MOC 40573-G: Microsoft Cloud Workshop: Hybrid identity

Course Summary

Description

In this workshop, you will learn to setup and configure a hybrid identity solution that integrates an existing on-premises identity solution with Azure. You will learn how to secure the virtual network by deploying a network virtual appliance and configure firewall rules and route tables. Additionally, you will set up access to the virtual network with a jump box and a site-to-site VPN connection.

Objectives

After taking this course, students will be able to:

- Design virtual networks in Azure with multiple subnets to filter and control network traffic.
- Ceate a virtual network and provision subnets.
- Create route tables with required routes.
- Build a management jump box.
- Configure firewalls to control traffic flow.
- Configure site-to-site connectivity.

Topics

- Whiteboard Design Session - Hybrid identity
- Hands-On Lab - Hybrid identity

Audience

This workshop is intended for Cloud Architects and IT professionals who have architectural expertise of infrastructure and solutions design in cloud technologies and want to learn more about Azure and Azure services as described in the "Summary" and "Skills gained" areas. Those attending this workshop should also be experienced in other non-Microsoft cloud technologies, meet the course prerequisites, and want to cross-train on Azure.

Prerequisites

Workshop content presumes 300-level of architectural expertise of infrastructure and solutions design. We suggest students take this prerequisite prior to attending this workshop: Microsoft Azure Essentials course, http://www.microsoft.com/en-US/azureessentials

Duration

One day

MOC 40573-G: Microsoft Cloud Workshop: Hybrid identity

Course Outline

I. Whiteboard Design Session - Hybrid identity

In this workshop, you will learn to setup and configure a hybrid identity solution that integrates an existing on-premises identity solution with Azure. You will learn how to secure the virtual network by deploying a network virtual appliance and configure firewall rules and route tables. Additionally, you will set up access to the virtual network with a jump box and a site-to-site VPN connection.

A. Review the customer case study
B. Design a proof of concept solution
C. Present the solution

II. Hands-On Lab - Hybrid identity

In this hands-on lab you will setup and configure a number of different hybrid identity scenarios. The scenarios involve an Active Directory single-domain forest named contoso.local, which in this lab environment, consists (for simplicity reasons) of a single domain controller named DC1 and a single domain member server named APP1. The intention is to explore Azure AD-related capabilities that allow you to integrate Active Directory with Azure Active Directory, optimize hybrid authentication and authorization, and provide secure access to on-premises resources from Internet for both organizational users and users who are members of partner organizations.

A. Integrate an Active Directory forest with an Azure Active Directory tenant.
B. Manage Authentication, Authorization, and Access Control in Hybrid Scenarios.
C. Configure application access in hybrid scenarios.