ERICSSON

Infrastructure Administrator Management Guide

Cloud Execution Environment

USER GUIDE

3/1553-CRA 119 1864/5 Uen A

Contents

1 Introduction

This User Guide (UG) contains information about the Cloud Execution Environment Identity and Access Management (CEE IdAM) tool, that is used to manage identities and credentials for Cloud Infrastructure Administrators, and to provide authentication and access control services for user accesses.

1.1 Prerequisites

The user of this document must be familiar with the following software and protocols:

- Linux operating system
- Lightweight Directory Access Protocol (LDAP)
- Using ‘‘sudo’’ to manage users with `superuser` privileges

The user of this document must have `superuser` privileges to be able to use the CEE IdAM tool. These privileges are available for root user and users who are members of the `sudo`, `ceesudo`, or `ceeuseradmin` groups.

2 CEE IdAM Architecture

The IdAM architecture in the CEE is shown in Figure 1.

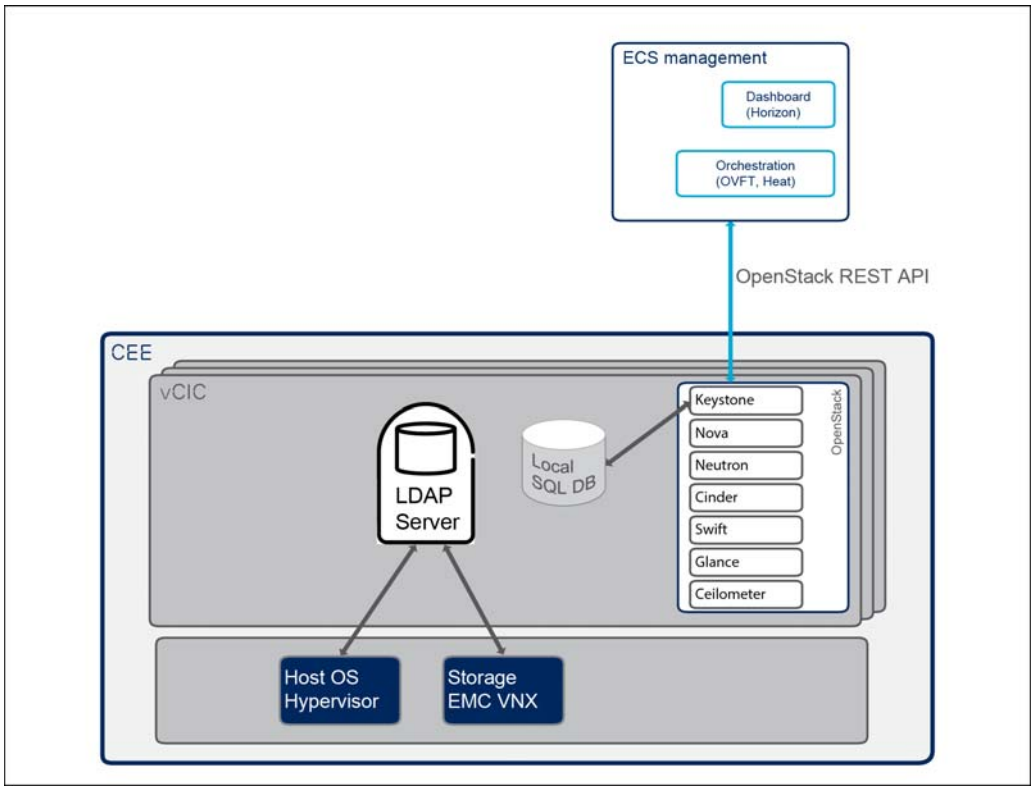

Figure 1 CEE IdAM Architecture

For a functional description of IdAM components, refer to *CEE Technical Description*.

3 User Roles

The Cloud Infrastructure Administrator name in CEE is `infra-admin`, which manages the following CEE infrastructure components:

- Compute blades
- Network switches
- Cloud Infrastructure Controllers (CICs)
- Storage system

Note: Linux users, storage system users (EMC VNX), and network device users (Extreme switches) are considered to be infrastructure users.

Cloud Infrastructure Administrator identities are stored in a High Available LDAP (HA-LDAP) directory server. The provisioning of `infra-admin` creates a new record in the LDAP back-end database.

4 Privileged Access

Users are granted privileged access through sudo. Sudo privileges are available for users who are members of one of the sudo groups. The default sudo configuration is located in the `/etc/sudoers/` directory. The CEE IdAM specific sudo settings can be configured in the `/etc/sudoers.d/cee_sudoers` file.

The predefined sudo groups are as follows:

- `sudo`

  This is the default system sudo group. It prompts users for password when executing a **`sudo`** command.

- `ceebackup`

  Members of this group are used for backup and restore processes and are allowed to issue **`sudo`** commands without being prompted for the password.

- `ceesudo`

  Members of this group are allowed to issue **`sudo`** commands without being prompted for the password.

- `ceeuseradmin`

  The members of this group are allowed to execute **`sudo cee-idam`** commands without being prompted for a password.

- `ceestatus`

  The members of this group are allowed to query `crm` status with **`sudo`**, without being prompted for a password.

4.1 Granting Superuser Privileges

A new user that has been created with the CEE IdAM tool has no superuser privileges by default.

To grant superuser privileges for a user, the user must be added to one of the predefined `sudo` user groups.

