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 Discovery, 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.

Inventory

Through permissions granted to the IAM role (AWS), AD app registration (Azure) or the service account (GCP), Multicloud Defense will continuously maintain an "evergreen" inventory model of the Cloud resources that exist in your Cloud Service Provider accounts, Subscriptions and Projects that are relevant to apply advanced network security. Once discovered, the resources are then made available in workflows that enable Administrators to quickly deploy Security Rules to mitigate risks of exposed applications.

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

Enable 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 Cloud Provider 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.

Step 4 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 5 Click **Finish** to save.

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

To review the discovered assets:

Navigate to **Manage** > **Inventory**.

Discovered Assets

By enabling Inventory in Regions for your Cloud Account, the Multicloud Defense Controller will continuously discover 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 for the selected Cloud Account.

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

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

Applications

Under the Applications section of **Inventory**, there are three (3) filter buttons: **Known Tags**, **Tags**, and **Applications**. Within **Applications**, users can invoke a workflow to create and apply protection for the specific application.

Known Tags

Known Tags shows applications identified by Application Load Balancers in your cloud account that the Administrator has identified by a known tag. These known tags are specified in the **Settings** > **Management** > **Account** > **Application Tags**.

Link for more information on how to configure 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.

Application

Application shows all Load Balancers and API Gateways for the Cloud accounts.

Security Insights

Insights are a Rules-based evaluations of assets discovered in AWS, Azure and GCP that are presented as Findings. 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. To leverage Insights, add a Cloud Account and enable Inventory Monitoring Regions.

Summary

Navigate to **Discover** > **Discovery Summary** to display a summary view of all discovered assets and the Insight Findings:

1. Network ACL.
2. Application Security Group.
3. Security Groups.
4. Subnets.
5. Route Tables.
6. Network Interfaces.
7. VPCs/VNets.
8. Applications.
9. Load Balancers.
10. Instances.

11. Tags.
12. Certificates.

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 Groups, 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.

Network ACL

Network 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 aMulticloud 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

Shows a high level map view by Region of Cloud assets in cloud accounts.

Insights

Insights are a Rules-based evaluations of assets discovered in AWS, Azure and GCP that are presented as Findings. 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. To leverage Insights, add a Cloud Account and enable Inventory Monitoring Regions.

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. The new Rule will appear in the Insights -> Rules and will 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 and Findings Overview

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:-

1. Application load balancers with no cloud service provider WAF enabled.
2. 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.
3. Instances with 2 or more network interfaces.
4. Security Groups with open outbound (0.0.0.0/0) access.
5. Public subnets - all AWS subnets with auto-assign public IP enabled.
6. Security groups with with too many egress ports (25 or more) open to the Internet.
7. Security ports with too many ingress ports (5 or more) open to the Internet.
8. Security Groups with 65,535 ports open for ingress with public access enabled.
9. 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.

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. Specify the Name, Description, Severity and Default Action, Catergory, Resource Type, Account and the number of finding meeting the Rule criteria.

4. Save the Rule.

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.

1. Configure Alert Profile to indicate if the user wants ServiceNow, PagerDuty, or Webhook notifications.
2. Configure Alert Rule of type Discovery and sub-type Insights Rule, and specify the severity.

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 on the Dashboard, and also in the Summary view in the Inventory section. The user can get information on all the resources that have associated Findings.

Enable DNS Logs

AWS: Enable DNS Logs

If you provided a S3 Bucket during the stack creation from the CloudFormation template in the previous section, a S3 bucket is created by the template that acts as the destination for the Route53 Query Logs. The VPCs that are monitored for the DNS query logs must be added manually.

Step 1 In AWS Console go to the Route53Query Logging .

Step 2 Select the Query Logger created by the template (Look for the logger with the Prefix name provided in the template).

Step 3 Select and add all the VPCs for which you want to get the traffic insights.

a. Click **Log queries for VPCs** or **Add VPC** under the *VPCs that queries are logged for* section.

b. Select all the VPCs and click **Choose**.

