ORACLE

Managing Emergency Access Accounts in Oracle Cloud Infrastructure

April 2023, version 1.0

Public

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.

Revision History

The following revisions have been made to this document.

DATE	REVISION
April 2023	Initial publication

Table of Contents

Overview **4**

Background **4**

Initial Configuration **4**

Process and Policy Considerations **5**

Securing Emergency Access Accounts **5**

Configuring Password Policies 5

Configuring Multifactor Authentication 7

Monitoring the Use of Emergency Access Accounts **9**

Configuring Alerts 9

Alerting on Changes to the Account 11

Auditing Account Use 11

Conclusion **12**

Overview

This technical paper describes how to implement a mechanism for emergency access to an Oracle Cloud Infrastructure (OCI) tenancy through OCI Identity and Access Management (IAM) without introducing unnecessary risk or contradicting security best practices.

Each OCI tenancy is created with an Administrators group and an associated tenant administration policy that grants full access to the tenancy. As a result, the equivalent of a superuser role is created, and it has permissions to manage all resources within the tenancy. OCI requires at least one user account to be assigned to the Administrators group to avoid customers losing the ability to manage their tenancy. To reduce risk, tenancy owners should use administrative accounts with superuser privileges only when necessary. Membership in the Administrators group should *not* be granted to all OCI cloud administrators. Security best practices suggest that this group should be used only for emergency access (or "break glass") purposes. Other cloud administrators should instead follow the principle of least privilege and be assigned only the access entitlements appropriate for their roles.

Because a user account in the Administrators group is highly privileged and not intended for regular use, several controls can be implemented to reduce the risk associated with such an account while still ensuring that it's available to use when required. This paper provides details on several of the relevant technical controls that can be implemented to achieve that goal.

Background

When an OCI tenancy is created, Oracle sets up a default administrator account for the tenancy. Tenancy owners can use this account to set up additional administrators. This default account is granted administrative privileges through membership in a group called Administrators that resides in the Default OCI IAM identity domain. This group can't be deleted and must always have at least one member.

Each new tenancy also has a policy created automatically that gives the Administrators group access to all the OCI API operations and all the OCI resources in the tenancy. This policy can't be changed or deleted. Any additional accounts added to the Administrators group, therefore, have full access to the entire tenancy and all the resources in it.

The requirement to have at least one member in the Administrators group and the related admin policy ensures that every tenancy has an emergency access account. If this group or policy could be deleted, or if all members could be removed from the group, then it would be possible to create a situation in which no user can assign access, and all users would be locked out of the tenancy.

Initial Configuration

When you create a user account for the purpose of emergency access, you must create it in the Default identity domain and assign it to the Administrators group. Clearly label the account for emergency access by assigning a username such as EmergencyAccess. The intent of this name is to avoid any potential confusion during access reviews.

Even if you access OCI through federated sign-in from an external identity provider, you should create the emergency access account locally. An identity provider outage is a key scenario in which you may require emergency access.

By default, OCI IAM requires an email address to be assigned when a user account is created. The email is used to deliver the initial account password and can also be used for account recovery. The email used for emergency access accounts should be appropriately controlled, and access to the mailbox should be monitored. To reduce the risk of account takeover through the password recovery process, use the guidance in this paper to enable multifactor authentication (MFA) for the emergency access account.

If you optionally create the account without the ability to receive email notifications, then account activation and initial password delivery can be achieved by using IAM APIs. Disabling email-based account recovery requires an account to be created without an email address. You can temporarily remove the email address requirement by disabling the **Primary email address required** setting for the identity domain on the **Domain Settings** page. You can then create the account without an email address before reenabling the email address requirement.

After you create this account and configure policies to create cloud administrators for specific purposes aligned with your security model (for example, identity admins who manage users, security admins who manage policies, storage admins who manage access to storage resources), you should remove any other members from the tenancy's Administrators group.

Note: Users with permission to modify users and groups in the Default identity domain can modify the emergency access user and the Administrators group. Take care with policies that grant these permissions, and review access regularly. You can also configure alerts to be generated when these objects are modified, as described later in this paper.

