Creating Administrative Users, Groups, and Policies

Creating Administrative users, groups and policies on the Oracle Private Cloud Appliance X9-2

May 9, 2022 | Version 1.01

PURPOSE STATEMENT

This document provides an overview of features and enhancements included in release 3.0.1. It is intended solely to help you assess the business benefits of upgrading to 3.0.1 and to 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.

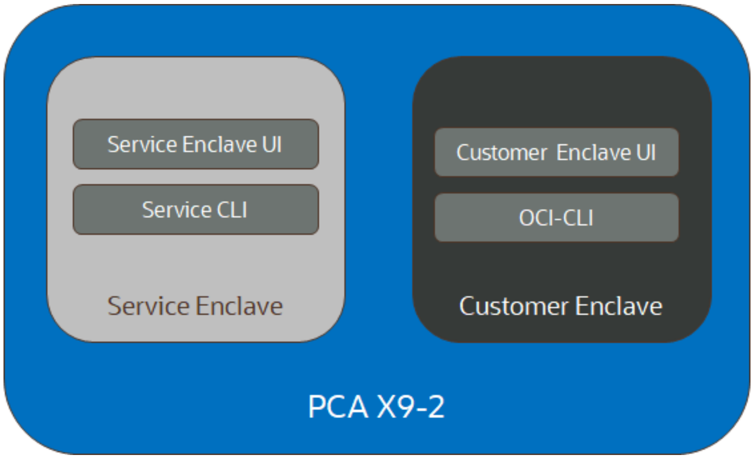
Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

WHITE PAPER GUIDELINES

Introduction

The PCA X9-2 administrative experience is very different from previous generations of PCA. In fact, there's very little that has been carried over from the older platform. While it's completely new for the PCA product line - it's not something that's completely new for Oracle Cloud Infrastructure (OCI) users. This reflects one of the main goals that our developers had - to create an on-premise product that looks and acts like our OCI products. If you are familiar with the OCI Console and the OCI CLI, then by default you're already ahead of the curve and your experience with the PCA X9-2 will be a very easy transition.

However, since the PCA X9-2 is an on-premise solution and OCI is of course a cloud solution, there will be some fundamental things that users of the PCA X9-2 will be responsible for that users of OCI would never be responsible for. For example, in OCI we have an operations team that maintain the hardware that the services run on. With an on-premise solution, that responsibility typically falls to the customer. To enable this, we have created two different and distinct planes of control that a customer will operate in. The first is the Customer Enclave, which is the same level of interaction that users have with OCI, including the Console and the CLI. The second is the Service Enclave, which is the on-premise equivalent of the OCI operations team. This is where the hardware is maintained and cared for.



In this paper we're going to discuss Administrative users, groups and the associated policies that go with them in the Service Enclave of the PCA X9-2.

Users & Groups

The Identity and Access Management service (IAM) lets you control who has access to the cloud resources within your tenancies. Note it is the task of a tenancy administrator to control what type of access a user group has, and to which specific resources that access applies. The responsibility to manage and maintain access control can be delegated to other privileged users, for instance by granting them full access to a sub-compartment of the tenancy.

Appliance administrator accounts are managed separately and provide access to appliance administration functions. This functionality is not related to the tenancy-level IAM service. (For more information, see the online online documentation, Section 3.1, "Administrator Access", in the chapter Appliance Administration Overview.

When a tenancy is created, a default user account is added to allow you to log in and perform initial setup tasks. This default user is included in a group named Administrators, which provides full access to all resources and operations within the tenancy. The group cannot be deleted and must always contain at least one user.

Once logged in, the tenancy administrator can start adding more users and organize them into groups. A group is a set of users who have the same type of access to a particular set of resources. The general principle is that users have no access rights at all, unless they have been explicitly granted permission.

User accounts can be created locally in the tenancy, but Oracle Private Cloud Appliance also supports federating with an existing identity provider. In this configuration, a tenancy administrator sets up a federation trust relationship between the tenancy and the identity provider, allowing users log in with their existing id and password. Federation configurations are outside of the scope of this article, however, detailed information can be found n the online documentation, Section 4.3, "Federating with Identity Providers".

The permission to access a resource and perform an operation is defined in a policy. Policies are defined to manage specific permissions. For more information, see the online documentation, Section 4.5, "How Policies Work".

To group and isolate resources, you organize them into compartments. Compartments are primary building blocks in a tenancy. You can compare them to the directories in a file system structure, where the tenancy is equivalent to the root directory. Compartments also help control and secure the access to resources. Unlike administrators, regular users only see the compartments to which they have access. Policy statements further refine the type of access. For more information, see the online documentation, Section 4.4, "Organizing Resources in Compartments".

