Oracle® Cloud

Settings Reference for Oracle CASB Cloud Service

Release 20.1.1.0
E99890-22
January 2020

Oracle Cloud Settings Reference for Oracle CASB Cloud Service, Release 20.1.1.0

E99890-22

Primary Author: John Wolley

Contents

Preface

Using Oracle CASB Cloud Service is comprehensive documentation that supports the monitoring and the remediation of security threats to cloud applications using Oracle CASB Cloud Service.

Audience

Oracle CASB Cloud Service Online Help is for anyone who wants to perform administrative tasks for cloud applications using Oracle CASB Cloud Service. Familiarity with cloud applications is helpful, but isn't required.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Certified Browsers

For the best user experience, and highest security protections, access Oracle CASB Cloud Service through one of these certified browsers:

- Internet Explorer v. 11
- Google Chrome v. 50
- Mozilla Firefox v. 42

Related Resources

For more information, see these Oracle resources:

- What's New for Oracle CASB Cloud Service
- Known Issues for Oracle CASB Cloud Service
- Oracle CASB Cloud Service Videos
- Oracle Public Cloud

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Oracle Cloud Infrastructure (OCI) Security Controls

Learn about the security control baseline settings for OCI.

Administrator user has API keys configured

Alert when an IAM administrator uses an API key.

> **Note:**
>
> This security control generates alerts only when OCI tenancy has been registered directly in Oracle CASB Cloud Service, using the **Tenancy** option. See Adding an OCI Instance. Once an OCI tenancy is registered, all KMS keys in that tenancy are monitored, regardless of the compartment in which they are stored.

Configuration: Enter comma-separated values for names of groups of users that you want to monitor.

Recommendation: Ensure that OCI access by administrators via API keys is performed as an exception. Do not hard code IAM credentials directly in software or documents to a wide audience.

Remediation Procedure: For step-by-step resolution procedures, see Member of the Administrators group used API keys.

Background Information: IAM API keys are credentials used to grant programmatic access to resources. IAM policies are used to govern access of IAM groups to resources in compartments and in the tenancy.

For more background information, see Services.

Alert on untagged resources

Alert if an untagged resource is found. Resource types that will trigger an alert if untagged: compute images (IMAGE), compute instances (INSTANCE), database systems (DB_SYSTEM), VCNs (VCN), object storage (BUCKET), and storage block volumes (VOLUME).

Configuration values: Enter comma-separated list of supported image tags. These are the only image tags that will not trigger this alert. Six formats are supported for entering image tags:

- `resourceType.nameSpace.definedKey=definedValue`

  Example: `VCN:PRODUCTION.status=upgraded`

- `nameSpace.definedKey=definedValue`

  Example: `PRODUCTION.status=upgraded`
- `resourceType.definedKey=definedValue`

  Example: `VCN:PRODUCTION.status=upgraded`
- `definedKey=devinedValue`

  Example: `status=upgraded`
- `resourceTpe.freeFormKey`

  Example: `VCN:APPROVED`
- `freeFormKey`

  Example: `APPROVED`

Recommendation: Verify that the configured tags are in use for compute images, compute instances, database systems, VCNs, object storage, and storage block volumes.

Remediation Procedure: To be provided.

Background Information: Untagged resources in OCI indicate that infrastructure has been created without the use of corporate-sanctioned tags. Uncontrolled infrastructure can result in a weakened security posture.

For more background information, see Services.

Apply Lag is too large in DataGuard

Section Title

(Optional) Enter reference information in this section.

Syntax

(Optional) Enter syntax information here.

Example 1-1 Example Title

(Optional) Enter an example to illustrate your reference here.

Automatically backup databases (Bare Metal | VM)

Alert when a database is not being backed up automatically.

Exception: Enter a comma-separated list of database OCIDs that should not trigger an alert.

Recommendation: Ensure that automatic backup is enabled.

Remediation Procedure: For step-by-step resolution procedures, see Enabling and Reconfiguring the Automatic Backups Feature.

Background Information: Enabling automatic backup ensures that you will be able to restore the database with minimal data loss, if there is a catastrophic hardware failure.

