White Paper

Cisco Application Centric Infrastructure and Microsoft SCVMM and Azure Pack

Introduction

Cisco® Application Centric Infrastructure (ACI) is a next-generation data center fabric infrastructure designed to meet today's rapidly changing business requirements. Cisco and Microsoft together support enterprise applications such as Exchange, SharePoint, and SQL to take advantage of the ACI framework and optimize application deployment and performance.

Cisco ACI is designed using an application policy model, allowing the entire data center infrastructure to better align with application delivery requirements and business policies of an organization. With Cisco ACI, the data center responds dynamically to the changing needs of applications, rather than having applications conform to constraints imposed by the infrastructure. The policies automatically adapt the infrastructure (network, security, application, computing, and storage) to the needs of the business to shorten application deployment cycles.

With an open, systems-based approach, Cisco ACI is designed to support leading data center infrastructure and virtualization technologies. Integrating with Microsoft Windows-based application servers running the Microsoft Hyper-V hypervisor, Cisco ACI provides tight integration between physical and virtual application environments. The Cisco ACI policy framework provides connectivity for Microsoft Hyper-V workloads through virtual topologies over Cisco Nexus® 9000 Series Switches.

Cisco ACI and its extensibility to network, applications, security, computing, and storage resources are well aligned with the Microsoft and Cisco goal of providing a holistic, unified data center infrastructure. Cisco ACI in the Microsoft-enabled data center benefits our customers with shorter application deployment times, resulting in more rapidly implemented business processes, quicker time to market, and a sustainable competitive advantage.

Cisco extends the Cisco ACI policy framework to the Microsoft Windows Server Hyper-V with Microsoft System Center and Microsoft Azure Pack. Microsoft Azure Pack provides a single pane of glass for definition, creation, and management of Microsoft's Cloud Service. Microsoft Azure Pack integrates with System Center and Windows Server to help provide a self-service portal for managing services such as websites, virtual machines, and service bus.

The Cisco ACI and Microsoft solution provides the following benefits:

- Improvement in deployment time and performance of applications such as Exchange, SharePoint, and SQL, with pre-built integration between the latest versions of Windows Server, System Center, and the Cisco ACI solution
- Reduction in data center complexity by using the existing management framework of Microsoft System Center for virtual workloads and transparently extending Cisco ACI policy to physical and Windows Server Hyper-V-enabled virtual environments
- Hybrid cloud computing by supporting application velocity in a cloud with consistent policy across applications, network, security, and services
- Optimization of application performance by supporting penalty-free overlay networks

- Fully integrated visibility into the health of applications such as Exchange, SharePoint, and SQL by holistically aggregating information across physical and Windows Server Hyper-V-enabled virtual components
- Superior scalability and performance by combining the flexibility of software with the performance of Cisco ACI hardware

OpFlex

OpFlex is an extensible policy protocol designed to exchange abstract policy between a network controller and a set of smart devices capable of rendering policy. OpFlex relies on a separate information model understood by agents in both the controller and the devices. This information model, which exists outside the OpFlex protocol itself, must be based on abstract policy, giving each device the freedom and flexibility to render policy within the semantic constraints of the abstraction. For this reason, OpFlex can support any device, including hypervisor switches, physical switches, and layer 4 through 7 network services.

OpFlex can be used for a number of purposes in Cisco ACI. One common use case is with Microsoft SCVMM and Azure Pack. With OpFlex, the ACI fabric can be extended all the way to the virtualized layer, allowing full policy enforcement and visibility directly into the hypervisor. Each edge device running Hyper-V is treated as a virtual switch. This allows traffic between two virtual machines on the same host to be switched locally. From an OpFlex perspective, each virtual switch with the physical leaf to which it is attached to request and exchange policy information. Additionally, OpFlex and Cisco APIC interact with Microsoft SCVMM and Azure Pack to configure and manage the virtual switches as needed.

