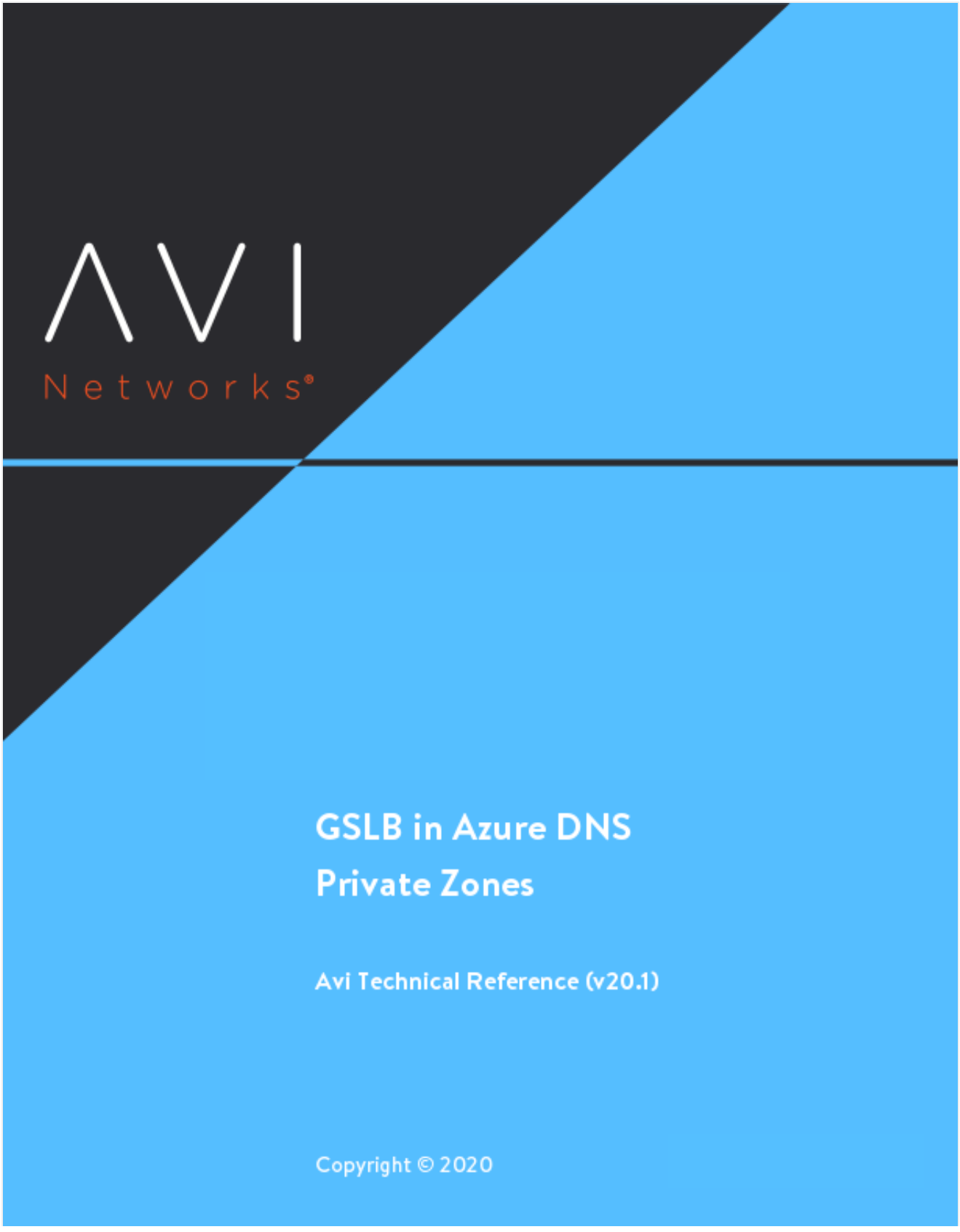


GSLB in Azure DNS Private Zones

Avi Technical Reference (v20.1)

GSLB in Azure DNS Private Zones

view online

Overview

Microsoft Azure DNS private zones enables creating zones inside the private networks that can span multiple Azure virtual networks and on-premises DCs (using VPN or Express Route). With private DNS zones, you can use your own custom domain names rather than the Azure-provided names that are available today. Using custom domain names you can customize the virtual network architecture to best suit your organization's needs. It provides name resolution for virtual machines (VMs) within a virtual network and between virtual networks. Additionally, you can configure zone names with a split-horizon view, which allows a private and a public DNS zone to share the same name. For complete information on Azure private DNS, refer to Use Azure DNS for private domains.

