# Qualys TotalCloud v2.x

## リリースノート

バージョン 2.5.0

2023 年 8 月 20 日

## 新機能

### 共通の機能

TotalCloud InventoryにOracle Cloud Infrastructure(OCI)のサポートを導入
CIS Foundationベンチマークフレームワークバージョン1.2のサポートを導入
Configureタブの機能強化
新しいトークン
新たな Mandatesの導入
既存のMandateの更新

### Microsoft Azure

コントロールタイトルの変更
コントロール チェックの変更

### Oracle Cloud Infrastructure

CIS Oracle Cloud Infrastructure Foundation ベンチマーク・ポリシーの新しいコントロール
CIS Oracle クラウド・インフラストラクチャのベスト・プラクティス・ポリシーの新しいコントロール

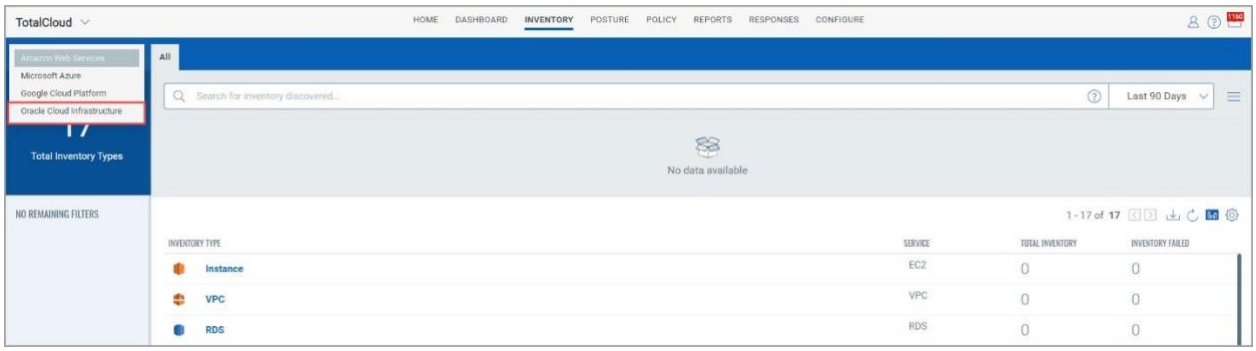
**Qualys TotalCloud 2.5.0 では、いくつかの改善と更新が実施されました。詳細はこちらをご覧下さい。**

# 共通の機能

## TotalCloud Inventory に Oracle Cloud Infrastructure(OCI)のサポートを導入

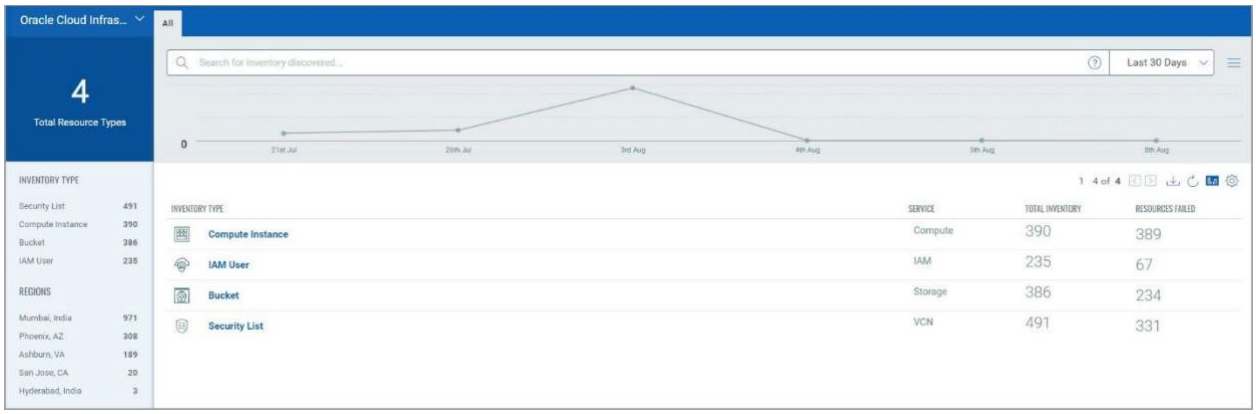
Oracle Cloud Infrastructure インベントリのサポートを導入しました。OCI クラウド・プロバイダを使用する組織は、QualysTotalCloud が提供するクラウド・リソースに対してコネクタ、インベントリおよびクラウド・ポスチャ評価機能を使用できるようになりました。

