Creating a Cloudbreak Credential on AWS

Date of Publish: 2018-09-14

http://docs.hortonworks.com

Contents

Cloudbreak credential options on AWS

Before you can start creating clusters, you must first create a Cloudbreak credential. Without this credential, you will not be able to create clusters via Cloudbreak.

If you are launching Cloudbreak from the quickstart template, you should use the key-based credential.

If you are installing Cloudbreak for production, as part of the installation steps you had two options to allow Cloudbreak to authenticate with AWS and create resources on your behalf: key-based or role-based authentication. Depending on your choice, you should configure key-based or role-based credential. We recommend using role-based credential.

Related Information

Core concepts

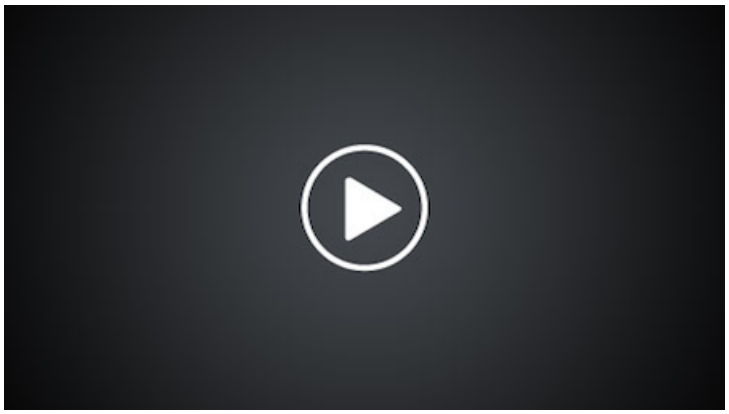
Authentication with AWS

Configuring authentication with AWS

Creating a key-based credential

Key-based authentication, the simpler way to authenticate with AWS, is typically used when getting started with Cloudbreak.

The following video demonstrates how to meet the prerequisites for and create the key-based Cloudbreak credential on AWS:



The minimum permissions required for that user are described in CredentialRole.

Related Information

Create CredentialRole

Prerequisites for key-based authentication

In order to use key-based authentication you must have an IAM user which has the required permissions as well as an access and secret key.

If you are using key-based authentication for Cloudbreak on AWS, you must:

- Have an existing user or create a new user in IAM. The minimum permissions required for that user are described in CredentialRole.

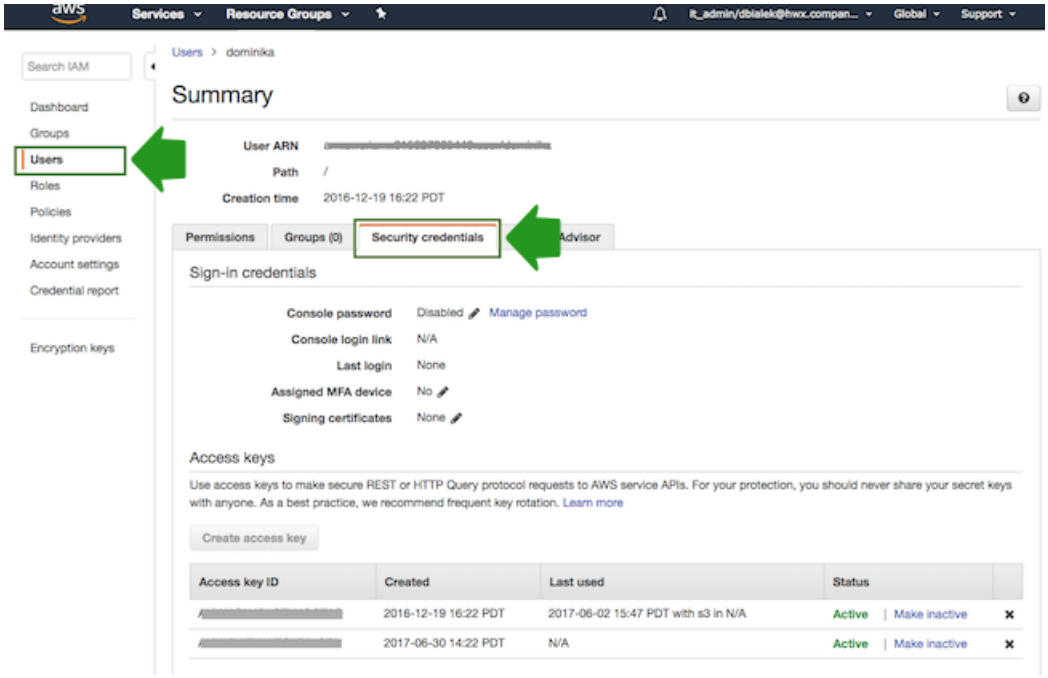
- Be able to provide an AWS access key and secret key associated with this user. Cloudbreak will use these keys to launch resources on your AWS account. You must provide the access and secret keys later in the Cloudbreak web UI later when creating a credential.