Avi Global Server Load Balancing (GSLB)

Global Server Load Balancing (GSLB) balances the load across application instances that have been deployed at multiple locations (typically, multiple data centers and/or public clouds). Application load at any one location is usually managed by a local load balancer, which could be Avi Vantage or a third-party ADC solution.

GSLB is usually implemented to achieve one or more of the following goals for an application: * Provide optimal application experience to users and clients across geographically distributed areas. * Offer resilience to the loss of a data center or network connection. * Perform non-disruptive migration or addition of another data center.

Avi GSLB performs the following functions: * Chooses the location (data center/cloud) for steering the client's requests. * Monitors the virtual services' health to choose the best location by ruling out the unhealthy ones. * Synchronizes configuration and the state across GSLB sites so that above mentioned functions operate without failures.

The first two functions performed by Avi GSLB is totally opaque to the end-users. Avi Vantage uses the Domain Name System (DNS) to provide optimal destination information to the user clients. When a client (typically browser) performs a DNS query on fully qualifies domain names (FQDN), Avi GSLB responds with the IP address (VIP) of the optimal application instance. The optimal address will change based on the load balancing algorithm, the health of the application instances, and the location of the clients.

For detailed explanation on Avi GSLB architecture and site operations, refer to Avi GSLB architecture.

Avi Integrated Solution for GSLB in Azure

In collaboration with Microsoft Azure, Avi Networks have devised a solution to provide highly available, optimal user experience. This solution seamlessly combines on-premises systems and the services across multiple locations within your Azure private DNS zone. The solution enables you to balance the load across application instances that have been deployed in multiple locations (within private DNS zone and on-prem DC) without any need for a fully qualified public domain name (FQDN) or public IP addresses.

As networks and applications scale, this solution also helps with the challenges such as performance, resiliency, migration, application testing without any downtime and helps gain application insights.

Deploying Avi GSLB alongside Azure private DNS zones provides you the following enterprise-grade benefits:

- Not limited to a region or subscription ID ? The virtual networks belonging to different subscription IDs or regions can be part of the same solution.

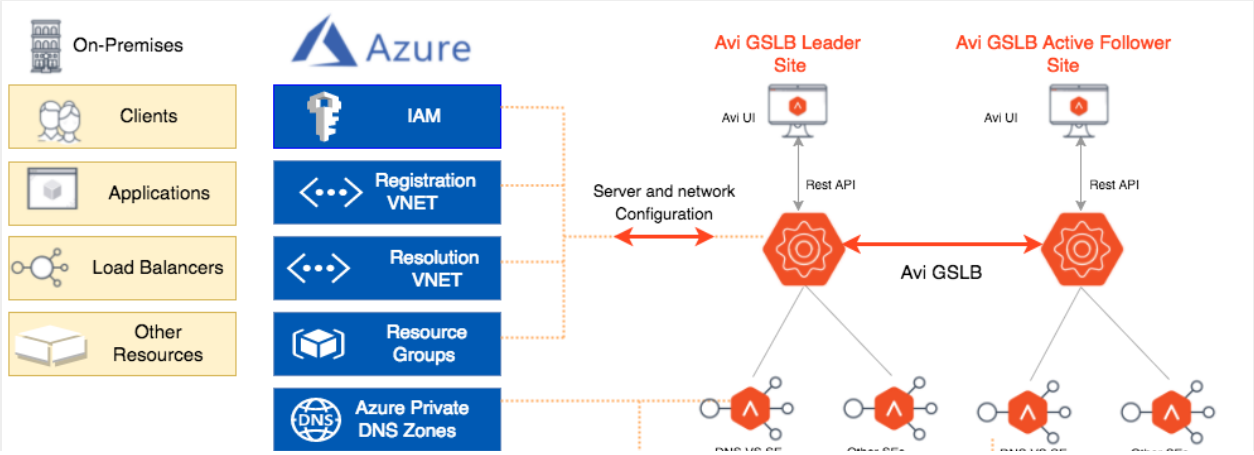
- Increased application availability ? The joint solution delivers high availability for your critical applications by monitoring your endpoints and providing seamless failover so that only healthy servers are returned on lookups.
- Improved application performance ? The solution improves application responsiveness by directing traffic to the endpoint within the lowest proximity for the client.
- Service maintenance without downtime ? The solution enables you to perform planned maintenance operations on your applications without downtime by directing traffic to alternative endpoints.
- Distribute traffic for complex deployments ? GSLB methods can be combined to create sophisticated and flexible rules to scale to the needs of larger and more complex deployments using two-level algorithms.
- Elasticity and autoscaling ? The analytics-driven, scale-out approach allows the load balancers to elastically provide on-demand autoscaling based on real time traffic patterns.
- Split-horizon DNS support ? This solution works seamlessly for the zones with a split-horizon view.

