[New Exams!AZ-500 Exam Dumps 60Q Free from Braindump2go[Q23-Q33

July/2019 Braindump2go AZ-500 Exam Dumps with PDF and VCE New Updated Today! Following are some new AZ-500 Exam Questions:1.|2019 Latest Braindump2go AZ-500 Exam Dumps (PDF & VCE) Instant Download: **https://www.braindump2go.com/az-500.html**2.|2019 Latest Braindump2go AZ-500Exam Questions & Answers Instant Download:https://drive.google.com/drive/folders/1sQAsVdJ79oBKFiswxjUzGT6Gt6a6PYWl?usp=sharingQUESTION 23You have an Azure virtual machines shown in the following table. You create an Azure Log Analytics workspace named Analytics1 in RG1 in the East US region.Which virtual machines can be enrolled in Analytics1?A. VM1 onlyB. VM1, VM2, and VM3 onlyC. VM1, VM2, VM3, and VM4D. VM1 and VM4 onlyAnswer: AExplanation:Note: Create a workspaceIn the Azure portal, click All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics. Click Create, and then select choices for the following items:Provide a name for the new Log Analytics workspace, such as DefaultLAWorkspace. OMS workspaces are now referred to as Log Analytics workspaces.Select a Subscription to link to by selecting from the drop-down list if the default selected is not appropriate.For Resource Group, select an existing resource group that contains one or more Azure virtual machines.Select the Location your VMs are deployed to. For additional information, see which regions Log Analytics is available in.Incorrect Answers:B, C: A Log Analytics workspace provides a geographic location for data storage. VM2 and VM3 are at a different location.D: VM4 is a different resource group.References: **https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-access**QUESTION 24You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit. You plan to deploy the cluster to production. You disable HTTP application routing.You need to implement application routing that will provide reverse proxy and TLS termination for AKS services by using a single IP address.What should you do?A. Create an AKS Ingress controller.B. Install the container network interface (CNI) plug-in.C. Create an Azure Standard Load Balancer.D. Create an Azure Basic Load Balancer.Answer: AExplanation:An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.References:**https://docs.microsoft.com/en-us/azure/aks/ingress-tlsTopic 3, Manage security operations**QUESTION 25You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.You are assigned the Global administrator role for the tenant. You are responsible for managing Azure Security Center settings.You need to create a custom sensitivity label.What should you do first?A. Create a custom sensitive information type.B. Elevate access for global administrators in Azure AD.C. Upgrade the pricing tier of the Security Center to Standard.D. Enable integration with Microsoft Cloud App Security.Answer: AExplanation:First, you need to create a new sensitive information type because you can't directly modify the default rules.References: **https://docs.microsoft.com/en-us/office365/securitycompliance/customize-a-built-in-sensitive-information-type**QUESTION 26 You have an Azure subscription named Sub1.In Azure Security Center, you have a security playbook named Play1. Play1 is configured to send an email message to a user named User1.You need to modify Play1 to send email messages to a distribution group named Alerts.What should you use to modify Play1?A. Azure DevOpsB. Azure Application InsightsC. Azure Monitor D. Azure Logic Apps DesignerAnswer: DExplanation:You can change an existing playbook in Security Center to add an action, or conditions. To do that you just need to click on the name of the playbook that you want to change, in the Playbooks tab, and Logic App Designer opens up.References:**https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks** QUESTION 27You create a new Azure subscription.You need to ensure that you can create custom alert rules in Azure Security Center.Which two actions should you perform? Each correct answer presents part of the solution.NOTE: Each correct selection is worth one point.A. Onboard Azure Active Directory (Azure AD) Identity Protection.B. Create an Azure Storage account.C. Implement Azure Advisor recommendations.D. Create an Azure Log Analytics workspace.E. Upgrade the pricing tier of Security Center to Standard.Answer: BDExplanation:D: You need write permission in the workspace that you select to store your custom alert.References:**https://docs.microsoft.com/en-us/azure/security-center/security-center-custom-alert**QUESTION 28 You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1.You have 100 on-premises servers that run Windows Server 2012 R2 and Windows Server 2016. The servers connect to LAW1. LAW1 is configured to collect security-related performance counters from the connected servers.You need to configure alerts based on the data collected by LAW1. The solution must meet the following requirements:- Alert rules must support dimensions.- The time it takes to generate an alert must be minimized.- Alert notifications must be generated only once when the alert is generated and once when the alert is resolved.Which signal type should you use when you create the alert rules?A. LogB. Log (Saved Query)C. MetricD. Activity LogAnswer: CExplanation:Metric alerts in Azure Monitor provide a way to get notified when one of your metrics cross a threshold. Metric alerts work on a range of multi-dimensional platform metrics, custom metrics, Application Insights

