Sangfor Hyper-Converged Infrastructure & Sangfor Cloud Platform

Release Notes

Product Version	6.9.0
Document Version	01
Released on	Aug. 11, 2023

Disclaimer

Products, services or features described in this document, whether wholly or in part, may be not within your purchase scope or usage scope. The products, services or features you purchase must be subject to the commercial contract and terms as agreed by you and Sangfor. 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 version upgrades or other reasons, the content of this document will be updated from time to time. Unless otherwise agreed, this document is used for reference only, and all statements, information, and recommendations therein do not constitute any express or implied warranties.

Technical Support

For technical support, please visit: https://www.sangfor.com/en/about-us/contact-us/technical-support

Send information about errors or any product related problem to tech.support@sangfor.com.

About This Document

This document is the release notes of Sangfor Hyper-Converged Infrastructure and Sangfor Cloud Platform version 6.9.0.

Intended Audience

This document is intended for:

- System / Network Administrator
- Technical Users

Note Icons

English Icon	Description
	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
	Indicates a hazardous situation, which if not avoided, could result in minor or moderate injury.
	Indicates a hazardous situation, which if not avoided, could result in settings failing to take effect, equipment damage, or data loss. NOTICE addresses practices not related to personal injury.
	Calls attention to important information, best practices, and tips. NOTE addresses information not related to personal injury or equipment damage.

Change Log

Date	Change Description
Aug. 11, 2023	This is the first release of this document.

Contents

1 HCI

1.1 Overview

1.1.1 Features

1. **Network health monitoring**: Support monitoring NIC health at the data link layer to promptly detect network latency and packet loss, quickly identify faults, and give alerts.
2. **RAID card status check**: Support monitoring the health of RAID cards in virtual storage. If it is detected that a RAID card has stopped running, the business system can promptly recover, and network isolation will be imposed on the corresponding node.
3. **Cyber attack protection**: Support to deploy aSecurity (aSEC) to configure cyber attack protection policies for VMs in the virtual network topology, protecting cloud-based business systems across seven layers of the communication process.
4. **Virtual patch protection**: Support deploying aSecurity (aSEC) for VM protection based on cyber attack protection policies to prevent vulnerability exploitation attacks without business interruption or VM restarts.
5. **Live migration across clusters**: Support live migration HCI6.3.0_R1_EN and HCI6.3.0_R2_EN to HCI6.9.0, avoiding business downtime and interruption caused by the cross-QEMU upgrade from an earlier version.

   For these 2 versions, the collection patch must be applied in order to support the migration across version.
6. **2-node cluster with 1 witness node**: For 2-node clusters, a physical endpoint device (box-type device) or virtual machine can be deployed to work as the witness node, effectively avoiding cluster split-brain failures and improving reliability.
7. **SNMP trap**: Support pushing configuration information, status information, and alerts of clustered nodes through SNMP traps. When an alert is triggered, it will be sent to a third-party monitoring platform through the SNMP trap API.

8. **Compatible with China's domestic GPUs**: With the support of X86 architecture, you can use three China domestically produced GPUs (Ascend Altas 300V Pro, Cambrian MLU270-S4, and Moore Threads MTT S2000) only in passthrough mode.
9. **Compatible with NVIDIA GPUs:** Support using Tesla P4 and A100-HGX-80G in passthrough or vGPU mode and using Quadro P4000, RTX 4000, RTX 5000, RTX 6000, T1000, T1000-8G only in passthrough mode.
10. **Encryption security compliance**: After encryption cards and HSMs are configured, support enabling SM encryption mode to protect critical data in information system applications by using compliant encryption algorithms, technologies, and products according to encryption security compliance requirements in China.
11. **Encryption cards**: Support using four domestic encryption cards (SYD1308-G and SJK1727 V2.0-A/B/C) in passthrough mode.
12. **HSMs**: Support using HSMs produced by Sansec and JIT to encrypt data of the HCI platform through the SM4 algorithm. HSMs can also be used to provide business services.
13. **Compatible with external storage:** Support adding non-ATS block storage devices as external block storage resources. Configure storage multipathing policies to provide link redundancy capabilities to enhance storage reliability.

1.1.1.1 Others

1. If HCI has been managed by SCP (earlier than SCP6.7.30) before upgrading to HCI6.9.0, please upgrade SCP to SCP6.7.30 and above (including SCP6.9.0) before upgrading HCI.
2. After upgrading SCP6.7.0 to SCP6.7.30 and above (including SCP6.9.0), please contact Sangfor Support for further inspection.
3. Since SCP6.8.0 has been containerized, to upgrade an earlier version to SCP6.8.0 or SCP6.9.0, please add a disk (400 GB) to the platform for container image storage so that databases will not be affected by disk IO from container images.

1. The offline licensing(virtual key) method is supported only when SCP6.8.0 is deployed on HCI6.8.0 or later.

2. When using a virtual key to upgrade to SCP6.8.0, the original license key file will become invalid, and required to renew the license key with the new device info. This licensing method is supported only when SCP6.8.0 is deployed on HCI6.8.0 or later. Therefore, resource pools of earlier versions may cause SCP licensing to fail.

3. It is required to use the licensing method with a USB key if aSecurity needs to be licensed.

1.1.2 Upgrade Methods

1.1.2.1 Active Upgrade(Quick Upgrade)

A quick upgrade is applicable to upgrade scenarios with the same host OS kernel version and is commonly used for upgrading a minor version to another of the same series (for example, 6.7.0_R2 > 6.7.0_R3) or upgrading one version to another released within a short period of time (for example, 6.7.0 > 6.8.0). Specifically, all physical nodes are directly upgraded without changing the run location and running status of VMs in the cluster. With the process active restart technology, a quick upgrade will only cause a business system jitter which will last for 3 seconds or shorter and will not interrupt the business system. A quick upgrade of the cluster takes a shorter time to complete.

A quick upgrade is mainly applicable to the following versions (and is commonly used for upgrading some of them):

Current Version	Target Version
HCI6.7.0_R1/R2	HCI6.8.0
HCI6.7.0_R1/R2/R3	HCI6.9.0
HCI6.8.0/R1	

1.1.2.2 Rolling Active Upgrade

In the event of host OS changes or kernel or driver version upgrades, all clustered nodes must be restarted, which will cause business service interruption. With live migration technology, rolling active upgrades can

significantly minimize the impacts on the services.

The rolling upgrade's functionality is migrating the VMs running on a node that needs to be upgraded to other nodes or clusters through live migration before restarting the node or cluster so that business services will not be interrupted. A rolling upgrade will not affect the business services, except that the live migration of VMs during the upgrade can cause business service fluctuations for about 1 second, and the overall upgrade process can be arranged.

The rolling upgrade will migrate production VMs running on nodes that need to be upgraded to other nodes in the same cluster and then migrate them back after the upgrade is complete and the upgraded nodes are restarted. The cluster to be upgraded must have sufficient resources. Rolling upgrade is mainly applicable to the following versions (and is commonly used for upgrading some of them):

Current Version	Target Version
HCI6.8.0 (Hygon)	sCloud 6.8.1 (Hygon)

1.1.2.3 Offline Upgrade

Offline upgrade requires all clustered nodes to be restarted. All clustered nodes must be restarted in the event of host OS changes or kernel or driver version upgrades. The cluster restart requires all business VMs to be shut down, making the business system unavailable. The offline upgrade is mainly applicable to the following versions (and is commonly used for upgrading some of them):

Current Version	Target Version
HCI6.0.0_R5_EN	HCI6.8.0
HCI6.3.0_R1/R2/R3_EN	
HCI6.0.0_R3/R4_EN	HCI6.9.0

1.1.3 Upgrade Path

1.1.3.1 Resource Pool Upgrade

Recommended Upgrade Path for HCI:

5.8.3 → Offline Upgrade → 6.0.0_R5 → Offline Upgrade → 6.9.0

5.8.6-6.0.0_R4 → Active Upgrade → 6.0.0_R5 → Offline Upgrade → 6.9.0

6.0.0 R5-6.3.0_R3 → Offline Upgrade → 6.9.0

6.7.0-6.8.0_R1→ Quick Upgrade/Rolling Upgrade → 6.9.0

The Versions Can Be Upgraded to HCI6.9.0:

aCloud 6.0.0 Series	6.0.0_R5_EN	-	-	-	**Offline Upgrade**
HCI6.0.1 Series	6.0.1_EN	6.0.1_R1_EN	-	-	
HCI6.1.0 Series	6.1.0_EN		-	-	
HCI6.2.0 Series	6.2.0_EN	6.2.70_EN	-	-	
HCI6.3.0 Series	6.3.0_EN	6.3.0_R1_EN	6.3.0_R2_EN	6.3.0_R3_EN	
HCI6.7.0 Series	6.7.0_EN	6.7.0_R2_EN	6.7.0_R3_EN	-	**Active Upgrade**
HCI6.8.0 Series	6.8.0	6.8.0_R1	-	-	

1.1.3.2 NFV Components Upgrade

Please upgrade the NFV components first if their version is lower than the version listed in the following table before upgrading the HCI.

Device	Version	HCI6.9.0	Classic Network	VPC	Notes
vAD	vAD6.6	√	√	-	
	vAD7.0.9_R1	√	√	√	
vNGAF	vNGAF7.1_R3	√	√	-	
	vNGAF8.0.8	√	√	-	Upgraded from vNGAF7.1_R3 is supported.
	vNGAF8.0.17	√	√	√	Support from vNGAF8.0.8 is supported. To use a customized version of

					vNGAF8.0.17, please install the upgrade package first and then the custom package.
	vNGAF8.0.26 (20200929)	√	√	√	Version patched supports both being installed using SSL service packs and being deployed.
vIAG	vIAG11.9	√	√	-	Must re-deploy.
	vIAG12.0.14	√	√	-	Upgrade from vIAG11.9 is supported.
	vIAG13.0.73	√	√	-	Recommend deploying this version of vIAG. Upgrade from the previous version is not supported due to insufficient partition size.
vSSL	vSSL7.6.0	√	√	-	
	vSSL7.6.8_R2 (20200928)	√	√	√	Support to deploy or upgrade by using the product upgrade package.

1.1.4 Upgrade Impacts

The impacts of upgrading HCI will vary depending on the upgrade method. For details, see the table below:

Method	Impacts on Services	Impacts on Customer O&M	Impacts on Customer Network
Quick Upgrade	A business system jitter will last for 3 seconds or shorter.	O&M personnel should not log in to the platform for operation and maintenance during the upgrade.	None
Rolling Upgrade	The business system performance will degrade (about 10 seconds) during migration, and I/O operations will be suspended for about 1 second.	O&M personnel should not log in to the platform for operation and maintenance during the upgrade. The upgrade will take	None

		about 40 minutes per node.	
Offline Upgrade	All VMs and NFV devices must be shut down before an offline upgrade. After the upgrade, they cannot be powered on before all 6.9.0 features take effect. The downtime will be around 1 hour.	O&M personnel should not log in to the platform for operation and maintenance during the upgrade.	None

The production VM can work after the platform is upgraded to 6.9.0 through a quick upgrade. However, the new version driver is not activated yet. You have to enter each cluster node in Maintenance Mode and restart them one by one during off-peak hours. The relevant features are described in the table below:

Upgrade Path	The impacts of not restarting the host	Remarks
6.7.0 > 6.8.0	None	None
6.8.0 > 6.9.0	Speed optimizations for VM cold migration do not take effect.	Changes to the kernel are not upgraded.
	Non-ATS storage cannot be mounted.	Changes to the driver module are not applied.

1.1.5 Upgrade Instruction for Customers

1. Before an upgrade, to ensure the business continuity of critical VMs, shutting down other virtual machines is recommended. Please check and record VMs that can be shut down in the table below:

System	Application Service	Run Location	Remarks
XX front end	Tomcat	XX.XX.XX.XX	XXXX

2. Before an upgrade, please confirm whether NFV devices need to be upgraded. Evaluate and arrange the time and personnel for the upgrade.

NFV Component	NFV Device Name	Run Location	Current Version	Target Version	Shutdown Allowed
NGAF	Egress firewall	XX.XX.XX.XX	XX.X.X	XX.X.X	Yes

3. An offline upgrade may take 4 to 6 hours. Please make appropriate time arrangements in advance and notify the business department to stop accessing the platform during the upgrade.
4. During the upgrade, O&M personnel of customers should not log in to the platform for operation and maintenance.

1.1.6 Implementation Procedure

1.1.6.1 Quick Upgrade

Type	Item	Estimated Time	Check with √ When Complete
Preparing for Upgrade	Check upgrade path		
	Obtain the latest aDeploy version		
	Prepare HCI update package		
	Check version information		
	Prepare license key		
	Read upgrade notes(in the release notes)		
aSecurity Upgrade	Upgrade aSecurity before upgrading MGR	About 30 minutes	
aNI Upgrade	Upgrade Network Insight (aNI) on HCI	About 30 minutes	
HCI Upgrade Process	Make sure there are no ongoing tasks	5 minutes	
	General page check	10 minutes	

	Health check	10 minutes	
	Enable maintenance mode	1 minute	
	Environment check before upgrading HCI	5 minutes	
	Upload HCI update package/Verify software edition	3 minutes	
	Distribute update package	Package size * Number of nodes/Transfer rate	
	Pre-upgrade check	15 minutes. The time varies according to virtual storage capacity. The larger the storage capacity is, the longer the upgrade process takes.	
	Control plane active upgrade	11 minutes	
	VM active upgrade	5 seconds for every 5 VMs with vmTools installed. 2 minutes for each VM without vmTools installed.	
	Virtual storage active upgrade	Number of clustered nodes*10 minutes	Related to the scale and load of VMs
	Active upgrade for virtual network	5 minutes	
	Apply new virtual storage version	Number of clustered nodes*10 minutes	
	Check business	30 minutes	
	License after upgrade	5 minutes	

1.1.6.2 Rolling Upgrade

Type	Item	Estimated Time	Check with √ When Complete
	Check upgrade path		

Preparing for Upgrade	Obtain the latest aDeploy version		
	Prepare HCI update package		
	Check version information		
	Prepare license key		
	Read upgrade notes(in the release notes)		
aSecurity Upgrade	Upgrade aSecurity before upgrading MGR	About 30 minutes	
aNI Upgrade	Upgrade Network Insight (aNI) on HCI	About 30 minutes	
HCI Upgrade Process	Make sure there are no ongoing tasks	5 minutes	
	General page check	10 minutes	
	Health check	10 minutes	
	Environment check before upgrading HCI	5 minutes	
	Upload HCI update package/Verify software edition	3 minutes	
	Distribute update package	Packet size/Transfer rate-Packet size*2/Transfer rate	
	Pre-upgrade check	15 minutes	The larger the virtual storage capacity is, the longer the upgrade process takes.
	Enable Maintenance Mode for the cluster	1 minute	
	Control plane active upgrade	25 minutes	
	Disable Maintenance Mode for the cluster	1 minute	
	Live migration of VMs across nodes in the same cluster	3 minutes for each VM	The migration time of each VM varies according to the data

			volume and I/O status when the VM is running.
	Enable Maintenance Mode for nodes	1 minute	Related to the cluster size and workload.
	Virtual storage active upgrade	10 minutes	
	Active upgrade for virtual network	5 minutes	
	Restart server manually	10 minutes	
	Disable Maintenance Mode for nodes	1 minute	
	Repeat the preceding steps (starting from the live migration of VMs)	About 40 minutes for each node	
	Check business	30 minutes	
	License after upgrade	5 minutes	

1.1.6.3 Offline Upgrade

Type	Item	Estimated Time	Check with √ When Complete
Preparing for Upgrade	Check upgrade path		
	Obtain the latest aDeploy version		
	Prepare HCI update package		
	Check version information		
	Prepare license key		
	Read upgrade notes(in the release notes)		
aSecurity Upgrade	Upgrade aSecurity before upgrading MGR	About 30 minutes	
aNI Upgrade	Upgrade Network Insight (aNI) on HCI	About 30 minutes	

HCI Upgrade Process	Make sure there are no ongoing tasks	2 minutes	
	General page check	10 minutes	
	Health check	5 minutes	
	Shut down all VMs	20-30 minutes	
	Shut down all NFV devices	10 minutes	
	Enable maintenance mode	1 minute	
	Check environment for upgrade	1 minute	
	Upload HCI update package	1 minute	
	Verify the update package via the QR code	1 minute	
	Distribute update package	Package size * Number of nodes/Transfer rate	
	Check environment	15 minutes	
	Perform offline upgrade	30 minutes	
	Power on VM	10 minutes	
	Check business	5 minutes	

The larger the cluster is, the longer it takes to convert the configuration file and the longer the upgrade time.

1.1.7 Post Upgrade Check

1.1.7.1 HCI Platform

PIC: Sangfor engineer

- Perform a health check on the HCI platform (**Virtual Storage Data Check** must be selected) and ensure all services work.
- Use aDeploy to perform a health check on the HCI platform and fix all issues according to the solutions.

- Install all SPs for the corresponding version according to check results of aDeploy.

1.1.7.2 Application System

PIC: Sangfor engineer and customer's O&M personnel

- Check whether all VMs installed with a guest OS are working and whether there are alerts, suspended, or failed VMs.
- Check whether the guest OS or console of VMs can be accessed and whether the file system works well.
- Check whether all application services are available and running without an unexpected shutdown, restart, etc.
- Analyze the causes of all the anomalies detected above and handle them promptly.

1.1.7.3 Business System

PIC: Sangfor engineer and customer's business personnel

- Verify whether services provided by the business system can be accessed by performing some common operations to see whether anomalies occur.
- Verify business system data by performing data addition, deletion, modification, and query to see whether anomalies occur.
- Verify the privileges of the business system by performing unauthorized operations to see whether anomalies occur.
- Analyze the causes of all the anomalies detected above and handle them promptly.

1.1.8 Rollback

The HCI platform is the infrastructure of business systems, and its upgrade process is relatively complicated. Arrange technical support engineer to ensure a smooth upgrade. During the upgrade, a team must be assigned to troubleshoot issues at different upgrade stages and confirm whether rollback is required. The specific rollback scenarios and upgrade stages are shown in the table below (rollback must be performed under the guidance of the R&D

personnel):

Item	Impacts on Services	Rollback Mechanism
aSecurity upgrade	None	Cancel the upgrade for rollback
aNI upgrade	None	Cancel the upgrade for rollback
Environment check before upgrading HCI	None	N/A
Upload/Distribute update package	None	Cancel the upgrade for rollback
Pre-upgrade check	None	Cancel the upgrade for rollback
Enable Maintenance Mode for the cluster	None	Disable Maintenance Mode for the cluster
Control plane active upgrade	None	Cancel the upgrade for rollback
VM active upgrade	IO fluctuation for 1 second	Cancel the upgrade for rollback
Virtual storage active upgrade	IO fluctuation for 1-3 seconds	Cancel the upgrade for rollback
Active upgrade for virtual network	IO fluctuation for 1 second	Cancel the upgrade for rollback
Apply storage features of the new version	None	Perform rollback according to the actual situation
Check business	Depending on the check method	N/A
License after upgrade	None	Revoke license

NOTE

1. If the current version is earlier than 5.8.6/6.7.0 and needs to be upgraded to a version later than 5.8.6/6.7.0, contact a Sangfor technical support representative in advance to ensure a smooth upgrade.

