MSFOCUS

NSFOCUS vUTS (VMware)

Deployment Guide



Version: V2.0R00IB05 (2023-09-25)

Confidentiality: RESTRICTED

© 2023 NSFOCUS

■ 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	3
1 Deployment Scenarios and Requirements	5
1.1 Deployment Scenarios	5
1.2 Environment and Hardware Requirements	6
2 Obtaining the Image File	7
3 Creating vUTS and Importing the Image File	8
4 Adding a Working Interface (NIC Passthrough Mode)	10
4.1 Setting NIC Passthrough for the Working Interface	10
4.2 Modifying vUTS Configuration	
4.2.1 Editing vUTS	
4.2.2 Adding a Hard Disk	
4.4. Adding/Deleting an NIC	
4.5. Starting vUTS	
5 Adding a Working Interface (NIC Bridge Mode)	14
5.1 Viewing Physical NICs	14
5.2 Adding a Standard Virtual Switch	14
5.3. Adding an Interface Group	
5.4. Configuring vUTS and Adding a NIC	
5.5 Starting vUTS	

Preface

This document describes the installation and deployment of NSFOCUS Unified Threat Sensor (UTS for short) on Vmware.

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 Deployment Scenarios and Requirements	Describes vUTS deployment scenarios and VMware environment requirements as well as hardware requirements.
2 Obtaining the Image File	Describes how to obtain the image file.
3 Creating vUTS and Importing the Image File	Describes how to create vUTS on VWware and import the image file.
4 Adding a Working Interface (NIC Passthrough Mode)	Describes how to add a working interface using an NIC in passthrough mode.
5 Adding a Working Interface (NIC Bridge Mode)	Describes how to add a working interface using an NIC in bridge mode.

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.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply

Convention	Description
	values are in italic font.
Note	Reminds users to take note.
C 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.
W arning	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 Deployment Scenarios and Requirements

There are two vUTS deployment scenarios.

1.1 Deployment Scenarios

The two deployment scenarios are as follows:

• Scenario 1: monitoring traffic of internal virtual machine assets (including internal lateral attack traffic).



• Scenario 2: monitoring traffic of external assets (same as the deployment on KVM)



1.2 Environment and Hardware Requirements

Item	Description
Environment requirements	WMware ESXi 6.0 and later
Hardware requirements	> 8 CPUs, > 16 GB memory

2 Obtaining the Image File

The image file **V2.0R00IB05.36584.ova** for installing vUTS on VMware is stored on the FTP server of NSFOCUS Engineering Team. Please contact NSFOCUS technical support to obtain the image file.

Remote site: /product_install/IIS/UTS/UTS_IB05 -? VADS-M -? VMWAF -? VNTA -? WAF -? LAS					
-? NF-WAN					
Filename	Filesize	Last modified	Permissio	Owner/Group	
С ТЕМР		11/3/2023 3:46:00 AM	drw×r-×r-×	1000 1000	
NSFOCUS UTS V2.0R00F05 User Guide.docx	3,044,680	10/13/2023 12:46:00 AM	-nw-rr	1000 1000	
UTS_IB05_READY_WORLD_x86_0922.qcow2	4,654,039,040	10/12/2023 9:13:00 PM	-rw-rr	1000 1000	
Z20210428UTS_V2.0_AUTO_DEPLOY_PACKGES.tar	52,848,640	10/13/2023 1:16:00 AM	-rw-rr	1000 1000	
20231026UTS V2.0 AUTO DEPLOY_PACKGES.tar	52,858,880	10/26/2023 8:53:00 PM	-nw-rr	1000 1000	
V2.0R00IB05.36584.ova	6,967,223,808	10/21/2023 2:17:00 AM	-rw-rr	1000 1000	
MD5.5t	160	10/21/2023 1:22:00 AM	-rw-rr	1000 1000	
Selected 1 file. Total size: 6,967,223,808 bytes					

3 Creating vUTS and Importing the Image File

To create vUTS and import the image file, follow these steps:

- Step 1 Select Create/Register VM.
- Step 2 On the Select creation type page, select Deploy a virtual machine from an OVF or OVA file and click Next.

1 New virtual machine		
Select creation type Select OVF and VMDK files Select storage License agreements Deployment options Additional settings Ready to complete	Select creation type How would you like to create a Virtual Machine? Create a new virtual machine Deploy a virtual machine from an OVF or OVA file Register an existing virtual machine	This option guides you through the process of creating a virtual machine from an OVF and VMDK files.
vm ware		
		Back Next Finish Cancel

Step 3 On the Select OVF and VMDK files page, type a unique name for vUTS. Select the image file and import it.



