Active System Manager Virtual Appliance Best Practices for VMware

This Dell technical white paper provides information about best practices for configuring Active System Manager Virtual Appliance in a VMware environment.

Author:
Dmitry Gomerman

This document is for informational purposes only and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.

January 2013| Rev 1.0

Contents

Introduction

The purpose of this white paper is to describe best practices for configuring, backing up, restoring, and updating the Active System Manager virtual appliance in a VMware environment. It also includes recommendations for hardware, virtualization platform, disaster recovery, scalability, sizing virtual machines (VMs), and managing virtual machine snapshots.

Hardware Recommendations

- All VMs, including the Active System Manager virtual appliance, should reside on shared centralized storage, preferably accessed over 10GbE or Fibre Channel network.
- It is recommended to use a 10GbE vMotion network to dramatically reduce the time required to migrate a VM.
- Set the BIOS to enable all populated sockets and enable all cores in each socket.
- Enable the processor's Turbo Mode, if the processor supports this feature.
- Enable hyper-threading in the BIOS.

Virtualization Platform

VMware® vSphere and a hypervisor cluster are not required to deploy the Dell Active System Manager OVF VM; however, they are required to take advantage of the following advanced features of vSphere.

- **vMotion** enables live migration of running virtual machines from one physical server to another with zero downtime, continuous service availability, and complete transaction integrity. This technology is critical to creating a dynamic, automated, and self-optimizing datacenter.
- **Distributed Resource Scheduler (DRS)** continuously monitors utilization across vSphere servers to intelligently allocate available resources across VMs according to business needs. It reads information about virtual guest operating systems, resources in use, and available resources to make informed decisions about load balancing and resource utilization.
- **High Availability (HA)** provides high availability for applications running on virtual machines. It automatically monitors the health of ESX hosts, and automatically restarts VMs on production servers with spare capacity when a host fails. In cases of operating system failure, HA restarts the affected VM on the same physical server.
- **Fault Tolerance (FT)** provides continuous availability for applications in the event of server failure by creating a live shadow instance of a VM that is in virtual lockstep with the primary instance. By allowing instantaneous failover between the two instances, FT eliminates even the smallest chance of data loss or disruption by triggering seamless stateful failover when protected VMs fail to respond. Additionally, it creates a new secondary VM after failover to ensure continuous application protection.
- **Site Recovery Manager (SRM)** provides seamless site recovery of an entire virtualized data center by managing storage, VM, and network failover.

Configuring the Active System Manager Virtual Appliance

When configuring an Active System Manager appliance, best practices include:

- Remove/disable any virtual hardware that the appliance does not need, including floppy drives, CD drives, USB ports, and so on, as described in the Vmware documentation.
- Use SCSI virtual disks whenever possible. Although it is not always the case, VMware SCSI disks generally have lower overhead on the hypervisor and better performance than IDE disks.
- Install VMware Tools for VM performance and management. VMware Tool include optimized network and video drivers and improved synchronization time between the host and VM. They also allow shutdown and restart of the operating system running on the VM, and improve VM health monitoring from VirtualCenter.
- Enable DRS and (optionally) High Availability (HA), as described in VMware documentation. HA monitors the health of ESX hosts, and automatically restarts VMs on servers with spare capacity if a host fails. In cases of operating system failure, HA restarts the affected VM on the same physical server, providing an additional layer of protection that ensures less down time for the Active System Manager appliance.
- Configure VMs to swap to centralized storage. Avoid swapping to local storage or host swapping to solid-state disks (SSD), which can slow down VM migrations using vMotion.
- When using the multiple–network adaptor feature, configure all vMotion vmnics under one vSwitch, and create one vMotion vmknic for each vmnic. In the vmknic properties, configure each vmknic to leverage a different vmnic as its active vmnic, with the rest marked as standby. This way, if any vMotion vmnics become disconnected or fail, vMotion will transparently switch over to one of the standby vmnics. When all vmnics are functional, each vmknic will route traffic over its assigned, dedicated vmnic.
- Use Network Time Protocol (NTP) to synchronize time. System time is an issue of great importance to many computer applications—databases, security monitoring tools, email systems, syslog, and other logging tools all use time stamps in writing transactions and noting various events. VMware Tools has an option for synchronizing VMs with the ESX host on which they run. Every ESX host in a given resource cluster should have its system clocks synchronized so that when a VM migrates from one ESX host to another, its system time remains consistent. For additional information, see http://kb.VMware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1003063.
- Enable the "hot add" feature for CPUs and memory on the Active System Manager guest operating system (OS).

Sizing Virtual Machines

A best practice when configuring resource pools at the host level is to avoid fully committing resources for the host CPU. Instead, leave at least 30% of the CPU unreserved for vMotion. When initiating vMotion, the VMkernel attempts to reserve CPU resources. If that reservation fails, then vMotion still proceeds, but its performance might be impacted. Similarly, when using resource pools for a cluster on which DRS is enabled, it is recommended to leave at least 10% of the CPU capacity unreserved. CPU reservations that fully commit cluster capacity can prevent DRS from migrating virtual machines between hosts.

The Active System Manager appliance requires a minimum of two virtual CPUs (vCPUs); however, it is important to make sure that the total number of vCPUs assigned to all VMs does not utilize more than 80% of the ESX host's CPU.

Minimizing use of the Memory Balloon driver, as well as swapping, requires allocating 8GB of reserved RAM.

Backing Up and Restoring the Virtual Appliance

To simplify backing up Active System Manager, it is recommended to run the Active System Manager virtual appliance from centralized storage.

One back-up strategy is to configure the storage array shared volume that contains the Active System Manager OVF to automatically create and manage nightly snapshots (this process differs from the VM snapshots described in the next section). It is recommended to keep at least one week's worth of snapshots.

