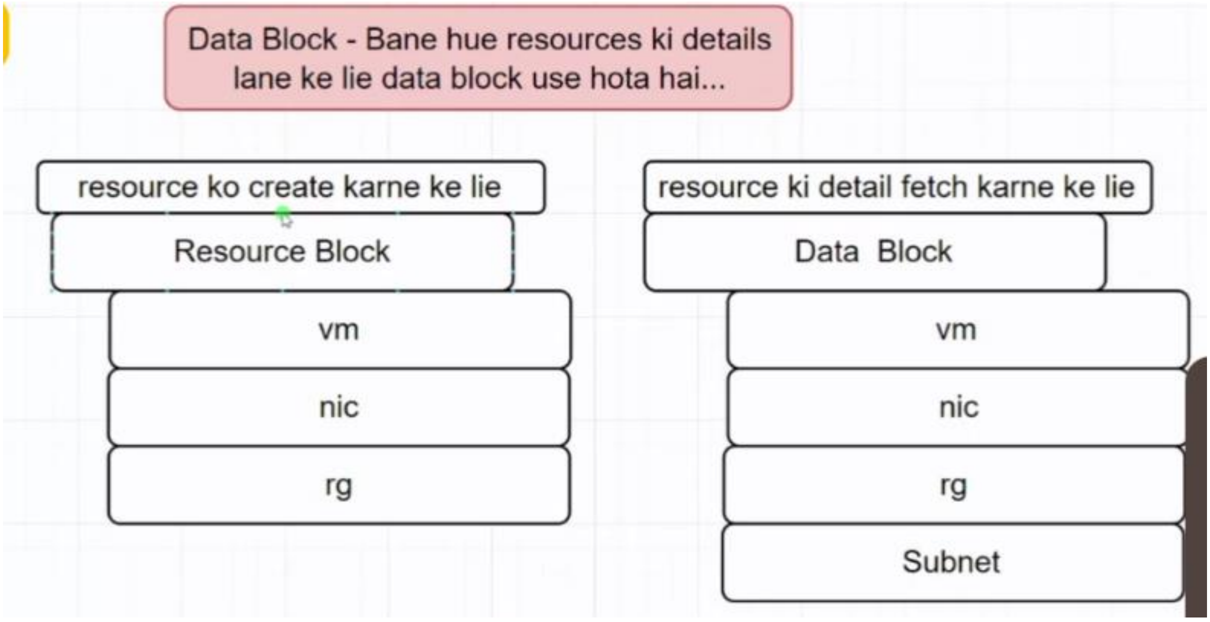
30) 11 August 2024 – AzureKeyVaultsAndDataBlocks

AGENDA - DATA BLOCK



Data Block - Bane hue resources ki details lane ke lie data block use hota hai...

