Prisma Cloud
IBM Cloud
Onboarding

Limited GA

PCS 23.8.2

408.753.4000 | 3000 Tannery Way, Santa Clara, CA 95054 | paloaltonetworks.com

Table of Contents

Overview

Prisma™ Cloud enables you to protect your resources deployed on the IBM Cloud infrastructure from a single console. When you add your IBM Cloud accounts on Prisma Cloud, you get complete visibility and control over potential risks within your IBM Cloud infrastructure across all the Multi-Zone Regions (MZR).

With Prisma Cloud, you can manage vulnerabilities, ensure compliance, and provide runtime defense for your resources in the IBM Cloud.

IBM Cloud Account Onboarding

To monitor your IBM resources, you first need to add your IBM Cloud accounts to Prisma Cloud. You can also access the Prisma Cloud Terraform Registry to onboard multiple IBM Cloud accounts. You must have administrator access to an IBM account to enable **read** permissions for Prisma Cloud.

Prisma Cloud uses the Terraform file to create a service ID and an API key with the required permissions for all the supported IBM services.

After you add your IBM Cloud account to Prisma Cloud, the API integration between IBM and Prisma Cloud is established, and you can monitor resource configuration issues using RQL and alerts.

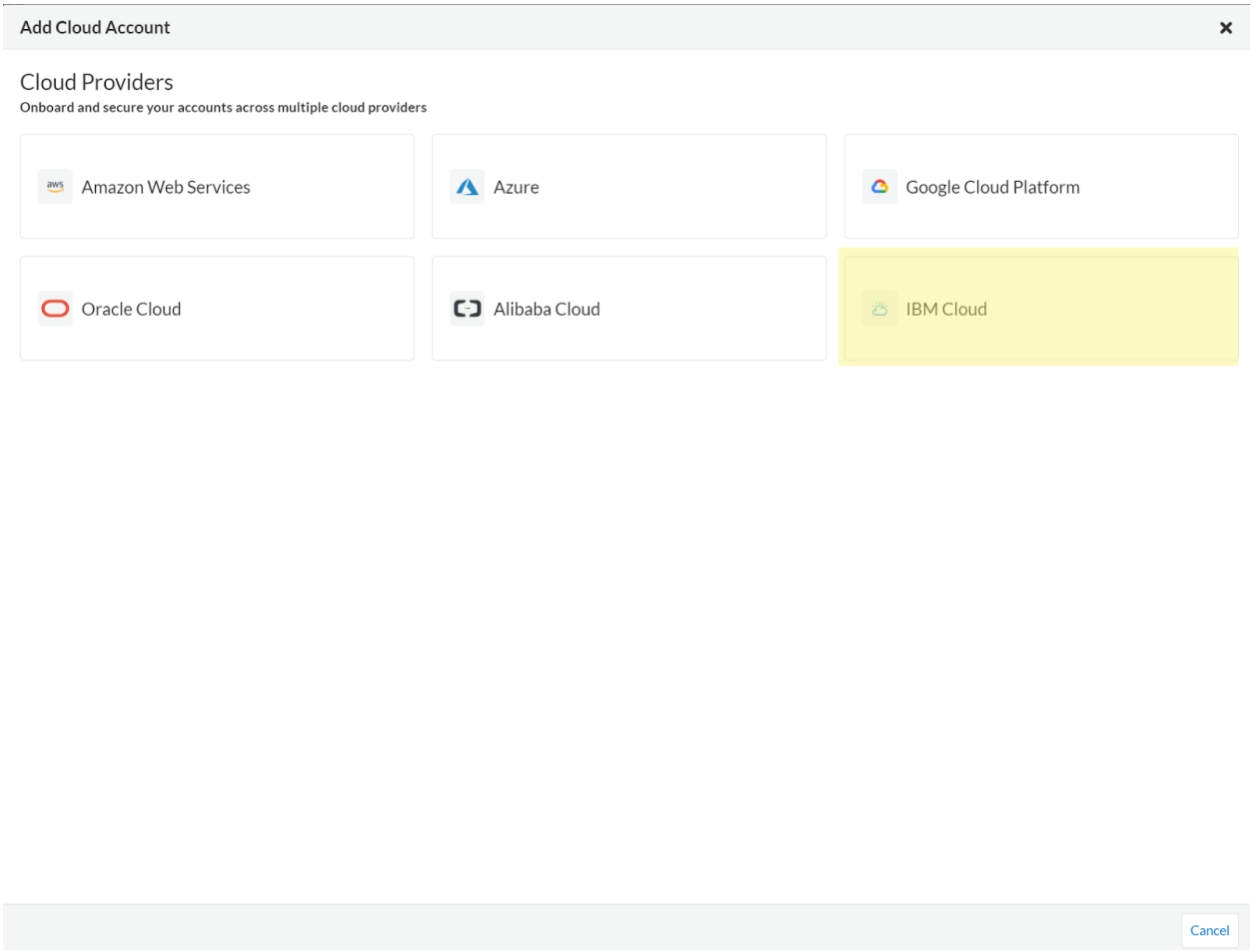
Prisma Cloud supports the ingestion of Configuration (Config) logs to identify IBM resource configuration issues.

> **Note:** Ingestion of IBM flow logs, audit event logs, and ingestions for the IBM Classic Infrastructure are not currently supported.

To begin monitoring your resources on IBM, you must complete the following steps:

Step 1: Add IBM Account

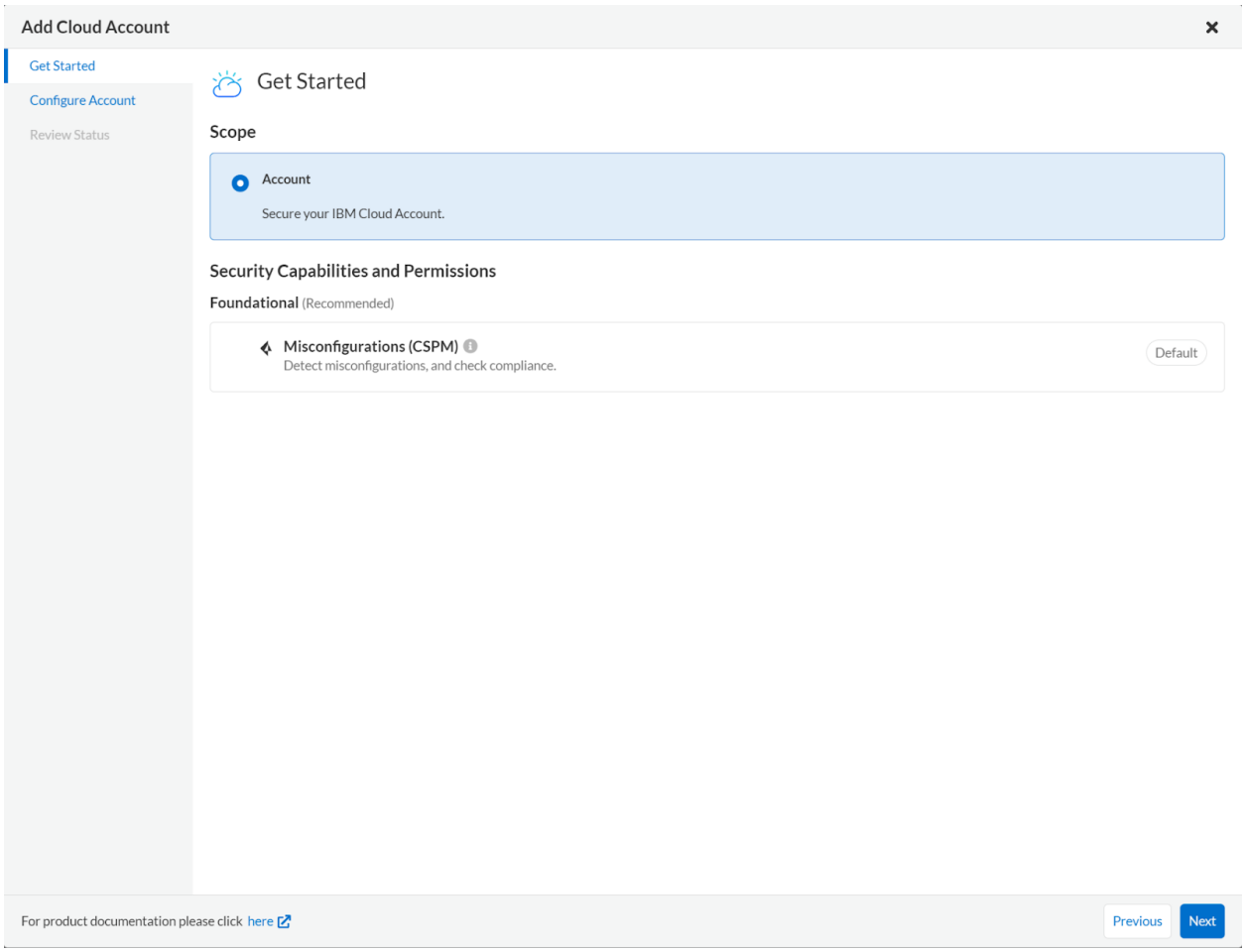
1. Access Prisma Cloud and select **Settings > Cloud Accounts > Add Cloud Account**.
2. Select **IBM Cloud** as the cloud account you want to onboard and **Get Started**.



3. Select **Account** under Scope.

   Note: Prisma Cloud does not support the onboarding of an IBM Enterprise account**.**

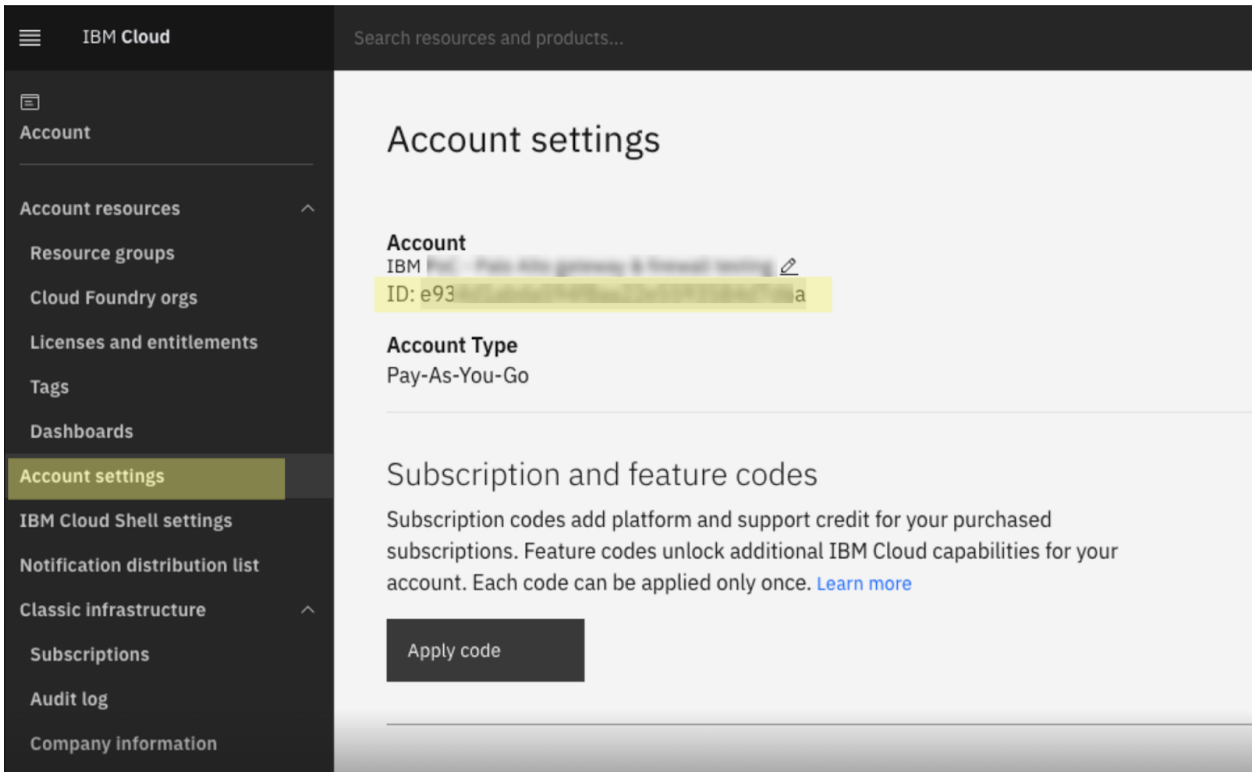
4. Under **Security Capabilities and Permissions**, the **Misconfigurations** capability is enabled by default. It grants the permissions required to scan cloud resources and ingest metadata.
5. Click **Next**.



