

# Configuring Windows Server Hybrid Advanced Services – Flexible Training («AZ801V»)

In diesem Kurs erfahren IT-Expertinnen und -Experten, wie sie fortgeschrittene Windows-Server-Dienste mithilfe lokaler, hybrider und cloudbasierter Technologien konfigurieren.

**Dauer:** 4 Tage

**Preis:** 3'400.– zzgl. 8.1% MWST

**Kursdokumente:** Offizielle Microsoft-Unterlagen und Microsoft Learn

**Herstellercode:** AZ-801

## Inhalt

Der Inhalt dieses Flexible Training leitet sich aus der Prüfung «AZ-801: [Configuring Windows Server Hybrid Advanced Services](#)» ab. Beginnen Sie schon jetzt auf Microsoft Learn mit der Vorbereitung auf den Kurs und nutzen Sie den Learning Support, wenn Sie Fragen haben. Während der jeweiligen 3h-Trainer-Sessions arbeiten Sie mit den offiziellen Microsoft-Kursunterlagen (mehr Informationen unter «Methodik & Didaktik»).

In diesem Kurs erfahren IT-Expertinnen und -Experten, wie Sie die Hybridfunktionen von Azure nutzen können, virtuelle und physische Serverworkloads zu Azure IaaS migrieren und Azure-VMs unter Windows Server schützen. In diesem Kurs erfahren IT-Expertinnen und -Experten auch, wie sie Aufgaben im Zusammenhang mit Hochverfügbarkeit, Problembehandlung und Notfallwiederherstellung ausführen. In diesem Kurs werden Verwaltungstools und -technologien wie Windows Admin Center, PowerShell, Azure Arc, die Azure Automation-Updateverwaltung, Microsoft Defender for Identity, Azure Security Center, Azure Migrate und Azure Monitor vorgestellt.

### Modul 1: Windows-Server-Sicherheit

In diesem Modul wird erläutert, wie Sie eine Active-Directory-Umgebung schützen, indem Sie Benutzerkonten mit den geringsten Rechten schützen und sie in der Gruppe „Geschützte Benutzer“ platzieren. In diesem Modul wird erläutert, wie Sie den Authentifizierungsbereich einschränken und potenziell unsichere Konten behandeln. Das Modul beschreibt ausserdem, wie sie die Sicherheitskonfiguration einer Windows-Server-Betriebsumgebung härten. Darüber hinaus wird im Modul die Verwendung von Windows Server Update Services zum Bereitstellen von Betriebssystemupdates auf Computern im Netzwerk erläutert. Schliesslich wird in diesem Modul behandelt, wie Sie Windows-Server-DNS absichern, um die Infrastruktur für die Netzwerknamensauflösung zu schützen.

#### Lektionen

- Schützen von Windows-Server-Benutzerkonten
- Härten von Windows Server
- Windows-Server-Updateverwaltung
- Absichern von Windows-Server-DNS

#### Lab: Konfigurieren der Sicherheit in Windows Server

- Konfigurieren von Windows Defender Credential Guard
- Ermitteln problematischer Konten
- Implementieren von LAPS

### Modul 2: Implementieren von Sicherheitslösungen in Hybridszenarien

In diesem Modul wird beschrieben, wie Sie lokale Windows-Server-Ressourcen und Azure-IaaS-Workloads schützen. In diesem Modul wird behandelt, wie Sie die Netzwerksicherheit für Windows-

Server-IaaS-VMs (Infrastructure-as-a-Service) verbessern und Netzwerksicherheitsprobleme für diese VMs diagnostizieren. Darüber hinaus bietet das Modul eine Einführung in Azure Security Center und erläutert das Onboarding von Windows Server-Computern in Security Center. Darüber hinaus beschreibt das Modul, wie Sie die Azure-Updateverwaltung aktivieren, Updates bereitstellen, eine Updatebewertung überprüfen und Updates für Azure-VMs verwalten. In dem Modul wird erläutert, wie adaptive Anwendungssteuerungen und die BitLocker-Datenträgerverschlüsselung verwendet werden, um Windows-Server-IaaS-VMs zu schützen. Schliesslich wird im Modul erläutert, wie sie Azure-IaaS-VMs unter Windows Server auf Änderungen an Dateien und der Registrierung sowie auf Änderungen an der Anwendungssoftware überwachen.