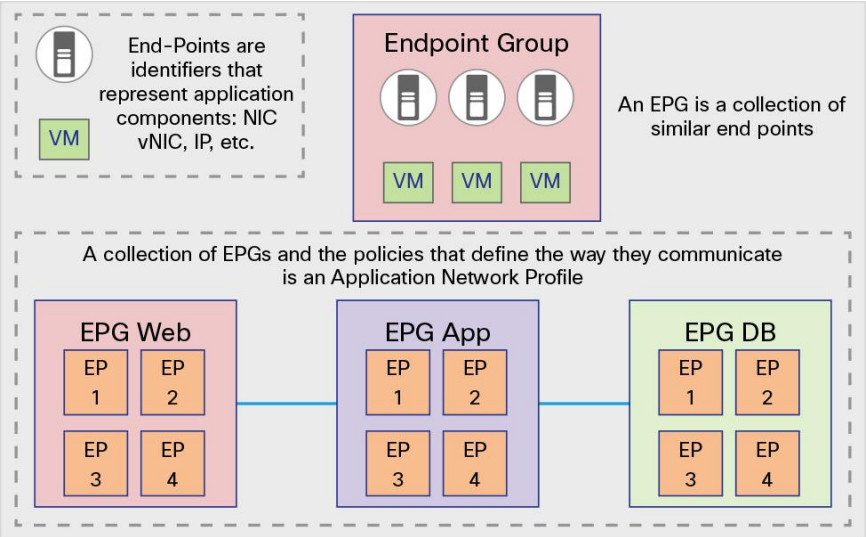
Fundamentals of ACI

ACI abstracts policy and connectivity from the underlying fundamental network constructs of VLANs, IP addresses, access lists, and quality of service (QoS) polices. Application network connectivity should be described in more abstract terms, such as endpoint groups, provider/consumers, and service-level agreements (SLAs) so it is relevant for the end user of the fabric.

ACI provides a highly secure multi-tenant solution, allowing the network infrastructure administration and data flows to be segregated. Tenants can be used for customers, business units, groups, etc. Tenants can be further divided into various layer 3 constructs, known as Virtual Routing and Forwarding (VRF). Contexts provide a way to further separate the organizational and forwarding requirements of a tenant. Within each VRF, a bridge-domain is created. A bridge domain is a layer 2 name space where the different subnets are defined. Assignment of all the subnets and default gateways takes place inside the bridge domain. By using separate forwarding instances, IP addressing can be duplicated in separate contexts for multi-tenancy.

Within the context, the model provides a series of objects that define the application. These objects are defined as endpoints and endpoint groups (EPG). Endpoints are devices (physical or virtual) that connect to the fabric and use it to interface with the network infrastructure (Figure 1). These endpoints can be compute, storage, network services, and security devices that attach to the fabric. At FCS, ACI will support endpoints to be classified as network interface cards (NICs) or virtual NICs (vNICs) and their associated VLAN or virtual extensible LAN (VXLAN). In the future, endpoints will be extended to IP addresses, MAC address, DNS name, VM attributes, 802.1x identity, and other common attributes.

Figure 1. Endpoints and EPGs



Endpoint group (EPG) is a term used to describe a collection of endpoints with the same type of attributes and identical network behavior (connectivity, security, QoS requirements, etc.).

Examples of common EPGs include:

- EPG defined by traditional network VLANs and all endpoints connected to a given VLAN placed in an EPG
- EPG defined by a VXLAN, which is the same as for VLANs except using a VXLAN
- Security zones
- Application tier (web, application, database)
- EPG mapped to a VMware ESXi port group