Block Volume is not encrypted with KMS (customer managed) key

Alert if the block volume is not encrypted with a Key Management Service (KMS) key.

Exceptions: Enter comma-separated values for block volumes that should not trigger this alert.

Recommendation: Assign a KMS key to this block volume.

Remediation Procedure: For step-by-step resolution procedures, see Creating a Volume.

Background Information: Encryption of volumes provides an additional level of security on your data. Management of encryption keys is critical to protecting and accessing protected data. Key management provides the ability to scale with growth ensuring availability and mobility, proof of compliance for audits, and reduction of costs for key lifecycle management, including key generation, distribution and revocation. Encryption and key management ensure data confidentiality, integrity, and availability.

Bucket is not encrypted with KMS (customer managed) key

Alert if the object storage bucket is not encrypted with a Key Management Service (KMS) key.

Exceptions: Enter comma-separated values for object storage buckets that should not trigger this alert.

Recommendation: Assign a KMS key to this bucket.

Remediation Procedure: For step-by-step resolution procedures, see To assign a Key Management key to a bucket.

Background Information: Encryption of object storage buckets provides an additional level of security on your data. Management of encryption keys is critical to protecting and accessing protected data. Key management provides the ability to scale with growth ensuring availability and mobility, proof of compliance for audits, and reduction of costs for key lifecycle management, including key generation, distribution and revocation. Encryption and key management ensure data confidentiality, integrity, and availability.

Compute Instance has a public IP Address

Alert if the instance has a public IP address.

Exceptions: Enter comma-separated values for instance IDs that should not trigger this alert.

Recommendation: Carefully consider allowing internet access to any instances. For example, you don't want to accidentally allow internet access to sensitive database instances.

Remediation Procedure: For step-by-step resolution procedures, see Instance has a public IP.

Background Information: In order for an instance to be publicly addressable, it must have a public IP, exist in a public VCN subnet, the VCN must have an Internet Gateway enabled and be configured for outbound traffic and the security list for the subnet must be configured for all IPs and all ports (0.0.0.0/0).

For more background information, see Services.

Compute Instance is running a Partner image

Alert if the instance is running a partner image.

Section Title

(Optional) Enter reference information in this section.

Syntax

(Optional) Enter syntax information here.

Example 1-2 Example Title

(Optional) Enter an example to illustrate your reference here.

Compute Instance is running a Platform image

Alert if the instance is running a platform image.

Section Title

(Optional) Enter reference information in this section.

Syntax

(Optional) Enter syntax information here.

Example 1-3 Example Title

(Optional) Enter an example to illustrate your reference here.

Compute Instance is running an Oracle image

Alert if the instance is running an Oracle image.

Section Title

(Optional) Enter reference information in this section.

Syntax

(Optional) Enter syntax information here.

Example 1-4 Example Title

(Optional) Enter an example to illustrate your reference here.

Compute Instance is running an Oracle-provided image

Alert if the instance is running on an Oracle-provided image, which is a public image.

Exceptions: Enter comma-separated values for instance IDs that should not trigger this alert.

Recommendation: Ensure that the instances are using approved images.

Remediation Procedure: To be provided.

Background Information: This identifies all instances built from OCI public images. Exceptions can be configured in Oracle CASB Cloud Service to reduce alerts from exempted instances.

For more background information, see Services.

Compute Instance is running image without supported tags

Alert if the instance is running on an unsupported image.

Configuration values: Enter comma-separated list of supported image tags. These are the only image tags that will not trigger this alert. Three formats are supported for entering image tags:

- `nameSpace.definedKey=definedValue`

  Example: `PRODUCTION.status=upgraded`
- `definedKey=definedValue`

  Example: `status=upgraded`
- `freeFormKey`

  Example: `APPROVED`

Exception: Enter a comma-separated list of compute instance OCIDs that should not trigger an alert.

Background Information: This identifies all instances running without configured tags. If your OCI tenancy uses tags as a control for your environment, this control will alert when an instance is running without an approved tag.

Recommendation: Ensure that the instances are using approved images.

Remediation Procedure: For step-by-step resolution procedures, see Instance created based on unapproved custom image.

