DEPLOYMENT GUIDE

INFOBLOX NIOS-X AS A SERVICE FOR GOOGLE'S CLOUD WAN

TABLE OF CONTENT

INTRODUCTION 3
- Google's Cloud WAN 3
- Prerequisites 3
  - Infoblox 4
  - Google Cloud 4

WORKFLOW 5

CONFIGURATION 6
- Google Cloud 6
  - Create a Cloud VPN Gateway 6
- Infoblox Portal 7
  - Create a NIOS-X as a Service Deployment 7
- Google Cloud 13
  - Create a Cloud VPN Tunnel 13

VERIFY CONNECTIVITY 17

TROUBLESHOOTING NIOS-X AS A SERVICE 18

NEXT STEPS 19

CONCLUSION 19

CONTACT AND SUPPORT 19
- Phone Support 19
- Online Support 19

INTRODUCTION

Infoblox Universal DDI™ Product Suite integrates DNS, DHCP and IP address management (IPAM) into a unified solution, providing centralized configuration and control across hybrid and multi-cloud environments. NIOS-X is an integral component of Universal DDI that delivers enterprise-grade DNS and DHCP services. This exclusive integration enables organizations to efficiently deploy market-leading critical network services while employing Google's global private network for unmatched performance, reliability and scale.

GOOGLE'S CLOUD WAN

Google's Cloud WAN is a cloud-native connectivity solution for global enterprises to connect their on-site locations, clouds and users through Google Cloud's premium tier infrastructure, replacing traditional telco-managed multiprotocol label switching (MPLS) and complex colocation infrastructure. It offers organizations three key advantages:

- **Premium Global Network:** Google's Cloud WAN leverages Google Cloud's premium tier network to provide global reach with industry-leading performance. This delivers consistently low latency across regions and ensures high reliability for mission-critical applications. The enterprise-grade network infrastructure eliminates the traditional trade-off between performance and cost that organizations face with MPLS solutions. Cross-Cloud Interconnect lets you connect any public cloud with Google Cloud through a secure, high-performance network, allowing organizations to run applications on multiple clouds, simplify software-as-a-service (SaaS) networking in a multi-cloud environment and migrate workloads from one cloud to another.
- **Integration of Best-of-Breed Services:** The connectivity solution supports best-of-breed networking and security services from Google and partner ecosystems. Global enterprises benefit from a tightly integrated third-party Google ecosystem offerings that includes DNS, DHCP and IP address management (DDI), Secure Access Service Edge (SASE) and SD-WAN capabilities. This reduces the complexity of integrating multiple vendor offerings while simultaneously freeing customers from infrastructure deployment through cloud-delivered services.
- **Significant Cost Optimization:** Google's Cloud WAN provides up to 40 percent savings in total cost of ownership (TCO) over a customer-managed WAN solution. They can realize additional savings by replacing on-premises infrastructure (hardware, virtualization software) with cloud services such as Infoblox NIOS-X as a Service for cloud-delivered DNS and DHCP services. *Architecture includes SD-WAN and third-party firewalls, and compares a customer-managed WAN using multi-site colocation facilities to a WAN managed and hosted by Google Cloud*.

This document is intended to guide network administrators through the first-time deployment of Infoblox NIOS-X as a Service for use with Google's Cloud WAN. There are some pre-requisites before you deploy this solution.

PREREQUISITES

Infoblox

These are the required steps on the Infoblox side before you are ready to deploy NIOS-X as a Service in Google's Cloud WAN setup.

Step 1: Active Infoblox Universal DDI Subscription

An active subscription for Universal DDI with an account on Infoblox Portal. If you don't currently have an active subscription, you can obtain one via the Google Cloud Marketplace using the Universal DDI private offer.

Step 2: Access to the Infoblox Portal

1. **Log In:** Access the Universal DDI platform using your credentials.
2. **Dashboard:** Familiarize yourself with the dashboard, which provides an overview of your network status and key metrics.

Step 3: Initial Setup and DDI Configuration

1. **Network Setup:** Configure your network settings, including IP ranges and DNS settings.
2. **Security Policies:** Set up security policies to protect against DNS threats.

