Infoblox

Deployment Guide

Best Practices and Architecture: vNIOS for Public Cloud

Table of Contents

Overview

Infoblox vNIOS is a virtual appliance designed for deployment as a Virtual Machine (VM) on public and private cloud platforms. Infoblox vNIOS is available for Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), as well as many private cloud platforms. vNIOS enables you to deploy robust, manageable, and cost effective Infoblox appliances in the public clouds.

Infoblox NIOS is the underlying software running on Infoblox appliances and provides core network services and a framework for integrating all the components of the modular Infoblox solution. It provides integrated, secure, and easy-to-manage DNS (Domain Name System), IPAM (IP address management) and other services.

Infoblox vNIOS for public cloud appliances can be joined to an existing on-premise or hybrid/multi cloud grid, or the entire grid can run in the cloud. The vNIOS appliance can be configured as a primary DNS server for your virtual networks. You can also use Infoblox Cloud Network Automation with vNIOS for public cloud to improve visibility of cloud resources and increase the flexibility of your cloud environment.

There are many considerations when creating or extending your network and Infoblox grid into a public cloud. This guide is not an exhaustive list, but provides some best practices and sample architectures for deploying vNIOS in Azure, AWS, and GCP.

Public Cloud Objects

In order to discuss best practices and architecture of vNIOS for public cloud platforms, it is important for an administrator to understand some common resources and terms that may apply to vNIOS deployments. The following are some of these common resources and terms:

- **Availability Set:** Availability sets in Azure ensure high availability of your VMs by distributing them across multiple physical servers, compute racks, and network switches.
- **Availability Zone:** Availability Zones are isolated locations within a region. Each region may contain multiple availability zones. In AWS and GCP, deploying vNIOS across different availability zones is a preferred way to achieve high availability.
- **Azure Resource Manager (ARM) Template:** ARM templates are JavaScript Object Notation (JSON) files that define resources and configurations for deployment in Azure. ARM templates allow you to create Infrastructure as Code.
- **AWS Direct Connect:** A direct, high speed connection from your on-premise network to AWS established through an AWS Partner.
- **Direct Peering:** This service establishes a direct connection between your on-premise network and Google's edge network. This connection works for the full suite of Google products, including GCP.
- **Express Route:** A direct, high speed connection from your on-premise network to Azure through a connectivity provider.
- **Load Balancer:** Public or Private load balancers balance traffic to pools of VMs from the internet or within virtual networks.
- **Marketplace:** Azure, AWS, and GCP all provide digital marketplaces that allow you to search for and deploy resources. Using the Azure Marketplace is one way to deploy vNIOS on that platform.
- **Network Security Group (NSG):** An NSG contains rules that allow or deny inbound or outbound traffic to AWS and Azure resources. These function as a basic firewall for your VMs.
- **Peering Connections:** A peering connection is a network connection between two AWS VPCs that allows traffic to be routed between them. In Azure, this is called VNet peering, which allows private

traffic between VNets, without using the internet, gateways, or encryption. In GCP, these connections are called VPC Network Peering, and can allow traffic between VPCs in different projects or even organizations.

- **Project:** A project in GCP is a container for everything you build. Resources within a project work together easily, but deliberate setup is required for resources to communicate between projects.
- **Resource Group:** A container for a logical grouping of resources in Azure. These can be used to divide production and non-production workloads or for granular Role Based Access Control (RBAC).
- **Region:** A region is a collection of datacenters or zones located in a one geographical area.
- **Virtual Private Cloud (VPC):** VPCs provide the networking layer for AWS and GCP. VPCs contain subnets, access gateways, routes, and other connectivity resources. AWS VPCs are regional resources, providing networking capabilities within a single region. GCP VPCs can span multiple regions.
- **VNet:** A virtual network in Azure used to set up communication between your VMs, on-premise networks, and the Internet. VNets define your private IP address space and can be divided into subnets.

Use Cases

Extending your Infoblox grid into Azure, AWS, or GCP with vNIOS appliances can provide solutions for many hybrid cloud infrastructure requirements and issues. The following are some of the common use cases:

DNS for Hybrid Cloud

A vNIOS appliance can be used as the primary DNS server in Azure VNets, and GCP / AWS VPCs. This allows you to extend your enterprise DNS and RPZ services into the public cloud. Clients running on these cloud platforms, attached to your VPCs and VNets, are able to use the same consolidated and secure DNS service as clients on-premise and in your private cloud environments. vNIOS appliances running the DNS service can be deployed in shared services or transit virtual networks and used for DNS resolution across other virtual networks via peering relationships. This is especially powerful when combined with the vDiscovery use case for automated creation of DNS records for your Azure, AWS, and GCP VMs.

DNS, IPAM, and Discovery for Cloud Resources

The Infoblox vDiscovery feature can be used for detecting and obtaining information about Tenants, VNETs / VPCs, Subnets, and Virtual Machines operating in your public cloud environments. Many organizations operate hybrid and multi-cloud environments that may contain many subscriptions and accounts. These environments tend to be very dynamic, with things such as VMs being created and terminated on a frequent basis. This makes it difficult to keep track of everything. With Infoblox vDiscovery, tasks can be configured to run automatically allowing your Infoblox vNIOS appliance to keep track of all cloud environments, storing this data in IPAM. Using vDiscovery in conjunction with the Cloud Network Automation (CNA) feature, you will gain enhanced visibility into your cloud environments, all within a ‘single pane of glass’.

DHCP Service for On-Premise Clients (AWS/GCP Only)

A vNIOS appliance running on AWS or GCP can provide DHCP service for your on-premise clients. This DHCP appliance can serve as your primary DHCP server or be configured as part of a failover pair with a NIOS DHCP server running on-premise for a hybrid, survivable solution. Two vNIOS appliances, each running in AWS or GCP could also be configured for DHCP failover for highly available, fault tolerant DHCP services. Using a vNIOS appliance running on AWS or GCP for DHCP requires using DHCP Relay or IP Helper on your router or layer 3 switch to send DHCP traffic from your on-premise network to your AWS or GCP VPC.

Reporting and Analytics (AWS/Azure Only)

Infoblox Reporting and Analytics automates the collection, analysis, and presentation of core network service data that assists you in planning and mitigating network outage risks so you can manage your networks more efficiently. You can quickly create custom security reports and dashboards to identify security issues, ensuring that your network is secure and available. You can easily meet audit requirements with pre-configured, customizable compliance reports or quickly and easily create your own. To keep your Infoblox Grid running smoothly, you can track and project utilization of the Grid and easily forecast when you will need to scale up. Deploying Reporting members in AWS or Azure allows you to migrate workloads from data center to the cloud and take advantage of the reliability and high availability of AWS and Azure deployments.

Fault Tolerance and Disaster Recovery

You can achieve Fault Tolerance and aid in Disaster Recovery of DDI services by deploying vNIOS appliances in public cloud environments. In case of failure in the Primary Datacenter (power outage, network outage, or other critical failure) an Infoblox vNIOS appliance enabled as a Grid Master Candidate (GMC) can be promoted to the Grid Master role so that Grid services can continue to operate. Deploying vNIOS appliances in multiple regions and across multiple public clouds can increase fault tolerance and survivability further. DNS services can also be redirected to servers operating in the public cloud, possibly without even requiring any manual intervention, helping to ensure the business can continue to operate. DHCP fault tolerance can be set up using Infoblox DHCP Failover configured between on-premise grid members and members running on AWS.

Maximum Availability

It is critical in a geographically distributed, hybrid cloud environment to ensure services and resources are available when and where they are needed. High availability of DDI services can be achieved by deploying vNIOS appliances in the public cloud using Availability Sets or Availability Zones. This will ensure availability despite planned and unplanned maintenance, taking advantage of uptime Service Level Agreements (SLA) offered by public cloud providers. You can ensure availability from all virtual networks by deploying vNIOS appliances into “shared service” or “transit” VPCs / VNets. Other virtual networks can be connected to these using peering connections.