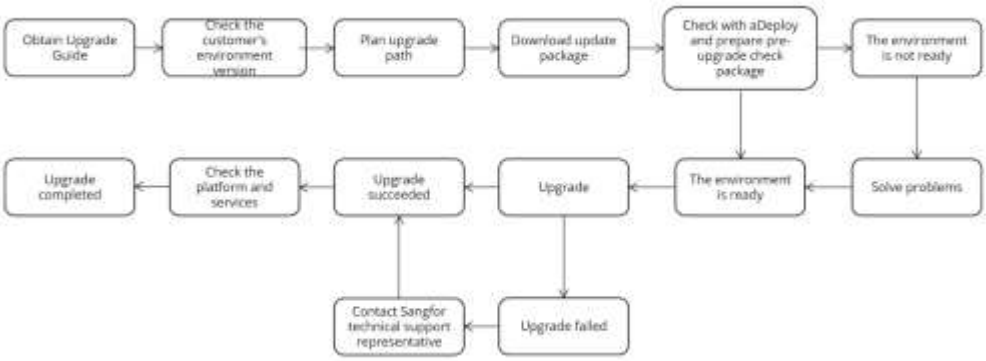
2. If the HCI upgrade fails, do not close the upgrade page and contact a Sangfor technical support representative for rollback.

1.2 Upgrade Guide

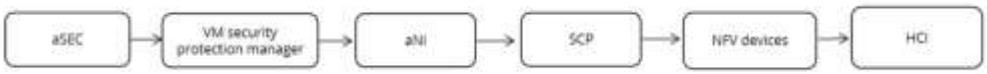
1.2.1 Upgrade Instructions

1.2.1.1 Upgrade Steps

Please follow the following steps to upgrade:



1.2.1.2 Upgrade Sequence



1.2.2 Upgrade Notes

General scenarios:

1. Before upgrading, please use the latest version of aDeploy (download address: https://download.sangfor.com/Download/Tools/aDeploy/aDeploy-server-en-install.zip to perform a pre-upgrade check and install a pre-upgrade check package.
2. If the current version is earlier than 5.8.6/6.7.0 and needs to be upgraded to a version later than 5.8.6/6.7.0, to ensure a smooth upgrade, contact a Sangfor technical support representative in advance.
3. A rolling active upgrade to HCI6.9.0 does not automatically restart the physical server. After the upgrade is complete, it is recommended to manually restart the physical server to make the upgrade take effect during off-peak hours.

4. Before upgrading, please ensure the license key is valid. Otherwise, the platform cannot be upgraded.

SP Installation:

1. If the current version contains custom packages (packages name: Custom-XXX), please contact a Sangfor technical support representative for upgrade evaluation.
2. If the current version contains SPs (packages name: sp-XXX), it can be upgraded directly.

Graphics Cards:

1. If the current version is earlier than 6.7.0, a GRID driver (supported versions 10.2 and 13.2) for HCI6.9.0 must be reimported again after the upgrade. After the HCI platform is upgraded and restarted, import a GRID driver for nodes as needed and then restart the nodes. Driver updates are also required for business VMs and will take effect after they are restarted.
2. If graphics cards are used in versions earlier than 6.2.0, aGPU license key is required after the upgrade. Otherwise, GPU-related features cannot be used.

iSCSI Virtual Disks

1. HCI cannot be upgraded when it provides services as an iSCSI server. Before upgrading, please go to iSCSI clients to disconnect all related connections.

Offline Upgrade

During the pre-upgrade check for an offline upgrade, if a message is prompted saying, "**A VM is running on the node. Please shut down the VM and try again.",** you can ignore this problem temporarily. Before an official upgrade, all virtual devices must shut down and run a pre-upgrade check again.

1.2.3 Upgrade Preparations

1.2.3.1 Packages, Documents, and Tools

Packages:

Name	Description	Obtain Through
HCI6.9.0 update package	Used for upgrading from an earlier version to HCI6.9.0.	Sangfor Community https://community.sangfor.com/plugin.php?id=service:download&action=view&fid=47#/12/all
HCI6.9.0 Witness node update package (**stretched cluster**)	Used for upgrading from an earlier version to HCI_Witness_ HCI6.9.0.	

Documents:

Name	Description	Obtain Through
HCI6.9.0 User Manual	Describes basic O&M and configuration in HCI.	Sangfor Knowledge Base https://knowledgebase.sangfor.com/indexPage?module=645
aDeploy User Guide	Provides instructions for using aDeploy.	

Tools:

Name	Description	Obtain Through
Chrome/Edge	The browser to access HCI and SCP web console.	Obtain from the internet.
PuTTY/MobaXterm	An SSH client for troubleshooting if needed.	Obtain from the internet.
MD5	Used for verifying the integrity of the upgrade package.	Check it when downloading the package file.
aDeploy	Used for pre-upgrade checks and other checks with aDeploy.	Sangfor Community https://community.sangfor.com/plugin.php?id=service:download&action=tool

License Key	1. For a version earlier than HCI5.8.2, please apply for a new HCI license key. 2. If the NFV devices need to be upgraded according to **Chapter 1.3.3 NFV Components**. Please apply for a new NFV license key. 3. Before upgrading, please confirm that the customer's license is not expired. Otherwise, the environment needs to be renewed. 4. Before upgrading, please check that the original NFV license key has not expired. Otherwise, the license needs to be renewed.	Contact corresponding personnel to obtain or confirm.

1.2.3.2 Environment Information

Fill in the corresponding IP information in the table below.

Type	Classification	IP Address	Netmask	Remarks(ETH)
HCI	The IP address for the management network			
	The IP address for the overlay network			
	The IP address for the storage area network			
	Elastic IP pool			
Physical	BMC NIC			

server				
Ethernet switch	The IP address for the management interface			

1.2.3.3 Customer Resources Coordination

During the upgrade, O&M personnel should not log in to the platform for operation and maintenance.

An offline upgrade may take 4 to 6 hours. Please make an appropriate time arrangement in advance and prepare for service interruption during the upgrade to reduce impact.

Before the active upgrade, please confirm whether NFV component versions need to be upgraded and evaluate the required upgrade time.

Please coordinate resources in advance according to the following requirements to ensure a smooth upgrade:

1. Determine when to upgrade and fully prepare for service interruption during the upgrade to reduce impact.
2. Obtain contact information of the responsible persons.
3. Ensure a computer (with Internet access and a stable connection to the device) is ready. Ensure the computer can install and run the upgrade client software.

Type	Name	Contact	Responsible For
Sangfor Technologies Inc.			Upgrading HCI and SCP
Customers			Coordinating resources and upgrade time. (Upgrade time:)
			Ensure O&M personnel will not log in to the platform for operation and maintenance.
			Arrange persons responsible for application systems to handle service

			opening and verification issues.

1.2.4 Pre-upgrade Check

1.2.4.1 Health Check

Click **Health Check** on the home page to go to the health check page. In addition to the default entities, select **Virtual Storage Data** and click **Start.** After the check is complete, if the score is lower than 100 points, handle the identified problems according to the check results and solutions, and then perform Health Check again. Before upgrading, please confirm that the health check score is 100 points.

1.2.4.2 Check with aDeploy

Apart from health check features, aDeploy supports checking common problems of customers. It optimizes the platform-based check mechanism and can check the environment before upgrading. If faults or alerts are reported, please handle the faults and alerts for the cluster before upgrading.

Refer to **Chapter 1.2.3.1 Packages, Documents, and Tools,** for the download link.

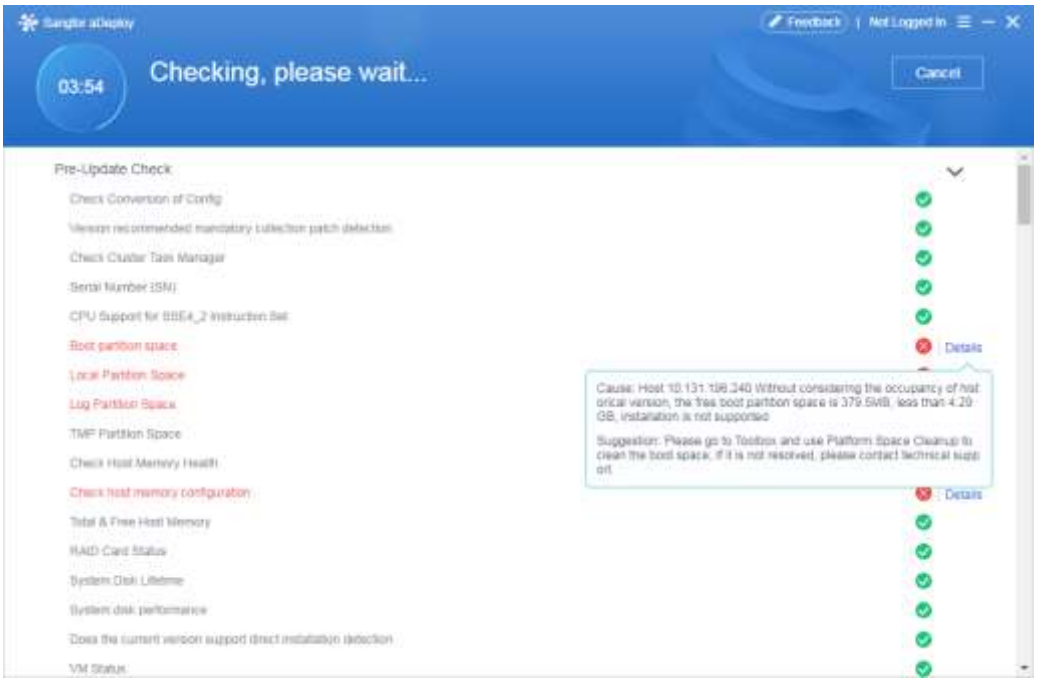
1.2.4.3 HCI Pre-Upgrade Check

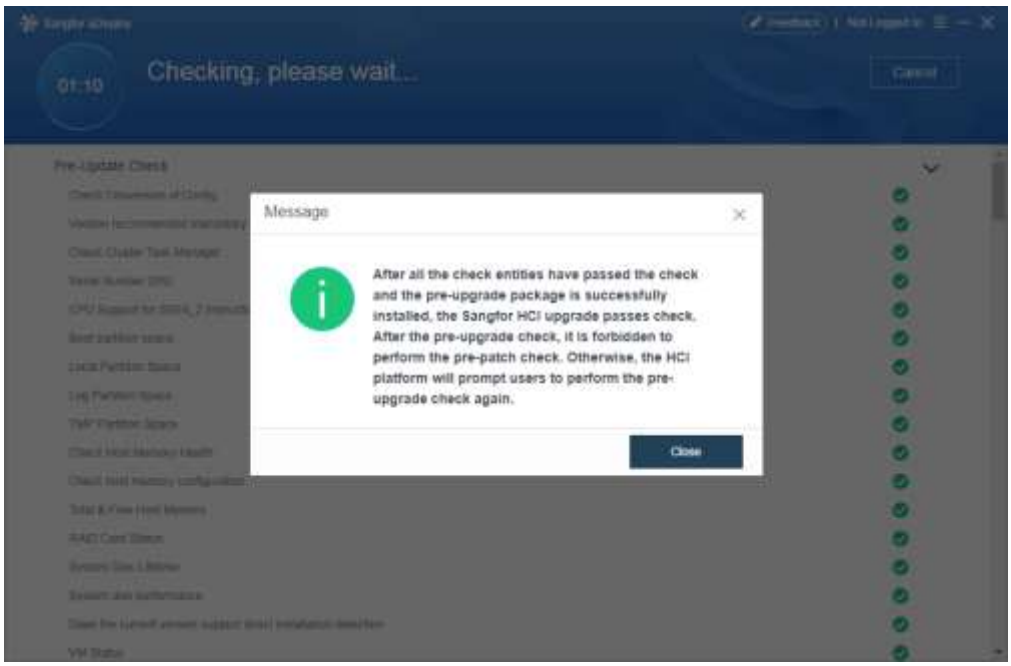
One week before upgrading HCI for a customer, please visit the customer or establish a remote connection to check whether the customer's environment meets the upgrade requirements using the pre-upgrade check package. This will help facilitate the subsequent upgrade process and does not require downtime. Make sure a pre-upgrade check is done before an official upgrade. If the pre-upgrade check for an official upgrade fails, it is recommended to reschedule for the upgrade.

Step 1. Use aDeploy to perform a pre-upgrade check and wait for the check to complete. Click **Details** next to the failed entities and handle them according to the solutions. Perform the pre-upgrade check again until all the entities pass the check.

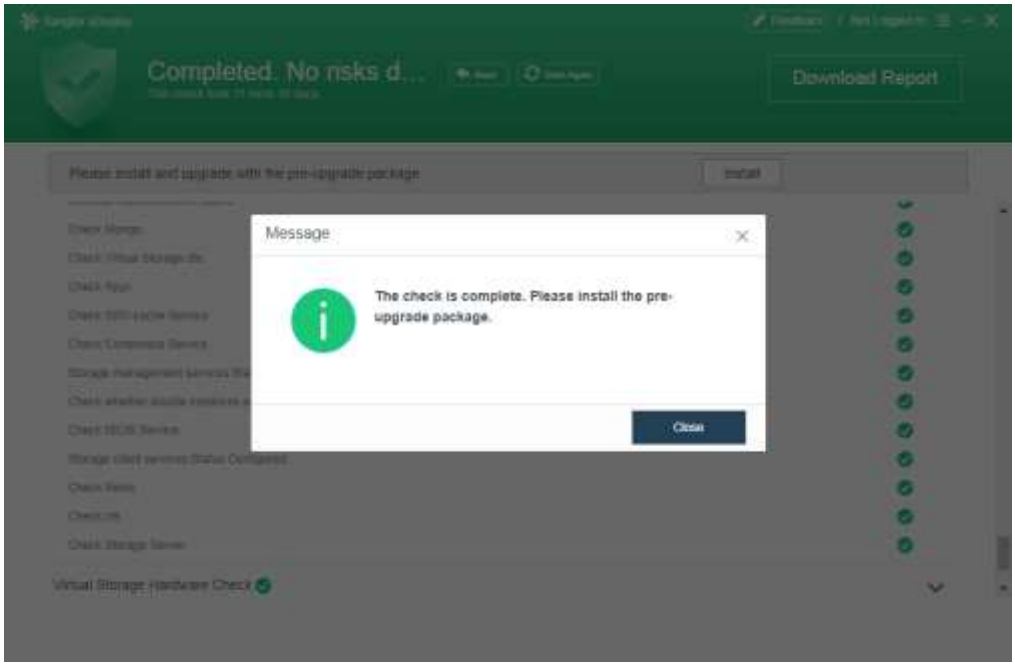
NOTICE

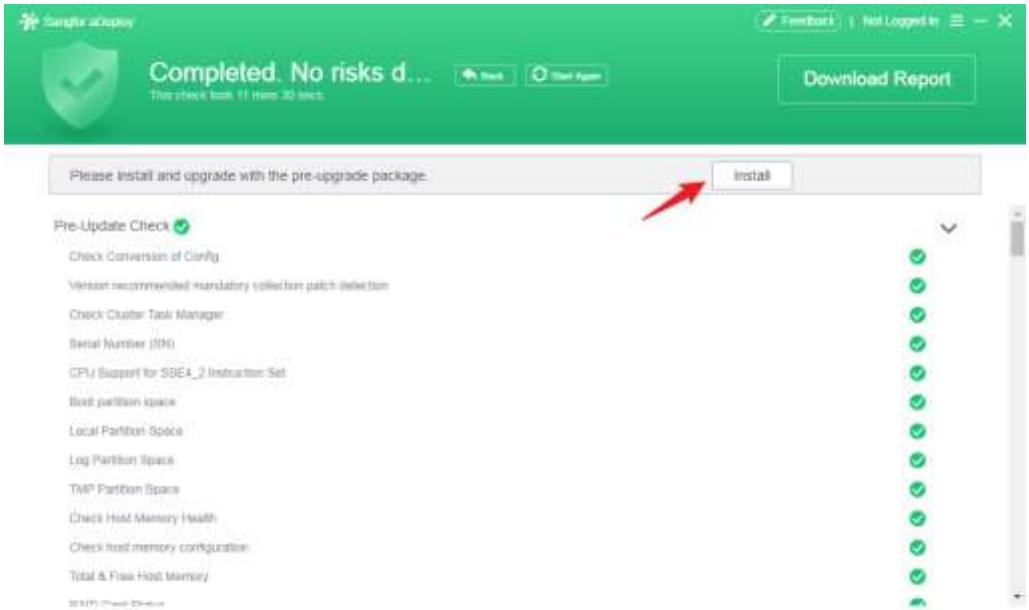
SP pre-installation check is prohibited after the pre-upgrade check. Else, HCI will request you to run the pre-upgrade check again.

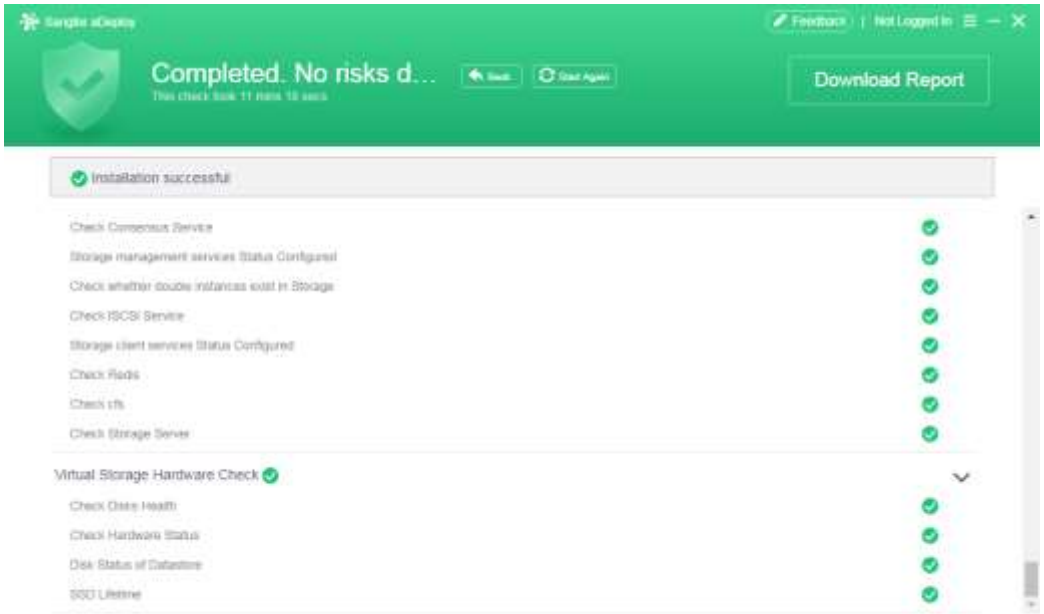




Step 2. After all the entities pass the check, click **Install** and wait for the installation to complete.







4. Troubleshooting instructions

a. For an offline upgrade, a message will be displayed after the pre-upgrade check is completed, indicating that a VM is running on the node. You may ignore this message temporarily. **Before an official upgrade, all virtual devices must shut down, and run a pre-upgrade check again.**

b. If the pre-upgrade check fails and a message indicates the pre-upgrade check failure, please contact a Sangfor technical support representative.

c. If a clustered node fails the pre-upgrade check and the pre-upgrade check does not proceed for more than 10 minutes, please contact a Sangfor technical support representative.

