

NSFOCUS Unified Threat Sensor Installation and Deployment Guide



Version: V2.0R001B05 (2023-09-25)

Confidentiality: RESTRICTED

■ Copyright © 2023 NSFOCUS Technologies, Inc. All rights reserved.

Unless otherwise stated, **NSFOCUS Technologies, Inc.** holds the copyright for the content of this document, including but not limited to the layout, figures, photos, methods, and procedures, which are protected under the intellectual property and copyright laws. No part of this publication may be reproduced or quoted, in any form or by any means, without prior written permission of **NSFOCUS Technologies, Inc.**

■ 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	5
1 Server Configuration Requirements	8
2 Preparations Before Installation	10
2.1 Preparing Hardware.....	10
2.2 Preparing Software.....	10
2.3 Preparing Network Environment.....	11
2.3.1 Applying for IP Addresses.....	11
2.3.2 Opening Ports.....	11
2.3.3 Selecting NICs	12
2.4 Preparing Disks	13
2.4.1 System Disk	14
2.4.2 Data Disk	14
3 Installing the Operating System on the Host	15
3.1 Installation Notes	15
3.2 Configuring BIOS Settings	16
3.3 Selecting an Installation Type for the Operating System	16
3.4 Checking KVM Configuration After Installation	17
4 Installing UTS.....	18
4.1 Installation Notes	18
4.2 Preparing Files	18
4.2.1 Deployment Scripts.....	19
4.2.2 Image File	19
4.3 Performing Environment Check.....	19
4.4 Deploying UTS	20
4.4.1 Automated Installation	20
4.4.2 Restarting the Host.....	53
4.4.3 Initial UTS Configuration	54
4.4.4 Creating a Snapshot	58
4.5 UTS Version Upgrade	59
4.5.1 Upgrading the System Engine.....	59
4.5.2 Upgrading the Intrusion Detection Rule Base.....	60
4.5.3 Upgrading the Web Application Rule Base.....	60

4.5.4 Upgrading the NTI Database	61
4.5.5 Upgrading the Virus Signature Database	61
4.5.6 Upgrading the Assessment Rule Base	62
5 Replacing the Image of UTS	63
5.1 Replacement Notes.....	63
5.2 Preparing a New Image File.....	63
5.3 Replacing the Image File.....	64
5.3.1 Backing Up the License	64
5.3.2 Shutting Down UTS.....	64
5.3.3 Creating a New Data Disk	64
5.3.4 Replacing the Image File and Data Disk.....	65
5.3.5 Starting UTS	66
5.3.6 Initial UTS Configuration	66
5.3.7 Creating a Snapshot	66
6 Common Basic Operations.....	67
6.1 Checking Network Interfaces	67
6.2 Checking Transparent Transmission Parameters of the Kernel.....	68
6.3 Binding and Checking Mirroring Transparent Transmission Interfaces.....	69
6.3.1 Viewing NIC Binding Information	69
6.3.2 Binding a Transparent Transmission Interface.....	70
6.3.3 Unbinding a Transparent Transmission Interface.....	71
6.4 Basic Operations of Data Disks.....	71
6.4.1 Creating a Data Disk	71
6.4.2 Viewing Data Disk Information	71
6.5 Basic Operations of Network Bridges.....	71
6.5.1 Creating a Network bridge	71
6.5.2 Binding a Physical NIC for the Network Bridge	71
6.5.3 Activating the Network Bridge	71
6.5.4 Deleting the Network Bridge	71
6.6 Basic Operations of vUTS.....	72
6.6.1 Defining a vUTS	72
6.6.2 undefining a vUTS	72
6.6.3 Shutting Down a vUTS	72
6.6.4 Starting a vUTS.....	72
6.6.5 Viewing Defined vUTSs	72
6.6.6 Autostarting a vUTS at System Startup.....	72
6.6.7 Disabling vUTS Autostart at System Startup	72
6.6.8 Editing vUTS Configuration	72
6.6.9 Creating a vUTS Snapshot	73
6.6.10 Viewing a vUTS Snapshot	73
6.6.11 Restoring from a Snapshot	73

6.7 Opening a VNC Port	73
6.8 Modifying the Memory Size of UTS	73
6.9 Logging In to the UTS Console	74
7 FAQ.....	75
7.1 Deployment Method.....	75
7.2 Requirements for the Host's Operating System.....	75
7.3 Garbled Code Occurs During Deployment Script Execution.....	75
7.4 IP Address Is Inaccessible After Host Restart	76
7.5 vUTS Automatically Shuts Down a Few Minutes After Startup.....	76
7.6 NICs Cannot Be Selected During Deployment.....	77
7.8 An Error Message Appears When Using virsh to Connect to the vUTS Console	78
7.9 vUTS Fails to Start After the Host is Shut down and Relocated	79
7.10 Problems Regarding High-Performance Mode	79
7.10.1 Failed to Bind a Transparent NIC	80
7.10.2 UTS Startup Error Caused by NIC Binding Failure.....	80
7.10.3 NIC Models That Do Not Support High-Performance Mode	80
7.11 No Interface Traffic Is Detected and the CPU's Main Frequency Shows 0 After UTS Startup in Common Mode	80
8 NIC Operations After UTS Deployment.....	82
8.1 NIC Operations in High-Performance Mode	82
8.1.1 Adding an NIC	82
8.1.2 Unbinding an NIC.....	85
8.1.3 Replacing an NIC.....	86
8.2 NIC Operations in Common Mode	87
8.2.1 Adding an NIC	87
8.2.2 Unbinding an NIC.....	88
8.2.3 Replacing an NIC.....	89
9 Uninstalling UTS	90
A Default Parameters	94
A.1 Initial Settings of the Management Interface.....	94
A.2 Default Accounts.....	94
A.3 Communication Parameters of the Console Port.....	94

Preface

This document describes the installation and deployment of NSFOCUS Unified Threat Sensor virtual machine (vUTS).

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





Organization

Chapter	Description
1 Server Configuration Requirements	Describes the configuration requirements for hardware and software of the server (host).
2 Preparations Before Installation	Describes preparations for installing vUTS.
3 Installing the Operating System on the Host	Describes how to install the operating system on a host.
4 Installing UTS	Describes how to install and deploy vUTS.
5 Replacing the Image of UTS	Describes how to replace the image of UTS.
6 Common Basic Operations	Describes common problems and their solutions encountered during vUTS installation and deployment.
7 FAQ	Describes common problems and their solutions encountered during vUTS deployment.
8 NIC Operations After UTS Deployment	Describes how to configure NICs after vUTS deployment.
9 Uninstalling UTS	Describes how to uninstall vUTS (VM).
A Default Parameters	Describes the default settings of vUTS.

Change History

Version	Description
V2.0R00IB05	Initial release.

Conventions

Convention	Description
Bold font	Keywords, names of screen elements like buttons, drop-down lists or fields, and user-entered text appear in bold font.
<i>Italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in italic font.
 Note	Reminds users to take note.
 Tip	Indicates a tip to make your operations easier.
 Caution	Indicates a situation in which you might perform an action that could result in equipment damage or loss of data.
 Warning	Indicates a situation in which you might perform an action that could result in bodily injury.
A > B	Indicates selection of menu options.

Customer 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
- Australia: +61 2 8599 0673 or +61 2 8599 0NSF
- Netherlands: +31 85 208 2673 or +31 85 208 2NSF
- Brazil: +55 13 4042 1673 or +55 13 4042 1NSF
- Japan: +81 3-4510-8673 or +81 3-4510-8NSF
- Singapore: +65 3158 3757
- Hong Kong: +852 5803 2673 or +852 5803 2NSF
- Middle East: +973 1619 7607

Documentation Feedback

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

Email: support@nsfocusglobal.com

1 Server Configuration Requirements

It is recommended that you use a Dell server as the host. Based on performance requirements and application scenarios, UTS supports the following two deployment modes:

- High-performance mode (IOMMU transparent transmission mode)

This mode requires the NIC to support the IOMMU transparent transmission mode. It also demands high CPU and memory performance. A single UTS deployed in high-performance mode can handle up to 10 Gbps traffic throughput.

[Table 1-1](#) describes configuration requirements for software and hardware in high-performance mode.

- Common mode (VIRTIO bridge mode)

This mode requires a regular NIC and has relatively low requirements for CPU and memory performance. A single UTS deployed in common mode can handle up to 2 Gbps traffic throughput.

[Table 1-2](#) describes configuration requirements for software and hardware in common mode.

Table 1-1 Recommended server configurations in high-performance mode

Item		Recommended Configuration	
Hardware	Hardware platform	WCS white labeling server	WCS white labeling server
	CPU	2 x CPU E5-2640V4 2.4 GHZ	2 x CPU E5-2640V4 2.4 GHZ
	Memory	64 GB	128 GB
	Hard disk space	≥ 4 TB	≥ 4 TB
Performance parameters	Throughput	5 Gbps	10 Gbps
Software	Operating system	Centos 7.0 and later, fully installed.	
Hardware	NIC	At least three NICs are required, used for the management interface, collaboration interface, and mirroring interface, respectively. <ul style="list-style-type: none"> • There is no limit on the models of NICs used for management and collaboration interfaces. • The model of the NIC used for the mirroring interface must be one of the following models that support transparent transmission: 	


		<ul style="list-style-type: none"> ✓ igb (Gigabit): 82575, 82576, 82580, I210, I211, and I350 (only Gigabit supported for optical port), as well as I354 and x722 version F02SP02 and later. ✓ ixgbe (10 Gigabit): 82598, 82599, X520, X540, X550, X710, and X722. <p> Note</p> <p>Currently, the x722 NIC is not recommended for the management interface.</p>
--	--	---

Table 1-2 Recommended server configuration in common mode

Item		Recommended Configuration
Hardware	CPU	10-thread CPU that supports virtualization (Intel (R) Xeon (R) CPU E5-2630 v2, 12 cores for example)
	Memory	32 GB
	NIC	At least three NICs are required, used for the management interface, collaboration interface, and mirroring interface, respectively. There is no limit on the models of NICs.
Software	Operating system	Centos 7.0 and later, fully installed.

2 Preparations Before Installation

This chapter contains the following sections:

Section	Description
Preparing Hardware	Describes hardware preparations.
Preparing Software	Describes software preparations.
Preparing Network Environment	Describes network environment preparations.
Preparing Disks	Describes disk preparations.

2.1 Preparing Hardware

Prepare hardware according to hardware configuration requirements described in [Table 1-1](#) or [Table 1-2](#).

2.2 Preparing Software

Installation files must be downloaded from the FTP server of NSFOCUS Engineering Team or obtained from NSFOCUS technical support personnel. Please contact NSFOCUS engineers for the FTP server address. [Table 2-1](#) describes how to obtain files.

Table 2-1 Path to obtain files

File Type	File	Description
UTS image file	Version F05: UTS_IB05_READY_WORL D_x86_0922.qcow2	Use the latest image if there is no special requirements.
Host system image	CentOS-7-x86_64- Everything-1708.iso	You are advised to use recommended operating systems for the host.
Deployment script	20210428UTS_V2.0_AUTO _DEPLOY_PACKGES.tar	The script is updated occasionally. The script file name contains an update date. Please download the latest version.

File Type	File	Description
Deployment guide	NSFOCUS Unified Threat Sensor V2.0R00IB05 Installation and Deployment Guide.pdf	The guide is updated occasionally. The file name contains an update date. Please download the latest version.

2.3 Preparing Network Environment

Prepare the network environment as follows before installation and deployment.

2.3.1 Applying for IP Addresses

You need to apply for two addresses that can be accessed from users, used as a host IP address and a UTS IP address respectively. Both the IP addresses must be in the same network segment.

2.3.2 Opening Ports

Open ports according to the actual requirements.

Table 2-2 Port opening policy

Version	Port	Location of a Port to Be Opened	Description
Version F05	443	UTS side (UTS will automatically open corresponding ports when functions are enabled. Pay attention to whether there is a firewall between UTS and the platform.)	Used for web access.
	22		Used for background access.
	8081		Used for PCAP forensics REST API. A platform can access it through this port.
	8805		Used for one-click blocking REST API. A platform can access it through this port.
	8080		Device management port, designed for platform access.
	10002		A interface service.
	5000–5050	Platform side (Ensure that these ports are opened on the platform and pay attention to whether there is a firewall between UTS and the platform.)	Reserved for collaboration with a platform.
	4399		Used to send status logs to a platform.
	443		Used for UTS access. UTS registers with a platform through this port.
		6069	Host side

2.3.3 Selecting NICs

You need to learn about which NICs support transparent transmission first.

Execute the following command to view NICs that support transparent transmission. The script is stored in the installation and deployment directory. For details, see Performing Environment Check. The result is shown in [Figure 2-1](#).

```
python Check_Nic.py `pwd`
```

Figure 2-1 Selecting NICs

```
[root@localhost home]# python Check_Nic.py `pwd`
Operating system version: CentOS Linux release 7.4.1708 (Core)----Operating system verification [ok]
Kernel version:3.10.0-693.el7.x86_64----Kernel version verification [ok]
NIC that supports IOMMU_Mode1: 02:00.0 Ethernet controller: Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)
NIC that supports IOMMU_Mode2: 02:00.1 Ethernet controller: Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)
NIC that supports IOMMU_Mode3: 03:00.0 Ethernet controller: Intel Corporation I350 Gigabit Network Connection (rev 01)
NIC that supports IOMMU_Mode4: 03:00.1 Ethernet controller: Intel Corporation I350 Gigabit Network Connection (rev 01)
NIC that supports IOMMU_Mode5: 03:00.2 Ethernet controller: Intel Corporation I350 Gigabit Network Connection (rev 01)
NIC that supports IOMMU_Mode6: 03:00.3 Ethernet controller: Intel Corporation I350 Gigabit Network Connection (rev 01)
NIC that supports IOMMU_Mode7: 04:00.0 Ethernet controller: Intel Corporation I350 Gigabit Network Connection (rev 01)
NIC that supports IOMMU_Mode8: 04:00.1 Ethernet controller: Intel Corporation I350 Gigabit Network Connection (rev 01)
NIC that supports IOMMU_Mode9: 81:00.0 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (rev 02)
NIC that supports IOMMU_Mode10: 81:00.1 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (rev 02)
NIC that supports IOMMU_Mode11: 81:00.2 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (rev 02)
NIC that supports IOMMU_Mode12: 81:00.3 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (rev 02)
Number of NICs that support IOMMU_Mode: 12, this vUTS can be deployed in either high-performance mode or common mode.
NIC quantity:12----NIC quantity verification [ok]
Memory available on current host:251G----Memory verification [ok]
Current CPU NUMA node info:
*****NUMA node(s): 2
*****NUMA node0 CPU(s): 0-13,28-41
*****NUMA node1 CPU(s): 14-27,42-55
Current host's CPU model:Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.40GHz----CPU type verification [ok]
CPU core quantity on current host:56----CPU core quantity verification [ok]
```

2.3.3.1 Selecting an NIC for the Management Interface

There is no limit on the model of an NIC used for the management interface. However, an NIC that supports transparent transmission is not recommended because high-performance mode requires the use of an NIC that supports transparent transmission for a mirroring interface. Reserve an NIC supporting transparent transmission for the mirroring interface, which can minimize future rework on UTS with a small number of NICs.



By default, the X722 NIC cannot be used for the management interface. To use it, upgrade the X722 driver i40e to v2.13.10. For information on how to upgrade it, contact NSFOCUS technical support.

For example, to select the NIC with the PCI identifier 0000:04:00.1 for the host's management interface, perform the following steps:

Step 1 Execute the following command to obtain the NIC name. The result is shown in [Figure 2-2](#).

```
ip addr
```

Figure 2-2 `ip addr` command output

```
[root@localhost UTS_V2.0_AUTO_DEPLOY_PACKGES]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
3: ens15f1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master br0 state UP group default qlen 1000
    link/ether 00:24:ec:f1:49:b0 brd ff:ff:ff:ff:ff:ff
```

Step 2 Execute the following command to obtain the PCI identifier of this NIC and check whether it is correct. The result is shown in Figure 2-3.

```
ethtool -i NIC-name
```

Figure 2-3 `ethtool -i` command output

```
[root@localhost UTS_V2.0_AUTO_DEPLOY_PACKGES]# ethtool -i ens15f1
driver: igb
version: 5.6.0-k
firmware-version: 1.63, 0x800009fb
expansion-rom-version:
bus-info: 0000:04:00.1
supports-statistics: yes
supports-test: yes
supports-eeprom-access: yes
supports-register-dump: yes
supports-priv-flags: yes
[root@localhost UTS_V2.0_AUTO_DEPLOY_PACKGES]#
```

----End

2.3.3.2 Selecting an NIC for the Mirroring Interface

Select an NIC for the mirroring interface based on deployment modes:

- High-performance mode
The model of the NIC used for the mirroring interface must be one of the following models that support transparent transmission:
 - igb (Gigabit): 82575, 82576, 82580, I210, I211, and I350 (only Gigabit supported for optical port), as well as I354 and x722 version F02SP02 and later.
 - ixgbe (10 Gigabit): 82598, 82599, X520, X540, X550, X710, and X722.
- Common mode (VIRTIO bridge mode)
There is no limit on the model of the NIC.

2.4 Preparing Disks

This section describes the requirements for system and data disks.

2.4.1 System Disk

You are advised to use an SSD as the system disk to build RAID 1.

Pay attention to the following precautions:

- If there is only one SSD, then use the system disk as RAID 0.
- If there is no SSD, you can use other disks as the system disk (SAS drive for example).
The system disk only supports read and write of a small amount of data. And there is no big difference in processing traffic among different system disks.
- In F04 and later versions, the system disk space is expanded to 16 GB by default. The partition where the system disk is located must meet the space requirements.

2.4.2 Data Disk

Use a mechanical hard drive as the data disk.

- If the traffic storage function is not enabled on UTS, you can use RAID 0, RAID 1, or RAID 5.
- If the traffic storage function is enabled on UTS, you must use RAID 0 and ensure sufficient disk space to build RAID 0.

In full traffic business scenarios, UTS may be required to support full traffic storage that requires high read/write performance and sufficient data disk space.

You can calculate data disk space needed based on the following data:

- The full traffic storage with a throughput of 1 Gbps requires a data disk with a write capability of at least 125 MBps and two disks with a write speed of over 80 MBps to build RAID 0.
- Storing mirrored traffic of 1 Gbps for one day requires a disk space of 10 TB.

3 Installing the Operating System on the Host

This chapter describes how to install the operating system on the UTS host. It contains the following sections:

Section	Description
Installation Notes	Describes notes of installing the operating system on the host.
Configuring BIOS Settings	Describes how to configure BIOS settings.
Selecting an Installation Type for the Operating System	Describes the requirement for the installation type of the operating system.
Checking KVM Configuration After Installation	Describes how to check the KVM configuration after installation.

3.1 Installation Notes

After installing the operating system on the host, use the following command to view the operating system version and check whether BIOS settings meet the requirements described in [Configuring BIOS Settings](#).

```
cat /etc/redhat-release
```



The operating system must be fully installed on the host.

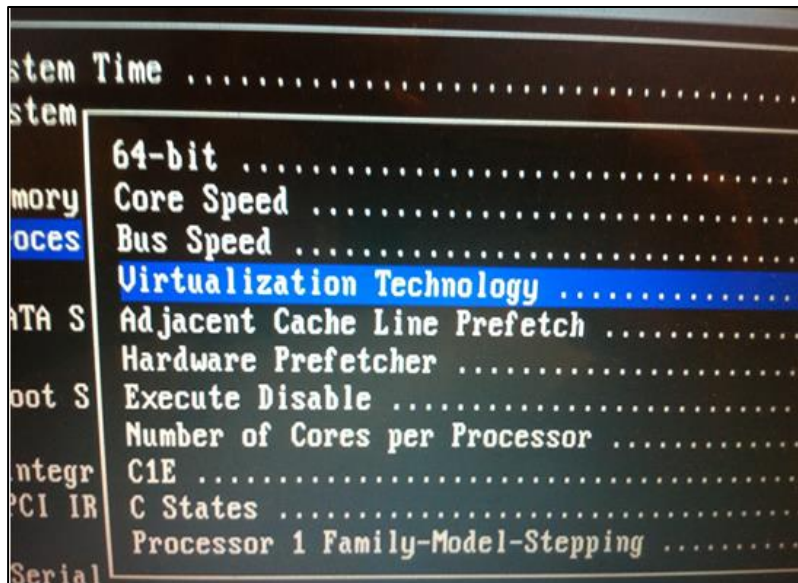
3.2 Configuring BIOS Settings

Start the host and access the BIOS. (For Dell machines, press **F2** to enter the BIOS setup. Note that the key may vary with machine vendors.)

- Enable **Virtualization Technology**. In high-performance mode, enable **Intel Virtualization Technology for Direct I/O** (Intel VT-d).
- On some servers where CPU virtualization is enabled, VT-d is automatically enabled. On other servers (such as Inventec and Portwell), you need to manually enable both virtualization and VT-d.
- BIOS versions may differ across different servers, so options may have varying names. During the setup, check all the BIOS options and set the ones containing words such as **Virtualization** and **Direct I/O** to **enabled**.

For example, in a machine of a certain version, you can configure BIOS settings under **System Setup > Processor Settings > Virtualization Technology**, as shown in [Figure 3-1](#).

Figure 3-1 BIOS setup

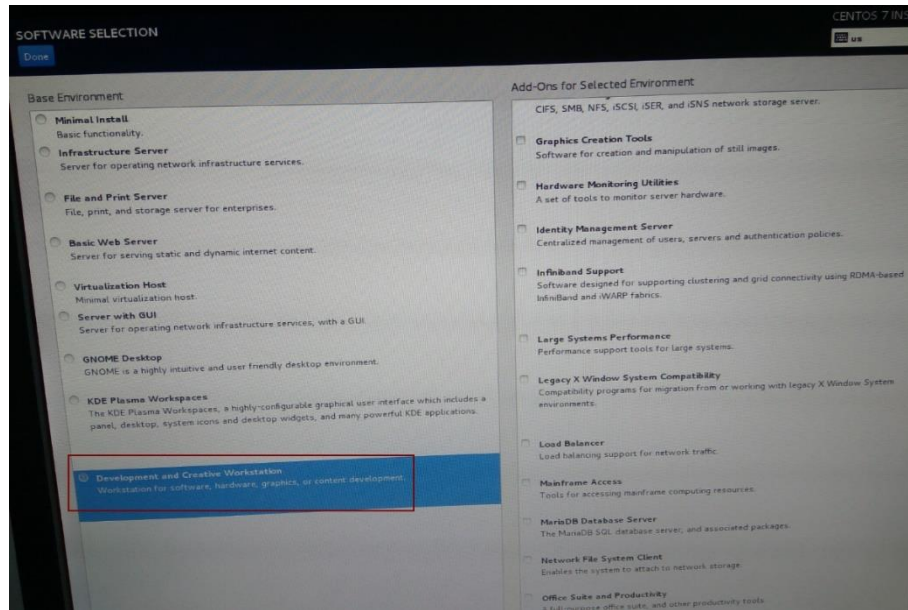


3.3 Selecting an Installation Type for the Operating System

Select an installation type for the operating system, as shown in [Figure 3-2](#).

Note that **Development and Creative Workstation** must be selected because a necessary component required for UTS basic services is included within this workstation option. Selecting improper environments will cause UTS unable to be deployed properly.