resource ko create karne ke lie

Resource Block

vm

nic

rg

resource ki detail fetch karne ke lie

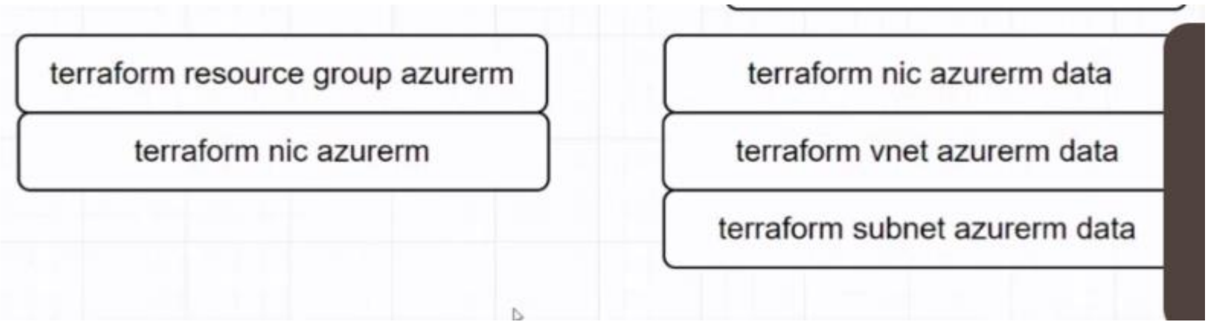
Data Block

vm

nic

rg

Subnet



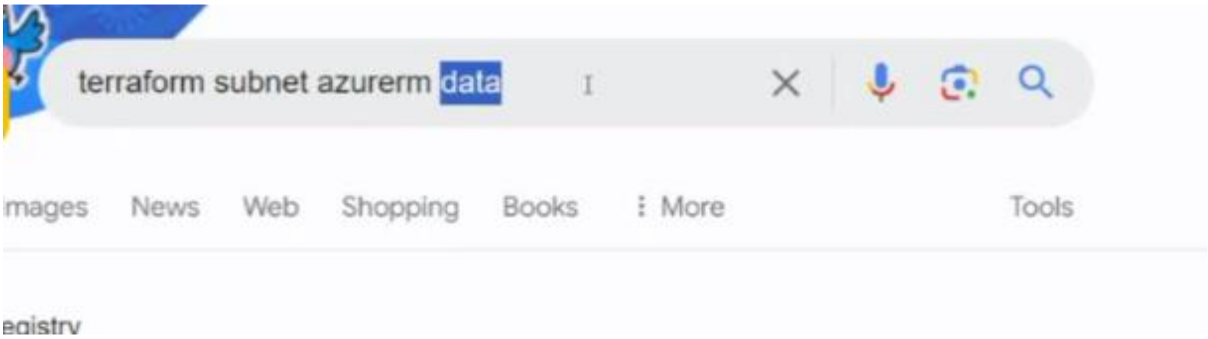
terraform resource group azurerm

terraform nic azurerm

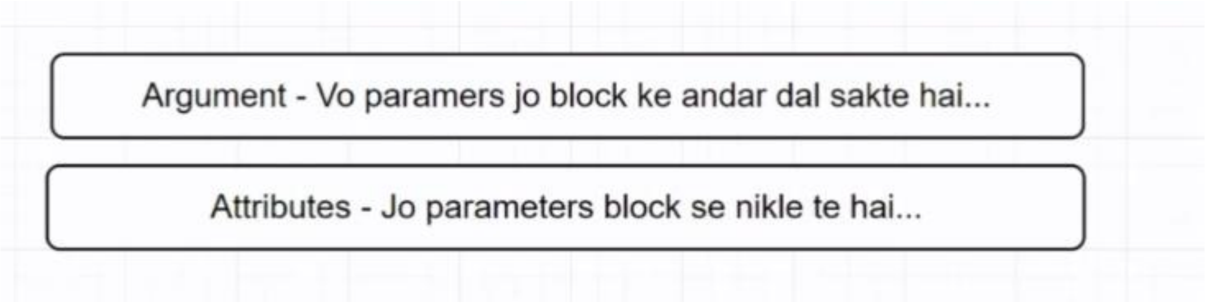
terraform nic azurerm data

terraform vnet azurerm data

terraform subnet azurerm data



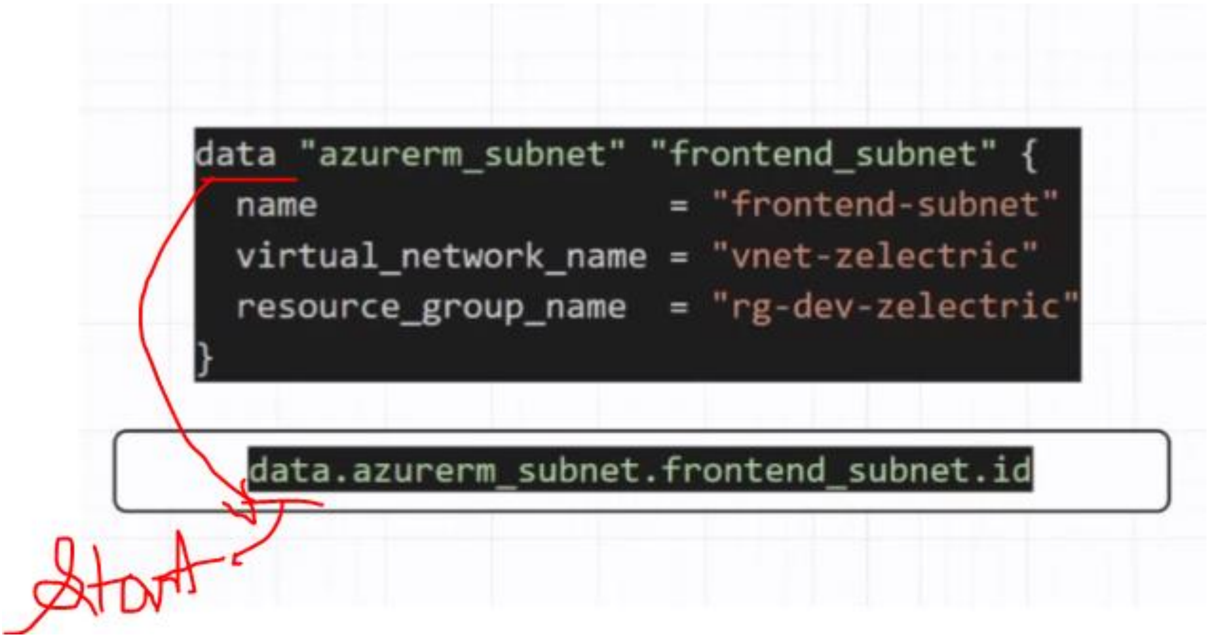
terraform subnet azurerm data



Argument - Vo paramers jo block ke andar dal sakte hai...

Attributes - Jo parameters block se nikle te hai...

2) To use data block we will use start from data as below



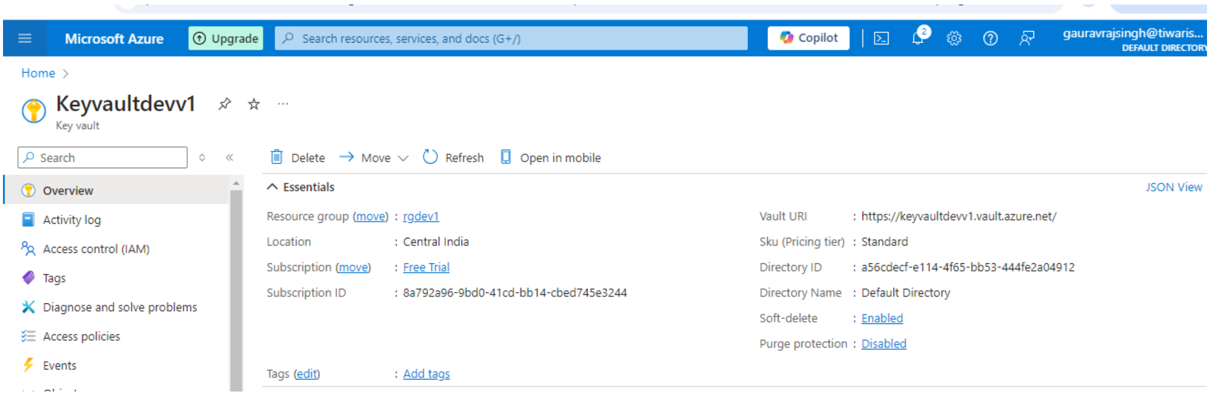
```
data "azurerm_subnet" "frontend_subnet" {
  name                 = "frontend-subnet"
  virtual_network_name = "vnet-zelectric"
  resource_group_name  = "rg-dev-zelectric"
}
```

```
data.azurerm_subnet.frontend_subnet.id
```