**注:** サブスクリプションのOCIを有効にするには、サポートに連絡する必要があります。




TotalCloudがOCIクラウド・リソースを検出できるようにするには、まずOCIコネクタを作成する必要があります。
新しいOCIコネクタの詳細については、コネクタ1.8.0リリース・ノートを参照してください。

OCIコネクタを設定すると、クラウド・リソースが検出され、TotalCloudのINVENTORYタブにリストされます。




検出されたリソースをコンプライアンスポリシーに対してテストし、クラウドの体制を評価できます。インベントリタイプをクリックし、検出されたリソースをクリックして詳細を確認します。

## CIS Foundation ベンチマークフレームワークバージョン 1.2 のサポートを導入

この更新により、TotalCloudはCISFoundationベンチマークフレームワークバージョン1.2のサポートを導入しました。

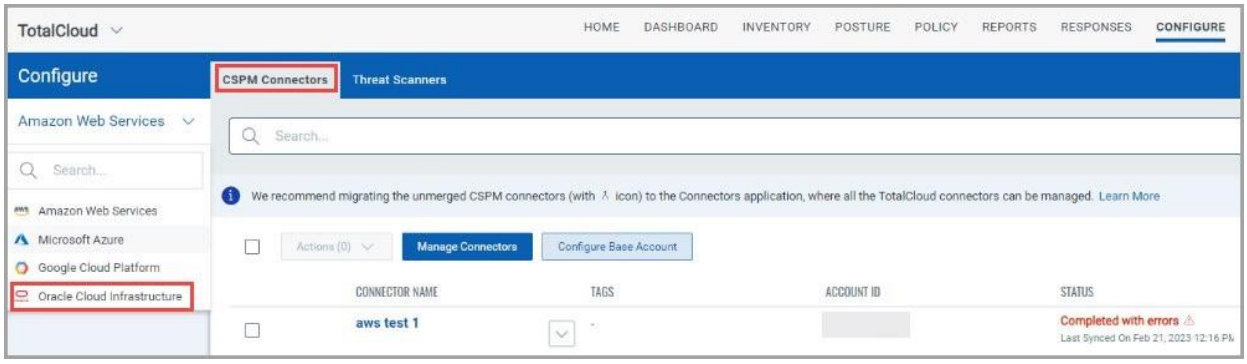
堅牢なセキュリティのベストプラクティスとガイドラインにクラウド環境を合わせることで、安全なクラウドインフラストラクチャを確保します。

## Configure タブの機能強化

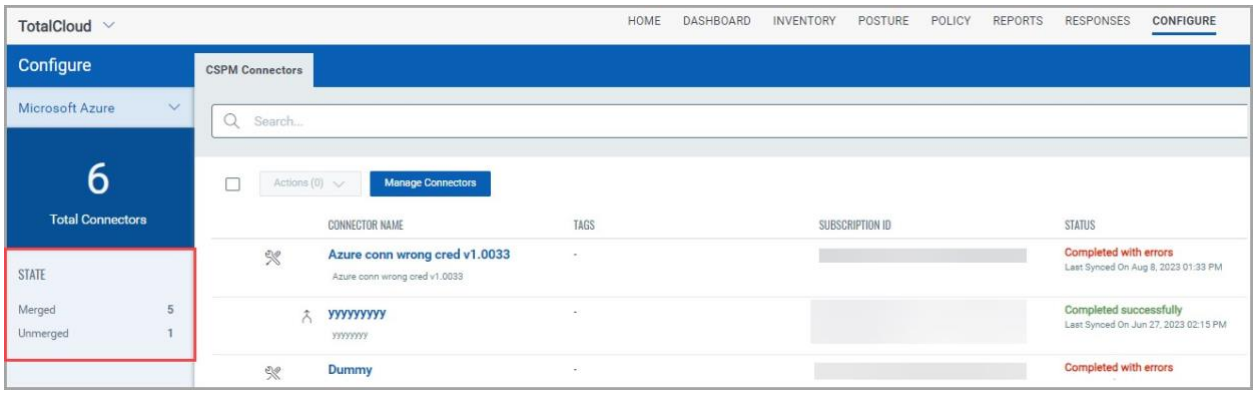
TotalCloud アプリケーションは、Configure タブに更新をもたらします。この更新により、コネクタ・アプリケーションで構成された CSPM コネクタの可視性が向上し、新しい OCI CSPM コネクタのトークンおよび CDR 脅威スキャナ用の新しいタブが導入されます。

