Exam Session - Cert Prep: Microsoft Azure Security Technologies (AZ-500)

cloudacademy.com/quiz/exam/3757933/results

#1

You are the owner of a resource group that contains the following Azure resources:VNet1, which contains Subnet1. Subnet1 is assigned a routing table, and a network security group named NSG-1.SubNet1 contains an ARM virtual machine with a private IP address only.VM-Database1 needs to connect to an on-premises static IP address (216.3.128.12) to request software updates. You do not want to reveal the IP address of the ARM virtual machine. All inbound traffic aside from the software updates should be blocked.Which steps should you take to allow the database to connect successfully for updates while limiting threats? (Choose 2 answers.)

✗

Deploy a private load balancer associated with the ARM virtual machine.

✓

Deploy a NAT gateway associated with Subnet1.

✗

Update NSG-1 to allow outbound traffic to and from 216.3.128.12 over port 443. Include no other rules allowing traffic.

✓

Update NSG-1 to allow outbound traffic to 216.3.128.12 over port 443. Include no other rules allowing traffic.

Explanation

Network security group security rules are evaluated by priority using the 5-tuple information (source, source port, destination, destination port, and protocol) to allow or deny the traffic. A flow record is created for existing connections. Communication is allowed or denied based on the connection state of the flow record. The flow record allows a network security group to be stateful.

Deploy a Network Address Translation or NAT gateway to enable Source Network Address Translation (SNAT). As Microsoft explains in its documentation:

Source Network Address Translation (SNAT) rewrites the source of a flow to originate from a different IP address and/or port. Typically, SNAT is used when a private network needs to connect to a public host over the internet. SNAT allows multiple compute resources within the private VNet to use the same single Public IP address or set of IP addresses (prefix) to connect to the internet.

🔗 https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource#source-network-address-translation
#2

How does Microsoft Defender for Cloud ensure compliance with company and regulatory security requirements?

✗
Customization by administrators

✗
Pre-defined policies in the Azure subscription

✓
Centralized Policy Management

✗
By making recommendations to remediate security vulnerabilities

Explanation

Through centralized policy management, compliance with company and regulatory security requirements is ensured.

🔗 https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/migrate/azure-best-practices/migrate-best-practices-security-management#best-practice-follow-azure-security-center-recommendations
Covered in this lecture
Preventing and Responding to Security Threats with Azure Security Center
Course:Managing Azure Data Protection and Security Compliance

2m

#3

As your company's database administrator and owner of a Cosmos DB account, you need to create a new Cosmos DB database to support an application currently being developed. You also need to grant access to a member of your IT staff who will be testing the new application. The developer will need to create containers and modify the Cosmos DB database settings to fine-tune them. Additionally, you will need to create the necessary credentials for the application, which will be hosted on Azure App Service web apps, to connect with the database, and will upload, modify and read data to fulfill expected requests. To simplify the testing process, you would like to create a set of application credentials that persists while the test resources themselves may be continuously created and deleted throughout the development process. You also want to provide access to the IT staff member following general security best practices. How should you proceed?

✓

Create the database using the primary or secondary read-write master key. Assign the IT staff member Account Contributor role through Azure Active Directory. Create a user-assigned managed identity for the application hosted on Azure App Service web apps.

✗

Create the database using the primary read-write master key. Provide access to the IT staff member using the secondary read-write master key. Create a user-assigned managed identity for the application hosted on Azure App Service web apps.

✗

Create the database using the primary or secondary read-write master key. Assign the IT staff member Account Contributor role through Azure Active Directory. Create a system-assigned managed identity for the application hosted on Azure App Service web apps.

✗

Create the database using the primary or secondary read-write master key. Provide access to the IT staff member using the primary read-only master key. Create a system-assigned managed identity for the application hosted on Azure App Service web apps.

Explanation

The master keys are essentially the root access keys for the Cosmos DB account owner, and can be used to create resources, but should not be shared. Assigning permissions via RBAC is the best course of action in this case, and creating a user-assigned managed identity means the credentials will persist and can be repeatedly assigned to new and different resources in the dev/test environment.

https://docs.microsoft.com/en-us/azure/cosmos-db/secure-access-to-data

Covered in this lecture

Using the Azure CLI
Course:Overview of Azure Services

6m

#4

Which of these roles are able to make changes to the default security policy in Microsoft Defender for Cloud? (Choose 2 answers).

✗
End User

✓
Contributor

✗
Subscriber

✓
Owner

Explanation

The ability to make changes to the default security policy requires you to be an owner, contributor, or a security administrator of the Azure subscription.

https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-policy

#5

As your company's IT security administrator, you need to assign credentials to project teams for application development and testing. Team A needs a new Cosmos DB database to support an application currently being developed. This team includes: Dev/Test members who will need to create Cosmos DB containers and modify the Cosmos DB database settings to fine-tune them. Project Administrators who will need to manage provisioning and governance of the Cosmos DB resources, to ensure they align with company policy. They will deploy the resources necessary, but will not have read or write access to these resources or their data once deployed. As the IT security administrator, you will also need to ensure the correct type of application credentials are implemented to be in accordance with company policy. The application being tested will be deployed using Azure App Service web apps. These App Service web apps will connect with the database to upload, modify and read data to fulfill typical client requests. To align with company policy, the application credentials should be deleted whenever the associated dev resources are deleted. To follow security best practices of least privilege and efficiency, how should you provide the necessary access credentials to your team members and Azure resources?