Step 4 Leave all options at their default values.

----End

4 Adding a Working Interface (NIC Passthrough Mode)

4.1 Setting NIC Passthrough for the Working Interface

Choose **Manage** > **Hardware** > **PCI Devices**. Select an unused NIC and click **Toggle passthrough** to enable passthrough mode. Then restart the host to make the settings take effect.

Navigator	localhost.localdomain	n - Manage							
Host	System Hardware	Licen	sing	Packages	Services Security & users				
Manage Monitor	PCI Devices		8	2 Toggle passthroug	h 🥒 Configure SR-IOV 🦯 Hardware label 🔹 💦 Reboot host	C Refresh	Q Searc	ch	
🕶 🔂 Virtual Machines 🛛 36	Power Management			Address 🗸	Description v	SR-IOV 🗸	Passthrough -	Hardware 🗸	
▼					0.00:00:0000	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D DMI2	Not capable	Not capable	
Monitor				0000:00:01.0	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D PCI	Not capable	Not capable		
⋆ B uts_gjh1				0000:01:	Broadcom MegaRAID SAS Invader Controller	Not capable	Disabled		
Monitor				0000:00:02.0	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D PCI	Not capable	Not capable		
More VMs				0000:02:	Intel(R) 82599 10 Gigabit Dual Port Network Connection	Disabled	Disabled		
Storage				0000:02:	Intel(R) 82599 10 Gigabit Dual Port Network Connection	Disabled	Active		
				0000:00:03.0	Intel Corporation Xeon E7 v4/Xeon E5 v4/Xeon E3 v4/Xeon D PCI	Not capable	Not capable		
Monitor More storage			Q	uick filters	~			207 item	
Networking									

4.2 Modifying vUTS Configuration

4.2.1 Editing vUTS

Select vUTS and right-click it to select Edit Settings. You can modify vUTS settings.

IIIware	🚰 uts_gjh1						000@10.07.3.21	a.∢ ∣ neip.≁	Q Search	
T Navigator	Power	•								
✓ ☐ Host Manage	Guest OS Snapshots	le 🔠 Monitor 🕨 Power	on 🔲 Power of	f 🔢 Suspend 👩 Restart		🖊 Edit 🛛 🧲 Refresh	Actions			
Monitor	Console		s_gjh1 est OS	Other Linux (64-bit)					CPU 0 MHz	
✓ B Virtual M ✓ B uts_1	Autostart	VMM CPU	npatibility ware Tools Js	No 8					MEMORY 0 B	-
Monii • 📑 uts_c Monii	 Export Export With Images 	Mor	nory	16 GB					STORAGE 108.66 GB	
More - 🗐 Storage	Edit settings	ware Tools is not installed in rations on the quest OS, e.g. s for this virtual machine	this virtual mach graceful shutdov	ine. VMware Tools allows de vn, reboot, etc. You should i	etailed install	l guest information to be d I VMware Tools. 🙀 Actio	displayed as we ns	ll as allowing y	ou to perform	×
✓ ☐ data: Moni*	Edit notes	al Information				✓ Hardware Configuration	on			
More	Kename	tworking				P CPU	8	vCPUs		
Networki	Answer question	Iware Tools	VMware Tools is	not installed. 🏠 Actions		Memory	1	6 GB		
	Diregister	orage	2 disks			Hard disk 1	1	6 GB		
		tes		🥖 Edit notes		Hard disk 2	1	00 GB		
	Help				J	USB controller	L	JSB 2.0		
	in a new window	sks								

4.2.2 Adding a Hard Disk

You can expand Hard Disk Drive 2 (which is 20 GB by default) or add more hard disks according to the on-site requirements.

To edit a hard disk, follow these steps:

- Step 1 Select vUTS and right-click it to select Edit Settings.
- Step 2 Click Add hard disk and configure the new hard disk.

Note that you should set the **Bus type** for the hard disk to **IDE**.



NSFOCUS vUTS (VMware) Deployment Guide



📴 Edit settings - uts_gjh1 (ESXi 7.0 U1 v	virtual machine)				
Virtual Hardware VM Options					
Add hard disk 🔳 Add network ada	apter 🛛 📃 Add o	other device	9		
► 🔲 CPU	8 ~ (
Memory	16	GB	~		
▶ 🚍 Hard disk 1	16	GB	~		\otimes
▶ 🚍 Hard disk 2	100	GB	~		8
SCSI Controller 0	LSI Logic Par	allel			8
🚭 USB controller 1	USB 2.0			~	\otimes
Metwork Adapter 1	VM Network			✓ Connect	\otimes
					Save Cancel

