

Brocade Vyatta Network OS VNF Platform Automated Provisioning User Guide, 5.2R1

Supporting VNF Platform

© 2016, Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, and MyBrocade are registered trademarks of Brocade Communications Systems, Inc., in the United States and in other countries. Other brands, product names, or service names mentioned of Brocade Communications Systems, Inc. are listed at www.brocade.com/en/legal/brocade-Legal-intellectual-property/brocade-legal-trademarks.html. Other marks may belong to third parties.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. assume no liability or responsibility to any person or entity with respect to the accuracy of this document or any loss, cost, liability, or damages arising from the information contained herein or the computer programs that accompany it.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit <http://www.brocade.com/support/oscd>.

Contents

About This Guide	5
Zero Touch Provisioning	7
Overview.....	7
Limitations.....	7
Architecture.....	7
Prerequisites.....	8
Configuration sample.....	8
Zero Touch Provisioning with a Preconfigured Bootstrap Server Address	11
Overview.....	11
Prerequisites.....	11
Terminology.....	11
Staging Zero Touch configuration on VNF platform.....	12
Setting up VNF platform for interactive bootstrap.....	12
Configuring the ztc.cfg file.....	12
Example of the ztc.cfg file.....	13
Bootstrap server requirements.....	13
Accessing bootstrap status	14
Configuring Zero Touch Provisioning at the branch.....	14
Call Home	17
Overview.....	17
Limitations.....	17
Configuration sample.....	17
Automated Provisioning Commands	19
service netconf call-home netconf-client <host_ip_address> port <port_number>.....	20
service netconf call-home netconf-client <host_ip_address> disable	21
show service netconf call-home status.....	22
Contacting Brocade Technical Support	23
Brocade customers.....	23
Brocade OEM customers.....	23

About This Guide

This guide describes how to configure Zero Touch Provisioning and Call Home for VNF platform.

Zero Touch Provisioning

- Overview.....7
- Limitations.....7
- Architecture.....7
- Prerequisites.....8
- Configuration sample.....8

Overview

VNF platform systems that are shipped with Zero Touch Provisioning enable you to deploy VNF platform automatically at the business site after you connect it to the Network Management System (NMS) network.

Zero Touch Provisioning enables you to set up VNF platform in your local or remote business site securely without the requirement of on-site network administrators.

Brocade Zero Touch Provisioning conforms to version 3 of the IETF draft titled *Zero Touch Provisioning for NETCONF Call Home*, available at <https://tools.ietf.org/html/draft-ietf-netconf-zerotouch-03>.

Limitations

The Brocade implementation of Zero Touch Provisioning has some limitations. Brocade Zero Touch Provisioning does not support image upgrades to VNF platform.

Architecture

You can refer to the IETF draft of the Zero Touch Provisioning feature for an understanding of the general architecture and work flow. This section describes the Brocade-specific components for Zero Touch Provisioning.

The Zero Touch Provisioning architecture consists of the following components:

Vendor	Specifies the Zero Touch device supplier, such as Brocade Communications Systems, Inc., Inc. The vendor provides the serial numbers and ownership vouchers for VNF platform.
Zero Touch system	Specifies VNF platform. After a vendor ships VNF platform with a factory configuration and some authentication information, you can connect the system to the Zero Touch network. VNF platform attempts the bootstrapping process when booting with the default factory configuration.
DHCP server	Specifies the DHCP server to which VNF platform attempts connection. If the connection is successful, the DHCP server dynamically assigns the network configuration parameters to VNF platform, such as IP addresses for interfaces and services. In addition, VNF platform may discover other bootstrap servers. VNF platform sequentially processes its list of bootstrap servers, prioritizing any that might have been discovered from the DHCP server. After VNF platform has successfully configured itself using the bootstrapping information, it notifies the bootstrapping server for monitoring purposes.
Bootstrap server	Provides the default VNF platform image and configuration to VNF platform. The bootstrap server presents a simple REST interface to VNF platform to obtain its bootstrapping information and notifies the bootstrapping server when it has successfully completed the bootstrapping process.
NMS	Specifies the server you deploy to establish a secure NETCONF connection to VNF platform.