Process and Policy Considerations

Emergency access accounts for cloud administration should always be handled in accordance with your organization's specific security policies, but there are a few best practices to consider. For example, an emergency access account should have a defined custodian (or group of custodians) who is responsible for managing that account's credential life cycle. The custodian is responsible for rotating and testing credentials after any authorized use of the account during an emergency. The mechanism and timing of this action should be defined in your emergency change management processes. After the emergency access credentials are set or rotated, you can secure them in a physical or virtual safe, which should be, by policy, accessed only during emergency procedures.

Securing Emergency Access Accounts

Because the emergency access account is highly privileged and intended to be used only in controlled situations, the best practice is to implement strong security controls around it. OCI IAM identity domains can be configured to grant specific controls to individual security groups.

Configuring Password Policies

You can apply a specific password policy to the Administrators group by using *group-based password policies* within the Default identity domain. To do this, create a password policy and assign it to the Administrators group with a priority of 1, which is the highest priority in OCI IAM identity domains, as shown in the following screenshot. This combination of settings ensures that accounts in the Administrators group are subject to these new password controls instead of the *default password policy*.

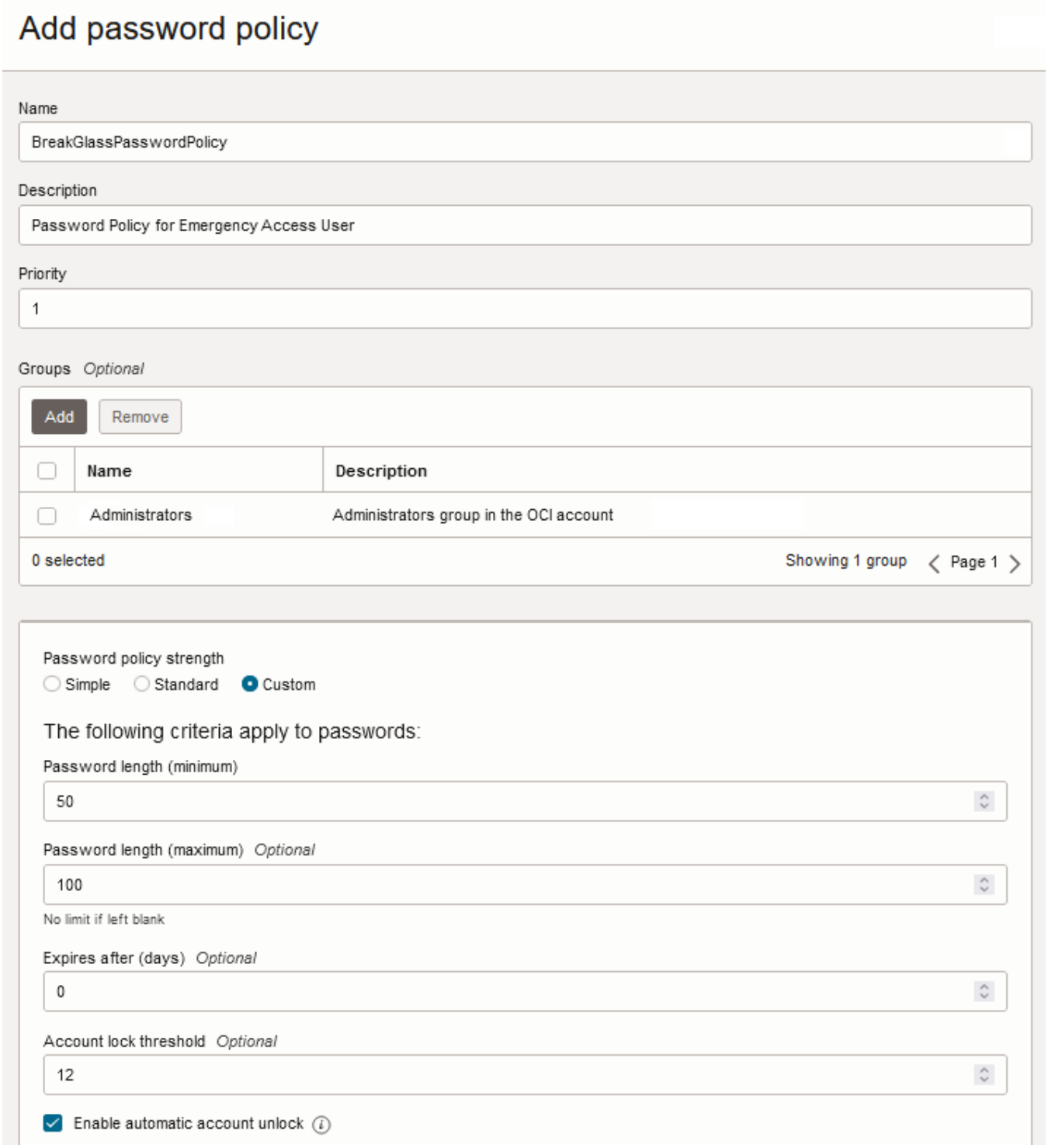

Figure 1: Password Policy for Emergency Access Accounts

You can configure this password policy to use a custom password strength, and then set the appropriate values, such as a 50-character minimum password length and removal of account expiration.