++

AGENDA – CREATE KEY VAULT ON PORTAL

1) Create keyvault

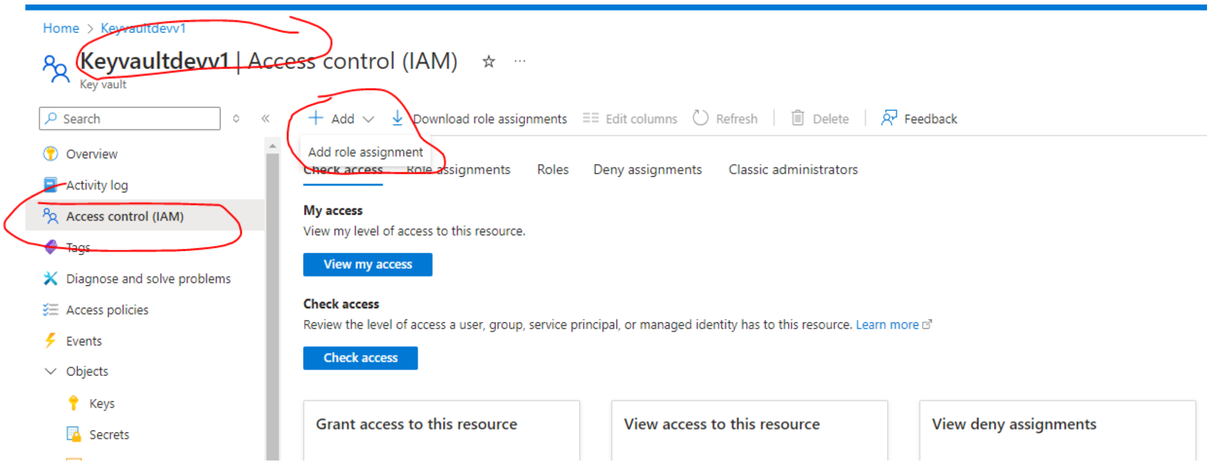


Keyvaultdevv1
Key vault

Essentials

Resource group (move)	: rgdev1	Vault URI	: https://keyvaultdevv1.vault.azure.net/
Location	: Central India	Sku (Pricing tier)	: Standard
Subscription (move)	: Free Trial	Directory ID	: a56cdecf-e114-4f65-bb53-444fe2a04912
Subscription ID	: 8a792a96-9bd0-41cd-bb14-cbed745e3244	Directory Name	: Default Directory
		Soft-delete	: Enabled
		Purge protection	: Disabled
Tags (edit)	: Add tags		

2) To create secret. Firstly provide access

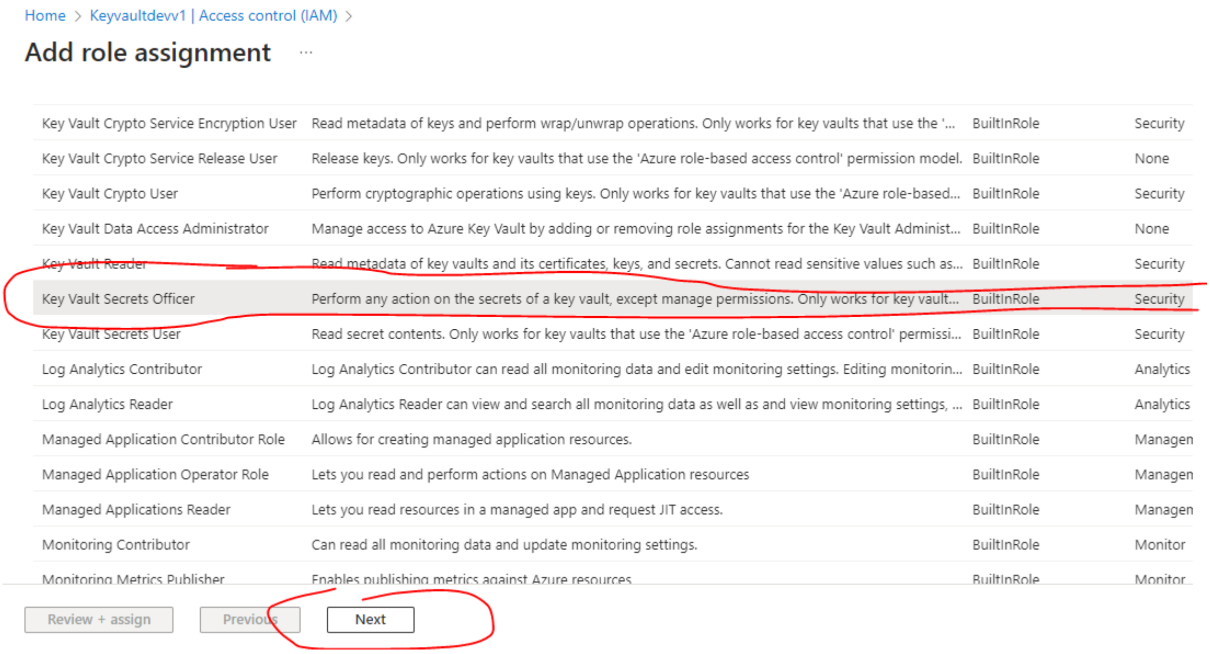


Keyvaultdevv1 | Access control (IAM)
Key vault

My access
View my level of access to this resource.

Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

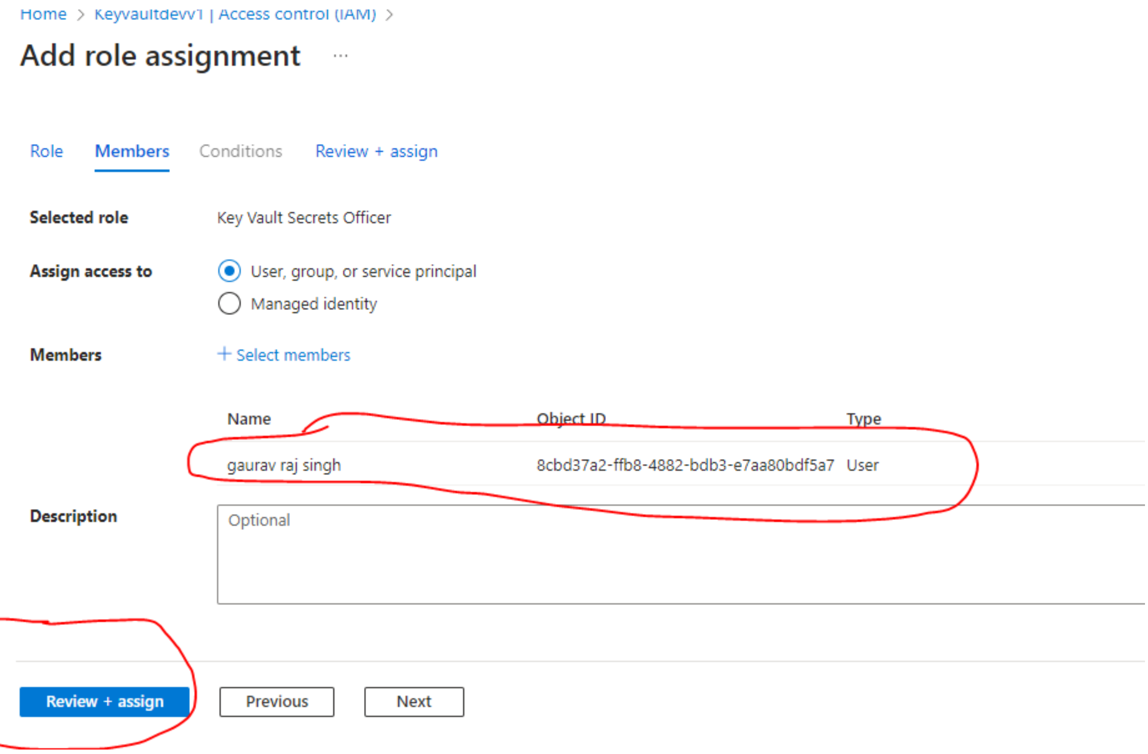
3) Now give below role access



Home > Keyvaultdevv1 | Access control (IAM) >

Add role assignment ···

Key Vault Crypto Service Encryption User	Read metadata of keys and perform wrap/unwrap operations. Only works for key vaults that use the '...	BuiltInRole	Security
Key Vault Crypto Service Release User	Release keys. Only works for key vaults that use the 'Azure role-based access control' permission model.	BuiltInRole	None
Key Vault Crypto User	Perform cryptographic operations using keys. Only works for key vaults that use the 'Azure role-based...	BuiltInRole	Security
Key Vault Data Access Administrator	Manage access to Azure Key Vault by adding or removing role assignments for the Key Vault Administ...	BuiltInRole	None
Key Vault Reader	Read metadata of key vaults and its certificates, keys, and secrets. Cannot read sensitive values such as...	BuiltInRole	Security
Key Vault Secrets Officer	Perform any action on the secrets of a key vault, except manage permissions. Only works for key vault...	BuiltInRole	Security
Key Vault Secrets User	Read secret contents. Only works for key vaults that use the 'Azure role-based access control' permissi...	BuiltInRole	Security
Log Analytics Contributor	Log Analytics Contributor can read all monitoring data and edit monitoring settings. Editing monitorin...	BuiltInRole	Analytics
Log Analytics Reader	Log Analytics Reader can view and search all monitoring data as well as and view monitoring settings, ...	BuiltInRole	Analytics
Managed Application Contributor Role	Allows for creating managed application resources.	BuiltInRole	Managen
Managed Application Operator Role	Lets you read and perform actions on Managed Application resources	BuiltInRole	Managen
Managed Applications Reader	Lets you read resources in a managed app and request JIT access.	BuiltInRole	Managen
Monitoring Contributor	Can read all monitoring data and update monitoring settings.	BuiltInRole	Monitor
Monitoring Metrics Publisher	Enables publishing metrics against Azure resources.	BuiltInRole	Monitor



Home > Keyvaultdevv1 | Access control (IAM) >

Add role assignment ···

Selected role Key Vault Secrets Officer

Assign access to ● User, group, or service principal ○ Managed identity

Members + Select members

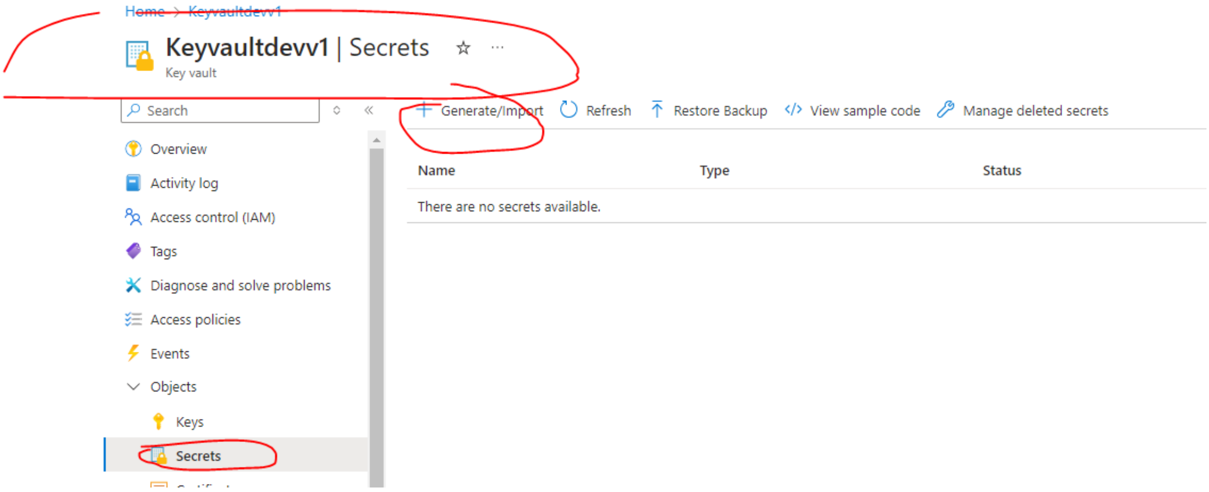
Name	Object ID	Type
gaurav raj singh	8cbd37a2-ffb8-4882-bdb3-e7aa80bdf5a7	User

Description Optional

++

AGENDA – CREATE SECRET

1)

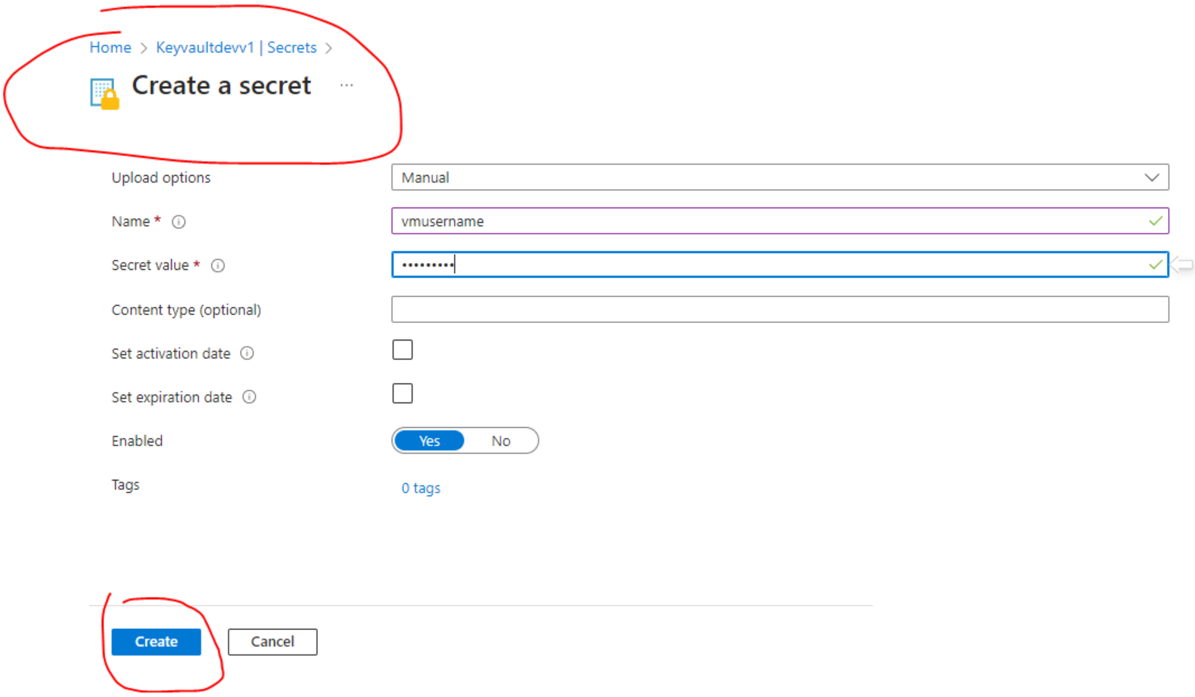


Keyvaultdevv1 | Secrets

Key vault

Name	Type	Status
There are no secrets available.		

