CDP Public Cloud Management Console

AWS Credentials

Date published: 2019-08-22
Date modified:

https://docs.cloudera.com/

Legal Notice

© Cloudera Inc. 2024. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Unless otherwise noted, scripts and sample code are licensed under the Apache License, Version 2.0.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 (“ASLv2”), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER’S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

Contents

Working with provisioning credentials for AWS

Refer to the following documentation to learn about creating and managing AWS credentials in CDP:

Related Information

Introduction to the role-based provisioning credential for AWS
Create a provisioning credential for AWS
Obtain CLI commands for creating a credential
Viewing available credentials
Modify a credential
Change environment's credential
Delete a credential

Introduction to the role-based provisioning credential for AWS

Creating a credential is a prerequisite for creating an environment. On AWS, you have a single option for creating a cloud credential: a role-based credential.

When working with an AWS environment, you are required to configure a way for CDP to authenticate with your AWS account and obtain authorization to create resources on your behalf. On AWS, there is a single option for doing this: the role-based credential. Role-based authentication uses an IAM role with an attached IAM policy that has the minimum permissions required to use CDP. As stated in AWS docs:

"An IAM role is similar to an IAM user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have standard long-term credentials such as a password or access keys associated with it. Instead, when you assume a role, it provides you with temporary security credentials for your role session."

The following table provides more information on the role-based credential:

	Role-based
IAM entity used by the credential	A cross-account IAM role
Security mechanism	An IAM role does not have standard long-term credentials such as a password or access keys associated with it. Instead, when an entity assumes a role, temporary security credentials for the role session are generated. Since CDP is set up with an AssumeRole policy, it can assume the IAM role. For more information about AssumeRole and granting permissions to create temporary security credentials, refer to AWS docs.
Use case	Suitable for an organization as it allows multiple users to use the same IAM role.
Overview of configuration steps	1. In the IAM console on AWS, create an IAM policy and a cross-account IAM role, and then assign the IAM policy to the IAM role. 2. Register the role ARN as a credential in CDP. Once done, CDP can assume the IAM role.

Related Information

IAM roles (AWS)
Granting permissions to create temporary security credentials (AWS)

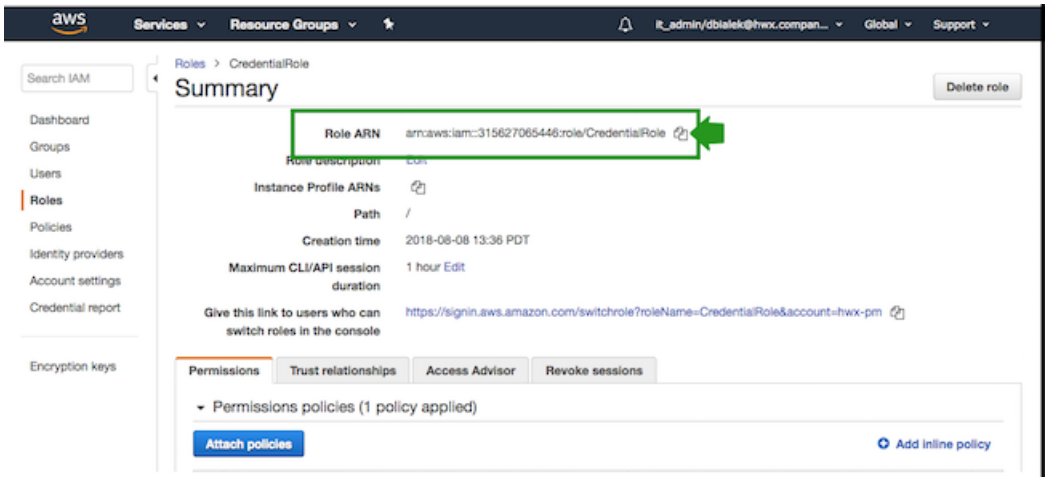
Create a provisioning credential for AWS

Create a role-based credential referencing the IAM role created earlier. This can be done from the CDP web interface or CDP CLI.

