BLUECAT™

Blueprint for AWS

BlueCat Blueprint for AWS

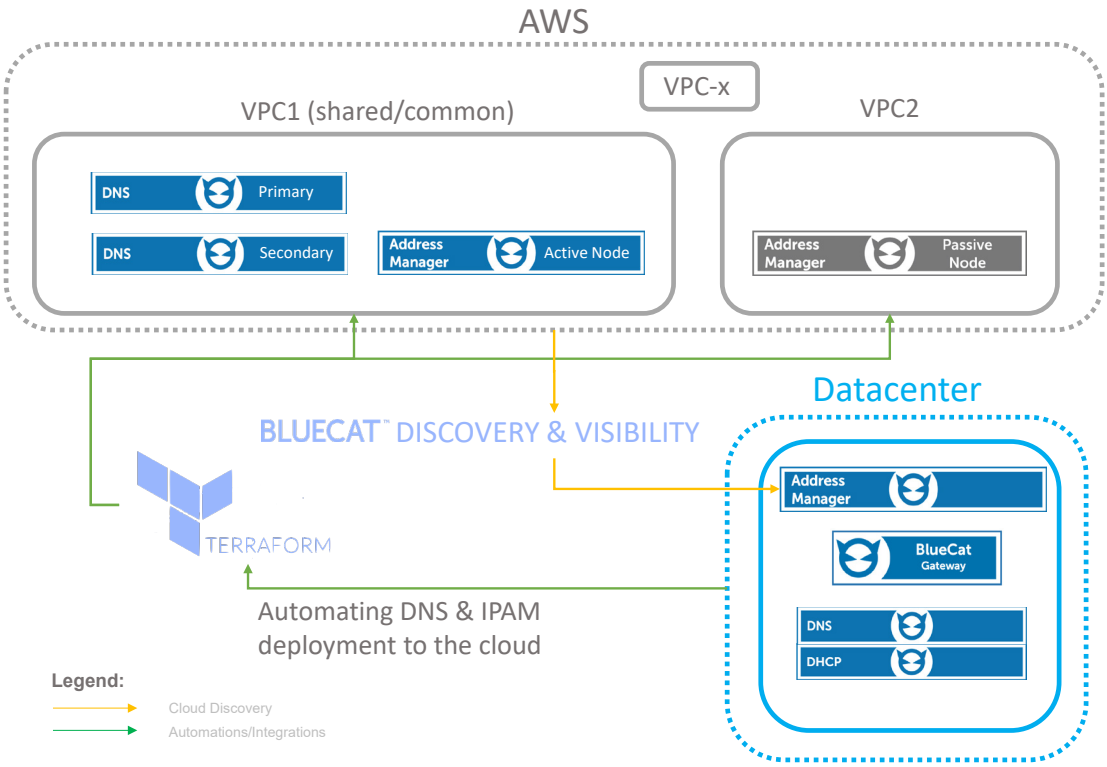
Overview

This blueprint provides an example BlueCat architecture that can be used as a guide while setting up your hybrid cloud DDI environment. Once implemented, instructions provided allow BlueCat Address Manager (BAM) and BlueCat Gateway to discover and import data from an Amazon cloud environment and monitor ongoing changes. This allows network teams to ensure the BAM database is always updated, and provides the ability to seamlessly query AWS, internal (BlueCat), and external DNS records from a consistent, centrally-managed platform.

By implementing the solutions in this guide, network teams can tackle the following challenges:

- Lack of visibility into cloud adoption and utilization across the enterprise
- Prolific DDI silos leading to zone conflicts, errors, and outages
- Limited automation and orchestration across the enterprise that slows innovation.

BlueCat Blueprint



This architecture sets up the following in AWS and or local datacenter:

- Moving compute infrastructure into AWS with zero-touch automation using Terraform
- Setting up a highly scalable automation platform, BlueCat Gateway server, to run custom automation applications such as BlueCat Discovery & Visibility
- Eliminating Route 53 DNS Silos in AWS by automating the discovery of cloud objects and pulling them into BlueCat Address Manager
- Viewing all IP address assignments, network allocation, and resource records across environments, all from a single web-based interface with BlueCat Address Manager (BAM)

Prerequisites

BlueCat Discovery & Visibility

The BlueCat Cloud Discovery & Visibility Adaptive Application introduces a method to retrieve data from AWS, Azure, and GCP Cloud and import discovered objects into Address Manager. This provides continuous, real-time visibility into the changes to your cloud infrastructure.

