HP Network Automation Software

For the Linux operating system

Software Version: 10.00

Satellite Guide

Document Release Date: May 2014

Software Release Date: May 2014

Legal Notices

Warranty

The only warranties for HP 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. HP 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 HP 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 Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

AMD is a trademark of Advanced Micro Devices, Inc.

Intel and Intel Itanium are trademarks of Intel Corporation in the U.S. and other countries.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

UNIX® is a registered trademark of The Open Group.

Oracle Technology — Notice of Restricted Rights

Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

For the full Oracle license text, see the `license-agreements` directory on the NA product DVD.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: **http://h20230.www2.hp.com/selfsolve/manuals**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: **http://h20229.www2.hp.com/passport-registration.html**

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at: **http://www.hp.com/go/hpsoftwaresupport**

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Chapter 1: Getting Started

This document contains information about configuring the HP Network Automation Software (NA) Satellite functionality.

Note: The Detect Network Devices and OS Analysis tasks do not work for devices managed by an NA satellite.

Note: Satellite installations are only supported on supported operating systems running in English.

Note: This document is updated as new information becomes available. To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

For more information, see "Documentation Updates" on page 2.

Terminology

The following terms are used throughout this guide:

- **Realm** — A collection of reachable networks with no overlapping IP addresses.
- **IP Space** — One or more realms that have no overlapping IP addresses.
- **NA Core** — A single NA Management Engine and the associated services (for example, syslog and TFTP).
- **NA Gateway** — A service that tunnels traffic to and from managed devices. The NA gateway routes SSH and Telnet traffic to other gateways. The gateway enables you to manage servers behind NAT'd devices and firewalls. In addition, the gateway supports bandwidth throttling on tunnels between realms and can be used anywhere SSL proxying or TCP port forwarding is used. Tunnels can be authenticated and encrypted using SSL.
- **Core Gateway** — An NA gateway running in the same realm as an NA core. The core gateway is the same software as the remote gateway. You simply configure the core gateway differently for a core gateway than for a remote gateway. Note that the core gateway realm should be named "Default Realm" if there is only one NA core.

  Note: The Administrative Settings - Device Access page uses the term Local Gateway Host to refer to the core gateway.

- **Remote Gateway** — An NA gateway running in a realm that does not include an NA core.

- **NA Remote Agent** — The NA remote agent includes:
  - A process that handles SNMP and coordinates with the NA Management Engine on the NA core.
  - A Syslog process that handles syslog notifications from local devices.
  - A TFTP process that enables TFTP access to local devices.
- **Satellite** — The NA functionality for remotely managing devices. A satellite consists of a remote gateway and the an NA remote agent.
- **Tunnel** — A point-to-point TCP/IP connection on a single port between two NA gateways that enables the gateways to communicate. The tunnel is the result of the gateway functionality.
- **Gateway Mesh** — A collection of two or more NA gateways that route traffic among themselves. At a minimum, a gateway mesh consists of one core gateway and one remote gateway.
- **Gateway Crypto Data File** — Includes private and public keys for SSL communication between NA gateways.

What Does the Satellite Functionality Do?

Today's enterprise networks are complex and can include many types of circuits that bridge connections between the corporate headquarters and a remote office. Often, the link between these offices traverses a VPN connection over public networks, a limited bandwidth circuit, or both. Because of these variables, security and efficiency are often paramount concerns.

The NA satellite functionality provides a secure means to route packets from the NA core to remote networks by creating an encrypted tunnel between the NA core and remote network. When more than one remote gateway is present, the NA Management Engine creates a gateway mesh within the network of tunnels that enables the NA core to securely reach any remote gateway through the gateway mesh.

It is recommended that the core gateway is running on the same host as the NA core for the following reasons:

- Performance — You can avoid TCP/IP socket overhead.
- Security — Packets are sent internally and cannot be snooped by other hosts on the network. The connection between the NA core and the core gateway is not encrypted. As a result, using a local connection on the same host is more secure.

Tip: The NA gateway does not run on the Windows operating system. When the NA core server uses a Windows operating system, the core gateway must be on a different server from the NA core.

The NA satellite functionality can simplify communication between the NA core and remote networks by encrypting packets and limiting the number of firewall ports that need to be opened. This approach can simplify the initial setup when communications are restricted by firewalls or where communication between networks must be secured.

Currently, the Detect Network Devices and OS Analysis tasks do not work for devices managed by an NA satellite.

Is the Satellite Functionality Right for You?

You can use a Satellite configuration if you are managing:

- Devices over a fast LAN, with strict firewall rules between the NA Core. The NA Satellite may ease the management of connections between the NA Core and the devices.
- Devices that have overlapping IP addresses. The NA Core cannot directly manage two devices with the same IP address. With the Satellite functionality, it is possible to partition the network into Realms and access all devices directly.
- Devices that restrict TFTP to a local server for speed, but primarily for security. Traffic over a local network is more secure than traffic that must traverse a firewall and possibly enter the Internet.
- Devices with a slow WAN link and subject to network interruption during software upgrades. The Satellite, which is on the same LAN as the remote devices, caches software images so they only have to be copied across the wire, from the NA core to the Satellite, one time.

