Answer Sheet

Q1)

You create an Azure Policy assignment to a subscription.

Which two of the following are valid scope exclusions?

- Initiative
- ✓ Resource

Explanation:-Resource group and resource are valid exclusion scopes if the policy assignment scope is at the subscription level. If you had scoped the assignment to a management group, you could select individual subscriptions within that management group as exclusions, in addition to child resource groups and resources.

- ✓ Resource group

Explanation:-Resource group and resource are valid exclusion scopes if the policy assignment scope is at the subscription level. If you had scoped the assignment to a management group, you could select individual subscriptions within that management group as exclusions, in addition to child resource groups and resources.

- Subscription
- Tenant
- Management group

Q2)

You have an Azure HDInsights cluster on a Azure VNet. You need to secure communication between the cluster and your on-premises network, establish name resolution and use on-premises AD credentials to administer the cluster.

You have to minimize costs. What do you deploy?

- ✓ Deploy network security groups on the Vnet

Explanation:-Deploy an on-premises data gateway - no.
Deploy AD Connect - no, local AD credentials used with HDInsight does not need synchronisation with AAD.
Deploy a site-to-site VPN - yes, you need to establish network connectivity.
Deploy a custom DNS server on the Vnet - yes, you need to establish name resolution for the solution. On-premises DNS integration requires you to set up a custom DNS server for the VNet.
Deploy network security groups on the Vnet - yes, you need to secure the communication between the Vnet and the OPE network.
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

- ✓ Deploy a custom DNS server on the Vnet

Explanation:-Deploy an on-premises data gateway - no.
Deploy AD Connect - no, local AD credentials used with HDInsight does not need synchronisation with AAD.
Deploy a site-to-site VPN - yes, you need to establish network connectivity.
Deploy a custom DNS server on the Vnet - yes, you need to establish name resolution for the solution. On-premises DNS integration requires you to set up a custom DNS server for the VNet.
Deploy network security groups on the Vnet - yes, you need to secure the communication between the Vnet and the OPE network.
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

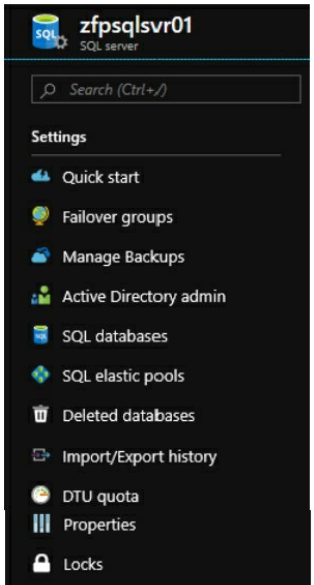
- Deploy an on-premises data gateway
- Deploy AD Connect
- ✓ Deploy a site-to-site VPN

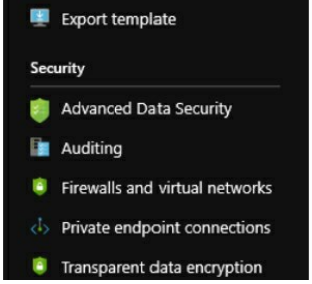
Explanation:-Deploy an on-premises data gateway - no.
Deploy AD Connect - no, local AD credentials used with HDInsight does not need synchronisation with AAD.
Deploy a site-to-site VPN - yes, you need to establish network connectivity.
Deploy a custom DNS server on the Vnet - yes, you need to establish name resolution for the solution. On-premises DNS integration requires you to set up a custom DNS server for the VNet.
Deploy network security groups on the Vnet - yes, you need to secure the communication between the Vnet and the OPE network.
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

---

Q3)

Check out the exhibit.





You have an Azure SQL database that you want to secure access to the database from your web application using a Managed Service Identity (MSI).

You create an app registration for your application in AAD and now need to give permission to the app on the Azure SQL Database server.

Which option do you choose?