Background Information: This identifies all instances running without configured tags. If your OCI tenancy uses tags as a control for your environment, this control will alert when an instance is running without an approved tag.

For more background information, see Services.

Database patches not applied (Bare Metal | VM)

Alert when a database is discovered which has one or more patches, available for number of days you specify, that have not been applied.

Configuration: Enter the number of days you want to allow after the time a patch is available before an alert is generated for the patch not being applied.

Exception: Enter a comma-separated list of database OCIDs that should not trigger an alert. For example:

`Patch1:[DB2,DB2]` or `Patch2:[*]`

Recommendation: Oracle recommends that released patches be applied to the database as soon as possible.

Remediation Procedure: For step-by-step resolution procedures, see Patching a DB System.

Background Information: Database patches address functionality, security, and performance issues. The vast majority of security breaches can be prevented by applying available patches.

Database version is not sanctioned (Bare Metal | VM | Exadata)

Alert when a database has not been upgraded to the certified version.

Configuration: Enter comma-separated lists for **Configuration values**.

- **Recommended Versions** - enter a comma-separated list of database OCIDs for which an alert should not be generated, even if they are running unsanctioned versions.
- **Do not alert for** - enter a comma-separated list of database versions that are sanctioned.

Recommendation: Oracle recommends that the deployed Database version is approved and tested.

Background Information: The sanctioned version of a database has the most recent security features and vulnerability patches.

DB System has public IP address (Bare Metal | VM | Exadata)

Alert when a database system is discovered which has a public IP address.

Exception: Enter a comma-separated list of database system OCIDs that should not trigger an alert.

Recommendation: Ensure that the database system does not have a public IP address.

Remediation Procedure: For step-by-step resolution procedures, see Enabling and Reconfiguring the Automatic Backups Feature.

Background Information: Use of a public IP address to access a database increases your exposure to potential security and business continuity risks.

DB System patches not applied (Bare Metal | VM)

Alert when a database system is discovered which has one or more patches, available for 90 days or more, that have not been applied.

Exception: Enter a comma-separated list of database system OCIDs that should not trigger an alert. For example:

`Patch1:[DBS2,DBS2]` or `Patch2:[*]`

Recommendation: Oracle recommends that released patches be applied to the DB system as soon as possible.

Remediation Procedure: For step-by-step resolution procedures, see Patching a DB System.

Background Information: Database system patches often include updates that eliminate known security vulnerabilities.

DB System version is not sanctioned (Bare Metal | VM | Exadata)

Alert when a database system is found with a version that is not sanctioned.

Configuration: Enter a comma-separated list of certified database system versions. If a database system version has more than three parts, you only need to enter the first three parts: `##.##.##`.

Exception: Enter a comma-separated list of database OCIDs that should not trigger an alert.

Recommendation: Oracle recommends that the deployed DB System version is approved and tested.

Background Information: DB Systems are tested and sanctioned by Oracle's internal testing. Running unsanctioned versions of DB Systems may increase your chances of a security breach, putting your data confidentiality, integrity, and availability at risk.

Disallow username in password

Section Title

(Optional) Enter reference information in this section.

Syntax

(Optional) Enter syntax information here.

Example 1-5 Example Title

(Optional) Enter an example to illustrate your reference here.

Failed database

Alert when a failed database is discovered.

Failed database system

Alert when a failed database is discovered.

Group of Administrators has too few members

Alert when an IAM group has fewer than a set number of administrators defined.

> **Note:**
>
> This security control generates alerts only when OCI tenancy has been registered directly in Oracle CASB Cloud Service, using the **Tenancy** option. See Adding an OCI Instance. Once an OCI tenancy is registered, all KMS keys in that tenancy are monitored, regardless of the compartment in which they are stored.

Configuration values: Enter comma-separated value pairs. First value is the IAM group name, followed by a colon (":"), followed by the minimum number of administrators the group is supposed to have. For example, `Admins:1, Managers:1`.

Recommendation: Ensure that a minimum of 2 administrators are created for a tenancy. This reduces the risk that an OCI tenancy is orphaned by lost credentials, change in staff, or other single point of failure events.

Remediation Procedure: To be provided.

Background Information: Configure Oracle CASB Cloud Service with the administrator group and the minimum number of administrators allowed for the tenancy.

