TestOut

TestOut Hybrid Server Pro: Advanced – English 5.0

Objective Mappings:

TestOut Hybrid Server Pro: Advanced
Microsoft AZ-801

Revised: 2023-08-03

Powered by LABSIM

Contents

This document contains four objective mappings. Click on a mapping to view its contents.

Objective Mapping: LabSim Section to TestOut Hybrid Server Pro: Advanced Objective

The TestOut Hybrid Server Pro: Advanced course and certification exam cover the following TestOut Hybrid Server Pro: Advanced objectives:

#	Domain	Module.Section
1.0	**Hybrid Infrastructure Administration**	
1.1	Perform administrative tasks 1.1.1 Manage event logs 1.1.2 Manage Services 1.1.3 Collect data with Log Analytics Agents 1.1.4 Collect performance counters in Azure 1.1.5 Manage alerts 1.1.6 Collect monitoring data from VMs using Azure Diagnostics Extension 1.1.7 Collect performance data from VMs using VM Insights	8.1, 8.2, 8.3, 8.4, 8.5
1.2	Migrate on-premises to Azure 1.2.1 Migrate file shares to Azure 1.2.2 Migrate Hyper-V hosts to Azure 1.2.3 Migrate virtual machines 1.2.4 Migrate virtual machine storage	7.1, 7.2, 7.3
2.0	**Secure and Update Windows**	
2.1	Secure Windows 2.1.1 Implement exploit mitigation policies 2.1.2 Protect systems with Windows Defender for Endpoint 2.1.3 Protect applications with Windows Defender Application Control 2.1.4 Enable Windows Defender SmartScreen 2.1.5 Implement group security policies	2.1, 2.2, 2.3, 2.5 3.1, 3.4, 3.5

2.2	Secure Active Directory user accounts 2.2.1 Protect user credentials with Windows Defender Credential Guard 2.2.2 Implement password policies 2.2.3 Implement password block lists 2.2.4 Deploy user rights policies 2.2.5 Configure account security policy settings 2.2.6 Delegate administrative control 2.2.7 Implement authentication policies and silos for administrative accounts	2.4 3.2, 3.3, 3.5, 3.6, 3.7
2.3	Secure Active Directory groups 2.3.1 Audit group policies 2.3.2 Manage Active Directory Administrator security groups	3.7 8.1
2.4	Secure domain controllers and VMs 2.4.1 Harden domain controllers 2.4.2 Use Azure Sential to monitor physical and virtual servers 2.4.3 Use Azure Security Center to resolve security issues	3.6, 3.7, 3.8
2.5	Implement storage security 2.5.1 Encrypt storage with Windows BitLocker 2.5.2 Use Azure disk encryption 2.5.3 Manage disk encryption keys in an IaaS VM environment	4.2, 4.3
3.0	**Backup and Disaster Recovery**	
3.1	Back up Windows servers 3.1.1 Use Azure Recovery Services Vault to back up files and folders 3.1.2 Create a new backup policy 3.1.3 Use the built-in backup agent to back up Azure VMs 3.1.4 Modify a backup policy in Azure Recovery Services Vault	6.1, 6.3
3.2	Recover Windows servers	6.2, 6.3

	3.2.1 Use Azure Recovery Services Vault to restore files and folders 3.2.2 Recover a VM from a snapshot 3.2.3 Recover a VM as a new Azure VM 3.2.4 Restore a VM from backup 3.2.5 Create a recovery plan for Azure 3.2.6 Configure on-premises VM for site recovery 3.2.7 Configure Azure VM for site recovery 3.2.8 Restore objects from the Active Directory Recycle Bin	8.8
3.3	Replicate Windows servers 3.3.1 Configure VM replication for offsite or an Azure region 3.3.2 Configure Hyper-V VM replication 3.3.3 Manage a Hyper-V replica server 3.3.4 Fail over a VM	6.3, 6.5
4.0	**High Availability and Failover Cluster Management**	
4.1	Configure failover clusters 4.1.1 Configure a network load balancing cluster 4.1.2 Create a failover cluster 4.1.3 Configure a quorum in a failover cluster 4.1.4 Setup a floating IP address for a cluster 4.1.5 Add a failover cluster role 4.1.6 Configure a failover cluster 4.1.7 Create a Scale-Out File Server	5.1, 5.2, 5.3, 5.4
4.2	Manage failover clusters 4.2.1 Manage a cluster workload 4.2.2 Implement load balancing for a cluster 4.2.3 Add storage to a cluster 4.2.4 Use Windows Admin Center to manage failover clusters 4.2.5 Recover a failed node in the cluster 4.2.6 Upgrade the operating system for a node in the cluster 4.2.7 Initiate a workload failover 4.2.8 Install Windows Updates on nodes in a cluster	5.2, 5.3, 5.4, 5.5, 5.6 8.4

