**HANDS-ON:**

Policy: Sadece Tenant seviyesinde olur.

Transparent Data Encryption on DB1 By Using Key1:

* Create a managed identity for Server1
* Configure permissions for Server1
* Add key1 to Server1
* Configure the TDE protector on Server1

Alert Rule Olusturma: Lock silinirse alert olusturma.

> Monitor

* Alerts > Create > Alert Rule > Scope: Management lock | Subs | Done
* Condition > Select condition: Delete management lock condition | Done
* Action group > Select action group: Create action group (new)
  + Name: Notification type: email/sms message/push/voice
  + Azure app push notifications checkbox: [dbbie@contoso.com](mailto:dbbie@contoso.com) | OK
  + Notification name: Debbie
  + Create
* Create

VM’in Belirlenen Threshold’u Gecmesi Durumunda Mail Atan Alert Olusturma:

* Vm1 > Alerts > Add metric alert | OK
* Metric: CPU percentage | Condition: Greater than | Threshold: 60 | Period: Last 15 minutes
* Notify via: email - check | Additional adm email: admin1@contoso.com

Database audit logs’larin Workspace’e Aktarilmasi:

* db1 > Properties > Auditing > Log Analytics > Configure
* Auditing: ON | Audit log destination: Log Analytics | Select: wspc1
* Save

Database’in Advanced Threat Protection Alerts (ATP) are Sent to User1:

* db1 > Advanced data security > Settings
* Enable Advanced Data security at database level – check
* Send alerts to: User1 | Save

Windows Server’in System Event Logs’taki Event’lerinin Workspace’e Aktarilmasi:

* wserver1 > Advanced settings > Data > Windows Event Logs
* Name: yeni | Type: system | + > all severities | Save

Vault’un AzureBackupReport’unun Workspace’e Gonderilmesi:

* vault1 > Diagnostic Settings > Add a diagnostic setting
* Name > Log: AzureBackupReport | Destination details: Send to Log Analytics
* Select: wspc1 | Save

NetworkSecurityRuleCounter Log’larini Storage Account’a Kaydetme:

* nsg1 > Diagnostic settings > Add diagnostic setting
* Name | Log: NetworkSecurityRuleCounter | Destination: Archive to a storage acc
* Storage account: storageaccount1 | Retention (days): 30 | Save

Azure Arc Enabled Servers Connected Machine Agent: To deploy the vulnerability assessment scanner to your on-premises and multi-cloud machines, connect them to Azure first with Azure Arc, yani once Azure Arc yuklenir.

Vulnerability Scanner Extension Installation: ARM template ile vm’e yuklemek icin.

* User-assigned managed identity
* Azure AD ID tanimlanir.

Security Center Alerts Notification: Brute force attack failed de olsa gonderilir. High - gunde 4, Medium – gunde 2, Low – gunde 1 mail gonderir.

Alerts:

* Acknowledged: can be changed to Closed.
* Closed: can be changed to New or Acknowledged.

Suppression: Action rule’de suppression uygulandiginda, mevcut alert rule ilgili resource icin uygulanmaz. Tag eklemek administrative operation degildir.

MFA Service Settings: Enforced: Registration tamamlanmis. Enable: Register olmamis. They will be prompted to complete the registration process the next time they sign in. User can access app1 from ip address sorularinda MFA’in disable olma durumunu dikkate alma.

MFA:

* Assignment type: Active ise otomatik role’u alir. - PIM, ConditionalAccess
* Assignment type: Eligible ise request eder. - PIM, ConAccess
* MFA authentication: Enforced ise otomatik girer. - PIM, ConAccess
* MFA authentication: Disabled ise prompt’a yonlendirilir. - PIM, ConAccess
* Approver Group’da ise de baska bir User request’I onaylar. - PIM, ConAccess
* Eger Assigned ve MFA Disabled ise must change password.
* Excluded da varsa ayni anda excluded dikkate alinir.
* User Risk Policy:
  + Disable dikkate alinmaz.
  + Excluded dikkate alinir.
* Sign in Risk Policy:
  + AAD Identity Protection Sign-in Risk Policy ise MFA: Disable ise User blocked olur.
  + Risk Policy’lerde, Exclude – PIM: Buradaki grup’tan dolayi onay istenmez.