Prerequisites

For the Zero Touch feature to be activated, it is essential that your network includes the DHCP server, bootstrap server, and NMS. All these components are described in the Zero Touch architecture.

The following list presents some key configurations for your network to enable Zero Touch Provisioning.

- Configure the DHCP server in your network to add `option 199`, which provides the IP address of the bootstrap server.
- Configure the bootstrap server to add VNF platform (based on the serial number) to the RESTCONF data store. The data store must be modeled as defined in the YANG module referred to in version 3 of the IETF draft titled *Zero Touch Provisioning for NETCONF Call Home*, available at <https://tools.ietf.org/html/draft-ietf-netconf-zerotouch-03>.
- Connect the Zero Touch-designated port of VNF platform (commonly the WAN port) to the network containing the DHCP server that is ready to supply `option 199`. After you power on VNF platform, the VNF platform configuration is fetched and loaded into the system.

Configuration sample

The configuration embedded in VNF platform must be a complete Vyatta-configuration boot file format.

```
-- start of response--
<?xml version='1.0' encoding='UTF-8'?>
<configuration>
<config>
<vyatta-config>
interfaces {
  dataplane dp0s3 {
    address 192.168.17.100/24
    address 3.3.3.3/24
  }
  dataplane dp0s4 {
    address 192.168.100.100/24
    address 2.2.2.2/24
  }
  dataplane dp0s8 {
    address dhcp
  }
}
service {
  netconf
  ssh
}
system {
  acm {
    enable
    operational-ruleset {
      rule 9985 {
        action allow
        command /show/tech-support/brief/
        group vyattaop
      }
      rule 9986 {
        action deny
        command /show/tech-support/brief
        group vyattaop
      }
      rule 9987 {
        action deny
        command /show/tech-support
        group vyattaop
      }
      rule 9988 {
        action deny
      }
    }
  }
}
```



```

        command /show/configuration
        group vyattaop
    }
    rule 9989 {
        action allow
        command "/clear/*"
        group vyattaop
    }
    rule 9990 {
        action allow
        command "/show/*"
        group vyattaop
    }
    rule 9991 {
        action allow
        command "/monitor/*"
        group vyattaop
    }
    rule 9992 {
        action allow
        command "/ping/*"
        group vyattaop
    }
    rule 9993 {
        action allow
        command "/reset/*"
        group vyattaop
    }
    rule 9994 {
        action allow
        command "/release/*"
        group vyattaop
    }
    rule 9995 {
        action allow
        command "/renew/*"
        group vyattaop
    }
    rule 9996 {
        action allow
        command "/telnet/*"
        group vyattaop
    }
    rule 9997 {
        action allow
        command "/traceroute/*"
        group vyattaop
    }
    rule 9998 {
        action allow
        command "/update/*"
        group vyattaop
    }
    rule 9999 {
        action deny
        command "*"
        group vyattaop
    }
}
ruleset {
    rule 9999 {
        action allow
        group vyattacfg
        operation "*"
        path "*"
    }
}
}
console {
    device ttyS0 {
        speed 9600
    }
}

```

Configuration sample

```
}
login {
  user vyatta {
    authentication {
      encrypted-password $1$4XHPj9eT$G3ww9B/pYDLSXC8YVvazP0
    }
    level superuser
  }
}
syslog {
  global {
    facility all {
      level warning
    }
  }
}
}
</vyatta-config>
</config>
<signature>
I+A/RS0SntreEboQH20w/4uMwKjB3xa17ERA9NYhdp7C5umLb1Jq4dEzd3LuWALnPcNebaLTIH9xI
Kn30l+CogkasgwrenQYQKlugHNkCqk4cBnTe/b5Jd4k1POF9wIq7trzfQgCSfbC0Sf4EsOtHKkyA
aMCyWAgxwqyxJVkBS+Q=
</signature>
</configuration>
-- end of response --
```

Zero Touch Provisioning with a Preconfigured Bootstrap Server Address

- Overview.....11
- Prerequisites..... 11
- Terminology..... 11
- Staging Zero Touch configuration on VNF platform..... 12
- Configuring Zero Touch Provisioning at the branch.....14

Overview

This chapter describes an alternative Zero Touch Provisioning that a service provide can implement.