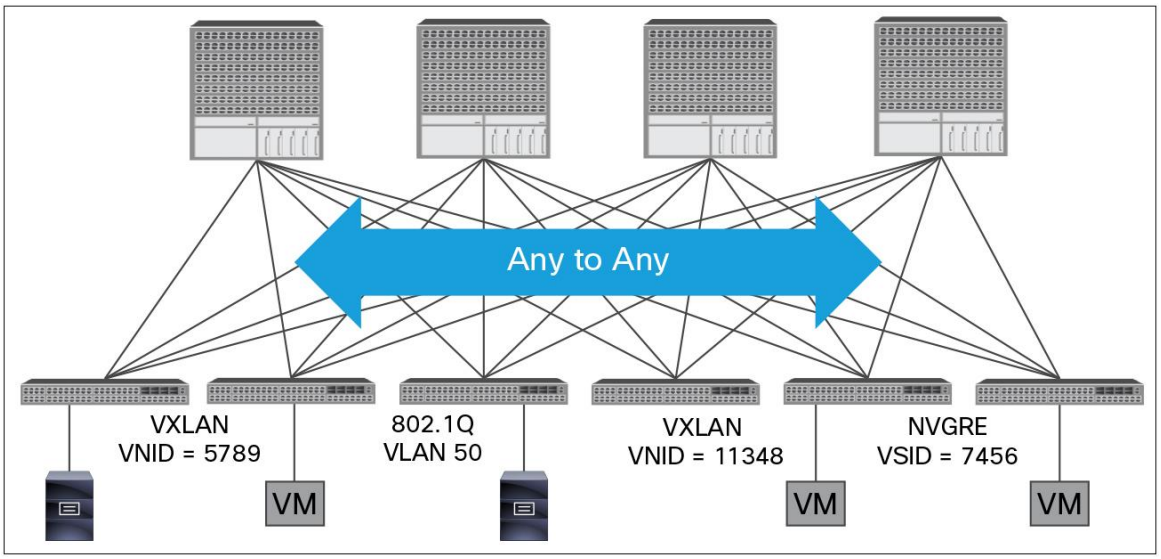
The policies that are used to describe the communication, services insertion, and QoS and SLAs are embedded between EPGs and are referred to as contracts. A contract is a set of network requirements that describes how EPGs can communicate with each other, as well as to the outside world. The ACI contract defines a filter, which includes a layer 4 ACL and an associated action that dictates whether the traffic is permitted, denied, logged, marked, redirected, or copied. ACI security follows an allowed list model, which denies all traffic by default. Administrators must explicitly allow communication between EPGs.

For each tenant, EPGs and policies are summarized into application network profiles (ANPs). These ANPs are the logical representation of the application infrastructure requirements. When the application is ready to be provisioned, a Cisco Application Policy Infrastructure Controller (APIC) can push the ANP and provision the entire stateless ACI fabric instantaneously.

Cisco ACI Integration with Multi-Hypervisors

One of the key benefits of ACI is the ability to be hypervisor-agnostic. The ACI is agnostic to the tenant traffic; it can be tagged with 802.1q (VLAN), VXLAN, or Network Virtualization Generic Routing Encapsulation (NVGRE) (Figure 2). Traffic forwarding is not limited to, nor constrained within, the encapsulation type or encapsulation overlay network.

Figure 2. Hypervisor-Agnostic Benefit of Cisco ACI



ACI takes full advantage of an extended VXLAN encapsulation frame format inside the fabric. All tenant traffic within the fabric is tagged at the first-hop leaf ingress port with an extended VXLAN header, which identifies the policy attributes of the application end point within the fabric. The VXLAN header carries the virtual network interface device (VNID) along with the EPG policy. As a result, the policy attributes are carried in every packet. As workloads move within the virtual environment, the policies attached to the workloads are enforced seamlessly and consistently within the infrastructure. When the packet leaves the fabric, it de-encapsulates the VXLAN header and encapsulates to any tag of the tenant's choice - VLAN, VXLAN, and NVGRE.

Virtual machine management (VMM) is a term used in ACI to define a hypervisor management system that has control over the virtual machines (VMs). An ACI Fabric can have multiple VMM domains across different hypervisor vendors. In collaboration with Microsoft, the VMM is defined as the Microsoft System Center Virtual Machine Manager (SCVMM).

Integrating ACI with Microsoft Hyper-V

The Cisco APIC integrates with a Microsoft SCVMM instance to transparently extend the Cisco ACI policy framework to Microsoft Hyper-V workloads. The Cisco APIC uses ANPs to represent the Cisco ACI policy. The ANPs model the logical representation of all components of the application and its interdependencies on the Cisco ACI fabric. This policy framework also includes a layer 4 through 7 service insertion mechanism, providing full-service lifecycle management based on workload instantiation and decommissioning.

After these ANPs are defined in the Cisco APIC, the integration between Microsoft SCVMM and the Cisco APIC helps ensure that these network policies can be applied to Microsoft Hyper-V workloads. The network policies and logical topologies (VLANs, subnets, etc.) that have traditionally-dictated application designs are now applied based on the ANP through the Microsoft APIC.

