

Sangfor Cyber Command Deployment Guide

Version:

Cyber Command 3.0.50C

Released On: 2021-4-29

Sangfor Technologies Inc.



Copyright © Sangfor Technologies Inc. 2021. All rights reserved.

Sangfor Technologies Inc. (hereinafter referred to as "Sangfor") and its affiliates reserve all intellectual property rights (including but not limited to copyrights, trademark rights, patent rights, and trade secrets) and related rights of text, images, pictures, photographs, audios, videos, charts, colors, layouts, etc. contained in or related to this document and its contents, unless otherwise stated or authorized by Sangfor. Without the prior written permission of Sangfor, this document and its content shall not be reproduced, forwarded, adapted, modified, displayed or distributed, or otherwise used by any means for any purpose.

Disclaimer

The products, services or features you purchase shall be subject to the commercial contract and terms of Sangfor. Products, services or features described in this document, whether wholly or in part, may not be purchased or used by you. Unless otherwise provided in the contract, Sangfor disclaims warranties of any kind, either express or implied, for the content of this document.

Due to product deployment or other reasons, the content of this document will be updated from time to time. Unless otherwise agreed, this document is only used as a guide, and all statements, information, and suggestions in this document do not constitute any express or implied warranties.

Preface

About This Document

This document introduces how to deploy Cyber Command 3.0.50C.

Product Version

Product	Version
Cyber Command	3.0.50C

This document will be updated when configuration is changed in new versions.

Intended Readers

- Network design engineer
- O&M personnel

Revision History

The revision history includes each document update. The latest document version contains updates from all previous document versions.

Version	Released On	Description
01	2021-4-29	This is the first release of this document.

Technical Support

Email: support@sangfor.com

Official Community: community.sangfor.com

International Service Centre: +60 127-117-129(7511)

Official Website: www.sangfor.com

Feedback

•

If you have any suggestions or comments for this document, you are welcomed to contact us in the following ways:

Sangfor Community: https://community.sangfor.com

- Contact local Sangfor office
- After-Sales Support: +60 127-117-129(7511)

Content

Prefacei
Contentiv
1. Overview
1.1. About This Version
1.1.1. What Is New
1.1.2. Others
1.1.3. Connection with Third-Party Products
1.2. Deployment Impacts
1.2.1. Impacts on Business
1.2.2. Impacts on O&M
1.2.3. Impacts on Network
1.2.4. Others
1.3. Deployment Preparation Related to Customers
1.3.1. Resources Required for Deployment
1.3.2. Deployment Notification
1.4. Deployment Process
1.5. Business Verification After Deployment
1.6. Rollback
2. Deployment Instruction
2.1. Preparation Before Deployment
2.1.1. Deployment Tools
2.1.2. Deployment Environment
2.1.3. Customer Resources
2.2. Confirmation Before Deployment
2.3. Deployment Procedure
2.3.1. Deployment Procedure

2.4. Check After Deployment	34
2.4.1. Platform Check	34
2.4.2. Business Verification	34
2.5. Handling of Upgrade Failure	35
2.6. Rollback	36

1. Overview

1.1. About This Version

1.1.1. What Is New

•New: The Licensing module is reconstructed.

The administrator can export the device inofo and send it to the device supplier to obtain the offline license key file

1. Go to the Licensing module, export and save the device information.



2. Send the device information file to device supplier and you can receive the license file.

3.Go to Licensing module on Cyber Command, and import the obtained license file to get licensed.

🕑 Cyber Com	man	nd (1055) Home Response Detection Assets	Reports More =	- 0
< 1/2 >		© Err	ror connecting to devices. Please check for network connectivity issues. Details	
System	«	Licensing		
Correlated Devices	>	Activation		
l System	~	1 Get Device Info	Apply License Key File Import License Key File	
Admin Account		Click the button below to get device information.	Send the Device Info file from step 1 to your device supplier to receive the license key file.	implete licensing.
Licensing		Export Device Info	Import	
Network General Logging Options ⊉ Update ∛ Maintenance 12 Databases	>	I Basics Satua: ^O Uniformand Device ID: CBAE(917 Type: - Usen - Version: 3.0.50 Model: -		
		Basic Licenses Pattorm Ucense Pattorm Ucense Database and Cyber Comm. Expiration Date: - Ifunction Module Licenses	Software Upgrade License Keys second gets dates: Epiration Date: -	

•New: This version can be deployed on VMware ESXi.

This version can be deployed on VMware EXSi by using Cyber Command 3.0.50C iso file.

•New: Two-factor authentication

When logging in, users not only need to enter their password and CAPTCHA, but also need to verify OTP.

1.To set up OTP for the super admin, go to **System** > **Admin Account**, and edit the admin account.

Then, choose "Password+OTP" as the authentication policy, enter the administrator password and set up OTP authentication.

No. Userna	ame ‡	Description	Edi	Required	××	Owner	Status ①	¢ Op	peration
1 admin 1. edi	it account	admin	Correction Policy Correction Policy Correction Policy Correction Policy Correction Policy Paddress:	To enable OTP authentication, administ password is required.	trator 0 put admin passwo cancel 0 ssion Z.select p	- rd assword + OTP	~	Ch	ange Password
				ОК	Cancel				

System	**	Admin Account						
Correlated Devices		+ New 30 Delete 🗸 5	nable 🚫 Disable 🥂 Refresh	C Login Management				
System		🗌 No. Usemame	2 Description	Set up OTP Authentication	×	Owner	Status ①	: Operation
Admin Account		- 1 edmin	admin	Steps:			~	Change Password
Licensing		🗆 2 Luke		 Install Authentication App Install Google Authenticator on your mobile device. 			~	Reset Password Delete
Network				③ Get Verification Code After Google Authenticator is installed, use it to scan the follo code, or enter the secret key to get a verification code.	sing QR			
Logging Options								
In Update								
S Maintenance				state Verification Code				
🗄 Databases				Google Authenticator Verification Code				
				Hease make use the system time is consistent with the ter- por device.Carrent typican Time.2021-04-55,000.02 (i) Constrained to set your and address in case pure of noise the writication cade via your mobile planes. (i)	e on innot Cancel			
								6

1. When logging in, a super admin not only needs to enter the password and CAPTCHA, but also needs to verify OTP generated by Google Authenticator.

	S	NGFOR SECURITY	€ +60 127117511(7129)
 Cyber Command			
	OTP Authentication x For security, please enter your OTP verification code. * Verification Code Oragie Automaticator Verification Code Please make sure the system time is consistent with the time on your device. Current System Trace 2014-023 10018 () Trianomandade to air system enail address in case you cannot income the synthesis code system that address in Code State Code Carlos Code) Trianomandade to air system enail address in case you cannot income the synthesis code system that address in Code State Code Carlos Code) Trianomandade to air system code address in Code Code State State Code Code Code Code) Trianomandade to air system code address in Code Code Code Code Code Code Code Code	Userane admin Passed	
	Case	Long In John John John John John John John John	4/3

•New: Import certificate

Import a certificate to solve loss and theft of the data transmitted by the browser.

System	**	General		
Correlated Devices	>	Web UI Ma	I Server () SMS Service S	ystem Time Certificati
System	U.	I Import Certifica	te	
Admin Account		Type:	PFX	•
Licensing		Certificate:	PFX	Browse
Network		* Password:	P12 .crt+.key	0
General		() Successfully	PEM	
Logging Options		server and re during that ti	fresh the page. The platform cannot be u ime	sed
1 Update	\rightarrow	in an anna AnaAn		
A Maintenance	>			
Databases	>			

•New: Connect FortiGate

Block access from risky IP addresses for more security.