Capabilities

- Functions across all peered VNets and on-prem DC.
- Provides seamless name resolution
  - Between VMs located in the same virtual network.
  - Between VMs in different virtual networks?.
  - For Azure hostnames from on-premises clients.?
- Provides access to applications hosted in one VNet from other VNets and vice versa. Also, access to applications hosted on-prem from Azure VNets and vice versa.
- Provides reliable health checks for endpoints supporting Ping, TCP, HTTP(S), and customs checks.
- Provides seamless DNS based failover without any production impact.
  - In case the VNet in a peered group is down, provides seamless operation as the endpoints present in that affected VNet will not be included in any DNS query until it is back up.
- Ensures high availability and reliability
- Allows an option to fallback to any site or refuse query.
- Enables DNS based policies
- Accelerates CI/CD deployment with the support of A/B testing for new features using priority algorithm.
- Provides autoscaling capabilities during peak traffic.
- Provides centralized provisioning with automated discovery of applications across sites.
- Supports application monitoring, logs, and analytics across sites.
- Supports customisable TTL
- Allows the option to send one or more DNS records.

Primary Components

The primary components involved in the integration are as shown below.



Avi GSLB Components

```
<td>Leader site</td>
<td>The site (Avi Controller cluster) from where the GSLB setup is configured.<br>
Hosts an authoritative DNS.<br>
Actively monitors the health of other GSLB sites.</td>
```

```
<td>Active follower site</td>
<td>Avi Controller cluster which receives configuration from the leader.<br>
Typically hosts an authoritative DNS.<br>
Actively monitors the health of other GSLB sites.</td>
```

```
<td>Passive follower site</td>
<td>Avi Controller cluster which hosts only load balancing virtual services.<br>
- Does not host DNS<br>
- Does not perform health monitoring for other sites</td>
```

```
<td>Third party site</td>
<td>A non-Avi site, which typically is a load balancer application, for instance, Azure Application Gateway. <br>
    Only provides a third party VIP: Port <br>
    Avi leader / active follower sites will perform health monitoring for every third party site.</td>
```

```
<td>GSLB service</td>
<td>The representation of a global application. Serves as a front-end for applications that are deployed at multiple si
```

```
<td>GSLB pool</td>
<td>Combines virtual services into a single entity and balances the load across them.</td>
```

```
<td>GSLB pool members</td>
<td>The virtual services that comprise a GSLB pool are called GSLB pool members. Members can be specified by<br>
    - Avi virtual service name,<br>
    - An IP address, to specify standalone servers or VIPs defined by third-party load balancers.</td>
```

```
<td>GSLB health monitor</td>
<td>Ping, TCP, UDP, DNS, and HTTP(S) health monitors are supported. <br>
Additionally, you can write and incorporate your own monitor using external health monitor option.<br>
    Refer to the following document for more details on monitors and configuring custom monitors : <br>
   <a href="https://avinetworks.com/docs/18.1/avi-gslb-service-and-health-monitors"> Avi GSLB Service Health Monitors <
```

Azure Private Zone Components

This service can be used in conjunction with your own DNS servers (such as Avi DNS virtual service as shown in the topology above), to resolve both on-premises and Azure hostnames. We can use name resolution between VMs and role instances within the same cloud service, without the need for an FQDN.