API Survivability and Scalability

The Infoblox Cloud Platform (CP) appliance can provide survivability and scalability for API service. When deployed on a public cloud platform, the CP appliance can accept API calls from branch offices and edge locations, even if your primary datacenter and Infoblox Grid Master is offline. The CP will continue to accept API calls while it is unable to communicate with the Infoblox Grid Master due to network disruptions. By deploying multiple CP appliances, you can scale out API performance and improve access by deploying in regions close to your branch locations.

Best Practices

Infoblox provides a very robust solution for managing your network, helping to simplify and automate many tasks for DNS, DHCP, IPAM (DDI) and other services. Deploying or extending your Infoblox grid into a public cloud can provide additional benefits and also presents different challenges. The following practices can help you get the most out of your vNIOS for public cloud deployments.

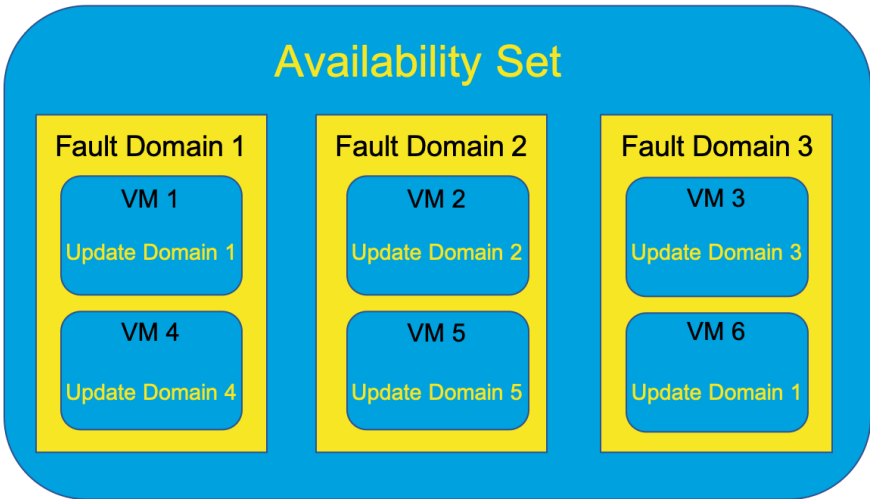
Maximize Availability

It is critical that core network services such as DNS, DHCP, and IPAM are constantly available when and where they are needed. For local/on-premise networks (both physical and virtual) the Infoblox High Availability (HA) feature provides redundancy and fault tolerance in an easy to manage and implement configuration using

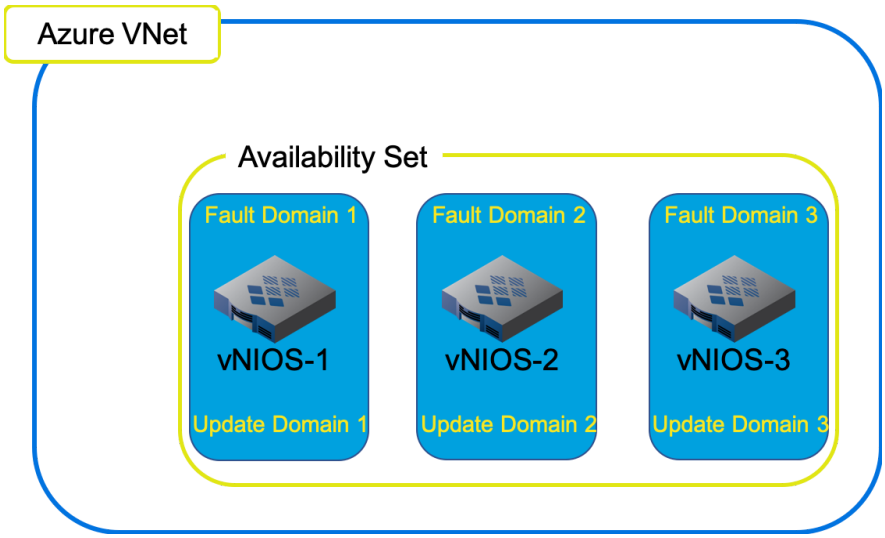
virtual router redundancy protocol (VRRP). However, this feature is not supported in vNIOS for public cloud deployments due to requirements of VRRP that are not supported for virtual networks in Azure, AWS, or GCP. You can still achieve highly available network services with vNIOS in public cloud by using availability features of public cloud platforms to ensure your Infoblox grid is able to consistently provide these crucial services.

Azure - Availability Sets

Microsoft Azure datacenters classify groups of hardware under two domains, update domains and fault domains. Update domains are groupings of hardware that may be patched or rebooted at the same time during maintenance periods. Fault domains describe hardware sharing a common power source and network switch. When VMs are deployed as part of an availability set, they are separated across 5 update domains and up to 3 fault domains by default.

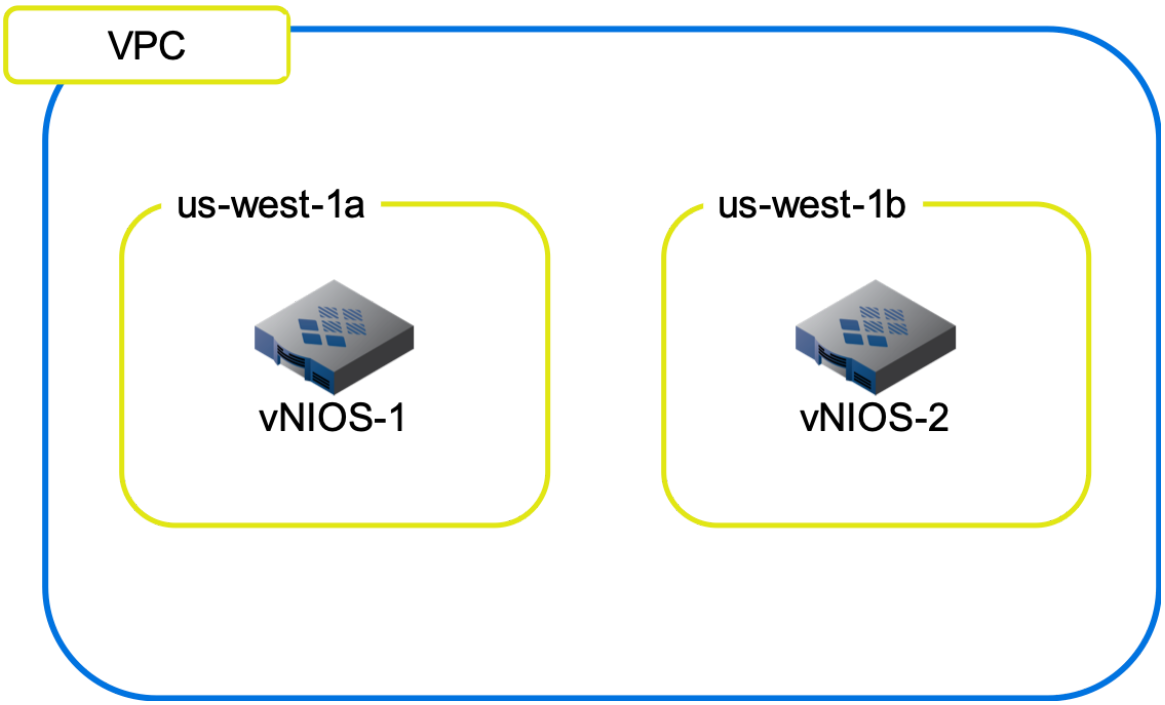


When you deploy at least two vNIOS for Azure VMs in an availability set, you ensure that at least one VM will remain available during planned or unplanned maintenance events. To deploy vNIOS appliances into availability sets, you will need to use Azure Resource Manager (ARM) templates as this option is not available for marketplace deployments. For more information, see the Infoblox Deployment Guide: Deploy vNIOS in Azure Using ARM Templates, at https://www.Infoblox.com.