✓

Create an Azure AD group for your Project Administrators assigned to this project, and assign the Cosmos DB Operator role to the Project Administrators group. Create an Azure AD group for the Dev/Test members assigned to this project and assign the Cosmos DB Account Contributor role to the Dev/Test group. Implement system-assigned managed identities for the applications hosted on Azure App Service web apps.

✗

Create an Azure AD group for your Project Administrators and Dev/Test members, and assign the Cosmos DB Operator role to that group. In addition, provide your Dev/Test team with the Cosmos DB account's primary read-write master key. Include the Cosmos DB account's secondary read-write master key within the Azure App Service web app code.

✗

Provide the Cosmos DB account's primary read-only master key to the Project Administrators. Provide the Cosmos DB account's primary read-write master key to the Dev/Test members. Implement user-assigned managed identities for the applications hosted on Azure App Service web apps.

✗

Assign the Cosmos DB Operator role to each Project Administrator's Azure AD user identity. Assign the Cosmos DB Account Contributor role to each Dev/Test member's Azure AD user identity. Implement system-assigned managed identities for the applications hosted on Azure App Service web apps.

Explanation

Cosmos DB master keys are essentially root access keys that should not be shared with other users, or used in code. In this case, creating a group for the project administrators and dev/test team members and assigned the correct permissions is the best choice and most efficient option.

System-assigned managed identities do not persist after the associated resources have been deleted, so they would be the best choice to follow policy in this case.

🔗 https://docs.microsoft.com/en-us/azure/cosmos-db/database-security

Covered in this lecture

AZ-303 Exam Preparation: Introduction

Course:AZ-303 Exam Preparation: Introduction

3m

#6

Which of the following security validation methods simply tests the responsiveness of your website at regular intervals?

✓

URL ping tests

✕

Custom telemetry tests

✕

playback of recorded web requests

✕

custom attack surface reviews

Explanation

At the most basic level, there is the URL ping test, which as the name implies, tests basic responsiveness of your website at regular intervals, logging results. The ping test can be configured through the Azure portal

/course/configuring-azure-application-and-data-security/implementing-security-validations-for-application-development/

Covered in this lecture

Implementing Security Validations for Application Development

Course:Configuring Azure Application and Data Security

1m

#7

Stuart is a contractor who needs read and write access to resources within two resource groups, Resource Group 1 and Resource Group 2. He will assist with updates to live applications within both resource groups.The role assignment has the following requirements:For security reasons, all hired contract employees must complete MFA for each login to Azure.Due to the urgency of the project, Stuart should have immediate access to all resource upon assignment.What choices below best meet these requirements? (Choose 2 answers)

✓

Assign an active role type.

✗

Assign an eligible role type.

✓

Require MFA while on active assignment.

✗

Require MFA upon role activation and active assignment.

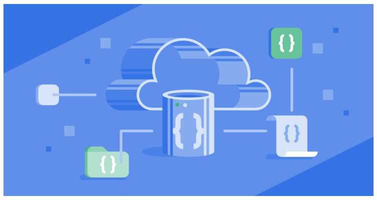
Explanation

There are two assignment types: active and eligible. Eligible assignments require an action to be activated, which could be MFA or providing a justification for activation. Active roles are essentially pre-approved, and require no further MFA or justification.

For Stuart to have immediate access, he needs an active role, and with an active role, MFA upon activation is not a valid option, only MFA while on active assignment.

🔗 https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-configure-role-settings#require-multi-factor-authentication

Covered in this lecture
Why Use Azure Active Directory Authentication?
Course:Azure Database Authentication and Access



3m

#8

Which of the following security validation methods is available through the implementation of Application Insights?

✓

custom telemetry tests

✗

URL ping tests

✗

playback of recorded web requests

✗

custom attack surface reviews

Explanation

Within the Microsoft.ApplicationInsights namespace, you can use the TelemeteryClient TrackAvailibity method. These tests are created in the context of an application insights resource. An Application Insights resource has the capacity to host up to 100 availability tests.

/course/configuring-azure-application-and-data-security/implementing-security-validations-for-application-development/

Covered in this lecture

Implementing Security Validations for Application Development

Course:Configuring Azure Application and Data Security

1m

#9

You are configuring Azure Firewall outbound network rule to allow connections to an IP address via Port 53. Which protocol should you select?

✓

UDP

✗

POP

✗

DHCP

✗

HTTPS

Explanation

To create our network rule, we need to select the Network Rule Collection tab. Now from here, we'll choose the option to add a network rule collection and we'll call this NetworkCollection. Again, we'll set our priority to 200 and we're going to allow our traffic. At this point, we need to define our rule. So under IP addresses, under the Rule section here. For our name, we're going to call it AllowDNS. We'll choose UDP for the protocol since DNS is UDP traffic.

https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal#configure-a-network-rule

#10

A company is using Azure Active Directory (Azure AD). The company has an assigned Global administrator and does not want someone else to have that level of access in Azure AD. However, they want to allow a new employee to manage groups, user accounts, and service requests. Which of the following roles should be assigned to the new employee?

