BLACKBIRD FOR TRAINING

Advanced Server Administration, Infrastructure, Security & Cloud Course



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 1-week 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



Course Outline:

Day 1: Server Hardware and Server Operating Systems

- Server Types and Form Factors: Tower, Rack and Blade Servers; Physical vs Virtual Hosts
- Server Hardware Components: CPUs, Memory, Power Supplies, Network Adapters and Out-of-Band Management
- RAID Levels and Storage Devices: RAID 0, 1, 5, 6 and 10; HDD vs SSD vs NVMe
- Installing Windows Server and Linux: Editions, Partitioning, Drivers and Post-Installation Configuration
- Managing Server Operating Systems: Users, Services, Updates and PowerShell and Bash Administration

Day 2: Server Roles and Server Networking

- DNS and DHCP Server Roles: Zones, Records, Scopes, Reservations and Failover
- Active Directory Domain Services: Domains, Organisational Units, Group Policy and Hybrid Identity with Microsoft Entra ID
- Web and Email Servers: IIS, Apache and Nginx, TLS Certificates and Mail Server Roles
- IP Addressing and Subnetting for Servers: IPv4 and IPv6, Static Addressing and VLAN Placement
- Network Protocols for Server Administrators: TCP/IP, LDAP, SMB, NFS, SMTP and NIC Teaming

Day 3: Storage Management and Virtualization

- RAID Setup and Management: Hardware vs Software RAID, Rebuilds and Hot Spares
- SAN vs NAS vs DAS: iSCSI, Fibre Channel, SMB and NFS Shares and Storage Spaces Direct
- Backup Strategies: Full, Incremental and Differential Backups, the 3-2-1 Rule and Restore Testing
- Hypervisors: VMware vSphere ESXi vs Microsoft Hyper-V, Host Sizing and Virtual Switches
- Managing Virtual Machines: Templates, Snapshots, Live Migration and Resource Allocation

Day 4: Server Security, Monitoring and Maintenance

- User Permissions and Access Control: Least Privilege, NTFS and Linux Permissions and Privileged Accounts
- Firewalls and Encryption: Windows Defender Firewall, firewalld, BitLocker, LUKS and TLS
- Patch Management and Hardening: Update Rings, Maintenance Windows and CIS Benchmarks
- Server Performance Monitoring: CPU, Memory, Disk and Network Counters, Baselines and Alerts
- Regular Maintenance: Log Review, Capacity Planning, Firmware Updates and Maintenance Schedules



Day 5: Troubleshooting and Cloud Integration

- Server Troubleshooting Methodology: Identifying, Isolating, Resolving and Documenting Faults
- Hardware and Software Troubleshooting: Disk and RAID Failures, Boot Issues, Service Crashes and Event Logs
- Network Troubleshooting for Servers: IP Conflicts, DNS and DHCP Faults and Connectivity Issues
- Cloud-Based Servers and Hybrid Environments: IaaS Virtual Machines, Azure Arc, Cloud Backup and Disaster Recovery
- Capstone Lab: Building the Hybrid Server Operations and Hardening Plan

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.

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.

