

**Q1) You have a hybrid configuration of Azure Active Directory (Azure AD). You have an Azure HDInsight cluster on a virtual network. You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication. Solution: You deploy Azure Active Directory Domain Services (Azure AD DS) to the Azure subscription. Does this meet the goal?**

☒ Incorrect

**Explanation:-**Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.

Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:

- Create Azure Virtual Network.
- Create a custom DNS server in the Azure Virtual Network.
- Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
- Configure forwarding between the cust

☐ Correct

**Q2) You have Azure Resource Manager templates that you use to deploy Azure virtual machines. You need to disable unused Windows features automatically as instances of the virtual machines are provisioned. What should you use?**

☐ application security groups

☐ Azure Logic Apps

☒ an Azure Desired State Configuration (DSC) virtual machine extension

**Explanation:-**You can use Azure Automation State Configuration to manage Azure VMs (both Classic and Resource Manager), on-premises VMs, Linux machines, AWS VMs, and on-premises physical machines. In this topic, we cover how to register only Azure Resource Manager VMs.

Azure Automation State Configuration provides a DSC pull server similar to the Windows Feature DSC-Service so that 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. Azure Automation can target virtual or physical Windows or Linux machines, in the cloud or on-premises.

Link - <https://docs.microsoft.com/en-us/azure/automation/tutorial-configure-servers-desired-state>

☐ device configuration policies in Microsoft Intune

**Q3) You create a new Azure subscription. You need to ensure that you can create custom alert rules in Azure Security Center. Which two actions should you perform?**

☐ Onboard Azure Active Directory (Azure AD) Identity Protection.

☒ Create an Azure Storage account.

**Explanation:-**You need write permission in the workspace that you select to store your custom alert.

☐ Implement Azure Advisor recommendations.

☒ Create an Azure Log Analytics workspace.

**Explanation:-**You need write permission in the workspace that you select to store your custom alert.

**Q4)**

**Fabrikam Inc. has adopted Azure as their cloud platform. Fabrikam currently has a hybrid identity model which is supported by ADConnect. Within the Azure environment there is 1 subscription labeled "Fab-Prod" which has a resource group labeled "Back-Office". The "Back-Office" resource group has the following resources:**

1. "ADConnect" VM is running on a standard A2M spec VM

2. "VPN-Gateway" is the VPN gateway which is configured for Site-to-Site VPN (Azure to on-premises)

There are 250 Azure Active Directory user accounts which has the Office E5 licenses assigned to each user individually. The Azure tenant is configured for Privilege Identity Management and has 3 global administrator accounts (Admin01, Admin02 and Admin03) enrolled which is used to manage the environment, these administrator accounts have EMS E5 license associated to each account. Admin01 is the subscription owner for the "Fab-Prod" subscription and permissions are handled via Privilege Identity Management (PIM). You create an additional administrator account labeled "Admin04" as a normal Azure AD user. This account should be eligible for "Global Administrator" access via Privilege Identity Management for safekeeping and auditing purposes.

**Solution:** You enroll "Admin04" as an Azure AD role member with the global admin permission.

**Does this solution meet the goal?**

☐ Incorrect

☒ Correct

**Q5)**

**Fabrikam Inc. has adopted Azure as their cloud platform. Fabrikam currently has a hybrid identity model which is supported by ADConnect. Within the Azure environment there is 1 subscription labeled "Fab-Prod" which has a resource group labeled "Back-Office". The "Back-Office" resource group has the following resources:**

1. "ADConnect" VM is running on a standard A2M spec VM

2. "VPN-Gateway" is the VPN gateway which is configured for Site-to-Site VPN (Azure to on-premises)

There are 250 Azure Active Directory user accounts which has the Office E5 licenses assigned to each user individually. The Azure tenant is configured for Privilege Identity Management and has 3 global administrator accounts (Admin01, Admin02 and Admin03) enrolled which is used to manage the environment, these administrator accounts have EMS E5 license associated to each account. Admin01 is the subscription owner for the "Fab-Prod" subscription and permissions are handled via Privilege Identity Management (PIM). You need to enroll "Admin02" into PIM so that the administrator is eligible to manage resources in

the "Fab-Prod" subscription for a maximum of 8-hour time period. Admin02 requires full access to all resources within the subscription however he should not be able to add additional role assignments to the subscription.

Which role should you assign to Admin02?

- ☐ Security administrator role
- ☒ Contributor role
- ☐ Reader role
- ☐ Owner role

Q6)

Fabrikam Inc. has adopted Azure as their cloud platform. Fabrikam currently has a hybrid identity model which is supported by ADConnect. Within the Azure environment there is 1 subscription labeled "Fab-Prod" which has a resource group labeled "Back-Office". The "Back-Office" resource group has the following resources:

1. "ADConnect" VM is running on a standard A2M spec VM
2. "VPN-Gateway" is the VPN gateway which is configured for Site-to-Site VPN (Azure to on-premises)

There are 250 Azure Active Directory user accounts which has the Office E5 licenses assigned to each user individually. The Azure tenant is configured for Privilege Identity Management and has 3 global administrator accounts (Admin01, Admin02 and Admin03) enrolled which is used to manage the environment, these administrator accounts have EMS E5 license associated to each account. Admin01 is the subscription owner for the "Fab-Prod" subscription and permissions are handled via Privilege Identity Management (PIM). You plan on rolling out Microsoft Intune to a control group of 20 random users. You need to assign EMS E3 licenses for all users which are part of the control group, this process should be scalable going forward and make license management for Intune users as easy as possible.