Figure 3-2 Selecting an installation type for the host's operating system



3.4 Checking KVM Configuration After Installation

1. Check whether the server supports KVM.

If the output contains **vmx** or **svm**, it indicates that the server supports KVM. Otherwise, the server's CPU does not support virtualization, and KVM cannot be installed.

```
cat /proc/cpuinfo |grep vmx    #intel cpu check command
cat /proc/cpuinfo |grep svm    # amd cpu check command
```

2. Check whether the KVM module of the server is properly loaded.

If the output is similar to the following ones, it indicated that the KVM module is properly loaded.

```
[root@localhost]# lsmod | grep kvm
kvm_intel          162153  12
kvm                525259  1 kvm_intel
```

3. If the KVM module is not properly loaded, you can run the following command to load it again.

```
[root@localhost]# modprobe kvm-intel
```

4 Installing UTS

This chapter describes how to install UTS. This chapter contains the following sections:

Section	Description
Installation Notes	Describes UTS installation notes.
Preparing Files	Describes files required for UTS installation and deployment.
Performing Environment	Describes how to check the UTS host environment.
Deploying UTS	Describes how to perform automated deployment and initial configuration, and create snapshots.
UTS Version Upgrade	Describes how to perform UTS version upgrade.

4.1 Installation Notes

After installing the CentOS operating system on the host, you need to install UTS services using the automated deployment scripts.

The installation and deployment scripts provided on the CD-ROM support automated installation of UTS services. Users only need to select or type them in sequence to complete the installation.

To deploy multiple UTS devices on one host, repeat the steps. Ensure that you use a separate directory for each UTS deployment.

4.2 Preparing Files



Note

Before preparing the files, read [Preparing Software](#) carefully and learn about information about software. The installation package name may vary. Please refer to the actual installation package name.

4.2.1 Deployment Scripts

Decompress the deployment scripts to the **/home** directory (or other directory) that has available space of at least 50 GB. For the file names, see [Preparing Software](#). Decompressed files are as shown in [Figure 4-1](#). Note that files may vary with different versions.

The decompressed deployment scripts are stored in the directory path **/home/UTS_V2.0_AUTO_DEPLOY_PACKGES**. For multiple deployments, make sure to change the directory name accordingly for each deployment.

Figure 4-1 Deployment script decompression

```
Autodeploy.sh
AutoNic_bond.py
bind_cpu.py
Check_Ip.py
Check_Nic.py
depackage.tar
dpdk_nic_bind.py
get_cpu_num.sh
p7zip-16.02-10.sdl7.x86_64.rpm
p7zip-plugins-16.02-10.sdl7.x86_64.rpm
Python-2.7.10.tgz
settings.py
```

4.2.2 Image File

Copy the image file of UTS version F05 to the following path:
/home/UTS_V2.0_AUTO_DEPLOY_PACKGES

4.3 Performing Environment Check

Execute the following command under the directory path where the decompressed deployment scripts are stored (see [Preparing Files](#)) to perform an automatic check on environment conditions of the current host (including the host's operating system version, kernel version, NIC, available memory, and CPU).

```
python Check_Nic.py `pwd`
```

Figure 4-2 Checking the environment

```
[root@localhost home]# python Check_Nic.py `pwd`
Operating system version: CentOS Linux release 7.4.1708 (Core)----Operating system verification [ok]
Kernel version:3.10.0-693.el7.x86_64----Kernel version verification [ok]
NIC that supports IOMMU_Mode1: 02:00.0 Ethernet controller: Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)
NIC that supports IOMMU_Mode2: 02:00.1 Ethernet controller: Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)
NIC that supports IOMMU_Mode3: 03:00.0 Ethernet controller: Intel Corporation I350 Gigabit Network Connection (rev 01)
NIC that supports IOMMU_Mode4: 03:00.1 Ethernet controller: Intel Corporation I350 Gigabit Network Connection (rev 01)
NIC that supports IOMMU_Mode5: 03:00.2 Ethernet controller: Intel Corporation I350 Gigabit Network Connection (rev 01)
NIC that supports IOMMU_Mode6: 03:00.3 Ethernet controller: Intel Corporation I350 Gigabit Network Connection (rev 01)
NIC that supports IOMMU_Mode7: 04:00.0 Ethernet controller: Intel Corporation I350 Gigabit Network Connection (rev 01)
NIC that supports IOMMU_Mode8: 04:00.1 Ethernet controller: Intel Corporation I350 Gigabit Network Connection (rev 01)
NIC that supports IOMMU_Mode9: 81:00.0 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (rev 02)
NIC that supports IOMMU_Mode10: 81:00.1 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (rev 02)
NIC that supports IOMMU_Mode11: 81:00.2 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (rev 02)
NIC that supports IOMMU_Mode12: 81:00.3 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+ (rev 02)
Number of NICs that support IOMMU_Mode: 12, this VUTS can be deployed in either high-performance mode or common mode.
NIC quantity:12----NIC quantity verification [ok]
Memory available on current host:251G----Memory verification [ok]
Current CPU NUMA node info:
*****NUMA node(s): 2
*****NUMA node0 CPU(s): 0-13,28-41
*****NUMA node1 CPU(s): 14-27,42-55
Current host's CPU model:Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.40GHz----CPU type verification [ok]
CPU core quantity on current host:56---CPU core quantity verification [ok]
```

After the check is complete, review the results as follows:

- If a result contains the word “Failure”, it indicates that the system does not meet UTS installation conditions. You need to prepare software and hardware environments according to [Server Configuration Requirements](#).
- If a result has no word “Failure”, you can continue the deployment.
- If a result contains the word "Warning", you can continue the deployment, but it may fail. Whenever possible, prepare software and hardware environments according to [Server Configuration Requirements](#).

4.4 Deploying UTS

Follow all the steps described from section [Automated Installation](#) to section [Creating a Snapshot](#) to complete the deployment.

4.4.1 Automated Installation

Execute the following two commands under the decompression directory described in [Preparing Files](#) to start the deployment.

```
chmod +x Autodeploy.sh
./Autodeploy.sh
```

The following sections describe the steps that require user interaction and the meaning of each option and input during the automated deployment process. If you cancel the installation or an error occurs during the installation causing an automatically exit of installation, re-execute the deployment script **Autodeploy.sh** to initiate the reinstallation.



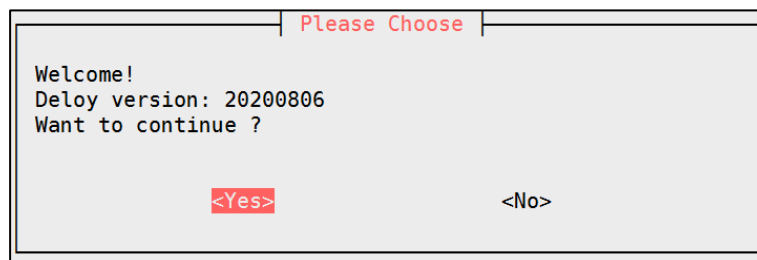
- In the current deployment directory, the **deploy.log** file records a detailed log of the deployment process. You can check the log if there are any issues during the deployment.
- If you cancel the installation or an error occurs during the installation causing an automatic exit of the installation, the system will undo any changes made during the installation process before exiting the installation..

4.4.1.1 Do You Want to Continue

You can press **TAB**, **←**, or **→**, choose **Yes** or **No**, and press **Enter** as required, as shown in [Figure 4-3](#).

- Choose **Yes** to continue automatic installation.
- Choose **No** to exit automatic installation. To perform installation again, re-execute the deployment script **Autodeploy.sh**.

Figure 4-3 Automated deployment: want to continue?

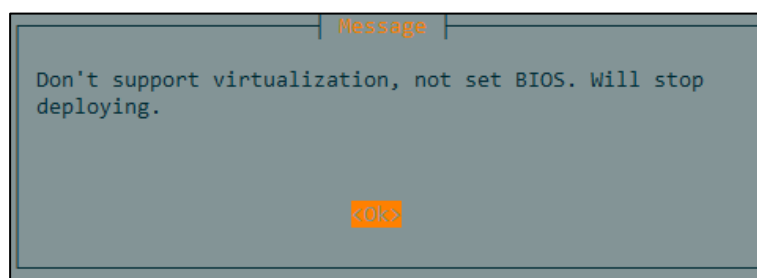


4.4.1.2 Checking Virtualization

To prevent installation failure due to insufficient preparations, the system will automatically check whether the host BIOS supports virtualization.

- If the BIOS supports virtualization, automated installation continues.
- If the BIOS does not support virtualization, a message box appears, as shown in [Figure 4-4](#). Press **Enter** to stop deploying. Re-execute the deployment script **Autodeploy.sh** after setting the BIOS according to [Configuring BIOS Settings](#).

Figure 4-4 Automated deployment: checking for virtualization

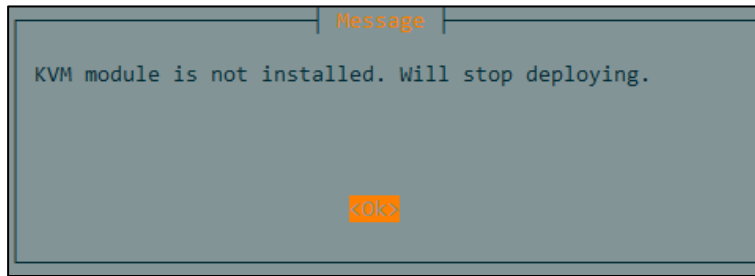


4.4.1.3 Checking KVM Configuration

To prevent installation failure due to insufficient preparations, the system will automatically check whether the KVM module is installed on the host.

- If it is installed, automated installation continues.
- If it is not installed, a message box appears, as shown in [Figure 4-5](#). Press **Enter** to stop deploying. Re-execute the deployment script **Autodeploy.sh** after setting the BIOS according to [Checking KVM Configuration After Installation](#).

Figure 4-5 Automated deployment: checking KVM configuration

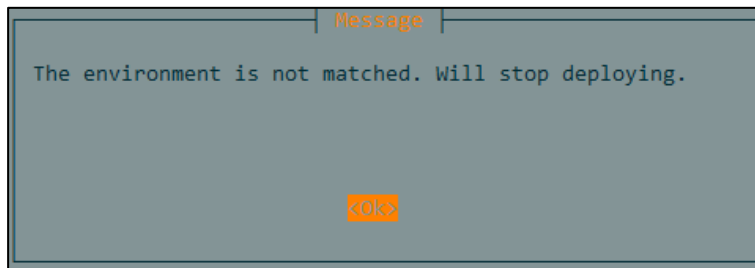


4.4.1.4 Checking the Environment

To prevent installation failure due to insufficient preparations, the system will automatically check the environment. For details, see [Performing Environment Check](#) Performing Environment.

- If the environment meets requirements, automated installation continues.
- If the environment does not meet requirements, a message box appears, as shown in [Figure 4-6](#). Press **Enter** to stop deploying. Prepare the environment again, and re-execute the deployment script **Autodeploy.sh**.

Figure 4-6 Automated deployment: checking the environment



4.4.1.5 Choosing a Deployment Mode

To choose a deployment mode, follow these steps:

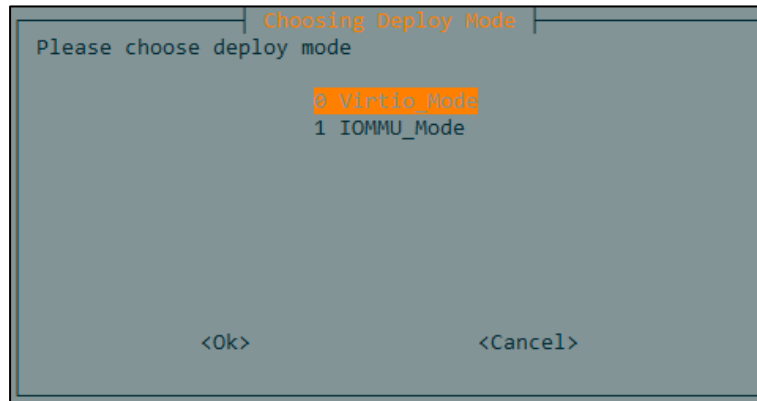
- Step 1** View the deployment modes that the current host can support, as shown in [Figure 4-7](#).

Virtio_Mode indicates common mode, and IOMMU_Mode indicates high-performance mode.



- In the dialog box as shown in [Figure 4-7](#), the options available are determined by NICs. If none of NICs supports IOMMU mode, only Virtio_Mode is available. If there is a NIC that supports IOMMU mode, both Virtio_Mode and IOMMU_Mode are available.
- If you cancel the installation or an error occurs during the installation causing an automatic exit of the installation, the system will undo any changes made during the installation process before exiting the installation.

Figure 4-7 Automated deployment: choosing a deployment mode

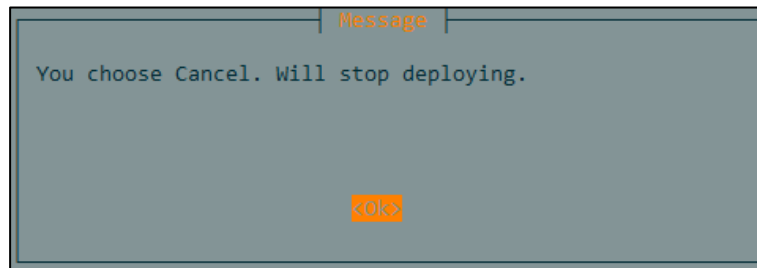


Step 2 Press **↑** or **↓** to choose a deployment mode.

Step 3 Press **TAB**, **←** or **→**, choose **Ok** or **Cancel** as required, and then press **Enter**.

- a. Click **Ok** to continue automated installation.
- b. Click **Cancel** to view a message box, as shown in [Figure 4-8](#). Press **Enter** to stop deploying. To perform installation again, re-execute the deployment script **Autodeploy.sh**.

Figure 4-8 Automated deployment: choosing a deployment mode (stop deploying)



----End

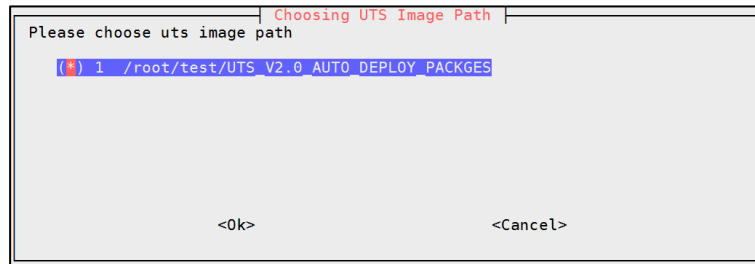
4.4.1.6 Choosing a vUTS Image Path

To choose a vUTS image path, follow these steps:

Step 1 View all available paths on the system, as shown in [Figure 4-9](#).

- a. The dialog box only displays the current deployment path.
- b. The default selection is the current deployment path.
- c. The image file must be placed in the current deployment path.

Figure 4-9 Automated deployment: choosing a vUTS image path



Step 2 Press **TAB** to enter a list.

You can press **TAB** to switch to the list, **Ok**, or **Cancel**.

Step 3 Press **↑** or **↓** and the space bar to choose a path to store the vUTS image file.

Step 4 Press **TAB**, choose **Ok** or **Cancel** as required, and then press **Enter**.

- a. Click **Ok** to continue automated installation.
- b. Click **Cancel** to view a message box, as shown in [Figure 4-8](#). Press **Enter** to stop deploying. To perform installation again, re-execute the deployment script **Autodeploy.sh**.

----End

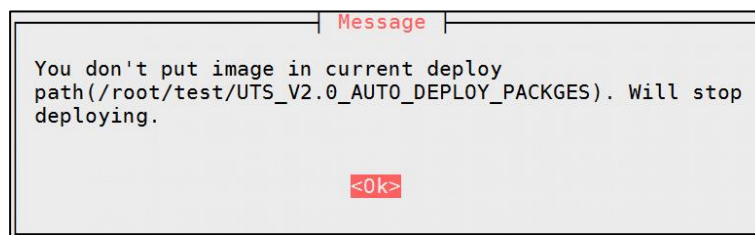
4.4.1.7 Choosing a vUTS Image File

To choose a vUTS image file, follow these steps:

Step 1 Check whether there is a vUTS image file in the current deployment path.

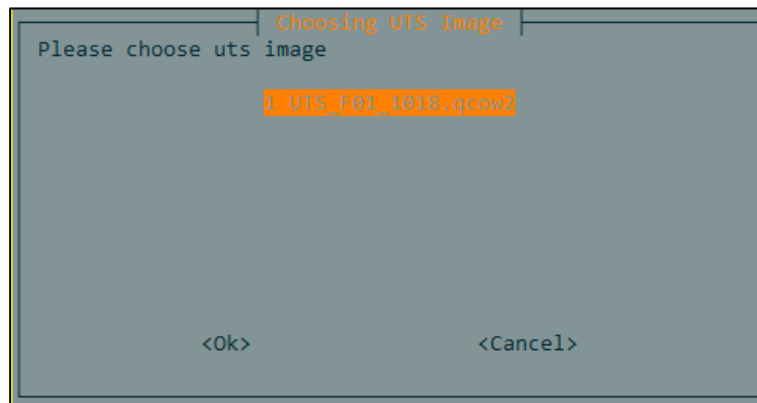
- a. If a message box appears, as shown in [Figure 4-10](#), it indicates that there is no vUTS image file in current deployment path and vUTS cannot be installed and deployed. press **Enter** to stop deploying. Copy the vUTS image file to the current deployment path and then re-execute the deployment script **Autodeploy.sh**.

Figure 4-10 Automated deployment: no vUTS image file in the current deployment path



- b. If a dialog box appears, as shown in [Figure 4-11](#), it indicates that there is a vUTS image file placed in the selected path. All image files with a .qcow2 file extension or compressed file names with a .7z file extension are displayed in the current deployment path.

Figure 4-11 Automated deployment: choosing a vUTS image file



Step 2 Press **↑** or **↓** to choose a vUTS image.

Step 3 Press **TAB**, **←** or **→**, click **Ok** or **Cancel** as required, and then press **Enter**.

- a. Click **Ok** to continue automated installation.
- b. Click **Cancel** to view a message box, as shown in [Figure 4-8](#). Press **Enter** to stop deploying. To perform installation again, re-execute the deployment script **Autodeploy.sh**.

---End

4.4.1.8 Choosing an NIC for the Management Interface of the Host

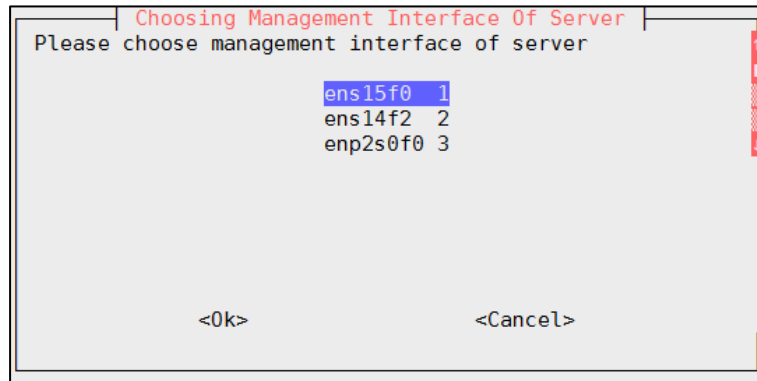
To choose an NIC for the management interface of the host, follow these steps:

Step 1 Display the names of all NICs on a server (that is, host) that can be used for the management interface.

You can choose one for the management interface of the server, as shown in [Figure 4-12](#).

- a. The x722 NIC is not displayed here. (Currently, the x722 NIC cannot be used for the management interface.)
- b. If there are bond NICs, only the master bond NIC is displayed, and slave NICs are not displayed. The bond NIC can be used for the management interface of the server.
- c. If a bond NIC has a VLAN sub-interface, only the VLAN sub-interface is displayed and the bond NICs are not displayed. The VLAN sub-interface can be used for the management interface of the server.

Figure 4-12 Automated deployment: choosing a management interface of the server



Step 2 Press **TAB** to enter a list.

- a. Press **TAB** to switch to the scroll bar, list, **Ok**, or **Cancel**.
- b. If the dialog box cannot display a complete list, switch to the scroll bar on the right side and press **↑** or **↓** to view it.

Step 3 Press **↑** or **↓** to choose an NIC for the management interface.

Step 4 Press **TAB**, choose **Ok** or **Cancel** as required, and then press **Enter**.

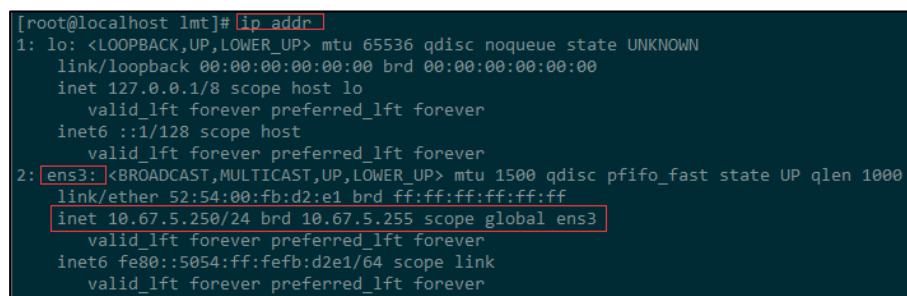
- a. Choose **Ok** to continue automated installation.
- b. Choose **Cancel** to view a message box, as shown in [Figure 4-8](#). Press **Enter** to stop deploying. To perform installation again, re-execute the deployment script **Autodeploy.sh**.

----End

Description for choosing an NIC for the management interface is as follows:

- In general, the NIC that enable access to the host is used for the management interface of UTS. You can choose the corresponding NIC name in the following way:
Run the **ip addr** command and find the name of a physical NIC with a valid IP address that enables access to the host. As shown in [Figure 4-13](#), the physical NIC named **ens3** has a valid IP address that allows access to the host. You can choose this NIC as the virtual bridge NIC.

Figure 4-13 Automated deployment: choosing the management interface of the server (description 1)



- If it is not the initial deployment, or if multiple UTS devices are deployed on one host, you can choose the NIC name already set during the previous deployment. As shown in [Figure 4-14](#), **ens15f1** is bound to the bridge **br0**. You can choose this NIC for the management interface of the server.

The same network bridge can be used when multiple UTSs are deployed.