Keep in mind that you will need servers on which to run the Gateway Mesh. Each Gateway will need to be installed to properly create the Gateway Mesh.

Installation Prerequisites

Before installing the NA satellite functionality, note the following:

- Satellite installations are only supported on supported operating systems running in English.
- You will need servers on which to run the gateway mesh.
- Within a realm, the IP address space must be unique.
- A gateway mesh can be used to add encryption to Telnet-managed devices. Encrypting Telnet connections is only an encryption between the core gateway and the remote gateway. After the packets leave the gateway, they are in clear text.
- All traffic between gateways is encrypted using SSL with a private key (stored in the Gateway Crypto Data file) created for each gateway mesh.
- Gateways can throttle traffic between realms. This throttling is useful if NA is using a slow link to manage remote devices in an effort to assure NA does not saturate the link when capturing a device's configuration.
- Multiple gateways can be installed in the same realm for redundancy. As a result, a remote gateway has both a realm name and a gateway name.
- Install a core gateway before installing any remote gateways.
- TCP port 2001 must be open from the remote gateway to the core gateway.
- During installation of a remote gateway, port 9090 must also be open from the remote gateway to the core gateway. After the remote gateway has been installed, port 9090 is no longer needed.

Note: You do not need to open port 3333 in your firewall. The NA gateway installer uses port 3333 to ensure that a remote gateway is not being installed on the same server as a core gateway. The NA gateway installer listens on port 3333 and then tries to connect to the core gateway on port 3333. The connection to port 3333 is supposed to fail. If the connection succeeds, the NA gateway installer exits with an error.

Chapter 2: Installing the NA Satellite Functionality

Satellite installation consists of the following tasks:

1. Install a core gateway for one NA core as described in "Install the First Core Gateway" on page 12.

   This step creates the Gateway Crypto Data file for communication security.

2. Install additional core gateways, one for each remaining NA core as described in "Install Additional Core Gateways" on page 13

   This step uses the Gateway Crypto Data file that was created during installation of the first core gateway.

3. Install a remote gateway in each remote realm as described in "Install Remote Gateways" on page 14.

   This step uses the Gateway Crypto Data file that was created during installation of the first core gateway.

4. Configure NA as described in "Configure NA to Communicate with the Core Gateways" on page 15.

5. Deploy the remote agent to each remote gateway server as described in "Install the NA Remote Agent on a Remote Gateway Server" on page 17.

6. Assign devices to be managed by each satellite as described in "Assign Devices to Satellites" on page 18.

Tip: After the initial core gateway is installed, additional core gateways and remote gateways can be installed in any order. For each core gateway, also complete step 4. For each remote gateway, also complete step 5.

Recommendations

The following recommendations should be used to ensure that the NA satellite functionality is installed and running properly.

- Install a core gateway for each NA core.
- If the NA core runs on a platform that supports the NA satellite, it is recommended to install the core gateway on the NA core server. It the NA core server platform is not compatible with the NA satellite, install the core gateway on a different system.
- If there are multiple core gateways, each remote gateway should have a tunnel to each core gateway.

Security

After installing the NA core on a supported platform, install the core gateways on the same server. This approach ensures that communication between the NA core and the core gateway is private.

Be sure to keep the Gateway Crypto Data file (the NA gateway installer creates the Gateway Crypto Data file when you install the first core gateway), in a safe place. The private key in this file controls who can connect to the gateway mesh. Each NA gateway in the gateway mesh has its own encryption keys, and they must know the public key for the core gateway to join the gateway mesh.

Note: The password for accessing the Gateway Crypto Data file cannot be recovered. If you cannot remember this password, uninstall and then re-install the satellite mesh.

Redundancy

For redundancy, you can install multiple satellites in one realm.

Configuring NA Satellite Functionality for IPv6

As of NA 10.00, satellites can manage devices using IPv6. NA satellite functionality can be deployed in any of the following scenarios:

- IPv4 only—All NA cores and satellites use IPv4 for communicating with managed devices and each other.

  During installation of all gateways, answer **no** to the following question: `Is this GW part of IPv6 mesh?`

- Dual stack—All NA cores and satellites can use IPv6 or IPv4 for communicating with managed devices and each other.

  During installation of all gateways, answer **yes** to the following question: `Is this GW part of IPv6 mesh?`

  Also, answer **yes** to the following question: `Is this a dual-stack server?` Then, specify an IPv6 address in response to the following question: `IP address to connect to the gateway on this machine?`

Prepare the Gateway Server for the NA Gateway Installer

The NA gateway installer has several dependencies on the operating system. Prepare each gateway server as described here.