Zero Touch Provisioning with a preconfigured bootstrap server address gives you an option to configure VNF platform during the first deployment at the business site after you connect it to the Network Management System network.

For information on the architecture of Zero Touch Provisioning, refer to [Architecture](#) on page 7.

Prerequisites

Zero Touch Provisioning with a preconfigured bootstrap server address requires the following components.

TABLE 1 Zero Touch components

Components	Description
Activation computer	A laptop or other computer system that is connected to the LAN port of VNF platform to launch a web browser.
Bootstrap server	A server that waits for registration requests from the VNF platform, authenticates the VNF platform device, authorizes the user that is in possession of the device by using an activation code and notifies other systems about the availability of the VNF platform device for further action.

Terminology

The following list describes some of the terms that are associated with Zero Touch Provisioning with a preconfigured bootstrap server address.

- Device authentication—SSL certificate validation by the bootstrap server or VNF platform.
- Activation code—Code required to activate VNF platform.
- Notification—Notification sent by VNF platform after the bootstrap configuration process is completed.
- Bootstrap status page—Portal on which you can verify the status of VNF platform. The status page is available only after the bootstrap server reboot is completed.

Staging Zero Touch configuration on VNF platform

This section describes the process of setting up the default VNF platform configuration, the configuration file details with an example, bootstrap server requirements and the way to access bootstrap status.

Setting up VNF platform for interactive bootstrap

This section describes the process of setting up the default VNF platform configuration by a service provider before shipping it to an end customer. The configuration process enables VNF platform to connect to the appropriate bootstrap server when the end customer powers it on and connects it to the required network.

Create the default factory configuration by using the CLI terminal to apply the manufacturer specified configuration. To onboard a device for interactive bootstrap, perform the following steps.

1. Enter the following command to create the `/config/zerotouch` directory:

```
mkdir -p /config/zerotouch.
```

2. Enter the following command to copy the `ztc-config.boot` file:

```
cp config.boot /config/zerotouch/ztc-config.boot.
```

3. Get the serial number of the device to be configured in the `ztc.cfg` file by entering the following command:

```
sudo dmidecode -s system-serial-number.
```

4. Download the IDDevID private key and certificate for the serial number by using a secure mechanism. This step is optional and is used for HTTPS bootstrap servers.

5. Enable the interactive bootstrap by creating the `create ztc.cfg` file with appropriate fields, including the bootstrap server URL and node.

Configuring the `ztc.cfg` file

The `ztc.cfg` file is located in the `/config/zerotouch/ztc.cfg` directory. This file contains different fields that are used by the interactive bootstrap code. The file uses a simple `option=value` format. Lines that start with a hash `#` are ignored.

The following fields are mandatory:

- `cert`—Filename for the IDDevID certificate.
- `priv`—Filename of IDDevID private key.
- `devid`—Device serial number. Provide the number only if the IDDevID certificate is not used. You must specify `cert`, `priv` or `devid`.
- `def_cfg`—Location of the default factory configuration that is compared to the running configuration.
- `url`—URL of the bootstrap server base.

The following options are optional:

- `capath`—Certificate path for validating bootstrap server certificate.
- `ca`—Certificate chain of the bootstrap server.
- `noverify`—Option not to verify the authenticity of the bootstrap server.
- `timeout`—Option for the bootstrap server connection to time out in seconds (default is 10 seconds).
- `node`—RESTCONF node. In the character string, `%devid%` is replaced with `devid`, which was previously specified. The default string is `/restconf/data/ietf-zerotouch-bootstrap-server:devices/device=%devid%`.
- `log`—Name of the log file. The default file is `/run/ztc.log`.

- `debug`—Name of the debug file. The default file is `/run/ztc.debug`.
- `httpd`—`http=1`. This value is required for starting the web portal at port 8000.
- `docroot`—Directory name for the HTTP files. The default directory is `/var/www/zerotouch`.
- `auth`—File in which the HTTP server stores the activation or authorization code provided by the client. The default file is `/run/ztc.cred`.
- `authmode`—Authorization mode. The value of `authmode` must equal to `devid`.