Step 2: Configure Account

1. Enter your IBM Cloud **Account Id** from the IBM Cloud console.

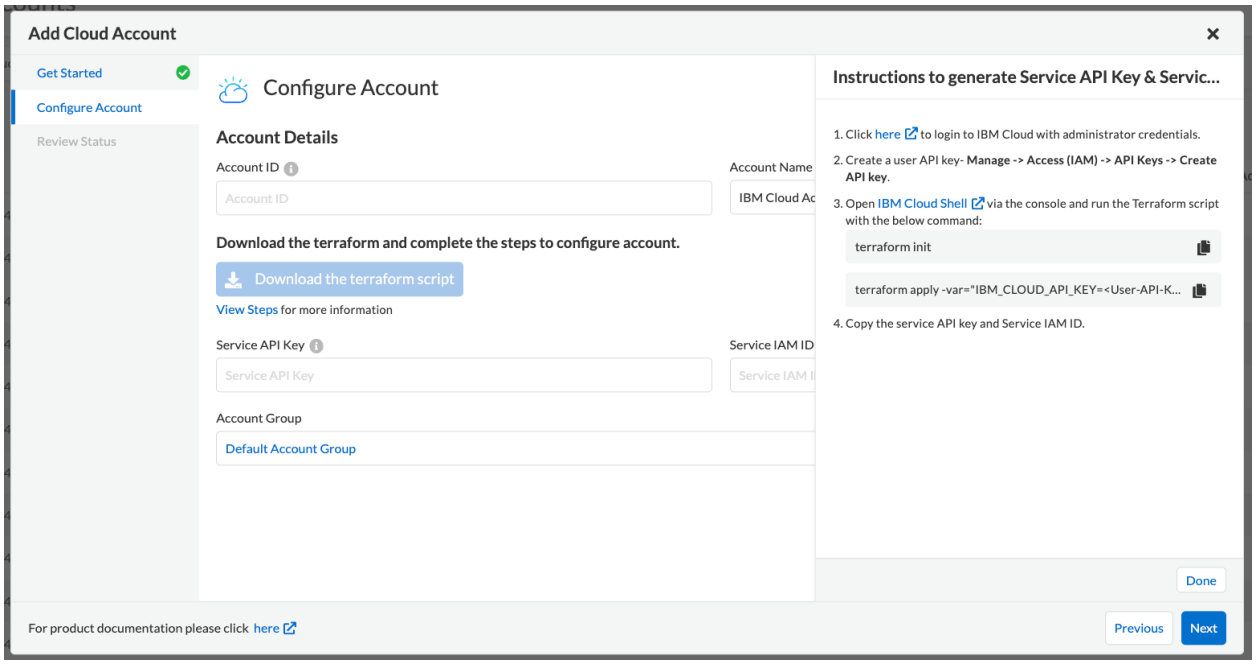
   You can find your `accountid` under **Manage > Account Settings.**

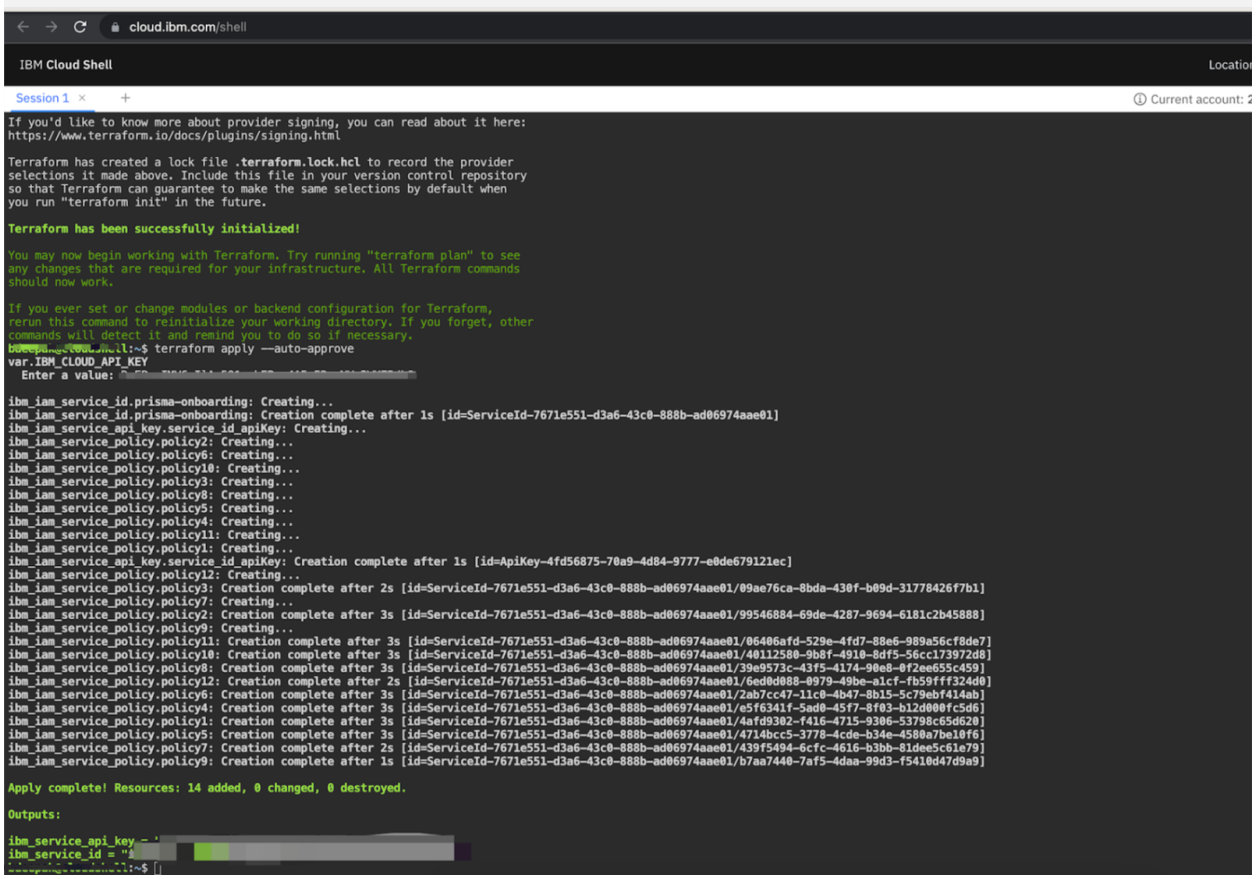


2. Enter a **Cloud Account Name.**

   A cloud account name uniquely identifies your IBM account on Prisma Cloud.

3. Download the Terraform script.
4. Click **View Steps** to follow the steps to generate the Service API Key and Service IAM ID from the IBM Cloud shell.

