Configuring High Availability

Ned Bellavance

Founder, Ned in the Cloud LLC

@ned1313 | nedinthecloud.com

Overview

Vault server clustering

Cluster communications
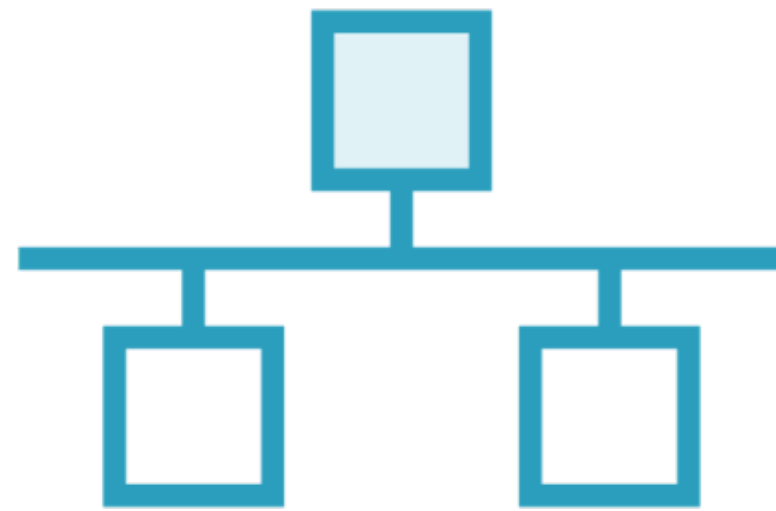
Scenario review

Vault replication options

Vault Server Clustering

High Availability Components

Compute

Network

Storage

Compute

- **Active and standby**
- **Forward or redirect**
- **Read-only for Enterprise**
- **Lock based in datastore**
- **Different storage for HA**

Network Components

Listener cluster_address

Node cluster_addr

Node api_addr

Direct access

Load balancer

Cluster Communications

```
listener "tcp" {
    address = 10.1.1.1:8200
    cluster_address = 10.1.1.1:8201
}
```

```
listener "tcp" {
    address = 10.1.1.2:8200
    cluster_address = 10.1.1.2:8201
}
```
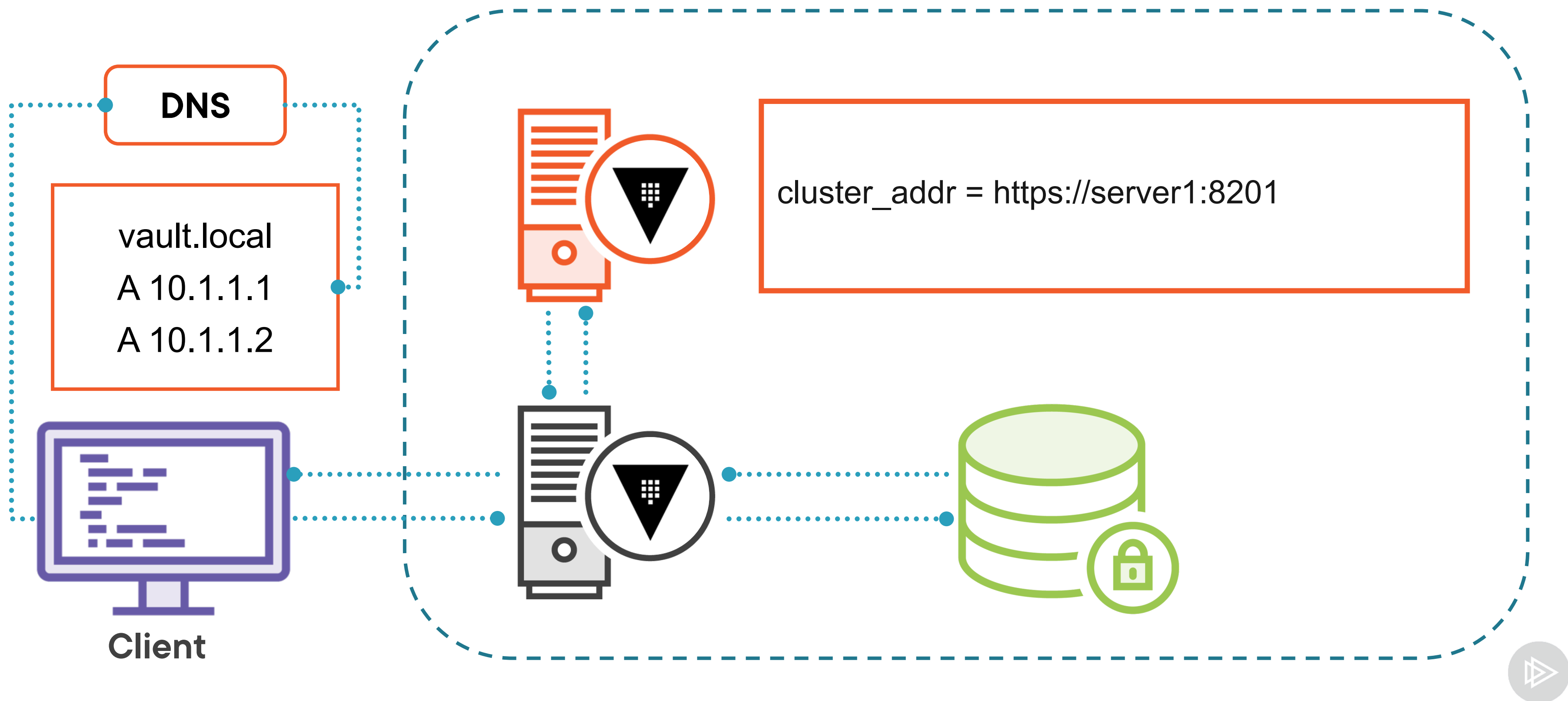
Cluster Communications