	4.2.9 Configure and manage Storage Spaces Direct	
5.0	**Troubleshoot Windows Servers**	
5.1	Troubleshoot Windows 5.1.1 Troubleshoot connectivity in a Hybrid environment 5.1.2 Troubleshoot and resolve a boot failure	3.8 8.6, 8.7
5.2	Troubleshoot virtual machines 5.2.1 Troubleshoot VM performance 5.2.2 Troubleshoot connectivity with VMs	8.6, 8.7

Objective Mapping: TestOut Hybrid Server Pro: Advanced Objective to LabSim Section

The TestOut Hybrid Server Pro: Advanced course covers the following TestOut Hybrid Server Pro: Advanced exam objectives:

Section	Title	Objectives
1.0	**Course Introduction**	
1.1	Course Introduction	
1.2	Windows and Azure Simulator Interface	
2.0	**Secure Windows Servers**	
2.1	Malware Protection	2.1 Secure Windows • 2.1.1 Implement exploit mitigation policies • 2.1.2 Protect systems with Windows Defender for Endpoint • 2.1.3 Protect applications with Windows Defender Application Control • 2.1.4 Enable Windows Defender SmartScreen
2.2	Windows Defender Exploit Guard	2.1 Secure Windows • 2.1.1 Implement exploit mitigation policies
2.3	Windows Defender Application Control	2.1 Secure Windows • 2.1.3 Protect applications with Windows Defender Application Control
2.4	Windows Defender Credential Guard	2.2 Secure Active Directory user accounts

		• 2.2.1 Protect user credentials with Windows Defender Credential Guard
2.5	Defender SmartScreen	2.1 Secure Windows • 2.1.4 Enable Windows Defender SmartScreen
3.0	**Secure Windows Server with Active Directory and Group Policy**	
3.1	Secure Windows Servers with Group Policies	2.1 Secure Windows • 2.1.5 Implement group security policies
3.2	Password Policies	2.2 Secure Active Directory user accounts • 2.2.2 Implement password policies • 2.2.3 Implement password block lists
3.3	User Rights Assignment and Protected Users	2.2 Secure Active Directory user accounts • 2.2.1 Protect user credentials with Windows Defender Credential Guard • 2.2.4 Deploy user rights policies
3.4	Audit Policies	2.1 Secure Windows • 2.1.5 Implement group security policies
3.5	Security Options	2.1 Secure Windows • 2.1.5 Implement group security policies 2.2 Secure Active Directory user accounts • 2.2.5 Configure account security policy settings

3.6	Secure a Hybrid Active Directory Infrastructure	2.2 Secure Active Directory user accounts • 2.2.7 Implement authentication policies and silos for administrative accounts 2.4 Secure domain controllers and VMs • 2.4.1 Harden domain controllers
3.7	Secure Hybrid Active Directory Accounts	2.2 Secure Active Directory user accounts • 2.2.5 Configure account security policy settings • 2.2.6 Delegate administrative control 2.3 Secure Active Directory groups • 2.3.2 Manage Active Directory Administrator security groups 2.4 Secure domain controllers and VMs • 2.4.1 Harden domain controllers
3.8	Resolve Security Issues by Using Azure Services	2.4 Secure domain controllers and VMs • 2.4.2 Use Azure Sential to monitor physical and virtual servers 5.1 Troubleshoot Windows • 5.1.1 Troubleshoot connectivity in a Hybrid environment
4.0	**Secure Windows Server Networking and Storage**	
4.1	Secure Windows Server Networking	

4.2	Secure Windows Server Storage (On-Premise)	2.5 Implement storage security • 2.5.1 Encrypt storage with Windows BitLocker
4.3	Secure Windows Server Storage (Azure)	2.5 Implement storage security • 2.5.3 Manage disk encryption keys in an IaaS VM environment
5.0	**Clustering and High Availability**	
5.1	Network Load Balancing and High Availability	4.1 Configure failover clusters • 4.1.1 Configure a network load balancing cluster
5.2	Implement Failover Clustering	4.1 Configure failover clusters • 4.1.2 Create a failover cluster • 4.1.4 Setup a floating IP address for a cluster 4.2 Manage failover clusters • 4.2.3 Add storage to a cluster
5.3	Configuring Cluster Quorum	4.1 Configure failover clusters • 4.1.3 Configure a quorum in a failover cluster 4.2 Manage failover clusters • 4.2.2 Implement load balancing for a cluster
5.4	Cluster Role Management and Workloads	4.1 Configure failover clusters • 4.1.5 Add a failover cluster role • 4.1.6 Configure a failover cluster

