AZURE FUNDAMANETALS

1. What is the Azure firewall? How to use the Azure firewall?
2. Differentiate authentication and authorization?
3. What is Azure Active Directory?
4. What are multifactor authentication and conditional access available in Azure?
5. What is resource lock? Describe why resource lock should be used?
6. What is Azure policy? Write it Usage.
7. What is the Azure government? What is Azure China 21Vianet?

Q1)

Azure Firewall is a cloud-native and intelligent network firewall security service that provides the best of breed threat protection for your cloud workloads running in Azure. It's a fully stateful, firewall as a service with built-in high availability and unrestricted cloud scalability. It provides both east-west and north-south traffic inspection.

Q2)

Azure App Service provides built-in authentication and authorization capabilities (sometimes referred to as "Easy Auth"), so you can sign in users and access data by writing minimal or no code in your web app, RESTful API, and mobile back end, and also Azure Functions. This article describes how App Service helps simplify authentication and authorization for your app.

Built in authentication

You're not required to use this feature for authentication and authorization. You can use the bundled security features in your web framework of choice, or you can write your own utilities. However, you will need to ensure that your solution stays up to date with the latest security, protocol, and browser updates.

Implementing a secure solution for authentication (signing-in users) and authorization (providing access to secure data) can take significant effort. You must make sure to follow industry best practices and standards, and keep your implementation up to date. The built-in authentication feature for App Service and Azure Functions can save you time and effort by providing out-of-the-box authentication with federated identity providers, allowing you to focus on the rest of your application.

- Azure App Service allows you to integrate a variety of auth capabilities into your web app or API without implementing them yourself.

- It’s built directly into the platform and doesn’t require any particular language, SDK, security expertise, or even any code to utilize.
- You can integrate with multiple login providers. For example, Azure AD, Facebook, Google, Twitter.

Q3) Azure Active Directory (Azure AD) is a cloud-based identity and access management service. This service helps your employees access external resources, such as Microsoft 365, the Azure portal, and thousands of other SaaS applications. Azure Active Directory also helps them access internal resources like apps on your corporate intranet network, along with any cloud apps developed for your own organization. For more information about creating a tenant for your organization, see Quickstart: Create a new tenant in Azure Active Directory.

To learn the differences between Active Directory and Azure Active Directory, see Compare Active Directory to Azure Active Directory. You can also refer Microsoft Cloud for Enterprise Architects Series posters to better understand the core identity services in Azure like Azure AD and Microsoft-365.

Q4)

Azure AD Multi-Factor Authentication can be enabled all users using security defaults. Management of Azure AD Multi-Factor Authentication is through the Microsoft 365 portal. For an improved user experience, upgrade to Azure AD Premium P1 or P2 and use Conditional Access. For more information, see secure Microsoft 365 resources with multi-factor authentication.

Q5)

As an administrator, you can lock an Azure subscription, resource group, or resource to protect them from accidental user deletions and modifications. The lock overrides any user permissions.

You can set locks that prevent either deletions or modifications. In the portal, these locks are called **Delete** and **Read-only**. In the command line, these locks are called **CanNotDelete** and **ReadOnly**.

- **CanNotDelete** means authorized users can read and modify a resource, but they can't delete it.
- **ReadOnly** means authorized users can read a resource, but they can't delete or update it. Applying this lock is similar to restricting all authorized users to the permissions that the **Reader** role provides.

Unlike role-based access control (RBAC), you use management locks to apply a restriction across all users and roles. To learn about setting permissions for users and roles, see Azure RBAC.

Lock inheritance

When you apply a lock at a parent scope, all resources within that scope inherit the same lock. Even resources you add later inherit the same parent lock. The most restrictive lock in the inheritance takes precedence.

Extension resources inherit locks from the resource they're applied to. For example, Microsoft.Insights/diagnosticSettings is an extension resource type. If you apply a diagnostic setting to a storage blob, and lock the storage account, you're unable to delete the diagnostic setting.

Q6)

Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity. It also helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.

Common use cases for Azure Policy include implementing governance for resource consistency, regulatory compliance, security, cost, and management. Policy definitions for these common use cases are already available in your Azure environment as built-ins to help you get started.

All Azure Policy data and objects are encrypted at rest. For more information, see Azure data encryption at rest.

Overview

Azure Policy evaluates resources in Azure by comparing the properties of those resources to business rules. These business rules, described in JSON format, are known as policy definitions. To simplify management, several business rules can be grouped together to form a policy initiative (sometimes called a *policySet*). Once your business rules have been formed, the policy definition or initiative is assigned to any scope of resources that Azure supports, such as management groups, subscriptions, resource groups, or individual resources. The assignment applies to all resources within the Resource Manager scope of that assignment. Subscopes can be excluded, if necessary. For more information, see Scope in Azure Policy.

Azure Policy uses a JSON format to form the logic the evaluation uses to determine whether a resource is compliant or not. Definitions include metadata and the policy rule. The defined rule can use functions, parameters, logical operators, conditions, and property aliases to match exactly the scenario you want. The policy rule determines which resources in the scope of the assignment get evaluated.

Understand evaluation outcomes

Resources are evaluated at specific times during the resource lifecycle, the policy assignment lifecycle, and for regular ongoing compliance evaluation. The following are the times or events that cause a resource to be evaluated:

- A resource is created or updated in a scope with a policy assignment.
- A policy or initiative is newly assigned to a scope.
- A policy or initiative already assigned to a scope is updated.
- During the standard compliance evaluation cycle, which occurs once every 24 hours.

For detailed information about when and how policy evaluation happens, see Evaluation triggers.

Control the response to an evaluation

Business rules for handling non-compliant resources vary widely between organizations. Examples of how an organization wants the platform to respond to a non-compliant resource include:

- Deny the resource change
- Log the change to the resource
- Alter the resource before the change
- Alter the resource after the change
- Deploy related compliant resources

Azure Policy makes each of these business responses possible through the application of effects. Effects are set in the **policy rule** portion of the policy definition.

Remediate non-compliant resources

While these effects primarily affect a resource when the resource is created or updated, Azure Policy also supports dealing with existing non-compliant resources without needing to alter that resource. For more information about making existing resources compliant, see remediating resources.

Q7)

Microsoft Azure operated by 21Vianet (Azure China) is a physically separated instance of cloud services located in China. It's independently operated and transacted by Shanghai Blue Cloud Technology Co., Ltd. ("21Vianet"), a wholly owned subsidiary of Beijing 21Vianet Broadband Data Center Co., Ltd..