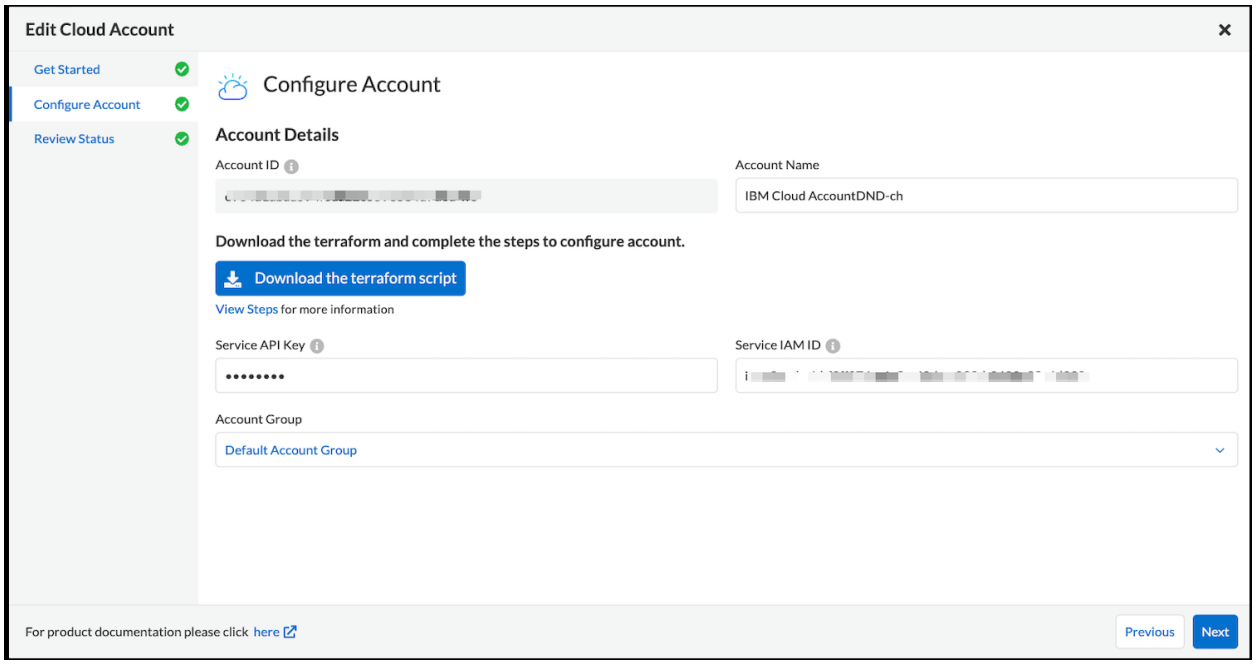

Add Cloud Account
Get Started
Configure Account
Review Status
Configure Account
Account Details
Account ID
Account Name
Download the terraform and complete the steps to configure account.
Download the terraform script
View Steps for more information
Service API Key
Service IAM ID
Account Group
Default Account Group
Instructions to generate Service API Key & Servic...
1. Click here to login to IBM Cloud with administrator credentials.
2. Create a user API key- Manage -> Access (IAM) -> API Keys -> Create API key.
3. Open IBM Cloud Shell via the console and run the Terraform script with the below command:
terraform init
terraform apply -var="IBM_CLOUD_API_KEY=<User-API-K...
4. Copy the service API key and Service IAM ID.
Done
For product documentation please click here
Previous
Next


cloud.ibm.com/shell
IBM Cloud Shell
Session 1
If you'd like to know more about provider signing, you can read about it here:
https://www.terraform.io/docs/plugins/signing.html
Terraform has created a lock file .terraform.lock.hcl to record the provider
selections it made above. Include this file in your version control repository
so that Terraform can guarantee to make the same selections by default when
you run "terraform init" in the future.
Terraform has been successfully initialized!
You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.
If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
terraform apply --auto-approve
var.IBM_CLOUD_API_KEY
Enter a value:
ibm_iam_service_id.prisma-onboarding: Creating...
ibm_iam_service_id.prisma-onboarding: Creation complete after 1s [id=ServiceId-7671e551-d3a6-43c0-888b-ad06974aae01]
ibm_iam_service_api_key.service_id_apiKey: Creating...
ibm_iam_service_policy.policy2: Creating...
ibm_iam_service_policy.policy6: Creating...
ibm_iam_service_policy.policy10: Creating...
ibm_iam_service_policy.policy3: Creating...
ibm_iam_service_policy.policy8: Creating...
ibm_iam_service_policy.policy5: Creating...
ibm_iam_service_policy.policy4: Creating...
ibm_iam_service_policy.policy11: Creating...
ibm_iam_service_policy.policy1: Creating...
ibm_iam_service_api_key.service_id_apiKey: Creation complete after 1s [id=ApiKey-4fd56875-70a9-4d84-9777-e0de679121ec]
ibm_iam_service_policy.policy12: Creating...
ibm_iam_service_policy.policy3: Creation complete after 2s [id=ServiceId-7671e551-d3a6-43c0-888b-ad06974aae01/09ae76ca-8bda-430f-b09d-31778426f7b1]
ibm_iam_service_policy.policy7: Creating...
ibm_iam_service_policy.policy2: Creation complete after 3s [id=ServiceId-7671e551-d3a6-43c0-888b-ad06974aae01/99546884-69de-4287-9694-6181c2b45888]
ibm_iam_service_policy.policy9: Creating...
ibm_iam_service_policy.policy11: Creation complete after 3s [id=ServiceId-7671e551-d3a6-43c0-888b-ad06974aae01/06406afd-529e-4fd7-88e6-989a56cf8de7]
ibm_iam_service_policy.policy10: Creation complete after 3s [id=ServiceId-7671e551-d3a6-43c0-888b-ad06974aae01/40112580-9b8f-4910-8df5-56cc173972d8]
ibm_iam_service_policy.policy8: Creation complete after 3s [id=ServiceId-7671e551-d3a6-43c0-888b-ad06974aae01/39e9573c-43f5-4174-90e8-0f2ee655c459]
ibm_iam_service_policy.policy12: Creation complete after 2s [id=ServiceId-7671e551-d3a6-43c0-888b-ad06974aae01/6ed0d088-0979-49be-a1cf-fb59fff324d0]
ibm_iam_service_policy.policy6: Creation complete after 3s [id=ServiceId-7671e551-d3a6-43c0-888b-ad06974aae01/2ab7cc47-11c0-4b47-8b15-5c79ebf414ab]
ibm_iam_service_policy.policy4: Creation complete after 3s [id=ServiceId-7671e551-d3a6-43c0-888b-ad06974aae01/e5f6341f-5ad0-45f7-8f03-b12d000fc5d6]
ibm_iam_service_policy.policy1: Creation complete after 3s [id=ServiceId-7671e551-d3a6-43c0-888b-ad06974aae01/4afd9302-f416-4715-9306-53798c65d620]
ibm_iam_service_policy.policy5: Creation complete after 3s [id=ServiceId-7671e551-d3a6-43c0-888b-ad06974aae01/4714bcc5-3778-4cde-b34e-4580a7be10f6]
ibm_iam_service_policy.policy7: Creation complete after 2s [id=ServiceId-7671e551-d3a6-43c0-888b-ad06974aae01/439f5494-6cfc-4616-b3bb-81dee5c61e79]
ibm_iam_service_policy.policy9: Creation complete after 1s [id=ServiceId-7671e551-d3a6-43c0-888b-ad06974aae01/b7aa7440-7af5-4daa-99d3-f5410d47d9a9]
Apply complete! Resources: 14 added, 0 changed, 0 destroyed.
Outputs:
ibm_service_api_key = "
ibm_service_id = "

Note: Once you run the Terraform script for the first time and if you need to re-run it for the same account, then you must manually perform the following steps:

1. Navigate to the **Manage > Access (IAM) > Roles** page in your IBM Cloud.
2. Search for the following custom roles and delete them:
   - Prismacustomroleiam
   - Prismacustomrolekms
   - Prismacustomrolesm

5. Paste the **Service API Key** and **Service IAM ID** in Prisma Cloud.

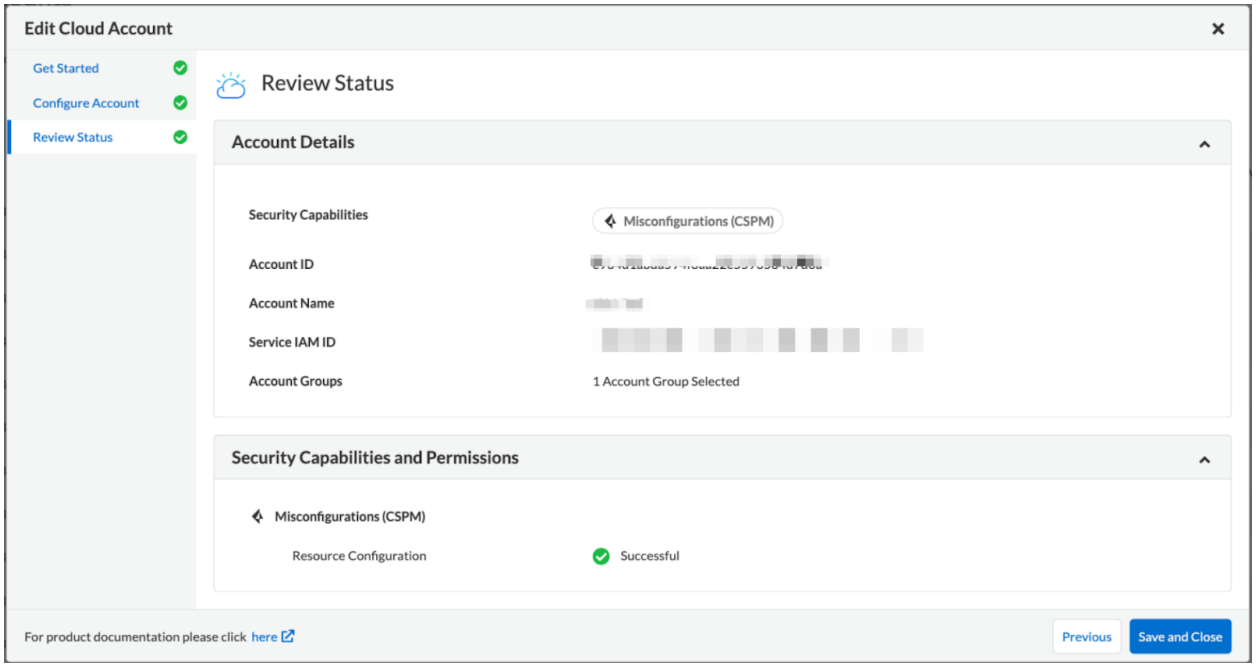


6. Select one or more account groups or select **Default Account Group**.

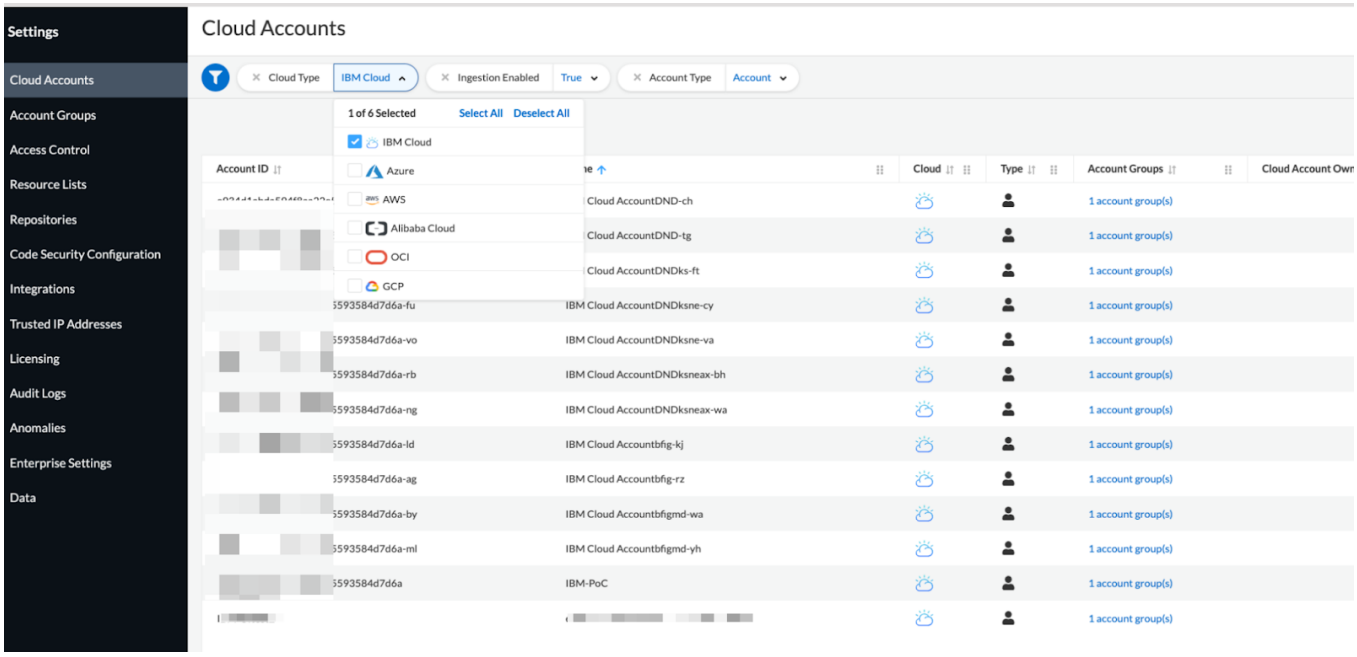
   You must assign each cloud account to an account group and create an Alert Rule for run-time checks to associate with that account group to generate alerts when a policy violation occurs.

7. Click **Next**.

Step 3: Review Status



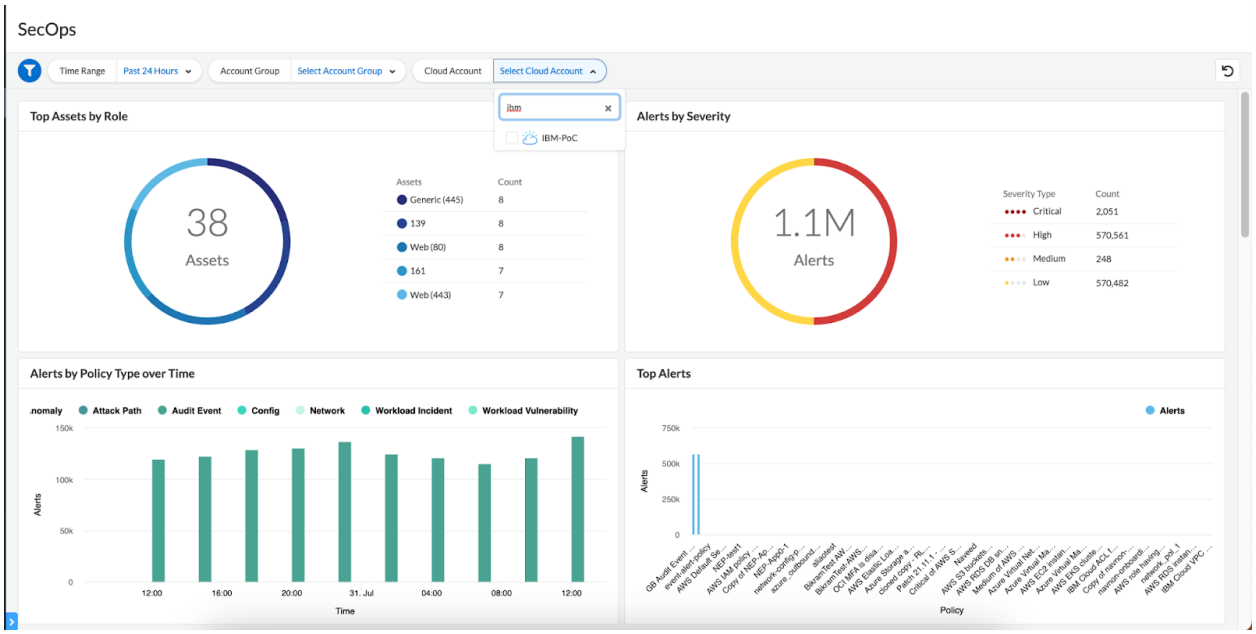
1. Verify the **Account Details** of the IBM account and status check for the Security Capabilities and Permissions.
2. Click **Save and Close** to complete onboarding.
3. After successfully onboarding the account, navigate to **Settings > Cloud Accounts** and set the **Cloud Type** filter to **IBM Cloud** to view your newly onboarded account.



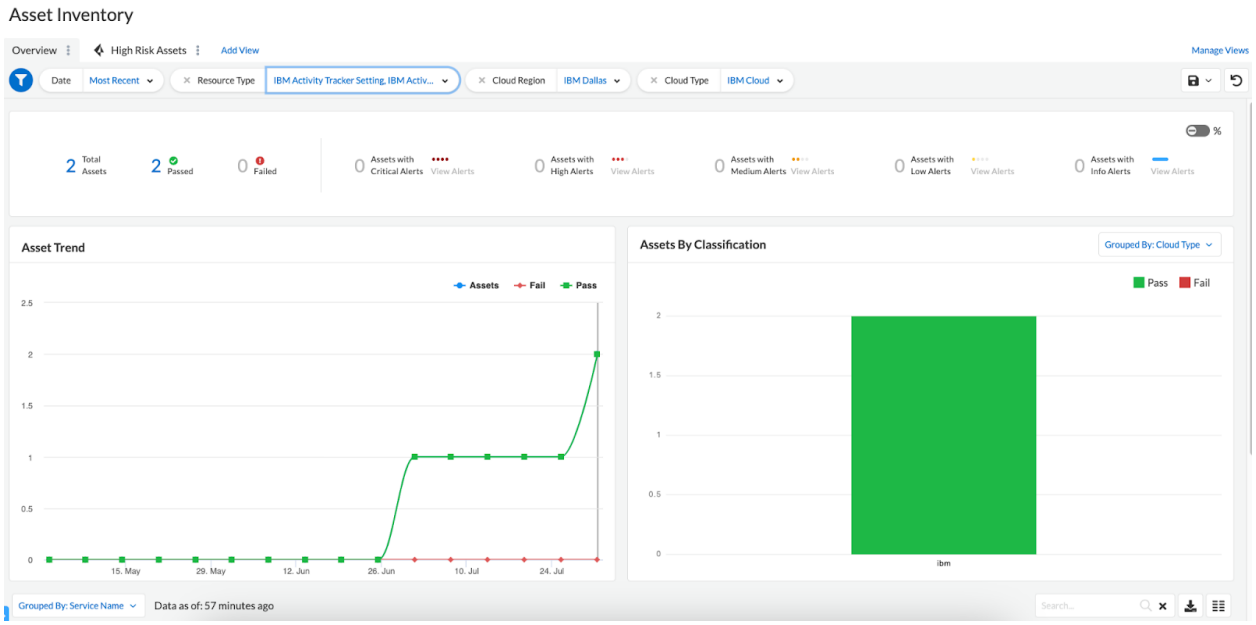
Next Steps

1. It can take up to an hour for the ingestion to complete after which you can view the resources in Prisma Cloud, review, and act on the alerts generated.

