Global Leader in Software-Defined Storage.

NexentaFusion 1.1.1

Installation QuickStart Guide

You can manage NexentaStor 5.1.1 appliances with its Command Line Interface (CLI) and REST APIs, or with the NexentaFusion graphical user interface (GUI).

This document includes the instructions to install NexentaFusion and covers the following tasks:

- Ensure that the NexentaFusion installation requirements are met.
- Deploy NexentaFusion.
- Register the NexentaStor appliances in NexentaFusion.

Document History

Revision	Description
October, 2016	1.0.0 GA version
December, 2016	1.0.1 GA version
April, 2017	1.0.2 GA version
October, 2017	1.1 GA version
January, 2018	1.1.1 GA version

Table of Contents

Installing NexentaFusion 1.1.1

NexentaFusion is a graphical user interface that provides centralized management of multiple NexentaStor appliances, tracks performance analytics trends, and monitors system faults. From a single pane, NexentaFusion provides appliance-specific summary views of hardware components, services, and storage logical objects such as shares, snapshots, and clusters. You can navigate the GUI using its intuitive tabs, drill-down menus, action cogwheels, and expand / contract arrows.

NexentaFusion supports a variety of deployment options, including deployment using Docker containers and installing from an OVA file.

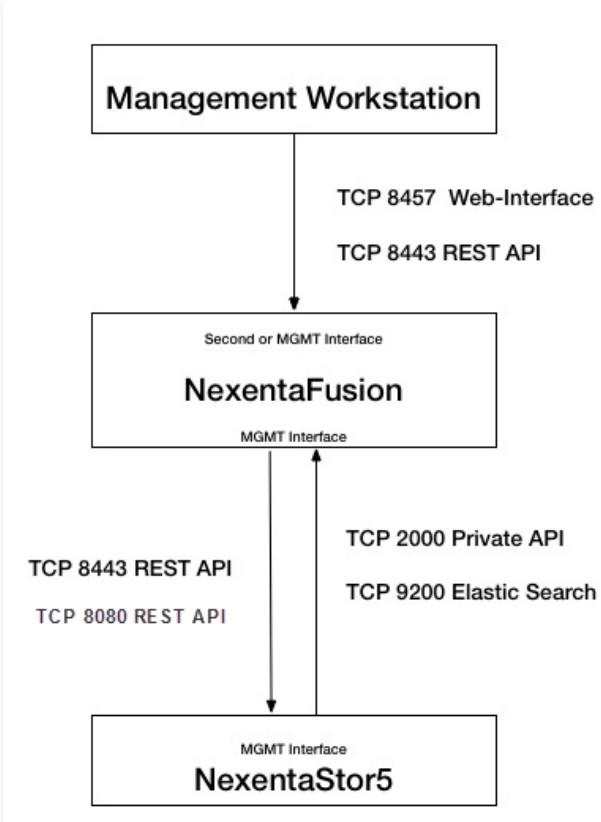
Network Requirements for Both Docker and OVA

The following ports need to be opened in the firewall to access NexentaFusion.

- TCP 8457 - Web Server
- TCP 2000 - Private API
- TCP 9200 - Elasticsearch
- TCP 8443/8080 - REST API

These ports must be accessible through the management address set with –e in the docker run command.

For information on the direction of TCP packets, see the diagram below.



Deployment Using NexentaFusion Docker Container

Use the steps listed here to start NexentaFusion GUI.

Prerequisites

The following table lists the resource requirements for our container.

Table 4: System Requirements

Resources	
CPUs	4 CPU cores for the container
Memory	16GB in total
Disk Size	10GB for NexentaFusion admin 80GB for analytics database

Deployment Procedure with Internet Connection

1. Open the terminal of the machine running Docker.
2. Pull the Fusion container.
   ```
   $ docker pull nexenta/fusion
   ```
3. Ensure that the image is pulled by running the following command:

   ```
   $ docker images

   Example:

   REPOSITORY      TAG     IMAGE ID        CREATED       SIZE

   nexenta/fusion  latest  271d1073a551    4 weeks ago   1.19GB
   ```

4. NexentaFusion requires two persistent volumes for server data and the analytics database.

   1 persistent volume of minimum size 10GB for NexentaFusion server data to be mapped to `/opt/docker/fusion`

   Another persistent volume of minimum size 80GB for the analytics database to be mapped to `/opt/docker/esdb`

5. Run the container.
   A sample `run` command is shown below:

   - Use the –v flag to map the persistent volume to the container.

