



Sangfor HCI

Release Notes

Product Version	6.7.0
Document Version	1.0
Released on	March. 30, 2022



Copyright © Sangfor Technologies Inc. 2022. All rights reserved.

Unless otherwise stated or authorized, Sangfor Technologies Inc. (hereinafter referred to as "Sangfor") and its affiliates reserve all intellectual property rights, including but not limited to copyrights, trademarks, patents, and trade secrets, and related rights to text, images, pictures, photographs, audio, videos, charts, colors, and layouts as presented in or concerning this document and content therein. Without prior written consent of Sangfor, this document and content therein must not be reproduced, forwarded, adapted, modified or displayed or distributed by any other means for any purpose.

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 is the release note of Sangfor Hyper-Convergence Infrastructure (HCI) version 6.7.0_EN.

Intended Audience

This document is intended for:

- Network Design Engineer
- Operations Engineer

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
March. 30, 2022	This is the first release of this document.

Contents

Technical Support	1
Change Log	2
Contents	3
1 Overview	4
1.1 Major Features	4
1.1.1 New Features	4
1.1.2 Others	5
1.2 Upgrade Impacts	6
1.2.1 Impacts on Services	6
1.2.2 Impacts on O&M	6
1.2.3 Impacts on Customer Network	6
1.2.4 Other Impacts	6
1.3 Upgrade Instructions for Customers	7
1.3.1 Upgrade Preparations	7
1.3.2 Notes	8
1.4 Implementation Procedures	8
1.5 Check Service Status After Upgrade	10
1.6 Rollback	10
2 Upgrade Guide	11
2.1 Confirmation Before Upgrade	11
2.1.1 Upgrade Tools	11
2.1.2 Environment Information	11
2.1.3 Customer Resources	11
2.2 Check Before Upgrade	11
2.3 Upgrade Procedure	12
2.3.1 Upgrade Path	12
2.3.2 Upgrade Procedure	12
2.4 Check After Upgrade	13
2.4.1 Platform	13
2.4.2 Service Status	13
2.5 Abnormalities Troubleshooting	13
2.6 Rollback	14

1 Overview

1.1 Major Features

1.1.1 New Features

- Communication domain (SCP)
- CPU overcommitment settings
- Support response mechanism for memory leak in-service process
- VM CPU clock speed QoS
- VM disk IO QoS
- VM live migration improvement
- HA and HA trigger optimization
- Linux OS file-level recovery
- Support multi-language keyboard input
- Network topology UI optimization
- Support standard link aggregation for Storage Network Interface
- Support backup copy
- Support scheduled weekly full backup

1.1.1.1 Scenarios and Values

1. Delivery Capability of Large-Scale Data Center:
 - a. It supports communication between multiple clusters. SCP supports a scale of 1024 hosts that are connected to each other.
2. Software-Defined Hardware HA:
 - a. More than 70% of memory hardware issues reported online can be solved by isolating and scanning ECC memory.
3. Platform HA:
 - a. Improve VM live migration for better business continuity.
 - b. Improve the HA success rate by HA and HA trigger optimization.
4. Resource Guarantee for Core Business:

- a. Provide CPU overcommitment ratio to avoid serious overcommitment. It meet the basic requirements of resource guarantee.
 - b. Increase CPU clock speed, network throughput, disk IOPS, and upper throughput limits for VMs, to prevent abnormally large consumption of resources by ordinary VMs.
 - c. Improve CPU scheduling algorithm to ensure the performance and stability of the VMs running the core business
5. Easy to Use:
- a. Optimize network topology.
 - b. Linux file-level restore is supported.
 - c. The multi-language keyboard layout is supported.
 - d. A 3-2-1 backup strategy is supported.

1.1.1.2 Target Customers

- 1. Customers with more than 50 hosts, mainly referring to group enterprises with centrally-built private cloud.
- 2. Managed cloud and second-level managed cloud ISP.