As an example of how users, groups, compartments, resources and policies interact with each other, consider the following scenario. You decide to create groups for different teams in your organization and assign a separate compartment for each team's resources. You allow each team to create and use instances within their compartment but prevent them from accessing the resources of another team. In addition, you might prefer to let a network administrator manage all network resources in the tenancy. To achieve this, you create all network-related resources in a dedicated network compartment, which only a network administrator is allowed to manage. Other users need to be allowed to use the network resources in their configurations, but they should not have permission to modify the network setup.

User Credentials

There are two types of credentials to be aware of with regard to users, *passwords* and *API signing keys*. Passwords should be well understood by any systems administrator. In PCA, passwords are created when a new user account is generated and are sent to the user via a secure method. When the user signs in for the first time, they are prompted to change their password. NOTE: After 7 days, the one-time password expires and a new one must be created by an administrator.

Users who need to make API requests must have an RSA public key added to their user profile. Both the private and public key must be in PEM format, with a minimum length of 2048 bits. Users either generate a private/public key pair through the Compute Web UI and download the private key, or generate the key pair on their local machine and upload the public key to their profile.

Alternatively, a tenancy administrator can generate the API keys and complete the profile setup for all users. This is a requirement for non-human user accounts: systems that make API requests without human operation. For such systems, the administrator needs to create a user account with signing keys, but without password.

On the system from where API requests are sent, a directory named .oci must be created inside the user home directory. The .oci directory must contain a configuration file with required parameters for interaction with the API server. Make sure it lists the correct path to where the private key file is stored, if it is not in the same directory. API requests are signed using the private key.

A user account can contain a maximum of 3 API signing keys at a time. API signing keys are different from the SSH keys you use to access a compute instance.

Compartments

After initial setup, your tenancy only contains a root compartment. A tenancy administrator needs to perform setup tasks and establish an organization plan. The plan should include the compartment hierarchy for organizing your resources and the definitions of the user groups that need access to the resources. These two things impact how you write policies to manage access, and therefore should be considered together. While an extensive review of compartments is beyond the scope of this article, the use of compartments can be broadly divided into two approaches; a) Everything in the Root compartment, and b) Separate Compartments for departments, projects, or some other organizational or relational designation. For the purposes of simplicity, we will assume that everything is in the root compartment. If you would like to better understand the possible uses of compartments, please see Section 4.4 of the online documentation, Organizing resources in Compartments, https://docs.oracle.com/en/engineered-systems/private-cloud-appliance/3.0/concept-3.0.1/iam-overview.html#iam-compartments

Groups

There are three groups into which administrative users may be placed:

Access to the administrative functionality is provided through separate interfaces: a Service Web UI, a Service CLI and a Service API, which are all highly restricted. Administrative functionality includes hardware management, tenancy management, system and component upgrade, system backup and restore, monitoring, and so on. Infrastructure administrators have one or more of the roles described below:

SuperAdmin	Administrators with the *SuperAdmin* role have unrestricted access to the Service Enclave. They are authorized to perform all available operations, including the setup of other administrator accounts and management of authorization groups (admin roles).
Admin	The *Admin* role grants permission to list, create, modify and delete practically all supported object types. Permissions excluded from this role are: administrator account and authorization group management, and disaster recovery operations.
Monitor	Administrators with a *Monitor* role are authorized to execute read-only commands. For example, using the `get` API calls, they can list and filter for objects of a certain type. Some objects related to specific features, such as the disaster recovery items, are excluded because they require additional privileges.

Policies

A policy is a document that specifies who can access which cloud resources in your tenancy, and how. A policy simply allows a group to work in certain ways with specific types of resources in a particular compartment. If you are not familiar with users, groups, or compartments, refer to the respective sections in the chapter Identity and Access Management Overview. https://docs.oracle.com/en/engineered-systems/private-cloud-appliance/3.0/concept-3.0.1/iam-overview.html For additional detail on how to create and use policies, please see Section 4.5 How Policies Work in the online documentation. https://docs.oracle.com/en/engineered-systems/private-cloud-appliance/3.0/concept-3.0.1/iam-overview.html#iam-policies

