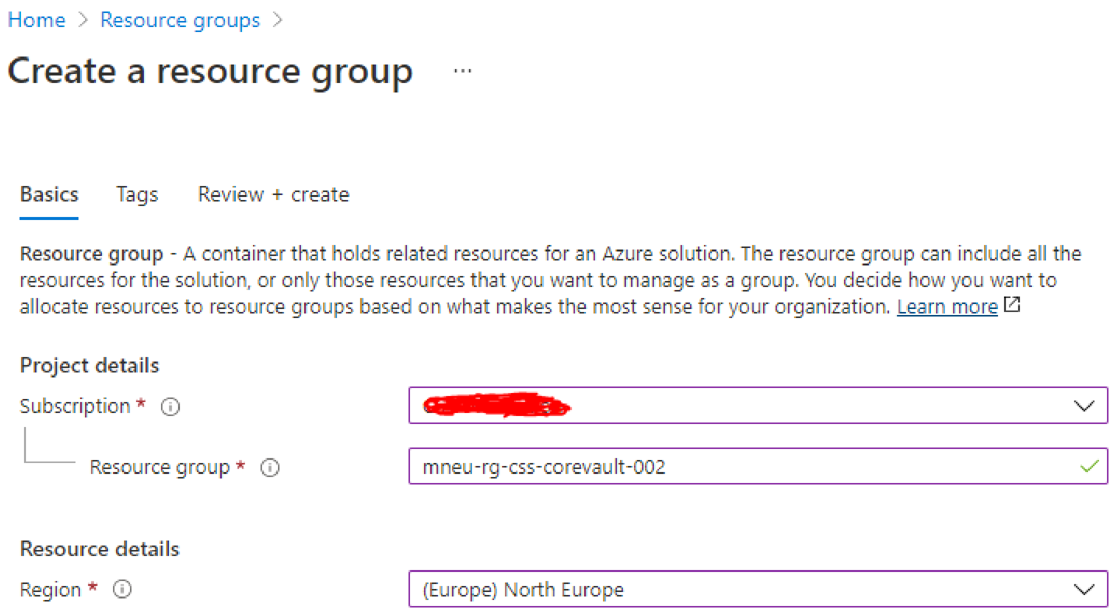
Configure Azure Service Principal secret expiry Notification

Perquisites:

- **Create Resource Group**



Home > Resource groups >

Create a resource group ···

Basics | Tags | Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Learn more

Project details

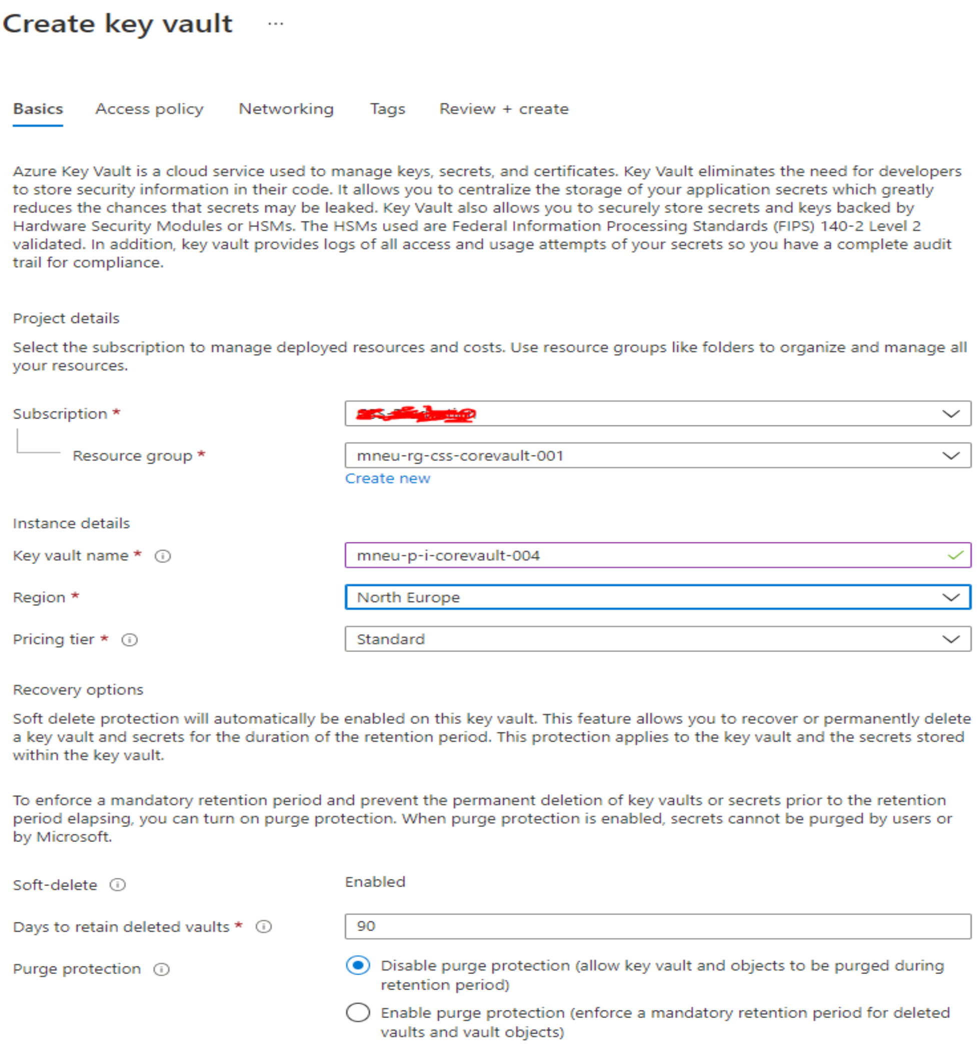
Subscription * : [redacted]

Resource group * : mneu-rg-css-corevault-002

Resource details

Region * : (Europe) North Europe

- **Create Azure Key vault**



Create key vault ···

Basics | Access policy | Networking | Tags | Review + create

Azure Key Vault is a cloud service used to manage keys, secrets, and certificates. Key Vault eliminates the need for developers to store security information in their code. It allows you to centralize the storage of your application secrets which greatly reduces the chances that secrets may be leaked. Key Vault also allows you to securely store secrets and keys backed by Hardware Security Modules or HSMs. The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. In addition, key vault provides logs of all access and usage attempts of your secrets so you have a complete audit trail for compliance.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : [redacted]

Resource group * : mneu-rg-css-corevault-001

Create new

Instance details

Key vault name * : mneu-p-i-corevault-004

Region * : North Europe

Pricing tier * : Standard

Recovery options

Soft delete protection will automatically be enabled on this key vault. This feature allows you to recover or permanently delete a key vault and secrets for the duration of the retention period. This protection applies to the key vault and the secrets stored within the key vault.

To enforce a mandatory retention period and prevent the permanent deletion of key vaults or secrets prior to the retention period elapsing, you can turn on purge protection. When purge protection is enabled, secrets cannot be purged by users or by Microsoft.