You can create a user or generate new access and secret keys for an existing user from the IAM Console > Users.

Modifying an existing IAM user

If you already have an IAM user:

- Make sure that the user has minimum permissions by creating the policy described in CredentialRole and assigning it to the user in the Permissions tab.
- If you need to generate a new access key and secret key, you can do this from the Security credentials tab:



Create a new IAM user

If you need to create a new IAM user, follow these steps:

1. In your browser, log in to your AWS account and navigate to the IAM console.
2. In the IAM console, navigate to the Users view, and click on Add user. This will open the Add user wizard.
3. Under User name, provide some name for your user, and under Access Type, select Programmatic access. Once done, click on the Next button to navigate to the next page.
4. Under Set permissions, select Attach existing policies directly and then click on Create policy. This will open the Create policy wizard in a new browser tab, allowing you to define a new policy.
5. In the Create policy wizard, navigate to the JSON view, and then copy and paste the CredentialRole policy.
6. On the Review policy page, provide some name for this policy. And click on the Create policy button to finalize the policy creation.
7. Now that the IAM policy has been created, navigate back to the previous tab where you started creating your IAM user…. And click on the refresh button to refresh the list of policies.
8. Next, search for the policy that you just created, select it, click on the Next button, and on the last page of the wizard, click on Create user.
9. This will create a new user and generate the access key and secret key for that user. You will need to provide this access key and secret key to Cloudbreak, so make sure to save them for example by using the Download button. Furthermore, this is the only time that you can access the secret key. If you don't save it at this point, you will need to generate a brand new key pair.

Create a key-based credential

Create a key-based Cloudbreak credential referencing your IAM user's access key and secret key.

Steps

1. In the Cloudbreak web UI, select Credentials from the navigation pane.
2. Click Create Credential.
3. Under Cloud provider, select “Amazon Web Services” or "AWS GovCloud".
4. Provide the following information:

Parameter	Description
Select Credential Type	Select Key Based.
Name	Enter a name for your credential.
Description	(Optional) Enter a description.
Access Key	Paste your access key.
Secret Access Key	Paste your secret key.

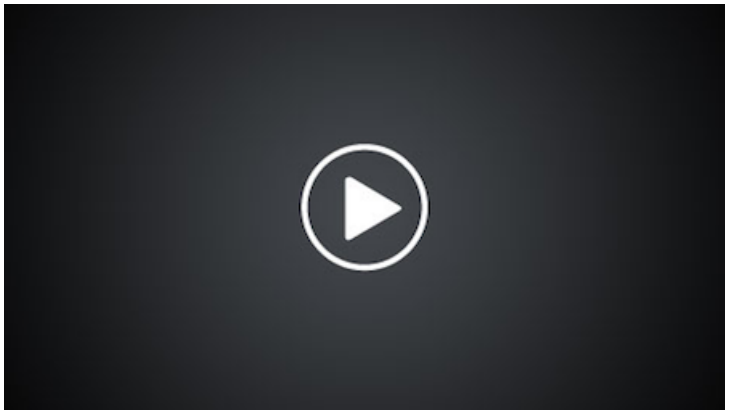
5. Click Create.
6. Your credential should now be displayed in the Credentials pane.

Now that you have created a Cloudbreak credential, you can start creating clusters.

Creating a role based credential

Creating a role-based Cloudbreak credential includes the following prerequisites and steps.

The following video demonstrates how to meet the prerequisites for and create the role-based Cloudbreak credential on AWS:



The minimum permissions required for that user are described in CredentialRole.

Create CredentialRole

In order to use role-based authentication, you must create the CredentialRole on AWS.

Use the following “CbPolicy” policy definition:

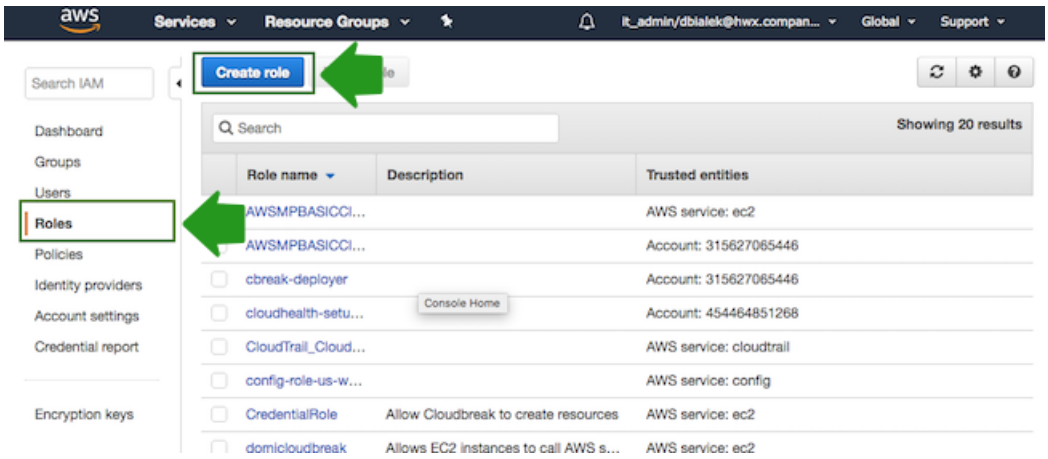
```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStackEvents",
                "cloudformation:DescribeStackResource",
                "cloudformation:DescribeStackResources",
                "cloudformation:DescribeStacks"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AllocateAddress",
                "ec2:AssociateAddress",
                "ec2:AssociateRouteTable",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:DescribeRegions",
                "ec2:DescribeAvailabilityZones",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
                "ec2:CreateSecurityGroup",
                "ec2:CreateSubnet",
                "ec2:CreateTags",
                "ec2:CreateVpc",
                "ec2:ModifyVpcAttribute",
                "ec2:DeleteSubnet",
                "ec2:CreateInternetGateway",
                "ec2:CreateKeyPair",
                "ec2:DeleteKeyPair",
                "ec2:DisassociateAddress",
                "ec2:DisassociateRouteTable",
                "ec2:ModifySubnetAttribute",
                "ec2:ReleaseAddress",
                "ec2:DescribeAddresses",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstances",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeSpotInstanceRequests",
                "ec2:DescribeVpcAttribute",
                "ec2:ImportKeyPair",
                "ec2:AttachInternetGateway",
                "ec2:DeleteVpc",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteRouteTable",
                "ec2:DeleteInternetGateway",
                "ec2:DeleteRouteTable",
                "ec2:DeleteRoute",
                "ec2:DetachInternetGateway",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:CopyImage",
```

```
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeVolumes",
                "ec2:DeregisterImage"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListRolePolicies",
                "iam:GetRolePolicy",
                "iam:ListAttachedRolePolicies",
                "iam:ListInstanceProfiles",
                "iam:PutRolePolicy",
                "iam:PassRole",
                "iam:GetRole"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "autoscaling:CreateAutoScalingGroup",
                "autoscaling:CreateLaunchConfiguration",
                "autoscaling:DeleteAutoScalingGroup",
                "autoscaling:DeleteLaunchConfiguration",
                "autoscaling:DescribeAutoScalingGroups",
                "autoscaling:DescribeLaunchConfigurations",
                "autoscaling:DescribeScalingActivities",
                "autoscaling:DetachInstances",
                "autoscaling:ResumeProcesses",
                "autoscaling:SuspendProcesses",
                "autoscaling:UpdateAutoScalingGroup"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:ListKeys",
                "kms:ListKeyPolicies",
                "kms:ListAliases"
            ],
            "Resource": "*"
        }
    ]
}
```