Managing Administrative Users

Users may be created and managed via the Service Enclave CLI or the BUI. To create a user in the CLI, ssh to the administrative enclave as an administrative user and create the user via the CLI as follows:

```
ssh admin@adminenclave -p 3006
Password:
PCA-ADMIN> list AuthorizationGroup
Command: list AuthorizationGroup
Status: Success
Time: 2021-08-25 08:38:58,632 UTC
Data:
  id                                     name
  --                                     ----
  587fc90d-3312-41d9-8be3-1ce21b8d9b41   MonitorGroup
  c18cc6af-4ef8-4b1c-b85d-ee3b065f503e   DrAdminGroup
  8f03faf2-c321-4455-af21-75cbffc269ef   AdminGroup
  5ac65f5d-1f8c-42ea-a1de-95a1941f009f   Day0ConfigGroup
  365ece7b-0a09-4a04-853c-7a0f6c4789f0   InternalGroup
  7da8be67-758c-4cd6-8255-e9d2900c788e   SuperAdminGroup
```

You may now create a new user in whichever authorization group you require:

```
PCA-ADMIN> createUserInGroup name=newuser password=************
confirmPassword=************ authGroup=365ece7b-0a09-4a04-853c-7a0f6c4789f0
Command: createUserInGroup name=testadmin password=***** confirmPassword=*****
authGroup=365ece7b-0a09-4a04-853c-7a0f6c4789f0
Status: Success
Time: 2021-08-25 08:48:53,138 UTC
JobId: 6dd5a542-4399-4414-ac3b-636968744f79

PCA-ADMIN> show user name=newuser
Command: show User name=newuser
Status: Success

Time: 2021-08-25 08:50:04,245 UTC
Data:
  Id = 682ebc19-8493-4e9a-817c-148acea4b1d4
  Type = User
  Name = newuser
  Default User = false
  AuthGroupIds 1 = id:365ece7b-0a09-4a04-853c-7a0f6c4789f0 type:AuthorizationGroup
name:InternalGroup
  UserPreferenceId = id:1321249c-0651-49dc-938d-7764b9638ea9  type:UserPreference
name:
```

User parameters may, of course, be changed. For example, to change the above user's password, use the `changepassword` command.

```
PCA-ADMIN> changePassword id=682ebc19-8493-4e9a-817c-148acea4b1d4
password=************ confirmPassword=************
Command: changePassword id=682ebc19-8493-4e9a-817c-148acea4b1d4 password=*****
confirmPassword=*****
Status: Success
Time: 2021-08-25 09:22:55,188 UTC
JobId: 35710cd9-26ac-4be9-8b73-c4cf634cc121
```

Some of the other commands that you may find useful are:

Delete a user account:

```
PCA-ADMIN> delete User name=testadmin
Command: delete user name=testadmin
Status: Success
Time: 2021-08-25 09:20:09,249 UTC
JobId: 56e9dfcb-6b64-4f9d-b137-171f538029d3
```

List users

```
PCA-ADMIN> list User
Command: list User
Status: Success
```

```
Time: 2021-08-25 08:49:01,064 UTC
Data:
  id                                     name
  --                                     ----
  401fce73-5bee-48b1-b86d-fba1d85e049b   admin
  682ebc19-8493-4e9a-817c-148acea4b1d4   testadmin
```

Add an admin to an authorization group:

```
PCA-ADMIN> list User
Command: list User
Status: Success
Time: 2021-08-25 08:49:01,064 UTC
Data:
  id                                     name
  --                                     ----
  401fce73-5bee-48b1-b86d-fba1d85e049b   admin
  682ebc19-8493-4e9a-817c-148acea4b1d4   testadmin
```

Remove an admin from an authorization group:

```
PCA-ADMIN> remove User name=testadmin from AuthorizationGroup id=587fc90d-3312-
41d9-8be3-1ce21b8d9b41
Command: remove User name=testadmin from AuthorizationGroup id=587fc90d-3312-41d9-
8be3-1ce21b8d9b41
Status: Success
Time: 2021-08-25 09:10:39,249 UTC
JobId: 44110d28-70af-4a42-8eb7-7d59a3bc8295
```

Change a password:

```
PCA-ADMIN> list User
Command: list User
Status: Success
Time: 2021-08-25 09:22:01,064 UTC
Data:
  id                                     name
  --                                     ----
  401fce73-5bee-48b1-b86d-fba1d85e049b   admin
  682ebc19-8493-4e9a-817c-148acea4b1d4   testadmin
```

```
PCA-ADMIN> changePassword id=682ebc19-8493-4e9a-817c-148acea4b1d4
password=************ confirmPassword=************
Command: changePassword id=682ebc19-8493-4e9a-817c-148acea4b1d4 password=*****
confirmPassword=*****
Status: Success
Time: 2021-08-25 09:22:55,188 UTC
JobId: 35710cd9-26ac-4be9-8b73-c4cf634cc121
```

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.

Creating Administrative Users, Groups, and Policies
May 2222
Author: Bob Bownes
Contributing Authors: