

Implementation Guide:

Multi account Cloud Discovery and Visibility with BlueCat DDI and AWS Control Tower

BLUECAT™

Table of Contents

Foreword	3
Solution overview and features	4
Architecture diagram	5
Deployment and Configuration Steps	6
Step 1: BlueCat DDI - Initial Setup	6
Step 2: Deploy BlueCat Cloud Discovery & Visibility software	7
Step 3: Deploy the solution for BlueCat integration with AWS Control Tower	7
Testing the Solution	8
Solution Estimated Pricing	10
FAQs	10
Partner contact information	10

Foreword

BlueCat Integrity is an intelligent DNS, DHCP, and IP Address Management (DDI) platform designed to eliminate complexity, automate provisioning, accelerate application deployment, and ensure business resilience. Integrity delivers feature-rich Recursive and Authoritative DNS, dual-stack supported Dynamic Host Configuration Protocol (DHCP), and IP Address Management (IPAM) providing an authoritative source of intelligence and insight into the relationship between all the devices, users, and IP addresses on the network.

BlueCat Cloud Discovery & Visibility (CD&V) provides complete visibility and control of cloud assets from a single-pane-of-glass, providing customers the ability to centralize resources and records across on-premises and cloud environments.

BlueCat unifies DDI services, and consistently provides centralized visibility across all environments — establishing a reliable network foundation fueling innovation and growth.

This Implementation Guide describes how AWS Marketplace customers can deploy BlueCat Address Manager (BAM) and BlueCat Cloud Discovery & Visibility (CD&V) automatically when creating new accounts with AWS Control Tower.

Solution overview and features

BlueCat provides a simple approach to collecting DNS, DHCP and IPAM (DDI) data generated from AWS accounts to provide discovery and visibility of network resources. Armed with this information, network administrators can plan and govern their AWS environment. This helps build a reliable, secure, and resilient network foundation primed for agility in the face of changing demands. BlueCat DDI software is integrated with AWS Control Tower to provide a seamless way of governing network environments and resources across multiple AWS Accounts.

This is achieved by deploying BlueCat Address Manager (BAM) and BlueCat Cloud Discovery and Visibility (CD&V) in a shared Networking account of Control Tower. Within the Networking account, CD&V monitors AWS Control Tower, immediately discovering all resources, and records any newly created accounts and any future changes within those accounts. This consistent observability pipeline feeds the DDI data to BAM for network administrators to centrally manage and analyze.

By uniquely integrating BlueCat solutions within AWS, network teams benefit from:

- **Accelerate Provisioning and Management of IP space:** Improve visibility and control of resources when provisioned with BlueCat.
- **Simple Configuration:** Maintain AWS keys associated with the enterprise AWS account to keep BlueCat up-to-date with realtime records and related information.
- **Zero-touch automation:** Accelerate resource discovery and data collection without manual intervention in accounts managed by AWS Control Tower.
- **Smart Security:** Automate access control for BAM and CD&V using AWS policy inheritance rules.

Architecture diagram

The solution is deployed using Amazon Machine Images and integrates with AWS Control Tower Lifecycle events. When a new account is created, or an existing one is enrolled using the AWS Control Tower Account Factory, the Lifecycle event triggers a Lambda function. The Lambda function creates an IAM role in the member account, and creates a request to BlueCat Cloud Discovery and Visibility to run against the newly added account. BlueCat Cloud Discovery and Visibility provisions SQS and SNS resources in each member account. Other deployment scenarios for the BlueCat components are also supported, including hybrid deployments on-prem.

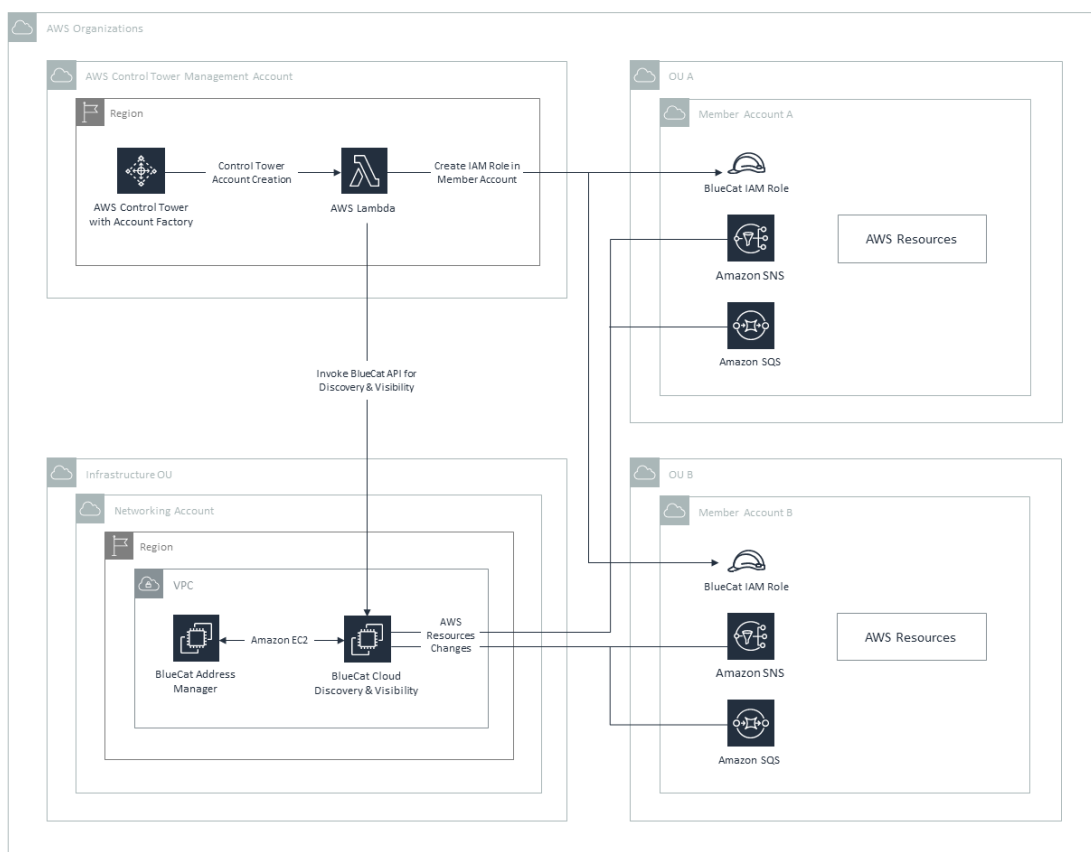


Figure 1: BlueCat integration with Control Tower - Architecture Diagram

Deployment and Configuration Steps

Prerequisites

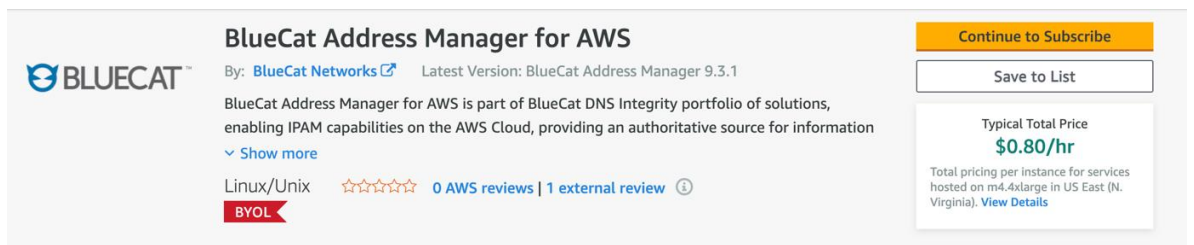
1. Ensure that AWS Control Tower is setup in your AWS Account by following the instructions [here](#).
2. Create a Networking account within Control Tower. This is a shared account which is used for hosting shared networking resources as per the multi-account best practice.
3. Create a VPC with public subnets in the Networking Account.

Step 1: BlueCat DDI - Initial Setup

1. Reference the documentation [here](#) for steps for the installation.
2. From your Networking account, subscribe to BlueCat Address Manager for AWS via the AWS Marketplace

Marketplace

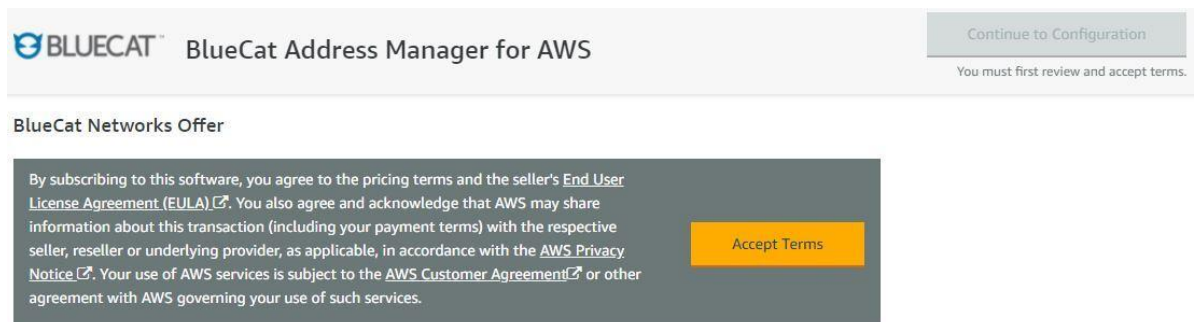
- a. Select the product from [AWS Marketplace](#)
- b. Choose **Continue to Subscribe**