The Cisco ACI service plugin helps enable management of network infrastructure through the APIC REST API. The Azure Pack provides a portal for administrators (providers) and a consumer self-service (tenant) portal for users to have the appropriate experience. The service management portal for the administrator allows new service providers to be added or modified, and to retrieve usage and billing statistics per user. The APIC IP address, login credentials, and others are all managed through the administrator role. The tenant can log in and be presented with a tenant-specific view that shows the application network profiles that the tenant is entitled to see. The tenant is able to create their own customized ANP which can consists of networks, compute and L4-7 network services on their self-service portal. Azure Pack pushes the ANP configuration automatically to APIC.

The Cisco APIC integrates with Microsoft SCVMM to simplify workload connectivity. To connect Windows Server Hyper-V workloads to the Cisco ACI fabric, the virtualization administrator simply needs to associate the virtual machines with the virtual machine networks created by the Cisco APIC that appear under the logical switch in Hyper-V.

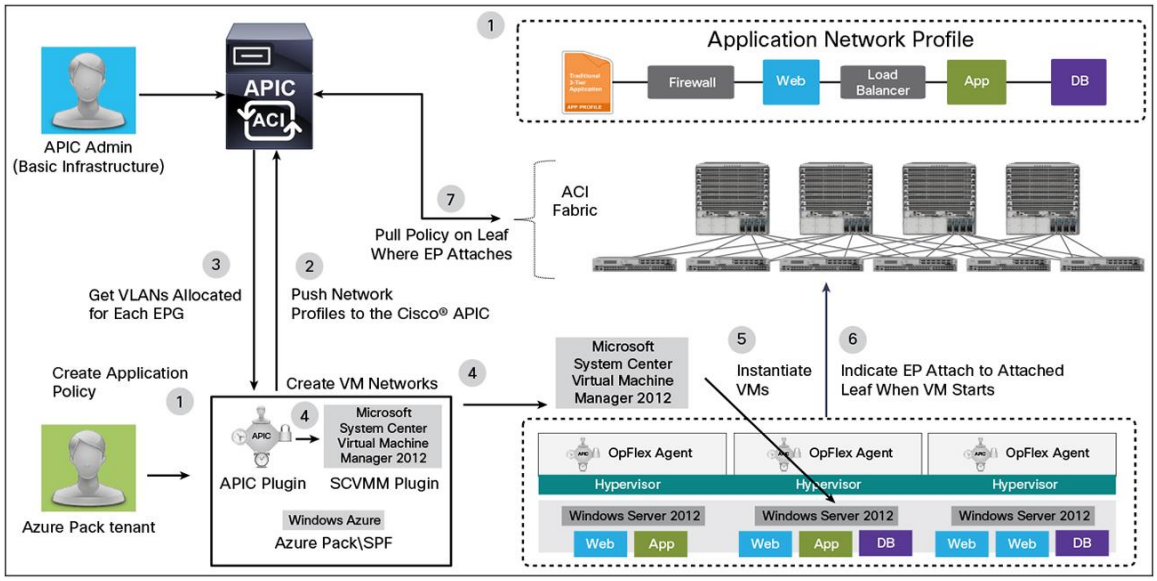
The Cisco ACI fabric is designed to provide overlay independence and can bridge frames to and from NVGRE, VLAN, VXLAN, and IEEE 802.1x encapsulations. This approach provides flexibility for heterogeneous environments in which services may reside on disparate overlays.

The Cisco APIC integration with Windows Server HyperV can enable dynamic workload mobility, management automation, and programmatic policy. As workloads move within the virtual environment, the policies attached to the workloads are enforced transparently and consistently within the infrastructure. This integration delivers a scalable and highly secure multitenant infrastructure with complete visibility into application performance across physical and Windows Server Hyper-V virtual environments.

Cisco ACI and Hyper-V

Figure 3 provides an illustration of the Cisco ACI and Microsoft Hyper-V workflow.

Figure 3. ACI and Hyper-V Workflow



For More Information

To learn more about Cisco ACI visit http://www.cisco.com/go/aci.

To learn more about Microsoft Virtual Networking visit http://www.microsoft.com/en-us/server-cloud/solutions/software-defined-networking.aspx#fbid=Z-wSsLVPicM.

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 C11-732080-00 10/14