NSFOCUS Log Audit System Installation Guide (x86)

Version: V2.0R02IB00 (2026-06-16)

Confidentiality: Restricted

■ Statement

The purchased products, services, or features are stipulated in the contract made between NSFOCUS and the customer. Part of products, services, and features described in this document may not be within the purchased scope or the usage scope.

All information in this document is provided "AS-IS" without guarantees of any kind, express or implied. The information in this document is subject to change without notice. It may slightly differ from the actual product due to version upgrade or other reasons.

■ Disclaimer

Please read the disclaimer carefully before using the product. Once you use the product, you acknowledge and agree to all the contents of this disclaimer. NSFOCUS shall not assume any responsibility for any loss or damage in the following circumstances:

- Data loss and system availability reduction caused by the negligence or misconduct of the system O&M or management personnel, for example, they do not handle alerts that affect system stability and availability in a timely manner.
- Data loss and system availability reduction caused by the fact that the traffic exceeds the planned hardware capacity.
- Data loss and system availability reduction or unavailability caused by natural disasters (including but not limited to floods, fires, and earthquakes) or environmental factors (including but not limited to network disconnection and power outage).

Contents

Preface

This document describes the installation and deployment of NSFOCUS Log Audit System ("LAS" for short) x86 virtualization edition.

This document is provided for reference only. It may slightly differ from the actual product due to version upgrade or other reasons.

Change History

Version	Description
V2.0R02IB00	Initial release.

Technical Support

Hardware and Software Support

Email: support@nsfocusglobal.com

Cloud Mitigation Support

Email: cloud-support@nsfocusglobal.com

Phone:

- USA: +1-844-673-6287 or +1-844-NSFOCUS
- UK: +44 808 164 0673 or +44 808 164 0NSF
- Netherlands Toll: +31 85 208 2673 or +31 85 208 2NSF
- Australia: +61 2 8599 0673 or +61 2 8599 0NSF
- Brazil: +55 13 4042 1673 or +55 13 4042 1NSF
- Japan: +81 3-4510-8673 or +81 3-4510-8NSF
- Singapore: +65 3158 3757
- Middle East: +973 1619 7607
- Hong Kong, China: +852 5803 2673 or +852 5803 2NSF
- Macao, China: +853 6825 8594
- Chinese Mainland: +86 10 5387 5981

Documentation Feedback

For any query regarding the usage of the documentation, you can contact us:

Email: info-support@nsfocus.com

1 Installing LAS (x86)

This section describes the installation steps and related preparations of LAS.

1.1 Configuration Requirements

The following describes the configuration requirements for the physical host and the virtual machine of LAS.

Physical Host Requirements

The virtualized LAS must run on a physical host. Ensure that the host meets the requirements shown in Table 1-1 and Table 1-2.

Table 1-1 Physical Host Requirements by Deployment Scenario

Scenario	Hardware Quantity
Basic Log Audit	1 Recommended server (x86 server)

Table 1-2 Physical Host Hardware Requirements

Hardware		Server
Minimum Configuration	CPU	2*E5-2640 V2 (4 cores, 8 threads)
	Memory	64 GB DDR3 1333MHz
	Hard Disk	8 TB (ext4 file system, 7200 RPM), Raid5
Recommended Configuration	SWAP Partition	Half of the memory, 32 GB
	NIC	Gigabit NIC
	RAID Controller	RAID controller with Raid cache
	Optical Drive	Built-in optical drive
	Power Supply	Hot-swappable redundant power supply (1+1), 1100 W

Note	• Available hard disk space mainly refers to the available disk space on the mounted partition where the /opt directory resides. • Gigabit network environment is required.

Virtual Machine Requirements

LAS virtual machine requirements are shown in Table 1-3.

Table 1-3 Virtual Machine Requirements

Hardware	Server
CPU	4 cores, 8 threads
Memory	16 GB / 32 GB
Hard Disk	• Minimum system disk size: 30 GB. • Minimum data disk size: 500 GB. Note The above are the minimum requirements. You can increase these values as needed.

1.2 Preparations

Before installing and deploying LAS, complete the preparations shown in Table 1-4.

Table 1-4 Preparations

Preparation Item		Description
LAS	IP Address	Ensure that the physical host has normal network connectivity.
	OS Login Account	Requires root account privileges.
	Time	The time zone must match the local region, and the time must be synchronized with Asia/Shanghai time.
	Hostname	Set the server hostname and ensure it is unique within the LAN. Special characters are not allowed.
	Service	LAS must be deployed independently. Do not deploy other services on it.
Host Accessing LAS	Browser	If pop-ups are blocked or Javascript is disabled, cancel those settings.

