AZ100T05

Manage Identities

college@sela.co.il   03-6176666

Manage Identities

AZ100T05 - Version: 1

🕐 1 days Course

Description:

This course teaches IT Professional how to use Azure Active Directory (AD) to provide employees and customers with a multi-tenant cloud-based directory and identity management system. Students will learn the differences between Azure AD and Active Directory Domain Services (AD DS), as well the differences in functionality offered by the different editions of Azure AD. Students also learn how to configure self-service password reset, or to use the option of password writeback to reset user passwords regardless of their location. Students are then introduced to Azure AD Identity Protection and learn how they can use it to protect their organizations from compromised accounts, identity attacks, and configuration issues. Students also learn how to integrate Azure AD with the many Software as a Service (SaaS) applications that are used, in order to secure user access to those applications.

Next, the concepts of Azure domains and tenants, and users and groups are explained and students learn how to work with the various Azure AD objects. Students are introduced to Azure role-based access control to be able to provide a more granular access based on the principle of least privilege. An administrator, or user, can do exactly the task they need to accomplish; no more, no less. Students also learn how to work with Azure joined devices and Hybrid AD joined devices, enabling their users to be productive wherever and whenever – but ensuring that corporate assets are protected and that devices meet security and compliance standards.

Students learn how to use Azure AD Connect to integrate their on-premises directories with Azure AD, providing a common identity for their users of Office 365, Azure, and SaaS applications integrated with Azure AD. Lastly, students also learn how to use Azure AD Application Proxy to be able to provide their users with remote access to web application

that are published on-premises, such as SharePoint sites, Outlook Web Access, or any other line of business (LOB) applications the organization has.

Intended audience:

This course is for Azure Administrators. Azure Administrators manage the cloud services that span storage, networking, and compute cloud capabilities, with a deep understanding of each service across the full IT lifecycle. They take end-user requests for new cloud applications and make recommendations on services to use for optimal performance and scale, as well as provision, size, monitor and adjust as appropriate. This role requires communicating and coordinating with vendors. Azure Administrators use the Azure Portal and as they become more proficient they use PowerShell and the Command Line Interface.

Prerequisites:

Successful Azure Administrators start this role with experience on operating systems, virtualization, cloud infrastructure, storage structures, and networking.

Objectives:

Implement Azure Active Directory, Self-Service Password Reset, Azure AD Identity Protection, and integrated SaaS applications.
Configure domains and tenants, users and groups, roles, and devices.
Implement and manage Azure Active Directory integration options and Azure AD Application Proxy.

Topics:

Module 1 - Managing Azure Active Directory

- Azure Active Directory Overview
- Self-Service Password Reset
- Azure AD Identity Protection

• Integrating SaaS Applications with Azure AD

Module 2 - Managing Azure Active Directory Objects

• Azure Domains and Tenants
• Azure Users and Groups
• Azure Roles
• Managing Devices

Module 3 - Implementing and Managing Hybrid Identities

• Azure Active Directory Integration Options
• Azure AD Application Proxy