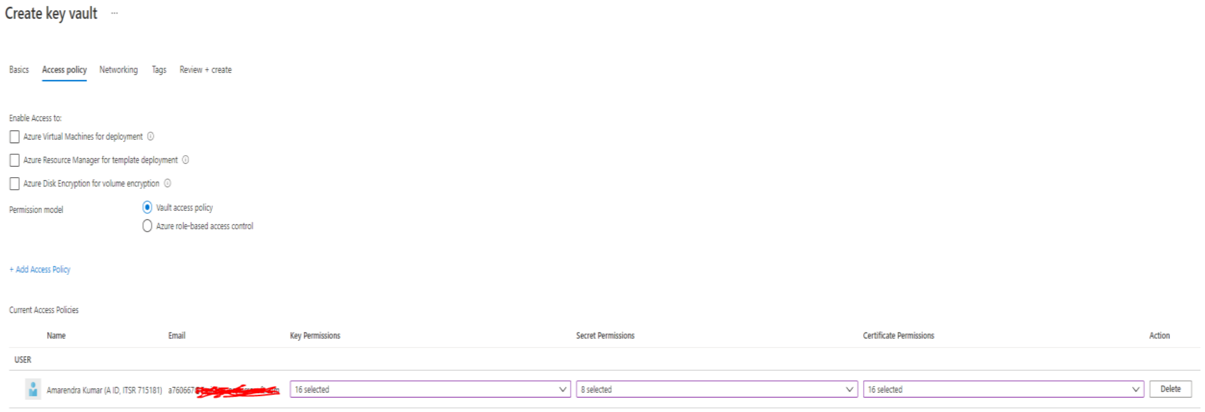
Soft-delete : Enabled

Days to retain deleted vaults * : 90

Purge protection :

● Disable purge protection (allow key vault and objects to be purged during retention period)

○ Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)



Create key vault ···

Enable Access to:

□ Azure Virtual Machines for deployment ⓘ

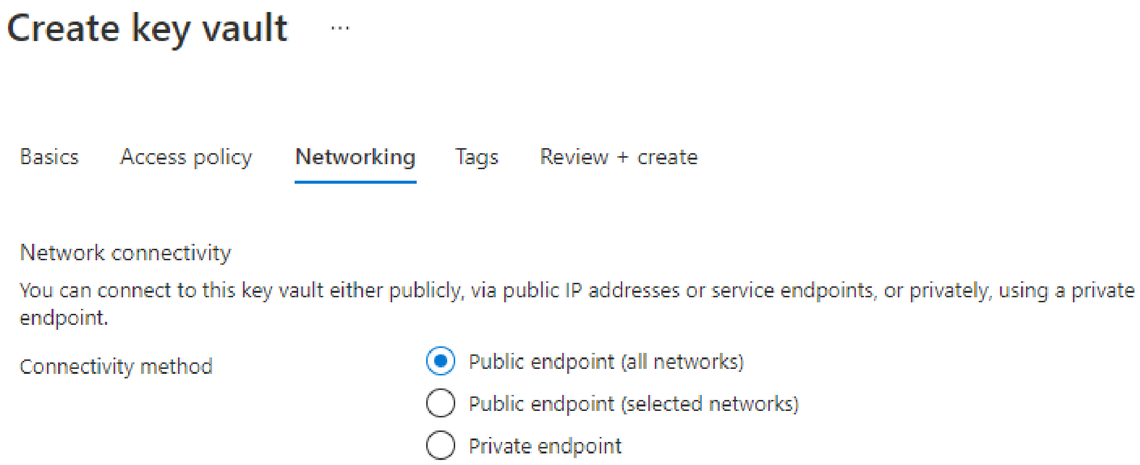
□ Azure Resource Manager for template deployment ⓘ

□ Azure Disk Encryption for volume encryption ⓘ

Permission model ● Vault access policy ○ Azure role-based access control

Current Access Policies

Name	Email	Key Permissions	Secret Permissions	Certificate Permissions	Action
USER					
Amarendra Kumar (A ID, ITSR 715181)	a760667[redacted]	16 selected	8 selected	16 selected	Delete

