Service Brief

Implementation

majentai

Cisco ACI Implementation

Cisco ACI Implementation is a structured engagement designed to design, implement, and operationalize a Cisco ACI fabric with clear segmentation and automation outcomes. Majentai guides teams from current-state readiness through blueprint and build, using a co-pilot approach for knowledge transfer and a path to long-term optimization with Infrastructure as Code.

Overview

This Cisco ACI Implementation is a guided deployment engagement designed to deliver a scalable ACI fabric with practical governance and operational readiness, with a clear path to expand into broader data center modernization and Zero Trust segmentation. The engagement aligns business and security goals to policy-driven automation, validating a repeatable deployment model that teams can run and scale.

- Fabric readiness and deployment strategy
- Physical and logical architecture blueprint
- Tenant, VRF, and BD logical modeling
- EPG and contract policy enforcement
- Day 2 operations and automation enablement

Business Outcomes

This engagement reduces deployment and security risk by translating requirements into enforceable ACI policy and a repeatable operating model. Majentai delivers a centralized fabric foundation that improves agility, supports consistent segmentation, and accelerates future expansion through automation and Day 2 workflows.

- Reduced configuration drift through IaC patterns
- Faster changes via centralized policy automation
- Lower lateral-risk with contract-based segmentation
- Clear path to scale and extend integrations

At a Glance

Objectives

- Define the right ACI deployment model and success criteria
- Deliver a scalable fabric design with segmentation conventions
- Build and validate policy-driven automation for operational adoption

Scope

- Standalone, Multi-Pod, or Multi-Site model selection
- ACI fabric build with APIC-led provisioning and migration support
- Integration planning for VMM domains and L4–L7 services

Deliverables

- ACI architecture blueprint document
- Access control matrix for policies
- Operational runbook plus automation scripts

Engagement Phases

Phase 1: Strategy and Discovery

Align business goals and technical requirements, assess current workloads, define success criteria and security objectives, and validate prerequisites including Nexus 9000 hardware and APIC readiness to confirm the optimal ACI deployment model.

Phase 2: Solution Design and Planning

Develop a physical and logical blueprint, including spine-leaf topology, tenant/VRF/BD conventions, and an integration plan for VMM domains and Layer 4–7 service insertion to enable consistent segmentation and centralized operations.

Phase 3: Build, Implement and Validate

Provision and bootstrap the fabric through APIC automation, execute a co-pilot migration approach from VLAN-centric to application-centric constructs, and configure EPGs, contracts, and filters to enforce an explicit-allow security model.

Phase 4: Operations & Recommendations

Operationalize Day 2 workflows with Infrastructure as Code using Terraform or Ansible, enable advanced segmentation and monitoring/visibility, and deliver knowledge transfer plus a prioritized roadmap for stabilization and expansion.

Majentai is a world-class Cybersecurity services provider, dedicated to implement, integrate and operate the most resilient Cybersecurity platforms using proven state-of-the-art technologies. With a team of seasoned experts and cutting-edge technology, we deliver comprehensive solutions tailored to our clients' unique needs, ensuring their digital assets remain secure in an increasingly complex cyber landscape.

For more information or to engage our services, please contact us at info@majentai.com or visit https://majentai.com