An alternate strategy is to configure real-time array replication between two or more storage arrays. Although the replication can be local, the best practice is to replicate between two separate data centers.

For detailed information on how to backup and restore the Active System Manager appliance, see the *Active System Manager User Guide*.

Virtual Machine Snapshots

NOTE: It is important to understand that VM snapshots alone are not an adequate backup strategy.

A snapshot is a virtual disk change log that is useful for preserving a VM's state and data at a specific point in time. It includes data such as power states and the files that comprise a virtual machine.

It can be helpful to think of a snapshot as temporary storage space. A new VM starts with a base temporary file (server-flat.vmdk). Creating a new snapshot and making changes to the server creates a new temporary file (server-000001.vmdk). Taking another snapshot creates another temporary file (server-000002-delta.vmdk)—all subsequent changes are saved to this new snapshot file. For example:

Base Disk -> server-flat.vmdk
Snapshot 1 -> server-0000001-delta.vmdk
Snapshot2 -> server-000002-delta.vmdk

All snapshots reference previous snapshots and the base disk (server-flat.vmdk) using a child ID (CID) and parentCID. For example:

- The base disk (server-flat.vmdk) has a CID of 1234ABCD.
- Snapshot1 (server-000001-delta.vmdk) has the parent CID of 1234ABCD and a unique CID (8-digit HEX).
- Snapshot 2 has a parentCID equal to the unique 8-digit HEX CID number of Snapshot1.

This pattern continues with each additional snapshot, resulting in what is called the "snapshot chain."

It is important to remember:

- Snapshots do not replace a comprehensive backup strategy.
- Use snapshots prior to applying a guest operating system or application patches.
- Specifically for Active System Manager, create a snapshot prior to applying Active System Manager patches or making fundamental configuration changes. See VMware documentation for instructions on creating and managing VM snapshots.

The best practice is to have only one snapshot in the snapshot manager at all times, because VM snapshots can quickly outgrow the base VMDK. Also, it is recommended to commit snapshots to the base disk at least once every week (click **Delete All** in snapshot manager). This keeps the size and the amount of data stored in temporary snapshot files to a minimum, helps to prevent data loss, and improves server performance.

For example, if making major upgrades to a program such as Microsoft® Exchange, then best practices include:

- Commit all snapshots to the base disk (server-flat.vmdk) by clicking **Delete All** in snapshot manager.
- After committing the snapshots, take a new snapshot. Make sure to label it with an informative description—for example, you might include the date and time the snapshot was taken.
- If server changes cause instability that requires reverting to a previous state, then open snapshot manager, highlight the desired snapshot, and click **Revert**. This will return the server to the exact state of the indicated snapshot. Keep in mind that any new files created since the snapshot to which the server is reverting will be completely deleted and unrecoverable.

For detailed information about VMware snapshots, see http://kb.VMware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1025279.

Updating the Active System Manager Virtual Appliance

Updating the Active System Manager virtual appliance upgrades the software to the most recent version, including any operating system security patches that are required. For detailed instructions on updating the virtual appliance, see the *Active System Manager User Guide*.

Best practices for updating the virtual appliance include:

- Use vMotion to apply ESX patches to the Active System Manager appliance without causing solution downtime.
- Make sure that the Active System Manager appliance runs inside a vSphere cluster, and that the cluster has enough available capacity to sustain placing any one host into maintenance mode.
- If DRS is disabled, then manually use vMotion to migrate all host VMs to other available servers.

- Place the vSphere hypervisor host running the Active System Manager virtual appliance into Maintenance Mode, as described in VMware documentation. If DRS is enabled, then vMotion will automatically migrate the VMs to other available hosts using vMotion.
- Apply ESX patches according to VMware recommendations, and then restart the host. After the host restarts and joins the vCenter cluster, take the host out of Maintenance Mode, as described in VMware documentation. If DRS is enabled on the cluster, it will automatically balance the VMs use the extra capacity made available by taking the newly patched host out of Maintenance Mode.

Disaster Recovery

Best practices for disaster recovery include:

- It is recommended to host the Active System Manager VM appliance in an HA-enabled cluster. Both host and VM monitoring should be enabled.
- If uninterrupted access to the Active System Manager appliance is required, then it is critical to enable FT.
- The expectation is to have independent (and possibly multiple) Active System Manager appliances within a datacenter (for example, one appliance in production and one for disaster recovery). Therefore, it is recommended to disable SRM for Active System Manager VMs.

For detailed instructions on configuring these features, see VMware documentation.

Scalability

Best practices for implementing a scalable infrastructure include:

- For best performance, limit each Active System Manager appliance to a maximum of 12 chassis, each with a maximum of 32 blade servers (384 servers in total).
- Multiple Active System Manager appliances can run concurrently in the same vSphere cluster.
- While it is possible to run multiple Active System Manager appliances on the same management network, it is recommended to run each Active System Manager appliance on an independent management network.

Sources

- http://searchvmware.techtarget.com/tip/Improving-VMware-ESX-Server-performance-10-best-practices
- http://blogs.vmware.com/performance/
- http://www.vmware.com/products/datacenter-virtualization/vsphere/features.html
- VMware white paper *Best Practices for Building Virtual Appliances* (http://www.vmware.com/resources/techresources/1011)
- VMware white paper *Enterprise Java Applications on VMware Best Practices Guide* (http://www.vmware.com/files/pdf/techpaper/Enterprise-Java-Applications-on-VMware-Best-Practices-Guide.pdf)

- VMware white paper *Performance Best Practices for VMware vSphere 5.1* (http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.1.pdf)
- VMware white paper *VMware vSphere vMotion Architecture, Performance and Best Practices in VMware vSphere 5* (http://www.vmware.com/files/pdf/vmotion-perf-vsphere5.pdf)