BlueCat Terraform Plugin

BlueCat & Terraform enable "infrastructure to act as code" for flexible configuration management. It allows network teams to create a version control library, run scheduled monitoring to detect unwanted changes, or instantly set up new environments. It does this by automating the augmentation, addition, or removal of files to your infrastructure based on the context coded by the user.

Integrity 9.2 or Greater

BlueCat Integrity is BlueCat's core offering, comprised of BlueCat Address Manager, our IP address management application, and authoritative DNS and DHCP servers. BlueCat Address Manager is a powerful IP Address Management (IPAM) solution allowing you to take control of your complex and dynamic network. With integrated core services, workflow and automation, BlueCat Address Manager enables you to centrally manage every connected device on your network from a single pane of glass. BlueCat Address Manager provides network intelligence and insight into the relationship between devices, users, and IP addresses that can be put into action to improve security and ensure reliable, always-on business connectivity.

Specialized Knowledge

Before you deploy, we recommend you become familiar with the following AWS services. (If you are new to AWS, see Getting Started with AWS.)

- Amazon EC2
- Amazon VPC
- AWS Directory Service for Microsoft Active Directory
- AWS CloudFormation

Deployment Steps

By default, the Gateway admin user has access to the Cloud Discovery & Visibility AWS workflow. If you have other BlueCat Gateway users that will interact with this workflow, you must configure the workflow permissions to grant those users access.

Deploy BlueCat Address Manager & DNS into the cloud

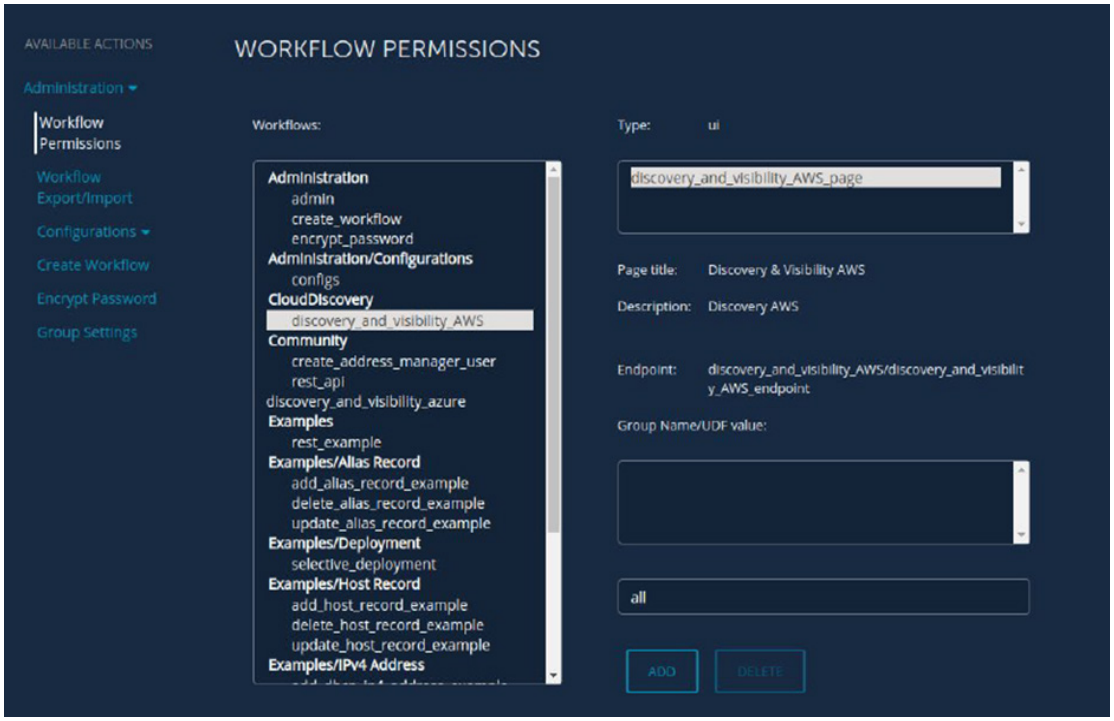
1. Download the example BlueCat deployment Terraform scripts from BlueCat Labs
2. Customize the Terraform (.tf) files as appropriate to match the configuration of the target cloud environment. Note, these scripts are specific to AWS, but can be used as templates for GCP or Azure
3. Initialize the Terraform environment: `$ terraform init`
4. Test the deployment actions: `$ terraform plan`
5. Review the output of the plan action to validate the configuration
6. Execute the deployment: `$ terraform apply`
7. Once the deployment is complete, log into the BlueCat Address Manager (BAM) and proceed with configuring the Gateway workflow for Discovery & Visibility

