

**Advanced Server Administration,
Infrastructure, Security & Cloud Course**

UK Training

PARTNER



Advanced Server Administration, Infrastructure, Security & Cloud Course

Introduction:

Advanced server administration, infrastructure, security and cloud work is the discipline of running Windows Server and Linux systems at scale across on-premises data rooms and public cloud platforms, covering identity, virtualisation, storage, automation, hardening, recovery and monitoring. This 5-day course is for infrastructure managers and for system administrators, infrastructure engineers, security analysts and support specialists, and delegates finish with a Hybrid Server Operations and Hardening Plan. It is taught at an advanced practitioner level through hands-on labs on Windows Server and Linux hosts, drawing on the CIS Benchmarks, published configuration guides for securing operating systems.

Course Objectives:

- Distinguish Active Directory Domain Services from Microsoft Entra ID, and Entra Connect from Cloud Sync, when designing hybrid identity for server estates
- Select virtualisation, storage and clustering options such as Hyper-V, Storage Spaces Direct and failover clustering for resilient server workloads
- Apply PowerShell, Bash and Ansible to automate administration, configuration management and patching across Windows Server and Linux fleets
- Compare CIS Benchmarks with Microsoft security baselines, and interpret compliance scan results to prioritise hardening work
- Compare backup with replication, and set recovery point and recovery time objectives that match each server workload
- Justify a Hybrid Server Operations and Hardening Plan covering baselines, automation, monitoring, recovery and extension to the cloud

Target Audience:

- System administrators who run Windows Server and Linux hosts day to day and decide which tasks to script, standardise or automate
- Infrastructure engineers who design virtualisation, storage and identity platforms and choose between on-premises and cloud-hosted options
- Security analysts who assess server configurations and judge which hardening baseline settings to enforce or accept as exceptions
- Technical support specialists who handle escalated server incidents and decide when a fault calls for rollback, restore or failover
- Infrastructure and IT operations managers who own server estates and set priorities for patching, recovery targets and cloud extension

UK Training
PARTNER



Course Outline:

Day 1: Foundations: Hybrid Server Estates and the Current-State Assessment

- On-Premises vs Hybrid Server Estates: Where Workloads, Identity and Management Planes Sit
- Windows Server and Enterprise Linux Roles: Matching Operating Systems to Workload Types
- Server Inventory and Configuration Baseline: Recording Versions, Roles, Patches and Owners
- Administrative Access Model: Tiered Privileged Accounts and Jump Host Design Choices
- Operational Maturity Assessment: Scoring Patching, Backup, Monitoring and Hardening Practices

Day 2: Architectures: Identity, Virtualisation and Storage for Hybrid Servers

- Active Directory Domain Services vs Microsoft Entra ID: Directory Roles in Hybrid Identity
- Microsoft Entra Connect vs Cloud Sync: Choosing a Directory Synchronisation Approach
- Hyper-V and KVM Virtualisation: Host Sizing, Virtual Switches and Live Migration
- Storage Spaces Direct and Failover Clustering: Building Resilient Hyperconverged Server Storage
- Linux Identity Integration: Joining Linux Servers to Active Directory With SSSD

Day 3: Applying Automation, Patching and Configuration Management Across Server Fleets

- PowerShell vs Bash Scripting: Automating Routine Windows Server and Linux Administration Tasks
- PowerShell Desired State Configuration: Declaring and Enforcing Windows Server Settings
- Ansible Playbooks and Roles: Configuration Management for Mixed Linux and Windows Fleets
- Patch Management Cycles: Testing Rings, Maintenance Windows and Rollback Planning
- Azure Update Manager and Azure Arc: Centralising Updates for On-Premises Servers