**Solution:** Create a new security group with an assigned membership type and configure group-based licensing.

Does this solution meet the goal?

- ☐ Incorrect
- ☒ Correct

Q7)

Fabrikam Inc. has adopted Azure as their cloud platform. Fabrikam currently has a hybrid identity model which is supported by ADConnect. Within the Azure environment there is 1 subscription labeled "Fab-Prod" which has a resource group labeled "Back-Office". The "Back-Office" resource group has the following resources:

1. "ADConnect" VM is running on a standard A2M spec VM
2. "VPN-Gateway" is the VPN gateway which is configured for Site-to-Site VPN (Azure to on-premises)

There are 250 Azure Active Directory user accounts which has the Office E5 licenses assigned to each user individually. The Azure tenant is configured for Privilege Identity Management and has 3 global administrator accounts (Admin01, Admin02 and Admin03) enrolled which is used to manage the environment, these administrator accounts have EMS E5 license associated to each account. Admin01 is the subscription owner for the "Fab-Prod" subscription and permissions are handled via Privilege Identity Management (PIM). You have been tasked to better manage all user accounts per department in the Azure AD tenant. You plan to group all user accounts automatically by using a dynamic group membership called ?Dynamic-Guests?.

Which of the following criteria is the best to identify these accounts as the below information has been set for all users? Select 2 methods.

- ☒ Department
- ☐ Location
- ☐ Manager
- ☒ Job title

Q8)

Fabrikam Inc. has adopted Azure as their cloud platform. Fabrikam currently has a hybrid identity model which is supported by ADConnect. Within the Azure environment there is 1 subscription labeled "Fab-Prod" which has a resource group labeled "Back-Office". The "Back-Office" resource group has the following resources:

1. "ADConnect" VM is running on a standard A2M spec VM
2. "VPN-Gateway" is the VPN gateway which is configured for Site-to-Site VPN (Azure to on-premises)

There are 250 Azure Active Directory user accounts which has the Office E5 licenses assigned to each user individually. The Azure tenant is configured for Privilege Identity Management and has 3 global administrator accounts (Admin01, Admin02 and Admin03) enrolled which is used to manage the environment, these administrator accounts have EMS E5 license associated to each account. Admin01 is the subscription owner for the "Fab-Prod" subscription and permissions are handled via Privilege Identity Management (PIM). You are tasked to secure all guest user identities by only allowing logging into Microsoft Teams via Windows and blocking sign ins from Android and iOS. When logging in the guest users must also use MFA.

Which technology should you implement to accomplish this goal?

- ☐ Identity Protection
- ☐ Privilege Identity Management
- ☒ Conditional Access

Q9)

Fabrikam Inc. has adopted Azure as their cloud platform. Fabrikam currently has a hybrid identity model which is supported by ADConnect. Within the Azure environment there is 1 subscription labeled "Fab-Prod" which has a resource group labeled "Back-Office". The "Back-Office" resource group has the following resources:

1. "ADConnect" VM is running on a standard A2M spec VM
2. "VPN-Gateway" is the VPN gateway which is configured for Site-to-Site VPN (Azure to on-premises)

There are 250 Azure Active Directory user accounts which has the Office E5 licenses assigned to each user individually. The Azure tenant is configured for Privilege Identity Management and has 3 global administrator accounts (Admin01, Admin02 and Admin03) enrolled which is used to manage the environment, these administrator accounts have EMS E5 license associated to each account. Admin01 is the subscription owner for the "Fab-Prod" subscription and permissions are handled via Privilege Identity Management (PIM).Correct or Incorrect:

You can configure an Azure Conditional Access policy for client applications like Microsoft Word.

- ☒ Incorrect  
☐ Correct

#### Q10)

Fabrikam Inc. has adopted Azure as their cloud platform. Fabrikam currently has a hybrid identity model which is supported by ADConnect. Within the Azure environment there is 1 subscription labeled "Fab-Prod" which has a resource group labeled "Back-Office". The "Back-Office" resource group has the following resources:

1. "ADConnect" VM is running on a standard A2M spec VM
2. "VPN-Gateway" is the VPN gateway which is configured for Site-to-Site VPN (Azure to on-premises)

There are 250 Azure Active Directory user accounts which has the Office E5 licenses assigned to each user individually. The Azure tenant is configured for Privilege Identity Management and has 3 global administrator accounts (Admin01, Admin02 and Admin03) enrolled which is used to manage the environment, these administrator accounts have EMS E5 license associated to each account. Admin01 is the subscription owner for the "Fab-Prod" subscription and permissions are handled via Privilege Identity Management (PIM).You are planning on rolling out a new Azure AD Conditional Access policy to restrict access to only specific device platforms.

Which of the following device platforms are supported by conditional access? Choose all that apply.