✗

Resource administrator

✗

Billing administrator

✗

Service administrator

✓

User administrator

Explanation

Azure Active Directory has the following roles available:

1. Global administrator - This role has access to all administrative features.
2. Billing administrator - This role allows a user to manage subscriptions.
3. Service administrator - The service administrator manages requests and monitors the health of designated services.
4. User administrator - This role manages groups, user accounts, and service requests.

https://docs.microsoft.com/en-us/azure/active-directory/active-directory-assign-admin-roles

#11

Which of the following tools can be used to extend on-premise Windows Server Active Directory to Azure AD?

✓

Azure AD Connect

✗

Azure AD Sync

✗

Azure AD

✗

Azure AD Premium

Explanation

Azure AD Connect is a tool to simplify the extension of on-premise AD to Azure AD.

https://azure.microsoft.com/en-us/documentation/articles/active-directory-whatis/

Covered in this lecture

Where Our Identities are Mastered

Course:Implementing Identity Synchronization with Azure AD Connect

1m

#12

How does Adaptive Application Control in Microsoft Defender for Cloud help to protect virtual machines from malware?

✓

Controlling the applications that can be run

✗

Monitoring application checksums

✗

Blocking inbound access

✗

Reducing access to VMs

Explanation

Adaptive Application Controls helps you harden virtual machines against malware by controlling the applications that can be run.

🔗 https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application

Covered in this lecture

Protecting Your Resources with Azure Security Center

Course:Managing Azure Data Protection and Security Compliance

1m

#13

As IT security manager for your company, you currently use Azure Active Directory to control employee access to Azure resources and environments. You discover two issues that need to be addressed:Many employees have authorized access to Azure resources based on each employee's previous team assignments. If certain employee credentials happen to be stolen, it could pose a large financial risk for the company.Currently, authorization to specific Azure resources can be inherited based on resource placement in a particular Azure resource group. You now want all resource assignments to be resource-specific. Which single feature of Azure Active Directory should you implement to address both of these security issues?

✓

Azure Privileged ID Management (PIM)

✗

Azure Active Directory Conditional Access

✗

Azure Active Directory Identity Protection

✗

Azure Active Directory Multi-Factor Authentication (MFA)

Explanation

Azure AD Privileged Identity Management (PIM) will allow you to solve these problems by implementing resource-specific authorization rather than hierarchically-inherited authorization. It also allows you to assign 'just-in-time' access, with a set expiration, rather than permanent access.

🔗 https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-eligible-visibility#azure-resource-role-approval-workflow
#14

The CIS Microsoft Azure Foundations Benchmark provides two levels of recommended security implementation. Which two statements apply to Level 1 recommendations? (Choose two answers)

✓
They should be implemented within all systems.

✗
They should be implemented within highly secure environments only.

✓
They will cause little to no service interruption.

✗
They can reduce service functionality.

Explanation

There are two different implementation levels that CIS bases their recommendations on. There are also several different categories of recommendations that are made. The two levels are called Level 1 and Level 2. I know, very original.
Level 1 recommendations are the minimum recommended security settings that should be configured on ALL systems.

Level 1 recommendations typically cause little or no interruption of services, nor do they usually result in reduce functionality.
Level 2 recommendations are designed for highly secure environments. That being the case, they can sometimes result in reduced functionality of the systems they are implemented on.

🔗 https://azure.microsoft.com/en-us/blog/cis-azure-security-foundations-benchmark-open-for-comment/
#15

Azure Update Management can manage operating system updates for which combination of operating systems and platforms?

✗

Any Azure-hosted virtual machine running supported Windows or Linux operating systems

✗

Any cloud-based virtual machine (Azure or non-Azure) running a supported Windows operating systems

✗

Any Azure-hosted or on-premises computer running supported Windows or Linux operating systems

✓

Any cloud-based (Azure or non-Azure) or on-premises computer running supported Windows or Linux operating systems

Explanation

You can use the Update Management solution in Azure Automation to manage operating system updates for your Windows and Linux computers in Azure, in on-premises environments, and in other cloud providers. You can quickly assess the status of available updates on all agent computers and manage the process of installing required updates for servers.

https://docs.microsoft.com/en-us/azure/automation/automation-update-management

Covered in this lecture

Assessing & Migrating Physical Machines

Course:Migrating Servers To Azure

8m

#16

Which of the following is not a feature of Azure AD Connect?

✓

Content Monitoring

✗

Filtering

✗

Password synchronization

✗

Password writeback

Explanation

Content Monitoring is not a feature of Azure AD Connect. The following is a list of Azure AD Connect features: Filtering, Password synchronization, Password writeback, Device writeback, Prevent accidental deletes, Automatic upgrade. Monitoring is provided through Azure AD Connect Health.