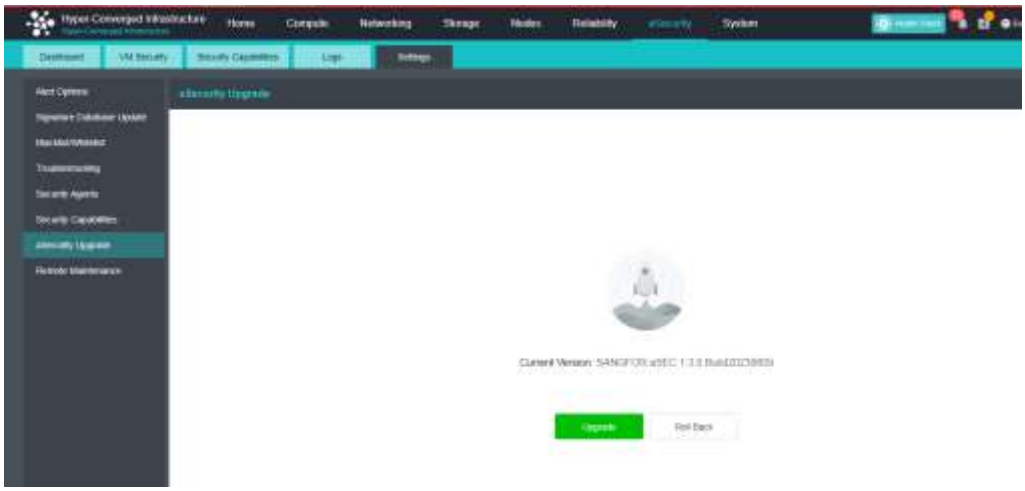
d. In versions earlier than HCI6.9.0, VM names can only contain digits, spaces, letters, Chinese characters, and special characters (（）【】_-.+()@). Invalid VM names will cause the pre-upgrade check to fail.

1.2.5 Upgrade Procedure

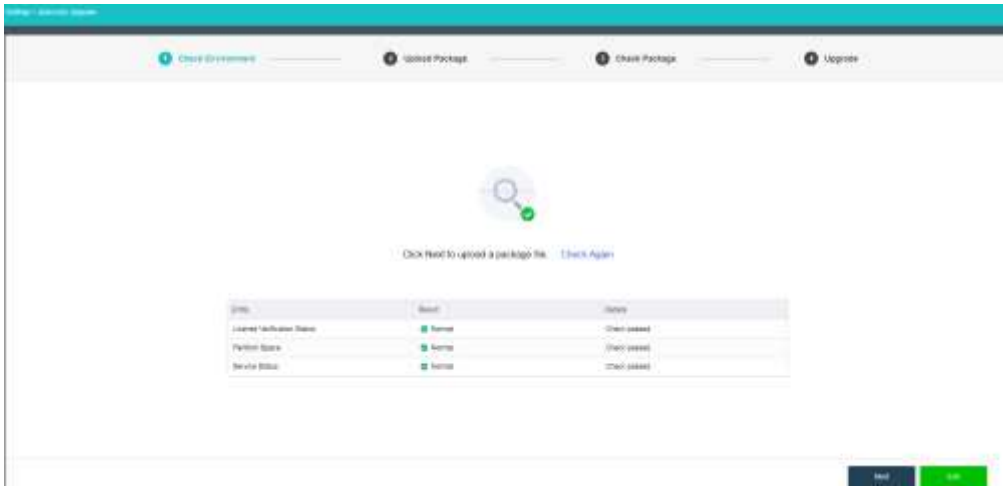
1.2.5.1 aSecurity Upgrade

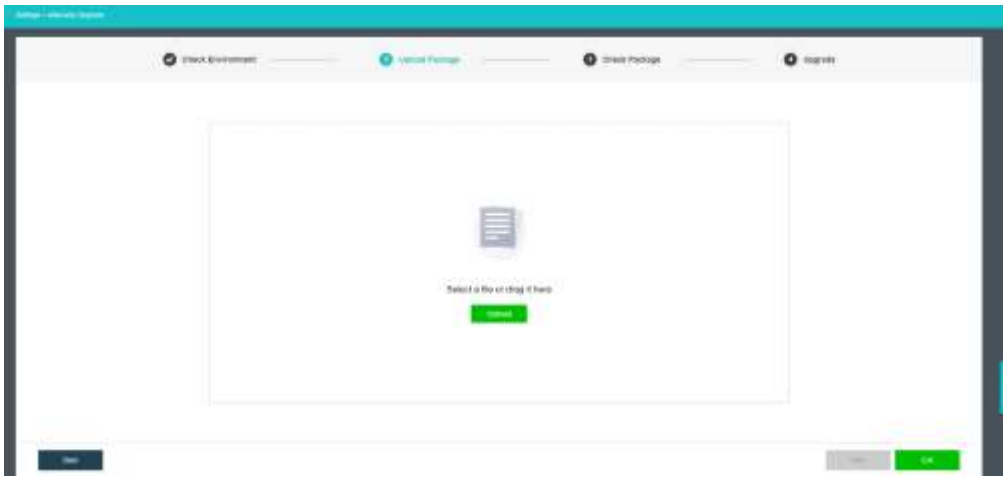
1. Upgrade aSecurity

Step 1. Go to **aSecurity > Settings > aSecurity Upgrade** and click **Upgrade**.



Step 2. Click **Next** to import the update package. Click **Next** after a successful import. If the update package passes the verification, click **Upgrade** and wait for the upgrade to complete. aSecurity will automatically restart after the upgrade is complete. The upgrade process will take about 30 minutes.





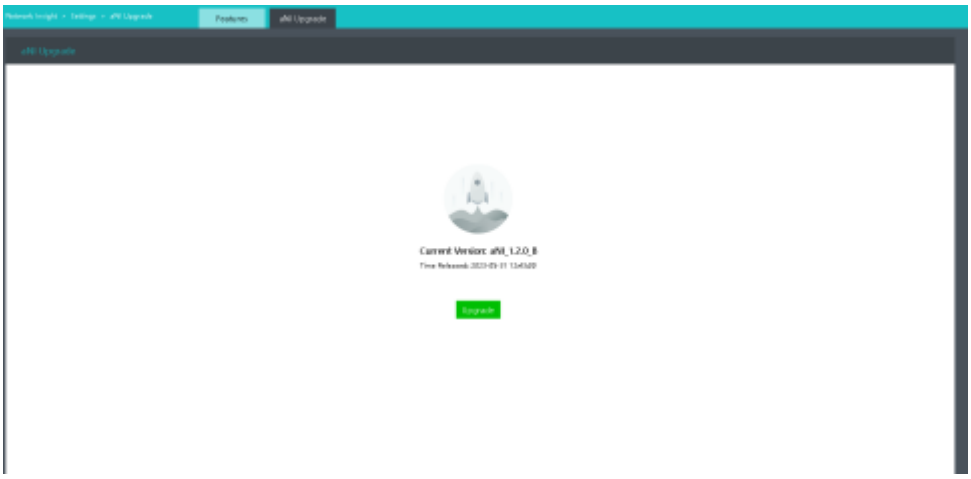
Step 3. After the upgrade, platform authentication, and licenses must be obtained again to use aSecurity capabilities.

2. Upgrade Security Protection Manager(Endpoint Secure)

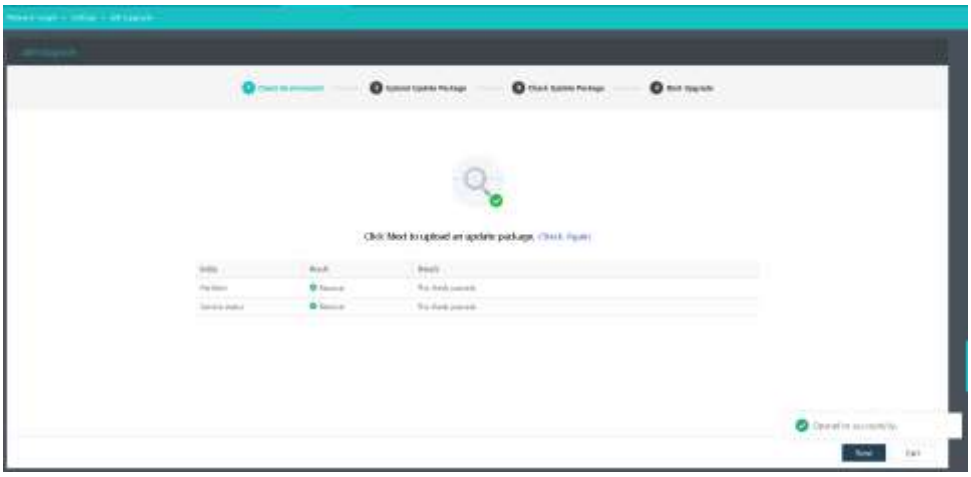
   To upgrade **Security Protection Manager(Endpoint Secure)**, kindly contact **Sangfor Technical Engineer** for assistance.

1.2.5.2 aNI Upgrade

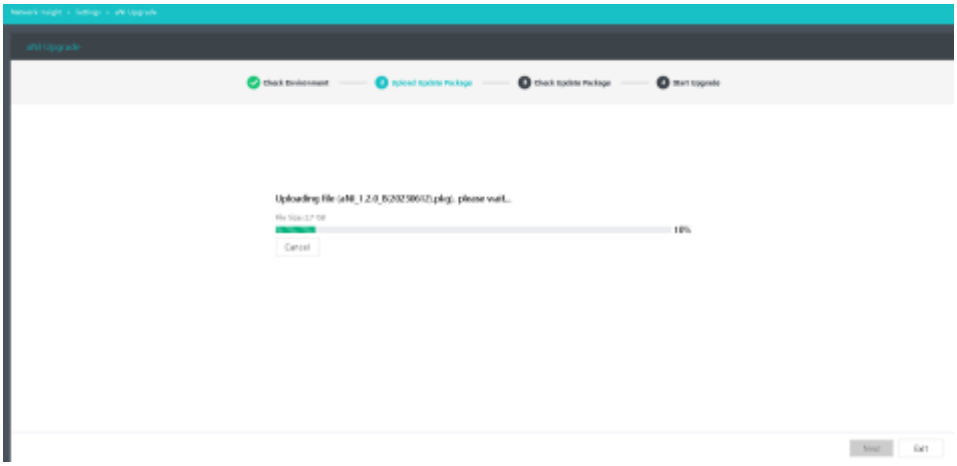
1. Go to **Networking** > **Network Insight** > **Settings** > **aNI Upgrade** and click **Upgrade**.

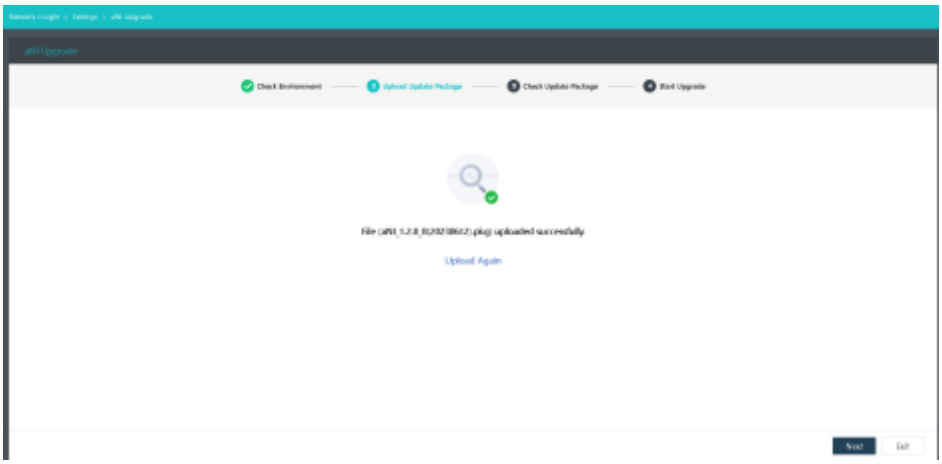


2. Wait for the environment check to complete.

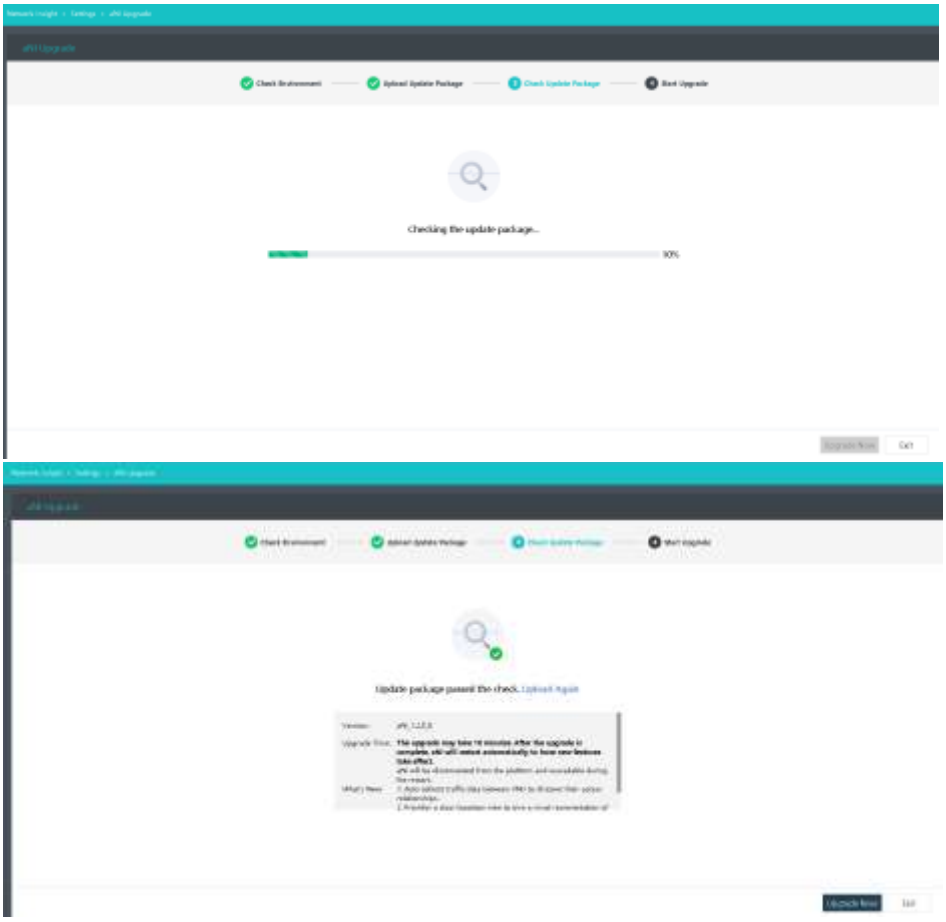


3. Upload the update package.



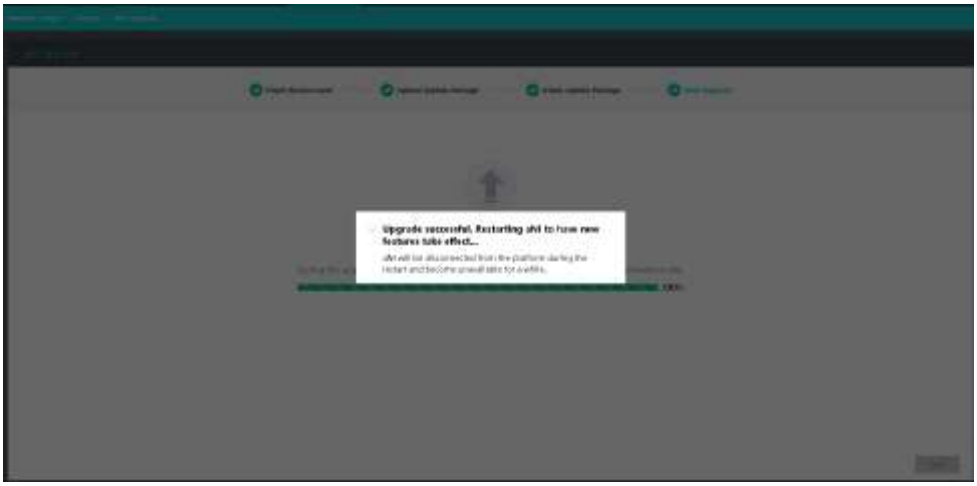


4. Wait for the update package check to complete.

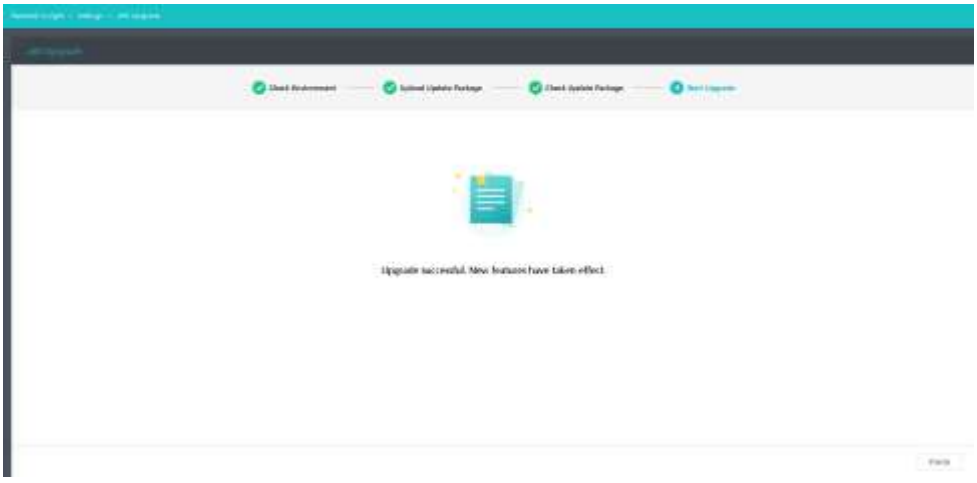


5. Start the upgrade.

6. Restart aNI.



7. The upgrade is complete.



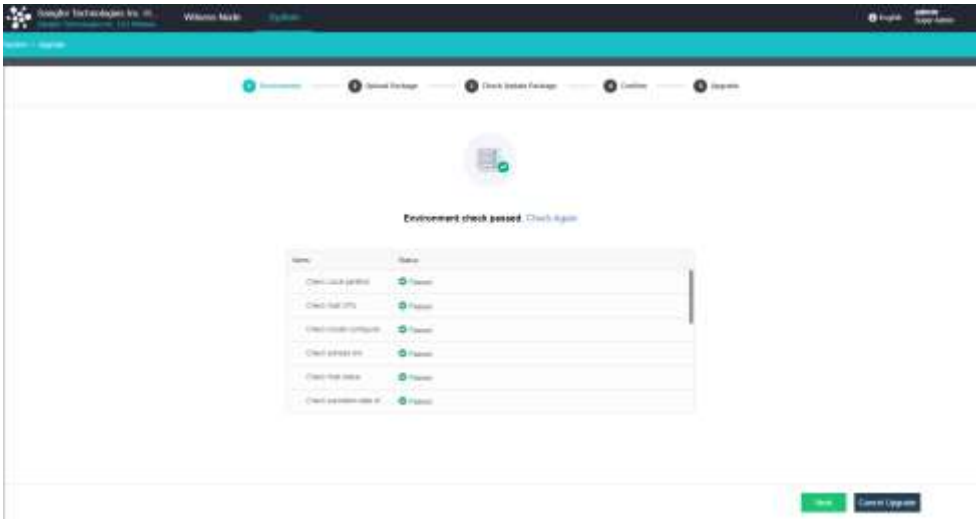
1.2.5.3 NFV Component Upgrade

For the upgrade procedure for NFV components, refer to the upgrade guide for corresponding products.