- ☒ All of these  
☐ macOS  
☐ Windows Phone  
☐ iOS  
☐ Android

#### Q11)

Fabrikam Inc. has adopted Azure as their cloud platform. Fabrikam currently has a hybrid identity model which is supported by ADConnect. Within the Azure environment there is 1 subscription labeled "Fab-Prod" which has a resource group labeled "Back-Office". The "Back-Office" resource group has the following resources:

1. "ADConnect" VM is running on a standard A2M spec VM
2. "VPN-Gateway" is the VPN gateway which is configured for Site-to-Site VPN (Azure to on-premises)

There are 250 Azure Active Directory user accounts which has the Office E5 licenses assigned to each user individually. The Azure tenant is configured for Privilege Identity Management and has 3 global administrator accounts (Admin01, Admin02 and Admin03) enrolled which is used to manage the environment, these administrator accounts have EMS E5 license associated to each account. Admin01 is the subscription owner for the "Fab-Prod" subscription and permissions are handled via Privilege Identity Management (PIM).The security department has requested that when configuring Single Sign On (SSO) for hybrid users that all user passwords are passed through the on-premises Active Directory domain controller for validation.

Solution: You configure Password Hash Sync and enable single sign on (SSO) with the ADConnect tool.

Does this solution meet the goal?

- ☒ Incorrect  
☐ Correct

#### Q12)

Fabrikam Inc. has adopted Azure as their cloud platform. Fabrikam currently has a hybrid identity model which is supported by ADConnect. Within the Azure environment there is 1 subscription labeled "Fab-Prod" which has a resource group labeled "Back-Office". The "Back-Office" resource group has the following resources:

1. "ADConnect" VM is running on a standard A2M spec VM
2. "VPN-Gateway" is the VPN gateway which is configured for Site-to-Site VPN (Azure to on-premises)

There are 250 Azure Active Directory user accounts which has the Office E5 licenses assigned to each user individually. The Azure tenant is configured for Privilege Identity Management and has 3 global administrator accounts (Admin01, Admin02 and Admin03) enrolled which is used to manage the environment, these administrator accounts have EMS E5 license associated to each account. Admin01 is the subscription owner for the "Fab-Prod" subscription and permissions are handled via Privilege Identity Management (PIM).Currently the on-premises identities are synced to Azure AD via the ADConnect tool installed on the "ADConnect" server which is connected to the on-premises network via the Site-to-Site VPN. The ADConnect tool has been configured and has been syncing identities for the past month without issue, however you received an email message saying?

Azure Active Directory (Azure AD) didn't register a synchronization attempt in the last 24 hours.

What could be the cause?

- ☐ Directory synchronization service has stopped
- ☒ All of these
- ☐ The admin account used for directory synchronization was changed
- ☐ There are network connection issues
- ☐ The work or school account used in the configuration wizard to setup directory synchronization has been deleted, disabled or password expired

Q13)

Fabrikam Inc. has adopted Azure as their cloud platform. Fabrikam currently has a hybrid identity model which is supported by ADConnect. Within the Azure environment there is 1 subscription labeled "Fab-Prod" which has a resource group labeled "Back-Office". The "Back-Office" resource group has the following resources:

1. "ADConnect" VM is running on a standard A2M spec VM
2. "VPN-Gateway" is the VPN gateway which is configured for Site-to-Site VPN (Azure to on-premises)

There are 250 Azure Active Directory user accounts which has the Office E5 licenses assigned to each user individually. The Azure tenant is configured for Privilege Identity Management and has 3 global administrator accounts (Admin01, Admin02 and Admin03) enrolled which is used to manage the environment, these administrator accounts have EMS E5 license associated to each account. Admin01 is the subscription owner for the "Fab-Prod" subscription and permissions are handled via Privilege Identity Management (PIM). You have been requested to evaluate the security posture of all identities in Azure Active Directory. You need to provide the following information per user:

Risk level  
Risk events  
Current status

**Solution:** You configure Azure AD Identity Protection.

Does this solution meet the goal?

- ☐ Incorrect
- ☒ Correct

Q14)

Fabrikam Inc. has adopted Azure as their cloud platform. Fabrikam currently has a hybrid identity model which is supported by ADConnect. Within the Azure environment there is 1 subscription labeled "Fab-Prod" which has a resource group labeled "Back-Office". The "Back-Office" resource group has the following resources:

1. "ADConnect" VM is running on a standard A2M spec VM
2. "VPN-Gateway" is the VPN gateway which is configured for Site-to-Site VPN (Azure to on-premises)

There are 250 Azure Active Directory user accounts which has the Office E5 licenses assigned to each user individually. The Azure tenant is configured for Privilege Identity Management and has 3 global administrator accounts (Admin01, Admin02 and Admin03) enrolled which is used to manage the environment, these administrator accounts have EMS E5 license associated to each account. Admin01 is the subscription owner for the "Fab-Prod" subscription and permissions are handled via Privilege Identity Management (PIM). You have been requested to create a new Azure AD application labeled "Office365-logging" which needs to retrieve information about user, admin and policy actions and events from Office 365. This app needs to support both work and school accounts including personal Microsoft accounts.

**Solution:** You create an Azure AD V1.0 endpoint

Does this solution meet the goal?

- ☒ Incorrect
- ☐ Correct

Q15) You have an Azure Active Directory (Azure AD) tenant named Adatum and an Azure Subscription named Subscription1. Adatum contains a group named Developers. Subscription1 contains a resource group named Dev.

