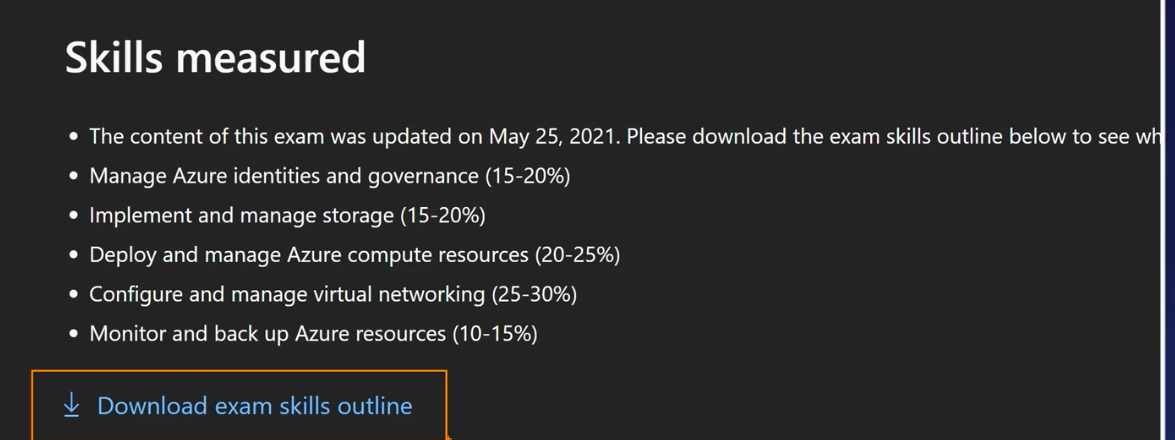
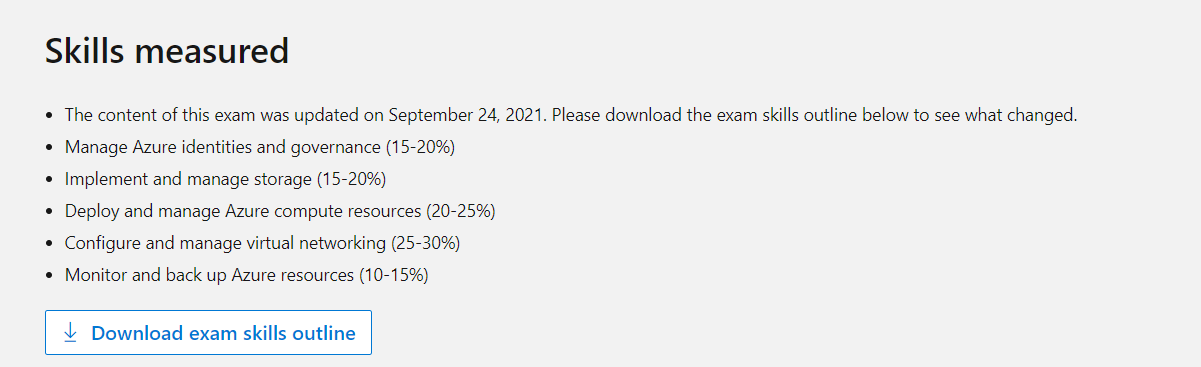
ITProTV



May 30 2022



# Manage Azure identities and governance (15–20%)

## Manage Azure Active Directory (Azure AD) objects

**create users and groups**

**create administrative units**

**manage user and group properties**

**manage device settings**

**perform bulk user updates**

**manage guest accounts**

**configure Azure AD join**

**configure self-service password reset**

## Manage role-based access control (RBAC)

* create a custom role
* provide access to Azure resources by assigning roles at different scopes
* interpret access assignments

## Manage subscriptions and governance

* configure Azure policies
* configure resource locks
* apply and manage tags on resources
* manage resource groups
* manage subscriptions
* manage costs
* configure management groups

# Implement and manage storage (15–20%)

## Secure storage

* configure network access to storage accounts
* create and configure storage accounts
* generate shared access signature (SAS) tokens
* manage access keys
* configure Azure AD authentication for a storage account
* configure access to Azure Files

## Manage storage

* export from Azure job
* import into Azure job
* install and use Azure Storage Explorer
* copy data by using AZCopy
* implement Azure Storage replication
* configure blob object replication