1. Install the packages provided with the NA gateway installer:

   a. Change to the `lib` directory where you unpacked the gateway installer bundle (`nas_gw-*.zip`).

   b. Run the following commands:

   ```
   rpm -ihv OPSWgw-ism-50.0.37394.0-1.x86_64.rpm
   rpm -ihv OPSWgw-50.0.37394.0-1.x86_64.rpm
   ```

2. The NA gateway installer requires 32-bit libraries. Ensure that the 32-bit libraries are available to the NA gateway installer. If necessary, install these libraries. For example, on Red Hat Enterprise Linux:

   ```
   yum install gtk2.i686
   yum install libXtst.i686
   ```

3. On all servers other than the first core gateway server, create symbolic links to the 64-bit libraries that the NA gateway installer needs:

   ```
   ln -s /usr/lib64/libcurl.so.<.X> /usr/lib64/libcurl.so.3
   ln -s /usr/lib64/libssl.so.<.X> /usr/lib64/libssl.so.6
   ln -s /usr/lib64/libcrypto.so.<.X> /usr/lib64/libcrypto.so.6
   ln -s /usr/lib64/libexpat.so<.X> /usr/lib64/libexpat.so.0
   ```

   Replace *.X* with the extension for the actual file in the `/usr/lib64` directory.

Install the First Core Gateway

Each core gateway is associated with one NA core. If the NA core runs on a platform that supports the NA satellite, it is recommended to install the core gateway on the NA core server. It the NA core server platform is not compatible with the NA satellite, install the core gateway on a different system.

Installing the first core gateway of a gateway mesh creates the Gateway Crypto Data file. This file includes public and private keys that enable SSL communication for the IP traffic within the gateway mesh. All other gateways in the gateway mesh also use this Gateway Crypto Data file.

During installation of the first core gateway, you will be asked to generate the following information:

- A password for access to the Gateway Crypto Data file
- The name of this gateway; choose a name that relates this gateway to the associated NA core

  Note: The gateway name cannot contain any spaces.

- The realm name; use `Default Realm` for all core gateways

Additionally, you might be asked for the following information:

- The IP address of the NA core server
- The location of the NA installation directory

To install the first core gateway

1. Log on to the gateway server as the root user.
2. Change to the directory containing the gateway installer bundle (`nas_gw-*.zip`).
3. Unzip the gateway installer bundle.

4. Prepare the gateway server as described in "Prepare the Gateway Server for the NA Gateway Installer" on page 11.
5. Run the gateway installer:

   ```
   perl install.pl
   ```

6. Supply the required information.

   Under Common Options, enter the number for the option to `Configure a new core mesh`.

7. If the core gateway is not on the NA core server, store a copy of the `saOPSWgw*/certificates/opswgw-mngt-server.pkcs8` file for later use.

Install Additional Core Gateways

Each core gateway is associated with one NA core. If the NA core runs on a platform that supports the NA satellite, it is recommended to install the core gateway on the NA core server. It the NA core server platform is not compatible with the NA satellite, install the core gateway on a different system.

During installation of each additional core gateway, you will be asked to generate the following information:

- The name of this gateway; choose a name that relates this gateway to the associated NA core

  Note: The gateway name cannot contain any spaces.

- The realm name

Additionally, you might be asked for the following information:

- The location of the directory containing the Gateway Crypto Data file (`opswgw-crypto.tgz.e`) that was created during installation of the first core gateway
  - If you copy the Gateway Crypto Data file to the gateway server before starting the installation, specify the path to the location of this file on the local server.
  - To use the Gateway Crypto Data file on the first core gateway server, use SCP format to specify the path. For example, `LOGINNAME@coregw1:/tmp/gw`
- The password for access to the Gateway Crypto Data file
- The IP address of the NA core server
- The location of the NA installation directory

To install an additional core gateway

1. Log on to the gateway server as the root user.
2. Change to the directory containing the gateway installer bundle (`nas_gw-*.zip`.).
3. Unzip the gateway installer bundle.
4. Prepare the gateway server as described in "Prepare the Gateway Server for the NA Gateway Installer" on page 11.
5. Run the gateway installer:

   ```
   perl install.pl
   ```

6. Supply the required information.

   Under Common Options, enter the number for the option to `Add a new core gateway to an existing mesh`. (Ensure that the option includes the word "core.")

7. If the core gateway is not on the NA core server, store a copy of the `saOPSWgw*/certificates/opswgw-mngt-server.pkcs8` file for later use.

Install Remote Gateways

Install a remote gateway in every realm that does not have an NA core.

During installation of each remote gateway, you will be asked to generate the following information:

- The name of this gateway; choose a name that relates this gateway to the associated NA core

  Note: The gateway name cannot contain any spaces.

