Dell EMC XC Series Appliances and XC Core Systems Best Practices for Running Windows Server 2016 with Hyper-V

Abstract

This best practices guidance is aimed XC Series Appliances and Core Systems configured to boot Hyper-V nodes from a Boot Optimized Server Storage (BOSS) card boot device. This document provides recommendations for maintaining the stability and performance of the platform and workloads, while also preserving the operational lifetime of the boot device.

August 2018

Revisions

Date	Description
January 2018	Initial release
August 2018	Updated content to include XC Core.

Table of contents

Preface

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.

The Dell EMC XC Series Appliances and XC Core Systems are optimized to host scalable compute, storage, networking, and virtualization workloads. The design focus for the XC Series appliance provides a simplified and scalable approach for handling workloads.

Executive summary

This best practices guidance is aimed at 14th generation XC Series configured to boot Windows 2016 with Hyper-V from a Boot Optimized Server Storage (BOSS) card. This document provides recommendations for maintaining the stability and performance of the platform and workloads, while also preserving the operational lifetime of the BOSS card.

For assistance or questions regarding any of the items listed in this document, please contact Dell EMC Technical Support.

1 Boss card information

1.1 Important information about the Boss (PCIe cards M.2 Drive)

The Boot Optimized Server Storage (BOSS) card shipped with XC Series appliances is the appliance boot device. This PCIe card supports up to two M.2 SATA SSDs configured in RAID1 for high availability.

Note: Write intensive activities and processes leveraged by XC Series appliances, are intended to take place on the SSDs and HDDs and not the BOSS boot device. Any applications defaulting write activity to the BOSS boot drive should be redirected accordingly.

1.1.1 Examples of write intensive applications not to be run on the boot device

- System Center Agents
  - System Center Configuration Manager (CCMExec.exe)
  - System Center Operations Manager (MonitoringHost.exe)
- Write-intensive Agents
- Databases
- Disk management utilities (third-party disk defragmentation or partitioning tools).
- Additional roles outside of the appliance's intended use (web server, domain controller, RDS, and so on.).
- Client-based Antivirus.
- Virtual machines. Ensure that the Virtual Machines run only on Solid State Drives (SSDs) and Hard Disk Drives (HDDs).

1.2 Redirection of SCOM and SCCM logs

Note: Currently, Nutanix KB 3253 is an internal Nutanix document for Nutanix and Partner resources only. For assistance implementing the redirection of SCCM and SCOM logging using Nutanix KB 3253, contact Dell EMC Tech Support.

When using *Microsoft System Center Operations Manager (SCOM)* and *Microsoft System Center Configuration Manager (SCCM)* third-party tools to manage and monitor the XC Series hosts, you must consider write-activity to the system boot drive. SCOM and SCCM make frequent and heavy writes to the boot devices. In some cases, heavy wear may cause premature failure.

To mitigate premature failure of boot devices due to the impact of the third-party SCCM and SCOM tools, Dell EMC recommends redirection of the SCCM and SCOM writes.

Nutanix KB 3253 provides the process to redirect logging for both existing and new implementations of SCOM and SCCM. This process details the steps to create and present an iSCSI target on the Nutanix Distributed File System (NDFS) then present it to the XC hosts running Hyper-V for redirection of SCOM and SCCM logging and activity.

1.3 Run virtual machines on the Nutanix Distributed File System only

The boot device is slower performing and much more limited in space than the XC hosts' SSDs and HDDs used for the highly available Nutanix Distributed File System (NDFS) clustered storage.

Virtual Machines (VMs) run on the boot device are not highly available and potentially fill up the local boot device, which results in crashing the host hypervisor. This adds additional wear on the boot device.

Note: The Nutanix Cluster Checker (NCC) v. 2.2.2 and later monitors for VMs running on the boot device.

Important: A common cause for VMs being run from the boot device is misconfiguration during any add-node or redeployment operation.

When adding or redeploying a Hyper-V node to the cluster, ensure that the **Virtual Hard Disks** and **Virtual Machines** locations are configured in **Hyper-V Manager** so that they are directed to the Nutanix Cluster Container location. For example, the storage UNC path for cluster having a fully qualified domain name of **cluster.domain.com** and container name of **ntnx-ctnr1** would contain **\\cluster.domain.com\ntnx-ctnr1**.