For more background information, see Services.

Group of Administrators has too many members

Alert when an IAM group has more than a set number of administrators defined.

> **Note:**
>
> This security control generates alerts only when OCI tenancy has been registered directly in Oracle CASB Cloud Service, using the **Tenancy** option. See Adding an OCI Instance. Once an OCI tenancy is registered, all KMS keys in that tenancy are monitored, regardless of the compartment in which they are stored.

Configuration values: Enter comma-separated value pairs. First value is the IAM group name, followed by a colon (":"), followed by the maximum number of administrators the group is allowed to have. For example, `Admins:1, Managers:3`.

Recommendation: Ensure that the number of administrators in your OCI tenancy does not exceed your internal information security policy.

Remediation Procedure: To be provided.

Background Information: Configure Oracle CASB Cloud Service with the administrator group and the maximum number of administrators allowed for the tenancy. By default, this security control is disabled. If you wish to enable it, you must enter **Configuration values** as described above.

For more background information, see Services.

IAM Key older than 90 days

Alert if an IAM API key is more than 90 days old.

> **Note:**
>
> This security control generates alerts only when OCI tenancy has been registered directly in Oracle CASB Cloud Service, using the **Tenancy** option. See Adding an OCI Instance. Once an OCI tenancy is registered, all KMS keys in that tenancy are monitored, regardless of the compartment in which they are stored.

Recommendation: Rotate IAM passwords and API keys regularly, at least every 90 days. Besides being a security best practice, this is also a common compliance requirement.

Remediation Procedure: For step-by-step resolution procedures, see API signing keys over 90 days old.

Background Information: Changing IAM passwords and API keys at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.

For more background information, see Services.

IAM password has not been rotated

Alert if the IAM password has not been rotated within the number of days specified in the security control.

Recommendation: Consider forcing a password change by resetting the user's password directly.

Remediation Procedure: For step-by-step resolution procedures, see Managing User Credentials.

Background Information: All IAM passwords should be rotated within the number of days specified in the security control.

IAM Password older than 90 days

Alert if an IAM password is more than 90 days old.

Recommendation: Consider forcing a password change by resetting the user's password directly. See To create or reset another user's Console password.

Remediation Procedure: For step-by-step resolution procedures, see IAM Credentials.

Background Information: Changing IAM passwords and API keys at least every 90 days is a security best practice. The longer that IAM credentials remain unchanged, the greater the risk that they can become compromised.

For more background information, see Services.

IAM Policy grants too many privileges

Alert if an IAM policy creates a tenancy administrator, or a service-level administrator at the tenancy or compartment level, and that administrator is not a member of the Administrators group. Tenancy administrators can manage all resources in a tenancy, and service-level administrators can manage all resources for a service in a tenancy or a compartment. Administrators created by adding users or groups to the Administrators group do not trigger an alert when this security control is enabled.

Recommendation: Ensure that the policy is restricted to allow only specific users to access the resources required to accomplish their job functions.

Remediation Procedure: For step-by-step resolution procedures, see Policy grants broad permissions.

Background Information: A policy is a document that specifies who can access which OCI resources that your company has, and how. A policy simply allows a group to work in certain ways with specific types of resources in a particular compartment.

For more background information, see Services.

Internet gateway is attached to a VCN

Alert if a VCN has Internet gateway access.

Exceptions: Enter comma-separated values for VCN IDs that should not trigger this alert.

Recommendation: Ensure that internet gateways are authorized to be attached to a VCN, and that this attachment doesn't expose resources to the internet. Ensure that security lists with ingress / inbound rules and those security lists are not configured to allow access from all IP addresses 0.0.0.0/0. Exceptions can be configured in Oracle CASB Cloud Service to reduce alerts from exempted VCNs.

Remediation Procedure: For step-by-step resolution procedures, see Internet gateway attached to VCN.

Background Information: A VCN has a collection of features for enforcing network access control and securing VCN traffic. Gateways provide external connectivity to hosts in a VCN. They include Internet Gateway (IGW) for Internet connectivity, Dynamic Routing Gateway (DRG) for on-premises connectivity with VPN or Fast Connect, and Local Peering Gateway (LPG) for connectivity to peered VCN.