Before you begin

Prior to performing these steps. you should create a cross-account role. See Cross-account access IAM role.

These steps assume that you have the ARN of the IAM role that you created in an earlier step. You can obtain the IAM Role ARN from the IAM console > Roles on AWS by selecting a role and clicking on your IAM role to navigate to its summary and then copying the Role ARN:



Required role: EnvironmentCreator

Steps

For CDP UI

1. Log in to the CDP web interface.

   Note:

   These steps show you how to create a credential from the Credentials page in the CDP web interface, but you may also create a credential directly from the Environments page as part of environment registration process.
2. Navigate to the Management Console.
3. Select Shared Resources > Credentials from the navigation pane.
4. Click Create Credential.
5. Select AWS to access credential options for Amazon Web Services.
6. Provide the following information:

Parameter	Description
Select Credential Type	Select Role Based (default value).
Name	Enter a name for your credential.
Description	(Optional) Enter a description.
Enable Permission Verification	Activate the Enable Permission Verification button if you want CDP to check permissions for your credential. CDP will verify that you have the required permissions for your environment.
IAM Role ARN	Paste the IAM Role ARN corresponding to the “CredentialRole” that you created earlier. For example arn:aws:iam::315627065446:role/CredentialRole is a valid IAM Role ARN.

7. Click Create.
8. Your credential should now be displayed in the Credentials pane.

For CDP CLI

1. You have three options:
   a. (The simplest option) In CDP CLI, use the following command to create a credential:

```
cdp environments create-aws-credential \
--credential-name <value> --role-arn <value>
```

   b. Alternatively, you can provide the credential information in the CDP web interface > Management Console > Environments > Shared Resources > Credentials > Create Credential and then click on SHOW CLI COMMAND and copy the JSON snippet. Next, save the JSON in a text file and use the following command to create a credential:

```
cdp environments create-aws-credential --cli-input-json <value>
```

   c. Alternatively, you can use the following commands: Use the first command to obtain the JSON snipped, then provide the missing information, and then use the second command to create the credential:

```
cdp environments create-aws-credential --generate-cli-skeleton
cdp environments create-aws-credential --cli-input-json <value>
```

After you finish

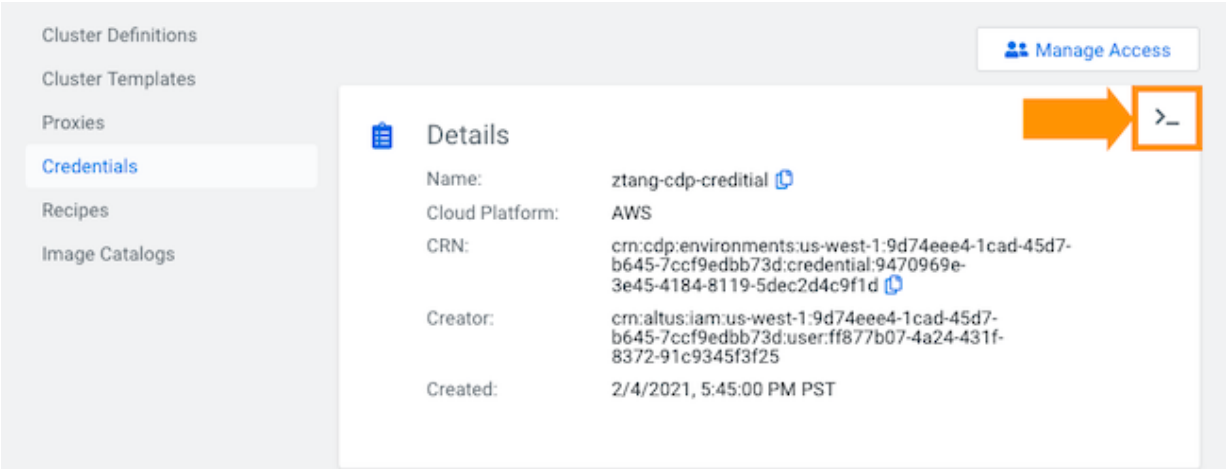
Now that you have created the credential, you can use it to register your AWS environment.

