Cisco Application Centric Infrastructure Integration with VMware

Cisco Extends the Cisco ACI Policy Framework to VMware Virtual Environments

Cisco Application Centric Infrastructure (ACI) simplifies and accelerates the entire application deployment lifecycle for the next-generation data center and cloud deployments.

Cisco ACI takes a systems based approach and provides tight integration between ACI ready physical infrastructure and VMware virtual elements. Cisco ACI integration with VMware virtual environments offers customers the ability to leverage a common policy based operational model across their physical and virtual environments.

The Cisco ACI application policy profile can be used to define complex real-world application relationships. Applications are a collection of virtual and physical workloads interconnected by virtual and physical networks. In today's networks the physical interconnectivity is made of VLANs and Access Control Lists. In today's virtual networks, everything is expected to be a virtual workload interconnected via virtual networks. With Cisco Application Centric Infrastructure (ACI) all workloads are created equal and you can connect them to each other via policies.

ACI completely abstracts the workload interconnectivity from the classic network constructs of VLANs and IP addresses. Cisco ACI brings together innovations spanning ASIC, hardware and software to VMware environments, and delivers penalty free overlays, without compromising on scale, security and performance.

This integration enables customers to overcome IT silos and drastically reduce cost and management complexity, through a single pane of glass.

Challenges

IT consumption models are changing. More and more applications are hosted in the cloud. Cloud, mobility, and big data applications are causing a shift in the data center model. New applications are placing demands on the infrastructure in new ways.

Successful IT businesses require Application velocity, i.e. the ability to deploy new applications much faster than before. The application environment in the datacenter is becoming richer in application diversity. Distributed applications (for example, Big Data and Hadoop), database applications (such as those from Oracle and SAP) that run on bare metal, virtualized applications running in multi-hypervisor environments, and cloud-based applications that are available on demand all impose different demands on infrastructure.

Existing virtual and physical networking technology must be changed to address the following needs:

- Infrastructure must become application aware and more agile to support dynamic application instantiation and removal.
- The non-virtual nature of new emerging applications means that the infrastructure must support physical, virtual, and cloud integration.
- Troubleshooting application performance is becoming more complex because of poor visibility with overlays.
- Separate management points for physical and virtual environment increase operational complexity and costs.
- Today's technologies use gateways for communication between the physical and virtual workloads, thus becoming choke points, limiting scale and introducing complexity.

The net result of these challenges is that customers are dealing with increasing operation complexity and limiting business agility and responsiveness.

Solution: Cisco ACI Integration with VMware

The Cisco ACI is a highly flexible, open, programmable environment that can be transparently integrated into VMware virtual environments. Cisco ACI integration with VMware focuses on delivering simplicity without compromising on infrastructure scale, responsiveness, security or end-to-end visibility.

The Cisco Application Policy Infrastructure Controller (APIC) is the main architectural component of the Cisco ACI integration with VMware virtual environment. It is the unified point of automation and management for the Cisco ACI fabric, policy enforcement, and health monitoring, for both physical and virtual environment.
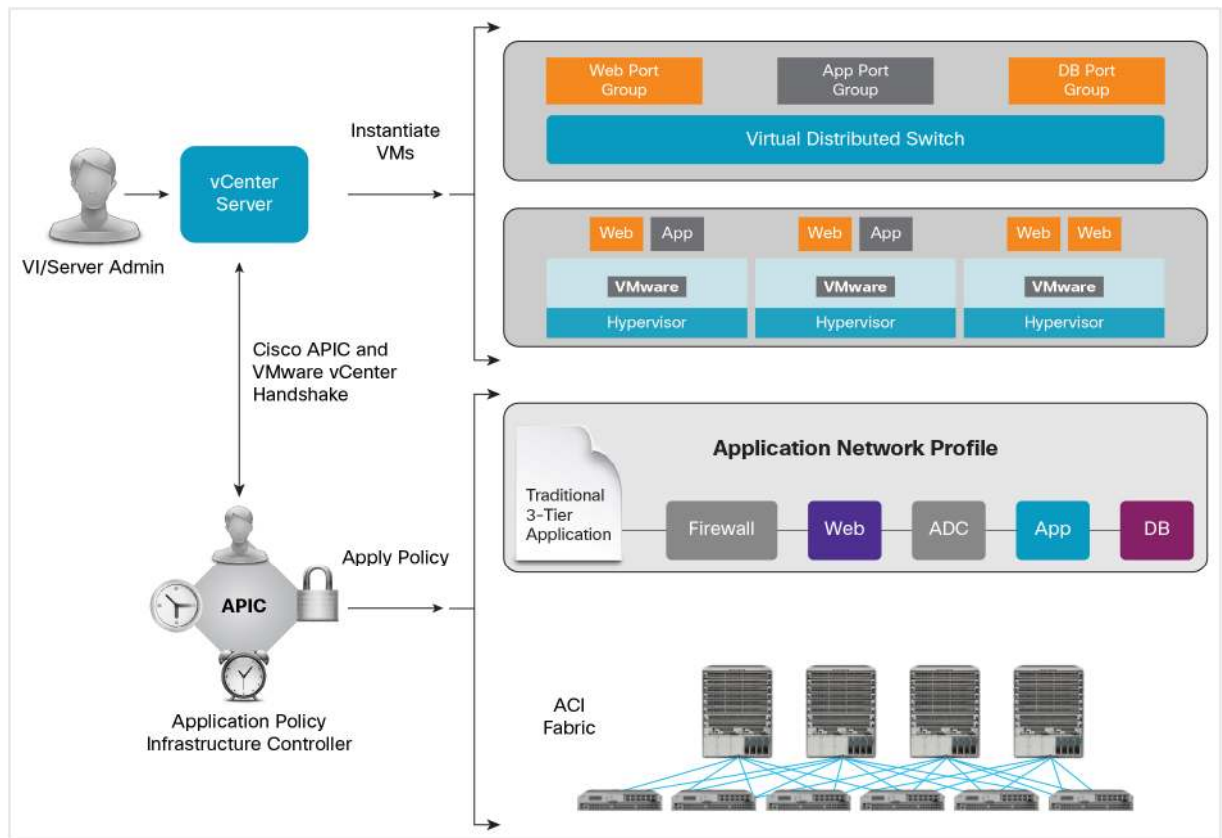
Connecting Virtual Machines to the Cisco ACI Fabric