1. Go to the Correlated Devices page and add a FortiGate device.

Cyber Con	nmar	nd @78333 Home Response De	etection Asset	s Reports	More				Holisti	• •	😫 admin	đ
System		Correlated Devices										
Correlated Devices	~	C Refresh		New		×	1					
Correlated Devices		Total Logs (today): 89507 0 Sangfor devices license	d. 15 licenses remaining									
Monitor System	,	STA • Online: 1 • Offline: 2	Endpoint • Online: 0	* Device IP: * Device Name:	FortiGate	0	IAM • Connecter	ed: 0 • Offline: 0	BBC • Online	• • • •	Hine: Q	
1 Update	3	Today's Synced Logs: 89k	Today's Synced Logs	Type:	Internet Access Management Endenlet Secure		N/A (sync not supp	ported)	N/A (sync not su			
🖏 Maintenance	>			SSL VPN								
🗄 Databases		+ New X Delete C Refresh			Wireless Access Controller Branch Business Center					Search		
		No. Name (IP Address) : Type :	IP Address I V		O FortiGate		fotal Synced Logis Tod	lay's Logs Last Synced 3	Status 🗧 Ale	rts (30 days) :	Operation	
	1 SANGFOR TS (10.22 Stealthy Thr	10.222.128.178 TS		Q STA, NGAF, FTA, Visioner, and Heat Security can be connected without being configured		17.77MB	0 2021-04-28 23:43:31	 Nor 	0)	Traffic Deta	ils.	
		2 SANGFOR STA (10.2. Stealthy Thr	10.222.88.180 11		on Cyber Command: Connecting Endpoint Secure or DAS needs to esable port 7443.		5.02M8	0 2021-04-26 21:30:57	• 08_		Details	
		3 SipDataPlatform (10 Stealthy Thr	*Username (): admin			58.16MB	0 2021-04-26 19:50:06	• off	2	Details		
				" Auth Password 🕢		1						
				Remarks:								
					OK Cance	el						
												6
										entries =	1.	C

2. Go to the Response page and set response policies

Cyber Command 3.0.50C Deployment Guide

(E	Home	Res	ponse Det	ection Assets	Reports Mo	re ⊨ ≡				•	Holistic	- 🕒 e adm	nin +
Response «	Re	sponse P	olicies		New	add resp	onse policies				×				
E Risky Servers	+	New	🗙 Delete 👘 🗸	Enable										Search	
🖵 Risky Hosts	Po	licy Sour	ce: All Pr	edefine	Conditions			Response							ΰB
E Risky Security Domains		No.	Name	Арр	Schedule:	O Always	Custom					Time Updated	Status	Operation	in
		1	Botnet	IP G	* Name:	Test					0	2019-10-16 23:32:57	Disabled	Enable	Delete
Response Policies		2	Trojan	IP G	Groups :	All					•	2019-10-16 23:32:57	Disabled	Enable	Delete
E Fix History		з	Worm	IP G	* Confidence				0.1			2019-10-16 23:32:57	Disabled	Enable	Delete
		4	Virus	IP G	Excel Trace	Compromised		-9-1-				2019-10-16 23:32:57	Disabled	Enable	Delete
		5	Blended Attack	IP G	Event Types	Malware						2019-10-16 23:32:57	Disabled	Enable	Delete
		6	Code Injection	IP G		Botnet	Trojan	Worm	Virus	Elended Attack		2019-10-16 23:32:57	Disabled	Enable	Delete
		7	Cryptomining	IP G		Code Injection	Cryptomining	Ransomware	Other Malicious Pr			2019-10-16 23:32:57	Disabled	Enable	Delete
		8	Ransomware	IP G		Cyber Attack	Cyber Attack					2019-10-16 23:32:57	Disabled	Enable	Delete
		9	Other Malicious P	IP G		Scanning & Eavesd	Exploit	DoS Attack	Backdoor Attack	Phishing		2019-10-16 23:32:57	Disabled	Enable	Delete
		10	Scanning and Eav	IP G		Interference	Brute-Force Attack	Other Cyber Attack				2019-10-16 23:32:57	Disabled	Enable	Delete
		ш	Exploit	IP G		Data Damage	a cat fr	1	B and the second seco			2019-10-16 23:32:57	Disabled	Enable	Delete
		12	DoS Attack	IP G		Other Data Damage	Data Ineft	Counterfeiting	Data Leakage	Data Loss		2019-10-16 23:32:57	Disabled	Enable	Delete
		13	Backdoor Attack	IP G		oner one onnage						2019-10-16 23:32:57	Disabled	Enable	Delete
		14	Phishing	IP G								2019-10-16 23:32:57	Disabled	Enable	Delete
		15	Interference	IP G								2019-10-16 23:32:57	Disabled	Enable	Delete
		16	Brute-Force Attack	IP G						Next	Cancel	2019-10-16 23:32:57	Disabled	Enable	-6
													28 entries	(1 2	



Response «	Respo	ise Pol	licies		New		×				
Risky Servers	+ N	w	🗙 Delete 👘	🗸 Enable	0	Ø	3			Search	
🖵 Risky Hosts	Policy	Sourc	e: All	Predefine	Conditio	s Response	Policy				ΰÐ
Risky Security Domains		ło.	Name	App	Correl	ted Block		Time Updated	Status	Operati	ion .
⊘ Security Events >		1	Botnet	IP G	Desire	Chandler NGA5		2019-10-16 23:32	57 Disabled	Enable	Delete
Response Policies		2	Trojan	IP G	Device	Sangfor Endpoint Secure (Hell)		2019-10-16 23:32	57 Disabled	Enable	Delete
Fix History		3	Worm	IP G		Fortinet FortiGate		2019-10-16 23:32	57 Disabled	Enable	Delete
		4	Virus	IP G	IF Add	ss: FortiGate(•	2019-10-16 23:32	57 Disabled	Enable	Delete
		5	Blended Attack	IP G	Cor	alated Block	Edit	2019-10-16 23:32	57 Disabled	Enable	Delete
		6	Code Injection	IP G				2019-10-16 23:32	57 Disabled	Enable	Delete
		7	Cryptomining	IP G				2019-10-16 23:32	57 Disabled	Enable	Delete
		8	Ransomware	IP G				2019-10-16 23:32	57 Disabled	Enable	Delete
		9	Other Malicious	P IP G				2019-10-16 23:32	57 Disabled	Enable	Delete
		10	Scanning and E	iv IP G				2019-10-16 23:32	57 Disabled	Enable	Delete
		11	Exploit	IP G				2019-10-16 23:32	57 Disabled	Enable	Delete
		12	DoS Attack	IP G				2019-10-16 23:32	57 Disabled	Enable	Delete
		13	Backdoor Attac	IP G				2019-10-16 23:32	57 Disabled	Enable	Delete
		14	Phishing	IP G				2019-10-16 23:32	57 Disabled	Enable	Delete
		15	Interference	IP G				2019-10-16 23:32	57 Disabled	Enable	Delete
		16	Brute-Force Att	ick IP G	Back	ОК	Cancel	2019-10-16 23:32	57 Disabled	Enable	
									28 entries	« < 1 2	2 2

Response «	Res	ponse P	olicies											
Risky Servers	+	New	🗙 Delete 👘 🗸 B	inable 🚫 Disable	C Refresh								Search	
Risky Hosts	Poli	cy Sour	ce : All Pro	defined Custom	Status : All	Enabled Disable	d Schedule :	All Always Custom						0 B
Risky Security Domains		No.	Name	Applicable Objects	Response	Device	File Action	Policy Source	Hits 0	Schedule	Time Updated	Status	Operation	
⊖ Security Events >		1	Test	All	Correlated Block	FortiGate		Custom	0	Always	2021-04-25 20:26:50	Enabled	Disable	Delete
@ Response Policies		2	Botnet	IP Groups	Access Control, T	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)	2019-10-16 23:32:57	Disabled	Enable	Delete
Fix History		3	Trojan	IP Groups	Threat Scan	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)	2019-10-16 23:32:57	Disabled	Enable	Delete
		4	Worm	IP Groups	Access Control, T	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)	2019-10-16 23:32:57	Disabled	Enable	Delete
		5	Virus	IP Groups	Access Control, T	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)	2019-10-16 23:32:57	Disabled	Enable	Delete
		6	Blended Attack	IP Groups	Browsing Risk No	IAM		Predefined	0	Always	2019-10-16 23:32:57	Disabled	Enable	Delete
		7	Code Injection	IP Groups	Browsing Risk No	IAM		Predefined	0	Always	2019-10-16 23:32:57	Disabled	Enable	Delete
		8	Cryptomining	IP Groups	Access Control, T	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)	2019-10-16 23:32:57	Disabled	Enable	Delete
		9	Ransomware	IP Groups	Access Control, T	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)	2019-10-16 23:32:57	Disabled	Enable	Delete
		10	Other Malicious P	IP Groups	Browsing Risk No	IAM, Endpoint Se	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)	2019-10-16 23:32:57	Disabled	Enable	Delete
		11	Scanning and Eav	IP Groups	Browsing Risk No	IAM		Predefined	0	Always	2019-10-16 23:32:57	Disabled	Enable	Delete
		12	Exploit	IP Groups	Access Control, T	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)	2019-10-16 23:32:57	Disabled	Enable	Delete
		13	DoS Attack	IP Groups	Threat Scan	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)	2019-10-16 23:32:57	Disabled	Enable	Delete
		14	Backdoor Attack	IP Groups	Threat Scan	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)	2019-10-16 23:32:57	Disabled	Enable	Delete
		15	Phishing	IP Groups	Threat Scan	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)	2019-10-16 23:32:57	Disabled	Enable	Delete
		16	Interference	IP Groups	Threat Scan	Endpoint Secure	Quarantine, Ignore	Predefined	0	Custom(22:00-08:00)	2019-10-16 23:32:57	Disabled	Enable	0