Step 4: Deployment

1. **Deploy Services:** Deploy the necessary DNS and DHCP services across your network.
2. **Monitor:** Use the monitoring tools to keep track of network performance and security.

Step 5: Management

1. **Manage IP Addresses:** Utilize the IPAM tools to manage and allocate IP addresses efficiently.
2. **Update Policies:** Regularly update your security policies to adapt to new threats.

This guide aims to help you get started with Universal DDI. If you need more detailed instructions, the Infoblox documentation, *Getting Started with Universal DDI*, is a great resource.

Google Cloud

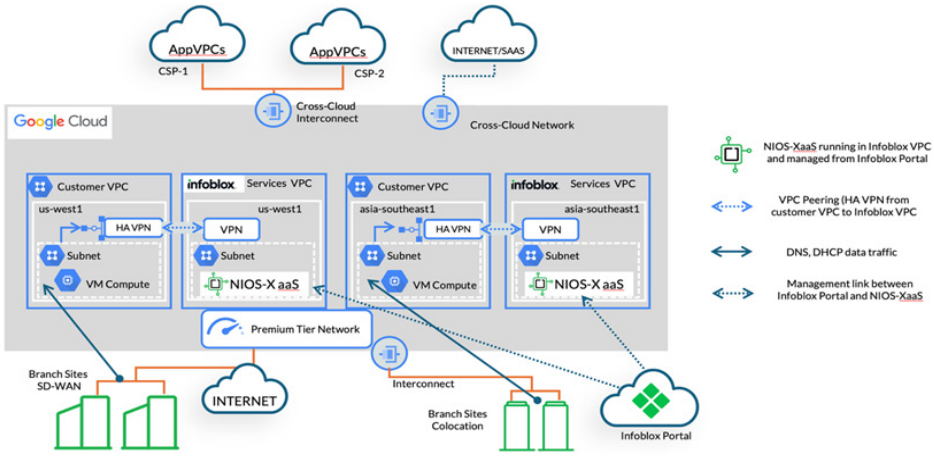
The deployment guide assumes that you have an account in Google Cloud and you have connected your on-premises sites to the nearest Google Cloud Point of Presence (PoP) location. Please review the *Choosing a Network Connectivity product* guide for more information on the best way to connect into Google Cloud regions.

The Infoblox NIOS-X as a Service integration with Google's Cloud WAN allows for businesses to simplify, secure and scale their networks. This integration allows for the provisioning of the critical network services directly to branch sites and cloud workloads. Infoblox-managed highly available services, such as DNS, DNS Security, NTP and DHCP, can be provisioned quickly in just a few steps. This allows for network and cloud operation teams to move rapidly and scale their deployments to meet modern business needs.

This architecture outlines the deployment of NIOS-X as a Service integrated with Google's Cloud WAN to deliver secure, scalable and centrally managed DDI services across distributed enterprise environments. The architecture consists of the following key components:

- **Google Cloud Virtual Private Cloud (VPC):** A dedicated network within Google Cloud that provides secure and isolated cloud resources.
- **Cloud VPN Gateway:** A virtual network service that enables you to securely connect your on-premises network or another cloud provider's network to your Google Cloud VPC via IPsec VPN tunnels.
- **Infoblox NIOS-X:** A robust DNS and DHCP protocol server deployed on-premises or in a hybrid cloud model managed through Infoblox Portal.
- **HA VPN:** A highly available and redundant VPN connection ensuring secure communication between Google Cloud and Infoblox NIOS-X.

The following diagram depicts the network architecture showing the deployment of NIOS-X as a Service with Google's Cloud WAN:



A Cloud VPN Gateway is provisioned within the Google Cloud environment. This gateway acts as the secure ingress point for traffic going to the Infoblox services from the customer's VPC. Within the Infoblox Portal, a new service deployment is configured. The deployment steps include:

- Assignment of a Service IP to listen for DNS and DHCP traffic from the clients
- Configuration of Border Gateway Protocol (BGP) routing with the cloud router in the customer VPC

To ensure fault tolerance, two **IPsec VPN** tunnels (primary and secondary) are established from the Cloud VPN Gateway to the Infoblox VPN Gateway. **BGP session** is established over these tunnels to enable dynamic route advertisement between the customer VPC and Infoblox VPC. Once the network and routing configurations are complete, **DNS and DHCP services** are available to clients across sites connected to the customer VPC. All DNS and DHCP services are centrally managed through the Infoblox Portal, ensuring unified visibility and control.