To add the user to one of the sudo groups issue the following command:

`sudo cee-idam user-modify -l` ***`<LOGIN>`*** **`-G`** ***`<GROUP>`***

Arguments:

- `-l <LOGIN>`, `--login <LOGIN>`

  User's login.

- `-G <GROUP>`, `--group <GROUP>`

  Add user to group.

Example 1 shows how to add the user “exampleuser” to the `sudo` user group.

```
<personal-user>@cic-1-0:~$ sudo cee-idam user-modify
-l exampleuser -G sudo
CEEIDAM (SUCCESS): User `exampleuser` is now member of group `sudo`
User modification completed
```

Example 1 Adding exampleuser to the sudo User Group

This user is now able to use `sudo` commands to execute commands that require superuser privileges.

5 Password Policies

The CEE IdAM tool supports the use of password policies for users provisioned by the LDAP repository. For more information refer to the OpenLDAP documentation, Reference [1].

5.1 Predefined Password Policies

There are three predefined password policies:

Standard Policy This is the default password policy applied to new users, if no other policy is specified. Password expiry is enabled and temporarily locks the user out after multiple failed login attempts.

Restricted Policy

This password policy is intended for users with a more strict password policy than the standard one.

Service Policy This password policy is for service accounts used for scripted access or system services, that are intended to function, for example, without password expiry to avoid service interruption.

Note: For user accounts without password expiration it is strongly recommended to set the Service policy.

Table 1 describes the configuration parameters and lists the preconfigured values for the three predefined policies.

Table 1 Password Policy Parameters and Default Values

Parameter	Description	Default Value		
		Standard policy	Restricted policy	Service policy
`pwdAttribute`	Holds the name of the attribute to which the password policy is applied.	*<userPassword>*	*<userPassword>*	*<userPassword>*
`pdwLockout`	If this attribute is set "TRUE", then the password is not used to authenticate after a specified number of consecutive failed bind attempts. The maximum number of consecutive failed bind attempts is specified in the `pwdMaxFailure` attribute. If this attribute is "FALSE", then the password remains valid regardless of failed attempts.	TRUE	TRUE	FALSE
`pwdLockoutDuration`	This attribute specifies in seconds how long the password cannot be used to authenticate due to too many failed bind attempts. If this attribute is not present, or if the value is "0", the password cannot be used to authenticate until a password administrator resets it.	1800	1800	0

Table 1 Password Policy Parameters and Default Values

pwdInHistory	Specifies the maximum number of used passwords stored in the pwdHistory attribute.	6	10	6
pwdCheckQuality	Indicates how the password quality is verified while being modified or added. If this attribute is not present, or if the value is “0” quality checking is not enforced. A value of “1” indicates that the server performs the password quality check. If the server is unable to check the quality (for example, due to a hashed password) the password will still be accepted. A value of “2” indicates that the server checks the quality, and if it is unable to verify, it returns an error refusing the password.	2	2	0
pwdExpireWarning	Specifies the maximum number of seconds before a password is due to expire and the expiration warning messages are returned to an authenticating user. If this attribute is not present, or if the value is "0", no warnings are returned. If not "0", the value must be smaller than the value of the pwdMaxAge attribute.	1296000	1296000	0
pwdMinAge	Holds the number of seconds that must elapse between modifications to the password.	0	1800	3600
pwdMaxAge	Holds the number of seconds after which a modified password expires. If this attribute is not present, or if the value is "0", the password does not expire. If not "0", the value must be greater than or equal to the value of the pwdMinAge.	7776000	7776000	0
pwdMinLength	When quality checking is enabled, this attribute holds the minimum number of characters that must be used in a password. If this attribute is not present, no minimum password length is enforced.	12	12	12
pwdGraceAuthNLimit	This attribute specifies the time limit of the grace authentications validity in seconds. If this attribute is not present or if the value is "0", no time limit applies on the grace authentications.	3	2	0
pwdAllowUserChange	This attribute indicates whether users can change their own passwords, although the change operation is still subject to access control. If this attribute is not present, the "TRUE" value is assumed. This attribute is intended to be used in the absence of an access control mechanism.	TRUE	TRUE	FALSE
pwdMustChange	This attribute specifies whether users must change their passwords when they first bind to the directory after a password is set or reset by a password administrator. If this attribute is not present, or if the value is "FALSE", users are not required to change their password upon binding after the password administrator sets or resets the password. This attribute is not set due to any actions specified by this document, it is typically set by a password administrator after resetting a user password. (Setting this value to TRUE does not force user to change password during first SSH login)	TRUE	TRUE	FALSE

Table 1 Password Policy Parameters and Default Values

pwdMaxFailure	This attribute specifies the number of consecutive failed bind attempts after which the password is not used to authenticate. If this attribute is not present, or if the value is "0", this policy is not checked, and the value of pwdLockout is ignored.	3	1	5
pwdFailureCountInterval	This attribute controls when the count of consecutive password failures is reset. If the attribute value is 0 (the default) the count of consecutive password failures is only reset on successful authentication. If the attribute value is greater than 0 it defines the time - in seconds - after which the count of consecutive password failures is reset, even if no successful bind attempt (authentication) has occurred.	120	120	120
pwdSafeModify	This attribute specifies whether the existing password must be sent along with the new password when being changed. If this attribute is not present, "FALSE" value is assumed. This attribute is not supported. The value MUST NOT be set to “TRUE”.	FALSE	FALSE	FALSE

5.2 Password Policy Management

This section describes how to create, modify, and delete password policies.