The specific values that you select for the password rules should follow your organization's security policies. However, a minimum length of 50 characters is a practical choice because it's virtually impossible to guess or to discover with a brute-force attack, while remaining reasonable to enter accurately.

Configuring Multifactor Authentication

Because the account is highly privileged, a best practice is to configure additional authentication factors beyond username and password. However, you should also ensure that the account login is not bound to a device or individual user that might not be available when emergency access is required. Using a Fast ID Online (FIDO) security key stored in the same physical safe as the password might be a good multifactor authentication (MFA) option for emergency access accounts.

You can configure MFA settings to apply specifically to the Administrators group by creating a sign-on rule in the default sign-on policy. You can use this rule to require specific factors for the emergency access account or to exempt the emergency access account from using MFA.

Important: A default sign-on policy is configured by default for all OCI tenancies, which means that an incorrect configuration might make you unable to recover access to the tenancy. When modifying this policy, *do not* log out of the session that is being used to modify the policy until you confirm that you're still able to access the environment in an alternative browser or private browser session.

Within the default sign-on policy, create a new rule for which membership in the Administrators group is the only condition, as shown in the following screenshot.

Figure 2: Creating a Sign-On Rule for Members of the Administrators Group

Ensure that **Allow access** is selected; denying access to all Administrators could prevent you from being able to recover access to the tenancy. Configure the actions associated with this rule to apply an appropriate authentication mechanism, either a specific authentication factor or allowing access with no additional factor required. The following screenshot shows a configuration in which a FIDO authenticator is required.