- The realm name; use a different realm name for each remote gateway

Additionally, you might be asked for the following information:

- The location of the directory containing the Gateway Crypto Data file (`opswgw-crypto.tgz.e`) that was created during installation of the first core gateway
  - If you copy the Gateway Crypto Data file to the gateway server before starting the installation, specify the path to the location of this file on the local server.
  - To use the Gateway Crypto Data file on the first core gateway server, use SCP format to specify the path. For example, `LOGINNAME@coregw1:/tmp/gw`
- The password for access to the Gateway Crypto Data file

- The IP address of the NA core server
- The location of the NA installation directory

To install a remote gateway

1. Log on to the gateway server as the root user.
2. Change to the directory containing the gateway installer bundle (`nas_gw-*.zip`.).
3. Unzip the gateway installer bundle.
4. Prepare the gateway server as described in "Prepare the Gateway Server for the NA Gateway Installer" on page 11.
5. Run the gateway installer:

   ```
   perl install.pl
   ```

6. Supply the required information.

   Under Common Options, enter the number for the option to `Add a new gateway to an existing mesh`. (Ensure that the option does *not* include the word "core.")

Configure NA to Communicate with the Core Gateways

To configure each NA core to communicate with the associated core gateway, do the following:

1. If the core gateway is not installed on the NA core server, copy the `opswgw-mngt-server.pkcs8` file from the core gateway to the `<NA_HOME>` directory, typically `C:\NA` or `/opt/NA`.
2. Log on to the NA console as an NA administrator.
3. On the Administrative Settings - Device Access page (**Admin > Administrative Settings > Device Access**), under Gateway Mesh, identify the core gateway.

   For the **Local Gateway Host** field, enter the DNS hostname or IP address of the core gateway associated with this NA core. If the core gateway is installed on the NA core server, specify `localhost`. This value was entered as the IP address of the core application server during installation of the core gateway.
4. Click **Save**.

Gateways Page

To test whether NA can communicate with the Core Gateway, on the main menu bar, click **Admin > Gateways**. The Gateway List page opens. The Gateway List page displays the currently configured Gateways and enables you to edit Gateway information. For information, see "Edit Gateway Page" on page 17.

Table 3 describes the Gateway List page.

Table 3 Gateway List Page Fields

Field	Description/Action
Deploy Remote Agent link	Open the Deploy Remote Agent page, where you can deploy an NA remote agent.
IP Space	Displays the IP space name. An IP space is one or more Realms that have no overlapping IP addresses.
Realm	Displays the Realm name. The Realm name is returned from the Gateway. The Realm name is set when the Gateway is installed and cannot be modified in NA. To change the Realm name, re-install the Gateway.
Gateway	Displays the Gateway name. The Gateway name is set when the Gateway is installed and cannot be modified in NA.
Host	Displays the hostname or IP address of the server on which the gateway is installed. If the gateway server has multiple IP addresses, this is the IP address that would be used from the gateway server. The Host IP address is only important if you have more than one gateway installed in the same realm. **Note:** You can install multiple satellites in the same realm for redundancy.
Partition	Displays the NA Partition name associated with the Realm name, if applicable.
Core	In a Multimaster Distributed System environment, the Core name is set on the Edit Core page. If the Realm name on the Edit Core page matches the Realm name for a Gateway, the Gateway List page displays the Core name of the Core.
Agent	Displays the name of the NA remote agent for satellites. The NA remote agent name can be changed on the Edit Gateway page. After you have installed the gateway mesh, you must install an NA remote agent on each remote gateway server. If no NA remote agents are installed, the Agent column is empty.
Actions	There is one option: • Edit — Opens the Edit Gateway page.

Edit Gateway Page

NA automatically sets the IP space name based on the realm name. If diagramming is enabled, each IP space is diagrammed separately. To show two realms in the same IP space diagram, edit the gateway to set the IP space name.

To open the Edit Gateway page, on the Gateway List page, click the Edit option in the Actions column. Table 4 describes the Edit Gateway page.

Table 4 Edit Gateway Page Fields

Field	Description/Action
Gateway	Displays the Gateway name. The Gateway name is set when the Gateway is installed and cannot be modified in NA.
Realm	Displays the Realm name. The Realm name is returned from the Gateway. The Realm name is set when the Gateway is installed and cannot be modified in NA.
IP Space	Displays the IP space name. An IP space is one or more Realms that have no overlapping IP addresses. Enter a new IP space name.
Host	Displays the hostname or IP address of the system on which the Gateway is installed. Enter a new host name or IP address.
Satellite	Displays the remote gateway running in a realm that does not have an NA core. This field is not editable. To change the satellite name, uninstall and then reinstall the remote gateway.

Install the NA Remote Agent on a Remote Gateway Server

On each satellite, the remote agent communicates with the devices that the satellite manages. Use the Deploy Remote Agent task in the NA console to install the remote agent onto the remote gateway server. Installing the remote agent on the remote gateway server completes the satellite configuration.

To install the NA remote agent on a remote gateway server

1. Log on to the NA console as an NA administrator.
2. On the Deploy Remote Agent page (**Tasks > New Task > Deploy Remote Agent**), configure the deploy agent task.