Note: The user managing the password policies must be a member of the predefined LDAP group `DirectoryAdmins` (`gidNumber` “10000”).

5.2.1 Creating a Policy

To create a policy, follow these steps:

1. Create a file with the following content on a CIC:

```
dn: cn=<MyPolicyName>,ou=Policies,<DcValues>
objectClass: top
objectclass: device
objectClass: pwdPolicy
cn: <MyPolicyName>
pwdAttribute: <UserPassword>
pwdLockoutDuration: 1800
pwdInHistory: 6
pwdCheckQuality: 1
pwdExpireWarning: 1296000
pwdMinAge: 0
pwdMaxAge: 7776000
pwdMinLength: 12
pwdGraceAuthNLimit: 3
pwdAllowUserChange: TRUE
pwdMustChange: TRUE
pwdMaxFailure: 3
pwdFailureCountInterval: 120
```

```
pwdSafeModify: FALSE
```

2. Replace the *<MyPolicyName>*, *<DcValues>*, and *<UserPassword>* with the appropriate values. *<DcValues>* is to be taken from `ericsson.idam.ldap.basedn` in config.yaml. For example `dc=cee,dc=ericsson,dc=com`.

3. Save the file as *<MyFile>*`.ldif`.

4. Apply the file with the following command:

```
ldapmodify -a -H ldap://192.168.2.21:389 -x -D ⇒
"cn=ldapadmin,ou=DirectoryAdmins,<DcValues>" -f ⇒
<MyFile>.ldif
```

5.2.2 Modifying a policy

To modify a policy follow these steps:

1. Create a file with the following content on a CIC:

```
dn: cn=<PolicyName>,ou=Policies,<DcValues>
changetype: modify
replace: <PolicyAttribute>
<PolicyAttribute>: <NewValue>
```

2. Replace the *<PolicyName>*, *<DcValues>*, *<PolicyAttribute>*, and *<NewValue>* with the appropriate values. *<DcValues>* is to be taken from `ericsson.idam.ldap.basedn` in config.yaml. For example `dc=cee,dc=ericsson,dc=com`.

3. Save the file as *<MyFile>*`.ldif` extension.

4. Apply the file with the following command:

```
ldapmodify -H ldap://192.168.2.21:389 -x -D ⇒
"cn=ldapadmin,ou=DirectoryAdmins,<DcValues>" -f ⇒
<myFile>.ldif
```

5.2.3 Delete a Policy

To delete a policy follow these steps:

1. Create a file with the following content on a CIC:

```
cn=<MyPolicyName>,ou=Policies,<DcValues>
```

2. Replace the *<MyPolicyName>* and *<DcValues>* with the appropriate values. *<DcValues>* is to be taken from `ericsson.idam.ldap.basedn` in config.yaml. For example `dc=cee,dc=ericsson,dc=com`.

3. Save the file as *<MyFile>*`.ldif` extension.

4. Apply the file with the following command:

```
ldapdelete -H ldap://192.168.2.21:389 -Wx -D ⇒
"cn=ldapadmin,ou=DirectoryAdmins,<DcValues>" -f ⇒
<MyFile>.ldif
```

5.3 Mapping Password Policies

A password policy can be mapped to the user when that user is created, or by modifying the existing user. By default the Standard policy is applied during the creation of a user if no specific policy is defined.

To add a user to a policy issue the following command:

```
sudo cee-idam user-modify -P <PolicyName> -l <UserLogin>
```

To force a password change during the first login the administrator must issue the following command:

```
sudo cee-idam user-modify -e -l <UserLogin>
```

6 Managing Cloud Infrastructure Users

The following subsections provide information about the CEE IdAM tool functions for managing infrastructure users in the LDAP database.

The following command provides information about the available subcommands:

```
sudo cee-idam -h
```

The following command provides information about the options for the given subcommand:

```
sudo cee-idam <subcommand> -h
```

Note: The following instructions only apply to LDAP users. Local user accounts are not managed with the CEE IdAM tool. For information about the local accounts refer to *Security User Guide*.

6.1 Command Argument List

Table 2 lists all of the arguments for the various **`cee-idam`** subcommands for managing `infra-admin` users.

Note: In some cases the same argument has different outcomes, when used with different subcommands. The available arguments and their specific meaning for a given subcommand are specified in the relevant sections.

Table 2 CEE IdAM Subcommand Arguments

Argument	Description
`-h, --help`	Shows the help message.
`-l, --login`	The login name of the user.
`-u,--user-id-number`	The ID number of the user (`uidNumber`).
`-U, --user-group`	Creates a group with the same name as the user and adds the user to the group. Sets the primary group ID number (`gidNumber`) of the user to this groups.
`-g, --gid-number`	The primary group ID number (`gidNumber`) of the user.
`-G, --group`	Adds the user to the specified group.
`-ng, --new-group-id-number`	Specifies the new ID number (`gidNumber`) for the group.
`-n, --name`	The name of the group.
`-m, --create-home`	Creates the home directory for the user.

`-d, --home-dir`	Updates the home directory location of the user.
`-b`	The base directory for the home directory of the user.
`-p, --password`	Sets the password for the user.
`-P, --policy`	Applies the defined password policy to the user.
`-e, --expire`	Forces the user to change password during the first login, or when issuing commands that require privileged access.
`--lock`	Lock the user's account (disable password access).
`--unlock`	Unlock the user's account (enable password access).
`-c, --comment`	Sets comment for the LDAP GECOS field.
`-s, --shell`	Sets the login shell for the user.
`-j, --json`	Returns verbose data in JSON format. The exact attributes returned are defined in the relevant subcommand sections, where this argument is applicable.

