Answer Sheet

Q1)

You have an Active Directory forest named contoso.com. You install and configure Azure AD Connect to use password hash synchronization as the single sign-on (SSO) method. Staging mode is enabled. You review the synchronization results and discover that the Synchronization Service Manager does not display any sync jobs.

You need to ensure that the synchronization completes successfully and that exports, imports and synchronization could run.

What should you do?

- From Synchronization Service Manager, run a full import.
- From Azure PowerShell, run Start-AdSyncSyncCycle "PolicyType Initial.
- Run Azure AD Connect and set the SSO method to Pass-through Authentication.
- ✅ Run Azure AD Connect and disable staging mode.

Explanation:-Staging mode must be disabled. If the Azure AD Connect server is in staging mode, password hash synchronization is temporarily disabled.

Q2) Which of the following is a fundamental sources of metrics collected by Azure Monitor, created by Azure resources and give you visibility into their health and performance?

- Guest OS metrics
- ✅ Platform metrics

Explanation:-There are three fundamental sources of metrics collected by Azure Monitor. Once these metrics are collected in the Azure Monitor metric database, they can be evaluated together regardless of their source.

Platform metrics are created by Azure resources and give you visibility into their health and performance. Each type of resource creates a distinct set of metrics without any configuration required. Platform metrics are collected from Azure resources at one-minute frequency unless specified otherwise in the metric's definition.

Guest OS metrics are collected from the guest operating system of a virtual machine. Enable guest OS metrics for Windows virtual machines with Windows Diagnostic Extension (WAD) and for Linux virtual machines with InfluxData Telegraf Agent.

Application metrics are created by Application Insights for your monitored applications and help you detect performance issues and track trends in how your application is being used. This includes such values as Server response time and Browser exceptions.

Custom metrics are metrics that you define in addition to the standard metrics that are automatically available. You can define custom metrics in your application that's monitored by Application Insights or create custom metrics for an Azure service using the custom metrics API.

Refer: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-platform-metrics

- Application metrics
- None of these

Q3) Which metric type is created by Azure resources?

- Guest OS metrics
- ✅ Platform metrics

Explanation:-There are three fundamental sources of metrics collected by Azure Monitor. Once these metrics are collected in the Azure Monitor metric database, they can be evaluated together regardless of their source.

Platform metrics are created by Azure resources and give you visibility into their health and performance. Each type of resource creates a distinct set of metrics without any configuration required. Platform metrics are collected from Azure resources at one-minute frequency unless specified otherwise in the metric's definition.

Guest OS metrics are collected from the guest operating system of a virtual machine. Enable guest OS metrics for Windows virtual machines with Windows Diagnostic Extension (WAD) and for Linux virtual machines with InfluxData Telegraf Agent.

Application metrics are created by Application Insights for your monitored applications and help you detect performance issues and track trends in how your application is being used. This includes such values as Server response time and Browser exceptions.

Custom metrics are metrics that you define in addition to the standard metrics that are automatically available. You can define custom metrics in your application that's monitored by Application Insights or create custom metrics for an Azure service using the custom metrics API.

Refer: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-platform-metrics

- Application metrics
- None of these

Q4) What is the default frequency of collecting platform metrics?

- ✅ one minute

Explanation:-Platform metrics are collected from Azure resources at one-minute frequency unless specified otherwise in the metric's definition.
Refer: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-platform-metrics

- 30 seconds
- two minute
- five minute

Q5) Which metric type includes Server response time?

- Guest OS metrics

Explanation:-Application metrics are created by Application Insights for your monitored applications and help you detect performance issues and track trends in how your application is being used. This includes such values as Server response time and Browser exceptions. Refer: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-platform-metrics

- Platform metrics
- ✔ Application metrics
- None of these

Q6) Which metric type includes Browser exceptions?

- Guest OS metrics

Explanation:-Application metrics are created by Application Insights for your monitored applications and help you detect performance issues and track trends in how your application is being used. This includes such values as Server response time and Browser exceptions. Refer: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-platform-metrics

- Platform metrics
- ✔ Application metrics
- None of these

Q7) Which metric type is applicable for Windows virtual machines with Windows Diagnostic Extension?

- ✔ Guest OS metrics

Explanation:-Guest OS metrics are collected from the guest operating system of a virtual machine. Enable guest OS metrics for Windows virtual machines with Windows Diagnostic Extension (WAD) and for Linux virtual machines with InfluxData Telegraf Agent. Refer: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-platform-metrics

- Platform metrics
- Application metrics
- None of these

Q8) Platform metrics are stored for _____.

- ✔ 93 days

Explanation:-These are performance counters collected by the Windows Diagnostic Extension (WAD) and sent to the Azure Monitor data sink, or via the InfluxData Telegraf Agent on Linux machines. Retention for these metrics is 93 days. Refer: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-platform-metrics

- 31 days
- 14 days
- 2 years

Q9) Azure Monitor starts collecting data from Azure resources when _____.

- they are first used
- they are added to a VPC
- ✔ they are created

Explanation:-As soon as you create an Azure resource, Azure Monitor is enabled and starts collecting metrics and activity logs which you can view and analyze in the Azure portal. With some configuration, you can gather additional monitoring data and enable additional features. Refer: https://docs.microsoft.com/en-us/azure/azure-monitor/insights/monitor-azure-resource#:~:text=As%20soon%20as%20you%20create,data%20and%20enable%20additional%20features.

- they generate their first error

Q10) What does the Activity log do not provide?

- when a resource is created
- when a resource is modified
- when a job is started
- ✔ None of these

Explanation:-The Activity log is a platform log in Azure that provides insight into subscription-level events. This includes such information as when a resource is modified or when a virtual machine is started. You can view the Activity log in the Azure portal or retrieve entries with PowerShell and CLI. For additional functionality, you should create a diagnostic setting to send the Activity log to Azure Monitor Logs, to Azure Event Hubs to forward outside of Azure, or to Azure Storage for archiving. This article provides details on viewing the Activity log and sending it to different destinations. Refer: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-log

---

Q11) Which functionality on Azure Monitor log queries in the Azure portal, is not provided by Log Analytics?

- Writing Azure Monitor log queries
- Executing Azure Monitor log queries
- Managing Azure Monitor log queries
- ✔ Correlating Activity log data with other monitoring data collected by Azure Monitor

Explanation:-Send the Activity log to a Log Analytics workspace to enable the features of Azure Monitor Logs which includes the following: Correlate Activity log data with other monitoring data collected by Azure Monitor. Consolidate log entries from multiple Azure subscriptions and tenants into one location for analysis together. Use log queries to perform complex analysis and gain deep insights on Activity Log entries. Use log alerts with Activity entries allowing for more complex alerting logic. Store Activity log entries for longer than 90 days. No data ingestion or data retention charge for Activity log data stored in a Log Analytics workspace. Refer: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-log

---

Q12) Which character separates commands while writing Azure Monitor log queries?

- ✔ |

Explanation:-Refer: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-log

- ;

- :
- ,

Q13) What is the maximum result limit for Log Analytics?

- ✅ 10000 rows

Explanation:-Maximum records returned by a log query - 10,000. Reduce results using query scope, time range, and filters in the query. Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/service-limits

- 5000 rows
- 25000 rows
- 50000 rows

Q14) How many past days data can be included in table or chart that is pinned to a shared dashboard in Log Analytics?

- ✅ 14 days

Explanation:-A table or chart that you pin to a shared dashboard has the following simplifications: Data is limited to the past 14 days. Refer: https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-portal#:~:text=A%20table%20or%20chart%20that,to%20the%20past%2014%20days.

- 7 days
- 15 days
- 30 days

Q15) The schema tables appear on which tab of the Log Analytics workspace?

- The Schema tab
- ✅ The Tables tab

Explanation:-The schema tables appear on the Tables tab of the Log Analytics workspace. The tables contain columns, each with a data type shown by the icon next to the column name. Refer: https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-portal#:~:text=The%20schema%20tables%20appear%20on,next%20to%20the%20column%20name.

- The design tab
- None of these

Q16) What refers to the look back window over which metric values are checked, while configuring a static threshold metric alert rule?

- ✅ Period

Explanation:-Period (The look back window over which metric values are checked) Refer: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric-overview

- Timeslot
- Lookback
- Timeslice

Q17) Which alert threshold sensitivity level will result in more alerts on smallest deviation?