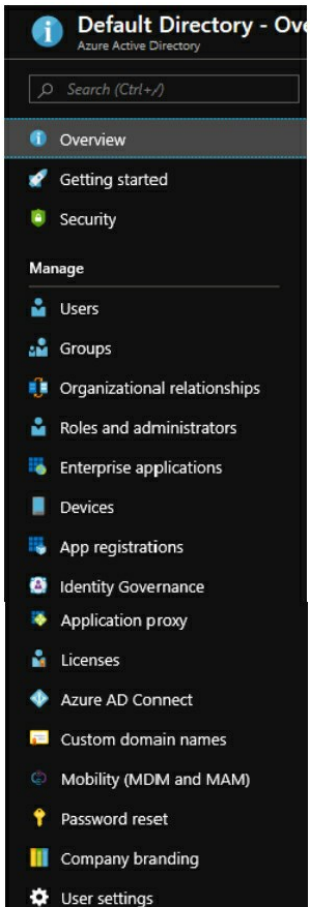
- Properties
- SQL databases
- ✅ Active Directory admin

Explanation:-You will first assign an AAD user access as the SQL Server administrator. You also have to put the registered app in an AAD group and assign that group permissions in the SQL database (using SQL commands). Lastly you have to modify your app to use modern authentication when connecting to the DB. https://docs.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-connect-msi

- Locks
- Advanced Data Security

Q4)

Review the exhibit.



What option do you choose to configure MFA authentication methods?

- Security
- ✅ Users

Explanation:-https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted#choose-verification-options

- Overview
- Groups
- Identity Governance
- User settings

Q5) Correct or Incorrect: MFA can be implemented by requiring a primary "system access" username and password, and a secondary "application access" username and password.

- Correct
- ✓ Incorrect

Explanation:-MFA requires more than one factor of authentication at the same time
Something you know (password)
Something you have (token / device / certificate)
Something you are (biometrics)
Using two passwords is just using the same factor twice and is not considered true MFA
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

---

Q6) Which of the following authentication methods are not supported for Azure MFA?

- MS authenticator app
- ✓ Email address

Explanation:-Security questions and email address are not supported for MFA. All the others are valid configurable authentication methods for both MFA and SSPR. App passwords are only applicable to MFA and not to SSPR.

- ✓ Security questions

Explanation:-Security questions and email address are not supported for MFA. All the others are valid configurable authentication methods for both MFA and SSPR. App passwords are only applicable to MFA and not to SSPR.

- Password
- OATH hardware token
- SMS

Q7) Match the Azure RBAC terms and definitions

- ✓ Group of access: assignment

Explanation:-https://docs.microsoft.com/en-us/azure/role-based-access-control/overview

- ✓ Group of resources: scope

Explanation:-https://docs.microsoft.com/en-us/azure/role-based-access-control/overview

- ✓ Group of permissions: role

Explanation:-https://docs.microsoft.com/en-us/azure/role-based-access-control/overview

- ✓ Group of users: principal

Explanation:-https://docs.microsoft.com/en-us/azure/role-based-access-control/overview

- Group of users: assignment
- Group of users: scope

Q8)

You deploy several VMs in Azure. You need to ensure that all the VMs have a consistent OS configuration including registry settings.

Which of the following options would you configure?

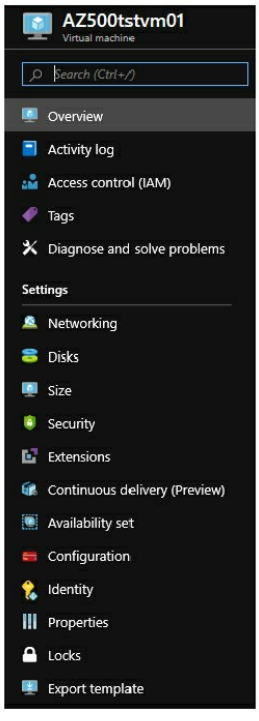
- Application Security Groups
- ✓ Desired State Configuration

Explanation:-Desired State Configuration (DSC) is used to ensure consistent VM deployment.
https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started

- ARM templates
- Device configuration policies

Q9)

Which option in the exhibit would you choose to configure endpoint security?



- Configuration
- ✅ Extensions

Explanation:-You must install the Microsoft Antimalware extension to enable endpoint security on the VM

- Security
- Networking
- Identity
- Locks

Q10)

You are configuring AIP policies. You specify two labels:

Label1: matches "Word1"

Label2: matches "Word2"

You create a document in MS Word that contains both words, which label is applied?

