NETASQ
CENTRALIZED MANAGER

INSTALLATION GUIDE

Document version: 1.2

Reference: naengde_ncm-getting-started

INTRODUCTION

Network architecture

NETASQ Centralized Manager requires 3 network interfaces:

- Eth0: interface for accessing the SSH console
- Eth1: interface for accessing appliances as well as the web portal
- Eth2 (for clusters): interface used for synchronizing both platforms

The server has to conform to the sizing conditions indicated in the document naent-no_ncm-sizing.pdf in the documentation section in the secure-access area on NETASQ's website.

Precautions

Once you have finished the configuration through the webconf wizard, the values relating to the domain name and the hostname can only be modified using the right NCM console commands.

The use of CentOS commands to modify these values is strictly not recommended.

In this document, we will assume that the server used conforms to the hardware requirements with 3 network interfaces in particular. Configurations with fewer interfaces will be covered in another document.

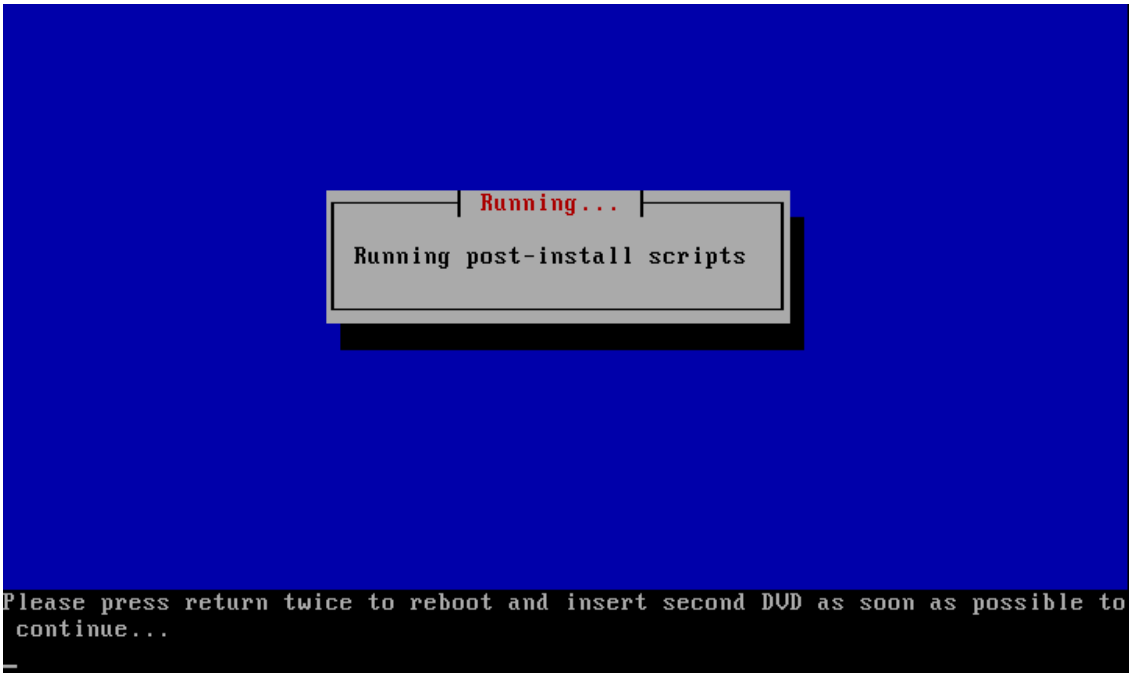
Installing NCM

Installation

Disk 1

Installing the CentOS 5.4 distribution. DVD no. 1 is “bootable”, so you only need to run the server with the disk in the drive. Press ENTER to launch the installation when the prompt appears.

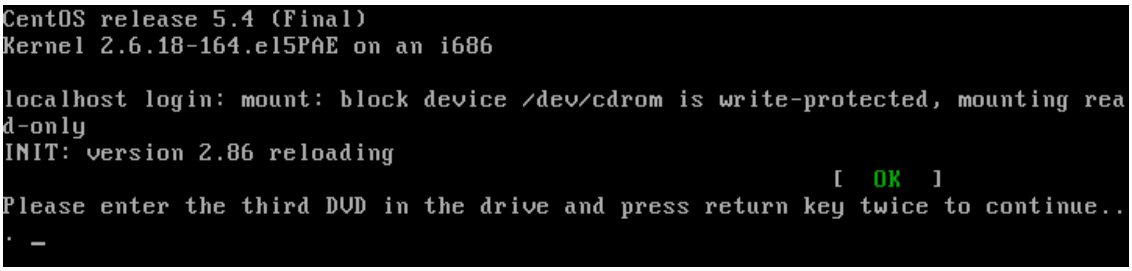
The server has to be rebooted but DVD no. 1 has to be removed from the drive to avoid rebooting on it. Insert disk no. 2 during the reboot phase.



