SimplicityIT
IT MADE SIMPLE

Assessment Methodology

Day-by-day deliverables for the 5-day AD to Entra ID readiness assessment

Engagement principles

Read-only. Provider reads Customer's environment, does not modify it. No changes to AD, no changes to Entra ID tenant, no agent installs that persist past Day 5.

Fixed fee. Scope and price are agreed at kickoff. Out-of-scope items are quoted in writing before work begins.

Defensible roadmap. The deliverable is a plan your security architect can defend in front of the audit team, not a sales pitch for a follow-on engagement.

Microsoft-native end to end. Active Directory, Entra ID, Entra Connect, Defender for Identity, Entra ID Protection. No third-party identity bridges in the recommendation.

The 5 days

DAY 1 Forest and domain discovery

Activities

- Kickoff call with Customer's identity lead. Confirm scope, access, and stakeholders.
- Run the Simplicity IT AD readiness toolkit (open-source, MIT-licensed, github.com/SIMPLICITY-IT-INC/simplicity-ad-readiness-toolkit) against the target environment. Read-only PowerShell that wraps Microsoft IdFix, AzureADAssessment, AADInternals, and BloodHound. No writes to Customer's directory.
- Inventory AD forests, domains, sites, subnets, domain controllers, FSMO role placement.
- Capture schema version, schema extensions, replication health (repadmin, dcdiag).
- Audit GPO posture: linked GPOs, WMI filters, security filtering, deprecated settings.
- Document the AD trust topology (parent-child, external, forest, shortcut trusts).
- AI-augmented post-processing of the toolkit CSV produces the baseline document, classified gap register, and Day 3 application-dependency report. Senior identity architect reviews every AI-augmented deliverable before customer handoff.

Deliverables

- Forest topology diagram.
- Domain controller inventory with OS version, patch level, and FSMO assignments.
- Replication health report.
- GPO inventory (active, unlinked, deprecated).

DAY 2 Identity inventory

Activities

- Inventory users, groups, service accounts, and computer objects with last-logon and password-age data.
- Identify privileged accounts (Domain Admins, Enterprise Admins, Schema Admins, custom delegated admin groups).
- Capture password policy (default domain, fine-grained, lockout thresholds).
- Enumerate Kerberos and NTLM authentication dependencies; flag NTLM-only applications.
- Identify stale accounts (no logon in 90+ days), orphaned objects, and security groups with no members.

Deliverables

- Identity census: counts by type, age, and authentication protocol.
- Privileged-account roster with tier classification.
- Stale-object cleanup list (pre-migration hygiene recommendations).
- NTLM dependency report.

DAY 3 Application dependency analysis

Activities

- Inventory applications bound to AD: LDAP queries (apps reading the directory), Kerberos SPNs (service-to-service auth), NTLM-only apps, RADIUS clients (VPN, Wi-Fi), and SAML / WS-Fed federations.
- Map each application to its Entra ID equivalent: SAML / OIDC app gallery, Entra App Proxy for legacy on-prem apps, or no-clean-path with remediation options.
- Identify ADFS dependencies and document the path to Entra ID federation or password hash sync.
- Flag applications that block cloud-only migration (hard NTLM dependencies, on-prem-only Kerberos, custom LDAP query patterns).

Deliverables

- Application dependency matrix: app, authentication protocol, AD binding type, Entra equivalent, migration risk.
- Federation inventory (ADFS, on-prem SAML IdPs).
- Cloud-only blocker list with recommended remediations.

DAY 4 Hybrid posture audit

Activities

- Assess Entra Connect Sync state: version, scoping filters, sync rules, password hash sync, seamless SSO, pass-through auth.
- Review AAD Connect Health alerts and recent sync errors.
- Audit hybrid Exchange (if applicable): mailbox split, AutoDiscover, hybrid configuration wizard state.
- Evaluate Conditional Access readiness: existing policies, MFA coverage, device compliance, risk-based access.
- Review Defender for Identity coverage and Entra ID Protection signal availability.

Deliverables

- Entra Connect health report.
- Hybrid Exchange state document (if applicable).
- Conditional Access gap analysis.
- Identity protection signal inventory.

DAY 5 Roadmap delivery

Activities

- Synthesize Days 1 to 4 into a phased migration roadmap with realistic effort and timeline estimates.
- Build the risk register: identified blockers, likelihood, impact, mitigation owner.
- Cost the follow-on migration engagement (Provider proposal, scoped from the actual findings).
- Present findings and the roadmap to Customer's identity-decision stakeholders.
- Issue an Azure Marketplace Private Offer for the follow-on engagement if Customer chooses to proceed.

Deliverables

- Findings report (PDF, ~30 pages).
- Executive presentation (PowerPoint).
- Phased migration roadmap with timeline and dependencies.
- Risk register.
- Follow-on engagement quote.
- Private Offer (optional).

What happens after Day 5

For 30 days following acceptance, Provider corrects any material non-conformity in the assessment deliverables at no additional charge. Customer may engage Provider for the follow-on migration via the Private Offer issued on Day 5, or use the roadmap with an internal team or another partner.

Optional follow-on engagements: full AD to Entra ID migration, Entra Connect optimization, Conditional Access design, Defender for Identity deployment, ADFS retirement. Quoted separately.

Roles and contacts

Role	Responsibilities
Provider identity lead	Daily execution, discovery, analysis, roadmap authoring.
Provider security architect	Risk-register review, Conditional Access design recommendations, escalation point.
Customer identity lead	Decision authority on assessment scope, attends Day 5 briefing, owns post-engagement decisions.
Customer Domain Admin	Provides read access to AD, answers protocol-level questions, validates dependency findings.