		• 4.1.7 Create a Scale-Out File Server 4.2 Manage failover clusters • 4.2.1 Manage a cluster workload
5.5	Manage Failover Clustering	4.2 Manage failover clusters • 4.2.4 Use Windows Admin Center to manage failover clusters • 4.2.5 Recover a failed node in the cluster • 4.2.6 Upgrade the operating system for a node in the cluster • 4.2.7 Initiate a workload failover • 4.2.8 Install Windows Updates on nodes in a cluster
5.6	Highly Available Storage Spaces	4.2 Manage failover clusters • 4.2.9 Configure and manage Storage Spaces Direct
6.0	**Implement Disaster Recovery**	
6.1	Windows Server Backup	3.1 Back up Windows servers • 3.1.1 Use Azure Recovery Services Vault to back up files and folders • 3.1.2 Create a new backup policy • 3.1.3 Use the built-in backup agent to back up Azure VMs
6.2	Windows Server Recovery	3.2 Recover Windows servers • 3.2.1 Use Azure Recovery Services Vault to restore files and folders

		• 3.2.2 Recover a VM from a snapshot • 3.2.3 Recover a VM as a new Azure VM • 3.2.4 Restore a VM from backup
6.3	Azure Site Recovery	3.1 Back up Windows servers • 3.1.4 Modify a backup policy in Azure Recovery Services Vault 3.2 Recover Windows servers • 3.2.5 Create a recovery plan for Azure • 3.2.6 Configure on-premises VM for site recovery • 3.2.7 Configure Azure VM for site recovery 3.3 Replicate Windows servers • 3.3.1 Configure VM replication for offsite or an Azure region
6.4	Azure Site Recovery Networking	
6.5	Hyper-V Replica	3.3 Replicate Windows servers • 3.3.1 Configure VM replication for offsite or an Azure region • 3.3.2 Configure Hyper-V VM replication • 3.3.3 Manage a Hyper-V replica server • 3.3.4 Fail over a VM
7.0	**Migrate Servers and Workloads**	
7.1	Migrate On-Premises Storage to On-Premises Servers or Azure	1.2 Migrate on-premises to Azure

		• 1.2.1 Migrate file shares to Azure • 1.2.4 Migrate virtual machine storage
7.2	Migrate On-Premises Servers to Azure	1.2 Migrate on-premises to Azure • 1.2.1 Migrate file shares to Azure • 1.2.2 Migrate Hyper-V hosts to Azure • 1.2.3 Migrate virtual machines • 1.2.4 Migrate virtual machine storage
7.3	Migrate Previous Versions to Windows Server	1.2 Migrate on-premises to Azure • 1.2.1 Migrate file shares to Azure • 1.2.2 Migrate Hyper-V hosts to Azure • 1.2.3 Migrate virtual machines • 1.2.4 Migrate virtual machine storage
7.4	Migrate IIS Workloads to Azure	
7.5	Migrate an AD DS Infrastructure to Windows Server 2022 AD DS	
8.0	**Monitor and Troubleshoot Windows Server Environments**	
8.1	Windows System Events	1.1 Perform administrative tasks • 1.1.1 Manage event logs • 1.1.3 Collect data with Log Analytics Agents • 1.1.4 Collect performance counters in Azure • 1.1.6 Collect monitoring data from VMs using Azure Diagnostics Extension

		• 1.1.7 Collect performance data from VMs using VM Insights 2.3 Secure Active Directory groups • 2.3.1 Audit group policies
8.2	Windows Configuration Tools	1.1 Perform administrative tasks • 1.1.2 Manage Services
8.3	Windows Performance Management	1.1 Perform administrative tasks • 1.1.4 Collect performance counters in Azure • 1.1.7 Collect performance data from VMs using VM Insights
8.4	Windows Admin Center and System Insights	1.1 Perform administrative tasks • 1.1.7 Collect performance data from VMs using VM Insights 4.2 Manage failover clusters • 4.2.4 Use Windows Admin Center to manage failover clusters
8.5	Monitor Windows Server by Using Azure Services	1.1 Perform administrative tasks • 1.1.6 Collect monitoring data from VMs using Azure Diagnostics Extension • 1.1.7 Collect performance data from VMs using VM Insights
8.6	Troubleshoot Windows Server On-Premises and Hybrid Networking	5.1 Troubleshoot Windows