Disk 2

This disk is not "bootable" and launches an update script once the OS has booted.

When it is ready, the installation program will tell you to insert Disk 3 into the drive.



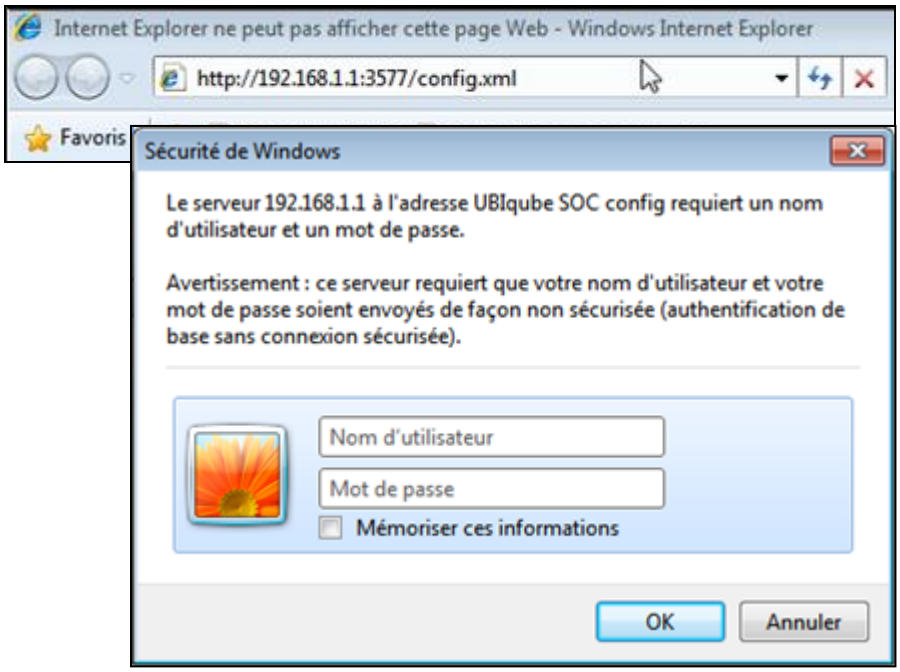
Disk 3

This is the longest phase and lasts for several minutes (about 30 minutes depending on the performance of the server). Many messages may scroll on the screen but you can ignore them. When the installation is complete, a banner will appear saying so.

Network configuration

The interface Eth2 is configured with the IP address 192.168.1.1/24 by default. At the beginning, this interface is used only for launching the Webconf web pre-configuration interface.

You only need to plug a computer to this interface with an address in the right network (192.168.1.0/24) then use a browser to launch the Webconf.



WEBCONF

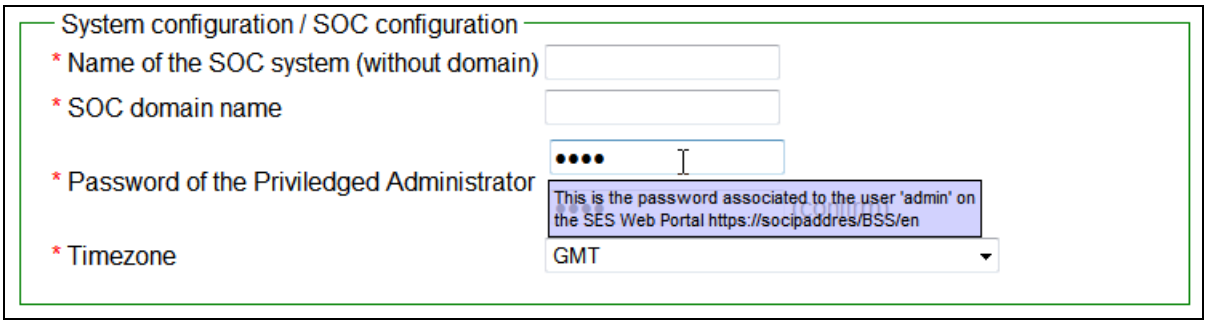
This is the screen that allows a quick and simple configuration of the NCM server:

Access: http://192.168.1.1:3577/config.xml.