- Label1 and Label2
- ✅ Label2

Explanation:-Label 2 is applied. AIP labels are applied in the order they are listed in the policy with the last matching label (or sublable) winning. Only one label is applied to the document. Only Office documents are supported.
https://docs.microsoft.com/en-us/azure/information-protection/faqs-infoprotect#can-a-file-have-more-than-one-classification

- Label1
- No label

Q11)

You are configuring Azure Update Management. You on boarded several VMs that have been deployed to different resource groups and regions.

You have configured the following update deployments:

- Item1: VM1, EastUS, RG1, Windows 2008R2

- Item2: VM2, WestUS, RG2, CentOS 6

You want to add additional VMs to the update deployments.

Which of the following can you do?

- ✅ Add VM6, EastUS, RG2, CentOS 6 to Item2

Explanation:-A favourite trope of the exam - knowing the limitations of adding instances with different properties (region, resource group, OS, etc.) to Azure services once you've already configured the service.
You can add any VM from and RG or Region to a Update Management deployment schedule as long as the new VM is also Windows or Linux respectively.
https://docs.microsoft.com/en-za/azure/automation/manage-update-multi#schedule-an-update-deployment

- Add VM5, EastUS, RG1, CentOS 6 to Item1
- ✅ Add VM4, WestEurope, RG1, Windows 2016 to Item1

Explanation:-A favourite trope of the exam - knowing the limitations of adding instances with different properties (region, resource group, OS, etc.) to Azure services once you've already configured the service.
You can add any VM from and RG or Region to a Update Management deployment schedule as long as the new VM is also Windows or Linux respectively.
https://docs.microsoft.com/en-za/azure/automation/manage-update-multi#schedule-an-update-deployment

- ✅ Add VM3, EastUS, RG2, Windows 2016 to Item1

Explanation:-A favourite trope of the exam - knowing the limitations of adding instances with different properties (region, resource group, OS, etc.) to Azure services once you've already configured the service.
You can add any VM from and RG or Region to a Update Management deployment schedule as long as the new VM is also Windows or Linux respectively.
https://docs.microsoft.com/en-za/azure/automation/manage-update-multi#schedule-an-update-deployment

---

Q12)

You are using Azure Key Vault to provide protection for a custom application your organisation is using.

Match the application security issue with the appropriate Key Vault object to be used to secure it.

- The connection string to REDIS cache is stored in the web application configuration file: Certificate
- The connection string to REDIS cache is stored in the web application configuration file: Key
- ✅ Connecting to the web application will be restricted to HTTPS only: Certificate
- ✅ SQL AlwaysEncrypted will be configured: Key
- ✅ Database connection string with username and password is stored in clear text in the web application configuration file: Secret
- ✅ The connection string to REDIS cache is stored in the web application configuration file: Secret

---

Q13)

You are securing your web application by removing connection strings to Azure SQL Database from the web.config configuration file.

What two options do you have in Azure to accomplish your goal?

- Azure SQL Database server Active Directory admin
- Azure Active Directory Application Registration
- ✓ Azure Active Directory Managed Service Identity (MSI)

Explanation:-https://docs.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-connect-msi

- ✓ Azure Key Vault secret

Explanation:-https://docs.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-connect-msi

- Azure SQL Database AlwaysEncrypted
- Azure SQL Database Transparent Data Encryption (TDE)

Q14)

You're configuring AIP and want to help your users find more information about the information protection policies and classifications.

What would you use to provide this information to users?

- Custom label
- ✓ Custom URL

Explanation:-Custom URL for "tell me more"

- Custom tooltip
- Custom policy

Q15)

You create a dynmaic group with the following dynamic membership rule:

(user.surname -contains "SS") or (user.surname -match "*we")

Which of the following users will be in the dynamic group?