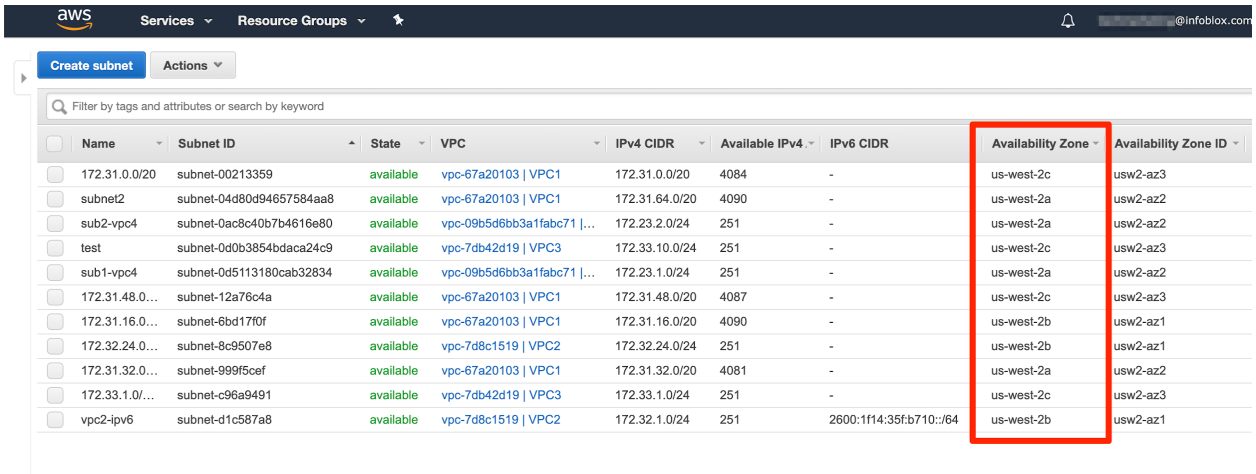


AWS and GCP - Availability Zones

Availability zones are isolated fault domains within a public cloud region. Availability zones often consist of separate datacenters. For both AWS and GCP, you can maximize availability of your vNIOS instances by deploying them across multiple availability zones.

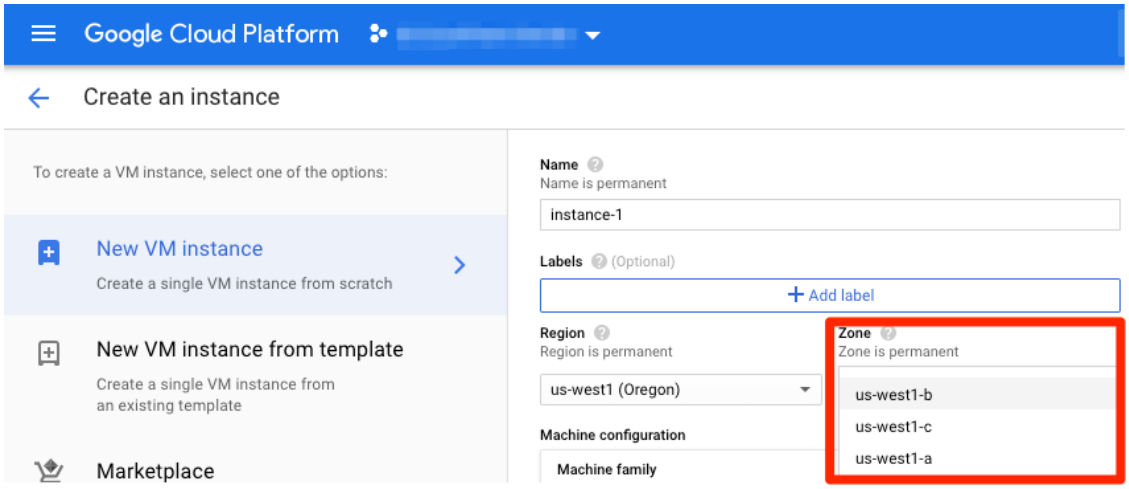


- In AWS, each subnet in a VPC is associated with an availability zone. When you create a new vNIOS instance, it is deployed in the availability zone associated with the subnets it is connected to. To maximize availability, you should deploy subnets in multiple availability zones across a region, and ensure vNIOS instances are deployed across these.



Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Availability Zone ID
172.31.0.0/20	subnet-00213359	available	vpc-67a20103 | VPC1	172.31.0.0/20	4084	-	us-west-2c	usw2-az3
subnet2	subnet-04d80d94657584aa8	available	vpc-67a20103 | VPC1	172.31.64.0/20	4090	-	us-west-2a	usw2-az2
sub2-vpc4	subnet-0ac8c40b7b4616e80	available	vpc-09b5d6bb3a1fabc71 |...	172.23.2.0/24	251	-	us-west-2a	usw2-az2
test	subnet-0d0b3854bdaca24c9	available	vpc-7db42d19 | VPC3	172.33.10.0/24	251	-	us-west-2c	usw2-az3
sub1-vpc4	subnet-0d5113180cab32834	available	vpc-09b5d6bb3a1fabc71 |...	172.23.1.0/24	251	-	us-west-2a	usw2-az2
172.31.48.0...	subnet-12a76c4a	available	vpc-67a20103 | VPC1	172.31.48.0/20	4087	-	us-west-2c	usw2-az3
172.31.16.0...	subnet-6bd17f0f	available	vpc-67a20103 | VPC1	172.31.16.0/20	4090	-	us-west-2b	usw2-az1
172.32.24.0...	subnet-8c9507e8	available	vpc-7d8c1519 | VPC2	172.32.24.0/24	251	-	us-west-2b	usw2-az1
172.31.32.0...	subnet-999f5cef	available	vpc-67a20103 | VPC1	172.31.32.0/20	4081	-	us-west-2a	usw2-az2
172.33.1.0/...	subnet-c96a9491	available	vpc-7db42d19 | VPC3	172.33.1.0/24	251	-	us-west-2c	usw2-az3
vpc2-ipv6	subnet-d1c587a8	available	vpc-7d8c1519 | VPC2	172.32.1.0/24	251	2600:1f14:35f:b710::/64	us-west-2b	usw2-az1

- In GCP, you can select the availability zone when deploying your vNIOS instance. It is not restricted by the subnets your instance is attached to as subnets are a regional object. For maximum availability, you should select different availability zones for each when deploying groups of vNIOS instances.



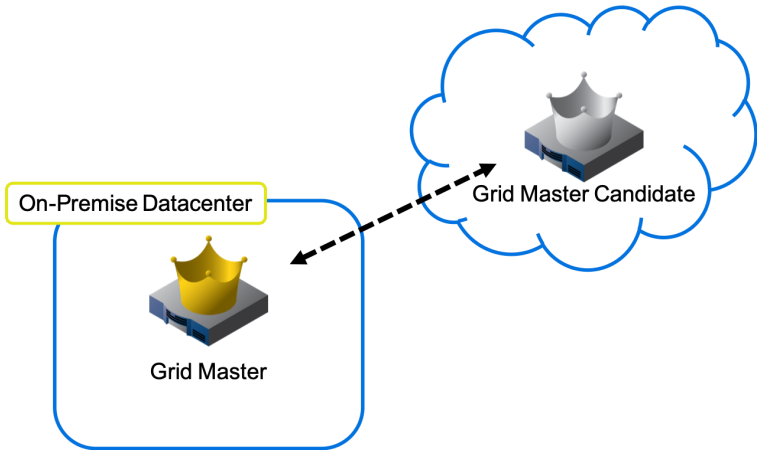
Survivability and Disaster Recovery

By deploying vNIOS into your hybrid and multi cloud environments, you can increase the survivability of your core network services.