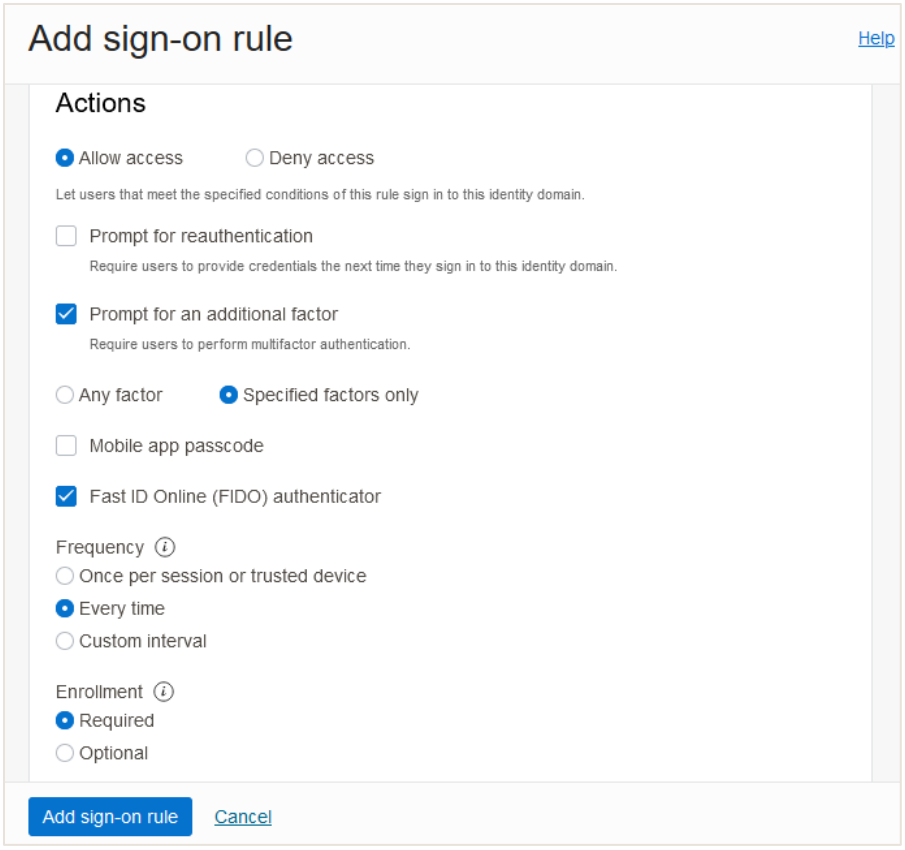

Figure 3: Configuring Sign-On Rule Actions to Require Emergency Access Accounts to Always Authenticate Using a FIDO Authenticator

When configuring the use of MFA, you can change **Frequency** to **Every time** to disallow the creation of *trusted devices*, which bypass the MFA requirement when the device is recognized from a previous session. You can also set **Enrollment** to **Required** to force all group members to enroll in MFA. OCI IAM challenges the user each time if they have enrolled in MFA. If the emergency access account authenticates using a different challenge mechanism, then you can specify that factor by using the **Specified factors only** option.

Because sign-on rules in a policy are evaluated in order until a match to the conditions is found, this new rule must be first in the evaluation order to ensure that it's always applied to the emergency access account. You do this by editing the rule priority and moving the new rule to the top of the list, as shown in the following screenshot.