WORKFLOW

1. Google Cloud:
   a. Designate an existing VPC or create a VPC to connect with NIOS-X as a Service.
   b. Create a Cloud VPN gateway.
   c. Acquire IPs of the VPN Gateway's interfaces.
2. Infoblox Portal:
   a. Create a Google Cloud Service Deployment.
   b. Create a pre-shared key (PSK) for use with the Google Cloud VPN and NIOS-X as a Service.
   c. Acquire an Identity string.
3. Google Cloud:
   a. Create a VPN Tunnel.
4. Verify connectivity.

CONFIGURATION

GOOGLE CLOUD

Create a Cloud VPN Gateway

Before configuring the NIOS-X as a Service connection in the portal, a Cloud VPN Gateway is required. Perform the following steps to configure a Cloud VPN Gateway:

1. Navigate to the VPN page in the Google Cloud interface by searching for VPN and clicking the **VPN** search result.

2. Click the **CLOUD VPN GATEWAYS** tab.

3. Click **CREATE VPN GATEWAY** to begin creating a VPN gateway.

4. Input a **VPN gateway name**.

5. Select the appropriate **Network** for the VPN gateway.

6. Select the preferred **Region** for the VPN gateway.

7. Keep all other settings as their defaults and click **CREATE**.

8. Once the Cloud VPN gateway has been created navigate back to the **CLOUD VPN GATEWAYS** tab.

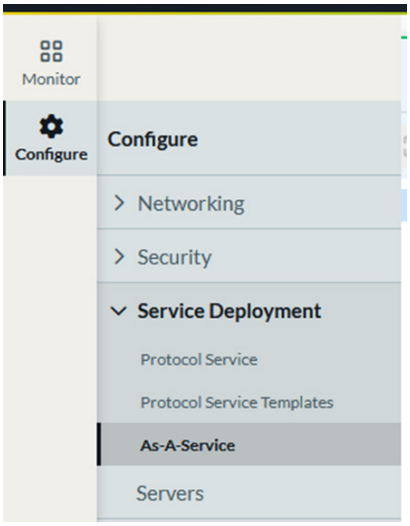
9. Locate the newly created VPN gateway and copy the IP addresses of both **Interface 0** and **Interface 1**. Save these IP addresses to a text document for use later in this guide.

INFOBLOX PORTAL

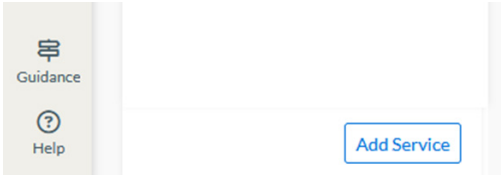
Create a NIOS-X as a Service Deployment

This portion of the guide covers how to configure NIOS-X as a Service on the Infoblox Portal once a Google Cloud VPN Gateway has been created. Perform the following steps to configure the NIOS-X as a Service connection in the Infoblox Portal.

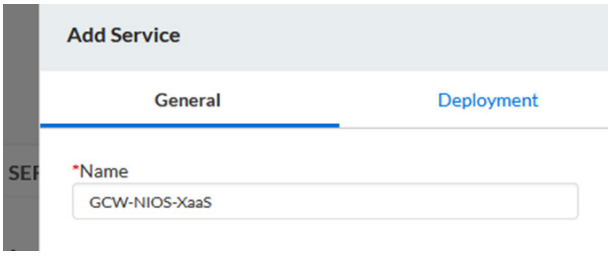
1. Navigate to the **As-A-Service** page on the Infoblox Portal. Highlight **Configure**, click **Service Deployment**, then click **As-A-Service** in the list.



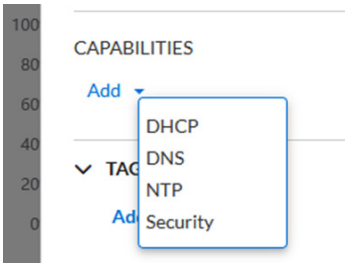
2. On the bottom left of the **As-A-Service** page, click **Add Service** to begin adding a new service deployment.



