Asset and Inventory Discovery

Discovery is an important component of Multicloud Defense's approach of **"Discover, Deploy and Defend"**.

Discovery provides real-time visibility into the current resources deployed in any onboarded cloud accounts. In addition, it provides an interface into VPC flow logs and DNS logs to give a complete picture of your cloud deployment. The Multicloud Defense Controller, through the permissions granted to the IAM role (AWS), AD app registration (Azure) or the service account (GCP), periodically crawls your cloud resources, and also keeps tab on the changes, to maintain an "evergreen" inventory model of the resources.

Using the **Discovery** tab, you have the ability to see the attributes of your resources and how they are interconnected. Multicloud Defense collates this information into a succinct view of the security posture of all your resources with respect to the configuration and with context to the traffic flows.

Discovery Summary

The Dicsovery Summary page is a collection of widgets that summarize the available traffic and inventory. You can use the **Filter** at the top of the page to change the history of the widgets.

Traffic Summary Widgets

Currently, Multicloud Defense presents a condensed block of the traffic in two widgets: one for DNS traffic and one for VPC and VNet flow logs. These windows into traffic differentiate between malicious traffic and DNS or VPC/VNet traffic, respectively. Click inside either of these widgets to zoom into a specific time frame.

You can enable or disable logs on either of these widgets from this summary page by simply clicking the **Logs** toggle. For more information on either of these types of logs and the traffic that is compiled, see Types of Traffic

Discovery Summary

The Discovery summary is a series of windows of inventory recovered by Multicloud Defense as part of the discovery process when connecting your cloud service provider. These statistics are condensed here for a quick preview. To see these in more detail, see Inventory, on page 2

Inventory

Through permissions granted to the IAM role (AWS), AD app registration (Azure) or the service account (GCP), Multicloud Defense continuously maintains an "evergreen" inventory model of the cloud resources as well as real-time discovery that exists in your cloud service provider accounts, subscriptions and projects that are relevant to apply advanced network security. Once discovered, the resources are available in workflows that enable administrators to quickly deploy security rules to mitigate risks of exposed applications. Any activity is immediately reported through the Multicloud Defense Controller.

When inventory is enabled, Multicloud Defense Controller will perform a full inventory discovery periodically. The default is 60 minutes, but is tunable). Real-time inventory discovery is enabled on regions where the CloudFormation template was deployed.

Part of the discovery process highlights the logs of each cloud service provide. Note the following types of logs per service provider:

- **AWS** - VPC flow logs, Mount53 flow logs, and DNS logs.
- **Azure** - NSG flow logs.
- **GCP** - VPC flow logs.

Note that Multicloud Defense does note provide the same level of support for all cloud service providers.

Applications

Application shows all load balancers and API gateways for the cloud accounts. Under the Applications section of **Inventory**, there are three filter buttons: **Known Tags**, **Tags**, and **Applications**. Within **Applications**, users can invoke a workflow to create and apply protection for the specific application.

Application Tags

Create a list of **Application Tags** used to identify applications. During the inventory discovery stage, all discovered load balancers that have the specified tags are treated as applications.

As an example, you can assign the **Application Tags** to all load balancers that act as applications. The value of this tag is shown as the **Application Tags** in the discovered inventory. See the table below as a visual example:

Load Balancer	Tag	Value
Load Balancer 1	ApplicationName	Billing
Load Balancer 2	ApplicationName	UserManagement

The discovered inventory will show the **Billing** and **UserManagement** applications in the discovered application assets.

To create a list of **application tags**, click **Create**.

Parameter	Description
Name	Pre-populated.

Parameter	Description
Description	User-specified description.
Value	The tag value that will be used assign to the load balancers.

For more information on application tags, see Application Tags.

Known Tags

Known Tags show applications identified by application Load Balancers in your cloud account that the administrator has identified by a known tag. These known tags are listed in **Settings** > **Management** > **Account** > **Application Tags**.

Tags

Tags shows all applications identified by application load balancers with fields showing the tag keys and tag values and whether these applications are secured by Multicloud Defense Gateways.

Discovered Assets

When you enable inventory discovery in regions for your cloud account, the Multicloud Defense Controller continuously discovers cloud assets. To view the discovered assets, navigate to **Discover** or **Manage** > **Inventory**. The default views show the discovered assets for all cloud accounts. To filter to a specific cloud account, use the **Select Account** to specify a particular cloud account and view discovered assets.

The discovered asset categories and what they refer to are as follows:

- Security Groups - AWS Security Groups (SGs) and Azure Network Security Groups (NSGs).
- Network ACL - AWS Network Access Control Lists (NACLs).
- Subnets.
- Route Tables.
- Network Interfaces.
- VPCs/VNets - AWS VPCs, Azure VNets and GCP VPCs.
- Applications - Applications are identified by AWS Application Load Balancers (ALBs).
- Load Balancers.
- Instances - AWS Instances, Azure Virtual Machines and GCP Compute Instances.
- Tags - AWS Tags, Azure Tags and GCP Labels.
- Certificates - AWS Certificates Manager (ACM) certificates.

Enable Asset Discovery and Inventory

To enable discovery of assets in your cloud account:

Step 1 Navigate to **Manage** > **Accounts**.

Step 2 Select the checkbox next to the cloud account and click **Manage Inventory**.

Step 3 Select the **Regions** where you have cloud assets that you would wish Multicloud Defense to discover. The refresh interval is the time in minutes after which the inventory is refreshed (recommended default of 60 min). Multicloud Defense also performs continuous discovery using the cloud service provider's APIs and events instead of a regular poll. The refresh time interval specified here is for a full re-crawl; this reconciles all assets for any missed events during real time discovery.

Note that different refresh intervals can be defined for different regions by adding a new row and selecting the desired regions. A region can belong to a single refresh interval only.

Step 4 Click **Finish** to save.

Note The Multicloud Defense Controller will request the asset inventory for the newly added region immediately after saving.

What to do next

To review the discovered assets, navigate to **Manage** > **Inventory**.

Security Insights

Insights are a rules-based evaluations of assets discovered in AWS, Azure and GCP that are presented asfindings. Insights can be used without deploying Multicloud Defense Gateways since they operate on the periodic and real-time inventory monitoring accommodated by the Multicloud Defense Controller.

Step 1 In the Multicloud Defense Controller interface, click **Add Account**. As an alternative, we strongly recommend using the Easy Setup wizard to connect to an account. Go through the steps to connect the account.

Step 2 Once the account is connected and onboarded, Enable Asset Discovery and Inventory.

Step 3 Navigate to **Discover** > **Discovery Summary**. This page displays a summary view of all discovered assets and the **Insight Findings**.

Types of Security Insights

Read through the following types of security insights to understand what the dashboard can do.

Security Groups

Customers often struggle with the proliferation of **Security Groups**. Security groups are often shared amongst resources that could present risk. Changes made to a security group intended for a specific resource could impact a larger group of resources.

Security groups provides a list of all security group, their details and the set of resources utilizing the security group. The **Is Inbound Public** and **Is Outbound Public** fields indicate security groups configured with 0.0.0.0/0.

In the search window, define the search criteria based on fields and their values with the option to create a rule based on the search criteria.

Rules

Rules provide a view of security groups based on their configured Inbound and outbound rules.

Ports

Ports provide a view of security groups based on their configured inbound and outbound ports.

Application Security Groups

Application Security Groups are an Azure construct similar to the AWS security group. Azure application security groups have a member of the security group that contains that system and it's interfaces. It has both membership and security controls. As a result, Multicloud Defense uses this membership construct to build dynamic policies. Create and use an application secuirty group within an Azure environment, Multicloud Defense recognizes the change and adapts the policy to incorporate it.

For more information about Azure's application security groups and how they operate, see the Microsoft Azure documentation.

Network ACL

Network access control list (ACL) provides a list of all network ACLs and their details. The **Is Inbound Public** and **Is Outbound Public** fields indicate network ACLs configured with 0.0.0.0/0.

Rules

Rules provide a view of network ACLs based on their configured inbound and outbound rules.

Subnets

Subnets provides a list of all subnets and their details. The **Is Public** field indicate subnets that are publicly accessible based on whether auto-assign public IP is enabled.

Route Tables

Route Tables provides a list of all route tables and their details. The **Is Inbound Public** and **Is Outbound Public** fields indicate route tables that are configured to provide default access the internet.

Network Interfaces

Network Interfaces provides a list of all network interfaces and their details. The **Is Inbound Public** and **Is Outbound Public** fields indicate network interfaces that are configured with a security group that is open (0.0.0.0/0), or route tables that allows default access to the internet.

VPCs\VNets

VPCs/VNets provides a list of all VPCs/VNets and their details.

Applications

Applications provides a list of all deployed application load balancers and their details. The **Secured** field identifies whether a Multicloud Defense Gateway and security policy is applied to secure the application and offers an ability to invoke a workflow to protect the application.

Load Balancers

Load Balancers provides a list of all deployed application, network and gateway load balancers and their details. The **Public** field shows whether resource is an internet-facing load balancer. The **CSP WAF Enabled** shows whether a CSP WAF has been enabled for the application load balancer.

Instances

Instances provides a list of all instances along with summary information on the number of security groups and interfaces that are assigned and configured for the resource. The **Is Inbound Public** and**Is Outbound Public** fields indicate instances that have network interfaces that are configured with a security group that is open (0.0.0.0/0), or route tables that allows default access to the internet.

Tags

Tags provides a list of all VPCs/VNets, subnets, security groups, instances and load balancers that are configured with tags.

Certificates

Certificates provides a list of all certificates available in AWS certificates manager along with summary information on issuer, domain name and expiry date.

Topology

this tab shows a high-level map view by region of cloud assets in cloud accounts. You can finetune the visuals with the **Filter** bar at the top of the screen. From here you can determine what cloud service provider accounts you want to pull data drom, which region of the world, specific VNet or VPCs, instances, and a period of time in history.

The **Global View** of the world map allows you to scroll in for a closer look at specific regions that are dictated by the Filter bar mentioned above. Immediately to the left of the map you can dictate which types of traffic and inventory you want to view. Check and uncheck the boxes appropriately for what you want to see .

Insights

Insights are a rules-based evaluations of assets discovered in AWS, Azure and GCP that are presented as findings.

Rules

Rules are a set of evaluations to identify findings in discovered assets. Multicloud Defense provides a set of default rules. New rules can be created by selecting an inventory category (e.g., security groups, applications, load balancers, tags, etc.), defining a search criteria, selecting **Add Rule** and specifying additional required information. Navigate to **Insights** > **Rules** to view the new rule. From there you can operate against existing and newly discovered assets.

Findings

Findings is a list of discovered assets that match the defined set of rules.

Rules and Findings

Rules can be configured to place checks and guardrails on your cloud resources.

Rules and Findings

Rules can be configured to place checks and guardrails on your cloud resources.

Pre-Defined Rules

Multicloud Defense Controller has some basic pre-defined rules:

- Application load balancers with no cloud service provider WAF enabled.
- Security groups with few instances (< 5) that have ingress open. Lots of low utilization security groups can create gaps that are hard to see and may make it easy to exploit.
- Instances with two or more network interfaces.
- Security groups with open outbound (0.0.0.0/0) access.
- Public subnets - all AWS subnets with **Auto-Assign Public IP** enabled.
- Security groups with with too many egress ports (25 or more) open to the internet.
- Security ports with too many ingress ports (5 or more) open to the internet.
- Security groups with 65,535 ports open for ingress with public access enabled.
- Certificates expiring in 30 days - AWS Certificate Manager only.

The cloud resources that match the rules, will be flagged as findings with a matching severity.

For information on custom rules, see Pre-Defined Rules, on page 7.

Custom Rules

The user can configure additional rules for a resource.

1. Navigate to **Discovery** > **Inventory** and select a resource e.g. load balancers.
2. Create a rule criteria in the text area and select **Add Rule**.
3. Enter content for the following entries and the number of finding meeting the rule criteria.
    - Name
    - Description
    - Severity

- Default Action
- Type
- Account

4. Click **Save**.

The default action of the rule can be either **info** or **alert**. If a rule is configured with a default action of alert, then any new findings for the rule results in an alert notification from the Multicloud Defense Controller. The following configurations are required if you want a default action of alert.

- Configure **Alert Profile** to indicate if the user wants ServiceNow, PagerDuty, or Webhook notifications.
- Configure **Alert Rule of type Discovery** and sub-type **Insights Rule** with the level of severity specified.

Findings

Based on the pre-defined and custom rules, you can view the findings for the resources. For easy access, the **Findings Summary** is located in the dashboard, and also in the Summary view in the Inventory tab.