Figure 4-14 Automated deployment: choosing the management interface of the server (description 2)

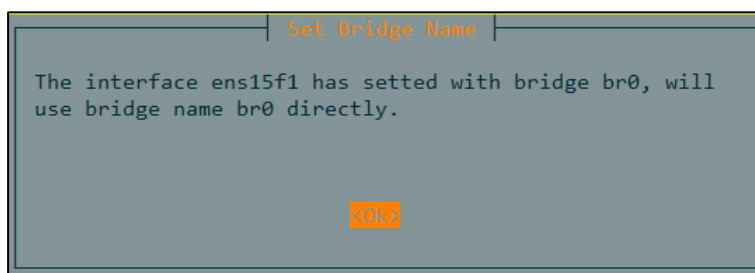
```
[root@localhost UTS_V2.0_AUTO_DEPLOY_PACKGES]# brctl show
bridge name      bridge id        STP enabled     interfaces
br0              8000.0024ecf149b0  no              ens15f1
                vnet0
                vnet1
                vnet2
                vnet3
                vnet4
                vnet5
                vnet6
                vnet7
kkbr0            8000.000000000000  no
virbr0           8000.5254009d1242  yes             virbr0-nic
```

4.4.1.9 Setting a Bridge Name

To set a bridge name, follow these steps:

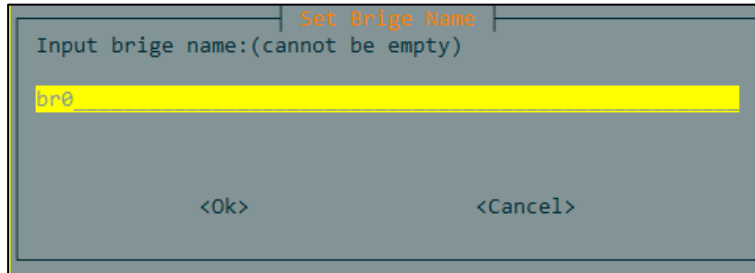
- Step 1** Check whether the selected NIC for the management interface of the host is configured with bridge settings.
- a. If a message box appears, as shown in [Figure 4-15](#), press **Enter** to stop deploying. It indicates that the selected NIC is already configured with the bridge **br0**. You can use the bridge name **br0** directly.

Figure 4-15 Automated deployment: setting a bridge name for the management interface NIC of the server (when the bridge settings are configured)



- b. If a dialog box appears, as shown in [Figure 4-16](#), it indicates that the selected NIC is not configured with bridge settings. You need to set a bridge name here.

Figure 4-16 Automated deployment: setting a bridge name for the management interface NIC of the server (when the bridge settings are not configured)



Step 2 Type the bridge name in the text box.

- a. It is **br0** by default. You can use this name if there are no special requirements.
- b. The bridge name cannot be empty and should not be in use by other interfaces. Otherwise, the dialog box appears and prompts you to type a name that meets the requirements. Choose **Cancel** to cancel the installation.

Step 3 Press **TAB**, **↑**, or **↓**, choose **Ok** or **Cancel** as required, and then press **Enter**.

- a. Choose **Ok**:
 - If the input is empty, a message box appears, as shown in [Figure 4-17](#). Press **Enter** to type a bridge name in the displayed dialog box.
 - If the typed bridge name has been used, a message box appears, as shown in [Figure 4-18](#). Press **Enter** to type a new name in the displayed dialog box.
 - If the typed name is not empty and not in use, automated installation continues.

Figure 4-17 Automated deployment: typing a bridge name when empty



Figure 4-18 Automated deployment: typing a new bridge name when the name has been used



- b. Choose **Cancel**:

A message box is displayed, as shown in [Figure 4-8](#). Press **Enter** to stop deploying. To perform installation again, re-execute the deployment script **Autodeploy.sh**.

----End

Description of the bridge name is as follows:

You can use the **brctl show** command to view the existing bridge names. As shown in [Figure 4-19](#), it indicates that there are already three existing bridges: **br0**, **kkbr0**, and **virbr0**.

Figure 4-19 Automated deployment: checking the existing bridge names

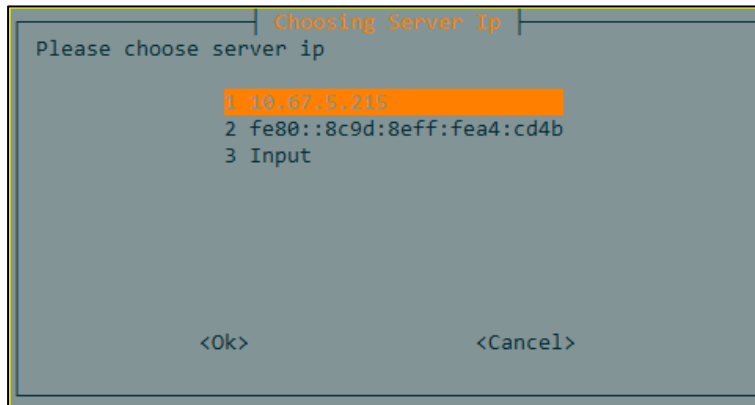
```
[root@localhost UTS_V2.0_AUTO_DEPLOY_PACKAGES]# brctl show
bridge name      bridge id                STP enabled  interfaces
br0              8000.0024ecf149b0       no           ens15f1
                vnet0
                vnet1
                vnet2
                vnet3
                vnet4
                vnet5
                vnet6
                vnet7
kkbr0            8000.000000000000       no
virbr0           8000.5254009d1242       yes          virbr0-nic
```

4.4.1.10 Configuring an IP Address for the Host

To configure an IP address for the host, follow these steps:

- Step 1** As shown in [Figure 4-20](#), option 1 and 2 are the configured IPv4 and IPv6 addresses before the NIC for the management interface of the host is configured. You can choose one of these IP addresses on demand. To configure a new IP address for the host, choose option 3 for manual input.
- By default, the IPv4 address is selected.
 - Choose one of the IP addresses already configured on the host if there are no special requirements. If you want to configure a new IP address for the host, the new address will replace the previous one.
 - Option 3 is not mandatory, only applicable to changing the IP address of the host.

Figure 4-20 Automated deployment: choosing an IP address for the host



Step 2 Press **↑** or **↓** to choose an IP address.

Step 3 Press **TAB**, **←** or **→**, choose **Ok** or **Cancel** as required, and then press **Enter**.

- a. If you choose option 1 or 2 and choose **Ok**, automated installation continues. If you choose option 3, a dialog box of typing a host IP address appears, as shown in [Figure 4-21](#).

After typing an IP address, press **TAB**, **↑**, **↓**, **←**, or **→**, choose **Ok** or **Cancel** as required, and then press **Enter**.

- Choose **Ok**. If the input is empty, a message box appears, as shown in [Figure 4-22](#). Press **Enter** to return to the dialog box of choosing an IP address. If the input is an invalid IPv4 or IPv6 address, a message box appears, as shown in [Figure 4-23](#). Press **Enter** to return to the dialog box of choosing an IP address. If the input is not empty and the IP address is valid, automated installation continues.
- Choose **Cancel** and return to the dialog box of choosing an IP address.

Figure 4-21 Automated deployment: typing a host IP address

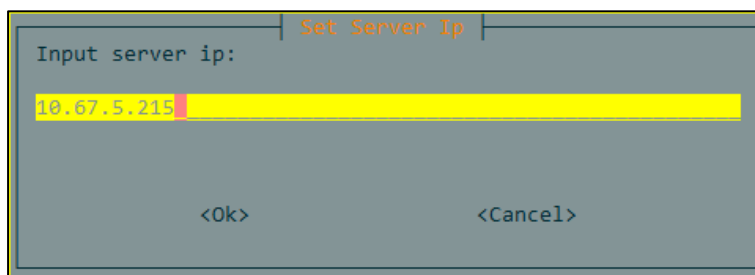


Figure 4-22 Automated deployment: typing a host IP address when empty

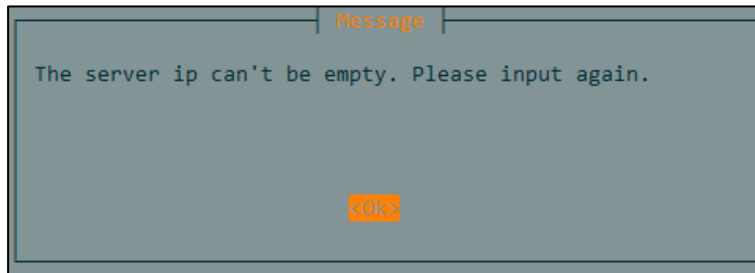


Figure 4-23 Automated deployment: typing a new host IP address when the address is invalid



- b. After you choose **Cancel**, a message box appears, as shown in [Figure 4-8](#). Press **Enter** to stop deploying. To perform installation again, re-execute the deployment script **Autodeploy.sh**.



Note

- An example of a valid IPv4 address is 192.168.2.1.
- An example of a valid IPv6 address is abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd.

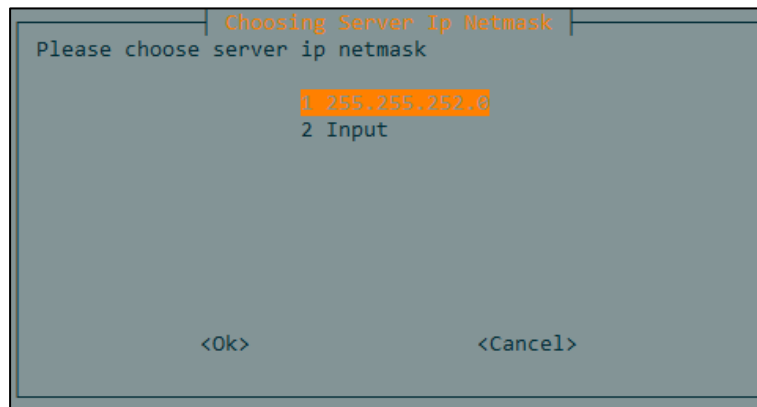
---End

4.4.1.11 Configuring a Subnet Mask for the Host IP Address

To configure a subnet mask for the host IP address, follow these steps:

- Step 1** As shown in [Figure 4-24](#), option 1 is the subnet mask configured for the host IP address. To reconfigure a subnet mask, choose option 2 for manual input.
- a. By default, option 1 is selected.
 - b. If the host IP is not changed, choose the previously used subnet mask (that is, option 1).
 - c. Option 2 is not mandatory, only applicable to changing the subnet mask.

Figure 4-24 Automated deployment: typing the subnet mask of the host IP address



Step 2 Press **↑** or **↓** to choose the subnet mask.

Step 3 Press **TAB**, **←** or **→**, choose **Ok** or **Cancel** as required, and then press **Enter**.

- a. Choose **Ok**. If you choose option 1, automated installation continues. If you choose option 2, a dialog box of typing the subnet mask appears, as shown in [Figure 4-25](#).

After typing the subnet mask, press **TAB**, **↑**, **↓**, **←**, or **→**, choose **Ok** or **Cancel** as required, and then press **Enter**.

- Choose **Ok**. If the input is empty, a message box appears, as shown in [Figure 4-26](#). Press **Enter** to return to the dialog box of choosing the subnet mask. If the input is invalid, a message box appears, as shown in [Figure 4-27](#). Press **Enter** to return to the dialog box of choosing the subnet mask. If the input is not empty and is valid, automated installation continues.
- Choose **Cancel** and return to the dialog box of choosing the subnet mask.

Figure 4-25 Automated deployment: typing a subnet mask

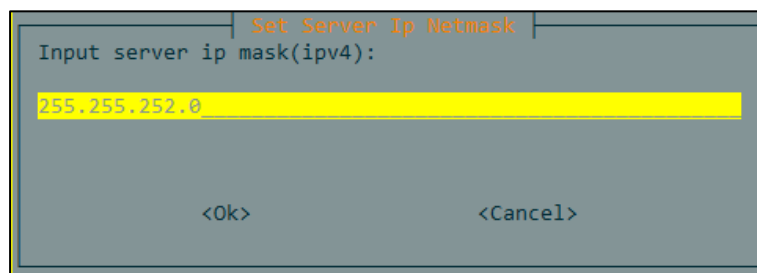


Figure 4-26 Automated deployment: typing a subnet mask when empty

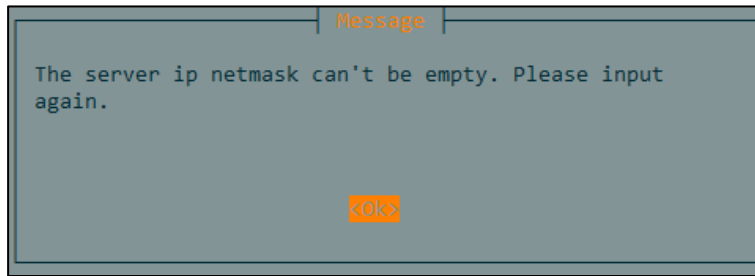
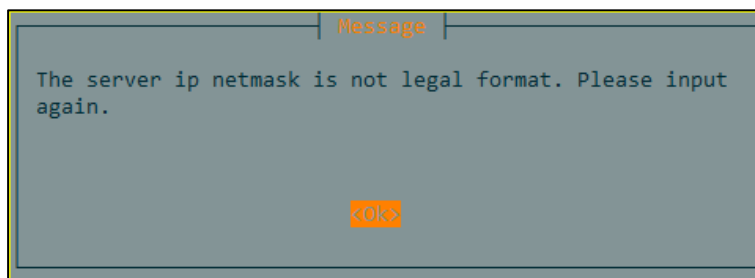



Figure 4-27 Automated deployment: typing a new subnet mask when the input is invalid



- b. After you choose **Cancel**, a message box appears, as shown in [Figure 4-8](#). Press **Enter** to stop deploying. To perform installation again, re-execute the deployment script **Autodeploy.sh**.

 Note	<p>Type a proper subnet mask based on the IP address configured for the host. For example, if the host IP address is an IPv4 address, the subnet mask must be an IPv4 address netmask.</p> <ul style="list-style-type: none"> • An example of a valid IPv4 address netmask is 255.255.255.0. • An example of a valid IPv6 address prefix length is 64.
--	--

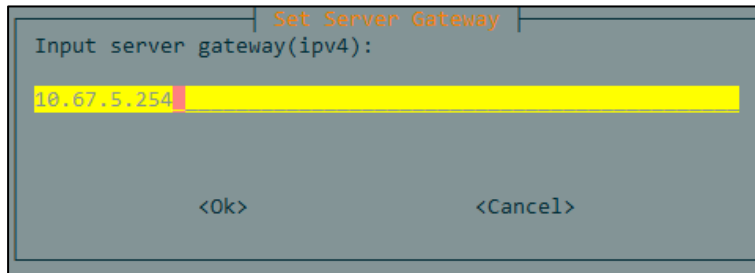
---End

4.4.1.12 Configuring a Gateway for the Host

To specify a gateway, follow these steps:

- Step 1** As shown in [Figure 4-28](#), choose a gateway for the host.
 - a. By default, the gateway corresponding to the host IP address is selected. The text box displays the default existing gateway address of the host.
 - b. If the previous IP address is used as the host IP address, you can use the default gateway address.

Figure 4-28 Automated deployment: typing the gateway address



Step 2 Press **TAB**, **←** or **→**, choose **Ok** or **Cancel** as required, and then press **Enter**.

a. Choose **Ok**:

- If the input is empty, a message box appears, as shown in [Figure 4-29](#). Press **Enter** to type the gateway again in the displayed dialog box.
- If the gateway is invalid, a message box appears, as shown in [Figure 4-30](#). Press **Enter** to type a new gateway address in the displayed dialog box.
- If the input is not empty and the gateway is valid, automated installation continues.

b. Choose **Cancel**:

A message box appears, as shown in [Figure 4-8](#). Press **Enter** to stop deploying. To perform installation again, re-execute the deployment script **Autodeploy.sh**.

Figure 4-29 Automated deployment: typing the gateway address (when empty)

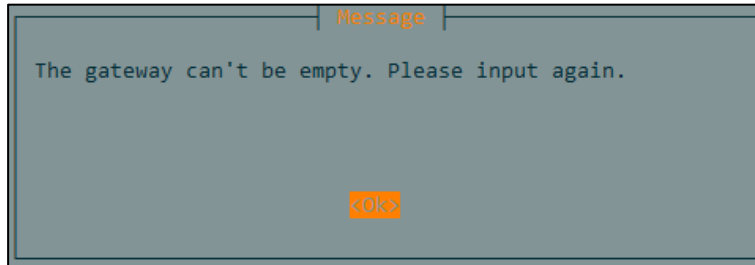
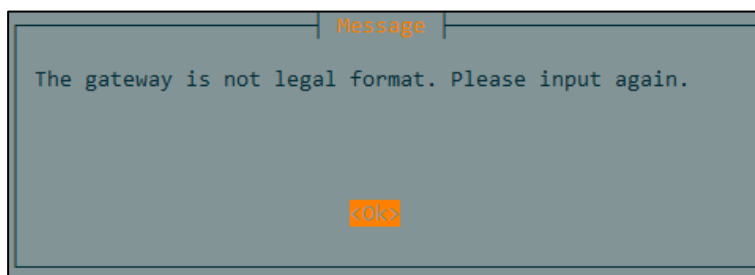


Figure 4-30 Automated deployment: typing a new gateway address (when the input is invalid)



**Note**

Type a corresponding gateway based on the host IP. For example, if the host IP address is an IPv4 address, the gateway address must be an IPv4 address.

- An example of a valid IPv4 address is 192.168.2.1.
- An example of a valid IPv6 address is abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd.

---End

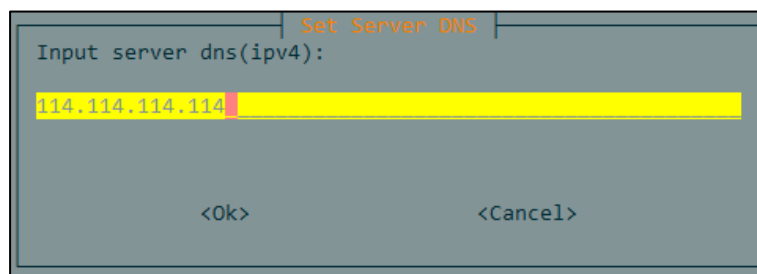
4.4.1.13 Configuring the IP Address of the DNS Server

To configure the IP address of the DNS server, follow these steps:

Step 1 As shown in [Figure 4-31](#), type the DNS server's IP address.

By default, it is **114.114.114.114**.

Figure 4-31 Automated deployment: typing the DNS server's IP address



Step 2 Press **TAB**, **←** or **→**, choose **Ok** or **Cancel** as required, and then press **Enter**.

a. Choose **Ok**:

- If the input is empty, a message box appears, as shown in [Figure 4-32](#). Press **Enter** to type DNS server's IP address again in the displayed dialog box.
- If the IP address is invalid, a message box appears, as shown in [Figure 4-33](#). Press **Enter** to type DNS server's IP address again in the displayed dialog box.
- If the input is not empty and the IP address is valid, automated installation continues.

b. Choose **Cancel**:

A message box appears, as shown in [Figure 4-8](#). Press **Enter** to stop deploying. To perform installation again, re-execute the deployment script **Autodeploy.sh**.

Figure 4-32 Automated deployment: typing the DNS server's IP address when empty

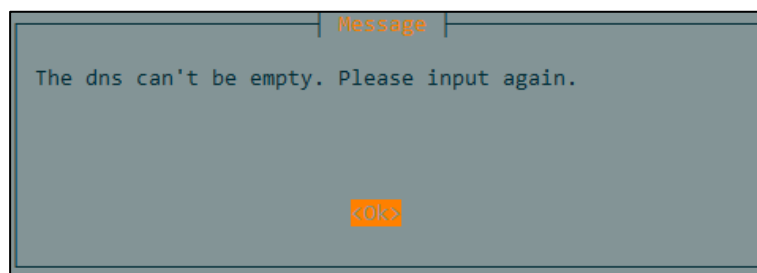
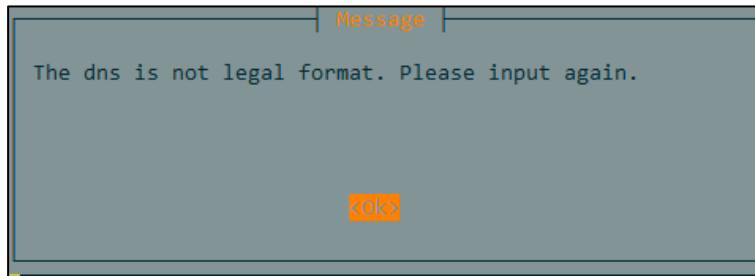


Figure 4-33 Automated deployment: typing DNS server's IP address when the address is invalid


Note

Type the DNS server's IP address corresponding to the host IP address. For example, if the host IP address is an IPv4 address, the DNS server's IP address must be an IPv4 address.

- An example of a valid IPv4 address is 192.168.2.1.
- An example of a valid IPv6 address is abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd.

---End

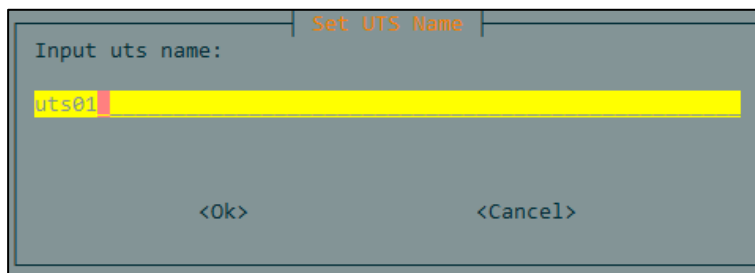
4.4.1.14 Setting a Name for vUTS

To set a name for vUTS, follow these steps:

Step 1 As shown in [Figure 4-34](#), type a vUTS name.

- a. By default, it is **uts01**. If this is the initial deployment of the first UTS device, you can use the default vUTS name.
- b. The vUTS name must be unique and cannot be **UTS** or left empty.

Figure 4-34 Automated deployment: typing the vUTS name



Step 2 Press **TAB**, **←** or **→**, choose **Ok** or **Cancel** as required, and then press **Enter**.

- a. Choose **Ok**:
 - If the input is empty, a message box appears, as shown in [Figure 4-35](#). Press **Enter** to type the name again in the displayed dialog box..
 - If the name is **UTS** or has been used, a message box appears, as shown in [Figure 4-36](#). Press **Enter** to type the name again in the displayed dialog box.
 - If the input is not empty and the name has not been used, automated installation continues.

b. Click **Cancel**:

A message box appears, as shown in [Figure 4-8](#). Press **Enter** to stop deploying. To perform installation again, re-execute the deployment script **Autodeploy.sh**.

Figure 4-35 Automated deployment: typing the vUTS name when empty



Figure 4-36 Automated deployment: typing the vUTS name when the name is invalid



---End

Description for typing the vUTS name is as follows:

You can use the **virsh list --all** command to view the names that have been used. As shown in [Figure 4-37](#), the names of deployed vUTSs cannot be reused for the new vUTS.

Figure 4-37 Automated deployment: viewing the names that have been used

```
[root@localhost UTS_V2.0_AUTO_DEPLOY_PACKGES]# virsh list --all
Id      Name                                     State
-----
30      centos7-yezhi                           running
34      centos7.3-yezhi                         running
89      danyang_62                              running
104     uts91                                    running
115     liuxijiao_UTSV2.0R00F01                 running
-       ckf_self                                 shut off
-       console7.3_4                            shut off
-       encready                                 shut off
-       GUANLI                                  shut off
-       kksp1                                    shut off
-       kkwa                                     shut off
-       kkyezhi                                 shut off
-       restapi_django                          shut off
-       ubuntu                                  shut off
-       uts-wa-taishi                           shut off
-       uts2.0-biaopin                          shut off
-       uts2.0-F01                              shut off
-       uts_8g                                  shut off
-       uts_xiaogao_F01_99                     shut off
-       yezhi_noatf                             shut off
```

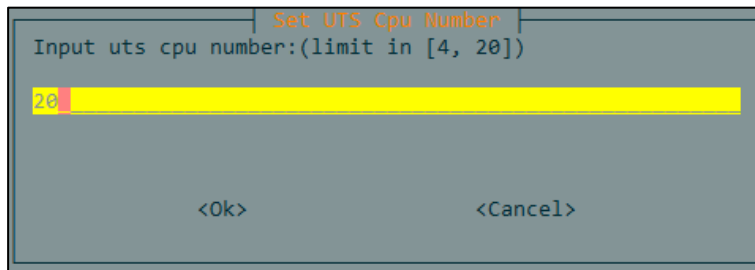
4.4.1.15 Configuring the Number of CPUs of vUTS

To configure the number of CPUs of vUTS, follow these steps:

Step 1 As shown in [Figure 4-38](#), configure the number of CPUs of vUTS.