🔗 https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect

#17

You are configuring data security settings for separate Azure SQL databases. Database A stores social security numbers, which you want to prevent any users or applications from viewing. The social security numbers appear in one column within a single table of Database A. Database B stores credit card information, including credit card numbers, which only privileged database administrators should be able to see. The credit card numbers appear in columns within several tables in Database B. How should you configure the data encryption settings for these databases to meet these requirements?

✓

Enable 'Always Encrypted' for Database A, and Dynamic Data Masking (DDM) for Database B.

✗

Enable 'Always Encrypted' for Database A and Database B.

✗

Enable Dynamic Data Masking (DDM) for Database A, and 'Always Encrypted' for Database B.

✗

Enable Dynamic Data Masking (DDM) for Database A and Database B.

Explanation

'Always Encrypted' prevents any users or applications from viewing or decrypting data, so in cases where data should be stored but never accessed by anyone accept the customer, this feature should be enabled.

Dynamic Data Masking allows only privileged users to view specific data.

How often data appears within a database would not affect the encryption feature you enable, only how you apply it, which is not a factor in answering this question.

🔗 /course/microsoft-azure-security-solutions/data-security-1/?context_id=73&context_resource=lp

#18

Azure Policy focuses on enforcing organizational standards on Azure _______________.

✓

resources

✕

users

✕

groups

✕

costs

Explanation

With policies, you can prevent users in your organization from breaking conventions that are needed to manage your organization's resources. It is important to note that policies and RBAC work together. However, there are differences. RBAC focuses on the actions a user can perform at different scopes while policy focuses on resource actions at various scopes.

🔗 https://docs.microsoft.com/en-us/azure/resource-manager-policy#how-is-it-different-from-rbac

#19

How many default data classification labels are there when you enable Azure Information Protection?

✕

3

✕

4

✓

5

✕

6

Explanation

The default labels for classification are Personal, Public, General, Confidential, and Highly Confidential. The last two labels expand to show sublabels, which provide examples of how a classification can have subcategories

https://docs.microsoft.com/en-us/azure/information-protection/quickstart-viewpolicy#view-your-labels
Covered in this lecture
How to Protect Your Data
Course:Configuring Azure Application and Data Security

1m

#20

Your organization wants to secure customer personal data stored within your Azure Virtual Machine (VM) environment. You suggest Azure Disk Encryption, which is an option available to both Linux and Windows VMs. While the encryption process is actually pretty straightforward, and is as easy as deploying a VM extension in PowerShell, what is one caveat to the process that adds a level of complexity?

✕

Bitlocker enabled and Azure Backup Service are mutually exclusive processes.

✕

Bitlocker is ineffective at encrypting the operating system.

✓

A mechanism must be in place to manage the encryption keys for the encrypted disk.

✗

The process of creating the encryption keys is complex.

Explanation

The one caveat to the Bitlocker process that adds a somewhat difficult level of complexity is managing the encryption keys that go along with encrypting your disk. After all, if you lock something away, someone has to keep track of the keys to reopen it. The good news is Azure provides what is called the Azure Key Vault service which is used to help you manage and control your disk-encryption keys and secrets used by cloud applications and services.

🔗 https://docs.microsoft.com/en-us/azure/key-vault/key-vault-whatis

#21

You are a Privileged Role Administrator within Azure Privileged Identity Management (PIM). You need to expedite numerous role requests, and have just assigned an Azure Active Directory user a Designated Approver role. You need the designated user to begin her newly assigned role as soon as possible. How can this be accomplished?

✗

Override the required justification for the role.

✗

As a privileged role administrator, you can override a required approval.

✓

Tell the user to invalidate their current token via the Application Access pane in PIM.

✗

When approving the role, check the 'Approve immediately' box within the 'Approve Requests' pane in PIM.

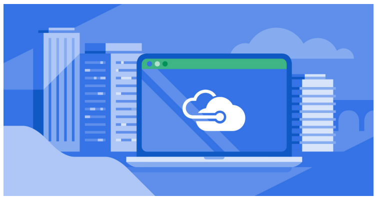
Explanation

The "Application access" pane allows you to limit possible delays and use a role immediately after activation.

🔗 https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-activate-role#use-a-role-immediately-after-activation

Covered in this lecture

Conclusion
Course:Implementing Azure Active Directory Privileged Identity Management



3m

#22

You work as a security manager for a company that builds and manages customer applications. As part of your service agreement, you allow customers to conduct spot checks of their applications in the production environment.You typically apply resource locks that prevent any modifications to all resources being checked, to prevent any accidental changes during the review.Your customer, Contoso, will be checking all resources within Resource Group 1 over the next five business days. Resource Group 1 contains 50 resources in total.Resource Group 1 contains a critical database hosted on VM1 that needs extensive updates and patching over the next five business days.What is the most efficient way to apply resource locks to the resources in Resource Group 1 to prevent accidental modifications, but still allow the database on VM1 to be modified?

✓

Move VM1 to a new resource group and then apply a CanNotDelete resource lock to VM1. Then apply a ReadOnly resource lock to Resource Group 1.

✕

Apply ReadOnly resource locks to all resources except VM1. Apply a CanNotDelete resource lock to VM1.