Example of the `ztc.cfg` file

This section provides an example of the `ztc.cfg` file. The following configuration attempts to connect to the bootstrap server at: `http://12.194.168.65/restconf/data/ietf-zerotouch-bootstrap-server:devices/device=1034150093`, where `1034150093` is the password.

```
url=http://12.194.168.65/
node=/restconf/data/ietf-zerotouch-bootstrap-server:devices/device=%devid%
devid=1034150093
def_cfg=zerotouch/ztc-config.boot
httpd=1
authmode=devid
```

Bootstrap server requirements

The following section describes the requirements for the bootstrap server. The server replies with a status code of 401 when wrong authentication is provided and a status code of 200 when correct authentication is provided. An example of a configuration file that is returned from the bootstrap server follows:

```
<?xml version='1.0' encoding='UTF-8'?>
<devices xmlns="urn:ietf:params:xml:ns:yang:ietf-zerotouch-bootstrap-server">
<device>
<configuration><config>
<interfaces xmlns="urn:vyatta.com:mgmt:vyatta-interfaces:1">
<dataplane xmlns="urn:vyatta.com:mgmt:vyatta-interfaces-dataplane:1">
<tagnode xmlns="urn:vyatta.com:mgmt:vyatta-interfaces-dataplane:1">dp0p4s0</tagnode>
<vif xmlns="urn:vyatta.com:mgmt:vyatta-interfaces-dataplane:1">
<tagnode xmlns="urn:vyatta.com:mgmt:vyatta-interfaces-dataplane:1">2</tagnode>
<address xmlns="urn:vyatta.com:mgmt:vyatta-interfaces-dataplane:1">177.168.250.12/24</address>
<address xmlns="urn:vyatta.com:mgmt:vyatta-interfaces-dataplane:1">2001:1890:e040::15:250:a12/64</
address>
<address xmlns="urn:vyatta.com:mgmt:vyatta-interfaces-dataplane:1">2001:1890:e040:15:250::a12/64</
address>
<vlan xmlns="urn:vyatta.com:mgmt:vyatta-interfaces-dataplane:1">2</vlan>
</vif>
</dataplane>
</interfaces>
<protocols xmlns="urn:vyatta.com:mgmt:vyatta-protocols:1">
<static xmlns="urn:vyatta.com:mgmt:vyatta-protocols-static:1">
<route6 xmlns="urn:vyatta.com:mgmt:vyatta-protocols-static:1">
<tagnode xmlns="urn:vyatta.com:mgmt:vyatta-protocols-static:1">:/0</tagnode>
<next-hop xmlns="urn:vyatta.com:mgmt:vyatta-protocols-static:1">
<tagnode xmlns="urn:vyatta.com:mgmt:vyatta-protocols-static:1">2001:1890:e040:15:250::a30</tagnode>
</next-hop>
</route6>
</static>
</protocols>
</config></configuration>
</device>
</devices>
```

Accessing bootstrap status

The Bootstrap client on Zero Touch Provisioning runs a web server at port 8000. If the LAN address is configured as 192.168.1.1, use the http://192.168.1.1:8000 URL on a browser from a laptop that is connected to the LAN port. To access the bootstrap status page, perform the following steps.

