Qualys TotalCloud v2.x

Release Notes

Version 2.5.0
August 20, 2023

What's new?

Common Features

Introduced Support for Oracle Cloud Infrastructure (OCI) in TotalCloud Inventory

Introduced Support for CIS Foundation Benchmark Framework Version 1.2

Enhancements to the Configure Tab

New Tokens

Introduced New Mandate

Updated Existing Mandate

Microsoft Azure

Control Title Changes

Control Check Modified

Oracle Cloud Infrastructure

New Controls in CIS Oracle Cloud Infrastructure Foundation Benchmark Policy

New Controls in CIS Oracle Cloud Infrastructure Best Practices Policy

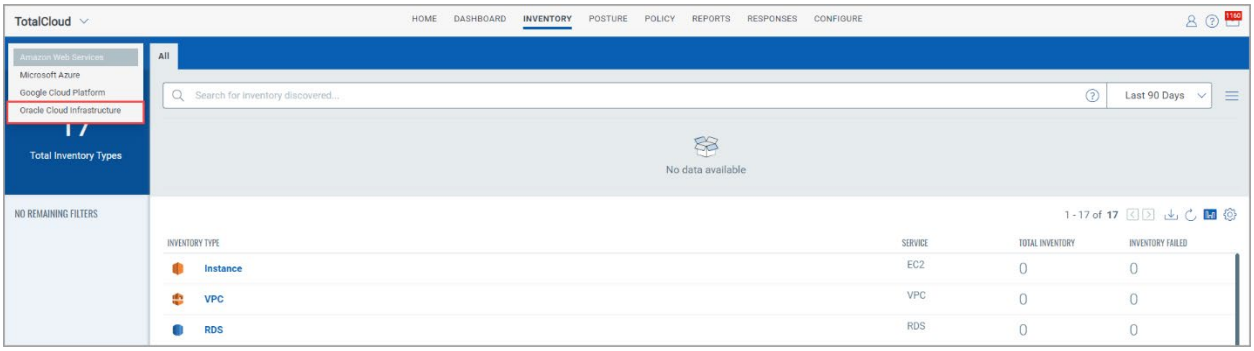
Qualys TotalCloud 2.5.0 brings you improvements and updates! Learn More

Common Features

Introduced Support for Oracle Cloud Infrastructure (OCI) in TotalCloud Inventory

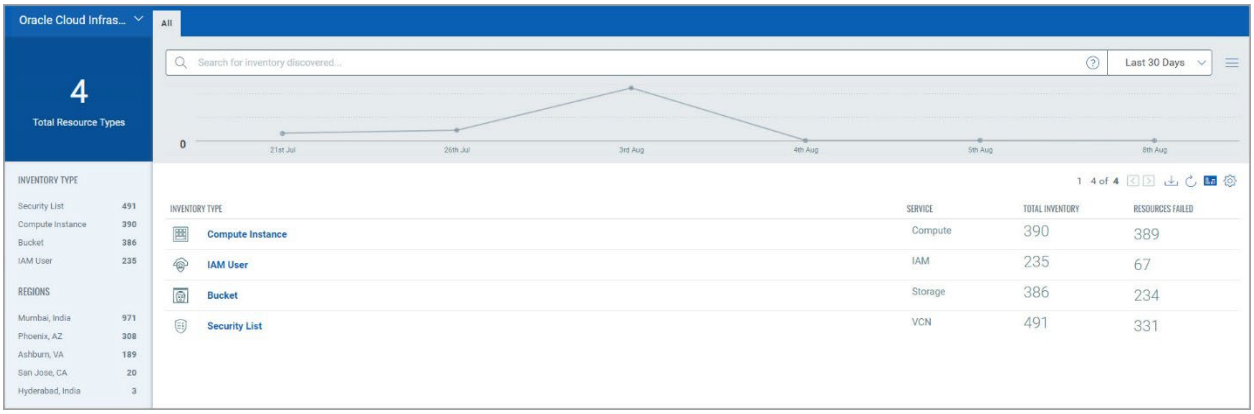
We have introduced support for Oracle Cloud Infrastructure inventory. Organizations with the OCI cloud provider can now use connector, inventory, and cloud posture assessment features Qualys TotalCloud offers for their cloud resources.

Note: You must contact support to enable OCI for your subscription.



To allow TotalCloud to discover your OCI cloud resources, you must first create an OCI connector.
Read more about the new OCI Connector in the Connector 1.8.0 Release Notes.