Grid Master Candidate on Public Cloud

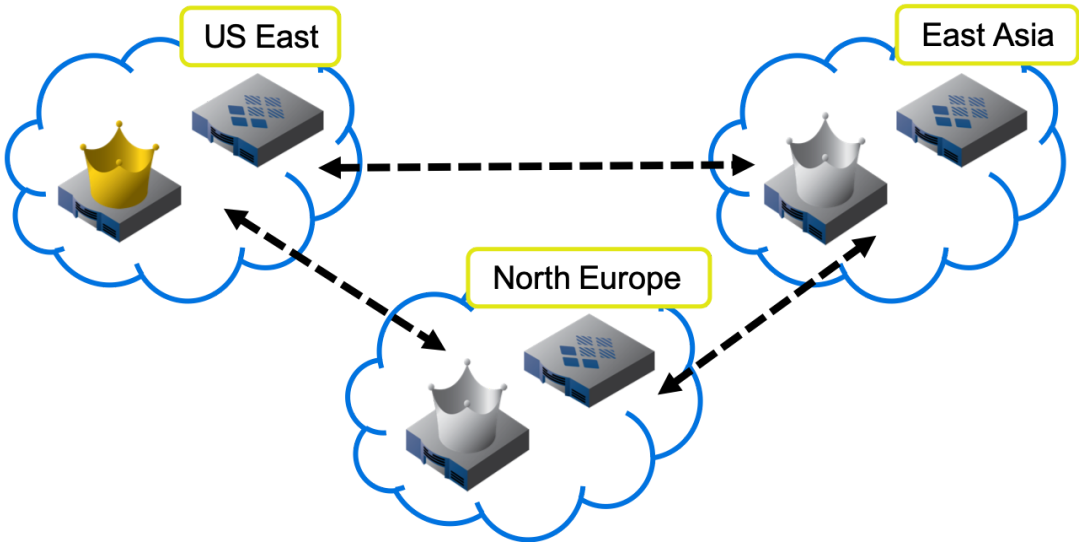
Deploying one or more grid master candidates into public cloud platforms greatly enhances the fault tolerance of your Infoblox grid. Each grid master candidate holds an identical copy of the grid master database. If the grid master service fails for any reason, including power outages, network disruptions, natural disasters, etc. a candidate can be promoted to the master role. By issuing a “promote to master” command, an administrator can force a grid master candidate to assume the grid master role. The new master then contacts all grid members to inform them of this change and resync the database as needed. This process takes only a few minutes, quickly restoring centralized monitoring and reporting.

By deploying grid master candidates into public cloud regions geographically dispersed from the organization’s primary datacenter, you can ensure survivability even in the case of large scale regional disasters.



Deployment Across Multiple Regions

The multiple regions available from public cloud providers allows you to distribute your vNIOS appliances and network services globally, providing fault tolerance in case of large scale outages or disasters. It can be useful to deploy vNIOS appliances providing network services, as well as grid master candidates across these multiple regions. For example, by deploying DNS servers in multiple regions and setting them up as name server groups in your grid, your DNS service can continue uninterrupted in case of outage in one of the regions.



Storage Considerations

Public cloud providers offer various options for the storage used for virtual machine disks. It is recommended that you use solid state drives (SSD) for vNIOS deployments on public cloud platforms when possible.

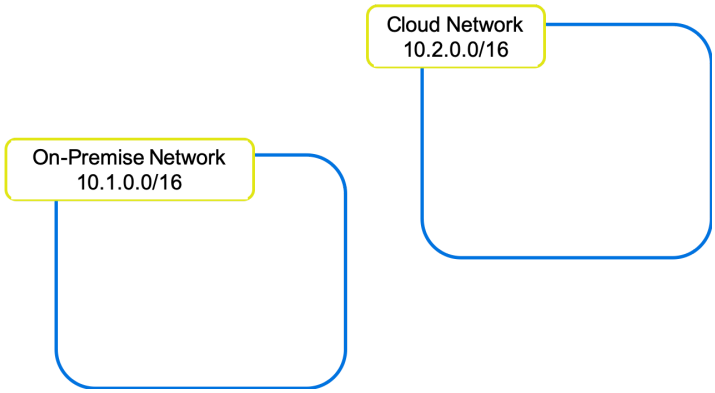
- **AWS:** AWS instance disks are stored as Elastic Block Store (EBS) volumes. There are 3 EBS types that can be selected for your boot disk. General Purpose SSD (gp2) is the base level for SSD and will work for many vNIOS deployments. Provisioned IOPS SSD (io1) support high levels of input and output and are recommended for vNIOS deployments in high volume environments. Magnetic (standard) EBS is not recommended for vNIOS deployments except in non-production environments.
- **Azure:** For Azure, the 2 tiers of storage account performance are Standard and Premium. Premium uses SSDs and is the required type in vNIOS for Azure deployments for disk storage. Standard uses magnetic disks and is required in vNIOS for Azure deployments for log storage. It is also important to note that there are multiple storage replication choices in Azure. vNIOS for Azure currently requires Locally-redundant storage (LRS).
- **GCP:** For GCP, select Standard Persistent Disks for the storage type. This is the only GCP disk type currently supported for vNIOS deployments.

Network Design

Expanding your network and core network services such as DDI provided by the Infoblox grid into a public cloud presents challenges for design, implementation, and maintenance/monitoring. The design principles presented in this section can help ensure your Infoblox DDI services are optimized across your hybrid cloud network.

IP Address Space

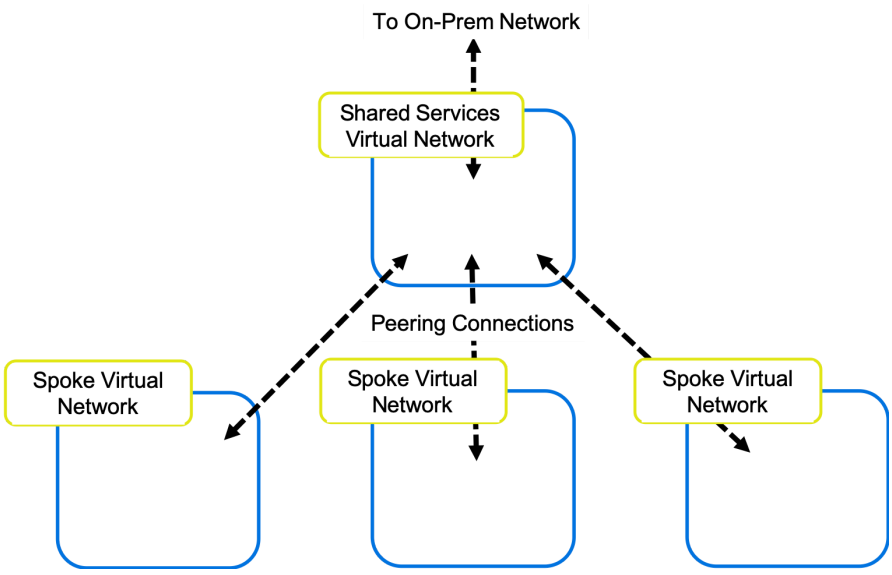
Ideally, you should create your cloud virtual networks using IP address space that does not overlap with the address space you use on premise. For example, if your on premise network uses the 10.1.0.0/16 address space, your cloud networks could use 10.2.0.0/16. This will allow for the simplest and most consistent IP address management (IPAM).



If you are unable to avoid overlapping address space, Infoblox IPAM can still be used to manage these spaces using different network views. This topic is discussed in the vDiscovery section of this document.