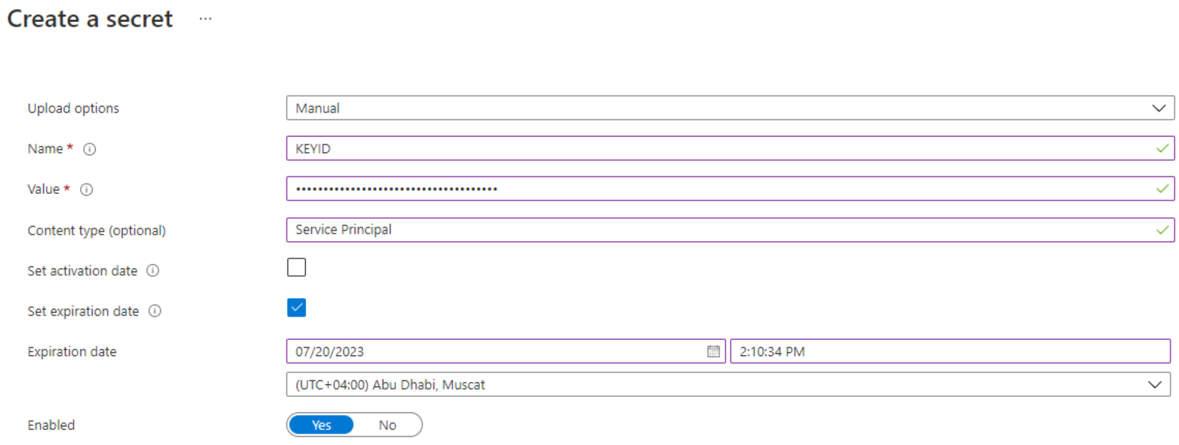


Create key vault ···

Network connectivity

You can connect to this key vault either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Connectivity method ● Public endpoint (all networks) ○ Public endpoint (selected networks) ○ Private endpoint

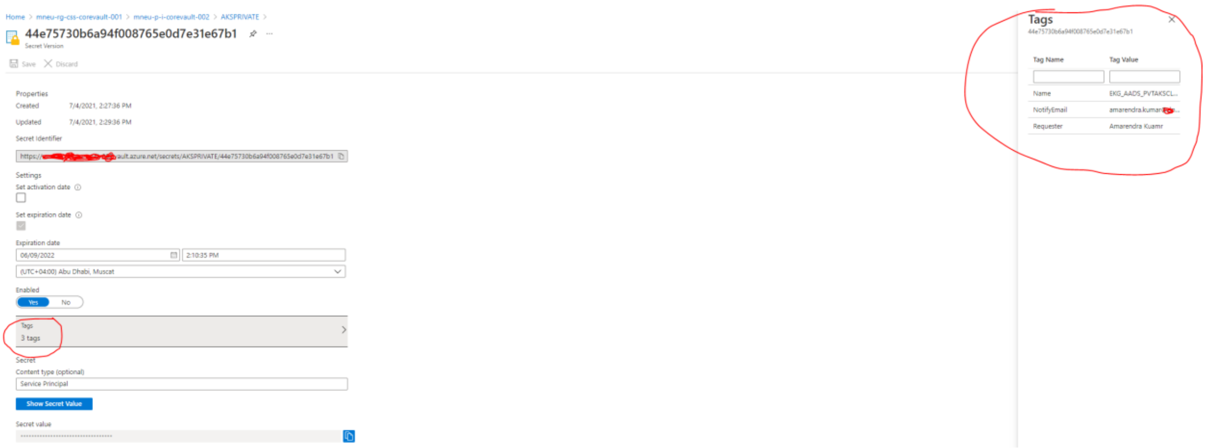


Create a secret ···

Upload options	Manual
Name * ⓘ	KEYID
Value * ⓘ	••••••••••••••••••••••••••••••••••••••
Content type (optional)	Service Principal
Set activation date ⓘ	□
Set expiration date ⓘ	☑
Expiration date	07/20/2023 2:10:34 PM (UTC+04:00) Abu Dhabi, Muscat
Enabled	[✓ Yes] No