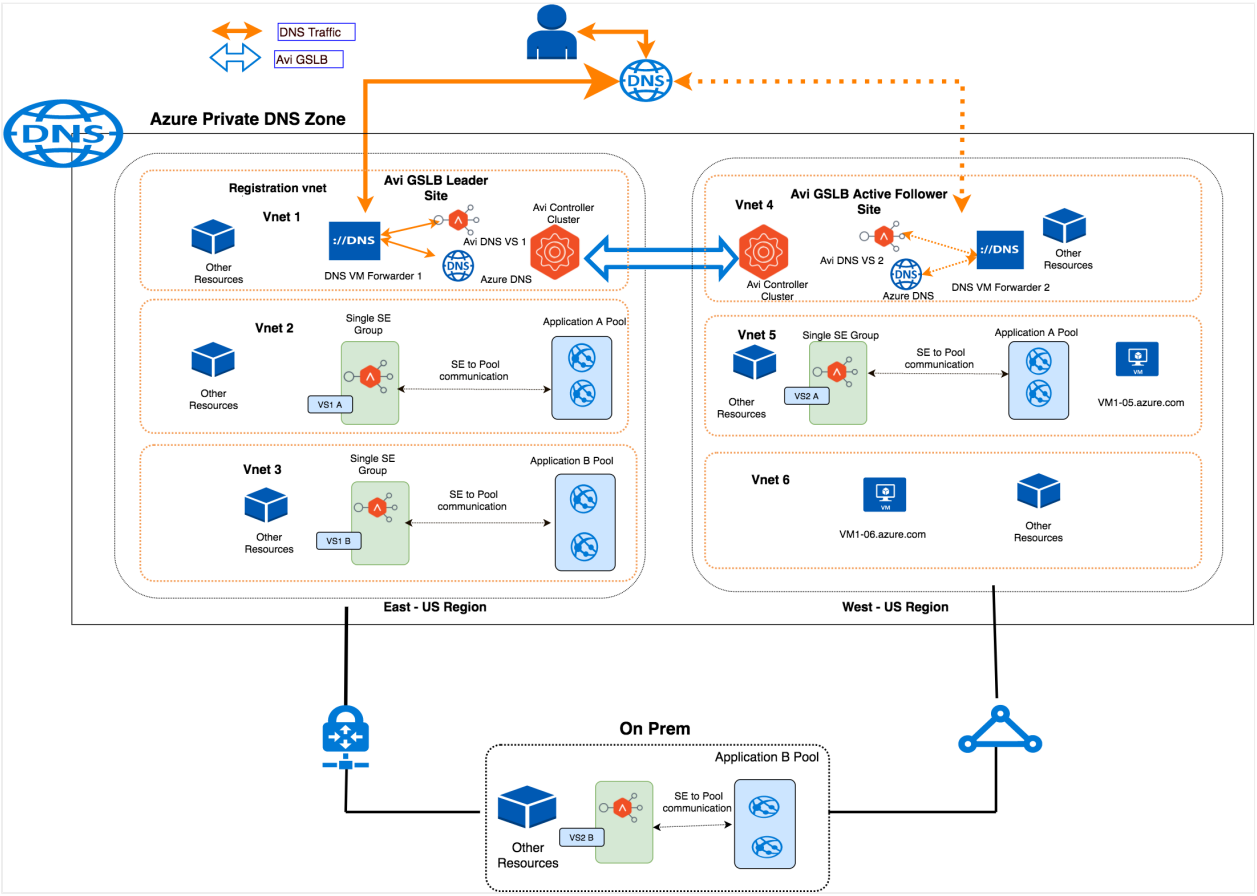
- Registration virtual networks ? When you designate a virtual network as a registration virtual network at the time of creating a private zone or later when you update the zone, Azure will dynamically register DNS A records in the private zone for the virtual machines within this virtual network. This will keep track of virtual machine additions or removals within the virtual network to keep your private zone updated. This is done automatically without any intervention.
- Resolution virtual networks ? You can also designate up to 10 virtual networks as resolution virtual networks while creating or updating a private zone. Forward DNS queries will resolve against the private zone records from any of these virtual networks.