   ```
   $  docker run --name fusion
   -v /opt/docker/esdb:/var/lib/elasticsearch
   -v /opt/docker/fusion:/var/lib/nef
   -e MGMT_IP="0.0.0.0"
   --ulimit nofile=65536:65536 --ulimit memlock=-1:-1
   -e TZ="America/Los_Angeles"
   --memory=16g
   -e ES_HEAP_SIZE="8g"
   -i -t
   --net=host
   nexenta/fusion
   ```

Notes:

- Replace 0.0.0.0 shown in the example above with your management IP.
- Use the –v flag to map the persistent volume to the container.
- `The --ulimit parameters` are required to set OS values properly for the elasticsearch database.
- Adjust the network settings, and/or use –p to map ports, as appropriate for your environment.
- `-e TZ="America/Los_Angeles"` is an optional parameter to set timezone. Default is UTC.
- Heap size should be limited to half the total memory size.

Let the system start the container – This can take a few minutes.

6. After a successful installation you should be able to log into the NexentaFusion GUI by pointing the browser to https:// <Management IP: 8457> in a supported web browser.

7. The initial login credentials are `admin / nexenta.`

   On the first login into the NexentaFusion GUI you will be asked to configure a new password.

   Note: When the NexentaFusion GUI is started shortly after starting up the container, you may see an error indicator on the main menu bar, indicating high CPU usage. This should disappear in a few minutes after the database startup completes.

Deployment Procedure without Internet Connection

1. On a machine that does have Internet access and docker installed, pull the container from Docker hub and save the tar file, and put it onto removable media.

```
$ docker pull nexenta/fusion

$ docker save -- output nexenta-fusion_image.tar nexenta/fusion
```

2. On the target machine where you wish to install Fusion, with no Internet access and docker already installed, load the container image from the tar file

```
$ docker load  -- input nexenta-fusion_image.tar
```

3. Proceed with Step 3 from the previous section.

Table 6: Some configurable parameters when deploying NexentaFusion Docker.

Parameter	Description
`--name`	Use this parameter to assign a name to the container.
`-v /opt/docker/esdb`	This folder will contain the elasticsearch database and logs.
`-v /opt/docker/fusion`	This folder will contain the server data, the localdb and the fusion logs.
`-e MGMT_IP` `Management IP`	The container's IP that is used for communication between NexentaFusion and NexentaStor appliances for appliance events, logs and analytics data. If you do not set this parameter, the NexentaFusion container will appear to function properly but the registered NexentaStor appliances will not send analytics, alerts, events and so on.

`--ulimit nofile=65536:65536 --ulimit memlock=-1:-1`	Required to set OS values properly for ESDB.
`-e TZ`	Optional parameter to set the timezone. If not set, it will default to UTC.
`--memory`	Limits the maximum amount of memory the container can use.
`-e ES_HEAP_SIZE`	Heap size should be limited to half the total memory size.
`--net`	Use this parameter to connect the container to a network. In the above example, "--net=host", the container uses the host's network settings. You can configure the container's network differently, but be sure that it is accessible from the browser, and MGMT_IP is accessible for NexentaStor appliances.
`nexenta/fusion`	The container image name.

Configuring Advanced Actions

After you deployed NexentaFusion using Docker container, use the "bundle" command at the docker command line to create and upload a support bundle. You must be root to run this tool.

Collect Support Bundle

```
usage: bundle [-q|-v|-d] [-u] [-c path] [-t "description" ] [-n name]
options:
      -q - quiet mode, all warning and diagnostic messages will be suppressed
      -v - verbose mode, print all messages to stdout
      -d - dialog mode, display messages using dialog boxes

default mode: quiet
      -u - upload the bundle to the Nexenta Support server
      -c path - bundle destination directory, default: /var/lib/nef/bundles
      -t text - bundle description text, default: ""
      -n name - bundle name, default: random UUID
```

Bundle Examples

```
      bundle -u --- Create bundle and upload it to the Nexenta Support server
      bundle -t "My bundle" -u --- Create bundle with description and upload
```

Note: Changing the support bundle name may impact uploading the bundle to the Nexenta Support server.

Bundles created using the docker command line will be visible in the Fusion UI on the Support screen for later removal only if they were created in the default destination directory.

Reset Self-signed Certificate

NexentaFusion uses a default HTTPS certificate. After you deployed NexentaFusion using Docker container, use the following command at the docker command line to reset the currently installed HTTPS certificate to a default self-signed certificate.

1. At the Docker command line, enter "fusion-reset-ssl".
2. Enter "y" when asked if you want to continue.

Deployment Using OVA

This section covers the following topics:

- The prerequisites for a successful NexentaFusion deployment in a virtual environment.
- Instructions on how to download and deploy NexentaFusion using OVA in any of the following ways:
    - Upgrade to the latest version from a previously installed version.
    - Perform a new installation.