Day 4: Analysing Server Hardening, Backup, Recovery and Monitoring Risks

- CIS Benchmarks vs Microsoft Security Baselines: Comparing Server Hardening Reference Profiles
- Benchmark Compliance Scanning With CIS-CAT, OpenSCAP and Lynis: Interpreting Findings
- Backup vs Replication: Azure Backup and Azure Site Recovery in Recovery Planning
- Recovery Point and Recovery Time Objectives: Setting Targets for Server Workloads
- Azure Monitor and Log Analytics: Alert Thresholds, Performance Baselines and Event Correlation

Day 5: Lab: Building the Hybrid Server Operations and Hardening Plan

- Lab Environment Review: Assessing a Mixed Windows Server and Linux Case Estate
- Hardening Lab: Applying CIS Benchmark Settings and Verifying Them by Automated Scan
- Lift-and-Shift vs Modernise: Planning Server Migration to Infrastructure as a Service
- Recovery Drill: Restoring a Server Workload and Measuring Results Against Objectives
- Hybrid Server Operations and Hardening Plan: Baselines, Automation, Recovery and Cloud Roadmap

UK Training
PARTNER



Skills You Will Gain:

- Hybrid Identity Design
- Hyperconverged Storage Configuration
- PowerShell and Bash Automation
- Ansible Configuration Management
- Server Hardening Assessment
- Patch Ring Planning
- Disaster Recovery Testing
- Hybrid Server Monitoring

Why Attend This Course:

- From configuring servers one by one through consoles to managing settings across Windows Server and Linux fleets with scripts and playbooks
- From applying security settings by habit to measuring every server against a named hardening benchmark and tracking the gaps
- From assuming backups will work to setting recovery objectives and proving them through scheduled restore and failover drills
- From isolated on-premises servers to presenting a Hybrid Server Operations and Hardening Plan for identity, monitoring and cloud extension

Conclusion:

Running servers well in a hybrid estate means treating Windows Server and Linux hosts as one managed, measured and recoverable fleet rather than as individual machines. The course makes three distinctions clear: on-premises directory services versus cloud identity, a hardening benchmark versus a vendor security baseline, and backup versus replication when recovery targets are set. It suits infrastructure managers and experienced practitioners, including system administrators, infrastructure engineers, security analysts and support specialists, who already administer servers daily and now need to automate, secure and extend them to the cloud at an advanced level.

Frequently Asked Questions FAQ:

What should delegates know before joining an advanced server administration, infrastructure, security and cloud course?

Delegates should already administer Windows Server or Linux systems, be comfortable at the command line and understand networking, DNS and directory basics. Earlier scripting experience helps, but the course reviews PowerShell and Bash patterns before using them in automation labs.

The graphic features the text 'UK Training' in a small, grey font above the word 'PARTNER' in a large, bold, black font. This text is positioned over a background of concentric grey circles and a chessboard pattern. In the foreground, three chess pieces—a king, a pawn, and a knight—are visible, rendered in a 3D style with gold and silver finishes.

UK Training
PARTNER

How does an advanced server administration, infrastructure, security and cloud course differ from a server support or cloud migration course?

It sits above day-to-day support and fundamentals courses and is broader than a cloud-only migration course. Delegates work on hybrid identity, virtualisation, automation, hardening benchmarks, recovery testing and monitoring across Windows Server and Linux, treating the cloud as an extension of existing server estates.

Why do CIS Benchmarks matter in advanced server administration, infrastructure, security and cloud work?

They give administrators a published, testable list of configuration settings for each operating system, so hardening can be measured rather than assumed. Scanning tools compare servers against a benchmark profile, show the gaps and let teams record justified exceptions instead of relying on personal habit.

What do delegates take back to work from an advanced server administration, infrastructure, security and cloud course?

Delegates take back a Hybrid Server Operations and Hardening Plan: a server inventory and maturity score, automation and patching approach, hardening baseline with exceptions, recovery objectives with a drill plan, monitoring thresholds and a phased roadmap for extending servers to cloud infrastructure.

UK Training

PARTNER

A graphic illustration of a chessboard with several chess pieces. A large gold king piece is in the foreground, with a silver pawn and a silver knight behind it. The board is checkered, and there are concentric circles in the background.