Deploying Vault Server

Ned Bellavance
MICROSOFT AZURE MVP

@ned1313 | nedinthecloud.com

Overview

Vault configuration options

Review scenario requirements

Hardening Vault server

Vault Server Configuration

Parameter Categories

General

High Availability

Listener

Seal

Telemetry

Storage

General Parameters

cluster_name

cache_size

disable_cache

disable_mlock

plugin_directory

log_level

default_lease_ttl

max_lease_ttl

default_max_request_duration

raw_storage_endpoint

pid_file

ui

Listener Parameters

Address information

Request information

X-Fowarded-For

Proxy behavior

TLS server

Client certificates

Listener Example

```
listener “tcp” {
  address = “0.0.0.0:8200”
  cluster_address = “0.0.0.0:8201”
  tls_cert_file = “path to cert file”
  tls_key_file = “path to key file”
}
```

Storage Options

Blob storage

Database

Key-value

File

Memory

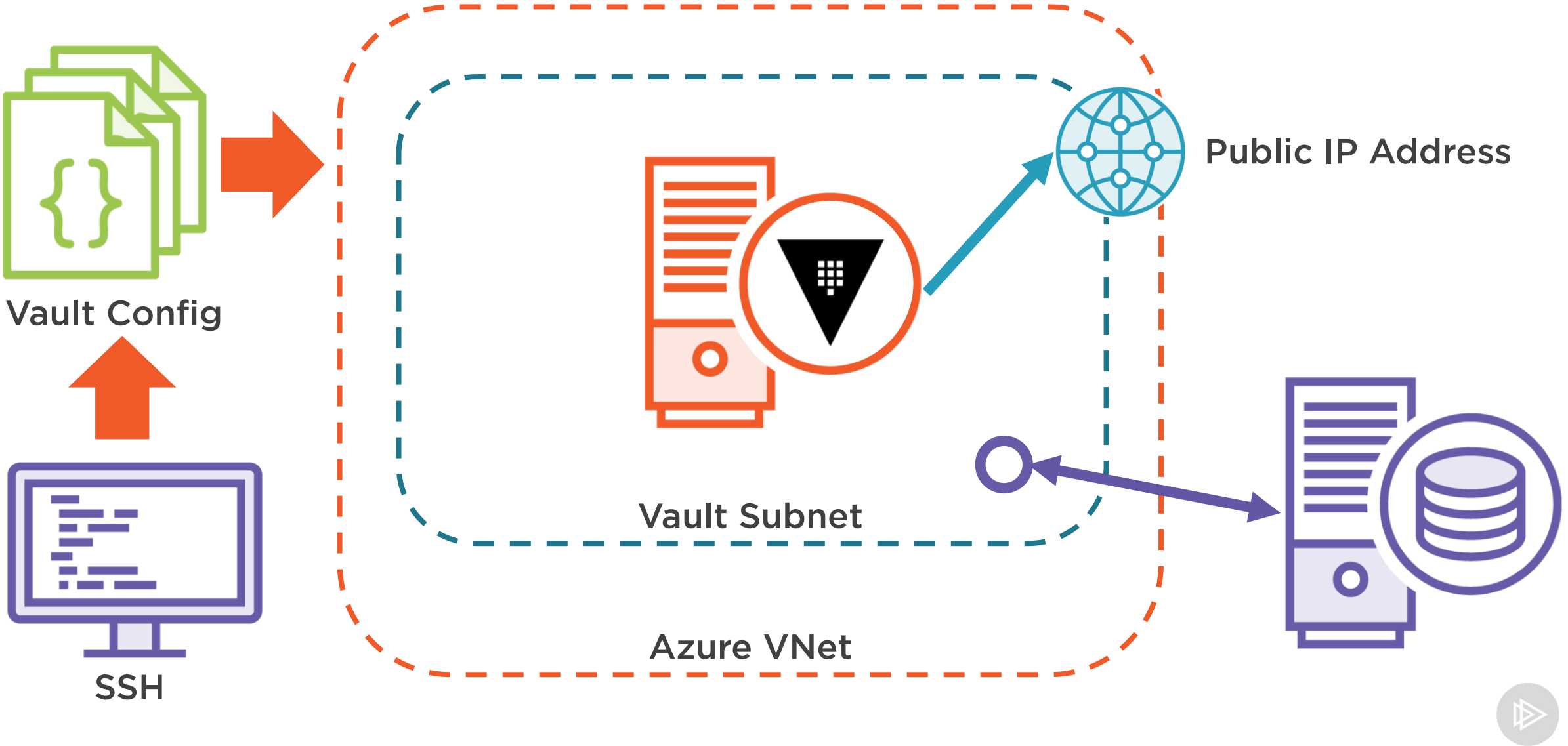
Storage Examples

```
storage “consul” {
  address = “127.0.0.1:8500”
  path = “vault”
}
storage “mysql” {
  address = “127.0.0.1:3306”
  username = “vaultuser”
  password = “mysql password”
}
```