		• 5.1.1 Troubleshoot connectivity in a Hybrid environment 5.2 Troubleshoot virtual machines • 5.2.2 Troubleshoot connectivity with VMs
8.7	Troubleshoot Windows Server Virtual Machines in Azure	5.1 Troubleshoot Windows • 5.1.1 Troubleshoot connectivity in a Hybrid environment • 5.1.2 Troubleshoot and resolve a boot failure 5.2 Troubleshoot virtual machines • 5.2.1 Troubleshoot VM performance • 5.2.2 Troubleshoot connectivity with VMs
8.8	Troubleshoot Active Directory	3.2 Recover Windows servers • 3.2.8 Restore objects from the Active Directory Recycle Bin
A.0	**TestOut Hybrid Server Pro: Advanced - Practice Exams**	
A.1	Prepare for TestOut Hybrid Server Pro: Advanced Certification	
A.2	TestOut Hybrid Server Pro: Advanced Domain Review	
B.0	**Microsoft Configuring Windows Server Hybrid Advanced Services AZ-801 - Practice Exams**	
B.1	Prepare for Microsoft Configuring Windows Server Hybrid Advanced Services AZ-801 Certification	

B.2	Microsoft Configuring Windows Server Hybrid Advanced Services AZ-801 Domain Review (20 Questions)	
B.3	Microsoft Configuring Windows Server Hybrid Advanced Services AZ-801 Domain Review (All Questions)	

Objective Mapping: LabSim Section to Microsoft AZ-801 Objective

The TestOut Hybrid Server Pro: Advanced course and certification exam cover the following Microsoft AZ-801 Configuring Windows Server Hybrid Advanced Services objectives:

#	Domain	Module.Section
1.0	**Secure Windows Server on-premises and hybrid infrastructures**	
1.1	Secure Windows Server operating system 1.1.1 - Configure and manage exploit protection 1.1.2 - Configure and manage Windows Defender Application Control 1.1.3 - Configure and manage Windows Defender for Endpoint 1.1.4 - Configure and manage Windows Defender Credential Guard 1.1.5 - Configure SmartScreen 1.1.6 - Implement operating system security by using Group Policies	2.1, 2.2, 2.3, 2.4, 2.5 3.1, 3.3, 3.4, 3.5 8.1
1.2	Secure a hybrid Active Directory (AD) infrastructure 1.2.1 - Configure password policies 1.2.2 - Enable password block lists 1.2.3 - Manage protected users 1.2.4 - Manage account security on a Read-Only Domain Controller (RODC) 1.2.5 - Harden domain controllers 1.2.6 - Configure authentication policies silos 1.2.7 - Restrict access to domain controllers 1.2.8 - Configure account security 1.2.9 - Manage AD built-in administrative groups 1.2.10 - Manage AD delegation 1.2.11 - Implement and manage Microsoft Defender for Identity	3.2, 3.3, 3.6, 3.7
1.3	Identify and remediate Windows Server security issues by using Azure services 1.3.1 - Monitor on-premises servers and Azure IaaS VMs by using Microsoft Sentinel 1.3.2 - Identify and remediate security issues with on-premises servers and Azure IaaS VMs by using Microsoft Defender for Cloud	2.1 3.8

1.4	Secure Windows Server networking 1.4.1 - Manage Windows Defender Firewall 1.4.2 - Implement domain isolation 1.4.3 - Implement connection security rules	4.1
1.5	Secure Windows Server storage 1.5.1 - Manage Windows BitLocker Drive Encryption (BitLocker) 1.5.2 - Manage and recover encrypted volumes 1.5.3 - Enable storage encryption by using Azure Disk Encryption 1.5.4 - Manage disk encryption keys for IaaS virtual machines	4.2, 4.3
2.0	**Implement and manage Windows Server high availability**	
2.1	Implement a Windows Server failover cluster 2.1.1 - Implement a failover cluster on-premises, hybrid, or cloud-only 2.1.2 - Create a Windows failover cluster 2.1.3 - Stretch cluster across datacenter or Azure regions 2.1.4 - Configure storage for failover clustering 2.1.5 - Modify quorum options 2.1.6 - Configure network adapters for failover clustering 2.1.7 - Configure cluster workload options 2.1.8 - Configure cluster sets 2.1.9 - Configure Scale-Out File Servers 2.1.10 - Create an Azure witness 2.1.11 - Configure a floating IP address for the cluster 2.1.12 - Implement load balancing for the failover cluster	5.1, 5.2, 5.3, 5.4
2.2	Manage failover clustering 2.2.1 - Implement cluster-aware updating 2.2.2 - Recover a failed cluster node 2.2.3 - Upgrade a node to Windows Server 2022 2.2.4 - Failover workloads between nodes 2.2.5 - Install Windows updates on cluster nodes 2.2.6 - Manage failover clusters using Windows Admin Center	5.5

