Answer Sheet

Q1) What is the maximum priority value that can be assigned to a Azure security rule ?

- No limit
- 9999
- 99999
- ✅ None of these

Explanation:-Rule priority, between 100 (highest priority) and 4096 (lowest priority). Must be unique for each rule in the collection. Refer: https://docs.microsoft.com/en-us/cli/azure/network/nsg/rule#:~:text=Rule%20priority%2C%20between%20100%20(highest,each%20rule%20in%20the%20collection.

Q2) Which of the following is not required if creating a network interface in Azure?

- ✅ Network security group

Explanation:-A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol. Refer: https://docs.microsoft.com/en-us/azure/virtual-network/security-overview

- Name
- Virtual network
- Subnet

Q3) If creating a network interface in Azure, which value for private IP address assignment field enables Azure automatically assigning the next available address from the address space?

- ✅ Dynamic

Explanation:-Private IP address assignment method - Dynamic: Azure assigns the next available address for the subnet address range the network interface is deployed in. Static: You assign an unused address for the subnet address range the network interface is deployed in. Refer: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface-addresses

- Automatic
- Auto
- System

Q4) The size of the AzureFirewallSubnet subnet is _____.

- /8
- /16
- /24
- ✅ None of these

Explanation:-The size of the AzureFirewallSubnet subnet is /26. For more information about the subnet size, see Azure Firewall FAQ. On the Azure portal menu or from the Home page, select Create a resource. Select Networking > Virtual network. Refer: https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal#:~:text=The%20size%20of%20the%20AzureFirewallSubnet,Select%20Networking%20%3E%20Virtual%20network.

Q5) How many private IP address per instance are used by Azure Application Gateway with no private front-end IP?

- 4
- 2
- ✅ 1

Explanation:-Application Gateway uses one private IP address per instance, plus another private IP address if a private front-end IP is configured. Refer: https://docs.microsoft.com/en-us/azure/application-gateway/configuration-overview#:~:text=Application%20Gateway%20uses%20one%20private,front%2Dend%20IP%20is%20configured.

- Depends upon available IP addresses

Q6) How many IP addresses in each subnet are reserved for internal use by Azure Application Gateway with no private front-end IP?

- ✅ 5

Explanation:-Azure also reserves five IP addresses in each subnet for internal use: the first four and the last IP addresses. For example, consider 15 application gateway instances with no private front-end IP. You need at least 20 IP addresses for this subnet: five for internal use and 15 for the application gateway instances. Refer: https://docs.microsoft.com/en-us/azure/application-gateway/configuration-overview#:~:text=Azure%20also%20reserves%20five%20IP,for%20the%20application%20gateway%20instances.

- 4
- 3
- 6

Q7) Which Microsoft cloud services can be connected with ExpressRoute?

- ✅ All of these

Explanation:-With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure and Office 365. Connectivity can be from an any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a co-location facility. Refer: https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction#:~:text=With%20ExpressRoute%2C%20you%20can%20establish,at%20a%20co%2Dlocation%20facility.

- Office 365
- Microsoft Azure

Q8) State whether the following statement holds correct or not.

"Changing the metering plan from Unlimited Data to Metered Data is not supported in ExpressRoute."

✅ CORRECT
Explanation:-Changing the metering plan from Unlimited Data to Metered Data is not supported. Refer: https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-circuit-portal-resource-manager
⚪ INCORRECT

Q9) Which Azure Virtual WAN type supports Site-to-site VPN only?

✅ Basic
Explanation:-Refer :https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-site-to-site-portal
⚪ Standard

Q10) Which Azure Virtual WAN type supports ExpressRoute?

⚪ Basic
✅ Standard
Explanation:-There are two types of virtual WANs: Basic and Standard. The following table shows the available configurations for each type.

Basic - Site-to-site VPN only

Standard -ExpressRoute, User VPN (P2S) VPN (site-to-site), Inter-hub and VNet-to-VNet transiting through the virtual hub

Refer: https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about

---

Q11) What of the following is not an advantage of Virtual WAN?

⚪ Integrated connectivity solutions in hub and spoke
⚪ Automated spoke setup and configuration
Explanation:-
⚪ Intuitive troubleshooting
✅ Fully managed container orchestration service
Explanation:-Virtual WAN offers the following advantages: 1. Integrated connectivity solutions in hub and spoke: Automate site-to-site configuration and connectivity between on-premises sites and an Azure hub. 2. Automated spoke setup and configuration: Connect your virtual networks and workloads to the Azure hub seamlessly. 3. Intuitive troubleshooting: You can see the end-to-end flow within Azure, and then use this information to take required actions. Refer: https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about

---

Q12) Identify the Azure Virtual WAN type which supports User VPN (P2S).

⚪ Basic
✅ Standard
Explanation:-There are two types of virtual WANs: Basic and Standard. The following table shows the available configurations for each type.

Basic - Site-to-site VPN only

Standard -ExpressRoute, User VPN (P2S) VPN (site-to-site), Inter-hub and VNet-to-VNet transiting through the virtual hub

Refer: https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about

---

Q13) Identify the DNS record which designate the primary name server and administrator responsible for a zone.

✅ SOA
⚪ MX
⚪ CNAME
⚪ AAAA

Q14) Which of the following DNS record contain arbitrary text and can also be used to define machine-readable data, such as security or abuse prevention information?

✅ TXT
Explanation:-Text record, which can contain arbitrary text and can also be used to define machine-readable data, such as security or abuse prevention information.
⚪ MX
⚪ CNAME
⚪ AAAA

Q15) State whether the following statement holds correct or not.

"Azure DNS name servers resolve over IPv6."

✅ Correct
Explanation:-Yes. Azure DNS name servers are dual stack. Dual stack means they have IPv4 and IPv6 addresses. To find the IPv6 address for the Azure DNS name servers assigned to your DNS zone, use a tool such as nslookup. An example is nslookup -q=aaaa . Refer: https://docs.microsoft.com/en-us/azure/dns/dns-faq
⚪ Incorrect

Q16) Which value in source port ranges field, will allow traffic on any port while configuring a inbound security rule?

- Allow
- All
- No value, let it be blank
- ✓ None of these

Q17) Which IP address should be listed in the source IP address field while configuring a inbound security rule, if the IP address to be specified is assigned to an Azure VM?

- ✓ Its private IP address

Explanation:-Reference: https://docs.microsoft.com/en-us/azure/virtual-network/security-overview

- Its public IP address

Q18) A lower priority value of a Azure security rule will have _____.

- ✓ Higher priority in processing

Explanation:-A number between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops. As a result, any rules that exist with lower priorities (higher numbers) that have the same attributes as rules with higher priorities are not processed. Refer: https://docs.microsoft.com/en-us/azure/virtual-network/security-overview

- Lower priority in processing

Q19) Which Azure Virtual WAN type supports Inter-hub and VNet-to-VNet transiting through the virtual hub?

- Basic
- ✓ Standard

Explanation:-Virtual WAN allows transit connectivity between VNets. VNets connect to a virtual hub via a virtual network connection. Transit connectivity between the VNets in Standard Virtual WAN is enabled due to the presence of a router in every virtual hub. This router is instantiated when the virtual hub is first created. Refer: https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about

Q20) Does the on-premises VPN device connect to multiple Hubs in Azure VirtualWAN?

- ✓ Yes

Explanation:-A connection is an active-active tunnel from the on-premises VPN device to the virtual hub. You can have one hub per region, which means you can connect more than 1,000 branches across hubs. Refer: https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about#:~:text=A%20connection%20is%20an%20active,than%201%2C000%20branches%20across%20hubs.

- No

Q21) Does Azure VirtualWAN support BGP?

- ✓ Yes

Explanation:-Configuring BGP on a Virtual WAN is equivalent to configuring BGP on an Azure virtual network gateway VPN. Your on-premises BGP peer address must not be the same as the public IP address of your VPN to device or the VNet address space of the VPN site. Refer: https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-site-to-site-portal#:~:text=Configuring%20BGP%20on%20a%20Virtual,space%20of%20the%20VPN%20site.

- No

Q22) Which role helps you manage all Azure resources, including access in Azure Active Directory?

- Azure AD Global administrator
- Account Administrator
- Service Administrator
- ✓ Owner

Explanation:-Owner - Has full access to all resources including the right to delegate access to others. Contributor - Can create and manage all types of Azure resources but can't grant access to others. Reader - Can view existing Azure resources. User Access Administrator - Lets you manage user access to Azure resources. Link - https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-steps

Q23) Which Azure Active Directory role, is a classic role and is conceptually the billing owner of a subscription with access to the Azure Account Center?

- ✓ Account Administrator

Explanation:-Account Administrator - This classic subscription administrator role is conceptually the billing owner of a subscription. This role has access to the Azure Account Center and enables you to manage all subscriptions in an account. For more information, see Classic subscription administrator roles, Azure Role-based access control (RBAC) roles, and Azure AD administrator roles. Refer: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

- Owner
- Service Administrator
- Azure AD Global administrator

Q24) Select the Azure Active Directory role which is a classic subscription role which enables you to manage all Azure resources, including access.