BlueCat Address Manager for AWS
By: [BlueCat Networks](#) Latest Version: BlueCat Address Manager 9.3.1
BlueCat Address Manager for AWS is part of BlueCat DNS Integrity portfolio of solutions, enabling IPAM capabilities on the AWS Cloud, providing an authoritative source for information
[Show more](#)
Linux/Unix ☆☆☆☆☆ 0 AWS reviews | 1 external review ⓘ
BYOL

Continue to Subscribe
Save to List
Typical Total Price
\$0.80/hr
Total pricing per instance for services hosted on m4.4xlarge in US East (N. Virginia). [View Details](#)

- c. Click **Accept Terms**



BlueCat Address Manager for AWS
Continue to Configuration
You must first review and accept terms.

BlueCat Networks Offer

By subscribing to this software, you agree to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You also agree and acknowledge that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the [AWS Privacy Notice](#). Your use of AWS services is subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services.

Accept Terms

- d. Click on **Continue to Launch** and launch the software on the EC2 instance. Make sure to deploy the EC2 instance in a public subnet of a VPC and it has a public IP assigned to it.
3. Note down the Public IP of the BlueCat Address Manager instance. This will be used later for visibility into the discovered resources from your AWS Environment. The BlueCat Address Manager portal can be accessed using: `https://<instance_public_ip>/`

Step 2: Deploy BlueCat Cloud Discovery & Visibility software

1. Create a Linux EC2 that meets the specifications listed [here](#).
2. Follow the installation steps in [Installation Guide](#) to deploy Cloud Discovery and Visibility.
3. Create the User Data Field and User in your BlueCat Address Manager. Reference the IP that you took note of earlier. Access the portal via `https://<IP address>/`. You can find instructions [here](#).
4. Login to Cloud Discovery and Visibility
 - a. Under actions, select Cloud Discovery
 - b. Click Discovery & Visibility AWS

Step 3: Deploy the solution for BlueCat integration with AWS Control Tower

1. In your AWS Control Tower management account, launch the [CloudFormation template](#) to deploy the integration of BlueCat CD&V with AWS Control Tower using [steps](#) for creating a CloudFormation Stack. The Cloudformation stack expects the following parameters shown in the figure and explained below.

BAMurl : This is the portal URL of BlueCat Address Manager. This is normally of the form <https://<publicIPBAM>>, where publicIPBAM is the public ip address of the instance where BAM is deployed.

Gatewayurl : This is the portal URL of BlueCat CD&V. This is normally of the form <https://<publicIPCDV>>, where publicIPCDV is the public ip address of the instance where CD&V is deployed.

Username/Password: These are the credentials used for logging into the CD&V portal.

Access Key: This is the AWS IAM access key of an IAM user created within the AWS Account where the BlueCat software was deployed.

Secret Key: This is the AWS IAM secret key of an IAM user created within the AWS Account where the BlueCat software was deployed.

BlueCatAccountId: is the AWS Account Id where the BlueCat software has been deployed.

BlueCatTemplateURL: is the URL of the cloudformation template which specifies the BlueCat IAM role permissions needed in managed accounts for CD&V to work (*use default value unless asked to change by BlueCat team*).

Region: Provide the region where you want to run the BlueCate Cloud Discovery & Visibility.

Testing the Solution

Testing the integration with a new account created in Control Tower:

1. Go to the AWS Control Tower dashboard Account Factory page and follow the [steps](#) to create a new Account.
2. Once the Account is created, login to the BlueCat CD&V portal. Access the portal via `https://<IP address>/`. Note: IP address obtained from Step 2 above.
 - a. Click the **Discovery** tab and validate that a new discovery session has been created for the new AWS Account.