For more background information, see Services.

KMS key not rotated

Alert if a Key Management Service (KMS) key is found that has not been rotated within the maximum number of days specified.

> **Note:**
>
> This security control generates alerts only when OCI tenancy has been registered directly in Oracle CASB Cloud Service, using the **Tenancy** option. See Adding an OCI Instance. Once an OCI tenancy is registered, all KMS keys in that tenancy are monitored, regardless of the compartment in which they are stored.

Configuration: Number of days after which a KMS key will be considered old.

Exceptions: Enter Comma-Separated Values (CSV) of KMS Key IDs for which the alerts shouldn't be triggered.

Recommendation: Rotate the KMS key that was found.

Remediation Procedure: For step-by-step resolution procedures, see Managing Keys.

Background Information: Best practice for information security is to periodically change, or rotate, passwords, keys, and cryptographic materials. Rotating your keys in KMS reduces the impact and probability of key compromise. You should rotate your keys regularly in compliance with your organization's security policies, and any time there is a security incident. Use the KMS console, API, or command line to rotate keys.

For more background information, see Managing Keys.

Load balancer SSL certificate expires in 5 Days

Alert when the SSL certificate in a load balancer will expire in 5 days.

Recommendation: Ensure that certificates are rotated on a timely basis.

Remediation Procedure: For step-by-step resolution procedures, see Load balancer SSL certificate expires in X days.

Background Information: To ensure continuous security and usability, SSL certificates must be rotated in OCI.

For more background information, see Services.

Load balancer SSL certificate expires in 45 Days

Alert when the SSL certificate in a load balancer will expire in 45 days.

Recommendation: Ensure that certificates are rotated on a timely basis.

Remediation Procedure: For step-by-step resolution procedures, see Load balancer SSL certificate expires in X days.

Background Information: To ensure continuous security and usability, SSL certificates must be rotated in OCI.

For more background information, see Services.

Load balancer SSL certificate expires in 90 Days

Alert when the SSL certificate in a load balancer will expire in 90 days.

Recommendation: Ensure that certificates are rotated on a timely basis.

Remediation Procedure: For step-by-step resolution procedures, see Load balancer SSL certificate expires in X days.

Background Information: To ensure continuous security and usability, SSL certificates must be rotated in OCI.

For more background information, see Services.

Load Balancers with no back-end sets

Alert when there are no back-end sets associated with a load balancer.

Exceptions: Enter comma-separated values for load balancer IDs that should not trigger this alert.

Recommendation: Ensure that you configure load balancers with back-end sets to control the health and access to a load balancer by defined instances. Exceptions can be configured in Oracle CASB Cloud Service to reduce alerts from exempted load balancers.

Remediation Procedure: For step-by-step resolution procedures, see Load balancer has no backend sets.

Background Information: A back-end set is a logical entity defined by a load balancing policy, a health check policy, and a list of back-end servers.

For more background information, see Services.

Load Balancers with no inbound rules or listeners

Alert when a security list of a load balancer has ingress rules that accept traffic from an open source (0.0.0.0/0).

Exceptions: Enter comma-separated values for VCN IDs that should not trigger this alert.

Recommendation: Ensure that your OCI load balancers use inbound rules or listeners to only allow access from known resources. Exceptions can be configured in Oracle CASB Cloud Service to reduce alerts from exempted load balancers.

Remediation Procedure: For step-by-step resolution procedures, see Load balancer has no inbound rules or listeners.

Background Information: OCI load balancers enable end-to-end TLS connections between a client's applications and your VCN. A listener is a logical entity that checks for incoming traffic on the load balancer's IP address. To handle TCP, HTTP, and HTTPS traffic, you must configure at least one listener per traffic type.

For more background information, see Services.

Maximum password length

Alert when password is discovered which is longer than the maximum length.

Minimum lowercase characters required

Alert when password is discovered which has fewer than the required minimum number of lower case characters.

Minimum numerals required

Alert when password is discovered which has fewer than the required minimum number of numeric characters.

Minimum password length

Alert when password is discovered which shorter than the required minimum length.

