Cisco Application Centric Infrastructure (Cisco ACI)

Q. What is Cisco ACI?

A. Cisco® Application Centric Infrastructure (Cisco ACI) is a comprehensive networking solution for data centers. It enables businesses to innovate faster and minimize downtime by radically simplifying, optimizing, and accelerating infrastructure deployment and expedites the application deployment lifecycle. Cisco ACI delivers a network policy–based framework that extends to the WAN and campus, translating intent into the network constructs necessary to dynamically provision the network, security, and infrastructure services. It enables building a data-center network fabric with up to hundreds of switches automatically, focusing on communications, through a single point of network configuration. With ACI, customers can manage complexity, maximize business benefits, and deploy workloads in any location, building a more agile, more secure network with automation, visibility, and operational consistency.

Q. At a high level, how does Cisco ACI work?

A. Cisco ACI captures higher-level business and user intent in the form of a network policy and converts this intent into the network constructs necessary to dynamically provision network, security, and infrastructure services. It uses a holistic systems-based approach, with tight integration between hardware and software and physical and virtual elements, an open ecosystem model, and innovative Cisco customer Application-Specific Integrated Circuits (ASICs) to enable unique business value for modern data centers. This unique approach uses a common policy-based operating model across the network, drastically reducing the cost and complexity of operating the network.

Q. What are main building blocks of Cisco ACI?

A. The Cisco ACI solution consists of two main components, the following building blocks:

- Cisco Application Policy Infrastructure Controller (APIC)
- Cisco Nexus® 9000 Series spine and leaf switches for Cisco ACI

Q. What does Cisco ACI do for my business?

A. Optimize your network

- A flexible and yet highly available network that allows agile application deployment within a site, across sites, and across global data centers while removing the need for a complex Data Center Interconnect (DCI) infrastructure
- Operational simplicity, with common policy, management, and operation models across application, network, and security resources
- Centralized network management and visibility with full automation and real-time network health monitoring
- Seamless integration of underlay and overlay
- Open northbound APIs to provide flexibility for DevOps teams and ecosystem partner integration

© 2023 Cisco and/or its affiliates. All rights reserved.

- A cloud-ready SDN solution
- Common platform for managing physical and virtual environments
- Automation of IT workflows and application deployment agility
- Open APIs and a programmable SDN fabric, with 65+ ecosystem partners

Accelerate multicloud

- Single policy and seamless connectivity across any data center and public cloud
- Any hypervisor, any workload, any location, any cloud
- Cloud automation enabled by integration with VMware vRealize Suite, Windows Azure Pack, OpenStack, Red Hat OpenShift, Kubernetes, and Cisco UCS® Director

Protect your business

- Create business continuity and provide disaster recovery
- Inherent security with a zero-trust allow list model and innovative features in policy enforcement, microsegmentation, and analytics
- Integrated security with Cisco security products and ecosystem partners
- Consistent security posture at scale across a multicloud environment

Q. What are some common Cisco ACI benefits or outcomes that actual customers describe?

A. Secure common network policy abstraction, governance, and compliance

- “Our most critical workloads have all been segmented,” Stengård notes, “and that makes our security team very happy.” Johan Stengård, solution architect for IT networks at Skanska Construction

Automated network connectivity, consistent network operations, network visibility, and network control for workload migration and next-generation applications.

- “Our Cisco ACI network is one of the largest data center fabrics in the world. It’s the ‘nerve center’ that provides connectivity between our subscribers and mobile services.” Ryota Mibu, Vice Division Manager, Cloud Platform, Rakuten Mobile
- “Cisco ACI is supporting roughly 1000 leaves on a number of large underlay fabrics, and all of the policies are consistent. That type of standardization and software-defined automation is important for operational efficiency, knowledge sharing, and business agility—on a global scale.” Vivien Strady, Global Head of Data Center and Network, Société Générale
- Agile resource elasticity with hybrid cloud networking
- “We’re sticking with a hybrid model,” says Johan Stengård, solution architect for IT networks at Skanska Construction. “Some apps will be in the cloud, some will be on-prem, and others will be split between the two.”

Business continuity and disaster recovery

- “Cisco ACI infrastructure is easy to implement because of the way Cisco pre-configures the solution—much of the guesswork is removed from the deployment. Pre-configurations can remove the guesswork from your infrastructure deployments. A key goal in implementing Cisco ACI was to ensure that we had established an active backup data center environment while reducing our associated costs. We’ve also enabled Layer 3 networking in our environment because we want to use both data centers independent from each other while also allowing them to converge. If the service running data center A fails, then the same service also runs in data center B. We run this alongside a few Docker containers and some high-availability proxies that share the load of both data centers.

© 2023 Cisco and/or its affiliates. All rights reserved.

This removes much of our anxiety around system failures, because if one data center fails, the services and other data centers can continue to run without requiring us to mediate." Franz Matthies, Senior IT-Security Specialist at HYPOPORT AG

Q. What are some common use cases?

A. Unified network management and operations: Simplify your network and save time by using unified management and embedded tools for operations, enabling you to scale more efficiently while automation ensures consistency.