Configure BlueCat Gateway with Discovery & Visibility

Configure BAM Settings:

8. Log in to BlueCat Gateway
9. Select **Administration** > **General Configuration**
   BAM Settings opens
10. Under **BAM URLs**, enter the IP address of the primary BAM, and select **HTTP** or **HTTPS** from the drop-down menu. (Optional) In the **BAM Alias** field, enter the name of the BAM. For example, Primary, Secondary, Test, or Production
11. (Optional) Enter the name of your **Default Configuration** in Address Manager. All workflows will be executed against that specific configuration
12. (Optional) Enter the name of your **Default View** in Address Manager. All workflows will be executed against that specific DNS view
13. Click **Save**
14. Click **Add another BAM** if you want to add another BAM

Configuring the workflow permissions



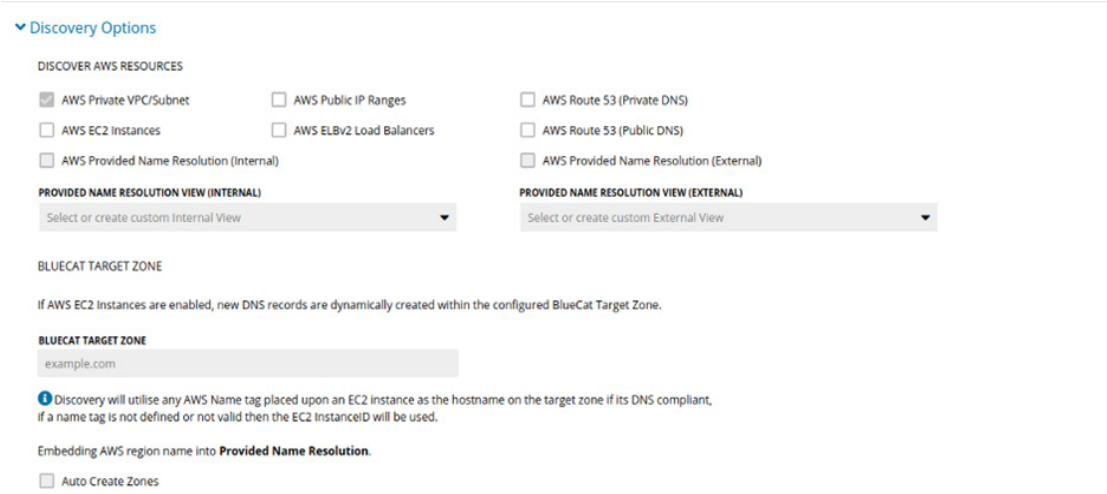
To configure the workflow permissions:

1. Log in to BlueCat Gateway
2. Under **AVAILABLE ACTIONS**, click **Administration > Workflow Permissions**
3. In the **Workflows** list, select **discovery_and_visibility_AWS**
4. Select **cloud_discovery_and_visibility_AWS_page**

5. Under the **Group Name/UDF value** list, select the appropriate user group
6. Click ADD

Cloud Discovery Options

The following section defines what information is imported from the AWS infrastructure.