The network firewall policy of LAS is shown in Table 1-5.

Table 1-5 LAS Network Firewall Policy

Service Name/Purpose	Port	Protocol	Input Rule	Output Rule
Online Upgrade	80	TCP	Deny	Accept
Nginx	443	TCP	Accept	Accept
NPAI V2	5002,5003,50071	TCP	Accept	Deny
NPAI V3	5050	TCP	Accept	Accept
NPAI V3	5009,5051	TCP	Accept	Deny
Cloud	5553,5005	TCP	Deny	Accept
Redis Service	6379	TCP	Accept	Deny
Device Addition	8081	TCP	Accept	Deny
Kafka	9092	TCP	Accept	Deny
FTP Storage Service	50061	TCP	Accept	Deny
NSFOCUS Log Collection	50071	TCP	Accept	Deny
Log Analysis Service	18630	TCP	Accept	Deny
Agent Communication UDP Port	17046	UDP	Accept	Deny
Agent Communication TCP Port	17047	TCP	Accept	Deny

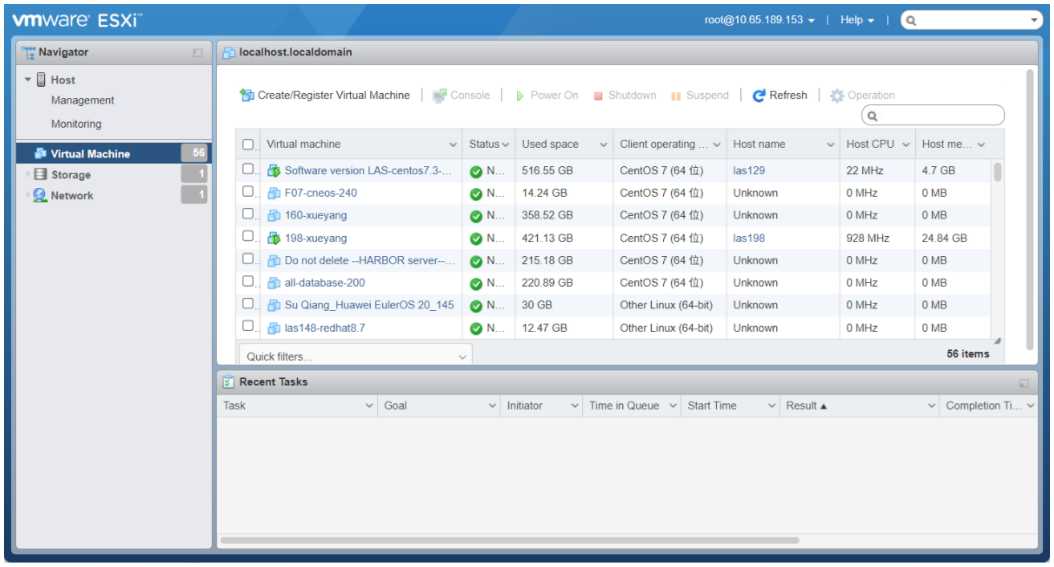
1.3 Importing LAS into Virtualization Platform

The following section uses VMware ESXi 6.7.0 as an example to introduce how to import a x86 virtualization edition of LAS into a virtualization platform. Before importing it, obtain the LAS virtualization file, for example, "install.LAS.V2.0R02IB00.x86_64.postgresql.20260420.85060.ova".

The steps for importing x86 VM LAS into VMware ESXi 6.7.0 are as follows:

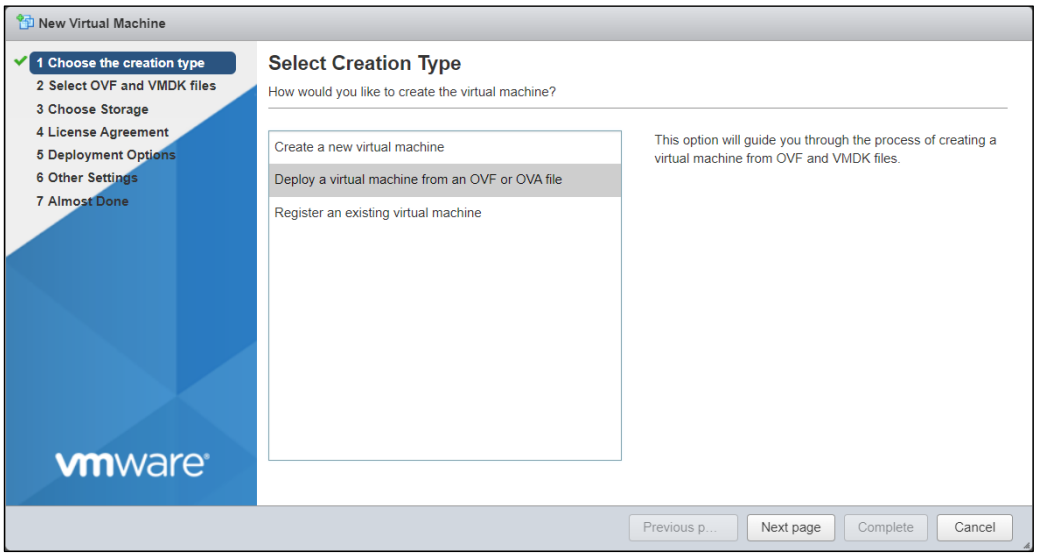
Step 1 Open VMware ESXi and click **Create/Register Virtual Machine**, as shown in Figure 1-1.