You need to provide the Developers group with the ability to create Azure logic apps in the Dev resource group.

**Solution:** On Subscription1, you assign the DevTest Labs User role to the Developers group.

Does this meet the goal?

- ☒ Incorrect

**Explanation:-**The DevTest Labs User role lets you connect, start, restart, and shutdown your virtual machines in your Azure DevTest Labs.

References: <https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#devtest-labs-user>

- ☐ Correct

Q16) You have an on-premises Active Directory domain named contoso.com.

You install and run Azure AD Connect on a server named Server1 that runs Windows Server.

You need to view Azure AD Connect events.

You use the Application event log on Server1.

Does that meet the goal?

- ☐ Incorrect
- ☒ Correct

**Explanation:-**References: <https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance>

Q17) You have an Azure subscription named Subscription1. Subscription1 contains a resource group named RG1. RG1 contains

resources that were deployed by using templates.  
You need to view the date and time when the resources were created in RG1.  
**Solution:** From the RG1 blade, you click Deployments.  
**Does this meet the goal?**

- ☐ Incorrect  
☒ Correct

**Q18) You company has an Azure subscription named Sub1. Sub1 contains an Azure web app named WebApp1 that uses Azure Application Insights. WebApp1 requires users to authenticate by using OAuth 2.0 client secrets. Developers at the company plan to create a multi-step web test app that preforms synthetic transactions emulating user traffic to Web App1.**

**You need to ensure that web tests can run unattended.  
What should you do first?**

- ☒ Upload the .webtest file to Application Insights.  
☐ In Microsoft Visual Studio, modify the .webtest file.  
☐ Add a plug-in to the web test app.  
☐ Register the web test app in Azure AD.

**Q19)**

**You have a hybrid configuration of Azure Active Directory (Azure AD).**

**You have an Azure HDInsight cluster on a virtual network.**

**You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.**

**You need to configure the environment to support the planned authentication.**

**Solution:** You create a site-to-site VPN between the virtual network and the on-premises network.

**Does this meet the goal?**

- ☐ Incorrect  
☒ Correct

**Explanation:-**You can connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.

Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:

- Create Azure Virtual Network.
- Create a custom DNS server in the Azure Virtual Network.
- Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
- Configure forwarding between the custom DNS server and your on-premises DNS server.

References: <https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network>

**Q20) You have a Microsoft 365 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.**

**You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:**

- **Source Anchor:** objectGUID
- **Password Hash Synchronization:** Disabled
- **Password writeback:** Disabled
- **Directory extension attribute sync:** Disabled
- **Azure AD app and attribute filtering:** Disabled
- **Exchange hybrid deployment:** Disabled
- **User writeback:** Disabled

**You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.**

**Solution:** You modify the Password Hash Synchronization settings.

**Does that meet the goal?**

- ☒ Correct

**Explanation:-**Protect against leaked credentials and add resilience against outages If your organization uses a hybrid identity solution with pass-through authentication or federation, then you should enable password hash sync for the following two reasons: The Users with leaked credentials report in the Azure AD management warns you of username and password pairs, which have been exposed on the "dark web." An incredible volume of passwords is leaked via phishing, malware, and password reuse on third-party sites that are later breached. Microsoft finds many of these leaked credentials and will tell you, in this report, if they match credentials in your organization – but only if you enable password hash sync!

- ☐ Incorrect

**Q21) You have an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.**

**You need to use automatically generated service principal for the AKS cluster to authenticate to the Azure Container Registry.  
What should you create?**

- ☐ an Azure Active Directory (Azure AD) group  
☒ a role assignment

**Explanation:-**References: <https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal>

- ☐ an Azure Active Directory (Azure AD) user  
☐ a secret in Azure Key Vault

**Q22)**

**You have an Azure Active Directory (Azure AD) tenant named Adatum and an Azure Subscription named Subscription1. Adatum contains a group named Developers. Subscription1 contains a resource group named Dev.**

**You need to provide the Developers group with the ability to create Azure logic apps in the Dev resource group.**

**Solution:** On Dev, you assign the Logic App Contributor role to the Developers group.  
**Does this meet the goal?**

 Incorrect

**Explanation:-**The Logic App Contributor role lets you read, enable and disable logic app.

References: <https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#logic-app-contributor>

 Correct





**Q23) You configure Azure AD Connect for Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) for an on-premises network.**

**Users report that when they attempt to access myapps.microsoft.com, they are prompted multiple times to sign in and are forced to use an account name that ends with onmicrosoft.com.**

**You discover that there is a UPN mismatch between Azure AD and the on-premises Active Directory.**

**You need to ensure that the users can use single-sign on (SSO) to access Azure resources.**

**What should you do first?**

-  From on-premises network, deploy Active Directory Federation Services (AD FS).
-  From the server that runs Azure AD Connect, modify the filtering options.
-  From on-premises network, request a new certificate that contains the Active Directory domain name.
-  From Azure AD, add and verify a custom domain name.