3. More > Toolkit > Correlated Response



Correlated Resp				🌻 Holistic 👻 😫 admin 👻
Correlated Response «	FortsGale			
	+ New × Delete C Refresh			IP Address Q
	No. IP Address	Device	Created	0 Operation
🕒 FortiGate				
		Add Correlated Address Block × Buics Object P Location Groups P Location Groups P Location F Location F Location F Location C Location Location C Location Location C Location Location Location Location Location Location Location Location Location Location Location Location Location Location Location Location Locatio		

Correlated Respo	onse	10 mm		🍨 Holistic 🗸	😫 adm	nin 👻
Correlated Response «	FortGate					
⊕ NGAF >	+ New X Delete C Refresh			IP Address		
	No. IP Address	Device	Created			Operation
📾 FortiGate	1 1.1.1.1	FortiGate (*)	2021-04-26 11:36			Delete
	1					

4. Enable or disable correlated response based on security events.

	Home						•	Holistic 👻 🖨 admin 👻
Response «	Risky Hosts							
Risky Servers	Pending Hosts All Hosts	Users		_				Display Options
Risky Hosts	C Refresh C Auto Refresh	: 3 minutes =		Correlated	Respons	e	×	Last 7 days
Risky Security Domains	Risk : All 🔻	Criticality :	All -	Scanning & up virus-infe	iavesdropp cted files.	ing. Virus event occurred. Suggestion: Enable browsing risk notification to inform user that host is infected. Enable threat scan to d	lean	08
Security Events >			lost (Risky/All)	4				Low
Response Policies	UnclassifiedServersIPRan	6		0	B	Correlated Block Block all outbound accesses from a sparific bost or inhound accesses to that host		
Fix History	UnclassifiedGroup	No.	s Fixed 👻 丨 📩 Exp Hostname	×		Access Control		Host, group, tag Correlated Response
	UserGroup 4	□ 1 □ 2	☆ 3.1.1.5 ☆ 3.1.1.2		*	Prevent a specific host from accessing specified IP address and port to block abnormal and attack behaviors. Threat Scan (HS)		Correlated Response
	UserGroup 8	3	☆ 3.1.1.8			Start a fullquick scan on host and quarantine/Inust detected malicious files.		Correlated Response
	The UserGroup 11	- 4	✿ 2.1.1.83		LQ.	Perform forensic investigation against a malicious domain to locate which parent or child process accesses that domain.	-	Correlated Response
	UserGroup 1	5	\$ 2.1.1.92					Correlated Response
	💭 UserGroup 6	6	☆ 2.1.1.58					Correlated Response
	🦢 💭 UserGroup 7	0 7	☆ 2.1.1.125					Correlated Response
		8	☆ 2.1.1.40					Correlated Response
		9	2.1.1.97			Next Close	,	Correlated Response

Response «	Risky Hosts			
E Risky Servers	Pending Hosts All Hosts	Users		Display Options
🖵 Risky Hosts	C Refresh C Auto Refresh	x 3 minutes *	Correlated Response ×	Last 7 days
🖽 Risky Security Domains	Risk : All 👻	Criticality : All 👻	Asset IP: 3.1.1.5 Create Response Policy ()	t B
⊘ Security Events >	E- All	Host (Risky/All)	Correlated Block	Low
Response Policies	- 💭 UnclassifiedServersIPRar	4	Device: O Sangfor NGAF (163)	
Fix History	💭 UnclassifiedGroup	🛃 Mark as Fixed 💌 🛛 💼 Expa	Sangfor Endpoint Secure	Host, group, tag
E	🐨 🐖 UserGroup 2	No. Hostname	Fortinet FortiGate	Correlated Response
	🖤 💭 UserGroup 3	1 \$3115	IP Address: FortiGate(10.67.43.111)	Correlated Response
	💭 UserGroup 4			
	🐖 UserGroup 5	2 👷 3.1.1.2	Correlated Block	Correlated Response
	UserGroup 8		Correlated Block X 2	
	🗁 💭 UserGroup 9	3 😭 3.1.1.8		Correlated Response
	💭 UserGroup 10		Remarks	
	🕬 💭 UserGroup 11	4 \$211.03		Correlated Response
	UserGroup 12			
	💭 UserGroup 1	□ 5 🟠 2.1.1.92	OK Cancel	Correlated Response
	💭 UserGroup 6	6 🕸 2.1.1.58		Correlated Response
	💭 UserGroup 7	□ 7 ☆ 2.1.1.125		Correlated Response
		□ 8 ☆ 2.1.1.40		Correlated Response
		9 👷 2.1.1.97	Back	Correlated Response

Response «	Risky Hosts				
Risky Servers	Pending Hosts All Hosts	Users			Display Options
Risky Hosts	C Refresh C Auto Refresh	h: 3 minutes 🝷	Correlated Response	×	Last 7 days
Risky Security Domains	Risk : All 👻	Criticality : All	Asset IP: 3.1.1.5 Create R	esponse Policy 🛈	0 B.
	E- All	Host (Risky/All)	Correlated Block		Low
Response Policies	UnclassifiedServersIPRa	ng	Device: Sangfor NGAS (20)		
E Fix History	Unclassified Group	Ko manc as roved *	Sangtor i indpoint Secure B Fortinet FortiGate		Host, group, tag
	UserGroup 3	No. Hostname	IP Address: FortiGate(10.67.43.111)		Correlated Response
	UserGroup 4	1 \$2 3.1.1.5		_	Correlated Response
	😳 🐖 UserGroup 5	2 🕸 3.1.1.2	Correlated Block Locking Edit	nlock -	Correlated Response
	UserGroup 8		Direction: All Lockout:		
	UserGroup 9	□ 3 ☆ 3.1.1.8	Remarks: None		Correlated Response
	UserGroup 10				
	UserGroup 11	4 👷 2.1.1.83			Correlated Response
	UserGroup 12	□ 5 ☆ 2.1.1.92			Correlated Response
	UserGroup 6	6 🕸 2.1.1.58			Correlated Response
	UserGroup 7	□ 7 <u>\$</u> 2.1.1.125			Correlated Response
		□ 8 <u>\$</u> 2.1.1.40			Correlated Response
		9 👷 2.1.1.97	Again	Close	Correlated Response

1.1.2. Others

None

1.1.3. Connection with Third-Party Products

Third-party products can be connected with APIs.

1.2. Deployment Impacts

The installation may take 1.5 hours.

1.2.1. Impacts on Business

None

1.2.2. Impacts on O&M

ISO installation may take 1.5 hours.

1.2.3. Impacts on Network

Deployment in bypass mode will have no impacts on network.

1.2.4. Others

None

1.3. Deployment Preparation Related to Customers

1.3.1. Resources Required for Deployment

1. You need to access to the VMware cloud environment of the customer and be familiar with the customer's network configuration.

2. Uploading the image to the cloud platform may take 50 minutes, and the entire deployment may take 1.5 hours.

3. The deployment environment should have enough resources and space (at least 8C32G+128G+4T).

1.3.2. Deployment Notification

1. The English version of 3.0.50C image can only be deployed in VMware virtual environment and cannot be deployed with physical hardware.

