AKS Backup & Restore Pipeline

Advanced Conversational Engagement

Exported on 06/06/2025

Table of Contents

1 Introduction:

This page provides a detailed guide on creating a backup vault, setting up a scheduler, executing the restoration process, and utilizing the pipeline effectively.

2 Prerequisite

We have enable Microsoft.DataProtection provider and Microsoft.ContainerService feature in microsoft.containerservice

2.1 Validation:

Use below script to validate feature and provider is enabled or not

```
az account set subscription <subscription-name>
az feature show --namespace Microsoft.ContainerService --name TrustedAccessPreview --query "properties.state" -o tsv
az provider show --namespace microsoft.dataprotection --query "registrationState" -o tsv
```

3 AKS Backup Configuration:

1. **base-infra-pipeline (**Pipeline link[1]**):**
    a. Storage Account is required to create a backup vault because it acts as the storage layer to store backup data securely. Use the **base-infra-pipeline** to create the required storage account
2. **base-aks-pipeline** (Pipeline link[2])
    a. Create a backup vault, during backup vault creation, a managed identity will be created on runtime, and provide necessary permissions to Managed Identity. Stage Name: **Create Backup Vault. Note:** Backup vault creation is one time activity.
    b. Trusted access to be enabled between AKS cluster and Backup vault, so that the vault can communicate with the Backup Extension to perform backup and restore operations. Stage Name: **Enable Backup Vault Trusted Access**
3. **post-aks-pipeline** (Pipeline link[3])
    a. Backup extension installation: Stage Name: **Deploy Backup Extension**
        - Step 1: creating **backup-app** namespace
        - Step 2: Deploying network policy
        - Step 3: The backup extension will be installed in the **backup-app** namespace. During the deployment of the backup extension, a new service principal will be created. The **Storage Blob Data Contributor** role must be assigned to this new service principal for the associated storage account.
        - **Note**: Check three pods should be running state in the backup-app namespace
4. **team-onboarding-pipeline** (Pipeline link[4])
    a. Backup Policy deployment it contain retention period and frequency of the backup, Stage Name **Deploy Backup Policy**
    b. Instance creation this is kind of container creation in storage account, Stage Name: **Create Backup Instance**

[1] https://dev.azure.com/cbsp-abnamro/GRD0001014/_build?definitionId=99476
[2] https://dev.azure.com/cbsp-abnamro/GRD0001014/_build?definitionId=83262
[3] https://dev.azure.com/cbsp-abnamro/GRD0001014/_build?definitionId=99476
[4] https://dev.azure.com/cbsp-abnamro/GRD0001014/_build?definitionId=83905

4 Use case:

- **Node pool down:**
    - Initiate the cluster reconciliation process using the maintenance pipeline. This step is designed to resolve most node-related issues effectively.
    - If the issue persists, proceed to delete and recreate the user node pool. Services will redeploy automatically upon recreation, manual restoration not required. **Note:** This operation will result in downtime lasting approximately 10–20 minutes.
- **Entire Cluster down:**
    - Delete the existing cluster to resolve any underlying issues.
    - Recreate the Cluster:
        - Set up a new cluster, noting that certain stages will be skipped during the recreation process.
            - base-aks-pipeline below stages to be ignored, remining stage should be executed
                - Create HSM Key
                - <Env name> Disk Encryption
                - Create Backup Vault
                - Note: isClusterRestore if this flag enable in the pipeline above stage execution will be ignored
            - post-aks-pipeline ingress and backup extension should be deployed
            - team-onboarding-pipeline below stages to be ignored, remining stage should be executed
                - Create UMI
                - Deploy Action Group
                - Deploy Metric Alert
                - Create Backup Instance
                - Note: isClusterRestore if this flag enable in the pipeline above stage execution will be ignored

5 AKS Cluster Restoration:

1. **base-aks-pipeline** (Pipeline link[5])
   a. Trusted access to be enabled between AKS cluster and Backup vault, so that the vault can communicate with the Backup Extension to perform backup and restore operations. Stage Name: **Enable Backup Vault Trusted Access**
2. **post-aks-pipeline** (Pipeline link[6])
   a. Backup extension installation: Stage Name: **Deploy Backup Extension**
      - Step 1: creating **backup-app** namespace
      - Step 2: Deploying network policy
      - Step 3: The backup extension will be installed in the **backup-app** namespace. During the deployment of the backup extension, a new service principal will be created. The **Storage Blob Data Contributor** role must be assigned to this new service principal for the associated storage account.
      - **Note**: Check three pods should be running state in the backup-app namespace
3. **team-onboarding-pipeline** (Pipeline link[7])
   a. Backup Policy deployment it contain retention period and frequency of the backup, Stage Name **Deploy Backup Policy**
4. **cluster-maintenance-pipeline** (Pipeline link[8])
   a. Latest backup restoration choose the team name and trigger the pipeline with **Restore Backup** stage.
   b. Specific version restoration
      i. first run trigger the pipeline with **List Recovery Points** stage, select your recovery point id from output.
      ii. Second run pass selected recovery point id as parameter and choose **Restore Backup** stage.

[5] https://dev.azure.com/cbsp-abnamro/GRD0001014/_build?definitionId=83262
[6] https://dev.azure.com/cbsp-abnamro/GRD0001014/_build?definitionId=99476
[7] https://dev.azure.com/cbsp-abnamro/GRD0001014/_build?definitionId=83905
[8] https://dev.azure.com/cbsp-abnamro/GRD0001014/_build?definitionId=84757