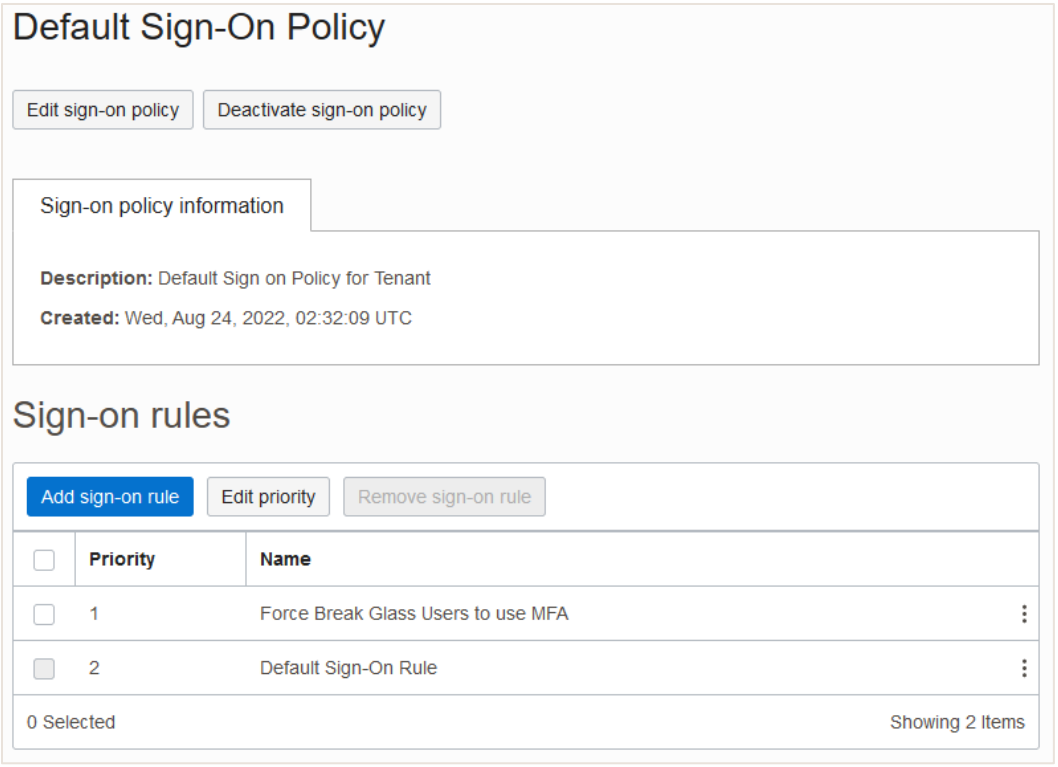

Figure 4: Sign-On Rule Priority Ensures That the Appropriate Rule Is Applied to Emergency Access Accounts

After the new sign-on rule is in place, if MFA was enabled, an emergency access account custodian should sign in to OCI to trigger an initial MFA enrollment. After MFA enrollment is configured and the authentication flow is tested, the credentials and any associated material required for MFA should be rotated and stored according to emergency access policies.

By configuring group-based password policies and group-based conditions in a sign-on rule, access controls for emergency access accounts can be configured independently of other accounts. This separation enables administrators to manage access controls for groups of users without impacting all other accounts in the tenancy.

Monitoring the Use of Emergency Access Accounts

Emergency access accounts are highly privileged and not intended for regular use. We recommend that you treat any use of these accounts as a potential breach of security policies and evaluate each use accordingly.

Configuring Alerts

OCI provides several services that you can configure to alert other administrators in the environment when the emergency access account is accessed. The OCI Events service provides a flexible mechanism for configuring automated responses to events of interest in many OCI services, including OCI IAM. You can use Events to send alerts through the OCI Notifications service.

First, configure a Notifications topic in OCI to use to send administrator alerts.

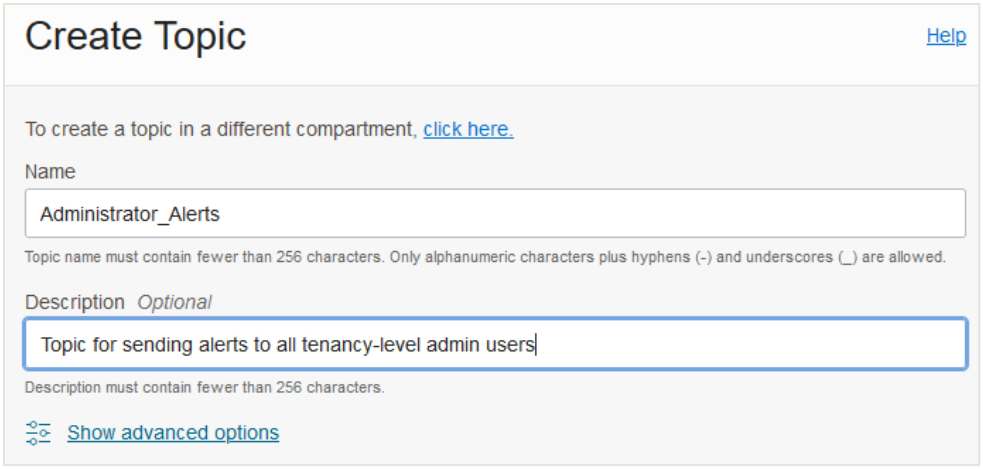

Figure 5: Creating a Notifications Topic to Use to Alert Administrators About the Use of the Emergency Access Accounts

After you create a topic, you can add one or more subscriptions, which receive notifications when triggered by an event. These notifications can be sent as emails, sent to Slack or PagerDuty, or trigger alternative notification workflows through OCI Functions or subscribing webhooks. Select a mechanism appropriate to the preferred methods of operation for your administrators.