- a. By default, it is **20** (in the standard configuration). If the number of CPU cores on a single node on the host is less than 20, the actual CPU number will be used as the default.
- b. The standard configuration is recommended whenever possible.
- c. The maximum and minimum values shown in the dialog box specify the range of CPU cores that can be automatically generated for a single node. The maximum value is 20 and the minimum value is 4.
- d. To ensure the vUTS performance, it is recommended that the number of deployed vUTSs on a host should not exceed the number of nodes. If only one UTS is installed on the host, type the maximum number of CPU cores allowed on a single node.

Figure 4-38 Automated deployment: typing the number of CPUs of vUTS



Step 2 Press **TAB**, **←** or **→**, choose **Ok** or **Cancel** as required, and then press **Enter**.

- a. Choose **Ok**:

- If the input is empty or not an integer, a message box appears, as shown in [Figure 4-39](#). Press **Enter** to view the dialog box to type the number again.
 - If the number is not in the range specified in the dialog box, a message box appears, as shown in [Figure 4-40](#). Press **Enter** to view the dialog box to type the number again.
 - If the number is an integer within the range, automated installation continues.
- b. Choose **Cancel**:
- A message box appears, as shown in [Figure 4-8](#). Press **Enter** to stop deploying. To perform installation again, re-execute the deployment script **Autodeploy.sh**.

Figure 4-39 Automated deployment: typing the number of CPUs again if it is empty or not an integer

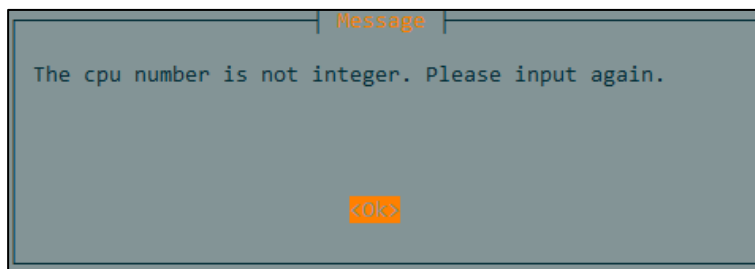


Figure 4-40 Automated deployment: typing the number again if it is outside the valid range



---End

Description for typing the number of CPUs for a vUTS is as follows:

You can use the **lscpu | grep NUMA** command to view the number of CPU cores on each node of the server. If only one vUTS is installed on the server, type the maximum number of CPU cores allowed on a single node.

For example, as shown in [Figure 4-41](#), it is a 2U server, with a maximum of 20 CPU cores for both node0 and node1. You can type 20 CPUs for a vUTS and deploy up to 2 vUTSs on this server, with one vUTS assigned to each node. To ensure the vUTS performance, it is recommended that the number of deployed vUTS on a server should not exceed that of nodes. For example, up to 2 vUTSs can be deployed on a 2U server.

Figure 4-41 Automated deployment: viewing the number of CPU cores on each node

```
[root@localhost UTS_V2.0_AUTO_DEPLOY_PACKGES]# lscpu | grep NUMA
NUMA node(s):                2
NUMA node0 CPU(s):           0-9,20-29
NUMA node1 CPU(s):           10-19,30-39
```

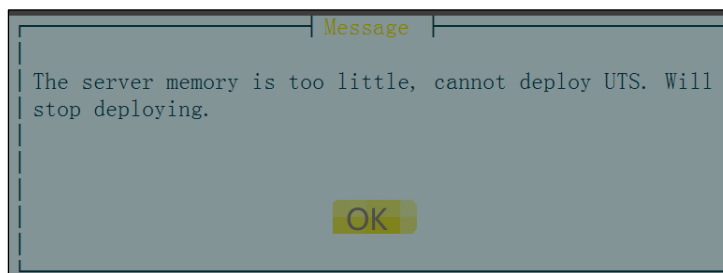
4.4.1.16 Configuring the Memory Size of vUTS

To configure the memory size of vUTS, follow these steps:

Step 1 Configure the memory size of vUTS.

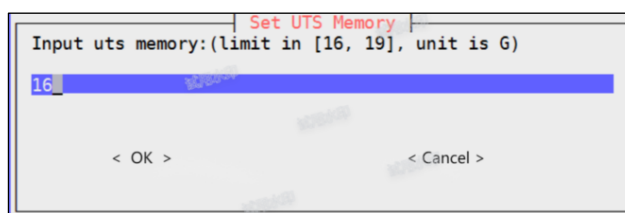
- a. If a message box appears, as shown in [Figure 4-42](#), press **Enter** to stop deploying. It indicates that the free memory size is less than 16 GB after you reserve 2 GB for the host, thus making UTS unable to be deployed. You need to expand the memory or disable unnecessary services on the host to ensure that the free memory reserved for the system is greater than 16 GB. Then re-execute the deployment script **Autodeploy.sh**.

Figure 4-42 Automated deployment: error message related to memory size



- b. If a dialog box appears, as shown in [Figure 4-43](#), it indicates that the free memory is enough to deploy vUTS after you reserve 2 GB of memory for the host.
 - By default, the memory size of a vUTS is **62** (GB, in the standard configuration). If the remaining free memory of the host is less than 62 GB after a 2 GB memory is reserved, the memory size of a vUTS is the free memory size minus 2 GB.
 - The standard configuration is recommended whenever possible.
 - If the free memory size is less than 16 GB after 2 GB is reserved for the host, the system exits deployment.
 - The maximum value shown in the dialog box refers to the maximum free memory size automatically generated minus 2 GB. If the actual free memory size exceeds 128 GB, the maximum value is 128 GB and the minimum value is 16 GB.

Figure 4-43 Automated deployment: typing the memory size of a vUTS



Step 2 Press **TAB**, ← or →, choose **Ok** or **Cancel** as required, and then press **Enter**.

a. Choose **Ok**:

- If the value is empty or not an integer, a message box appears, as shown in [Figure 4-44](#). Press **Enter** to view the dialog box to type a value again.
- If the value is not in the range specified in the dialog box, a message box appears, as shown in [Figure 4-45](#). Press **Enter** to view the dialog box to type a value again.
- If the value is an integer within the range, automated installation continues.

b. Choose **Cancel**:

A message box appears, as shown in [Figure 4-8](#). Press **Enter** to stop deploying. To perform installation again, re-execute the deployment script **Autodeploy.sh**.

Figure 4-44 Automated deployment: typing the memory size again when it is empty or not an integer

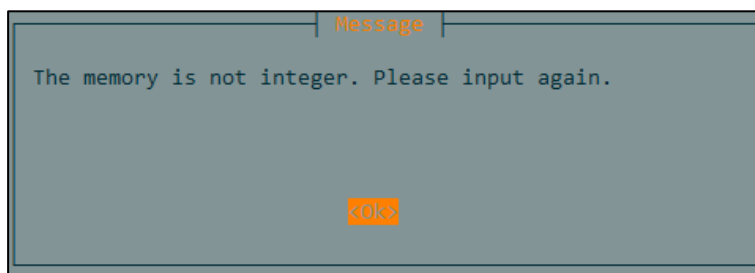
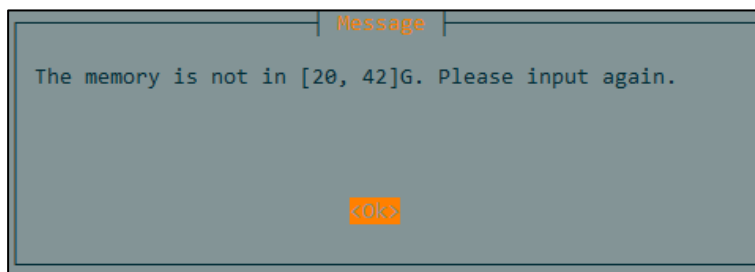


Figure 4-45 Automated deployment: typing the memory size again when it is not in the valid range



---End

Description for typing the memory size of a vUTS is as follows:

Run the **free -h** command. The maximum memory size is automatically calculated. The value in the **used** column subtracted from the value in the **total** column is the value of free memory size. For example, as shown in [Figure 4-46](#), the calculation of free memory size is as follows: 125 GB – 42 GB = 83 GB. The maximum memory size to be typed is the free memory size minus 2 GB (reserved for the system). That is, 83 GB – 2 GB = 81 GB. Thus, the maximum memory size is 81 GB.

Figure 4-46 Automated deployment: free memory of a vUTS

```
[root@localhost ~]# free -h
```

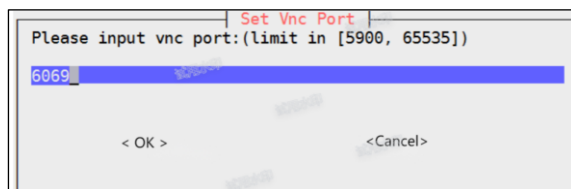
	total	used	free	shared	buff/cache	available
Mem:	125G	42G	42G	19M	40G	82G
Swap:	19G	0B	19G			

4.4.1.17 Configuring a VNC Port for vUTS

To configure a VNC port number for vUTS, follow these steps:

- Step 1** As shown in [Figure 4-47](#), type a VNC port number used for connection to the vUTS.
- By default, it is **6069**.
 - The range is 5900–65535.
 - The VNC port number must be an integer within the valid range and should not be in use.

Figure 4-47 Automated deployment: typing a VNC port number



- Step 2** Press **TAB**, **←** or **→**, choose **Ok** or **Cancel** as required, and then press **Enter**.
- Choose **Ok**:
 - If the number is empty or not an integer, a message box appears, as shown in [Figure 4-48](#). Press **Enter** to type the number again.
 - If the number is not in the range specified in the dialog box, a message box appears, as shown in [Figure 4-49](#). Press **Enter** to type the number again.
 - If the number is already in use, a message box appears, as shown in [Figure 4-50](#). Press **Enter** to type the number again.
 - If the number is an integer within the range and not in use, automated installation continues.
 - Choose **Cancel**:

A message box appears, as shown in [Figure 4-8](#). Press **Enter** to stop deploying. To perform installation again, re-execute the deployment script **Autodeploy.sh**.

Figure 4-48 Automated deployment: typing a new VNC port number when the number is empty or not an integer

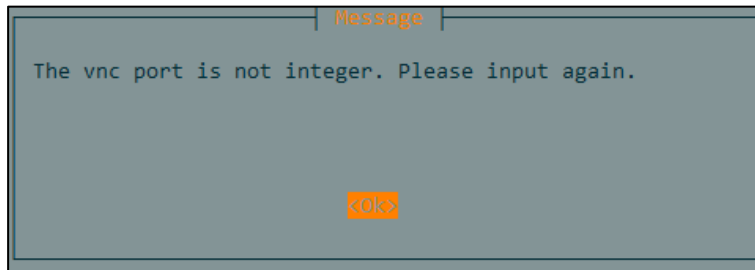


Figure 4-49 Automated deployment: typing a new VNC port number when the number is not in the range

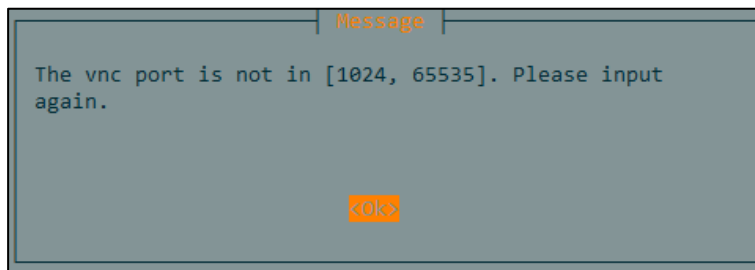


Figure 4-50 Automated deployment: typing a new VNC port number when the number is in use



---End

Description for typing a VNC port number is as follows:

Run the `netstat -anp | grep tcp | grep LISTEN` command to view the ports that have been used, as shown in [Figure 4-51](#). The port numbers after the colons in the fourth column have been used.

Figure 4-51 Automated deployment: viewing the ports that have been used

```
[root@localhost UTS_V2.0_AUTO_DEPLOY_PACKGES]# netstat -anp | grep tcp | grep LISTEN
tcp        0      0 127.0.0.1:25          0.0.0.0:*           LISTEN    2602/master
tcp        0      0 0.0.0.0:6077         0.0.0.0:*           LISTEN    487/qemu-kvm
tcp        0      0 0.0.0.0:20514        0.0.0.0:*           LISTEN    4807/rsyslogd
tcp        0      0 0.0.0.0:6668         0.0.0.0:*           LISTEN    5578/qemu-kvm
tcp        0      0 0.0.0.0:6060         0.0.0.0:*           LISTEN    34773/qemu-kvm
tcp        0      0 0.0.0.0:111          0.0.0.0:*           LISTEN    1/systemd
tcp        0      0 192.168.122.1:53     0.0.0.0:*           LISTEN    3696/dnsmasq
tcp        0      0 0.0.0.0:22           0.0.0.0:*           LISTEN    39826/sshd
tcp        0      0 127.0.0.1:631        0.0.0.0:*           LISTEN    2190/cupsd
tcp6       0      0 :::25                :::*                 LISTEN    2602/master
tcp6       0      0 :::20514              :::*                 LISTEN    4807/rsyslogd
tcp6       0      0 :::3306                :::*                 LISTEN    27147/mysqld
tcp6       0      0 :::111                 :::*                 LISTEN    1/systemd
tcp6       0      0 :::22                  :::*                 LISTEN    39826/sshd
tcp6       0      0 :::1:631               :::*                 LISTEN    2190/cupsd
```

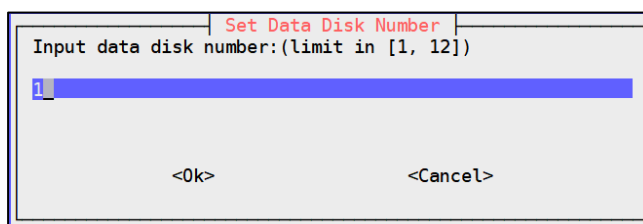
4.4.1.18 Configuring the Number of Data Disks

To configure the number of data disks, follow these steps:

Step 1 As shown in [Figure 4-52](#), configure the number of data disks as required.

- a. The range is 1-12, with **1** as the default.
- b. Specify the number of disks based on the number of logical disks generated after configuring physical disks in a RAID array. For example, the number is 8 if eight physical disks are combined into a single disk RAID 0 that creates eight logical disks mounted on eight data partitions.
- c. The total capacity of physical disks or logical disks configured with RAID that is allocated to vUTS should not exceed 16 TB.
- d. Note that even if the total capacity of logical disks exceeds 20 TB, up to 16 TB data disk should be allocated to vUTS.

Figure 4-52 Automated deployment: typing the number of data disks



Step 2 Press **TAB**, **←** or **→**, choose **Ok** or **Cancel** as required, and then press **Enter**.

- a. Choose **Ok**:
 - If the number is empty or not an integer, a message box appears, as shown in [Figure 4-53](#). Press **Enter** to type the number again.
 - If the number is not in the range specified in the dialog box, a message box appears, as shown in [Figure 4-54](#). Press **Enter** to type the number again.
 - If the value is an integer within the range, automated installation continues.
- b. Choose **Cancel**:

A message box appears, as shown in [Figure 4-8](#). Press **Enter** to stop deploying. To perform installation again, re-execute the deployment script **Autodeploy.sh**.

Figure 4-53 Automated deployment: typing the number of data disks again when the number is empty or not an integer

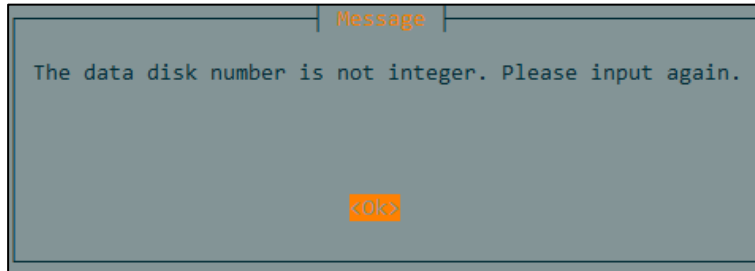
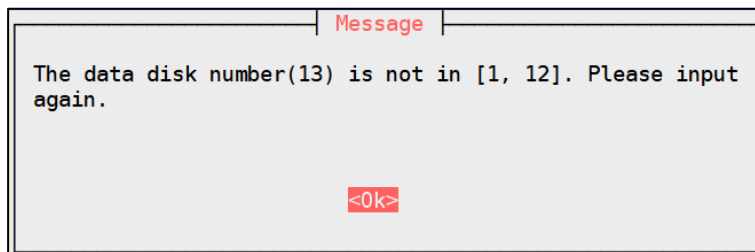


Figure 4-54 Automated deployment: typing the number of data disks again when the number is not in the range



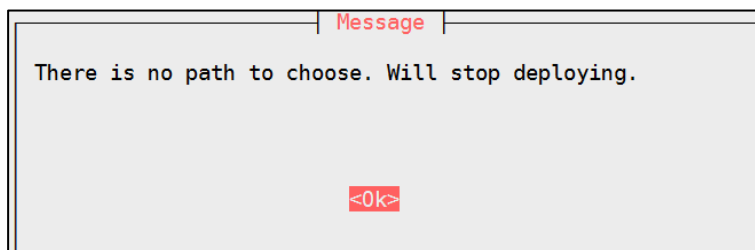
---End

4.4.1.19 Choosing a Path to Store Data Disks

To choose the storage path of data disks, follow these steps:

- Step 1** Check all available paths for storing data disks on the host.
- If a message box appears, as shown in [Figure 4-55](#), press **Enter** to stop deploying. It indicates no paths available for storing data disks (excluding the system path) on the host, and UTS cannot be installed and deployed. Configure a physical disk into a RAID array or directly mount the physical disk to the system, and then re-execute the deployment script **Autodeploy.sh**.

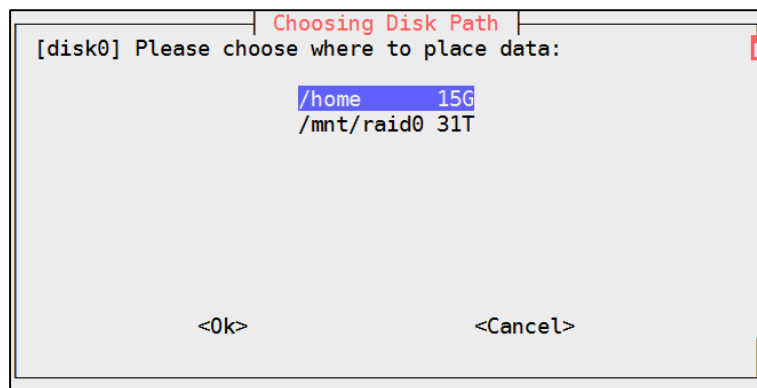
Figure 4-55 Automated deployment: no path to store data disks



- If a dialog box appears, as shown in [Figure 4-56](#), it indicated that there is a path available for storing data disks on the host.

- The dialog box only displays the storage directories and does not display system paths (including `/devtmpfs`, `tmpfs`, and `/dev/mapper/centos-root`, `/boot`, `/var`, `/tmp`, and `/`).
- Do not use the excluded path names mentioned above when mounting physical disks, regardless of whether those disks are set up as RAID or not.
- When typing more than one disks (see [Configuring the Number of Data Disks](#)) and configuring these disks, you should configure the path and size for each disk.
- The dialog box displays the total space size of a path instead of the space size that can be allocated to vUTS. When typing the space size of data disks, you will know that value.

Figure 4-56 Automated deployment: path to store data disks



Step 2 Press **TAB** to enter a list.

- Press **TAB** to switch to the scroll bar, list, **Ok**, or **Cancel**.
- If the dialog box cannot display a complete list, switch to the scroll bar on the right side and press **↑** or **↓** to view it.

Step 3 Press **↑** or **↓** to choose a path to store data disks.

Choose a path with a larger space size.

Step 4 Press **TAB**, choose **Ok** or **Cancel** as required, and then press **Enter**.

- Choose **Ok** to continue automated installation.
- Choose **Cancel**. A message box appears, as shown in [Figure 4-8](#). Press **Enter** to stop deploying. To perform installation again, re-execute the deployment script `Autodeploy.sh`.

----End

4.4.1.20 Configuring the Space Size of a Data Disk

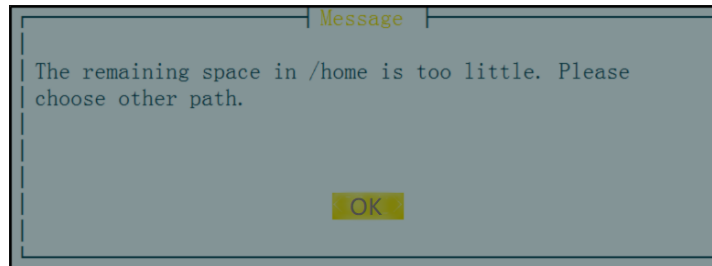
To configure the space size of a data disk, follow these steps:

Step 1 Configure the space size of a disk to be created.

- If a message box appears as shown in [Figure 4-57](#), it indicates that the remaining space of the selected path is too small to configure a disk. Press **Enter** to return to the dialog box described in [Choosing a Path to Store Data Disks](#) to choose a path again.

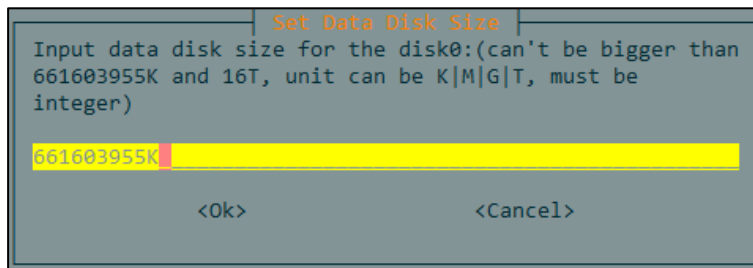
The space size of the selected path that can be allocated to vUTS is calculated as follows:
 Allocated capacity = Available capacity – virtual disk capacity under this path – 100 GB capacity reserved for the system.

Figure 4-57 Automated deployment: the selected path has too small remaining space to configure a disk



- b. If a dialog box appears as shown in [Figure 4-58](#), it indicates that the selected path can be used to configure a disk. Type the space size of a disk to be created.
- The default value is the available space size described in Choosing a Path to Store Data Disks minus 100 GB (that is, 100 x 1024 x 1024 KB). However, if the value is greater than 16 TB, the default value is set to 17179869184K (that is, 16 TB).
 - Unit must be included and should be one of the following: KB, MB, GB, or TB.
 - The input can be neither 0 nor greater than 16 TB, and cannot exceed the available size of the selected partition minus 100 GB (that is, the value displayed in the dialog box).

Figure 4-58 Automated deployment: typing the space size of a disk to be created



Step 2 Press **TAB**, **←** or **→**, choose **Ok** or **Cancel** as required, and then press **Enter**.

