JUPITER PRIME
Consulting • Training • Advisory
جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

# Directory Services and Account Lifecycle Training Course for IT Team Leads

26 – 30 September 2027
Amman

**jupiterprime.uk**
info@jupiterprime.uk
Registered in the United Kingdom and Saudi Arabia

# Directory Services and Account Lifecycle Training Course for IT Team Leads

**Ref:** 2460_93011 **Date:** 26 – 30 September 2027 **Location:** Amman **Fees:** 3300 GBP

Directory Services and Account Lifecycle is a 1-week training course for IT team leads and system administrators who run user identities, groups and authentication across server estates, and who leave with an Account Lifecycle Control Plan. Every joiner, role change, contractor and dormant credential now widens or narrows the attack surface of an organisation, so directory hygiene has become a leadership concern. Jupiter Prime Training sets this subject in its operational and security context.

## Why Directory Services and Account Lifecycle Matters Now

Three forces shape directory work today. Hybrid estates mean one person may hold accounts in on-premises directories, cloud tenants and line-of-business applications at once. Attackers increasingly target credentials rather than software flaws, using stale or over-privileged accounts to move sideways. Auditors and business owners expect evidence that access matches role and is removed promptly on exit. Good control limits breach impact; weak control leaves orphaned accounts and service credentials nobody owns.

## Who Gains Most from Directory Services and Account Lifecycle

- Leads accountable for directory structure, naming and organisational unit design
- Administrators who create, change and disable user and service accounts
- Owners of authentication settings, password rules and multi-factor sign-in
- Specialists handling privileged access and administrative tiering
- Coordinators who answer access review and audit evidence requests

Infrastructure and service desk groups that attend together gain most, because they leave with one shared joiner, mover and leaver routine instead of separate habits.

## Directory Services and Account Lifecycle Capabilities

Participants move from fixing account tickets to shaping how identities are created, grouped, trusted and retired.

- Design an organisational unit and group structure that mirrors delegation needs — directory owners
- Specify joiner, mover and leaver triggers linked to human resources events — service desk and HR partners
- Apply role-based access groups and least privilege to file, application and server rights — data owners
- Build an administrative tiering model for privileged and service accounts — security leads
- Assess federation and single sign-on trust settings with external services — architecture boards
-

Communicate access review findings and remediation status — auditors and senior IT managers

## Key Directory Services and Account Lifecycle Terms

- Directory service — a central database that stores users, computers and groups and answers authentication and lookup requests across a network.
- Account lifecycle — the stages an identity passes through, from provisioning at joining, through role changes, to disabling and deletion at leaving.
- Organisational unit — a container inside a directory used to group objects so that policies and administrative rights can be delegated.
- Privileged account — an identity with rights to change systems, security settings or other accounts, needing tighter control and monitoring.
- Federation — a trust arrangement that lets one identity provider vouch for users so they can sign in to partner services.
- Orphaned account — an active account with no current owner, often left after a leaver or a finished project.

## Directory Services and Account Lifecycle Day by Day

### Day 1: The Directory Estate and Its Pressures

- Directory Inventory and Trust Map — Where Identities Actually Live
- Credential-Based Attack Paths — Why Stale Accounts Matter
- Organisational Unit Design Principles — Delegation and Policy Scope
- Naming and Attribute Standards — Search, Reporting and Automation Quality
- Hybrid Directory Synchronisation — Which Source Holds Authority

### Day 2: Groups, Policies and Authentication

- Role-Based Group Nesting — Rights That Follow Job Function
- Group Policy Objects and Precedence — Consistent Server and Desktop Settings
- Password and Lockout Rules — Usability Versus Guessing Resistance
- Multi-Factor Sign-In Options — Which Users and Systems First
- Kerberos and Token Basics — Diagnosing Authentication Failures Quickly

### Day 3: Joiner, Mover and Leaver Control

- HR Event Triggers — Timing of Account Creation and Removal
- Mover Rights Clean-Up — Preventing Privilege Accumulation Across Roles
- Contractor and Guest Expiry Dates — Temporary Access Boundaries
- Service Account Ownership Records — Accountability for Non-Human Identities
- Dormant Account Detection Scripts — Disable, Investigate or Delete

## Day 4: Privilege, Federation and Audit

- Administrative Tiering Model — Separating Domain, Server and Workstation Rights
- Just-in-Time Elevation and Vaulting — Reducing Standing Privilege
- Federation and Single Sign-On Trusts — Partner and Cloud Access Risk
- Directory Change Auditing — Which Events to Log and Alert
- Periodic Access Recertification — Owner Sign-Off on Group Membership

## Day 5: Practising the Account Lifecycle Control Plan

- Estate Health Scorecard — Applying Inventory and Naming Findings
- Group Rationalisation Exercise — Applying Role-Based Nesting to Live Cases
- Leaver Simulation Walkthrough — Testing Trigger Timing End to End
- Privileged Access Gap Review — Applying Tiering to Current Admins
- Account Lifecycle Control Plan — Owners, Triggers, Reviews and Metrics

## Applying Directory Services and Account Lifecycle After the Course

- Run a dormant and orphaned account sweep using the detection scripts and owner records, reporting decisions to service owners.
- Lead a first recertification cycle for the five most sensitive groups, with named owners signing off membership.

## Directory Services and Account Lifecycle Questions FAQ

### What is Directory Services and Account Lifecycle management and why does it matter now?

It is the discipline of structuring directories and controlling every account from joining to leaving. It matters now because attackers favour stolen or forgotten credentials, and hybrid estates spread identities across many systems that must stay consistent.

### Which roles gain most from Directory Services and Account Lifecycle training?

IT team leads and system administrators gain most. You benefit if you design directory structure, process access requests, own authentication settings or answer audit questions about who holds which rights.

### How does Directory Services and Account Lifecycle training differ from a general cybersecurity course?

It focuses on identities rather than networks or endpoints. It goes deep into groups, policies, privileged tiering, federation and the joiner, mover and leaver routine.

## What do you bring back from Directory Services and Account Lifecycle training?

You bring back a control plan for your own estate. It names account owners, provisioning and removal triggers, privileged tiers, review cycles and the measures you will report.

## Directory Services and Account Lifecycle: The Way Forward

The Account Lifecycle Control Plan first informs which accounts to disable and which groups to restructure. Infrastructure leads, service desk supervisors and security owners use it to agree triggers and review dates. After its first cycle, revisit the privileged tier boundaries and the guest expiry rules, since these drift fastest as projects, partners and cloud services change.