✕

Apply a ReadOnly resource lock to Resource Group 1. Then apply a CanNotDelete resource lock to VM1.

✕

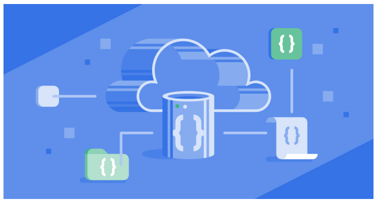
Apply a ReadOnly resource lock to Resource Group 1, and apply that lock to the customer reviewer's Azure AD guest user account.

Explanation

Resource locks, when applied, apply to all users and roles. They cannot be applied to only specific users or roles. When a resource lock is applied to a resource group, it is inherited by all the resources within it, and in the case that multiple locks are applied to a single resource, the most restrictive lock will take effect.

/course/managing-azure-subscriptions-resource-groups/resource-locks/

Covered in this lecture
Resource Locks
Course:Managing Azure Subscriptions and Resource Groups



3m

#23

A company hosts a web-based .Net application in Azure. They require that whenever an abnormal activity occurs, such as high page request rate, a custom application is notified so that it can be handled accordingly. Which option below meets this requirement?

✗

Create an alert in the Azure dashboard and configure the email alert. Ensure the custom application consumes the email alerts.

✗

Create a custom powershell utility to check the the application request rate and then alerts the custom application accordingly.

✓

Create an alert and use the Webhook functionality to send the notification to the custom application.

✗

Create a custom utility that monitors and checks the application request rate and then sends the alert to the custom application.

Explanation

Webhooks allow one to route an Azure alert notification to other systems for post-processing or custom actions. A lot of custom systems support webhooks, hence this is the ideal implementation to alert third party systems to any irregularities generated by alerts in Azure.

https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/insights-webhooks-alerts

#24

You have deployed multiple AKS nodes with a Linux operating system and as a security best practice, you want to regularly review and update security settings for the operating system. Which statements below describe how security patches are applied to AKS nodes with a

Linux operating system? (Choose 2 answers)

✓

All node operating systems are automatically upgraded nightly.

✓

AKS automatically applies the latest updates.

✕

AKS automatically reboots nodes as required to complete an update.

✕

AKS automatically performs node pool upgrades nightly.

Explanation

In the case of Linux nodes, Azure automatically applies the latest OS security patches on a nightly basis. However, it's important to note that if a particular Linux OS update requires a host reboot, that reboot is NOT automatically performed. Instead, you can manually reboot the node when it's convenient. You can also use Kured, which is an open-source reboot daemon for Kubernetes.

🔗 https://docs.microsoft.com/en-us/azure/aks/node-updates-kured

#25

When access to a virtual machine with Just-in-Time VM Access enabled, you provide all of the following except which choice?

✓

Approved Azure AD users

✕

Approved IP addresses

✕

Approved port number

✕

Approved time of access

Explanation

When configuring Just in Time VM Access, the approved ports, IP addresses and time to access can all be set. However, you are not creating a policy to apply to Azure AD users. This is applied to specific resources, so at no point do you allocate access to specific users. The users gain access for each approved request.

/course/managing-azure-data-protection-and-security-compliance/manage-vm-access/
Covered in this lecture
Managing VM Access
Course:Managing Azure Data Protection and Security Compliance

5m

#26

When configuring Azure Firewall network rules to allow connections to an application's DNS server, which port number(s) should you select?

✓
53

✗
22

✗
25

✗
67 and 68

Explanation

SSH - 22

SSH is also referred to as 'Secure Shell'. It operates on the port number 22 of the TCP protocol. It carries out the task of remotely connecting to a remote server or host. It allows you to execute a number of commands and move your files remotely as well. However, it is one of the most secure ways of accessing your files remotely. Using this port, you can remotely connect to a computer and move your files with ease. This port sends the data over the network in an encrypted form which adds an extra layer of security on it. In addition to this, only authorized people will be able to remotely log on to their systems using the Port 22 which makes sure that the information does not get into unauthorized hands. It provides the chance to move files within networks as well as gives the privilege to move files between different networks securely. It operates at the Application Layer of the TCP/IP Model and is considered as one of the most secure and reliable ports for accessing files remotely.

DNS - 53

DNS is referred to as 'Domain Name System'. It operates on the port 53 of TCP and UDP protocols. DNS makes use of relational databases to link the host names of the computers or networks to their respective IP Addresses. The port 53 waits for requests from DHCP to transfer the data over the network. It operates on the Application Layer of the TCP/IP Model.

DHCP - 67, 68

DHCP is also known as 'Dynamic Host Configuration Protocol'. It basically runs on the UDP protocol. The basic purpose of DHCP is to assign IP Address related information to the clients on a network automatically. This information may comprise of subnet mask, IP Address etc. Many of the devices are automatically configured to look for IP Addresses using DHCP when they connect on a network. It makes it quite reliable to assign all the devices on a network with automatically produced IP Addresses. It generally operates on the Application layer of the TCP/IP Model. DHCP basically makes use of 2 ports; Port 67 and Port 68.

https://www.examcollection.com/certification-training/network-plus-overview-of-common-tcp-and-udp-default-ports.html

Covered in this lecture
Creating and Configuring Microsoft Azure Firewall
Course:Implementing Azure Network Security

17m

#27

A company currently has an on-premise setup which consists of Active Directory for their on-premise identity store. They want to extend their on-premise solution to Azure. They also want to implement single-sign on from their on-premise environment. Which of the following can be used to achieve this?