System Requirements

Table 3: System Compatibility

Resources	
VMware ESXi	6.0
VMware Workstation	12.x
VMware Fusion	8.x
VMware Player	12.x
Browsers	Latest Chrome and Firefox v47 or newer

Table 4: System Requirements for VM Installation

Resources	
CPUs	4vCPU
Memory	16GB in total
Disk Size	80GB (Thin Provisioned)
Port Groups	1 or 2 (ensure that they are on different subnets)

Network Requirements

The following Ports must be open:

- TCP 8457 - Web Server
- TCP 2000 - Private API
- TCP 9200 - Elasticsearch
- TCP 8443/8080 - REST API

Deploying NexentaFusion OVA

For deploying OVA, refer to the appropriate VMware documentation based on your infrastructure.
The following example covers the steps to deploy OVA using the vSphere 6.0 client or the vSphere Web Client. To deploy the OVA, ensure that you have the right VMware hardware version, and proper network mapping.

Before deploying NexentaFusion ensure that the ESXi time is set properly.

1. Download the OVA from the URL in the fulfillment email
2. In the vSphere client, click on File → Deploy OVA
   Or in the vSphere Web Client, right click on the hosts or cluster → Deploy OVA
    - Browse the OVA file, begin the OVA import
      Map the networks used in this OVF template to networks in your inventory
3. Power On the VM

Note: If you need to deploy the OVA on the node without internet connection, use the same steps to deploy the OVA from the CDROM or thumb drive.

Configuring Network

About NexentaFusion Network Interfaces

NexentaFusion OVA is created with two defined interfaces eth0 and eth1. As a result NexentaFusion 1.1.1 supports configuration with two separate networks and also supports configuration with a single network for both the management access and public access.

- Management access: Interface to be used for communication from the NexentaStor appliance to NexentaFusion, for appliance events and analytics data.
- Public access: Interface to be used to access the NexentaFusion GUI.

Proposed Configuration

There are 2 methods to configure the network interfaces:

Using a single interface and IP address for management and UI access

- NexentaFusion OVA is created with two defined interfaces eth0 and eth1, and by default one of the interfaces will not be connected/ powered ON. This allows you to use a single interface and IP address for management and public access after the OVA is successfully deployed.

  To configure this single interface, see “Using a Single Interface”.

Using both interfaces to separate the management access from the Web access

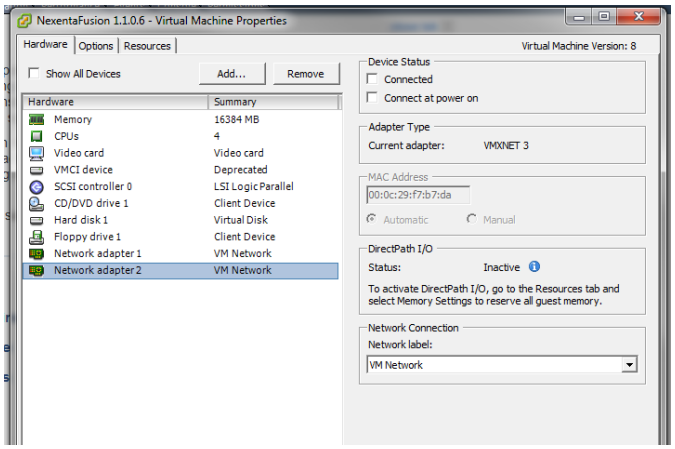
To utilize this capability, you need to have 2 separate networks:

- A public network for web access to the GUI
- A private network, not accessible to the public, on which you configure the management address, for communication from the NexentaStor appliance to NexentaFusion, for appliance events and analytics data.

To use both the interfaces, follow these steps prior to powering on the VM and after deploying the OVA:

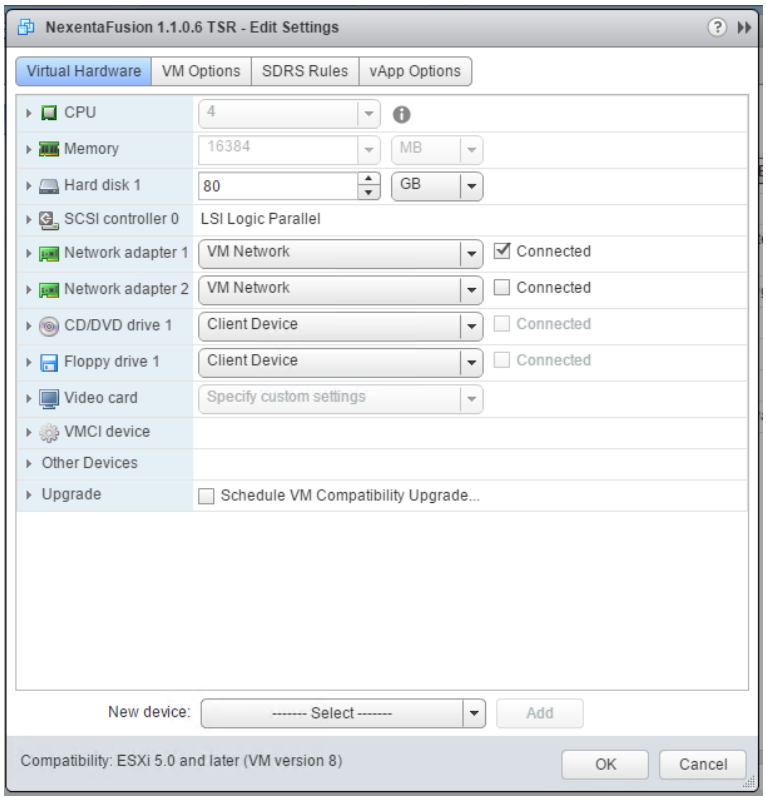
In vSphere client:

1. Select the VM
2. Click “Edit Settings”
3. Under the Hardware tab, select the Network adapter 2
4. Navigate to the Device Status
5. Select the checkbox Connected and Connect at power on
6. Click Ok



In vSphere Web client:

1. Right click the VM in the inventory
2. Select Edit Settings
3. On the Virtual Hardware tab, select the Network adapter 2
4. Select the checkbox Connected
5. Click OK.



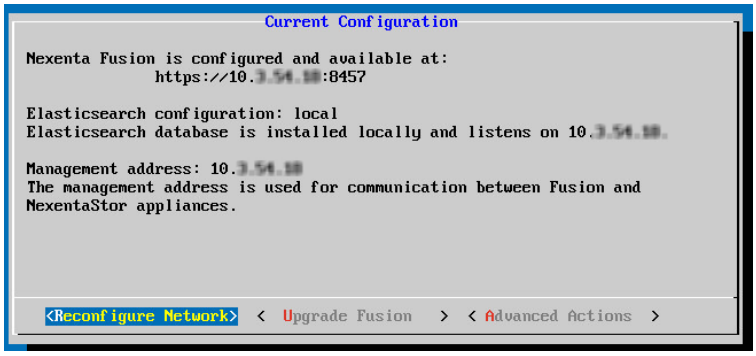
To configure both the interfaces, see “Using Both the Interfaces”.

Using A Single Interface

After deploying the OVA and powering on the VM, switch to the Console window to monitor the startup of Fusion and the Console wizard. The Fusion startup code will query the network interfaces and their addresses. Fusion will set the management address as the first non-loopback address. This reconfiguration process can take several seconds.

When the wizard startup is complete, it will display the current network configuration.

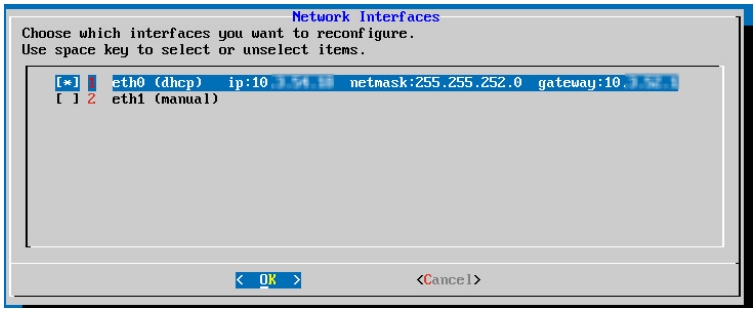
> Note: If the management address still displays as 127.0.0.1, wait a few seconds to allow Fusion startup to complete, then click "Reconfigure Network" and "Cancel" to refresh the configuration settings.



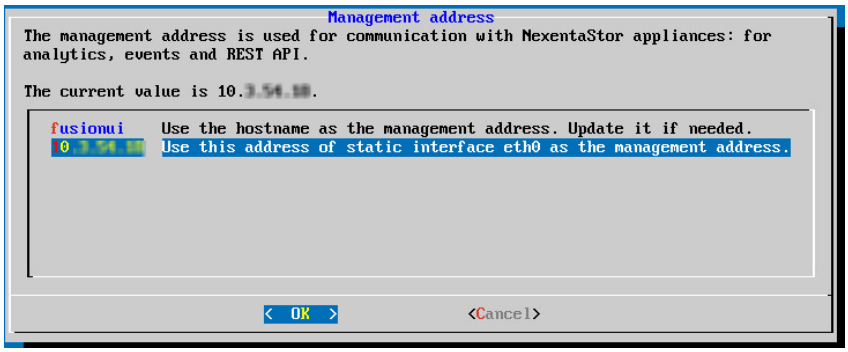
This default configuration can be edited to, for example, use a fully-qualified host name as the management address.

