

AD CS Migration Checklist

Preparing Your Windows Server 2016
Environment for January 2027



Windows Server 2016 reaches End of Support on January 12, 2027. If Active Directory Certificate Services (AD CS) is part of your environment, migration requires more than moving a server.

AD CS can support authentication, encryption, secure communications, and trust across applications, devices, and infrastructure. Before migrating it to a supported environment, organizations need to understand the current certificate infrastructure, its dependencies, and how it fits into the future infrastructure landscape.

Use this checklist to prepare for a controlled AD CS migration while identifying opportunities to modernize the environment around it.

01 | Understand Your Current AD CS Environment



Identify all Windows Server 2016 servers running AD CS.



Document the Certificate Authority (CA) hierarchy, including Root CA, Enterprise Root CA, and Subordinate/Issuing CAs.



Record the current CA configuration and operating environment.



Identify the CA database and private key locations.



Confirm that appropriate backups of the CA database and private key are available.



Document the certificate templates currently in use.



Review current certificate issuance, enrolment and renewal processes.



Identify whether the CA is installed on a dedicated member server or co-hosted on a Domain Controller

Why it matters:

A clear view of the existing environment provides the foundation for deciding what needs to move, what needs to change and what needs to be preserved.

02 | Map Dependencies Around AD CS



Identify applications that rely on certificates issued by the CA.



Identify servers, endpoints, and network devices using certificates.



Identify certificate-based authentication and network access services.



Review automated certificate enrolment and renewal mechanisms.



Identify certificates supporting business-critical applications and services.



Document dependencies between AD CS and other identity or infrastructure services.



Identify any dependencies that span on-premises and cloud environments.



Identify any custom integrations or third-party solutions that interact with the CA

Why it matters:

The CA may run on a single server, but its dependencies can extend across the environment. Understanding those relationships helps reduce the risk of disruption during migration.

03 | Define the Target Environment



Determine whether AD CS will remain on-premises, move to a cloud environment or form part of a broader hybrid infrastructure strategy.



Confirm the target Windows Server version and infrastructure platform.



Consider how the target environment fits with your existing identity and security architecture.



Determine how AD CS will be managed, monitored, and secured after migration.



Identify related legacy infrastructure that could be modernized as part of the same program.



Consider whether any existing dependencies can be simplified or removed during the transition.

Why it matters:

The goal is not simply to move AD CS away from Windows Server 2016. The target environment should support the organization's broader infrastructure and operational requirements.

04 | Build the Migration Plan



Define the migration approach and sequence.



Establish responsibilities across infrastructure, application, and security teams.



Confirm backup and recovery procedures before migration.



Determine how the CA configuration, database, and private key will be transferred or restored.



Identify dependencies that require testing before cutover.



Define the cutover approach and required maintenance window.



Establish a rollback or recovery plan.

Why it matters:

A well-defined migration plan accounts for both the CA and the services that depend on it, reducing the risk of unexpected issues during the transition.

05 | Test and Validate Before Cutover



Test certificate issuance.



Test certificate renewal.



Validate certificate-based authentication.



Validate critical applications and services that depend on certificates.



Test device and endpoint certificate enrolment.



Verify required trust relationships and configurations.



Confirm that monitoring and alerting work in the new environment.



Document test results and resolve outstanding issues before retiring the legacy environment.

Why it matters:

A successful server migration does not necessarily mean a successful service migration. Validation should extend to the applications, devices and services that rely on AD CS.

06 | Prepare for Ongoing Operations



Update infrastructure and operational documentation.



Confirm ownership for ongoing AD CS management.



Review administrative access and security controls.



Confirm backup and recovery processes for the migrated CA.



Establish monitoring for certificate expiry and renewal.



Confirm processes for managing certificates and templates going forward.



Review the operating model across on-premises and cloud environments.



Retire the Windows Server 2016 environment only after migration and validation are complete.

Why it matters:

Migration establishes a new environment. Ongoing management, monitoring and recovery processes keep it reliable and supportable over time.

Beyond Migration

Use the Opportunity to Modernize

A Windows Server 2016 End-of-Support deadline creates a reason to examine infrastructure that may otherwise remain unchanged.

For AD CS, that means looking beyond the CA server itself. Understanding dependencies can reveal how certificate services connect applications, identity, endpoints, and infrastructure across on-premises and cloud environments.

That visibility can help organizations make more deliberate decisions about workload placement, architecture, and operations, rather than simply recreating the legacy environment on a newer platform.

Use migration as an opportunity to move from legacy dependencies to an infrastructure environment built for what comes next.

Need help planning your AD CS migration?

Anunta helps organizations assess, plan, migrate, validate, and operate infrastructure across hybrid and cloud environments.

Talk to an Anunta expert.