

Secure Hybrid Infrastructure with Windows Server 2025

Hyper-V, Azure Arc, clustering and Azure Local operations

FA-0689 · 4 days

DevOps, Cloud & Infrastructure · Cybersecurity

Introduction

This four-day course develops advanced operational skills for experienced Windows Server administrators. It combines hybrid management, security hardening, troubleshooting, Hyper-V and failover-cluster practice with Azure Local and recovery planning.

Selected scenarios use Windows Server 2025 and suitable lab infrastructure. Azure Local deployment and cloud integrations are discussed or demonstrated according to the available validated hardware, access and licensing; the course does not promise a production deployment or a fully secured enterprise estate.

Learning outcomes

- Administer selected Windows Server 2025 workloads using PowerShell and Windows Admin Center.
- Explain and practise suitable Azure Arc onboarding, inventory and policy-management tasks.
- Apply selected hardening, delegated-administration and auditing controls in the lab.
- Troubleshoot representative AD, DNS, Kerberos, Group Policy and performance failures.
- Configure selected Hyper-V storage/network settings and evaluate cluster validation, quorum and failover.
- Assess Azure Local architecture, prerequisites and operational requirements.
- Plan backup and replication, define RPO/RTO targets and document recovery testing.

Prerequisites

- Experience administering Windows Server, Active Directory, DNS, DHCP, Group Policy and networking.
- Advanced practical PowerShell skills, basic virtualisation knowledge and awareness of backup, security and availability.
- Prior Hyper-V, clustering, Azure, Arc or Windows Admin Center exposure is helpful.

Training outline

1. Day 1 — Advanced administration and hybrid management

Windows Server 2025 platform overview

- Key administrative improvements
- Hybrid management direction
- Server Core versus Desktop Experience
- Upgrade, migration, and lifecycle considerations
- Server role planning and operational standards

Azure Arc-enabled server management

- Azure Arc architecture and use cases
- Server onboarding requirements
- Connected Machine agent overview
- Resource groups, subscriptions, tags, and governance structure
- Azure Policy and compliance visibility
- Hybrid inventory and configuration management
- Azure Arc security and access considerations

Windows Admin Center for enterprise administration

- Gateway deployment and access model
- Managing servers, roles, services, certificates, firewall, updates, and storage
- Managing Hyper-V and virtual switches
- Managing Failover Clusters
- RBAC and delegated administration

- Windows Admin Center in the Azure portal for Arc-enabled servers
- Extension management and Azure integration

Operational server management

- Patch and update planning
- Hotpatch eligibility, Azure Arc onboarding and periodic baseline updates that can still require restarts
- Server health checks
- Event log review
- Performance monitoring
- Capacity monitoring
- Change control and operational documentation

2. Day 2 – Hardening, privileged access and troubleshooting

Security hardening strategy

- Microsoft security baseline approach
- Defense-in-depth model
- Role and feature minimization
- Local administrator control
- Service hardening
- Firewall hardening
- RDP and remote administration security
- SMB security
- PowerShell security

Privileged access protection

- Enterprise Access Model for hybrid privileged access, with the AD tier model as on-premises context
- Control, management and workload access separation; relate this to legacy Tier 0, 1 and 2 boundaries
- Privileged Access Workstations
- Credential exposure reduction
- Just Enough Administration
- Administrative delegation
- Privileged group monitoring

Advanced auditing and monitoring

- Advanced Audit Policy Configuration
- Authentication and logon auditing
- Privilege use auditing
- Group membership change auditing
- PowerShell logging
- Event forwarding
- SIEM integration considerations
- Security incident evidence collection

Structured troubleshooting methodology

- Problem scoping
- Change correlation
- Evidence collection
- Root cause analysis
- Corrective action planning
- Post-incident review

Core infrastructure troubleshooting

- Active Directory replication and domain controller health
- DNS resolution and SRV record issues
- Kerberos authentication and SPN issues
- Group Policy processing issues
- Time synchronization issues
- Server performance bottlenecks
- Useful tools: Event Viewer, Performance Monitor, Dcdiag, Repadmin, Nslookup, Klist, Gpresult, Test-NetConnection, PowerShell

PowerShell automation

- Remote administration
- Server inventory reporting
- Service and event log automation
- AD health checks

- Security reporting
- Patch and compliance reporting
- Script logging and error handling
- Operational runbook development

3. Day 3 — Hyper-V, storage and failover clustering

Hyper-V advanced administration

- Host planning and configuration
- VM generation selection
- Processor and memory configuration
- Dynamic Memory
- Production checkpoints and their limitations: checkpoints are not a backup strategy
- Virtual TPM and Secure Boot
- VM configuration versions
- Host and guest integration services

Hyper-V performance tuning

- CPU allocation
- Memory pressure analysis
- NUMA considerations
- Storage I/O tuning
- Network throughput tuning
- Performance counters
- Host versus guest bottleneck isolation

Hyper-V storage design

- VHDX planning
- Fixed versus dynamic disks
- Storage QoS
- CSV storage usage
- Storage path design
- Backup-aware storage planning

Hyper-V networking

- Virtual switch types
- Switch Embedded Teaming
- VLANs
- Management network separation
- Live Migration network design
- Storage network design
- Cluster network design

Failover Clustering essentials

- Cluster architecture
- Node, network, storage, and domain requirements
- Cluster validation
- Cluster roles
- Cluster Shared Volumes
- Cluster-aware updating
- Highly available virtual machines

Quorum and resiliency design

- Quorum models
- Dynamic quorum
- Dynamic witness
- Cloud witness
- Split-brain prevention
- Witness placement
- Site and network failure considerations

Cluster troubleshooting

- Cluster event logs
- Cluster validation reports
- Cluster communication failures
- CSV issues
- Live Migration failures

- Quorum failures
- Role failover analysis

4. Day 4 – Azure Local and disaster-recovery planning

Azure Local architecture

- Azure Local purpose and positioning
- Azure Arc-enabled infrastructure model
- Compute, storage, and network architecture
- Relationship to Hyper-V, clustering, and Storage Spaces Direct
- Azure portal integration
- Cloud-based deployment, updates, and monitoring

Azure Local deployment planning

- Validated hardware and supported deployment topology planning
- Network requirements
- Storage requirements
- Identity and DNS requirements
- Azure subscription and Arc requirements
- Prerequisite validation
- Post-deployment checks

Azure Local operations

- VM management
- Storage monitoring
- Cluster health monitoring
- Update management
- Capacity management
- Node maintenance
- Security and access control
- Operational alerts and supportability

Storage Spaces Direct overview

- Storage pool design
- Cache and capacity devices
- Resiliency types
- Cluster Shared Volumes
- ReFS considerations
- Drive replacement
- Repair and rebalance operations
- Storage performance monitoring

Backup and recovery strategy

- Business impact analysis
- RPO and RTO planning
- 3-2-1 as a planning heuristic, with isolation, retention and verified restores
- System state and bare-metal recovery
- VM backup considerations
- Application-consistent backup
- Backup retention and security
- Restore validation

Replication and disaster recovery

- Replication versus backup
- Hyper-V Replica concepts
- Planned failover
- Unplanned failover
- Test failover
- Azure Backup and Azure Site Recovery concepts
- DR runbook planning
- DR testing and documentation
- Failback planning

Final enterprise scenarios

- Securing a hybrid Windows Server estate

- Troubleshooting AD, DNS, Kerberos, and GPO failures
- Designing a highly available Hyper-V cluster
- Planning Azure Local for enterprise workloads
- Building a practical backup and DR strategy
- Reviewing operational maturity and next steps