Follow the steps below to reconfigure.

1. Click Reconfigure Network to configure the interface
2. Type the "admin" password: nexenta
3. Click OK to reconfigure eth0



4. Follow the prompts in the wizard
   The wizard provides you with the options to configure the interfaces as static or DHCP, and set up the netmask, gateway, DNS and search domain.
5. Now you will be prompted to configure the management address
6. If you have configured your interface with dhcp, it is recommended that you select the hostname as the management address. The hostname must be resolvable
7. Optionally change the hostname



USING BOTH THE INTERFACES

To utilize this capability, you need to have 2 separate networks:

- A public network for web access to the GUI
- A private network, not accessible to the public, on which you configure the management address, for communication from the appliance to the elasticsearch database, and between NexentaFusion and the database.

To configure both the interfaces:

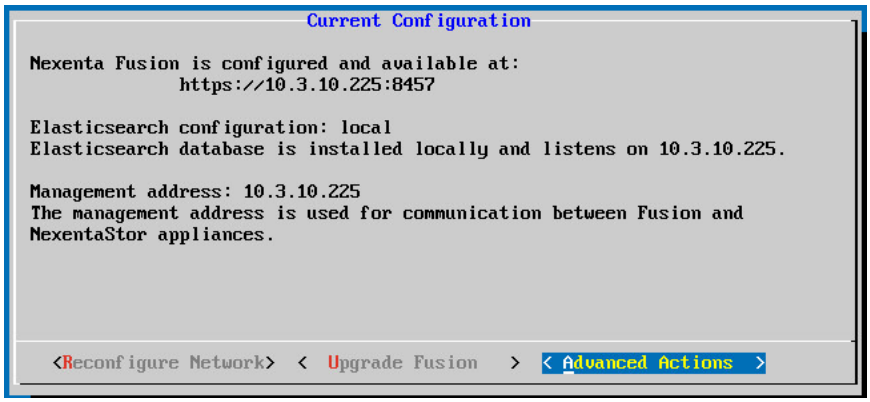
1. After you deploy the OVA, power-on the VM
2. Open the console window
3. Select 'Reconfigure Network' to configure the interfaces
4. Select both the interfaces for reconfiguration
5. Configure one of the interfaces for web access to the GUI
6. Configure the other for communication from the appliance to the elasticsearch database, and between NexentaFusion and the database
7. Now you will be prompted to configure the management address. Select the interface that you configured for communication between Fusion and database.
8. Follow the prompts in the wizard
9. The wizard provides you with the options to configure the interfaces as static or DHCP, and set up the netmask, gateway, DNS and search domain.

Note: If you configure a Fusion server that has more than one network adapter on the same physical network and protocol subnet, you may experience unexpected results.

Configuring Advanced Actions

After you deployed the OVA, follow these steps to collect a Support Bundle and to a create Self-signed HTTPS Certificate.

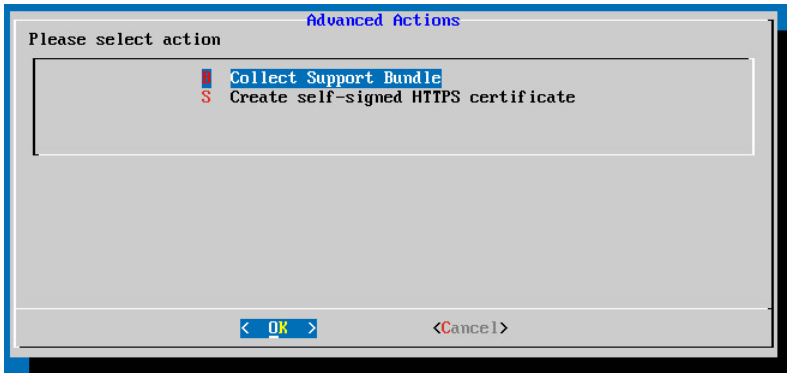
1. After you deploy the OVA, power-on the VM
2. Open the console window
3. Select **Advanced Actions** to perform the advanced actions



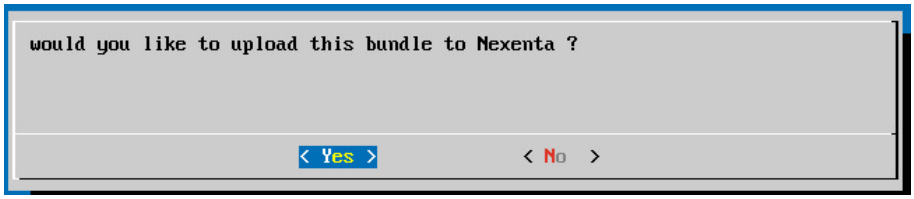
Collect Support Bundle

A support bundle (SB) is an archive containing important system information for Nexenta support service (system configuration files, database logs and so on). From the console, support bundles can be created even when the Fusion management layer is not functioning, which makes bundles useful for troubleshooting purposes.