1.1.2 Others

- 1. VM Migration within the cluster
 - a. **Network** option is added. It allows users to choose the network interface used for migration.
 - b. **Migration Speed** option is added. It allows users to specify the migration speed.
- 2. VXLAN
 - a. VXLAN supports Unicast. The new environment with 6.7.0 will be using Unicast, while the cluster upgraded from the old version will still use multicast.
- 3. Virtual Router(VR)
 - a. VR scheduling is added to achieve the HA of the VR within the

cluster.

4. Virtual Topology

- a. Enhancement of virtual topology UI.
- b. Few types of layouts add, including Tree, Ring, Rectangular, Horizontal, and Vertical.

5. Distributed Firewall

- a. The firewall policy is added, which can contain multiple firewall rules.
- b. Support to copy firewall rules which easier the configuration for a large number of firewall rules.

1.2 Upgrade Impacts

1. The offline upgrade will interrupt the business. All VMs and virtual network devices need to be shut down before the upgrade. Hosts need to be restarted after the upgrade.
2. During the active upgrade, VMs and virtual network devices do not need to be shut down or restarted, but the virtual network will be interrupted for about 3 seconds; After the upgrade, hosts do not need to be restarted.

1.2.1 Impacts on Services

Upgrading to 6.7.0 from lower versions requires shutting down all the VMs and virtual network devices.

1.2.2 Impacts on O&M

None.

1.2.3 Impacts on Customer Network

None.

1.2.4 Other Impacts

None.

1.3 Upgrade Instructions for Customers

1.3.1 Upgrade Preparations

You can upgrade to version 6.7.0_EN from the following versions:

- 6.0.0_R5_EN
- 6.0.1_EN_B
- 6.0.1_EN
- 6.0.1_R1_EN
- 6.1.0_EN
- 6.1.0_R1_EN
- 6.2.0_EN_B
- 6.2.0_EN
- 6.3.0_EN_B
- 6.3.0_EN
- 6.3.0_R1_EN_B
- 6.3.0_R1_EN
- 6.3.0_R2_EN_B
- 6.3.0_R2_EN
- 6.7.0_EN_B
- 6.7.0_EN



1. Support upgrade from versions with any service pack installed but not support upgrade from custom versions.
2. Before upgrading the old version earlier than 6.7.0_EN, you need to use aDeploy(version 3.5.1 and above) for pre-upgrade inspection and install the pre-upgrade package in aDeploy.
3. Versions earlier than 5.8.3_EN (excluding 5.8.3_EN) need to be upgraded to 5.8.3_EN before upgrading to subsequent versions.

4. 5.8.3_EN and 5.8.5_EN can be upgraded to 6.7.0_EN only after being upgraded to 6.0.0_R5_EN, 6.2.0_EN, 6.3.0_R1_EN or 6.3.0_R2_EN.
5. Versions later than 6.0.0_R_EN can be immediately upgraded to 6.7.0_EN.
6. 6.7.0_EN can only be immediately upgraded from versions later than 6.0.0R5_EN and by offline upgrade.

1.3.2 Notes

1. As a cluster scales out, converting configuration files takes longer, and so does the upgrade process. For reference: upgrading an 11-node cluster running 1,000 virtual machines may take 30 minutes, while upgrading a 2-node cluster running 1,000+ virtual machines (virtual storage: 6.4 TB) may take 14 minutes.
2. After the upgrade, for the device with a graphics card inserted but has not enabled IOMMU, it is required to enable IOMMU and restart again.
3. During the upgrade process, the creation of storage-based snapshots and linked clones and change of storage policies cannot be performed on the VM before new upgrades take effect.
4. Names of the VMs on HCI can only contain letters, digits, Chinese characters, and the following special characters: () 【 】 _ . + () @ . Otherwise, the invalid name will cause pre-upgrade check failure before upgrading HCI to 6.7.0_EN.
5. You can only perform an offline upgrade to upgrade to 6.7.0_EN from lower versions.

