Cisco Application Centric Infrastructure for the Microsoft Cloud Platform

**BENEFITS**
- Automated policy deployment with centralized, simplified control
- Complete control of your entire infrastructure, including physical and virtual environments
- Deep visibility and health at a glance that allows you to go as deep as you want to troubleshoot and isolate problems

When applications need to change where and how they execute in response to demand and infrastructure requirements, new levels of flexibility and agility are required in the data center. In this environment, you need to dynamically transform both physical and virtual infrastructures to respond quickly to these changing needs.

Cisco® Application Centric Infrastructure (Cisco ACI™) for the Microsoft Cloud Platform is a secure, agile environment that simplifies security tasks and accelerates application deployments. Through centrally managed application policies, Cisco ACI automates all of your security device provisioning and configuration. This allows Microsoft Azure pack administrators to securely set up tenants and deliver a broad range of services as they deploy applications.

With Cisco ACI, administrators can manage their applications with exceptional control, reduced OpEx, and extreme flexibility. And Cisco ACI makes it easy to add and delete network and security services based on the application, and simplifies and automates service insertion for load balancing, firewalls, intrusion detection systems, and more.

By combining the extensive ability of Cisco ACI to monitor applications enabled by the Cisco Nexus® 9000 Series Switches, this approach to automation and policy deployment can increase the efficiency of IT operations by 20 to 58 percent*. Automated policy-based provisioning also provides enhanced application performance and shorter end-to-end application deployment cycles.
Trends and Challenges

The degree and frequency of change that modern applications require creates challenges for network administrators. To address these challenges, Cisco has developed a policy-driven infrastructure where policies are defined by the needs of the application. Cisco ACI is an innovative data center architecture that simplifies, optimizes, and accelerates the entire application lifecycle through a common policy management framework.

A policy-driven approach lets you create secure and easily deployed application profiles that align your data center infrastructure with the requirements of the application and the business policies of your organization. With Cisco ACI, you can respond dynamically to the changing needs of applications, rather than having applications conform to constraints imposed by the infrastructure.

By specifying the requirements and boundaries of execution for the application, these profiles form a common language that unifies and automates workflows. Administrators don’t need to understand the details of each application. Instead, they simply need to know which profile to apply.

Cisco has worked across multiple elements of Microsoft’s cloud platform, including Hyper-V, System Center Virtual Machine Manager (SCVMM), and Windows Azure Pack, to create an integrated solution that gives Microsoft’s platforms new capabilities. By combining the flexibility of Microsoft’s infrastructure solutions with the scale and performance delivered by Cisco ACI, you can more easily support large-scale, diverse, and multitenancy requirements.

Key Capabilities

Cisco ACI for the Microsoft Cloud Platform brings a new level of flexibility and agility to enterprise and service provider environments. The result is exceptional control of the Microsoft Cloud Platform and virtual and physical infrastructure, with reduced OpEx and greater flexibility.

Cisco ACI for the Microsoft Cloud Platform treats all workloads, physical or virtual, as endpoints. The connections are managed through a common policy framework across a broad ecosystem of management orchestration and network devices. This approach enables detailed and flexible segmentation of both physical and virtual endpoints based on group policies, improving the security of applications and automating compliance.

Cisco ACI automated provisioning means that IT teams can spend less time on manual processes, reducing SLA times in areas such as data center access (62%), access control lists (53%), and local server load balancing (55% projected time savings).^

An Open Ecosystem for Greater Innovation

The Cisco ACI open ecosystem delivers customer choice and interoperability, while decreasing costs and supporting increasing innovation. These benefits are achieved through OpFlex, a new open and extensible southbound protocol that supplies policy directly to data center networks. Unlike commonly used SDN protocols, it supplies application policy, not low-level configuration, to network devices. This allows devices to self-configure and freely expose new innovation.