   Under Task Options, note the following:

   - For **Action**, select Install **(or Reinstall)**.
   - For **Deploy Agent to Gateway**, select the target remote gateway from the list.

- For **Login**, do one of the following:
  - Select **As Root**, and then enter the password for the root user on the remote gateway server.
  - Select **As Non-root**, select the method for gaining root access to the remote gateway server, and then enter the relevant password.
- For **Managing Core**, enter the IP address of the NA core that should receive communication from the remote gateway. This value was entered as the IP address of the core application server during installation of the core gateway. For dual-stack satellites, use only the IPv4 portion of the IP address.
- For **In Realm**, select the realm name of the core gateway associated with the managing core. In most cases, this value is `Default Realm`.

For more information, see "Deploy Remote Agent Page Fields" in the NA help.

3. Click **Save**.
4. *Dual stack satellites only*. After deploying the remote agent, set the TFTP server on the satellite to run on the IPv6 address of the remote gateway server.
   a. Connect to the remote gateway server as the root user.
   b. Change to the following directory:

      ```
      /opt/opsware/nassat/jre
      ```

   c. Back up the `nassat.rcx` file to a location outside the gateway installation directory.
   d. In a text editor, such as vi, open the `nassat.rcx` file.
   e. Add the following line:

      ```
      <option name="TFTP/Server/IPv6">$ipV6address$</option>
      ```

   f. In the new line, replace `$ipV6address$` with the IP address of the remote gateway server.
   g. Save the `nassat.rcx` file.
   h. Restart the gateway by running the following command:

      ```
      /etc/init.d/nassat restart
      ```

Assign Devices to Satellites

For each satellite, specify which devices that satellite should manage. Follow these steps:

1. Log on to the NA console as an NA administrator.
2. On the Partitions page (**Admin > Security Partitions**), click **New Partition**.

3. Enter a partition name, select the realm name of the remote gateway for the satellite, and then select the devices that the satellite should manage.

Gateway Communication Configuration

For each gateway, the `/etc/opt/opsware/opswgw-<gateway_name>/opswgw-properties` file configures communication within the gateway mesh.

This topic describes several of the gateway communication configuration properties.

Tunnel Source

The `opswgw.TunnelSrc` parameter defines a tunnel between this gateway and the gateway identified in the parameter. Each gateway directs communication on the available tunnel with the lowest cost.

The tunnel source consists of the following fields:

- IP address of the target gateway server
- Port on the target gateway server that receives communications from this gateway
- Tunnel cost, which applies in the case of redundant satellites and backup tunnels (for example, with disaster recovery configuration)
- Bandwidth, which can throttle traffic from the gateway; 0 equates to no throttling
- Location of the gateway crypto data file

In the IPv4-only format, the field separator is the colon (:). For example:

```
opswgw.TunnelSrc=10.68.5.1:2001:100:0:/var/opt/opsware/crypto/opswgw-
RemoteGw/opswgw.pem
```

As of NA 10.00, dual-stack installations use the at sign (@) as the field separator. For example:

```
opswgw.TunnelSrc=fc00:aff:38:1:250:56ff:feba:33b4@2001@100@0@/var/opt/opsware/c
rypto/opswgw-RemoteGw/opswgw.pem
```

Egress Filter

The `opswgw.EgressFilter` parameter identifies the protocols and associated ports over which the gateway can send traffic to other gateways.

- For a core gateway, the egress filter defines the supported communication to all remote gateways.
- For a remote gateway, the egress filter defines the supported communication to some or all of the gateways in the gateway mesh.

The egress filter contains multiple comma-separated entries. Each entry consists of the following fields:

- Protocol name (tcp or udp)
- Destination IP address; use the asterisk (*) wildcard to permit connections to any endpoint
- Destination port number
- Source IP address; on a core gateway, this value can be a name from the ingress map
- Source realm; leaving this field blank limits the connections to those coming from a root realm, that is from a core gateway to a remote gateway

In the IPv4-only format, the field separator is the colon (:). For example:

```
opswgw.EgressFilter=tcp:*:443:127.0.0.1:*,tcp:*:22:NA:,tcp:*:23:NA:,tcp:*:513:N
A:
```

As of NA 10.00, dual-stack installations use the at sign (@) as the field separator. For example:

```
opswgw.EgressFilter=tcp@*@443@::ffff:127:0:0:1@*,tcp@*@22@NA@,tcp@*@23@NA@,tcp@
*@513@NA@
```

Ingress Map

The `opswgw.IngressMap` parameter maps the IP address of a source host to a recognizable name that is used in the egress filter. The ingress map applies to core gateways only.