✗

Use a Windows 2019 server with Active Directory and IIS installed. Create a custom web application to carry out the single sign-on process.

✗

Register with a third-party vendor to carry out the single sign-on process with Azure.

✓

Use a Windows 2019 server with Active Directory Federation services installed. Ensure that a web proxy server is also set up. Make sure the Azure Active Directory Connect tool is also set up for synchronization between the on-premise Active Directory and Azure Active Directory.

✗

Use a Windows 2019 server with Remote Administration tools installed. This will provide the ability to implement single-sign on with Azure.

Explanation

Active Directory Federation services can provide single sign-on for users when the identity store is located on-premise. The Active Directory Federation service is available as an installable role on a Windows Server, which includes version 2019. The Web proxy role can also be installed on a separate server, to enable web applications to pre-authenticate access using Active Directory Federation Services (AD FS)

https://msdn.microsoft.com/en-us/library/aa479079.aspx

Covered in this lecture
Identity and Access Management
Course:Microsoft Azure Security Solutions

8m

#28

When you configure key management for storage accounts, you must ensure which of the following key vault configurations?

✓

The key vault is in the same region as the storage account

✗

The key vault is in the same subscription as the storage account

✗

The key vault is linked to a container within the storage account

✗

The key vault API service is run from a data center in your subscription region

Explanation

Azure Key Vault is a multi-tenant service and uses a pool of Hardware Security Modules (HSMs) in each Azure location.

All HSMs at Azure locations in the same geographic region share the same cryptographic boundary (Thales Security World). For example, East US and West US share the same security world because they belong to the US geo location. Similarly, all Azure locations in Japan share the same security world and all Azure locations in Australia, India, and so on.

A backup taken of a key from a key vault in one Azure location can be restored to a key vault in another Azure location, as long as both of these conditions are true:

- Both of the Azure locations belong to the same geographical location
- Both of the key vaults belong to the same Azure subscription

For example, a backup taken by a given subscription of a key in a key vault in West India, can only be restored to another key vault in the same subscription and geolocation; West India, Central India or South India.

https://docs.microsoft.com/en-us/azure/key-vault/key-vault-ovw-security-worlds

#29

Which cluster types can Enterprise Security Package enable for in HDInsight?

✗

Hadoop, Spark

✓

Hadoop, Spark, Interactive Query

✗

Hadoop, Storm, R-Server

✗

Interactive Query, Spark, R-Server

Explanation

Enterprise Security Package (previously known as HDInsight Premium) provides multi-user access to the cluster, where authentication is done by Active Directory and authorization by Apache Ranger and Storage ACLs (ADLS ACLs). Authorization provides secure boundaries among multiple users and allows only privileged users to have access to the data based on authorization policies.

Security and user isolation are important for an HDInsight cluster with EnterpriseSecurity Package.

🔗 https://docs.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-manage

#30

You have a microservice application hosted on Azure App Services named Azure Service Environment 1. The application communicates with on-premise database servers and data analysis applications. You need to find an effective monitoring solution to do the following:Monitor performance of Azure Service Environment 1 and the on-premise database servers.Provide alerts when communication between the on-premise database and Azure Service Environment 1 is disrupted.Provide quantitative data regarding customer usage.What Azure services or features within Azure App Service can meet all your requirements?

✓

Azure Application Insights

✗

Azure Monitor

✗

Azure App Service Diagnostic Logs

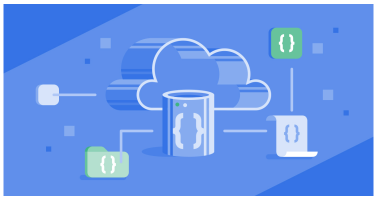
✗

Azure App Service Metrics

Explanation

Application Insights can collect data from applications in Azure, running on-premise, or on other clouds. The integration with Azure Web Apps makes it exceptionally easy to use in Azure.

/lab/deploying-monitoring-azure-app-service-web-apps/monitoring-azure-web-apps-application-insights/
Covered in this lecture
Intelligent Insights
Course:Azure SQL and SQL Server Database Monitoring



4m

#31

Your organization is implementing an application that will be published through the Azure Active Directory (Azure AD) application proxy primarily enabling access to on-premises applications. The application relies on a central on-premises directory like Windows Server Active Directory. What statement describes how identity and access management occur?

✗

Access to this application is enabled through an X.509 certificate and SSH key.

✗

Access to this application is enabled through directory information and token issuance.

✗

The access credential may be a federation token or user-name and password for an account that was previously provisioned in the application.

✓

Access to this applications is enabled by triggering the proxy to deliver the application content to the end user while honoring the on-premises sign-on requirement.

