Dell XC Core

Hyperconverged Appliances Release Notes

December 2024

DELL Technologies

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

Revision history

Date	Document revision	Description of changes
December 2024	1.3	Added information about XC Core XC4000r, 4510c, 4520c, 4000c, and 4000w models
July 2022	1.2	Added information about XC750-24 SSD and HDD combination.
December 2021	1.1	Added the following platforms: • XC6520 • XC7525
September 2021	1.0	Initial release for 15th generation platforms. The following platforms are included: • XC450 • XC650 • XC750 • XC750xa

1

Executive summary

This document contains release notes for the 15th generation XC Core appliances.

2

New platforms

This section specifies the new platform and the minimum versions required.

Platform	Minimum AOS LTS version	ESXi 6.7	ESXi 7.0
XC450	5.20.1.1	6.7 U3 A10	7.0 U2 A03
XC650	5.20.1.1	6.7 U3 A10	7.0 U2 A03
XC750	5.20.1.1	6.7 U3 A10	7.0 U2 A03
XC750XA	5.20.1.1	6.7 U3 A10	7.0 U2 A03
XC6520			
XC7525			
XC40000r			
XC4510c			
XC4000z			
XC4000w			
XC4520c			

UEFI is a requirement for 15th generation. 14th generation platforms only support legacy BIOS boot.

3

Important SED information

Topics:

Removing the SED

If you incorrectly remove a Self-Encrypting Drive (SED), it puts that drive into an unusable state. To avoid this situation, follow these instructions.

To remove a Self-Encrypting Drive (SED) from a Nutanix cluster:

WARNING: Do not remove any SEDs from your key management server before properly removing them from the Nutanix Cluster.

1. Use the Prism Web Console to prepare to remove the drive for replacement.
2. As part of the disk removal process, the data encryption key (DEK) for that SED automatically cycles on the drive controller. The previous DEK is lost and all new disk reads are indecipherable.
3. After this process is completed, a yellow LED indicator blinks on the drive to be removed.

Reverting the drive to a usable state

You can securely revert the drive to a usable state using the SED's PSID serial number. You do this using the self_encrypting_drive secure_revert command from the Nutanix CVM.

Data previously written to the drive will be inaccessible after securely reverting an SED.

For more information, about this issue, see Nutanix Knowledge Base (KB) Article Number 1940, Resetting Self-Encrypted Drives, and Nutanix KB Article Number 2554, About Self-Encrypting Drives (SEDs) in a Nutanix Cluster. You must log in using the Nutanix Portal to access KB articles, go to https://my.nutanix.com.

4

XC750-24 Drive Capacity

This section describes important information about the XC750 SSD and HDD combination.

Prior to the first time power on, ensure that the SSD drives are populated in the first slot from left to right; for example, a 4-SSD configuration can populate slots 0,1,2, and 3. HDD can populate slots 4,5, and 6, until all HDDs are populated.

If HDDs are populated first, and the system has been powered on, see the Rapid Appliance Self Recovery (RASR) section or contact Dell Support for RASR recovery instructions.

A

Rapid Appliance Self Recovery

Use the Rapid Appliance Self Recovery tool (RASR) to restore the factory settings on the Dell XC Node system.

CAUTION: The restoration process erases all drives on the system. Ensure that the customer contacts Dell Support before using the RASR tool.

Prerequisites

- The Dell XC Node system must have power connected to the power supplies, a valid network connection, and an iDRAC connection.
- Some Keyboard, Video, Mouse (KVM) devices, especially those which use USB passthrough, may interfere with the RASR process, resulting in RASR being detected as a mount point. Remove the KVM during the RASR process and run the RASR recovery from the iDrac console using the Virtual Console instead of a KVM The RASR ISO is new for 15G servers and works with 14th generation XC Node systems. 13G servers are not supported by the RASR ISO, so you must rely on the onboard SD card method.

Supported devices

- XC640
- XC6420
- XC740xd
- XC940
- Core XC6420
- Core XC450
- Core XC640
- Core XC650
- Core XC740xd
- Core XC740xd2
- Core XC750
- Core XCXC750xa
- Core XC940
- Core XCXR2
- Core XC6520
- Core XC7525
- XC4000r
- XC4510c
- XC4520c
- XC4000w (has a separate ISO)

Hypervisor options and AOS support

- VMware ESXi 6.5 U3 Build 15256549 (14 Generation XC support only)
- VMware ESXi 6.7U3 Build 15160138 (14 & 15 Generation XC support)
- VMware ESXi 7.0U2 Build 17867351 (14 & 15 Generation XC support)
- VMware ESxi8.0 U1c build 22088125
- AOS Version 5.20.1.1 (14 & 15 Generation XC support)
- AHV version AHV-20201105-2096 (14 & 15 Generation XC support)

Features and use

- Factory reset of the entire node to factory defaults. All data on all disks are erased.
- Recovery of a node if there are four or more nodes in the cluster. Guidance required by Dell support.

Non-use statement:

- Recovery of a node if there are three nodes or fewer in the cluster. Consult Dell EMC support for recovery options.
- Upgrade of the Hypervisor or Acropolis operating system (AOS) for cluster nodes.
- Backup or restore operation of a Dell XC Nutanix node.

Downloading instructions

1. Go to www.dell.com/support.
2. In the **Enter a Service Tag** > **Serial Number** box, enter the product name. For example, **XC640**.
3. Select your product from the list that is displayed.
4. Click **Drivers & downloads**.
5. From the **Category** menu, select **Miscellaneous Utilities**.
6. In the **Name** column, expand the hyperlinked RASR title.
7. To view information about earlier versions, click **Older versions**.
8. Click **Download Now** to download the file.
9. When the **File download** window opens, click **Save** to save the file to your hard drive.

Installation instructions (except witness)

Installation requires access to the iDrac and Virtual Console.

1. To connect to virtual media map the CD or DVD.
2. Browse to the RASR ISO file that was saved previously and click **Map Device**.
3. Set **Next boot option** to the virtual CD, DVD, or ISO.
4. Boot the system and allow it to Boot into the RASR ISO.
5. Choose **[F]** for Factory reset. **[Q]** quits the operation and reboots the node.
6. You are prompted to ask if you are sure.
   a. Enter **Y** to move to the next step, the Hypervisor selection menu.
   b. Enter **N** to stop the process.
7. Choosin **Hypervisor Example [70]** selects VMware ESXi 7.0U3.
8. At the next assurance prompt, enter **Y** to proceed with the imaging process.

   The imaging process is data destructive.
9. After the imaging process finishes, you see a message that the Factory Install has completed. Press **Enter** and reboot the server.
10. The node begins a Hypervisor installation during which several reboots occur. Allow this process to complete.

XC4000w recovery instructions

This process only applies to XC4000w because it has no iDRAC so recovery can only be done by creating a bootable USB drive from the install iso.

1. Create a bootable USB media from the provided XC witness installer iso. Place the usb onto the usb port of the XC4000w.
2. Reboot the witness node (from iDRAC or physically) to boot into the USB.
3. Wait some time and retrieve the IP address of the witness installer from iDRAC of one of the included 4510c or 4520c nodes. Or login with serial console (automatically logs in) Default ssh credentials are xcrecover / westOrange3!
4. From the installation menu follow prompts to confirm recovery and **ENTER** to image the host disk. This could take ~15 minutes. When it is complete you will be prompted to type **ENTER** to reboot to the host.

5. Remove the USB drive after installation has completed you can wipe/reformat the USB drive, it is no longer needed.