#### Lektionen

- Implementieren von Netzwerksicherheit für Windows-Server-IaaS-VMs
- Überwachen der Sicherheit von virtuellen Windows-Server-IaaS-Computern
- Verwalten von Azure-Updates
- Erstellen und Implementieren von Anwendungspositivlisten mit adaptiver Anwendungssteuerung
- Konfigurieren der BitLocker-Datenträgerverschlüsselung für Windows-IaaS-VMs
- Implementieren von Änderungsnachverfolgung und Überwachung der Dateiintegrität für Windows-Server-IaaS-VMs

#### Lab: Verwenden von Azure Security Center in Hybridszenarien

- Bereitstellen von Azure-VMs unter Windows Server
- Konfigurieren von Azure Security Center
- Onboarding einer lokalen Windows Server-Instanz in Azure Security Center
- Überprüfen der Hybridfunktionen von Azure Security Center
- Konfigurieren der Windows Server-Sicherheit auf Azure-VMs

#### Modul 3: Implementieren von Hochverfügbarkeit

In diesem Modul werden Technologien und Optionen zum Erstellen einer hochverfügbaren Windows-Server-Umgebung beschrieben. Das Modul führt freigegebene Clustervolumen für den clusterknotenübergreifenden Zugriff auf gemeinsamen Speicher ein. Im Modul werden ausserdem Failoverclustering, Stretched Cluster und Clustersets für die Implementierung von Hochverfügbarkeit von Windows-Server-Workloads behandelt. Im Modul werden dann Hochverfügbarkeitsbereitstellungen für Hyper-V- und Windows-Server-VMs erläutert, z. B. Netzwerklastenausgleich, Livemigration und Speichermigration. Darüber hinaus werden im Modul Hochverfügbarkeitsoptionen für Freigaben behandelt, die auf Windows-Server-Dateiservern gehostet werden. Schliesslich wird in diesem Modul beschrieben, wie Sie die Skalierung für VM-Skalierungsgruppen und VMs mit Lastenausgleich sowie Azure Site Recovery implementieren.

#### Lektionen

- Einführung in freigegebene Clustervolumen
- Implementieren des Windows-Server-Failoverclustering
- Implementieren der Hochverfügbarkeit von Windows-Server-VMs
- Implementieren der Hochverfügbarkeit von Windows-Server-Dateiservern
- Implementieren von Skalierbarkeit und Hochverfügbarkeit mit Windows-Server-VMs

#### Lab: Implementieren von Failover-Clustering

- Konfigurieren von iSCSI-Speicher
- Konfigurieren eines Failoverclusters
- Bereitstellen und Konfigurieren eines hochverfügbaren Dateiservers
- Überprüfen der Bereitstellung eines hochverfügbaren Dateiservers

#### Modul 4: Notfallwiederherstellung in Windows Server

In diesem Modul wird „Hyper-V-Replikat“ als BCDR-Lösung (Business Continuity & Disaster Recovery) für eine virtuelle Umgebung eingeführt. In diesem Modul werden Szenarien und Anwendungsfälle für

das Hyper-V-Replikat sowie die Voraussetzungen für seine Verwendung erläutert. Ausserdem erfahren Sie in diesem Modul, wie Sie Azure Site Recovery in lokalen Szenarien für die Notfallwiederherstellung implementieren.