i) Create for vmusername

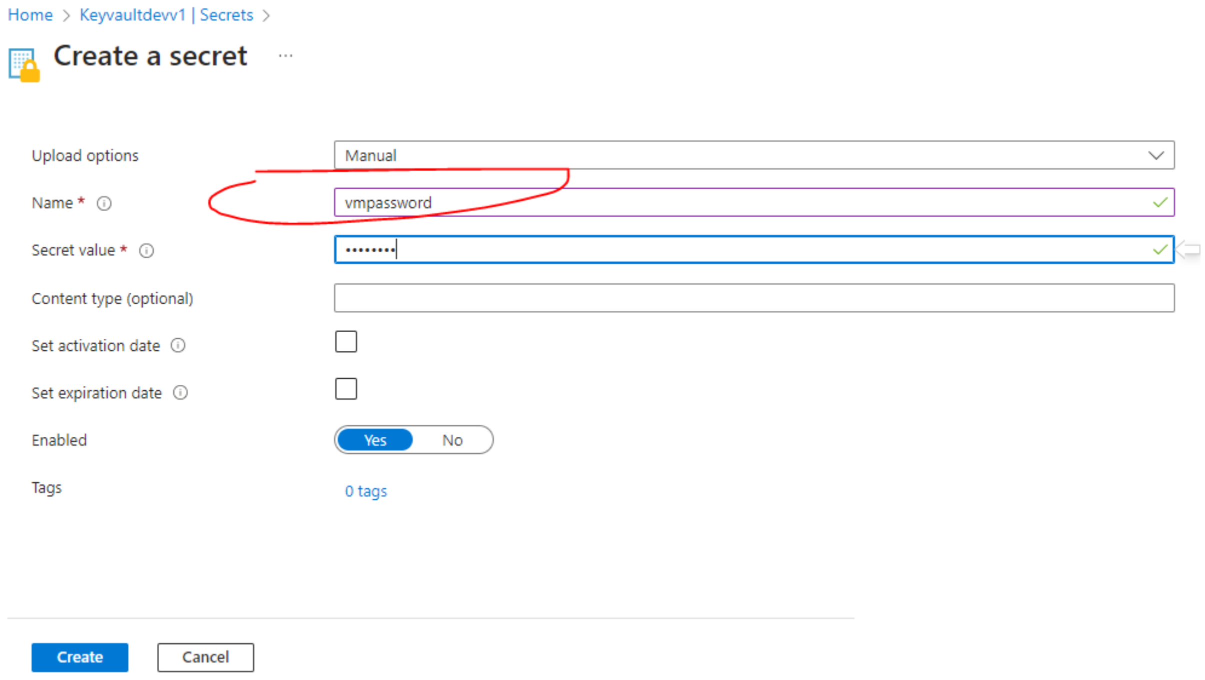


Create a secret

Upload options	Manual
Name *	vmusername
Secret value *	•••••••••
Content type (optional)	
Set activation date	□
Set expiration date	□
Enabled	[✓ Yes] No
Tags	0 tags

Secret value = adminuser

ii) Create for vmpassword


Home > Keyvaultdevv1 | Secrets >

Create a secret

Upload options: Manual

Name *: vmpassword

Secret value *: ••••••••

Content type (optional):

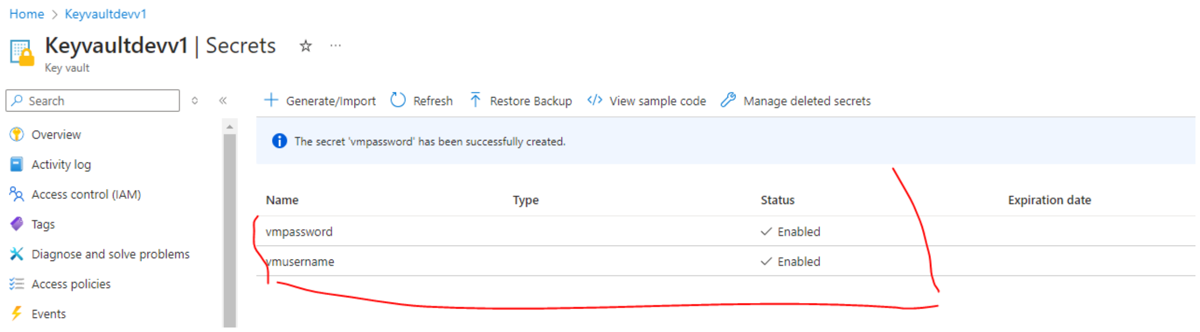
Set activation date: □

Set expiration date: □

Enabled: Yes No

Tags: 0 tags

Secret value = mom6daD?


Home > Keyvaultdevv1

Keyvaultdevv1 | Secrets

Key vault

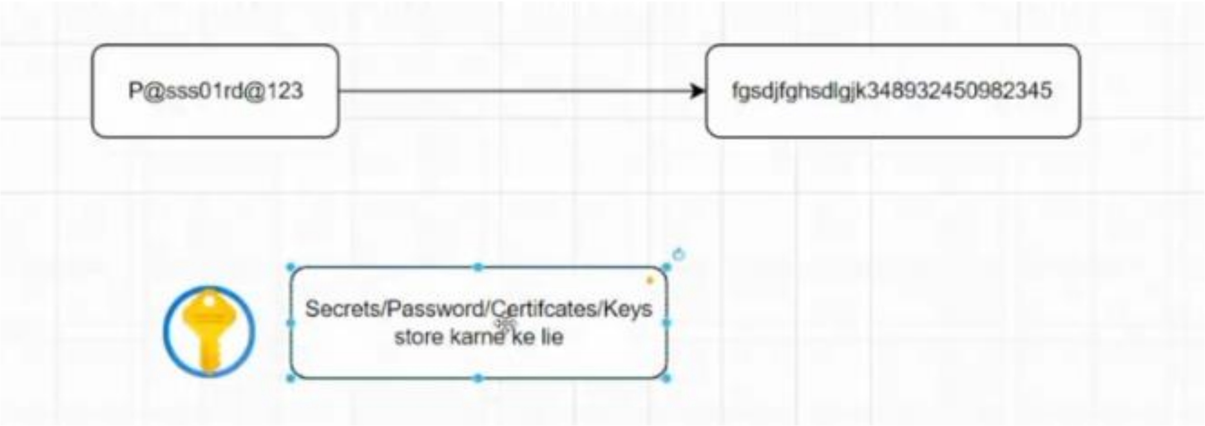
The secret 'vmpassword' has been successfully created.