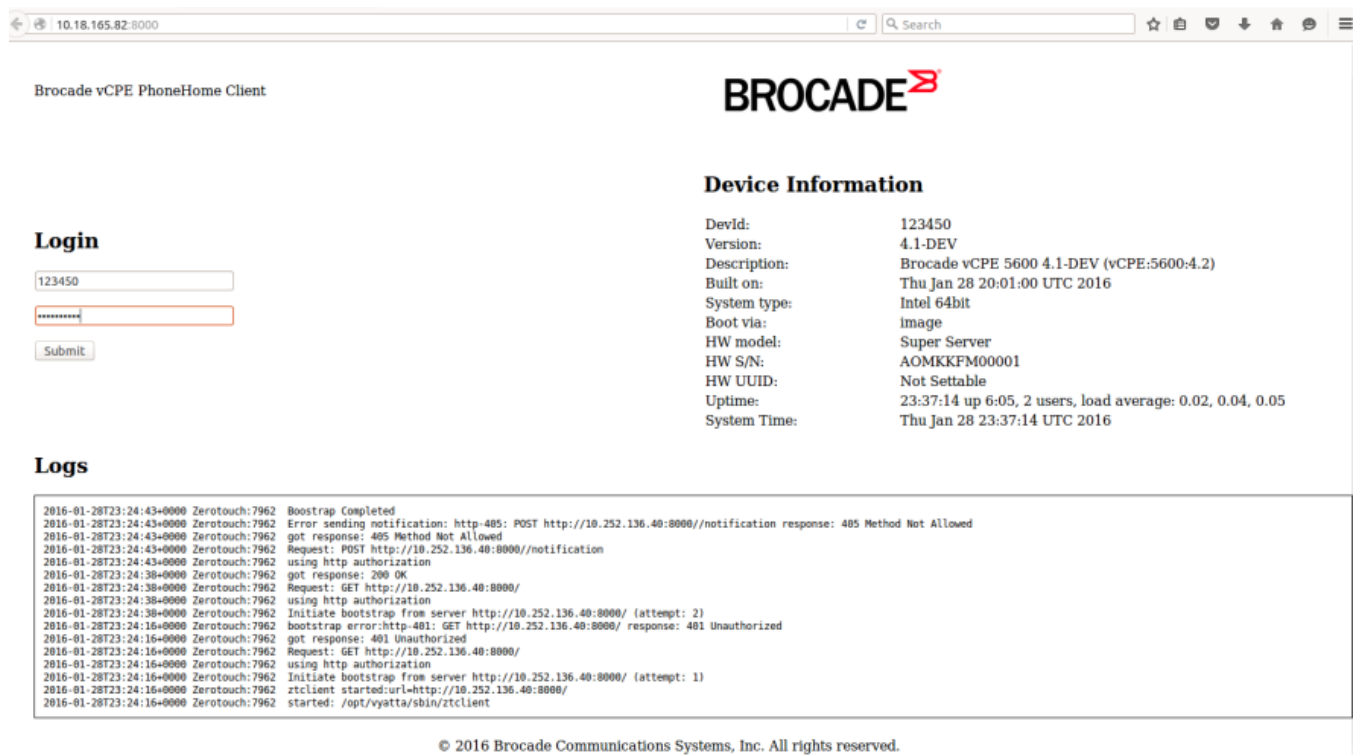
1. Launch a web application to access the VNF platform status page at http://192.168.0.1:8000/.

NOTE

The IP address may differ based on your configuration and the setup of the device.

