

# Minimal AWS Cross Account Policy for Data Lake and Data Hub (Preview)

Date published: 2021-05-27

Date modified: 2021-08-06

## Legal Notice

© Cloudera Inc. 2021. 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.

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.

*This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided 'as is' without warranty or support. Further, Cloudera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.*

## Contents

<b>Legal Notice</b>	<b>2</b>
<b>Contents</b>	<b>3</b>
<b>Revision history</b>	<b>4</b>
<b>About this feature</b>	<b>4</b>
<b>Reduced access policy definition</b>	<b>4</b>
Customize the scope of iam:PassRole	4
Further permissions reduction	7

*This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided 'as is' without warranty or support. Further, Cloudera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.*

## Revision history

2021-08-06	Updated the requirements for customizing the scope of iam:PassRole
2021-06-03	Updated link to the minimal <a href="#">policy</a>
2021-06-02	Updated link to the minimal policy
2021-05-27	Initial draft

## About this feature

If you are planning to only run Data Hub in your CDP environment, you don't need all the actions in the default cross account role provided on the create credential UI and in the provisioning credential documentation (See [IAM policy definition](#)). Using a significantly reduced cross account policy is possible as an alternative.

**Note:** This is a preview feature and the cross-account policy is subject to change without notification. Please check the github pages periodically to check for updates.

## Reduced access policy definition

The IAM role used for the provisioning credential should use the updated reduced access [policy](#) instead of the policy provided in the UI and documentation. You should:

1. Copy this policy.
2. Update it as described in [Customize the scope of iam:PassRole](#) below.
3. You can optionally reduce the permissions further, as described in [Further permissions reduction](#) below.

## Customize the scope of iam:PassRole

CDP utilizes the *iam:PassRole* as part of the cloud identity federation setup process via IDBroker on AWS. The default policy uses "\*" as the resource scope for this action:

```
{
  "Effect": "Allow
  "Action": [
    "iam:PassRole"
  ],
  "Resource": "*"
}
```

However the scope can be reduced to just a few roles. To do this, you need to edit the following block and replace the "\*" with the ARNs of the following roles used for the environment:

- IDBROKER\_ROLE
- LOG\_ROLE
- RANGER\_AUDIT\_ROLE

*This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided 'as is' without warranty or support. Further, Cloudera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.*

- **DATALAKE\_ADMIN\_ROLE**

You chose the name for these roles when you set up CDP as part of the [Minimal Setup for Cloud Storage](#) or [AWS Quick Start](#).

After updating according to the [Minimal Setup for Cloud Storage](#), the PassRole policy excerpt should look similar to the following:

```
{
  "Effect": "Allow
  "Action": [
    "iam:PassRole"
  ],
  "Resource": [
    "arn:aws:iam::$ACCOUNTID:role/IDBROKER_ROLE",
    "arn:aws:iam::$ACCOUNTID:role/LOG_ROLE",
    "arn:aws:iam::$ACCOUNTID:role/RANGER_AUDIT_ROLE",
    "arn:aws:iam::$ACCOUNTID:role/DATALAKE_ADMIN_ROLE"
  ]
}
```

If you used the [AWS Quick Start](#), the PassRole policy excerpt should look like this:

```
{
  "Effect": "Allow
  "Action": [
    "iam:PassRole"
  ],
  "Resource": [
    "arn:aws:iam::$ACCOUNTID:role/<prefix>-idbroker-role",
    "arn:aws:iam::$ACCOUNTID:role/<prefix>-log-role",
    "arn:aws:iam::$ACCOUNTID:role/<prefix>-ranger-audit-role",
    "arn:aws:iam::$ACCOUNTID:role/<prefix>-datalake-admin-role"
  ]
}
```

If you have already created these roles and you don't know the name of these roles, you can obtain them using the following steps:

### **IDBROKER\_ROLE**

1. Log in to CDP web interface and navigate to the **Management Console** service > **Data Lakes**.
2. Scroll down to where you see **Event History** and select the **Hardware** tab.
3. Locate the EC2 instance for the **idbroker** node (if you are running Medium Duty Data Lake, you will see two IDBroker nodes, you can use either) :

*This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided 'as is' without warranty or support. Further, Cloudera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.*

# CLUDERA TECHNICAL PREVIEW DOCUMENTATION

Environments / svv-aws / Data Lake / Hardware

Environment Details

NAME: svv-aws | CREDENTIAL: eng-dim-weekly | REGION: us-west-2 | AVAILABILITY ZONE: us-west-2b

Services: Atlas, CM-UI, HBase UI, Name Node, Ranger, Solr Server, Token Integration

Cloudera Manager Info

CM URL: https://svv-aws-datalake-gateway.svv-aws.xcu2-8y8x.dev.cldr.work/svv-aws-datalake/cdp-proxy/cmf/home/ | CM VERSION: 7.4.1 | PLATFORM VERSION: 7.2.9-1.cdh7.2.9.p1.14062417 | LOGS: Command logs, Service logs

Event History | Endpoints (6) | Tags (6) | **Hardware** | Network | Telemetry | Repository Details | Image Details | Recipes (0) | Cloud Storage | Attached clusters (0) | Database | Upgrade

Master

ID	FQDN	Status	Private IP	Public IP
i-07fe5627529cb130a	svv-aws-datalake-master0.svv-aws.xcu2-8y8x.dev.cldr.work	Running	10.116.133.192	CM Server

Idbroker

ID	FQDN	Status	Private IP	Public IP
i-0011589ce16b3febc	svv-aws-datalake-idbroker0.svv-aws.xcu2-8y8x.dev.cldr.work	Running	10.116.132.70	