1. Under **Discovery Options**, select the information that you would like to import:

- **AWS Private VPC/Subnet**—select this checkbox to import all AWS VPC and Subnet network information. The private VPCs/Subnets are converted into IPv4 and IPv6 blocks and networks on Address Manager
- **AWS Public IP Ranges**—select this checkbox to import all AWS public address space information. The public VPCs are converted into IPv4 and IPv6 blocks and networks on Address Manager
- **AWS EC2 Instances**—select this checkbox to import all EC2 instance information. The EC2 instances are converted into devices on Address Manager
- **AWS ELBv2 Load Balancers**—select this checkbox to import all ELBv2 information. This is converted into the ELBv2 device type on Address Manager
- **AWS Route53 DNS (Private DNS)**—select this checkbox to import all private AWS Route53 DNS zone record information. The DNS zone records are converted into private DNS records on Address Manager
- **AWS Route53 DNS (Public DNS)**—select this checkbox to import all public AWS Route53 DNS zone record information. The DNS zone records are converted into public DNS records on Address Manager
- **AWS Provided Name Resolution (Internal)**—select this checkbox to import internal DNS record information. The internal DNS records are converted into internal DNS records on Address Manager with the prefix defined in the **BLUECAT TARGET ZONE** field
- **PROVIDED NAME RESOLUTION VIEW (INTERNAL)**—enter the name of the view that will be created in Address Manager or select an existing view in Address Manager that will contain the internal AWS provided name resolution information
- **AWS Provided Name Resolution (External)**—select this checkbox to import external DNS record information. The external DNS records are converted into external DNS records on

Address Manager with the prefix defined in the BLUECAT TARGET ZONE field

- **PROVIDED NAME RESOLUTION VIEW (EXTERNAL)**—enter the name of the view that will be created in Address Manager or select an existing view in Address Manager that will contain the external AWS provided name resolution information
- **BLUECAT TARGET ZONE**—enter the name of the DNS zone on Address Manager that will contain EC2 instance DNS records
- **Auto Create Zones**—select this checkbox to embed AWS availability zones for EC2 Instances and embed AWS region names for ELBv2 into the Provided Name Resolution

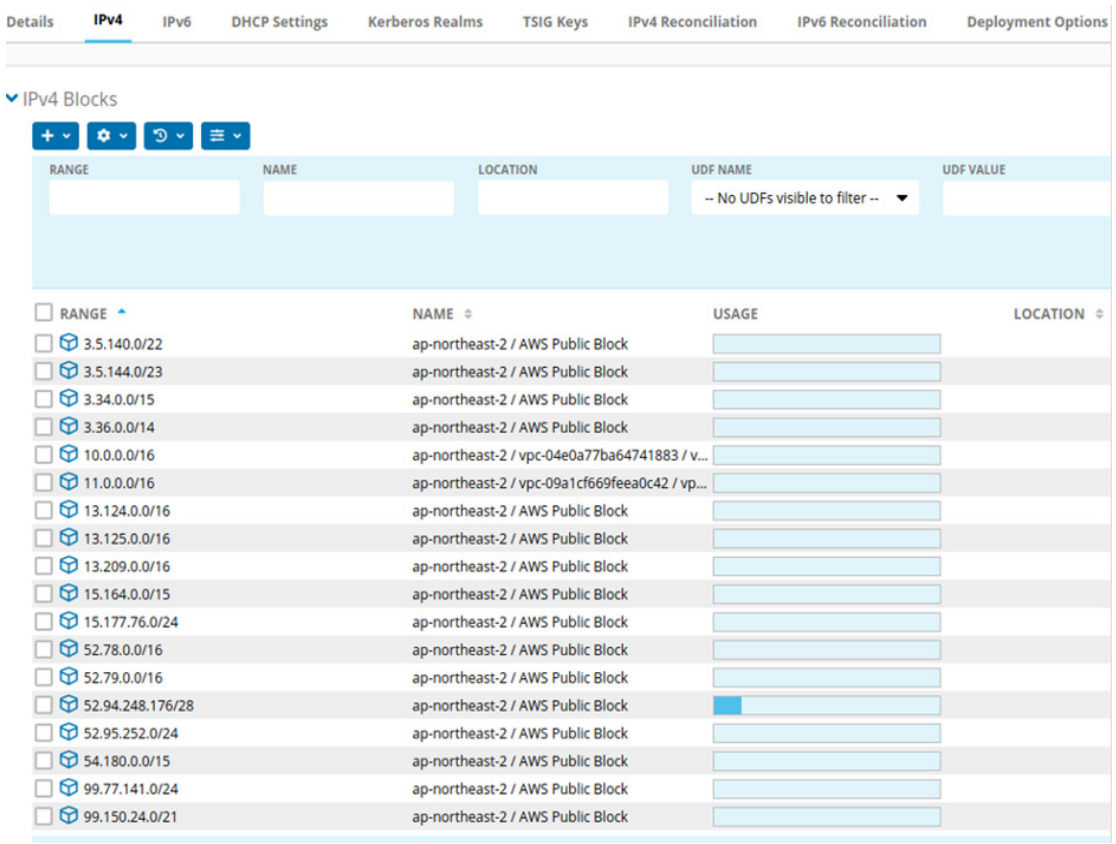
2. Click "Start Discovery"
3. Wait for the blue bar message: [INFO] Visibility Started. If any errors occur re-check your inputs and hit "Start Discovery" to retry