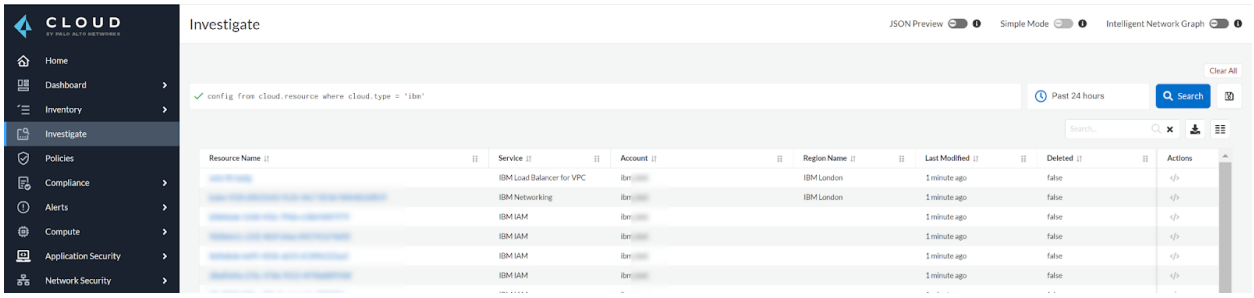
2. On the Prisma Cloud Dashboard, you can filter by IBM Cloud Accounts. Prisma Cloud supports only configuration ingestion for IBM Cloud accounts and displays only the relevant configuration ingestion data.



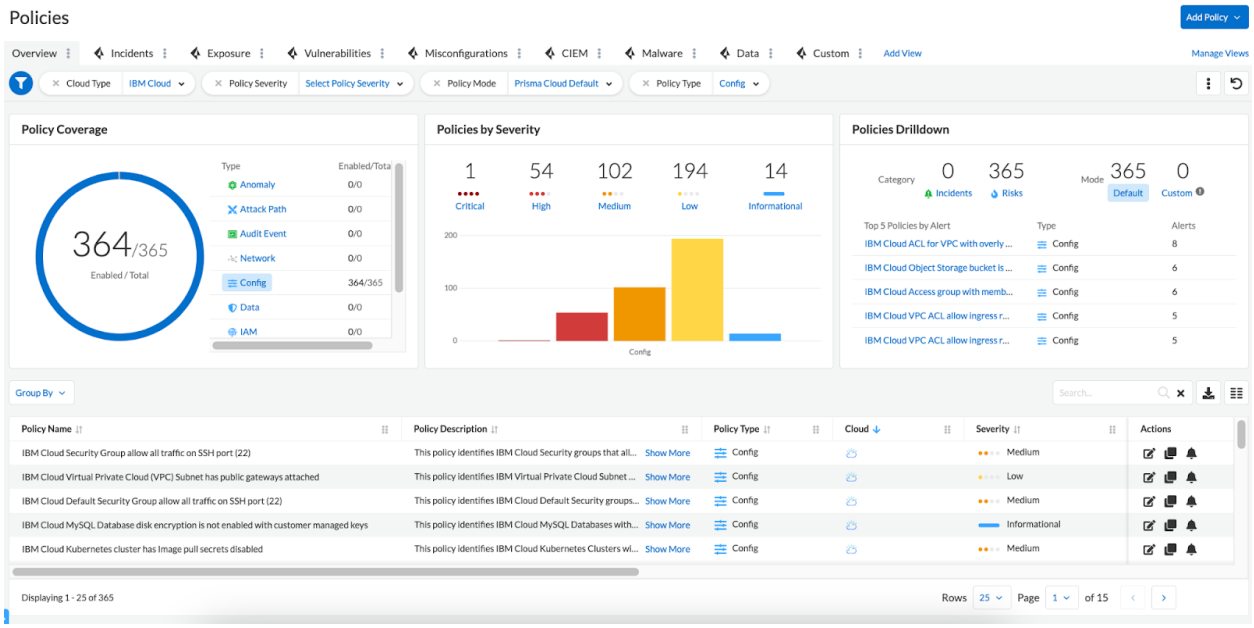
3. Start using the Prisma Cloud Asset Inventory for visibility. Set the Cloud Type filter as **IBM Cloud** to view the data for the supported services. You can also filter the data based on the IBM **Cloud Region** and **Resource Type** (Service name).



4. To verify if the configuration logs for your IBM Cloud-related resources have been analyzed, you can run a query on the **Investigate** page.

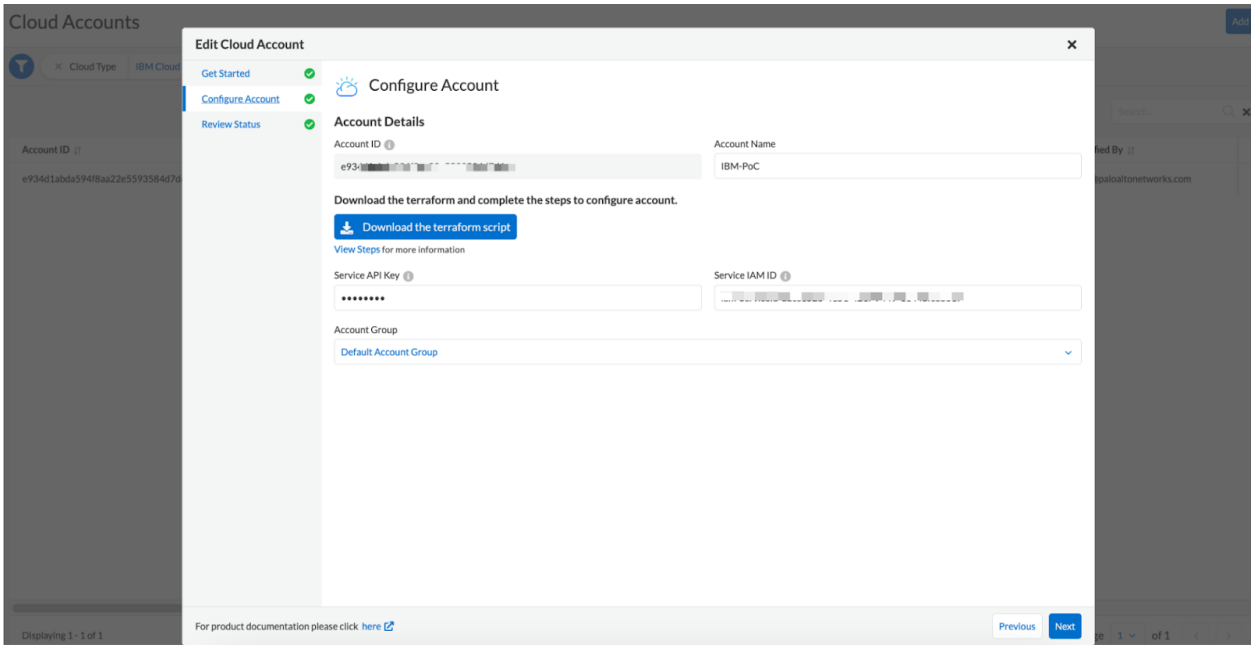


5. Review the Prisma Cloud default **Policies** for IBM Cloud. Set the **Cloud Type** filter as **IBM** Cloud and view all the Configuration policies that are available to detect any misconfiguration in your infrastructure.