DNS VM Forwarder

DNS VM forwarder is a BIND DNS server hosted on Azure. It is deployed for conditionally forwarding DNS queries based on the subdomains. This is the first point of contact for all the requests coming in for *.azure .com. Once the requests are received by the DNS forwarder, it will check for the FQDN names and based on the rules will forward the requests either to Azure DNS or Avi DNS virtual service. Avi DNS virtual service will handle all the traffic related to applications that need to be handled by GSLB. Azure DNS will handle all internal hostname resolution. For instance, for azure.com zone, there are two DNS VM forwarders configured to forward requests from gslb.azure.com to Avi DNS and to Azure DNS.

Points to Note: * You can configure multiple DNS VM forwarders. * If you are planning to host Avi DNS virtual service, it is recommended to configure the forwarders in the same VNets. (Refer to the sample topology provided) * The DNS VM Forwarder IP addresses need to be configured as custom DNS for all VNets in Azure. Similarly, it needs to be configured on corporate DNS for on-prem clients.

Sample Topology



Topology details:

- Two Avi GSLB sites - one in Azure Vnet1 (GSLB leader site) and other in Vnet4 (Avi GSLB active follower site).
- One on-prem DC which is connected to Azure VNets using express route/VPN gateway.
- Client machine that can be present on-prem or in Azure.
- Multiple VNets (Registration and Resolution) in Azure as part of the private DNS zone.
- Application (Application B) residing on-prem that must be accessible from the Azure VNets.
- Application (Application A) residing in Azure that should be reachable from on-prem clients and from clients in Azure (same VNet and other VNets as well).
- VMs hosted in Azure should have inter VNet and intra VNet communication.

Considerations

Avi Controller and GSLB

- It is not required to have Avi Controller/GSLB site in all VNets, locations.
- GSLB site can be present either on-prem or in Azure or at both places.
- One GSLB site/Avi Controller can take care of all GSLB functioning. In such a case, no further GSLB configuration would be possible until the site is back up. So, it is recommended to have at least two sites that are designated as the leader site and the active follower site for any GSLB configuration changes, if required. For complete information on GSLB sites, refer to Avi GSLB Site Configuration and Operations.

Clouds

Create different clouds on the Avi Controller to specify the network and location details for one cloud per VNet. Installation of Avi Controller in Azure and configuration of cloud is explained here.

Avi Service Engines

Avi Service Engines will be deployed in all VNets that are load balancing resources and applications. * DNS virtual service can be deployed in two or three VNets depending on the deployment size and traffic volume. Avi DNS virtual service is not required for all VNets. For topologies discussed in this document, Avi DNS virtual services are deployed in two locations. * You can have the application pools, Avi SEs running in the same VNet as that of the Controller.