Explanation

It important to understand that the way the authorization is enacted on the target application varies depending on how the application was integrated with Azure AD. There are on-premises applications. These applications are published through the Azure AD application proxy primarily enabling access to on-premises applications. These applications rely on a central on-premises directory like Windows Server Active Directory. Access to these applications is enabled by triggering the proxy to deliver the application content to the end user while honoring the on-premises sign-on requirement.

🔗 https://docs.microsoft.com/en-us/azure/active-directory/active-directory-enable-sso-scenario#integrated-application-benefits

#32

Microsoft Defender for Cloud security policies can do all except which of the following?

✗

Data collection from deployed resources

✗

Security recommendations based on general best practices

✗

Provide instructions on how to address existing security vulnerabilities

✓

Enforce compliance with general security best practices

Explanation

Microsoft Defender for Cloud is focused on monitoring your environment and alerting you to potential security threats. On its own, it does not enforce compliance - this is possible through Azure Policy.

🔗 https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-policy

#33

When configuring Azure Firewall, which type of rule is specific to Azure Firewall and allows it to access fully qualified domain names from a subnet?

✓

Application rules

✗

Network rules

✗

Network Security Group rules

✗

Application Security Group rules

Explanation

Azure Firewall supports rules and rule collections. A rule collection is a set of rules that share the same order and priority. Rule collections are executed in order of their priority. Network rule collections are higher priority than application rule collections, and all rules are terminating.

There are three types of rule collections:

Application rules: Configure fully qualified domain names (FQDNs) that can be accessed from a subnet.
Network rules: Configure rules that contain source addresses, protocols, destination ports, and destination addresses.
NAT rules: Configure DNAT rules to allow incoming connections.

https://docs.microsoft.com/en-us/azure/firewall/firewall-faq#what-are-some-azure-firewall-concepts
#34

You want to connect the Azure VNets for three separate branch offices. You are designing a hub and spoke model network topology to do this. The central hub will serve as a firewall between the different locations during backend communication, and also a central location for disaster recovery backup storage. Now you are considering whether to connect your hub-and-spoke model with VNet peering connections or Azure VPN Gateways. Each option has its own benefits. Which statements comparing VNet peering and VPN Gateways in a hub-and-spoke model are correct? (Choose 2 answers)

✓

If you implement the model with Azure VPN Gateways, all VNets **can be cross-region.**

If you implement the model with VNet peering connections, the VNets **can be cross-region with Global VNet Peering.**

✓

Whether the connections are made with Azure VPN Gateways or VNet peering connections, the VNets can be **within different Azure subscriptions** and associated **with separate Azure AD tenants**.

✗

If you implement the model with Azure VPN Gateways, all VNets **can be in different regions**.

If you implement the model with VNet peering connections, the VNets **must be in the same region**.

✕

If you implement the model with Azure VPN Gateways, the VNets can be **within different Azure subscriptions** that are **associated with the same Azure tenant.**

If you implement the VNets with VNet peering connections, the VNets can be **within different Azure subscriptions** and **associated with separate Azure AD tenants**.

Explanation

You could accomplish this network topology using VNet peering or Azure VPN Gateways, but each option has its requirements and limitations.

1. Connecting via VNet peering would require a router to be deployed in the central hub VNet, but this is not required for VNG connections.
2. VNet peering works both across separate tenants and subscriptions.
3. Hostname resolution is not possible for VMs connecting from different VNets through a peering connection. Azure DNS is required for these VMs to connect. However, name resolution is possible through a VNG connection.
4. VNets must be connected via Global VNet Peering.

/course/azure-network-connectivity-name-resolution/virtual-network-peering/

Covered in this lecture

Virtual Network Peering

Course:Azure Network Connectivity and Name Resolution

4m

#35

You are configuring security settings for your Azure Data Lake, and want to integrate a Data Lake service endpoint within an existing VNet. Which steps should you implement to configure this? (Choose 2 answers)

✕

Configure your Azure Data Lake in the same resource group as your VNet

✓

Configure a Microsoft Azure Active Directory Service endpoint

✓

Deploy the endpoint in your selected VNET

✗

Disable connectivity from Azure services outside of the selected VNET

Explanation

To use virtual network integration with data lake storage gen1, you must create a virtual network in the same region as your data lake storage account. You need to configure a service endpoint with the Microsoft Azure Active Directory as the service. After creating your virtual network in the same region as your data lake, you need to go to your data lake and click on Firewall and virtual networks. Choose the Selected network radio button and then Add existing virtual network. In the Add networks blade, select your virtual network and the subnet and click Add. Below the firewall section under exceptions, you can enable connectivity from Azure services outside of your selected network.

/course/configuring-azure-application-and-data-security/securing-azure-data-lake-storage-with-virtual-network-integration/

Covered in this lecture

Securing Azure Data Lake Storage with Virtual Network Integration

Course:Configuring Azure Application and Data Security

1m

#36

In comparison to Azure Kubernetes Clusters (AKS), how does the Azure Container Instances (ACI) service offer an increased level of security better-suited for multi-tenant environments?

✗

ACI offers fine-grained permission controls through Azure Active Directory that is currently not supported by AKS.

