# Release Notes for Dell EMC XC Series Appliances and XC Core Systems

Read this information prior to deploying your appliances or systems.

Abstract

This document includes release notes and other important information about the XC Series Appliances and XC Core Systems.

August 2018

# Revisions

| Date | Description |
|---|---|
| March 2018 | Added information on Kerberos. |
| November 2017 | Initial release |
| August 2018 | Updated content to include XC Core. |

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

© 2017 – 2018 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Dell believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

# Table of contents

# Executive summary

**NOTE**: The information in this document applies to both, Dell EMC XC Series Appliances as well as the Dell EMC XC Core System offering. Sections or information that apply to only one of the offerings (XC Series or XC Core) will be called out explicitly.

This document contains release notes and other valuable information for the Dell EMC XC Series Appliances and XC Core Systems.

**NOTE**: You can identify 14th generation appliances as they have a numeral “4” in the model number, for example XC6**4**0. The 13th generation appliances have a numeral “3” in the model number, for example XC630.

# 1 Release notes

## 1.1 False SATADOM errors on 14th Generation PowerEdge servers based appliances

**Description**:

On XC Series appliances, which are based on 14th Generation PowerEdge systems, there may be a number of messages in Prism and NCC checks referring to SATADOM issues.

Customers may encounter scenarios such as:

- No option to repair host boot device in Prism
- Issues with running SATADOM checks on the Prism Health page
- “SATADOM does not exist" error message in NCC logs

**Solution**:

This issue is caused by false reporting in NCC; NCC is expecting a SATADOM whereas 14th Generation based systems use a mirrored BOSS configuration.

This issue still exists in NCC 3.1.2, check for newer NCC version.

## 1.2 GUI status does not update after an expand cluster operation

**Description**:

Following a cluster expansion operation, the Prism GUI does not show the updated cluster status.

**Solution**:

This is cosmetic only, the system refreshes after a minute, or you can refresh the page to update the current status.

## 1.3 Foundation is downgraded during an expand cluster operation

**Description**:

When adding a new node to a cluster through the **Expand Cluster** operation, new nodes with a higher installed Foundation version are downgraded to match the version running on the existing nodes. The expected behavior is for the cluster to update Foundation on the cluster with the new node's higher version.

If either AOS or Foundation versions are lower on the new node, they will be updated to existing cluster version. This is expected behavior.

**Solution**:

This will be addressed in a future software release.

No other action is necessary. The Foundation version may remain as-is or you may update Foundation using the update software process in Prism after completing cluster expansion.

An Improvement Request has been opened with Nutanix.

## 1.4 HTTP Status 500 error in Prism during a “Register Failover Cluster” or “Upgrade” operation

**Description**:

On 14th Generation XC Series appliances, an error message has been seen in Prism while navigating to the Settings Gear Icon, registering the Nutanix cluster with vCenter. Then completing the HTTP Proxy setup and going to Upgrade Software. In addition, this was seen with Hyper-V 2012 R2 clusters in the process creating a failover cluster.

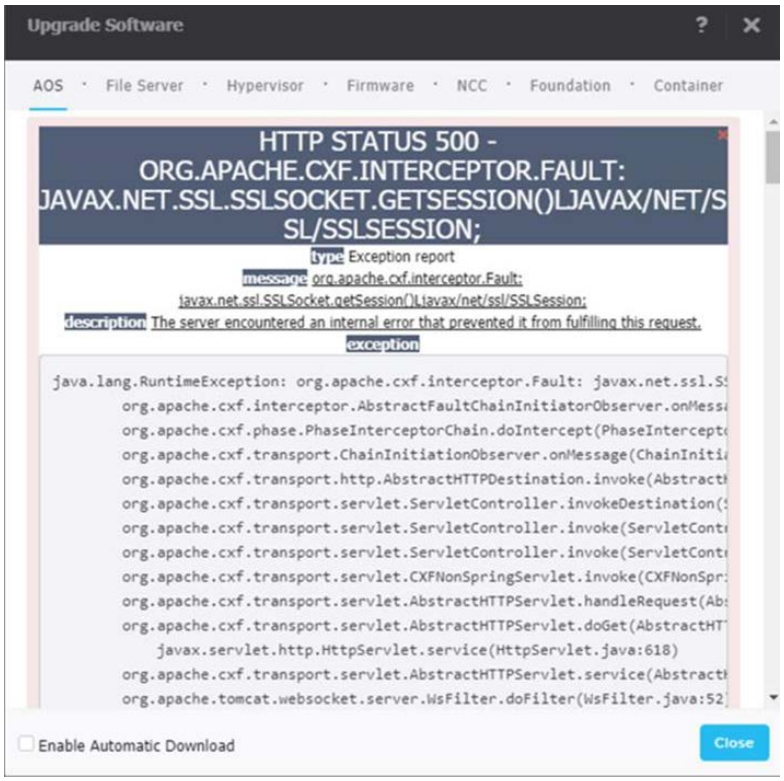


Figure 1 Example screen of the error message.

Solution:

Nutanix is aware of this issue and a fix will be included in a future update.

For further help, contact Dell EMC Support.

## 1.5 Kerberos setup for Hyper-V

After AOS 5.1.3, NTLM is no longer used for authentication with the SMB containers. For more information about Kerberos setup for Hyper-V, see: **https://portal.nutanix.com/#/page/docs/details?targetId=Web-Console-Guide-Prism-v51:hyp-kerberos-enable-t.html**

# 2 Important SED information

## 2.1 Correctly 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.
1. 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.
2. After this process completes, a yellow LED indicator blinks on the drive to be removed.

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

### 2.1.1 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.

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

#### 2.1.1.1 Nutanix KB articles

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.