Conditional Access Policies: Users who log into the Azure Portal from untrusted locations need to authenticate using Multi-factor authentication.

Azure Security Center: Azure configurations veya workload’larin non-compliant with (or: ISO 27001) standards.

Azure Information Protection Label Files:Automatic classification applies to Word, Excel, and PowerPoint when documents are saved, and apply to Outlook when emails are sent. Automatic classification does not apply to Microsoft Notepad.

Don’t ask again for 14 days: MFA’i ayni device ile girdigi surece 2 hafta sormaz.

Firewall: > Subnet olustur > Firewall olustur > NAT rule collection olustur.

Hub-SpokeNet:

* GatewaySubnet: user-defined route that points private IP address of firewall as next hop address.
* SpokeVnetSubnet: Disables BGP route propagation and defines private IP address of firewall as default gateway.

Branch Policies: It enforces your team’s change management standard/code quality.

Grant PowerShell Access to VMs by JIT VM access: Permission: Read, Port: 5986

User Assigned Managed Identity: Birden fazla Resource’a baglayacak sekilde tanimlanabilir.

System Assigned Managed Identity: Yalniz tek bir resource’u baglar.

Automatic Provisioning: on olursa her tur VM’e Microsoft Monitoring Agent yuklenebilir.

Custom Alert Rules: Azure Security Center’da olusturmak icin once Upgrade pricing tier of Security center to Standard sonra Workspace kurulur.

Action Group: Custom alert rule’un triggered oldugunda mail olarak gonderilmesi icin Azure Monitor’den action group tanimlanip ilgili User’lar secilir.

Kerberos: is an authentication protocol that is used to verify the identity of a user or host. Windows server’dan File share’a veya User’a ulasirken kullanilan token. User credentials ile baglanilabilir. Kerberos, Access key’i kullanmaz.

Azure Automation State Configuration = Azure Desired State Configuration (DSC) virtual machine extension: target nodes automatically receive configurations, conform to the desired state, and report back on their compliance. The built-in pull server in Azure Automation eliminates the need to set up and maintain your own pull server. Gereksiz olan programlar kapatilir kurulumda. Tum Linux, Windows, On-prem, Azure ve AWS VM’lerde kullanilir.

MDM Security Baseline profile: Servers are not Mobile, and MDM is Mobile Device Management, so the only answer to choose here is Windows 10-Windows 11 as it can be installed on a laptop making it Mobile.

Application Security Group: Ayni Vnet icindeki tum NIC’lere associate edilebilir.

Adaptive application control: Security Center’dan configure edilir. It is an intelligent, automated end-to-end application whitelisting solution from Azure Security Center. It helps you control which applications can run on your Azure and non-Azure VMs (Windows and Linux), which, among other benefits, helps harden your VMs against malware. Viruslere karsi koruma da saglar.

Initiativ Definitions: Azure Security Center sadece bunlari destekler. Policy Definitions’u desteklemez. Custom-Security Category farketmez. Initiative olusturup or Management group’i scope olarak secerek istenen policy definitions’lari flere subs’a deploy edebiliriz.

Policy Initiative: Policy definitions’lari Management group’a baglayarak bircok subscription’a baglanabilir. Resource graph – yanlis. Policy definition deploy etmeden once intiative olusturulur.

Policy Definition: Yalniz tek bir subscription’a baglanir.

Regulatory Compliance Assessment: An initiative contains multiple policy definitions and assigned to rg. To identify which resources do not match/noncompliant policy definitions we use. Security center > Security policy’in altinda bulunur.

Monitoring in Azure Security Center Initiative Definition: When enabled, it views which security settings are assigned to subscription by default.

Lock: Read-Only: Ilgili RG’a ilave rsource koymayi da engeller. Herseyi engeller.