2. Deployment of 3.0.50C English version is only compatible with VMware ESXI5.0 \VMware ESXI 6.0\VMware ESXI 7.0

3. The follow	wing cpu models are measured: (Include but not
limited):	
48 CPUs x I	ntel(R) Xeon(R) Gold 5220R CPU @ 2.20GHz
28 CPUs x]	Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.40GHz
44 CPUs x]	Intel(R) Xeon(R) CPU E5-2699 v4 @ 2.20GHz
20 CPUs x]	Intel(R) Xeon(R) Silver 4210 CPU @ 2.20GHz

4. The English version of 3.0.50C can only support the following configuration:

|--|

Scenario	Supported	Memory	CPU	Disk	NICs
Virtual Environment Deployment					
				System: 128G	
	Yes	32G	8 cores	Data: 4T	4
'				System: 128G	
	Yes	96G	32 cores	Data: 4T	4
				System: 128G	
	Yes	128G	40 cores	Data: 4T	4
				System:	
VMware ESXi				1200	
5.0.0/6.0.0/7.0.0	Yes	256G	40cores	Data: 4T	4
Physical Hardware Deployment	No				

1.4. Deployment Process

- •Prepare the ISO image of Cyber Command 3.0.50C.
- •Import the image, configure environment and start auto installation. This may take 1.5 hours.

1.5. Business Verification After Deployment

- 1. Check whether you can log in normally without errors displayed.
- 2. If STA is connected, go to Logs page to check whether new logs are generated constantly.
- 3. Check as required whether customer business is normal.

1.6. Rollback

None

2. Deployment Instruction

2.1. Preparation Before Deployment

2.1.1. Deployment Tools

Prepare the ISO image of Cyber Command 3.0.50C.

2.1.2. Deployment Environment

None

2.1.3. Customer Resources

Refer to the chapter Deployment Preparation Related to Customers.

2.2. Confirmation Before Deployment

Refer to the chapter Deployment Impacts.

2.3. Deployment Procedure

2.3.1. Deployment Procedure

1. Cyber Command 3.0.50C Deployment

Step 1: Get the ISO image of 3.0.50C and import it to the customer's VMware cloud environment.

Step 2: Configure the virtual machine. Select ISO image of 3.0.50C for the virtual CD/DVD drive.

Step 3: Power on the virtual machine and select automatic installation

Step 4: Wait for the system to install automatically.

2. VMware esxi Deployment

Confidentiality Level: Public in project team

vmware esxi						toolg
Navigator D	database1					
- III Host Manage Montor	B Register a VM	Bi Increase capacity C Refresh Q Actions				STORAGE USED: 18.98 TB
• 60 Virtual Machines	Type	VMFS6				
• E Storage	Location	Amts/volumes/6013/3a2-alla68714-7b81-4	80:24108287	_		
Montor	Hosts Virtual Machines	A second in success of the second sec	anni 🖣 Granda daundara I. C	N Datas		
More storage		Votes - Downcad - Decete - Move -	Copy Create directory C	Retresh		
• Q Networking	VMES details	Optional a file to the selected datastore	es 0121.VMware-STA	4		
	Version	10.222.124.132_cgh	1-0224-VMware-ST			
	Local	10 222 125 210				
	Block state	in 10.222.88.13				
	UUD	in 10 222 88 33				
	Extent 0	in 10.222.88.59				
	Extent 1	160160				
	Extent 2	a 30.25C				
	Extent 3	3.0.48C				
	Extent 4	a 49c-1-wy				
	Extent 5	- 600G测试	1			
	Extent 6	协议审计目动化				
	Extent 7	ISO ISO	11	111		
	Extent 8	/ 🗐 (database1) ISO/				
						Close
	Recyni tasks		GERMAN CONSIGN	and the second se		
	Task	v Tagat v		weired	</td <td>V Rettill a</td>	V Rettill a
	Kename		1004 0.			Considered Roccessfully

1.1 Upload the obtained image to VMware, which may take about 50 minutes.

1.2 Create a new virtual machine.

vmware" Esxi"				
📲 Navigator 🗆	🕞 localhost.localdomain - Virtual Machines			
✓ ☐ Host Manage	The Create / Register VM	C Refresh	🛟 Actions	
Monitor	Virtual machine	Status ~	Used space ~	Guest OS
👻 🚰 Virtual Machines 🛛 16	test_zbb	Normal	378 GB	CentOS 7 (64
▼ 10.222.88.33	□ 🔓 49c-1-wy	Normal	628 GB	CentOS 6 (64
Monitor	□ 🚯 3.0.48C	Normal	8.16 TB	CentOS 7 (64
▼ 10.222.88.61	□ 5 10.222.88.66	Normal	1.13 TB	CentOS 7 (64
Monitor	□ ⓑ 10.222.88.33	Normal	2.14 TB	CentOS 7 (64
More VMs	10.222.88.61	🔥 Warning	648.09 GB	CentOS 7 (64
▼ Storage	🗋 📑 3.0.25C	Normal	628 GB	CentOS 7 (64
 database1 	□ 🚯 10.222.124.132_cgh	Normal	894.94 GB	CentOS 7 (64
Monitor	□ a 10.222.88.59	Normal	628 GB	CentOS 7 (64

Select the option of creating a new virtual machine.

🔁 New virtual machine		
 Select creation type Select a name and guest OS Select storage 	Select creation type How would you like to create a Virtual Machine?	
3 Select storage 4 Customize settings 5 Ready to complete	Create a new virtual machine	This option guides you through creating a new virtual machine. You will be able to customize processors, memory,
	Deploy a virtual machine from an OVF or OVA file Register an existing virtual machine	network connections, and storage. You will need to install a guest operating system after creation.
vm ware*		
		Back Next Finish Cancel

Select VMware EXSi 7.0 (you can also select VMware EXSi 5.0 or VMware EXSi 6.0).

🔁 New virtual machine - 3.0.50C (ESX	i 7.0 virtual machine)		
 New virtual machine - 3.0.50C (ESX 1 Select creation type 2 Select a name and guest OS 3 Select storage 4 Customize settings 5 Ready to complete 	T.0 virtual machine) Select a name and guest Specify a unique name and OS Name 3.0.50C Virtual machine names can contain up to Identifying the guest operating system hi installation.	OS 80 characters and they must be unique within each ESXI instance. ere allows the wizard to provide the appropriate defaults for the operating system	
	Compatibility Guest OS family Guest OS version	ESXI 7.0 virtual machine Linux CentOS 7 (64-bit)	
vm ware [.]		Back Next Finish Cancel	

Select Linux OS and CentOS 7 (64-bit) version as below.

Select storage, ensuring that the environment have enough space. Then, click Next.

🔁 New virtual machine - 3.0.49C (ESXi 7.0 virtual machine)							
 1 Select creation type 2 Select a name and guest OS 3 Select storage 4 Customize settings 5 Ready to complete 	Select storage Select the storage type and datastore Standard Persistent Memory Select a datastore for the virtual machine's co	onfiguration files	and all of its' vi	irtual disks.			. 4
	Name ~	Capacity 🗸	Free ~	Туре ~	Thin pro 🗸	Access	~
	database1	65.5 TB	46.52 TB	VMFS6	Supported	Single 1 if	tems
vmware							13
			Ва	ck Ne:	xt Finis	h C	ancel

Configure the virtual machine as following: 8-core CPU, 32G memory, 128 GB system disk, and 4 TB data disk. Version 3.0.50C supports 1 to 4 NICs.

🔁 New virtual machine - 3.0.50C (ESX	(i 7.0 virtual machine)		
 1 Select creation type 2 Select a name and guest OS 3 Select storage 4 Customize settings 5 Ready to complete 	Configure the virtual machine hardware an Virtual Hardware VM Options	nd virtual machine additional options	
	🔜 Add hard disk 🛛 🛤 Add network ad	dapter 🛛 🚍 Add other device	
	F 🖬 CPU	8 🗸 🚺	
	► 🛲 Memory	32 GB ~	
	▶ 🚍 Hard disk 1	128 GB ~	\odot
	▶ 🛄 New Hard disk	4 TB ~	0
	SCSI Controller 0	VMware Paravirtual	0
	SATA Controller 0		\otimes
	WSB controller 1	USB 2.0 ~	8
	Init Network Adapter 1	VM Network	\otimes
vm ware [*]	▶ 🗐 CD/DVD Drive 1	Host device V Connect	\otimes
		Back Next Finish	Cancel

Select an image to be added to virtual CD/DVD drive.