By centralizing policy but distributing control, networks can become much more scalable, resilient, and interoperable. Cisco ACI increases customer choice by supporting open APIs, open source, open standards, and open Cisco ACI policies and protocols (Figure 1).
Figure 1. The Cisco ACI Open Ecosystem Delivers Customer Choice and Interoperability, while Decreasing Costs and Supporting Increasing Innovation.

Open and Standard APIs

Published Data Model

Open Source

Open Standards

Cisco contributes technology specifications to open-source and standards communities, working closely with organizations such as Microsoft and OpenStack for standards-driven open integration. Microsoft supports OpFlex for Hyper-V virtual networking integration with Cisco Application Policy Infrastructure Controller (APIC). Cisco and our partners have submitted OpFlex to the IETF for standardization.

A Powerful, Application-Centric Approach to Security

Complete security coverage is achieved by deploying policy-driven security instances through all tiers of the data center. The application-centric policies of Cisco ACI reduce the number and complexity of security rules that need to be managed. They easily correlate security policies with business policies, leading to simplified compliance and audit efforts.

The application-centric approach of Cisco ACI enhances security by isolating and segmenting across tenants through read-write restrictions (Figure 2). This approach prevents any tenant from seeing any other tenant's configuration unless assigned permissions by the administrator. Administrators can set up users with different access controls, where every tenant can have multiple applications. When setting up self-service portals, applications can be segmented and isolated using security services to lock down applications, making it easier to help ensure compliance.

Figure 2. Cisco ACI for the Microsoft Cloud Platform Operationalizes the Attack Continuum Workflow

<table>
<thead>
<tr>
<th>Network invasion</th>
<th>ACI security measures</th>
<th>Problem resolved</th>
</tr>
</thead>
<tbody>
<tr>
<td>In many security breaches, only a single End Point Group (EPG) is compromised</td>
<td>Restricting communication and data flows to and between endpoint groups</td>
<td>Cisco ACI for the Microsoft Cloud identifies, contains, and eliminates threat</td>
</tr>
<tr>
<td>Application-centric infrastructures provide a forward-looking solution</td>
<td>Accelerates attack detection across physical and virtual network boundaries</td>
<td>Ensures easier security compliance</td>
</tr>
</tbody>
</table>
Cisco ACI for the Microsoft Cloud Platform offers granular role-based access control and two-factor authentication. The APIC manages the access, authentication, and accounting functions of the fabric and supports local and external authentication and authorization. Cisco ACI gives you strong protection by restricting communication and data flows to and between endpoint groups, as well as accelerated threat detection by gathering time-stamped network traffic data and offering real-time network intelligence.

Take Full Advantage of the Microsoft Cloud Platform

There are three key Microsoft components in Cisco ACI for Microsoft Cloud Platform: Hyper-V integration, Systems Center integration, and Azure Pack integration. Hyper-V integration connects physical servers together by managing networking through a consistent policy approach. Integration with Systems Center allows you to plug in to the VMM, set up networking, and apply policy models. Azure Pack integration enables you to set up tenancy and self-service portals based on Microsoft Cloud Platform and Cisco ACI. Cisco ACI paired with Azure Pack enables Microsoft to offer rich, customer-facing self-services for enterprises looking to act as service providers. Azure integration provides capabilities for deploying agile infrastructure on an as-a-service basis, with both load balancer as a service and firewall as a service.

The combination of Microsoft software and Cisco hardware delivers tenant services faster, and with greater precision, through powerful application policies and management tools. Security device provisioning can be automated using centrally managed application policies, avoiding error-prone manual efforts while dramatically accelerating application deployments. Also, Cisco ACI enables unified security policy lifecycle management that speeds and simplifies implementation by enforcing policies anywhere in the data center.

Cisco ACI uses automated policy-based provisioning for application deployment across Microsoft Cloud Platform and across virtual and physical infrastructures. By applying security policies consistently to physical and virtual workloads, Cisco ACI offers a transparent and consistent method for integrating virtual and physical network devices into application networks, wherever they are located (Figure 3). Automating service-chaining capabilities simplifies and accelerates some of the most complex tasks required to set up new applications in multitenant data centers.

