HPE Network Virtualization

Software Version: 9.1x

Security Guide

Document Release Date: November 2016

Hewlett Packard
Enterprise

Contents

Legal Notices

Warranty

The only warranties for HPE products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Welcome to this Guide

Welcome to the HPE Network Virtualization Security Guide. This guide provides information for working with Network Virtualization in a secure environment.

Security requirements for the enterprise are constantly evolving and this guide should be viewed as HPE's best effort to meet those stringent requirements. If there are additional security requirements that are not covered by this guide, please open a support case with the HPE support team to document them and we will include them in future editions of this guide.

It is strongly recommended to run Network Virtualization on dedicated test machines that do not contain or provide access to sensitive information. In addition, you should also thoroughly review your lab network topology and access permissions before using Network Virtualization.

Secure Implementation and Deployment

For installation and deployment information, refer to the *HPE Network Virtualization User Guide*.

This section provides information on implementing and deploying Network Virtualization in a secure manner with the help of digital certificates.

A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a Certification Authority (CA). It contains the IP address of the machine for which it was issued, a validation date, and the digital signature of the certificate-issuing authority.

Certificates created by Network Virtualization utilities have the following attributes:

- Signature hash algorithm: sha256
- Encryption algorithm: RSA (2048 Bits)

Ports used by Network Virtualization

By default, NV Test Manager uses port 8182 for communication. You can change the NV Test Manager port during or after installation.

(Applies to NV 9.10 Patch 1 or later) If NV is set up as a proxy, it opens the port that the user defined during installation. This setting can be changed from the Test Manager **Settings** tab. The default port is 8888.

NV Server uses port 8443.

For details on changing the default ports, refer to the *HPE Network Virtualization User Guide*.

Generating and installing certificates

There are two instances when Network Virtualization generates digital certificates:

- When installing the NV Server.
- When installing any other Network Virtualization component in secure mode.

Network Virtualization doesn't install certificates to the operating system trusted Certificate Authorities Store (CA). When needed, the user can manually import the certificate into the CA.

When installing NV Analytics in secure mode, you should import the certificate into the CA of the Analytics computer. Consult with your system administrator on the process.

The self-signed certificate is issued per computer. The password is randomly generated.

(Applies to NV 9.10 Patch 1 or later) NV proxy uses the same certificate as NV Test Manager.

How to harden default security settings

You can heighten the security settings of the application in the following ways:

- Replace the self-signed certificate with a user created certificate. Consult with your system administrator on the process.
    - By default the certificate for the Apache Tomcat used by NV Server is installed under "C:\Program Files (x86)\HP\NVServer\ApacheTomcat\conf".
    - When replacing the NV Test Manager certificate, update the name, password, and location of the new certificate in the configuration file "C:\Program Files (x86)\HP\NV\conf\config.properties", under the following keys:
        - "com.shunra.bootstrapper.certificate.path"
        - "com.shunra.bootstrapper.certificate.pass". The password should be encrypted using the 'generateencrypted.bat' batch file located in the 'bin' folder.
- Use unique user ids and passwords for NV Server and NV Test Manager administrators and users. Refer to *HPE Network Virtualization User Guide* for details.
- Install NV Test Manager is secure mode. Refer to *HPE Network Virtualization User Guide* for details.
- During installation, change the default ports used by NV Test Manager. Refer to *HPE Network Virtualization User Guide* for details.
- When installing NV Test Manager or NV Analytics on a personal computer, don't allow opening the NV listening port in the firewall rules.

- Use firewall rules to prevent too many connections from a single host. This will mitigate run-of-the-mill Denial of Service attacks.
  Following is an example of an **iptables** command, which you can use to limit the number of concurrent connections that can be established to port 80 from a single client host:

```
# iptables -A INPUT -p tcp --syn --dport 80
-m connlimit --connlimit-above 50 -j REJECT
```

  This would, however, have side-effects if many users were legitimately connecting from a single IP (e.g. mega-proxy), so the number of connections would need to be tuned reasonably, depending on the traffic expected.

Network and Communication Security

This section provides information on network and communication security.

Securing communication using SSL certificates

Communication with NV Server is always done in a secure manner using TLS 1.0 or higher. This includes communication between NV Test Manager and NV Server as well as communication between NV Server and the user browser.

When NV Test Manger is installed in secure more, communication between the user browser and NV Test Manager is done in a secure manner using TLS 1.0 or higher.

(Applies to NV 9.10 Patch 1 or later) When NV proxy is used during a test, the NV proxy works as a 'man in the middle' proxy, were HTTPS traffic is encrypted between the client and the NV proxy and between the NV proxy and the server. While a test is running, the NV Proxy inspects the secure communication and analyses it. When no NV test is running, the NV proxy forwards the traffic to and from the server and clients.

APIs and References

This section provides information on user authentication.

Security features in the API

To use NV Application Programming Interface (API) the caller must authenticate to NV Test Manager or NV Server by passing a valid user name and password.
When working with NV Test Manager which is installed in secure mode, the API caller must use HTTPS communication.

Refer to the *HPE Network Virtualization API* documentation for more details.

General Questions

Question: How can I report security issues?
Answer: Report security issues using the following link:

https://h41268.www4.hpe.com/live/index.aspx?qid=11503

Question: Where can I obtain the latest information regarding security vulnerabilities in HPE Network Virtualization?

Answer: You can obtain the latest information regarding security vulnerabilities and also register for alerts, via this webpage:

https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/secBullArchive?ac.admitted=1389784040189.876444892.199480143