Blueprints: ARM templates, Azure policies, RG ve RBAC yuklenebilir. Tenant, Management Group veya Subscription seviyesinde tanimlanabilir. Management group'a tanimlarsak altindaki istenen Subscriptiona assign edilir. En azindan contributor rolu gerekiyor kurulum icin. Subs’lara identically role assignment yapar. Mevcut resource’lara etkisi olmaz. Blueprint ile kurulan resource’lar blueprint disinda silinemez ve degistirilemez.

Blueprint: Management group icin blueprint olusturmadan once RBAC modifiye edilir.

Blueprint Olusturma: SecurityPolicyInitiative ile her yeni rg’ye standard role assignments set.

* Create a Blueprint definition.
* Publish a Blueprint version,
* Assign a blueprint.

deployIfNotExists: Configure Azure policy which should use a managed identity associated with policy assignment durumunda kullanilir. Policy’leri modify ederken kullanilir.

Custom Sensitivity Label: olusturmak icin Global Admin olarak once custom sensitive information type olusturulur. << You can’t directly modify the default roles.

CountIf(): returns True of False and can used at a column.

Count(): returns the number of records.

Standard tier: modify the operating system security configurations via Azure Security Center.

Configure Access Review: The review will be assigned to a new collection of reviews and reviewed by resource owners.

* Create an access review program
* Create an access review control
* Set Reviewers to Group owners

Conditional Access: Trusted olmayan IP’lere uygulanir. Trusted IP’ler dogrudan baglanir. MFA disabled ise de talep edildigi halde giris olur.

Administrative Operation Alert: Lock eklemek, Resource olusturmak. Tag eklemek administrative operation degil.

**ANTIMALWARE:**

Microsoft Antimalware: Microsoft Defender for Cloud, you get the following high-severity recommendation: `Install endpoint protection solutions on virtual machine`. Add an Microsoft Antimalware extension to each VM to deploy.

Microsoft Antimalware Yukleme: (120: saat 2 demek.)

* VM1 > Extensions > Add > Microsoft Antimalware extension | OK
* Scheduled: Enabled | Scan type: Full | Scan day: Sunday | Scan time: 120

**DATABASE:**

Always Encrypted enabled: Database ise Developer’larin database’e girebilmesi icin The column encryption key / The column master key available olmali onlara.

Always Encrypted: Column bazinda encryption yapar. Sadece ilgili web-app’a Key Vault’u kullanarak managed identity ile giris saglar. Access policy ile key’i alir managed identity.

Vulnerability to SQL injection alert is triggered: When a faulty SQL statement is generated in the database by an application. db1 > Advanced Data Security ile configure edilir.

A Possible Vulnerability to SQL Injection: Db ve Synapse Analytics’in webapp’in medium seviyesinde faulty SQL statement in database olusturdugunda olusan alarmdir.

Vnet/Subnet’e Izin Verme: Ilgili Subnet’e db’ye ulasim izni veren rule tanimlama. Aytica trusted servicelere ve guvenilen IP araliklarina da istenirse burada izin verilir.

* Server > Properties > Firewalls and virtual networks > Vnet1/Subnet1
* IP: 23.2.34.5
* Trusted services - check > Add

System Assigned Managed Identity: VM veya Webapp’den database’e secure access saglar by using a contained user.

Configure Database to Meet Data and Application Requirements:

* Create Administrator for db1 > Connect db1 from SSMS > Create contained database users

User’a Izin Verme: Herhangi bir User’in database’e SSMS uzerinden ulasabilmesi icin db server’a admin olarak tanimlanmali.

* Server > Properties > Azure Directory Admin > Set Admin

Service Endpoint: Subnet’lere uygulanir ve Resource’larin Storage Account ve Database’lerle baglantisini saglar. Endpoint tanimlansa da ilgili resource’un da izin vermesi gerek ilgili Subnet’e.

**DEFENDER:**

Defender: Tum resource’lari DNS’ten korur, Virtual network’u korumaz. Container, VM, Resource Manager, Key Vault, Storage, App Service, DNS, Db … korur.