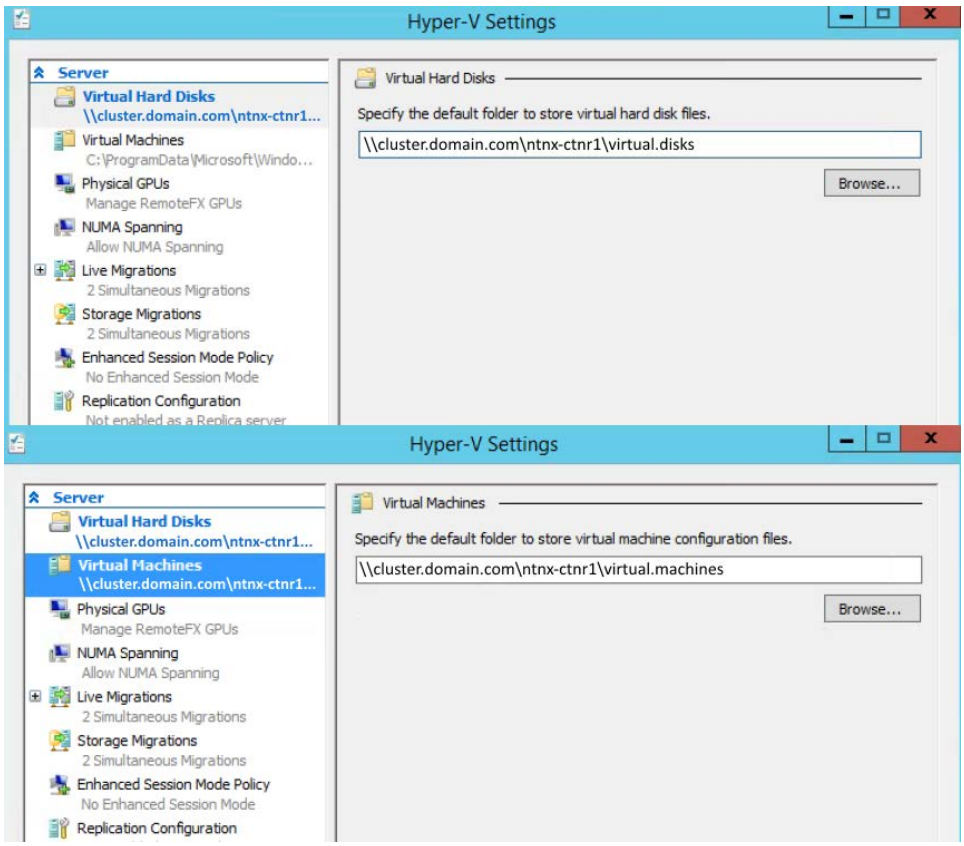

Figure 1 Hyper-V Manager Virtual Hard Disk and Virtual Machine UNC path

Note: In a Nutanix cluster, the path to the virtual hard disk files and virtual machine configuration files **should never** be a path containing a local drive letter.

1.4 Anti-malware software

Microsoft recommends against installation of anti-malware on the Windows Server 2016 with Hyper-V host operating system. However, if there is a regulatory compliance or other reason requiring that anti-malware software be run in the host operating system, Microsoft requires the following scan exclusion rules:

- Directories where virtual machines and virtual disks are stored
- C:\windows\system32\vmms.exe
- C:\windows\system32\vmwp.exe

If these exclusion rules are not created, you may encounter errors when creating and starting virtual machines.

Furthermore, the use of anti-malware in the management operating system may be associated with a non-trivial performance impact and premature wear out of the BOSS boot drive.

For additional information, see Microsoft's Plan for Hyper-V security in Windows Server 2016.

To remove Windows Defender Antivirus, use the following PowerShell command:

```
Uninstall-WindowsFeature -Name Windows-Defender
```

This uninstall requires a reboot.

For further information, see:

https://docs.microsoft.com/en-us/windows/threat-protection/windows-defender-antivirus/windows-defender-antivirus-on-windows-server-2016

1.5 Limiting additional Microsoft roles

Dell EMC and Nutanix recommend that you only install the following roles on an XC Series node running Windows 2016 with Hyper-V:

- Hyper-V
- Failover clustering
- Remote desktop services when running the add-in GPU card.

Microsoft also recommends limiting or removing unnecessary roles and services installed on a Windows Server running Hyper-V, as per the Hyper-V Best Practices Analyzer.

2 Required Microsoft updates

Microsoft suggest that all critical updates are applied and that all nodes in the cluster have matching updates.

2.1 Cluster Aware Updating feature

Cluster Aware Updating (CAU) is a Microsoft feature that enables automated rolling updates of clustered servers. CAU transparently performs the following tasks for each node in sequence:

- Individually places each node of the cluster into node maintenance mode
- Moves the clustered roles off the node
- Installs the updates and any dependencies
- Performs any necessary restart
- Brings the node out of maintenance mode
- Restores the clustered roles on the node
- Moves to update the next node

The CAU feature is only compatible with Windows Server 2016, 2012r2, 2012 and clustered roles that are supported on those versions.

For additional information about the Cluster Aware Updating feature, including overview, requirements, and best practices, see Cluster-Aware Updating Overview.

2.2 Mixed cluster recommendations

Windows 2012R2 and Windows 2016 clusters should not be mixed in the same cluster unless in the upgrade process.

Mixed generation (13th and 14th generation) appliances can be in the same cluster after AOS version 5.1.3.