6.2 Listing Users

Retrieve all users provisioned by the LDAP database with the following command:

```
sudo cee-idam user-list
```

Note: A list of users is presented showing the login name and user ID.

Example 2 shows how to list the users provisioned by the LDAP database.

```
<personal-user>@cic-1-0:~$ sudo cee-idam user-list
ID          Login
-----------------
10000       test1
10001       test2
10002       test3
```

Example 2 List of Users Provisioned by LDAP

Retrieve all users available in the system, including the ones that are not managed by `cee-idam`, with the following command:

```
getent passwd
```

6.3 Retrieving User Details

Retrieve user details with the following command:

```
sudo cee-idam user-get
```

The following options are available:

```
sudo cee-idam user-get [-h] (-u <USER_ID_NUMBER> |⇒
-l <LOGIN>) [-j]
```

Arguments:

- `-h, --help`

  Show the help message and exit.

- `-u <USER_ID_NUMBER>, --user-id-number <USER_ID_NUMBER>`

  User's ID number (`uidNumber`).

- `-l <LOGIN>, --login <LOGIN>`

  User's login.

- `-j, --json`

  Return verbose data in JSON format.

When the `-j` option **is not used** the following information is displayed in plain text format:

- User ID Number
- User name

Table 3 shows the LDAP attribute descriptions when the `-j` option **is used**. The output is in JSON format.

Table 3 LDAP attributes

LDAP Attribute	Description
`cn`	Holds the login name of the user at the creation.
`displayName`	The value of the `displayName` is the same as the value of the `cn` attribute.
`gecos`	Holds the comment option from the CEE IdAM tool, or the “LDAP user” as default value.
`gidNumber`	The ID of the primary group of the user.
`givenName`	The value of the `givenName` is the same as the value of the `cn` attribute.

homeDirectory	Holds the CEE IdAM home folder parameters, the default value is /home/*<cn-value>*
loginShell	Holds the value from the CEE IdAM shell-configuration option, the default value is /bin/bash.
memberOf	The groups where the user is a member.
objectClass	The LDAP object classes applied to the user. For internal system use only.
pwdPolicySubentry	Points to the password policy applied to the user. The default value is cn=Standard,ou=Policies,*<DcValues>*. *<DcValues>* is taken from ericsson.idam.ldap.basedn in config.yaml. For example dc=cee,dc=ericsson,dc=com.
shadowLastChange	The date of the last password change.
sn	The value of this attribute is the same as the value of the cn attribute.
uid	The user login ID, its value is the same as the value of the cn attribute.
uidNumber	The uid number of the user.

Example 3 shows how to retrieve the user details of ‘‘test_user’’.

```
<personal-user>@cic-1-0:~$ sudo cee-idam user-get -l test_user
ID          Login
-----------------
10036       test_user
```

Example 3 Retrieving User Details

Example 4 shows how to retrieve the user details of ‘‘test_user’’ including LDAP attributes.

```
<personal-user>@cic-1-0:~$ sudo cee-idam user-get -l test_user -j
{
 "cn": [
  "test_user"
 ],
 "displayName": [
  "test_user"
 ],
 "gecos": [
  "LDAP user"
 ],
 "gidNumber": [
  "100"
 ],
 "givenName": [
  "test_user"
 ],
```

```
 "homeDirectory": [
  "/home/test_user"
 ],
 "loginShell": [
  "/bin/bash"
 ],
 "memberOf": [
  "cn=ldap_users,ou=Groups,dc=cee,dc=ericsson,dc=com"
 ],
 "objectClass": [
  "top",
  "posixAccount",
  "shadowAccount",
  "inetOrgPerson",
 ],
 "pwdPolicySubentry": [
  "cn=Standard,ou=Policies,dc=cee,dc=ericsson,dc=com"
],
 "shadowLastChange": [
  "16492"
 ],
 "sn": [
  "test_user"
 ],
 "uid": [
  "test_user"
 ],
 "uidNumber": [
  "10036"
 ],
 "userPassword": [
  "{SSHA}LoEFeQJjwEDxPxRIqfGgo3DzAHFuio0s"
 ]
}
```


Example 4 Retrieving User Details with LDAP Attributes

6.4 Listing Groups of a User

Retrieve all groups where the user is a member with the following command:

cee-idam user-get-groups [-h] (-u *<USER_ID_NUMBER>* |⇒ -l *<LOGIN>*)

Arguments:

- `-h, --help`

  Show the help message and exit.

- `-u <USER_ID_NUMBER>, --user-id-number <USER_ID_NUMBER>`

User's ID number (`uidNumber`).

- `-l <LOGIN>`, `--login <LOGIN>`

  User's login.

- `-j`, `--json`

  Return verbose data in JSON format.

Example 5 shows how to retrieve the list of groups that `test_user` is a member of.

```
<personal-user>@cic-1-0:~$ sudo cee-idam user-get-groups⇒
 -l test_user
ID          Name
----------------
10003       test_group
```

Example 5 Retrieving User Group Details for test_user

6.5 Creating Users

Create users with the following command:

```
sudo cee-idam user-create
```

The following options are available:

```
cee-idam user-create [-h] [-b <BASE_DIR> | ⇒
-d <HOME_DIR>] [-g <GID_NUMBER>] | -U] [-c <COMMENT>] ⇒
[-m] [-P <Policy>] [-u <UID_NUMBER>] ⇒
<LOGIN>
```

Positional arguments:

- `LOGIN`

  User's login.

