

# Create Windows VMs behind a load balancer

- [Overview](#)
- [Problem](#)
- [Solution](#)
- [Related articles](#)

## Overview

<b>Platform:</b>	<b>Azure</b>
<b>Owner of this SOP:</b>	Fully Managed POD A
<b>Cloud Services:</b>	Instance Management

## Problem

When requesters are asking for creating Windows VM behind the load balancer.

tester	Reviewer
@ Ramkumar Samudram (Deactivated)	

## Solution

1. Clone the Blue Print 8 repo <https://gitlab.com/bhp-cloudfactory/azure-blueprints/azr-iaas-single-tier> into a your repository under new project e.g. <https://gitlab.com/bhp-cloudfactory/tooling-foundations/fm-sops/winvmwithlb>
2. Change all the variables in the tfvars file as per your requirement. Please go through the blue print read me file for more details

```
WINVMWITHLB
├── winvmwithlb
│   ├── .idea
│   │   ├── .gitignore
│   │   ├── doc
│   │   └── env_vars
│   │       └── npe.auto.tfvars
│   ├── scripts
│   ├── templates
│   ├── .gitlab-ci.yml
│   ├── .pre-commit-config.yaml
│   ├── .terraform-docs.yaml
│   ├── data.tf
│   ├── locals.tf
│   ├── meta.tf
│   ├── outputs.tf
│   ├── primary_site.tf
│   ├── providers.tf
│   ├── README.md
│   ├── resource-group.tf
│   ├── secondary_site.tf
│   └── variables.tf
├── OUTLINE
└── TIMELINE

winvmwithlb > env_vars > npe.auto.tfvars
1  availability_set_name      = "aue1winvmavs01"
2  load_balancer_name        = "aue1winvmlb01"
3  resource_group_name       = "it-aue1-npe-arg-fmpodawin2019"
4  location                   = "Australia East" #Azure location
5  network_resource_group_name = "it-aue1-npe-arg-network" # Name of
6  subnet_name                = "sub-iaas" # THE SUBNET NAME WHERE THIS VM IS C
7  virtual_network_name       = "it-aue1-npe-vnt-10.125.121.0" # THE VNET NAM
8  rsv_resource_group_name    = "it-aue1-npe-arg-backup"
9  recovery_vault_name        = "it-aue1-npe-rsv-grs"
10 backup_policy_name         = "AU_Non-Production_VM"
11
12
13 secondary_availability_set_name = "ausewinvmavs01"
14 secondary_load_balancer_name    = "ausewinvmlb01"
15 secondary_resource_group_name  = "it-aue1-npe-arg-fmpodawin2019-secondary"
16 secondary_location              = "Australia Southeast" #Azure loca
17 secondary_subnet_name           = "sub-iaas" # THE SUBNET NAME WHERE THIS V
18 secondary_virtual_network_name  = "it-ause-npe-vnt-10.125.201.0" # THE VNE
19 secondary_rsv_resource_group_name = "it-aue1-npe-arg-backup"
20 secondary_recovery_vault_name   = "it-ause-npe-rsv-grs"
21 secondary_backup_policy_name    = "Non-Production-VM"
22
23 #datadog_enabled = 0
24 #shared_landscape_resource_group = "YOUR SHARED SUBSCRIPTION RESOUR
25 #shared_landscape_secondary_resource_group = "YOUR SHARED SUBSCRIPTION SECON
26 domain_enabled = true # mark true if VMs need to join Domain
27 enable_backup = false # Backup ### Uncomment if backup needs to be disabled
28 sku = "Basic"
29 frontend_ip_primary = {
30   "sample1" = {
31     name = "Frontendip001" ### NAME
```

