Oracle Security Zones for Oracle Cloud Infrastructure

Oracle Cloud Infrastructure Security

September 2020, Version 1.01.0

Public

Purpose statement

This document provides an overview of features and enhancements included in Oracle Cloud Infrastructure. It is intended solely to help you plan your I.T. projects.

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

Customers need security to be easier to implement and maintain; this the core of Oracle Cloud Infrastructure's approach to cloud security. Customers want more than just a guideline from their cloud service provider. They want a proactive and faster approach from their providers to achieve a better security posture for their applications and infrastructure.

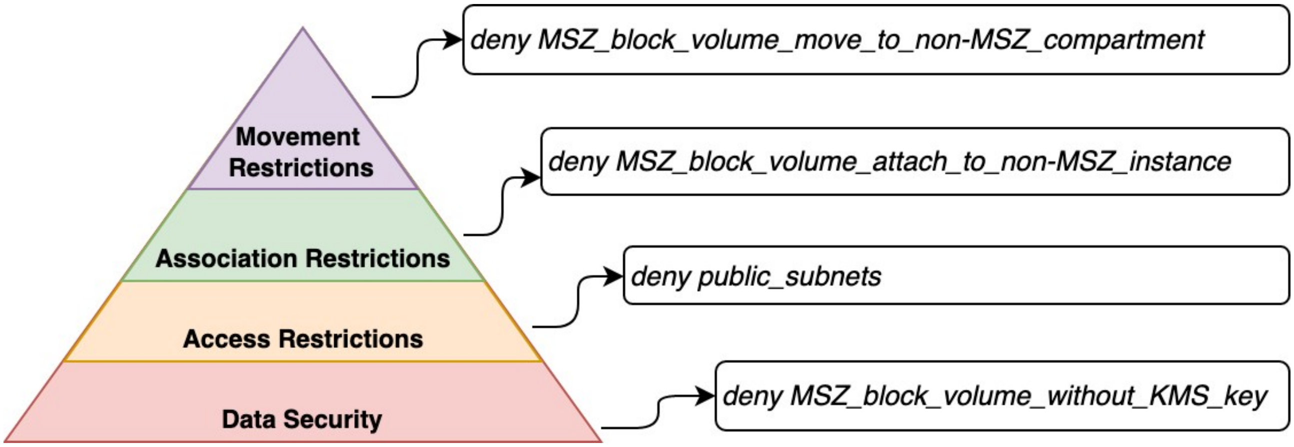
Oracle Cloud Infrastructure Security Zones helps ensure customers implement effective security controls in Oracle Cloud Infrastructure services by enforcing them from the start and removing the chance of someone violating them later. With Security Zones, customers get clarity about what is needed to reach their security objectives at the start. Customers can create a security zone, which is a logical partition that contains a predefined set of security policies. Resources created inside this zone will be subject to all zone policies. These policies build a connection topology to help customers manage their cloud security posture for their compartments.

When creating a security zone, the customer must define what recipe their security zone is associated with. The recipe is a set of policies that are the cornerstones of Oracle Security Zones. Policies define whether an action will weaken security posture and hence, if it should be denied. The first recipe that will be released with Oracle Security Zones will be Oracle's most stringent recipe: Maximum Security Zone. While the Maximum Security Zones recipe and strict policy enforcement may not work in every customer environment, the ability to create a zone with a custom set of policies is expected to be available in the future.

