendence.

- System - Controls scope globally (across all networks)
- Network - Controls scope within concrete networks
- Workspace - Controls scope within concrete workspaces
- Device - Controls scope within concrete devices.

The enforcement scope broadens when you move up a security level: Device ' [Workspace] ' Network ' System. Note that the workspace level is only applicable for workspace or design device related operations.

Permission levels

The system level includes permissions that apply to generic system operations that do not concern a network, workspace, or device. The system level does not include any concrete resources, as it is meant for operations that are not related to networks, workspaces, or devices, and also for convenience as a fallback level during access control checks.

The network level includes permissions that apply to operations pertaining to a network, its sub-containers, and the devices within it.

The workspace level includes permissions that apply to operations pertaining to the workspace and design devices, including virtual devices.

The device level includes permissions that apply to operations pertaining to the device. Permissions explicitly assigned at this level trigger the Global Device Security Policy.

Secured resources

Instances of network, workspace, and device are considered secured resources and are managed under the network, workspace, and device levels, respectively.

The specific secured resources must be explicitly and individually associated to the Principal before permission assignment can be made for the Principal. Not explicitly associating a resource to the Principal is equivalent to the Principal having no permission on that resource. Permissions can be assigned in two ways against the resources for the Principal.

Default permissions

After associating the desired set of resources with the Principal, you may assign default permissions to the entire set. This means each resource inherits the same permissions.

This is convenient because the administrator does not have to assign the same permission set to all the individual resources that have been associated to the Principal. Note that default permissions are not supported for the devices. The Global Device Security policy section details this information.

Override permissions

If specific overrides are desired on certain resources as exceptions to the default permission, assign default permissions against each specific resource.

Avoiding exposure to passwords

Some of the Perl files under the folder show the passwords in clear text.

To avoid exposure to the passwords, you must remove the following files from the `$VOYENCE_HOME/conf/setup` folder, after the installation:

- AppServer.pl

- Common.pl

Security enforcement rules

9

Permissions are enforced by initiating the access check, and by anchoring at one of the security levels: device, network, workspace, or system. The choice of the security level depends on the operation performed.

For instance, system level is selected for system operations, such as user management operations; and network level is chosen for network-centric operations, such as modifying a network, managing views, viewing device details, and so on.

Enforcement at the network, workspace, and the device levels also requires an access context, which involves the target concrete resource that is being accessed directly or indirectly by the user operation.

This helps in examining the permissions associated with that resource for the user attempting the access. Every service method enabling the user operation is secured by an interceptor that implements the appropriate access checks for the methods.

The access controller implements business logic to determine if the supplied Principal has the correct privileges required for the service method.

This chapter includes the following topics:

Checking the NCM system

Complete the following steps for the system level check.

Procedure

1 Determine if the Principal has System Administrator permissions at the system level. If yes, consider that Principal authorized, and return.

This check is an optimization from executing the rest of the checks.

2 Check if the required privileges are a subset of the permissions assigned to the Principal at the system level. If yes, consider the supplied Principal as authorized, and return. If no, the supplied Principal is not authorized.

Checking the NCM network

Complete the following steps for the network level check.

Procedure

1 Determine if the Principal has System Administrator permissions at the system level. If yes, consider that Principal authorized.

   This check is an optimization from executing the rest of the checks.

2 Identify the target concrete network from the access context.

3 Check if the network is explicitly associated to the Principal. If no, skip to step 8 of this procedure.

4 Obtain overridden permissions for the Principal on the network, if configured. If there are no overridden permissions, skip to step 6 of this procedure.

5 Check if the required privileges are a subset of the permissions assigned to the Principal, against the target workspace. If yes, consider the supplied Principal as authorized and return. If no, consider the supplied Principal is not authorized.

6 Obtain default permissions for the Principal on the network identified in step 2 of this procedure, if any.

7 Check if the required privileges are a subset of the permissions assigned to the Principal, against the target workspace. If yes, consider the supplied Principal as authorized and return. If no, go to the next step.

8 Perform the system level checks. Checking the NCM system

Checking the workspace

Complete the following steps for the workspace level check.

Procedure

1 Determine if the Principal has System Administrator permissions at the system level. If yes, consider that Principal authorized.

   This check is an optimization from executing the rest of the checks.

