Cisco Application Centric Infrastructure and Microsoft Integration

Introduction

Cisco® Application Centric Infrastructure (ACI) is designed using an application-policy model. This approach allows the entire data-center infrastructure to align more effectively with an organization’s application delivery requirements and business policies. With Cisco ACI, the data center can respond 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.

Cisco ACI - which can be extended to network, applications, security, computing, and storage resources - supports the Microsoft and Cisco goal of providing a holistic, unified data center infrastructure. When Cisco ACI is used in a Microsoft-enabled data center, it benefits our customers with shorter application deployment times, helping to speed implementation of business processes, accelerate time to market, and provide a sustainable competitive advantage.

Today, customers need an infrastructure that provides a generational advance in agility, elasticity, and scalability across shared resources, while delivering more automation and self service. So Cisco has taken the initiative to deeply integrate with Microsoft and offer customers a choice of two modes of operation (Figure 1):

- Cisco ACI with Microsoft System Center Virtual Machine Manager (SCVMM): This mode of operation is for customers who are interested in SCVMM as the virtual machine manager for the virtualized Microsoft Hyper-V workloads in their new or existing data centers. The Cisco Application Policy Infrastructure Controller (APIC) integrates with Microsoft SCVMM instances to transparently extend the Cisco ACI policy framework to Microsoft Hyper-V workloads.

- Cisco ACI and Microsoft Windows Azure Pack (WAP): This mode of operation is for customers who are interested in using Microsoft WAP to manage their new or existing data centers. One powerful advantage of Cisco ACI is the open framework through the Northbound Representational State Transfer (REST) API object model. This framework allows the Cisco APIC to integrate with any existing or new orchestration systems. Cisco has built a plugin that natively integrates with Microsoft WAP.
Overview

Figure 1. Two Modes of Operation for Cisco ACI

Microsoft System Center Virtual Machine Manager Integration

SCVMM is Microsoft's virtual machine support center for Windows-based systems. It upholds Microsoft's focus on efficiency with features to help virtualization administrators consolidate multiple physical servers within a central virtualized environment.

The Cisco APIC integration with Windows Server Hyper-V allows dynamic workload mobility, management automation, and programmatic policy. As workloads move within the virtual environment, policies attached to each workload 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 can support various encapsulations, which is one of its key benefits. Because it is agnostic to tenant traffic, traffic can be tagged as 802.1q (VLAN), virtual extensible LAN (VXLAN), or Network Virtualization using Generic Routing Encapsulation (NVGRE). Traffic forwarding is not limited to, nor constrained within, the encapsulation type or encapsulation overlay network. Cisco ACI provides a unified model where one policy can be applied to a “bare metal” host or a virtual machine (Figure 2). In the integration with SCVMM, The Cisco APIC dynamically assigns a VLAN to a virtual machine network. The VLAN encapsulation that is assigned is locally significant, so VLAN overlap is natively supported with the Cisco ACI model. This behavior simplifies customers' operations, because they don’t have to monitor, manage, and track which VLAN is assigned to which network.

**Note:** At the time of this writing, Cisco ACI supports VLAN encapsulation for Microsoft SCVMM.
Virtual machine management (VMM) is a term used in Cisco ACI to define a hypervisor management system that has control over virtual machines. A Cisco ACI fabric can have multiple VMM domains across different hypervisor vendors. In collaboration with Microsoft, the VMM is defined as the Microsoft SCVMM. Using the VM Networking tab shown in Figure 3, Microsoft SCVMM is added as a VMM domain.

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 application network profiles (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 Layer 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 VMM domain is associated to the endpoint group (EPG), which triggers the automatic creation of a virtual machine network in Microsoft SCVMM (Figure 4). The Cisco APIC integrates with Microsoft SCVMM to simplify workload connectivity. To connect Windows Server Hyper-V workloads to the Cisco ACI fabric, a virtualization administrator simply needs to associate the virtual machines with the virtual machine networks created by the Cisco APIC (Figure 5), which appear under the logical switch in Hyper-V.