### Lektionen

- Implementieren eines Hyper-V-Replikats
- Schützen Ihrer lokalen Infrastruktur vor Notfällen mit Azure Site Recovery

### Lab: Implementieren des Hyper-V-Replikats und der Windows-Server-Sicherung

- Implementieren von Hyper-V-Replikaten
- Implementieren der Sicherung und Wiederherstellung mit der Windows-Server-Sicherung

## Modul 5: Implementieren von Wiederherstellungsdiensten in Hybridszenarien

Dieses Modul behandelt Tools und Technologien für das Implementieren der Notfallwiederherstellung in Hybridszenarios. Das vorherige Modul hingegen konzentriert sich auf BCDR-Lösungen für lokale Szenarios. Das Modul beginnt mit Azure Backup als Dienst zum Schützen von Dateien und Ordnern. Anschliessend wird das Implementieren von Recovery-Tresoren und Azure-Backup-Richtlinien erläutert. In diesem Modul wird beschrieben, wie Sie Windows-IaaS-VMs wiederherstellen, lokale Workloads sichern und wiederherstellen und Azure-VM-Sicherungen verwalten. In den Modulen wird auch behandelt, wie Sie die Notfallwiederherstellung für die Azure-Infrastruktur bereitstellen, indem Sie Replikation, Failover und Failback für virtuelle Azure-Computern mit Azure Site Recovery verwalten und durchführen.

### Lektionen

- Implementieren von Hybridsicherung und -wiederherstellung mit IaaS unter Windows Server
- Schützen Ihrer Azure-Infrastruktur mit Azure Site Recovery
- Schützen Ihrer virtuellen Computer mithilfe von Azure Backup

### Lab: Implementieren von Azure-basierten Wiederherstellungsdiensten

- Implementieren der Lab-Umgebung
- Erstellen und Konfigurieren eines Azure Site Recovery-Tresors
- Implementieren des Hyper-V-VM-Schutzes über einen Azure Site Recovery-Tresor
- Implementieren von Azure Backup

## Modul 6: Upgrade und Migration in Windows Server

In diesem Modul werden Ansätze zum Migrieren und Aktualisieren von Windows-Server-Workloads erläutert, die unter älteren Windows-Server-Versionen ausgeführt werden. Das Modul behandelt die erforderlichen Strategien zum Verschieben von Domänencontrollern zu Windows Server 2022 und beschreibt, wie das Active-Directory-Migrationstool Domänen innerhalb einer Gesamtstruktur konsolidieren oder Domänen zu einer neuen AD-DS-Gesamtstruktur migrieren kann. Im Modul wird ausserdem die Verwendung des Speichermigrationsdiensts erläutert, um Dateien und Dateifreigaben von vorhandenen Dateiservern zu neuen Servern zu migrieren, auf denen Windows Server 2022 ausgeführt wird. Schliesslich wird in diesem Modul behandelt, wie Sie die Cmdlets der Windows-Server-Migrationstools installieren und verwenden, um häufig verwendete Serverrollen aus früheren Windows-Server-Versionen zu migrieren.

### Lektionen

- Active Directory Domain-Services-Migration
- Migrieren von Dateiserverworkloads mithilfe von Storage Migration Service
- Migrieren von Windows-Server-Rollen

### Lab: Migrieren von Windows-Server-Workloads zu IaaS-VMs

- Bereitstellen von AD-DS-Domänencontrollern in Azure
- Migrieren von Dateiserverfreigaben mithilfe des Speichermigrationsdiensts

## Modul 7: Implementieren der Migration in Hybridszenarien

In diesem Modul werden Ansätze zum Migrieren von Workloads, die in Windows Server ausgeführt werden, zu einem virtuellen IaaS-Computer (Infrastructure-as-a-Service) erläutert. In diesem Modul wird die Verwendung Azure Migrate zum Bewerten und Migrieren von lokalen Windows-Server-Instanzen zu Microsoft Azure vorgestellt. Das Modul behandelt auch die Migration einer in Windows Server ausgeführten Workload zu einem virtuellen IaaS-Computer (Infrastructure-as-a-Service) und zu Windows Server 2022 mithilfe von Windows-Server-Migrationstools oder des Speichermigrationsdiensts. Schliesslich wird in diesem Modul beschrieben, wie Sie das Tool zur Anwendungscontainerisierung von Azure Migrate verwenden, um ASP.NET-Anwendungen zu containerisieren und zu Azure App Service zu migrieren.