3. In the **Add Service** panel, input a **Name** for the new service.



4. Add the desired capabilities to the service via **Add** located under the **CAPABILITIES** header.



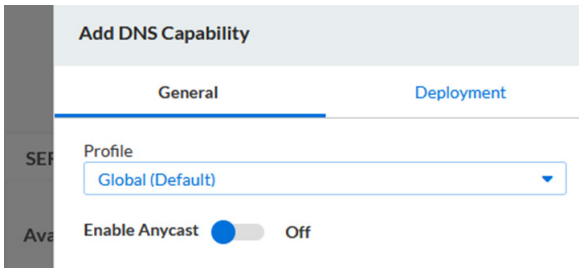
5. Configure the capability with the appropriate **Policy** or **Profile**. For DNS, enable Anycast if desired.

   Note: Each service will show a different set of configuration parameters. The example screenshot is from the DNS service.

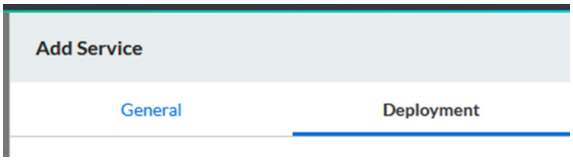
For more information on security profiles, DNS configuration profiles or DHCP configuration profiles, please visit the following Infoblox documentation pages:

- Security profiles: *Configuring Security Policies*
- DNS configuration profiles: *Configuring DNS Config Profiles*
- DHCP configuration profiles: *Configuring DHCP Config Profiles*

Repeat steps 4 and 5 in this section to add any additional required services.



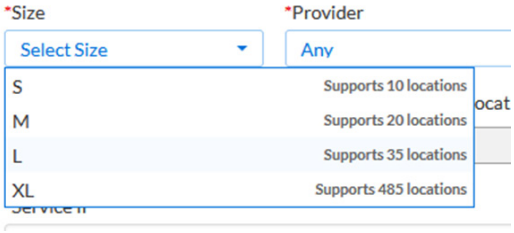
6. Click the **Deployment** tab located at the top of the **Add Service** panel.



7. Click **Add Service Deployment**.

8. Input a **Name** for the new service deployment.

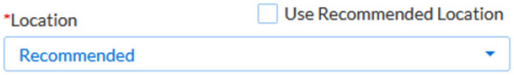
9. Select the appropriate **Size** for the service deployment.



10. Select the **Provider** for the Service Deployment.

11. Select the **Location** for the service deployment.

Note: You may optionally keep **Use Recommended Location** *selected, which will automatically select a location based on the locations connected to it.*



12. Input a **Service IP**.

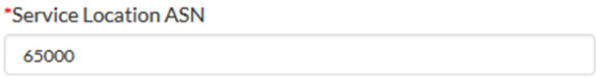
Note: This is the as-a-service IP that will be providing services like DNS and DHCP to clients. This must be an IP in a private range.

13. Select **Dynamic**(**BGP**) for the **Routing** protocol.

Note: Static routing is not currently supported for the NIOS-X as a Service connection with Google's Cloud WAN.

14. Input an ASN in the **Service Location ASN** field.

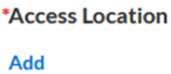
Note: For the ASN you will need to input a private ASN in the **Service Location ASN** *field. Note, this ASN will be the same as the ASN input in the Google Cloud Router configured later in this guide.*



15. Input a Primary Source IP and a Secondary Source IP.

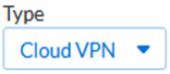
Note: These IPs are for additional services like Anycast and zone transfers. These IPs must be in a private range. For more information on the **Primary Neighbor IP** *and* **Secondary Neighbor IP** *usage, please see the Infoblox documentation page, Configuring an IPSec Tunnel.*

16. Click **Add** located under the **Access Location** header.

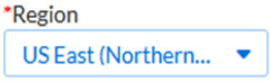


17. Select **GCP** as the **Provider**.

18. Select **Cloud VPN** as the **Type**.

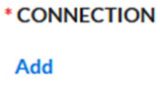


19. Select the appropriate **Region** for the connection.



20. Provide a **Name** for the **Access Location**.

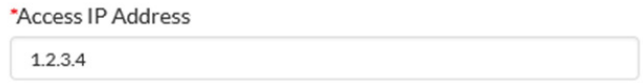
21. Click **Add** under the **CONNECTION** header to add a new connection.