Once you have set up your OCI connector, the cloud resources are discovered and listed on the Inventory tab of TotalCloud.



The discovered resources can be tested against compliance policies to assess cloud posture. Click any inventory type and click the discovered resources to learn more about them.

Introduced Support for CIS Foundation Benchmark Framework Version 1.2

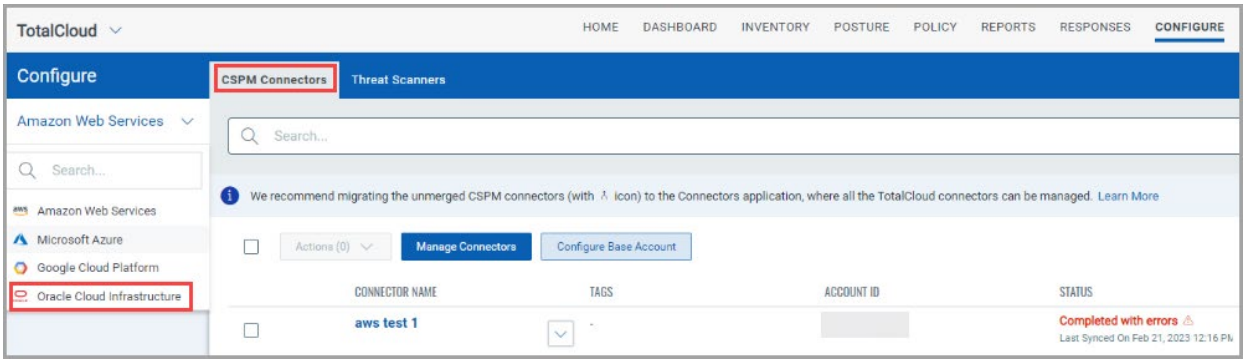
With this update, TotalCloud introduced support for the CIS Foundation Benchmark Framework version 1.2. Ensure a secure cloud infrastructure by aligning your cloud environment with robust security best practices and guidelines.

Enhancements to the Configure Tab

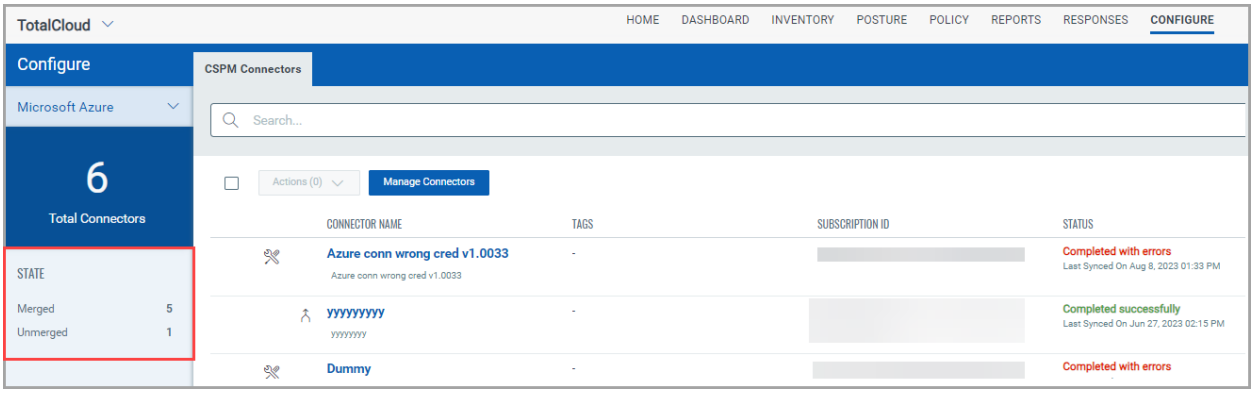
TotalCloud application brings updates to the Configure tab. The updates improve the visibility of your CSPM connectors configured in the Connectors application, introduce tokens for the new OCI CSPM connectors, and a new tab for CDR Threat Scanners.

Renamed Connectors Tab to CSPM Connectors

The full list of CSPM connectors configured on the Connectors application is visible on the CSPM Connectors tab. Select from the supported cloud providers on the left to view their available connectors.

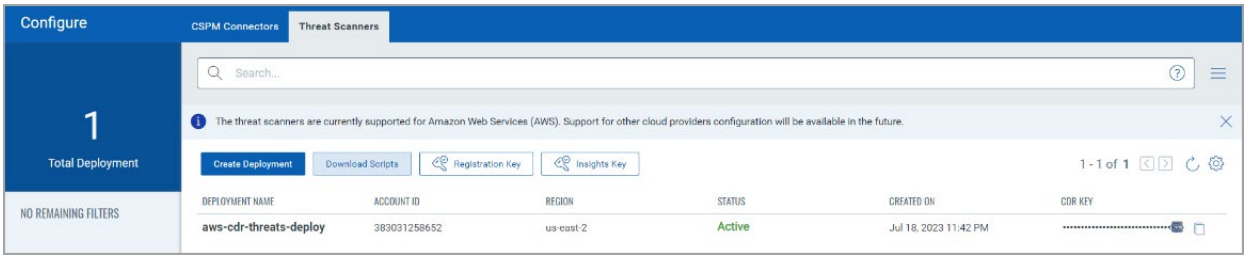


The CSPM Connectors tab brings additional features along with the name change. You can now find the total number of merged and unmerged connectors on the left pane, under 'State'.

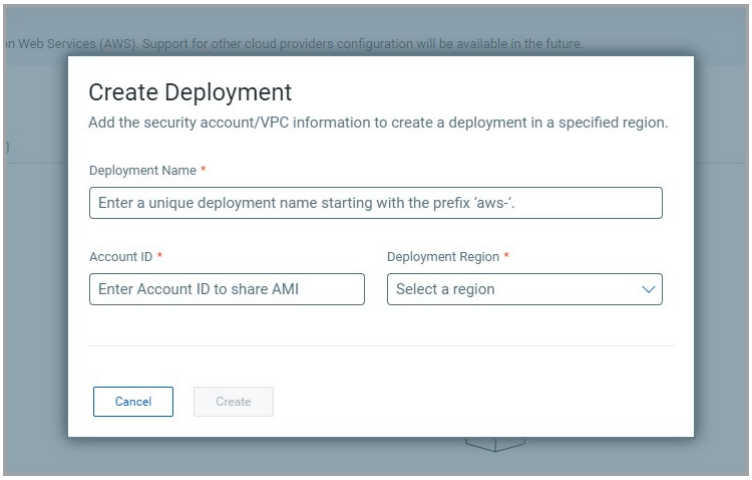


CDR Threat Scanner Deployments

TotalCloud updates the CDR deployment method by introducing the Threat Scanners tab. You no longer need to contact support to obtain your CDR keys and necessary files. All the configurations required to onboard your CDR deployment are available in the new Threat Scanners tab under the Configure tab of TotalCloud.



Click **Create** to begin your CDR journey.



Provide your account details and the region where CDR must be configured.

Click **Create** to deploy the Threat Scanner.

The deployment is listed on the Threat Scanner screen. The 'status' column shows the status of your deployment. As you progress with your CDR onboarding steps, the deployment status updates from Pending to Licensed and Activated.

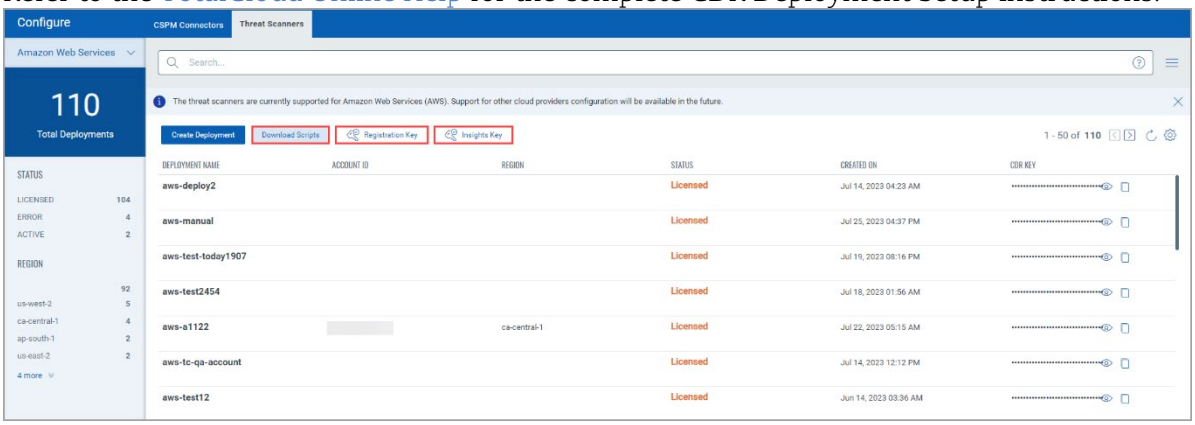
Download Scripts - Download the Terraform scripts to onboard your CDR Scanner. The zip file contains templates for Standalone CDR deployment, High-availability mode CDR deployment, and setting up a traffic mirror.