Figure 1-1 Creating/Registering VM



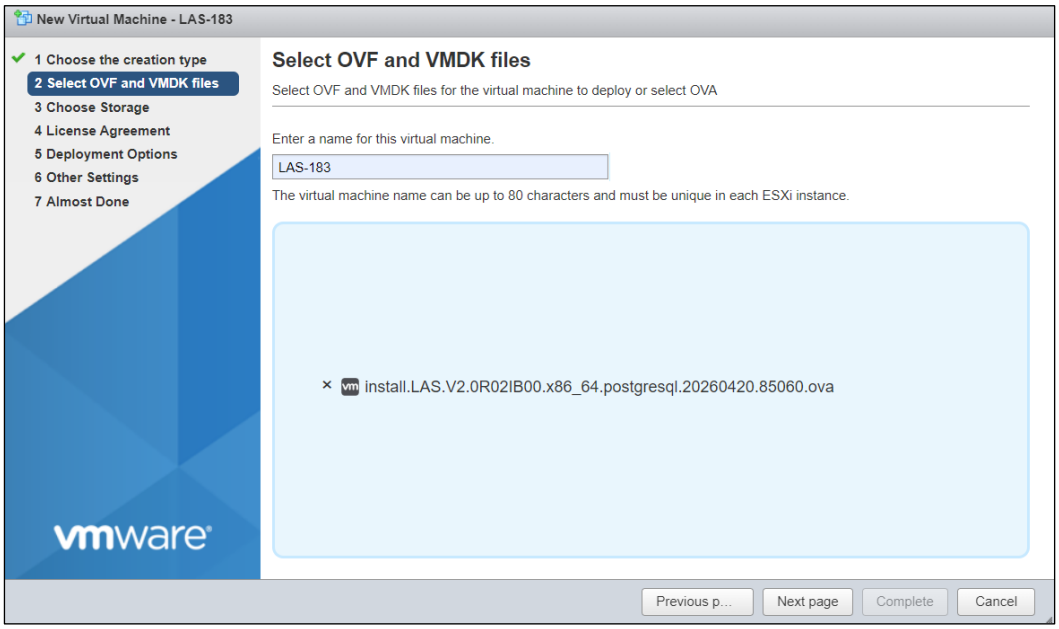
Step 2 Select **Deploy a virtual machine from an OVF or OVA file**, as shown in Figure 1-2.

Figure 1-2 Selecting Creation Type



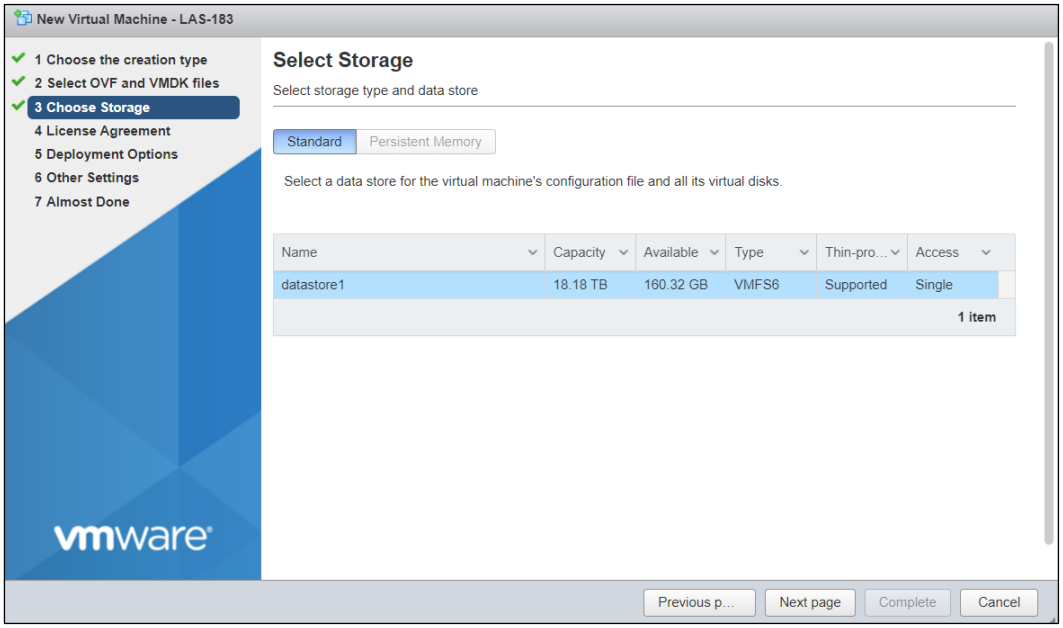
Step 3 Configure the VM name, as shown in Figure 1-3.

