Network Services Hub

Configuration Guide

Version: 1.0
Status: Portfolio sample
Owner: Rima Sharma

This sample configuration guide is created for portfolio purposes.

Overview of Network Services Hub

Network Services Hub is a virtualization platform for hosting and managing virtual network services in a data center environment. It supports the complete lifecycle of these services, including deployment, configuration, and operation.

Network Services Hub provides a centralized management layer that runs on industry-standard infrastructure. By using an open, hypervisor-based architecture, Network Services Hub enables organizations to move from proprietary hardware appliances to a flexible, software-defined model.

To support different operational workflows, Network Services Hub offers multiple management interfaces, including a web interface, a command-line interface, and a REST API.

Key Features and Capabilities

- **Hardware acceleration:** Uses technologies such as SR-IOV to help virtual services run with near-native network performance and low latency.
- **Centralized image library:** Stores disk images such as QCOW2 and ISO in one location for consistent deployment and version control.
- **Automated bootstrapping:** Allows configuration scripts or files to be applied automatically when a virtual instance is created.
- **Separate management plane:** Uses dedicated management access to enable administrators to manage the system.
- **Vendor-agnostic hosting:** Supports standard virtual appliances, allowing organizations to choose services from different vendors.

Management Interface Modes

Network Services Hub supports two operational modes for the management interface. These modes determine how management traffic is handled in relation to hosted service traffic.

Shared Mode

In shared mode, the management interface carries the management traffic of Network Services Hub and the traffic associated with hosted services. This mode allows you to assign the management interface to services when network resources are limited.

Dedicated Mode

In dedicated mode, the management interface is reserved exclusively for the management traffic of Network Services Hub. Hosted services are not permitted to use this interface. This mode provides stronger isolation for management operations.

Note:

You cannot switch to dedicated mode while the management interface is in use by a hosted service.

Configure the Management Interface Mode

You can configure the management interface mode during initial setup or later by using one of the following methods:

Web Interface

1. Go to **Administration** > **Host Settings**.
2. Select **Shared** or **Dedicated** from the Management Interface Mode list.
3. Click **Apply**.

Command-Line Interface

```
# nsh set mgmtInterfaceMode <shared | dedicated>
```

REST API

```
curl -u admin:password -X POST
https://nsh.example.com/api/nsh/settings
-H "Content-Type: application/json"
-d '{
  "mgmtInterfaceMode": "<shared | dedicated>"
}'
```

Access Control

Network Services Hub allows you to control access to the services exposed through the management interface and prevent any unauthorized access. With access control, only traffic originating from approved source networks is allowed.

Access control is enforced through configurable access rules. Each access rule defines the source networks permitted to access a service and the action to apply when traffic matches the rule. When access control is enabled, incoming traffic is evaluated against configured rules, and only permitted traffic is allowed to access services.

Create Access Control Rules

Access control rules can be created or managed by using one of the following configuration methods:

Web Interface

1. Go to **Administration** > **Access Control**.
2. Click **Add Rule**.
3. Enter the source network, for example, `192.0.2.0/24`.
4. Select the services to protect.
5. Choose **Allow** or **Deny**.
6. Assign a priority value. Rules are evaluated based on priority. Higher-priority rules are processed first.
7. Click **Apply**.

Command-Line Interface

```
# nsh acl add source {ipAddress} service {serviceName} action <allow
| deny> priority {priorityValue}
```

REST API

```
curl -u admin:password -X POST
https://nsh.example.com/api/nsh/acl/rules
-H "Content-Type: application/json"
-d '{
  "source": "{ipAddress}",
  "service": "{serviceName}",
  "action": "<allow | deny>",
  "priority": {priorityValue}
}'
```

User Management

Network Services Hub supports both local users and externally authenticated users. Local users are defined and authenticated by Network Services Hub, and external users are authenticated through an integrated authentication service. If a user account exists both locally and externally, external authentication takes precedence.

Note:
Only local users can access the Network Services Hub by using the system console. Externally authenticated users must use remote access methods.

Supported User Roles

Network Services Hub uses role-based access control (RBAC) to manage user permissions. Each role grants a predefined set of privileges.

Role	Description
Administrator	Administrators have full read and write access to the Network Services Hub. They can: ▪ Create, modify, and delete user accounts ▪ Configure Network Services Hub settings ▪ Create, manage, and remove hosted services ▪ Access all diagnostic and support functions
Service manager	Service managers can: ▪ Create and manage hosted services ▪ View Network Services Hub configuration ▪ Change their own passwords ▪ Access a limited set of diagnostic commands
Operator	Operators have read-only access to the Network Services Hub information. They can: ▪ View configuration and status information ▪ Change their own passwords ▪ Access basic diagnostic commands
VM operator	VM operators have operator-level access and can additionally access virtual machine consoles for hosted services.
Custom roles	Administrators can define custom roles with specific permissions to meet operational requirements.

Create, Modify, or Delete a User

You can create, modify, or delete a user by using one of the following methods:

Web Interface

Create a User

1. Go to **Administration > Users**.
2. Click **Add User**.
3. Enter a user name, for example, `ops-user`.
4. Select a role, for example, **Operator**.
5. Set and confirm the initial password.
6. Click **Apply**.

Modify a User

1. Locate the user in the user list.
2. Select **Edit**.
3. Update the role or password, and click **Apply**.

Delete a User

1. Locate the user in the user list.
2. Click **Delete**.

Command-Line Interface

```
# nsh users set name {userName} role {role} password {password}
```

Note: User deletion is not supported through the command-line interface.

REST API

Create a User

```
curl -u admin:password -X POST
https://nsh.example.com/api/nsh/users
-H "Content-Type: application/json"
-d '{
  "name": "{userName}",
  "role": "{role}",
  "password": "{password}"
}'
```

Modify a User

```
curl -u admin:password -X PUT
https://nsh.example.com/api/nsh/users/{userName}
-H "Content-Type: application/json"
-d '{
  "role": "{role}",
  "password": "{password}"
}'
```

Delete a User

```
curl -u admin:password -X DELETE
https://nsh.example.com/api/nsh/users/{userName}
```