**Q24) You have an Azure subscription that contains a virtual machine named VM1.**

**You create an Azure key vault that has the following configurations:**

- **Name:** Vault5
- **Region:** West US
- **Resource group:** RG1

**You need to use Vault5 to enable Azure Disk Encryption on VM1. The solution must support backing up VM1 by using Azure Backup.**

**Which key vault settings should you configure?**

-  Locks
-  Secrets
-  Access policies

**Explanation:-**References: <https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault>

 Keys

**Q25) You have an Azure Active Directory (Azure AD) tenant named Adatum and an Azure Subscription named Subscription1. Adatum contains a group named**

**Developers. Subscription1 contains a resource group named Dev.**

**You need to provide the Developers group with the ability to create Azure logic apps in the Dev resource group.**

**Solution: On Dev, you assign the Contributor role to the Developers group.**

**Does this meet the goal?**

 Correct

**Explanation:-**The Contributor role lets you manage everything except access to resources. It allows you to create and manage resources of all types, including creating Azure logic apps.

References: <https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#contributor>

 Incorrect

**Q26) You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.**

**An administrator named Admin1 has access to the following identities:**

**An OpenID-enabled user account**




**A Hotmail account**

**An account in contoso.com**

**An account in an Azure AD tenant named fabrikam.com**

**You plan to use Azure Account Center to transfer the ownership of Sub1 to Admin1.**


**To which accounts can you transfer the ownership of Sub1?**

-  contoso.com only
-  contoso.com, fabrikam.com, and Hotmail only
-  contoso.com and fabrikam.com only

**Explanation:-**When you transfer billing ownership of your subscription to an account in another Azure AD tenant, you can move the subscription to the new account's tenant. If you do so, all users, groups, or service principals who had role based access (RBAC) to manage subscriptions and its resources lose their access. Only the user in the new account who accepts your transfer request will have access to manage the resources.

Reference: <https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer>

<https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transferring-subscription-to-an-account-in-another-azure-ad-tenant>

 contoso.com, fabrikam.com, Hotmail, and OpenID-enabled user account

**Q27) You have a Microsoft 365 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.**

**You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:**

**Source Anchor: objectGUID -**

- **Password Hash Synchronization: Disabled**
- **Password writeback: Disabled**
- **Directory extension attribute sync: Disabled**
- **Azure AD app and attribute filtering: Disabled**
- **Exchange hybrid deployment: Disabled**
- **User writeback: Disabled**



**You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.**  
**Solution: You modify the Source Anchor settings.**  
**Does that meet the goal?**

- ☐ Correct
- ☒ Incorrect

---

**Q28) You have an Azure policy as shown in the following exhibit.**  
**What is the effect of the policy?**

- ☒ You can create Azure SQL servers in ContosoRG1 only.
- ☐ You are prevented from creating Azure SQL servers anywhere in Subscription 1.
- ☐ You can create Azure SQL servers in any resource group within Subscription 1.
- ☐ You are prevented from creating Azure SQL Servers in ContosoRG1 only.

---

**Q29) You have an on-premises Active Directory domain named contoso.com.**  
**You install and run Azure AD Connect on a server named Server1 that runs Windows Server.**  
**You need to view Azure AD Connect events.**  
**You use the Directory Service event log on Server1.**  
**Does that meet the goal?**

- ☒ Incorrect
- ☐ Correct

---

**Q30) You set the multi-factor authentication status for a user named admin1@contoso.com to Enabled.**  
**Admin1 accesses the Azure portal by using a web browser.**  
**Which additional security verifications can Admin1 use when accessing the Azure portal?**

- ☐ an app password, a text message that contains a verification code, and a notification sent from the Microsoft Authenticator app
  - ☐ an app password, a text message that contains a verification code, and a verification code sent from the Microsoft Authenticator app
  - ☒ a phone call, a text message that contains a verification code, and a notification or a verification code sent from the Microsoft Authenticator app
- Explanation:-References:** <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>
- ☐ a phone call, an email message that contains a verification code, and a text message that contains an app password

---

**Q31)**

**You have an on-premises Active Directory domain named contoso.com.**  
**You install and run Azure AD Connect on a server named Server1 that runs Windows Server.**  
**You need to view Azure AD Connect events.**  
**You use the Security event log on Server1.**  
**Does that meet the goal?**

- ☒ Incorrect
- Explanation:-References:** <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/tshoot-connect-object-not-syncing>
- ☐ Correct

---

**Q32) You are implementing authentication for applications in your company. You plan to implement self-service password reset (SSPR) and multifactor authentication (MFA) in Azure Active Directory (Azure AD).**  
**You need to select authentication mechanisms that can be used for both MFA and SSPR.**  
**Which two authentication methods should you use? Each correct answer presents a complete solution.**

- ☐ Security questions
  - ☒ Azure AD passwords
- Explanation:-References:** <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>
- ☐ App passwords
  - ☐ Email addresses
  - ☒ Short Message Service (SMS) messages
- Explanation:-References:** <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

---

**Q33)**

**You have a hybrid configuration of Azure Active Directory (Azure AD).**  
**You have an Azure HDInsight cluster on a virtual network.**  
**You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.**  
**You need to configure the environment to support the planned authentication.**  
**Solution: You deploy the On-premises data gateway to the on-premises network.**  
**Does this meet the goal?**

- ☒ Incorrect

**Explanation:-**Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.  
**Note:** To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:

- Create Azure Virtual Network.
- Create a custom DNS server in the Azure Virtual Network.

- Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
- Configure forwarding between the custom DNS server and your on-premises DNS server.

References: <https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network>

☐ Correct

---

**Q34) Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory Azure (Azure AD) tenant named contoso.com.**

**The company develops a mobile application named App1.**

**App1 uses the OAuth 2 implicit grant type to acquire Azure AD access tokens.**

**You need to register App1 in Azure AD.**

**What information should you obtain from the developer to register the application?**

☒ a redirect URI

**Explanation:-**For Native Applications you need to provide a Redirect URI, which Azure AD will use to return token responses.

References: <https://docs.microsoft.com/en-us/azure/active-directory/develop/v1-protocols-oauth-code>

- ☐ an application ID
- ☐ a key
- ☐ a reply URL

---

**Q35) You have a web app named WebApp1 that uses an Azure App Service plan named Plan1. Plan1 uses the D1 pricing tier and has an instance count of 1.**

**You need to ensure that all connections to WebApp1 use HTTPS.**

**What should you do first?**

- ☐ Modify the connection strings for WebApp1.
- ☐ Disable anonymous access to WebApp1.
- ☐ Scale out Plan1.
- ☒ Scale up Plan1.

**Explanation:-**The D1 (Shared) pricing tier does not support HTTPS.

---

**Q36) You have an Azure subscription named Subscription1. Subscription1 contains a resource group named RG1. RG1 contains resources that were deployed by using templates.**

**You need to view the date and time when the resources were created in RG1.**

**Solution: From the Subscription blade, you select the subscription, and then click Resource providers.**

**Does this meet the goal?**

☒ Incorrect

☐ Correct

---

**Q37) You have an Azure subscription named Subscription1. Subscription1 contains a resource group named RG1. RG1 contains resources that were deployed by using templates.**

**You need to view the date and time when the resources were created in RG1.**

**Solution: From the RG1 blade, you click Automation script.**

**Does this meet the goal?**

☒ Incorrect

☐ Correct

---

**Q38) You are securing access to the resources in an Azure subscription.**

**A new company policy states that all the Azure virtual machines in the subscription must use managed disks.**

**You need to prevent users from creating virtual machines that use unmanaged disks.**

**What should you do?**

- ☐ Azure Monitor
- ☐ Azure Security Center
- ☐ Azure Service Health
- ☒ Azure Policy

---

**Q39) You have an Azure web app named webapp1.**

**You need to configure continuous deployment for webapp1 by using an Azure Repo.**

**What should you create first?**

- ☐ an Azure Storage account
- ☐ an Azure Application Insights service
- ☐ an Azure DevTest Labs lab
- ☒ an Azure DevOps organizations

**Explanation:-**To use Azure Repos, make sure your Azure DevOps organization is linked to your Azure subscription.

Reference: <https://docs.microsoft.com/en-us/azure/app-service/deploy-continuous-deployment>

---

**Q40) You need to enforce Microsoft Azure Multi-Factor Authentication (MFA) by using conditional access for all users who are NOT physically present in the office.**

**What should you include in the configuration?**

☒ a named location in Azure Active Directory (Azure AD)

**Explanation:-**References: <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

- ☐ an Azure MFA Server
- ☐ a sign-in risk policy
- ☐ a user risk policy



Q41) You create the following Azure role definition.

```
{
  Name: "Role1",
  Id: "80808080-8080-8080-8080-808080808080",
  IsCustom : false,
  Description: "",
  Actions : [
    Microsoft.Storage/*/read,
    Microsoft.Network/*/read,
    Microsoft.Compute/*/read,
    Microsoft.Compute/virtualMachines/start/action,
    Microsoft.Compute/virtualMachines/restart/action,
    Microsoft.Authorization/*/read],
  NotActions: [],
  DataActions: [],
  NotDataActions: [],
  AssignableScopes: []
}
```

You need to create Role1 by using the role definition.

Which two values should you modify before you create Role1? Each correct answer presents part of solution.

✔ IsCustom

**Explanation:**-Part of example:

IsCustom: true,

AssignableScopes: [

/subscriptions/{subscriptionId1},

/subscriptions/{subscriptionId2},

/subscriptions/{subscriptionId3}]

The following shows what a custom role looks like as displayed in JSON format. This custom role can be used for monitoring and restarting virtual machines.

```
{
  Name: "Virtual Machine Operator",
  Id: "88888888-8888-8888-8888-888888888888",
  IsCustom: true,
  Description: "Can monitor and restart virtual machines.",
  Actions: [
    Microsoft.Storage/*/read,
    Microsoft.Network/*/read,
    Microsoft.Compute/*/read,
    Microsoft.Compute/virtualMachines/start/action,
    Microsoft.Compute/virtualMachines/restart/action,
    Microsoft.Authorization/*/read,
    Microsoft.ResourceHealth/availabilityStatuses/read,
    Microsoft.Resources/subscriptions/resourceGroups/read,
    Microsoft.Insights/alertRules/*,
    Microsoft.Insights/diagnosticSettings/*,
    Microsoft.Support/*
  ],
  NotActions: [],
  DataActions: [],
  NotDataActions: [],
  AssignableScopes: [
    /subscriptions/{subscriptionId1},
    /subscriptions/{subscriptionId2},
    /subscriptions/{subscriptionId3}
  ]
}
```