To automate the sending of notifications to administrators when an emergency access account is used, create an event rule in the Events service, specifying **Identity SignOn** as the service and **Interactive Login** as the event type. You can then add a condition to match on the **actorName** attribute. The following screenshot shows an example event definition.

Note: Because interactions with the Default identity domain occur in the root compartment, this rule must be created in that top-level compartment.

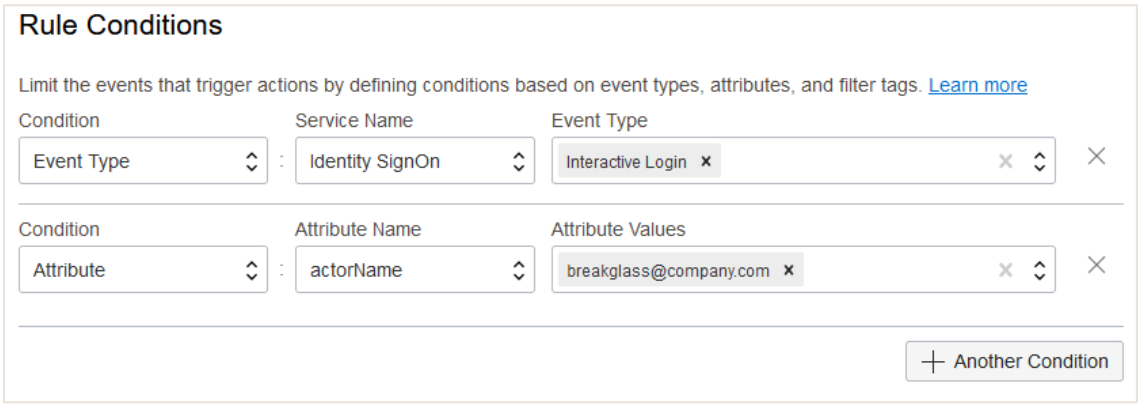

Figure 6: Configuring an Event Rule to Capture an Authentication Event by Emergency Access Accounts

With this configuration in place, when an emergency access account is used, other administrators are notified, and appropriate responses should be captured in their runbooks. Appropriate responses might involve validating the access against existing open issues or Operations Center responses, or account recovery workflows if the use of the emergency access account is deemed inappropriate or malicious.

Alerting on Changes to the Account

You can use a similar configuration to alert on changes to the emergency access account, such as adding the ability to create an API key or other potentially problematic behaviors. Such changes cause the **Identity** service to emit **Update** events, which can be triggered by using the configuration shown in the following screenshot. In this configuration, the conditions check the **resourceName** of the modified user resource, as opposed to the actor, because this change might be made by a different user, such as an account custodian or IAM admin.