✅ Service Administrator

Explanation:-Service Administrator - This classic subscription administrator role enables you to manage all Azure resources, including access. This role has the equivalent access of a user who is assigned the Owner role at the subscription scope. For more information, see Classic subscription administrator roles, Azure RBAC roles, and Azure AD administrator roles. Refer: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

- Account Administrator
- Owner
- Azure AD Global administrator

Q25) Select the Azure Active Directory role which is automatically assigned to whom ever created the Azure AD tenant.

- Service Administrator

Explanation:-Azure AD Global administrator - This administrator role is automatically assigned to whomever created the Azure AD tenant. Global administrators can do all of the administrative functions for Azure AD and any services that federate to Azure AD, such as Exchange Online, SharePoint Online, and Skype for Business Online. You can have multiple Global administrators, but only Global administrators can assign administrator roles (including assigning other Global administrators) to users. Note that this administrator role is called Global administrator in the Azure portal, but it's called Company administrator in the Microsoft Graph API and Azure AD PowerShell. For more information about the various administrator roles, see Administrator role permissions in Azure Active Directory. Refer: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

- Account Administrator
- Owner
- ✅ Azure AD Global administrator

Q26) Which file type is used for bulk upload of group members in Azure Active Directory?

✅ CSV

Explanation:-Using Azure Active Directory (Azure AD) portal, you can add a large number of members to a group by using a comma-separated values (CSV) file to bulk import group members. Refer: https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-bulk-import-members#:~:text=Using%20Azure%20Active%20Directory%20(Azure,to%20bulk%20import%20group%20members.

- XLS
- XLSX
- None of these

Q27) Which approach for managing Azure AD joined device involves policies being delivered as part of the MDM enrolment process?

✅ MDM-only

Explanation:-A cloud-based MDM is a SaaS application that provides device management capabilities in the cloud. It is a multi-tenant application. This application is registered with Azure AD in the home tenant of the MDM vendor.

- Co-management

Q28) Which approach for managing Azure AD joined device involves SCCM agent being installed on an MDM-managed device?

- MDM-only
- ✅ Co-management

Explanation:-Refer: https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview

---

Q29) Which authentication method is not applicable for Self-Service Password Reset (SSPR)?

- Email address
- ✅ App passwords

Explanation:-Azure Active Directory (Azure AD) self-service password reset (SSPR) gives users the ability to change or reset their password, with no administrator or help desk involvement. If a user's account is locked or they forget their password, they can follow prompts to unblock themselves and get back to work. This ability reduces help desk calls and loss of productivity when a user can't sign in to their device or an application. Refer: https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr

- Security questions
- Password

Q30) Which authentication method is not applicable for MFA?

- Password
- ✅ Email address
- SMS
- Voice call

Q31) Which setting is recommended for Write back passwords to on-premises AD in SSPR?

- Azure AD Identity Protection.
- ✅ Password writeback

Explanation:-Enable password writeback for SSPR - Sign in to the Azure portal using a global administrator account. Search for and select Azure Active Directory, select Password reset, then choose On-premises integration.

- Azure AD Connect.

Q32) Does SSPR allow users to unlock account without resetting password in SSPR?

✅ Yes

Explanation:-SSPR Allow users to unlock account without resetting password. Refer: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment

⚪ No

Q33) State whether the following statement holds correct or not.

"Under SSPR, on-premises admin accounts can only change their password in their on-premises environment."

✅ Yes

⚪ No

Q34) State whether the following statement holds correct or not.

"In SSPR, on-premises admin accounts can use the secret questions and answers as a method to reset their password."

✅ No

Explanation:-By default, administrator accounts are enabled for self-service password reset, and a strong default two-gate password reset policy is enforced. This policy may be different from the one you have defined for your users, and this policy can't be changed. You should always test password reset functionality as a user without any Azure administrator roles assigned.

With a two-gate policy, administrators don't have the ability to use security questions.

Refer: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#security%20questions

If SSPR is enabled, you must select at least one of the following options for the authentication methods. Sometimes you hear these options referred to as "gates." We highly recommend that you choose two or more authentication methods so that your users have more flexibility in case they are unable to access one when they need it. Additional details about the methods listed below can be found in the article The authentication methods are Mobile app notification, Mobile app code, Email, Mobile phone, Office phone, and Security questions. Refer: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks

⚪ Yes

Q35) Under RBAC, which of the following is an identity in Azure Active Directory that is automatically managed by Azure?

✅ Managed Identity

Explanation:-Managed identity - An identity in Azure Active Directory that is automatically managed by Azure. You typically use managed identities when developing cloud applications to manage the credentials for authenticating to Azure services. Refer: https://docs.microsoft.com/en-us/azure/role-based-access-control/overview

⚪ service principal

⚪ group

⚪ user