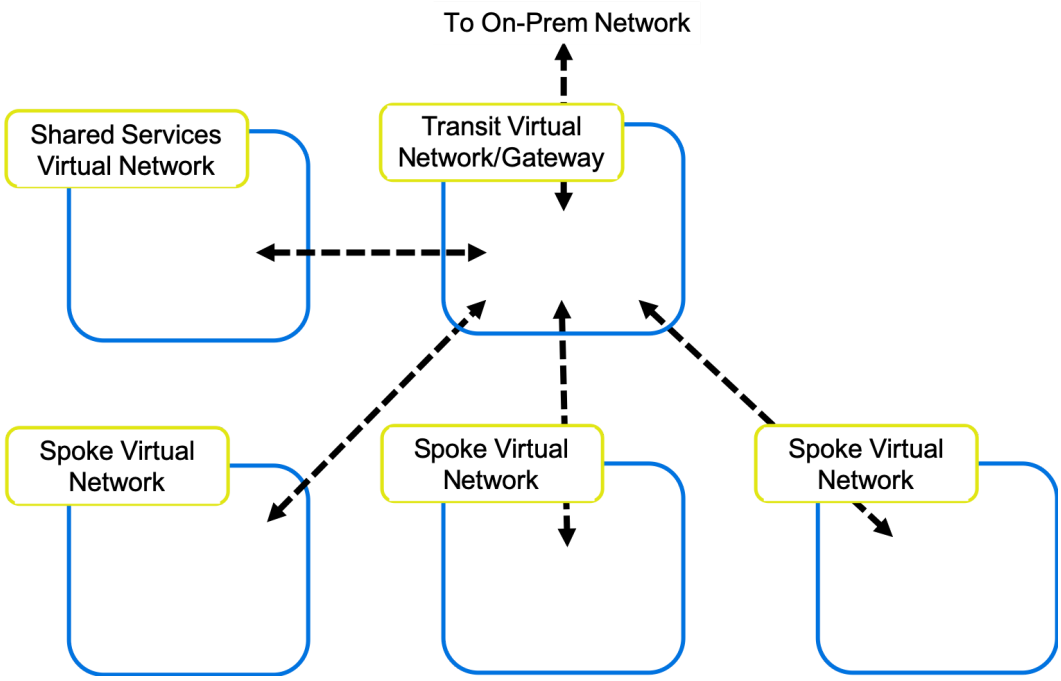
Hub and Spoke Design

A hub and spoke design for your cloud networks allows critical services to be accessed from all networks where they are required. It can reduce costs by centralizing these core services into a “shared services” VNet or VPC. The hub and spoke design also facilitates control of traffic flow since all traffic is routed through the shared services/transit virtual network. There are two basic designs for a public cloud hub and spoke network.



In the original hub and spoke cloud network, core services such as DDI are placed in a shared services (hub) virtual network. All other virtual networks (spokes) are connected to the shared services network via peering connections. Major public cloud providers such as AWS, Azure, and GCP support peering virtual networks

across availability zones and regions, allowing this network design to span globally. The shared services virtual network also has a connection to the on-premise network. This connection is used for traffic from all virtual networks.



The second design separates core services from traffic flow. In this design, virtual networks are connected to a transit virtual network or transit gateway (for AWS). All routing between on-premise and cloud networks is done through this transit connection. Shared services are placed in their own virtual network which is also connected to the transit virtual network.

Connections to On-premise Network

There are two common methods for connecting your on-premise network to your public cloud networks, site-to-site virtual private networks (VPN) or direct connection solutions. The Infoblox grid master and grid members can use either connection type to communicate with each other or provide network services. You must ensure network security groups and firewalls between your on-premise and public cloud networks allow traffic required for grid communication. A list of ports and protocols used by NIOS can be found in the administrator's guide, available at https://docs.infoblox.com.

Major public cloud providers such as AWS, Azure, and GCP offer both VPN and direct connect solutions. A short description of direct connect solutions from each provider can be found in the overview section of this document. Factors to consider when deciding between these solutions are cost, bandwidth, speed, and availability.

vNIOS Appliance Placement

It is common to deploy vNIOS for public cloud appliances in the shared services virtual network. From there, they can provide DNS and IPAM services across your entire hub and spoke network. This method is suitable for both hub and spoke designs shown above. Depending on your use case for Infoblox in the public cloud, you will want to deploy vNIOS appliances across virtual networks in multiple regions as well. See the deployment scenarios section of this document for placement recommendations for these various use cases.

Appliance Types

Infoblox offers many models of virtual NIOS appliances on major public cloud platforms. Which model to use for each appliance depends on factors such as use case, grid size, expected traffic, and role of the appliance. You can find lists of available models for each public cloud provider as well as recommended virtual hardware for each model in the appliance documentation available at https://docs.infoblox.com.

Infoblox offers two types of appliances for deployment on public cloud platforms, Trinzic Enterprise appliances and Cloud Platform appliances. These appliance types are each suitable for different use cases.

Trinzic Enterprise (TE) Appliance

This is the standard vNIOS appliance. It is suitable for many roles within the grid and comes in many sizes suited for varying use. Some features of the TE appliance are:

- Role: Grid Master, Grid Master Candidate, Grid Member
- Can be deployed on-premise as physical hardware or virtual appliance and in the cloud as a virtual appliance.
- Provides DNS, DHCP, and IPAM (DDI) services.
- Provides Cloud Network Automation (CNA) with addition of CNA license.

Cloud Platform (CP) Appliance

The CP appliance provides API services in distributed datacenters and cloud environments. Using a CP appliance, you can send API calls directly to this appliance instead of all calls going to the grid master. The CP appliance continues to provide API services even if communication with the grid master is lost.

- Role: Grid Member
- Can be deployed in public or private clouds as a virtual appliance.
- Provides API services independent of the grid master. Used for survivability and scalability of API services.
- Provides DNS, DHCP, and IPAM (DDI) services.
- Continues to provide services even when communication is disrupted to the grid master.

Cloud Network Automation

The Cloud Network Automation (CNA) license provides many benefits for integrating your Infoblox grid with public and private cloud environments.

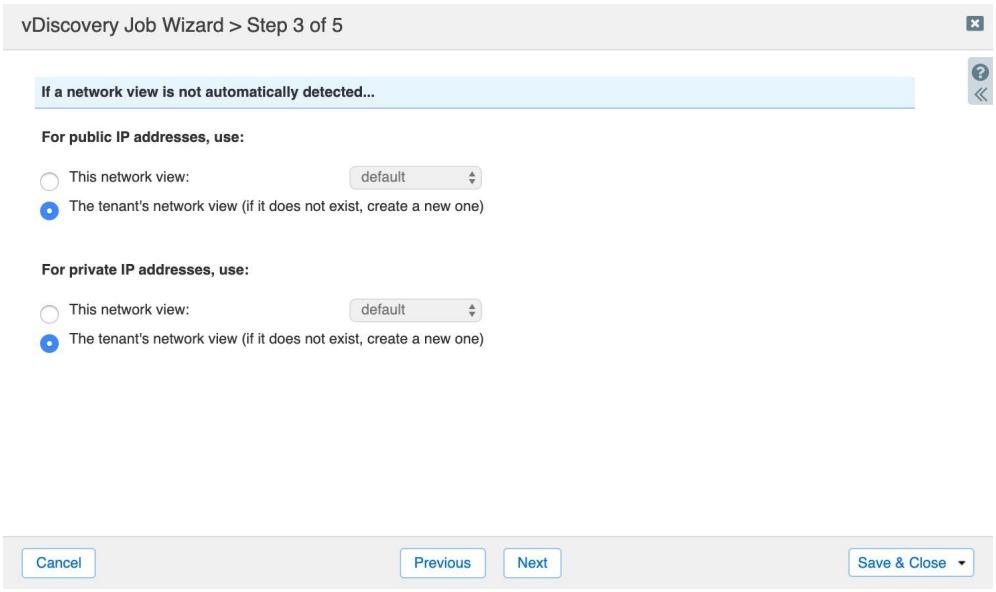
- Adds the Cloud tab in Grid Manager. This tab contains additional tabs for viewing cloud tenants, network, VMs, and cloud appliances.
- Enables Route 53 sync and AWS API proxy features. These add additional functionality for DNS and IPAM services when working with AWS.
- Adds the ability to automatically create DNS records for VMs as part of the vDiscovery process.
- Adds cloud specific dashboard widgets as well as cloud reports.

vDiscovery

Infoblox vDiscovery provides enhanced visibility of your resources in public and private clouds. Using vDiscovery, you can collect data on your tenants, VPCs, subnets, and VMs. The CNA license is not required for vDiscovery, but it greatly enhances it by allowing you to automatically create DNS records for discovered VMs

and adding additional data views through the cloud tab. Without the CNA licence, you can still view cloud networks found by vDiscovery in the IPAM tab. Some considerations when setting up vDiscovery include:

- To run vDiscovery for public cloud resources, the member running the vDiscovery job must be able to resolve public cloud API endpoints, such as ec2.us-west-2.amazonaws.com. Enabling the DNS Resolver in grid properties is the quickest way to ensure resolution is possible.
- The most common reason for vDIscovery to fail is network or IP address conflicts. This occurs when there are multiple networks using the same IP ranges and is common in multi-cloud environments. To avoid these conflicts and manage IPAM data for these networks, set up vDiscovery to create and use the tenant's network view.



