VMware and Cisco Virtualization Solution: Scale Virtual Machine Networking

What You Will Learn

The tight integration between Cisco and VMware has delivered a unique solution that allows the network team to manage virtual networking with the same features and capabilities as the physical network without affecting the server team.

Introduction

Server virtualization and consolidation have become a central strategy for many server teams trying to address their companies' growing demands for server resources while still combating server sprawl—all within the context of declining budgets.

While server virtualization delivers well-documented benefits to the server team, it introduces a number of complications for the network team. At the very least, these complications can reduce operational efficiency for the network team, and in some circumstance they can have a broader and more significant effect on the data center.

Lack of Transparency

Perhaps the most significant challenge for the network team is the lack of visibility in the virtual machine environment. In a traditional physical environment, with one server per network port, the process of mapping necessary policy for features such as security and quality of service (QoS) to that server is simple. In a virtualized environment, dozens of virtual servers may be connected to a physical port through a software switch that resides on the server as part of the hypervisor. These factors require reassessment to determine the best way to support a virtualized environment.

Because dozens of virtual machines, each with different network and security policy requirements, may reside on one physical port, application of policy at the physical port level is no longer tenable. Such an approach severely complicates the ability of the network and server teams to ensure that the correct network policy is applied to a particular virtual machine (that is, a particular application).

This same challenge extends to troubleshooting. For example, in a physical environment, if users of an application are experiencing application-responsiveness problems, the traffic on the port to which the server running the application is connected can easily be analyzed to determine whether a network component is causing the problem. In a virtualized environment, the traffic from all the virtual machines is blended together, so isolating traffic from a particular virtual machine at the physical port is much more difficult to do. In addition, because of the software switch in the hypervisor, the network team cannot use the same tools and processes it would normally use to troubleshoot and manage the rest of the network.

One additional transparency-related concern arises from the hypervisor-based switch. Traffic can be switched between virtual machines on the same server without any capability to control or audit this interaction, a situation that introduces a number of concerns related to security and policy compliance.

Virtual Machine Portability Challenges

One of the significant benefits of server virtualization is live migration, or the capability to move a running virtual machine from one physical server to another without any disruption. This feature has clear benefits for capabilities such as resource balancing, system availability, and even simple server maintenance. However, it does introduce some challenges from a network perspective.

Foremost among these is the fact that, as a virtual machine moves, its network policy (VLAN, QoS features, security policy, etc.) also needs to move. In the past, movement of policy along with the virtual machine has generally been handled through one of two scenarios. In the first scenario, all servers are adjacent at Layer 2, and all services are mapped to all ports. While this scenario maintains the flexibility of live migration, it is generally counter to both network design and security best practices. In the second scenario, live migration is simply not used, which undermines much of the potential value of a server virtualization strategy.

One subtle challenge of live migration is that you can never really be sure where a virtual machine is running. A virtual machine may manually or automatically be moved from one server to another for any number of reasons, so the network must be capable of provisioning all services everywhere and yet delivering services only exactly when and exactly where they are needed.

Blurred Organizational Roles

The practicalities of deploying server virtualization often lead to a blurring of organization roles. Because the network is now split between the hypervisor switch in the server and the rest of the physical network, server administrators may find themselves managing network resources or trying to interpret and implement security policy. At the very least, this approach to roles is an inefficient use of time, but a larger concern is that this approach may result in implementations that depart from best practices or are not complaint with policy requirements. The alternative—involving the network team for most virtual machine moves, additions, and changes—is not a scalable approach as virtual machines become the predominant application platform and as server virtualization strategies become more reliant on automated features.

Solution Benefits

The joint Cisco® and VMware solution combines Cisco Nexus™ 1000V Series Switches and VMware vSphere to specifically address the challenges of scaling a virtualization strategy. A Cisco Nexus 1000V Series Switch is a pure software switch that integrates directly into the VMware vSphere hypervisor. The VMware vSphere solution was designed with an understanding that the network plays a central role in any viable data center virtualization strategy. The joint solution represents a blend of Cisco's networking expertise with VMware's server virtualization expertise, and it was designed specifically to help customers scale their virtualization strategies.