This access mode is only possible with the interfaces eth0/eth2 (interface for accessing appliances/backups).

Login: **socconfig**
Password: **b5ty9uvh4**

SOC configuration



Name of the SOC system
This setting defines the name of the NCM server. The name is important as many configuration files or parameters are based on it. This name can only be modified using the NCM's CLI mode.

Manager Password
Here, enter the "Privileged administrator" 's password

This password is associated with the 'admin' account on the web portal. (je ne sais pas s'il faut mettre "admin" ou "manager" en suivant la saisie d'écran)

The password field cannot be empty, and the password must contain at least 8 characters including 2 numbers.

Company's General Information

Most of the fields defined on this page are used for generating the certificate that the web portal uses.

Company Name
Enter the name of your company here, without spaces or underscores.
This field is mandatory.

Company address
Address of the company
This field is mandatory.

City
Enter the city of your company here, without spaces or underscores.
This field is mandatory.

State
Enter the State (region) of your company here, without spaces or underscores.

Company country
Enter the country code (e.g. FR, RU, BE, etc.) of your company here, without spaces or underscores.
This field is mandatory.

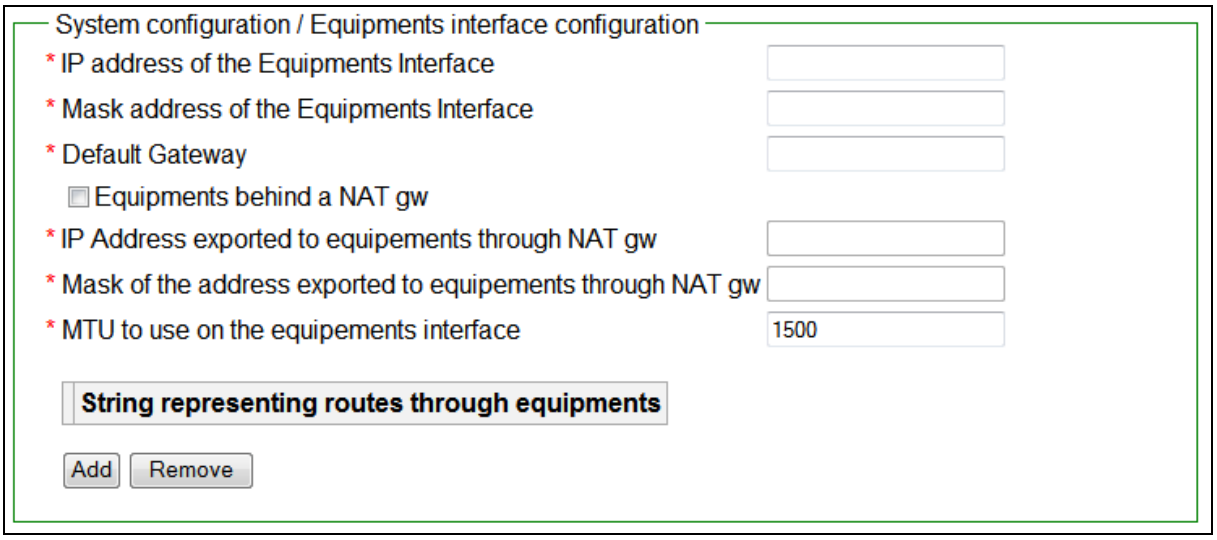
Telephone Number
Telephone number.

Company Web Site URL
URL of the company's website.

Organization Unit of the company
Here, enter the name of your IT department (Organizational Unit), without spaces or underscores.

Equipments management interface parameters

This section is for the configuration of the appliance management interface (eth1). The NCM's administration web portal is also accessed on this interface.



The interface is protected by firewall rules and has to be connected to a network that can contact administered appliances.

IP address of the Equipments interface
IP address of the interface eth1. This is the interface used for connecting to remote firewalls in order to administer them.

Default Gateway
NCM default gateway that can be used for contacting administered appliances.

Equipments behind a NAT gw
When an NCM server is placed in a DMZ or a network located behind a NAT gateway, this option has to be selected in order to specify the address/mask that will be visible for administered firewalls.

String representing routes through equipments
Static routes can be added in order to use a path other than the default gateway.