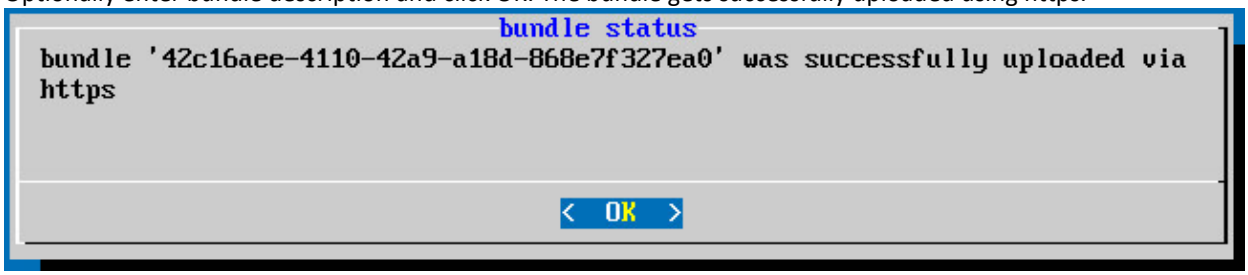
4. Select Collect Support Bundle
5. Click Ok



6. Select Yes to upload this bundle to Nexenta



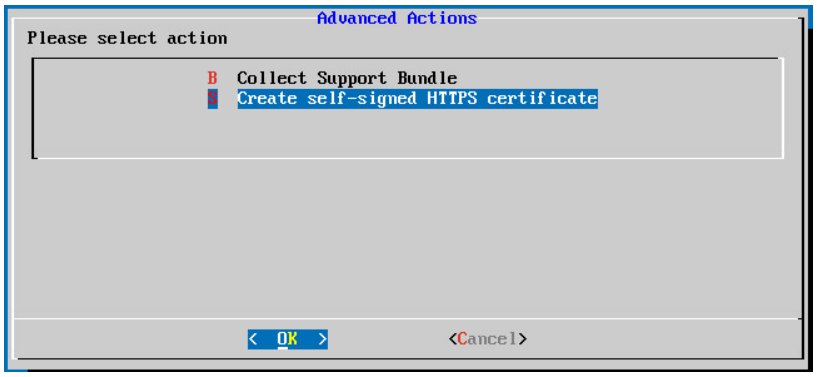
7. Optionally enter bundle description and click OK. The bundle gets successfully uploaded using https.



Reset Self-signed Certificate

NexentaFusion uses a default HTTPS certificate. Choose this option to reset the currently installed HTTPS certificate to a default self-signed certificate.

1. After you deploy the OVA, power-on the VM
2. Open the console window
3. Select **Advanced Actions** to create self-signed certificate
4. Select Create self-signed HTTPS certificate
5. Click OK



6. Click **Yes** to reset
7. This recreates the self-signed certificate

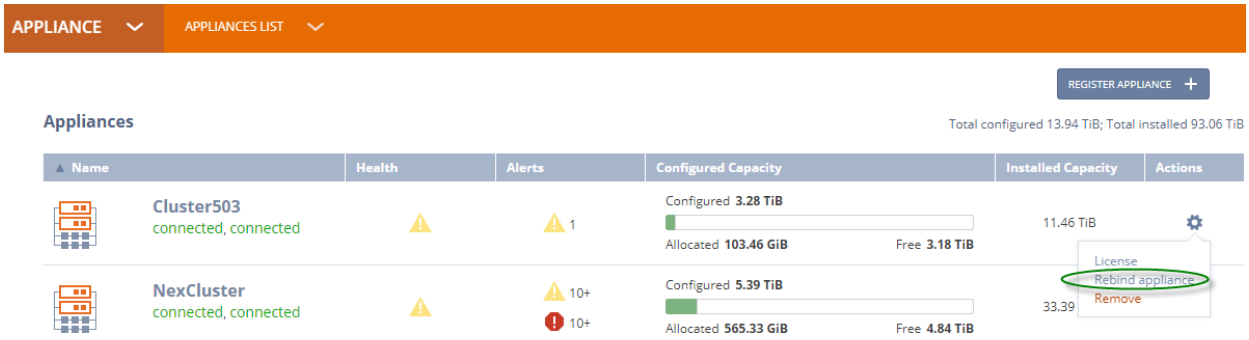
Troubleshooting

- Unable to retrieve appliance events and analytics data:

  Make sure the management address is accessible by the Appliance. If you have used the hostname as the management address, make sure it is resolvable.
  Run the following command from the Appliance to verify if the node is bound to NexentaFusion.

```
CLI@node> node status
 FUSION IP     LOG SEVERITY   ESDB SERVERS
 10.3.79.132   error          10.3.79.132
```

  If the appliance failed to bind, navigate to the NexentaFusion GUI and under Appliance list, select the relevant appliance, click on its COG and click **Rebind appliance**.



