

# Provision Azure File Share with Private Endpoint and Storage Account

- Overview
- Problem
- Prerequisites
- Solution
- Related articles

## Overview

<b>Platform:</b>	<b>Azure</b>
<b>Owner of this SOP:</b>	Fully Managed POD A
<b>Cloud Services:</b>	File Share Provisioning

## Problem

When requesters are asking for creating Azure File share with Private Endpoint and Storage account.

tester	Reviewer
@ Ramkumar Samudram (Deactivated)	

## Prerequisites

- Install VS Code
- Access to Terraform workspace and azure portal

## Solution

- Clone the Blue Print 10 repo "<https://gitlab.com/bhp-cloudfactory/azure-blueprints/azr-file-share> " into your repository under new project e.g. <https://gitlab.com/bhp-cloudfactory/tooling-foundations/fm-sops/azrfileshare>
- Change all the variables in the tfvars file to suit your application

```

env_vars > npe.auto.tfvars
1  # Storage Account
2  base_name      = "it"
3  name          = "fmpodastorage"
4  resource_group_name = "it-aeu1-npe-arg-fmpodafileshare"
5  create_resource_group = true           # set this to false if you already have a resource group
6  resource_group_lock_level = ""         # Specifies the Lock Level of the resource group
7  location       = "Australia East"
8  account_tier   = "Standard" # Account tier
9  account_replication_type = "LRS" # Replication type
10 storageid_log_dest = "/subscriptions/01818878-c294-4617-a15a-8b7934a433c4"
11
12 #key-vault information for data block
13 key_vault_name = "it-fmpoda"
14 key_vault_rg   = "it-aeu1-npe-arg-operations"
15
16 # Endpoint
17 storage_endpoint_subnet = {
18   name           = "sub-iaas"
19   resource_group_name = "it-aeu1-npe-arg-network"
20   virtual_network_name = "it-aeu1-npe-vnt-10.125.121.0"
21 }
22
23 # Tags
24 tags = {
25   BusinessUnit = "Fully Managed POD A"
26   CostCentre   = "1410.C.50048.0001"
27   Env          = "NPE"
28   Owner        = "danny.seow1@bhp.com"
29   SecondaryOwner = "ayush.tripathi@bhp.com"
30   DeploymentType = "automated"
31   SolutionName  = "toolingdev"
32   RequestID     = "Testing"
33 }

```

- Change the variables in the env.sh file to match your environment

```

scripts > env.sh
6  # ADD VM(S) SUBSCRIPTION ID HERE
7  export SUBSCRIPTION_ID="01818878-c294-4617-a15a-8b7934a433c4"
8
9  # NPE
10 export TFB_ORG="BHPEG-Dev"
11
12 # prod uncomment the below and comment the above for a prod workspace
13 #export TFC_ORG="BHPEG"
14
15 # Extracted from the device naming standard document
16 export CLOUD_SERVICE_PROVIDER="m" # 'a' for Amazon Web Service, 'm' for Microsoft Azure
17 export ASSET="it" # it (IT), bma (BMA), bmc (BMC), nswec (NSWEC), niw (Nickel West), od (Olympic Dam),
18 # Azure REGIONS      BHP CLOUD REGION IDENTIFIER
19 # "Australia East"   = "aeu1" // New South Wales
20 # "Australia South East" = "ause" // Victoria
21 # "North Central US" = "usnc" // Illinois
22 # "South Central US" = "ussc" // Texas
23 # "West US 2"        = "usw2" // Washington state (seattle)
24 # "East US"          = "use1" // Virginia
25 export REGION="aeu1"
26
27 export ENV=${ENVIRONMENT}
28 export TFC_ADDR="app.terraform.io"
29
30 #export TFC_WORKSPACE_NAME="it-aeu1-npe-prismabaseline-bpazr005"
31 export TFC_WORKSPACE_NAME="a_azr_toolingdev_npe_fmpodastorage_01818878-c294-4617-a15a-8b7934a433c4"
32 export TFC_VERSION="1.0.3"
33

```

- In fetch\_secrets.sh update "your\_tfc\_token\_name" to keyvault variable which has your token

```

AZUREFILESARE
├── doc
├── env_vars
├── npe.auto.tfvars
├── scripts
│   ├── env.sh
│   └── fetch_secrets.sh
├── file_share.sh
├── seed_creds.py
├── terraform-apply.sh
├── terraform-destroy.sh
├── terraform-plan.sh
├── update_workspace.py
├── update_workspace.sh
├── validate.sh
├── templates
├── configversion.json.template
├── destroy.json.template
└── scripts
    └── fetch_secrets.sh
        1  #!/bin/bash
        2
        3  if [ "$client_id" == "" ]
        4  then
        5      az login --identity --allow-no-subscriptions --output none
        6  else
        7      az login --service-principal --username $client_id --password "$client_secret" --tenant $tenant_id --outp
        8  fi
        9
        10 export client_id=`az keyvault secret show --name sp-app-id --vault-name it-fmpoda | jq -r .value`
        11 export client_secret=`az keyvault secret show --name sp-app-secret --vault-name it-fmpoda | jq -r .value`
        12
        13 export TFB_TOKEN=`az keyvault secret show --name tfb-token --vault-name it-fmpoda | jq -r .value`
        14
        15 # These gitlab trigger tokens are shared between all spoke accounts for executing pipelines in azure-foundati
        16 # Do not change the key vault references
        17 export TFC_HSPACE_TOKEN=`az keyvault secret show --name TFC-HSPACE-TOKEN --vault-name it-akv-001 | jq -r .val
        18
        19