Arguments:

- `-h, --help`

  Show the help message and exit.

- `-b <BASE_DIR>`

  The base directory for the home directory of the user.

- `-d <HOME_DIR>`, `--home-dir <HOME_DIR>`

Update the users home directory location.

- `-g <GID_NUMBER>`, `--gid-number <GID_NUMBER>`

  Update primary group ID (gidNumber).

- `-U`, `--user-group`

  Set to create a group with the same name as the user. Sets the primary group ID number of the user to this groups and adds the user to this group.

- `-c <COMMENT>`, `--comment <COMMENT>`

  Set comment for the LDAP GECOS field.

- `-m`, `--create-home`

  Set to create the home directory for the user.

  Note: The home directory is automatically created at the first login of the user.

- `-P <POLICY>`, `--policy <POLICY>`

  Password policy to be applied to the user.

- `-u <USER_ID_NUMBER>`,`--user-id-number <USER_ID_NUMBER>`

  User's ID number (uidNumber)

Example 6 shows how to create the user `exampleuser` in the `/home` directory with "Example User" as comment.

```
<personal-user>@cic-1-0:~# sudo cee-idam user-create -b "/home"⇒
 -c "Example User" -m exampleuser
CEEIDAM (INFO): Saving user to LDAP...
CEEIDAM (SUCCESS): User saved to the LDAP database.
```

Example 6 Creating User exampleuser

After the user has been successfully created, the initial password must be set and marked for expiration, so that the user must change it during the first login. For more information see Section 8.1 on page 26.

6.6 Deleting Users

Delete users with the following command:

```
sudo cee-idam user-delete [-h] (-u <USER_ID_NUMBER> |⇒
-l <LOGIN>)
```

Arguments:

- `-h, --help`

  Show the help message and exit.

- `-u <USER_ID_NUMBER>, --user-id-number <USER_ID_NUMBER>`

  User's ID number (uidNumber).

- `-l, <LOGIN>, --login, <LOGIN>`

  User's login.

Note: One of the arguments `-u` or `-l` must be used in order to delete a user.

```
<personal-user>@cic-1-0:~# sudo cee-idam user-delete⇒
 -l exampleuser
CEEIDAM (INFO): Deleting user from LDAP...
CEEIDAM (SUCCESS): User `exampleuser` deleted.
```

Example 7 Deleting the User exampleuser

Note: If a home directory has been created for the user, it must be deleted manually.

6.7 Modifying Users

Users can be modified with the following command:

```
sudo cee-idam user-modify [-h] (-l <LOGIN> | ⇒
-u <USER_ID_NUMBER>) [-c <COMMENT>] [-g <GID_NUMBER>] ⇒
[-P <POLICY>] [-p <PASSWORD>] [-G <GROUP>] [-s <SHELL>] ⇒
[-e] [-m] [-d <HOME_DIR>]
```

The following options are available:

Arguments:

- `-h, --help`

  Show the help message and exit.

- `-l <LOGIN>, --login <LOGIN>`

  User's login.

- `-u <USER_ID_NUMBER>, --user-id-number <USER_ID_NUMBER>`

  User's ID number (uidNumber)

- `-c <COMMENT>, --comment <COMMENT>`

  Set comment for the LDAP GECOS field.

- `-g <GID_NUMBER>`, `--gid-number <GID_NUMBER>`

  Update primary group ID number (gidNumber).

- `-P <POLICY>`, `--policy <POLICY>`

  Password policy applied to the user.

- `-p <PASSWORD>`, `--password <PASSWORD>`

  Set password. The user password is given in a clear text format and saved as a base64 SSHA hash and salt buffer.

- `-G <GROUP>`, `--group <GROUP>`

  Add user to group.

- `-s <SHELL>`, `--shell <SHELL>`

  Set users login shell.

- `-e`, `--expire`

  Set to force users to change their password during the first login, or when using tools like sudo while logged in.

- `-m`, `--create-home`

  Set to create the home directory for the user.

  Note: The home directory is automatically created at the first login of the user.

- `-d <HOME_DIR>`, `--home-dir <HOME_DIR>`

  Update the users home directory location.

- `--lock`

  Lock the user's account (password and SSH access disabled).

- `--unlock`

  Unlock the user's account (password and SSH access enabled).

7 Managing Groups

The following subsections provide information about group management.

7.1 Listing Groups

The groups provisioned in LDAP are retrieved with the following command:

sudo cee-idam group-list

A list of groups is presented showing group name and group number.

Example 8 shows how to list the LDAP provisioned groups.

```
<personal-user>@cic-1-0:~$ sudo cee-idam group-list
ID          Name
----------------
10000       DirectoryAdmins
10001       ldap-users
20001       storage_admin
20002       storage_storageadmin
20003       storage_sanadmin
20004       storage_networkadmin
20005       storage_operator
20006       storage_securityadmin
27000       sudo
27001       ceesudo
27002       ceestatus
27003       ceeuseradmin
```

Example 8 Listing Groups

The list of all available groups in the system, including the ones that are not managed by `cee-idam`, is retrieved with the following command:

getent group

7.2 Retrieving Group Details

Local or remote LDAP group details are retrieved with the following command:

sudo cee-idam group-get

The following options are available:

sudo cee-idam group-get [-h] (-g *<GROUP_ID_NUMBER>* |⇒ -n *<NAME>*) [-j]

Optional arguments:

- `-h`, `--help`

  Show the help message and exit.