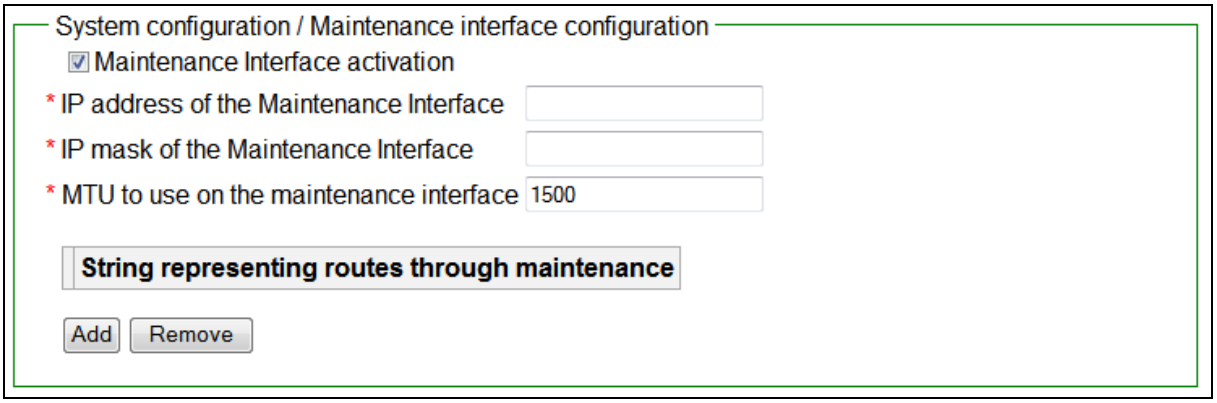
If you change the IP address of the NCM management interface (eth1), your firewalls will become inaccessible to NCM. You will need to manually update the firewalls!

The syntax for adding routes is as follows:

```
172.16.1.0/16 via 192.168.1.254
```

Maintenance interface parameters

This interface is for remote access in console on the NCM server



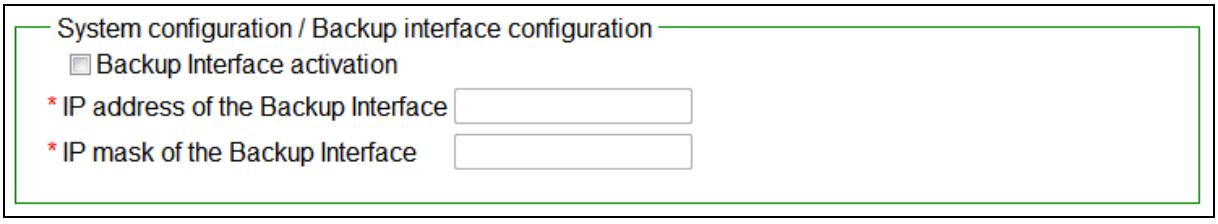
This is the interface referenced as Eth0. It is exclusively dedicated to remote administration, especially with CLI mode accessible in SSH.

This interface has limited access and you are advised to place it in a DMZ (or protected administration network).

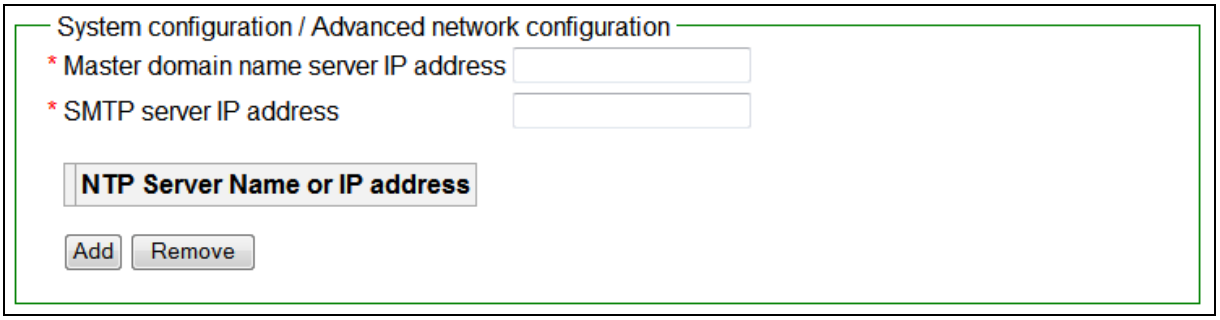
Maintenance Interface activation
This interface can be disabled in an advanced configuration mode (not covered in this document).

