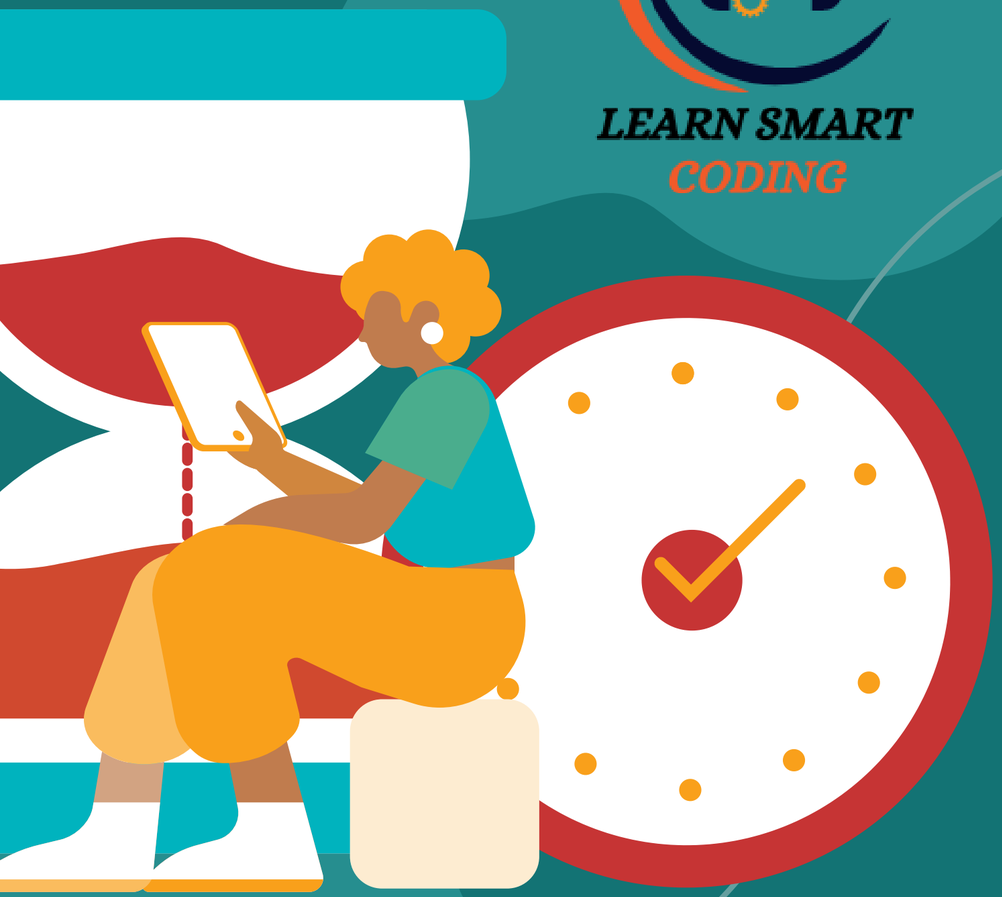
LEARN SMART CODING

Interview Q&A | Short Answers!



RBAC (Role-Based Access Control)

SUBSCRIBE LIKE

https://www.youtube.com/@learnsmartcoding

What is RBAC in Azure?

RBAC is an authorization system that defines granular access permissions for users, groups, or applications at different scopes within Azure resources.

What are the three main components of RBAC in Azure?

The three main components of RBAC are roles, role assignments, and role definitions. Roles define a set of permissions, role assignments associate roles with users or groups, and role definitions define the permissions included in a role.

How do you assign a role to a user or group in Azure?

LEARN SMART CODING

You can assign a role to a user or group in Azure by creating a role assignment and specifying the user or group, the role, and the scope (e.g., subscription, resource group, resource).

hat are the built-in roles in Azure RBAC?

Azure RBAC provides several built-in roles with predefined sets of permissions, such as Owner, Contributor, Reader, and User Access Administrator, among others.

How do you create custom roles in Azure RBAC?