The ingress map contains multiple comma-separated entries. Each entry consists of the following fields:

- IP address
- Name

In the IPv4-only format, the field separator is the colon (:). For example:

```
opswgw.IngressMap=127.0.0.1:NA
```

As of NA 10.00, dual-stack installations use the at sign (@) as the field separator. For example:

```
opswgw.IngressMap=::ffff:127:0:0:1@NA
```

Changing the Gateway Communication Configuration

When NA documentation or Support recommends changing any of the parameters in the `opswgw-properties` file, follow these steps:

1. Connect to the gateway server as the root user.
2. Change to the following directory:

   `/etc/opt/opsware/opswgw-<gateway_name>`

3. Back up the `opswgw.properties` file to a location outside the gateway installation directory.
4. In a text editor, such as vi, open the `opswgw.properties` file.
5. Edit the specified parameters.
6. Restart the gateway by running the following command:

   ```
   /etc/init.d/nassat restart
   ```

Handling Multiple NICs on the Satellite Host

If the remote gateway server has multiple Network Interface Cards (NICs), you can configure the satellite to use a particular NIC. After installing the remote agent, edit the `/opt/opsware/nassat/jre/nassat.rcx` file to change the value for `tftp/server` to the gateway NIC IP address devices should use to TFTP their configurations to the satellite.

You should also change the `syslog/server` value in the `nassat.rcx` file. This is the logging address that is configured on a device when the Configure Syslog task is run in NA.

Note: Each time you re-deploy the remote agent, you must modify the `nassat.rcx` file again.

Enabling SCP Transfers from a Satellite

By default, NA supports TFTP only for backing up device software and configurations through the satellite. To enable SCP transfers from remotely-managed devices to the satellite, follow these steps:

1. Identify an SCP account to use. Navigate to the FTP and SSH Device Access section of the Administrative Settings - Device Access page (**Admin > Administrative Settings > Device Access**).
   - If values are specified for the `FTP/SSH User` and `FTP/SSH Password` fields, you must use this information for the SCP account.
   - If no values are specified for the `FTP/SSH User` and `FTP/SSH Password` fields, determine a user name and password to use for the SCP account. Configure that account.

     Note: The FTP/SSH user name must be different from the NA user names for accessing the NA console.

2. On the satellite system, configure the identified SCP account. For example, the following commands configure an account with user name `nascp` and password `napass`:

   ```
   chmod -R o+rx /opt/opsware/nassat/server/ext/tftp
   useradd -d /opt/opsware/nassat/server/ext/tftp/tftpdroot nascp
   passwd nascp
   ```

   At the password prompt, enter: `napass`

Note: The home directory for this user must be `/opt/opsware/nassat/server/ext/tftp/tftpdroot`.

3. On the NA core server, add the `DeviceAccess/scp/allow_satellite` option to the `adjustable_options.rcx` file:
   a. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
   b. In the `adjustable_options.rcx` file, add the following line:

```
<option name="DeviceAccess/scp/allow_satellite">true</option>
```

   c. Save the `adjustable_options.rcx` file.
   d. Reload the .rcx settings by doing one of the following:
      - Run the `reload server options` command from the NA proxy.
      - Restart the NA services.

Uninstall an NA Satellite

To remove an NA satellite from the gateway mesh, do the following:

1. Remove the remote agent from the remote gateway server as described in "Removing the Remote Agent from the Remote Gateway Server" below.
2. Uninstall the remote gateway as described in "Uninstalling a Gateway" on the next page.

Removing the Remote Agent from the Remote Gateway Server

The remote agent must be removed before uninstalling the remote gateway. To uninstall the remote agent from the remote gateway server, follow these steps:

1. Log on to the NA console as an NA administrator.
2. On the menu bar, click **Tasks > New Task > Deploy Remote Agent**. The Deploy Remote Agent page opens. (You can also navigate to this page by clicking the Deploy Remote Agent link on the Gateway List page.)
3. Under Task Options in the Action field, click **Uninstall**.
4. Click **Save Task**.

Uninstalling a Gateway

To uninstall a gateway, do the following:

1. Change to the directory where you unzipped the `gateway.zip` file to install the gateway.
2. Enter the following command:

   ```
   ./saOPSWgw*/uninstall --removeall
   ```

3. *Optional*. Delete the gateway installation directory.

Upgrading the Satellite Mesh

To upgrade the NA satellite mesh from NA 9.xx to NA 10.00, follow these steps:

1. Identify servers for the core gateways and the satellites that meet the satellite specifications listed in the *NA Support Matrix*.
2. Uninstall the remote agent from each satellite in the gateway mesh as described in "Removing the Remote Agent from the Remote Gateway Server" on the previous page.
3. On each core gateway server or remote gateway server, uninstall the gateway as described in "Uninstalling a Gateway" above.
4. Install the satellite mesh as described in "Installing the NA Satellite Functionality" on page 10.

Appendix A: Troubleshooting

The NA Satellite has two levels of security to ensure that unauthorized processes cannot access the Satellite. Failures in the NA Satellite are usually the result of a configuration error that causes these security checks to deny connections. The following sections describe how to check these security levels if NA Satellite operations are failing.