🔂 Edit settings - uts_gjh1 (ESXi 7.0 U1 v	irtual machine)
Disk File	[datastore1] gjhgjh/UTS_IB05_READY_WORLD_x86_0922_thin.vmdk
Shares	Normal ~ 1000 ~
Limit - IOPs	Unlimited ~
Controller location	SCSI controller 0 ~ SCSI (0:0) ~
Disk mode	Dependent ~
Sharing	None V i Disk sharing is only possible with eagerly zeroed, thick provisioned disks.
▼ 🖾 Hard disk 2	100 GB ~
Maximum Size	25.12 TB
-	
	Save Cancel

4.4. Adding/Deleting an NIC

You can add or delete network interface cards (NICs) according to the on-site requirements. A minimum of three NICs are required, with the first two serving as management interfaces.

For working interfaces, click **Add other device** to add a new PCI device. Then configure NIC passthrough. For details, see Setting NIC Passthrough for the Working Interface.

🔁 Edit settings - uts_gjh1 (ESXi 7.0 U1 virtual machine)				
Virtual Hardware VII Options				
🔜 Add hard disk 🛛 🛤 Add network ad	apter 📃 Add other device			
+ 🔲 CPU	8 ~ ()			
► Memory	16 GB ~			
▶ 🛄 Hard disk 1	16 GB ~	۲		
+ 🛄 Hard disk 2	100 GB ~	8		
SCSI Controller 0	LSI Logic Parallel	8		
🔁 USB controller 1	US8 2.0 V	۲		
Network Adapter 1	VM Network VI Connect	\otimes		
Network Adapter 2	test 🗸 🗸 Connect	8		
Network Adapter 3	test 🗸 🗸 Connect	8		
▶ 🎯 CD/DVD Drive 1	Host device V Connect	0		
▶ 🗐 Video Card	Default settings V			
► Kew PCI device	82599 10 Gigabit Dual Port Network Connection - 0000:02:00.0 🗸	۲		



4.5. Starting vUTS

After the deployment is complete, start vUTS.

Note that VMware may take some time to load on this page during the initial start-up process. Please be patient and wait.

GRUB Loading stage1.5. Bootloader loading, please wait Press any key to continue. Press any key to continue. Press any key to continue. Press any key to continue. Press any key to continue. -	GRUB Loading stage1.5. Bootloader loading, please wait Press any key to continue. Press any key to continue. Press any key to continue. Press any key to continue. Press any key to continue.			
Bootloader loading, please wait Press any key to continue. Press any key to continue. Press any key to continue. Press any key to continue. Press any key to continue. -	Bootloader loading, please wait Press any key to continue. Press any key to continue. Press any key to continue. Press any key to continue. Press any key to continue. -	GRUB Loading stage1.	5.	
Bootloader loading, please wait Press any key to continue. Press any key to continue. Press any key to continue. Press any key to continue. Press any key to continue. -	Bootloader loading, please wait Press any key to continue. Press any key to continue. Press any key to continue. Press any key to continue. Press any key to continue. -			
Press any key to continue. Press any key to continue. Press any key to continue. Press any key to continue. Press any key to continue. -	Press any key to continue. Press any key to continue. Press any key to continue. Press any key to continue. Press any key to continue. -	Bootloader loading,	please wait	
Press any key to continue. Press any key to continue. Press any key to continue. Press any key to continue. -	Press any key to continue. Press any key to continue. Press any key to continue. Press any key to continue. -	Press any key to con	ntinue.	
Press any key to continue. Press any key to continue. Press any key to continue. -	Press any key to continue. Press any key to continue. Press any key to continue. -	Press any key to con	ntinue.	
Press any key to continue. Press any key to continue. -	Press any key to continue. Press any key to continue. -	Press any key to con	ntinue.	
Press any key to continue. -	Press any key to continue. -	Press any key to cor	ntinue.	
-	_	Press any key to con	ntinue.	

5 Adding a Working Interface (NIC Bridge Mode)

Ensure that at least one physical NIC is not set to passthrough mode.

5.1 Viewing Physical NICs

Choose Networking > Physical NICs to view physical NICs availale.