Azure: DNS Logs

Azure currently does not expose DNS log queries. Multicloud Defense Controller cannot enable logs for this cloud service provider.

GCP: Enable DNS Logs

To enable GCP DNS query logs, follow the below steps.

Step 1 Navigate to VPC network in GCP console.

Step 2 Open Google cloud shell and execute this command:

```
gcloud dns policies create POLICY_NAME --networks=NETWORK --enable-logging
```

Step 3 Navigate to **Cloud Storage** section and create a storage bucket. You can leave everything as default when creating storage bucket.

Note *Both DNS and VPC logs can share the same cloud storage bucket.*

Step 4 Navigate to **Logs Route** section.

Step 5 Click on **Create Sink**.

Step 6 Provide a sink name.

Step 7 Select "Cloud Storage bucket" for sink service.

Step 8 Select the cloud storage bucket that was created above.

Step 9 In "Choose logs to include in sink" section, put in this string: `resource.type="dns_query"`.

Below steps are the same as mentioned in VPC flow log for GCP. If you are sharing cloud storage bucket, you only need to perform below steps once.

Step 10 Click **Create Sink**.

Step 11 Navigate to **IAM** > **Roles**.

Step 12 Create a custom role with this permission: **storage.buckets.list**.

Step 13 Create another custom role with following permission:

storage.buckets.get storage.objects.get storage.objects.list.

Step 14 Add both custom role to the service account created for Multicloud Defense Controller. When adding the second custom role, put this condition:

```
(resource.type == "storage.googleapis.com/Bucket" || resource.type ==
 "storage.googleapis.com/Object") &&
resource.name.startsWith('projects/_/buckets/<cloud storage name>')
```

Step 15 Navigate to **Pub/Subs**.

Step 16 Click on **Create Topic**.

Step 17 Provide a Topic name and click **create**.

Step 18 Click on **Subscriptions**. You will find that there is a subscription created for the topic that was just created.

Step 19 Edit the subscription.

Step 20 Change Delivery type as **Push**.

Step 21 Once **Push** is selected, enter in the endpoint URL: `https://prod1-webhook.vtxsecurityservices.com:8093/webhook/<tenant name>/gcp/cloudstorage`. Tenant name is assigned by Multicloud Defense. To view tenant name, navigate to Multicloud Defense Controller and click on your username.

Step 22 Click **Update**.

Step 23 Create a cloud storage notification by opening a Google cloud shell and execute this command: `gsutil notification create -t <TOPIC_NAME\> -f json gs://<BUCKET_NAME>`.

Enable VPC Flow Logs

AWS: Enable VPC Flow Logs

If you provided a S3 Bucket during the stack creation from the CloudFormation template in the previous section, a S3 bucket is created by the template that acts as the destination for the VPC Flow Logs. Flow logs must be enabled for each of the VPCs.

Step 1 Go to the VPCs section on the AWS Console.
Step 2 Select the VPC and select the **Flow Logs** tab for that VPC.
Step 3 Select **All** as theFilter.
Step 4 Select **Send to an Amazon S3 bucket** as the Destination.
Step 5 Provide the S3 Bucket ARN copied from the Outputs of the CloudFormation template stack.
Step 6 Choose **Custom Format** as the Log Record Format.
Step 7 Select all the fields from the Log Format dropdown.
Step 8 Click **Create Flow Log**.