```

- Provide the new fileshare name and your key vault name in file\_share.sh file

```

npe.auto.tfvars
├── scripts
│   ├── env.sh
│   ├── fetch_secrets.sh
│   └── file_share.sh
├── seed_creds.py
├── terraform-apply.sh
├── terraform-destroy.sh
├── terraform-plan.sh
├── update_workspace.py
├── update_workspace.sh
├── validate.sh
├── templates
├── configversion.json.template
├── destroy.json.template
├── envvariable.json.template
├── run.json.template
├── uploadstate.json.template
├── variable_new.template
├── .gitlab-ci.yml
├── terraform-docs.yaml
└── data.tf
    3  # replace YOUR_KEY_VAULT with the actual key-vault name.
    4  # replace YOUR_FILE_SHARE_NAME with the name of the file share to be provisioned.
    5
    6  export fileshare="fmpodafileshare"
    7
    8  az login --service-principal --username $client_id --password "$client_secret" --tenant $tenant_id --output n
    9  az account set --subscription $SUBSCRIPTION_ID
   10  az account show
   11
   12  #Creating new file share
   13  storage_account_name=`az keyvault secret show --name storage-account-name --vault-name it-fmpoda | jq -r .val
   14  secret=`az keyvault secret show --name storage-key-primary1 --vault-name it-fmpoda | jq -r .value`
   15  az storage share create --name $fileshare --account-key $secret --account-name $storage_account_name --quota
   16
   17  #Snapshot
   18  az storage share snapshot --name $fileshare --account-key $secret --account-name $storage_account_name --quot
   19
   20
   21  # Recovery Services Vault ### (Optional- if it doesn't exist in the subscription).Uncomment this to create
   22
   23  # export resource_group_name="YOUR_RESOURCE_GROUP_NAME"
   24  # export recovery_services_vault_name="RECOVERY_SERVICES_VAULT_NAME"
   25  # export location="YOUR_LOCATION"
   26  # az backup vault create --location $location --name $recovery_services_vault_name --resource-group $resource
   27

```

- Commit and push your changes
- Verify that the pipeline executes as expected and that a terraform workspace is created and run
- Verify the terraform plan in your TF workspace
- If you are satisfied with the plan output, initiate the apply stage in pipeline

a\_azr\_toolingdev\_npe\_fmpodastorage\_01818878-c294-4617-a15a-8b7934a433c4
Resources
23
Terraform version
1.1.0
Updated
9 hours ago

No workspace description available. [Add workspace description.](#)

Overview
Runs
States
Variables
Settings

Unlocked
Actions

Queued from GitLab CI/CD Pipeline

API Integration triggered a run from API 7 days ago
Run Details

Plan finished 7 days ago
Resources: 13 to add, 0 to change, 0 to destroy

Cost estimation finished 7 days ago
Resources: 0 of 10 estimated - \$0.00/mo - +\$0.00

Policy check passed 7 days ago
Policies: 13 passed, 0 failed

Apply finished 7 days ago
Resources: 13 added, 0 changed, 0 destroyed

- Manually start create\_share stage in pipeline after successful creation of storage account.

bhp-cloudfactory > ... > FM-Sops > Azfilesshare > Pipelines

All	5	Finished	Branches	Tags
Filter pipelines				
Status	Pipeline ID	Triggerer	Commit	Stages
<div>passed</div>	#433021714 latest		main - 94c70d5b Update scripts/file_sha...	<div>create_share: passed</div> <div><div>✓</div><div>✓</div><div>✓</div><div>✓</div><div>✓</div></div>

- Check and confirm whether the required fileshare is created as per requirement

it1fmpodastorage1ald | File shares

Storage account

Search (Ctrl+ /)

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage browser (preview)

Data storage

Containers

File shares

+ File share

Refresh

File share settings

Active Directory: Not configured

Soft delete: 7 days

Maximum capacity: 5 TiB

Search file shares by prefix (case-sensitive)

Show deleted shares

Name	Modified	Tier	Quota	
fmpodafileshare	12/20/2021, 1:30:55 PM	Transaction optimized	50 GiB	...

Related articles

- Mount the Azure file share - Cloud Platform - Confluence (atlassian.net)
- FileShare soft delete - Cloud Platform - Confluence (atlassian.net)
- Schedule backups on Azure File Share - Cloud Platform - Confluence (atlassian.net)
- File Share - Files restore from snapshot or backup - Cloud Platform - Confluence (atlassian.net)