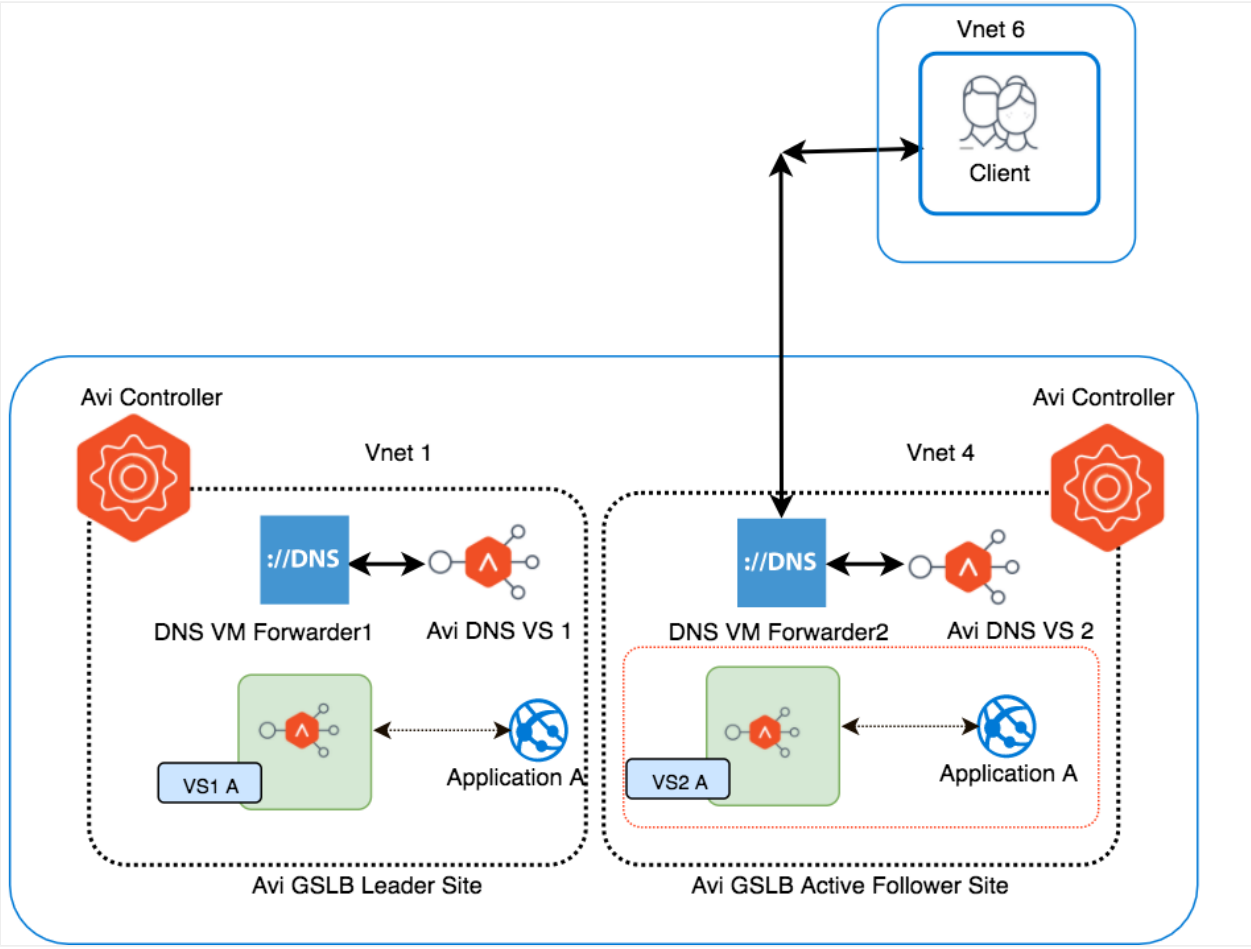
DNS

As explained in the topology, the DNS VM forwarder component conditionally forwards the traffic either to Avi DNS virtual service or to Azure DNS as explained above.

Request Flow

This section covers the request flows for the resolution of applications hosted in the following: * One VNet from other VNet * Azure VNets from on-prem * Virtual machines in different virtual networks

Resolution of applications hosted in one VNet from other VNet



FQDN Address Resolution

1. Client in West-US Vnet 6 sends HTTPS request to download the home page of Application A. Its FQDN (A.gslb.azure.com) needs to be mapped to an IP address not yet known to the client. As the DNS server configured for this VNet is ? DNS Forwarder IP?, the request will go to the DNS VM Forwarder for resolution.

2. DNS VM Forwarder, in turn, will forward the request based on a subdomain to Avi?s DNS (one of the two GSLB DNS instances, in this case to DNS-VS2), and eventually the IP for A.gslb.azure.com will be returned to the client.