Mixed processor versions can be in the same cluster as long as the same processor type. For example, Intel Processor compatibility mode must be enabled on every virtual machine for Live Migration to occur. This lowers the virtual machine's processor to the lowest version of processor. For more information, see:

https://technet.microsoft.com/en-us/library/gg299590.aspx

3 Kerberos enablement on Nutanix Hyper-V clusters

After AOS version 5.1.3, NTLM is not used to access the SMB3 shares. Kerberos must be set up on all Nutanix Hyper-V clusters. For more information, see:

https://portal.nutanix.com/#/page/docs/details?targetId=HyperV-Admin-AOS-v55:hyp-kerberos-enable-t.html

3.1 Kerberos time

Time skew should not be more than 5 minutes.

https://technet.microsoft.com/en-us/library/jj852172(v=ws.11).aspx

3.1.1 Time considerations

3.1.1.1 About Network Time Protocol (NTP)

Accurate time on the hypervisor and the Controller VM (CVM) on all XC Series clusters, regardless of the hypervisor type (ESXi, KVM, or Hyper-V) being run. Syncing to three or five external Stratum One time sources, the same as used by your Active Directory (AD) servers.

- Accurate timestamps are also important for troubleshooting interactions with third-party software products, which may require synchronized time between the hypervisor and the Controller VM to determine which files to back up.
- Accurate time synchronization between Nutanix clusters paired in Disaster Recovery (DR) configurations is important so that snapshots do not expire too quickly or too late.
- Graphs in the Prism interface rely on the CVM time. Incorrect time skews graphs, especially in relation to other monitoring platforms, which rely on other clock sources.

3.1.1.2 Configuring NTP servers

To add (or delete) an NTP server entry, do the following:

1. In **Prism**, on the main page, click the **Gear** icon.
2. On the **Gear** menu (see Main Menu Options), select **NTP Servers**.
3. On the **NTP Servers** dialog box, do one of the following.

   a. To add an NTP server, in the **NTP Server** box, type the server IP address or fully qualified host name and then click **Add**. The name or address is added to the **HOST NAME OR IP ADDRESS** list (below the NTP Server field).
   b. To delete an NTP server entry, in the **Servers** list, click the **delete (x) icon** for that server.

4. In the dialog box that appears to verify the action; click **OK**. The server is removed from the list.

3.1.1.3 Configuring Time Zone

The Nutanix Controller VM (CVM) defaults to Pacific Time, specifically America/Los_Angeles time configuration. Failure to configure the time zone correctly results in NCC warnings.

1. To change the time zone across all CVMs in the cluster, issue the following command:

   ```
   $ ncli cluster set-timezone timezone=cluster_timezone
   ```

Note: To determine the correct time zone, refer to the List of tz database time zones

For example, to set the time zone to Ireland, issue:

```
nutanix@NTNX-CHASSIS1-3-CVM:~$ ncli cluster set-timezone
timezone=Europe/Dublin
Please reboot the CVM or restart all services on the cluster so that logs
are timestamped with the new Timezone.
Cluster Id                : 00055e17-c0b2-4015-029b-
7cd30abf42fa::18788105532625791 4
    Cluster Uuid              : 00055e17-c0b2-4015-029b-7cd30abf42fa
    Cluster Name              : cluster1
    Cluster Version           : 5.1.3
    External IP Address       : 192.168.10.154
    External Data Services... :
    Node Count                : 3
    Block Count               : 2
    Support Verbosity Level   : BASIC_COREDUMP
    Lock Down Status          : Disabled
    Shadow Clones Status      : Enabled
    Password Remote Login ... : Enabled
    Timezone                  : Europe/Dublin
    Has Self Encrypting Disk  : no
    Common Criteria Mode      : Disabled
nutanix@NTNX-CHASSIS1-3-CVM:~$
```

2. Restart the CVMs so that log files are stamped with the correct time zone.

4 Active Directory and DNS best practices

4.1 Active Directory, Organizational Units (OUs), and Group Policy Objects (GPOs)

To minimize misapplication of GPOs and other policies to the XC Series hosts configured to run Hyper-V, Dell EMC recommends placing the XC Series hosts in to their own OU and linking only specific GPOs to that OU.

By default, when adding to Active Directory, the Nutanix cluster nodes are added to the computer's Computers OU. Any GPOs assigned to the Computers OU will be applied to the nodes. The nodes should be moved to their own OU and group policy reapplied. Leaving them in the Computers OU potentially exposes the nodes to enforcement of policies and security settings that are not ideal for a production Hyper-V node, yet perfectly suitable for a desktops running Windows.

When adding a node to a cluster, the same behavior is also observed. It is important to move any added node into the same OU that contains the other cluster nodes.

4.2 Disjointed domain and DNS namespace

A disjointed namespace occurs when one or more domain member computers have a primary Domain Name Service (DNS) suffix that does not match the DNS name of the Active Directory domain of which the computers are members.

An example of disjointed namespace is a member computer with a primary DNS suffix of `corp.company.com` in an Active Directory domain named `xyz.corp.company.com`.

While not a strictly prohibited configuration, environments configured with a disjointed namespace introduce additional challenges and considerations for both Nutanix clusters running on Hyper-V and other tools reliant upon DNS. Whenever possible, Dell EMC recommends having a single Active Directory Domain and DNS namespace.

A disjointed namespace causes an error to be reported in Nutanix Cluster Check (NCC) stating the AOS cluster computer object is not configured correctly in Active Directory.

In addition to Nutanix issues, other tools, like System Center will require additional configuration steps.