Ta Navigator	C localiosLlocaldomain - Networking				
✓ ☐ Host Manage Monitor	Port groups Virtual switches Physical NICs ✓ Edt settings C Refresh © Actions	Vilkemel NICs TCP/IP stacks Firewall rules			Q Search
▼	Name ~	Driver ~	MAC address ~	Auto-negotiate ~	Link speed
+ 👸 uts_f05aaaaaaaaa	Jun vmnic0	Mill igbn	3cecef80.a3.ec	Enabled	1000 Mbps, full duplex
Monitor	per vmnic1	Mill igbn	3cecef80:a3:ed	Enabled	100 Mbps, full duplex
→ B uts_gjh1	Mill vmnic3	mill ingben	18:c0.4d:b8:1f.6b	Enabled	Link down
Monitor	JEE vmnic4	jem igbn	18:c0.4d:ba:66:12	Enabled	1000 Mbps, full duplex
More VIIIs	MM vmnic5	MM igbn	18:c0:4d:ba:66:13	Enabled	1000 Mbps, full duplex
* 🗐 Storage 📃 1	He vmnic6	MM igbn	18:c0:4d:ba:66:14	Enabled	1000 Mbps, full duplex
 datastore1 	HE vmnic7	MM igbn	18:c0:4d:ba:66:15	Enabled	1000 Mbps, full duplex
Monitor					7 item
More storage					

5.2 Adding a Standard Virtual Switch

Choose **Networking** > **Virtual Switches**. Type a vSwitch name. Select the physical NIC for the **Uplink** field and select **Accept** for the **Promiscuous Mode** field.

Add standard virtual switch - New switch Switch Name New switch MTU 1500 @ Uplink 1 vmnic4 - Up, 1000 mbps • Link discovery Click to expand • Security Promiscuous mode • Accept @ Reject MAC address changes MAC address changes Accept @ Reject Accept @ Reject Add Cancel	1	1
Mduplink VSwitch Name New switch MTU 1500 Uplink 1 vmnic4 - Up, 1000 mbps • Link discovery Click to expand • Security Security Promiscuous mode Accept ● Reject MAC address changes Accept ● Reject Forged transmits Accept ● Reject	🔚 Add standard virtual switch - New sw	vitch
vSwitch Name New switch MTU 1500 Image: Security Link discovery Click to expand Security Promiscuous mode Promiscuous mode Accept Image: Reject MAC address changes Accept Image: Reject Forged transmits Image: Accept Image: Reject Add Cancel	🚟 Add uplink	
MTU 1500 Image: Security Link discovery Click to expand Security Image: Security Promiscuous mode Image: Accept Image: Security MAC address changes Image: Accept Image: Security Forged transmits Image: Accept Image: Security	vSwitch Name	New switch
Uplink 1 vmnic4 - Up, 1000 mbps Image: Constraint of the second of	MTU	1500 🗘
Link discovery Click to expand Security Promiscuous mode Promiscuous mode Image: Accept Image: A	Uplink 1	vmnic4 - Up, 1000 mbps 🗸 🖉
Security Promiscuous mode Accept Accept Reject Forged transmits Accept Reject Add Cancel	Link discovery	Click to expand
Promiscuous mode	✓ Security	
MAC address changes O Accept O Reject Forged transmits O Accept O Reject Add Cancel	Promiscuous mode	O Accept O Reject
Forged transmits Accept Reject Add Cancel	MAC address changes	O Accept O Reject
Add Cancel	Forged transmits	O Accept O Reject
Add Cancel		
		Add Cancel

5.3. Adding an Interface Group

Choose **Networking** > **Virtual Switches**. Type an interface group name and select the newly created standard virtual switch.

🕺 Add port group - New port group	
Name	New port group
VLAN ID	0 🗘
Virtual switch	vSwitch0 ~
✓ Security	
Promiscuous mode	O Accept O Reject O Inherit from vSwitch
MAC address changes	O Accept O Reject O Inherit from vSwitch
Forged transmits	O Accept O Reject O Inherit from vSwitch
	Add Cancel

5.4. Configuring vUTS and Adding a NIC

Select vUTS and right-click it to select **Edit Settings**. Click **Add network adapter**, and select E1000 as the NIC adapter.

🖆 Edit settings - uts_gjh1 (ESXi 7.0 U1 vi	rtual machine)		
Virtual Hardware VM Options			
Add hard disk 🛤 Add network ad	apter 🔚 Add other device		
CPU	8 ~ ()		
► Memory	16 GB ~		
▶ 🛄 Hard disk 1	16 GB ~		\otimes
▶ 🛄 Hard disk 2	100 GB ~		\otimes
SCSI Controller 0	LSI Logic Parallel		\otimes
SB controller 1		\checkmark	\otimes
Network Adapter 1	VM Network	V Connect	8
Network Adapter 2	test	✓ Connect 2	8
Real Network Adapter 3	test	Connect	
New Network Adapter	666	✓ Connect	8
> i CD/DVD Drive 1	Host device	✓ □ Connect	\otimes
· • • • • • • • • • • • • • • • • • • •			
			Save Cancel

5.5 Starting vUTS

After the deployment is complete, start vUTS.