2.3	Implement and manage Storage Spaces Direct 2.3.1 - Create a failover cluster using Storage Spaces Direct 2.3.2 - Upgrade a Storage Spaces Direct node 2.3.3 - Implement networking for Storage Spaces Direct 2.3.4 - Configure Storage Spaces Direct	5.6
3.0	**Implement disaster recovery**	
3.1	Manage backup and recovery for Windows Server 3.1.1 - Back up and restore files and folders to Azure Recovery Services vault 3.1.2 - Install and manage Azure Backup Server 3.1.3 - Back up and recover using Azure Backup Server 3.1.4 - Manage backups in Azure Recovery Services vault 3.1.5 - Create a backup policy 3.1.6 - Configure backup for Azure Virtual Machines using the built-in backup agent 3.1.7 - Recover a VM using temporary snapshots 3.1.8 - Recover VMs to new Azure Virtual Machines 3.1.9 - Restore a VM	6.1, 6.2
3.2	Implement disaster recovery by using Azure Site Recovery 3.2.1 - Configure Azure Site Recovery networking 3.2.2 - Configure Site Recovery for on-premises VMs 3.2.3 - Configure a recovery plan 3.2.4 - Configure Site Recovery for Azure Virtual Machines 3.2.5 - Implement VM replication to secondary datacenter or Azure region 3.2.6 - Configure Azure Site Recovery policies	6.3, 6.4
3.3	Protect virtual machines by using Hyper-V replicas 3.3.1 - Configure Hyper-V hosts for replication 3.3.2 - Manage Hyper-V replica servers 3.3.3 - Configure VM replication 3.3.4 - Perform a failover	6.1, 6.5
4.0	**Migrate servers and workloads**	

4.1	Migrate on-premises storage to on-premises servers or Azure 4.1.1 - Transfer data and share 4.1.2 - Cut over to a new server by using Storage Migration Service 4.1.3 - Use Storage Migration Service to migrate to Azure Virtual Machines 4.1.4 - Migrate to Azure file shares	7.1
4.2	Migrate on-premises servers to Azure 4.2.1 - Deploy and configure Azure Migrate appliance 4.2.2 - Migrate VM workloads to Azure IaaS 4.2.3 - Migrate physical workloads to Azure IaaS 4.2.4 - Migrate by using Azure Migrate	7.2
4.3	Migrate workloads from previous versions to Windows Server 2022 4.3.1 - Migrate Internet Information Services (IIS) 4.3.2 - Migrate Hyper-V hosts 4.3.3 - Migrate Remote Desktop Services (RDS) host servers 4.3.4 - Migrate Dynamic Host Configuration Protocol (DHCP) 4.3.5 - Migrate print servers	7.3 8.6
4.4	Migrate IIS workloads to Azure 4.4.1 - Migrate IIS workloads to Azure Web Apps 4.4.2 - Migrate IIS workloads to containers	7.4
4.5	Migrate an AD DS infrastructure to Windows Server 2022 AD DS 4.5.1 - Migrate AD DS objects, including users, groups and Group Policies, using Active Directory Migration Tool 4.5.2 - Migrate to a new Active Directory forest 4.5.3 - Upgrade an existing forest	7.5
5.0	**Monitor and troubleshoot Windows Server environments**	
5.1	Monitor Windows Server by using Windows Server tools and Azure services	8.1, 8.3, 8.4, 8.5

	5.1.1 - Monitor Windows Server by using Performance Monitor 5.1.2 - Create and configure Data Collector Sets 5.1.3 - Monitor servers and configure alerts by using Windows Admin Center 5.1.4 - Monitor by using System Insights 5.1.5 - Manage event logs 5.1.6 - Deploy Log Analytics agents 5.1.7 - Collect performance counters to Azure 5.1.8 - Create alerts 5.1.9 - Monitor Azure Virtual Machines by using Azure diagnostics extension 5.1.10 - Monitor Azure Virtual Machines performance by using VM insights	
5.2	Troubleshoot Windows Server on-premises and hybrid networking 5.2.1 - Troubleshoot hybrid network connectivity 5.2.2 - Troubleshoot on-premises connectivity	8.6
5.3	Troubleshoot Windows Server virtual machines in Azure 5.3.1 - Troubleshoot deployment failures 5.3.2 - Troubleshoot booting failures 5.3.3 - Troubleshoot VM performance issues 5.3.4 - Troubleshoot VM extension issues 5.3.5 - Troubleshoot disk encryption issues 5.3.6 - Troubleshoot storage 5.3.7 - Troubleshoot VM connection issues	2.1 8.7
5.4	Troubleshoot Active Directory 5.4.1 - Restore objects from AD recycle bin 5.4.2 - Recover Active Directory database using Directory Services Restore Mode 5.4.3 - Recover SYSVOL 5.4.4 - Troubleshoot Active Directory replication 5.4.5 - Troubleshoot hybrid authentication issues 5.4.6 - Troubleshoot on-premises Active Directory	8.8