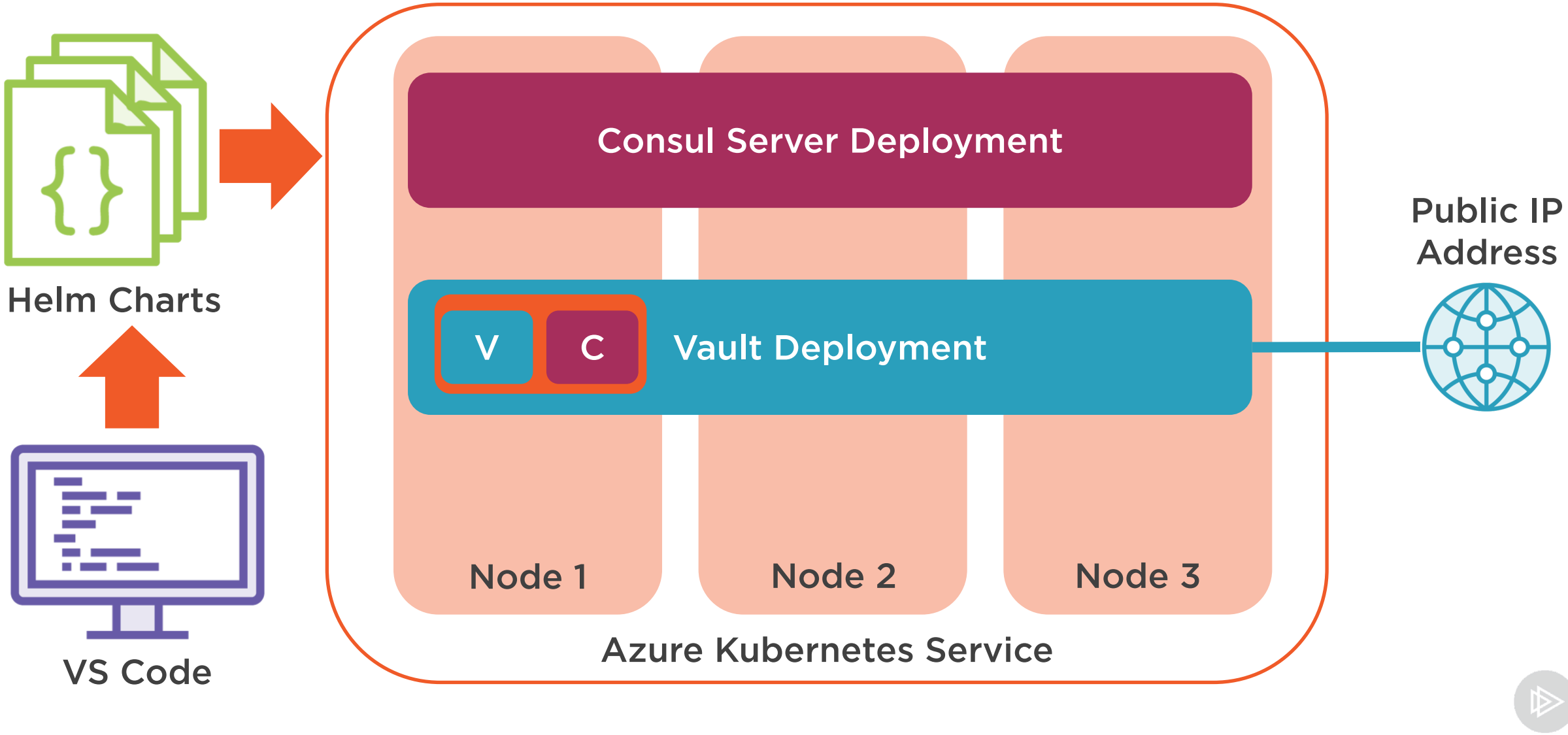
Globomantics Requirements

- Use third-party certificates
- SLA of 99.99% for Vault
- Auto unseal of Vault
- Azure Monitor telemetry
- Daily backups

Azure VMs Deployment



Azure Kubernetes Service Deployment



Vault Hardening

End-to-end TLS

Restrict traffic

Disable remote access

Disable swap and command history

Run unprivileged

Vault Hardening Cont...

- Immutable and frequent upgrades
- Avoid root token
- SELinux or AppArmor
- Enable auditing
- Protect storage

Summary

Many configuration options

Sane default settings

Hardening goes beyond Vault

Coming up:

- Managing Administrator Access Using Roles