Guidelines for Implementing VMware vSphere 4 with the Cisco Nexus 1000V Virtual Switch

Cisco and VMware: Virtualizing the Data Center

VMware vSphere 4 introduced a number of new features enabling customers to further virtualize their datacenter environments. One of these new features was the VMware vNetwork Distributed Switch (vDS) that simplified virtual networking with a distributed model that presents a single aggregated virtual switch across multiple ESX/ESXi 4 hosts.

vDS also introduced third party virtual switch support for the Cisco Nexus 1000V. The Nexus 1000V follows the same distributed model as vDS, but uses an enhanced feature set and network operational model similar to that used with physical Cisco Catalyst and Nexus switches.

Overview of Guidelines and Considerations

Deploying VMware vSphere 4 with the Cisco Nexus 1000V introduces a number of considerations in using some vSphere 4 features. Note that these considerations relate only to the first release of vSphere 4 and ESX 4.0 (build 164009). Some of these considerations may get addressed in later updates and releases.

The products and features affected and requiring additional consideration are:

- Host Profiles
- vShield Zones
- iSCSI Multipathing
- AppSpeed
- Site Recovery Manager 4.0 (SRM)
- VMware Accesspoint

The considerations for each of these are explained in further detail below.

Implementation Guidelines

Host Profiles

Host Profiles is a new feature with vSphere 4 that allows users to create a common ESX or ESXi template to provision and configure multiple hosts. The host profile contains information about the number of uplinks or physical network interface cards (pnics) that need to be connected to the virtual machine.

Implementation with VMware vDS and Cisco Nexus 1000V

Host profiles in the vSphere 4 GA Release (Build 164009) supports only one dvUplink (Distributed Virtual Uplink) portgroup per vDS. Customers requiring more than one dvUplink portgroup in the same vDS cannot currently use the host profiles feature to provision the vDS.

VMware vShield Zones

VMware vShield Zones is a virtual asset aware distributed firewall integrated into vSphere 4 through the vCenter Server SDK. vShield Zones is a critical security component for protecting virtualized datacenters from attacks and misuse helping customers achieve compliance mandated goals.

Implementation

vShield Zones provides isolation and segmentation zoning feature set to protect guest virtual machine workloads. The vShield Zones product consists of one centralized vShield Manager per vCenter Server and vShield Zones modules for the ESX hosts. The vShield Zones modules are automatically deployed in the data path between the physical network adapters and the guest virtual machines when used in conjunction with the VMware vNetwork Standard Switch (vSS) or the VMware vNetwork Distributed Switch (vDS). vShield Zones is integrated into the vDS or vSS through the creation of two virtual switch instances—one trusted instance with guest virtual machine Portgroups connecting through the vShield Zones agent to the untrusted instance supporting the physical network adapters (vmnics). This is implemented on each host requiring vShield Zones protection.

The Cisco Nexus 1000 virtual switch will fully support the vShield Zones module as of the VMware vSphere 4 Update 1 release using a new Cisco Nexus "service-port" feature that allows redirection of traffic to security virtual appliances for processing. In the interim, it is possible to integrate the vShield and the Cisco Nexus 1000V virtual switch by connecting all guest virtual machines through a Nexus 1000V Port Profile and placing the physical network adapters on a VMware vDS or vSS. A vShield Zones agent interconnects the VMware vDS or vDS virtual switch and the Cisco Nexus 1000V. This interim approach allows you to manage the virtual machine networking aspects via the Nexus 1000V Port Profiles, but manage the physical network adapters through the VMware virtual switches.

iSCSI Multipathing and offload

Provides multipathing capability to iSCSI storage. This feature enables high availability of iSCSI storage by ensuring multiple paths to storage and spread traffic evenly across physical network adapters. iSCSI offload is hardware acceleration of storage traffic offloaded to specialized hardware.

Implementation

iSCSI multipath is not currently supported by the VMware vDS and Cisco Nexus 1000V. Customers wishing to use iSCSI multipath can use the VMware vNetwork Standard Switch (vSS) to connect the vmkernel ports for the iSCSI initiators.

VMware AppSpeed

VMware vCenter AppSpeed provides proactive performance management and service-level reporting for applications running within virtual machines. VMware vCenter AppSpeed provides IT administrator visibility into multi-tier applications (performance, usage and dependencies) running across both virtual and physical infrastructure.

Implementation

The AppSpeed feature provides performance statistics for a VM by capturing VM network traffic. Customers can use AppSpeed with vDS or Nexus 1000V after performing a few steps of configuration as described in the VMware AppSpeed User Manual. These steps are not necessary when performing the configuration on a VMware vSS.

VMware vCenter Site Recovery Manager 4.0 (SRM)

VMware vCenter Site Recovery Manager (SRM) provides manageable and automated disaster recovery.

Implementation

SRM 4.0 and above, supports vSphere 4 with VMware vDS or Cisco Nexus 1000V. Refer to the Site Recovery Manager 4.0 Documentation for more details on implementing SRM http://www.vmware.com/support/pubs/srm_pubs.html.

VMware vCenter Lab Manager 4

VMware vCenter Lab Manager 4 combines the functionality of VMware Lab Manager 3 and VMware Stage Manager. Lab Manager 4 allows IT organizations to provide on-demand access and automated management of the internal cloud for test and development. Application owners, development, QA, and training teams can deploy, capture, and share multi-tier application environments in seconds while IT remains in administrative control. Lab Manager saves time, simplifies administration of fast changing environments, and enables project teams to get to market faster.

Implementation

VMware vCenter Lab Manager 4 dynamically creates and removes virtual networks in the course of its normal operation. It leverages the VMware vDS to enable host-spanning private networks, a new feature in Lab Manager 4. As Lab Manager involves creation of and removal of networks, and the Cisco Nexus 1000V takes control over network creation/removal away from the VMware infrastructure, the Cisco Nexus 1000V is not compatible with Lab Manager 4**.**

VMware Data Recovery

VMware Data Recovery is a product that integrates into the backup and recovery mechanism used by the customers.

Implementation

The current implementation does not restore the network configuration during a restore. Customers using Data Recovery should manually restore the network configuration for proper functioning of the vSphere hosts after restore.

Distributed Power Management

VMware Distributed Power Management (DPM) is a feature that allows for CPUs and physical servers to be powered down in the event no load is present on the servers. The "wake on LAN" feature is used to bring up the servers and CPUs as and when necessary. This allows customers to dynamically power off servers not used by the workload.

Implementation

The vSphere hosts with Cisco Nexus 1000V installed cannot participate in DPM since these hosts are not recognized as being capable of "wake on LAN". However, if the hosts have an Integrated Lights Out (ILO) or Intelligent Platform Management Interface (IPMI) capability, then DPM can be configured to work with vSphere 4 and the Nexus 1000V.

For more information, visit: **www.vmware.com**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

VMware, Inc
3401 Hillview Ave
Palo Alto, CA 94304
USA
www.vmware.com
Tel: 1-877-486-9273 or 650-427-5000
Fax: 650-427-5001