### Lektionen

- Migrieren von lokalen Windows-Server-Instanzen zu virtuellen Azure-IaaS-Computern
- Aktualisieren und Migrieren von Windows-Server-IaaS-VMs
- Containerisieren und Migrieren von ASP.NET-Anwendungen zu Azure App Service

### Lab: Migrieren von lokalen VMs-Servern zu IaaS-VMs

- Implementieren der Bewertung und Ermittlung von Hyper-V-VMs mithilfe von Azure Migrate
- Implementieren der Migration von Hyper-V-Workloads mithilfe von Azure Migrate

## Modul 8: Server- und Leistungsüberwachung in Windows Server

In diesem Modul werden verschiedene Tools zum Überwachen des Betriebssystems und der Anwendungen auf einem Windows-Server-Computer sowie die Konfiguration eines Systems zur Optimierung der Effizienz und zur Behebung von Problemen beschrieben. In diesem Modul erfahren Sie, inwiefern die Ereignisanzeige einen praktischen und zugänglichen Ort zum Beobachten eintretender Ereignisse bietet und wie Sie die Daten im Ereignisprotokoll interpretieren. Das Modul behandelt ausserdem die Implementierung einer Überwachung und Diagnose, um gesetzliche Bestimmungen einzuhalten, Benutzeraktivitäten im Blick zu behalten und Probleme zu behandeln. Schliesslich wird im Modul erläutert, wie Sie AD-DS-Dienstfehler oder Leistungsbeeinträchtigungen behandeln, einschliesslich Wiederherstellung gelöschter Objekte und der AD-DS-Datenbank, und wie Sie Probleme bei der Hybridauthentifizierung beheben.

### Lektionen

- Überwachen der Leistung von Windows Server
- Verwalten und Überwachen von Windows-Server-Ereignisprotokollen
- Implementieren von Windows-Server-Überwachung und -Diagnose
- Problembehandlung für Active Directory

### Lab: Überwachung und Problembehandlung bei Windows Server

- Festlegen einer Leistungsbaseline
- Identifizieren der Quelle eines Leistungsproblems
- Anzeigen und Konfigurieren zentralisierter Ereignisprotokolle

## Modul 9: Implementieren der Betriebsüberwachung in Hybridszenarien

In diesem Modul wird das Verwenden von Überwachungs- und Problembehandlungstools, Prozessen und bewährten Methoden behandelt, um die App-Leistung und Verfügbarkeit von Windows-Server-IaaS-VMs und Hybridinstanzen zu optimieren. Das Modul beschreibt, wie Sie Azure Monitor für IaaS-VMs in Azure und in lokalen Umgebungen implementieren und Abhängigkeitszuordnungen verwenden. Anschliessend wird erläutert, wie Sie die Diagnose aktivieren, um Daten zu einem virtuellen Computer zu erhalten, wie Sie VM-Metriken im Metrik-Explorer von Azure anzeigen und eine Metrikwarnung zur Überwachung der VM-Leistung erstellen. In diesem Modul wird dann im Anschluss behandelt, wie Sie die VM-Leistung mithilfe von Azure Monitor VM Insights überwachen. Das Modul beschreibt dann verschiedene Aspekte der Problembehandlung für lokale und hybride Netzwerkkonnektivität.

einschliesslich der Diagnose häufiger Probleme mit DHCP, Namensauflösung, IP-Konfiguration und Routing. Schliesslich werden im Modul die Behandlung von Konfigurationsproblemen, die sich auf die Konnektivität mit in Azure gehosteten virtuellen Windows-Server-Computern auswirken, sowie Ansätze zum Beheben von Problemen mit VM-Start, Erweiterungen, Leistung, Speicher und Verschlüsselung untersucht.

## Lektionen

- Überwachen von IaaS-VMs und -Hybridinstanzen unter Windows Server
- Überwachen der Integrität Ihrer virtuellen Azure-Computer mithilfe des Metrik-Explorers von Azure und mit Metrikwarnungen
- Überwachen der Leistung von VMs mithilfe von Azure Monitor VM Insights
- Problembehandlung für lokale und hybride Netzwerke
- Behandeln von Problemen bei virtuellen Computern mit Windows Server in Azure