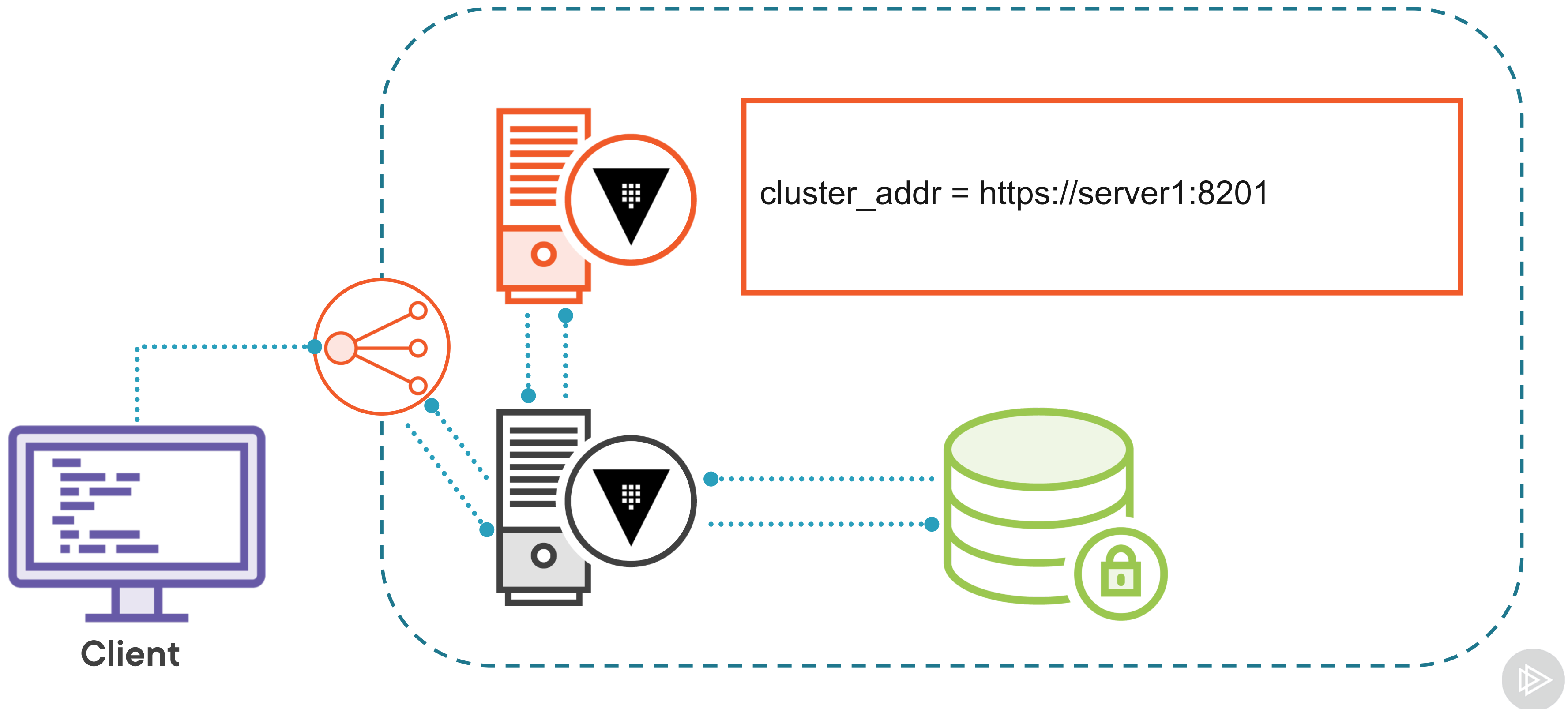cluster_addr = https://server1:8201
api_addr = https://server1:8200