### Connectors タブの名前を CSPM Connectors に変更

コネクタ アプリケーションで設定された CSPM コネクタの完全なリストは、CSPM Connectors タブに表示されます。左側のサポートされているクラウド プロバイダーから選択して、使用可能なコネクタを表示します。



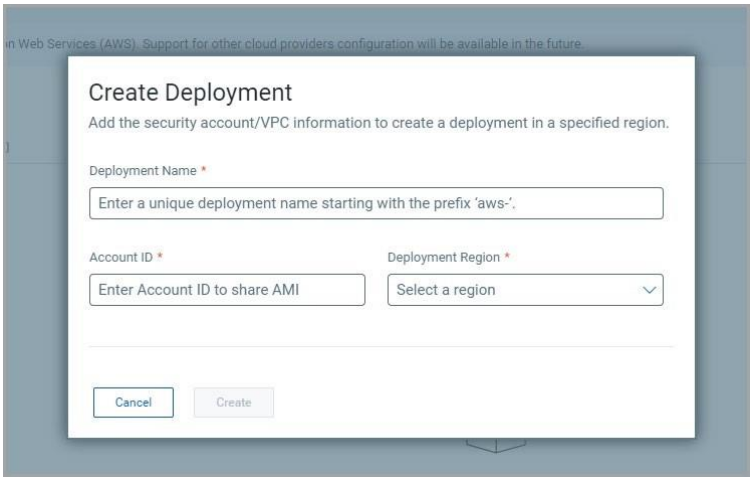

CSPM コネクタタブには、名前の変更とともに追加機能があります。これで、マージされたコネクタとマージされていないコネクタの総数が左側のペインの [状態] の下に表示されます。




### CDR 脅威スキャナの展開

TotalCloud は、Threat Scanners タブを導入することで CDR の展開方法を更新します。CDR キーと必要なファイルを取得するためにサポートに連絡する必要がなくなりました。
CDR 展開のオンボーディングに必要なすべての設定は、TotalCloud の [設定] タブにある新しい Threat Scanners タブで使用できます。


Create をクリックして、CDR ジャーニーを開始します。




アカウントの詳細と、CDR を設定する必要があるリージョンを指定します。

Create をクリックして、脅威スキャナを展開します。

展開が Threat Scanners 画面に表示されます。Status 列には、デプロイの状態が表示されます。CDR のオンボーディング手順を進めると、展開ステータスが Pending から Licensed および Activated に更新されます。

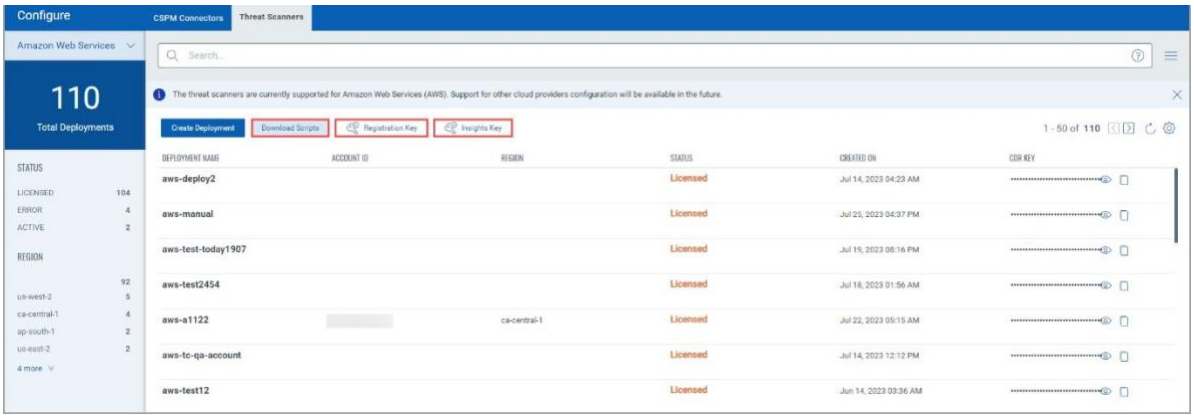
**Download Scripts** – Terraform スクリプトをダウンロードして、CDR スキャナーをオンボードします。zip ファイルには、スタンドアロン CDR 展開、ハイ アベイラビリティ モード CDR 展開、およびミラートラフィックの設定用のテンプレートが含まれています。