Create Tags for secret in Key Vault

1. Name
2. NotifyEmail
3. Requester



Home > mneu-rg-css-corevault-001 > mneu-p-i-corevault-002 > AKSPRIVATE >

44e75730b6a94f008765e0d7e31e67b1

Secret Version

Properties

Created	7/4/2021, 2:27:36 PM
Updated	7/4/2021, 2:29:36 PM

Secret Identifier

https://[redacted]vault.azure.net/secrets/AKSPRIVATE/44e75730b6a94f008765e0d7e31e67b1

Settings

Set activation date ⓘ

□

Set expiration date ⓘ

☑

Expiration date

06/09/2022 2:10:35 PM

(UTC+04:00) Abu Dhabi, Muscat

Enabled

[✓ Yes] No

Tags

3 tags

Secret

Content type (optional)

Service Principal

Secret value

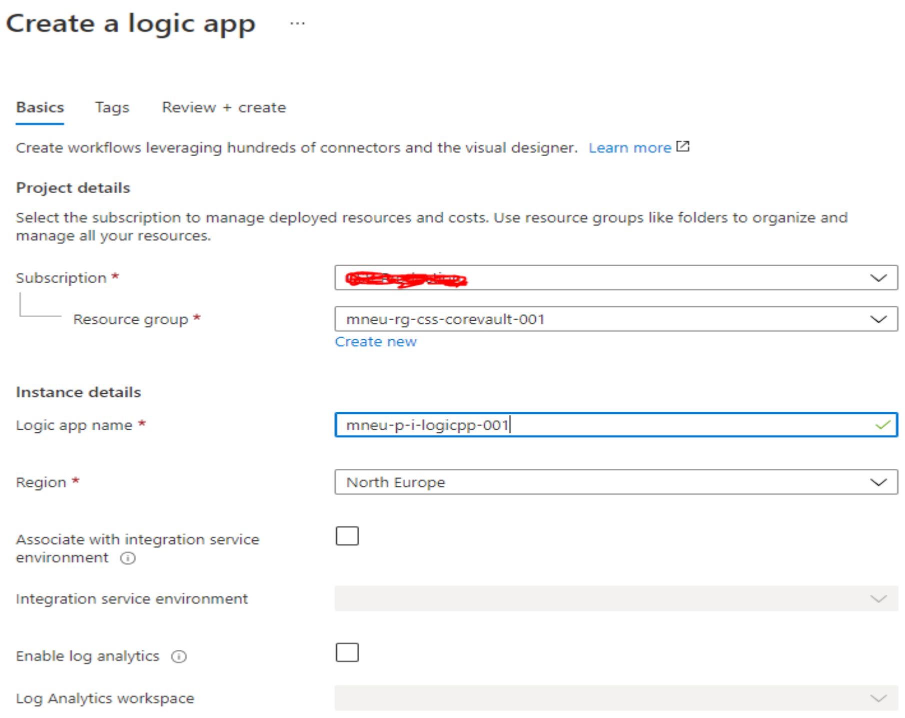
•••••••••••••••••••••••••••••••••

Tags

44e75730b6a94f008765e0d7e31e67b1

Tag Name	Tag Value
Name	EKG_AADS_PVTAKSCL...
NotifyEmail	amarendra.kumar[redacted]...
Requester	Amarendra Kuamr

- **Create Azure Logic app**



Create a logic app ···

Create workflows leveraging hundreds of connectors and the visual designer. Learn more