cluster_addr = https://server2:8201
api_addr = https://server2:8200

Network Traffic - Request Forwarding

DNS

vault.local
A 10.1.1.1
A 10.1.1.2

cluster_addr = https://server1:8201

Client

Network Traffic - Request Forwarding

cluster_addr = https://server1:8201

Client

Network Traffic – Client Redirection

DNS

vault.local
A 10.1.1.1
A 10.1.1.2

api_addr = https://server1:8200

Client

Network Traffic – Client Redirection

api_addr = https://server1:8200
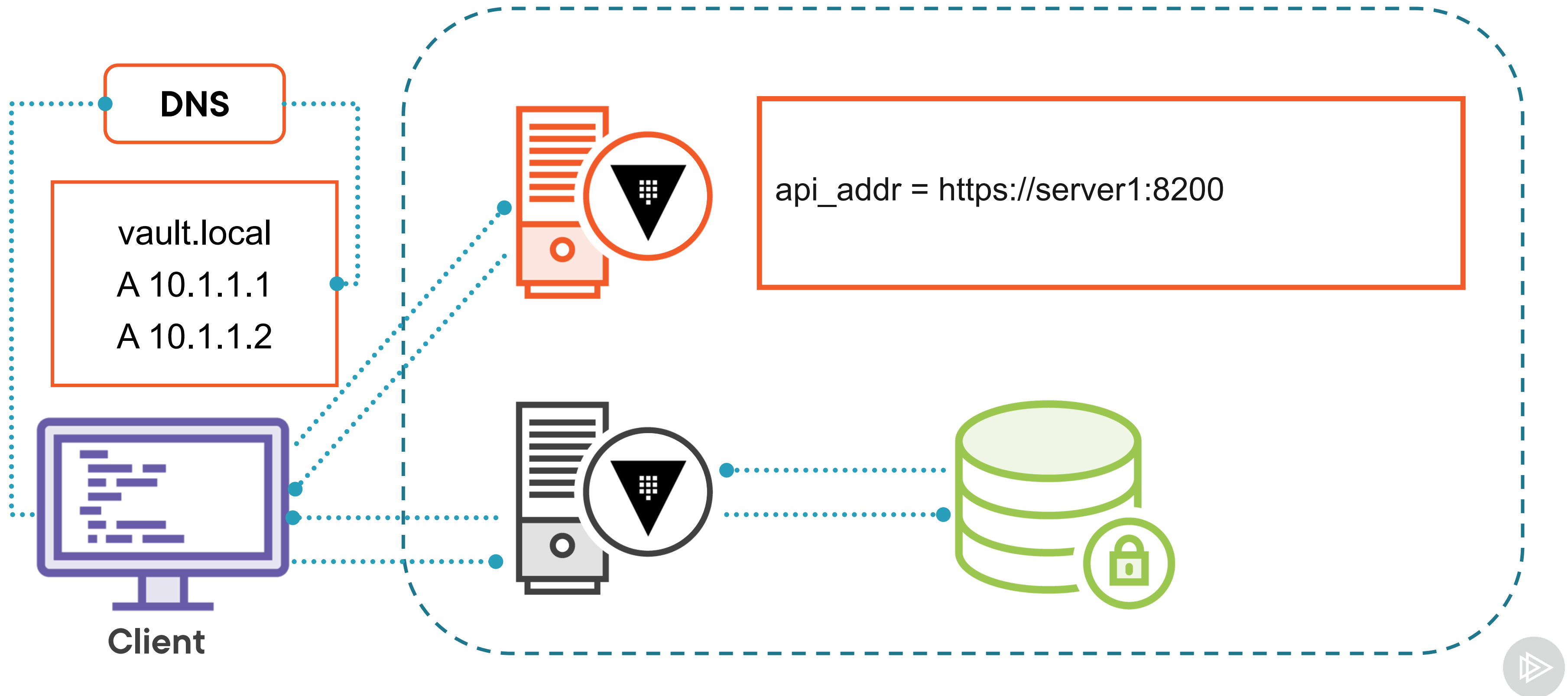
Client
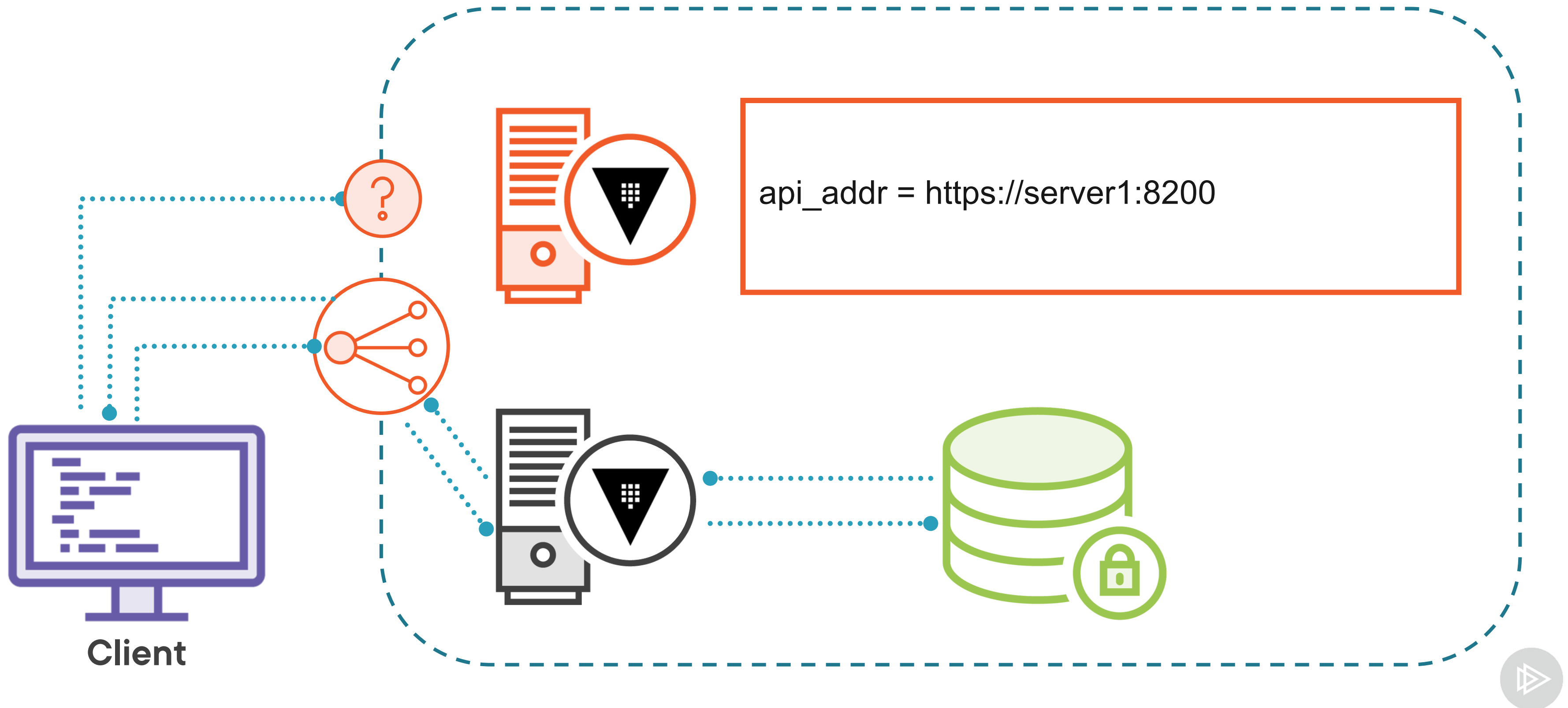
Globomantics Requirements