Figure 4. Adding SCVMM VMM Manager

![Figure 4](image1.png)

Figure 5. Attaching a Virtual Machine Network to a Virtual Machine

![Figure 5](image2.png)
The features just described are native to the Cisco ACI solution and have been translated to Microsoft SCVMM constructs. Table 1 shows you the 1:1 mapping: For example, a Cisco ACI EPG is a virtual machine network in Microsoft SCVMM.

<table>
<thead>
<tr>
<th>Cisco ACI</th>
<th>Microsoft SCVMM</th>
</tr>
</thead>
<tbody>
<tr>
<td>EPGs</td>
<td>Virtual machine networks</td>
</tr>
</tbody>
</table>

**Windows Azure Pack Integration**

A Cisco ACI resource provider in Microsoft WAP drives the APIC for network management. Networks are created in SCVMM and are available in WAP for respective tenants.

The WAP for Windows Server provides a solution for enterprises looking to act as service providers, as well as for service providers that want to attract enterprise workloads. Running on top of Windows Server and System Center, the WAP for Windows Server delivers the power of Windows Azure into a data center, so customers can offer a rich, self-service, multitenant cloud with experiences and services that are consistent with Windows Azure. WAP is available to Microsoft customers at no additional cost. It comes as a collection of Windows Azure technologies that install in enterprise and service provider data centers, integrating with their existing Microsoft System Center and Windows Server environments.

Through the integration of Cisco ACI and Microsoft WAP, we can now offer a rich set of network services in a secure multitenant design. Together, ACI framework and WAP are designed to deliver a true multitenant solution. Tenants could be employees within an organization, business units, application owners, or applications. Or if you’re a service provider, they could be hosting customers (individuals or organizations that pay you to provide IT services). The WAP portal is divided into a provider (administrator) portal and a consumer self-service (tenant) portal.

**WAP Admin Portal**

WAP administrators (admins) manage and monitor the resources at data centers, allocate those resources to the various services, and manage the WAP tenant subscriptions and billing for services consumed by WAP tenants. The portal offers many services to help WAP admins with management. One key feature is the ability to host plans, which allows admins to establish various combinations of services, resource clouds, and quotas - and make them available for subscription to specific WAP tenant groups. Cisco ACI integration allows ACI networking to be added to the WAP plans, along with the existing compute resources. The WAP plans allow an admin to offer differentiated services to customers and, in return, have a different cost associated to the service. For example, the WAP admin could create a Gold, Bronze, and Silver plan and offer different compute and networking services to each of the plans.

**Note:** Please refer to the Microsoft website for more information on the WAP admin portal

**Cisco ACI Networking Plans**

Cisco ACI offers two kinds of networking plans in the WAP admin portal - the Shared Service Plan and the Virtual Private Cloud (VPC) plan. Both plans offer rich Cisco ACI networking services natively to WAP tenants, and the plans can be offered based on tenant requirements. With either plan, the WAP admin has the flexibility to create different offerings for their paying tenants.
Table 2. Summary of Features Supported by Cisco ACI Plans

<table>
<thead>
<tr>
<th>Features Offered</th>
<th>Shared Service Plan</th>
<th>Virtual Private Cloud Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Isolated networks</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Stateless firewall</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Provider Dynamic Host Configuration Protocol (DHCP)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Shared load balancer</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Public Internet access</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Shared service</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Bring Your Own Address space (private address) and DHCP</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>

* In a VPC plan, a load balancer and DHCP are not supported for private address space. Both features are still offered to a VPC tenant, but the load balancer and DHCP are owned by the shared infrastructure.

Use Cases for a Virtual Private Cloud and Shared Service Plan

Figure 6. Comparing a Shared Network Plan and Virtual Private Network Plan

Shared Service Plan

In a typical enterprise, users want application connectivity, without worrying about the IP address. They also want to use self-service methods to manage the application and have the flexibility to add security services, L4-7 network services, and similar offerings.

In a shared service plan (Figure 6), the following features are offered:

- Isolated networks
- Stateless firewall
- IP addresses managed by the infrastructure
- DHCP server managed by infrastructure
- Shared load balancer
- Tenant-to-tenant shared services
- Public Internet access
**Note:** At the time of this writing, Cisco ACI supports Citrix and F5 Load Balancer for L4-7 services integration with Microsoft WAP.