Post-discovery - Accessing and Navigating AWS Data in BAM

After configuring the Discovery & Visibility AWS workflow, you can log in to Address Manager and verify the AWS infrastructure data is importing correctly.

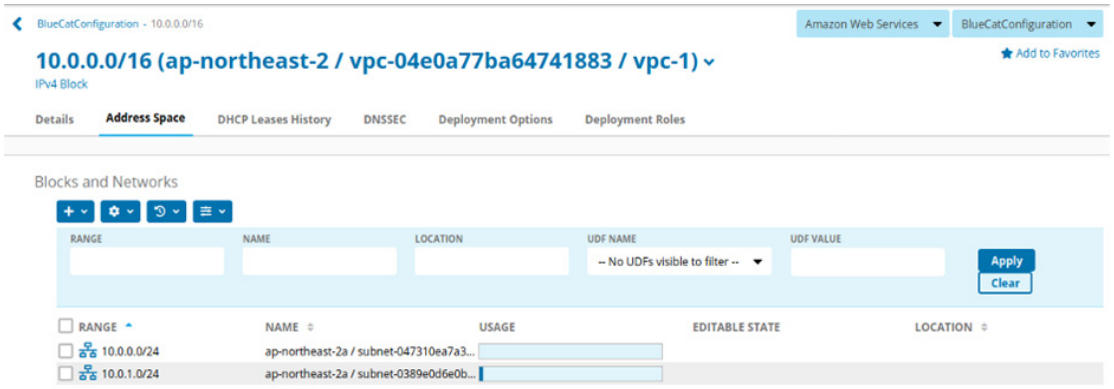
Navigating VPC Data

By default, AWS provides additional public VPCs which will appear under the IPv4 tab within the IP Space tab if you enabled the import of the **AWS Public IP Ranges** from the **Discovery Options** settings. The following image shows the imported public IP ranges from AWS.