Discovery Status

DISCOVERY ID	START TIME	STATUS	AWS REGION	AWS ACCOUNT	BAM CONFIGURATIONS
1	11/03/2021 21:52:29	Completed	us-west-1		<ul style="list-style-type: none"> ControlTower-Test ControlTower-Test/App-043354663882c1ab1AWS-ISS-Dev ControlTower-Test/Route53 Public Hosted Zones/0818946

Discovery History

RESOURCE TYPE	START TIME	END TIME	BAM TOTAL	CLOUD TOTAL
Configurations	11/03/2021 21:52:29	11/03/2021 21:52:45	3	3
Public DNS Zones	11/03/2021 21:52:32	11/03/2021 21:52:34	2	2
Private DNS Zones	11/03/2021 21:52:30	11/03/2021 21:52:32	1	1
Load Balancers	11/03/2021 21:52:30	11/03/2021 21:52:30	0	0
Virtual Machines	11/03/2021 21:52:30	11/03/2021 21:52:30	14	14
Public IP Ranges	11/03/2021 21:52:29	11/03/2021 21:52:30	88	44
Subnet CIDRs	11/03/2021 21:52:29	11/03/2021 21:52:29	7	7
Subnets	11/03/2021 21:52:29	11/03/2021 21:52:29	7	7
VPC CIDRs	11/03/2021 21:52:29	11/03/2021 21:52:29	4	4
VPC Networks	11/03/2021 21:52:29	11/03/2021 21:52:29	4	4

- b. Go to the **Visibility** tab to ensure that a new visibility job is running as shown below.

Visibility Status

DISCOVERY ID	START TIME	END TIME	STATUS	AWS REGION	AWS ACCOUNT	BAM CONFIGURATIONS	BAM USERNAME
1	11/03/2021 21:52:46		Running	us-west-1		<ul style="list-style-type: none"> ControlTower-Test ControlTower-Test/App-043354663882c1ab1gw-admin ControlTower-Test/Route53 Public Hosts 	

Visibility History

CREATE TIME	ACTION	RESOURCE TYPE	RESOURCE NAME	RESOURCE REGION	ACTOR	STATUS
No data to display						

3. Login to the BlueCat Address Manager (BAM) portal and see that IP based resources of the new AWS account are displayed. The BlueCat Address Manager portal can be accessed using: `https://<instance_public_ip>/`. This IP was noted earlier in Step 1.3.

The screenshot shows the BlueCat Address Manager (BAM) portal interface. The top navigation bar includes 'My IPAM', 'IP Space', 'DNS', 'Devices', 'TFTP', 'Servers', 'Groups', and 'Administration'. The main content area is titled 'ControlTower-Test' and shows configuration information. Under the 'IPv4 Blocks' section, there is a filter bar with fields for 'RANGE', 'NAME', 'LOCATION', 'UDF NAME', and 'UDF VALUE'. Below the filter is a table listing IPv4 blocks with columns for 'RANGE', 'NAME', 'USAGE', and 'LOCATION'. The table contains 20 rows of data, each representing an IPv4 block with its corresponding name and usage details.

4. Login to the newly created AWS member account and launch an EC2 instance. Once the EC2 instance is deployed, you should see the resource changes appear in the BlueCat Address Manager portal, as shown below.

The screenshot shows the BlueCat Address Manager (BAM) portal interface, specifically the 'Devices' section. The top navigation bar is the same as in the previous screenshot. The main content area is titled 'ControlTower-Test' and shows configuration information. Under the 'Devices' section, there is a filter bar with fields for 'DEVICE TYPE' and 'DEVICE SUBTYPE'. Below the filter is a table listing devices with columns for 'NAME', 'DEVICE TYPE', 'DEVICE SUBTYPE', 'IP ADDRESSES', 'INSTANCE STATE', and 'NAME TAG'. The table contains 10 rows of data, each representing an EC2 instance with its corresponding IP addresses and instance state.

Testing the integration with existing AWS accounts of Control Tower:

Prerequisite: An existing AWS account that has been created via AWS Control Tower Account Factory must be present in the environment.

In order to update an existing AWS account with BlueCat Control Tower integration:

- Log in to the management account of Control Tower
- Navigate to AWS Service Catalog console
- Click on 'Provisioned Products' from the left-hand pane
- Select the Provisioned Product that corresponds to the account that was created via AWS Control Tower Account Factory. This is the target account with which to test the integration.
- Click on the 'Actions' dropdown and select 'Update'
- Fill in the parameters entered when creating the account from AWS Control Tower Account Factory. (Ensure that the same parameters are entered and nothing is changed)
- Click 'Update'

This will invoke the 'UpdateManagedAccount' API call which will trigger the Lambda function that was created as a part of this solution deployment.

Test the functionality of BlueCat as mentioned in the steps 2-4 above.

Solution Estimated Pricing

Contact [BlueCat Team](#) to learn more.

FAQs

You can find a list of FAQs for the BlueCat DDI and Cloud Discovery and Visibility in our documentation [here](#).

Partner contact information

For general inquiries, contact partners@bluecatnetworks.com.