**Virtual Private Plan**

In a service-provider use-case, WAP tenants not only want to manage their applications, but also to bring their own address space. In addition, they want the flexibility provided by self-service capabilities when adding security services, L4-7 network services, and similar offerings.

In a virtual private cloud plan (Figure 6), the following features are offered:

- Isolated networks
- Stateless firewall
- IP addresses managed by the tenant
- DHCP server managed by the tenant
- Shared load balancer
- Tenant-to-tenant shared services
- Public Internet access

**Note:** At the time of this writing, Cisco ACI supports Citrix and F5 Load Balancer for L4-7 services integration with Microsoft WAP.

These features are native to the Cisco ACI solution and have been translated to Microsoft WAP. Table 3 shows the 1:1 mapping. For example, when a new subscriber is created in WAP admin portal, it gets configured as a new Cisco ACI tenant. Similarly when a WAP tenant creates a new network and firewall rule, a new EPG and contract are configured on the Cisco APIC.

<table>
<thead>
<tr>
<th>Cisco ACI</th>
<th>Microsoft WAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant</td>
<td>Subscriber ID</td>
</tr>
<tr>
<td>EPGs</td>
<td>Networks</td>
</tr>
<tr>
<td>Contract</td>
<td>Firewall</td>
</tr>
</tbody>
</table>

Here is a closer look at what these features entail:

- Networks: In Cisco ACI, the term “network” refers to EPGs, which are used to provide a new model for mapping applications to the network. Rather than using forwarding constructs, such as addressing or VLANs, to apply connectivity and policy, EPGs use a grouping of application endpoints. EPGs are mapped to isolated networks in the WAP portal. The isolated networks act as containers for collections of applications, or application components and tiers, that can be used to apply forwarding and policy logic. They allow the separation of network policy, security, and forwarding from addressing and, instead, apply it to logical application boundaries. When an isolated network is created in WAP, in the backend it is created as a virtual machine network in SCVMM. A WAP tenant can use the WAP Virtual Machines Tab to manage their compute resources and can attach the virtual machine to its appropriate network.
● Firewall: Cisco ACI is built on a highly secure model, in which traffic between EPGs (isolated networks) is denied, unless defined by policy contracts. An ACI contract is mapped to a firewall in the WAP portal. These stateless firewall rules describe a set of Layer 4 TCP or UDP port numbers that define the communication between the various networks.

● Shared load balancer: Cisco ACI treats services as an integral part of an application. Any services that are required are treated as a service graph that is instantiated on the Cisco APIC. Users define the service for the application, while service graphs identify the set of network or service functions that are needed by the application. Cisco ACI has an open ecosystem of L4-7 service vendors that integrate natively with ACI. This is done through device packages written and owned by the vendors. The APIC manages the network services and inserts the services in line with the ACI policy model. For WAP, ACI offers an F5 and Citrix load balancer, both virtual or physical form factor, which are physically connected to the ACI fabric and shared across the different WAP tenants. Once the load balancer has been integrated into ACI, the WAP admin can choose to add the load balancer as a premium service and upsell the plan. The WAP admin manages Virtual IP (VIP) range for the shared load balancer to simplify the WAP tenant's workflow.

● Tenant-to-tenant shared services: Cisco ACI offers shared services between tenants in the same infrastructure. This feature has been extended to the WAP portal to allow WAP tenants to provide services (such as MongoDB) and other WAP tenants to consume these services. The WAP admin can delegate a separate plan for a provider WAP tenant and a consumer WAP tenant. A provider WAP tenant is defined as a tenant who manages and owns the shared service, such as MongoDB. A consumer WAP tenant is a tenant who consumes the shared service. WAP admins have control over which WAP tenants are providers and consumers. They also manage which services can be shared and can revoke these services at any time.

● Public Internet access: The Cisco ACI fabric connects to the outside through Layer 2 or Layer 3 extensions. These constructs are also available for WAP tenants to access other services within the data center, across the data center, or even to the Internet.

● In a VPC plan, WAP tenants can define their own address spaces, bring a DHCP server, and even map their address space to a network. A VPC tenant can also be offered services, such as load balancer, from the shared service plan. In this scenario, a device would have multiple vNICs. One vNIC would connect to the private address space, and another would connect to the shared service infrastructure. The vNIC that connects to the shared service infrastructure would have an address assigned by the infrastructure and also consume a shared load balancer owned by the infrastructure.