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

```
WINVMWITHLB
├── winvmwithlb
│   ├── .idea
│   │   ├── .gitignore
│   │   ├── doc
│   │   └── env_vars
│   │       └── npe.auto.tfvars
│   ├── scripts
│   │   ├── apply-workspace.sh
│   │   ├── cyberark.py
│   │   ├── cyberark.sh
│   │   └── env.sh
│   ├── fetch_secrets.sh
│   ├── seed_creds.py
│   ├── terraform-apply.sh
│   ├── terraform-destroy.sh
│   ├── terraform-plan.sh
│   ├── update_workspace.py
│   ├── update_workspace.sh
│   ├── upload_variables.py
│   ├── validate.sh
│   ├── win_secrets_inject.py
│   ├── templates
│   ├── .gitlab-ci.yml
│   ├── .pre-commit-config.yaml
│   ├── .terraform-docs.yaml
│   ├── data.tf
│   └── variables.tf
├── OUTLINE
└── TIMELINE

winvmwithlb > scripts > env.sh
1  #!/bin/bash
2
3  # this should be the same as the name of your auto.tfvars file under env_vars folder e.g npe.auto.tfvars
4  export ENVIRONMENT="npe"
5
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 TFB_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), nswee (NSWEE), niw (Nickel West), od (Olympic Dam)
18 # Azure REGIONS BHP CLOUD REGION IDENTIFIER
19 # "Australia East" = "aue1" // 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="aue1"
26
27 export ENV=${ENVIRONMENT}
28 export TFC_ADDR="app.terraform.io"
29
30 export TFC_WORKSPACE_NAME="a_azr_toolingdev_npe_fmpodalb_01818878-c294-4617-a15a-8b7934a433c4"
31 export TFC_VERSION="1.0.3"
```

4. in fetch\_secrets.sh update your key vault name in the required field

```
WINVMWITHLB
├── winvmwithlb
│   ├── .idea
│   ├── .gitignore
│   ├── doc
│   ├── env_vars
│   ├── npe.auto.tfvars
│   ├── scripts
│   │   ├── apply-workspace.sh
│   │   ├── cyberark.py
│   │   ├── cyberark.sh
│   │   ├── env.sh
│   │   └── fetch_secrets.sh
│   ├── seed_creds.py
│   ├── terraform-apply.sh
│   ├── terraform-destroy.sh
│   ├── terraform-plan.sh
│   ├── update_workspace.py
│   ├── update_workspace.sh
│   ├── upload_variables.py
│   ├── validate.sh
│   ├── win_secrets_inject.py
│   ├── templates
│   ├── .gitlab-ci.yml
│   └── .pre-commit-config.yaml
└── 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 --output
        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 export TFC_ADDR="app.terraform.io"
        16
        17 # These gitlab trigger tokens are shared between all spoke accounts for executing pipelines in azure-foundati
        18 # Do not change the key vault references
        19 export TFC_WSPACE_TOKEN=`az keyvault secret show --name TFC-WSPACE-TOKEN --vault-name it-akv-001 | jq -r .val
        20
        21 export winvm_secrets_inject_gl_token=`az keyvault secret show --name winvm-secrets-inject-token --vault-name
        22
        23
        24 ##CyberArk token
        25 export cyberark_token=`az keyvault secret show --name cyberark-token --vault-name it-akv-001 | jq -r .value`
        26
```

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

**a\_azr\_toolingdev\_npe\_fmpodalb\_01818878-c294-4617-a15a-8b7934a433c4**

Resources47Terraform version1.1.2Updated5 hours ago

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

OverviewRunsStatesVariablesSettings

UnlockedActions

Current Run

Queued from GitLab CI/CD Pipeline

CURRENT

Applied

#run-24mgUSYJoDMUxLtg | API Integration triggered via API

5 hours ago

- 9. Logon to Azure portal and verify that whether the Load balancers are created as per requirement

Load balancing | Load Balancer

Search (Ctrl+/) Create Manage view Refresh Export to CSV Open query Assign tags Feedback

Overview

Load Balancing Services

Application GatewayFront DoorLoad BalancerTraffic Manager

Filter for any field... Subscription == it-npe-toolingdev Resource group == all Location == all Add filter

Showing 1 to 2 of 2 records.

No groupingList

Name	Resource group	Location	Subscription
ae1winnvmlb01	it-it-ae1-npe-arg-fmpodawin2019	Australia East	it-npe-toolingdev
ausewinnvmlb01	it-it-ae1-npe-arg-fmpodawin2019-s-	Australia Southeast	it-npe-toolingdev

Related articles

- [AWS VPC Endpoints configuration change](#)
- [Renewal / Upload SSL certificate for existing Application](#)
- [Monitoring GitLab Access Audit Report](#)

- [Azure Storage Account Blueprint SOP - BPAZR022](#)
- [Azure App Service FTP Credential Sharing and Reset Procedure](#)