2 Identify the target concrete workspace from the access context.

3 Check if the workspace is explicitly associated to the Principal. If no, skip to step 6 of this procedure.

4 Obtain overridden permissions for the Principal on the target workspace if configured; if no overridden permissions exist, skip to step 7 of this procedure.

5 Check if the required privileges are a subset of the permissions assigned to the Principal, against the target workspace. If yes, consider the supplied Principal as authorized and return. If no, consider the supplied Principal as not authorized and return.

6 Identify the containing network from the workspace from the access context.

7 Check if the network is explicitly associated to the Principal. If no, skip to step 14 of this procedure.

8 Obtain overridden permissions for the Principal on the network if configured; if no overridden permissions exist, skip to step 12 of this procedure.

9 Check if the required privileges are a subset of the permissions assigned to the Principal, against the target workspace. If yes, consider the supplied Principal as authorized and return. If no, go on to next step.

10 Obtain default permissions for the Principal on the target workspace if any.

11 Check if the required privileges are a subset of the permissions assigned to the Principal, against the target workspace. If yes, consider the supplied Principal as authorized and return. If no, continue on to next step.

12 Obtain default permissions for the Principal on the network identified earlier.

13 Check if the required privileges are a subset of the permissions assigned to the Principal, against the target workspace. If yes, consider the supplied Principal as authorized and return. If no, go on to next step.

14 Perform the system level checks. Checking the NCM system

Checking the device

Complete the following steps for the device level check.

Procedure

1 Determine if the Principal has System Administrator permissions at the system level. If yes, consider that Principal authorized.

   This check is an optimization from executing the rest of the checks.

2 Identify the target concrete device from the access context.

3 If the device is a Virtual Design device, skip to step 10 of this procedure.

4 Check if the device is explicitly associated to the Principal. If not, skip to step 7 of this procedure.

   The Global Device Security policy is now active. Obtain device permissions for the Principal.

5 Obtain device permissions for the Principal.

6 Check if the required permissions are a subset of the permissions assigned to the Principal in question, on the device. If yes, consider the supplied Principal as authorized and return. If not, continue on to the next step.

7 Check if the device is explicitly associated to any other Principal. If not, skip to step 10 of this procedure.

8 Obtain permissions on this device for the Others Principal.

9 Check if the required permissions are a subset of the permissions assigned to the Others Principal on the device. If yes, consider the supplied Principal as authorized, and return. If not, consider the supplied Principal as not authorized, and return.

10 If the device is a design device (copy of operational or just virtual), obtain the containing workspace. It the device is an operational device, skip to step 14 of this procedure.

11 Check if the workspace is explicitly associated to the Principal. If not, skip to step 15 of this procedure.

12 Obtain overridden permissions for the Principal on the target workspace, if configured. If there are no overridden permissions, skip to step 14 of this procedure.

13 Check if the required privileges are a subset of the permissions assigned to the Principal, against the target workspace. If yes, consider the supplied Principal as authorized and return. If not, consider the supplied Principal as not authorized, and return.

14 Identify the containing network from the workspace if the device is a design device, or the primary network of the device.

15 Check if the network is explicitly associated to the Principal. If not, skip to step 18 of this procedure.

16 Obtain overridden permissions for the Principal on the network if configured. If no overridden permissions exist, skip to step 18 of this procedure.

17 Check if the required privileges are a subset of the permissions assigned to the Principal, against the target workspace. If yes, consider the supplied Principal as authorized and return. If not, consider the supplied Principal as not authorized, and return.

18 Obtain default permissions for the Principal on the target workspace if design device. If not design device, skip to Step 20 of this procedure

19 Check if the required privileges are a subset of the permissions assigned to the Principal, against the target workspace. If yes, consider the supplied Principal as authorized and return. If not, continue on to the next step.

20 Obtain default permissions for the Principal on the network identified earlier.

21 Check if the required privileges are a subset of the permissions assigned to the Principal, against the target workspace. If yes, consider the supplied Principal as authorized and return. If not, continue on to the next step.

22 Check the system.Checking the NCM system

Effects of group membership

Users and Groups, in addition to the directly assigned permissions, inherit permissions by virtue of their membership to another Group. Transitive memberships enable permission inheritance beyond the direct parent group. Permissions of a Principal and parent groups, are additive when obtaining effective permissions for the Principal.