- a. Choose **Ok**:
- If the input is empty or not in a correct format, a message box appears, as shown in [Figure 4-59](#). Press **Enter** to return to the dialog box to choose a disk path again. (For details, see Choosing a Path to Store Data Disks.)
 - If the input is greater than 16 TB or the limit displayed in the dialog box, a message box appears, as shown in [Figure 4-60](#). Press **Enter** to view the dialog box to choose a disk path again. (For details, see Choosing a Path to Store Data Disks.)
 - If the input is 0, a message box appears, as shown in [Figure 4-61](#). Press **Enter** to view the dialog box to choose a disk path again. (For details, see Choosing a Path to Store Data Disks.)

- If the input is within the limit, not greater than 16 TB, and in a correct format, automated installation continues.
- b. Choose **Cancel**. A message box appears, as shown in [Figure 4-8](#). Press **Enter** to stop deploying. To perform installation again, re-execute the deployment script **Autodeploy.sh**.

Figure 4-59 Automated deployment: typing the space size of data disks when the number is empty or not in a correct format

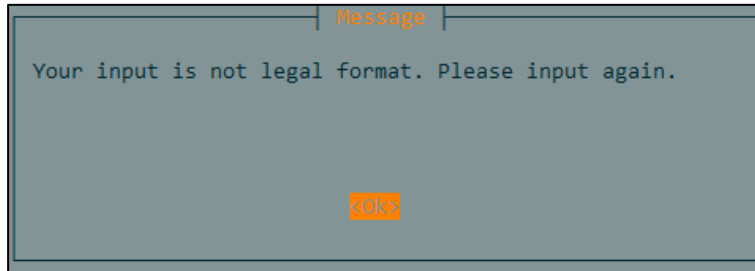


Figure 4-60 Automated deployment: typing the space size of data disks when the number is greater than the limit or 16 TB

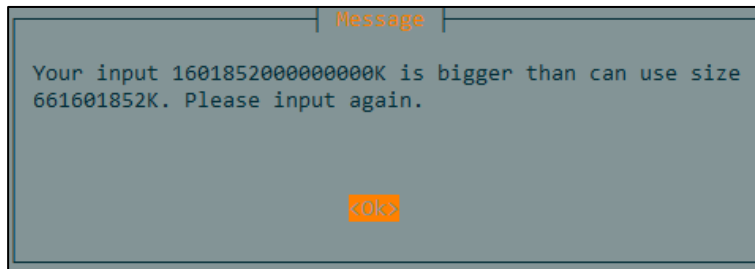
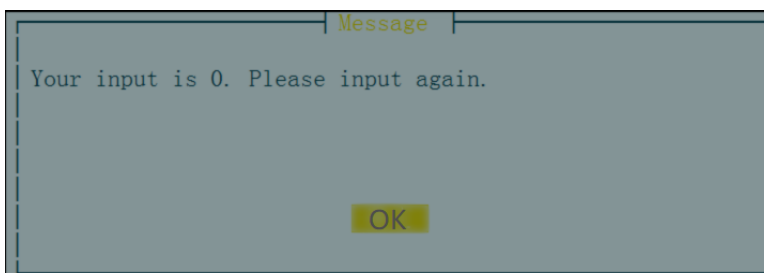


Figure 4-61 Automated deployment: typing the space size of data disks when the number is 0



----End

4.4.1.21 Configuring a Working Interface for vUTS

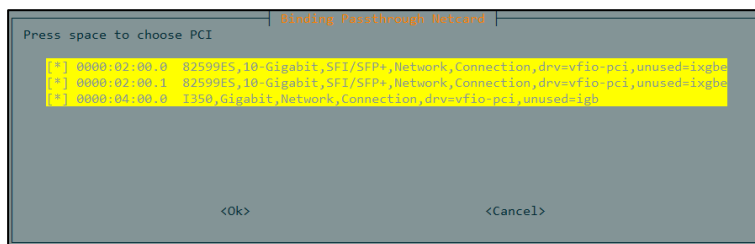
Configure a working interface for vUTS according to the selected deployment mode described in [Choosing a Deployment Mode](#).

High-Performance Mode

In high-performance mode, to configure a working interface, follow these steps:

- Step 1** As shown in [Figure 4-62](#), the dialog box displays all NICs that support transparent transmission and can be used for working interfaces.
- The dialog box does not display already selected NICs (see [Choosing an NIC for the Management Interface of the Host](#)).
 - By default, all NICs are selected. Unbind the NICs that are not required. (Note that the waiting time for UTS initialization is related to the number of bound NICs. The more the NICs, the longer the waiting time.)
Choose the NICs to be bound based on the traffic volume or according to actual situation. For example, if the traffic volume is greater than 1 GB, generally, you can bind one to two 10-Gigabit NICs. If the traffic enters UTS in a multi-link manner, you can bind NICs as required.
 - Choose at least one NIC. Otherwise, re-selection is required.
 - If other vUTSs have been deployed on the host, you cannot choose NICs that are already in use. Otherwise, when you run the **virsh start** command to start the UTS, an error message is displayed, indicating that the deployed vUTS cannot be started.

Figure 4-62 Automated deployment: NIC information displayed



- Step 2** Press **TAB** to enter a list.
- Press **TAB** to switch to the scroll bar, list, **Ok**, or **Cancel**.
 - If the dialog box cannot display a complete list, switch to the scroll bar on the right side and press **↑** or **↓** to view it.
- Step 3** Press **↑** or **↓** and the space bar to choose NICs.
- The asterisk (*) indicates that the NIC is selected, while null indicates the NIC is not selected.
 - If two asterisks (***) appear, it indicates that the NIC is selected, while one asterisk (*) indicates that the NIC is not selected.
- Step 4** Press **TAB**, choose **Ok** or **Cancel** as required, and then press **Enter**.
- Choose **Ok**:
 - If no NIC is selected, a message box appears, as shown in [Figure 4-63](#). Press **Enter** to return to the dialog box to choose NICs again.
 - If more than one NICs are selected, automated installation continues.
 - Click **Cancel**. A message box appears, as shown in [Figure 4-8](#). Press **Enter** to stop deploying. To perform installation again, re-execute the deployment script **Autodeploy.sh**.

Figure 4-63 Automated deployment: choosing NICs again



---End

Common Mode

In common mode, to configure a working interface, follow these steps:

Step 1 Configure the space size of a disk to be created. See Unbinding an NIC.

- a. If a message box appears, as shown in [Figure 4-64](#), press **Enter** to stop deploying. It indicates that no NICs are available for common mode, and all NICs are already bound in high-performance mode. Unbind NICs (see Unbinding an NIC) and execute the deployment script **Autodeploy.sh** again.

Figure 4-64 Automated deployment: no NICs available for common mode



- b. If a message box appears, as shown in [Figure 4-65](#), it displays all NICs available that can be used for working interfaces of vUTS, indicating that there are NICs that can be bound in bridge mode.
 - The dialog box only displays NICs used for transparent transmission and does not display the already selected NICs (see Choosing an NIC for the Management Interface of the Host).
 - By default, all NICs are selected. Unbind the NICs that are not required. (Note that the waiting time for UTS initialization is related to the number of bound NICs. The more the NICs, the longer the waiting time.)

Choose the NICs to be bound based on the traffic volume or according to actual situation. For example, if the traffic volume is greater than 1 GB, generally, you can bind one to two 10-Gigabit NICs. If the traffic enters UTS in a multi-link manner, you can bind NICs as needed.
 - Choose at least one NIC. Otherwise, you need to select NICs again.

- If other UTSs have been deployed on the host, you cannot choose NICs that are already in use. Otherwise, when you run the **virsh start** command to start UTS, an error message is displayed, indicating that the deployed UTS cannot be started.

Figure 4-65 Automated deployment: NICs available for working interfaces



Step 2 Press **TAB** to enter a list.

- a. Press **TAB** to switch to the scroll bar, list, **Ok**, or **Cancel**.
- b. If the dialog box cannot display a complete list, switch to the scroll bar on the right side and press **↑** or **↓** to view it.

Step 3 Press **↑** or **↓** and the space bar to choose NICs.

- a. The asterisk (*) indicates that the NIC is selected, while null indicates the NIC is not selected.
- b. If two asterisks (**) appear, it indicates that the NIC is selected, while one asterisk (*) indicates that the NIC is not selected.

Step 4 Press **TAB**, choose **Ok** or **Cancel** as required, and then press **Enter**.

- a. Choose **Ok**:
 - If no NIC is selected, a message box appears, as shown in [Figure 4-63](#). Press **Enter** to return to choose NICs again.
 - If more than one NICs are selected, automated installation continues.
- b. Choose **Cancel**. A message box appears, as shown in [Figure 4-8](#). Press **Enter** to stop deploying. To perform installation again, re-execute the deployment script **Autodeploy.sh**.

----End

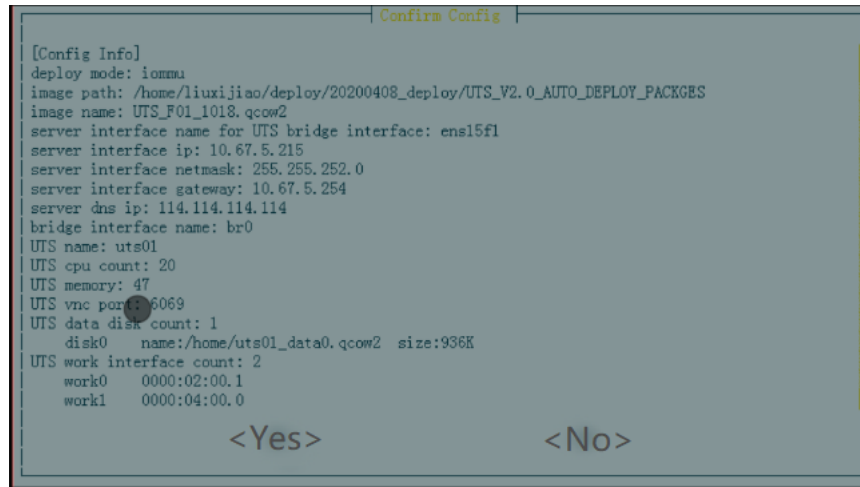
4.4.1.22 Confirming the Configuration Information

To confirm the configuration information, follow these steps:

Step 1 As shown in [Figure 4-66](#), the dialog box displays all the settings you configure by following the steps described from section Choosing a Deployment Mode to section Configuring a Working Interface for vUTS. Confirm whether the configuration is correct.

Note that after performing the previous steps, you have completed the configuration information, and however, the configuration has not taken effect. If there are any incorrect settings, you can stop the deployment and configure them again.

Figure 4-66 Automated deployment: confirming the configuration information



```

[Config Info]
deploy mode: iommu
image path: /home/liuxijiao/deploy/20200408_deploy/UTS_V2.0_AUTO_DEPLOY_PACKGES
image name: UTS_F01_1018.qcow2
server interface name for UTS bridge interface: ens15f1
server interface ip: 10.67.5.215
server interface netmask: 255.255.252.0
server interface gateway: 10.67.5.254
server dns ip: 114.114.114.114
bridge interface name: br0
UTS name: uts01
UTS cpu count: 20
UTS memory: 47
UTS vnc port: 5069
UTS data disk count: 1
  disk0  name:/home/uts01_data0.qcow2  size:936K
UTS work interface count: 2
  work0  0000:02:00.1
  work1  0000:04:00.0

<Yes>          <No>

```

Step 2 Press **TAB** to enter a list.

- a. Press **TAB** to switch to the scroll bar, **Yes**, or **No**.
- b. If the dialog box cannot display a complete list, switch to the scroll bar on the right side and press **↑** or **↓** to view it.

Step 3 Press **TAB**, choose **Yes** or **No** as required, and press **Enter**.

- a. Choose **Yes** to confirm the settings and continue automated installation.
- b. Choose **No**. A message box appears, as shown in [Figure 4-8](#). Press **Enter** to stop deploying. To perform installation again, re-execute the deployment script **Autodeploy.sh**.

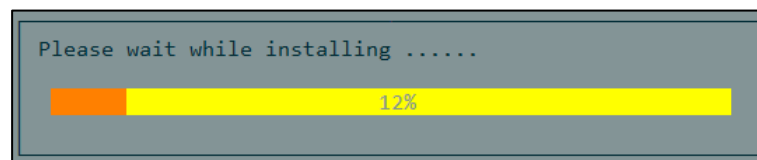
---End

4.4.1.23 Installing vUTS

Based on the confirmed configuration information, the system backend will automatically perform vUTS installation. As shown in [Figure 4-67](#), the installation progress is displayed and will be completed automatically.

- If the installation is successful, automated installation continues.
- If an error occurs, a message box appears. Press **Enter** to stop deploying. Follow the prompts in the dialog box to troubleshoot and solve errors, and then re-execute the deployment script **Autodeploy.sh**.

Figure 4-67 Automated deployment: vUTS installed automatically



```

Please wait while installing .....
12%

```

4.4.1.24 Configuring vUTS to Automatically Start at System Startup

As shown in [Figure 4-68](#), determine whether setting vUTS to automatically start at system startup. Press **TAB**, choose **Yes** or **No** as required, and press **Enter**.

- Choose **Yes** to set vUTS to start at system startup. Then automated installation continues.
- Choose **No** to disable automatic start of vUTS at system startup. Then automated installation continues.

Figure 4-68 Automated deployment: setting vUTS to start at system startup



Note

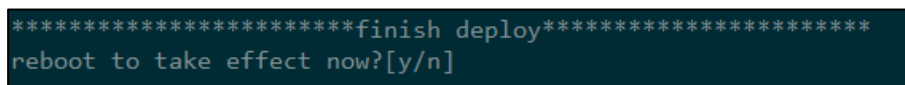
If choosing **No**, you need to manually start UTS every time the host restarts. The command is as follows: **virtsh start UTS-name**.

4.4.2 Restarting the Host

After the installation is complete, the system informs you to restart the host, as shown in [Figure 4-69](#).

- Type **y** to restart the host.
- Type **n** not to restart the host.

Figure 4-69 Restarting the host



Caution

- If it is the first vUTS deployment, you need to restart the host to make certain parameters to take effect.
- Before restarting the host, check for any obvious errors by examining the debug log file **deploy.log** in the current deployment directory. If there are any errors (except for a high-performance NIC binding error that may be handled by restarting the system), it is recommended to redeploy vUTS after correcting the errors.

4.4.3 Initial UTS Configuration

The initial configuration includes configuring the IP address, system time, and importing licenses.

4.4.3.1 Configuring an IP Address for UTS

To configure an IP address, follow these steps:

- Step 1** After the host restarts, log in to the console port by using the following command. (For the administrator account of the console port, see Default Parameters).

```
virsh console uts01
```

- Step 2** After the successful login, the main menu for system configuration is displayed, as shown in [Figure 4-70](#).

If a prompt appears indicating that the system initialization is not completed yet, be patient and wait until the main menu is displayed.

Figure 4-70 Main menu for system configuration

```
localhost login: conadmin
Password:
Last login: Tue Jan 31 15:40:02 on
WARNING: yacc table file version is out of date
-----
System Main Menu:
 1: Init Network.
 2: Bind Hardware.
 3: Reset Admin Password.
 4: Reset Auditor Password.
 5: Open/Close Remote Assist.
 6: Show Ip address.
 7: Reset System Time.
 8: Show System Time.
 9: Initialize System Configuration.
10: Reboot System.
11: Shutdown System.
12: Create Lvm Partition.
13: Stop Service.
14: Change Https Port.
15: Add New Disk in Lvm Partition.
16: Modify Lvm Partition Size.
 0: Exit.
-----
```

- Step 3** Choose option 1 to configure an IP address for UTS, as shown in [Figure 4-71](#).

Note that the IP address of UTS is configured here, rather than that of the host.

Figure 4-71 UTS console port configuration: network information

```
§:1
ip address(192.168.1.1/16):10.14.45.66/16
Gateway:10.14.255.254
Init OK.
```

Step 4 After completing the above steps, execute the **ping** command on a user's PC to check the connection to this IP address.

---End

4.4.3.2 Calibrating the System Time

As shown in [Figure 4-70](#), choose option 8 in the menu to view the system time. If it is not consistent with the current time, choose option 7 to reset it, as shown in [Figure 4-72](#).

Figure 4-72 Calibrating the system time

```
$:7
Please input time(example 2019-05-22 14:22:30): 2023-01-31 16:41:00
Reset OK.
Please reboot system.
```

4.4.3.3 Importing the License

When using UTS for the first time, you are required to perform the following configurations on the web-based manager of UTS:

Step 1 Check that the management host communicates properly with UTS. (Open port 443 if the traffic needs to go through a firewall.)

Step 2 Open your browser and access UTS via HTTPS by typing the management IP address of UTS, for example, **https://192.168.1.1**, in the address bar.

Step 3 Click **Advanced** and click **Accept the Risk and Continue** to jump to the login page of the UTS web-based manager.

Step 4 Type a correct user name and password and click **Log In**.

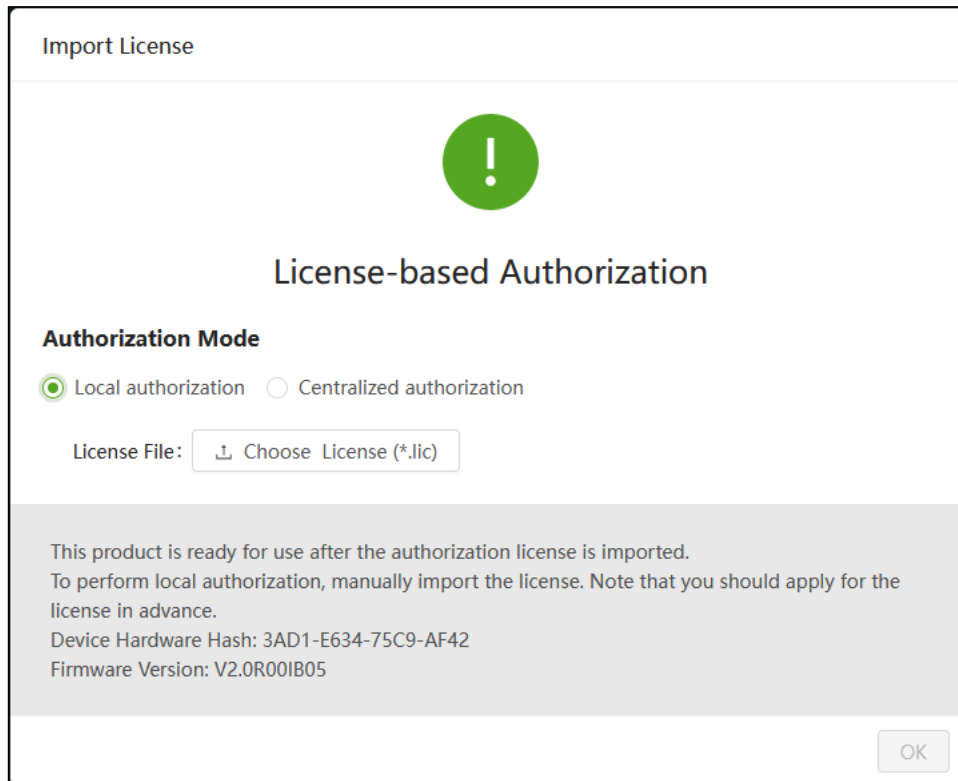
Upon the initial login, use the default **admin** account. For the initial administrator account and password, see Default Parameters.

Step 5 When logging in with the default password for the first time, the system will force a password change. After changing the password, click **OK**.

Step 6 Import the license.

- a. After you log in again with the changed password, the dialog box of importing the license pops up, as shown in [Figure 4-73](#). You are required to import a correct license file before continuing to use this device.

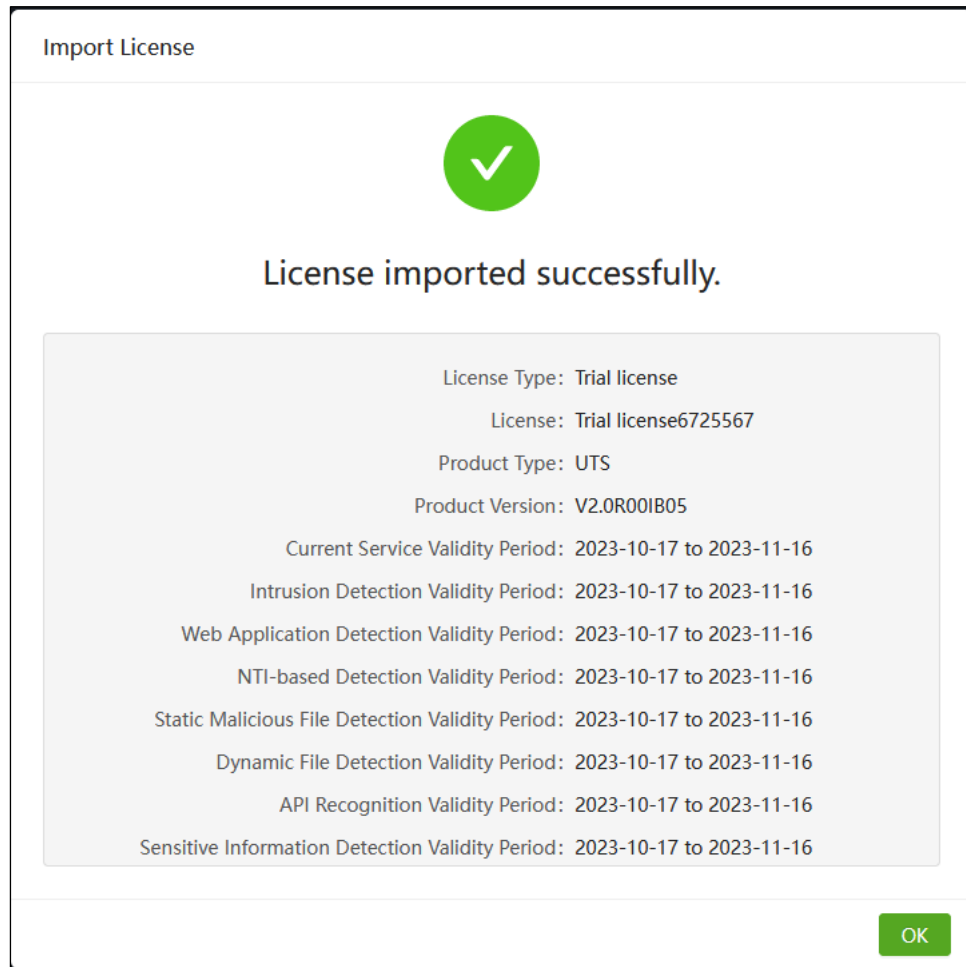
Figure 4-73 License authorization dialog box



b. Local authorization

Choose **Local authorization**. After choosing a correct license file, click **OK**, and then click **Import** in the displayed dialog box, as shown in [Figure 4-74](#).

Figure 4-74 Prompt of license imported successfully




c. Centralized authorization.

- Set the authorization mode to **Centralized authorization**. Type the address and port number of the authorization device (that is, NSFOCUS Enterprise Security Platform, abbreviated as ESP-C), and then click **OK**, as shown in [Figure 4-75](#).
- Use ESP-C to perform the centralized authorization. For details, see *NSFOCUS ESPC User Guide*.