Figure 3. Cisco ACI Manages Application Policies Centrally to Reduce Errors and Accelerate Application Deployment
Cisco ACI for Microsoft Cloud Platform helps secure the inside of your data center using application-centered network policies that segment and isolate application tiers and close an important gap to on-demand application delivery. Cisco ACI and the APIC SDN controller allow for security policies down to the individual tenant, application, or workload, providing protection that meets the most stringent business and compliance requirements. Also, Cisco ACI helps security administrators better evaluate the availability aspect of data security when performing capacity planning and analyzing security breaches. This helps enable real-time IT risk assessment and reduces the risk of noncompliance.

Use Cases

Cisco ACI for the Microsoft Cloud offers:

| Flexibility              | • Simplifies operations while enabling scale  
|                         | • Brings exceptional agility to the network infrastructure  
|                         | • Optimizes infrastructure performance and enables faster application deployment |
| Consistency             | • Delivers a superior way to unify IT teams and drastically reduce costs and complexity  
|                         | • Offers exceptional control of Microsoft Cloud Platform and virtual and physical environments  
|                         | • Gives you visibility across physical and virtual infrastructure components |
| Open solutions          | • Helps ensure interoperability and choice with open standards that enable customization and vendor solutions  
|                         | • Lets you extend, enhance, and customize your solution with open interfaces that give you more insight and control  
|                         | • Lets you integrate your cloud management across layers of infrastructure with solutions enabled by an open ecosystem |
| Security                | • Provides superior protection by restricting communication and data flows to and between groups of any endpoints  
|                         | • Accelerates attack detection across physical and virtual network boundaries  
|                         | • Makes it easier to help ensure security compliance |

Secure the Inside of Your Data Center

Cisco ACI for the Microsoft Cloud Platform security framework secures the inside of your data center using application-centered network policies that segment and isolate application tiers. This closes an important gap to on-demand application delivery. Cisco ACI has three key components that help provide this security:

- **Multitenancy** is supported natively in fabric hardware with full isolation and segmentation across tenants by creating read-write restrictions that prevent any tenant from seeing another tenant’s configuration, statistics, faults, or event data unless authorized by the administrator.

- **Microsegmentation** divides the data center into smaller, more-protected zones. Instead of a single, hardened perimeter defense with free traffic flow inside the perimeter, a microsegmented data center has security services provisioned at the perimeter, between application tiers, and even between devices within tiers. The theory is that even if one device is compromised, the breach will be contained to a smaller fault domain.

Microsegmentation uses application-centered network policies and a whitelist security model. Whitelists are an innovative “zero trust” policy in which only things you specifically allow are let into the system, instead of the usual blacklists, which only keep specific things out. Use of whitelists strictly limits which applications and layers can communicate and access specific data. This model divides east-west traffic into multiple security zones with rules of communication across web-application and application-database tiers via policies programmed in the application network profile.
- **Granular authentication** is used by Cisco ACI for role-based access control and authentication as well as accounting. It uses two-factor authentication based on user login and password and an additional smartcard- or token-based authentication. Policies manage the access, authentication, and accounting functions of the Cisco ACI fabric. The APIC supports both local and external authentication and authorization, Lightweight Directory Access Protocol (LDAP), and role-based access control (RBAC) to control read and write access for all managed objects and to enforce Cisco ACI administrative and pertenant administrative separation. In short, the process consists of identifying the user, specifying the domain, and assigning roles.

**Cisco Services for Cisco ACI**

When considering Cisco ACI, it’s important to define your desired business outcomes and plan each stage of the journey. Then you can accelerate the benefits of Cisco ACI while mitigating the risks.