Under all circumstances user permissions override group permissions when the user is a member (immediate or transitive). This is possible when both the user and the group have overridden permissions on a secured resource.

Available permissions

10

Permissions may be set for system, network, workspace, or device.

System-level permissions are provided in this table:

System scope	Permissions available
General	■ System Admin ■ Override Credentials ■ Manage Users/Groups ■ Manage User Access ■ Manage Data Field ■ Manage Templates ■ Manage Queries ■ Manage Compliance Standards ■ View Event Manager
Network	■ Create
Device	■ Manage OS ■ Manage OS Inventory
Job	■ Schedule ■ Approve

Network-level permissions are provided in this table:

Network scope	Permissions available
General	■ Override Credentials ■ Manage User Access ■ Manage Templates ■ Manage Queries ■ Manage Compliance
Network	■ Edit ■ Delete ■ View

Device	■ Create ■ Edit ■ Assign Credentials ■ View Details ■ View Sensitive Data ■ Manage OS ■ Run Non-Scheduled ■ Run Cut-through
Job	■ Schedule ■ Approve
View	■ Create ■ Edit ■ Delete
Workspace	■ Create ■ Edit ■ Delete ■ View

Device-level permissions are provided in this table:

Device scope	Permissions available
Device	■ Edit ■ Assign Credentials ■ View Details ■ View Sensitive Data ■ Manage OS ■ Run Non-Scheduled ■ Run Cut-through
Job	■ Schedule ■ Approve

Workspace-level permissions are provided in this table:

Workspace scope	Permissions available
Workspace	■ Edit ■ Delete ■ View

Device	■ Create ■ Edit ■ Assign Credentials ■ View Details ■ Manage OS ■ Run Non-Scheduled ■ Run Cut-through
Job	■ Schedule ■ Approve

Using groups as roles

11

While Network Configuration Manager supports detailed security control on user access, it also has the ability to almost emulate role-based access through the use of Groups.

A user role can easily be mapped to a Group, which can be assigned the appropriate permissions to the existing concrete resources. The choice of concrete resources assists to restrict access to only those resources that are useful in Managed Service Provider environments.

Assigning roles to users and groups can be achieved by making them members of the group representing the role.

Note After new concrete resources come into existence, they must be explicitly associated to these role groups before they show the desired authorization behavior.

Security hardening

12

This section provides instructions for hardening Network Configuration Manager after installation.

Ensure all security patches recommended by the operating system vendor(s) are applied. The instructions in this guide pertain only to the Network Configuration Manager product and software installed by the product.

This chapter includes the following topics:

Pre-hardening requirements

Before continuing with any of the hardening instructions, ensure Network Configuration Manager has been installed with the default versions of third-party software.

Stop the Network Configuration Manager services before completing the hardening tasks. The *VMware Smart Assurance Network Configuration Manager Installation Guide* provides more information.

Stopping the Network Configuration Manager services

Issue these commands to stop the Network Configuration Manager services.

Procedure

- Use the command appropriate for the operating system where [Product_Directory] is the directory where Network Configuration Manager is installed:
  - Linux: **service vcmaster stop**

Post-hardening requirements

After completing the hardening procedures, start the Network Configuration Manager services.

Starting the Network Configuration Manager services

Issue these commands to start the Network Configuration Manager services.

Procedure

- Use the command appropriate for the operating system where [Product_Directory] is the directory where Network Configuration Manager is installed:
  - Linux: **service vcmaster start**

Restricting the pgdba user from host level login for Linux

To restrict the pgdba user from host level login privileges for Linux, complete the following steps in the maintenance window:

Procedure

1. Log in to the NCM Application server hosts, as the root user.
2. Run the following command on the Application Server hosts:

   source /etc/voyence.conf
3. Stop all NCM services on the Application Server host, by running the following command:

   service vcmaster stop
4. If the NCM Database server is remote, run the following commands on the server, as the root user:

   source /etc/voyence.conf

   service controldb stop
5. Run the following commands on the NCM Database server:
   a. Run the following command in the Linux shell on the host where the controldb resides to back up appropriate files:

      cp –p $VOYENCE_HOME/db/controldb/scripts/controldb.init /tmp/_[etc–init.d–]controldb.bak

b Update the pgdba user shell permissions, and then update the NCM controldb initialization script, to allow the correct controldb operation under a pdgba user with restricted shell privileges:

```
sed –i 's/su – pgdba –c/su – pgdba –s \/bin\/bash –c/g' $VOYENCE_HOME/db/controldb/scripts/controldb.init
```

```
cp –p /etc/passwd /tmp/passwd.bak
```

```
usermod –s /sbin/nologin pgdba
```

c Restart the system:

```
reboot
```

6 If the NCM Database server is remote, start all the NCM services on the Application server host, by running the following command:

```
service vcmaster start
```

Restoring the pgdba user shell permissions back to default

To restore the pgdba user shell permissions back to default, complete the following steps:

Procedure

1 Log in to the NCM Application server hosts, as the root user.

2 Run the following command on the Application Server hosts:

```
source /etc/voyence.conf
```

3 Stop all the NCM services on the Application Server host, by running the following command:

```
service vcmaster stop
```

4 If the NCM Database server is remote, run the following commands on the server, as the root user:

```
source /etc/voyence.conf
service controldb stop
```

5 Run the following commands on the NCM Database server:

a Run the following commands in the Linux shell on the host where the controldb resides, to restore the NCM controldb initialization script and pgdba user shell permissions:

```
cat /tmp/_[etc–init.d–]controldb.bak > $VOYENCE_HOME/db/controldb/scripts/controldb.init
```

```
usermod –s /sbin/nologin pgdba
```

b Restart the system:

```
reboot
```

6 If the NCM Database server is remote, start all NCM services on the Application Server host, by running the following command:

```
service vcmaster start
```

Securing port 1099

The JMX port 1099 has been made accessible from localhost only and any access from remote host has been disabled.

To enable the access to this port from a remote host, the following steps need to be performed:

Procedure

1 Remove the following parameters from the `/etc/init.d/ncm_as` file:

- **`-Dcom.sun.management.jmxremote.port=1099`**
- **`-Dcom.sun.management.jmxremote.host=127.0.0.1`**

2 Restart the ncm-as service.

Disabling HTTP ports in Tomcat services

To disable HTTP ports in Tomcat services, complete the following steps:

Procedure

1 Start the ncm-as service.

2 Open the `$VOYENCE_HOME/ncmcore/conf/server.xml` file.

3 Comment out the following section to remove the HTTP port reference:

```
<Connector port="8881" protocol="HTTP/1.1"^M
 connectionTimeout="20000"^M
 redirectPort="8880" /> ^M
```

4 Save the file.

5 Restart the ncm-as service.

Also, follow the above procedure (step 1-5) for NCM MSA.

a Edit the `<Tomcat_Home>/conf/server.xml` file to remove the HTTP port reference for `8080 -> 8443`.

b Edit the `$VOYENCE_HOME/ncmmsa/conf/server.xml` file to remove the HTTP port reference for `9180 -> 9443`.

Note MSA service runs fine after disabling the HTTP port, and no other changes are required.

Enabling NCM client and API to use HTTPS port

To enable the NCM client and API to use HTTPS port, complete the following steps:

Procedure

1 Edit the following files:

- `[root@<ncm-ip>:smarts-ncm]# find . -name config.properties`
- `./ncmcore/webapps/ws/WEB-INF/classes/config.properties`
- `./ncmcore/webapps/ncm-webapp/WEB-INF/classes/config.propertie`
- `./ncmcore/webapps/ncm-webapp/samples/J2EE/conf/config.properties`

2 In the respective files, change the following to use HTTPS port.

```
cc.remoting.servlet.base=https://<ncm-ip>:8880/ncm-webapp/remoting/
```

3 Save the files.

Enabling NCM UI to use HTTPS port

To enable the NCM UI to use HTTPS port, complete the following steps:

Procedure

1 Edit the following files:

- `-find . -name powerup.jnlp`
- `./ui/html/powerup.jnlp`
- `./webstart/ui/html/powerup.jnlp`
- `./ncmcore/webapps/voyence/powerup.jnlp`

2 In the respective files, change the following to use HTTPS port.

```
<property name="jnlp.cc.remoting.servlet.base" value="https://$$hostname:8880/ncm-webapp/
remoting/"/>
```

3 Save the files.

Apache STIG Hardening Fixed Issues in 10.1.1

As part of 10.1 release, the following Apache STIG hardening issues have been addressed in NCM.