- Fargo Wells
- ✓ Frank Lowe

Explanation:-Peter Bless - yes, REGEX is not case sensitive and the surname contains "ss".
Simon BLESS - yes, REGEX is not case sensitive and the surname contains "SS".
Fargo Wells - no, the wildcard in "*we" must match at least one character.
Frank Lowe - yes, the surname ends with "we" and has preceeding characters.
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership#supported-values

- ✓ Peter Bless

Explanation:-Peter Bless - yes, REGEX is not case sensitive and the surname contains "ss".
Simon BLESS - yes, REGEX is not case sensitive and the surname contains "SS".
Fargo Wells - no, the wildcard in "*we" must match at least one character.
Frank Lowe - yes, the surname ends with "we" and has preceeding characters.
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership#supported-values

- ✓ Simon BLESS

Explanation:-Peter Bless - yes, REGEX is not case sensitive and the surname contains "ss".
Simon BLESS - yes, REGEX is not case sensitive and the surname contains "SS".
Fargo Wells - no, the wildcard in "*we" must match at least one character.
Frank Lowe - yes, the surname ends with "we" and has preceeding characters.
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership#supported-values

---

Q16)

You have the following resource groups containing the listed resources:

- RG1; VM1 (stopped)

- RG2; VM2 (stopped)

- RG3; VM3 (stopped)

You have locks configured as follows:

- Lock1; Read-only; RG1

- Lock2; Delete; RG1

- Lock3; Delete; RG2

- Lock4; Read-only; RG3

Which of the following actions can you perform?

- You can delete VM2
- You can delete VM1
- ✓ You can start VM2

Explanation:-You can start VM1 [No] Start is considered a change and is prevented by RO Lock1 inherited from RG1.
You can start VM2 [Yes] No-delete Lock3 inherited from RG2 does not prevent changes (including start/stop) to VM2.
You can delete VM1 [No] Delete is prevented by RO locks. RO Lock1 inherited from RG1 prevents delete. No-delete Lock2 inherited from RG1 also prevents delete.
You can delete VM2 [No] No-delete Lock3 inherited from RG2 prevents delete.
You can delete VM3 [No] Delete is prevented by RO locks. RO Lock4 inherited from RG3 prevents delete.
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources

- You can start VM1
- You can delete VM3

Q17)

You have an Azure container registry. You have users with these roles.

- User1: Contributor

- User2: Reader

- User3: AcrPush

- User4: AcrPull

Select what each user can do?

- ✅ User4 can pull an image

Explanation:-User1 can sign an image [No] Only AcrSign can do that, not even owner can.
User2 can pull an image [No] Reader can only do ARM things.
User3 can pull an image [Yes] AcrPush can also pull.
User4 can pull an image [Yes] Obviously.
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles

- User1 can sign an image
- User2 can pull an image
- ✅ User3 can pull an image

Explanation:-User1 can sign an image [No] Only AcrSign can do that, not even owner can.
User2 can pull an image [No] Reader can only do ARM things.
User3 can pull an image [Yes] AcrPush can also pull.
User4 can pull an image [Yes] Obviously.
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles

---

Q18)

You need to manage inbound and outbound traffic rules at scale to specific VMs with minimum effort.

You plan on creating separate inbound and outbound NSG rules with CIDR notation. Is this the easiest method to manage multiple VMs?

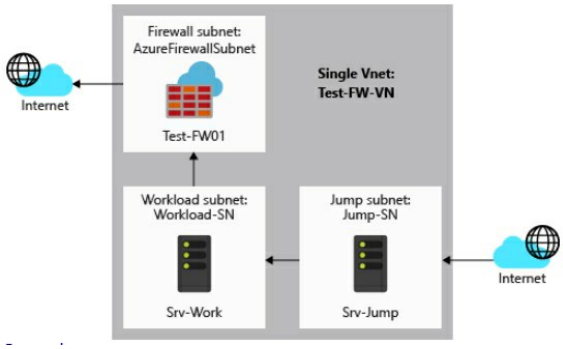
- Correct
- ✅ Incorrect

Explanation:-You need to make use of Application Security Groups (ASG's). ASG's allows you to group VM's to make management easier, for example you can group several VMs with an ASG and only make changes once to the ASG instead of manually adding/removing/editing NSG rules with CIDR notation. https://docs.microsoft.com/en-us/azure/virtual-network/security-overview#application-security-groups

---

Comprehension:

You are deploying Azure Firewall as in the exhibit.