- Business outcome:
  - One place to easily understand the data center's network, health, performance, redundancy, troubleshooting, and operational status
- Metrics:
  - Reduction in time for provisioning, configuration, troubleshooting, and upgrades
  - Reduction in configuration errors

Private cloud networking: Accelerate your business with a private-cloud-ready data center network that provides simple integrations with the most popular virtualization platforms to give you cloud-like agility internally.

- Business outcome:
  - Agility to change network elements that support applications, in lockstep with the application real-time lifecycle
- Metrics:
  - Reduction in time for business applications to be delivered and deployed
  - Reduction in time for network moves, additions, changes, and deletions

Automation and integrations: Optimize your network administration workflows by leveraging programmability with APIs and/or integration with ecosystem partners to save time, reduce errors, and accelerate your rate of change.

- Business outcome:
  - Doing more with less by leveraging the enhanced capabilities around API automation and service insertion that drive operational efficiencies
- Metrics:
  - Reduction in operational costs by automating routine tasks
  - More resource time for projects to advance the business

Geographic diversity and Business Continuity/ Disaster Recovery (BC/DR): Protect your business by enabling workload portability between multiple data centers, ensuring always-on applications, simplifying migrations, and contributing to BC/DR plans.

- Business outcome:
  - Application availability of 100 percent, regardless of data-center maintenance, migration, capacity, or other service interruption
- Metrics:
  - Application availability
  - Reduced risk of downtime

Public- and hybrid-cloud integration: Accelerate your adoption of a multicloud environment while providing consistent network and security policies within the data center and in the public cloud.

- Business outcome:
  - Enabling the business to gain agility from using the public cloud while reducing risk by uniformly applying network and security rules using the same toolset regardless of deployment

© 2023 Cisco and/or its affiliates. All rights reserved.

- Metrics:
  - Time savings
  - Acceleration of time to market
  - Reduction in errors
  - CapEx reduction

Security and compliance: Reduce attack surfaces and enhance your network security with a zero-trust model, line-rate encryption, continuous compliance with business rules, and ensuring network security policy.

- Business outcome:
  - Visibility of network and security changes that meet compliance requirements
- Metrics:
  - Reduction of risk
  - Increased availability
  - Reduction of security incidents and number of unplanned changes

Q. Are there Cisco ACI integrations with other Cisco products?

A. Yes, there are several. Here are some common examples:

- Cisco Nexus Dashboard: With Cisco Nexus Dashboard, you get a unified operations view across all your sites and services. Cisco Nexus Dashboard scales out based on the size and number of sites and the operational services used to manage them. It also provides the operations team with a simple and consistent way for service access control and lifecycle management of the unified operations' infrastructure and services. Cisco Nexus Dashboard delivers unprecedented simplicity by integrating multiple data-center operational tools that deliver best-in-class automation and insights from a single pane of glass to manage, monitor, and troubleshoot the network. Along with a uniform onboarding experience for data-center sites and operational services such as Cisco Nexus Dashboard Insights (formerly Nexus Insights), Cisco Nexus Dashboard Orchestrator (formerly Multi-Site Orchestrator), Cisco Nexus Dashboard Data Broker (formerly Nexus Data Broker), and third-party ecosystem applications, the operator now has a single landing page and a consistent user experience for the administrator and operator to manage the lifecycle of the infrastructure.
- Cisco ACI and AppDynamics®: This combined solution provides high-quality application performance monitoring, a rich diagnostic capability for application and network performance, and faster root-cause analysis of infrastructure anomalies. This will significantly reduce the time it takes to identify and troubleshoot end-to-end application performance issues.
- Cisco ACI and Cisco DNA-C/ISE: Automates the mapping and enforcement of segmentation policies based on the user's security profile as they access resources within the data center. This enables security administrators to manage end-to-end, user-to-application segmentation seamlessly. As a result, any unauthorized or suspicious access to resources and potential threats can quickly be controlled and remediated.
- Cisco ACI and Cisco SD-WAN integration for branch offices (network edge): Through this integration, customers can automate WAN path selection between the branch office and the on-premises data center based on application policies. For example, traffic from a stock trader in a branch office in Chicago can be automatically sent over the fastest possible WAN link to access the trading application hosted in a data center in New York, based on the application policies and SLAs configured.

© 2023 Cisco and/or its affiliates. All rights reserved.

Q. What is the value of the Cisco ACI partner ecosystem?

A. Cisco ACI has the industry's broadest ecosystem integration and is the leading industry-trusted data center networking solution. Piecemeal, nonintegrated solutions raise the complexity and cost of end-to-end digitization; Cisco ACI addresses this issue, reducing both complexity and cost.