The APIC integrates with VMware vCenter instance to seamlessly extend the ACI policy framework to vSphere workloads. The APIC uses Application Network Profiles to represent the ACI policy. The Application Network Profiles model the logical representation of all components of the application and its interdependencies on the ACI fabric. This policy framework also includes L4-L7 service insertion mechanism, providing full service life-cycle management based on workload instantiation and decommission.

Once these Application Network Profiles are defined in APIC, the integration between vCenter and APIC ensures that these network policies can be applied to vSphere workloads. The network policies and logical topologies (VLANs, subnets etc.,) which have traditionally dictated application design are now applied based on the Application Network Profile through APIC.

The Cisco APIC integrates with VMware vCenter to simplify workload connectivity. For example, you do not have to use VLANs to define basic networking connectivity. To connect VMware workloads to the Cisco ACI fabric, the virtualization administrator simply needs to associate the virtual machines with the port groups that appear under the virtual distributed switch (VDS).

Figure 1. Cisco ACI VMware Integration

Integrating VMware Overlays with Cisco ACI

VMware virtualized overlay models use Virtual Extensible LAN (VXLAN) for tunneling. This tunneling allows virtual machine connectivity independent of the underlying network. In these environments, one or more virtual networks are built using the chosen overlay technology, and traffic is encapsulated as it traverses the physical network.

The Cisco ACI integration with VMware provides overlay independence and can bridge frames to and from VXLAN, network virtualization generic routing encapsulation (NVGRE), VLAN, and IEEE 802.1x encapsulation. This approach provides flexibility for heterogeneous environments, which may have services residing on disparate overlays.

The Cisco APIC integration with vCenter enables dynamic workload mobility, management automation, and programmatic policy. As workloads move within the virtual environment, the policies attached to the workloads are enforced seamlessly and consistently within the infrastructure.

This integration delivers a scalable and secure multi-tenant infrastructure with complete visibility into application performance across physical and VMware virtual environments.

Solution Benefits

Cisco ACI integration with VMware provides the following benefits:

- Single point of policy management for physical and VMware virtual environments through APIC
- Faster application deployment, with transparent instantiation of applications in vSphere virtual environments
- Enable VMware vApps to connect both physical and virtual workloads
- Extend the flexibility of overlay networks to physical workloads on VLANs
- Enable seamless mobility of workloads across VXLAN overlay networks
- Completely decoupled controller from data path ensures that network traffic is not impacted even when controller is down
- Superior scale and performance by combining the flexibility of software with the performance of Cisco ACI hardware
- Full integrated visibility into the health of the application through holistic aggregation of information across physical and vSphere virtual environments
- Lower operational expenditure without incurring the additional per virtual machine cost of software based overlays

For More Information

- Cisco ACI strategy: http://www.cisco.com/go/aci
- VMware: http://www.vmware.com

Printed in USA

C22-729866-00   11/13