Figure 1-3 Configuring VM Name



Step 4 Select the target data storage, as shown in Figure 1-4.

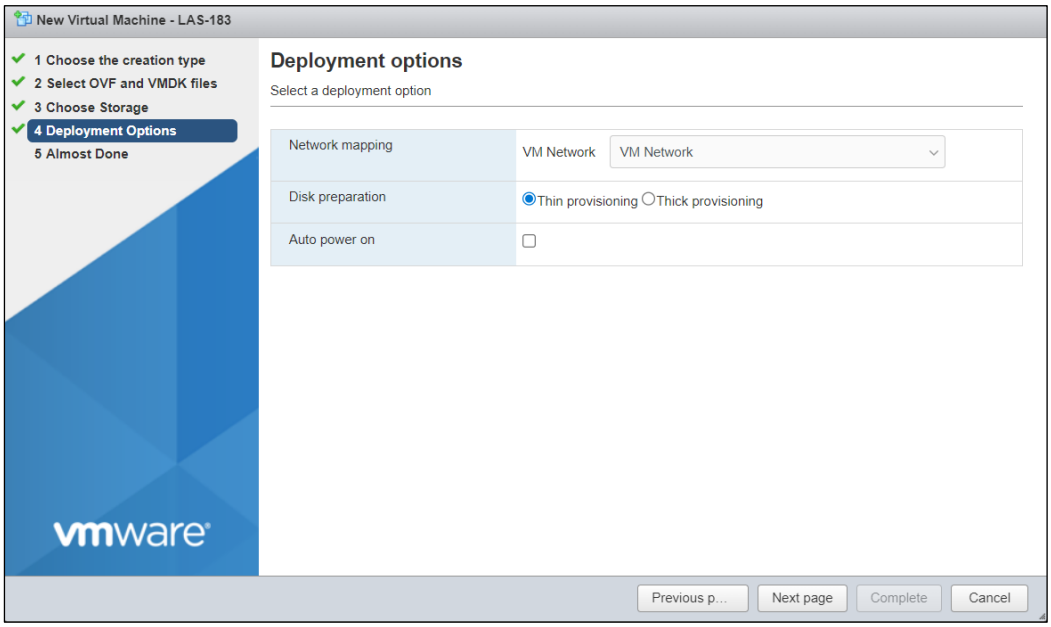
Figure 1-4 Selecting Storage



Step 5 Select Deployment options, as shown in Figure 1-5.

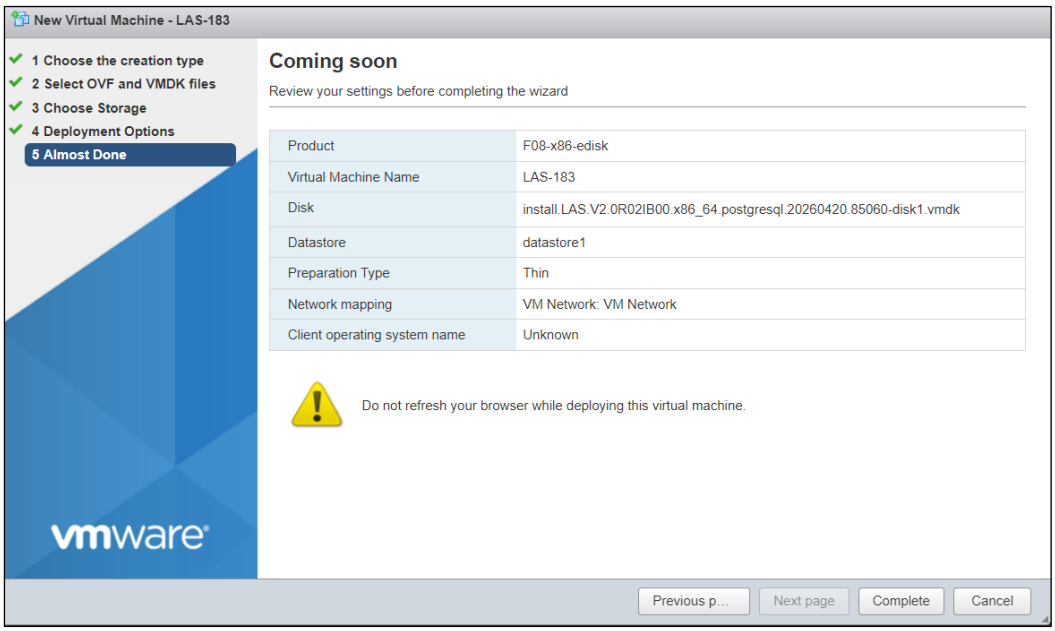
Do not select **Auto Power On**.

Figure 1-5 Select Deployment Options



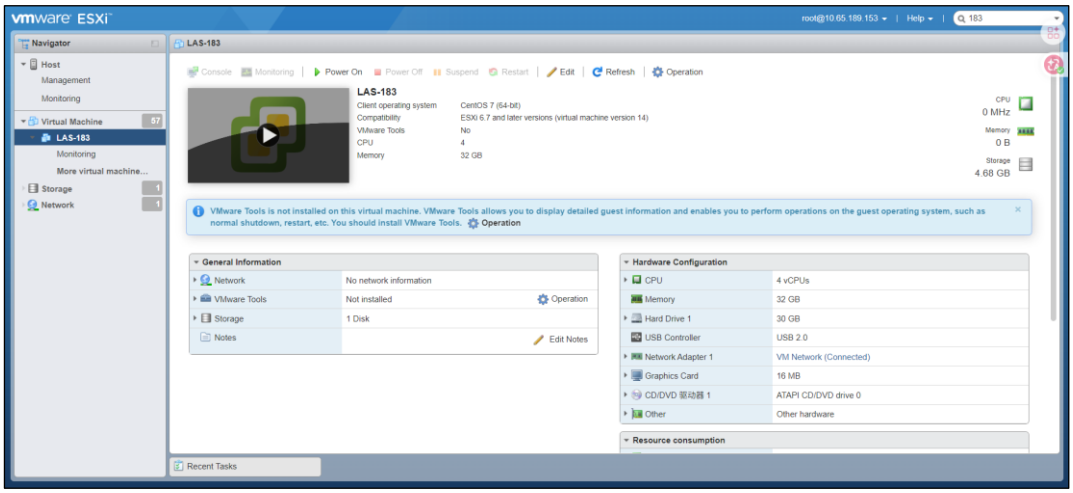
Step 6 Confirm the configurations and click **Complete**, as shown in Figure 1-6.

Figure 1-6 Configuration Confirmation



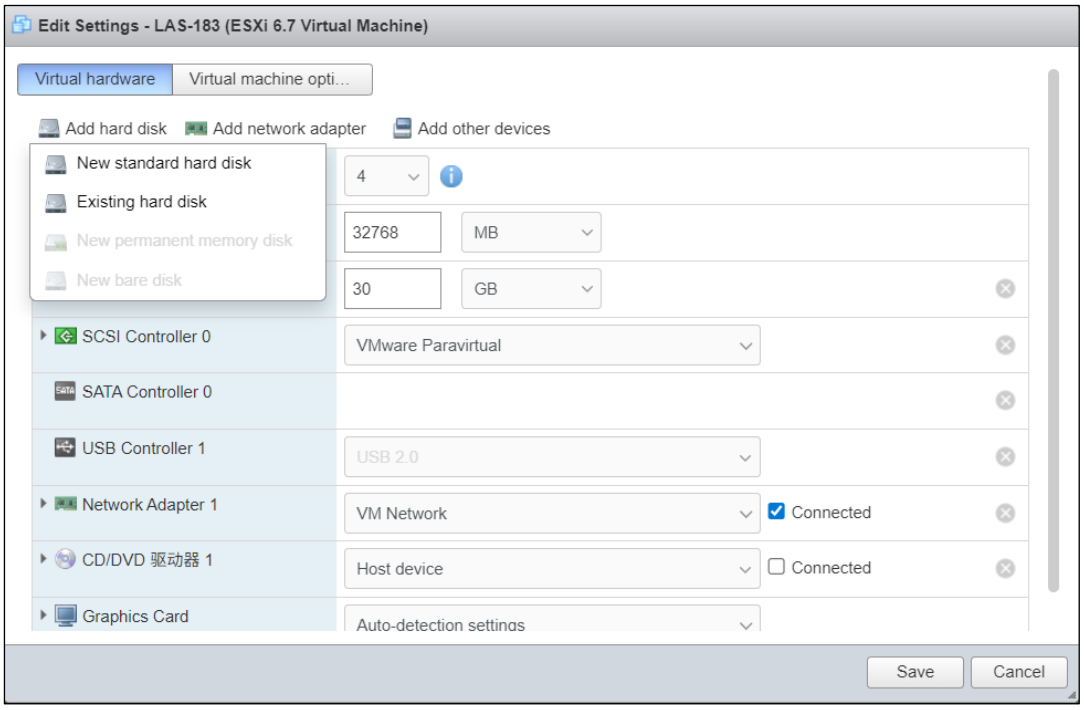
Step 7 View VM information, as shown in Figure 1-7.