Project details

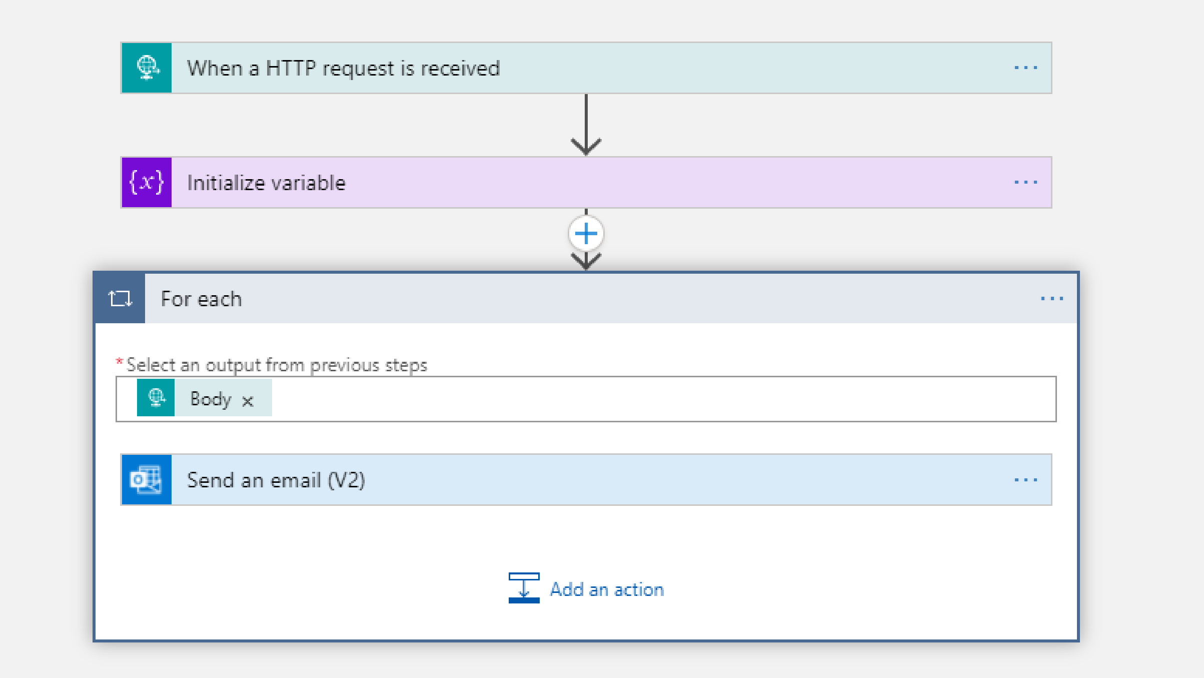
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	[redacted]
Resource group *	mneu-rg-css-corevault-001 Create new