**Registration Key** – 登録キーは、クラウド用に生成される一意のキーです。CDR スキャナをオンボードするために必要になります。

**Insights Key** – インサイトキーは、アセットログとリアルタイムの脅威検出データを取得するためにインサイト API に使用されます。

**CDR Key** - デプロイごとに一意のキー。このキーは、リアルタイムのクラウド検出と監視を開始するために必要です。

CDR 導入セットアップの詳細な手順については、TotalCloud Online Help を参照してください。




# 新しいトークン

このリリースでは、OCI インベントリ、コネクタおよび評価機能用の新しいトークンのサポートが導入されました。

### CSPM コネクタトークン

このトークンは、TotalCloud の CSPM connectors タブで、マージされたコネクタまたは未解決のコネクタを見つけることができます。

次の場所に移動します。 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. |

これらのトークンは、トータルクラウドの CSPMConnectors タブで紹介されています。これらのトークンを使用して、OCI CSPM コネクタに関する関連情報を検索します。

次の場所に移動します。 Configure > CSPM Connectors > Oracle Cloud Infrastructure.

新しいトークンリスト:

| **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

これらのトークンは、の Threat Scanners タブで紹介されている OCI コネクタで確認できます 。これらのトークンを使用して、デプロイに関する関連情報を検索します。

次の場所に移動します。 **Configure > Threat Scanners.**

新しいトークンリスト:

| 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 インベントリ・トークン

これらのトークンは、TotalCloud の Inventory タブで紹介されている OCI リソースに対して見つけることができます 。これらのトークンを使用して、検出された OCI リソースに関する関連情報を検索します。

次の場所に移動します。Inventory > Oracle Cloud Infrastructure.

新しいトークンリスト:
検出されたバケットのトークン

| **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. |

検出された IAM ユーザーのトークン

| 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. |

検出されたインスタンスのトークン

| 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 |

検出されたセキュリティ・リストのトークン

| 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 評価トークン

これらのトークンは、TotalCloud の Posture タブで導入された OCI 評価用です。これらのトークンを使用して、OCI コントロールの評価に関する関連情報を検索します。

次の場所に移動します。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 |

## 新たな Mandates の導入

このリリースでは、新しい Mandates のサポートが導入されました。

| 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 |

## 既存の Mandate の更新

このリリースでは、オーストラリア信号局 – エッセンシャル エイト マチュリティ モデル (Doc ID-5781) の Mandate のドキュメント ID を更新しました。

| 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 では、Azure コントロールに次の更新が加えられています。

## コントロールタイトルの変更

CIS Microsoft Azure Foundations Benchmark のコントロール タイトルに次の変更が導入されました。

| 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) |

## コントロール チェックの変更

CIS Microsoft Azure Foundations Benchmark コントロール チェックに次の変更が加えられました。

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

# オラクル・クラウド・インフラストラクチャ

## CIS Oracle Cloud Infrastructure Foundation ベンチマーク・ポリシーの新しいコントロール

CIS Oracle Cloud Infrastructure Foundation ベンチマーク・ポリシーに次の新しいコントロールが導入されました。

| 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 |

## CIS Oracle クラウド・インフラストラクチャのベスト・プラクティス・ポリシーの新しいコントロール

CIS Oracle Cloud Infrastructure Foundation ベンチマーク・ポリシーに次の新しいコントロールが導入されました。

| 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 |

# 対処された問題

- レポートのデータ取得を最適化しました。これにより、TotalCloud データのダウンロードが成功し、より高速になりました。
- CID 50094、50038、190、191 の検出ロジックを強化しました。
- CID 50053、52020、50347、50250 の検出ロジックを強化して、誤検知のケースを防止しました。
- コネクタの実行後にリージョンが更新されたときに、リソースが評価例外を PASSE に移動できない問題を修正しました。