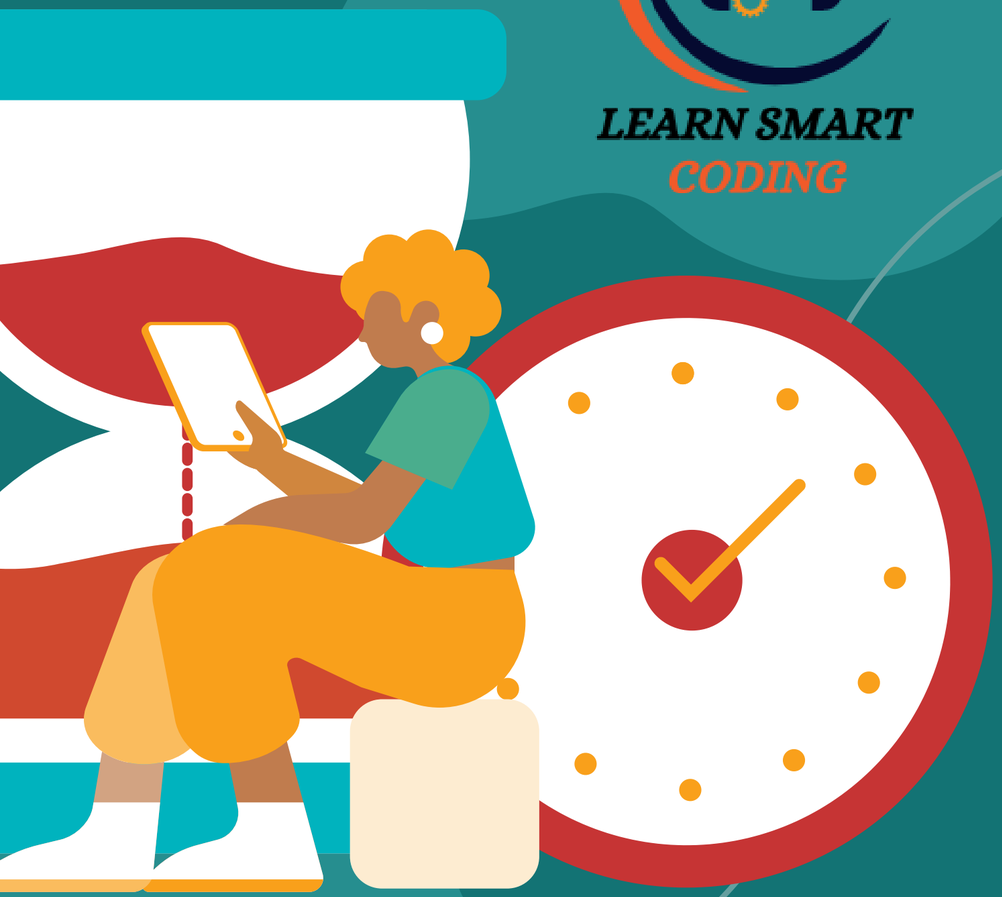
LEARN SMART CODING

You can create custom roles in Azure RBAC by defining a role definition JSON file that specifies the desired permissions and then using Azure CLI or Azure PowerShell to create the custom role based on that definition.

LEARN SMART CODING

Interview Q&A | Short Answers!

Managed Identity



SUBSCRIBE LIKE

https://www.youtube.com/@learnsmartcoding

What is Azure Managed Identity?

LEARN SMART CODING

Azure Managed Identity is a feature that provides an identity for Azure resources to authenticate with Azure AD without needing to manage credentials explicitly.

How do you create a Managed Identity for an Azure resource?

LEARN SMART CODING

You can create a Managed Identity for an Azure resource (such as Azure Functions or Azure VM) through the Azure portal, Azure CLI, or Azure Resource Manager templates.

What are the types of Managed Identity in Azure?

LEARN SMART CODING

There are two types of Managed Identity: system-assigned and user-assigned. System-assigned Managed Identity is enabled directly on an Azure resource, while user-assigned Managed Identity is created as a standalone Azure resource and can be assigned to one or more Azure resources.

How does Managed Identity provide authentication for Azure resources?

LEARN SMART CODING

Managed Identity obtains an access token from Azure AD that can be used to authenticate requests made by the Azure resource to other Azure services.

How does Managed Identity improve security in Azure?

Managed Identity eliminates the need to store credentials in code or configuration files, reducing the risk of exposure to security threats such as credential theft.

let's delve a bit deeper

The main difference between a service principal and a managed identity lies in their scope, lifecycle, and purpose:

Scope

Service Principal:

Service principals are Azure Active Directory (Azure AD) identities that represent applications, services, or automation tasks. They can be scoped to specific Azure subscriptions, resource groups, or individual resources.

Scope

LEARN SMART CODING

Managed Identity:

Managed identities are identities assigned to Azure resources, such as Azure Virtual Machines, Azure Functions, or Azure App Services. They are scoped to the lifecycle of the Azure resource they are associated with and inherit permissions based on that resource's configuration.

Lifecycle

LEARN SMART CODING

Service Principal:

Service principals have a separate lifecycle from Azure resources. They need to be created explicitly, and their credentials (such as client secrets or certificates) need to be managed and rotated periodically for security.

Lifecycle

LEARN SMART CODING

Managed Identity:

Managed identities are created automatically when you enable them on an Azure resource. They are managed by Azure and do not require explicit creation or management of credentials.