✗

ACI can be deployed into VNets while AKS clusters cannot.

✓

ACI offers greater application isolation with the use of a hypervisor.

✗

ACI integrates with Azure Security Center while AKS clusters do not.

Explanation

Historically, containers have offered application dependency isolation and resource governance but have not been considered sufficiently hardened for hostile multi-tenant usage. Azure Container Instances guarantees your application is as isolated in a container as it would be in a VM.

https://docs.microsoft.com/en-us/azure/container-instances/container-instances-overview#hypervisor-level-security

Covered in this lecture

Container-Related Services in Azure

Course:Building Containers with Azure DevOps

4m

#37

What actions does the following Azure Blob Storage lifecycle policy implement? { "rules": [{   "name": "agingRule",   "enabled": true,   "type": "Lifecycle",   "definition": { "filters": {   "blobTypes": ["blockBlob"],   "prefixMatch": ["container1/sample"] },   "actions": {   "baseBlob": {   "tierToCool": { "daysAfterModificationGreaterThan": 30 },   "tierToArchive": { "daysAfterModificationGreaterThan": 90 }   }   }   }   }]}

✓

It moves block blobs in a container1 with object names starting with "sample" to the cool tier after 30 days since the last update, and to the archive tier after 90 days since the last update.

✗

It moves all block blobs in the container named "container1/sample" to cool tier after 30 days since the last update, and to the archive tier after 120 days since the last update.

✗

It moves all blobs in container1 with object name starting "sample" to the cools tier after 30 days since the last update, and to the archive tier after 90 days since the last update.

✗

It moves block blobs in container1 with object names starting with "sample" to the cool tier after 30 days since the last update, and to the archive tier after 120 days since the last update.

Explanation

Reviewing the lifecycle policy, it deals with block blobs in container1 with an object name starting with "sample". The lifecycle rules move the objects to cool and then archive after 30 or 90 days since the object was last updated, not since it was originally uploaded.

The actions, moving to cool or archive, are implemented after the stated amount of time has passed, and the time period for one action also counts toward the time period for any subsequent actions. This means after the object is moved to the cool tier, the 30-day duration also counts toward moving the object to archive, so only 60 additional days would need to pass without an update for a given object to be moved to the archive tier. So only 90 days have to pass without an update, not 120, for any object affected by this policy to move to the archive tier.

🔗 https://docs.microsoft.com/en-us/azure/storage/blobs/storage-lifecycle-management-concepts?tabs=azure-portal#policy

#38

Of the following choices, which is the name of the most current Active Directory synchronization tool?

✓

Azure AD Connect

✕

Azure Active Directory Synchronization Services (DirSync)

✕

Azure Active Directory Synchronization Services (AAD Sync)

✕

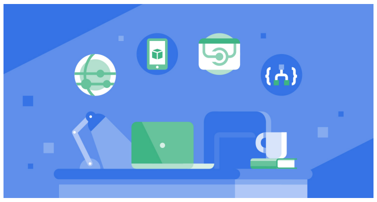
Forefront Identity Manager (FIM)

Explanation

Azure AD Connect is the most current Active Directory synchronization tool. The other tools are considered legacy and/or deprecated but still functional.

🔗 https://docs.microsoft.com/en-us/microsoft-365/enterprise/deploy-microsoft-365-directory-synchronization-dirsync-in-microsoft-azure?view=o365-worldwide

Covered in this lecture
Deploy Azure AD Connect
Course:Designing for Azure Identity Management



3m

#39

How does Just in Time Virtual Machine Access reduce attack exposure?

✗

Turning VMs off when they're not in use

✗

Blocking outbound access to VMs

✗

Controlling the applications that can be run

✓

Reducing access to VMs

Explanation

Just in time virtual machine access reduces your attack exposure by allowing you to deny persistent access to VMs.

https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time

Covered in this lecture
Managing Access to Resources with JIT Provisioning
Course:Implementing Azure Network Security

2m

#40

You are the senior Azure SQL Database architect for a Wall Street brokerage firm. Your firm has numerous governmental regulations that require retention of the automatic full Azure SQL database backups for 7 years, which is far beyond Azure's Database automatic backup feature of 7-35 days. What does Microsoft recommend as the best way to accomplish your long backup requirements?

✗

Use the Azure SQL Database Geo-replication tool as it can handle backups for that time period.

✓

Use the Azure SQL Database Long-Term Backup Retention feature.

✗

Run nightly tape backup jobs and store the tapes in a third-party vault offsite.

✗

Use a third-party backup and recovery tool to store the databases for seven years on a rotating basis.

Explanation

The Long-Term Backup Retention feature enables you to store your Azure SQL Database backups in an Azure Recovery Services vault for up to 10 years. This feature can be used for applications that have regulatory, compliance, or other business purposes that require you to retain the automatic full database backups beyond the 7-35 days provided by SQL Database's automatic backups.

https://docs.microsoft.com/en-us/azure/sql-database/sql-database-long-term-retention
Covered in this lecture
Database Backups
Course:Implementing High Availability and Disaster Recovery for Azure SQL Databases

13m