- `-g` *<GROUP_ID_NUMBER>*, `--group-id-number` *<GROUP_ID_NUMBER>*

  Group's ID number.

- `-n` *<NAME>*, `--name` *<NAME>*

  Group's name.

- `-j`, `--json`

  Return verbose data in JSON format.

When the `-j` option **is not used** the following information is displayed in plain text format:

- Group name
- Group ID

Example 9 shows how to retrieve the group details of the “sudo” group in plain text format.

```
<personal-user>@cic-1-0:~$ sudo cee-idam group-get -n sudo
Group details:
ID          Name
----------------
27000       sudo
```

Example 9 Getting the Group Details of sudo Group

Table 4 shows the LDAP attribute descriptions when the `-j` option **is used**. The output is in JSON format.

Table 4 LDAP Attribute Descriptions

LDAP Attribute	Description
`cn`	Holds the name of the group at the creation.
`gidNumber`	This is the group ID number.
`member`	This if the full distinguished name of the user belonging to the group.
`objectClass`	The LDAP object classes applied to the group. For internal system use only.

Example 10 shows how to retrieve group details for the sudo group “sudo” in JSON format.

```
<personal-user>@cic-1-0:~$ sudo cee-idam group-get -n sudo -j
{
 "cn": [
  "sudo"
 ],
 "gidNumber": [
  "27000"
 ],
 "member": [
  "cn=foobar2,ou=Users,dc=cee,dc=ericsson,dc=com",
  "cn=phnbert,ou=Users,dc=cee,dc=ericsson,dc=com",
  "cn=zckszfr,ou=Users,dc=cee,dc=ericsson,dc=com",
 ],
 "objectClass": [
  "posixGroup",
  "groupOfNames"
 ]
}
```

Example 10 Getting the Group Details of sudo Group in JSON Format

7.3 Creating Groups

Groups are created with the following command:

sudo cee-idam group-create

The following options are available:

sudo cee-idam group-create [-h] [-g *<GROUP_ID_NUMBER>*] ⇒ *<group_name>*

Positional arguments:

- ***<group_name>***

  The name of the group.

Arguments:

- `-h`, `--help`

  Show help message and exit.

- `-g` *<GROUP_ID_NUMBER>*, `--group-id-number` *<GROUP_ID_NUMBER>*

  Group ID

Example 11 shows how to create the group ‘‘examplegroup’’.

```
<personal-user>@cic-1-0:~$ sudo cee-idam group-create ⇒
examplegroup
CEEIDAM (INFO): Saving group to LDAP...
CEEIDAM (SUCCESS): Group saved to the LDAP database.
```

Example 11 Creating the Group examplegroup

7.4 Deleting Groups

Groups are deleted with the following command:

sudo cee-idam group-delete

The following options are available:

**sudo cee-idam group-delete [-h] (-g *<GROUP_ID_NUMBER>* | ⇒
-n *<NAME>*)**

Arguments:

- `-h`, `--help`

  Show help message and exit.

- `-g` *<GROUP_ID_NUMBER>*, `--group-id-number` *<GROUP_ID_NUMBER>*

  Group ID.

- `-n` *<NAME>*, `--name` *<NAME>*

  Group's name.

Example 12 shows how to delete the group ‘‘examplegroup’’.

```
<personal-user>@cic-1-0:~$ sudo cee-idam group-delete ⇒
-n examplegroup
CEEIDAM (INFO): Deleting group from LDAP...
CEEIDAM (SUCCESS): Group `examplegroup` deleted.
```

Example 12 Deleting Group examplegroup

Note: Users can still have the deleted group defined as their primary group (`gidNumber`). Use the **`sudo cee-idam user-modify`** command with the `-g` option to change the primary group for the user.

7.5 Modifying Groups

Groups are modified with the following command:

sudo cee-idam group-modify

The following options are available:

**sudo cee-idam group-modify [-h] (-g *<GROUP_ID_NUMBER>* |⇒
-n *<NAME>*) -ng *<NEW_GROUP_ID_NUMBER>*]**

Arguments:

- `-h, --help`

  Show help message and exit.

- `-g <GROUP_ID_NUMBER>, --group-id-number <GROUP_ID_NUMBER>`

  Group ID (groupNumber)

- `-n <NAME>, --name <NAME>`

  Group's name.

- `-ng <NEW_GROUP_ID_NUMBER>, --new-group-id-number <NEW_GROUP_ID_NUMBER>`

  New ID number (`gidNumber`) to be set for the group.

Note: When the `gidNumber` of a group is modified, the primary group attribute will not be updated automatically for the users who had that group specified as their primary group. For these users the `gidNumber` attribute must be manually changed with **`sudo cee-idam user-modify -g`**.

Example 13 shows how to modify ‘‘examplegroup’’ to have a new Group ID (`gidNumber`).

```
<personal-user>@cic-1-0:~$ sudo cee-idam group-modify⇒
 -n examplegroup -ng 17654
CEEIDAM (INFO): Modifying group in LDAP...
CEEIDAM (SUCCESS): Group modified in the LDAP database.
```

Example 13 Modifying Group examplegroup to have a New Group ID

7.6 Deleting Users from Groups

Delete a user from a group with the following command:

sudo cee-idam delete-user-from-group

The following options are available:

**sudo cee-idam delete-user-from-group [-h]⇒
(-g *<GROUP_ID_NUMBER>* | -n *<NAME>*)⇒
(-u *<USER_ID_NUMBER>* |-l *<LOGIN>*)**

Arguments:

- `-h, --help`

  Show the help message and exit.