We can help you:

- Develop a Cisco ACI adoption strategy based on business and technology needs
- Provide migration strategy and operational readiness
- Deploy proof of concept to gain experience and reduce deployment risk
- Design application-centric data centers based on Cisco ACI fabric pods and policy templates

To optimize business outcomes, we offer a full range of services. The first step is Cisco Solution Support for Cisco ACI (SSPT for ACI), which offers a “one-stop shop” for managing all of your Cisco ACI needs. Cisco ACI implementation does not need to be complex. Cisco is connected to an entire ecosystem ready to help you unlock and support the full potential of your network.

Cisco Solution Support provides solution expertise and accountability for centralized management and resolution of complex issues that might arise within your covered Cisco multivendor solution.

**Cisco Solution Support:**

- Resolves complex issues 41% more quickly than product support alone
- Helps you increase uptime and employee productivity
- Gives you priority access to a Cisco primary point of contact
- Address both Cisco and key solution technology partner products

**Centralized, Coordinated Support for Cisco ACI Environments**

SSPT for ACI responds by offering interoperability troubleshooting, issue isolation, and end-to-end case management across the Cisco ACI ecosystem, speeding resolution with fast, expert technical support from Cisco and Cisco ACI third-party vendors.

SSPT for ACI includes product support with Cisco SMARTnet™ equivalent services exclusively for:

- Cisco ACI fabric devices (Cisco Nexus 9000 Series leaf and spine switches)
- Cisco ACI software licenses
- APIC
SSPT for ACI requires product support for all third-party products in your Cisco ACI ecosystem. Three SSPT for ACI offers are available to meet your specific situation to keep your Cisco ACI ecosystem secure and operating at peak performance (Table 1).

Table 1.  Cisco Solution Support for Cisco ACI Services

|---------------------------------------------|-------------------------------------------------------------------------------|------------------------------------------------------------------------|-----------------|
| Cisco Solution Support Plus for Cisco ACI (SSPT Plus for ACI) | For customers who:  
  • Are virtualizing their entire infrastructure  
  • Want to use the full functionality of APIC control across their entire Cisco ACI ecosystem  
  • Use APIC capabilities to manage devices and interface with all third-party Cisco ACI vendor products using northbound and southbound APIs and Cisco OpFlex™ | Yes | Yes |
| Cisco Solution Support for ACI (SSPT for ACI) | For customers who:  
  • Are virtualizing their network and managing Layer 4 through 7 services through the APIC | Yes | Yes |
| Cisco Solution Support Express for ACI (SSPT Express for ACI) | For customers who:  
  • Manage Cisco Nexus 9000 Series leaf and spine switches as Layer 2 through 3 fabric switches with limited functionality from the APIC  
  • Will continue using traditional networking devices, such as load balancers, firewalls, and security, which will not be recognized by the APIC for Cisco ACI | No | Yes |

Cisco Capital

Financial to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

Next Steps

For more information, contact your Cisco or Microsoft representative, or visit:

- Solution brief:  [Cisco Application Centric Infrastructure Integration with Microsoft](http://www.cisco.com/go/aci)
- White paper:  [Cisco Application Centric Infrastructure and Microsoft SCVMM and Azure Pack](http://www.cisco.com/go/acimicrosoft)
- Video demo:  [Solution Integration with Cisco ACI and Microsoft Windows Azure Pack](http://www.cisco.com/go/datacenter)
- Video:  [Microsoft SVP Brad Anderson talks about Cisco ACI and Microsoft Cloud Platform](https://communities.cisco.com)
- [http://www.cisco.com/go/acimicrosoft](http://www.cisco.com/go/acimicrosoft)
- [http://www.cisco.com/go/datacenter](http://www.cisco.com/go/datacenter)
- [https://communities.cisco.com](https://communities.cisco.com)

 Cisco Preparing Its Datacenters for the Next Generation of Virtualization and Hybrid Cloud with Its Application Centric Infrastructure, Matthew Marden, IDC, May 2014