4. Click on the instance id. You will be redirected to the EC2 console.
5. In the **Instance Details** section for this node, you can see the name of the IAM role being used by this instance. Click on this role to get to the details.
6. Copy the ARN of the instance profile. It follows the following naming convention:  
`arn:aws:iam::<12-digit-AWS-account-id>:instance-profile/<name-of-idbroker-role>`

## LOG\_ROLE

1. Navigate to **Environments**.
2. Click on the existing environment
3. Click on the **Summary** tab.
4. Scroll to **Logs Storage and Audits** and you will see the **Instance Profile** entry.
5. Copy the ARN of the **Instance Profile**:

Logs Storage and Audits

Storage Location: s3a://eng-sdx-daily-qe/sdxinfra-8bfmoi/audit

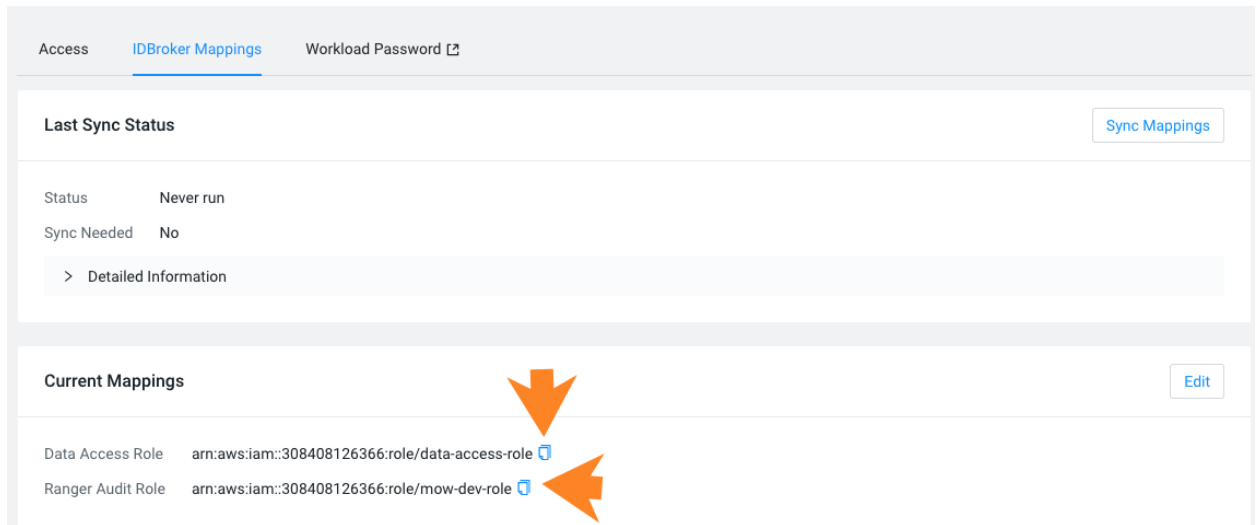
Instance Profile: arn:aws:iam::308408126366:instance-profile/mow-dev

## RANGER\_AUDIT\_ROLE and DATALAKE\_ADMIN\_ROLE

1. Navigate to **Environments**.
2. Click on the existing environment.
3. From the **Actions** menu, select **Manage Access**.

*This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided 'as is' without warranty or support. Further, Cloudera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.*

4. Click on the **IDBroker Mappings** tab.
5. Under **Current Mappings** you will see the mappings for the **Data Access Role** and **Ranger Audit Role**.
6. Copy the ARNs of the **Data Access Role** and **Ranger Audit Role**.



## Further permissions reduction

You can reduce these policies even further by pre-creating some resources:

- If you set up your own VPC and subnets (using [this](#) guide), then the following actions can be removed from the policy:
  - ec2:CreateVpc
  - ec2:CreateNatGateway
  - ec2:CreateRouteTable
  - ec2:CreateSubnet
  - ec2:CreateVpcEndpoint
  - ec2:CreateInternetGateway
  - ec2>DeleteSubnet
  - ec2>DeleteInternetGateway
  - ec2:AttachInternetGateway
  - ec2:DetachInternetGateway
  - ec2:DescribePrefixLists
  - ec2:AllocateAddress
  - ec2:AssociateRouteTable
  - ec2:CreateRoute
  - ec2>DeleteRouteTable
  - ec2>DeleteVpcEndpoints
  - ec2:DisassociateRouteTable

*This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided 'as is' without warranty or support. Further, Cloudera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.*

## CLUSTERA TECHNICAL PREVIEW DOCUMENTATION

- `ec2:ReleaseAddress`
- `ec2>DeleteRoute`
- `ec2>DeleteNatGateway`
- `ec2>DeleteVpc`
- If you use your own security groups (using [this](#) guide), then the following actions can be removed from the policy:
  - `ec2:CreateSecurityGroup`
  - `ec2:AuthorizeSecurityGroupIngress`
  - `ec2:RevokeSecurityGroupEgress`
  - `ec2:AuthorizeSecurityGroupEgress`
- If you use private IPs or set up CCM to communicate with the CDP Control Plane (as described [here](#)), then the following actions can be removed from the policy:
  - `ec2:AllocateAddress`
  - `ec2:ReleaseAddress`
- If you create your own DynamoDB table for S3Guard (described [here](#)), then the following actions can be removed from the policy:
  - `dynamodb>DeleteTable`

*This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided 'as is' without warranty or support. Further, Cloudera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.*