Cisco Nexus 1000V Series Switches are virtual implementations of a Cisco NX-OS Software switch. The logical architecture of the switch is analogous to the architecture of a modular switch such as the Cisco Nexus 7000 Series Switches or the Cisco Catalyst® 6500 Series Switches. Cisco Nexus 1000V Series Switches have two software components. The first component is the virtual Ethernet module (VEM), which resides in the server and acts like a virtual line card. Virtual machines plug into the VEM the same way that physical servers plug into a physical line card. The second software component is the virtual supervisor module (VSM), which runs on a separate virtual or physical appliance and handles control plane functions.

Virtual Machine—Level Granularity

Because each virtual machine is plugged in to its own virtual port, Cisco Nexus 1000V Series Switches can differentiate traffic at the virtual machine level, and policy, as port profiles, can once again be defined and applied at the virtual machine level. This approach helps ensure that workloads with different policy (security, regulatory, and service level) requirements can coexist on a single physical server and still be treated appropriately. The network team can help ensure compliance with the relevant policies, while the server team can achieve a higher server consolidation ratio, since servers can be consolidated based on workload and resource requirements instead of policy compliance requirements.

Furthermore, this policy stays mapped to the virtual machine during VMware VMotion live migration, so the virtual machine–level policy is transparently and automatically enforced by the Cisco Nexus 1000V Series Switch as the virtual machine moves across physical servers in a VMware vSphere cluster with no window of vulnerability in which policy is not being enforced. As a result, the network team no longer has to be involved in virtual machine moves, additions, and changes, and the server team can make better use of advanced VMware vSphere features such as Distributed Resource Scheduling (DRS) and Fault Tolerance (FT).

Simplified Operations

The Cisco Nexus 1000V Series offers significant benefits to the network team. Essentially, it allows the virtual network to be managed exactly like the physical network environment. Since Cisco Nexus 1000V Series Switches are Cisco NX-OS switches, configuration will be a familiar endeavor to anyone familiar with Cisco IOS® Software or Cisco NX-OS, with a consistent interface, consistent command structure, and consistent features. Even familiar tools such as NetFlow and Encapsulated Remote Switched Port Analyzer (ERSPAN) are available. Further, these features can now be applied at the virtual machine level, so an access control list (ACL) can be applied to a specific virtual machine, or ERSPAN capture can be performed for traffic from a particular virtual machine.

Because of the tight integration between the Cisco and VMware environments, VMware VMotion migration is a smooth process. As the virtual machine moves, unneeded services are automatically decommissioned at the originating server, and the required policy is configured at the destination server. The entire move is stateful and nondisruptive. One advantage of this approach from a troubleshooting perspective is that features such as interface counters remain intact, and a NetFlow capture will continue uninterrupted during VMware VMotion migration.

Distinct Organizational Roles

The joint Cisco and VMware solution allows the server and network teams both to focus on their areas of expertise and responsibility. After the server and network teams define the available policies (port profiles), the server team is free to create, move, and destroy virtual machines without the need to either manage network resources or depend on the network team to complete network reconfiguration in a timely manner. Similarly, the network team is no longer drawn into day-to-day server operations while still maintaining assurance that the server team is adhering to both operational best practices and security and compliance policies.

Why Cisco?

Cisco and VMware have forged a unique partnership designed to deliver the types of solutions customers will need as they virtualize their data centers. The Cisco Nexus 1000V Series is the first result of the companies' shared vision and joint research and development efforts. Customers benefit from the collaboration of two industry leaders with a solution that offers outstanding value, features, and level of integration.

For More Information

More information can be found at the following locations:

- http://www.cisco.com/go/1000V
- http://www.cisco.com/go/vnlink
- http://www.cisco.com/go/datacenter
- http://www.vmware.com/products/cisco-nexus-1000V/index.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA

C02-552517-00 07/09