Select creation type Select a name and guest OS	Customize settings Configure the virtual machine hardwa	are and virtual machine additional options
Select storage		
Ready to complete	SCSI Controller 0	VMware Paravirtual
	SATA Controller 0	8
	USB controller 1	USB 2.0 ~
	► Metwork Adapter 1	VM Network 🗸 🗸 Connect 💿
	✓ (iii) CD/DVD Drive 1	Datastore ISO file V Connect 💿
	Status	Connect at power on
	CD/DVD Media	[database] ljq/CyberCommand-3.0.50C-2021-04-22.isc Browse
	Controller location	SATA controller 0 v SATA (0:0) v
	► 🛄 Video Card	Default settings ~
M Ware	► I Security devices	Not configured

Select the option to connect at power on.

1 Select creation type 2 Select a name and guest OS 3 Select storage	Customize settings Configure the virtual machine hardw	vare and virtual machine additional options	
4 Customize settings 5 Ready to complete	► 🛄 New Hard disk	4 TB ~	\otimes
	► 🐼 SCSI Controller 0	VMware Paravirtual	\otimes
	SATA Controller 0		\otimes
	USB controller 1	USB 2.0 ~	\otimes
	► Mai Network Adapter 1	VM Network	\otimes
	✓ (ii) CD/DVD Drive 1	Host device V Connect	\otimes
	Status	Connect at power on	
	CD/DVD Media	None	~
	Controller location	SATA controller 0 v SATA (0:0) v	
vm ware	▶ 🛄 Video Card	Default settings v	

Click to finish the creation.

🔁 New virtual machine - 3.0.50C (ESXi	New virtual machine - 3.0.50C (ESXi 7.0 virtual machine)						
 1 Select creation type 2 Select a name and guest OS 3 Select storage 	Ready to complete Review your settings selection before finit	shing the wizard					
 4 Customize settings 5 Ready to complete 	Name	3.0.50C					
	Datastore	datebase1					
	Guest OS name	CentOS 7 (64-bit)					
	Compatibility	ESXi 7.0 virtual machine					
	vCPUs	8					
	Memory	64 GB					
	Network adapters	1					
	Network adapter 1 network	VM Network					
	Network adapter 1 type	VMXNET 3					
	IDE controller 0	IDE 0					
	IDE controller 1	IDE 1					
	SCSI controller 0	VMware Paravirtual					
	SATA controller 0	New SATA controller					
	Hard disk 1						
	Capacity	128GB					
Viiivare	Datastore	[datebase1] 3.0.50C/					

Select the created virtual machine.

Manage	😭 Create / Register VM 💣 Compile 🐌 Power on 🔳	Power off 👔 Suspend 🙋 Refresh 🍈 Actio	⇒.			Q Search	
Monitor	. Virtual machine	✓ Status ✓ Used s	pace ~ Guest OS	~ Host name	- Host CPU	 Host memory 	¥
🎝 Virtual Machines 🗾 5	1. 20 Incl. o. do many male vit Stat	Ø threat E to 0	benGhTassid.	0100-200-2000rts	365 015	64.93 (66)	
* 🙆 3.0.50C	(S) B art 2 Mt steeles	🖕 Second: 3.52 TT	sherioy 2 streat;	Applitude, Incurrent and	111 2 360	stay inpr	
Monitor	C. A. D	S New CALD	0662379446	iblenam	1944	5.45	
i 🦛 Nillion-Hallin AL-	El de Cudell wand cavery	 Alonesi 4.157 	dater367354cdj	strop-dork:264-6ale	55 5Nc	dc/ E= 35	
4 🏚 990/bijtst-mettele	C. 50 3.0 50C	Normal 1.05 TE	CentOS 7 (64-bit)	Unknown	0 MHz	0 MB	
 S \$14,32,32,45,44880 + More Vils Storage Fit database 	Quick filtersv						5 items "
Monitor More storage							
• Q 900M Manitor							
More networks							

Click the button to power on the created virtual machine.

You will go to the installation page. Press Enter to select automatic installation



Wait during the automatic installation, which may take 1.5 hours.



After the automatic installation is complete, click Reboot.

	CONFIGUR	ATION			CENTOS 7 INSTA	Help!
CentOS	USER SET	TINGS				
	C -	ROOT PASSWORD Root password is set			SER CREATION o user will be created	d.
	Complete!					31
			Cent	OS is now successf	ully installed and ready f Go ahead and reboor to	or you to usel start using it Reboot

	J.0.	490	
			Unmounting /mmt/sysimage/dev/shm
			Unmounting /mnt/sysimage/home/fantom/var/logs
Γ	OK]	Stopped Load/Save Random Seed.
LF	AILE	DI	Failed unmounting /run/install/repo.
Γ	OK]	Unmounted /mmt/sysimage/sys/fs/selinux.
Γ	OK]	Unmounted /mnt/sysimage/home/fantom/var/tmp.
			Unmounting /mnt/sysimage/sys
Ľ	OK]	Stopped Configure read-only root support.
Γ	OK]	Unmounted /mnt/sysimage/dev/pts.
E	OK]	Unmounted /mnt/sysimage/proc.
E	OK]	Unmounted Temporary Directory.
E	OK]	Unmounted Configuration File System.
Ľ	OK]	Unmounted /mmt/sysimage/run.
Ľ	OK]	Unmounted /mmt/sysimage/boot/efi.
Ľ	OK]	Unmounted /mnt/sysimage/dev/shm.
E	OK]	Unmounted /mnt/sysimage/home/fantom/var/logs.
E	OK]	Unmounted /mnt/sysimage/sys.
			Unmounting /mnt/sysimage/home/fantom
			Unmounting /mnt/sysimage/boot
I	OK]	Stopped target Swap.
			Deactivating swap /dev/sda6
			Unmounting /mnt/sysimage/dev
Ľ	OK]	Unmounted /mnt/sysimage/dev.
Ľ	OK]	Unmounted /mnt/sysimage/boot.
[OK]	Deactivated swap /dev/disk/by-uuid/8fdbf0ac-1707-4792-84d4-4949f4afc8d5.
L	OK	1	Deactivated swap /dev/disk/by-path/pci-UUUU:03:00.0-scsi-0:0:0:0-part6.
L	UK	1	Deactivated swap /dev/disk/by-partuuid/171ad1eb-644c-45a7-a20e-0c1c41783228.
L	UK]	Deactivated swap /dev/disk/by-label/sipswap.
L	UK]	Deactivated swap /dev/sdab.
L	UK]	Unmounted /mnt/sysimage/home/fantom.
		-	Unmounting /mmt/sysimage
Ļ	UK	1	Unmounted /mmt/sysimage.
L	UK	1	Reached target Unnoult All filesystems.
L	UK	L	Stopped target Lucal file Systems (FFE).
L	UK	L	Stopped Remount Noot and Kernel File Systems,
Ľ	UN	1	Stopped Create Static Device houses in Zaev.
1			



After installation, you need to enter the background to configure the IP address. The default login account is "admin" with the password "adminsangfornetwork".

For example, if you want a PC (10.32.0.0/16) to access the web console, you need to add

the next hop address of 10.32.0.0 in the background.

SIS3.0.49.0 " #
SIS3.0.49.0 T static IP
S1S3.0.49.0 - #
SIS3.0.49.0 " # ip a a 10.222.125.209/16 dev eth0
SIS3.6.49.6 " a please change to your own
\$1\$3.8.49.6 " #
SIS3.0.49.0 " #
SIS3.8.49.8 ⁻ #
SIS3.8.49.8 " # ip r a 18.32.8.8/16 via 18.222.255.254 dev eth8
SIS3.8.49.8 # network segment Material and test
SIS3.8.49.8 #
SIS3.8.49.8 (7) #
SIS3.8.49.8 - #
SIS3.8.49.8 ~ # ip r
18.32.8.8/16 via 18.222.255.254 dev eth8
18.222.8.8/16 dev eth8 proto kernel scope link src 18.222.125.289
10.251.251.0/24 dev eth0 proto kernel scope link src 10.251.251.252
169.254.8.8/16 dev eth8 scope link metric 1882
172.17.8.8/16 dev docker8 proto kernel scope link src 172.17.8.1
\$1\$3.8.49.8 " #
SIS3.8.49.8 - #
\$1\$3.8.49.6 - #
SIS3.0.49.0 ⁻ #
SIS3.8.49.8 ⁻ # ip algrep eth8
2: eth0: <broadcast,multicast,up,lower_up> mtu 1580 qdisc mq state UP group default qlen 1000 inet 10.251.251.252.24 brd 10.251.251.255 scope global eth0</broadcast,multicast,up,lower_up>
inet_18.222.125.289/16_scope_global_eth8
\$1\$3.0.49.0 " #
\$1\$3.0.49.0 " #
\$1\$3.0.49.0 " #
SIS3.8.49.8 T # A

The default login account of the Web console is "admin" with the password "admin".