Figure 1-7 Viewing VM Information



Step 8 Click **Edit** to add a virtual hard disk, as shown in Figure 1-8.

Figure 1-8 Adding Hard Disk



Tip	Select **New Standard Hardware Disk** or **Existing Hard Disk** as appropriate. In Most Cases, select **New Standard Hardware Disk**.

Step 9 Add a disk of at least 500 GB and allocate optimal memory and CPU to the VM. The configured CPU must exceed the minimum requirements.

----End

1.4 Configuring LAS

After importing LAS x86 edition into the virtualization platform, power on the VM. Then the system automatically mounts the system disk and data disk.

The initialization steps on the console are as follows:

Step 1 Log in to the console using the developer account (with a one-time password; contact NSFOCUS technical support to obtain the password), as shown in Figure 1-9.

Figure 1-9 Console Login

Step 2 Use the **df –h** command to check the **mnt** directory.

- If the **mnt** directory does not exist, the disks have been mounted successfully, as shown in Figure 1-10.
- If the **mnt** directory exists, the disks have not been fully mounted. Wait for the **mnt** directory to disappear automatically.

After disk mounting is complete, the system restarts automatically.

Figure 1-10 Checking the **mnt** Directory

```
develop>df -h
Filesystem                Size  Used Avail Use% Mounted on
/dev/mapper/crypted_root  7.6G  3.8G  3.4G  53% /mnt/cf
unionfs                   7.6G  3.8G  3.4G  53% /
/dev/sda3                  22G  3.3G   19G  15% /opt
devtmpfs                   16G     0   16G   0% /dev
tmpfs                      16G   64K   16G   1% /dev/shm
tmpfs                      16G  1.2M   16G   1% /run
tmpfs                      16G     0   16G   0% /sys/fs/cgroup
/dev/sda1                 194M   60M  125M  33% /boot
tmpfs                     3.2G     0  3.2G   0% /run/user/0
/dev/sdb3                  10G   33M   10G   1% /tmp
/dev/sdb4                 464G  126M  464G   1% /opt/nsfocus/espc/data
```

Step 3 After the system restarts automatically, run the **df –h** command again to check the **mnt** directory, as shown in Figure 1-11.

Figure 1-11 Double-checking the **mnt** Directory

```
develop>df -h
Filesystem                Size  Used Avail Use% Mounted on
/dev/mapper/crypted_root  7.6G  3.8G  3.4G  53% /mnt/cf
unionfs                   7.6G  3.8G  3.4G  53% /
/dev/sda3                  22G  3.3G   19G  15% /opt
devtmpfs                   16G     0   16G   0% /dev
tmpfs                      16G   64K   16G   1% /dev/shm
tmpfs                      16G  1.2M   16G   1% /run
tmpfs                      16G     0   16G   0% /sys/fs/cgroup
/dev/sda1                 194M   60M  125M  33% /boot
tmpfs                     3.2G     0  3.2G   0% /run/user/0
/dev/sdb3                  10G   33M   10G   1% /tmp
/dev/sdb4                 464G  126M  464G   1% /opt/nsfocus/espc/data
```

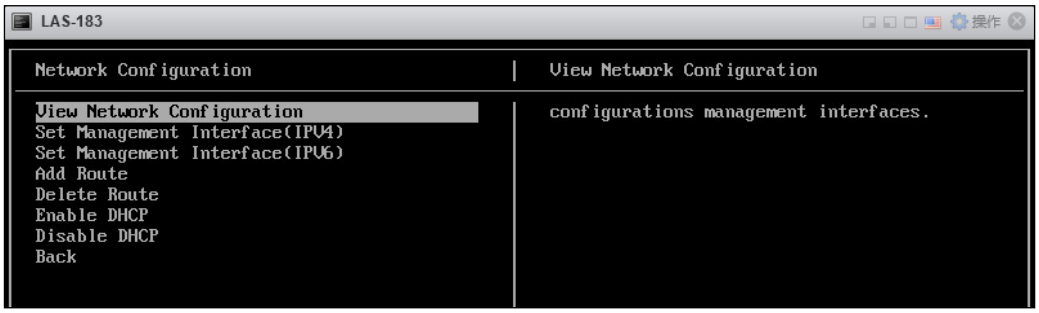
Step 4 Log in to the **conadmin** account. For the username and password, see Default Parameters.