V-13736: The *LimitRequestBody* directive is set to a value of "1610612736" in the `httpd.conf` file.

V-13737: The *LimitRequestFields* directive is set to a value of 100.

V-13738: The *LimitRequestFieldSize* directive is set to a value of 8190.

V-13739: The *LimitRequestLine* directive is set to a value of 8190.

V-26294: The following modules are not loaded in the Apache httpd server:

- info_module
- status_module

V-26368: The *LoadModule autoindex_module* directive must be commented, if present in the Apache `httpd.conf` file.

V-26326: The listen directive in `<VOYENCE_HOME>/conf/httpd.conf` is set to the `<IPAddress>:<Port>` on which the Apache server is listening.

V-26287: The following modules are not loaded in the Apache httpd server:

- dav_module
- dav_fs_module
- dav_lock_module

V-2259: The permission of `<VOYENCE_HOME>/conf/httpd.conf` is set to 640.

V-13735: The options directive in the Apache httpd.conf file is set to *None*.

V-26324: The options directive in the root directory of the Apache `httpd.conf` file is set to *None*.

V-26396: For all the non-root directory in the Apache `httpd.conf` file, the following two entries are added:

- Order allow, deny
- Deny from all

V-26323: For the root directory in the Apache `httpd.conf` file, the following entry is added:

- Order denies, allow

> **Note** Adding *Deny from all* in the root directory is impacting the NCM functionality and hence its not added in the root directory of Apache `httpd.conf` file.

V-13733: The options directive in the root directory of the Apache `httpd.conf` file is set to *None*.

V-13734: The options directive in the root directory of the Apache `httpd.conf` file is set to *None*.

PostgreSQL STIG Hardening Fixed Issues in 10.1.1

As part of 10.1.1 release, the following PostgreSQL STIG hardening issues have been addressed in NCM.

V-72909: log_destination has updated as 'syslog' and syslog_facility as 'LOCAL0' in postgres.conf to capture the log messages in /var/log/messages.

V-72925: log_connections and log_disconnections set as 'on' in postgres.conf file to log connections, date/time, username, and session identifier.

V-72929: pgaudit.log is set as 'role' in postgres.conf file to log the changes in the permissions, privileges, and roles granted to users and roles.

V-72939: pgaudit.log is set as 'ddl' in postgres.conf file to audit the removal of security objects from the database.

V-72987: The appropriate log_line_prefix is set in postgres.conf to capture the identity of any user/subject or process associated with an event.

V-73005: log_hostname is set as 'on' in postgres.conf to log the hostname.

V-73015: password_encryption is set as 'on' in postgres.conf to identify if any passwords have been stored without being hashed and salted.

V-73023: The script $VOYENCE_HOME/tools/StorageVolumeUtil.sh is available to monitor the disk space in the database server. This script needs to be edited to replace *dummyemail@domain.com* with the user's email id to get the email notification. Use this script, to schedule a cron job to run around the clock.

V-73033: log_connections, log_disconnections, log_line_prefix are set as on in postgres.conf to verify the audit record does not log events required by the organization.

V-73037: statement_timeout,tcp_keepalives_idle,tcp_keepalives_interval are set as 10s in postgres.conf file to invalidate session upon user logout or other session termination.

V-73045: PostgreSQL uses syslog to transfer audit records to a centralized log management system.

V-73047: In postgres.conf file SSL is set as on to maintain the authenticity of communications sessions by guarding against man-in-the-middle attacks.

Note To fix STIG V-73047 in Remote Database Server, Please follow the below instructions after the complete installation of Database and Application servers.

Procedure:

1 Copy `$VOYENCE_HOME/conf/server.crt` and `$VOYENCE_HOME/conf/server.key` from Application Server to Database Server.

2 Run the Perl script `$VOYENCE_HOME/tools/configureSSL.pl` by providing the copied `server.crt` and `server.key` with the location details as the input in the Database Server.