NA Gateway Installer Error Messages

The following error message indicates that the NA gateway installer cannot access needed 64-bit libraries:

```
wget: error while loading shared libraries: libssl.so.6: cannot open shared
object file: No such file or directory
```

To correct the problem, create the symbolic links to the needed libraries as described in "Prepare the Gateway Server for the NA Gateway Installer" on page 11.

Security in the Gateway Mesh

The first security level is in the Gateway Mesh. Only the NA Core host is allowed to connect to the Core Gateway. If the Core Gateway is installed with the incorrect IP address of the NA Core, connections will fail.

To check if the Gateway Mesh security is denying a connection, look for the word “disallow” in the Core Gateway log file by executing the following command at a shell prompt on the Core Gateway host:

```
grep disallow /var/log/opsware/opswgw-*/opswgw.log
```

If there is a line that states a connection is disallowed from a certain IP address, the security on the Core Gateway is the issue. The solution is to make sure the NA Admin Setting for Local Gateway and Gateway IngressMap are in sync.

If the Core Gateway is on the same host as the NA Core, the IP address in the IngressMap should be 127.0.0.1. The Local Gateway Admin Setting should be localhost or 127.0.0.1.

If the Core Gateway is on a separate host, the Local Gateway Admin Setting must have the correct IP address of the Core Gateway. The IngressMap must have the correct IP address of the NA Core host.

To modify the IngressMap line in the `properties` file, edit the `/etc/opt/opswgw-*/opswgw.properties` file. If there is more than one Gateway installed, replace the asterisk (*) with the name of the Gateway. Find the IngressMap line that looks like the following:

```
opswgw.IngressMap=127.0.0.1:NA
```

Security in the NA Core and Satellite

The second security level is in the NA Core and NA Satellite. They only accept connections from known hosts.

On the NA Core, the known host is the Local Gateway Admin Setting. On the Satellite, the known host is always localhost. To check for this, look for “Rejected” in the NA Core jboss wrapper log. Enter:

```
grep Rejected $NA/server/log/jboss_wrapper.log
```

(where `$NA` is the root of your NA Core installation).

If the Deploy Remote Agent task was run with an incorrect hostname for the NA Core host, the Satellite will not be able to connect back to the NA Core. To check for this, enter the above 'grep' command on the NA Satellite host. For information, see "Removing the Remote Agent from the Remote Gateway Server" on page 22.

In addition, check to ensure that the EgressFilter on the Core Gateway has the correct IP address for the NA Satellite by editing the Gateway *properties* file on the Satellite host. Locate the line that looks like the following:

```
opswgw.EgressFilter=tcp:*:443:XXX.XXX.XXX.XXX:*,tcp:*:22:NA:,tcp:*:23:NA:,tcp:*
:513:NA:
```

(where `XXX.XXX.XXX.XXX` is 127.0.0.1).

Redundant Core Gateways are not supported by the Gateway installer. However, if you want to have redundant Core Gateways (not recommended), edit the `adjustable_options.rcx` file and add the other Core Gateway IP addresses by adding the following lines to the file:

```
<array name="rpc/allowed_ips">
<value>10.255.52.10</value>
<value>10.255.54.22</value>
</array>
```

The IP addresses above should be replaced with the correct IP addresses for your NA Core Gateways.

Appendix B: Sharing the Gateway Mesh

This appendix includes information about setting up HP Network Automation Software (NA) and HP Server Automation Software (SA) to share the same gateway mesh.

Overview

Keep the following in mind when sharing the gateway mesh:

- Start by creating the gateway mesh for an SA installation. NAcan use the gateway mesh that is installed by SA, but SA cannot use the gateway mesh installed by NA.
- During configuration, modify the SA core gateways used by NA to identify the NA hosts to the gateway mesh.
- During configuration, modify the SA satellites to enable egress to the ports that NA uses to manage devices.

Installation Steps

For each NA core, identify the SA core gateway that will be used by that NA core:

1. On the SA host, edit (or create) the `/etc/opt/opsware/opswgw-cgws`*`N`*`-`*`core`*`/opswgw.custom` file.
   - *N* is the SA core number.
   - *core* is the SA core name.

   For example: `/etc/opt/opsware/opswgw-cgws1-VMCORE1/opswgw.custom`
2. Add the following lines to the end of the file:

   ```
   opswgw.EgressFilter=tcp:*:443:127.0.0.1:*
    opswgw.IngressMap=192.168.99.1:NA
   ```
3. Change `192.168.99.1` to the correct IP address for the NA core.
4. If the SA gateway mesh includes multiple core gateway (cgw) slices, do the following:
   a. Add an IngressMap entry for NA to each of them to the `/etc/opt/opsware/opswgw-cgws`*`N`*`-`*`core`*`/opswgw.custom` file.
   b. Edit the `<NA_HOME>/jre/adjustable_options.rcx` file to insert the following lines immediately before the `</options>` at the end of the file:

      ```
      <array name="rpc/allowed_ips">
          <value>192.168.99.2</value>
      </array>
      ```
   c. Change `192.168.99.2` to the correct IP address for the second core gateway slice.

d. For each core gateway slice, insert a copy of the `<value>192.168.99.2</value>` line between the `array` statements, and then set the IP address to the correct value for one core gateway slice.