Defender: BlockStorage, BlockBlobStorage ve StorageV2 korunur. Storage korunmaz. FileStorage ve Data Lake storage monite edilir.

**IDENTITY PROTECTION:**

Identity Protection: Global Administrator and Security Administrator have full access.

Remediate Users and Configure Policies: Global admin, Security Administrator.

Onboard Azure AD Identity Protection: Global admin. (Security admin password’leri degistiremez.)

P2 license: User Risk policies and sig-in policy by implementing Azure AD Identity Protection.

**K8S – ACR:**

K8s’e User’larin Authenticate Olmasi:

* Create Azure AD server component.
* Create Azure AD client component.
* Deploy the cluster.
* Create RBAC binding.
* Access cluster with Azure AD

secureValue: Containerdeki secureValue’ye yalniz container’den; Value’ye hem portal hem de container’den ulasilabilir.

groupMembershipClaims: K8s manifestinde cluster’in domaine baglanabilmesi icin doldurulmali.

ACR’de Scan: Vulnerabilities’e karsi enable edildikten sonraki yeni veya modified Linux imageler scan edilir. Standard tier olmali.

Ingress Controller: is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services by using a single IP address.

Container Network Interface (CNI) Plug-In: Containerlere Vnet’ten ayri ayri IP atar ve Resource’larla gorusebilirler. VM’e install edilir. Windows-Linux VM’lerde calisir. Vnet’te endpoint olsa bile container’ler CNI olmadan Storage Account’a ulasamazlar.

Kubernetes RBAC-enabled cluster: Azure AD can only be enabled on Kubernetes RBAC-enabled cluster. Azure AD legacy integration can only be enabled during cluster creation. User’lar icin giris cluster olusturulurken configure edilebilir. Sonra edilemez.

Container Groups: A container group is useful when building an application sidecar for logging, monitoring, or any other configuration where a service needs a second attached process. Within a container group, container instances can reach each other via localhost on any port, even if those ports aren't exposed externally on the group's IP address or from the container.

Content Trust: Kurulmadan oncekileri etkilemez. Sonrakileri ise enabled ise etkiler.

Content Trust: AcrImageSigner, AcrPush rollerinin ikisini tanimlayarak gondeririz. Owner rolu tek basina fazla yetkili.

AcrPush: Hem push hem pull yapabilir. Contributor, Owner daha fazlasini.

Reader: least privileged role which allows for the downloading of images from the Azure Container Registry.

Graphical user interface, application

Description automatically generated

Auto-generated service principal: AKS kurulunca otomatik olarak kurulur. Buna RBAC baglayarak ACR’ye baglantisini kurabiliriz.

Access Policy: Container seviyesinde olusturularak prevent the blobs in container from being modified.

**KEY VAULT:**

Enable Disk Encryption:

Azure Disk Encryption, Azure Resource Manager veya Azure VM for deployments configure edilebilir.

* vault1 > Properties > Access policies
* Enable access to: Azure Disk Encryption for volume encryption
* Run Set-AzVMDiskEncryptionExtension

Access Policies: Disk encryption yapip vm1’in Azure Backup’ini desteklemesi icin configure edilmeli.

RBAC: Vault PIM kullanmaz. RBAC ve Azure Key Vault access policies’in combination’u kullanir.

Soft Delete: Key, Secret soft delete varsa recover edilebilir ama Policy edilemez. Soft delete durumundaki Key ve Secret ile ayni isimli key ve secret olusturulamaz.

Parameters File: When ARM templates need multiple deployments of identically configured VMs. Name of the key vault and the name of the secret will be provided as inline parameters.

Linked template: can dynamically generate a resource ID that will designate the key vault containing appropriate secret during deployment of each identically configured VM.

APP’i Vault’a Yetkilendirme: Just register an Azure AD App then go to API Permissions and select Azure Key Vault, you will find a single permission to add "user\_impersonation" under Delegated Permissions without Admin Consent.

Delegate Access to Another User for Vault: Owner ve User Access Administrator yapabilir. Security Admin yapamaz.