22. Input a **Name** for the new connection.

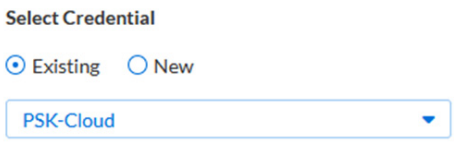
23. Click **Add Primary** to add a new **PATH** to the connection.

24. Input the IP assigned to Interface 0 of your Google VPN Gateway as the **Access IP Address**.

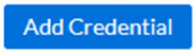


25. Click **Add Credential** to add a PSK.

26. Select **Existing** to use an existing PSK or select **New** to begin adding a new one.
Note: This PSK must match the one that is input in Google's VPN Tunnel Configuration later in this guide.



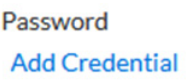
27. Click **Add Credential** to confirm the PSK selection.



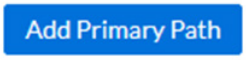
28. Input a **Neighbor IP Address**.
    Note: Save this IP for use later in this guide. This IP assists with peering between the Google VPN Gateway and the Service endpoint. This may be any IP.

29. Input an **Access Location ASN**.
    Note: For the ASN you will need to input a private ASN in the **Access Location ASN** *field. This* **Access Location ASN** *must match the cloud router ASN and must be different from the service location and VPN peering ASN.*

30. Optional: If you are using BGP authentication, input a **Password** by clicking **Add Credential.**

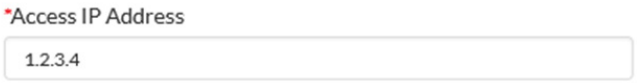


31. Click **Add Primary Path**.



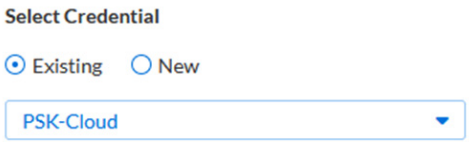
Once the primary path has been created, add a secondary path via clicking **Add Secondary**.

32. Input the IP assigned to Interface 1 of your Google VPN Gateway as the **Access IP Address**.



33. Click **Add Credential** to add a PSK.

34. Select **Existing** to use an existing PSK or select **New** to begin adding a new one.
    Note: This PSK must match the one that is input in Google's VPN Tunnel Configuration later in this guide.



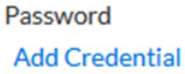
35. Click **Add Credential** to confirm the PSK selection.

36. Input a **Neighbor IP Address**.
    Note: Save this IP for use later in this guide. This IP assists with peering between the Google VPN Gateway and the service endpoint. This may be any IP.

37. Input an **Access Location ASN**.

    Note: For the ASN you will need to input a private ASN in the **Access Location ASN** *field. This* **Access Location ASN** *must match the cloud router ASN and must be different from the service location and VPN peering ASN.*

38. Optional: If you are using BGP authentication, input a **Password** by clicking **Add Credential**.



39. Click **Add Secondary Path**.

40. Click **Add Connection** to confirm the creation of the new connection.

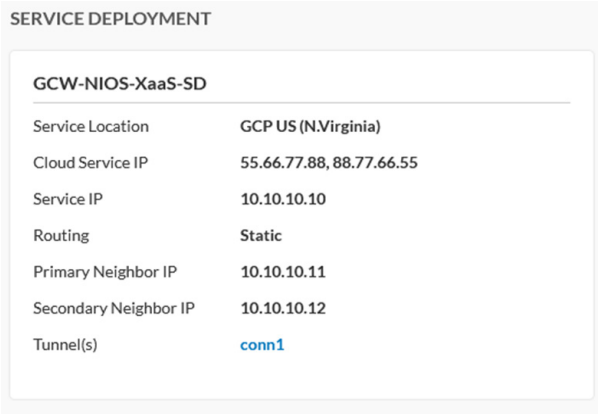
41. Click **Add Location** to confirm the creation of the new location.