To use the product normally, licensing is required. Otherwise, you can only enter the page about system settings.

		SANGFOR SECURITY	© +60 12711751
Cyber Command		e	
Cyber Command is a platform that significantly improves customer's secur		Cyber C	ommand
detection and response capability. Cyber Command monitors internal netw	vork traffic,		
correlates existing security events, applies artificial intelligence and behavi			
analysis, aided with global threat intelligence. Unlike other toots, Cyber Co	mmand	Username	
uncovers anacks that breach existing security controls, and impact analysi identifies hidden threats within the network. This allows customers to signi	is licently		е
improve ability to understand the current threat landscape. Cyber Commar			
simplifies the response of security operations with native integration with n	ietwork	Password	
		Enter the characters	
			3 M 3/2

After entering the web console, you need to manually add the permanent route and IP address. Otherwise, the IP address information just configured will be invalid after the device restarts.

System «	Network .			
Correlated Devices	Interfaces Static Routes DNS Servers			
🕲 System 🖂	+ New Solete C Refresh			
Admin Account	No. Dst IP	E Netmask	I Next-Hop IP	C Operation
Licensing				
Network		Add Static Deute		
General		Add static houle		
Logging Options		Protocol: 0 IPv4 0 IPv6		
± Update >		* Dst IP: 0.0.0.0		
A Maintenance >		*Netmask: 0.0.0.0		
🛱 Databases >		* Next-Hop IP 10.222.255.254	add the next-hop ip which added in console	
		OK Cancel		
		/		
	/			
	just for exampl	le .		
				6
				0 entries a v v
				a second s
System «	Network			
Correlated Devices	Interfaces Static Routes DNS Servers			
ि Sustem	✓ Enable S Disable C Refresh			
Admin Account	No. Interface Name	Description	IP Address	Status 0
Norma Account	□ 1 eth0		10.251.251.252/24	~
Licensing		Fift Interfere	10.222.125.209/16	
Network	2 eth1	Edit Interface ×		×
General	3 eth2	Status: 🗹 Enable		×
Logging Options		Name: eth0	it is build in 10	
🖆 Update >		Description:		
& Maintenance >		IP Address: 10.251.251.252/24 0		
8º Databases >		10.222.125.209/16	and the there is a second second	
			manually add the IP which you have set in console	
		OK Cancel		

Note:

Virtualization deployment requires a basic configuration. If CPU cores, memory size, system disk and data disk size are non-standard, the system may fail to start normally or the gateway may be unreachable.

Connection with STA

Wen Cyber Command is licensed, it needs to be connected with an STA device so as to receive traffic. The following operations should be performed on STA:

1. Log in to STA.

SANGFOR			
110 HEAL SHOW +61 1771 7780 774	1 10 10 10 10 10 10 10 10 10 10 10 10 10	Stealth Threat Analytics	
	Smart Choice, Sangtor Solution	Password Captcha	
© 2017-2021 SANGHOR Tech	nologies Inc. Al rights reserved.	Log In the second s	V .

2. Ensure that the customer's traffic is connected and will be forwarded from the switch's mirror port. This also depends on the customer's network configuration.

- Status	Status	
System	48., CU Utage 58., Memory Utage 38., Diak Utage	Threats: 0 System Time: 2021-04-25 15:58:34 Uptime: 21 Hours 46 Mins 1 Secs
	Sessionsi Current-	Throughput All mirror ports *
	Session: Concurrent New Sessions/Sec	0400041 (bgs Inbound: 129.23) 000 000 000 000 000 000 000 0
	Interface	Cyber Command #
	eða eði eði	Link State: Normal Server IP: 10.222.111.222
) Network		
• Objects		
Access Control		

3. Go to STA and specify a Cyber Command IP address to be connected and test connectivity.

Then, choose the log transmission mode which is usually set to the "Advanced logs" mode.

🞯 Stealth Threat	Analytics V3.0.25C							User: admin	[log out]
Status	Cyber Command								
	Z Enable	2	3						
	Cyber Command Server IP:	10 222 111 222	() The Course	and days					
	Outbound Bandwidth:	10.222.111.222	Test Connect	ctivity					
	Log Types:		r suppo						
General	 Standard logs () Simulified logs () 		🖾 Web attack						
Administrator	Advanced logs	Security detection	Vuln exploit						
	 LAN access logs () Custom logs () 		Server weakness detection						
	2	Access detection	Elegitimate access Sett Risky/illegitimate access	ttinos					
		Protocol audit	HTTP (i) Saft HTTP (i) Saft DNS (i) Saft DNS (ii) Saft SNB (iii) Saft SNB (iiii) Saft SNB (iiiii) Saft TELNET (iiiiiii) Saft SNB (iiiiiiii) Saft SNB (iiiiiiiiiii) Saft SNB (iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	ttinos ttinos ttinos ttinos ttinos					
	Advanced OK	4							

4. Check the STA status on Cyber Command and ensure that STA is connected normally.

🕢 Cyber Comn	nan	nd 🚥 Home Response Detection Assets Reports More 😑 🗣 elamin -
System		Consider Devices
Correlated Devices	-	C Reinh
Correlated Devices		Total Lags (body): 6223 1 Sanglor devices licensed; 0 Ecremes remaining (not court in STA; Re-reputation & threat analytics system)
Monitor		🔝 STA 📷 IAM 🍙 Endpoint Secure 🚃 NGAF 🚜 BBC
System	>	Voline 2 + Office 2 + Office 2 + Office 2 + Office 0
⊥ Update	>	Today's Synced Logs: 6225 N/A (tync not supported) Today's Synced Logs: 0 Today's Synced Logs: 0 N/A (tync not supported)
🖏 Maintenance	>	••
82 Databases	>	+ New X Dulte C Refresh
		No. Name (IP Address) 🕆 Type 🗘 IP Address 🔅 Version 🗘 Licensed 🗘 Sync Mode Today's Synced Lógis Total Synced Logis Total Synced Logis Alart Synced 🖒 Status 2 Alerts (10 days) 2 Operation
		1 SANGFOR STA_1102 Statelity Thr : TS3.027.6577_B Licenses Used Contom 72.271M8 369.27M8 0 2021-04-29.2304.57 • Nor 4 Traffic Details

This means that Cyber Command has processed traffic normally.

Cyber Command V30.55C Home Resp	oonse Detection Assets Repo	rts More ≡			🔹 Holistic 👻	😫 admin 👻
STA * Online: 2 * Online: 1 STA * Office: 0 Secure * Office: 0	NGAF *Online: 0 *Offline: 0	IAM	• Connected: 0	BBC + Online: 0 + Offline: 0	6 2 57% 44%	46%
Overview Security Event Scans						
Overall Security						
Uptime: 0 0 1 1 days	34 Q New Events (30 days)	0 Fixed	GoldenEye Traceback () IP/Domain/URL/Port			Search
Security Rating	Pending Endpoints () 3300 Pending Servers Press	042 Ging Hosts	Hot Events ① Ramnit Conficter	Crystonicing ExemalBluer (5315) DOD Mining View PenerCheat Cocored Not occurred	Ransomware DriveThtLife Dark Cloud Trojan Backlink	
L Committee						Display Options
Server Security Server Distribution		×	Top 5 Risky Servers			View More > X
			No. IP	Groups Major Threats		Risk Level 0
Compromised: 3295 High: 5 3307 Medium: 0	Exploit Improper Configuration	3209	1 192.168.28.222 - 2 192.168.31.188 -	New Webshell Exploit	ion) [Webshell]	10)Compromised
Risky Server Low: 7 Very-Low: 0	Weak Password Unencrypted Traffic	3315	3 192.168.21.143 - 4 192.168.34.143 -		ion Webshell	10)Comprom.

2. VMware vSphere Client Deployment

Upload ISO file to VMware datastore.

