Configuring Dell Storage Manager for High Availability

Dell Storage Engineering
November 2019

A Dell EMC Best Practices Guide

Revisions

Date	Description
November 2016	Initial release
November 2019	vVols branding update

Acknowledgements

Author: Darin Schmitz

Table of contents

Executive summary

With Dell™ Storage Manager (DSM) 2016 and later, services that run on the Data Collector server have become a critical piece of infrastructure in the storage area network. Not only is the Data Collector server used for daily administration and troubleshooting, but it also contains services that require high availability such as:

- Live Volume Auto Failover tiebreaker
- VMware® vStorage APIs for Storage Awareness (VASA) provider for VMware® vSphere ® Virtual Volumes™ (vVols)
- Application Protection Manager integration
- Dell Storage PowerShell and REST API endpoint
- Threshold and system alerting through SMTP or SNMP
- SMI-S provider used by Microsoft® System Center Virtual Machine Manager (SCVMM)

In most cases, short periods of downtime such as a maintenance window for a reboot after patching is acceptable, but for the most part, these services need to remain highly available. For example, the VMware VASA provider service must be available to power on virtual machines residing on VMware vVols, and Live Volumes need the tiebreaker service available for auto-failover to mediate any array failures.

This guide discusses high-level techniques and strategies for protecting the DSM Data Collector server from outages, reduce risk, and promote high uptime of its critical storage services.

1 Basic protection

To protect Dell Storage Manager, there are some initial steps that should be taken to provide the bare minimum protection of the Data Collector and its SQL database.

1.1 Virtual machine

Current guidance from the DSM documentation recommends that for best results, the Data Collector be installed onto a Windows Server® virtual machine. High availability features of the VMware and Hyper-V® hypervisors are discussed in section 2.

1.2 Redundant storage

The DSM Data Collector virtual machine should be backed by redundant storage. Since array-based storage can offer up to five nines of availability, as well as snapshots, replication, and other data-protection features, the virtual machine data is best protected within a storage array. Also, where possible, it is recommended to store the Data Collector virtual machine on storage outside of the failure domain. For example, store the VM on redundant storage outside of the arrays that DSM is managing, such as a data center management cluster.

However, in environments where only local storage is available, additional precautions are required to ensure the local storage is redundant, such as using RAID or drive mirroring. In addition, to protect against multiple drive failures in a single host, multiple copies of the Data Collector virtual machine should be kept using a feature such as Hyper-V Replica as discussed in section 2.

Important: The Data Collector that runs the VASA provider, as well as the vCenter® server for the environment, should never be stored within a VMware vVol storage container. This is because the VASA provider within DSM is responsible for all Virtual Volume bind and unbind operations required for powering on and off virtual machines. If DSM becomes unavailable, virtual machines cannot be powered on, but existing virtual machines that are already bound to the protocol endpoint will keep running.

1.3 Snapshots

The Data Collector should have a regular array snapshot schedule assigned to take periodic backups of both the Data Collector and its associated SQL database server. The actual snapshot schedule and retention policy will vary depending on the organization's recovery point objectives (RPO), but the bare minimum should be a daily snapshot.

However, when using VMware vVols, the snapshot frequency should be increased depending on how frequently storage changes occur within the environment. Keep in mind that the VASA provider data is stored within the Data Collector SQL database, so the frequency of the snapshots should align with how often configuration changes are made. For example, if virtual machine storage configuration changes are made hourly, then the schedule should take snapshots of both the Data Collector and the SQL database hourly. However, if the environment is static, snapshots can be taken less frequently.

1.4 Replication

If multiple Dell SC Series arrays are available in the environment, replicate the virtual machine and its corresponding SQL database to a secondary array. The snapshot schedule determines when data is transferred to the secondary array unless using synchronous replication or when replicating the active snapshot asynchronously.

1.5 Redundant networking

To help ensure high uptime of the Data Collector, the LAN and SAN networks should follow standard industry best practices for redundancy configuration, ensuring there are no single points of failure in either network. Multipathing should be used on the SAN, while NIC teaming should be used on the LAN.

1.6 SQL database

While it is acceptable for pre-production to install the SQL database on the same virtual machine as the Data Collector services, for production the SQL database should be stored on a separate virtual machine. In the event the Data Collector virtual machine is lost, the VASA data will remain protected within the database isolated in the other virtual machine.

1.7 Remote Data Collector

When using the remote Data Collector, it is important to remember that only saved restore points are mirrored from the primary. Performance statistics, VASA data, vVol configuration data, and APM data are not copied between the primary and secondary Data Collector databases.

2 Host availability

Since the Data Collector services need to remain highly available, the hypervisor can be used to provide additional protections for greater uptime.

2.1 VMware

When running the Data Collector virtual machine on VMware vSphere, there are several key features that can protect the virtual machine.

2.1.1 vMotion

The VMware vSphere vMotion® feature allows the virtual machines to be migrated between physical hosts, and is an important piece to provide proactive uptime. Should a VMware ESXi™ host need maintenance, vMotion can safely move the DSM virtual machines to another node in the cluster before a planned outage.

2.1.2 VMware vSphere High Availability (HA)

With regards to unplanned outages, VMware vSphere High Availability will protect the virtual machine from host failures, as well as individual virtual machine failures. In the event either the host fails or the virtual machine stops responding to heartbeats, it will be restarted on a different ESXi host in the cluster. When using vSphere HA, the Data Collector downtime is limited to how long it takes the virtual machine to reboot on a different host.

2.1.3 VMware vSphere Fault Tolerance (FT)

VMware vSphere Fault Tolerance increases uptime even further by statefully mirroring the virtual machine to a separate ESXi host in the cluster. In the event of a failure, the virtual machine can resume operations immediately, picking up where the previous virtual machine left off.

The use of VMware Fault Tolerance with vSphere 6.x is highly recommended to ensure that the DSM Data Collector has the highest availability possible. Although vSphere 5.x also provides fault tolerance, to ensure adequate performance of the Data Collector, the dual vCPU functionality of vSphere 6.x is required. When utilizing VMware Fault Tolerance, the only expected downtime will be for operating system patching reboots during the virtual machine's regularly scheduled maintenance window.

2.2 Microsoft

The Microsoft Windows Server product line also has a number of technologies to provide high availability for the DSM Data Collector and SQL database machines.

2.2.1 Microsoft failover clustering

Since the DSM Data Collector services by themselves are not cluster aware, traditional failover clustering cannot be used. However, the DSM services can run within a virtual machine on Hyper-V, and leverage Hyper-V failover clustering.

2.2.2 Microsoft Hyper-V with failover clustering

When using Hyper-V, if a host fails, the virtual machines will be restarted on another host in the cluster, limiting downtime to how long the VMs take to reboot on another node in the cluster.

2.2.3 Live Migration

Microsoft Hyper-V Live Migration also can provide the important role of being able to proactively move the virtual machines to another node in the cluster for maintenance. Should a host need rebooting, the virtual machine can safely be migrated to another node in the cluster proactively.

2.2.4 Hyper-V Replica

In situations where there is no array-based storage to store the DSM VMs, a standalone Hyper-V host with local redundant disks, in conjunction with using Hyper-V Replica, can ensure that the VMs can be recovered on another host server or cluster in the environment. Where possible, the replicas should also be stored outside of the failure domain of the arrays being managed.

3 Conclusion

With the help of hypervisor technologies, Dell Storage Manager can be configured such that it can achieve very high availability. For more detailed technical information about the various technologies discussed in this paper, refer to the related best practices guides at Dell.com/StorageResources.

A Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

Storage technical documents and videos provide expertise that helps to ensure customer success on Dell EMC storage platforms.

.