1.2.5.4 Witness Node Upgrade

Please upgrade the witness node before upgrading the stretched cluster or "2+1" cluster environment (skip the following steps if the HCI cluster is non-stretched).

1. Go to the witness node management page and click **Upgrade**.
2. The witness node will enter cluster upgrade mode during the upgrade, and the cluster environment check will run.



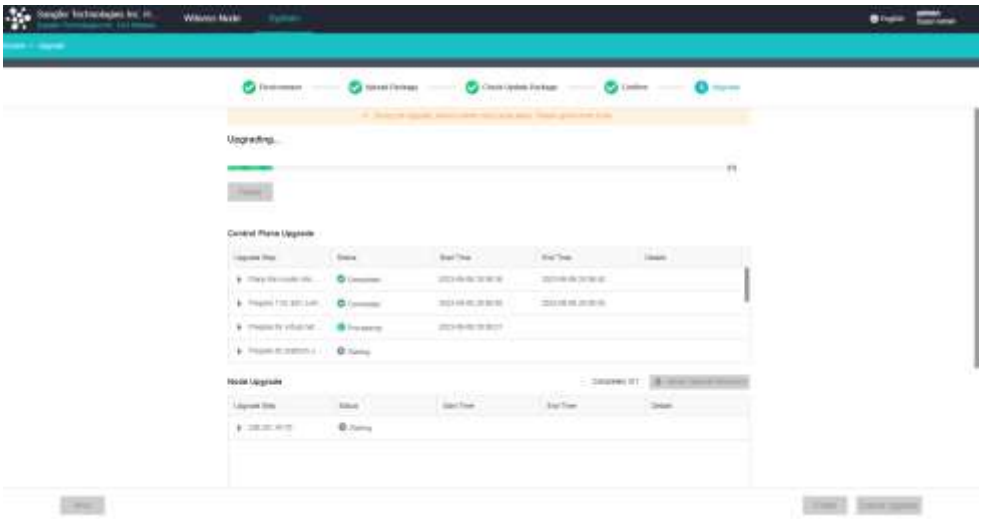
3. Upload the witness node update package.

4. Check the update package. (If the current version does not support the active upgrade using the update package, click **Next** to perform an offline upgrade. If the active upgrade is supported, please wait until all checking steps are finished before the upgrade. If any step fails, fix the issues first.)

1.2.5.4.1 Active Upgrade

1. After confirming that the update package is correct, click **Next**.

2. During the control plane upgrade, you will be logged out. Please wait about 1 minute and then reload the page to log in again.



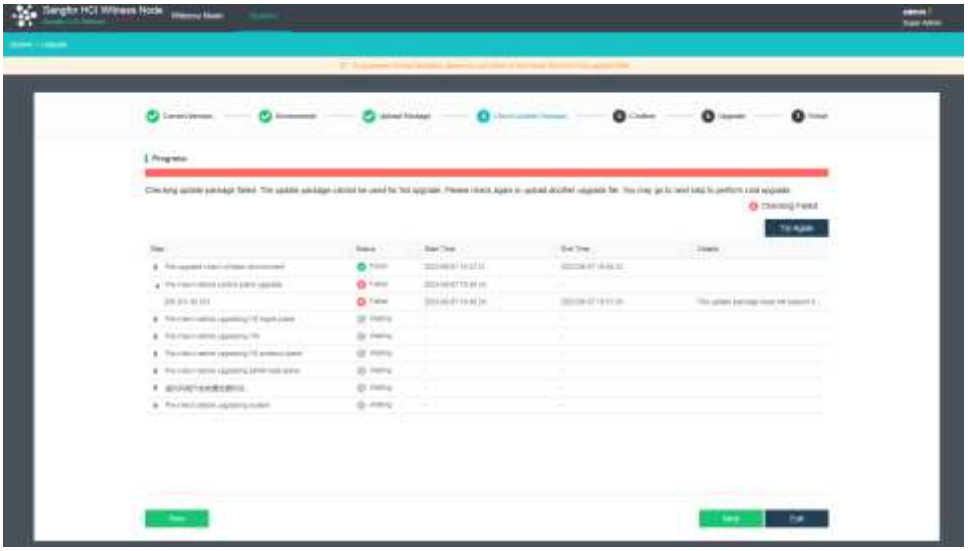
3. The upgrade is complete.

4. Check that the current version is the latest version.

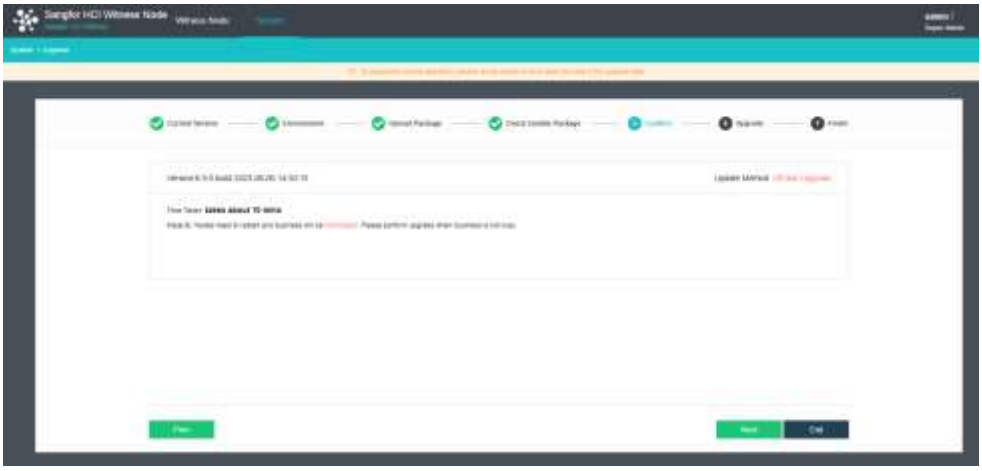
After the upgrade, please wait for the background of the witness node to take effect before upgrading other nodes in the cluster.

1.2.5.4.2 Offline Upgrade

1. After confirming that the update package is correct, click **Next**.

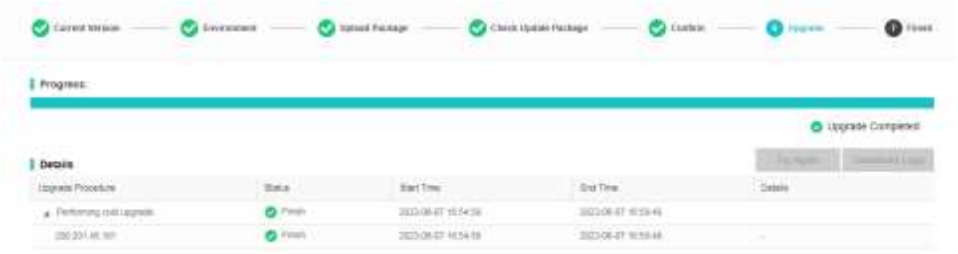


2. The offline upgrade requires all nodes to be restarted, which will cause business service interruption.



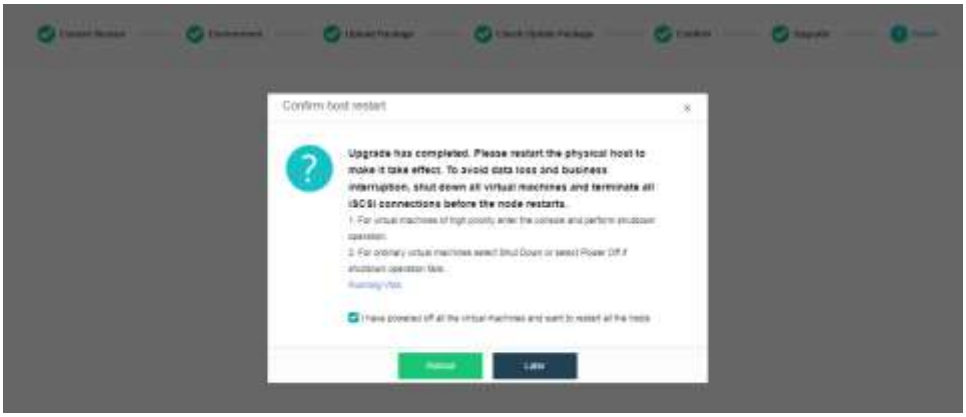
3. Click **Next** to start the upgrade.

4. The upgrade progress is shown in the figure below.



5. The upgrade is complete.

6. Restart the nodes.



NOTICE

After the offline upgrade of the witness node is complete, and the witness node is restarted, its status will still be displayed as offline. It is because the version of the witness node is inconsistent with other nodes in the cluster. To solve this problem, please upgrade other nodes.

1.2.5.5 HCI Upgrade

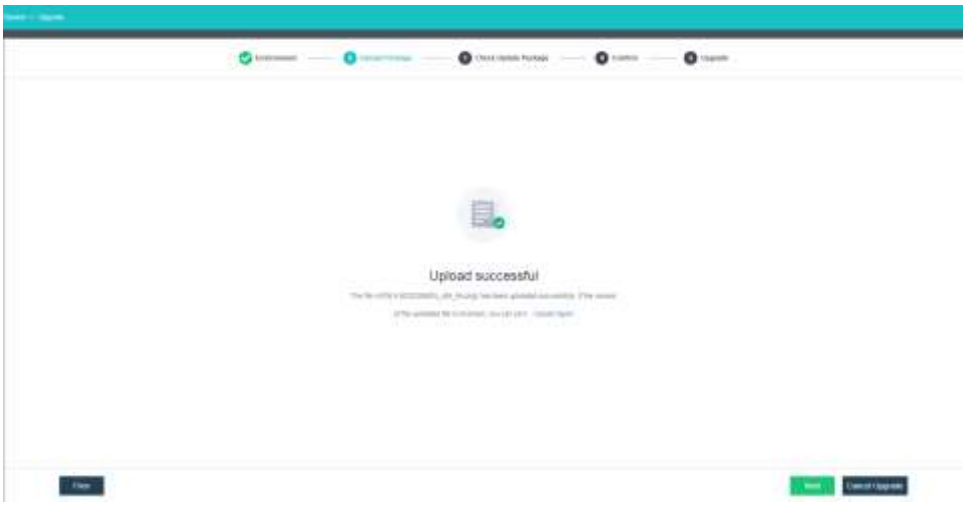
1. Use aDeploy to perform the pre-upgrade check and install the pre-upgrade check package (see Chapter 2.4.3 HCI Pre-Upgrade Check), then go to **System** > **Upgrade** and click **Start Upgrade**. The cluster will enter Maintenance Mode and run the environment check.

NOTICE

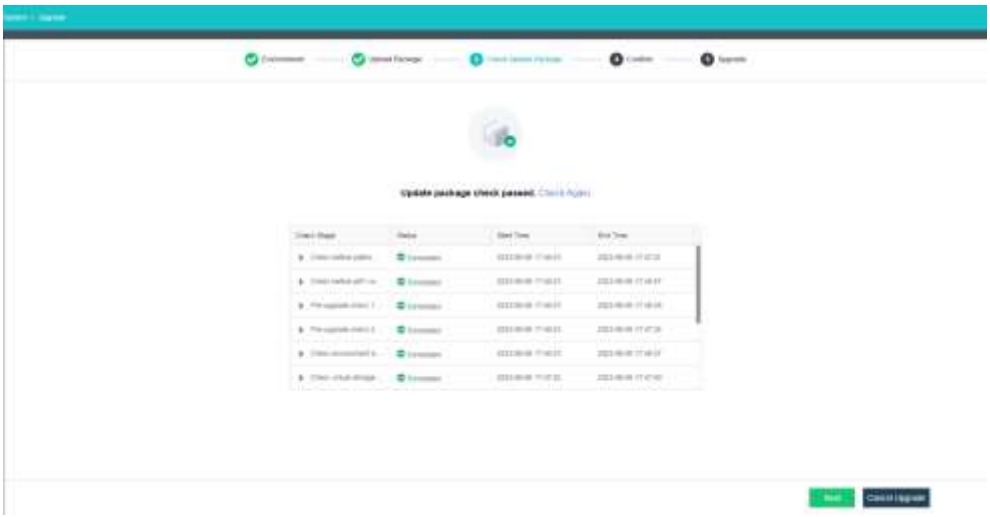
After the pre-upgrade check package is installed, a suffix will be displayed in Current Version, as shown in the figure above.

2. Click **Start Upgrade**. The environment check starts.

3. After the environment passes the check, upload the HCI update package.

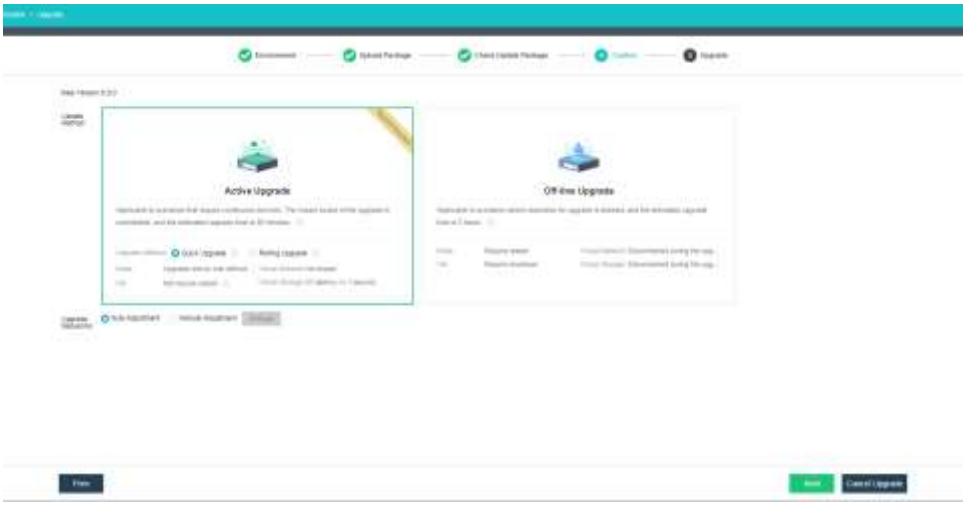


4. The update package passes the check.

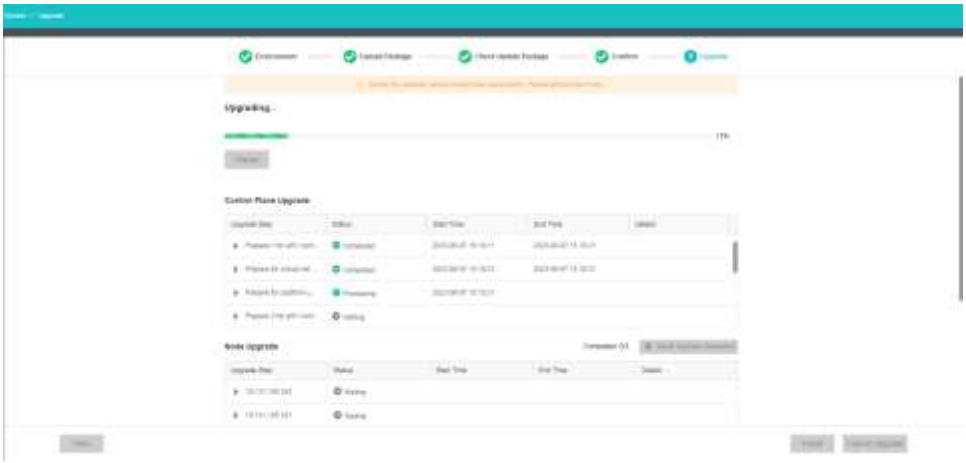


1.2.5.5.1 Quick Upgrade

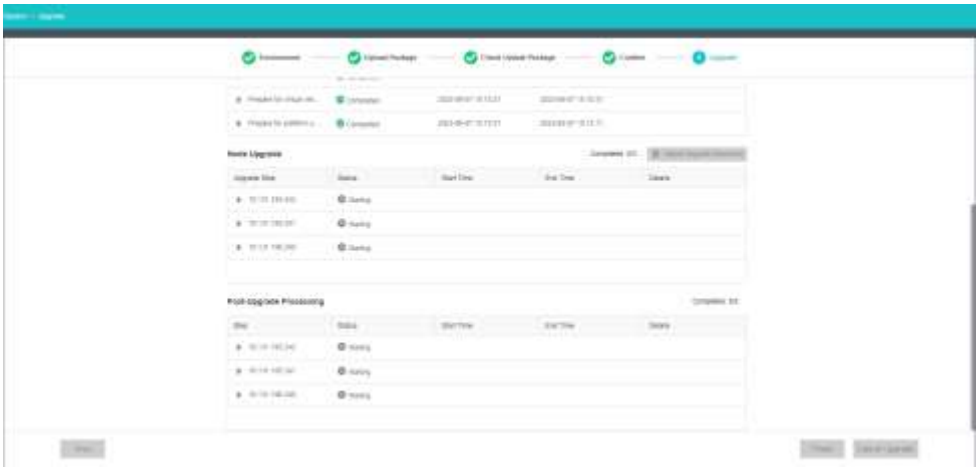
1. Select **Quick Upgrade** for **Upgrade Method** and click **Next**.



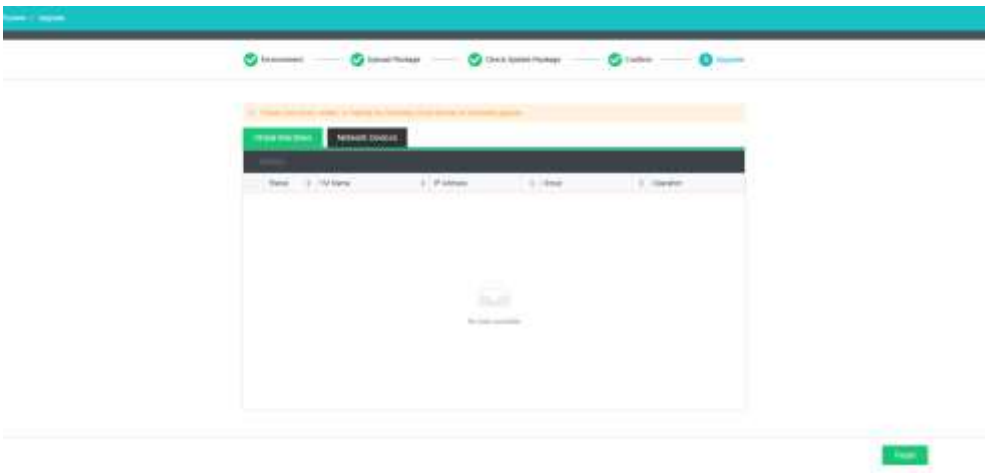
2. The quick upgrade starts.



3. The upgrade tasks at each stage are shown during the upgrade process.



4. After the upgrade, the system will ask whether to perform live migration for VMs and NFV devices. VMs not installed with vmTools need to be migrated to complete the upgrade.