## Configure Azure files and Azure Blob Storage

* create an Azure file share
* create and configure Azure File Sync service
* configure Azure Blob Storage
* configure storage tiers
* configure blob lifecycle management

# Deploy and manage Azure compute resources (20–25%)

## Automate deployment of virtual machines (VMs) by using Azure Resource Manager templates

* modify an Azure Resource Manager template
* configure a virtual hard disk (VHD) template
* deploy from a template
* save a deployment as an Azure Resource Manager template
* deploy virtual machine extensions

## Configure VMs

* configure Azure Disk Encryption
* move VMs from one resource group to another
* manage VM sizes
* add data disks
* configure networking
* redeploy VMs
* configure high availability
* deploy and configure virtual machine scale sets

## Create and configure containers

* configure sizing and scaling for Azure Container Instances
* configure container groups for Azure Container Instances
* configure storage for Azure Kubernetes Service (AKS)
* configure scaling for AKS
* configure network connections for AKS
* upgrade an AKS cluster

## Create and configure Azure App Service

* create an App Service plan
* configure scaling settings in an App Service plan
* create an App Service
* secure an App Service
* configure custom domain names
* configure backup for an App Service
* configure networking settings
* configure deployment settings

# Configure and manage virtual networking (25–30%)

## Implement and manage virtual networking

* create and configure virtual networks, including peering
* configure private and public IP addresses
* configure user-defined network routes
* implement subnets
* configure endpoints on subnets
* configure private endpoints
* configure Azure DNS, including custom DNS settings and private or public DNS zones

## Secure access to virtual networks

* create security rules
* associate a network security group (NSG) to a subnet or network interface
* evaluate effective security rules
* implement Azure Firewall
* implement Azure Bastion

## Configure load balancing

* configure Azure Application Gateway
* configure an internal or public load balancer
* troubleshoot load balancing

## Monitor and troubleshoot virtual networking

* monitor on-premises connectivity
* configure and use Azure Monitor for Networks
* use Azure Network Watcher
* troubleshoot external networking
* troubleshoot virtual network connectivity

## Integrate an on-premises network with an Azure virtual network

* create and configure Azure VPN Gateway
* create and configure Azure ExpressRoute
* configure Azure Virtual WAN

# Monitor and back up Azure resources (10–15%)

## Monitor resources by using Azure Monitor

* configure and interpret metrics
* configure Azure Monitor logs
* query and analyze logs
* set up alerts and actions
* configure Application Insights

## Implement backup and recovery

* create a Recovery Services vault
* create a Backup vault
* create and configure backup policy
* perform backup and restore operations by using Azure Backup
* perform site-to-site recovery by using Azure Site Recovery
* configure and review backup reports

**The exam guide below shows the changes that were implemented on September 24, 2021.**

ITPROTV Course

User Source – Azure AD(cloud only identities), Microsoft Account(Used to create subscription), Windows Server AD (From on premises), Guest

Create a user or invite user (Guest)

On Premise accounts cannot be edited in Azure Active Directory

Azure Cli – **az** ad user create

Powershell - Connect-azureAD

Creating User via powershell needs 4 parameters. Displayname, password profile, upn and mailnickname

Deleted users are available for 30 days

### Create and Manage Groups

Group types – Security and Microsoft 365

Security – Assign permissions, roles and it’s a main type of group. Nested groups.

Microsoft 365 – Shared mailboxes, access to Sharepoint . Only users can be added.

Membership type for groups – Assigned, dynamic user and dynamic device

Assigned – Specify who is the member of the group.

You cannot change the group type

You can change the membership type

Dynamic Users – Conditional rules.

Dynamic Device – Conditional rules

Via Azure Cli - Create a group – az ad group create –display-name “blaa” –mail-nickname “blaa”

Via Azure PS – Connect-AzureAD | New-AzureADGroup -**DisplayName**”” -**MailEnabled** $value -**SecurityEnabled** $value -**MailNickName** “NotSet”

Security Enabled – AD group. If this is set to false then you will create Office 365 group

### Manage Guest Account

Access to people who don’t belong to organizations  
Invite them to organization  
We need the guest email address and invite

Can be added to roles, groups

Perform Bulk User Updates

BulkRestoring users – Get object ID of the users to restore in the template and upload bulk restore