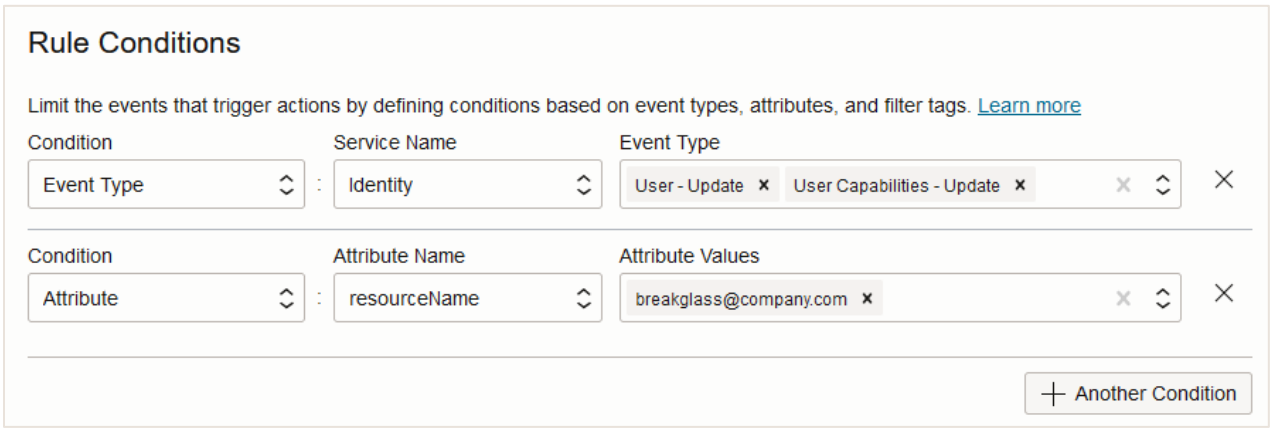

Figure 7: Configuring an Event Rule to Capture Any Changes to the Emergency Access Account

As an additional precaution, you can configure an alert for when another user is added to the Administrators group. Because this group is being used only for emergency access accounts, adding a user to it represents a violation of the security policies for the tenancy. This event definition also uses the **Identity** service, with the **Group - Add User To** event type, using the group name as a condition.

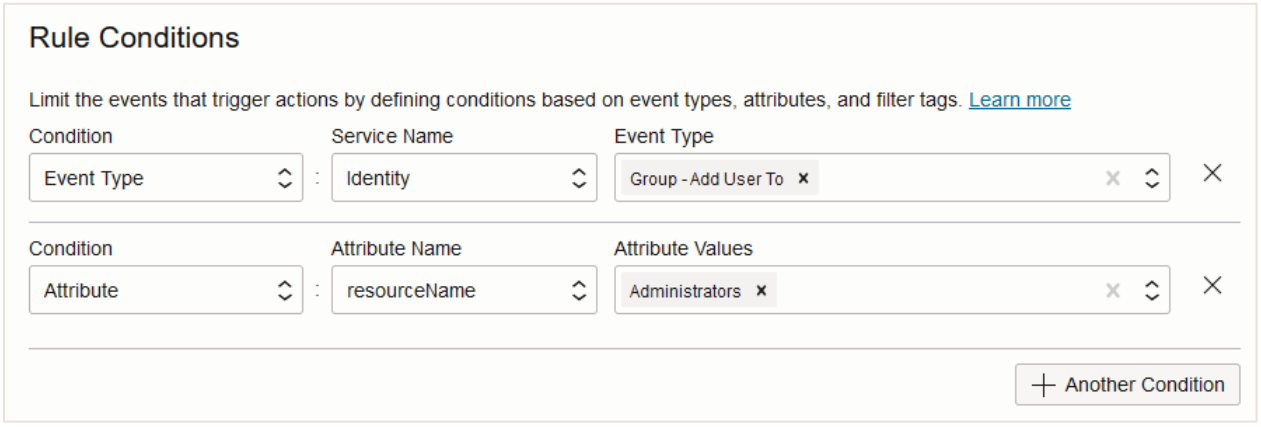

Figure 8: Configuring an Event Rule to Capture Any Changes to the Administrators Group

Auditing Account Use

All OCI administration activities are recorded by the OCI Audit service. As a result, no additional configuration is required to ensure that use of the emergency access account is logged and that those logs are protected from malicious modification. Depending on your organization's specific security policies, you might want to configure archiving and retention policies for the Audit logs, by using a combination of OCI's Service Connector Hub and Object Storage services. In addition, you can use Service Connector Hub to forward the Audit logs to a Security Incident and Event Management (SIEM) tool.

Conclusion

This paper provides guidance on how to implement a mechanism for emergency access to an OCI tenancy without introducing unnecessary risk or contradicting general security best practices. This configuration uses the built-in Administrators group and its related security policy, which grants full access to the tenancy. The paper discusses how to enable strong authentication for emergency access accounts, as well as alert on and audit the use of these highly privileged accounts. The details provided are informational only. Although they intend to adhere to general security best practices, tenancy administrators should defer to their organization's own security policies.

For more information, see the OCI Security Best Practices documentation and OCI IAM with identity domains documentation.