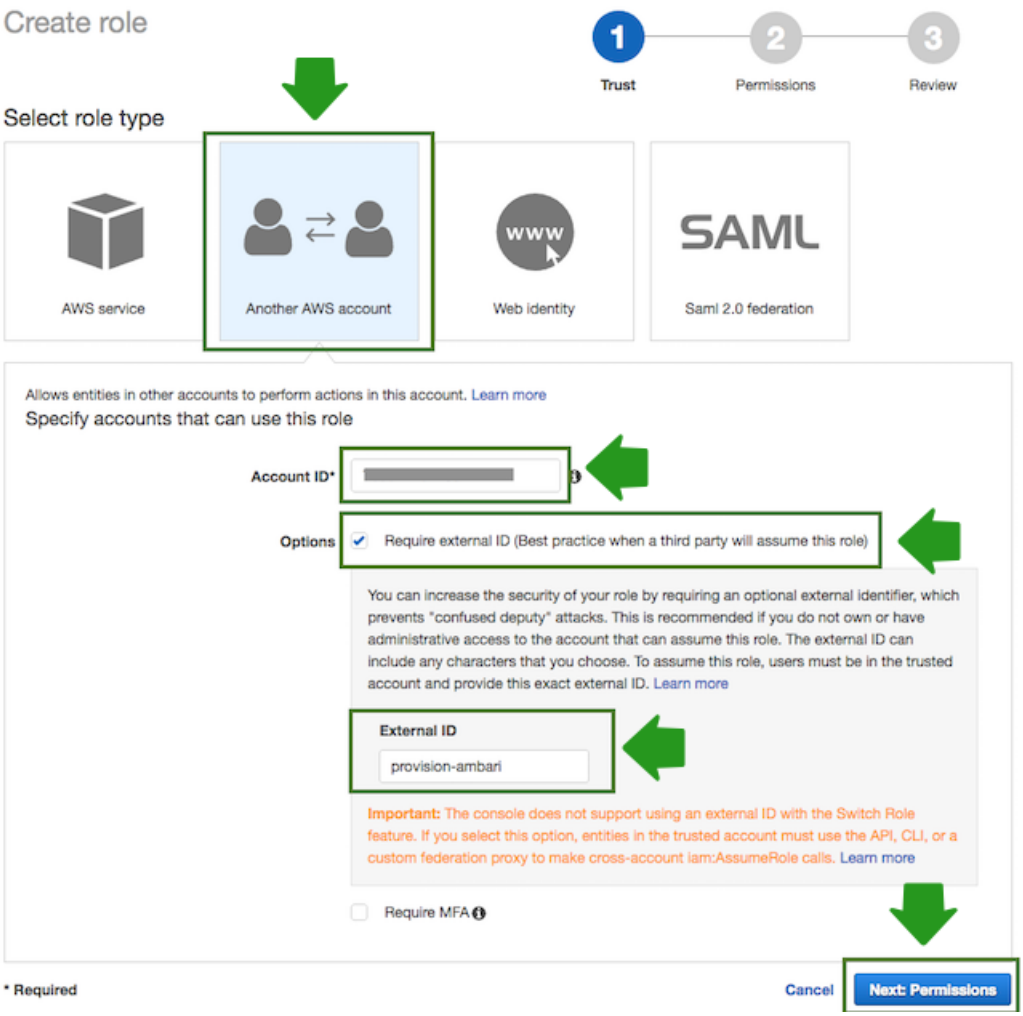
Steps

1. Navigate to the IAM console > Roles and click Create Role:

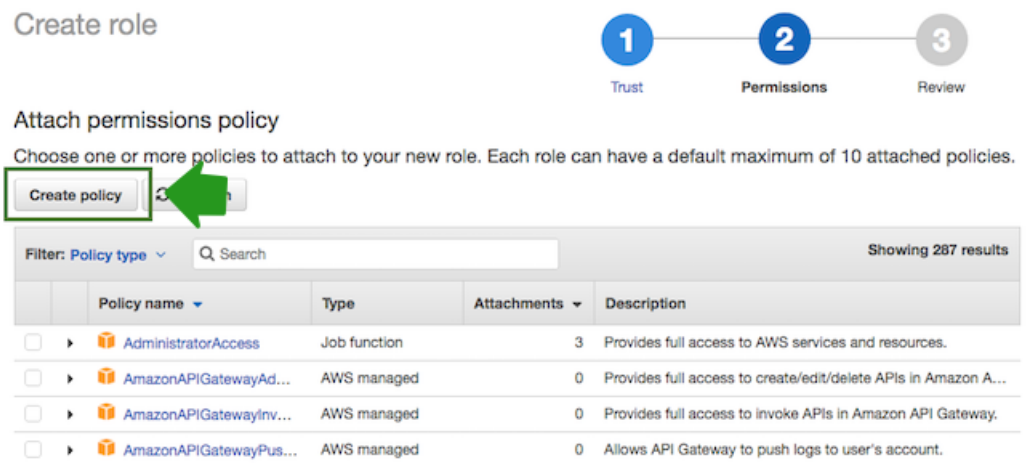


2. In the “Create Role” wizard, select Another AWS account role type. Next, provide the following:

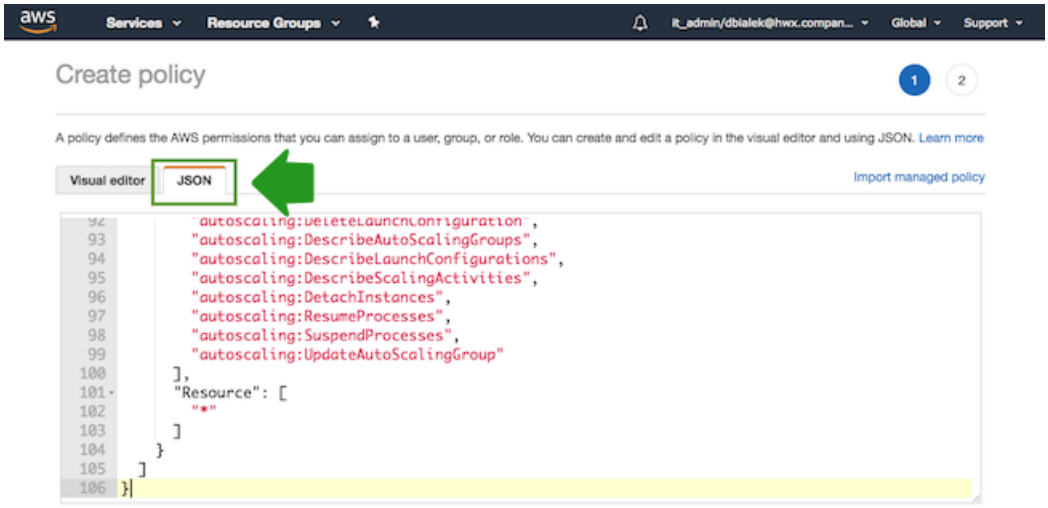
   - In the Account ID field, enter your AWS account ID.
   - Under Options, check Require external ID.