Minimum special characters required

Alert when password is discovered which has fewer than the required minimum number of special characters.

Minimum uppercase characters required

Alert when password is discovered which has fewer than the required minimum number of upper case characters.

Network security group: Egress rule contains disallowed destination IP/port

Alert when the egress rule for a network security group (NSG) contains a disallowed destination IP address and port number.

Configuration: Enter comma-separated protocol-port number list pairs for each destination to be disallowed, enclosing port numbers in square brackets:

`<protocol>:[<port#>],<protocol>:[<port#>], …`

For example: `TCP:[22],UDP:[22]`

Exceptions: Enter comma-separated NSGid-protocol-port number list pairs for each destination to be disallowed, enclosing port number lists in square brackets:

For example: `TCP:[22],UDP:[22]`

Recommendation: To prevent unauthorized access or attacks on Compute instances, Oracle recommends that you use an NSG security list to allow SSH or RDP access only from authorized ICIDR blocks, rather than leaving them open to the internet (0.0.0.0/0). For additional security, you can temporarily enable SSH (port 22) or RDP (port 3389) access on an as-needed basis using the Network security group API UpdateSecurityList.

Remediation Procedure: To be provided.

Background Information: NSGs act as a virtual firewall for your Compute instances and other kinds of resources. An NSG consists of a set of ingress and egress security rules that apply only to a set of VNICs of your choice in a single VCN, for example, all the Compute instances that act as Web servers in the Web tier of a multi-tier application in your VCN.

Network security group: Ingress rule contains disallowed destination IP/port

Alert when the ingress rule for a network security group contains a disallowed destination IP address and port number.

Configuration: Enter comma-separated protocol-port number list pairs for each destination to be disallowed, enclosing port numbers in square brackets:

`<protocol>:[<port#>],<protocol>:[<port#>], …`

For example: `TCP:[22],UDP:[22]`

Exceptions: Enter comma-separated NSGid-protocol-port number list pairs for each destination to be disallowed, enclosing port number lists in square brackets:

Recommendation: To prevent unauthorized access or attacks on Compute instances, Oracle recommends that you use an NSG security list to allow SSH or RDP access only from authorized ICIDR blocks, rather than leaving them open to the internet (0.0.0.0/0). For additional security, you can temporarily enable SSH (port 22) or RDP (port 3389) access on an as-needed basis using the Network security group API UpdateSecurityList.

Remediation Procedure: To be provided.

Background Information: NSGs act as a virtual firewall for your Compute instances and other kinds of resources. An NSG consists of a set of ingress and egress security rules that apply only to a set of VNICs of your choice in a single VCN, for example, all the Compute instances that act as Web servers in the Web tier of a multi-tier application in your VCN.

New patch (older than X days) for Database is available

Alert when database is discovered for which one or more patches have been available for 90 days or longer.

OCI compartment not registered in Oracle CASB

Alert when an OCI compartment is found that is not registered in Oracle CASB Cloud Service.

Recommendation: Ensure that the compartment is registered in Oracle CASB Cloud Service.

Remediation Procedure: For step-by-step resolution procedures, see Adding an OCI Instance.

Background Information: A compartment is a logical container within your tenancy used to segregate Oracle Cloud Infrastructure (OCI) resources. Unregistered OCI compartments are not monitored by CASB and can create blind spots resulting in a weakened security posture. Users and their activities will not trigger policy alerts nor will these activities contribute to their user profiles.

A compartment must be registered in Oracle CASB in order for CASB to monitor its resources. This security control identifies compartments that are not registered.

Public bucket is found

Alert if a public bucket is found.

Exceptions: Enter comma-separated public bucket names that should not trigger this alert.

- Format: `region-A:[bucket1, bucket2, bucket3], region-B:[bucket4]`
- Example: `eu-frankfurt-1:[PublicBucket]`

Recommendation: Ensure that the bucket is sanctioned for public access, and if not, direct the OCI administrator to restrict the bucket policy to allow only specific users access to the resources required to accomplish their job functions.

Remediation Procedure: For step-by-step resolution procedures, see Public buckets detected.