Cisco ACI's broad ecosystem helps organizations develop a holistic infrastructure strategy that takes an architectural approach toward solving the unique challenges of multicloud data center deployments. Using this architecture, Cisco can guide organizations in a step-by-step journey that optimizes their technology investments and accelerates solution deployments across any location and any cloud.

Q. What are the components of Cisco ACI and how do I buy?

A. The minimum set of components required to enable an on-premises ACI fabric are:

- Cisco Application Policy Infrastructure Controller (APIC)
  - The infrastructure controller is the main architectural component of the Cisco ACI solution. It is the unified point of automation and management for the Cisco ACI fabric, policy enforcement, and health monitoring. The APIC appliance is a centralized, clustered controller that optimizes performance and unifies the operation of physical and virtual environments. The controller manages and operates a scalable multitenant Cisco ACI fabric.
- Cisco Nexus 9000 Series spine and leaf switches for Cisco ACI
  - The Cisco ACI fabric is a full-mesh topology of high-speed links (40/100/400 G) between redundant spine switches and leaf switches. The Cisco Nexus 9500 Series Switches operate as ACI spine switches and the Cisco Nexus 9300 Series Switches as ACI leaf or spine switches. Modular spines provide the scale and capability to incrementally add ACI leafs to the ACI fabric and grow the ACI fabric to the maximum scale.
  - Cisco ACI licenses are applied per Cisco Nexus 9000 device (leaf switch only) in a physical on-premises ACI deployment. The per-device ACI licenses are offered as tiered licenses for easy consumption. Add-on licenses are charged per device, based on value-added feature offerings. For details see the Cisco ACI ordering guide.

Recent questions from the 11/1/22 Cisco ACI webinar:

Q. What is the last version of Cisco ACI that can run on Gen 1 Nexus switches?

A. Cisco ACI Release 4.2 is the last train that supports Gen 1 Nexus switches.

We have a feature in Cisco ACI Release 5.2(7) that makes it easier to migrate away from Gen 1 to Nexus FX3 cloud-scale switches

Q. How do you collect telemetry data? And how far back can we go to review historical data?

A. With the Nexus Dashboard software platform, telemetry and assurance data is collected and stored for up to 30 days, and flow telemetry is stored for up to 7 days.

Q. Is Nexus Insights to be replaced with a new product?

A. Yes, Nexus Dashboard Insights (NDI) replaces Nexus Insights. NDI is the key Day2Ops service on the Nexus Dashboard platform. Nexus Dashboard helps configure, deploy, and manage your sites from a locally hosted environment. Cisco Nexus Cloud is a separate solution to manage your Nexus switches through SaaS from the cloud. Visibility and insights capabilities are built directly into Cisco Nexus Cloud and are not a separate product.

© 2023 Cisco and/or its affiliates. All rights reserved.

Q. What are the migration options from an APIC appliance to virtual APIC?

A. With the release of Cisco ACI Release 6.1.2(f), the virtual APIC is for greenfield deployments only. You can always use the import configuration feature, but mixed support for both virtual and physical appliances will be in a future release.

Q. Will a mixed environment including both physical and virtual APICs be supported?

A. Yes (see the answer to the previous question), but not at initial lease of the virtual APIC cluster in Cisco ACI Release 6.1.2(f).

Q. Why not design all application components within an application profile instead of using endpoint security groups (ESGs)?

A. The Endpoint Security Groups (ESG) process simplifies things for you. You can design all application components within an application profile, but you will have multiple, different Endpoint Groups (EPGs) and need to create contracts so they can talk to each other. In addition, if you want to create any microsegmented EPGs, the scope is at the bridge-domain level, whereas by using ESG, the scope widens to the VRF level.

Q. Can you deploy Nexus devices with an EVPN VXLAN fabric without using an APIC?

A. Yes, you can. Nexus devices run in two modes: in standalone mode, where you can bring up your own VXLAN fabric manually, or in ACI mode, which is a turnkey solution where a VXLAN fabric is automatically built during the fabric discovery process.

Q. What is the best approach to migrate multiple VDCs to an ACI fabric? Also, does Cisco ACI not support VDCs or allow any options other than VRF?

A. Cisco ACI acts like a tenant sitting above a VRF in the policy model, and maps quite nicely to a VDC. A tenant is an administrative boundary, such as a VDC in 7k, an account in AWS, or a subscription in Microsoft Azure.

Q. Can Cisco ACI be used an alternative to VMware NSX for microsegmentation, or is it not positioned that way?

A. Yes, it can, and is. In addition, Cisco ACI can span an entire VRF and include VMs, bare-metal solutions, and containers.

Q. Where can I get more information?

A. Cisco ACI: https://www.cisco.com/site/us/en/products/networking/cloud-networking/application-centric-infrastructure/index.html.

Cisco Application Policy Infrastructure Controller (APIC): https://www.cisco.com/c/en/us/products/cloud-systems-management/application-policy-infrastructure-controller-apic/index.html.

Cisco Cloud Network Controller: https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/cloud-aci.html.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)