standard and custom metrics.Note: Signals are emitted by the target resource and can be of several types. Metric, Activity log, Application Insights, and Log.References:**https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric**
QUESTION 29Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.The company develops an application named App1. App1 is registered in Azure AD.You need to ensure that App1 can access secrets in Azure Key Vault on behalf of the application users.What should you configure?A. an application permission without admin consentB. a delegated permission without admin consentC. a delegated permission that requires admin consentD. an application permission that requires admin consentAnswer: BExplanation:Delegated permissions - Your client application needs to access the web API as the signed-in user, but with access limited by the selected permission. This type of permission can be granted by a user unless the permission requires administrator consent.Incorrect Answers:A, D: Application permissions - Your client application needs to access the web API directly as itself (no user context). This type of permission requires administrator consent and is also not available for public (desktop and mobile) client applications.References:
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apisQUESTION 30
Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory Azure (Azure AD) tenant named contoso.com.The company develops a mobile application named App1. App1 uses the OAuth 2 implicit grant type to acquire Azure AD access tokens.You need to register App1 in Azure AD.What information should you obtain from the developer to register the application?A. a redirect URIB. a reply URLC. a keyD. an application IDAnswer: AExplanation:For Native Applications you need to provide a Redirect URI, which Azure AD will use to return token responses.References:
https://docs.microsoft.com/en-us/azure/active-directory/develop/v1-protocols-oauth-codeQUESTION 31From the Azure portal, you are configuring an Azure policy.You plan to assign policies that use the DeployIfNotExist, AuditIfNotExist, Append, and Deny effects.Which effect requires a managed identity for the assignment?A. AuditIfNotExistB. AppendC. DeployIfNotExistD. DenyAnswer: CExplanation:When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity.References:**https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources**
QUESTION 32You have an Azure subscription that contains an Azure key vault named Vault1.In Vault1, you create a secret named Secret1.An application developer registers an application in Azure Active Directory (Azure AD).You need to ensure that the application can use Secret1.What should you do?A. In Azure AD, create a role.B. In Azure Key Vault, create a key.C. In Azure Key Vault, create an access policy.D. In Azure AD, enable Azure AD Application Proxy.Answer: AExplanation:Azure Key Vault provides a way to securely store credentials and other keys and secrets, but your code needs to authenticate to Key Vault to retrieve them.Managed identities for Azure resources overview makes solving this problem simpler, by giving Azure services an automatically managed identity in Azure Active Directory (Azure AD). You can use this identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without having any credentials in your code.Example: How a system-assigned managed identity works with an Azure VMAfter the VM has an identity, use the service principal information to grant the VM access to Azure resources. To call Azure Resource Manager, use role-based access control (RBAC) in Azure AD to assign the appropriate role to the VM service principal. To call Key Vault, grant your code access to the specific secret or key in Key Vault.References:**https://docs.microsoft.com/en-us/azure/key-vault/quick-create-net**
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overviewQUESTION 33You have an Azure SQL database.You implement Always Encrypted.You need to ensure that application developers can retrieve and decrypt data in the database.Which two pieces of information should you provide to the developers? Each correct answer presents part of the solution.NOTE: Each correct selection is worth one point.A. a stored access policyB. a shared access signature (SAS)C. the column encryption keyD. user credentialsE. the column master keyAnswer: CEExplanation:Always Encrypted uses two types of keys: column encryption keys and column master keys. A column encryption key is used to encrypt data in an encrypted column. A column master key is a key-protecting key that encrypts one or more column encryption keys.References:
https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine
!!!RECOMMEND!!!1.|2019 Latest Braindump2go AZ-500 Exam Dumps (PDF & VCE) Instant Download:
https://www.braindump2go.com/az-500.html2.|2019 Latest Braindump2go AZ-500 Study Guide Video Instant Download:
YouTube Video: YouTube.com/watch?v=-d1W44dDS2o