2. Enter the VNF platform device ID or serial number as the username and the activation code as the password.

FIGURE 1 Bootstrap status page



Configuring Zero Touch Provisioning at the branch

To configure Zero Touch Provisioning at the branch, perform the following steps

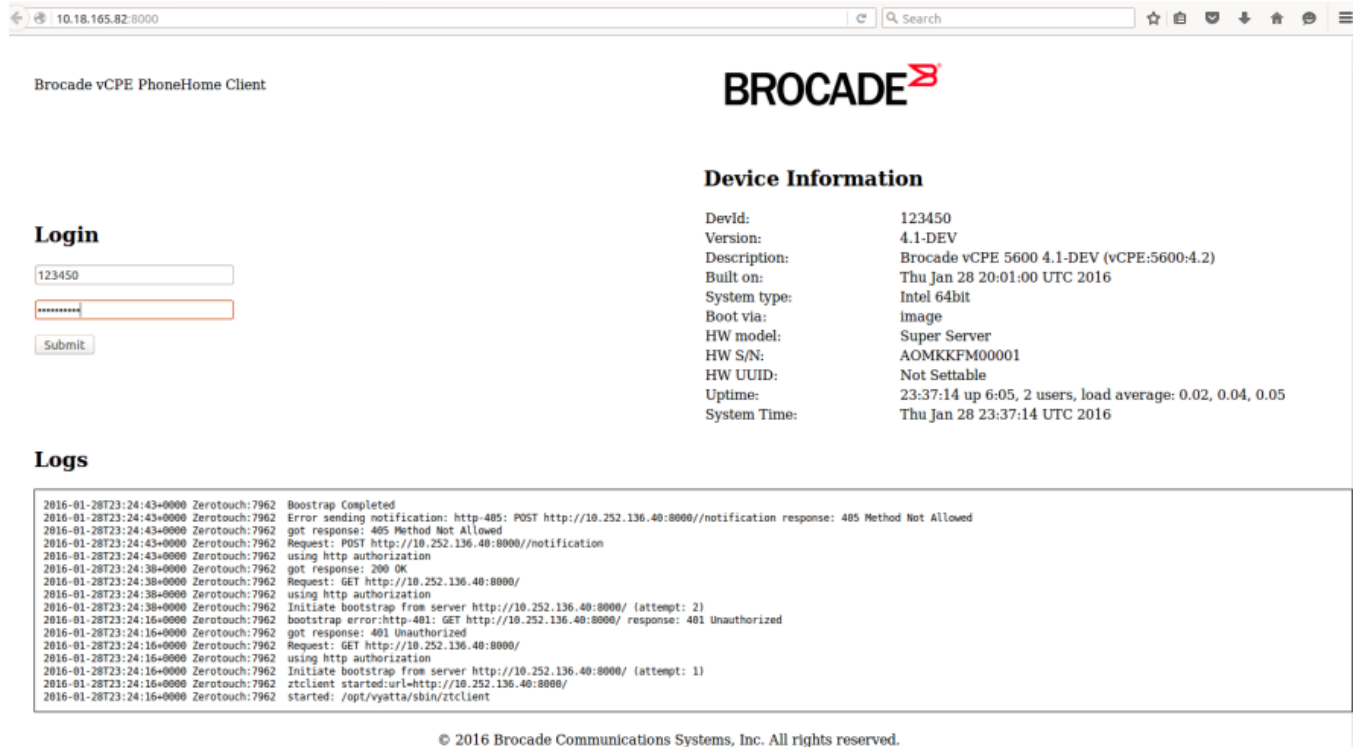
1. Connect VNF platform with default factory configuration to a bootstrap server in your network.
2. Connect the WAN port to the LTE modem, to reach the bootstrap service.
3. Connect an activation computer to the LAN port.
4. Launch a web browser to access the VNF platform status page at http://192.168.0.1:8000/ .

NOTE

The IP address may differ based on your configuration and the setup of the device.

5. Enter the VNF platform device ID or serial number as the username and the activation code as the password.

FIGURE 2 Bootstrap status page



VNF platform receives the bootstrap configuration from the bootstrap server after the verification of the activation code; the configuration is stored and saved. Then VNF platform sends HTTP notification to the bootstrap server, and the bootstrap advertises its availability to other services.

Call Home

- [Overview.....](#)17
- [Limitations.....](#)17
- [Configuration sample.....](#)17

Overview

The Call Home feature allows VNF platform to initiate a secure connection with configured remote management systems for additional configuration or register the presence of the system.

Call Home supports both the initial deployment of VNF platform and on-going management. During the Zero Touch procedure on VNF platform, the configuration is automatically fetched and may contain the Call Home server address and the **set service netconf** command. The system automatically initiates a secure connection with an NMS and is ready to be further provisioned and managed by that NMS.

Limitations

The Brocade implementation of Call Home has specific limitations as discussed in this section.

The following list describes those limitations:

- The Call Home specification in the IETF draft supports both SSH and TLS transports. Currently, Brocade supports the SSH transport only. The SSH protocol is defined in the IETF draft *The Secure Shell (SSH) Transport Layer Protocol*, available at <https://tools.ietf.org/html/rfc4253>.
- The Call Home specification in the IETF draft supports both NETCONF and RESTCONF as configuration servers. Currently, Brocade supports NETCONF configuration servers only. The NETCONF support for SSH is defined in the IETF draft *Using the NETCONF Protocol over Secure Shell (SSH)*, available at <https://tools.ietf.org/html/rfc6242>.

For more information about Call Home, refer to the IETF draft *NETCONF Call Home and RESTCONF Call Home*, available at <https://tools.ietf.org/html/draft-ietf-netconf-call-home-08>.

Configuration sample

In a scenario where the Zero Touch procedure does not push the Call Home server address to the system, you can use the **service netconf call-home netconf-client <host> port <port>** command to initiate the Call Home service.

Assume that a VNF platform guest is connected to a NMS server. The NMS server has an IP address of 10.0.0.1.

To configure Call Home, perform the following steps.