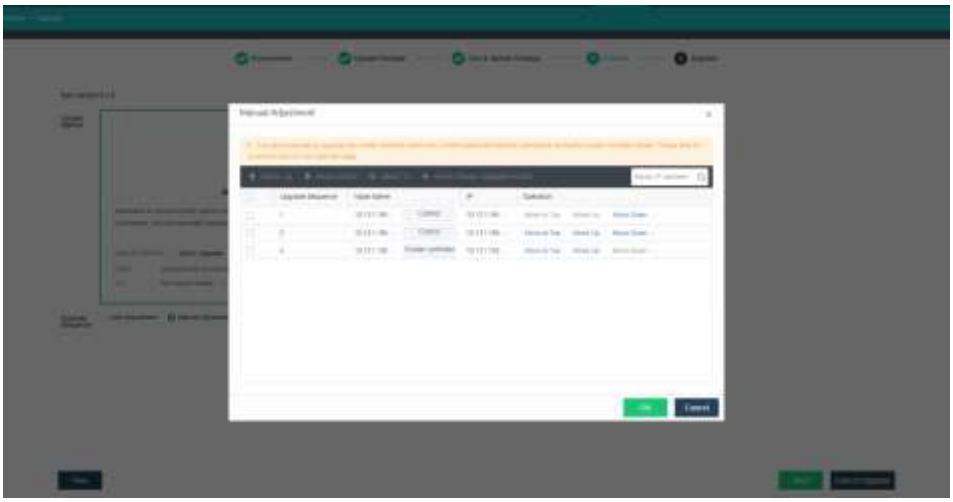


5. The upgrade is complete.

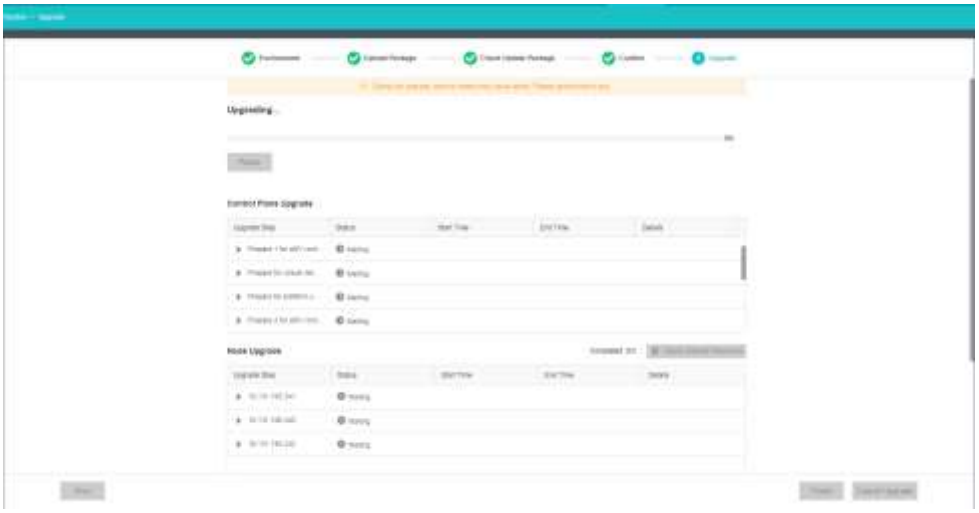
1.2.5.5.2 Rolling Upgrade

1. Select **Rolling Upgrade** for **Upgrade Method** and click **Next**.

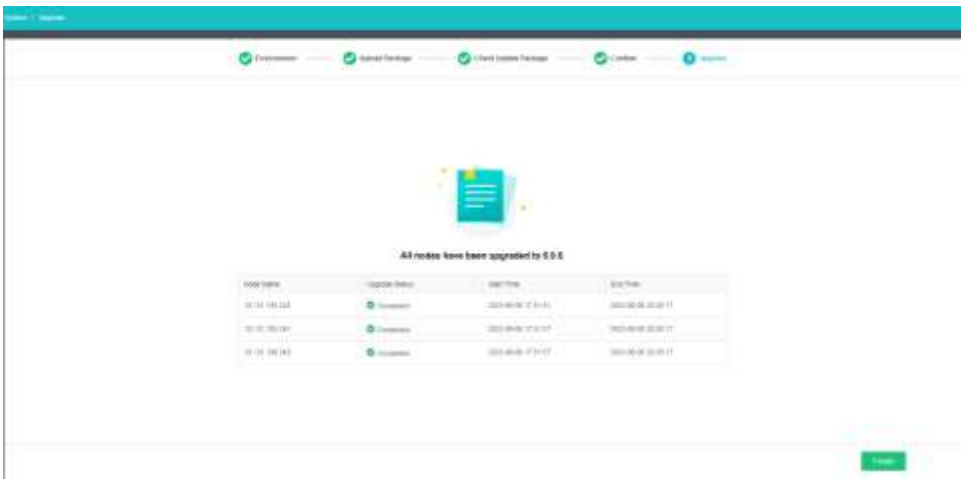
2. Select **Manual Adjustment** for **Upgrade Sequence** to adjust the sequence of nodes for the upgrade, or select **Auto Adjustment**. After the upgrade sequence adjustment is complete, click **Next**.



3. During the Rolling upgrade, all the nodes' control planes will upgrade first, followed by the data plane upgrade (one node each time). Before the data plane upgrade starts, the running VMs will be migrated to a node that is not in the upgrading state. During the control plane upgrade, you will be logged out. Please wait about 1 minute and then reload the page to log in again.



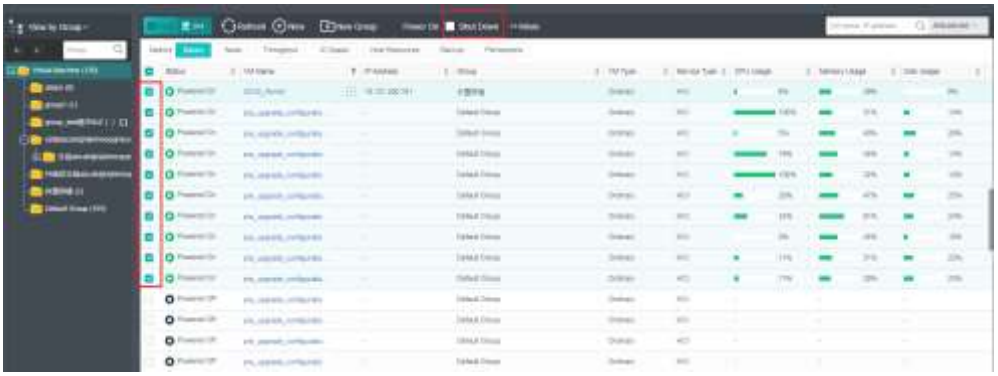
4. The upgrade is complete.



1.2.5.5.3 Offline Upgrade

1. Shut down all VMs.

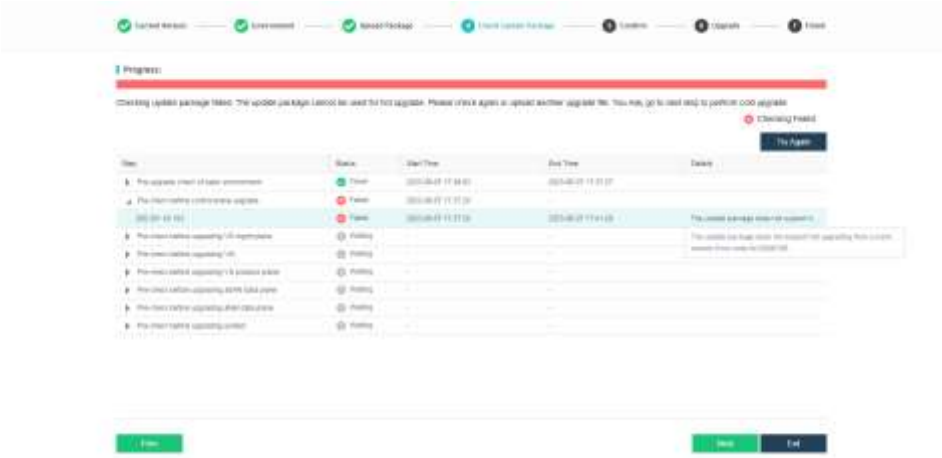
   Select all VMs and shut them down. If the operation fails, go to their consoles to shut them (including suspended VMs) down separately.



2. Shut down all NFV devices.

   Go to **Networking** > **Topology**, click **Running** to view all NFV devices (excluding routers and switches), and shut them down.

3. Run the pre-upgrade check, and the system advises to perform an offline upgrade. Click **Next** to proceed.



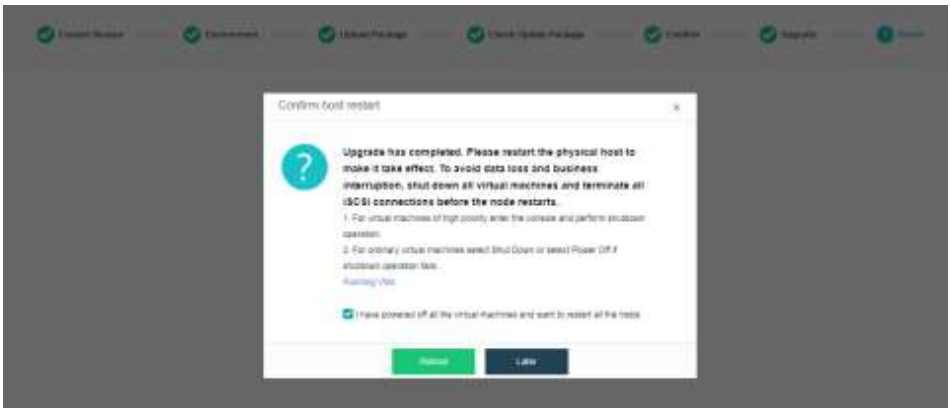
4. You can start the offline upgrade after all NFV devices are shut down and require all nodes to be restarted, which will cause business service interruption.

5. Click **Next** to start the upgrade.

6. The upgrade progress is shown in the figure below.

7. The upgrade is complete.

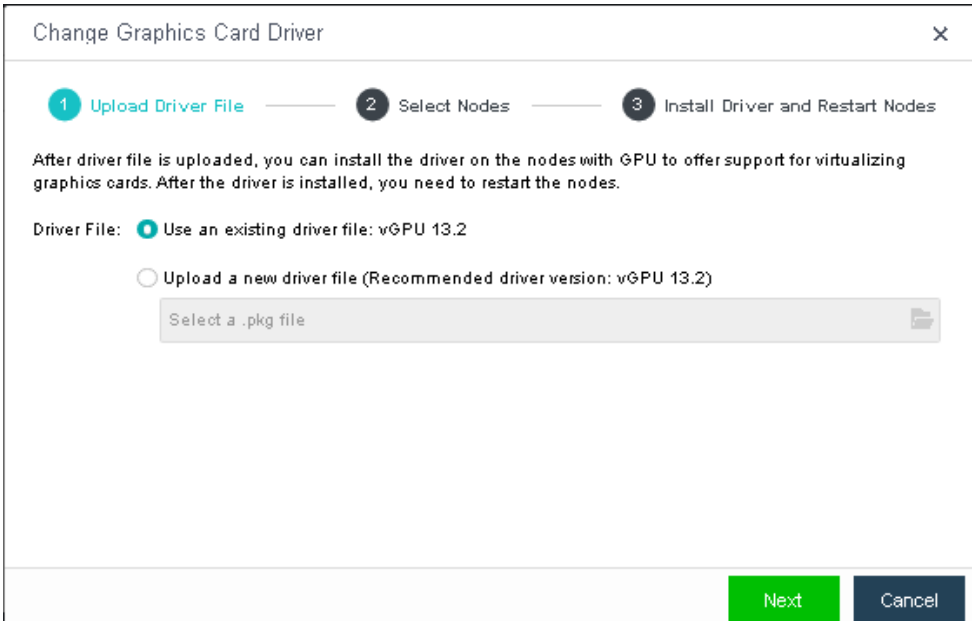
8. Restart the nodes.



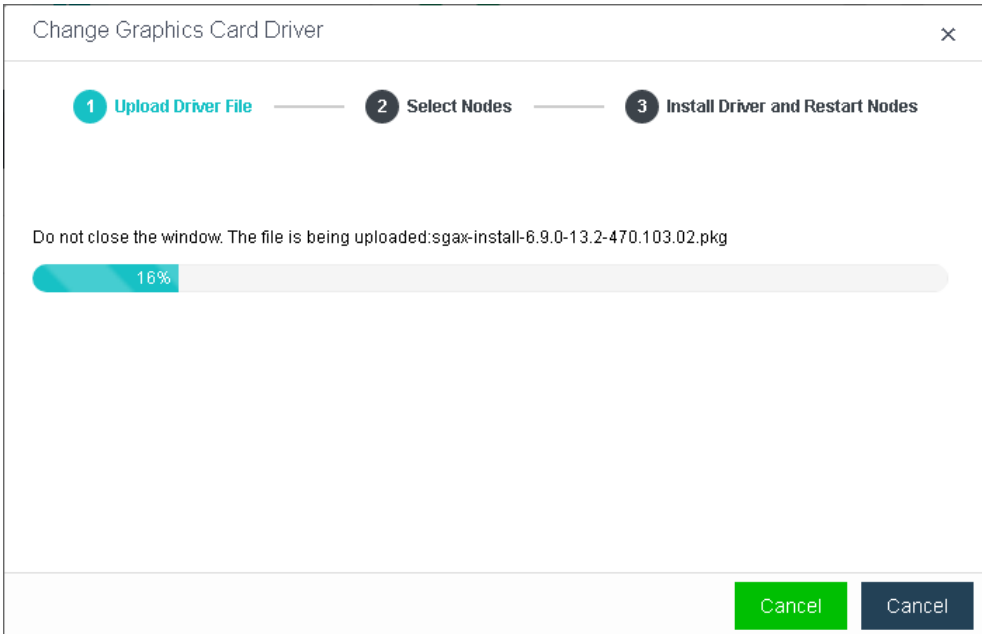
1.2.5.6 Graphics Card Driver Upgrade

The GRID driver update requires restarting nodes. Importing the vGPU driver file after the upgrade and restarting the corresponding nodes is recommended.

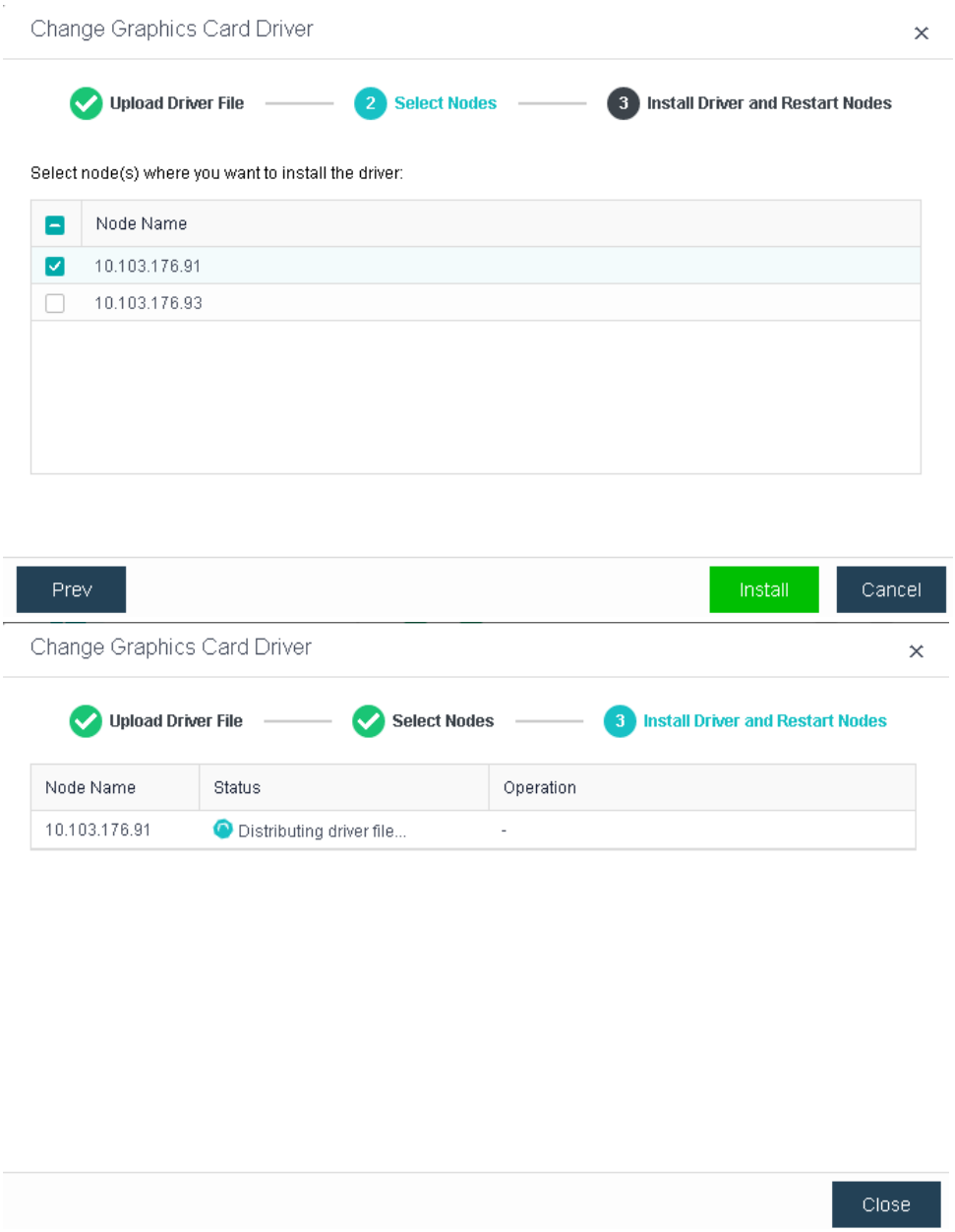
1. Go to **Nodes** > **Graphics Cards** and click **Change Graphics Card Driver** to import the GRID driver.



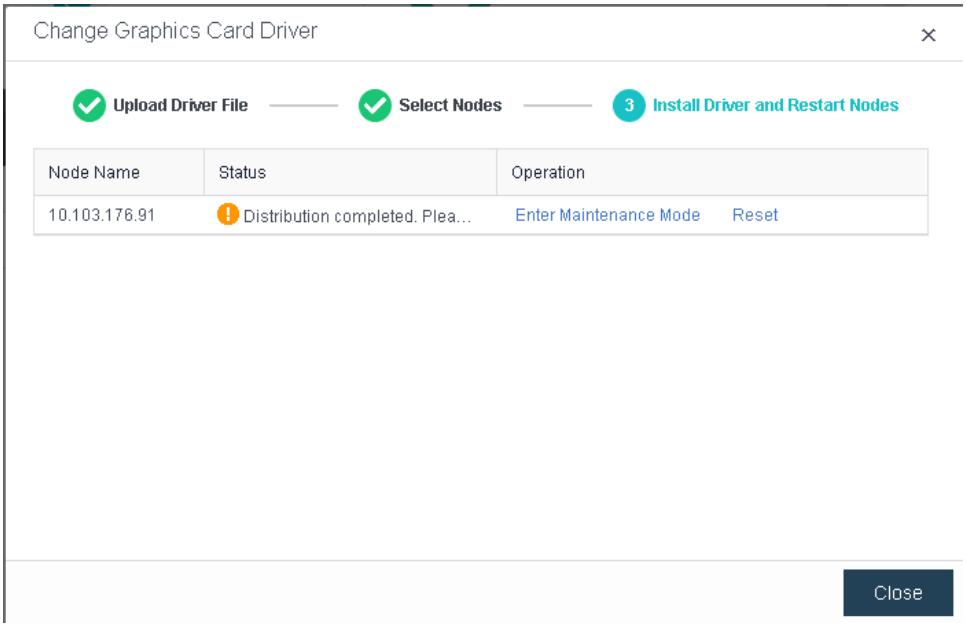
2. Wait until the driver file is uploaded.



3. Select nodes where you want to install the driver and wait for the driver file to be distributed.



4. Click **Enter Maintenance Mode** and then click **Reset** to make the driver take effect.



1.2.6 Abnormalities Troubleshooting

Pre-Upgrade Failures

Scenario	Versions	Solutions	Notes
Timeout while distributing installation package because the management interface of the cluster controller only supports 100 Mbps.	Upgrade from Earlier versions to HCI6.0.1 and above.	Ensure the management interface supports at least 1000 Mbps before the upgrade.	Management interfaces less than 1000Mbps are not supported.
Timeout while checking update.suc.exec.precheck .flag and update.rep.finished.flag during the upgrade.	Upgrade from versions earlier than 5.8.6 to versions earlier than 6.0.1.	Check the configuration of nodes in the cluster. Contact a Sangfor technical support representative to mark nodes with low configuration to skip the check.	This problem has been fixed and will not occur while upgrading versions earlier than HCI5.8.6 to HCI6.0.1 and above.
Failed to verify the pre-upgrade check package because the memory usage occupied by the running services is too high.	Upgrade from HCI5.8.6 to HCI5.9.0 and above.	Restart the vtp-datareport-server reporting service.	This problem has been fixed and will not occur when upgrading HCI5.8.7_R1 to

			later versions.
Pre-upgrade check failed because the memory usage occupied by the running services is too high, exceeding expectations.	Upgrade from HCI5.8.6 and above versions to HCI5.9.0 and HCI6.0.0.	Contact a Sangfor technical support representative to skip this check step.	This problem has been fixed and will not occur while upgrading earlier versions to HCI6.0.1 and above.
The VXLAN interface is configured with an IP address but without an IP address pool.	Active upgrade.	Configure the VXLAN IP pool before the upgrade.	This problem will be detected by the pre-upgrade check. The IP address pool must be configured to start the upgrade.
aCloud cannot be upgraded after powering off the aCMP VM because aCloud is licensed by aCMP.	Offline upgrade from HCI5.8.5.	Power on the aCMP VM to activate the license, and do not power off it before restarting aCloud.	This problem does not exist in other versions.
In the upgrade retry scenario, since other nodes already have the success marks of the pre-upgrade check, the cluster control will be deleted after the pre-upgrade check, thus blocking the upgrade process.	Upgrade from earlier versions to HCI5.8.6 and later.	Contact a Sangfor technical support representative to clean up the success marks of the pre-upgrade check of other nodes.	-
0x0006/0x0005 is reported during the pre-upgrade check of the offline upgrade.	Upgrade from Earlier versions to HCI5.8.6 and later.	Contact a Sangfor technical support representative.	This problem has been fixed and will not occur while upgrading earlier versions to 6.0.1 and later.

The ZK service encountered an error during the active upgrade.	Upgrade from earlier versions to HCI5.8.6 and later.	Upgrade again. If the problem persists, please contact a Sangfor technical support representative.	-
The virtual storage service encountered an error during the pre-upgrade check.	Earlier versions to HCI6.0.1.	Contact a Sangfor technical support representative.	This problem exists only in HCI6.0.1.

Upgrade Failures

Method	Stage	Failure	Solutions	Whether Rollback Is Supported
Offline Upgrade/Active Upgrade	Check Environment for Upgrade	The environment check failed.	Troubleshoot and try again. If the problem persists, please contact a Sangfor technical support representative.	Yes, exit the upgrade to roll back to the original version.
	Upload Update Package	The update package upload failed.		
	Pre-Upgrade Check	Pre-upgrade check failed.		
	Upgrade	Host power encountered an error.	Troubleshoot and try again (upgrades from earlier versions to 5.8.6 and above do not support retry). If the problem persists, please contact a Sangfor technical support representative.	No. To roll back to the original version, please contact a Sangfor technical support representative.
		The host management interface encountered an error.		
		Other errors occurred.		
Offline Upgrade	Restart	Any error occurred.	Contact a Sangfor technical support	Contact a Sangfor technical support

			representative.	representative to confirm whether rollback is supported.

2 SCP

2.1 Overview

2.1.1 SCP New Features

1. **SNMP trap**: Support pushing configuration information, status information, and alerts of clustered nodes through SNMP traps. When an alert is triggered, it will be sent to a third-party monitoring platform through the SNMP trap API.
2. **Encryption security compliance**: After encryption cards and HSMs are configured, support enabling SM encryption mode to protect critical data in information system applications by using compliance encryption algorithms, technologies, and products according to encryption security compliance requirements in China.
3. **Encryption cards**: Support using four domestic encryption cards (SYD1308-G and SJK1727 V2.0-A/B/C) in passthrough mode.
4. **HSMs**: Support using HSMs produced by Sansec and JIT to encrypt data of SCP through the SM4 algorithm. HSMs can also be used to provide business services.
5. **Compatible with China's domestic GPUs**: With the support of X86 architecture, you can use three domestically produced GPUs (Ascend Altas 300V Pro, Cambrian MLU270-S4, and Moore Threads MTT S2000) only in passthrough mode.
6. **Compatible with NVIDIA GPUs**: Support using Tesla P4 and A100-HGX-80G in passthrough or vGPU mode and using Quadro P4000, RTX 4000, RTX 5000, RTX 6000, T1000, T1000-8G only in passthrough mode.
7. **Object storage**: Provide fool-proof design for object storage lifecycle.

Support enabling small object merging and versioning features by integrating with aStor 309R1.

8. **File storage**: Support managing the file storage pool, including managing directories, accounts, and NFS shares.
9. **Global QoS limits**: Support configuring limits on the CPU clock speed, disk IO, and NIC traffic for VMs in the HCI6.9.0 resource pool and above to apply unified QoS settings to all VMs in the resource pool.
10. **SCP resource permission control**: The permission control feature is optimized to support fine-grained control of hundreds of operation permissions related to VMs, resource pools, and NFV devices.

2.1.1.1 Others

1. If HCI has been managed by SCP (earlier than SCP6.7.30) before upgrading to HCI6.9.0, please upgrade SCP to SCP6.7.30 and above (including SCP6.9.0) before upgrading HCI.
2. After upgrading SCP6.7.0 to SCP6.7.30 and above (including SCP6.9.0), please contact Sangfor Support for further inspection.
3. Since SCP6.8.0 has been containerized, to upgrade an earlier version to SCP6.8.0 or SCP6.9.0, please add a disk (400 GB) to the platform for container image storage so that databases will not be affected by disk IO from container images.

1. The offline licensing(virtual key) method is supported only when SCP6.8.0 is deployed on HCI6.8.0 or later.

2. When using a virtual key to upgrade to SCP6.8.0, the original license key file will become invalid, and required to renew the license key with the new device info. This licensing method is supported only when SCP6.8.0 is deployed on HCI6.8.0 or later. Therefore, resource pools of earlier versions may cause SCP licensing to fail.

3. It is required to use the licensing method with a USB key if aSecurity needs to be licensed.

2.1.2 Upgrade Path

2.1.2.1 Sangfor Cloud Platform(SCP)

The Versions Can Be Upgraded to SCP6.9.0:

aCMP 5.8.6 Series	5.8.6_EN	5.8.6R1_EN	-	-	-	**Offline Upgrade**
aCMP 5.8.8 Series	5.8.8_EN	-	-	-	-	
aCMP6.0.10 Series	6.0.10_R1_EN	6.0.10_R2_EN	-	-	-	
SCP6.1.0 Series	6.1.0_EN	-	-	-	-	
SCP6.2.0 Series	6.2.0_EN	SCP6.2.70_EN	-	-	-	
SCP6.3.0 Series	6.3.0_EN	6.3.70_EN	6.3.80_EN	-	-	
SCP6.7.0 Series	6.7.0_EN	6.7.30_EN	-	-	-	
SCP6.8.0 Series	6.8.0_EN		-	-	-	

2.1.2.2 NFV Components Upgrade

Please upgrade the NFV components first if their version is lower than the version listed in the following table before upgrading the HCI.

Device	Version	HCI6.9.0	Classic Network	VPC	Notes
vAD	vAD6.6	√	√	-	
	vAD7.0.9_R1	√	√	√	
vNGAF	vNGAF7.1_R3	√	√	-	
	vNGAF8.0.8	√	√	-	Upgraded from vNGAF7.1_R3 is supported.
	vNGAF8.0.17	√	√	√	Support from vNGAF8.0.8 is supported. To use a customized version of vNGAF8.0.17, please install the upgrade package first and then the custom

					package.
	vNGAF8.0.26 (20200929)	√	√	√	Version patched supports both being installed using SSL service packs and being deployed.
vIAG	vIAG11.9	√	√	-	Must re-deploy.
	vIAG12.0.14	√	√	-	Upgrade from vIAG11.9 is supported.
	vIAG13.0.73	√	√	-	Recommend deploying this version of vIAG. Upgrade from the previous version is not supported due to insufficient partition size.
vSSL	vSSL7.6.0	√	√	-	
	vSSL7.6.8_R2 (20200928)	√	√	√	Support to deploy or upgrade by using the product upgrade package.

2.1.3 Upgrade Impacts

1. All the SCP upgrades are offline upgrades. An offline upgrade requires restarting all SCP VMs, but will not affect the running production system.

2.1.4 Upgrade Instructions for Customers

1. During the upgrade, O&M personnel of customers should not log in to the platform for operation and maintenance.

2.1.5 Implementation Procedure

Refer to **Chapter 2.2.5.3 SCP Upgrade**.

2.1.6 Upgrade Tools

1. When the license key for a version before SCP6.2.0 is free of charge and the feature of managing nodes is in use, an Enterprise Edition or Enterprise Plus Edition license is required to upgrade to a new version. Otherwise, this

feature cannot be used.

2. To upgrade a version before SCP6.2.0 to SCP6.2.0 and above, you must replace the aOC license with the SCP license key. There are three license types: Advanced Edition, Enterprise Edition, and Enterprise Plus Edition.
3. aHCM license for SCP6.3.0 and above will specify the maximum number of nodes. If an aHCM license is activated before the upgrade, a license for a maximum of 500 nodes will be given by default after the upgrade.
4. In versions earlier than SCP6.3.0, Application Center and Hybrid Cloud features are available only when the Enterprise Plus Edition license is activated. For SCP6.3.0 and above, independent licensing through Application Center and aHCM can be done when the Advanced Edition or Enterprise Edition license is activated.
5. Nodes can be managed in versions earlier than SCP6.3.0 when the Enterprise Edition or Enterprise Plus Edition license is activated. In SCP6.3.0, the Advanced Edition license can also be used with the node license in aHCM.
6. In versions earlier than SCP6.3.0, the license for managing Hybrid Cloud VMs has an expiration date. In SCP6.3.0, the license has no expiration date but specifies the maximum number of nodes that can be managed. For Enterprise Plus Edition, the maximum number of Hybrid Cloud VMs that SCP can manage depends on the number of licensed host CPUs.

The number of independently licensed Hybrid Cloud VMs or the VM quantity in a free license, whichever is greater, shall prevail. The specific rules are as follows:

- **Enterprise Plus Edition**: For the SCP license of 20 CPU cores and below, a free license for managing 50 Hybrid Cloud VMs will be granted.
- **Enterprise Plus Edition**: For the SCP license of 20 CPU cores (excluded) to 40 CPU cores (included), a free license for managing 100 Hybrid Cloud VMs will be granted.
- **Enterprise Plus Edition**: For the SCP license of more than 40 CPU cores, a free license for managing 999,999 Hybrid Cloud VMs will be granted.
- For customers who have purchased Enterprise Edition with 10 CPU cores and a license for managing fewer than 50 Hybrid Cloud VMs, a free license for managing 50 Hybrid Cloud VMs will be granted after SCP is upgraded to Enterprise Plus Edition.

- For customers who have purchased Enterprise Edition with 10 CPU cores and a license for managing more than 50 Hybrid Cloud VMs, the number of Hybrid Cloud VMs that can be managed will remain unchanged after SCP is upgraded to Enterprise Plus Edition.

7. Before upgrading versions earlier than SCP6.3.0_EN, please enable the **UUID generator** for SCP VMs on the HCI cluster where SCP resides to ensure that the security optimization feature takes effect.

8. When SCP6.7.0_EN manages an earlier version of HCI, after the HCI platform is upgraded to 6.7.0_EN, data sync may fail for Distributed Firewall while upgrading SCP6.7.0 to SCP6.7.30. Please contact a Sangfor technical support representative.
9. Before upgrading an earlier version of SCP to SCP6.8.0, please ensure there are four SCP VMs disks, and the capacity of disk 4 is 400 GB or more.

2.1.7 Post Upgrade Check

After the upgrade is completed, start and verify the SCP services.

2.1.8 Rollback

SCP supports snapshot-based rollback. Before upgrading SCP, take a snapshot of the platform. Then, if the upgrade fails, rollback can be performed based on the snapshot.

NOTE

Snapshot-based rollback can be performed in the event of an upgrade failure rather than a

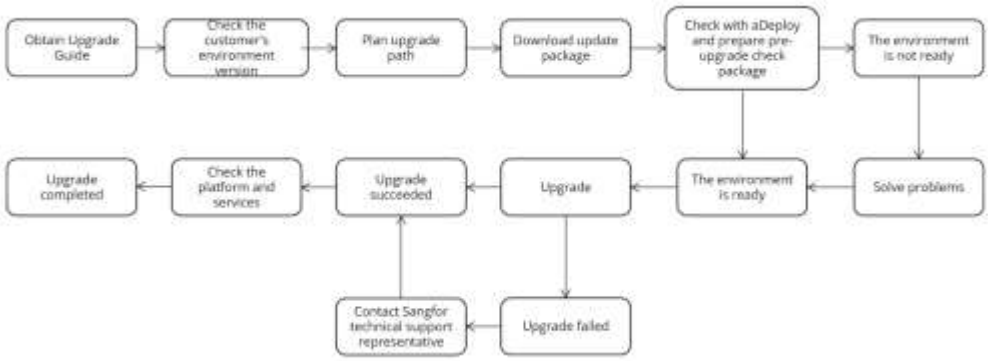
configuration change failure.

2.2 Upgrade Guide

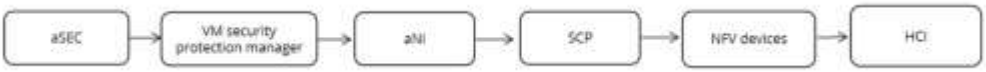
2.2.1 Upgrade Instructions

2.2.1.1 Upgrade Steps

Please follow the following steps to upgrade:



2.2.1.2 Upgrade Sequence



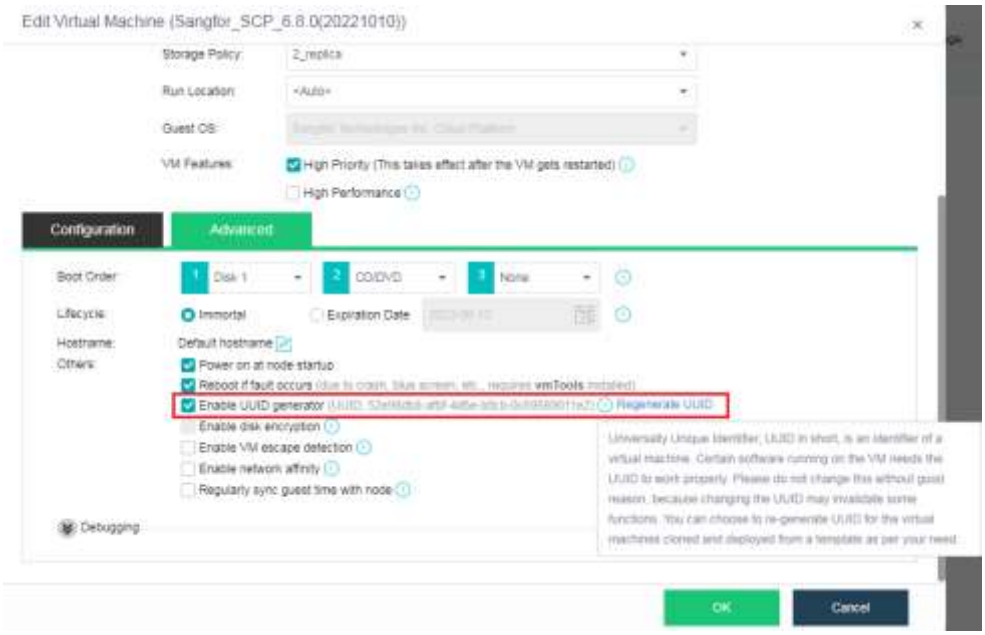
2.2.2 Upgrade Notes

2.2.2.1 SCP Upgrade

1. Upgrade the standby node for a cluster with active and standby nodes before upgrading the active node. You can upgrade the cluster mode directly.
2. In the active-standby disaster recovery scenario, before upgrading the platform, disable disaster recovery policies, and enable them after the upgrade is complete.
3. Before upgrading SCP6.7.0 or an earlier version to SCP6.9.0, please check

and ensure there are four SCP VMs disks and the capacity of disk 4 is at least 400 GB.

4. Before upgrading versions earlier than SCP6.3.0_R1, please enable the **UUID generator** for SCP VMs on the HCI cluster where SCP resides to ensure that the security optimization feature takes effect.



2.2.3 Upgrade Preparations

2.2.3.1 Packages, Documents, and Tools

Packages:

Name	Description	Obtain Through
SCP6.9.0_EN update package	Used for upgrading from an earlier version to SCP6.9.0_EN.	Sangfor Community https://community.sangfor.com/plugin.php?id=service:download&action=view&fid=47#/12/all
Active and standby pre-upgrade package (optional)	After the active and standby pre-upgrade package is upgraded, the active and standby nodes can be upgraded simultaneously.	https://download.sangfor.com/Download/Product/HCI/HCI6.2.0_EN/SCP6.2.0_EN/SP-SCP_IG_PRE_UPGRADE_EN_01.pkg

Documents:

Name	Description	Obtain Through
SCP6.9.0 user manual	Describes basic O&M and configuration in SCP.	Sangfor Knowledge Base https://knowledgebase.sangfor.com/indexPage?module=645
aDeploy User Guide	Provides instructions for using aDeploy.	