Admin ARM Template ile Resource Deploy Ederken Vault Secret’a Access Edebilmesi:

* vault1 > Properties > Access policies
* Enable access to: ARM for template deployment – check | Save

User1’i Key Vault’a Yetkilendirme:

* vault1 > Properties > Access control > Add a role assignment > Add
* Select: Key Vault Secrets Officer role | Select: User1 | Save

User1’e Secret-Keys Bazinda Delete, Get, List, Backup Yetkisi Verme: Secret, Certificate, Key permissions verilebilir.

* vault1 > Properties > Access policies > Add access policy
* Secret permissions: Get, List, Backup > Select principal: User1

Secrets: support backing up VM1 by using Azure Backup.

Restore Secret Backup to Another Vault: Ayni Geography (farkli region olabilir) ve ayni Subs icindeyse restore edilebilir. Key ve Secret icin de gecerlidir.

Azure Disk Encryption: Key Vault ve VM ayni Region’da olmali. VMs, Standard tier olmali. 2GB’dan fazla RAM olmali. Type: A, D, DS, G, GS, F, and so on.

Customer Managed Key: Azure Files, Azure Blob storage support data encryption by using the keys stored in the key vault.

**MONITOR:**

Metric Signal Type: Metric alerts in Azure Monitor provide a way to get notified when one of your metrics cross a threshold. Metric alerts work on a range of multi-dimensional platform metrics, custom metrics, Application Insights standard and custom metrics. The performance counter directly linked to the Metric signal type.

Automatic Provisioning: Azure Security Center’dan turn on edilir. VM’lere Microsoft Monitoring Agent install edilmeli. Linux ve Windows’a da yuklenebilir.

Alert Olusturma: Azure Monitor ve Azure Sentinel’de alert olusturulabilir.

Activity Log: Start, stop, log in vb kayitlari gosterir.

Logs: Security eventlerini analyse edebiliriz.

Azure Resource Manager template: to deploy the Microsoft Monitoring Agent to all the servers automatically.

Log Analytics Workspace: Monitor’de security alert olusturmak icin ilk olusturulur.

**PRIVILEGED IDENTITY** **MANAGEMENT (PIM):**

Privileged Identity Management (PIM): to secure Azure AD roles. Kullanabilmek icin:

> Consent to PIM

> Verify your identity by using multi-factor authentication (MFA)

> Sign up PIM for Azure AD roles

User Can Only Activate Sec Admin Role in 5 Hours: No

JIT: VM’e enable edildikten sonra calismasi icin Subnet veya VM’e NSG bagli olmali. Basic veya Standard Load balancer olmasi farketmez. NSG bagli degilse unsupported ikazi verir.

Identical Role Assignment: PIM kullanilirsa Subs’lara Identical Role Assignment yapar,

Privileged Role Administrator or Global Administrator: role can manage privileged assignments for other administrators.  
Global Administrators, Security Administrators, Global Readers, and Security Readers: can also view assignments to Azure AD roles in PIM.

VM’e JIT ile Baglanmak icin Gerekli Role-Based Access:

“Microsoft.Security/locations/jitNetworkAccessPolicies/initiate/action”

“Microsoft.Compute/virtualMachines/read”.

**ROLES – RBAC:**

Members of a security group can include users, devices, other groups, and service principals, which define access policy and permissions.

Owners of a security group: can include users and service principals.

Members of a Microsoft 365 group: can only include users. Group uye olamaz.

Built-in AD roles: can't be cloned, but

Built-in subscription roles: can be cloned.

Custom roles: of either type can be cloned (Azure AD, Azure Subscription).

Azure AD Global Administrator account: used to create the Azure AD Connector account and configure Azure AD.

Group Naming Policy: Eger bir isim yasakli ise Group name olarak her iki Microsoft 365 ve Security Group’da da Global Admin ve User Admin istisna olurlar. Security Group/Mic 365 Group farketmez.

Billing Administrator: Only the billing administrator of an account can transfer ownership of a subscription from Azure Account Center. Ilgili email adresi yazilarak devredilir.