- ✅ High level

Explanation:-Alert threshold sensitivity is a high-level concept that controls the amount of deviation from metric behavior required to trigger an alert. This option doesn't require domain knowledge about the metric like static threshold. The options available are:

High – The thresholds will be tight and close to the metric series pattern. An alert rule will be triggered on the smallest deviation, resulting in more alerts.

Medium – Less tight and more balanced thresholds, fewer alerts than with high sensitivity (default).

Low – The thresholds will be loose with more distance from metric series pattern. An alert rule will only trigger on large deviations, resulting in fewer alerts.

Refer: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-dynamic-thresholds

- Low Level

Q18) Under which alert threshold sensitivity level, alert rule will trigger on large deviation?

- ✅ Low Level

Explanation:-Alert threshold sensitivity is a high-level concept that controls the amount of deviation from metric behavior required to trigger an alert. This option doesn't require domain knowledge about the metric like static threshold. The options available are:

High – The thresholds will be tight and close to the metric series pattern. An alert rule will be triggered on the smallest deviation, resulting in more alerts.

Medium – Less tight and more balanced thresholds, fewer alerts than with high sensitivity (default).

Low – The thresholds will be loose with more distance from metric series pattern. An alert rule will only trigger on large deviations, resulting in fewer alerts.

Refer: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-dynamic-thresholds

- High level

Q19) Which of the following Application Insights cannot monitor?

- ✅ None of these

Explanation:-Refer: https://azuredevopslabs.com/labs/vsts/monitor/

- Page views
- AJAX calls
- Exceptions

Q20) Which peering type in Azure, connect virtual networks within the same Azure region?

- Whole network peering
- Universal network peering
- ✅ Virtual network peering

Explanation:-Virtual network peering enables you to seamlessly connect networks in Azure Virtual Network. The virtual networks appear as one for connectivity purposes. The traffic between virtual machines uses the Microsoft backbone infrastructure. Like traffic between virtual machines in the same network, traffic is routed through Microsoft's private network only.

Azure supports the following types of peering:

Virtual network peering: Connect virtual networks within the same Azure region. Global virtual network peering: Connecting virtual networks across Azure regions.

Refer: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

- Global network peering

Q21) Which peering type in Azure, connect virtual networks across the Azure region?

- ✅ Global network peering

Explanation:-Virtual network peering enables you to seamlessly connect networks in Azure Virtual Network. The virtual networks appear as one for connectivity purposes. The traffic between virtual machines uses the Microsoft backbone infrastructure. Like traffic between virtual machines in the same network, traffic is routed through Microsoft's private network only.

Azure supports the following types of peering:

Virtual network peering: Connect virtual networks within the same Azure region. Global virtual network peering: Connecting virtual networks across Azure regions.

Refer: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

- Local network peering
- Universal network peering
- Virtual network peering

Q22) Network traffic between peered virtual networks is for _____.

- ✅ private only

Explanation:-Virtual network peering enables you to seamlessly connect networks in Azure Virtual Network. The virtual networks appear as one for connectivity purposes. The traffic between virtual machines uses the Microsoft backbone infrastructure. Like traffic between virtual machines in the same network, traffic is routed through Microsoft's private network only. Refer: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

- public uses internet only
- mixed both public and private

Q23) What should be the status of connectivity between peered virtual networks, if you want to apply network security groups to block or deny specific access?

- Close the network security group rules between the virtual networks
- ✅ Open full connectivity between peered virtual networks

Explanation:-You can apply network security groups in either virtual network to block access to other virtual networks or subnets. When configuring virtual network peering, either open or close the network security group rules between the virtual networks. If you open full connectivity between peered virtual networks, you can apply network security groups to block or deny specific access. Full connectivity is the default option. To learn more about network security groups, see Security groups. Refer: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

---

Q24) What is the default connectivity option when configuring virtual network peering?

- ✅ Full connectivity

Explanation:-You can apply network security groups in either virtual network to block access to other virtual networks or subnets. When configuring virtual network peering, either open or close the network security group rules between the virtual networks. If you open full connectivity between peered virtual networks, you can apply network security groups to block or deny specific access. Full connectivity is the default option. To learn more about network security groups, see Security groups. Refer: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

- Connectivity as per security groups

Q25) Gateway transit is not supported by _____.