Name	Type	Status	Expiration date
vmpassword		✓ Enabled	
vmusername		✓ Enabled	

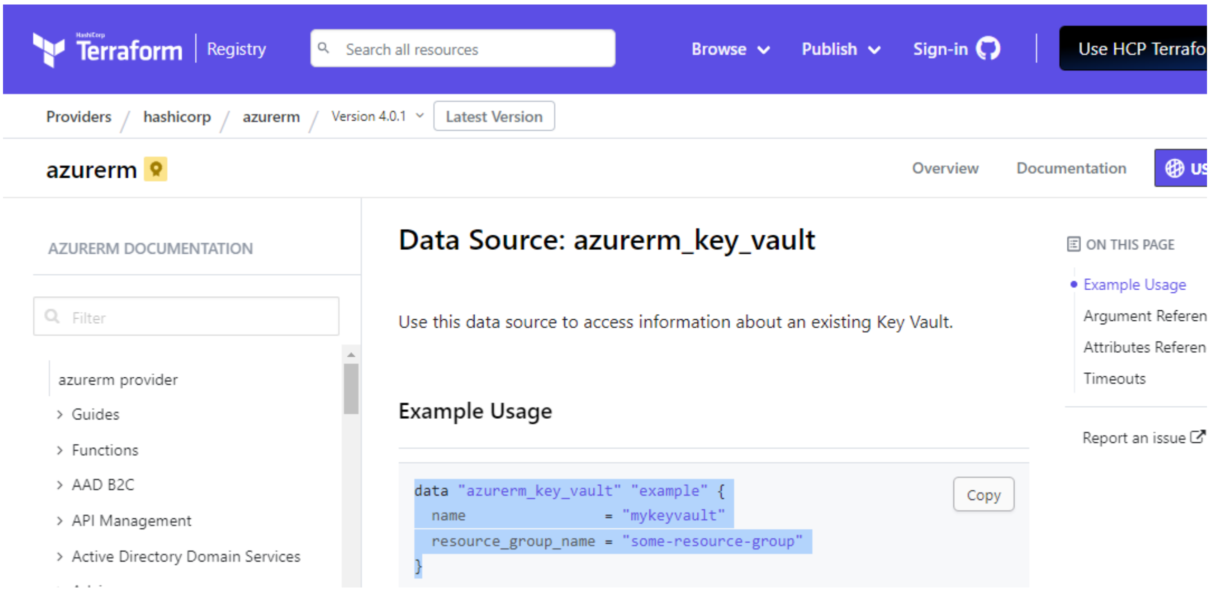
++

AGENDA – KEY VAULT

1) Limited privilege access – Never give highest privilege access to anyone, just provide limited privilege access so that work can be done.


P@sss01rd@123
fgsdjfghsdlgjk348932450982345
Secrets/Password/Certifcates/Keys store karne ke lie

2) SEARCH – azurerm keyvault data



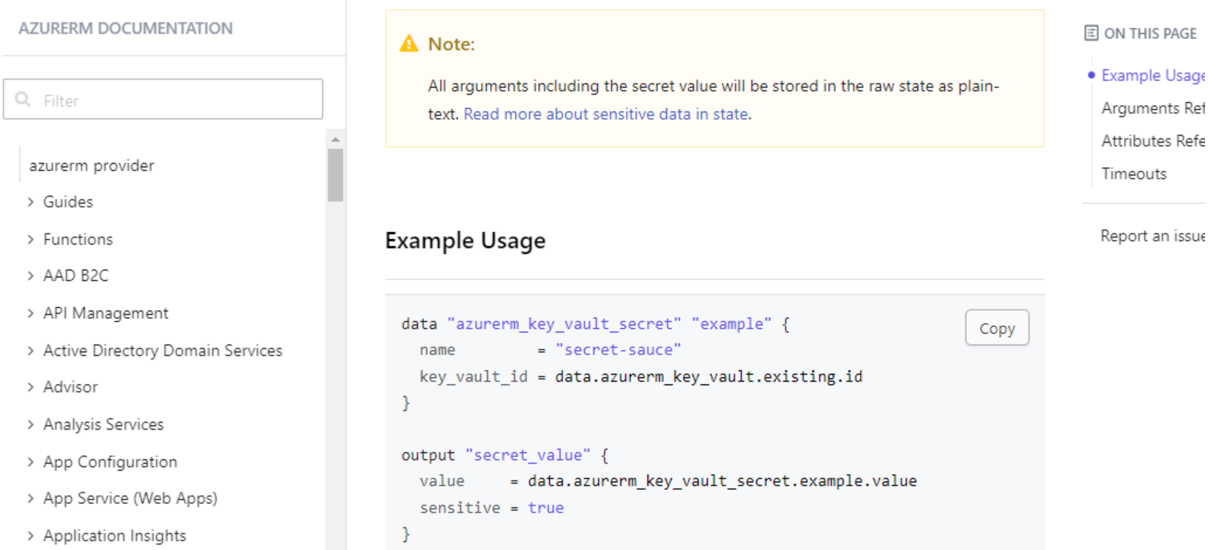
Data Source: azurerm_key_vault

Use this data source to access information about an existing Key Vault.