References: <https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles>

● DataActions

● Description

● Id

✔ AssignableScopes

**Explanation:**-Part of example:

IsCustom: true,

AssignableScopes: [

/subscriptions/{subscriptionId1},

/subscriptions/{subscriptionId2},

/subscriptions/{subscriptionId3}]

The following shows what a custom role looks like as displayed in JSON format. This custom role can be used for monitoring and restarting virtual machines.

```
{
  Name: "Virtual Machine Operator",
  Id: "88888888-8888-8888-8888-888888888888",
  IsCustom: true,
  Description: "Can monitor and restart virtual machines.",
  Actions: [
    Microsoft.Storage/*/read,
    Microsoft.Network/*/read,
    Microsoft.Compute/*/read,
    Microsoft.Compute/virtualMachines/start/action,
    Microsoft.Compute/virtualMachines/restart/action,
```

```
Microsoft.Authorization/*/read,  
Microsoft.ResourceHealth/availabilityStatuses/read,  
Microsoft.Resources/subscriptions/resourceGroups/read,  
Microsoft.Insights/alertRules/*,  
Microsoft.Insights/diagnosticSettings/*,  
Microsoft.Support/*  
],  
NotActions: [],  
DataActions: [],  
NotDataActions: [],  
AssignableScopes: [  
  /subscriptions/{subscriptionId1},  
  /subscriptions/{subscriptionId2},  
  /subscriptions/{subscriptionId3}  
]  
}  
}  
References: https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles
```

---

**Q42) You sign up for Azure Active Directory (Azure AD) Premium.**

**You need to add a user named admin1@contoso.com as an administrator on all the computers that will be joined to the Azure AD domain.**

**What should you configure in Azure AD?**

- ☐ General settings from the Groups blade
- ☐ User settings from the Users blade
- ☒ Device settings from the Devices blade

**Explanation:**-When you connect a Windows device with Azure AD using an Azure AD join, Azure AD adds the following security principles to the local administrators group on the device:

- The Azure AD global administrator role
- The Azure AD device administrator role

The user performing the Azure AD join

In the Azure portal, you can manage the device administrator role on the Devices page. To open the Devices page:

1. Sign in to your Azure portal as a global administrator or device administrator.
2. On the left navbar, click Azure Active Directory.
3. In the Manage section, click Devices.
4. On the Devices page, click Device settings.
5. To modify the device administrator role, configure Additional local administrators on Azure AD joined devices.

References: <https://docs.microsoft.com/en-us/azure/active-directory/devices/assign-local-admin>

- ☐ Providers from the MFA Server blade

---

**Q43) You have an Azure subscription named Sub1 that contains the Azure key vaults shown in the following table:**

**In Sub1, you create a virtual machine that has the following configurations:**

- **Name: VM1**
- **Size: DS2v2**
- **Resource group: RG1**
- **Region: West Europe**
- **Operating system: Windows Server 2016**

**You plan to enable Azure Disk Encryption on VM1.**

**In which key vaults can you store the encryption key for VM1?**

- ☒ Vault1 or Vault3 only

**Explanation:**-In order to make sure the encryption secrets don't cross regional boundaries, Azure Disk Encryption needs the Key Vault and the VMs to be co-located in the same region. Create and use a Key Vault that is in the same region as the VM to be encrypted.

Reference: <https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisites>

- ☐ Vault1, Vault2, Vault3, or Vault4
- ☐ Vault1 or Vault2 only
- ☐ Vault1 only

---

**Q44) You are troubleshooting a security issue for an Azure Storage account.**

**You enable the diagnostic logs for the storage account.**

**What should you use to retrieve the diagnostics logs?**

- ☐ SQL query editor in Azure
- ☐ the Security & Compliance admin center
- ☒ AzCopy

**Explanation:**-References: <https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-logging?toc=%2fazure%2fstorage%2fblobs%2ftoc.json>

- ☐ File Explorer in Windows

---

**Q45) You company has an Azure Active Directory (Azure AD) tenant named contoso.com.**

**You plan to create several security alerts by using Azure Monitor.**

**You need to prepare the Azure subscription for the alerts.**

**What should you create first?**

- ☐ an Azure Automation account
- ☐ an Azure event hub
- ☒ an Azure Log Analytics workspace
- ☐ An Azure Storage account

**Q46) You have an Azure subscription that contains the storage accounts shown in the following table. You enable Azure Advanced Threat Protection (ATP) for all the storage accounts. You need to identify which storage accounts will generate Azure ATP alerts. Which two storage accounts should you identify? Each correct answer presents part of the solution.**

- ☐ storagecontoso4
- ☐ storagecontoso5
- ☒ storagecontoso2

**Explanation:**-Example:

Storage Threat Detection is available for the Blob Service.

References: <https://azure.microsoft.com/en-us/blog/advanced-threat-protection-for-azure-storage-now-in-public-preview/>

- ☐ storagecontoso3
- ☒ storagecontoso1

**Explanation:**-Example:

Storage Threat Detection is available for the Blob Service.

References: <https://azure.microsoft.com/en-us/blog/advanced-threat-protection-for-azure-storage-now-in-public-preview/>

---

**Q47) You have a web app named WebApp1. You create a web application firewall (WAF) policy named WAF1. You need to protect WebApp1 by using WAF1. What should you do first?**

- ☒ Deploy an Azure Front Door.