- `-g <GROUP_ID_NUMBER>, --group-id-number <GROUP_ID_NUMBER>`

  Group's ID number (gidNumber)

- `-n <NAME>, --name <NAME>`

  Group's name.

- `-u <USER_ID_NUMBER>, --user-id-number <USER_ID_NUMBER>`

  User's ID number (uidNumber).

- `-l <LOGIN>, --login <LOGIN>`

  User's login.

Example 14 shows how to delete the user ‘‘test_user’’ from the group ‘‘test_group’’.

```
<personal-user>@cic-1-0:~# sudo cee-idam delete-user-from-group ⇒
-l test_user -n test_group
CEEIDAM (SUCCESS): User `test_user` was removed from
group `test_group`.
```

Example 14 Deleting test_user from test_group

Note: Groups and users can also be referenced by their ID numbers using the `-g` and `-u` options.

8 Managing Passwords

This section describes password management for `infra-admin` and LDAP users.

Users can change their own password with the **`passwd`** command without superuser privileges.

8.1 Managing Passwords for Cloud Infrastructure Administrators

To change the password of a user issue one of the following commands:

```
sudo passwd exampleuser
```

or

```
sudo cee-idam user-modify [-h] -(l <LOGIN>) -e ⇒
-p <PASSWORD>
```

Arguments:

- `-h`, `--help`

  Show the help message and exit.

- `-l` *`<LOGIN>`*, `--login` *`<LOGIN>`*

  User's login.

- `-p` *`<PASSWORD>`*, `--password` *`<PASSWORD>`*

  Set password.

- `-e`, `--expire`

  Set to force users to change their password during the first login, or when using tools like sudo while logged in.

  Note: A password created or reset by a superuser must always be changed during the first login.

Note: When the superuser changes the password for another user with the CEE IdAM tool, a new password is given as a command line parameter.

Example 15 shows how to change the user password with the **`passwd`** command.

```
<personal-user>@cic-1-0:~$ sudo passwd exampleuser
  New password:
  Re-enter new password:
  LDAP password information changed for exampleuser
  passwd: password updated successfully
  <personal-user>@cic-1-0:~$
```

Example 15 Changing Password with passwd

Example 16 shows how to change the user password with the **cee-idam user-modify** command and forcing a password change during the first login.

```
<personal-user>@cic-1-0:~$ sudo cee-idam user-modify ⇒
-l exampleuser -e -p 'examplepassword'
CEEIDAM (INFO): Expiring password for user `exampleuser`.
CEEIDAM (SUCCESS): User's password has been expired.
CEEIDAM (INFO): Setting password for user `exampleuser`.
CEEIDAM (SUCCESS): User's password has been set.
User modification completed
<personal-user>@cic-1-0:~$
```

Example 16 Changing Password with cee-idam user-modify

9 SSH-key Management

The SSH-key management feature is primarily reserved for future or internal system use. The CEE IdAM tool can be used to generate private and public SSH-key pairs for the users. The private SSH-keys are stored under *<defined-directory>*/id_rsa and the public SSH-keys can be stored in the LDAP database. Public SSH-keys are backed up and can be restored using the CEE Backup and Restore procedures.

9.1 Creating Keys

To generate the SSH-key pairs issue the following command:

sudo cee-idam keys-create [-h] -l *<LOGIN>* -d *<DIRECTORY>*

Optional arguments:

- -h, --help

  Show the help message and exit.

- -l *LOGIN*, --login *LOGIN*

  User's login.

- -d *DIRECTORY*, --directory *DIRECTORY*

  Specifies the directory under which the “id_rsa” private key is created. The public key is stored in the LDAP database.

Example 17 shows how to create SSH-key pairs.

```
<personal-user>@cic-1-0:~$ sudo cee-idam keys-create -l ceeadm -d ⇒
"/home/ceeadm/.ssh"
CEEIDAM (SUCCESS): RSA public key saved to the LDAP database:
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCopiunGm0o6xuES0urFaUvUnYYJZ05Vk+Vtno⇒
nJ3UC5MWnI/IcMYKJKkiA3Cu5Ipdis/Mvxl/LTArhmf+6h5n+Ns4iCUVEOfaieN3K/V99V7VAeA⇒
s4WGpKnesEusCH3e/17KxHG6JSmWe2fWM1s1NhIqaFSM3oiEDpZYBM/yVTEI4p3Aq0lFr7a+zxp⇒
ngiuCtxgzNH/XiGY5ET2uPcQ/5C0YDFiivjeL1pTjR3H2FWzaVbx0MHk7PurhY2fdlS0ErcAXWv⇒
qk3NqzAKoEdsbPMOa2EaVIr7hhjx5XV28J1FONCI2VHFAOLzRttxkB74VLCOJDOQadkDFQ4aNfq⇒
x35vX ceeadm@hostname
```

Example 17 Creating SSH-key Pair

9.2 Retrieving Keys

To retrieve public keys from LDAP issue the following command:

sudo cee-idam keys-get [-h] -l *<LOGIN>*

Optional arguments:

- `-h, --help`

  Show the help message and exit.