- Unable to access the UI after configuring the network:

  Check your network, make sure you have access to the IP address you are trying to use. Ensure that the gateway is configured.

Accessing NexentaFusion GUI

After a successful installation, the console wizard displays the URL for accessing the Nexenta Fusion from the supported web browser. Point your browser to the URL that is displayed. The initial login credentials are `admin / nexenta`.

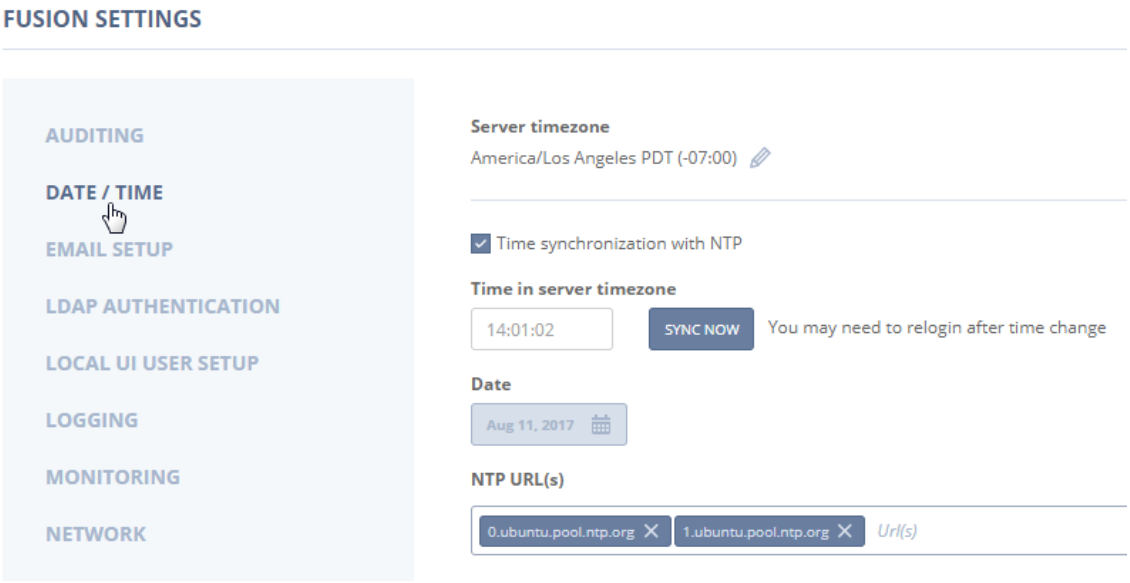
Note: On the first login into the Web UI you will be asked to configure a new password.

Configuring NTP and TimeZone

You can synchronize the NexentaFusion time setting with the NTP server, or manually configure the time in the server time zone. To synchronize the NexentaFusion time setting with the NTP server, you must add a reachable NTP hostname. This section demonstrates how to automatically synchronize the NexentaFusion time setting with the NTP server, as well as how to manually configure the date and time.

Use the following sequences to configure date and time for the Fusion server:

1. Log in to NexentaFusion as an administrator, click the Main COG in the top right corner of the window, and select Settings from the drop-down list.
2. In the left panel, select Date/Time.



To set the server timezone:

1. Click the pencil icon to display the change timezone dialog. Select the server timezone country and locale.
2. Enter your login name, and click Save & Reboot.

To synchronize with the NTP server:

3. Click the time synchronization with NTP check box.
4. Enter the URL for the NTP server of your choice.
5. Click Save.

To set the date and time if NTP servers have been configured:

6. Click “SYNC NOW” to set the server time with the time retrieved from the NTP server.

To manually set the date and time:

7. Deselect the time synchronization with NTP check box.
8. In the Time in server timezone field, enter the hour, minutes, and seconds (hh:mm:ss)
9. Click inside the Date field, and select a date from the pop-up calendar.
10. Click Save.

Registering NexentaStor Appliances

Follow these steps to connect the NexentaStor appliances you want to manage with the NexentaFusion interface.

> Note
> To register an appliance using NexentaFusion, the appliance must be licensed.
>
> Clustered appliances must be licensed and configured using the CLI before they can be registered with NexentaFusion. Both clustered nodes must be up and running to successfully complete the registration process.