1.4 Implementation Procedures

Active Upgrade Process			
Type	Item	Estimated Time	Check the box(√) when complete
Preparing for Upgrade	Check upgrade path		
	Prepare update package for pre-upgrade check		

	Prepare the HCI update package		
	Check version information		
	Prepare license key		
	Read upgrade notes		
Upgrade Process	Make sure there are no ongoing tasks	2 mins	
	General page check	10 mins	
	Health check	5 mins	
	Enable maintenance mode	1 min	
	Test before upgrading HCI	5 mins	
	Upload HCI upgrade package/verify authentication	1 min	
	Distribute update package	Package size*number of nodes/Transfer rate	
	Pre-upgrade check	15 mins	
	Control plane active upgrade	11 mins	
	VM active upgrade	XX second(s) for every 5 VMs with vmTools installed. XXX minute(s) for every VM without vmTools installed.	
	Virtual storage active upgrade	Number of clustered nodes*5 mins (related to the scale and load of VMs)	
	Apply new virtual storage version	Number of clustered nodes*5 mins (related to the scale and load of VMs)	
	Check business	5 mins	
	License after upgrade	5 mins	

1. Use aDeploy(version 3.5.1 and above) for inspection.
2. Fix the detected issues. Use aDeploy to install the package for a pre-upgrade check.

3. Shut down all the virtual machines and virtual network devices for an offline upgrade.
4. Check whether the upgrade package to be installed is the official upgrade package of 6.7.0_EN.
5. Check the upgrade environment.
6. Load the official upgrade package of 6.7.0_EN.
7. After the active upgrade is completed, exit the upgrade. The offline upgrade requires restarting the host to complete the upgrade.

1.5 Check Service Status After Upgrade

Check whether the VMs are running and whether the backup policies and snapshot policies are executed normally.

1.6 Rollback

Rollback: No

Rollback is not supported. You can contact Sangfor technical support representative if the upgrade fails to recover from backups.

2 Upgrade Guide

2.1 Confirmation Before Upgrade

2.1.1 Upgrade Tools

1. Suppose the aServer for testing or cluster is plugged with the USB Key with the **For Sangfor Testing** mark. You can get the license key file of all modules by scanning the code and getting the license for the corresponding module by importing the license file in **System > Licensing**.
2. Get aDeploy tools from <https://community.sangfor.com/plugin.php?id=service:download&action=tool>.
3. Get the upgrade package from <https://community.sangfor.com/plugin.php?id=service:download&action=view&fid=47#/12/all>.

2.1.2 Environment Information

None.

2.1.3 Customer Resources

None.

2.2 Check Before Upgrade

Before the upgrade, use aDeploy(version 3.5.1 and above) for inspection to check that there is no hardware or other problem.