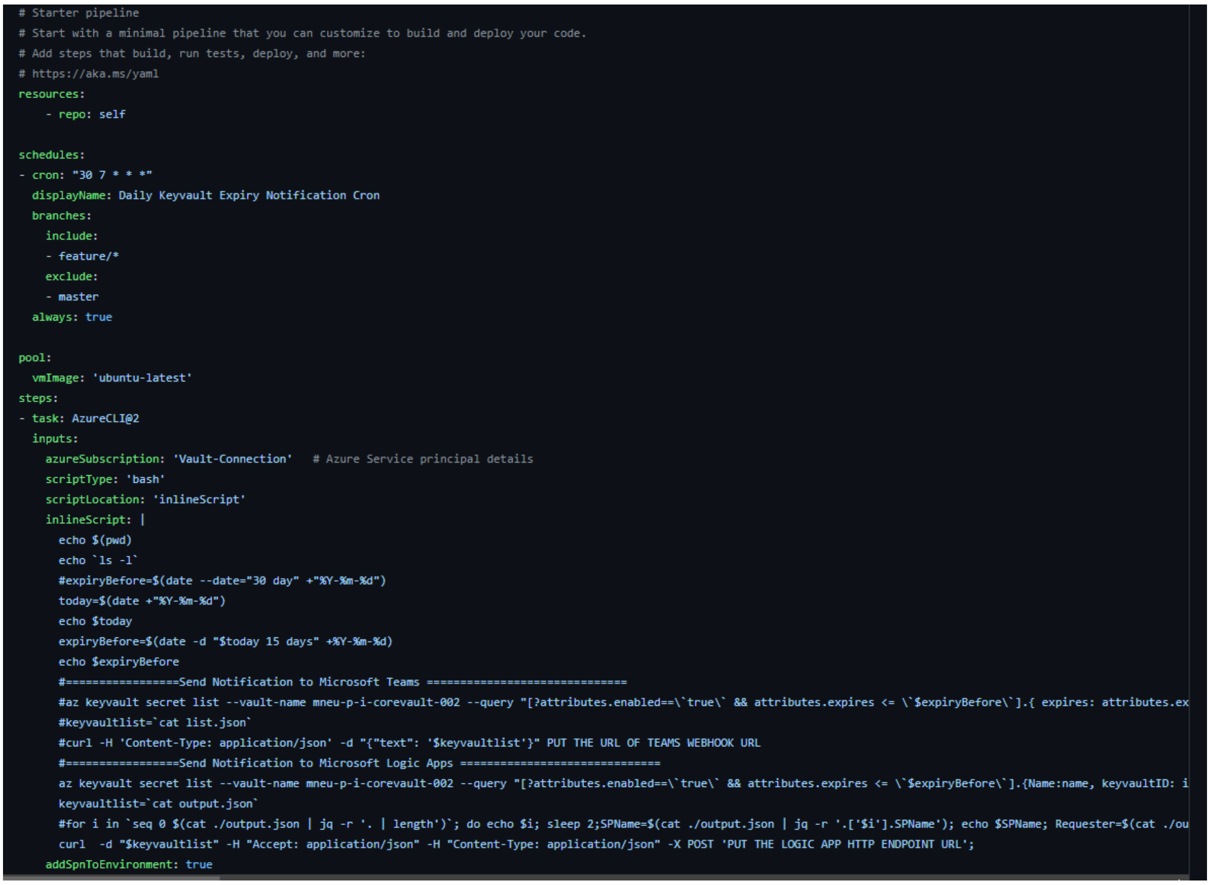
Instance details

Logic app name *	mneu-p-i-logicpp-001
Region *	North Europe
Associate with integration service environment ⓘ	□
Integration service environment	
Enable log analytics ⓘ	□
Log Analytics workspace	

Logic app designer //- code availble in git


When a HTTP request is received
Initialize variable
For each
* Select an output from previous steps
Body ×
Send an email (V2)
Add an action

- Create Azure Devops pipeline
    - Create Azure repo & upload the pipeline.yaml file