Registration Key - The Registration key is a unique key generated for your cloud. You will require it to onboard your CDR Scanner.

Insights Key - The Insights key is used for the Insight API to fetch Asset logs and real-time threat detection data.

CDR Key – A unique key for each deployment. This key is necessary to start real-time cloud detection and monitoring.

Refer to the TotalCloud Online Help for the complete CDR Deployment Setup instructions.



New Tokens

With this release, we have introduced support for new tokens for the OCI inventory, connector, and evaluation features.

CSPM Connector Tokens

You can find this token for finding merged or unmeged connectors in the CSPM Connectors tab of TotalCloud.

Navigate to **Configure** > **CSPM Connectors** > Any Cloud Provider.

Name	Description
state	Use a **text value (Merged, Unmerged)** to help you find the connectors with state you are looking for.

You can find these tokens for OCI connectors introduced in the **CSPM Connectors** tab of TotalCloud. Use these tokens to find relevant information regarding your OCI CSPM Connectors.

Navigate to **Configure** > **CSPM Connectors** > **Oracle Cloud Infrastructure**.

List of new tokens:

Name	Description
name	Use **values within quotes** to help you find the connector name you are looking for
username	Use **values within quotes** to help you find connectors created by a given username
tenantid	Use a **text value #####** to search connectors created with specific Tenant ID
isDisabled	Use **values true | false** to find the connectors that are in disabled/enabled state
tags.name	Use **values within quotes** to help you find connectors that are grouped by the tag name

Threat Scanner Tokens

You can find these tokens for OCI connectors introduced in the **Threat Scanners** tab of TotalCloud. Use these tokens to find relevant information regarding your Deployments.

Navigate to **Configure** > **Threat Scanners.**

List of new tokens:

Name	Description
status	Use a **text value #####** to search for deployments with the provided status
region	Use a **text value #####** to search for deployments with the provided region

OCI Inventory Tokens

You can find these tokens for OCI resources introduced in the **Inventory** tab of TotalCloud. Use these tokens to find relevant information regarding your discovered OCI resources.

Navigate to **Inventory** > **Oracle Cloud Infrastructure**.

List of new tokens:

Tokens for Discovered Buckets

Name	Description
bucket.id	Use a **text value #####** to find OCI bucket ID of interest.
bucket.name	Use a **text value #####** to find OCI Bucket name of interest.
bucket.namespace	Use a text value ##### to find buckets with the associated namespace.
bucket.compartmentId	Use a **text value #####** to find Buckets of specified compartmentID
bucket.createdBy	Use a **date range** or specific date to define when the bucket was created.
bucket.replicationEnabled	Use the values **true** | **false** to find Buckets with replication enabled.
bucket.isReadOnly	Use the values **true** | **false** to find Buckets that are read-only.
bucket.versioning	Use a **text value (Enabled, Disabled)** to find buckets of specified versioning.
bucket.autoTiering	Use a **text value (Disabled, InfrequentAccess)** to find buckets with specified storage tier transition permissions.
bucket.objectEventsEnabled	Use the values **true** | **false** to find Buckets that have Events enabled for object state changes.
bucket.kmsKeyId	Use a **text value #####** to find Buckets of specified KMS Key ID.
bucket.objectLevelAuditMode	Use a **text value #####** to find Buckets with the specified audit mode.
bucket.publicAccessType	Select from the dropdown (NoPublicAccessType, ObjectRead, ObjectReadWithoutList) to find buckets with the provided public Access Type.

bucket.storageTier	Select from the dropdown (Archive, InfrequentAccess, Standard) to find buckets with the provided storage tier.
bucket.timeCreated	Use a date range or specific date to define when the user was created.

Tokens for Discovered IAM Users

Name	Description
user.id	Use **values within quotes** to help you find IAM users with a certain user ID
name	Use **values within quotes** to help you find IAM users with a certain user name
user.isMfaActivated	Use the values **true** | **false** to find IAM users with multi-factor authentication enabled
user.lifecycleState	Select from the dropdown to find users with the selected lifecycle state
user.canUseConsolePassword	Use the values **true** | **false** to find IAM users with console password enabled
user.tenantId	Use a **text value #####** to find IAM users of specified Tenant ID
user.lastSuccessfulLoginTime	Use a **date range** or specific date to define when the user last successfully logged in
user.timeCreated	Use a **date range** or specific date to define when the user was created.
user.timeModified	Use a **date range** or specific date to define when the user was modified.

Tokens for Discovered Instances

Name	Description
instance.availabilityDomain	Select the availability domain you're interested in. Select from names in the drop-down menu
instance.compartmentId	Use a **text value #####** to find OCI instances with a certain Compartment ID
instance.faultDomain	Use a **text value #####** to find OCI instances with the given fault domain
instance.id	Use a **text value #####** to find OCI instances having a certain Instance ID
instance.imageId	Use a **text value #####** to find OCI instances with a certain Image (AMI) ID
instance.isPVEncryptioninTransitEnabled	Use **true | false** to view the instances with PV Encryption in Transit enabled/disabled
instance.lifecycleState	Select from the dropdown to find instances with the selected lifecycle state
instance.privateIp	Use a **text value #####** to find OCI instances having network interface with a certain private IP address
instance.publicIp	Use a **text value #####** to find OCI instances having network interface with a certain public IP address
instance.secureBootEnabled	Use **true | false** to view the instances with Secure

	Boot enabled/disabled
instance.shape	Select from the dropdown to find OCI instances having a specified shape

Tokens for Discovered Security Lists

Name	Description
securitylist.compartmentId	Use a **text value #####** to find Security Lists with a certain Compartment ID.
securitylist.egressSecurityRules.destination	Use an **integer value #####** to find security lists having egress rules with a certain destination
securitylist.egressSecurityRules.destinationPortRange.min	Use an **integer value #####** to find security lists with the given minimum number in destination port range allowing outbound traffic
securitylist.egressSecurityRules.destinationPortRange.max	Use an **integer value #####** to find security lists with the given maximum number in destination port range allowing outbound traffic
securitylist.egressSecurityRules.isStateless	Use true | false to find security lists for outbountd traffic that are stateless.
securitylist.egressSecurityRules.protocol	Select from the drop-down to find security lists with the given protocol
securitylist.egressSecurityRules.sourcePortRange.min	Use an **integer value #####** to find security lists with the given minimum number in source port range allowing outbound traffic
securitylist.egressSecurityRules.sourcePortRange.max	Use an **integer value #####** to find security lists with the given maximum number in the source port range, allowing outbound traffic
securitylist.id:	Use a **text value #####** to find Security Lists with a certain ID
securitylist.ingressSecurityRules.destinationPortRange.min	Use an **integer value #####** to find security lists with the given minimum number in destination port range allowing inbound traffic
securitylist.ingressSecurityRules.destinationPortRange.max	Use an **integer value #####** to find security lists with the given maximum number in the destination port range, allowing inbound traffic
securitylist.ingressSecurityRules.isStateless	Use **true | false** to find security lists for inbound traffic that are stateless
securitylist.ingressSecurityRules.protocol	Select from the drop-down to find security lists with the given protocol
securitylist.ingressSecurityRules.source	Use a text value **#####** to find security lists with the given traffic source
securitylist.ingressSecurityRules.sourcePortRange.min	Use an **integer value #####** to find security lists with the given minimum number in source port range, allowing inbound traffic
securitylist.ingressSecurityRules.sourcePortRange.max	Use an **integer value #####** to find security lists with the given maximum number in the source port range, allowing inbound traffic
securitylist.lifecyclestate	Select a lifecycle state (PROVISIONING, AVAILABLE, TERMINATING, TERMINATED) to find security groups having the selected lifecycle state. Select from the dropdown
securitylist.vcnId	Use a **text value #####** to find Security Lists

	with a certain VCN ID
securitylist.timeCreated	Use a **date range** or specific date to define when the securitylist was created

OCI Evaluation Tokens

You can find these tokens for OCI evaluations introduced in the **Posture** tab of TotalCloud. Use these tokens to find relevant information regarding your OCI Control evaluations.

Navigate to **Posture** > **Oracle Cloud Infrastructure** > Open **Control Evaluation** of any control.