2.3 Upgrade Procedure

2.3.1 Upgrade Path

Target Version	HCI5.0_EN	HCI5.2_EN	HCI5.3_EN	HCI5.3_R1_EN	5.5.3_EN	5.5.5_EN	5.5.6_EN	5.5.7_R1_EN	5.5.8_EN	5.5.8_R1_EN	6.0.0_EN	6.0.0_R3_EN	6.0.0_R4_EN	6.0.0_R5_EN	6.0.1_EN	6.0.1_R1_EN	6.0.1_R2_EN	6.0.1_R3_EN	6.2.0_EN	6.3.0_EN	6.3.0_R1_EN	6.3.0_R2_EN	6.7.0_EN
Source Version (S)																							
aDeploy 2.0_EN	S→T				S→5.2EN→T									S→5.2EN→5.5.3EN→T					S→5.2EN→5.5.3EN→T	S→5.2EN→5.5.3EN	S→5.2EN→5.5.3EN	S→5.2EN→5.5.3EN→6.0.0_R5_EN	
HCI5.0_EN					S→T									S→5.5.3EN→T					S→5.5.3EN→T	S→5.5.3EN→T	S→5.5.3EN→T	S→5.5.3EN→6.0.0_R5_EN→T	
HCI5.2_EN					S→T									S→5.5.3EN→T					S→5.5.3EN→T	S→5.5.3EN→T	S→5.5.3EN→T	S→5.5.3EN→6.0.0_R5_EN→T	
HCI5.3_EN					S→T									S→5.5.3EN→T					S→5.5.3EN→T	S→5.5.3EN→T	S→5.5.3EN→T	S→5.5.3EN→6.0.0_R5_EN→T	
HCI5.3_R1EN					S→T									S→5.5.3EN→T					S→5.5.3EN→T	S→5.5.3EN→T	S→5.5.3EN→T	S→5.5.3EN→6.0.0_R5_EN→T	
5.5.3_EN														S→T					S→T	S→T	S→T	S→6.0.0_R5_EN→T	
5.5.5_EN														S→T					S→T	S→T	S→T	S→6.0.0_R5_EN→T	
5.5.6_EN														S→T					S→T	S→T	S→T	S→6.0.0_R5_EN→T	
5.5.7_R1_EN														S→T					S→T	S→T	S→T	S→6.0.0_R5_EN→T	
5.5.8_EN														S→T					S→T	S→T	S→T	S→6.0.0_R5_EN→T	
5.5.8_R1_EN														S→T					S→T	S→T	S→T	S→6.0.0_R5_EN→T	
6.0.0_EN														S→T					S→T	S→T	S→T	S→T	
6.0.0_R3_EN														S→T					S→T	S→T	S→T	S→T	
6.0.0_R4_EN														S→T					S→T	S→T	S→T	S→T	
6.0.0_R5_EN														S→T					S→T	S→T	S→T	S→T	
6.0.1_EN														S→T					S→T	S→T	S→T	S→T	
6.0.1_R1_EN														S→T					S→T	S→T	S→T	S→T	
6.1.0_EN														S→T					S→T	S→T	S→T	S→T	
6.1.0_R1_EN														S→T					S→T	S→T	S→T	S→T	
6.2.0_EN														S→T					S→T	S→T	S→T	S→T	
6.3.0_EN														S→T					S→T	S→T	S→T	S→T	
6.3.0_R1_EN														S→T					S→T	S→T	S→T	S→T	
6.3.0_R2_EN														S→T					S→T	S→T	S→T	S→T	
6.7.0_EN														S→T					S→T	S→T	S→T	S→T	
Note	S→T	Immediate upgrade																					
	S→Version→T	Upgrades the intermediate version and then upgrade to the target version																					
		Active upgrade supported																					
		Offline upgrade only																					
		Scenarios that do not exist																					

2.3.2 Upgrade Procedure

1. Use aDeploy(version 3.5.1 and above) for pre-upgrade inspection.
2. Fix the detected issues. Use aDeploy to install the pre-upgrade package.
3. The offline upgrade is only supported for upgrading to 6.7.0_EN from lower versions, which requires shutting down all the VMs and virtual network devices, and 6.7.0_EN will be able to active upgrade to later versions.
4. Ensure that the HCI version to be upgraded is the official upgrade package of 6.7.0_EN.
5. Check the upgrade environment.
6. Load the official upgrade package of HCI6.7.0_EN.
7. After the active upgrade is completed, exit the upgrade. The offline upgrade requires restarting the host to complete the upgrade. (The current 6.7.0_EN only supports an offline upgrade from lower versions.)

2.4 Check After Upgrade

2.4.1 Platform

Check whether the upgrade task is completed and whether the current version is HCI6.7.0_EN in **System > System Maintenance > Upgrade**.

2.4.2 Service Status

Check whether VMs in HCI are running properly and whether backup policies and snapshot policies work normally.

2.5 Abnormalities Troubleshooting

Scenario 1: There are VMs or virtual network devices which have not been shut down.

Solution: Shut down VMs and virtual network devices.

Scenario 2: Network is unstable due to reboot or unstable cluster.

Solution: Wait for the cluster or network to become stable and then perform the upgrade again.

Scenario 3: The pre-upgrade check detected invalid VM names.

Solution: Exit maintenance mode and change invalid VM names. Names of the VMs on HCI can only contain letters, digits, Chinese characters, and the following special characters: () 【 】 _ . + () @ .

Scenario 4: Configuration conversion failed during the upgrade.

Solution: Contact a Sangfor technical support representative.

Scenario 5: The pre-upgrade check detected that VM's NIC connection dropped.

Solution: Contact a Sangfor technical support representative.

2.6 Rollback

Rollback: No

Rollback is not supported. You can contact Sangfor technical support representative if the upgrade fails to recover from backups.



SANGFOR