Figure 4-75 Centralized authorization dialog box

Import License



License-based Authorization

Authorization Mode

Local authorization
 Centralized authorization

Authorization Device Information

* HOST :

* Port :

This product is ready for use after the authorization license is imported.
 Use NSFOCUS Enterprise Security System (ESP-C) to perform centralized authorization. You need to provide ESPC information.
 Device Hardware Hash: 3AD1-E634-75C9-AF42
 Firmware Version: V2.0R00IB05


Note

- Before login, check whether the check box of blocking pop-ups or disabling JavaScript is selected in your browser. If yes, deselect the check box.
- You are advised to use the latest Chrome browser or Firefox browser and set the screen resolution to 1024 x 768 or higher.
- When using this system for the first time, you can use the default administrator account to log in.

---End

4.4.4 Creating a Snapshot

After [Initial UTS Configuration](#) is complete, you need to create a system snapshot of the initial configuration, enabling convenient restoration in the future.

The command for creating a system snapshot is as follows:

```
virsh snapshot-create-as UTSXXX UTSXXX-snapshotname
//UTSXXX refers to the UTS name, and UTSXXX-snapshotname refers to the snapshot name.
```



- Creating a snapshot is an indispensable step that cannot be ignored.
- Shut down UTS before creating a snapshot or restoring from the snapshot.

4.5 UTS Version Upgrade

After the UTS deployment is complete, you can offline upgrade the engine, various rule bases, NTI databases, geodatabases, and virus signature databases.



- Version updates are released occasionally.
- Sometimes upgrade page timeout may lead to upgrade failure. It is recommended to change the timeout interval to **0** before upgrading, and then restore it after completing the upgrade.

4.5.1 Upgrading the System Engine

To upgrade the engine, follow these steps:

- Step 1** Obtain the latest engine upgrade package from the official website at <http://update.nsfocus.com/update/bsaUtsIndex>
- Step 2** After downloading the upgrade package to the local management host, log in to the UTS web-based manager. (For the account and password, see Default Parameters.)
- Step 3** Choose **System > System Upgrade > Offline Upgrade**. Manually upgrade the system, as shown in [Figure 4-76](#).

Figure 4-76 System upgrade page

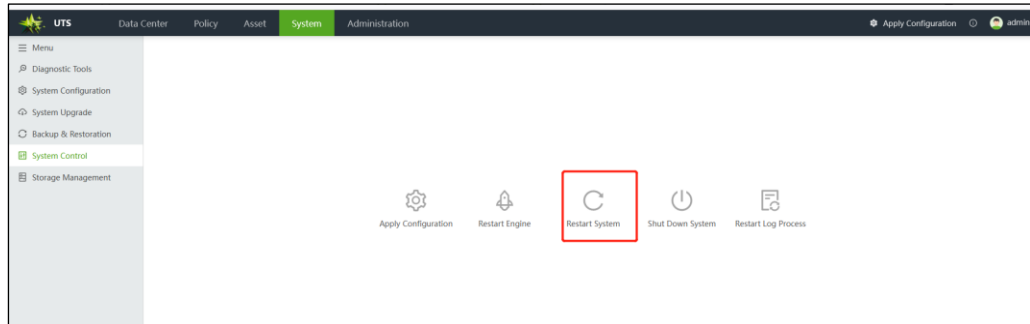
The screenshot shows the UTS web interface. The 'System' tab is active, and the 'Offline Upgrade' sub-tab is selected. A dropdown menu is open, showing 'System (*.bin)' selected, with a 'Select File' button next to it. Below this, there is a 'Current Version Info' section with several components and their versions: System (*bin) V2.0R000805, Intrusion detection rule base (*.rule) V2.0R00130248, Web application rule base (*.wcl) 6.0.7.3.56040, NTI database (*.nti) 20200620, and Virus signature database (*.av) 20200620. At the bottom, there is an 'Offline Upgrade History (1)' table with one entry showing a successful upgrade from version 2.0.0.00805.36584 to 2.0.0.00805.100000.bin.

Upgrade Start Time	Upgrade Package Type	Upgrade Version	Upgrade Status	Description
2023-10-17 13:48:57	System	eol.agentpatch.uts_x86.2.0.0.00805.100000.bin	Success	Previous version: 2.0.0.00805.36584, upgraded to: eol.agentpatch.uts_x86.2.0.0.00805.100000.bin

- Step 4** (Optional) Restart the system.

Some upgrade packages states that you need to restart the system to make it take effect. After upgrading, choose **System > System Control** to manually restart UTS, as shown in [Figure 4-77](#).

Figure 4-77 System restart icon



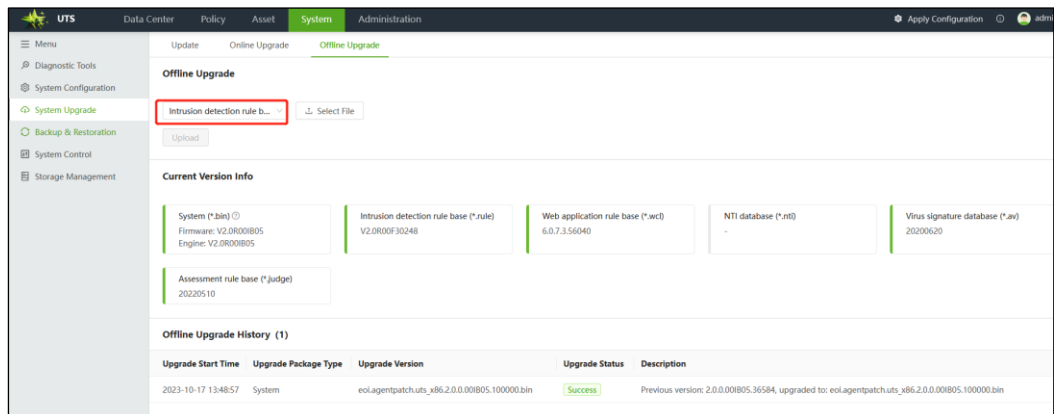
----End

4.5.2 Upgrading the Intrusion Detection Rule Base

Use the same method for obtaining an intrusion detection rule base upgrade package and upgrading the intrusion detection rule base. For details, see [Upgrading the System Engine](#).

Choose **System > System Upgrade > Offline Upgrade**. Manually upgrade it, as shown in [Figure 4-78](#).

Figure 4-78 Intrusion detection rule base upgrade page

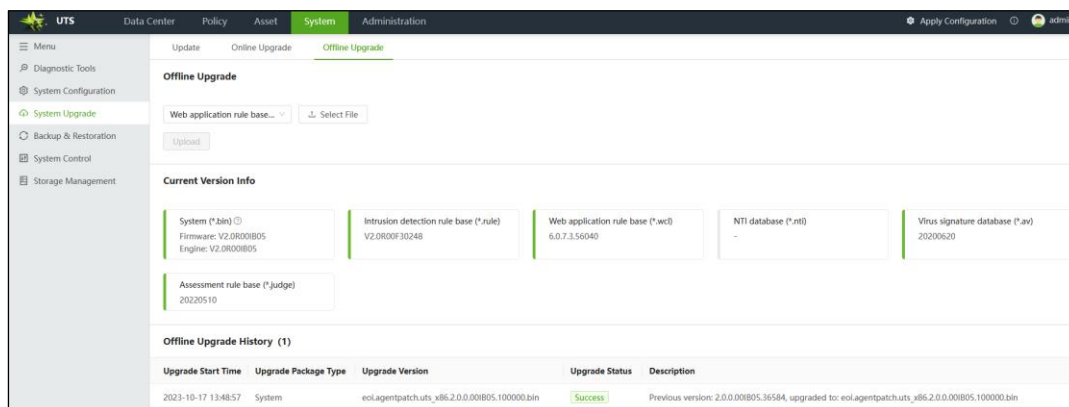


4.5.3 Upgrading the Web Application Rule Base

Use the same method for obtaining a web application rule base upgrade package and upgrading the Web application rule base. For details, see [Upgrading the System Engine](#).

Choose **System > System Upgrade > Offline Upgrade**. Manually upgrade it, as shown in [Figure 4-79](#).

Figure 4-79 Web application rule base upgrade page

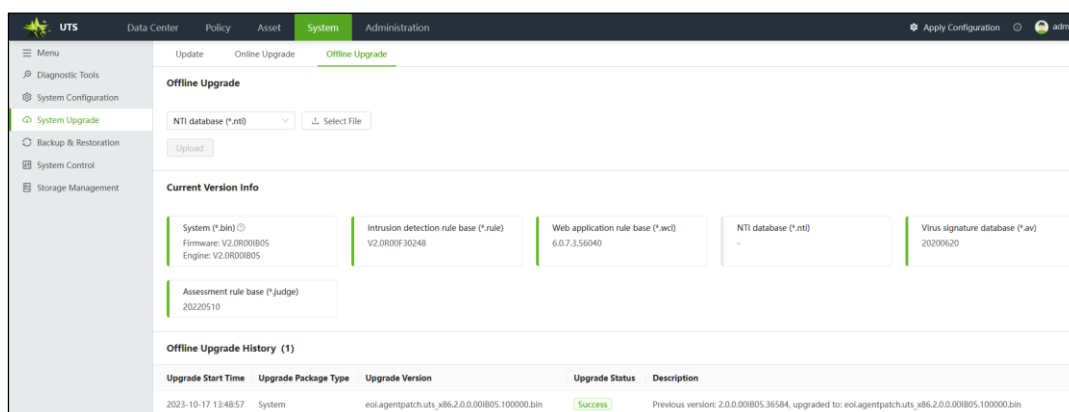


4.5.4 Upgrading the NTI Database

Use the same method for obtaining an NTI database upgrade package and upgrading the NTI database. For details, see [Upgrading the System Engine](#).

Choose **System** > **System Upgrade** > **Offline Upgrade**. Manually upgrade it, as shown in [Figure 4-80](#).

Figure 4-80 NTI database upgrade page

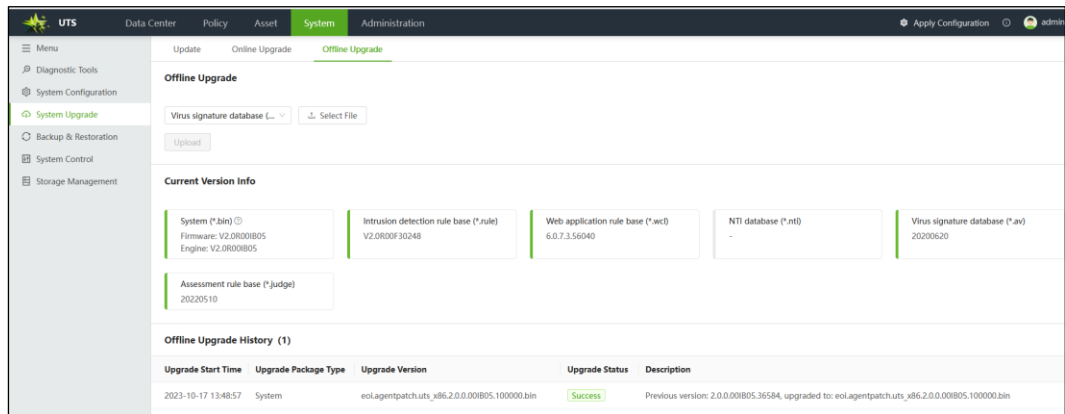


4.5.5 Upgrading the Virus Signature Database

Use the same method for obtaining a virus signature database upgrade package and upgrading the virus signature database. For details, see [Upgrading the System Engine](#).

Choose **System** > **System Upgrade** > **Offline Upgrade**. Manually upgrade it, as shown in [Figure 4-81](#).

Figure 4-81 Virus signature database upgrade page

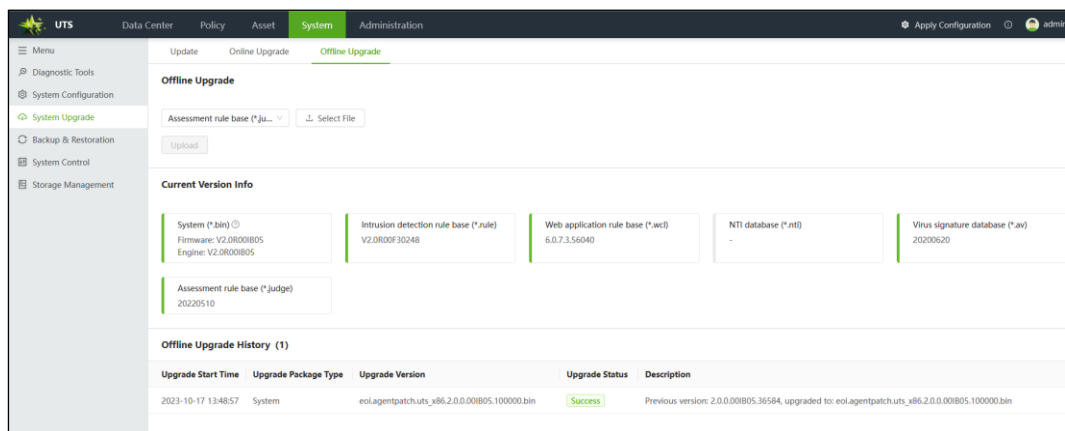


4.5.6 Upgrading the Assessment Rule Base

Use the same method for obtaining an assessment rule base upgrade package and upgrading the assessment rule base. For details, see [Upgrading the System Engine](#).

Choose **System** > **System Upgrade** > **Offline Upgrade**. Manually upgrade it, as shown in [Figure 4-82](#).

Figure 4-82 Assessment rule base upgrade page



5 Replacing the Image of UTS

This chapter contains the following sections:

Section	Description
Replacement Notes	Describes circumstances where the image requires replacement.
Preparing a New Image File	Describes preparations before replacing the image of UTS.
Replacing the Image File	Describes how to replace the image of UTS.

5.1 Replacement Notes

Replace the image of UTS in the following circumstances.

- UTS installation and deployment are complete.
- Version upgrades.
- An image is damaged during operation.

5.2 Preparing a New Image File

To prepare a new image file, follow these steps:

Step 1 Obtain the latest image file. For details, see [Preparing Software](#).

Step 2 Use the following command to view the path where the old image file is stored, as shown in [Figure 5-1](#).

```
virsh edit UTS-name
```


Figure 5-1 Viewing the image file path where the image is stored

```
<devices>
<emulator>/usr/libexec/qemu-kvm</emulator>
<disk type='file' device='disk'>
<driver name='qemu' type='qcow2' />
<source file='/mnt/raid0/F01/UTS_F02_06201.qcow2' />
<target dev='vda' bus='virtio' />
<address type='pci' domain='0x0000' bus='0x00' slot='0x06' function='0x0' />
</disk>
```

Step 3 Delete the old image.

For example, as shown in [Figure 5-1](#), delete `UTS_F02_06201.qcow2` in the path `/mnt/raid0/F01/`.

Step 4 Place the latest image file in the same path.

---End

5.3 Replacing the Image File

This section describes how to replace the image file of vUTS.

5.3.1 Backing Up the License

If the system is damaged and you are unable to log in to the web-based manager, you can skip this step and contact NSFOCUS technical support personnel to produce the license.

It is recommended to back up the old license before replacing the image.

Log in to the web-based manager and choose **System > Backup & Restoration > Backup** to back up the current license file.

5.3.2 Shutting Down UTS

Use the following command to view the running UTS, and then select and shut down the UTS to replace the image, for example, `virsh shutdown uts_f01`, as shown in [Figure 5-2](#).

```
virsh list --all
```

Figure 5-2 Shutting down UTS before replacing the image file

```
[root@isop234 UTS_V2.0_AUTO_DEPLOY_PACKGES]# virsh list --all
 Id      Name                               State
-----
 26     uts_f01                            running
```

If vUTS cannot be shut down, run the following command to force a shutdown:

```
virsh destroy uts_f01
```

5.3.3 Creating a New Data Disk



- If the versions of the old and new images are the same (such as replacing version F05 with version F05), you do not need to replace the data disk if there is no special requirement and can skip this step.
- Otherwise, this skip is required. (For example, replace version F04 with version F05.)

Use the following command to create a new data disk. In this example, **utsdisk.qcow2** is the name of the data disk and you can rename it. **200G** refers to a maximum storage capacity of 200 GB to store data and you can be reset the capacity.)

Note that the capacity of a single disk in the Ext4 file system cannot exceed 16 TB.

```
qemu-img create -f qcow2 -o compat=0.10 utsdisk.qcow2 200G
```

If there is a need for data backup on the old data disk, place the old data disk in the background. If there is no such requirement, directly delete it.

5.3.4 Replacing the Image File and Data Disk

To replace the image file and data disk, follow these steps:

Step 1 Use the following command to check the path where the image file and data disk are stored:

```
virsh edit UTS-name
```

The **vda** drive letter must be used to specify the image file path, while the **vdb** drive letter must be used to specify the data disk path.

Figure 5-3 Confirming the path where the image and data disk are stored

```
<devices>
  <emulator>/usr/libexec/qemu-kvm</emulator>
  <disk type='file' device='disk'>
    <driver name='qemu' type='qcow2' />
    <source file='/mnt/raid0/F01/UTS_F02_06201.qcow2' />
    <target dev='vda' bus='virtio' />
    <address type='pci' domain='0x0000' bus='0x00' slot='0x06' function='0x0' />
  </disk>
  <disk type='file' device='disk'>
    <driver name='qemu' type='qcow2' />
    <source file='/mnt/raid0/F01/utsdisk.qcow2' />
    <target dev='vdb' bus='virtio' />
    <address type='pci' domain='0x0000' bus='0x00' slot='0x0a' function='0x0' />
  </disk>
```

Step 2 Type new paths for the image and data disk respectively, as shown in [Figure 5-4](#).

Type new paths based on the actual configuration.

Figure 5-4 The replaced image and data disk paths

```
<devices>
<emulator>/usr/libexec/qemu-kvm</emulator>
<disk type='file' device='disk'>
  <driver name='qemu' type='qcow2' />
  <source file='/mnt/raid0/zcy/f04/standard_F04_20220520.qcow2' />
  <target dev='vda' bus='virtio' />
  <address type='pci' domain='0x0000' bus='0x00' slot='0x08' function='0x0' />
</disk>
<disk type='file' device='disk'>
  <driver name='qemu' type='qcow2' />
  <source file='/mnt/raid0/zcy/f04/utsdisk.qcow2' />
  <target dev='vdb' bus='virtio' />
  <address type='pci' domain='0x0000' bus='0x00' slot='0x09' function='0x0' />
</disk>
```

Step 3 Replace the image path with the latest one, and replace the disk path with the newly created one.

Step 4 Save the changes and exit.

----End

5.3.5 Starting UTS

Use the following command to start UTS, as shown in [Figure 5-5](#).

```
virsh start UTS name
```

Figure 5-5 Starting UTS

```
[root@isop234 UTS_V2.0_AUTO_DEPLOY_PACKGES]# virsh start uts_f01
Domain uts_f01 started
```

5.3.6 Initial UTS Configuration

For details, see [Initial UTS Configuration](#).

5.3.7 Creating a Snapshot

For details, see [Creating a Snapshot](#).

6 Common Basic Operations

If an error occurs during automated deployment, you can identify the problem according to the error message, and then troubleshoot it.

This chapter contains the following sections:

Section	Description
Checking Network Interfaces	Describes how to check network interfaces.
Checking Transparent Transmission Parameters of the Kernel	Describes how to view transparent transmission parameters of the kernel.
Binding and Checking Mirroring Transparent Transmission Interfaces	Describes how to bind and check image transparent transmission interfaces.
Basic Operations of Data Disks	Describes basic operations of data disks.
Basic Operations of Network Bridges	Describes basic operations of network bridges.
Basic Operations of vUTS	Describes basic operations of vUTS.
Opening a VNC Port	Describes how to open a VNC port.
Modifying the Memory Size of UTS	Describes how to modify UTS memory.
Logging In to the UTS Console	Describes how an SSH administrator log in to the UTS console.

6.1 Checking Network Interfaces

The configuration file of network interfaces is stored in the path `etc/sysconfig/network-scripts/ifcfg-xx`, as shown in [Figure 6-1](#).

Figure 6-1 Configuration file of network interfaces

```

TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ens2f0
UUID=6c4af7ad-ab14-4e40-9406-fb800e7cd533
DEVICE=ens2f0
ONBOOT=no
    
```

The configuration file of the NIC used for the management interface of UTS is stored in the path `/etc/sysconfig/network-scripts/ifcfg-br0`, as shown in [Figure 6-2](#).

Figure 6-2 Configuration file of the NIC used for the management interface of UTS

```

TYPE=Bridge
BOOTPROTO=static
IPV4_FAILURE_FATAL=no
NAME=br0
DEVICE=br0
ONBOOT=yes
IPADDR=10.67.5.218
PREFIX=22
GATEWAY=10.67.5.254
DNS1=114.114.114.114
NM_CONTROLLED=no
    
```

Use the following command to view network bridge information, as shown in [Figure 6-3](#).

```
brctl show
```

Figure 6-3 Network bridge information

```

[root@localhost ~]# brctl show
bridge name      bridge id                STP enabled  interfaces
br0               8000.0024ecf0b339        no           ens15f0
                 vnet0
                 vnet1
                 vnet2
                 vnet3
                 vnet4
                 vnet5
br1               8000.000000000000        no
br2               8000.000000000000        no
virbr0           8000.525400c70877        yes          virbr0-nic
    
```

6.2 Checking Transparent Transmission Parameters of the Kernel

Perform the following steps:

- Check the `/etc/default/grub` file, as shown in the content in red font.

```
GRUB_TIMEOUT=5
```

```
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=2
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL_OUTPUT="console"
GRUB_CMDLINE_LINUX="rd.lvm.lv=centos00/swap vconsole.font=latarcyrheb-sun16
rd.lvm.lv=centos00/root hugepages=1024 crashkernel=auto vconsole.keymap=us rhgb
quiet intel_iommu=on"
GRUB_DISABLE_RECOVERY="true"
```

- Rewrite grub.

Based on the actual installation directory, choose one of the following two commands. When grub is installed in the default boot directory, use the second command.

```
grub2-mkconfig -o /boot/efi/EFI/centos/grub.cfg
grub2-mkconfig -o /boot/grub2/grub.cfg
```

- Verify the configuration.

```
[root@localhost~]# dmesg | grep IOMMU
[ 0.000000] DMAR: IOMMU enabled
[ 0.120711] DMAR-IR: IOAPIC id 10 under DRHD base 0xfbfcc000 IOMMU 0
[ 0.120712] DMAR-IR: IOAPIC id 8 under DRHD base 0xc7ffc000 IOMMU 1
[ 0.120713] DMAR-IR: IOAPIC id 9 under DRHD base 0xc7ffc000 IOMMU 1
```

6.3 Binding and Checking Mirroring Transparent Transmission Interfaces

Operations in this section are applicable to high-performance mode only.

The provided two script files and one NIC interface information file are as follows:

```
dpdk_nic_bind.py /* A NIC binding tool */
AutoNic_bond.py /* Automatically binding a configured NIC to the pci_info file */
pci.info /* Information about the NIC that needs to be bound by a user */
```

6.3.1 Viewing NIC Binding Information

As shown in [Figure 6-4](#), the NICs that have been bound and are being used for transparent transmission interfaces are displayed under **Network devices using DPDK-compatible driver**, while the NICs available for binding on the server are displayed under **Network devices using kernel driver**.