30 days to restore from deleted items

Configure Azure AD Join

MS Learn

4 Tooling Options are available

1. Azure Portal
2. Azure Cli
3. Azure Powershell
4. Azure Cloud Shell

Azure Cloud Shell

* Linux users – Bash experience
* Windows users – PowerShell

Azure PowerShell – Linux, MacOS, Windows

* Can be added to Windows Powershell or Powershell Core
* Used to manage resources
* Interactive Mode (One command at a time) or Scripting Mode (Multiple commads)

AZ is the formal name for Azure PowerShell Module

Using AZ you can work with the following

1. Resource Groups
2. Storage
3. VM
4. Azure AD
5. Containers
6. Machine Learning

Azure CLI – Linux, MacOS, Windows

Azure CLI is a cmd line program

Admins can use terminal, cmdline or Script instead of web browser

Azure CLI is also available in browser in Azure Cloud Shell

Interactive or Scripted

Commands in CLI are structured in groups and subgroups (Storage – (account, blob, share, queue))

Key – To find commands use az find (az find blob) or if you need help az storage blob –help

Azure Management Options

1. Azure Portal – you cannot automate repetitive tasks. Time consuming and prone to error
2. Azure Powershell and CLI – Cross platform. For CLI – First login using az login command
3. Azure Cloud shell
4. Azure Mobile App – Monitoring and managing resources from mobile. IOS, Android,Phone/tab

To switch to powershell core from Bash – Type pwsh

Bash defaults to Azure CLI – az

Cloud shell has developer tools, text editors and others.

When accessing Cloud Shell – You need to create a Azure Storage Account.

This Storage area stores any scripts, data and used as your $HOME folder.

Azure Mobile App

* Check status and metrics
* Alerts and notifications
* Diagnose and fix issues
* Azure Alerts
* Start, stop and restart vm or web app
* Connect to vm
* RBAC management
* Run saved scripts

Programmatically control using REST API, Azure SDK

Open support tickets using Help and Support Options in the Portal

Azure Advisor – Recommend HA, Security, Performance, Operation Excellence and cost.

**Azure Resources and Resource Groups**

Scenario – No Standardization | Critical resources deleted | Who owns which resources | No organization of company resources

Azure Resource Manager: Work with resources in your solution as a group

* Deploy, Update or delete all resources in a single operation
* Template for deployment
* Provides Security, Auditing and Tagging to manage resources after deployment
* Consistent management layer – Do tasks through 5 options
  + Azure PowerShell, Azure CLI, Azure Portal, REST API and Client SDKs
* Deploy resources in consistent state
* Declarative templates
* Correct order of deployment by defining dependencies
* Apply Access control to all services in RG. RBAC is native to management platform.
* Apply tags to resources to logically organize all the resources in your subscription
* Same tag resources billing cost view

Concept Works

Azure Identity Models

1. Cloud Identity – Azure AD User, a cloud account
2. Synced Identity – Synced from On Prem
3. Managed Identity – login.microsoftonline.com – Azure AD authentication
   * Password Synchronization
   * Passthrough Authentication – No need of domain federation
4. Federated Identity – Authentication happens on Prem – ADFS

Portal.office.com -> login.microsoftonline.com – ADFS – AD

AD -> ADFS -> login.microsoftonline.com -token ->portal.office.com

**Azure AD Connect**

Sync users and use applications provisioned on Azure AD to use – Gallery, custom apps, on prem apps

AAD connect procedure:

1. Verify domain in azure ad
2. Domain joined windows server 2008 r2 or later
3. Add 50k objects in azure ad and 300k after verifying
4. Need global admin cred
5. SQL express installed. More than 100k objects use SQL full

Methods: 3 methods

|  |  |  |
| --- | --- | --- |
| Password Synchronization | Pass Through Authentication | Federation with ADFS or PingFederate |
| Has synced to Azure AD  Authentication is processed by Azure AD  Authentication request is processed by Azure AD and no by on Prem AD  Domain is managed | Authentication processed by azure AD  Authentication request is passed to On Prem AD  Domain is managed | Authentication to be processed by on prem idp  Authentication request are redirected to on prem |

3 Accounts are created when installing AAD Connect

1. MSOL\_guid – Read/Write operation on Local AD – Query on prem AD – Created on prem
2. Sync\_guid – query info in Azure AD – Read/Write - Created in Azure AD
3. Service Account – AAD (AD sync service account) – Read / Write to database

A picture containing diagram

Description automatically generated

Sync Rules of AAD Connect

1. Local AD Connector space
2. Metaverse
3. Azure AD Connector space