User Access Administrator: performs role assignment or views the list of assignments.

Dynamic User: Hem Security Group hem de Microsoft 365 Group Type’lara kurulabilir.

Dynamic Group: You can create a dynamic group for devices or for users, but you can't create a rule that contains both users and devices.

Bastion Ports: Ingress traffic from public internet: 443, ports to target VM subnet: 3389

Microsoft 365 Group: Security Group’a uye olamaz.

Subscription’u Baska Tenant’a Tasima: Subs level role assignments ve VM managed identities are lost.

Application Developer: can register app in AAD. Oncesinde app, enterprise application olarak eklenmeli. Token encryption’i enable etmek icin de enterprise application gerekli.

Retention of Deleted User/Group: 1 ay icinde restore edilebilirler. Security Group asla geri cagrilamaz.

Virtual Machine Administrator Login: View Virtual Machines in the portal and login as administrator. It can’t reset the password of built-in Administrator account of VM2.

Key Vault Contributor: Owner ile birlikte can configure network access to Key Vault.

Owner: Only owner can change permissions on resources. Or User Access Administrator.

Owner: can transfer ownership of a subscription to another Tenant. Account Admin de.

Microsoft.Network: Manages Bastion, Application Security Groups.

Microsoft.Compute/\*: Yalniz VM’leri komuta eder. VM’leri Vnet’e baglayamaz. Web app, Container instance’yi calistiramaz.

Identity Store for File Share: Azure file share icin Azure AD only. Folders in file share icin Azure AD ve AD DS.

Storage Account Access:

* Blob storage: Shared key, SAS, Azure AD
* File share: Shared key
* Tables: Shared key, SAS, Azure AD

Bulk Add Members: the user principal name (UPN) and display name of each user file’a yazilir.

Role Atama User’lara:

* Create Json file
* Run the New-AzRoleDefinition cmdlet
* Run the New-AzRoleAssignment cmdlet

**SENTINEL:**

Playbook: to automate mitigation of incidents in Sentinel. Minimum administrative effort. Sentinel’de Kusto Query language ile olusturulan query’lere automate response verir.

Custom Alert Rules: olusturmak icin Sentinel’de LA workspace olusturulur. Pricing tier of Security center Standard yapilir.

Analytics: Sentinel threat identify edilince incident olusturur.

Playbooks: a ticket is logged in service management platform when an incident is created in Sentinel.

Modify Mevcut Playbook: Condition veya action eklenebilir.

* Playbook1 > Azure Logic Apps Designer

Logic Apps Designer: You can modify automation to send email to User1/distribution group.

Azure Logic App: create a workflow automation in Azure Security Center that will automatically remediate a security vulnerability.

**STORAGE ACCOUNT:**

Shared Access Signature (SAS): File service, Blob Service baglanabilir. Blob’a Azure portal veya Azure Storage Explorer vasitasiyla baglanilabilir. File service’e Azure Storage Explorer.

Storage Explorer: Retrieve diagnostics logs saved in blob container for Azure Storage account. Hem blob hem file share’e ulasilabilir.

AzCopy: Retrieve diagnostics logs saved in a blob container for an Azure Storage account.

AzCopy: ile log data’larini analiz icin download edebilecegimiz Azure command line tool’dur.

DataActions[]: Blob level’da calisir. Azure Storage Level’da calismaz. Read a list of blobs in a container. Write a storage blob in a container. Delete a message in a queue. Data plane actions.

Actions[]: Azure Storage Account level’da calisir. Manage access to storage account. Create, update or delete a blob container. Delete a resource group and its resources. Control plane actions.

File Shares: Verify that identity-based authentication over SMB is enabled

Share Access Signature: Only grant users access to contoso2023 mi kontrol edilebilir.

Ilgili Vnet/Subnet’e Izin Verme: Vnet uzerinden baglanabilmek icin ilgili Subnet’te Microsoft.Storage Service Endpoint de olmali.