File Edit View Inventory Administration Plug-ins Help		
🖸 🔯 🔥 Home 🕨 👸 Inventory 🖌 🔂 Datastores and D	Datastore Clusters	🔊 - Search Inventory
vcenter.zjw.com 10.222.3.35 10.222.3.46	datastore1 (2) Getting Stated, Summary, Virtual Machines, Hosto, Configuration, Tasks & Evento, Alarma, Permissione,	
(i) debaued (i) debau	Character States of the second of the s	×
	Basic Tasks of Browse this da	Nodified

The upload may take 30 minutes. The ISO file in the following screenshot is just an example.

-			-		-							
₽	ß	ø	8	8	B	×	0					
Fold	ers Seard	h					[database0] iso					
	- 💋 22					^	Name	Size	Туре	Path	Modified	
	- 🧖 SIP	_10.222.1	25.27				6 0105-VMware-SIP-3.0.49.iso	7.357.596.00 KB	ISO image	[database0] iso	2021/2/26 1:15:11	
	- 💋 31_	2										
	- 🜔 ccor	m_10.222	. 123. 173									
	- 🥖 wins	server201	2_lxp									
	F D STA	3.0.17										
	- 🎁 AF8	3.0.8-253										
	- 💋 iso											

Create a new virtual machine.

File Edit View Inventory Administration Plug-ins Help	
🕞 💽 🔝 Home 🕨 👸 Inventory 🕅 Hosts and Clusters	
et et 25	
🖃 🛃 vcenter.zjw.com	10.222.3.46 VMware ESXi, 6.0.0, 2494585
⊡ 10.222.3.35 □ 10.222.3.46 □ 10.222.3.46	Getting Started Summary Virtual Machines Resource Allocation Performance Configuration
10.222.3.57	What is a Host?
au.222.3.60	A host is a computer that uses virtualization software, such as ESX or ESXI, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual machines access to storage and network connectivity.
	Basic Tasks
	Create a new virtual machine

Click the button to create a new virtual machine and then click Next.

		close tab Y									
	🕝 Create New Virtual Mac	thine							-		×
rt c t	Configuration Select the configuration fo	or the virtua	al machine						Virtual M	achine \	/ersion: 11
h	Configuration Name and Location Storage Guest Operating System Network Create a Disk Ready to Complete		guration Typical Create a new ' Custom Create a virtui	virtual machi	ne with the	most comm	r specific confi	d configur guration c	ation optio	ns.	
							< Back	N	lext >	c	ancel

Select a host and click Next.

Create New Virtual Ma	chine	-		\times
ame and Location Specify a name and locat	ion for this virtual machine	Virtual M	1achine Ver	sion: 1
onfiguration	Name:			
ame and Location	3.0.49C			
orage Jest Operating System	Virtual machine (VM) names may contain up to 80 chara vCenter Server VM folder.	cters and they must be unique with	in each	
etwork	Inventory Location:			
eate a Disk eady to Complete	10.222.3.46			
			-	
			_	

Select a resource pool and click Next.

🕜 Create New Virtual Machine

Resource Pool

Within which resource pool do you want to run this virtual machine?



Virtual Machine Version: 11

 \times

Select storage size, ensuring it is large enough.

hine ge for the virtual machine f Select a destination stor	les age for the virtua	I machine files		Vi	— [irtual Machir	ne Version: 1
ge for the virtual machine f Select a destination stor	les age for the virtua	I machine files		Vi	irtual Machir	ne Version: 1
Select a destination stor	age for the virtua	I machine files				
Name	1 1		•			
	Drive Type	Capacity	Frovisioned	Free	Туре	Thin Prov
📑 database0	Non-SSD	36.38 TE	3 55.19 TB	6.78 TB	VMFS5	Supporte
datastore1 (2)	SSD S for this virtual I	111.75 GE	3 54.92 GB	110.80 GB	VMFSS	Supporte >
Select a datastore:						
Name	Drive Type	Capacity P	Provisioned	Free	Туре	Thin Provi
	C Disable Storage DR Select a datastore: Name	Disable Storage DRS for this virtual r Select a datastore: Name Drive Type	Disable Storage DRS for this virtual machine Select a datastore: Name Drive Type Capacity F	Disable Storage DRS for this virtual machine Select a datastore: Name Drive Type Capacity Provisioned	Oisable Storage DRS for this virtual machine Select a datastore: Name Drive Type Capacity Provisioned Free	Oisable Storage DRS for this virtual machine Select a datastore: Name Drive Type Capacity Provisioned Free Type

Select Linux OS and CentOs 4/5/6/7 (64-bit) version for the virtual machine.

Then, click Next.

🕜 Create New Virtual Mach	ne	_		\times
Guest Operating System Specify the guest operating	system to use with this virtual machine	Virtual M	lachine Versi	on: 11
Configuration Name and Location Resource Pool Storace Guest Operating System Network Create a Disk Ready to Complete	Guest Operating System:	T the appropriate	defaults for	
	< Back	Next >	Cance	±

Version 3.0.50C supports 1 to 4 NICs. Supported NIC types: VMXNET3, VMXNET2 (enhanced), and e1000.

Which network connection	s will be used by the virtual machine?			
Configuration Name and Location Resource Pool Storane Guest Operating System Network Create a Disk Ready to Complete	Create Network Connections How many NICs do you want to connect? Network Adap NIC 1: VM Network VMX If supported by this virtual machine version, more than 4 NICs of virtual machine is created, via its Edit Settings dialog. Adapter choice can affect both networking performance and migrat the VMware KnowledgeBase for more information on choosing am supported for various guest operating systems and hosts.	NET 3	Connect al Power On T ter the ity. Consult rk adapters	t

Add a 128 GB system disk. Then, click Next.

		ologo ta	b V			
🕝 Create New Virtual Mach	ine			_		×
Create a Disk Specify the virtual disk size	and provisioning policy			Virtual Mac	hine Vers	sion: 11
Configuration Name and Location Resource Pool Storage Guest Operating System Network Create a Disk Ready to Complete	Datastore: Available space (GB): Virtual disk size: Thick Provision Lazy Zero Thick Provision Eager Zer Thin Provision	database0 6940.0 128 GB V sed roed				
			< Back	Next >	Cano	cel

Click Continue to finish specific configurations for the virtual machine.

🕝 Create New Virtual Machine

- 0

Virtual Machine Version: 11

 \times

Ready to Complete

Click Finish to start a task that will create the new virtual machine

Configuration	- Cattions for the second interal mark	4:
Name and Location	Name:	nine: 3.0.50C
Storage	Folder	10 222 3 86
Guest Operating System	Host/Cluster	10 222 3 86
Network	Resource Pool:	lig
Create a Disk Boody to Complete	Datastore	datactora
Ready to complete	Guest OS:	CentOS 4/5/5/7 (64-bit)
	NICe:	1
	NIC 1 Network	1 VM Network
	NIC 1 Type:	VMVNET 2
	Dick provisioning	Thick Provision Larry Zamad
	Vistual Diale Sizes	130 CR
	virtual Disk Size:	120 GD
	 Edit the virtual machine set Creation of the virtual mac system. Install a guest OS 	tings before completion thine (VM) does not include automatic installation of the guest operating on the VM after creating the VM.
		< Back Continue Cancel

Change CPU to 8 cores and change memory size to 32G.

🚱 3.0.50C - Virtual Machine Prop	perties		_		×
Hardware Options Resources vSer	vices		Virtual Machin	e Version:	11 🛝
Show All Devices	Add Remove	Number of virtual sockets:	1	•	
Hardware	Summary	Number of cores per socket:	8	-	
Memory (edited)	32768 MB				
🔲 CPUs (edited)	8	lotal number of cores:	8		
 Video card VMCI device SCSI controller 0 CD/DVD drive 1 Hard disk 1 Floppy drive 1 Network adapter 1 	Video card Deprecated LSI Logic Parallel Client Device Virtual Disk Client Device VM Network	Changing the number of virtu. OS is installed might make you unstable. The virtual CPU configuration might violate the license of t	ial CPUs after .r virtual mach specified on t ie guest OS,	the guest ine	
			ОК	Cancel	

Add a 4-TB data disk, ensuring that the environment has sufficient resources.

Hardware Options Resources
Ha Device Type What sort of device do you wish to add to your virtual machine?
Device Type Select a Disk Advanced Options Ready to Complete Choose the type of device you wish to add. Image: Select a Disk Advanced Options Ready to Complete Image: Select a Disk Advanced Options Ready to Complete Image: Select a Disk Ready to Complete Image: Select a Disk Image: Select a Disk Advanced Options Ready to Complete Image: Select a Disk Image: Select a Disk
< Back Next > Cancel
Finish Cancel

Click Next.