Objective Mapping: Microsoft AZ-801 Objective to LabSim Section

The TestOut Hybrid Server Pro: Advanced course covers the following Microsoft AZ-801 Configuring Windows Server Hybrid Advanced Services exam objectives:

Section	Title	Objectives
1.0	**Course Introduction**	
1.1	Course Introduction	
1.2	Windows and Azure Simulator Interface	
2.0	**Secure Windows Servers**	
2.1	Malware Protection	1.1 Secure Windows Server operating system • 1.1.1 - Configure and manage exploit protection • 1.1.2 - Configure and manage Windows Defender Application Control • 1.1.3 - Configure and manage Windows Defender for Endpoint • 1.1.4 - Configure and manage Windows Defender Credential Guard • 1.1.5 - Configure SmartScreen 1.3 Identify and remediate Windows Server security issues by using Azure services • 1.3.2 - Identify and remediate security issues with on-premises servers and Azure IaaS VMs by using Microsoft Defender for Cloud 5.3 Troubleshoot Windows Server virtual machines in Azure • 5.3.2 - Troubleshoot booting failures
2.2	Windows Defender Exploit Guard	1.1 Secure Windows Server operating system

		• 1.1.1 - Configure and manage exploit protection • 1.1.4 - Configure and manage Windows Defender Credential Guard • 1.1.5 - Configure SmartScreen
2.3	Windows Defender Application Control	1.1 Secure Windows Server operating system • 1.1.2 - Configure and manage Windows Defender Application Control
2.4	Windows Defender Credential Guard	1.1 Secure Windows Server operating system • 1.1.4 - Configure and manage Windows Defender Credential Guard
2.5	Defender SmartScreen	1.1 Secure Windows Server operating system • 1.1.5 - Configure SmartScreen
3.0	**Secure Windows Server with Active Directory and Group Policy**	
3.1	Secure Windows Servers with Group Policies	1.1 Secure Windows Server operating system • 1.1.6 - Implement operating system security by using Group Policies
3.2	Password Policies	1.2 Secure a hybrid Active Directory (AD) infrastructure • 1.2.1 - Configure password policies • 1.2.2 - Enable password block lists
3.3	User Rights Assignment and Protected Users	1.1 Secure Windows Server operating system • 1.1.6 - Implement operating system security by using Group Policies 1.2 Secure a hybrid Active Directory (AD) infrastructure • 1.2.3 - Manage protected users

3.4	Audit Policies	1.1 Secure Windows Server operating system • 1.1.6 - Implement operating system security by using Group Policies
3.5	Security Options	1.1 Secure Windows Server operating system • 1.1.6 - Implement operating system security by using Group Policies
3.6	Secure a Hybrid Active Directory Infrastructure	1.2 Secure a hybrid Active Directory (AD) infrastructure • 1.2.4 - Manage account security on a Read-Only Domain Controller (RODC) • 1.2.5 - Harden domain controllers • 1.2.6 - Configure authentication policies silos
3.7	Secure Hybrid Active Directory Accounts	1.2 Secure a hybrid Active Directory (AD) infrastructure • 1.2.7 - Restrict access to domain controllers • 1.2.8 - Configure account security • 1.2.9 - Manage AD built-in administrative groups • 1.2.10 - Manage AD delegation • 1.2.11 - Implement and manage Microsoft Defender for Identity
3.8	Resolve Security Issues by Using Azure Services	1.3 Identify and remediate Windows Server security issues by using Azure services • 1.3.1 - Monitor on-premises servers and Azure IaaS VMs by using Microsoft Sentinel • 1.3.2 - Identify and remediate security issues with on-premises servers and Azure IaaS VMs by using Microsoft Defender for Cloud
4.0	**Secure Windows Server Networking and Storage**	

4.1	Secure Windows Server Networking	1.4 Secure Windows Server networking • 1.4.1 - Manage Windows Defender Firewall • 1.4.2 - Implement domain isolation • 1.4.3 - Implement connection security rules
4.2	Secure Windows Server Storage (On-Premise)	1.5 Secure Windows Server storage • 1.5.1 - Manage Windows BitLocker Drive Encryption (BitLocker) • 1.5.2 - Manage and recover encrypted volumes
4.3	Secure Windows Server Storage (Azure)	1.5 Secure Windows Server storage • 1.5.3 - Enable storage encryption by using Azure Disk Encryption • 1.5.4 - Manage disk encryption keys for IaaS virtual machines
5.0	**Clustering and High Availability**	
5.1	Network Load Balancing and High Availability	2.1 Implement a Windows Server failover cluster • 2.1.6 - Configure network adapters for failover clustering
5.2	Implement Failover Clustering	2.1 Implement a Windows Server failover cluster • 2.1.1 - Implement a failover cluster on-premises, hybrid, or cloud-only • 2.1.2 - Create a Windows failover cluster • 2.1.4 - Configure storage for failover clustering • 2.1.11 - Configure a floating IP address for the cluster
5.3	Configuring Cluster Quorum	2.1 Implement a Windows Server failover cluster • 2.1.5 - Modify quorum options