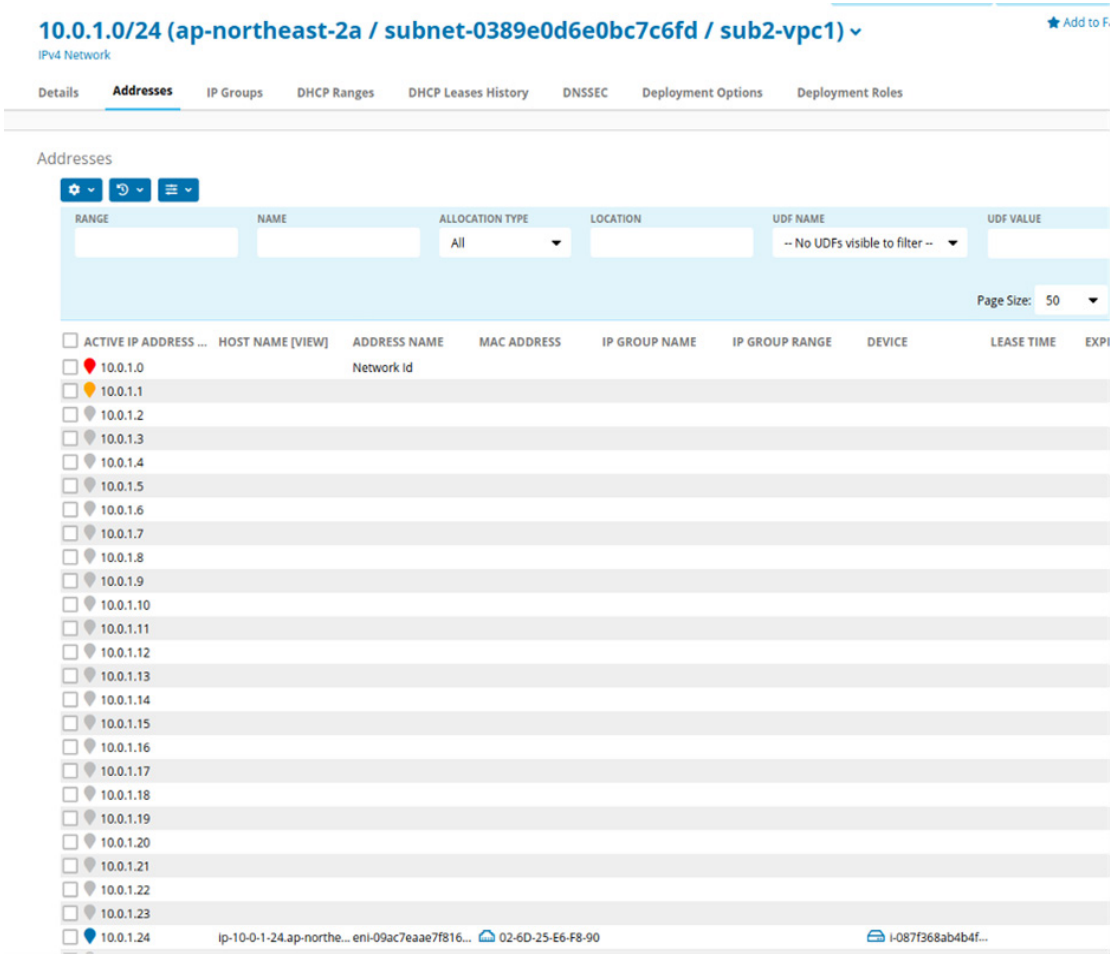
Navigating Subnet Data

Subnet information is created based on VPCs and are imported as IPv4 networks and IPv6 networks under their respective blocks. The following image displays two sample IPv4 networks that were created under an imported VPC network.



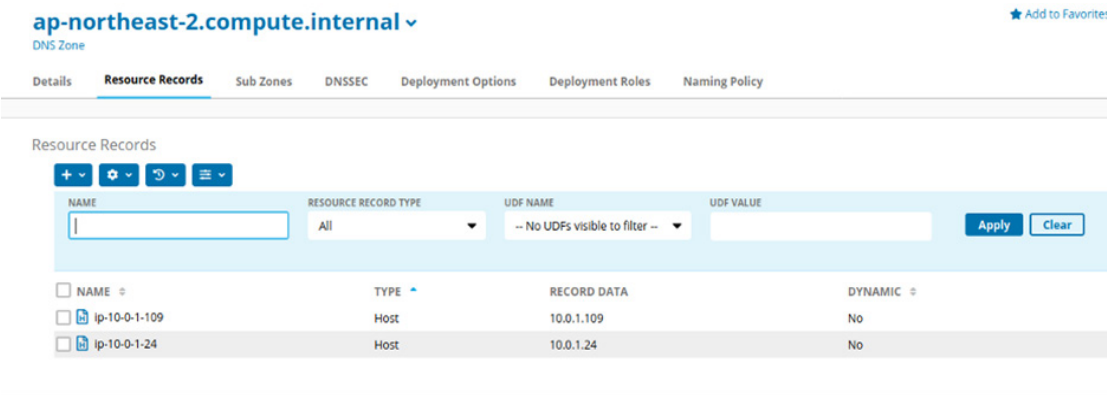
Navigating EC2 Data

Within the IP Space, the addresses associated to the EC2 instances are also assigned to the EC2 device in Address Manager. The following image displays the IP address assigned to the EC2 instance in the Address Manager user interface.