Background Information: In the Oracle Cloud Infrastructure Object Storage service, a bucket is a container for storing objects in a compartment within an Object Storage namespace. The compartment has policies that indicate what actions a user can perform on a bucket and all the objects in the bucket. Object Storage supports anonymous, unauthenticated access to a bucket. A public bucket public that has read access enabled for anonymous users allows anyone to obtain object metadata, download bucket objects, and optionally list bucket contents.

For more background information, see Services.

Require all users to have Multi Factor Authentication (MFA) Enabled

Alert when access to Oracle Cloud without MFA is detected.

Exception: Enter a comma-separated list of OCIDs that should not trigger an alert:

- User OCIDs in the **Do not alert for Users** box.
- Group OCIDs in the **Do not alert for Groups** box.

Recommendation: Enable MFA for all users, using the Oracle Mobile Authenticator (OMA) application on each user's mobile device and the one-time passcode (OTP) sent to the user's registered email address.

Remediation Procedure: For step-by-step resolution procedures, see Enabling Multi-Factor Authentication Security for Oracle Cloud.

Background Information: Multifactor authentication provides an additional layer of security, on top of user name and password. A second verification factor is required each time a user logs in. During the authentication process, users can enable a single device as a trusted device for a maximum period of one day. The email passcode must not be valid for more than 10 minutes. All this provides a degree of protection from password spraying, credential stuffing, and account takeover attacks.

Security list allows unrestricted traffic to non-public port

Alert when a security list uses ports that accept traffic from an open source (0.0.0.0/0).

Restricted ports: Enter comma-separated values for ports which you want to have restricted access. For example, `TCP:[80],TCP:[443-445]`.

Do not alert for: Enter comma-separated values for security list IDs that should not trigger this alert.

Recommendation: Use VCN security lists to restrict network access to instances in a subnet. To prevent unauthorized access or attacks on compute instances, Oracle recommends that you use a VCN security list to allow SSH or RDP access only from authorized ICIDR blocks, rather than leaving them open to the internet (0.0.0.0/0). For additional security, you can temporarily enable SSH (port 22) or RDP (port 3389) access on an as-needed basis, using the VCN API UpdateSecurityList. For performing instance health checks, Oracle recommends that you configure VCN security lists to allow ICMP pings. Exceptions can be configured in Oracle CASB Cloud Service to reduce alerts from exempted security lists with known IP addresses and ports.

Remediation Procedure: For step-by-step resolution procedures, see Security list allows traffic from any IP address (open source).

Background Information: A VCN has a collection of features for enforcing network access control and securing VCN traffic. Security lists provide stateful and stateless firewall capability to control network access to your instances. A security list is configured at the subnet level and enforced at the instance level. You can apply multiple security lists to a subnet where a network packet is allowed if it matches any rule in the security lists.

For more background information, see Services.

Security list allows traffic to restricted port

Alert when a security list of a VCN has inbound rules that accept traffic to:

Restricted ports: Enter comma-separated values for ports that you want to have restricted access. For example, `TCP:[80],TCP:[443-445]`. (TCP, UDP, and ICMP protocols are supported.)

Do not alert for: Enter comma-separated values for security list IDs that should not trigger this alert, in the format, `<SecurityListID>:<Source>:<ProtocolName>:[<ports>]`. For example:

- `SLID1:192.168.0.0/16:TCP:[80,82,83-85]`
- `SLID1:192.168.0.0/0:UDP:[80,82,83-85]`

Recommendation: Ensure that your security lists do not allow the 0.0.0.0/0 IP address range to control access to your instances. While VCNs would require a public facing IP address and an internet facing gateway with an open security list, defense in depth dictates that security lists be limited to known resources. It should be noted that a NAT instance can also provide internet access. Exceptions can be configured in Oracle CASB Cloud Service to reduce alerts from exempted security lists.

Remediation Procedure: For step-by-step resolution procedures, see Security list allows traffic to sensitive ports.

Background Information: A VCN has a collection of features for enforcing network access control and securing VCN traffic. Security lists provide stateful and stateless firewall capability to control network access to your instances. A security list is configured at the subnet level and enforced at the instance level. You can apply multiple security lists to a subnet where a network packet is allowed if it matches any rule in the security lists.

For more background information, see Services.