Tools:

Name	Description	Obtain Through
Chrome/Edge	The browser to access HCI and SCP web console.	Obtain from the internet.
PuTTY/MobaXterm	An SSH client for troubleshooting if needed.	Obtain from the internet.
MD5	Used for verifying the integrity of the upgrade package.	Check it when downloading the package file.
aDeploy	Used for pre-upgrade checks and other checks with aDeploy.	Sangfor Community https://community.sangfor.com/plugin.php?id=service:download&action=tool
License Key	1. For a version earlier than HCI5.8.2, please apply for a new HCI license key. 2. If the NFV devices need to be upgraded according to **Chapter 1.3.3 NFV Components**. Please apply for a new NFV license key. 3. Before upgrading, please confirm that the customer's license is not expired. Otherwise, the environment needs to be	Contact corresponding personnel to obtain or confirm.

	renewed. 4. Before upgrading, please check that the original NFV license key has not expired. Otherwise, the license needs to be renewed.	

2.2.3.2 Environment Information

Fill in the corresponding IP information in the table below.

Type	Classification	IP Address	Netmask	Remarks
Active SCP	The IP address for the management interface			
Standby SCP	The IP address for the management interface			

2.2.3.3 Customer Resources Coordination

During the upgrade, O&M personnel should not log in to the platform for operation and maintenance.

Please coordinate resources in advance according to the following requirements to ensure a smooth upgrade:

1. Determine when to upgrade and fully prepare for service interruption during the upgrade to reduce impact.
2. Obtain contact information of the responsible persons.
3. Ensure a computer (with Internet access and a stable connection to the device) is ready. Ensure the computer can install and run the upgrade client software.

Type	Name	Contact	Responsible For
Sangfor Technologies			Upgrading HCI and SCP

Inc.			
Customers			Coordinating resources and upgrade time. (Upgrade time:)
			Ensure O&M personnel will not log in to the platform for operation and maintenance.
			Arrange persons responsible for application systems to handle service opening and verification issues.

2.2.4 Pre-upgrade Check

2.2.4.1 Check with aDeploy

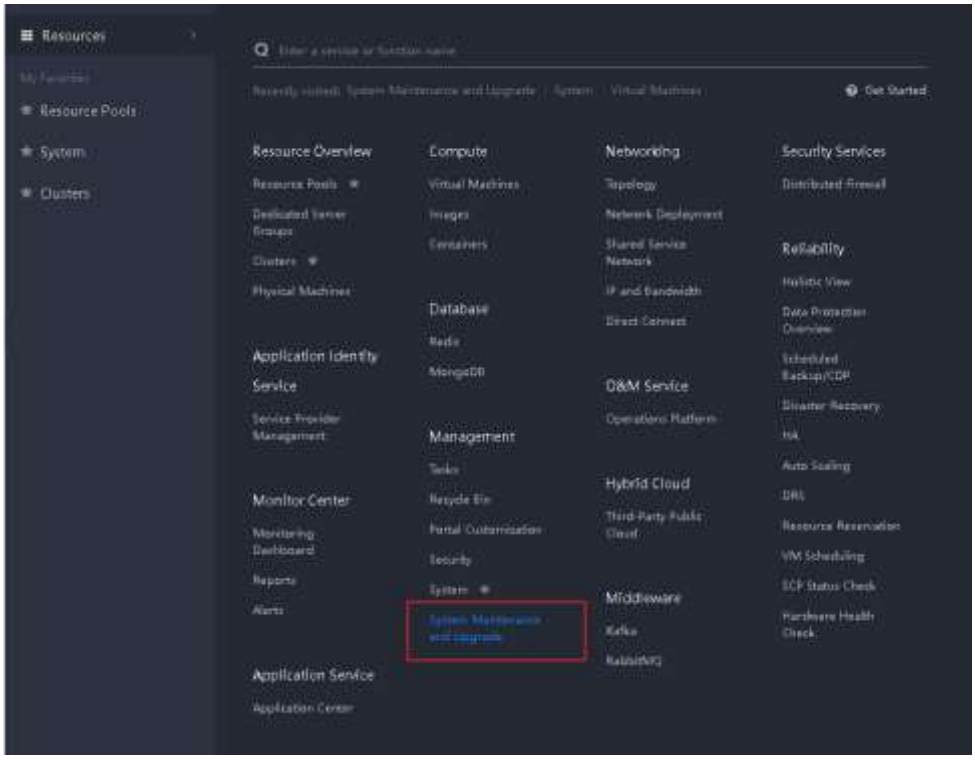
Apart from health check features, aDeploy supports checking common problems of customers. It optimizes the platform-based check mechanism and can check the environment before upgrading. If faults or alerts are reported, please handle the faults and alerts for the cluster before upgrading.

Refer to **Chapter 2.2.3.1 Packages, Documents, and Tools,** for the download link.

2.2.4.2 SCP Pre-Upgrade Check

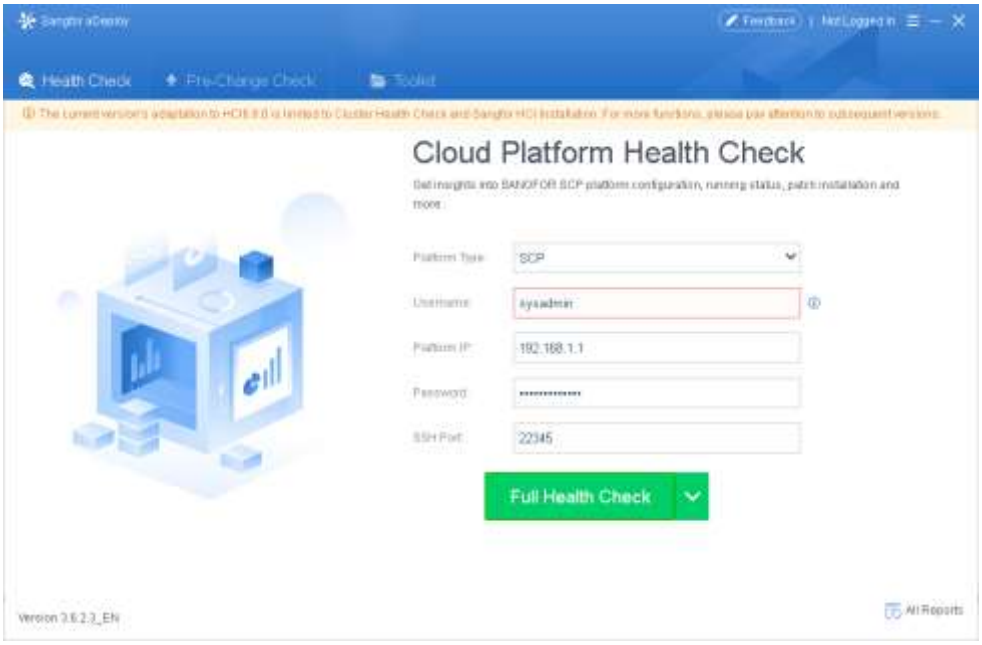
1. **Check the current version.**

   Go to **Resources** > **Management** > **System Maintenance and Upgrade** > **Upgrade** to view the current SCP version.

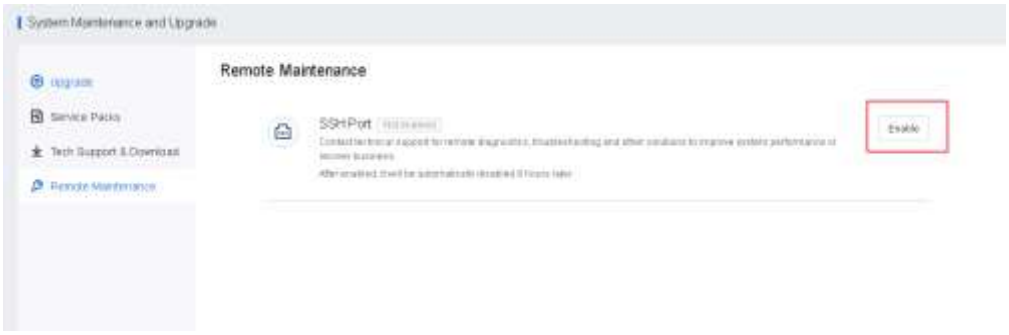


2. **Check with aDeploy.**

- Platform Type: Select **SCP**.
- Username: Enter **sysadm** for SCP6.3.0 and above or **root** for other versions.
- SSH Port: Enter **22345**. For versions earlier than SCP6.1.0, enter **22**.



If an error message indicates that the SSH service port needs to be enabled, go to **Resources** > **Management** > **System Maintenance and Upgrade** > **Remote Maintenance** and click **Enable**.



3. **Check active/standby SCP.**

   Before upgrading, check whether SCP is in active/standby mode. Then, log in to the management portal of SCP, and go to **Reliability > SCP Status Check > SCP Failover** to check whether there is a standby node. If yes, upgrade the active and standby pre-upgrade package first to upgrade the active and standby nodes simultaneously. For details, refer to **Chapter 2.2.3.1 Packages, Documents, and Tools**.

4. **Check before upgrading for disaster recovery scenarios.**

   In disaster recovery scenarios, there is no particular upgrade sequence for primary and secondary sites (they can be upgraded simultaneously). Before upgrading, check the current tasks of primary and secondary sites to ensure that no disaster recovery-related task is in progress. It is recommended to

manually stop ongoing disaster recovery tasks (if any) before upgrading. After the upgrade, ensure the platform runs properly and start disaster recovery tasks.

5. **Check if there is any ongoing task.**

   If there is an ongoing task in **Tasks**, please wait for the task to finish before upgrading, or manually cancel the task and start the task after the upgrade.

6. **Check the SCP VMs disk number and capacity.**

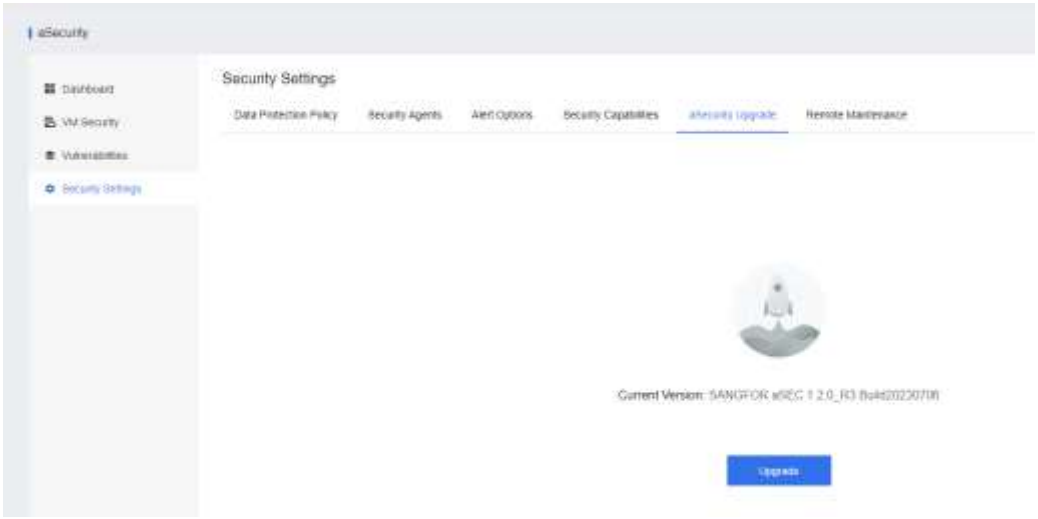
   Check whether SCP has four disks and whether the capacity of disk 4 is 400 GB or more. If disk four does not exist or its capacity is less than 400 GB, add a disk or expand the capacity for an existing disk before upgrading.

2.2.5 Upgrade Procedure

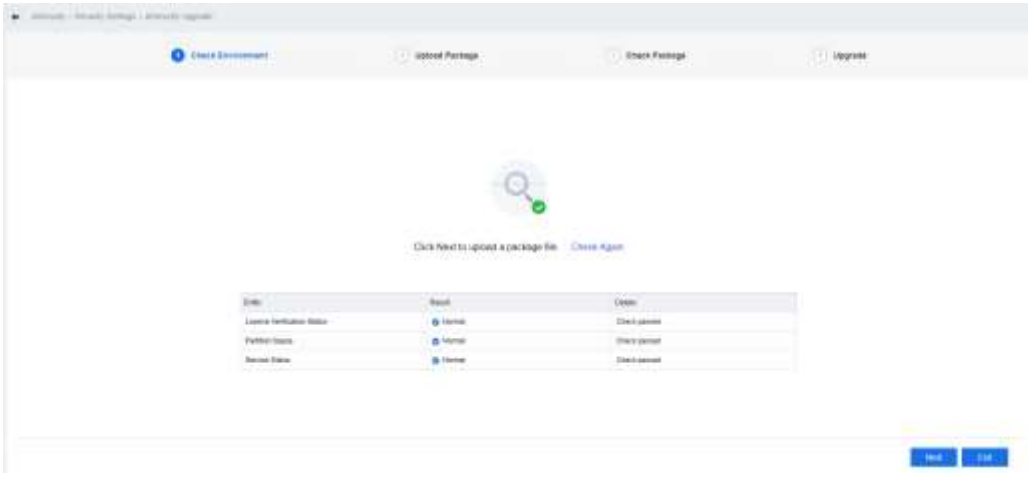
2.2.5.1 aSecurity Upgrade

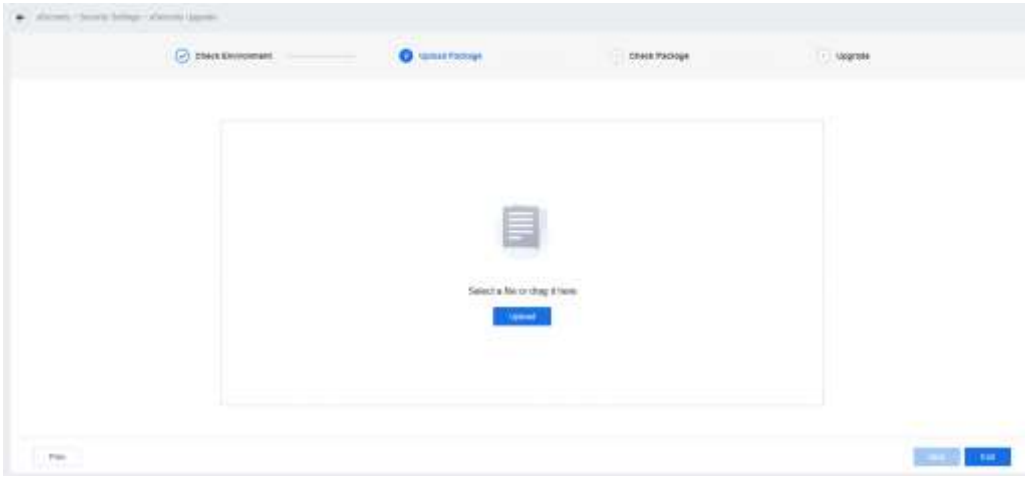
1. Upgrade aSecurity

Step 1. Go to **Security Services > aSecurity > Settings > aSecurity Upgrade** and click **Upgrade**.

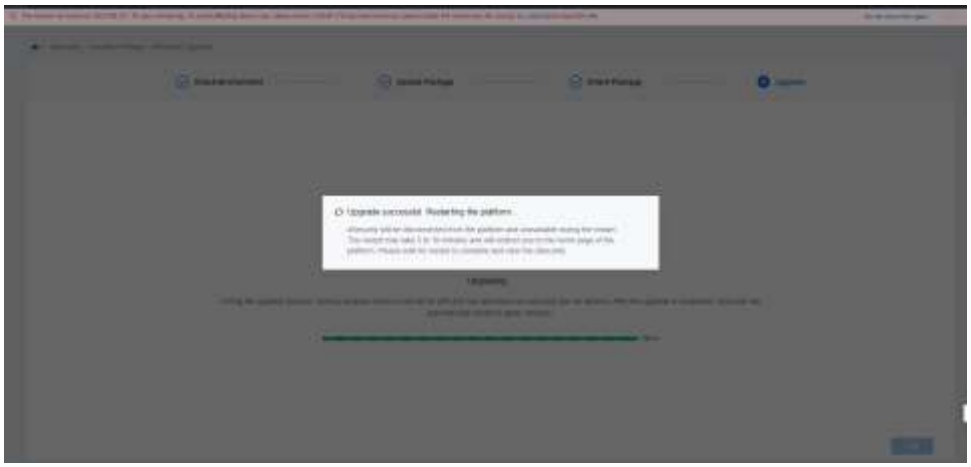


Step 2. Click **Next** to import the update package. Click **Next** after a successful import. If the update package passes the verification, click **Upgrade** and wait for the upgrade to complete. aSecurity will automatically restart after the upgrade is complete. The upgrade process will take about 30 minutes.





Step 3. After the upgrade, platform authentication, and licenses must be obtained again to use aSecurity capabilities.

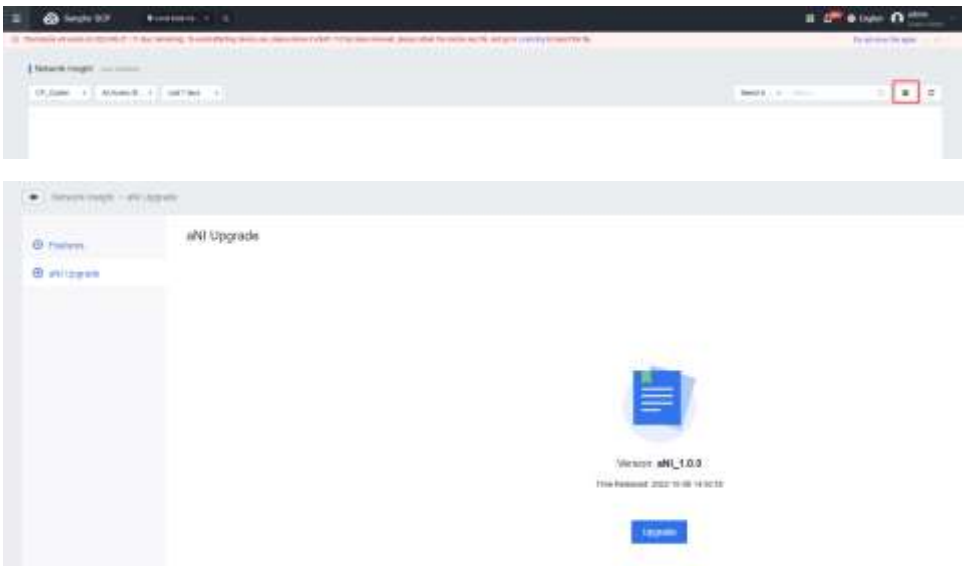


2. Upgrade Security Protection Manager(Endpoint Secure)

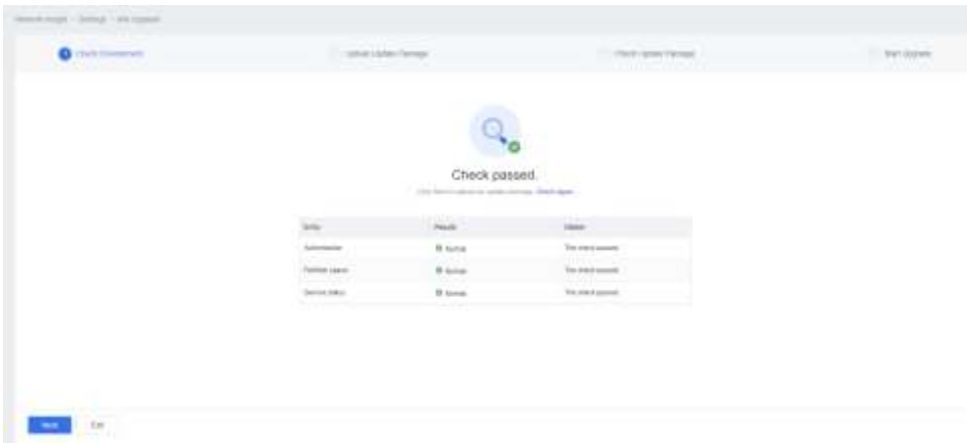
To upgrade **Security Protection Manager(Endpoint Secure)**, kindly contact **Sangfor Technical Engineer** for assistance.