42. Click **Add Deployment** to confirm the creation of the new service deployment.

43. Click **Save** to confirm all changes.

44. Once the new service deployment has been created, expand the list in the **Services** panel. Locate and click the new service deployment.

45. On the new access location's page, locate the **SERVICE DEPLOYMENT** panel and copy the **Cloud Service IP** to a text document of your choosing for use later in this guide.



GOOGLE CLOUD

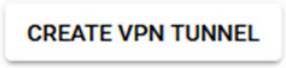
Create a Cloud VPN Tunnel

This portion of the guide walks through the configuration of a cloud VPN tunnel in the Google Cloud interface. Perform the following steps to configure a cloud VPN tunnel.

1. Navigate to the **VPN** page in the Google Cloud interface by searching for VPN and clicking the **VPN** search result.

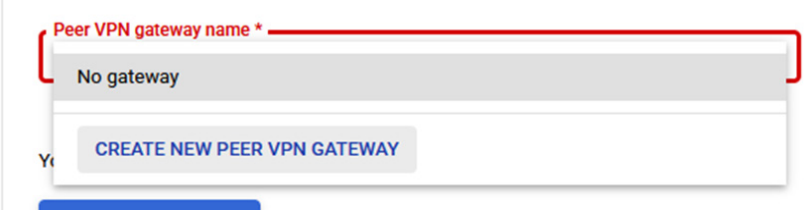
2. Click the **CLOUD VPN TUNNELS** tab.

3. Click **CREATE VPN TUNNEL**.



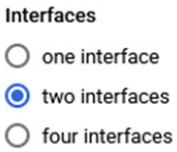
4. Select the **VPN gateway** that was created earlier in this guide.

5. Create a new peer VPN gateway by clicking the dropdown and clicking **CREATE NEW PEER VPN GATEWAY**.



6. Input a **Name** for the peer VPN gateway.

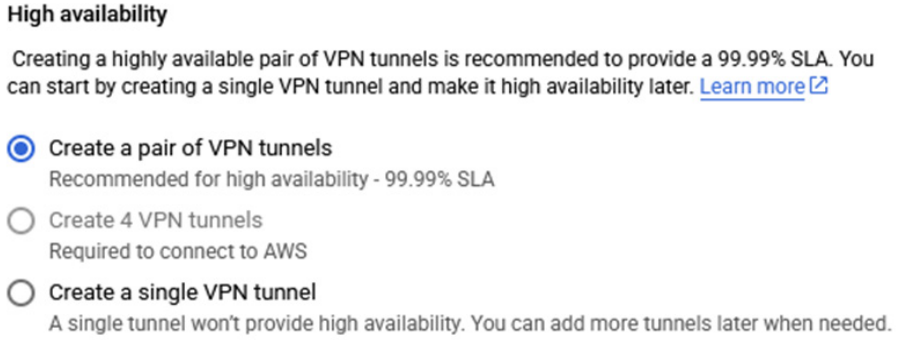
7. Select **two interfaces** under the **Interfaces** header.



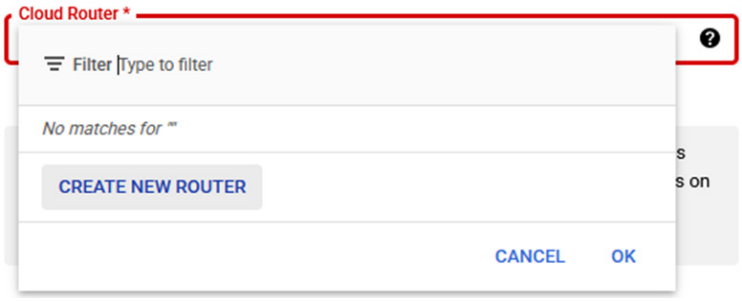
8. Input the IPs acquired from step 45 on page 13 in the **Interface 0** and **Interface 1** text fields.

9. Click **CREATE**.

10. Keep the default selection of **High availability** as **Create a pair of VPN tunnels**.



11. Click the **Cloud Router** dropdown, then click **CREATE NEW ROUTER** in the list.



12. Give the new cloud router a **Name**.

13. Input a **Cloud Router ASN**.
Note: This must match the **Access Location ASN** *that was input in the Infoblox Portal when creating the path.*

14. Input an appropriate **BGP peer keepalive interval**.
Note: This value must be between 20 and 60 seconds.

15. Keep all other settings as their defaults and click **CREATE** to create the new Google Cloud Router.

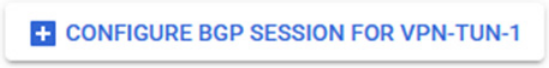
16. Input a **Name** for the first VPN tunnel.