6. Configure Alert Rule to include IBM policies.
7. To update the permissions of an already onboarded IBM Cloud account to ingest new APIs or to ingest additional attributes in the IBM Cloud API:
    a. Navigate to **Settings > Cloud Accounts**.
    b. Click the Edit icon for the account you want to update.

c. In the edit flow, download the Terraform script and perform steps 4 to 7 as listed in **Configure Account**.



Known Issues

When attempting to rerun the onboarding terraform script for the same account multiple times, an error occurs—`This role name has already been used, please update the existing one or change the role name.`

To address the error, follow these steps in your IBM Console:

1. Go to IBM Cloud and navigate to **Manage > Access (IAM) > Roles** page.
2. Search for the custom roles listed below and delete them:
    - Prismacustomroleiam
    - Prismacustomrolekms
    - Prismacustomrolesm

APIs Ingested by Prisma Cloud

To know the list of all the APIs that Prisma Cloud supports for retrieving data about the resources in your IBM Cloud environment, see the following table.

IBM Service	API	Permissions
IBM Networking	ibm-vpc	is.vpc.vpc.list is.vpc.vpc.read
IBM Networking	ibm-vpc-network-acl	is.network-acl.network-acl.list is.network-acl.network-acl.read
IBM Networking	ibm-vpc-network-security-group	is.security-group.security-group.list is.security-group.security-group.read
IBM Networking	ibm-vpc-network-subnet	is.subnet.subnet.list is.subnet.subnet.read
IBM Networking	ibm-vpc-network-public-gateway	is.public-gateway.public-gateway.list is.public-gateway.public-gateway.read
IBM Networking	ibm-vpc-network-vpn-gateway	is.vpn.vpn.list
IBM Networking	ibm-vpc-network-vpn-ike-policy	is.vpn.vpn.list
IBM Networking	ibm-vpc-network-vpn-ipsec-policy	is.vpn.vpn.list
IBM Virtual Server for VPC	ibm-vpc-virtual-server-instance	is.instance.instance.list is.instance.instance.read
IBM Virtual Server for VPC	ibm-vpc-virtual-server-instance-group	is.instance-group.instance-group.list is.instance-group.instance-group.read
IBM Virtual Server for VPC	ibm-vpc-virtual-server-image	is.image.image.list is.image.image.read
IBM IAM	ibm-iam-user	user-management.user.retrieve user-management.user-setting.retrieve
IBM IAM	ibm-iam-policy	iam.policy.read
IBM IAM	ibm-iam-identity-account-setting	iam-identity.account.get
IBM IAM	ibm-iam-role	iam.policy.read
IBM IAM	ibm-iam-trusted-profile	iam-identity.profile.get
IBM IAM	ibm-iam-access-group	iam-groups.groups.list

IBM IAM	ibm-iam-access-group-member	iam-groups.groups.list iam-groups.members.list
IBM IAM	ibm-iam-identity-account-activity-report	iam-identity.report.create iam-identity.report.get
IBM IAM	ibm-iam-service-id	iam-identity.serviceid.list
IBM Load Balancer for VPC	ibm-vpc-loadbalancer	is.load-balancer.load-balancer.view
IBM Activity Tracker	ibm-activity-tracker-route	atracker.route.list
IBM Activity Tracker	ibm-activity-tracker-setting	atracker.setting.get
IBM Activity Tracker	ibm-activity-tracker-target	atracker.target.list
IBM Activity Tracker	ibm-activity-tracker-instance	resource-controller.instance.retrieve global-search-tagging.resource.read
IBM Block Storage for VPC	ibm-vpc-block-storage-volume	is.volume.volume.read
IBM Block Storage for VPC	ibm-vpc-block-storage-snapshot	is.snapshot.snapshot.list is.snapshot.snapshot.read
IBM Kubernetes	ibm-kubernetes-cluster	containers-kubernetes.cluster.read
IBM Kubernetes	ibm-kubernetes-worker	containers-kubernetes.cluster.read
IBM Cloud Databases for PostgreSQL	ibm-postgresql-deployment-info	GET /v5/:platform/deployments/:deployment_id GET /v5/ibm/deployments/:deployment_id/allowlists/ip_addresses
IBM Cloud Databases for MySQL	ibm-mysql-deployment-info	GET /v5/:platform/deployments/:deployment_id GET /v5/ibm/deployments/:deployment_id/allowlists/ip_addresses
IBM Cloud Object Storage	ibm-object-storage-bucket	cloud-object-storage.account.get_account_buckets cloud-object-storage.bucket.get_cors cloud-object-storage.bucket.get_lifecycle
IBM Flow Log Collector for VPC	ibm-vpc-flow-log-collector	is.flow-log-collector.flow-log-collector.read
IBM Key Protect	ibm-key-protect-key	kms.secrets.list kms.policies.read
IBM Key Protect	ibm-key-protect-instance-policy	kms.instancepolicies.read
IBM Key Protect	ibm-key-protect-registration	kms.registrations.list

IBM Secrets Manager	ibm-secret-manager-secret	secrets-manager.secrets.list secrets-manager.secret-policies.get
IBM Secrets Manager	ibm-secret-manager-secret-group	secrets-manager.secret-groups.list
IBM Cloud Container Registry	ibm-container-registry-image	container-registry.image.list
IBM Event Streams	ibm-event-streams-instance	resource-controller.instance.retrieve global-search-tagging.resource.read
IBM Log Analysis	ibm-log-analysis-instance	resource-controller.instance.retrieve global-search-tagging.resource.read

IBM Cloud Policies

To know the list of all the available Prisma Cloud out-of-the-box (OOTB) policies for IBM Cloud by default, see **Git Repo**.