Currently, NA can only use one core gateway slice, but future versions might be able to fail over to other slices.

5. Restart the core gateway:

```
/etc/init.d/opswgw-sas restart opswgw-cgws
```

If more than one NA core uses the same SA core gateway, add multiple lines to each file, one line for the IP address of each NA core.

For each remote gateway that NA uses:

1. Edit the `/etc/opt/opsware/opswgw-`*gateway*`/opswgw.properties` file.

   gateway is the name of the gateway specified at SA satellite installation time.

2. Add the following lines:

```
opswgw.EgressFilter=tcp:*:22:NA:,tcp:*:23:NA:,tcp:*:513:NA:,tcp:*:80:NA:,tcp
:*:443:NA:
opswgw.EgressFilter=tcp:127.0.0.1:8443:NA:
opswgw.ProxyPort=3002
```

   These lines provide the following configuration:

   - The first line enables NA to use all of the ports that are needed to manage different types of devices (SSH, Telnet, rlogin, http, and https).
   - The second line enables the NA core to communicate with the NA remote agent that listens for RPC calls on port 8443.
   - The third line adds a second ProxyPort that matches the ProxyPort that NA expects (3002).

3. Restart the remote gateway:

```
/etc/init.d/opswgw-sas restart opswgw
```

4. Copy the `spog.pkcs8` file from the `/var/opt/opsware/crypto/twist/spog.pkcs8` on the SA host to `<NA_HOME>/spog.pkcs8` on the NA host.

   `<NA_HOME>` is the directory where NA is installed.

5. In the NA console, open the Admin Settings - Device Access page (**Admin > Administrative Settings > Device Access**).

6. In the Gateway Mesh section of the Admin Settings - Device Access page, configure NA to use the SA core gateway.

   - **Local Gateway Host**: IP Address of SA (core gateway) host
   - **Local Gateway Proxy Port**: 3002
   - **Local Gateway Admin Port**: 8085
   - **Gateway Admin Private Key Filename**: spog.pkcs8

   For information, see the *NA User Guide*.

7. For each remote gateway host, run the Deploy Remote Agent task in the NA console.

8. If an SA satellite is running the OS Provisioning Media Server, reconfigure the NA remote Agent on that host to use the TFTP server used by the OS Provisioning Media Server.

   a. Edit the `/opt/opsware/nassat/nassat.rcx` file to set the value for the `TFTP/Server` option to `/opt/opsware/boot/tftpboot` (the path to the TFTP root directory used by the OS Provisioning Media Server).

   b. Edit the `/etc/xinetd.d/tftp` file to change `server_args = -s /tftpboot` to `server_args = -c -s /tftpboot`

      The `-c` flag enables NA to create files in the TFTP root directory. This function is needed to capture network device configurations. (SA uses TFTP to push files out to servers. As a result, the create ability is not needed for SA.)

   c. Verify that the `/opt/opsware/boot/tftpboot` directory is owned by the user specified in the `/etc/xinetd.d/tftp` file.

   d. Restart the TFTP daemon (in.tftpd) by sending the HANGUP signal to the xinetd process:

      ```
      kill -1 `ps ax | grep xinetd | grep -v grep | awk '{print $1}'`
      ```

9. Edit the `/etc/init.d/nassat` file and comment out the StartTFTP line by putting a number sign (`#`) at the front of the line:

   ```
   # StartTFTP
   ```

10. Restart the NA agent:

    ```
    /etc/init.d/nassat restart
    ```

Uninstalling the Gateway Mesh

To uninstall the gateway mesh:

1. For each remote gateway host, in the NA console run the Deploy Remote Agent task with **Uninstall** selected.
2. For each remote gateway used by NA:
   a. Edit the `/etc/opt/opsware/opswgw-gateway/opswgw.properties` file

      gateway is the name of the gateway specified at SA satellite installation time.

   b. Remove the following lines from the file:

      ```
      opswgw.EgressFilter=tcp:*:22:NA:,tcp:*:23:NA:,tcp:*:513:NA:,tcp:*:80:NA:,
      tcp:*:443:NA:
      opswgw.EgressFilter=tcp:127.0.0.1:8443:NA:
      ```

   c. Restart the remote gateway:

      ```
      /etc/init.d/opswgw-sas restart opswgw
      ```

3. In the NA console, open the Admin Settings - Device Access page (**Admin > Administrative Settings > Device Access**).
4. In the Gateway Mesh section of the Admin Settings - Device Access page, configure NA to not use any gateways by clearing the **Local Gateway Host** field.

   For information, see the *NA User Guide*.

We appreciate your feedback!

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Satellite Guide, May 2014 (Network Automation Software 10.00)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to ovdoc-nsm@hp.com.