Microsoft Azure : Hybrid Identity

WorkshopPLUS

Duration: 4 days

Focus Area: Operations and Monitoring

Difficulty: 300- Advanced

Overview

Organizations can transform by adopting innovative technology that creates value and differentiates them in the market. This course provides participants with the deep knowledge and understanding on how to successfully extend on-premises AD DS to cloud to give your users seamless sign on experience across all in-house applications and applications hosted in the cloud and Office 365.
If you have device management for authentication and authorization requirements for your business or have end-to-end Identity Management Lifecycle requirements, this course is essential for you.

Objectives

After completing this training, students will be able to:

- Understand the challenges an organization can have managing Apps, Devices, Users and Data.
- Discuss how a Hybrid Identity enables users to access their data anywhere with SSO and self-service experiences while protecting data by enforcing strong authentication, conditional access control, configuring SSO and ensuring compliance with governance, attestation and reporting.
- Understand how Azure AD Connect is used for connecting to Azure AD/Office 365 and extending the on-premises ADDS and other local directories to Azure AD.
- Learn about Azure AD Premium features and how to implement them successfully

Key Takeaways

Course Material

- Complete end to-end Cloud Identity Technologies: Authentication, Single Sign On (SSO) , Active Directory Federation Services (AD FS) Active Directory Synchronization
- Best of cloud and on-premises solutions. Improve security by leveraging Azure AD security features.

Hands-on Labs

- Most of the concepts covered above will be supported by hands-on labs and demos.
- Attendees have access to resources and labs for up to 6 months after workshop completion.

Agenda

Day 1

- Cloud Identity Framework

Day 2

- Identity synchronization
- Authentication options

Day 3

- Azure AD Management

Day 4

- Azure AD Security
- Devices

Plan for four full days. Early departure on any day is not recommended.

Course Details

Module 1: Cloud Identity Framework

- IT challenges and Microsoft Approach
- Azure AD licensing and key concepts
- Azure Active Directory and it's major components
- Azure AD Deployment Scenarios
- Identity management using the portal and PowerShell
- Azure AD B2B and B2C

Module 2: Identity synchronization

- Azure AD synchronization concepts
- Azure AD Connect configuration options
- Azure AD Connect advanced configuration

Module 3: Authentication options

- Password synchronization
- Active Directory Federation Services
- Pass-through authentication
- Seamless single Sign-on
- Modern Authentication
- Alternate Login ID

Module 4: Azure AD Management

- Application management
- Group management
- Azure AD application proxy
- Password management

Module 5: Azure AD Security

- Protecting identities through features like Smart Account Lockouts, MFA, Azure Information protection
- Protecting applications using features as Conditional Access and disabling legacy authentication
- Security auditing and activity reports
- Azure AD Connect Health

Module 6: Devices

- Devices Concepts and Scenarios
- How to configure the use of devices
- How Workplace Join and Hybrid Azure AD Join works
- Join Windows 10 to Azure AD
- Troubleshooting device registration

Recommended Qualifications

This WorkshopPLUS is intended for customers and partners planning to deploy Microsoft Office 365 Infrastructure, extend on-premises Active Directory Domain Services (AD DS) to Microsoft Azure, or wanted to refresh or gain advance knowledge of Microsoft Hybrid, and Cloud Identity and wanted to learn from Microsoft Cloud experts on managing Identities across on-premises and Azure. Version 1.1 Prerequisites: Although it is not required, it's recommended that students that take part in this workshop have basic knowledge on Active Directory Domain Services.

Hardware Requirements

- An Intel Core-i5-based PC
- USB port
- Microsoft/Windows Live ID to connect to the virtual environment
- 4 GB RAM
- 128 GB HDD
- Windows 8.1 or later
- Office 2013 Professional Plus
- Internet access with at least 1 Mbps bandwidth per student.

For more information

Contact your Henson Group representative for further details.