Example Usage

```
data "azurerm_key_vault" "example" {
  name                = "mykeyvault"
  resource_group_name = "some-resource-group"
}
```

3) SEARCH – azurerm keyvault secret data

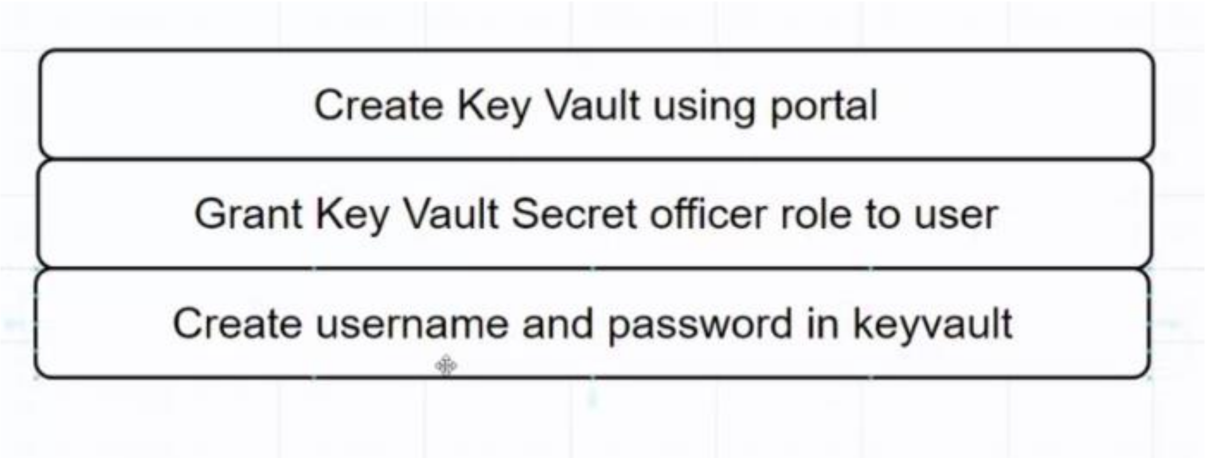


Note:

All arguments including the secret value will be stored in the raw state as plain-text. Read more about sensitive data in state.

Example Usage

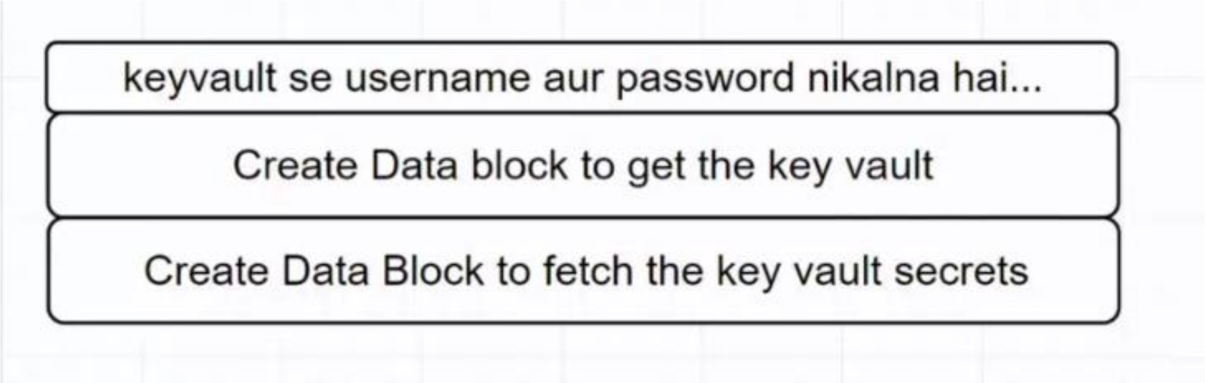
```
data "azurerm_key_vault_secret" "example" {
  name         = "secret-sauce"
  key_vault_id = data.azurerm_key_vault.existing.id
}

output "secret_value" {
  value     = data.azurerm_key_vault_secret.example.value
  sensitive = true
}
```



Create Key Vault using portal

Grant Key Vault Secret officer role to user

Create username and password in keyvault

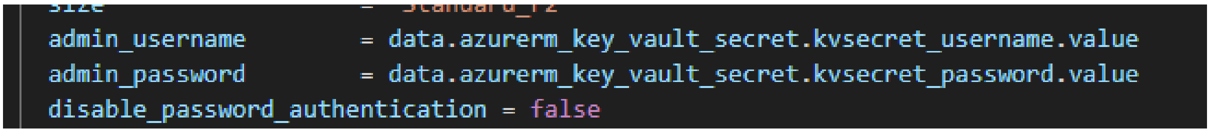


keyvault se username aur password nikalna hai...

Create Data block to get the key vault

Create Data Block to fetch the key vault secrets

4) Change “admin_username” and “admin_password” attributes value as below after creating data blocks in VM code.



```
size                  = "Standard_F2"
admin_username        = data.azurerm_key_vault_secret.kvsecret_username.value
admin_password        = data.azurerm_key_vault_secret.kvsecret_password.value
disable_password_authentication = false
```