Best Practices/Caveats

This section highlights best practices and caveats that were discovered or encountered during the validation testing.

Design & Implementation Best Practices

This section discusses best practices for this solution. Review documents links in Commvault Simpana, page A-1 for complete coverage of best practices.

During the validation testing, Hyper-V networking was originally implemented in two sites. These sites were later changed to Nexus 1000V using two different methods. The first method repurposed the vNIC interfaces on the Hyper-V hosts from Hyper-V switch uplinks to Nexus 1000V uplinks. This method required removing VM and Hyper-V network configurations, implementing the Nexus 1000V configuration, then reconfiguring the VM configurations.

The second method added vNICs to the Hyper-V hosts (UCS B200 M3) Service Profile on the UCSM, which required reboots. The Nexus 1000V was then implemented in parallel to the Hyper-V networking. VMs were then moved from Hyper-V to the Nexus 1000V with little impact. Neither of these methods resulted in problem-free migrations and disruptions to the Hyper-V cluster while troubleshooting issues did occur. If the Nexus 1000V is going to be deployed in an environment, it might be desirable to deploy it at the start to avoid this migration.

As noted in this document, Nexus 1000V was replaced with the native Hyper-V virtual switch later in the CCA-MCP design to reduce complexity. However, this BaaS Commvault lab testing stayed with the N1kv component.

Commvault Simpana

This section provides sizing and best practice guides.

CommServe

- CommServe System Requirements
- CommCell Performance Tuning Guide
- CommCell Scalability Guide

MediaAgent

Building the MediaAgents in pairs, using partitioned DDBs and NAS file shares provides the best availability within the environment.

Separate SSD based arrays for the DDB and Index Cache provides the best performance and growth potential for each individual MA.

- MediaAgent System Requirements
- DeDuplication Building Block Guide
- DeDuplication Best Practices

Web Proxy

- Commvault Firewall Best Practices

Reporting Server

- Private Metrics Reporting Server system requirements

Virtual Server iDataAgent for Hyper-V

- System Requirements
- Best Practices

Virtual Server iDataAgent for VMware

- CVLT VSA Building Block Guide
- Best Practices

Windows File System iDA

- Best Practices

Linux File System iDA

- Best Practice

Microsoft SharePoint iDA

- Best Practices
- Microsoft SQL Server iDABest Practices

Microsoft SQL Server iDA

- Best Practices

Oracle / Oracle RAC iDA

- Best Practices—Oracle
- Best Practices—Oracle RAC

Caveats

This section discusses solution caveats.

Cisco CSR 1000V

Interface Renumbering After Moving to New Hyper-V Host—When the Cisco CSR 1000V is installed on a Microsoft Hyper-V cluster, the interface numbers can change after a Hyper-V host failover event to a new host server or live migration. In both cases, the condition is not seen until after a reboot. The following steps can be taken to mitigate this issue.

Prior to executing a live migration enter the **clear platform software vnic-if nvtable** command.

The command can also be successful if executed after the failover, but only before the config is saved or the VM restarted.

Configuring static MAC addresses for the network interfaces.

In the event that the interfaces have been renumbered and the IP addressing is removed, the following steps can be used to recover.

1. Execute **clear platform software vnic-if nvtable** command.

2. Copy saved config to startup config.

3. Reboot the CSR.

Cisco Nexus 1000V

Migrating VM from Hyper-V Switch to Nexus 1000V—After migrating to the Nexus 1000V, when configuring existing VM Network Adapter interfaces that were previously configured for a Hyper-V switch, the change may not complete or the VM may fail to start. In either case, you may need to remove the existing interfaces and create new ones.

Cisco UCS C240 M3

Broadcast Packets—During validation testing, an issue was discovered that impacted the C240 servers from receiving broadcast packets. The issue was isolated to the VIC 1225 network driver in release 2.0(3d) and was resolved in the VIC driver in release 2.0(3i). Refer to CSCur44975 for more details.