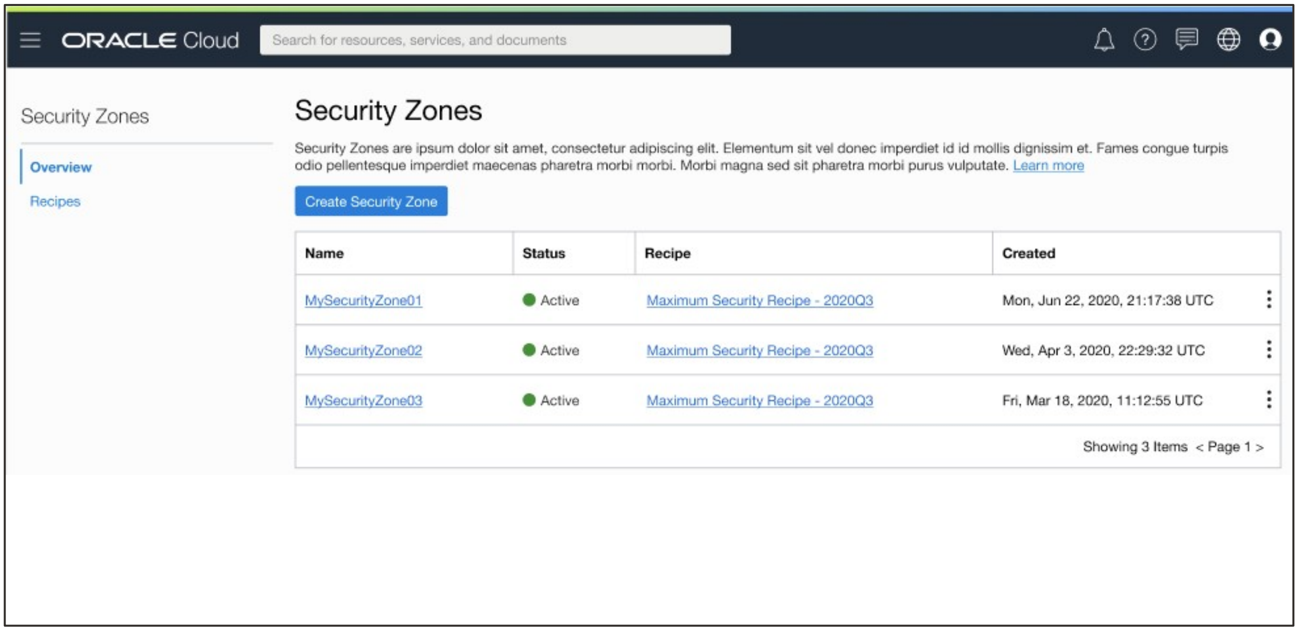
Policy goals have a hierarchical structure, akin to a Maslow diagram. Data Security is the most fundamental requirement, followed by Access, Restrictions, and Movement restrictions. Some examples of such policies are described in the diagram.

- **Data security**: Key Management Service (KMS), or Oracle Vault, is an example of a data security policy which requires that all block volumes must be encrypted with a key. In this case, Oracle is enforcing not only encryption, which greatly enhances security posture, but Oracle Security Zones also enforces the use of KMS. This improves security posture even further by adding an authentication layer for accessing the keys and other best practices such as key rotation and key invalidation.

- **Access restrictions**: An example for access restrictions is the policy preventing the creation of a public subnet.
- **Association restrictions**: An example of association restrictions is a restriction which allows block volumes to be mounted only by compute instances that are also in a security zone.
- **Movement restrictions**: Lastly, an example of movement restrictions is one where customers can use the policy that prevents the movement of a block volume from a security zone to a compartment that is not in such a zone.


Movement Restrictions
Association Restrictions
Access Restrictions
Data Security
deny MSZ_block_volume_move_to_non-MSZ_compartment
deny MSZ_block_volume_attach_to_non-MSZ_instance
deny public_subnets
deny MSZ_block_volume_without_KMS_key

Customers can navigate to the Security Zones console by going to the Security section under the Main menu of the Oracle Cloud Infrastructure interface. The customer journey starts with creating a Security Zone. On creation, the Security Zone is empty of any resource.



Security Zones

Security Zones are ipsum dolor sit amet, consectetur adipiscing elit. Elementum sit vel donec imperdiet id id mollis dignissim et. Fames congue turpis odio pellentesque imperdiet maecenas pharetra morbi morbi. Morbi magna sed sit pharetra morbi purus vulputate. Learn more

Name	Status	Recipe	Created
MySecurityZone01	● Active	Maximum Security Recipe - 2020Q3	Mon, Jun 22, 2020, 21:17:38 UTC
MySecurityZone02	● Active	Maximum Security Recipe - 2020Q3	Wed, Apr 3, 2020, 22:29:32 UTC
MySecurityZone03	● Active	Maximum Security Recipe - 2020Q3	Fri, Mar 18, 2020, 11:12:55 UTC

Showing 3 Items < Page 1 >

When creating a resource in a compartment, which can be used to organize and isolate your cloud resources, that is associated with a security zone, the new resource is subject to **all** of the policies in that Security Zone recipe. Security Zones recipes cannot be applied to resources after they are created. When the customer issues a resource creation request (for example when creating a new storage bucket) in a security zone, those resource parameters and settings are evaluated against all of the policies associated with that security zone. If a resource configuration setting goes against any one of the enforced policies, request to create the resource is denied, and an error message is displayed. The error message will have descriptive text elaborating on the policies that were triggered. As long as there is no conflict with any of the policies, the resource is created. Therefore, Oracle can enforce that all the resources in a security zone follow all of the policies associated with it.

In this way, Oracle helps our customers prevent misconfiguration or accidentally harming their security posture. Learn more about Oracle Security Zones and try Oracle Cloud for free today.

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com   facebook.com/oracle   twitter.com/oracle

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

Disclaimer: This document is for informational purposes. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described in this document may change and remains at the sole discretion of Oracle Corporation.