Azure: Enable NSG Flow Logs

Step 1 Go to **Resource Groups** section in Azure portal.
Step 2 Click on **create** button.
Step 3 Select the subscription and provide a name for this new resource group.
Step 4 Select a **region**. (example: (US) East US).
Step 5 Click "**Review + create** " button.
Step 6 Go to **storage accounts** section.
Step 7 Click on **Create** button.
Step 8 Select subscription and resource group that was just created.
Step 9 Select the same region as the resource group.
Step 10 Provide a name for the storage account.
Step 11 Redundancy **CANNOT** be locally-redundant storage(LRS).
Step 12 Click "**Review + create** " button. This will create a storage account where nsg flow log will be stored.
Step 13 Go to **subscription** section and find your subscription.
Step 14 Navigate to **resource providers**.
Step 15 Ensure that **microsoft.insights** and **Microsoft.EventGrid** providers are registered. If they are not registered, click on **Register** button.
Step 16 Go to **Network Watcher** section.
Step 17 Click on Add and add the regions that you want nsg flow logs to be enabled.
Step 18 Go to **Network Watcher** > **NSG flow logs**.

Step 19 Create flow logs for the NSG where you want to enable NSG flow log. Provide the storage account created above and retention days as 30.

Step 20 Navigate to the storage account created and click on **Events**.

Step 21 Click on **Event Subscription**.

Step 22 Provide a name for this event subscription.

Step 23 Select the resource group that was created above.

Step 24 Provide a System Topic Name.

Step 25 For Filter to Event Types, default is "**Blob Created**" and "**Blob Deleted**".

Step 26 For Endpoint Type, select "**Web Hook**".

Step 27 Click on the "Select an endpoint" link.

Step 28 Subscriber Endpoint is `https://prod1- webhook.vtxsecurityservices.com:8093/webhook/<tenant_name>/azure`. Tenant name is assigned by Multicloud Defense. You can find tenant name by clicking on the username in Multicloud Defense Controller.

GCP: Enable VPC Flow Logs

To enable GCP VPC flow logs, follow the below steps.

Step 1 Navigate to VPC network in GCP console.

Step 2 Select the subnet to enable VPC flow log.

Step 3 Ensure that flow logs is turned on. If it is off, click on edit and turn flow logs on.

Step 4 Turn on flow log on all subnets where you want to enable flow log.

Step 5 Navigate to **Cloud Storage** section and create a storage bucket. You can leave everything as default when creating storage bucket.

Note *Both DNS and VPC logs can share the same cloud storage bucket*.

Step 6 Navigate to **Logs Route** section.

Step 7 Click on **Create Sink**.

Step 8 Provide a sink name.

Step 9 Select "Cloud Storage bucket" for sink service.

Step 10 Select the cloud storage bucket that was created above.

Step 11 In "Choose logs to include in sink" section, put in this string: `logName:(projects/<project-id>/logs/compute.googleapis.com%2Fvpc_flows)`

Below steps are the same as mentioned in DNS query log for GCP. If you are sharing cloud storage bucket, you only need to perform below steps once.

Step 12 Click Create Sink.

Step 13 Navigate to **IAM** > **Roles**.

Step 14 Create a custom role with this permission: **storage.buckets.list**.

Step 15 Create another custom role with following permission: storage.buckets.get storage.objects.get storage.objects.list.

Step 16 Add both custom role to the service account created for Multicloud Defense Controller. When adding the second custom role, put this condition:

```
(resource.type == "storage.googleapis.com/Bucket" || resource.type ==
"storage.googleapis.com/Object") && resource.name.startsWith('projects/_/buckets/<cloud
storage name>')
```

Step 17 Navigate to **Pub/Subs**.

Step 18 Click on **Create Topic**.

Step 19 Provide a Topic name and click create.

Step 20 Click on **Subscriptions**. You will find that there is a subscription created for the topic that was just created.

Step 21 Edit the subscription.

Step 22 Change Delivery type as **Push**.

Step 23 Once **Push** is selected, enter in the endpoint URL:`https://prod1-webhook.vtxsecurityservices.com:8093/webhook/<tenant name>/gcp/cloudstorage`. Tenant name is assigned by Multicloud Defense. To see tenant name, navigate to Multicloud Defense Controller and click on your username.

Step 24 Click Update.

Step 25 Create a cloud storage notification by opening a Google cloud shell and execute this command: `gsutil notification create -t <TOPIC_NAME> -f json gs://<BUCKET_NAME>`.