Obtain CLI commands for creating a credential

In addition to being able to obtain CDP CLI commands for credential creation from CDP CLI help, you can also obtain them from the CDP web interface.

You can quickly obtain CDP CLI commands for creating a credential from the Management Console:

- (Required role: Owner) From details of an existing credential by clicking >_ in the top right corner:



If you obtain the command from this page, you should change the value of the --credential-name before running the command.

- (Required role: EnvironmentCreator) From the create credential wizard by providing all required parameters and then clicking >_ SHOW CLI COMMAND in the bottom of the page.
- (Required role: EnvironmentCreator) From the register environment wizard by providing all required parameters and then clicking >_ SHOW CLI COMMAND in the bottom of the credential section.

Viewing available credentials

You can access all existing credentials from CDP web interface by navigating to the Management Console > Shared Resources > Credentials page. You can also list credentials from CDP CLI using the cdp environments list-credentials command.

Modify a credential

You can modify an existing credential if needed. You can modify all parameters except the credential name. This shows you how to modify a credential from the CDP web interface. There is currently no way to modify a credential from CDP CLI.

The modify credential option is meant for cases such as updating your access and secret key on AWS in case it expired or changed.

If the credential that you are trying to modify is already attached to an environment, ensure that the modification that you are making still allows access to the resources, such as the data lake, running within that environment.

Note:

If you are trying to update the IAM policy used for the credential, do not follow these instructions. Instead, edit the policy via the AWS Management Console or AWS CLI as described in Editing IAM Policies in AWS docs.

Required role: SharedResourceUser or Owner

Steps

For CDP UI

1. Log in to the CDP web interface.
2. Navigate to the Management Console.
3. Select Shared Resources > Credentials from the navigation pane.
4. Select the credential that you would like to modify and click on or navigate to the credential's details and click Edit.
5. Provide the new credential information. You must provide all required parameters, even if they are same as previously.
6. Click on Save.

   This updates the credential across all the environments that are currently using it.

For CDP CLI

If you would like to modify a credential from the CDP CLI, use cdp environments modify-credential.

Change environment's credential

You can change the credential attached to an environment as long as the new credential provides the required level of access to the same AWS account as the old credential.

Required roles:

- EnvironmentAdmin or Owner of the environment
- SharedResourceUser or Owner of the credential

Steps

For CDP UI

1. Log in to the CDP web interface.
2. Navigate to the Management Console.
3. Select Environments from the navigation pane.
4. Click on a specific environment.
5. Navigate to the Summary tab.
6. Scroll down to the Credential section.
7. Click to access credential edit options.
8. Select the new credential that you would like to use.
9. Click to save the changes.

For CDP CLI

If you would like to delete a credential from the CDP CLI, use:

```
cdp environments update-environment-credential --environment-name <value>
 --credential-name <value>
```

Delete a credential

You can delete a credential as long as no environment is currently using it.

Before you begin

A credential can only be deleted if it is not currently being used by any environments. If the credential that you are trying to delete is currently being used by one or more environments, you must remove the dependency by either deleting all such environments or changing their credential.

Required role: Owner

Steps

For CDP UI

1. Log in to the CDP web interface.
2. Navigate to the Management Console.
3. Select Shared Resources > Credentials from the navigation pane.
4. Select the credential that you would like to delete and click on .

5. Confirm the deletion by clicking Yes.
   This deletes the credential.

For CDP CLI

If you would like to delete a credential from the CDP CLI, use

```
cdp environments delete-credential --credential-name <value>
```

.