Backup interface parameters

Interface used for setting up a backup architecture.



Advanced network configuration



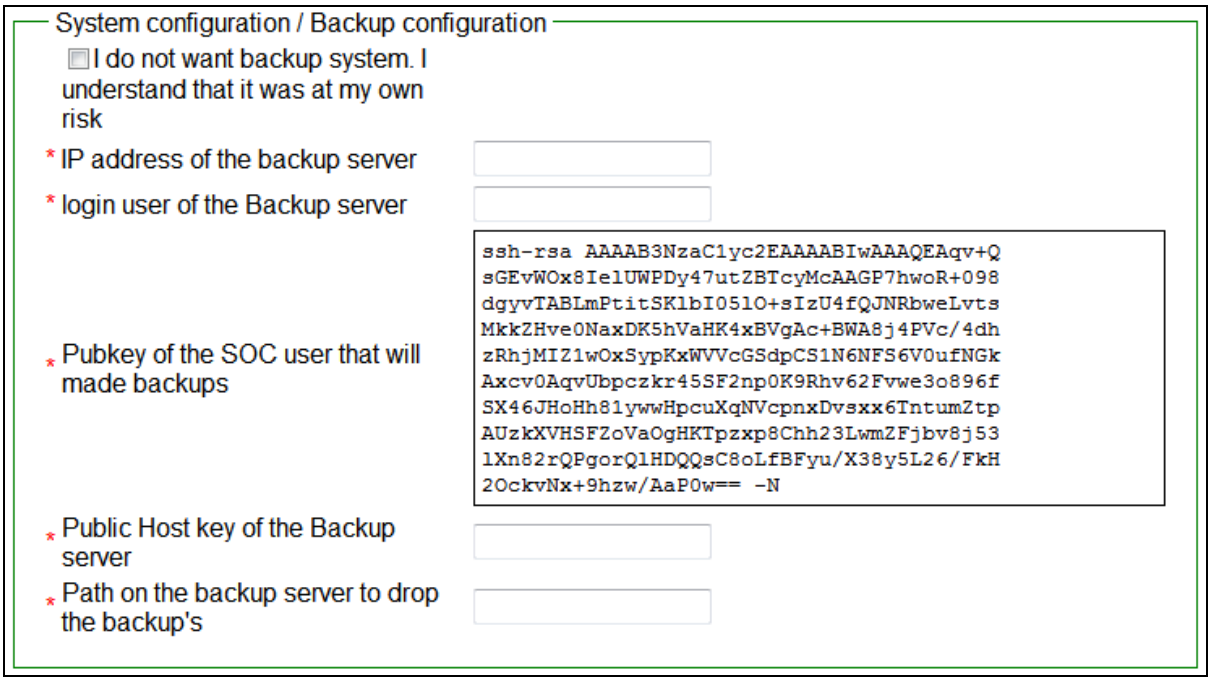
Master domain name server IP address
IP address of the DNS server that NCM uses. NCM can act as a DNS server for administered firewalls. Whenever NCM cannot resolve a query, it will send the request to this server.

SMTP server IP address
IP address of the SMTP server needed for notifications.

NTP
External NTP servers on which NCM will synchronize.

Backup configuration

This menu allows configuring the connection with the backup server when a cluster is configured.



IP address of the backup server
IP address of the backup NCM server.

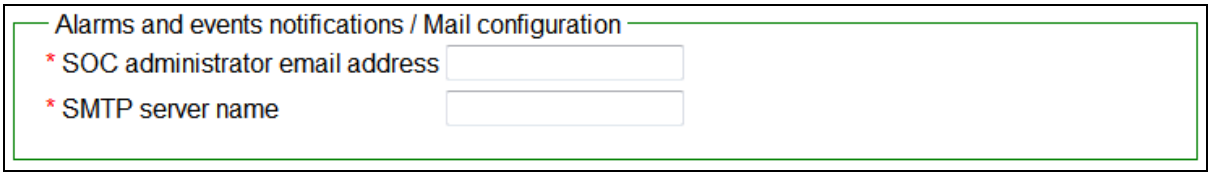
Login user of the Backup server
Account that must exist on the server concerned and which is dedicated to backups.

Pubkey of the SOC user that will made backups
Public key of user who will make backups.

Public Host Key of the backup server
Key used for authenticating the backup server on the master.