* Storage Account1 > Firewalls and virtual networks > allow access from selected networks > Add existing vnet: vnet2 > Select: Subnet2

Prevent HTTP Connections to Storage Account:

* storageacc1 > Configuration > Secure transfer required - Enabled

Storage Account’u Encrypt Etme:

* storageacc1 > Encryption > Use your own key – check
* Key vault: vault1 | Encryption key: key1 | Save

Network Watcher’s NSG flow log: capability you can log data to an Azure Storage Account for network traffic that flows through a NSG for many VMs.

**UPDATE MANAGEMENT:**

Update Deployment: can apply to Windows VMs or Linux VMs but not both. The VMs can be in different regions, different subscriptions and different resource groups.

Update Management: VM’ler Stop olmamali. Ayni anda ya Windows ya Linux VM’ler icin update management kurulabilir.

Dynamic Group Query: Update Management in Azure Automation’da kurulur: Minimizes the need to edit deployment to update machines; Automatic updates for VMs. VM grubudur. Azure veya disinda kurulabilir.

**WEB-APP:**

App assignments: User3 is in Group3 that is a member of Group2, but nested groups aren't supported in App assignments so only direct Group 2 members will see the app and work. Owner da gorebilir.

Application Registration: Application Object ve Service Principal Object olusur. Azure AD user’larini, Microsoft Graph kullanarak modify edebilir.

WEBSITE\_LOAD\_CERTIFICATES: Web app1’e yuklenen certifikate’in app code tarafindan ulasilabilmesi icin: add an app setting to web app1 configuation.

App1 > Self-service: Allow users to request access to this application.

App1 > Roles and administrators: Here you can assign User2 to the role.

Grant tenant-wide Admin Consent: Global Admin, Privileged Role Admin, Cloud Application Admin, Application Administrator. A user can also be authorized to grant. Apps’leri publish etmeden once grant etmek icin yetkili roller.

Self-Service App Access: Ilk default yazilan (GroupX) dogrudan girer. Allow users to request: Yes ve To which group: GroupY durumunda, talepte bulunanlarla GroupX ve GroupY girebilir.

Owner of Group: Self-Service App Access durumunda Owner degismez.

Application Security Group’u NIC’e Ekleme: > VM1 > Networking > Configure application security groups > Select: appsec1

Application Insights: Webapp, Oauth 2.0 authenticate ediliyorsa yeni web test’i unattended olarak eklemek icin .webtest file Application Insights’a upload edilir.

Redirect URI: Webapp1 uses Oauth 2 implicit grant to acquire Azure AD access tokens. To register webapp1 in Azure AD we use it.

App Registration and Generate a Password for Web App:

* Azure AD > App reg > New reg
  + Name | account type: only this org directory | app type: web | URI: <https://contoso.org/exampleapp>
* Certificates & Secrets
  + Client secrets > New client secret
  + Description | Duration

Enable Users to Authenticate to Web App with Azure AD:

* webapp1 > Properties > Authentication
* App service authentication: On
* Action to take request when request is not authentication: Log with Azure AD

Azure AD Authentication for Web Application: Client ID, Tenant ID gerekli.

WAF: Web App’a dogrudan WAF baglanamaz. Ya Front Door ya da Application Gateway’a baglanabilir.

Web App CosmosDb Azure AD Baglantisi:

* CosmosDb’de; authenticate Azure AD users and generate resource tokens.
* WebApp’de: authenticate Azure AD users and relay resource token.

**WORKSPACE:**

Microsoft Monitoring Agent: Azure Resource Manager template can deploy many servers automatically with WorkspcaeID and WorkspaceKey.

Computer Group: 500 vm’e workspace yuklu ama Update Assessment Solution’in workspace’e sadece 100 vm’in log’larini cekmek icin Computer group kurulur.

* Create a computer group
* Create a scope configuration
* Apply the scope configuration to the solution

Workspace: Kusto Query Lang ile loglara sorgulama yapilabilir ve 1 yil saklar. Tum Region

Audit Log Destination for LA Workspace: Anywhere

Audit Log Destination for Storage Account: Storage account ile diger storage account ayni region’da olmali. General Purpose V1, Blob hepsi olur. Cool da kullanilabilir.