2.2.5.2 aNI Upgrade

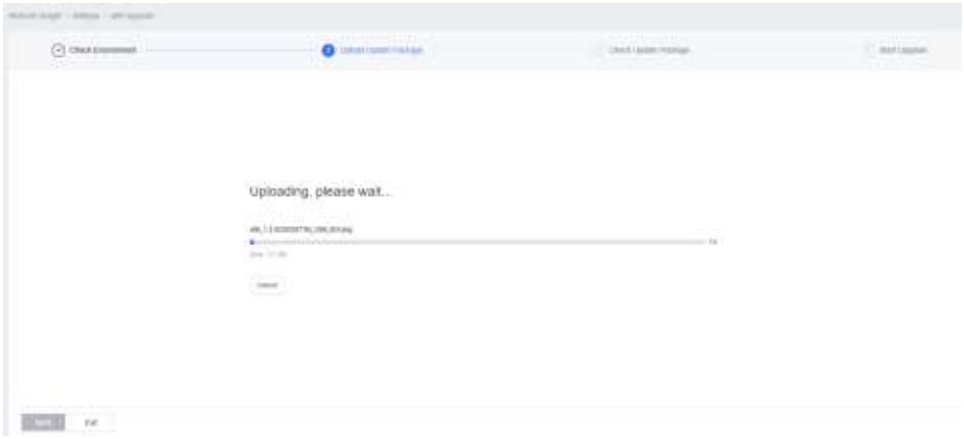
1. Go to **Networking** > **Network Insight**, click  , select **aNI Upgrade** and click **Upgrade**.



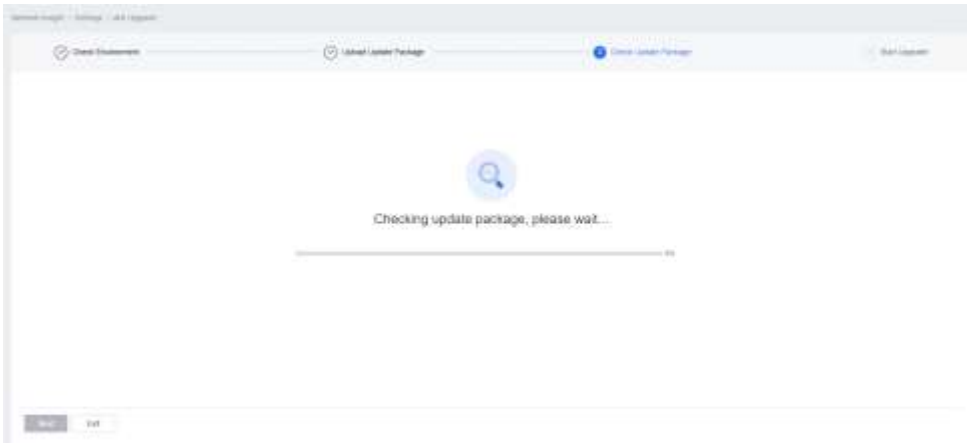
2. Wait for the environment check to complete.



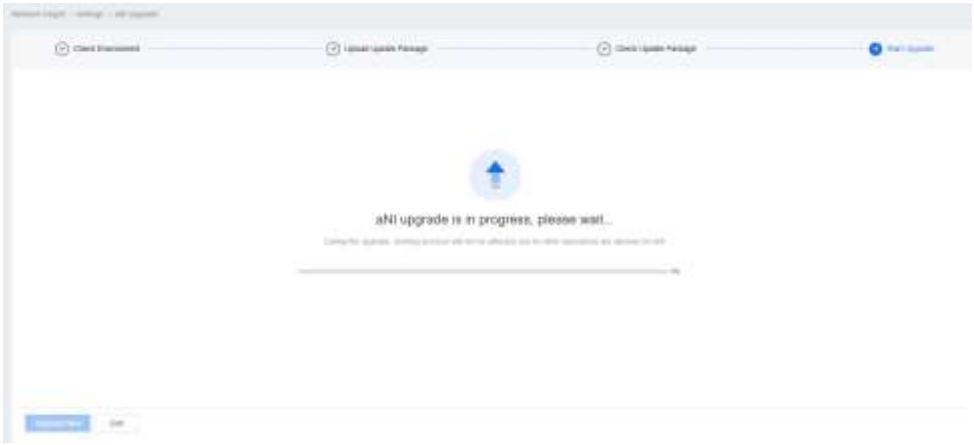
3. Upload the update package.



4. Wait for the update package check to complete.

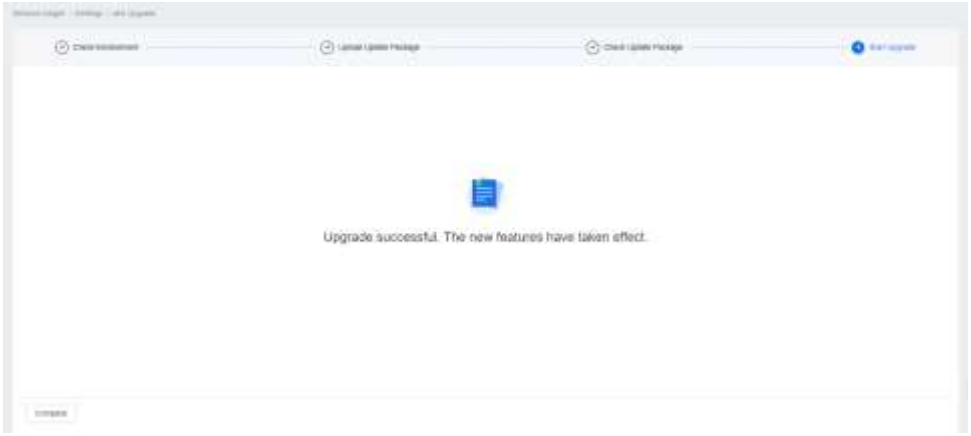


5. Start the upgrade.



6. Restart aNI.

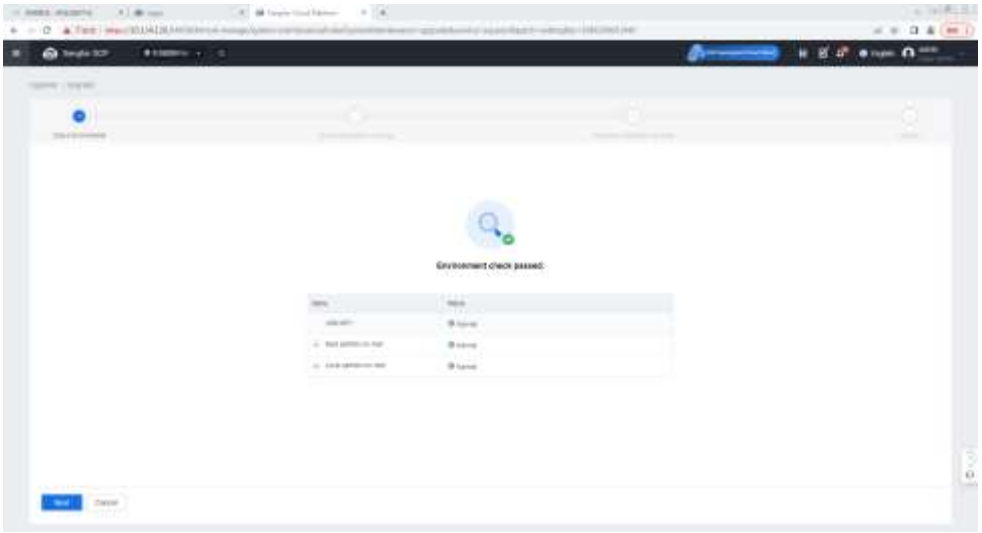
7. The upgrade is complete.

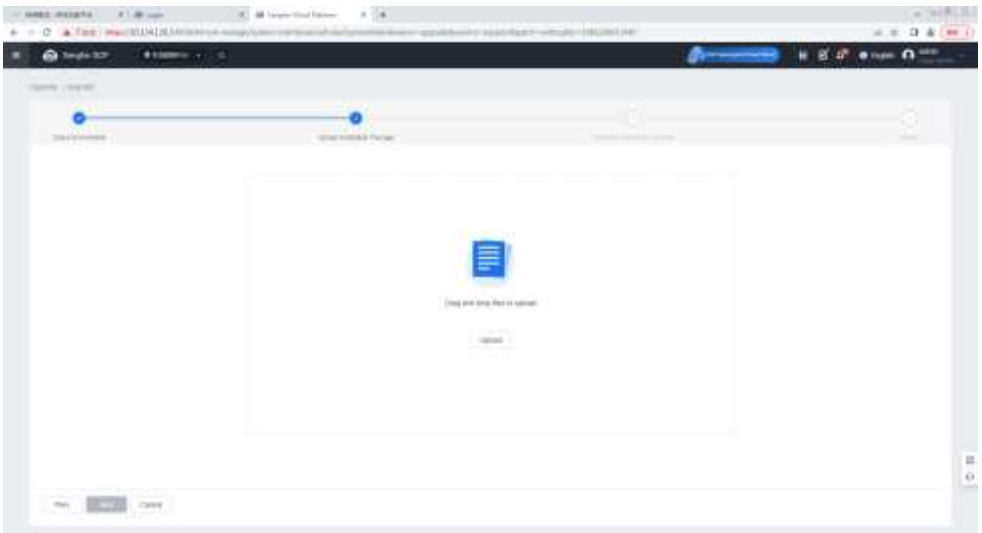


2.2.5.3 SCP Upgrade

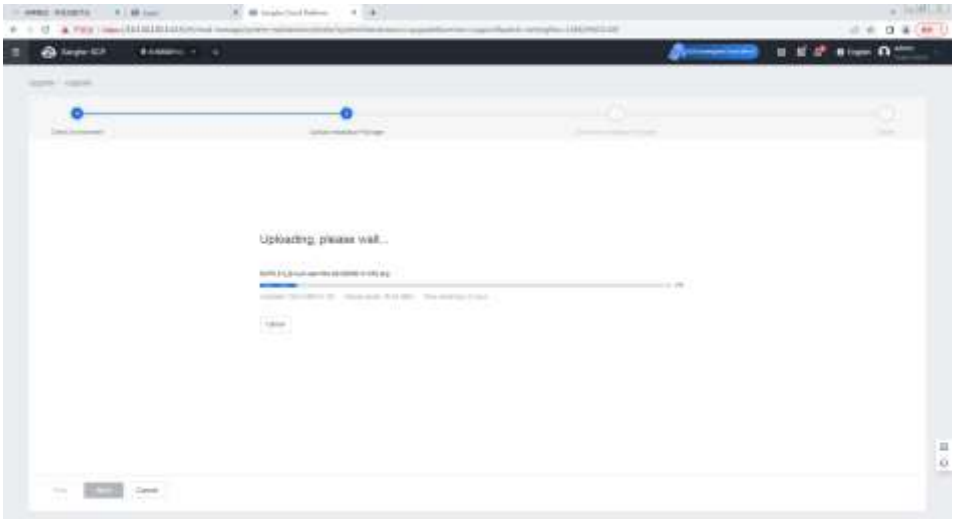
1. Go to **System Maintenance and Upgrade** > **Upgrade** and click **Enable** to enable Maintenance Mode.

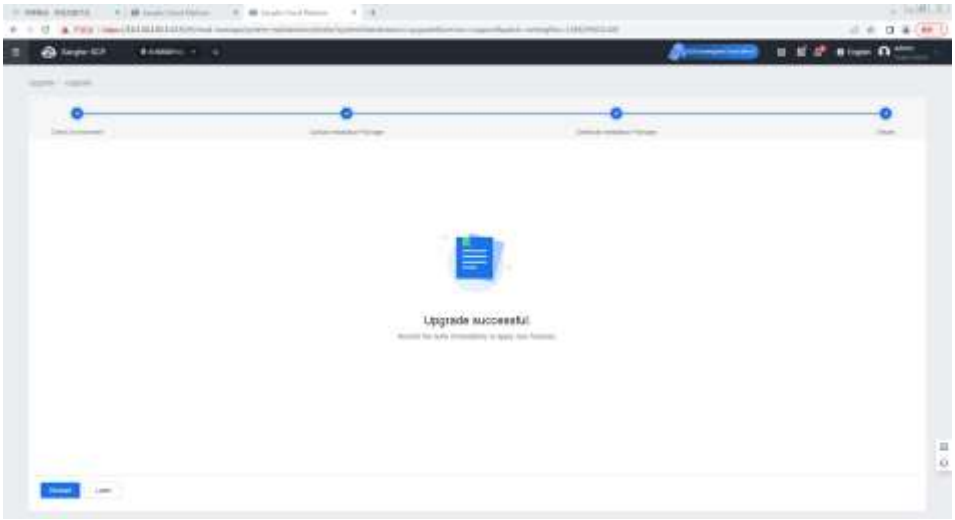
2. Click **Upgrade** and confirm that the new version of SCP is consistent with HCI, then upload the update package and click **Start**.

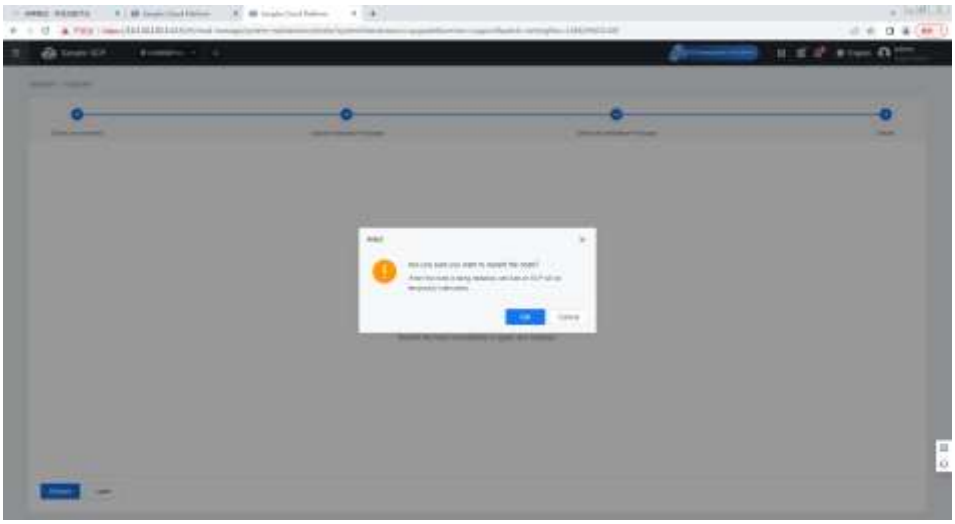




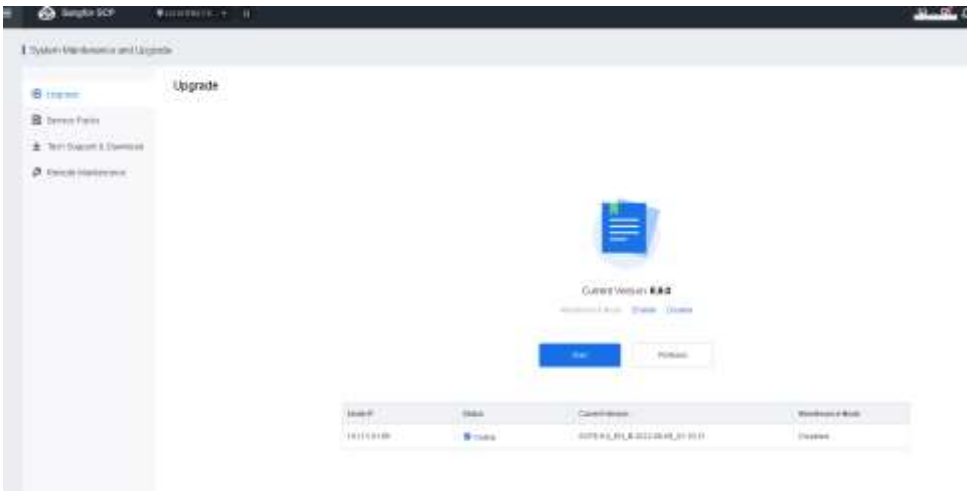
3. Wait for the upgrade to complete, and then restart the platform.







4. After the restart, check whether the current version is SCP6.9.0 in **System Maintenance and Upgrade** > **Upgrade**.



NOTE

For upgrades from SCP6.7.0_EN(managed HCI6.7.0_EN and above) to versions later than SCP6.8.0_EN, you need to contact Sangfor Technical Support for further assistance.

2.2.5.4 NFV Component Upgrade

For the upgrade procedure for NFV components, refer to the upgrade guide for corresponding products.

2.2.6 Abnormalities Troubleshooting

Pre-Upgrade Failures

Scenario	Versions	Solutions	Notes
While upgrading SCP (earlier than 6.8.0) to SCP6.9.0 in case that the disk 4 (/dev/vdd) is in use, the following messages will be displayed: a. The disk (/dev/vdd) has been partitioned, but its datastore does not meet the requirements. Please contact a Sangfor technical support	Upgrade from earlier versions to SCP6.9.0.	1. Contact the customer to confirm whether the added disks can be removed or migrate the disk data. 2. Exit the upgrade process. 3. Delete disks added by the customer on the HCI	

representative. b. The file system of disk 4 (/dev/vdd) does not meet the requirements. Please contact a Sangfor technical support representative.		platform. 4. Add a disk with a capacity of 400 GB to the SCP VM on the HCI platform. 5. Upgrade again.	
While upgrading SCP (earlier than 6.8.0) to SCP6.9.0, the following message will be displayed: a. The disk (/dev/vdd) does not exist. Please add a new disk with a capacity of 400 GB or more.	Upgrade from earlier versions to SCP6.9.0.	1. Exit the upgrade process. 2. Add a disk with a capacity of 400 GB to the SCP VM on the HCI platform. 3. Upgrade again.	
While upgrading SCP (earlier than 6.8.0) to SCP6.9.0, the following message will be displayed: a. Error occurred while partitioning the disk (/dev/vdd). Please delete the disk and add the disk again and upgrade again.	Upgrade from earlier versions to SCP6.9.0.	1. Exit the upgrade process and go to the HCI platform to power off the SCP VM. 2. Delete disks newly added for the SCP VM on the HCI platform. 3. Add a disk with a capacity of 400 GB to the SCP VM on the HCI platform. 4. Power on the SCP VM and upgrade again.	
While upgrading SCP (earlier than 6.8.0) to SCP6.9.0, the following message will be displayed: a. GRUB upgrade failed. Please do not restart the SCP VM. If the problem persists, please contact a Sangfor technical support	Upgrade from earlier versions to SCP6.9.0.	1. Upgrade again. 2. No impact if the upgrade is successful. 3. If the upgrade fails again, do not power off or restart the SCP VM. Contact a Sangfor technical support	

representative.		representative.	

SANGFOR