- `-l <LOGIN>, --login <LOGIN>`

  User's login.

Example 18 shows how to retrieve public keys from LDAP.

```
<personal-user>@cic-1-0:~$ sudo cee-idam keys-get -l ceeadm
CEEIDAM (INFO): Dumping public keys from `ceeadm`...
-----
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDKWOxvtZIR+X6znZiCLld8QPJx0uhn7p66⇒
tvJBNWWg1Ie6mMJRTzo10S6I0nsURbwJA3nhC4Ko9gavUomnRUlbUi9/pERcoSAs1C0hqkjj⇒
i/jIwHqcbX261UzxSw6ajB/oJETYHs0fl0wZdt8M9bndJF8QlEDGWyQHtoVk5ohOloNaWjRG⇒
1ZT1XGflWxg0WgWb+wo0ddiOOqCyDUYg60vlMUABjQR/xEIHZjhQxXmoinLzewm8h/ilG05n⇒
P75kT4CZ8i4DZwnPlLzM5Vo8GUCbmsXQc66kWa0pMBki0vvlTriwzno9vx77b6mwE4T9AwiZ⇒
h9FPhrJicVYnr7KxAN03 ceeadm@192.168.0.24
-----
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC8Dm3cTit0elLNS6JQPZmnLGGvP2B4Sf9L⇒
c2UMuTm5uuTFpew7/bupYp20O3ovys5jVpI7EHOsde0BkBgMKk0r1k+mm8rTET+W5gwR+Ms5⇒
szE72sIZeV8j02adq5yqMRaVS8Lgwsoc4TL3P7ZSB2cIyCnSj+K16IOUAreMmgkRMpgfrpIH⇒
kIfA9/beztUcjeVIezc7b6E9FyPxKO4cs80ijH9mRVMsNid4naEopI0g0WWYIBMFG4HrfoXB⇒
TyJ1VdZgjzymd6GhHru9asplB0GqzxRNBlbCjT4UYtK6lFUcfl8GOJDQ7QimJgI3Cirhuyiq⇒
r+2djeFsAPFSEIxlmbE/ ceeadm@192.168.0.21
-----
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDd7QxPGHsKlWaejnXF+in9pCt71VdPQ/U2⇒
RE42HyVDFfRWYE5+TXV5CXBvR4yLsKI2M6ciHaOC7/V7R8ld+m2B7Yy4CctxDtXGgktJneF/⇒
GiQhHXPPaqsTSiWoT2jonxPoleZA8FHrR/k1wH4K8k+7KCRQDbVQIaVy+jennllVcQ91im2L⇒
gwN8u2GYsCXueUeI2QnguIvCKYlEmOWAqh72WQhaGVg3G/LJA6SNJXko6GxuS8/3DI7Pn0i/⇒
WWoo9hz3S04qgoEvVx8MlfgBfUcOBij2iGA4Kg3yhZNBAtyPilFHHomi50FEFydD5EoKQ3Xd⇒
ZC87ZE2KhttFKNdPom5H ceeadm@192.168.0.25
-----
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCXU64NikfoSv5H7ywdjL7i9w8S5HJsx1Nq⇒
fGgbtjhkvIGxt6GKkME8jnNOTtKJZu+i5wuC4NyUeAumyvvbPo6YPfStpUeDSNTbei6GwPsS⇒
MW5oh79wfpxUOOCOc8CkcrXH0RKefFbWfNbkDnTpxUvl+N3gqfCLO4peFERiiNfRHenWVbBT⇒
XB4YZ3Q8hqrKd7GbUtwSZH3lPbOj6UcXapghkrP8UbSBX6+5MuYriu93zAlBVFaDnX5GJ1Ah⇒
4rUGgd/ex9qtZ3fxL7cYy/i+9IZMXg4WK/VgWJYfwbhOqtCXFHYX3/dxHphinVizFBJx6g+A⇒
AG6ULnRIzEPscaVpxcwH ceeadm@winzip
-----
```

Example 18 Retrieving Public Keys from LDAP

9.3 Deleting Keys

To delete the public keys of a user issue the following command:

`sudo cee-idam keys-delete [-h] -l <LOGIN> [-k <KEY>]`

Optional arguments:

- `-h, --help`

  Show the help message and exit.

- `-l <LOGIN>, --login <LOGIN>`

  User's login.

- `-k <KEY>, --key <KEY>`

  Specifies the public SSH key to delete.

Example 19 shows how to delete the public SSH keys of the user `ceeadm`.

```
<personal-user>@cic-1-0:~$ sudo cee-idam keys-delete⇒
 -l ceeadm
CEEIDAM (INFO): Deleting `ceeadm`'s public key from LDAP...
CEEIDAM (SUCCESS): `ceeadm`'s public key has been deleted.
CEEIDAM (INFO): Deleting `ceeadm`'s public key from LDAP...
CEEIDAM (SUCCESS): `ceeadm`'s public key has been deleted.
CEEIDAM (INFO): Deleting `ceeadm`'s public key from LDAP...
CEEIDAM (SUCCESS): `ceeadm`'s public key has been deleted.
CEEIDAM (INFO): Deleting `ceeadm`'s public key from LDAP...
CEEIDAM (SUCCESS): `ceeadm`'s public key has been deleted.
```

Example 19 Deleting Public Keys

Reference List

[1] *OpenLDAP Documentation, http://www.openldap.org/doc/*