**Explanation:**-References: <https://docs.microsoft.com/en-us/azure/frontdoor/quickstart-create-front-door>

- ☐ Create an ASG
- ☐ Deploy Azure Firewall.
- ☐ Add an extension to WebApp1.

---

**Q48) You have a hybrid Azure environment. All computers run Windows 10 and are managed by using Microsoft Intune. You need to create a Microsoft Azure Active Directory (Azure AD) conditional access policy that will allow only Windows 10 computers marked as compliant to establish a VPN connection to the on-premises network. What should you do first?**

- ☒ From the Azure Active Directory admin center, create a new certificate

**Explanation:**-Reference: <https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/ad-ca-vpn-connectivity-windows10>

- ☐ Enable Application Proxy in Azure AD
- ☐ From Active Directory Administrative Center, create a Dynamic Access Control policy
- ☐ From the Azure Active Directory admin center, configure authentication methods

---

**Q49) You have an Azure subscription that contains a user named User1 and an Azure Container Registry named ConReg1. You enable content trust for ConReg1. You need to ensure that User1 can create trusted images in ConReg1. The solution must use the principle of least privilege. Which two roles should you assign to User1? Each correct answer presents part of the solution.**

- ☐ AcrQuarantineWriter
- ☐ Contributor
- ☒ AcrPush

**Explanation:**-References: <https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust> <https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles>

- ☐ AcrQuarantineReader
- ☒ AcrImageSigner

**Explanation:**-References: <https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust> <https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles>

---

**Q50) You have an Azure Storage account named storage1 that has a container named container1. You need to prevent the blobs in container1 from being modified. What should you do?**

- ☐ From container1, modify the Access Control (IAM) settings.
- ☐ From storage1, enable soft delete for blobs.
- ☒ From container1, add an access policy.

**Explanation:**-References: <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage?tabs=azure-portal>

- ☐ From container1, change the access level.

---

**Q51) You have an Azure subscription named Subscription1 that is used by several departments at your company. Subscription1 contains the resources in the following table. Another administrator deploys a virtual machine named VM1 and an Azure Storage account named Storage2 by using a single Azure Resource Manager template. You need to view the template used for the deployment. From which blade can you view the template that was used for the deployment?**

- ☒ RG1
- ☐ VM1
- ☐ Storage2
- ☐ Container1

---

**Q52) You have an Azure Active Directory (Azure AD) tenant. All administrators must enter a verification code to access the Azure portal.**

**You need to ensure that the administrators can access the Azure portal only from your on-premises network. What should you configure?**

- ☒ the multi-factor authentication service settings

**Explanation:-**verification code to access needs MFA. References: <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings>

- ☐ the default for all the roles in Azure AD Privileged Identity Management
- ☐ an Azure AD Identity Protection user risk policy
- ☐ an Azure AD Identity Protection sign-in risk policy

---

**Q53) You have an Azure subscription named Sub1 that contains the resources shown in the following table. You need to ensure that you can provide VM1 with secure access to a database on SQL1 by using a contained database user. What should you do?**

- ☒ Enable a managed service identity on VM1.

**Explanation:-**References: <https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/services-support-managed-identities>

- ☐ Create a secret in KV1.
- ☐ Create a key in KV1.
- ☐ Configure a service endpoint on SQL1.

---

**Q54) Your company uses Azure DevOps. You need to recommend a method to validate whether the code meets the company's quality standards and code review standards. What should you recommend implementing in Azure DevOps?**

- ☒ branch policies

**Explanation:-**Branch policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards.

References: <https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azure-devops&viewFallbackFrom=vsts>

- ☐ branch permissions
- ☐ branch locking
- ☐ branch folders

---

**Q55) You have an Azure subscription that contains 10 virtual machines. You need to ensure that you receive an email message when any virtual machines are powered off, restarted, or deallocated. What is the minimum number of rules and action groups that you require?**

- ☐ one rule and three action groups
- ☐ one rule and one action group
- ☐ three rules and three action groups
- ☒ three rules and one action group

---

**Q56) You have an Azure subscription that contains 10 virtual networks. The virtual networks are hosted in separate resource groups. Another administrator plans to create several network security groups (NSGs) in the subscription. You need to ensure that when an NSG is created, it automatically blocks TCP port 8080 between the virtual networks. Solution: You create a resource lock, and then you assign the lock to the subscription. Does this meet the goal?**

- ☐ Correct
- ☒ Incorrect

**Explanation:-**How can I freeze or lock my production/critical Azure resources from accidental deletion? There is way to do this with both ASM and ARM resources using Azure resource lock.

References: <https://blogs.msdn.microsoft.com/azureedu/2016/04/27/using-azure-resource-manager-policy-and-azure-lock-to-control-your-azure-resources/>

---

**Q57) You have an Azure subscription named Sub1. You have an Azure Storage account named Sa1 in a resource group named RG1. Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies. You discover that unauthorized users accessed both the file service and the blob service. You need to revoke all access to Sa1. Solution: You create a lock on Sa1. Does this meet the goal?**

- ☒ Incorrect

**Explanation:-**To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.

- ☐ Correct