Note	After the disks are mounted and the system restarts automatically, use the **conadmin** account to modify the IP address of LAS. If disk mounting has not been completed yet, the IP change will fail.

Step 5 Select **Network Configuration** and modify the IP address of LAS, as shown in Figure 1-12.

Note	If the network does not support DHCP and a static IP is required, disable DHCP first and then configure the IP address.

Figure 1-12 Modifying IP Address



Step 6 Modify the IP address through the serial port. After waiting for 10 minutes, the VM LAS can be used normally.

----End

2 Deploying LAS (x86)

After the VM LAS is installed, the default mode is watermark-based authentication. Users can switch the authentication method as needed.

The authentication methods of VM LAS x86 are described in Table 2-1.

Table 2-1 Authentication Methods of VM LAS x86

Authentication Method	Description
Cloud Authentication	To use Cloud authentication, the LAS device must be connected to the network and able to maintain connectivity with the NSFOCUS Cloud. When a certificate is imported into the LAS device, it sends the certificate information to the NSFOCUS Cloud authentication platform for device activation. After a successful activation, it enters the authentication process. LAS periodically sends authentication requests to the Cloud. after a successful authentication, LAS runs normally and all functions are available.
Watermark-based Authentication	Applicable when the device running LAS cannot connect to the public network. After importing a certificate into the LAS device, provide the information in the certificate to NSFOCUS technical support to obtain the corresponding watermark file. After importing the watermark file, it is compared with the certificate file. If they match, authentication succeeds and LAS runs normally with full functionality.

The deployment of LAS differs slightly depending on the authentication method. The following sections use the Firefox browser as an example to describe how to switch authentication modes for different authentication methods.

Note	Do not modify or delete the accounts, passwords, or directories created by LAS.

For factory defaults and supported browsers, see A Appendix.

2.1 Logging in to LAS

The steps for logging in to the web-based manager of LAS are as follows:

Step 1 On the login page, enter the default administrator username and password. See Default Parameters.

Step 2 Click **Log In**.

The first time you log in to LAS, a dialog box for changing the login password appears.

Step 3 Configure a new login password.

Configure the new login password according to the format and length requirements shown on the page.

Step 4 Click **OK**.

Then log in again with the new password.

----End

2.2 Switching to Cloud Authentication

To switch to Cloud authentication mode, perform the following steps:

Step 1 Hover over the  icon, choose **License** > **Certificate Upload**, and confirm the authentication mode to be changed.

Step 2 Click **Replace** to enter the authentication mode selection page.

Step 3 Click **Cloud Authentication** to enter the certificate upload page.

Step 4 Click **Select Certificate File**, choose a valid certificate file from the local machine, and the page displays the certificate information.

Step 5 Click **Confirm Import**. After activation succeeds, the system prompts for a restart.

Step 6 Click **OK**. You will be logged out and required to log in again after 3~ 5 minutes to complete the authentication mode switch.

----End

2.3 Switching to Watermark-based Authentication

To switch to watermark-based authentication mode, perform the following steps:

Step 1 Hover over the  icon, choose **License** > **Certificate Upload**, and confirm the authentication mode to be changed.

Step 2 Click **Replace** to enter the authentication mode selection page.

Step 3 Click **Watermark-based Authentication** to enter the certificate upload page.

Step 4 Click **Select Certificate File**, choose a valid certificate file from the local machine.

Step 5 Copy the device information and provide it to NSFOCUS technical support to obtain the watermark file.

Step 6 Click **Upload Watermark** to import the valid watermark file obtained. After authentication succeeds, the system prompts for a restart.

Step 7 Click **OK**. You will be logged out and required to log in again after 3~ 5 minutes to complete the authentication mode switch.

----End

2.4 Cluster Deployment

LAS cluster deployment includes deploying secondary nodes and adding secondary nodes on the primary node.

Deploying Secondary Nodes

Since the VM LAS is deployed automatically, you must configure a secondary node through the console. Otherwise, it can only be used as a standalone node or a primary node.