Figure 6-4 NIC binding information

```
[root@uts Bond_NIC]# ./dpmk_nic_bind.py -s
Network devices using DPMK-compatible driver
=====
0000:06:00.1 'I350 Gigabit Network Connection' drv=vfio-pci unused=igb
0000:82:00.0 'I350 Gigabit Network Connection' drv=vfio-pci unused=igb
0000:82:00.1 'I350 Gigabit Network Connection' drv=vfio-pci unused=igb
=====
Network devices using kernel driver
=====
0000:01:00.0 'Ethernet Controller 10-Gigabit X540-AT2' if=eth8 drv=ixgbe unused=vfio-pci
0000:01:00.1 'Ethernet Controller 10-Gigabit X540-AT2' if=eth9 drv=ixgbe unused=vfio-pci
0000:04:00.0 'I350 Gigabit Network Connection' if=eth0 drv=igb unused=vfio-pci
0000:04:00.1 'I350 Gigabit Network Connection' if=eth1 drv=igb unused=vfio-pci
0000:04:00.2 'I350 Gigabit Network Connection' if=eth2 drv=igb unused=vfio-pci
0000:04:00.3 'I350 Gigabit Network Connection' if=eth3 drv=igb unused=vfio-pci
0000:06:00.0 'I350 Gigabit Network Connection' if=eth4 drv=igb unused=vfio-pci
```

6.3.2 Binding a Transparent Transmission Interface

Add the information of transparent NICs to be bound to the `pci.info` file, and then run `AutoNic_bond.py` to automatically bind it.

```
[root@uts Bond_NIC]# vi pci.info
0000:06:00.1
0000:82:00.0
0000:82:00.1
[root@uts Bond_NIC]# python AutoNic_bond.py
```

Checking Whether the NIC Is Successfully Bound

Check whether the NIC is successfully bound, as shown in [Figure 6-5](#).

Figure 6-5 Checking whether the NIC is successfully bound

```
[root@uts Bond_NIC]# ./dpmk_nic_bind.py -s
Network devices using DPMK-compatible driver
=====
0000:06:00.1 'I350 Gigabit Network Connection' drv=vfio-pci unused=igb
0000:82:00.0 'I350 Gigabit Network Connection' drv=vfio-pci unused=igb
0000:82:00.1 'I350 Gigabit Network Connection' drv=vfio-pci unused=igb
```

Checking Whether the Transparent Transmission Device Is Successfully Added

After a transparent transmission interface is bound successfully, the corresponding character device is displayed under the `/dev/vfio` directory. You can view the PCI information of the NIC corresponding to the character device.

```
[root@uts ~]# ls -l /dev/vfio/
total 0
crw----- 1 root root 241, 0 Mar 6 17:14 22
crw----- 1 root root 241, 1 Mar 6 17:14 45
crw----- 1 root root 241, 2 Mar 6 17:14 46
crw-rw-rw- 1 root root 10, 196 Mar 6 17:14 vfio
[root@uts ~]# ls /sys/kernel/iommu groups/22/devices/
0000:06:00.1
```

6.3.3 Unbinding a Transparent Transmission Interface

Run the following commands to unbind an NIC:

```
[root@uts Bond_NIC]# ./dpdk_nic_bind.py -u 0006:06:00.1
[root@uts UTS_V2.0_AUTO_DEPLOY_PACKGES]# ./dpdk_nic_bind.py -b igb 0006:06:00.1 #
igb is determined based on unused, as shown in Figure 6-4.
```

6.4 Basic Operations of Data Disks

6.4.1 Creating a Data Disk

Note that the capacity of a single virtual data disk in the Ext4 file system cannot exceed 16 TB.

```
qemu-img create -f qcow2 -o compat=0.10 utsdisk.qcow2 200G
```

6.4.2 Viewing Data Disk Information

```
#qemu-img info uts-extend.qcow2
image: uts-extend.qcow2
file format: qcow2
virtual size: 100G (107374182400 bytes)
disk size: 11G
cluster_size: 65536
Format specific information:
compat: 0.10
```

6.5 Basic Operations of Network Bridges

6.5.1 Creating a Network bridge

Run the following command to create a network bridge.

```
[root@localhost~]#brctl addbr xxx //xxx is the name of the network bridge
```

6.5.2 Binding a Physical NIC for the Network Bridge

Run the following command to bind a physical NIC for the network bridge.

```
[root@localhost~]#brctl addif physical NIC-name
```

6.5.3 Activating the Network Bridge

Run the following command to activate the network bridge.

```
[root@localhost~]#ip link set xxx up
```

6.5.4 Deleting the Network Bridge

Run the following commands to delete the network bridge.


```
[root@localhost~]#ip link set xxx down //Deactivate the network bridge first
[root@localhost~]#brctl delbr xxx //Delete it
```

6.6 Basic Operations of vUTS

6.6.1 Defining a vUTS

Run the following command to define a vUTS and configure it.

```
[root@localhost~]#virsh define uts.xml
```

6.6.2 Undefining a vUTS

Run the following command to undefine a vUTS.

```
[root@localhost~]#virsh undefine uts.xml
```

6.6.3 Shutting Down a vUTS

```
[root@localhost~]#virsh shutdown uts01
```

If vUTS cannot be shut down by using the above command, you can use the following command to force it to shut down. (This may damage the system. Exercise caution during the operation.)

```
[root@localhost~]#virsh destroy uts01
```

6.6.4 Starting a vUTS

```
[root@localhost~]#virsh start uts
```

6.6.5 Viewing Defined vUTSs

```
[root@localhost~]#virsh list --all /* View all defined vUTSs */
```

6.6.6 Autostarting a vUTS at System Startup

```
[root@localhost~]#virsh autostart xxx /* Enable vUTS autostart at
system startup */
```

6.6.7 Disabling vUTS Autostart at System Startup

```
[root@localhost~]#virsh autostart --disable xxx /* Disable UTS VM autostart at
system startup */
```

6.6.8 Editing vUTS Configuration

If you need to change vUTS configurations, you can run the following command to edit vUTS. vUTS is maintained by libvirt, so you should shut down vUTS before editing it. This can ensure consistency and avoid any conflicts.

```
[root@localhost~]#virsh edit uts
```

6.6.9 Creating a vUTS Snapshot

Run the following command to create a vUTS snapshot.

```
[root@localhost~]#virsh snapshot-create-as -domain UTS-name --name Snapshot-name
```

6.6.10 Viewing a vUTS Snapshot

```
[root@localhost~]#virsh snapshot-list UTS-name
```

6.6.11 Restoring from a Snapshot

Run the following command to restore from a snapshot.

```
virsh snapshot-revert UTS-name Snapshot-name
```

6.7 Opening a VNC Port

A firewall is enabled on the Linux system by default. To ensure external connections to the configured port using Virtual Network Computing (VNC), you need to open VNC ports.

Run the following command on the host to open a VNC port:

```
[root@localhost~]#/sbin/iptables -I INPUT -p tcp --dport 6669 -j ACCEPT
```

Run the following command on the host to view the VNC port, as shown in [Figure 6-6](#).

```
virsh edit uts01
```

Figure 6-6 Opening the VNC port

```
<graphics type='vnc' port='6669' autoport='no' listen='0.0.0.0'>
  <listen type='address' address='0.0.0.0' />
</graphics>
```

6.8 Modifying the Memory Size of UTS

You can modify the memory size of UTS. On the host, perform the following steps:

Step 1 Run the following command to obtain the name of UTS to be modified.

```
[root@localhost ~]# virsh list -all
```

Step 2 If the UTS status is displayed as **running**, you need to run the following command to shut down it. (Note: In this example, GUANLI is the name of UTS to be modified.)

```
[root@localhost ~]# virsh shutdown GUANLI
```

Step 3 If the status does not change after more than half an hour, you can run the following command to force UTS to shut down.

```
[root@localhost ~]# virsh destroy GUANLI
```

Step 4 Run the following command to access the editing page.

```
[root@localhost ~]# virsh edit GUANLI
```

- a. Type **i** to access the Edit mode. Then, type the same value for both the **memory** and **currentMemory** nodes, as shown in the red frames in [Figure 6-7](#).

Figure 6-7 Modifying the memory size of vUTS

```
<domain type='kvm'>
  <name>GUANLI</name>
  <uuid>722ac067-4b8d-436e-aae7-861f3661384f</uuid>
  <memory unit='KiB' >6291456</memory>
  <currentMemory unit='KiB' >6291456</currentMemory>
  <vcpu placement='static' cpuset='0'>1</vcpu>
```

- b. Type **ctrl+[** to access Command mode, and then type **:wq** to save the edited configuration file and exit the editing page.

Step 5 Start UTS and run the following command to check whether the memory size is successfully changed.

```
[root@localhost ~]# virsh start GUANLI
```

---End

6.9 Logging In to the UTS Console

Log in to the host with the SSH administrator account and password (see Default Parameters). Then execute the following command on the host to log in to the UTS console:

```
virsh console uts-name
```

7

FAQ

This chapter describes frequently asked questions (FAQ) regarding the installation and deployment of UTS.

7.1 Deployment Method

Automatic deployment must be adopted. For details, see [Installing UTS](#).

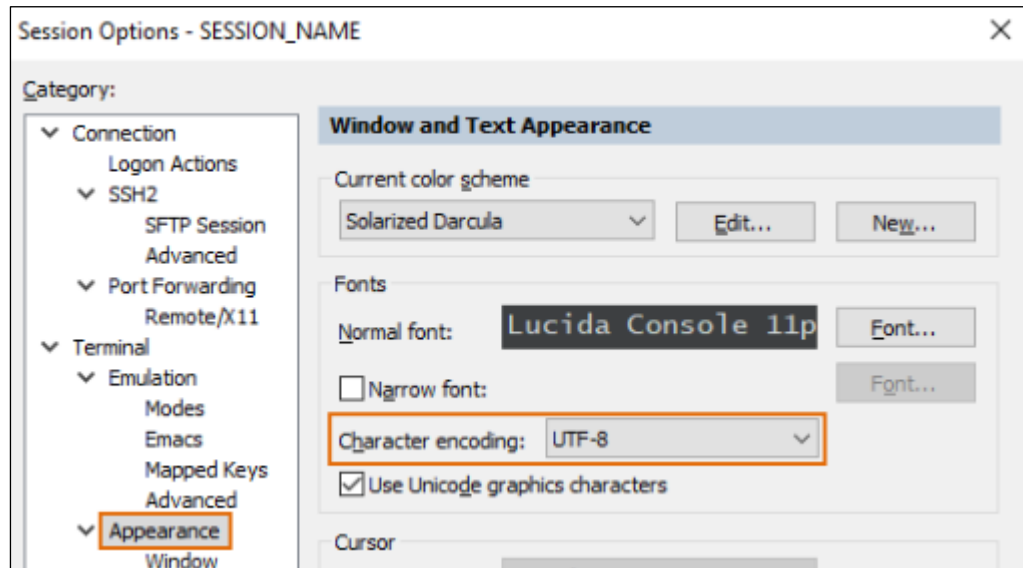
7.2 Requirements for the Host's Operating System

The host's operating system must be CentOS 7 and later, and it should be completely installed on the host. Other operating systems such as Red Hat operating systems are not supported. The software and hardware of the host must meet the requirements described in [Server Configuration Requirements](#).

7.3 Garbled Code Occurs During Deployment Script Execution

When logging in to the host using Xshell or SecureCRT, you need to change the character encoding option of the connection to UTF-8. The following takes SecureCRT as an example, as shown in [Figure 7-1](#).

Figure 7-1 Changing the character encoding of the connection (using SecureCRT)



7.4 IP Address Is Inaccessible After Host Restart

There are two possible causes:

- Incorrect physical NIC selected as the bridge interface. To resolve this problem, delete the original bridge interface first, and then manually create a bridge interface. For details, see [Choosing an NIC for the Management Interface of the Host](#).
- MAC address flapping.
 - MAC address flapping occurs when multiple network NICs are restarted. To fix it, you need to set the HWADDR value in the NIC file.
 - The value of the HWADDR field should be in the format of AA:BB:CC:DD:EE:FF, representing the hardware address of the Ethernet device. On hosts with multiple NICs, this field is used to ensure that every NIC is assigned a correct name, regardless of the loading order of these NICs.
 - Add HWADDR=AA:BB:CC:DD:EE:FF to the file of the physical NIC bound to the host **br0**, and then run the **systemctl restart network** command to restart the network. Here, AA:BB:CC:DD:EE:FF is the MAC address of the physical NIC.

7.5 vUTS Automatically Shuts Down a Few Minutes After Startup

Description

No errors are reported during vUTS startup. vUTS starts up normally, but automatically shuts down after a few minutes, as shown in [Figure 7-2](#).

Figure 7-2 vUTS automatically shuts down a few minutes after startup

```
[root@localhost UTS_V2.0_AUTO_DEPLOY_PACKGES]# virsh start uts01
error: Failed to start domain uts01
error: 所需操作无效: PCI device 0000:02:00.1 is in use by driver QEMU, domain liuxijiao_UTSV2.0R00F01
```

Solution

After inspection, it is found that the host has a total of 64 GB of memory and vUTS occupies 60 GB, leaving insufficient memory for the host. When the memory of vUTS is reduced to 30 GB, vUTS can run properly and stably.



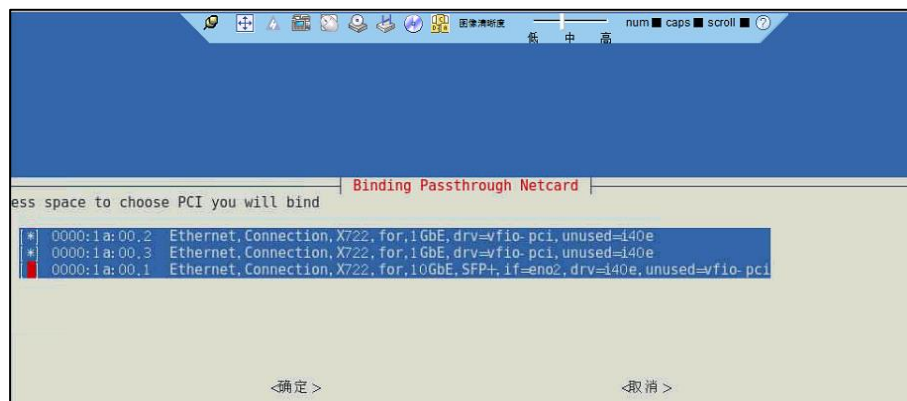
The latest automated deployment script has been updated to reserve sufficient memory for the host. If the problem continues to occur, it could be due to the host having additional memory requirements. You need to reduce the memory assigned to vUTS. If the problem persists, please contact NSFOCUS technical support personnel.

7.6 NICs Cannot Be Selected During Deployment

Description

During deployment, the normal page for selecting NICs is as shown in [Figure 7-3](#). If the screen size is very small, options marked with * may not be displayed.

Figure 7-3 NICs cannot be selected during deployment



Solution

Click **Cancel** to exit the deployment. Maximize the screen size of the execution environment and re-execute the **Autodeploy.sh** script.

7.7 The License Becomes Unavailable After UTS Redeployment

Description

Due to the strong connection between the license and the device hash, which is associated with the characteristics of vUTS, the hash will change after device redeployment. This will result in the license being unavailable.

Solution

Replace the image, and then the license will become available. If you use the automated deployment script to create a new vUTS, you need to prepare the license again.

7.8 An Error Message Appears When Using virsh to Connect to the vUTS Console

Description

When the **virsh console uts01** command is executed, an error message is displayed, as shown in [Figure 7-4](#).

Figure 7-4 Error message displayed when virsh is used to connect to the vUTS console

```
[root@uts UTS_V2.0_AUTO_DEPLOY_PACKGES]# virsh console uts01
Connected to domain uts01
Escape character is ^]
error: operation failed: Active console session exists for this domain
[root@uts UTS_V2.0_AUTO_DEPLOY_PACKGES]# █
```

Solution

The error message indicates that there is already a virsh console running. Run the following command to find the running process ID and kill it, and then run the **virsh console uts01** command to reconnect to the vUTS console, as shown in [Figure 7-5](#).

```
ps -ef | grep virsh | grep -v grep
```

Figure 7-5 Using virsh to reconnect to the vUTS console

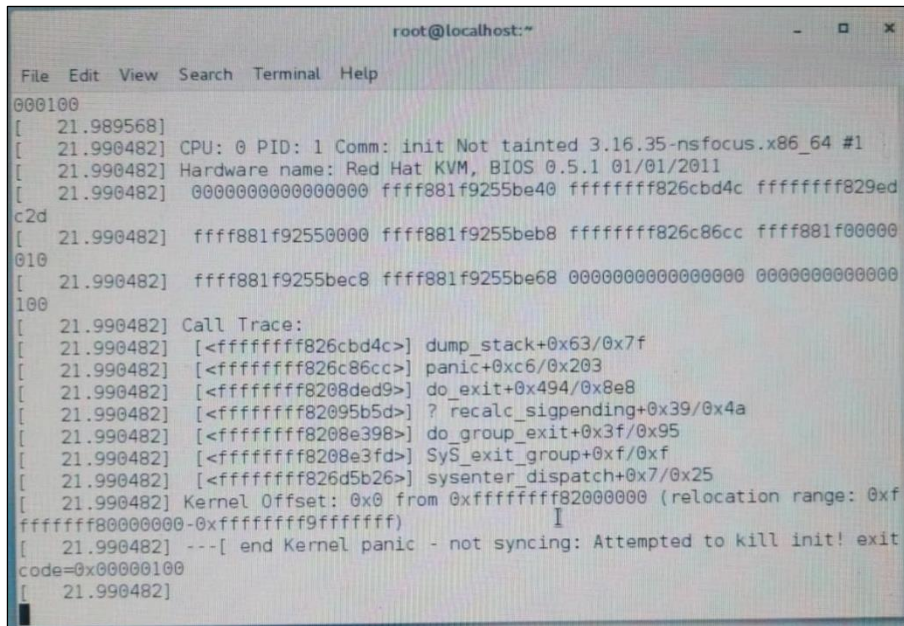
```
root@uts UTS_V2.0_AUTO_DEPLOY_PACKGES]# ps -ef |grep virsh
oot      5105  4904  0 12:47 pts/1    00:00:00 virsh console uts01
oot      6091  5929  0 13:33 pts/3    00:00:00 grep --color=auto virsh
root@uts UTS_V2.0_AUTO_DEPLOY_PACKGES]# kill -9 5105
root@uts UTS_V2.0_AUTO_DEPLOY_PACKGES]# virsh console uts01
onected to domain uts01
scape character is ^]
```

7.9 vUTS Fails to Start After the Host is Shut down and Relocated

Description

After UTS is shut down and relocated, start vUTS and attempt to log in the vUTS console, but an error message is displayed, as shown in [Figure 7-6](#).

Figure 7-6 vUTS fails to start after host shutdown and relocation



```

root@localhost:~#
File Edit View Search Terminal Help
000100
[ 21.989568]
[ 21.990482] CPU: 0 PID: 1 Comm: init Not tainted 3.16.35-nsfocus.x86_64 #1
[ 21.990482] Hardware name: Red Hat KVM, BIOS 0.5.1 01/01/2011
[ 21.990482] 0000000000000000 ffff881f9255be40 ffffffff826cbd4c ffffffff829ed
c2d
[ 21.990482] ffff881f92550000 ffff881f9255beb8 ffffffff826c86cc ffff881f00000
010
[ 21.990482] ffff881f9255bec8 ffff881f9255be68 0000000000000000 0000000000000
100
[ 21.990482] Call Trace:
[ 21.990482] [<ffffffffff826cbd4c>] dump_stack+0x63/0x7f
[ 21.990482] [<ffffffffff826c86cc>] panic+0xc6/0x203
[ 21.990482] [<ffffffffff8208ded9>] do_exit+0x494/0x8e8
[ 21.990482] [<ffffffffff82095b5d>] ? recalc_sigpending+0x39/0x4a
[ 21.990482] [<ffffffffff8208e398>] do_group_exit+0x3f/0x95
[ 21.990482] [<ffffffffff8208e3fd>] SyS_exit_group+0xf/0xf
[ 21.990482] [<ffffffffff826d5b26>] sysenter_dispatch+0x7/0x25
[ 21.990482] Kernel Offset: 0x0 from 0xffffffff82000000 (relocation range: 0xf
fffffff80000000-0xffffffff9fffffff)
[ 21.990482] ---[ end Kernel panic - not syncing: Attempted to kill init! exit
code=0x00000100
[ 21.990482]

```

Solution

- The error message indicates that vUTS has been damaged. You need to replace the vUTS image file.
- Before shutting down the host, shut down vUTS. Otherwise, it may cause damage to vUTS. Running the **virsh shutdown** command is the safest way to shut down vUTS.



The following high-risk operations may cause damage to UTS.

- Shutting down the host directly before shutting down vUTS.
- Running the **virtsh destroy** command to shut down vUTS.

7.10 Problems Regarding High-Performance Mode

This section describes problems regarding high-performance mode.

7.10.1 Failed to Bind a Transparent NIC

Description

The following error message is displayed when you bind a transparent NIC:

```
vfio-pci: probe of 0000:45:00.0 failed with error -22
```

Solution

After host installation is complete, enable virtualization in the BIOS. Different BIOS versions have varying **Settings** locations after startup. It is recommended that you review all available BIOS options and ensure options such as **Visualization**, **Direct IO**, and **Vt-d** are **enabled**.

After setup, restart the host and execute the following script to rebind the transparent NIC.

```
python AutoNic_bond.py
```

7.10.2 UTS Startup Error Caused by NIC Binding Failure

Description

When you attempt to start UTS after binding the NIC, an error message like "vfio pci bind failed" is displayed. Run the `dmesg |grep -i IOMMU` command, and find that the word "enabled" is displayed in the output.

Solution

A major cause for the problem is that not all virtualization options are enabled for the BIOS. To fix it, access the BIOS and set options such as **VT-x**, **VT-d**, **IOMMU**, and **Direct IO** (not case sensitive) to **enabled**.

If the problem persists, redeploy UTS in common mode when the user traffic is not greater than 2 Gbps.

7.10.3 NIC Models That Do Not Support High-Performance Mode

NIC models that support high-performance mode are listed in [Server Configuration Requirements](#), and however, there are many variations of these models. While some NIC variations claim to support high-performance mode, the transparent NIC binding failure may arise after deployment. Even if the host is restarted, the binding failure may persist.

Contact NSFOCUS technical support personnel to verify whether this type of NIC supports high-performance mode.

7.11 No Interface Traffic Is Detected and the CPU's Main Frequency Shows 0 After UTS Startup in Common Mode

After UTS is started in common mode, there is no interface traffic detected. Check the background, and find that the server process is not Up. The possible cause is the failure of the bridge NIC bound to UTS.

Solution

Step 1 Run the **brctl show** command on the host to check whether all bridge interfaces have been started.

Step 2 If only **br0** is Up, it can be determined that the configurations of other bridge interfaces fail. You can manually add them by running the following commands.

```
brctl addbr kkbr0      \\ kkbr0 represents the bridge interface name.
brctl addif kkbr0 ens15f1  \\ ens15f1 is the name of a physical NIC, indicating
which physical NIC the bridge interface is bound to.
ip link set kkbr0 up
ip link set ens15f1 up
brctl setageing kkbr0 0
```

Step 3 Restart UTS.