- Global virtual network peering
- ✅ Whole network peering

Explanation:-Gateway transit between virtual networks created through different deployment models is supported. The gateway must be in the virtual network in the Resource Manager model. To learn more about using a gateway for transit, see Configure a VPN gateway for transit in a virtual network peering. Refer: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

- Virtual network peering

Q26) Bidirectional link creation in VNet peering amongst virtual networks, is indicated by which state?

- Started
- ✅ Connected
- Initiated
- Ready

Q27) Single link creation in VNet peering amongst virtual networks, is indicated by which state?

- Started
- Connected
- ✅ Initiated
- Ready

Q28) A VNet peering connection between virtual networks routes traffic between them through _____.

- IPv6 addresses
- ✅ IPv4 addresses

Q29) Is peering of a VNet with a VNet in a different subscription allowed?

- ✅ Yes

Explanation:-You can create a peering between two virtual networks. The networks can belong to the same subscription, different deployment models in the same subscription, or different subscriptions. Refer: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

- No

Q30) Can VNet peering be done between two VNets with matching or overlapping address ranges?

- ✅ No

Explanation:-No. Address spaces must not overlap to enable VNet Peering. Refer: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-faq

- Yes

Q31) Which encryption is used by VNet peering traffic?

- ✅ None of these

Explanation:-IPsec is an IETF standard. It encrypts data at the Internet Protocol (IP) level or Network Layer 3. You can use IPsec to encrypt an end-to-end connection between your on-premises network and your virtual network (VNET) on Azure. Refer: https://docs.microsoft.com/en-us/azure/expressroute/expressroute-about-encryption

- HTTPS
- SSL
- TLS

Q32) Is transitive peering supported in VNet peering?

- ✅ No

Explanation:-Azure supports the following types of peering: Virtual network peering: Connect virtual networks within the same Azure region. Global virtual network peering: Connecting virtual networks across Azure regions. Refer: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

- Yes

Q33) What can be used to create a virtual network peering?

- Azure PowerShell
- ✅ All of these

Explanation:-Refer: https://docs.microsoft.com/en-us/azure/virtual-network/

- The Azure command-line interface (CLI)
- The Azure portal

Q34) Which of the following will prevent management overhead?

- ✅ Fewer large VNets

Explanation:-With gateway transit enabled on VNet peering, you can create a transit VNet that contains your VPN gateway, Network Virtual Appliance, and other shared services. As your organization grows with new applications or business units and as you spin up new VNets, you can connect to your transit VNet with VNet peering. This prevents adding complexity to your network and reduces management overhead of managing multiple gateways and other appliances. Refer: https://azure.microsoft.com/en-us/blog/vnet-peering-and-vpn-gateways/

- Multiple small VNets

Q35) State whether the following statement holds correct or not.

"All resources in a VNet can communicate outbound to the internet, by default."

- ✅ CORRECT

Explanation:-All resources in a VNet can communicate outbound to the internet, by default. You can communicate inbound to a resource by assigning a public IP address or a public Load Balancer. Refer: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview

INCORRECT

Q36) Which connection type of on-premises computers and networks to a Azure virtual network, is between a virtual network and a single computer?

Site-to-site VPN

Point-to-site virtual private network (VPN)

Explanation:-point-to-Site VPN connections are useful when you want to connect to your VNet from a remote location, such when you are telecommuting from home or a conference. You can also use P2S instead of a Site-to-Site VPN when you have only a few clients that need to connect to a VNet. Point-to-Site connections do not require a VPN device or a public-facing IP address. P2S creates the VPN connection over either SSTP (Secure Socket Tunneling Protocol), or IKEv2. Refer: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal

Azure ExpressRoute

Q37) Which of the following indicates these two features - Connection is private and traffic does not go over the internet?

Site-to-site VPN

Azure ExpressRoute

Explanation:-Azure ExpressRoute: Established between your network and Azure, through an ExpressRoute partner. This connection is private. Traffic does not go over the internet.

Refer: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview

Point-to-site virtual private network (VPN)

Network security groups

Q38) Which connection type of on-premises computers and networks to a Azure virtual network, does not go over the internet?