11. Log in to the NexentaFusion application.
12. Go to the Appliance List view and click on the **Register Appliance** button.
    - To register clustered nodes: If both nodes have the same credentials, enter FQDN or the IP address of one of the nodes in the cluster. Otherwise, you will be prompted for the IP of both nodes in the cluster.
    - To register a single node: enter its IP address.
13. You can edit the port number to override the default value and provide the associated details.
14. Follow the wizard prompts. See the NexentaFusion documentation for more details.
15. Verify the information on the Registration screen. You can enter additional settings now or later.
16. Click **Confirm**.
17. Repeat steps 2 to 6 for each additional NexentaStor appliance you want to manage.

Reconfiguring Network

To reconfigure the NexentaFusion network via the UI

1. Navigate to Fusion Main COG -> Fusion Settings -> Network
2. Make necessary network changes

To reconfigure NexentaFusion network via console wizard

1. Open NexentaFusion VM console
2. Click on "Reconfigure Network"
3. Make necessary network changes

Upgrading to the Latest NexentaFusion

Power off the Fusion VM and then create a snapshot on your hypervisor before upgrading. Consult your hypervisor product documentation for specifics on creating snapshots.

With Internet Connection

1. Open the Nexenta Fusion VM console.
2. Click on Upgrade Fusion button.
3. Configure the proxy server if you need to use one to access the repositories for upgrading NexentaFusion software packages.
4. Optionally, provide the user name and the password as part of the URL as shown in the example below.

   https://user:pass@ip:port

   or just use http as shown below

   http://ip:port

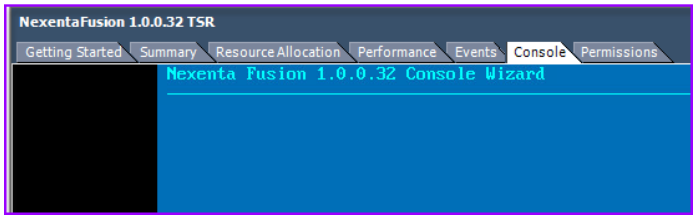
5. If upgrade is available, click OK to continue with the upgrade.
6. After successful upgrade, click OK to reboot the NexentaFusion server.
7. Validate that the version has changed by checking the version number on the top left of console wizard.

Without Internet Connection

You can upgrade to the latest NexentaFusion from the darksite CD provided by Nexenta.

1. Mount the ISO to Nexenta Fusion VM.
2. Log in as admin, open console or SSH into Fusion VM.
3. Mount cdrom `sudo mount \/dev\/cdrom \/media\/cdrom`.
4. Add the NexentaFusion repository using the command `sudo apt-add-repository "deb file:///media/cdrom fusion main"`.
5. Take a snapshot of the NexentaFusion server.
6. Update and upgrade using `sudo apt-get update -y && sudo apt-get upgrade fusion`.
7. Reboot the NexentaFusion server.
8. Validate that the version has changed by checking the version number on the Nexenta Fusion console wizard tab.

Figure: Validating the Upgrade



Note: In case of unsuccessful upgrade, please contact support@nexenta.com.

Additional Resources

After installing NexentaStor 5.1.1and NexentaFusion 1.1.1, use the resources listed in Table 4 for more information. These documents are posted in https://nexenta.com/products/documentation.

Table 4: Related Documents

Document Name	Description
NexentaStor 5.1.1	
CLI Configuration QuickStart	Provides basic information and instructions for: • Configuring the network and snapshots. • Creating pools, file systems, volume groups, and volumes. • Sharing file systems and volumes.
CLI Reference Guide	Includes: • A list of NexentaStor commands, subcommands, and descriptions. • A list of UNIX-like utilities to use in NexentaStor.
VVOL Admin Guide	Documents a policy-based approach for managing external storage in virtualized environments by allowing automated provisioning of VMs.
vCenter QuickStart	Provides information on how to use the vCenter Web Client plugin to manage multiple NexentaStor 5.x appliances.
HA QuickStart	Includes CLI steps to configure clusters for high availability (HA).
REST APIs QuickStart	Contains instructions to get online REST API documentation to configure and manage your appliances.
Product Guide	Provides an overview of the NexentaStor capabilities.
High Performance Replication (HPR) User Guide	This document demonstrates how to configure High Performance Replication (HPR) to replicate datasets using the NexentaStor Command Line Interface (CLI) and using the NexentaFusion GUI.
Data-At-Rest Encryption with Self-Encrypting Drive Configuration Guide	This document demonstrates how to protect the data at rest.
NexentaFusion 1.1.1 User Guide	The NexentaFusion User Guide and GUI online help (click HELP under the COG wheel icon in the top menu bar) are available.