Name	Description
resource.id	Use a **text value #####** to show resources based on the unique resource ID
tenantId	Use a **text value #####** to show OCI resources based on the unique tenant ID

Introduced New Mandates

We have introduced support for new mandates in this release.

Doc ID	Document Name	Publisher	Version
5822	Technology Risk Management (TRM) Guidelines	Monitory Authority of Singapore (MAS)	January 2021
6181	US Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 1	US Government – Office of the Under Secretary of Defense for Acquisition & Sustainment – OUSD(A&S)	v2.0
6182	US Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 2	US Government – Office of the Under Secretary of Defense for Acquisition & Sustainment – OUSD(A&S)	v2.0

Updated Existing Mandate

In this release, we have updated the Doc ID of the Australian Signals Directorate - Essential Eight Maturity Model (Doc ID-5781) mandate.

Doc ID	Document Name	Publisher	Version
7382	Australian Signals Directorate - Essential Eight Maturity Model	Australian Cyber Security Center (ACSC))	November 2022

Microsoft Azure

TotalCloud 2.5.0 brings the following updates to Azure controls.

Control Title Changes

We have introduced the following changes to control titles for CIS Microsoft Azure Foundations Benchmark.

CID	Title	New Title
50033	Ensure that all attached VM disks are encrypted	Ensure that all Attached VM Disks are encrypted with Customer Managed Key (CMK)
50038	Ensure that all disk snapshots are encrypted	Ensure that all disk snapshots are encrypted with Customer-managed key(CMK)

Control Check Modified

We have introduced the following changes to CIS Microsoft Azure Foundations Benchmark control checks.

CID	Title	Services
50033	Ensure that all attached VM disks are encrypted	Disk

Oracle Cloud Infrastructure

New Controls in CIS Oracle Cloud Infrastructure Foundation Benchmark Policy

We have introduced the following new controls in CIS Oracle Cloud Infrastructure Foundation Benchmark Policy.

CID	Title
40003	Ensure no Object Storage buckets are publicly visible
40004	Ensure Versioning is Enabled for Object Storage Buckets
40008	Ensure Object Storage Buckets are encrypted with a Customer Managed Key CMK
40014	Ensure no security lists allow ingress from 0.0.0.0/0 to port 22
40015	Ensure no security lists allow ingress from 0.0.0.0/0 to port 3389
40016	Ensure the default security list of every VCN restricts all traffic except ICMP
40017	Ensure MFA is enabled for all users with a console password
40018	Ensure user API keys rotate within 90 days or less

40019	Ensure user Customer Secret keys rotate within 90 days or less
40020	Ensure user Auth Tokens rotate within 90 days or less
40021	Ensure no network security groups allow ingress from 0.0.0.0/0 to port 22
40022	Ensure no network security groups allow ingress from 0.0.0.0/0 to port 3389
40023	Ensure API keys are not created for tenancy administrator users

New Controls in CIS Oracle Cloud Infrastructure Best Practices Policy

We have introduced the following new controls in CIS Oracle Cloud Infrastructure Foundation Benchmark Policy.

CID	Title	Service	Resource
40001	Ensure Secure Boot is enabled on Compute Instance	Compute	Instance
40002	Ensure Compute Instance boot volume has in-transit data encryption is Enabled	Compute	Instance
40005	Ensure Emit Object Events is Enabled for Object Storage Buckets	Storage	Bucket
40006	Ensure Bucket Pre-Authenticated Request allows Read Only Access	Storage	Bucket
40007	Ensure Bucket does not persists Expired Pre-Authenticated Request	Storage	Bucket
40009	Ensure no Object Storage buckets are left Untagged	Storage	Bucket
40010	Ensures password policy requires at least one lowercase letter	IAM	IAM Password
40011	Ensures password policy requires at least one uppercase letter	IAM	IAM Password
40012	Ensures password policy requires at least one numeric	IAM	IAM Password
40013	Ensures password policy requires at least one Special Character	IAM	IAM Password

Issues Addressed

-We have optimized the fetching data for Reports. This ensures successful and faster downloads of TotalCloud data.

-We have enhanced the detection logic of CID 50094, 50038, 190 and 191.

-We have enhanced the detection logic of CID 50053 ,52020, 50347 and 50250 to prevent false positive cases.

-We fixed an issue where resources failed to move evaluation exceptions to PASSE when the region is updated after connector runs.