Select a Disk Create a Disk Advanced Options Ready to Complete Disk Image: Create a new virtual disk <th>Add Hardware</th> <th></th> <th>></th>	Add Hardware		>
Device Type Select a Disk Create a Disk Advanced Options Ready to Complete Disk Create a new virtual disk to use. Disk Create a new virtual disk Reuse a previously configured virtual disk. Create Mappings Give your virtual machine direct access to SAN. This option allows you to use existing SAN commands to manage the storage and continue to access it using a datastore.	Select a Disk		
	Device Type Select a Disk Create a Disk Advanced Options Ready to Complete	A virtual disk is composed of one or more files on the host file system. Together these files appear as a single hard disk to the guest operating system. Select the type of disk to use. Disk C Create a new virtual disk C Use an existing virtual disk Reuse a previously configured virtual disk. C Raw Device Mappings Give your virtual machine direct access to SAN. This option allows you to use existing SAN commands to manage the storage and continue to access it using a datastore.	

Click Next.

🕝 Add Hardware		×
Create a Disk Specify the virtual disk siz	ze and provisioning policy	
Device Type Select a Disk Create a Disk Advanced Options Ready to Complete	Capacity Disk Size: 4 - TB Disk Provisioning Thick Provision Lazy Zeroed Thick Provision Eager Zeroed Thin Provision Location Store with the virtual machine Specify a datastore or datastore cluster: Browse Browse	
	< Back Next > Ca	ncel

Click Next.

Device Type	
<u>elect a Disk</u> C <u>reate a Disk</u> Advanced Options Ready to Complete	Virtual Device Node
	Mode
	C Persistent Changes are immediately and permanently written to the disk.
	 Nonpersistent Changes to this disk are discarded when you power off or revert to the snapshot.

Click Finish to complete the steps to add a disk.

🗿 Add Hardware					\times
Ready to Complete					
Review the selected opt	ions and click Finish to add	the hardware.			
Device Type	 Options:				
Select a Disk					
Create a Disk	Hardware type: Create disk:	Hard Disk New virtual disk			
Ready to Complete	Disk capacity:	4 TB			
nearly to complete	Disk provisioning:	Thick Provision Lazy Zeroed			
	Datastore: Virtual Device Node:	database0 SCSI (0:1)			
	Disk mode:	Persistent			
	1				
			. 1	I	
		< B	ack	Finish	Cancel
					///

Select an image to be added to virtual CD/DVD drive. Select the option to connect at power on.

Select the directory to start uploading ISO.

Hardware Options Resources	Add Remove	Device Status Connected Connect at power on Connect at power on Connect Type Connect Type Connect Type Connect this device, you must power on the virtual machine and then click the Connect CD/DVD button in the toolbar. C Host Device C a a a a a a a a a a a a a a a a a a a	
_		Finish Cancel	
3.0.50C - Virtual Machine Prop Hardware Options Resources Show All Devices	Add Remove	Device Status Connected	×
	/		
Browse Datastores		- U X	
Look in: jq	▼ €	this device, you must power on t	the
Name Image Image Image	File Size -04 5 GB 202 5 GB 	LastModified nd then dick the Connect CD/DVD 2021/4/21 22:14:: bar. 2021/4/21 16:27:: e Browse (recommended) Cancel (recommended) IDE (1:0) •	•
		Finish Can	

After the file is added successfully, click Finish and wait for VMware to create a new virtual machine.

Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Ti 💎	Start Time	Con
Create virtual machine	10.222.3.46	45% 💶	Copying Virtual Machine configuration	VSPHERE.LO	vcenter.zjw.c	2021/3/10 20:29:47	2021/3/10 20:29:47	

Select the newly created virtual machine and turn on the power to go to the automatic installation page. The operation steps are the same as VMware EXSi and will not be repeated here.

2.4. Check After Deployment

2.4.1. Platform Check

Log in to web console and go to System > Update > Cyber Command to check that the version is SIS3.0.50C.



2.4.2. Business Verification

Verify basic functions used by customers.

Log in and go to the Logs page to check whether there are new logs synchronized from STA.

Export ()	Tips		Open Mon	tor C Refresh C	Auto Refresh 🔻							🗢 Basic
All Logs •	89,903	jin a a	.1 AND dat_p	ort:8000 or 1.1.1.1 (use ==	for IPv6 address, e.g., "2005:1")			Direction		2021-04-25 00:00:00 - 2	021-04-25 07:30:56	🖬 ★ 🗖 G
AND • 🕕 Add												
Total Entries : 39502879 (Interval: 10mir) @											
Secure Access (38959- Database Serve	e (407	Php	code injectio	Web-access clear	text — Web Server (19916)	Buffer overflow inspe		Password contains 6 o- Requer	it method fil	er Web-access weak	pas- Suspicious Traffic (14	13
sunt												
100k	1.0			1.1.1.1.1		1.1.1	1 II w					
0 04-25 00:30		11:00	-	01:30 02:00	02:30 03:00	03:30	04:00	04:10 05:00	05:30	06:00	06.30 07.00	07:30
		No.	Mark T	Time .	Log Type 🝸	Sec IP 🝸	Sec Port T	Dist IP 🝸		Dst Port	Data Source	T
Selected Fields		:1	ø	2021-04-24 16:30:55	Traffic	192.168.24.33	43881	192.44.17.84		135	NovaSensor	(10.222.125.220)
Time		2	ø	2021-04-24 16:30:55	Traffic	192.168.24.231	58029	192.44.1.201		21	NovaSensor	(10.222.125.220)
Log Type		3	P	2021-04-24 16:30:55	Teaffic	192.168.30.147	1480	192.44.6.34		80	NovaSensor	(10.222.125.220)
Src IP	(4	ø	2021-04-24 16:30:55	Traffic	192.44.12.84	20	192.168.39.17		58046	NovaSensor	(10.222.125.220)
Src Port	(5	ø	2021-04-24 16:30:55	Traffic	192.44.15.143	52	192.168.24.89		4930	NovaSensor	(10.222.125.220)
Dst IP	(E	6	P	2021-04-24 16:30:55	Traffic	192.44.12.83	63505	192.168.36.139		80	NovaSensor	(10.222.125.220)
Dat Port		7	P	2021-04-24 16:30:55	Traffic	192.168.26.96	58030	192.44.12.154		21	NovaSensor	(10.222.125.220)
Data Source	Ð	8	ø	2021-04-24 16:30:55	Traffic	192.44.21.93	20	192.168.36.19		58047	NovaSensor	(10.222.125.220)
		9	ø	2021-04-24 16:30:55	Traffic	192.44.18.191	58778	192,168.24.78		80	NovaSensor	(10.222.125.220)
Available Fields	•	10	P	2021-04-24 16:30:55	Traffic	192.168.34.25	20	192.44.12.110		64783	NovaSensor	(10.222.125.220)
Attack Type	• 🗉	11	ø	2021-04-24 16:30:55	Traffic	192.168.30.82	20	192.44.4.62		58200	NovaSensor	(10.222.125.220)
Log Subtype	• =	12	ø	2021-04-24 16:30:55	Traffic	192.44,11.84	20	192.168.35.121		58044	NovaSensor	(10.222.125.220)
Log Severity		13	4	2021-04-24 16:30:55	Traffic	192.44.13.228	20	192.168.36.56		58044	NovaSensor	(10.222.125.220)

2.5. Handling of Upgrade Failure

• Scenario 1: Fail to start automatic installation.

Troubleshooting:

1. Check whether the host resources on the deployment environment are sufficient

2. Check whether the option to connect at power on is not selected when the image is selected for the added virtual CD/DVD drive.

• Scenario 2: Console cannot be accessed when deployment is finished and network has been configured.

Troubleshooting:

1. Check the resource configuration of the deployment environment. Check whether the data disk is configured and whether the data disk size is too small.

2. Check whether the MAC address of the management interface matches the MAC address of the NIC that the virtual machine uses to access the network.

• Scenario 3: Network error occurs after login to console

Troubleshooting:

1. Errors occur on pages of the console when Elasticsearch database is not started. In this case, wait for the Elasticsearch database to be started.

Log in to the background to check the console version has been Cyber Command 3.0.50C.

2.6. Rollback

None