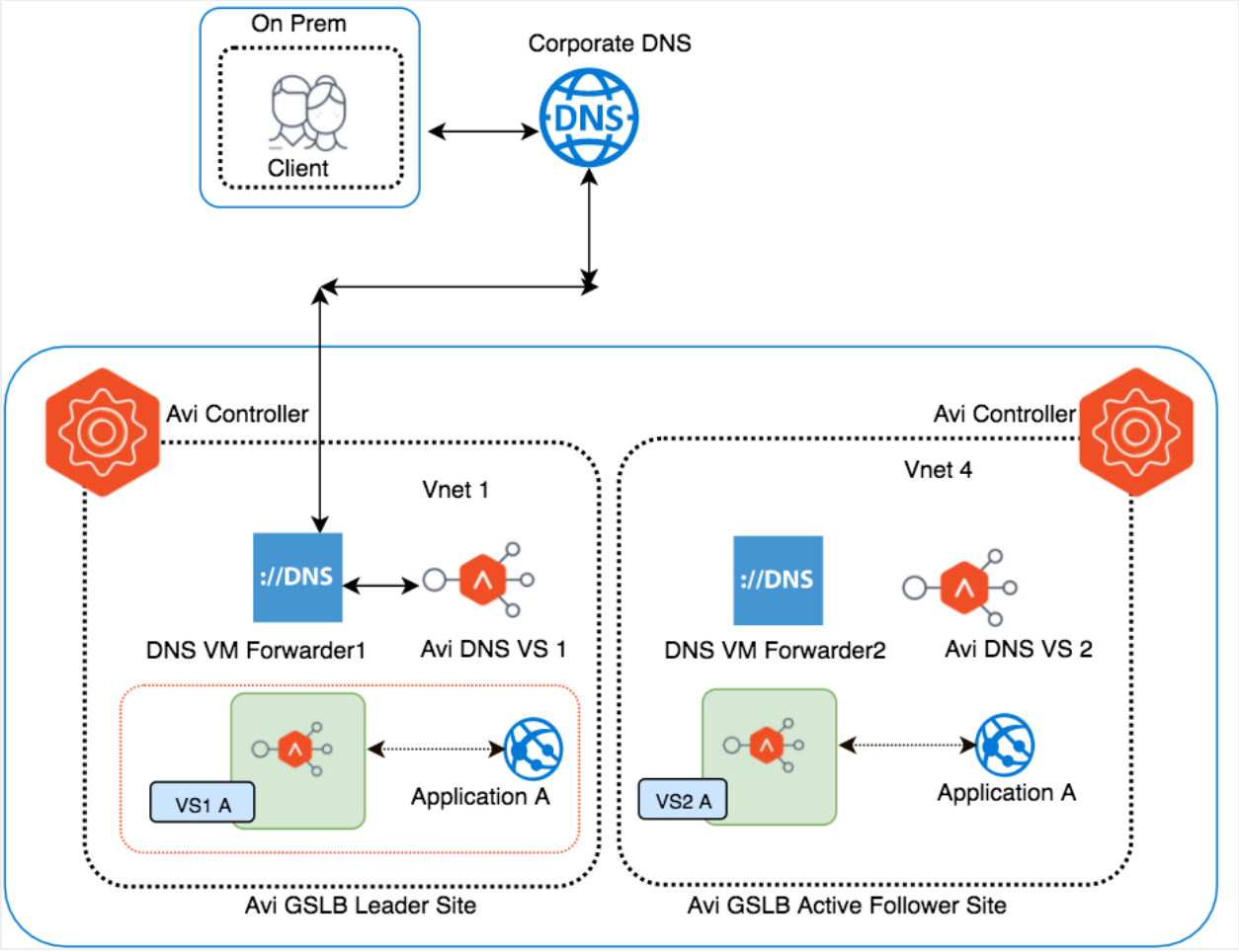
Application Traffic flows to Optimal Virtual Service

DNS-2 has two candidates for the optimal virtual service choice: VS1-A, VS2-A. It chooses VS2-A2 based on the load balancing algorithm, health, client location, etc. DNS-2 responds to the DNS query with the VIP of VS2-A, which eventually makes it to the original client. The client uses the VIP of VS2-A to send its HTTP request.

Local Load Balancing

Service Engines receive the request that has been directed to the VIP of VS2-A. It then load-balances it to one of VS2-A?s servers (app instances). VS2-A responds directly to the client.

Resolution of applications hosted in Azure VNets from on premises



FQDN Address Resolution

1. The client that is present on-prem wants to access Application A. The client sends an HTTPS request to download the home page of Application A. Its FQDN (A.gslb.azure.com) needs to be mapped to an IP address that is not yet known to the client.

2. As the DNS server configured for this subdomain on corporate DNS is *DNS Forwarder IP*, the request will go to DNS Forwarder VM for resolution. It will in turn forward the request to Avi?s DNS (one of the two GSLB DNS instances, in this case to DNS VS1), and eventually, the IP for A.azure.com will be returned to the client.