You want to ensure all traffic from Workload-SN going to www.google.com is routed through the Azure Firewall.

Q19) What do you have to create in Workload-SN in to ensure that Test-FW01 will inspect outgoing traffic?

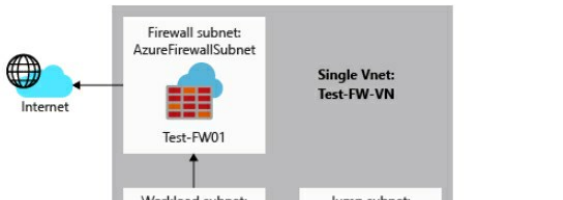
- Firewall Rule
- ✅ Route Table

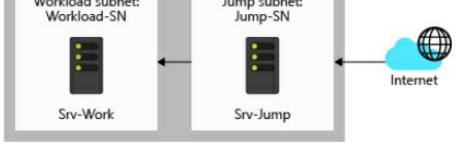
Explanation:-https://docs.microsoft.com/en-gb/azure/firewall/tutorial-firewall-deploy-portal

- NSG

Comprehension:

You are deploying Azure Firewall as in the exhibit.





You want to ensure all traffic from Workload-SN going to www.google.com is routed through the Azure Firewall.

Q20) How should the next hop in Workload-SN be configured as?

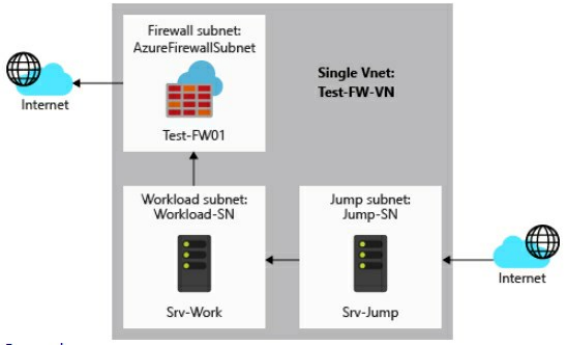
- FW Name
- ✔ FW Internal IP

Explanation:-https://docs.microsoft.com/en-gb/azure/firewall/tutorial-firewall-deploy-portal

- FW Public IP
- Blank

Comprehension:

You are deploying Azure Firewall as in the exhibit.



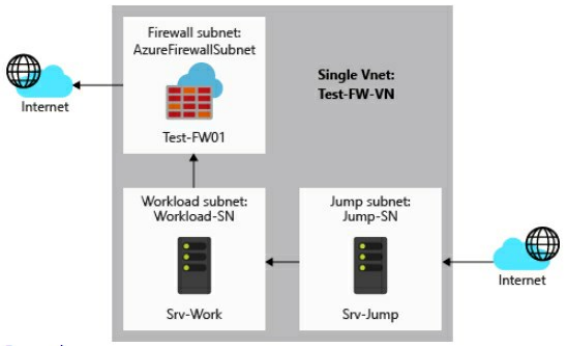
You want to ensure all traffic from Workload-SN going to www.google.com is routed through the Azure Firewall.

Q21) What address prefix should you configure in Workload-SN?

- Blank
- 255.255.255.255/255
- ✔ 0.0.0.0/0
- FW Internal IP

Comprehension:

You are deploying Azure Firewall as in the exhibit.



You want to ensure all traffic from Workload-SN going to www.google.com is routed through the Azure Firewall.

Q22) What should you configure on Test-FW01?

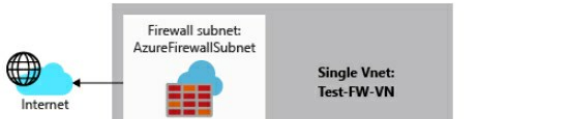
- Route Table
- ✔ Application rule

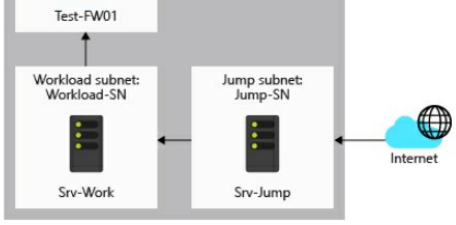
Explanation:-What should you configure on Test-FW01 [Application rule] (for www.google.com) https://docs.microsoft.com/en-gb/azure/firewall/tutorial-firewall-deploy-portal

- Network rule
- Nothing

Comprehension:

You are deploying Azure Firewall as in the exhibit.