Site-to-site VPN

Azure ExpressRoute

Explanation:-ExpressRoute. ExpressRoute enables you to extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. This connection is private. Traffic does not go over the internet. Refer: https://docs.microsoft.com/en-us/azure/networking/networking-overview

Point-to-site virtual private network (VPN)

Q39) A primary IP configuration has _____.

a private IPv4 address

Explanation:-Each network interface is assigned one primary IP configuration. A primary IP configuration:

Has a private IPv4 address assigned to it. You cannot assign a private IPv6 address to a primary IP configuration. May also have a public IPv4 address assigned to it. You cannot assign a public IPv6 address to a primary (IPv4) IP configuration. Refer: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface-addresses

a private IPv6 address

Q40) State whether the following statement holds correct or not.

"Azure DNS supports DNSSEC."

TRUE

FALSE

Explanation:-No. Azure DNS doesn't currently support the Domain Name System Security Extensions (DNSSEC). Refer: https://docs.microsoft.com/en-us/azure/dns/dns-faq

Q41) State whether the following statement holds correct or not.

"Azure DNS support zone transfers."

TRUE

FALSE

Explanation:-No. Azure DNS doesn't currently support zone transfers. DNS zones can be imported into Azure DNS by using the Azure CLI. DNS records are managed via the Azure DNS management portal, REST API, SDK, PowerShell cmdlets, or the CLI tool. Refer: https://docs.microsoft.com/en-us/azure/dns/dns-faq

Q42) State whether the following statement holds correct or not.

"Azure DNS support URL redirects."

FALSE

Explanation:-No. URL redirect services aren't a DNS service. They work at the HTTP level rather than the DNS level. Some DNS providers bundle a URL redirect service as part of their overall offering. This service isn't currently supported by Azure DNS. Refer: https://docs.microsoft.com/en-us/azure/dns/dns-faq

TRUE

Q43) Select the DNS record which maps host names to their IPv4 address?

A

Explanation:-Address Mapping record (A Record)—also known as a DNS host record, stores a hostname and its corresponding IPv4 address. IP Version 6 Address record (AAAA Record)—stores a hostname and its corresponding IPv6 address. Canonical Name record (CNAME Record)—can be used to alias a hostname to another hostname. Refer: https://ns1.com/resources/dns-types-records-servers-and-queries#:~:text=Address%20Mapping%20record%20(A%20Record,a%20hostname%20to%20another%20hostname.

- AAAA
- CNAME
- MX

Q44) Mapping host names to their IPv6 address, is done by which DNS record?

- ✅ AAAA

Explanation:-As you can see, a mapping from a name to an IPv6 address is performed using an AAAA resource record, with the IPv6 address given as a hexadecimal address (RFC 3596). Task 1. Add AAAA records in your DNS server for the hostnames of the devices that can be reached through the IPv6 protocol.

- A
- CNAME
- MX

Q45) Select the DNS record which enlists alias names.

- ✅ CNAME

Explanation:-An ALIAS record is a virtual host record type which is used to point one domain name to another one, almost the same as a CNAME. In short, an ALIAS record allows you to specify a hostname in your DNS records which then resolve to the correct A/AAAA records at the time of a request.

- AAAA
- A
- MX

Q46) The DNS record used in routing requests to mail servers, is _____.

- ✅ MX

Explanation:-Mail exchanger record (MX Record)—specifies an SMTP email server for the domain, used to route outgoing emails to an email server. Name Server records (NS Record)—specifies that a DNS Zone, such as “example.com” is delegated to a specific Authoritative Name Server, and provides the address of the name server.

- CNAME
- AAAA
- A

Q47) Delegation of a DNS zone to an authoritative server, is done by which DNS record?

- AAAA
- CNAME
- MX
- ✅ NS

Explanation:-Name Server records (NS Record)—specifies that a DNS Zone, such as “example.com” is delegated to a specific Authoritative Name Server, and provides the address of the name server. Reverse-lookup Pointer records (PTR Record)—allows a DNS resolver to provide an IP address and receive a hostname (reverse DNS lookup) Refer: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/reviewing-dns-concepts

---

Q48) Select the DNS record which defines a name associated with an IP address.

- ✅ PTR

Explanation:-The 'pointer' record is exactly the opposite of the 'A' record; the PTR address will give you the domain associated with a given IP address. The PTR record is used in reverse-lookup zones for reverse DNS searches.

- MX
- CNAME
- AAAA

Q49) What is the minimum priority value that can be assigned to a Azure security rule ?

- None of these
- 1
- ✅ 100

Explanation:-
A value between 100 and 4096 that's unique for all security rules within the network security group

Refer: https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group

- TRUE