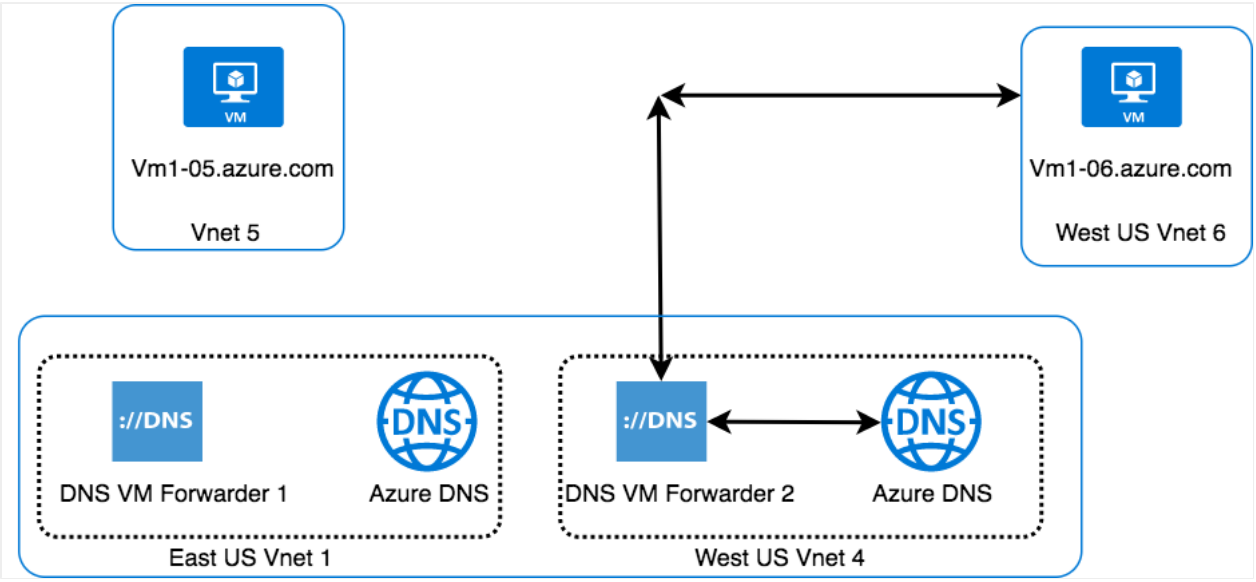
Application Traffic Flows to Optimal Virtual Service

DNS VS1 has two candidates for the optimal virtual service choice: VS1 A, VS2 A. It chooses VS1 A based on the load balancing algorithm, health, client location, etc. DNS VS1 responds to the DNS query with the VIP of VS1 A, which eventually makes it to the original client. The client uses the VIP of VS1 A to send its HTTP request.

Local Load Balancing

SEs receive the request that has been directed to the VIP of VS1 A. It then load-balances it to one of VS1 A?s two servers. VS1 A responds directly to the client.

Name Resolution between VMs in different Virtual Networks



1. VM1-06 present in West US Vnet 6 needs to communicate with VM1-05 present in Vnet 5 for ssh connection. The hostname of the VMs need to be mapped to an IP address not yet known to other VM.

2. As the DNS server configured for this VNet is *DNS Forwarder IP*, the request will go to DNS Forwarder VM for the resolution which in turn will forward the request to Azure private DNS (Register the VMs' names as explained in the previous section). Azure DNS will return the IP of VM1-05.

3. Vm1-06 will use the IP address of Vm1-05 for ssh connection.

Analytics

Avi Vantage includes built-in application analytics with enterprise-grade GSLB solution. With millions of data points collected in real time, the platform delivers network-DVR like capabilities and application analytics to help troubleshoot applications. This DNS analytics displayed over specific time intervals (last 15 minutes, hour, day, week etc.) provides detailed and aggregated information about DNS queries from clients, including FQDN, query-type, significant errors, and responses (IP-addresses, CNAME, SRV).

This also helps in checking the health status of the endpoints deployed across multiple locations in Azure DNS private zones as well as on-prem DCs. It also shows RTT, errors, user transactions for the endpoints to give you real-time insights about your network.