		• 2.1.10 - Create an Azure witness • 2.1.12 - Implement load balancing for the failover cluster
5.4	Cluster Role Management and Workloads	2.1 Implement a Windows Server failover cluster • 2.1.1 - Implement a failover cluster on-premises, hybrid, or cloud-only • 2.1.7 - Configure cluster workload options • 2.1.8 - Configure cluster sets • 2.1.9 - Configure Scale-Out File Servers
5.5	Manage Failover Clustering	2.2 Manage failover clustering • 2.2.1 - Implement cluster-aware updating • 2.2.2 - Recover a failed cluster node • 2.2.3 - Upgrade a node to Windows Server 2022 • 2.2.4 - Failover workloads between nodes • 2.2.5 - Install Windows updates on cluster nodes • 2.2.6 - Manage failover clusters using Windows Admin Center
5.6	Highly Available Storage Spaces	2.3 Implement and manage Storage Spaces Direct • 2.3.1 - Create a failover cluster using Storage Spaces Direct • 2.3.2 - Upgrade a Storage Spaces Direct node • 2.3.3 - Implement networking for Storage Spaces Direct • 2.3.4 - Configure Storage Spaces Direct
6.0	**Implement Disaster Recovery**	
6.1	Windows Server Backup	3.1 Manage backup and recovery for Windows Server

		• 3.1.1 - Back up and restore files and folders to Azure Recovery Services vault • 3.1.2 - Install and manage Azure Backup Server • 3.1.3 - Back up and recover using Azure Backup Server • 3.1.4 - Manage backups in Azure Recovery Services vault • 3.1.5 - Create a backup policy • 3.1.6 - Configure backup for Azure Virtual Machines using the built-in backup agent • 3.1.7 - Recover a VM using temporary snapshots 3.3 Protect virtual machines by using Hyper-V replicas • 3.3.1 - Configure Hyper-V hosts for replication
6.2	Windows Server Recovery	3.1 Manage backup and recovery for Windows Server • 3.1.7 - Recover a VM using temporary snapshots • 3.1.8 - Recover VMs to new Azure Virtual Machines • 3.1.9 - Restore a VM
6.3	Azure Site Recovery	3.2 Implement disaster recovery by using Azure Site Recovery • 3.2.1 - Configure Azure Site Recovery networking • 3.2.2 - Configure Site Recovery for on-premises VMs • 3.2.3 - Configure a recovery plan • 3.2.4 - Configure Site Recovery for Azure Virtual Machines • 3.2.5 - Implement VM replication to secondary datacenter or Azure region • 3.2.6 - Configure Azure Site Recovery policies

6.4	Azure Site Recovery Networking	3.2 Implement disaster recovery by using Azure Site Recovery • 3.2.1 - Configure Azure Site Recovery networking • 3.2.2 - Configure Site Recovery for on-premises VMs • 3.2.3 - Configure a recovery plan • 3.2.4 - Configure Site Recovery for Azure Virtual Machines • 3.2.5 - Implement VM replication to secondary datacenter or Azure region • 3.2.6 - Configure Azure Site Recovery policies
6.5	Hyper-V Replica	3.3 Protect virtual machines by using Hyper-V replicas • 3.3.1 - Configure Hyper-V hosts for replication • 3.3.2 - Manage Hyper-V replica servers • 3.3.3 - Configure VM replication • 3.3.4 - Perform a failover
7.0	**Migrate Servers and Workloads**	
7.1	Migrate On-Premises Storage to On-Premises Servers or Azure	4.1 Migrate on-premises storage to on-premises servers or Azure • 4.1.1 - Transfer data and share • 4.1.2 - Cut over to a new server by using Storage Migration Service • 4.1.3 - Use Storage Migration Service to migrate to Azure Virtual Machines • 4.1.4 - Migrate to Azure file shares
7.2	Migrate On-Premises Servers to Azure	4.2 Migrate on-premises servers to Azure • 4.2.1 - Deploy and configure Azure Migrate appliance