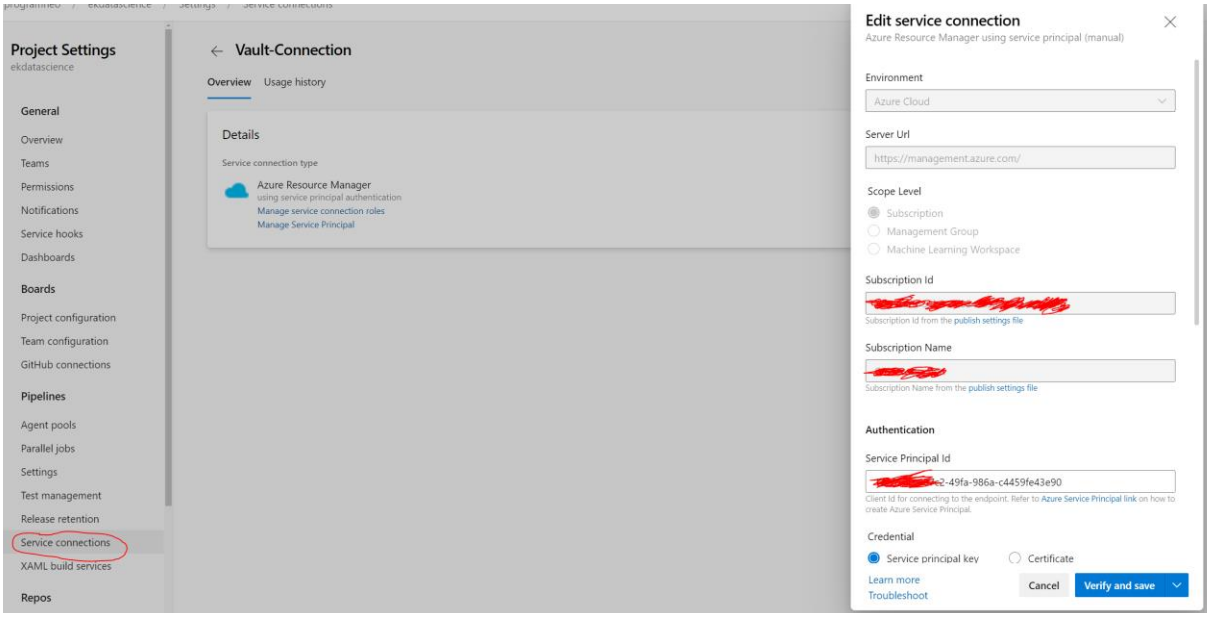


```
# Starter pipeline
# Start with a minimal pipeline that you can customize to build and deploy your code.
# Add steps that build, run tests, deploy, and more:
# https://aka.ms/yaml
resources:
    - repo: self

schedules:
- cron: "30 7 * * *"
  displayName: Daily Keyvault Expiry Notification Cron
  branches:
    include:
    - feature/*
    exclude:
    - master
  always: true

pool:
  vmImage: 'ubuntu-latest'
steps:
- task: AzureCLI@2
  inputs:
    azureSubscription: 'Vault-Connection'   # Azure Service principal details
    scriptType: 'bash'
    scriptLocation: 'inlineScript'
    inlineScript: |
      echo $(pwd)
      echo `ls -l`
      #expiryBefore=$(date --date="30 day" +"%Y-%m-%d")
      today=$(date +"%Y-%m-%d")
      echo $today
      expiryBefore=$(date -d "$today 15 days" +%Y-%m-%d)
      echo $expiryBefore
      #=================Send Notification to Microsoft Teams ==============================
      #az keyvault secret list --vault-name mneu-p-i-corevault-002 --query "[?attributes.enabled==\`true\` && attributes.expires <= \`$expiryBefore\`].{ expires: attributes.ex
      #keyvaultlist=`cat list.json`
      #curl -H 'Content-Type: application/json' -d "{"text": '$keyvaultlist'}" PUT THE URL OF TEAMS WEBHOOK URL
      #=================Send Notification to Microsoft Logic Apps ==============================
      az keyvault secret list --vault-name mneu-p-i-corevault-002 --query "[?attributes.enabled==\`true\` && attributes.expires <= \`$expiryBefore\`].{Name:name, keyvaultID: i
      keyvaultlist=`cat output.json`
      #for i in `seq 0 $(cat ./output.json | jq -r '. | length')`; do echo $i; sleep 2;SPName=$(cat ./output.json | jq -r '.['$i'].SPName'); echo $SPName; Requester=$(cat ./ou
      curl  -d "$keyvaultlist" -H "Accept: application/json" -H "Content-Type: application/json" -X POST 'PUT THE LOGIC APP HTTP ENDPOINT URL';
    addSpnToEnvironment: true
```

- Create service connection using Service Principal as below



Vault-Connection

Details

Service connection type: Azure Resource Manager, using service principal authentication

Manage service connection roles

Manage Service Principal

Edit service connection

Azure Resource Manager using service principal (manual)

Environment: Azure Cloud

Server Url: https://management.azure.com/

Scope Level: ● Subscription ○ Management Group ○ Machine Learning Workspace

Subscription Id: [redacted]

Subscription Id from the publish settings file

Subscription Name: [redacted]

Subscription Name from the publish settings file

Authentication

Service Principal Id: [redacted]2-49fa-986a-c4459fe43e90

Client Id for connecting to the endpoint. Refer to Azure Service Principal link on how to create Azure Service Principal.

Credential: ● Service principal key ○ Certificate