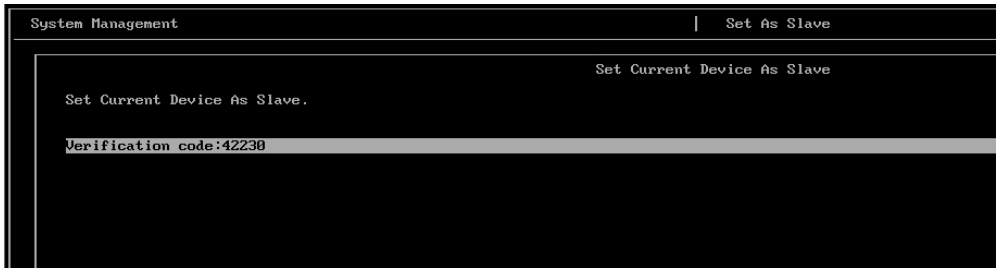
The steps for configuring a secondary node are as follows:

Step 1 Use the conadmin account to enter the console management page, as shown in Figure 2-2.

Figure 2-1 System Management Page

Step 2 Select **Set As Slave** to set the node as a secondary node. The system automatically generates a security code, as shown in Figure 2-2.

Figure 2-2 Set as Secondary Node



----End

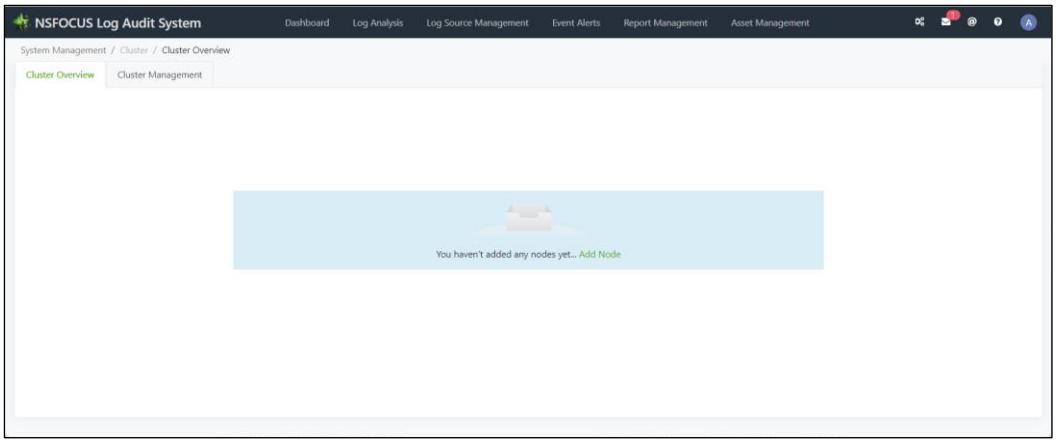
Adding Secondary Nodes

When a node is not set as a secondary node, it is a primary node. The steps for adding a secondary node on the primary node are as follows:

Step 1 Log in to the primary node of LAS.

Step 2 Hover over the icon and choose **Cluster > Cluster Overview**, as shown in Figure 2-3.

Figure 2-3 Primary Node Configuration

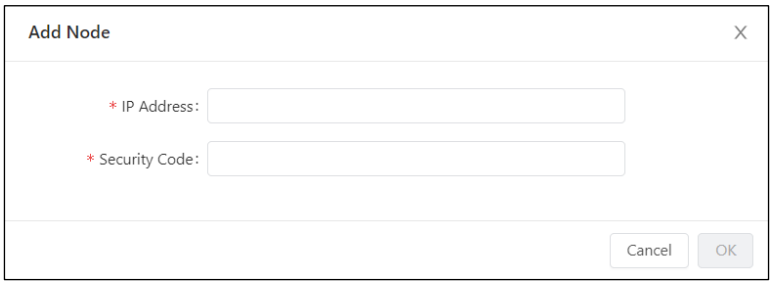


Step 3 Click **Cluster Management** to enter the page shown in Figure 2-4.

Figure 2-4 Cluster Management

Step 4 Click **Add Node** to enter the add node page, as shown in Figure 2-5.

Figure 2-5 Adding Node



Step 5 Configure the secondary node IP and security code. For details, see Deploying Secondary Node.

Note	• All the clustered nodes must be of the same type (either hardware or VM versions). • The major version, that is, the F version, must be consistent among all nodes.

Step 6 After the secondary node is added successfully, the result is shown in Figure 2-6.

Figure 2-6 Node Added Successfully

----End

A Appendix

A.1 Default Parameters

Role	Username	Password
System administrator	admin	admin@123456
Console administrator	conadmin	conadmin@123456

A.2 Supported Browsers

Browser	Version
Firefox	Latest version
Chrome	Latest version