		• 4.2.2 - Migrate VM workloads to Azure IaaS • 4.2.3 - Migrate physical workloads to Azure IaaS • 4.2.4 - Migrate by using Azure Migrate
7.3	Migrate Previous Versions to Windows Server	4.3 Migrate workloads from previous versions to Windows Server 2022 • 4.3.1 - Migrate Internet Information Services (IIS) • 4.3.2 - Migrate Hyper-V hosts • 4.3.3 - Migrate Remote Desktop Services (RDS) host servers • 4.3.4 - Migrate Dynamic Host Configuration Protocol (DHCP) • 4.3.5 - Migrate print servers
7.4	Migrate IIS Workloads to Azure	4.4 Migrate IIS workloads to Azure • 4.4.1 - Migrate IIS workloads to Azure Web Apps • 4.4.2 - Migrate IIS workloads to containers
7.5	Migrate an AD DS Infrastructure to Windows Server 2022 AD DS	4.5 Migrate an AD DS infrastructure to Windows Server 2022 AD DS • 4.5.1 - Migrate AD DS objects, including users, groups and Group Policies, using Active Directory Migration Tool • 4.5.2 - Migrate to a new Active Directory forest • 4.5.3 - Upgrade an existing forest
8.0	**Monitor and Troubleshoot Windows Server Environments**	
8.1	Windows System Events	1.1 Secure Windows Server operating system • 1.1.6 - Implement operating system security by using Group Policies

		5.1 Monitor Windows Server by using Windows Server tools and Azure services • 5.1.1 - Monitor Windows Server by using Performance Monitor • 5.1.2 - Create and configure Data Collector Sets • 5.1.5 - Manage event logs
8.2	Windows Configuration Tools	
8.3	Windows Performance Management	5.1 Monitor Windows Server by using Windows Server tools and Azure services • 5.1.1 - Monitor Windows Server by using Performance Monitor
8.4	Windows Admin Center and System Insights	5.1 Monitor Windows Server by using Windows Server tools and Azure services • 5.1.1 - Monitor Windows Server by using Performance Monitor • 5.1.2 - Create and configure Data Collector Sets • 5.1.3 - Monitor servers and configure alerts by using Windows Admin Center • 5.1.4 - Monitor by using System Insights • 5.1.5 - Manage event logs • 5.1.6 - Deploy Log Analytics agents • 5.1.7 - Collect performance counters to Azure • 5.1.8 - Create alerts • 5.1.9 - Monitor Azure Virtual Machines by using Azure diagnostics extension • 5.1.10 - Monitor Azure Virtual Machines performance by using VM insights

8.5	Monitor Windows Server by Using Azure Services	5.1 Monitor Windows Server by using Windows Server tools and Azure services • 5.1.6 - Deploy Log Analytics agents • 5.1.7 - Collect performance counters to Azure • 5.1.8 - Create alerts • 5.1.9 - Monitor Azure Virtual Machines by using Azure diagnostics extension • 5.1.10 - Monitor Azure Virtual Machines performance by using VM insights
8.6	Troubleshoot Windows Server On-Premises and Hybrid Networking	4.3 Migrate workloads from previous versions to Windows Server 2022 • 4.3.4 - Migrate Dynamic Host Configuration Protocol (DHCP) 5.2 Troubleshoot Windows Server on-premises and hybrid networking • 5.2.1 - Troubleshoot hybrid network connectivity • 5.2.2 - Troubleshoot on-premises connectivity
8.7	Troubleshoot Windows Server Virtual Machines in Azure	5.3 Troubleshoot Windows Server virtual machines in Azure • 5.3.1 - Troubleshoot deployment failures • 5.3.2 - Troubleshoot booting failures • 5.3.3 - Troubleshoot VM performance issues • 5.3.4 - Troubleshoot VM extension issues • 5.3.5 - Troubleshoot disk encryption issues • 5.3.6 - Troubleshoot storage • 5.3.7 - Troubleshoot VM connection issues
8.8	Troubleshoot Active Directory	5.4 Troubleshoot Active Directory

		• 5.4.1 - Restore objects from AD recycle bin • 5.4.2 - Recover Active Directory database using Directory Services Restore Mode • 5.4.3 - Recover SYSVOL • 5.4.4 - Troubleshoot Active Directory replication • 5.4.5 - Troubleshoot hybrid authentication issues • 5.4.6 - Troubleshoot on-premises Active Directory
A.0	**TestOut Hybrid Server Pro: Advanced - Practice Exams**	
A.1	Prepare for TestOut Hybrid Server Pro: Advanced Certification	
A.2	TestOut Hybrid Server Pro: Advanced Domain Review	
B.0	**Microsoft Configuring Windows Server Hybrid Advanced Services AZ-801 - Practice Exams**	
B.1	Prepare for Microsoft Configuring Windows Server Hybrid Advanced Services AZ-801 Certification	
B.2	Microsoft Configuring Windows Server Hybrid Advanced Services AZ-801 Domain Review (20 Questions)	
B.3	Microsoft Configuring Windows Server Hybrid Advanced Services AZ-801 Domain Review (All Questions)	