## Lab: Überwachung und Problembehandlung von IaaS-VMs, auf denen Windows Server ausgeführt wird

- Aktivieren von Azure Monitor für VMs
- Einrichten eines virtuellen Computers mit Startdiagnose
- Einrichten von Log-Analytics-Arbeitsbereichen und Azure Monitor VM Insights

## Key Learnings

- Härten der Sicherheitskonfiguration der Windows-Server-Betriebsumgebung
- Verbessern der Hybridsicherheit mit Hilfe von Azure Security Center, Azure Sentinel und Windows Update Management
- Anwenden von Sicherheitsfunktionen, um kritische Ressourcen zu schützen
- Implementieren von Lösungen für hohe Verfügbarkeit und Notfallwiederherstellung
- Implementieren von Wiederherstellungsdiensten in Hybridszenarien
- Planen und Implementieren von hybriden und reinen Cloud-Migrations-, Sicherungs- und Wiederherstellungsszenarien
- Durchführen von Upgrades und Migrationen in Bezug auf AD DS und Speicher
- Verwalten und Überwachen von Hybridszenarien mit WAC, Azure Arc, Azure Automation und Azure Monitor
- Implementieren der Service- und Leistungsüberwachung und Anwenden von Fehlerbehebung

## Methodik & Didaktik

### Digicomp Flexible-Learning-Ansatz:

- **Trainings-Modalität:** Sobald Sie das Training gebucht haben, beginnt die individuelle Vorbereitung mit Microsoft Learn und unserem Learning Support. Während einer Dauer von 4 Wochen finden 6-8 halbtägige (je 3h) virtuelle Live-Sessions mit unseren Azure-MCT-Experten statt. Die Sessions sind bereits geplant und lassen sich super mit dem Arbeitsalltag verbinden. Zwischen den Sessions bleibt genügend Zeit, das gelernte Wissen zu verarbeiten.
- **Learning Support:** Mittels Foren haben Sie die Möglichkeit, jederzeit Fragen zu stellen und innert weniger Stunden einen Lösungsansatz zu erhalten, der Sie weiterbringen wird. Ihr Zugang bleibt bis 30 Tage nach Abschluss des offiziellen Trainings bestehen, um ein nachhaltiges Lernerlebnis zu ermöglichen.
- **Detaillierter Session-Plan:** Klicken Sie dazu am Ende der Seite, wo Sie Ihr gewünschtes Datum auswählen, auf «**Stundenplan**».

## Zielpublikum

Dieser viertägige Kurs richtet sich an Windows-Server-Hybridadministratoren, die Erfahrung mit Windows Server haben und die Funktionen ihrer lokalen Umgebungen erweitern möchten, indem sie lokale und hybride Technologien kombinieren.

Windows-Server-Hybridadministratoren, die bereits lokale Kerntechnologien implementieren und verwalten, möchten ihre Umgebungen sichern und schützen, virtuelle und physische Workloads zu Azure IaaS migrieren, eine hochverfügbare, vollständig redundante Umgebung bereitstellen und Überwachung und Problembehandlung durchführen.

## Zertifizierung

Dieses Flexible Training bereitet Sie vor auf:

- **Prüfung:** «AZ-801: Configuring Windows Server Hybrid Advanced Services» für den zweiten und letzten Schritt für die
- **Zertifizierung:** «Microsoft Certified: Windows Server Hybrid Administrator Associate»

Dieses Zertifikat können Sie auch [in unserem Bootcamp](#) (inkl. Prüfungen AZ-800 und AZ-801) erwerben.

## Haben Sie Fragen oder möchten Sie einen Firmenkurs buchen?

Wir beraten Sie gerne unter 044 447 21 21 oder [info@digicomp.ch](mailto:info@digicomp.ch). Detaillierte Infos zu den Terminen finden Sie unter [www.digicomp.ch/weiterbildung-microsoft-technology/microsoft-azure/microsoft-certified-windows-server-hybrid-administrator-associate/kurs-configuring-windows-server-hybrid-advanced-services-flexible-training-az-801](https://www.digicomp.ch/weiterbildung-microsoft-technology/microsoft-azure/microsoft-certified-windows-server-hybrid-administrator-associate/kurs-configuring-windows-server-hybrid-advanced-services-flexible-training-az-801)