Standby database is disabled in DataGuard

Alert when a standby database is discovered which is disabled in DataGuard.

Standby DB System should be not in the same AD as primary

Alert when a standby database is discovered in the same AD as the primary.

Configuration: ???

Recommendation: Ensure that the standby database is not in the same AD as the primary.

Remediation Procedure: For step-by-step resolution procedures, see Using Oracle Data Guard.

Background Information: Use of a public IP address to access a database increases your exposure to potential security and business continuity risks.

For more background information, see ???.

Storage Block Volume is not attached

Alert if the block volume is not attached to any of the instances.

Recommendation: Ensure that detaching the block volume is authorized by the OCI administrator.

Remediation Procedure: For step-by-step resolution procedures, see Block volume detached from instance.

Background Information: Detaching a block volume decouples the volume from its associated instance and could affect data available. This could affect data availability from business-critical data to point-in-time copies of volumes as backups.

For more background information, see Services.

Tenancy administrator privilege granted to additional IAM group

Alert if the tenancy administrator privilege is granted to an additional IAM group.

Exceptions: Enter a comma-separated list of OCI tenancy OCIDs that should not trigger this alert.

Recommendation: Verify with the OCI administrator that this entitlement grant was sanctioned and that the membership of the group remains valid after the grant of the administrator privilege.

Remediation Procedure: For step-by-step resolution procedures, see Tenancy administrator privilege grant to an IAM group.

Background Information: Every tenancy comes with a default administrators group, whose members can perform any action on all resources in that tenancy. This high-privilege entitlement must be controlled and restricted to only those users who need it to perform their job functions.

For more background information, see Services.

VCNs with no inbound Security Lists

Alert when a security list of a VCN has ingress rules that accept traffic from an open source (0.0.0.0/0).

Exceptions: Enter comma-separated values for security lists that should not trigger this alert.

Recommendation: Ensure that your OCI VCNs use security lists with ingress or inbound rules to only allow access from known resources. Exceptions can be configured in Oracle CASB Cloud Service to reduce alerts from exempted VCNs.

Remediation Procedure: For step-by-step resolution procedures, see No ingress rules in security lists.

Background Information: A VCN has a collection of features for enforcing network access control and securing VCN traffic. Security lists provide stateful and stateless firewall capability to control network access to your instances. A security list is configured at the subnet level and enforced at the instance level. You can apply multiple security lists to a subnet where a network packet is allowed if it matches any rule in the security lists.

For more background information, see Services.

Virtual Network Interface Cards without associated Network security group

Alert when the a Virtual Network Interface Card (VNIC) without an associated network security group (NSG) is detected.

Exceptions: Enter comma-separated values for Oracle Cloud IDs (OCIDs) of VNICs that should not trigger this alert.

Recommendation: Verify that the configured VNIC is associated with at lest one NSG.

Remediation Procedure: For step by step resolution procedure, see To add or remove a VNIC from a network security group.

Background Information: A VNIC is a networking service component that enables a networked resource such as a Compute instance to connect to a virtual cloud network (VCN). The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN.

2

What's New - Latest Release

This chapter contains the information for the latest release, from "What's New for Oracle CASB Cloud Service."

Topics:

Week of July 28, 2019

This is what's new in the latest release of Oracle CASB Cloud Service.

Component	Description of New Features
Oracle CASB Cloud Service	• Several enhancements have been added for **Oracle Cloud Infrastructure (OCI)** monitoring: – **Bulk registration of compartments**. In one step, you can now register as many compartments from the same OCI instance as you want to. See Adding an OCI Instance. – **Display monitored regions**. When you are adding or updating an OCI instance, you can view the monitored regions for the instance. See Adding an OCI Instance and Updating an OCI Instance. – **New security controls**. When you are updating the security control baseline for an OCI instance, you will now see the new security controls listed below – help links display information for configuring the controls: * IAM password has not been rotated * Compute Instance is running an Oracle image • **Filter values in Access Map.** You can select the type of events that you want in the Access Map by selecting an appropriate value from the **Filter** drop-down. Oracle CASB Cloud Service remembers this selection for the current session. See Dashboard.

View the What's New Archive.