17. Input an **IKE pre-shared key**.
Note: This should be the same PSK that was utilized in the Infoblox Portal when creating the first path.

18. Input a **Name** for the second VPN tunnel.

19. Click **CREATE & CONTINUE**.

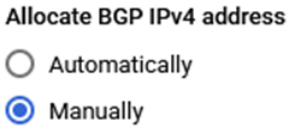
20. On the Configure BGP sessions page, click the button **CONFIGURE BGP SESSION FOR** …. associated with your VPN's first tunnel.



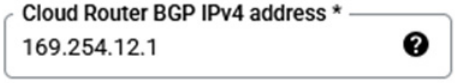
21. Input a **Name** for the tunnel's BGP session.

22. Input the **Peer ASN**.

23. Select the **Manually** bubble located under the **Allocate BGP IPv4 address** header.



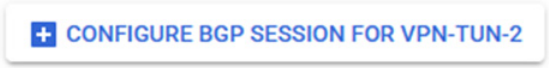
24. Input the **Cloud Router BGP IPv4 address**.
Note: This must be the same IP input for Neighbor 1 in the Infoblox cloud portal when creating the access location for this deployment.



25. Input the Cloud Router BGP IPv4 address.
Note: This should be the same IP input for Neighbor 2 in the Infoblox cloud portal when creating the access location for this deployment.

26. Keep all other settings as their defaults. Then, click **SAVE AND CONTINUE**.

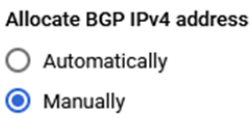
27. On the Configure BGP sessions page, click the button **CONFIGURE BGP SESSION FOR** .... associated with your VPN's second tunnel.



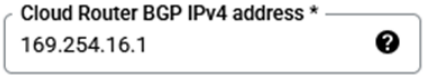
28. Input a **Name** for the tunnel's BGP session.

29. Input the **Peer ASN**.

30. Select the **Manually** bubble located under the **Allocate BGP IPv4 address** header.



31. Input the **Cloud Router BGP IPv4 address**.
    Note: This should be the same IP input for Neighbor 1 in the Infoblox cloud portal when creating the access location for this deployment.



32. Input the **Cloud Router BGP IPv4 address**.
    Note: This should be the same IP input for Neighbor 2 in the Infoblox cloud portal when creating the access location for this deployment.

33. Keep all other settings as their defaults. Then, click **SAVE AND CONTINUE**.

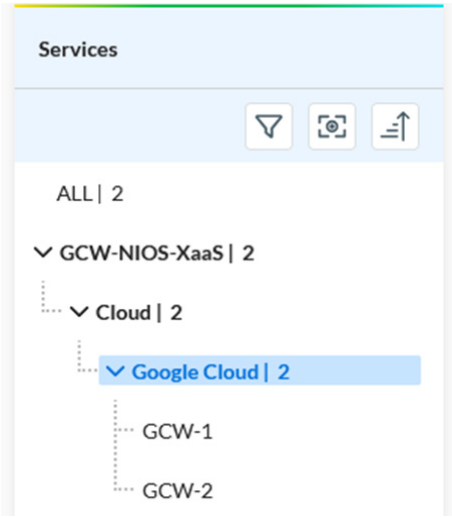
34. Click **SAVE BGP CONFIGURATION** to confirm the BGP configuration for the VPN tunnels.

35. Review the summary and reminder page to verify that all parameters are correct. Click **OK** to confirm the creation of the VPN tunnels.