Purpose

LEARN SMART CODING

Service Principal:

Service principals are typically used to authenticate applications, services, or scripts to access Azure resources programmatically. They are commonly used in scenarios where an application needs to authenticate and access Azure resources independently of a user.

Lifecycle

LEARN SMART CODING

Managed Identity:

Managed identities are used to authenticate Azure resources themselves when accessing other Azure resources or external services. They provide a secure way for Azure resources to authenticate without the need for explicit credentials, reducing the risk of credential exposure.

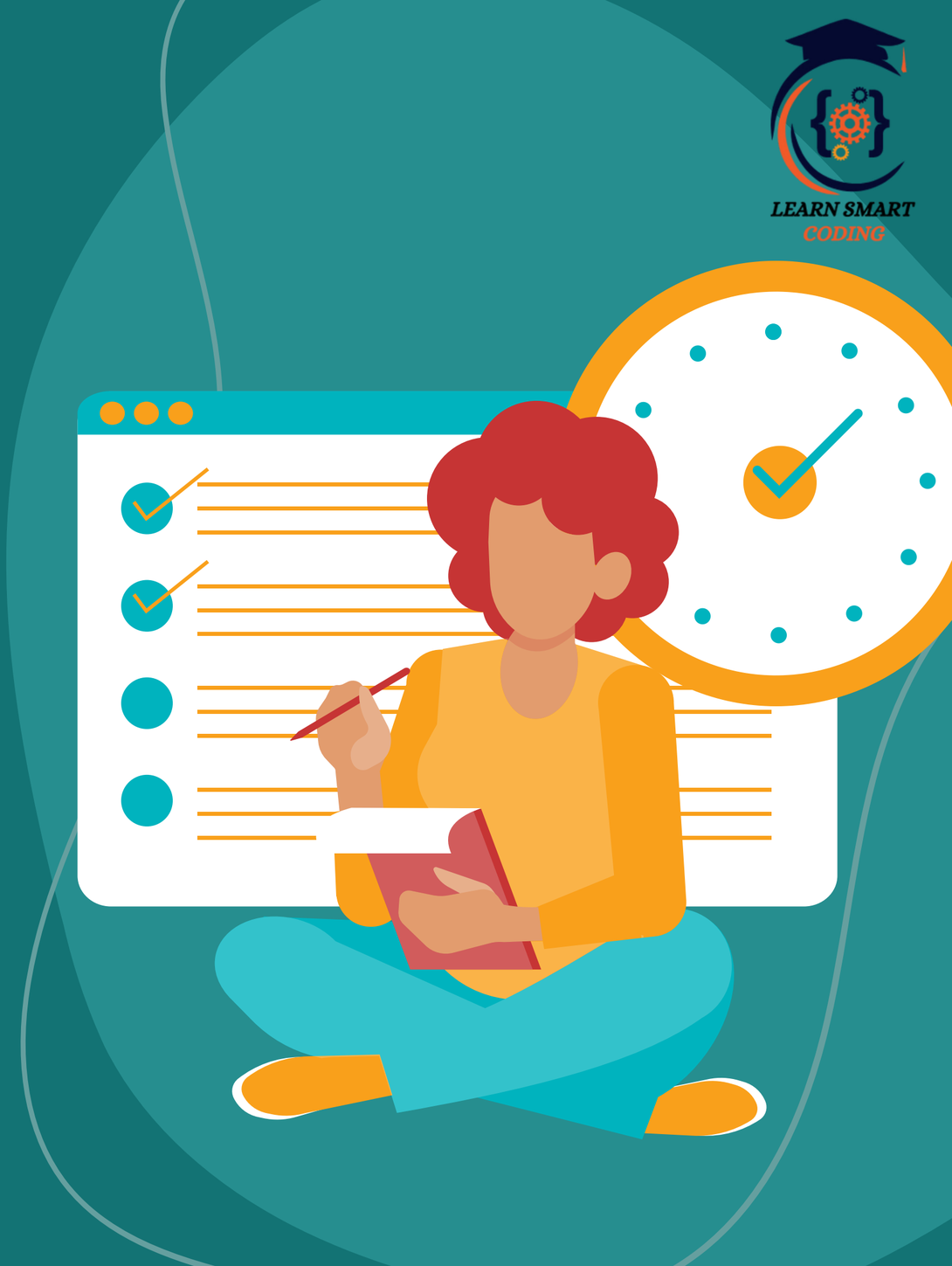
Docs to refer

Goto https://GitHub.com/learnsmartcoding for the sample code for practicing AZ-204 exam

1. Repo for key vault: https://github.com/learnsmartcoding/azure-az204-complete-course

All the videos are available at the below channel

2. https://www.youtube.com/@learnsmartcoding



Thank you for watching

LEARN SMART
CODING

SUBSCRIBE LIKE

https://www.youtube.com/@learnsmartcoding