GLOBOMANTICS

Deploy in Azure

Publicly available endpoint

Use third-party certificates

SLA of 99.99% for Vault

Auto unseal of Vault

Azure VMs Deployment

Vault subnet

Azure VNet

Public hostname

CNAME

Globomantics.xyz

DNS
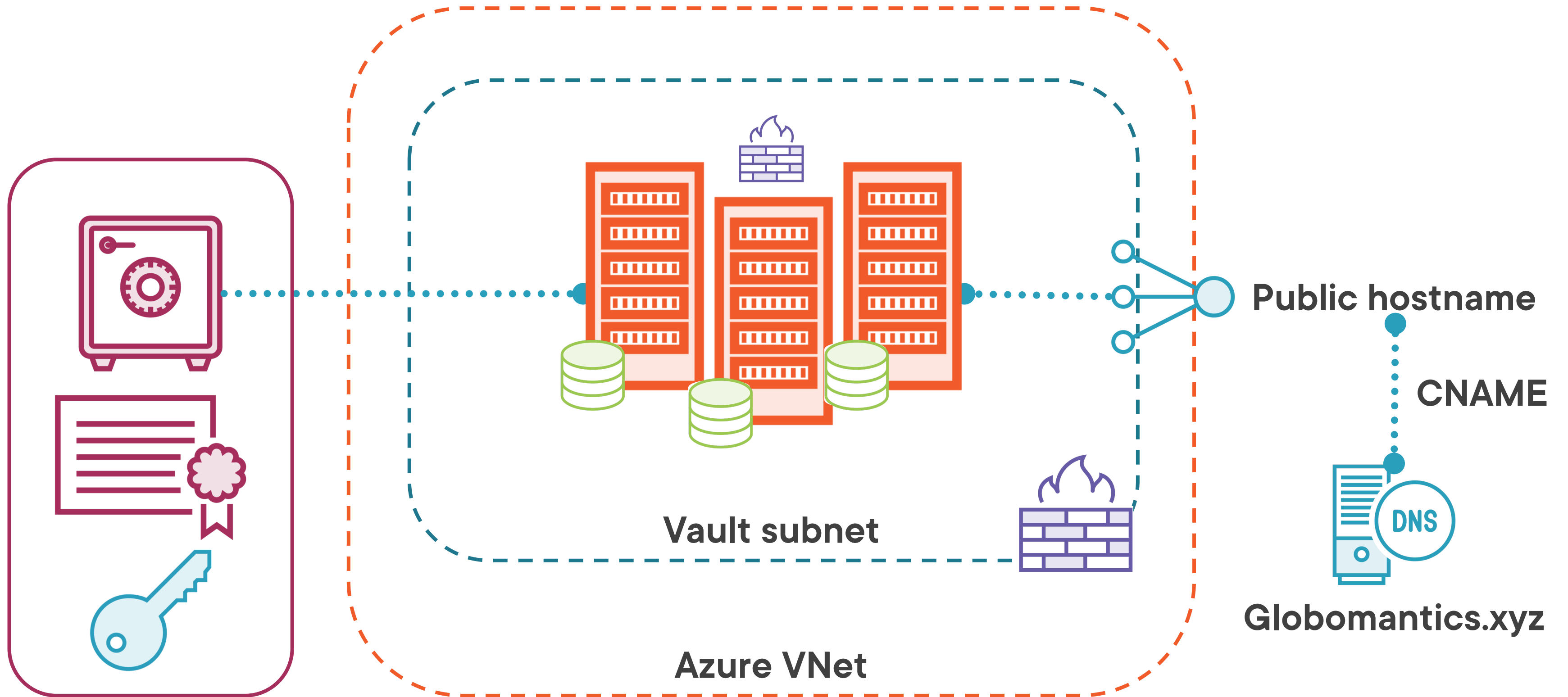
Vault-Config.hcl

```hcl
# HA parameters
cluster_addr = "https://LOCAL_IPV4:8201"
api_addr = "https://SERVER_HOSTNAME:8200"

# Listener parameters
listener "tcp" {
 address       = "0.0.0.0:8200"
 cluster_address = "0.0.0.0:8201"
}
```

Demo

Tasks

- Deploy new infrastructure
- Initialize and validate cluster
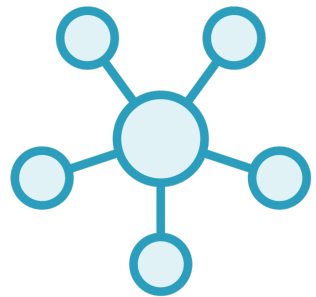
Vault Replication

Vault Replication

Enterprise only

Cluster is unit of replication

Replication is one-to-many

Replication is asynchronous

Replication Options

Disaster recovery
Replicates tokens and leases
No requests to secondaries

Performance
Replicates data only
Read-only requests allowed

Module Summary

Vault clusters run in an active/standby model

Vault clusters require HA storage

Vault client communication can be forwarded or redirected

Replication is between Vault clusters supporting DR or performance

Up Next: Configuring Basic Authentication