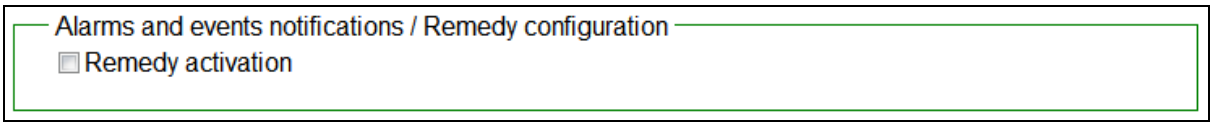
Path on the backup server to drop the backup's
Path to folder where backup files are stored. The user created for the backups needs reading/writing privileges on this folder.

Mail configuration

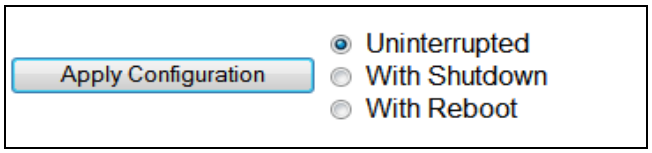


E-mail address and name of the mail server for the administrator who must receive all NCM system alerts.

Remedy configuration



Apply Configuration



With Shutdown
Recommended whenever a network operation is performed (IP/Mask) before a physical migration (change of rooms, for example).

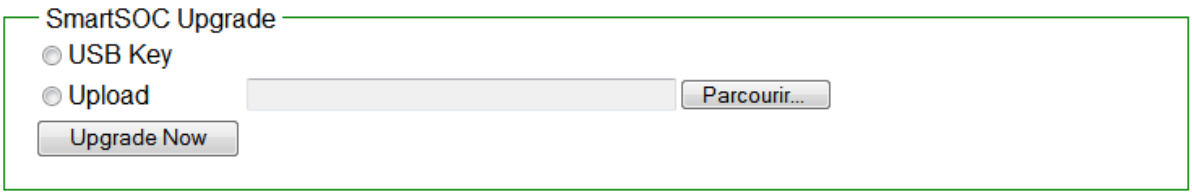
With reboot
Recommended method.

Uninterrupted
To be used only for minor changes. If a network setting is defined, choose a reboot instead.

Backup Restoration

Restoration requires proper configuration of the backup parameters. If this is so, backup files can be retrieved on the right server to be distributed over an existing configuration.

SmartSOC/NCM upgrade



Possibility of upgrading the version of a system.

Summary of network traffic and firewall rules

The NCM server is configured by default with filter rules that avoid unnecessary incoming/outgoing access. Here is a table that displays the rules concerned.

Interface	Component	Protocol	Direction of the query	Description
Maintenance interface Eth0	Web portal	TCP 80/443	IN/OUT	HTTP(S)
	Maintenance	TCP 22	IN/OUT	SSH
		ICMP echo-reply	IN/OUT	Ping
		TCP/UDP 53	IN/OUT	DNS
		TCP 3577	IN	Webconf (http)
Configuration interface Eth1	Web portal	TCP 80/443	IN/OUT	HTTP(S)
	SecEngine	TCP 22	IN/OUT	SSH
		TCP 23	OUT	Telnet
		TCP 69	OUT	TFTP
		TCP 20/21	IN/OUT	FTP
		TCP/UDP 53	IN/OUT	DNS
	EventTracker	TCP 25	IN/OUT	SMTP
		UDP 514	IN	Syslog
		UDP 161/162	IN/OUT	SNMP: NCM allows retrieving info but also allows sending
		ICMP echo-reply	IN/OUT	Ping
	OS	TCP/UDP 123	IN	NCM acts as an NTP server
Backup interface Eth2	Web portal	TCP 80/443	IN/OUT	HTTP(S)
	Maintenance	TCP 22	IN/OUT	SSH
		ICMP echo-reply	IN/OUT	Ping
		TCP/UDP 53	IN/OUT	DNS
		TCP 3577	IN	Webconf (http)

Upgrading NCM

Upgrading the NETASQ Centralized Manager platform consists of upgrading the product's software solution.

Follow the procedure below to do so:

1. Retrieve the upgrade file from the secure-access areas on NETASQ's website
2. Copy the file *update_NCM_version_1_2. bin* into the folder */upgrades* on the target host
3. Connect to the NETASQ Centralized Manager maintenance interface
4. Execute the command */opt/ubi-webconf/upgrade_smartsoc.sh exer*

NETASQ Centralized Manager will then upgrade the platform's software.