- **AWS:** Each vDiscovery job will discover resources for a single region based on the endpoint provided when setting up the job. To discover resources across multiple regions, set up vDiscovery jobs for each.

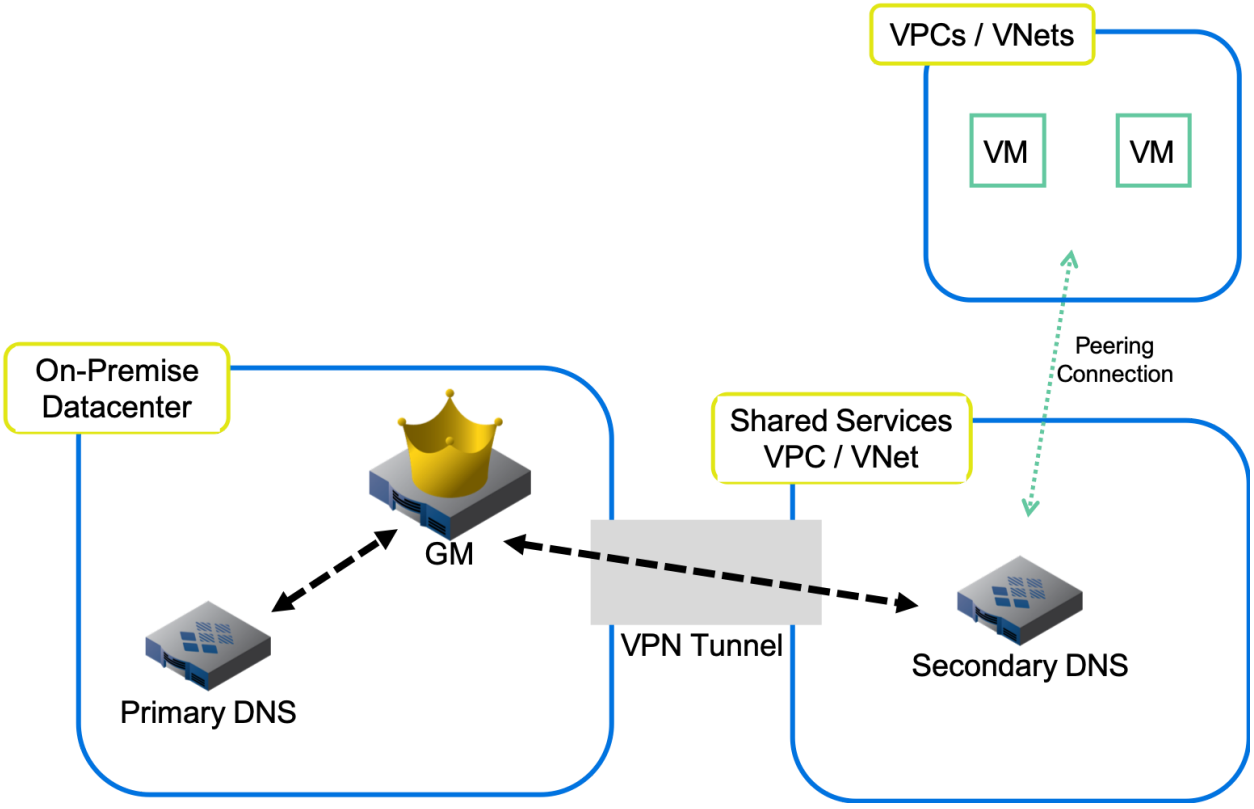
  AWS allows you to create a subnet in your VPC that uses the same CIDR prefix and mask as for the host VPC, for example a VPC with CIDR 10.1.0.0/16 could contain a single subnet with CIDR 10.1.0.0/16. NIOS does not allow subnets in an AWS VPC with the same prefix and mask, and will not discover these resources.
- **GCP:** vDiscovery will only find resources for a single project. To conduct discovery for resources in multiple projects, configure a job for each.
- **Azure:** vDiscovery for Azure can discover resources across multiple subscriptions. Ensure the app registration you use for vDiscovery has reader permissions on all subscriptions you want to enable this for. vDiscovery can also be limited to specific resource groups in Azure by only setting permissions at that level.

Deployment Scenarios

The deployment scenarios presented in this section are outlines for architecting solutions that satisfy many of the use cases for Infoblox hybrid and public cloud deployments. These scenarios do not necessarily show every component needed for the solution; each public cloud provider has unique requirements for network setup, etc. Quantities, models, and locations of NIOS or vNIOS appliances should be adjusted based on volume of traffic, availability needs, and fault tolerance needs. Combining concepts from multiple scenarios is also possible. These scenarios are not an exhaustive list of possible deployment architectures.