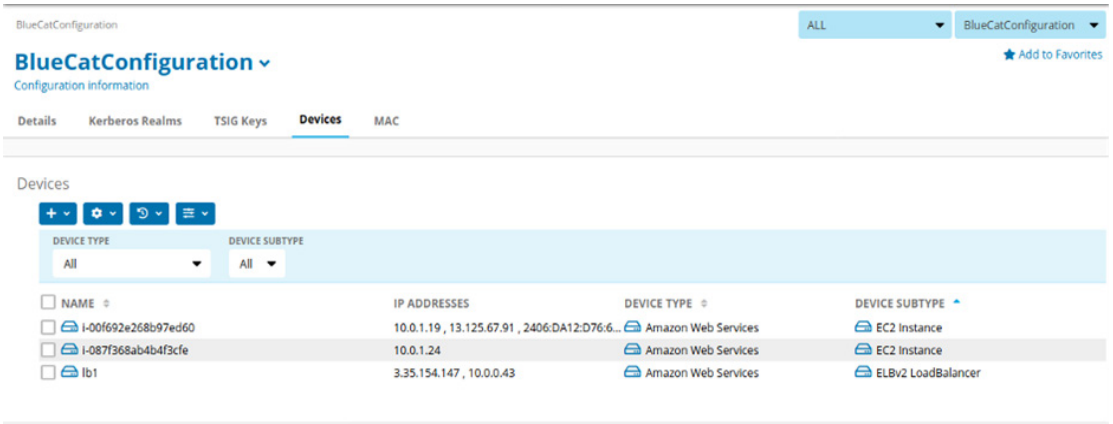
Navigating DNS Data

When clicking on the internal DNS view in Address Manager, you can see the DNS zone data is populated from the AWS infrastructure, including resource records. The following image displays the DNS resource record data imported from the internal DNS zone.



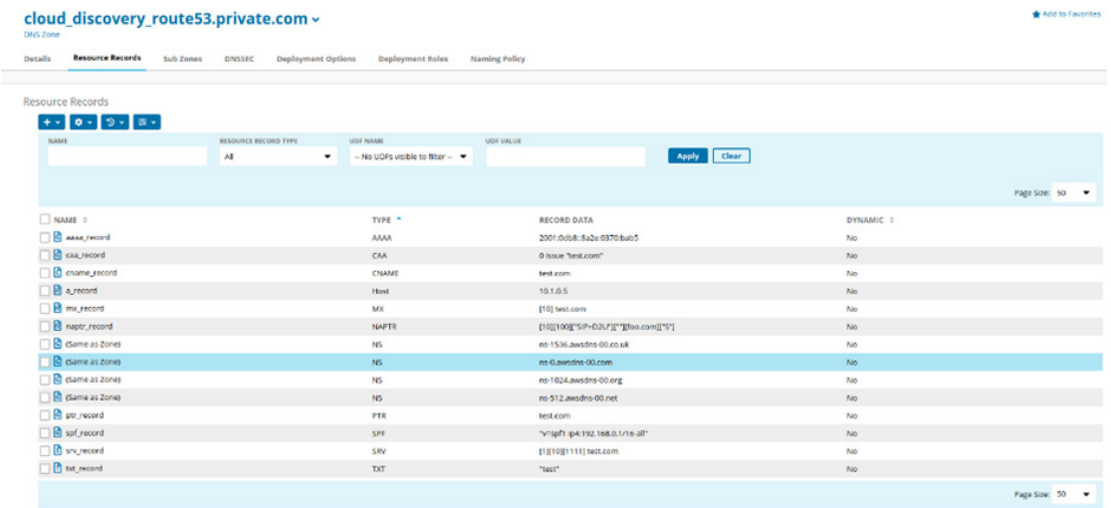
Navigating ELBv2 Data

When the ELB are imported into the Address Manager, they are imported as devices. The following image displays the ELBv2 devices in the Address Manager user interface.



Navigating Route53 Data

In the following image, the Route53 private hosted zone data is populated in Address Manager under the Route53 private view.



For More Information

Terraform scripts can be adapted and applied to any cloud vendor, download the sample script on BlueCat Labs

See product guides for using BlueCat Discovery and Visibility with Azure and GCP