The WAP admin has full visibility into all of its WAP tenants, the networks they have created (Figure 7), and services that have been provided and consumed (Figure 8). They can also revoke services from the WAP tenants (Figure 9).
Figure 7. Full Visibility into WAP Tenants and Networks

Figure 8. View of WAP Tenants Shared Services
WAP Tenant Portal

The Management Portal for Tenants look and feel (Figure 10) is similar to the Windows Azure Developer portal. WAP tenant users can list items, view their status, and provision new items. Once a WAP tenant provisions one or more virtual machines, the WAP tenant portal offers a rich set of information to help manage the environment. The WAP tenant can track usage data, as well as perform some configuration of the virtual machine based on the permissions in their subscribed plan. This dashboard also provides the ability to easily stop, start, and pause the virtual machine - and connect to it remotely. With ACI integration, a Cisco Networking Tab is added to the WAP tenant portal. This provides a WAP tenant with all the essentials needed to establish a fully functional application with rich networking services offered by the ACI fabric. WAP tenants can now create networks backed by Cisco ACI, security policy between networks, and they have the option to add a shared load balancer, as well as consume or provide services. The WAP tenant portal is a very easy-to-use, self-service portal, which allows WAP tenants to manage their own resources.

When WAP tenants log in, they are presented with a Cisco ACI tab. This tab offers all the Cisco ACI networking feature sets available for the WAP tenant’s use.

- Networks: A WAP tenant creates an ACI network (Figure 11) based on their application design. An ACI network acts as a container for collections of applications, or application components and tiers, that can be used to apply forwarding and policy logic. Each network will be associated to one or more virtual machines hosted on SCVMM. Once a network is created on the portal, the WAP tenant can attach the network to the appropriate virtual machine (Figure 12) under the Virtual Machines tab on the left panel.
Figure 10. WAP Tenant Portal

Figure 11. WAP Tenant Portal: Creating a New Network
Firewall: By default, Cisco ACI networks are based on a white-list model for security reasons. As a result, all traffic within a Network is denied unless allowed through a stateless firewall rule. Under the + -> ACI -> FW tab in the WAP tenant portal, tenants can create a stateless firewall rule between two networks and define the TCP and UDP port numbers (Figure 13).

Figure 12. Associating a Virtual Machine to a Network

Figure 13. WAP Tenant Portal: Creating Firewall Rules
● Load balancer: WAP tenants can add a load balancer to their applications (Figure 14). They simply go to the + -> ACI -> Load Balancer tab in the WAP tenant portal, then choose which network should consume the load balancer and define the port and protocol. WAP will automatically assign a VIP address from the range defined by the WAP admin. It will also detect all the backend devices that are part of that network to load balance.

**Figure 14.** WAP Tenant Portal - Adding Load Balancer

![Image](image_url)

● Shared service: WAP tenants who are consumers (Figure 15) can consume a network service by going to + -> ACI -> Shared Service. The WAP consumer tenant chooses the network where the service should be consumed from and picks a shared service from the list. WAP tenants who are providers (Figure 16) can provide a service by going to + -> ACI -> Shared Service -> Action -> Provide. The WAP provider tenant chooses the network where the service exists, the service name, description, and protocol number (the L4 port number to allow communication to this service). The name of the service and description will show up in the consumer tenant portal.
Figure 15. WAP Tenant Portal: Consuming a Shared Service

Figure 16. WAP Tenant Portal: Providing a Shared Service
Software and Hardware Support for Microsoft SCVMM and Windows Azure Pack Integration

Cisco requirements for both Microsoft SCVMM and Windows Azure Pack:

- Cisco ACI hardware
- Cisco ACI software

Cisco ACI plugins for Microsoft SCVMM, Hyper-V, and WAP plugins

Cisco ACI Virtualization Configuration Guide

Microsoft Requirements

Microsoft SCVMM-only integration requirements:

- Windows Server 2012
- Systems Center 2012 Release 2
- License

Microsoft WAP-only integration requirements:

- Windows Server 2012
- Systems Center 2012 Release 2 with SPF
- Windows Azure Pack