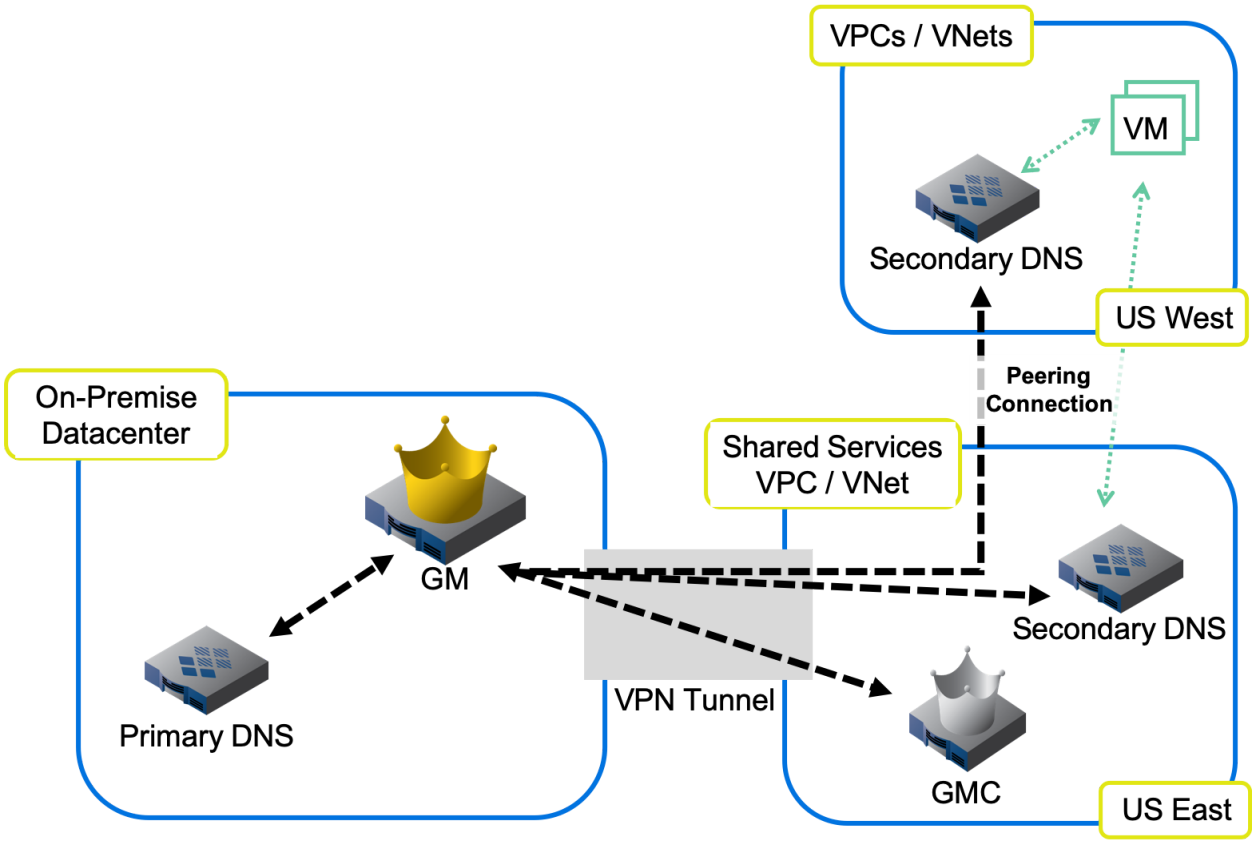
1. Hybrid Cloud - DNS and Discovery

- Grid Master (GM) on-premise, managing all grid members
- Primary DNS server on-premise, serving DNS for on-premise clients
- Secondary DNS server on public cloud in shared service VPC, serving DNS for public cloud client VMs
- Grid members running on public cloud can be deployed in availability sets or multiple availability zones for maximum availability
- vDiscovery from GM for visibility of public cloud resources



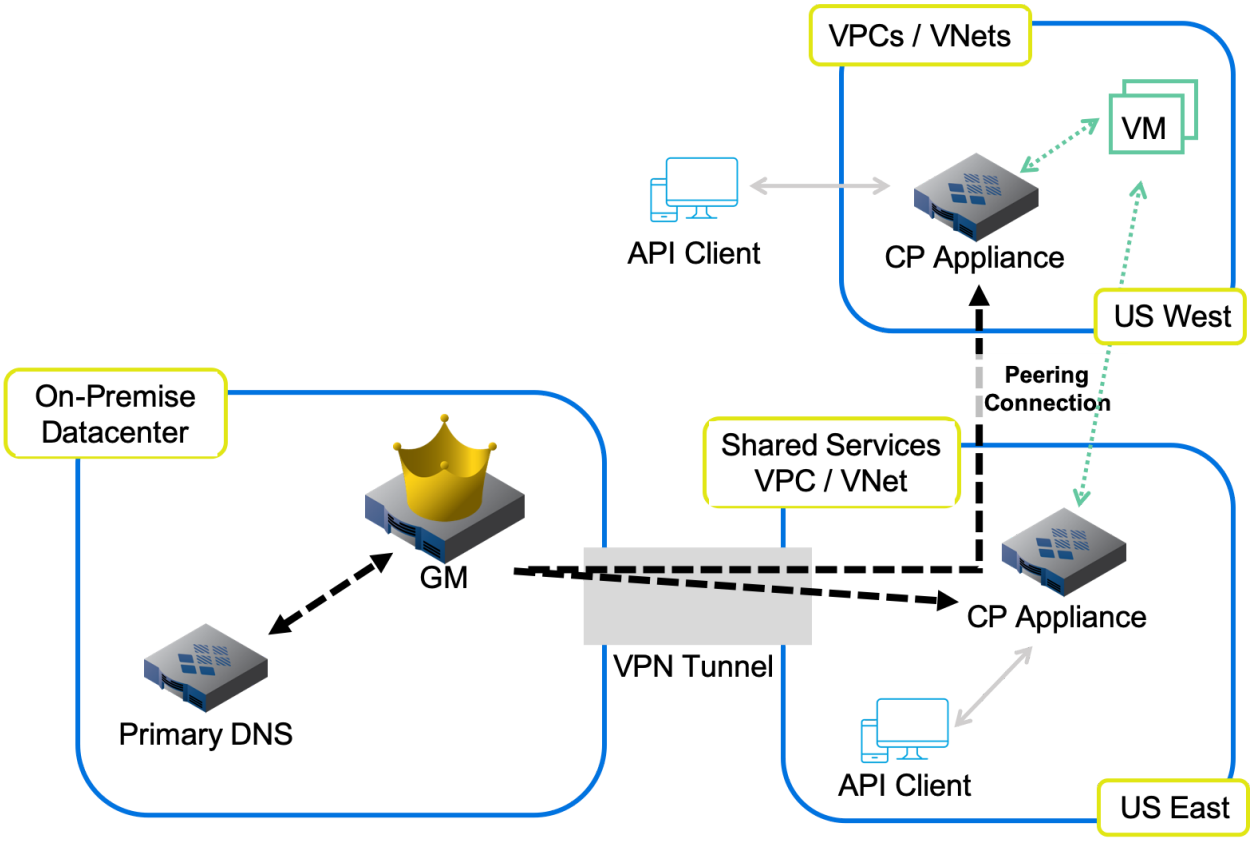
2. Hybrid Cloud - Fault Tolerance/Disaster Recovery, DNS, and Discovery

- Grid Master (GM) on-premise, managing all grid members
- Grid Master Candidate (GMC) deployed as vNIOS on public cloud in shared service VPC
- Primary NIOS DNS server on-premise, serving DNS for on-premise clients
- Secondary vNIOS DNS server on public cloud in shared service VPC, serving DNS for public cloud client VMs
- Additional vNIOS TE or CP appliance deployed for DNS in different region for fault tolerance/disaster recovery
- Grid members running on public cloud can be deployed in availability sets or multiple availability zones for maximum availability
- vDiscovery from GM for visibility of public cloud resources



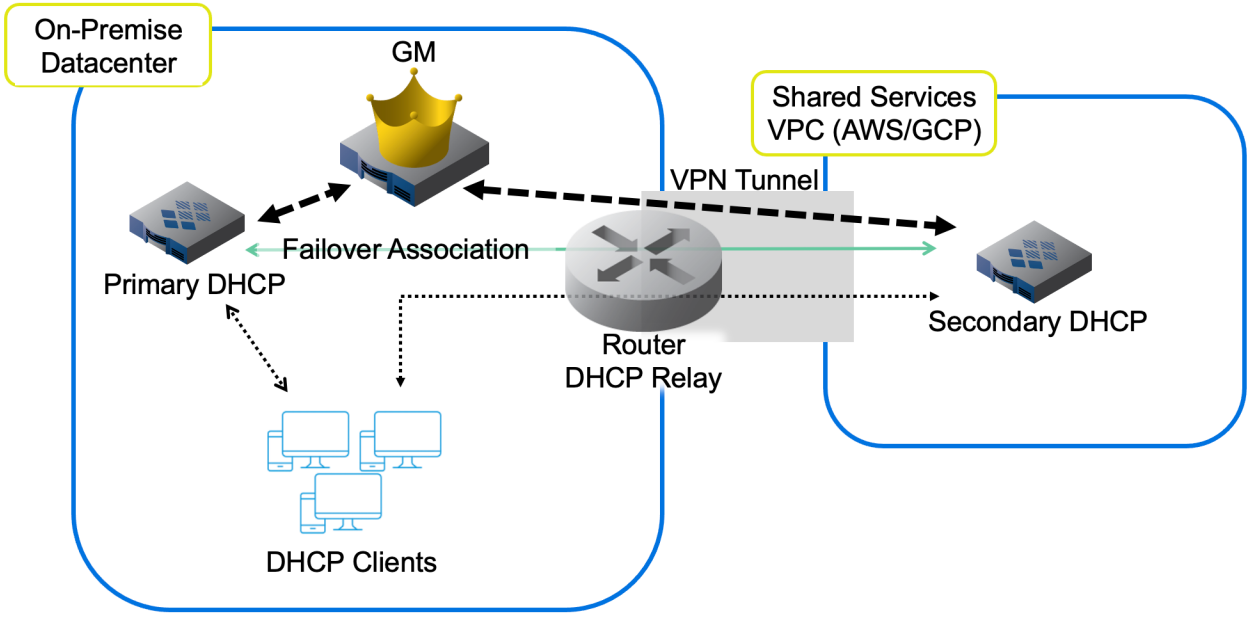
3. Hybrid Cloud - CP Appliances for API Survivability, DNS, and Discovery