TABLE 2 Configuring Call Home

Step	Command
Log in to VNF platform and switch to configuration mode.	<code>vyatta@vyatta# config</code>
Initiate the Call Home service.	<code>vyatta@vyatta# set service netconf call-home netconf-client 10.0.0.1 port 443</code>

TABLE 2 Configuring Call Home (continued)

Step	Command
Save the configuration.	<code>vyatta@vyatta# commit</code>
Switch to operational mode.	<code>vyatta@vyatta# exit</code> <code>logout</code>
Display the result.	<code>vyatta@vyatta:~\$ show service netconf call-home status</code>

If you want to disable Call Home, you can use the **service netconf call-home netconf-client <host> disable** command.

Automated Provisioning Commands

- service netconf call-home netconf-client <host_ip_address> port <port_number>..... 20
- service netconf call-home netconf-client <host_ip_address> disable 21
- show service netconf call-home status..... 22

service netconf call-home netconf-client <host_ip_address> port <port_number>

service netconf call-home netconf-client <host_ip_address> port <port_number>

Enables the Call Home feature by specifying a NETCONF client and port.

Syntax

set service netconf call-home netconf-client *host_ip_address* port *port_number*

delete service netconf call-home netconf-client *host_ip_address* port *port_number*

show service netconf

Command Default

Call Home is disabled by default.

Parameters

host_ip_address

The IPv4 or IPv6 address for a NETCONF client to which VNF platform connects for establishing Call Home.

port_number

The number of a port in the NETCONF client. The number ranges from 1 through 65,535.

Modes

Configuration mode.

Configuration Statement

```
netconf {
  call-home {
    netconf-client host_ip_address {
      port port_number
    }
  }
}
```

Usage Guidelines

Use this command to enable the Call Home feature by specifying a NETCONF client and port.

Use the **set** form of the command to enable the Call Home feature.

Use the **delete** form of the command to delete the Call Home port details.

Use the **show** form of the command to display the details for a Call Home configuration.

service netconf call-home netconf-client <host_ip_address> disable

Disables the Call Home client.

Syntax

```
set service netconf call-home netconf-client host_ip_address disable
show service netconf
```

Command Default

Call Home is disabled by default.

Parameters

host_ip_address

The IPv4 or IPv6 address for a NETCONF client to which VNF platform connects for establishing Call Home.

Modes

Configuration mode.

Configuration Statement

```
netconf {
  call-home {
    netconf-client host_ip_address {
      disable
    }
  }
}
```

Usage Guidelines

Use this command to disable the NETCONF Call Home client.

Use the **set** form of the command to disable the NETCONF Call Home client.

Use the **show** form of the command to display the details for a Call Home configuration.

show service netconf call-home status

Displays the status of the last Call-Home operation.

Syntax

show service netconf call-home status

Modes

Operational mode.

Usage Guidelines

Command Output

The **show service netconf call-home status** command displays the following information:

Output field	Description
failed	The Call Home operation failed.
succeeded	The Call Home operation succeeded.
started	The Call Home operation is in progress.
not-started	The Call Home operation was not attempted.
unknown	The Call Home operation status could not be determined.

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online, by telephone, or by e-mail. Brocade OEM customers should contact their OEM/solution provider.

Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to www.brocade.com and select **Support**.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

Online	Telephone	E-mail
<p>Preferred method of contact for non-urgent issues:</p> <ul style="list-style-type: none">• Case management through the MyBrocade portal.• Quick Access links to Knowledge Base, Community, Document Library, Software Downloads and Licensing tools	<p>Required for Sev 1-Critical and Sev 2-High issues:</p> <ul style="list-style-type: none">• Continental US: 1-800-752-8061• Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33)• Toll-free numbers are available in many countries.• For areas unable to access a toll-free number: +1-408-333-6061	<p>support@brocade.com</p> <p>Please include:</p> <ul style="list-style-type: none">• Problem summary• Serial number• Installation details• Environment description

Brocade OEM customers

If you have purchased Brocade product support from a Brocade OEM/solution provider, contact your OEM/solution provider for all of your product support needs.

- OEM/solution providers are trained and certified by Brocade to support Brocade® products.
- Brocade provides backline support for issues that cannot be resolved by the OEM/solution provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/solution provider.