You want to ensure all traffic from Workload-SN going to www.google.com is routed through the Azure Firewall.

Q23) What should you configure on Test-FW01 to ensure successful DNS resolution from Workload-SN?

- Route Table
- ✅ Network rule

Explanation:-What should you configure on Test-FW01 to ensure successful DNS resolution from Workload-SN? [Network rule] (for destination port 53) https://docs.microsoft.com/en-gb/azure/firewall/tutorial-firewall-deploy-portal

- Application rule
- Nothing

Q24) Correct or Incorrect : when there are 2 NSG's associated to the same subnet, when one NSG denies traffic on port 80 inbound and another allows traffic on port 80 inbound to the same VM, the traffic will automatically be blocked due to the one NSG rule that denies the traffic.

- Incorrect
- ✅ Correct

Explanation:-Whenever a VM/subnet is associated to 2 or more NSG's and there are conflicting rules on each NSG (i.e. one NSG has allow and one NSG deny) the NSG which has the deny rule will take preference and traffic will not pass through. https://docs.microsoft.com/en-us/azure/virtual-network/security-overview

---

Q25)

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?

- Correct
- ✅ Incorrect

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

Q26)

Your company plans to create separate subscriptions for each department. Each subscription will be associated to the same Azure Active Directory (Azure AD) tenant.

You need to configure each subscription to have the same role assignments.

What should you use?

- Azure Blueprints
- ✅ Azure AD Privileged Identity Management (PIM)

Explanation:-The Azure AD Privileged Identity Management (PIM) service also allows Privileged Role Administrators to make permanent admin role assignments.

- Azure Security Center
- Azure Policy

Q27)

You have an Azure subscription.

You create an Azure web app named Contoso1812 that uses an S1 App service plan.

You create a DNS record for www.contoso.com that points to the IP address of Contoso1812.

You need to ensure that users can access Contoso1812 by using the https://www.contoso.com URL.

Which two actions should you perform?

- ✅ Upload a PFX file to Contoso1812.

Explanation:-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.

- Scale out the App Service plan of Contoso1812.
- Add a deployment slot to Contoso1812.
- Scale up the App Service plan of Contoso1812.
- Turn on the system-assigned managed identity for Contoso1812.
- ✅ Add a hostname to Contoso1812.

Explanation:-You can configure Azure DNS to host a custom domain for your web apps. For example, you can create an Azure web app and have your users access it using either www.contoso.com or contoso.com as a fully qualified domain name (FQDN).

Q28)

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?

- Correct
- ✅ 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.

Q29)

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?

- Correct
- ✅ Incorrect

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

Q30)

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.

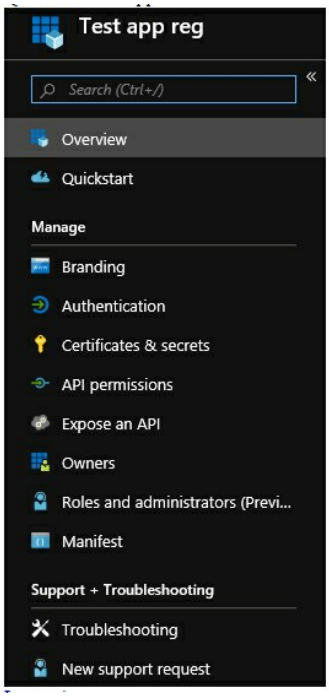
What should you use?

- application security groups
- ✅ 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.

- device configuration policies in Microsoft Intune
- Azure Logic Apps

Q31)



When doing an app registration in Azure AD, what option in the exhibit allows configuration of the services the application has access to?

- Expose an API
- ✓ API permissions
- Certificates & secrets
- Authentication
- Roles and administrators