---End

8 NIC Operations After UTS Deployment

After UTS is deployed, there will be needs to add, replace, and unbind NICs. The following describes how to perform these operations in different deployment modes. Note that all of the following steps are performed on the host.

This chapter contains the following sections:

Section	Description
NIC Operations in High-Performance Mode	Describes NIC operations in high-performance mode.
NIC Operations in Common Mode	Describes NIC operations in common mode.

8.1 NIC Operations in High-Performance Mode

In high-performance mode, NICs on UTS perform transparent transmission through DPDK binding.

8.1.1 Adding an NIC

All of the following operations are performed on the host. Note that all the steps must be performed, without skipping any of them.

8.1.1.1 Shutting Down UTS

```
virsh shutdown uts01 //uts01 can be replaced with the actual uts name.
```

Note that if UTS cannot be shut down, run the following command to force a shutdown.

```
virsh destroy uts01
```

8.1.1.2 Binding an NIC

Navigate to the directory for initial deployment. By default, the path is `/home/UTS_V2.0_AUTO_DEPLOY_PACKGES`.

NSFOCUS Engineering Team provides the following two script files and one NIC interface information file.

```

dpdk_nic_bind.py          /* NIC binding tool*/
AutoNic_bond.py          /* Automatically bind the user-configured NIC
with the pci_info file.*/
pci.info                 /* NIC information that the user needs to
bind*/
Check_Nic.py            /* Check whether the NIC supports high-
performance mode.*/

```

Viewing NIC Binding Information

As shown in [Figure 8-1](#), the DPDK-compatible driver list contains transparently bound NICs, and the kernel driver list contains NICs available for binding in the server.

Figure 8-1 Viewing NIC binding information

```

[root@uts Bond_NIC]# ./dpdk_nic_bind.py -s
Network devices using DPDK-compatible driver
=====
0000:06:00.1 'I350 Gigabit Network Connection' drv=vfio-pci unused=igb
0000:82:00.0 'I350 Gigabit Network Connection' drv=vfio-pci unused=igb
0000:82:00.1 'I350 Gigabit Network Connection' drv=vfio-pci unused=igb

Network devices using kernel driver
=====
0000:01:00.0 'Ethernet Controller 10-Gigabit X540-AT2' if=eth8 drv=ixgbe unused=vfio-pci
0000:01:00.1 'Ethernet Controller 10-Gigabit X540-AT2' if=eth9 drv=ixgbe unused=vfio-pci
0000:04:00.0 'I350 Gigabit Network Connection' if=eth0 drv=igb unused=vfio-pci
0000:04:00.1 'I350 Gigabit Network Connection' if=eth1 drv=igb unused=vfio-pci
0000:04:00.2 'I350 Gigabit Network Connection' if=eth2 drv=igb unused=vfio-pci
0000:04:00.3 'I350 Gigabit Network Connection' if=eth3 drv=igb unused=vfio-pci
0000:06:00.0 'I350 Gigabit Network Connection' if=eth4 drv=igb unused=vfio-pci

```

Checking Whether the NIC to Be Added Supports Transparent Transmission (High-Performance Mode)

Run the following command to perform the `Check_Nic.py` script detection. If the script prompts that high-performance mode is not supported, the NIC cannot be added in high-performance mode.

```
[root@uts UTS_V2.0_AUTO_DEPLOY_PACKGES]# python Check_Nic.py `pwd` em1
```

Checking Whether the NIC Is Bound to a Network Bridge (Common Mode)

If the NIC you want to add has previously been bound to a network bridge, you need to unbind it from the network bridge first. For information on how to perform unbinding, see [Unbinding an NIC](#).

Adding NIC Information

Run the following command to add the NIC information to the `pci.info` file.

Note that the information format should be `domain:bus:slot.function`. Otherwise, an error message is displayed.

```

[root@uts UTS_V2.0_AUTO_DEPLOY_PACKGES]# vi pci.info
0000:06:00.1
0000:82:00.0
0000:82:00.1

```

Automatically Binding the NIC

Execute the `AutoNic_bond.py` script to auto bind the NIC.

```
[root@uts UTS_V2.0_AUTO_DEPLOY_PACKGES]# python AutoNic_bond.py
```

Checking Whether the NIC Is Successfully Bound

You can check whether the NIC is successfully bound, as shown in [Figure 8-2](#).

Figure 8-2 Checking whether the NIC is successfully bound

```
[root@uts Bond_NIC]# ./dpsk_nic_bind.py -s
Network devices using DPDK-compatible driver
=====
0000:06:00.1 'I350 Gigabit Network Connection' drv=vfio-pci unused=igb
0000:82:00.0 'I350 Gigabit Network Connection' drv=vfio-pci unused=igb
0000:82:00.1 'I350 Gigabit Network Connection' drv=vfio-pci unused=igb
```

Checking Whether the Transparent Device Is Successfully Added

After the NIC binding is complete, a corresponding character device is created and placed in the `/dev/vfio` directory. You can also view the corresponding NIC PCI information of the character device.

```
[root@uts ~]# ls -l /dev/vfio/
total 0
crw-----. 1 root root 241, 0 Mar 6 17:14 22
crw-----. 1 root root 241, 1 Mar 6 17:14 45
crw-----. 1 root root 241, 2 Mar 6 17:14 46
crw-rw-rw-. 1 root root 10, 196 Mar 6 17:14 vfio
[root@uts ~]# ls /sys/kernel/iommu_groups/22/devices/
0000:06:00.1
```

8.1.1.3 Restarting the Automatically Bound NIC

After the deployment is complete, theoretically speaking, there is an operation to restart the automatically bound NIC. You can check whether this operation exists and add it if it does not. Check whether the following command is contained in the `/etc/rc.local` file.

```
/usr/bin/python /home/UTS_V2.0_AUTO_DEPLOY_PACKGES/AutoNic_bond.py > /dev/null 2>&1
```

8.1.1.4 Modifying KVM Settings

```
virsh edit uts01
```

To add the `hostdev` node, add the following code:

```
<hostdev mode='subsystem' type='pci' managed='yes'>
  <driver name='vfio' />
  <source>
    <address domain='0x0000' bus='0x06' slot='0x00' function='0x1' />
  </source>
</hostdev>
```



Note

The domain, bus, slot, and function values are determined based on the added NIC. In the example mentioned above, those values are derived from the added NIC with the PIC address of **0000.06:00.1**.

If multiple NICs are to be added, you need to add multiple **hostdev** nodes.

8.1.1.5 Starting UTS

```
virsh start uts01
```

8.1.2 Unbinding an NIC

8.1.2.1 Shutting Down UTS

```
virsh shutdown uts01
```

Note that if UTS cannot be shut down, use the following command to force a shutdown.

```
virsh destroy uts01
```

8.1.2.2 Unbinding an NIC

Navigate to the directory for initial deployment. By default, the path is **/home/UTS_V2.0_AUTO_DEPLOY_PACKGES**.

Prepare two script files and one NIC interface information file as follows:

```
dpdk_nic_bind.py          /* NIC binding tool*/
pci.info                  /* Bind NIC information to this file*/
```

Viewing NIC Binding Information

As shown in [Figure 8-3](#), the DPDK-compatible driver list contains transparent bound NICs, and the kernel driver list contains NICs available for binding in the server.

Figure 8-3 Viewing NIC binding information

```
[root@uts Bond_NIC]# ./dpdk_nic_bind.py -s
Network devices using DPDK-compatible driver
=====
0000:06:00.1 'I350 Gigabit Network Connection' drv=vfio-pci unused=igb
0000:82:00.0 'I350 Gigabit Network Connection' drv=vfio-pci unused=igb
0000:82:00.1 'I350 Gigabit Network Connection' drv=vfio-pci unused=igb
Network devices using kernel driver
=====
0000:01:00.0 'Ethernet Controller 10-Gigabit X540-AT2' if=eth8 drv=ixgbe unused=vfio-pci
0000:01:00.1 'Ethernet Controller 10-Gigabit X540-AT2' if=eth9 drv=ixgbe unused=vfio-pci
0000:04:00.0 'I350 Gigabit Network Connection' if=eth0 drv=igb unused=vfio-pci
0000:04:00.1 'I350 Gigabit Network Connection' if=eth1 drv=igb unused=vfio-pci
0000:04:00.2 'I350 Gigabit Network Connection' if=eth2 drv=igb unused=vfio-pci
0000:04:00.3 'I350 Gigabit Network Connection' if=eth3 drv=igb unused=vfio-pci
0000:06:00.0 'I350 Gigabit Network Connection' if=eth4 drv=igb unused=vfio-pci
```

Unbinding an NIC

Execute the **dpdk_nic_bind.py** script to unbind the NIC and then bind the NIC information to the kernel.

```
[root@uts UTS_V2.0_AUTO_DEPLOY_PACKGES]# ./dpdk_nic_bind.py -u 0006:06:00.1
[root@uts UTS_V2.0_AUTO_DEPLOY_PACKGES]# ./dpdk_nic_bind.py -b ixgbe 0006:06:00.1
```

Delete the NIC information in the **pci.info** file.

```
[root@uts UTS_V2.0_AUTO_DEPLOY_PACKGES]# vi pci.info
0000-82: 00.0
0000-82: 00.1
```

Checking Whether the NIC Unbinding Is Successful

```
[root@uts UTS_V2.0_AUTO_DEPLOY_PACKGES]# ./dpdk_nic_bind.py -s
```

If the NIC information to be unbound is displayed in the network device using the kernel driver, it indicates that the unbinding is successful.

If the NIC information to be unbound is displayed in the network device using the DPDK-compatible driver, it indicates that the unbinding is failed.

8.1.2.3 Modifying KVM Settings

```
virsh edit uts01
```

To delete the **hostdev** node, delete the following code:

```
<hostdev mode='subsystem' type='pci' managed='yes'>
  <driver name='vfio' />
  <source>
    <address domain='0x0000' bus='0x06' slot='0x00' function='0x1' />
  </source>
</hostdev>
<address type='pci' domain='0x0000' bus='0x00' slot='0x0a' function='0x0' />
</hostdev>
```



The domain, bus, slot, and function values are determined based on the added NIC. In the example mentioned above, those values are derived from the added NIC with the PIC address of **0000.06:00.1**.

If multiple NICs are to be deleted, delete the corresponding multiple **hostdev** nodes.

8.1.2.4 Starting UTS

```
virsh start uts01
```

8.1.3 Replacing an NIC

When there is a need to replace an NIC, follow the steps below.

8.1.3.1 Unbinding the Old NIC

For details, see [Shutting Down UTS](#), [Unbinding an NIC](#), and [Modifying KVM Settings](#).

8.1.3.2 Replacing with a New NIC

Shut down the host and replace with a new NIC.

8.1.3.3 Binding the New NIC

For details, see [Adding an NIC](#).

8.2 NIC Operations in Common Mode

In common mode, the bridge NIC is used on UTS.

8.2.1 Adding an NIC

All of the following operations are performed on the host.

8.2.1.1 Shutting Down UTS

```
virsh shutdown uts01
```

Note that if UTS cannot be shut down, run the following command to force a shutdown.

```
virsh destroy uts01
```

8.2.1.2 Binding an NIC

Binding the NIC to a Bridge

Execute the following commands to bind the NIC **ens6f0** to the bridge **kkbr0**.

```
brctl addbr kkbr0
brctl addif kkbr0 ens6f0
ip link set ens6f0 up
ip link set kkbr0 up
brctl setageing kkbr0 0
```



- **kkbr0** is the bridge name, which is used to distinguish the previous bridge names where the last digit is incremented. **ens6f0** is the name of the newly added NIC.
- If the NIC name cannot be viewed, a possible cause could be that this NIC has been bound in high-performance mode and needs to be unbound first. For information on how to perform unbinding in high-performance mode, see [Unbinding an NIC](#).
- If multiple NICs need to be added in common mode, execute the above commands multiple times. Additionally, pay attention to the bridge names where the last digit is incremented.

Checking Whether the Binding Is Successful

Execute the following command to check whether the NIC is bound to the bridge **kkbr0**. The output is shown in [Figure 8-4](#).

```
brctl show
```


Figure 8-4 Checking whether the binding to a bridge is successful

```
[root@localhost ~]# brctl show
bridge name      bridge id                STP enabled  interfaces
br0              8000.0024ecf149b0       no          ens15f1
                vnet0
                vnet1
                vnet2
                vnet3
                vnet4
                vnet5
                vnet6
                vnet7
kkbr0            8000.000000000000       no
virbr0          8000.5254009d1242       yes         virbr0-nic
[root@localhost ~]# vi /etc/rc.local
```

8.2.1.3 Restarting Automatically Bound NICs

Add the commands described in [Binding an NIC](#) to the `/etc/rc.local` file to bind an NIC.

If multiple NICs are to be bound, you need to add all of them.

8.2.1.4 Modifying KVM Settings

```
virsh edit uts01
```

Add the following code to add the corresponding interface node.

```
<interface type='bridge'>
  <source bridge='kkbr0' />
  <model type='virtio' />
</interface>
```



Note

- **bridge** is the name of the network bridge, which can be added by adding the commands described in [Binding an NIC](#).
- If multiple NICs are to be added, add the corresponding multiple interface nodes.

8.2.1.5 Starting UTS

```
virsh start uts01
```

8.2.2 Unbinding an NIC

8.2.2.1 Shutting Down UTS

```
virsh shutdown uts01
```

Note that if UTS cannot be shut down, run the following command to force a shutdown.

```
virsh destroy uts01
```

8.2.2.2 Modifying KVM Settings

```
virsh edit uts01
```

Delete the following code to delete the corresponding interface node:

```
<interface type='bridge'>
<source bridge='kkbr0' />
<model type='virtio' />
<address type='pci' domain='0x0000' bus='0x00' slot='0x08' function='0x0' />
</interface>
```



Note

If multiple NICs are to be deleted, delete the corresponding multiple interface nodes.

8.2.2.3 Unbinding an NIC

Delete the commands described in section [Restarting Automatically Bound NICs](#) and added to the `/etc/rc.local` file. After deletion, restart the host.



Note

Only the commands required for unbinding the NIC should be deleted.

8.2.2.4 Restarting UTS

```
virsh start uts01
```

8.2.3 Replacing an NIC

When there is a need to replace an NIC, do as follows.

8.2.3.1 Unbinding the Old NIC

For details, see [Shutting Down UTS](#), [Modifying KVM Settings](#), and [Unbinding an NIC](#).

8.2.3.2 Replacing with a New NIC

Shut down the host and replace with a new NIC.

8.2.3.3 Binding the New NIC

For details, see [Adding an NIC](#).

9 Uninstalling UTS

To uninstall UTS, perform the following steps on the host:

Step 1 Obtain the name of vUTS to be uninstalled, as shown in [Figure 9-1](#).

```
virsh list --all
```

Figure 9-1 Obtaining the vUTS name

```
[root@localhost network-scripts]# virsh list --all
Id      Name                State
-----
1       uts_zcy              running
5       threat_probe        running
13      uts_5_14             running
-       mttest              shut off
-       threat01            shut off
-       uts_f04_x           shut off
-       uts_f05             shut off
-       uts_T015_5.94      shut off
-       uts_zj              shut off
```

Step 2 Find the path where the data disk and image files are stored.

```
virsh edit uts-name
```

An example is shown in [Figure 9-2](#):

- /home/taishi/UTS_V2.0_AUTO_DEPLOY_PACKGES/UTS_F01_1018.qcow2** is the image file path of uts01. (Note that the file with the drive letter **vda** is the vUTS image file.)
- /home/taishi/UTS_V2.0_AUTO_DEPLOY_PACKGES/data2.qcow2** and **/home/uts_wa_taishi.qcow2** are the data disk paths of uts01. (Note that the file with a drive letter such as **vdb** and **vdc** is the data disk file.)

Figure 9-2 Finding the path where the data disk and image files are stored

```

<devices>
  <emulator>/usr/libexec/qemu-kvm</emulator>
  <disk type='file' device='disk'>
    <driver name='qemu' type='qcow2' />
    <source file='/home/taishi/UTS_V2.0_AUTO_DEPLOY_PACKGES/UTS_
    F01_1018.qcow2' />
    <target dev='vda' bus='virtio' />
    <address type='pci' domain='0x0000' bus='0x00' slot='0x06' f
    unction='0x0' />
  </disk>
  <disk type='file' device='disk'>
    <driver name='qemu' type='qcow2' />
    <source file='/home/uts wa taishi.qcow2' />
    <target dev='vdb' bus='virtio' />
    <address type='pci' domain='0x0000' bus='0x00' slot='0x0a' f
    unction='0x0' />
  </disk>
  <disk type='file' device='disk'>
    <driver name='qemu' type='qcow2' />
    <source file='/home/taishi/UTS_V2.0_AUTO_DEPLOY_PACKGES/data
    2.qcow2' />
    <target dev='vdc' bus='virtio' />
    <address type='pci' domain='0x0000' bus='0x00' slot='0x0b' f
    unction='0x0' />
  </disk>
  <disk type='file' device='edrom'>

```

Step 3 Confirm the deployment mode of UTS.

```
virsh edit uts-name
```

If you can find the **hostdev** node in the configuration file, it indicates that UTS is deployed in high-performance mode; otherwise, it is deployed in common mode. As shown in [Figure 9-3](#), it indicates that UTS is deployed in high-performance mode.

Figure 9-3 Confirming the deployment mode

```

</graphics>
<video>
  <model type='cirrus' vram='16384' heads='1' primary='yes' />
  <address type='pci' domain='0x0000' bus='0x00' slot='0x02' f
  unction='0x0' />
</video>
<hostdev mode='subsystem' type='pci' managed='yes'>
  <driver name='vfio' />
  <source>
    <address domain='0x0000' bus='0x02' slot='0x00' function='
    0x1' />
  </source>
  <address type='pci' domain='0x0000' bus='0x00' slot='0x09' f
  unction='0x0' />
</hostdev>
<memballoon model='virtio'>
  <address type='pci' domain='0x0000' bus='0x00' slot='0x07' f
  unction='0x0' />
</memballoon>
</devices>

```

Step 4 Use the following command to shut down UTS.

```
virsh shutdown uts01 //Replace uts01 with the actual vUTS name
```

If UTS cannot be shut down, you can use the following command to force a shutdown:

```
virsh destroy uts01
```

Step 5 Unbind NICs.

Based on different deployment modes, unbind NICs as follows:

- High-performance mode
 - a. Access the installation and deployment directory. (By default, the path is `/home/UTS_V2.0_AUTO_DEPLOY_PACKGES`. Choose the directory according to the actual situation.)

```
cd /home/UTS_V2.0_AUTO_DEPLOY_PACKGES/
```

- b. Run the `vi AutoNic_bond.py` command to set unbinding. Find the content, as shown in the red frame in [Figure 9-4](#), change **b** to **u**, and then delete **vfio-pci**.

Figure 9-4 Modifying the binding script



```
print bond_list
# Bind an NIC
base_str = file_path+'dpmc_nic_bind.py -b vfio-pci'
for etem in bond_list:
```

- c. Execute the following command to unbind the NIC.

```
python AutoNic_bond.py
```

- Common mode

You can skip this step if UTS is deployed in common mode.

Step 6 Uninstall UTS.

```
virsh undefine uts-name
```

Step 7 (Optional) Delete the related files.

Delete all the data disk files. If you do not want to delete them, you can skip this step.

```
rm -rf image-file
rm -rf disk-file
rm -rf deployment-directory
```

Step 8 Restore the management interface configuration, as shown in [Figure 9-5](#).

- a. Access the directory where the host NIC configuration backup files are located: `cd /etc/sysconfig/network-scripts/data`
- b. Check backup status: `ll` command
- c. Choose the earliest backup date: `cd 20190218-12:38` (Choose the date according to the actual situation.)
- d. Overwrite current NIC configuration: `cp -rf * /etc/sysconfig/network-scripts/`
If a confirmation prompt appears, type **y**.
- e. Delete the configuration file of the network bridge: `rm -f /etc/sysconfig/network-scripts/ifcfg-br0`

Figure 9-5 Restoring management interface configurations

```
[root@localhost ~]# cd /etc/
[root@localhost data]# ll
total 132
drwxr-xr-x. 2 root root 4096 Mar  7 19:04 20190210-19:04
drwxr-xr-x. 2 root root 4096 Apr  8 19:22 20190408-19:22
drwxr-xr-x. 2 root root 4096 Apr 11 11:26 20190411-11:26
drwxr-xr-x. 2 root root 4096 Apr 11 11:30 20190411-11:30
drwxr-xr-x. 2 root root 4096 Apr 11 11:31 20190411-11:31
drwxr-xr-x. 2 root root 4096 Apr 11 11:33 20190411-11:33
drwxr-xr-x. 2 root root 4096 Apr 11 11:37 20190411-11:37
drwxr-xr-x. 2 root root 4096 Apr 11 11:38 20190411-11:38
drwxr-xr-x. 2 root root 4096 Apr 11 11:41 20190411-11:41
drwxr-xr-x. 2 root root 4096 Apr 11 12:07 20190411-12:07
drwxr-xr-x. 2 root root 4096 Apr 11 12:11 20190411-12:11
drwxr-xr-x. 2 root root 4096 Apr 11 12:35 20190411-12:35
drwxr-xr-x. 2 root root 4096 Apr 11 12:44 20190411-12:44
drwxr-xr-x. 2 root root 4096 Apr 11 12:48 20190411-12:48
drwxr-xr-x. 2 root root 4096 Apr 11 13:30 20190411-13:30
drwxr-xr-x. 2 root root 4096 Apr 16 10:56 20190416-10:56
drwxr-xr-x. 2 root root 4096 Apr 16 10:57 20190416-10:57kkbak
```

Step 9 Delete UTS configurations in the `rc.local` file.

Run the `vi` command to edit the boot file `/etc/rc.local`, delete the following configurations, and then run the `wq` command to save the change.

- a. Delete the management interface bridge configuration.

Find the configuration statement related to `br0` and delete it, as shown in the following example:

```
/usr/sbin/brctl addif br0 ens15f0
```

- b. Delete working interface binding configuration based on different deployment modes.
 - High-performance mode

Find the configuration statement related to `AutoNic_bond.py` and delete it, as shown in the following example:

```
/usr/bin/python /home/UTS_V2.0_AUTO_DEPLOY_PACKGES/AutoNic_bond.py > /dev/null
2>&1
```

- Common mode

Find the configuration statement related to `brctl` and delete it, as shown in the following example:

```
brctl addbr kkbr0
brctl addif kkbr0 ens16f3
ip link set ens16f3 up
ip link set kkbr0 up
brctl setageing kkbr0 0
```

If there are multiple similar statements, delete the ones related to UTS NICs.

Step 10 Restart the host.

```
reboot
```

----End

A

Default Parameters

Default parameters include initial settings of the management interface and initial accounts of various login methods.

A.1 Initial Settings of the Management Interface

IP address (M interface)	192.168.1.1
Netmask	255.255.255.0

A.2 Default Accounts

Role	User Name	Password
Super administrator	admin	admin2022.Uts
Auditor	auditor	auditor2022Uts.
Console administrator	conadmin	conadmin
SSH administrator	Contact NSFOCUS technical support for the user name and password of the SSH administrator, and use SSH management under the guidance of the technical support personnel.	

A.3 Communication Parameters of the Console Port

Baud Rate	115200
Data Bits	8