Implementation Guide

Automating BigID data-source credentials provisioning with AWS Control Tower

Table of Contents

Foreword

BigID's data intelligence platform helps organizations to "know their enterprise data" and take actions for privacy, protection, and perspective. Customers deploy BigID to proactively discover, manage, protect, and get more value from their regulated, sensitive, and personal data across their data landscape.

The purpose of this AWS Implementation Guide is to help enable AWS Marketplace customers to ***seamlessly auto-provision credentials for the BigID application (specifically the scanner component)*** in AWS Control Tower environment while taking full advantage of the resources pre-configured by AWS Control Tower as part of the initialization.

Solution overview and features

AWS Control Tower integration with BigID helps automate the credentials provisioning process for BigID. Specifically, it will configure the BigID's Remote-Scanner components with the right AWS Identity and Access Management (IAM) roles and policies to perform read-only scans on applicable data-sources in a Multi-Account AWS environment.

AWS Control Tower lifecycle events like account creation (and/or update) will trigger the process of IAM policy and/or IAM role creation and deploy in the applicable AWS Account. The newly created IAM Policy will be mapped to the IAM role that would be "assumed" by the BigID Remote-Scanner component at runtime during the scan process.

With AWS Control Tower + BigID integration, you can:

- ✓ Automate the process of configuring credentials for BigID to scan your AWS data-sources like Amazon RDS, S3, DynamoDB, DocumentDB, etc.
- ✓ Auto install and/or update custom enterprise specific IAM policies on new and/or existing AWS accounts as they are created or updated, as well as auto attach (and/or delete) these polices to the IAM role that is "assumed" by the BigID Remote-Scanner component

AWS Control Tower + BigID Integration Architecture

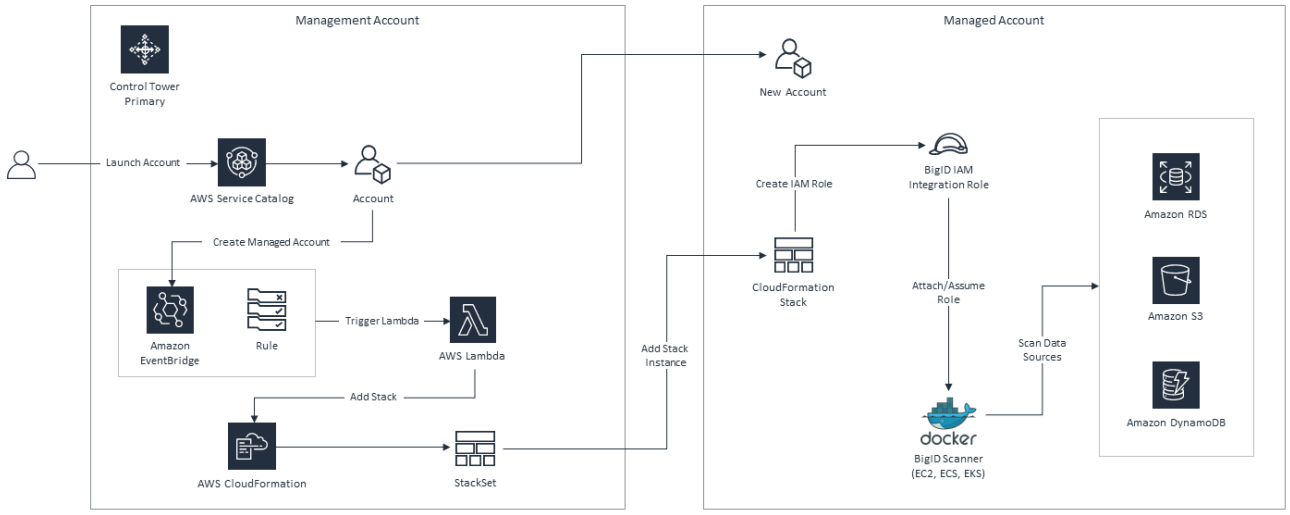


Fig-1 AWS Control Tower workflow on AWS Account events (create/update)

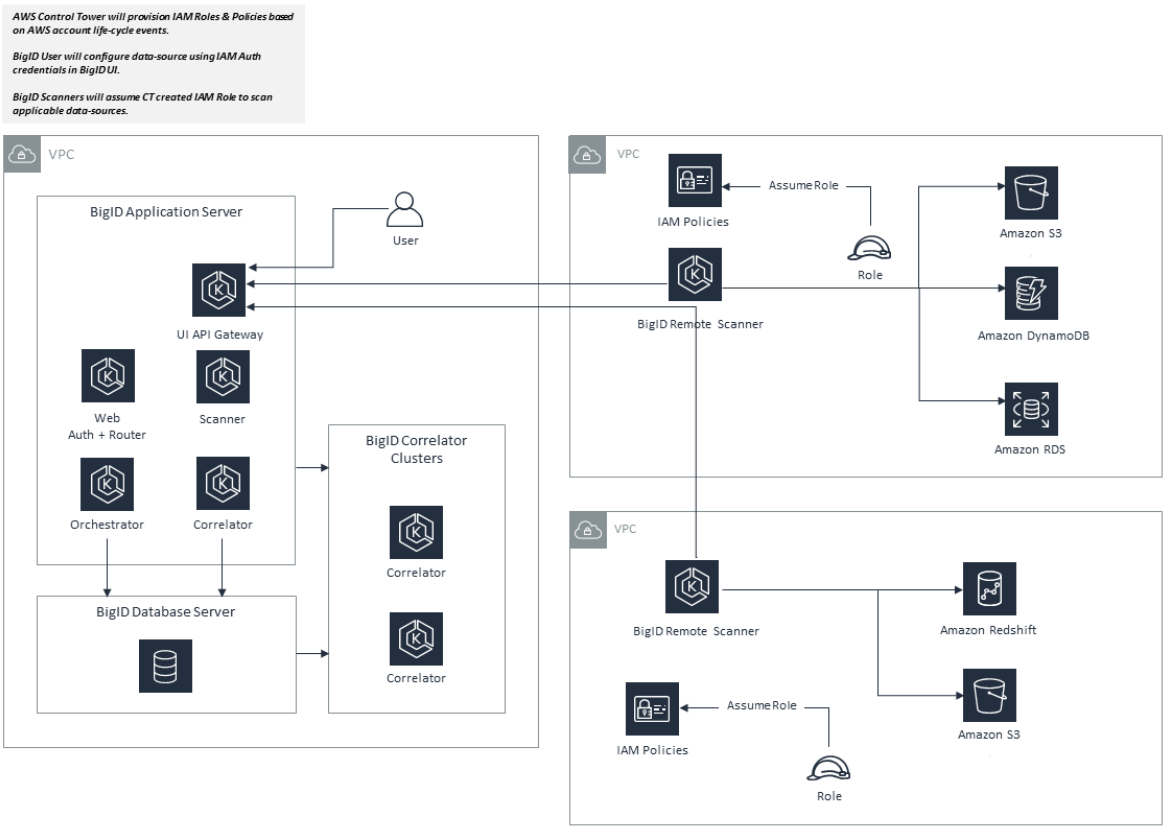


Fig-2 BigID data source credentials auto provisioning using AWS Control Tower

Fig-1 shows the sequence of activities (workflow) that are triggered by an Account event in AWS Control Tower environment.

Fig-2 architecture diagram provides a reference view of how BigID's Scanner component deployed in a typical enterprise's AWS environment can be integrated with AWS Control Tower. The BigID Product comprise of Application Server and Scanner. BigID Application Server may be hosted in one VPC in a particular account while there may be multiple distributed BigID-Remote-Scanner components installed closer to different AWS (or non-AWS) data-sources in different AWS VPC's and/or AWS accounts that needs to be scanned by BigID. These remote scanners need read credentials to perform the task of scanning.

This AWS Control Tower integration will automate the process of provisioning customer specific, BigID read-only IAM roles and policies. It will also allow the BigID-Remote-Scanner component to "assume" this role.

BigID users will then map the IAM role to the applicable AWS data-source while configuring the credentials for the data-source.

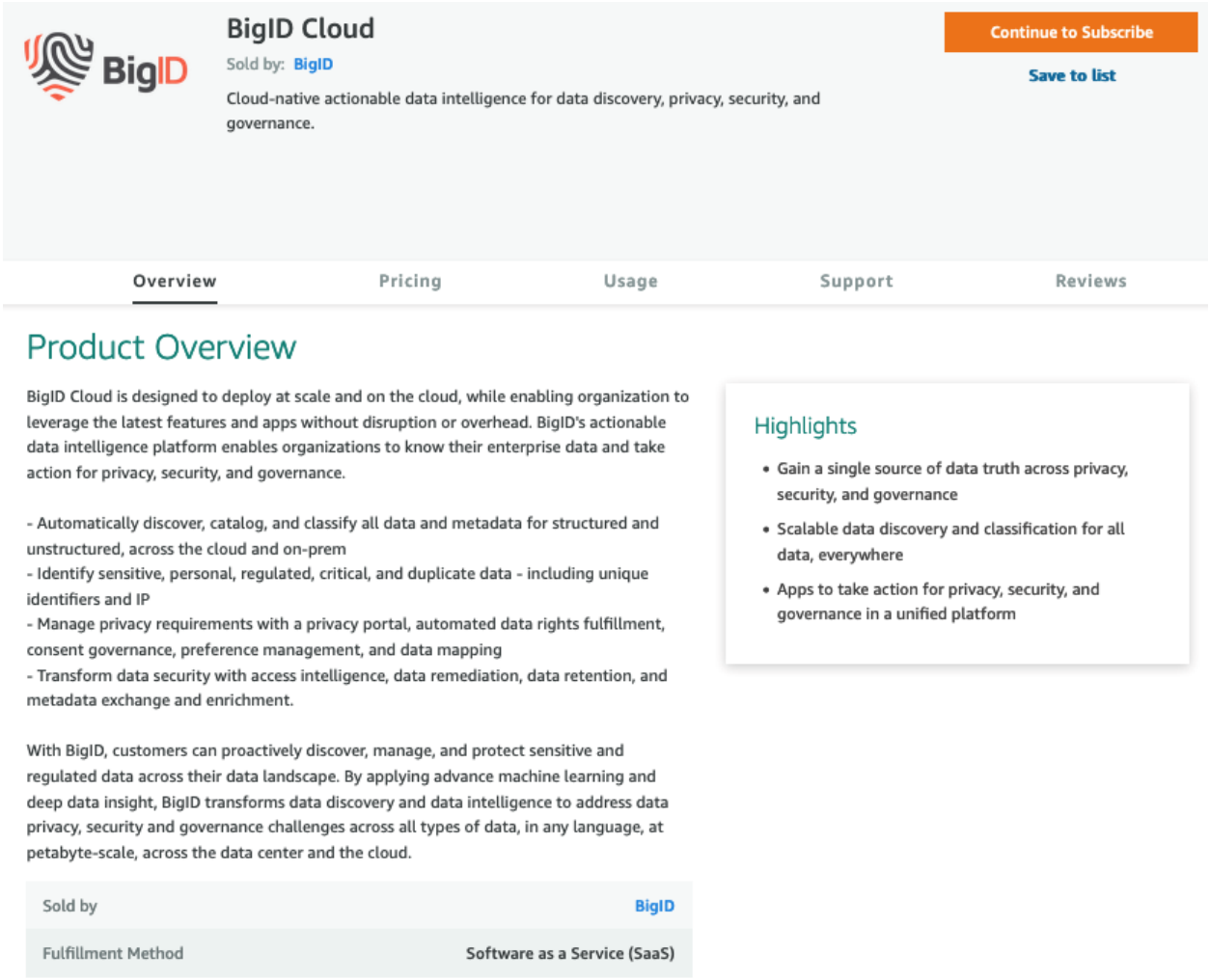
Pre-requisites

- BigID Product (Application Server, etc.) installed in the customers AWS environment
- AWS Control Tower configured to manage enterprise AWS multi-account environment
- Reference policy file with read-only grants to all BigID supported AWS data-sources.
    - This policy file will be used by default by AWS Control Tower BigID integration process to provision credentials for BigID Remote scanners.
    - Customers may use this policy file as a starting point and remove any grants that do not apply in their specific env (use least privilege)

Deployment and Configuration Steps

Step 1: Subscribe to BigID Cloud on AWS Marketplace

Locate the BigID listing in the AWS Marketplace



Click on the **Continue to Subscribe** button.

In the new screen, you can configure your contract. You can select the **Contract Duration**, **Renewal Settings** and **Contract Options**.

Once you have configured your contract, choose the **Create contract** button. You will be prompted to confirm the contract. If you agree to the pricing, select the **Pay Now** button.

Choose **Setup your account** to proceed to BigID portal to complete the registration. If you are newly subscribing to BigID, fill up the form in BigID portal to complete the registration.

Step 2: Launch BigID and AWS Control Tower integration solution

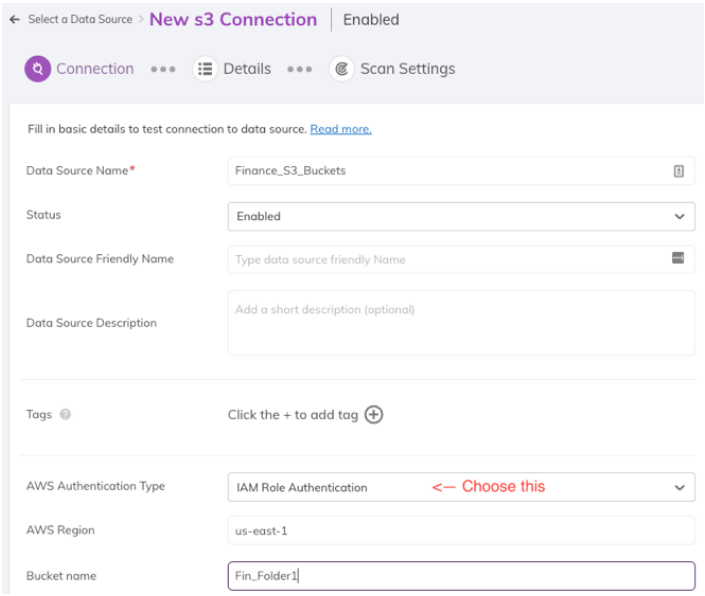
- To launch this solution, download the CloudFormation template
- Log in to AWS Control Tower Management Account with Administrator access.
- Select the Home Region, AWS Region where AWS Control Tower is launched.
- Navigate to AWS CloudFormation console and choose **Create stack, With new resources (standard)**.
- Choose **Upload a template file** and select the file you downloaded above and choose **Next.**
- Type in a Stack name of your choice and leave the default BigIDIAMRoleName. Optionally you could change it a per your needs.
- Choose **Next**, **Next**
- In Review step, review the options selected and checkbox **I acknowledge that AWS CloudFormation might create IAM resources** and choose **Create stack**

You successfully deployed the BigID and AWS Control Tower integration solution. When the new AWS Accounts are created using AWS Control Tower Account Factory, the required cross-account IAM role is automatically created on the new Accounts. For existing accounts, you need to manually add the choice of your accounts in CloudFormation stackset **BigIDScannerIAMRoleStackSet**, which is deployed by this solution.

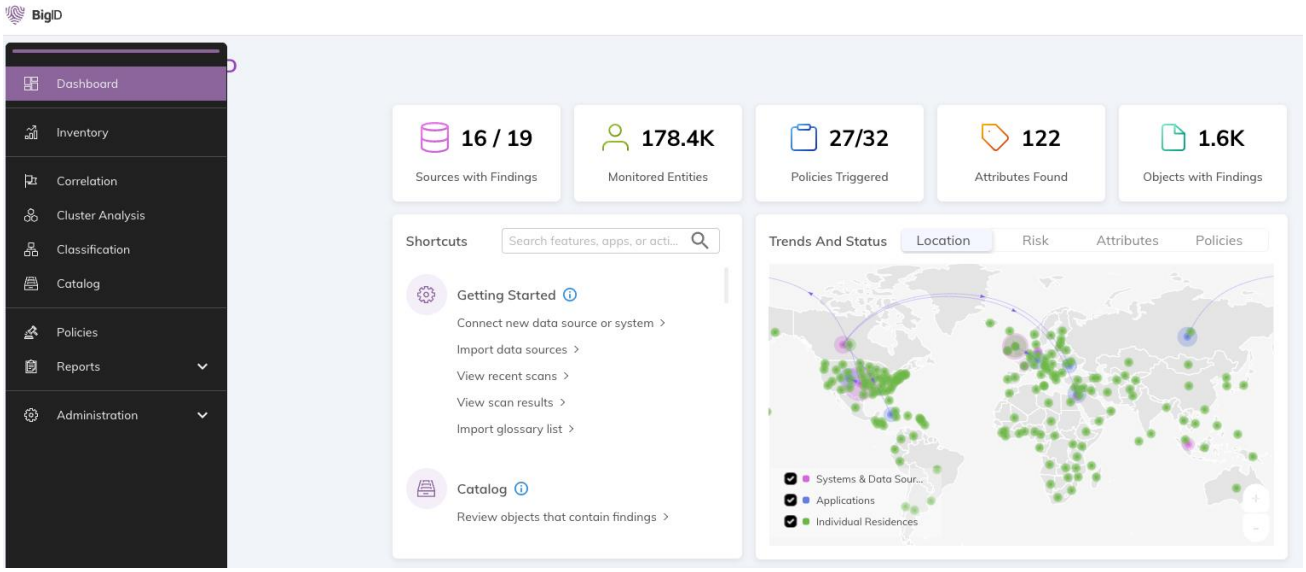
Step 3: Post launch verification

Once the cross-account roles are successfully created, work with your BigID representative to setup the scanners on these accounts as per your business needs.

- Work with the BigID Services team to install BigID application and BigID scanners as applicable in your environment (based on your corporate policies, latency needs and sizing estimations). All BigID components are deployed as container images and managed either via Docker-Compose on AWS EC2 OR using a Kubernetes on AWS EKS.
- Configure a BigID Scanner (on EC2 or EKS) and ensure they are mapped to the AWS IAM Role created using the template mentioned above (default BigIDScannerRole)
- Always choose the "IAM Role Authentication" method while creating any AWS data-sources.



- Login to your BigID dashboard to get the consolidate view of your data attributes across multiple AWS accounts as shown below.



Note: The IAM policy created as part of this solution is just a starter policy, please review it thoroughly with your System-Admin/DevOps team.

FAQs

Effect of AWS Control-Tower integration on BigID Data-Sources configuration process?

The AWS Control-Tower integration helps simplify the credentials setup during BigID Data-Sources configuration process. AWS Data-Sources within BigID will be configured in a similar way as earlier, i.e., users will still specify details of the data-sources e.g., to add AWS S3 as a data-source, users will need to provide the S3 bucket and/or folders details. However, users will choose the "IAM Role Authentication" option to configure credentials instead of "Credentials Authentication". This approach of configuring credentials assumes the applicable IAM Roles with appropriate read-only access policies to the applicable data-sources has been auto-provisioned by AWS Control-Tower.

Additional resources

If you are new to AWS, see Getting Started with AWS.

Learn more about AWS Marketplace.

To get started with AWS Control Tower, check out Getting Started with Control Tower.

Partner contact information

For questions regarding BigID offerings on AWS Marketplace, please visit https://bigid.com/contact/.

BigID documentation

General BigID Documentation

General Installation Documentation

AWS EC2 Installation Documentation

AWS EKS Installation Documentation