- Grid Master (GM) on-premise, managing all grid members
- Primary NIOS DNS server on-premise, serving DNS for on-premise clients
- Cloud Platform (CP) appliances deployed in multiple public cloud regions, serving DNS, IPAM, and API queries for clients outside of primary datacenter
- vDiscovery from GM or CP members for visibility of public cloud resources



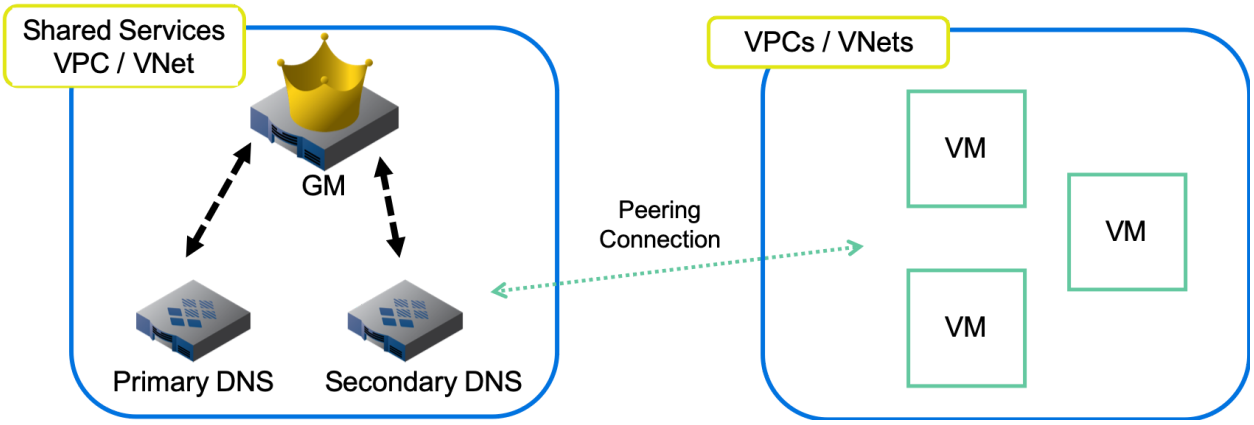
4. Hybrid Cloud - DHCP Failover (AWS/GCP Only)

- Grid Master (GM) on-premise, managing all grid members
- Primary NIOS DHCP server on-premise, serving DHCP for on-premise clients
- Secondary vNIOS DHCP server on AWS in shared service VPC, DHCP Failover Association configured with primary server
- On-premise router configured for DHCP Relay or IP Helper to allow DHCP traffic to AWS vNIOS appliance



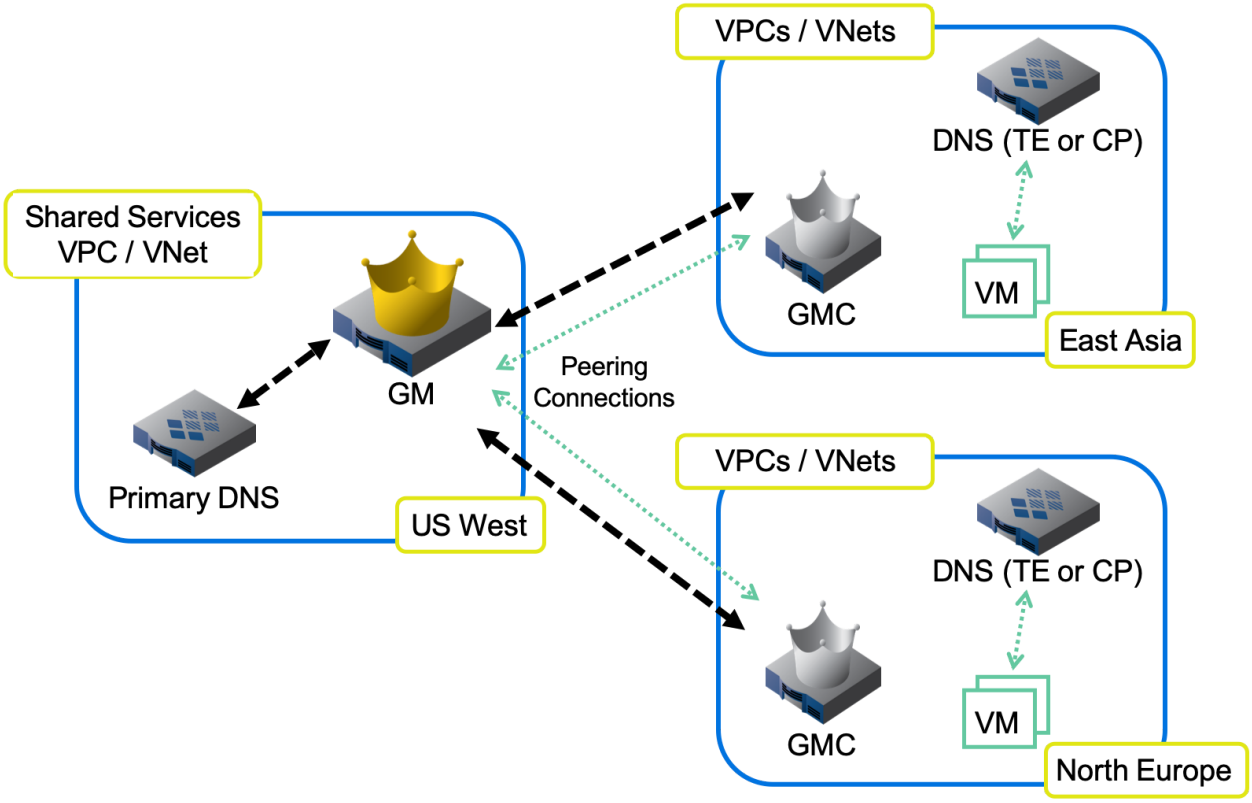
5. Full Public Cloud - DNS and Discovery

- Grid Master (GM) running as vNIOS on public cloud, in shared services VPC, managing all grid members
- Primary DNS server on public cloud, serving DNS for all clients
- Secondary DNS server on public cloud, serving DNS for all clients
- Grid members running on public cloud can be deployed in availability sets or multiple availability zones for maximum availability
- vDiscovery from GM for visibility of public cloud resources



6. Full Public Cloud - Fault Tolerance/Disaster Recovery, DNS, and Discovery

- Grid Master (GM) running as vNIOS on public cloud, in shared services VPC, managing all grid members
- Grid Master Candidates (GMC) deployed as vNIOS in different regions for fault tolerance/disaster recovery
- Primary NIOS DNS server on public cloud, in shared services VPC, serving DNS for all clients
- Additional vNIOS TE or CP appliances deployed for DNS in different regions to serve clients and provide fault tolerance/disaster recovery
- Additional CP appliances in different regions can also provide API survivability and scale
- Grid members running on public cloud can be deployed in availability sets or multiple availability zones for maximum availability
- vDiscovery from GM or CP members for visibility of public cloud resources



Conclusion

Deploying Infoblox vNIOS on AWS, Azure, or GCP can provide solutions for many of your hybrid cloud requirements, including DNS services, IPAM, DHCP services, resource visibility/management, automation via API, and many more. Infoblox offers many models for both TE and CP appliances on public cloud platforms, allowing you to deploy the right device for each solution. Integrating your Infoblox grid with public cloud features such as availability sets, availability zones, and regions provides additional solutions for high availability, survivability, scalability, and disaster recovery.

Additional Information

- For Deployment Guides and other resources for specific Infoblox solutions, or deployments on specific cloud platforms, visit https://www.infoblox.com/resources/.
- For official documentation on Infoblox NIOS and vNIOS appliances for specific cloud platforms, visit https://docs.infoblox.com/.
- For blogs and help from Infoblox Experts, visit the Infoblox community at https://community.infoblox.com/.

Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com