Linux Diagnostic Extension (LAD) 3.0: Linux VM’lerin metric ve log’larini monite etmede kullanilir.

LA Workspace: Ilgili resource VM’un ornegin tum audit failure data’sini security log’tan alip Storage account’a aktarir.

LA Workspace Agent’in VM’e Yuklenmesi:

* LA Workspaces > Create new > wrsp1 > OK
* wspc1 > Data sources: Virtual machines > Select: vm3
* Connect (vm3 connect edilir. Boylece agent yuklenir.)

LA Workspace’in Manual Olarak On-prem VM’e Yuklenmesi:

* wspc1 > Agents management > Windows servers > Download Windows Agent
* Install Agent > Workspace ID | Workspace Key: Primary key | Install

Loglarin VM’lerden Cekilmesi: Agent yuklendikten sonra Windows event logs, Windows performance counters, Linux performance counters veya syslogs secilip configure edilerek cekilir.

* wscp1 > Agents configuration > Windows performance counters
  + + add performance counter > Performance counter name: Memory
  + Sample rate: 60 | Apply
* wscp1 > Agents configuration > Windows event logs
  + + Add windows event log > Log name: System | Error, Warning, Info – check
  + Apply

**AZURE ACTIVE DIRECTORY:**

Password hash synchronization: requires the least effort regarding deployment, maintenance, and infrastructure. This level of effort typically applies to organizations that only need their users to sign into Office 365, SaaS apps, and other Azure AD-based resources. When turned on, password hash synchronization is part of the Azure AD Connect sync process and runs every two minutes.

A federated authentication system: relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD. It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load.

Pass-through authentication: you need one or more (we recommend three) lightweight agents installed on existing servers. These agents must have access to your on-premises Active Directory Domain Services, including your on-premises AD domain controllers. They need outbound access to the Internet and access to your domain controllers. For this reason, it's not supported to deploy the agents in a perimeter network.

Pass-through Authentication with SSO: password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.

Password Hash Syncronization with SSO: Server ihtiyaci en azdir. User logon restrictions apply to user accounts which are synced to tenant.

Password Hash Synchronization: cannot support the password policies and user logon limitations.

Active Directory Integrated Authentication: Bir Federated domain’den Azure AD credentials ile Windows’a log in olabilirsiniz veya managed domain that is configured seamless sign-on for pass-through and password hash authentication.

On-prem AD account’u ile Azure AD’ye baglanilabilir SQL’e ulasilabilir.

Synchronization Rules Editor: After on-prem sync all on-premises identities to Azure AD.  
You can prevent users who have a givenName attribute that starts with TEST from being synced to Azure AD. Global Admin ve User Admin kuralin disina cikabilir. Microsoft 365 group/Security group farketmez.

Enable HTTPS After Migration: Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using AES256 / DES

HTTPS: Ilgili web app’i domainname’e baglamak icin web app’e bir hostname verilir ve PFX file upload edilir.

Domain name Atama:

A root "A" record pointing to contoso.com  
A root "TXT" record for verification  
A "CNAME" record for the www name that points to the A record  
F: To use HTTPS, you need to upload a PFX file to the Azure Web App. The PFX file will contain the SSL certificate required for HTTPS.

External collaboration settings: modifiye edilerek external user’in [user2@outlook.com](mailto:user2@outlook.com) vb adresi ile AAD Tenant’a davet edilmesini configure eder. Users blade’te bulunur. User administrator role can invite external partner to tenant.

AAD Global Administrator: is used to create the Azure AD Connector account and configure Azure AD from Azure AD Connect. Ayrica modify da eder.

Express Settings installation in Azure AD Connect: Global Admin role, Enterprise Admins group yapabilir.

Group Olusturma: Global administrator ve User administrator olusturabilir Security/Microsoft 365 farketmez. Group administrator group olusturamaz.

Dynamic Membership Rule:

* -contains “ON” : London, MONTREAL, Kolonya, Anton
* -match “\*on” : London, Anton