For example:

```
perl $VOYENCE_HOME/tools/configureSSL.pl /server.crt /server.key
```

3 In Application Server, restart vcmaster services to connect with SSL configured Database.

```
service vcmaster restart
```

V-73061: log_file_mode set as 0600 in postgres.conf file and postgresql.conf file permission is set as 0600.

V-73123: The appropriate log_line_prefix set in posgres.conf file to produce audit records containing sufficient information to establish where the events occurred.

STIG V-2265: .java and .jpp files has been removed from the web server, except for the below sample files.

There are some .java sample files which are present in the below directories. These sample files can be moved to a different loation or zipped.

There wont be any functionality impact.

`./ncmcore/webapps/ncm-webapp/samples/WS/src/com/voyence/api/samples/`

`./ncmcore/webapps/ncm-webapp/samples/J2EE/src/com/voyence/api/samples/discovery/`

Web Services hardening

13

This section provides instructions for hardening web services used with Network Configuration Manager.

This chapter includes the following topics:

Apache HTTP Server hardening

The Apache HTTP Server settings can be adjusted to harden the security of the server.

Adjust the hardening settings on each Application Server, Device Server, and Combination Server.

Removing the Group Write Bit from the Document Root Directory

The following steps will remove the group writable bit from the Apache HTTP Server document root directory.

The following steps only apply to Linux.

Procedure

1. Change directories to `[Product_Directory]/ui`, where `[Product_Directory]` is the directory where Network Configuration Manager is installed.
2. Run the following command using root privileges, **`chmod –R g–w,o–w html`**

Apache Tomcat Server hardening

The Apache Tomcat Server settings can be adjusted to harden the security of the server.

Removing the Default Web Applications

The following steps will remove the documentation, examples, and management interface from the Tomcat web server. None of these are required for Network Configuration Manager to operate.

The following steps must be performed on each Application Server and Device Server.

Procedure

1. Change directories to `[Tomcat Directory]/webapps`, where `[Tomcat Directory]` is the directory where Apache Tomcat is installed.
2. Delete the following directories, if they exist:
   - balancer
   - jsp-examples
   - ROOT
   - DOCS
   - webdev

Communication hardening

14

This section provides instructions for hardening communication services used with Network Configuration Manager.

This chapter includes the following topics:

Hardening the Vmware Smart Assurance Network Configuration Manager Integration Adapter for Smarts Manager

You can encrypt communications between the VMware Smart Assurance Network Configuration Manager Integration Adapter for Smarts Manager and the VMware Smart Assurance programs.

You must configure communication settings for:

- Each instance of Service Assurance Manager and IP Availability Manager in the environment
- The Tomcat server in the Network Configuration Manager environment

Procedure

1. Go to the `BASEDIR/smarts/local/conf` directory of the Service Assurance or IP Availability Manager whose communications you want to encrypt.
2. Open the `runcmd_env.sh` script.
3. Set the *SM_INCOMING_PROTOCOL* variable to **`SM_INCOMING_PROTOCOL=1,0`**
4. Set the *SM_OUTGOING_PROTOCOL* variable to **`SM_OUTGOING_PROTOCOL=1,0`**
5. Restart the VMware Smart Assurance services in order for the changes to take effect.
6. Repeat this process for each instance of Service Assurance Manager and IP Availability Manager that requires encrypted communication.

Enabling encryption for NCM Integration Adapter for VMware Smart Assurance

Enable the Network Configuration Manager Integration Adapter for VMware Smart Assurance to support encrypted communication.

Procedure

1. Open the Tomcat file, `/etc/init.d vc-smarts`
2. Type these lines after the *CATALINA_HOME* variable assignment:

```
#-------------------------
# Enable Smarts Encryption
JAVA_OPTS="$JAVA_OPTS -Dcom.smarts.outgoing_protocol=1"
export JAVA_OPTS
#-------------------------
```

3. Restart Tomcat.

Troubleshooting and getting help

15

VMware support, product, and licensing information can be obtained as follows:

Product information — For documentation, release notes, software updates, or information about VMware products, go to VMware Online Support at: docs.vmware.com.

Technical support — Go to VMware Online Support at: support.vmware.com. You will see several options for contacting VMware Technical Support. Note that to open a service request, you must have a valid support agreement. Contact your VMware sales representative for details about obtaining a valid support agreement or with questions about your account.