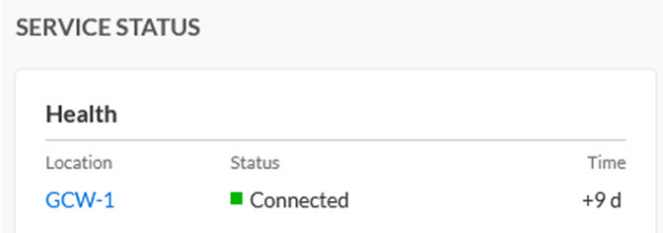
VERIFY CONNECTIVITY

Once the previous sections have been completed your NIOS-X as a Service tunnel should be up and running. To check the status of NIOS-X as a Service to Google's Cloud WAN, perform the following steps:

1. Locate and click the service deployment that was configured in this guide in the Infoblox Portal.



2. Locate the **SERVICE STATUS** panel and verify that the status is **Connected**.



3. Access a client that has connectivity to the NIOS-X as a Service service deployment. Open a terminal on that client and verify the status of the services that were deployed.
   Example: If DNS was configured, run a dig or nslookup on a domain using the NIOS-X as a Service service as the resolver.

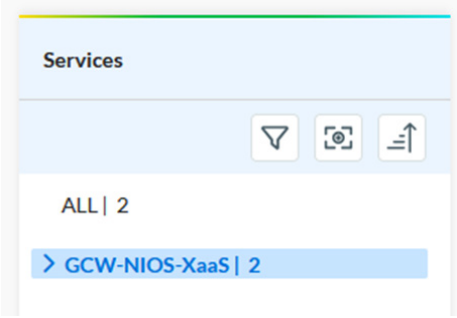
```
C:\Users\MyUser>nslookup infoblox.com
Address:  10.10.10.10

Non-authoritative answer:
Name:    infoblox.com
Addresses:  151.101.130.253
```

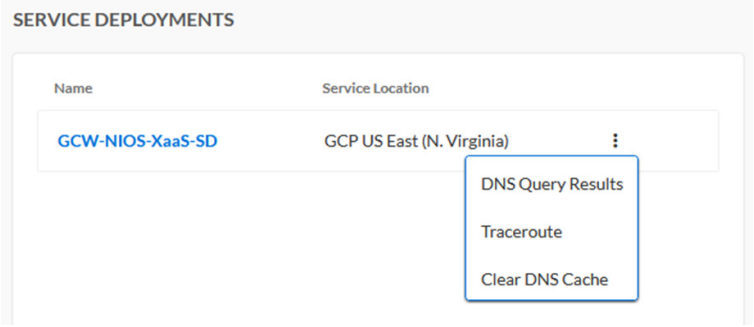
TROUBLESHOOTING NIOS-X AS A SERVICE

Built-in troubleshooting tools exist in the portal for NIOS-X as a Service. To access them, access the Infoblox Portal and navigate to the As-A-Service page.

1. In the **Services** panel of the As-A-Services page, locate and click on the top level of the NIOS-X as a Service deployment you wish to troubleshoot.



2. Click the ellipses associated with your NIOS-X as a Service instance in the **SERVICE DEPLOYMENTS** panel to access these tools. For more information on these tools, visit the Infoblox documentation page, *Troubleshooting NIOS-X-as-a-Service*.



NEXT STEPS

Infoblox NIOS-X as a Service can be used similarly to any of Infoblox's cloud-based services. For more information on next steps in configuration and use, please visit the following Infoblox documentation pages:

- DNS
- DHCP
- Configuring NTP Servers
- Configuring Security Policies

CONCLUSION

Congratulations on deploying Infoblox NIOS-X as a Service with Google's Cloud WAN. NIOS-X as a Service can be managed the same way as any other Infoblox Portal service. It can be applied to DHCP ranges, DNS zones, etc. By deploying NIOS-X as a Service for Google's Cloud WAN, you are combining Infoblox's industry-leading DDI capabilities with Google's premium global network infrastructure. Integrating these products delivers a comprehensive cloud-native solution that eliminates infrastructure complexity while ensuring enterprise-grade performance and security.

CONTACT AND SUPPORT

To contact Infoblox Support, you have several options depending on your location and needs:

Phone Support

Infoblox provides 24/7 technical support via phone for various regions. For a comprehensive list of support contact numbers, visit the Infoblox Support Contact Information Page.

Online Support

- Support Portal: Log in at support.infoblox.com to open a case, access documentation and manage your support tickets.
- Email Support: For general inquiries, you can email info@infoblox.com.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20250616v1