200 XP

Summary

5 minutes

Azure Storage provides a layered security model. Use this model to secure your storage accounts to a specific set of supported networks. When you set up network rules, only applications that request data over the specified networks can access your storage account.

Authorization is supported by a public preview of Azure Active Directory credentials (for blobs and queues), a valid account access key, or a shared access signature (SAS) token. Data encryption is enabled by default, and you can proactively monitor systems by using Advanced Threat Protection.

Check your knowledge

1. You are working on a project with a 3rd party vendor to build a website for a customer. The image assets that will be used on the website are stored in an Azure Storage account that is held in your subscription. You want to give read access to this data for a limited period of time. What security option would be the best option to use?

- ○ CORS Support
- ○ Storage Account
- ○ Shared Access Signatures

2. When configuring network access to your Azure Storage Account, what is the default network rule?

- ○ To allow all connections from all networks
- ○ To allow all connection from a private IP address range
- ○ To deny all connections from all networks

3. Which Azure service detects anomalies in account activities and notifies you of potential harmful attempts to access your account?

- ○ Azure Defender for Storage
- ○ Azure Storage Account Security Feature
- ○ Encryption in transit

Check your answers