   - In the External ID, enter “provision-ambari”.



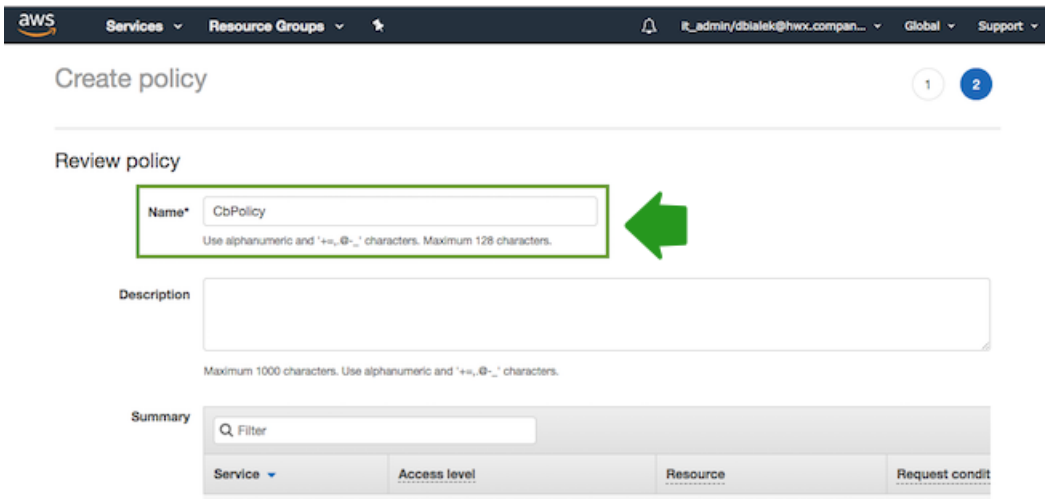
3. When done, click Next: Permissions to navigate to the next page in the wizard.
4. Click Create policy and the create policy wizard will open in a new browser tab:



5. Select the JSON view, and copy and paste the policy definition. You can either copy it from the section preceding these steps or download and copy it from here:

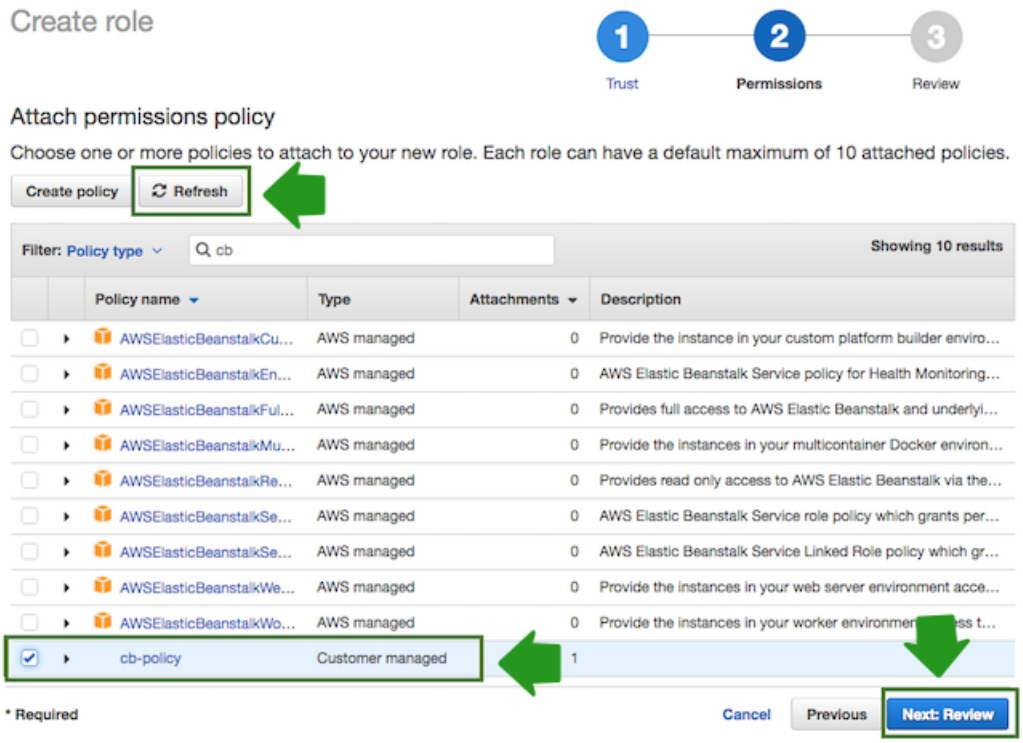


6. When done, navigate to Review policy.
7. On the Review policy page, in the Name field, enter a name for your policy, such as "CbPolicy":



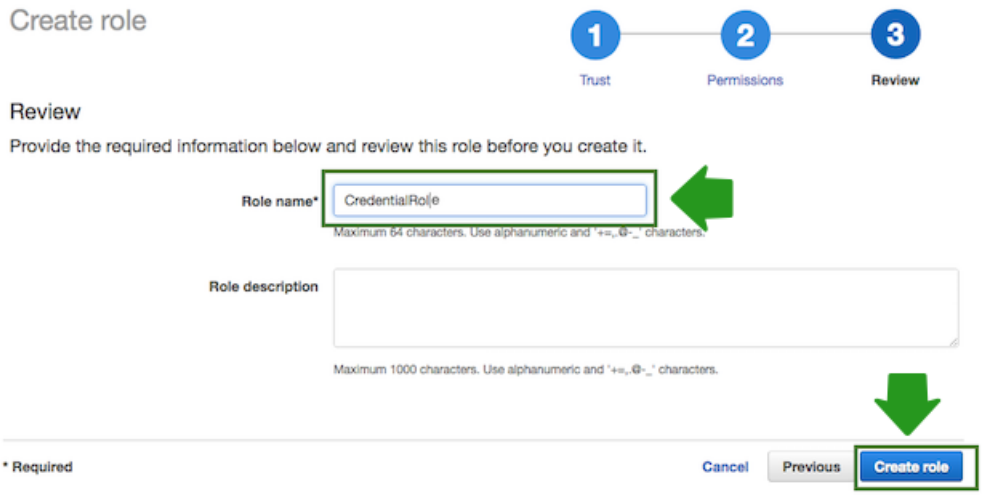
8. When done, click Create Policy.
9. Return to the previous browser tab where you started creating a new role (since the create policy wizard was opened in a new browser tab).

10. Click Refresh. Next, find the “CbPolicy” that you just created and select it by checking the box:



11. When done, click Next: Review.

12. In the Roles name field, enter role name, for example “CredentialRole”.



13. When done, click Create role to finish the role creation process.

Once you are done, you can proceed to launch Cloudbreak.

Create a role-based credential

Create a role-based Cloudbreak credential referencing the CredentialRole.

Prerequisites

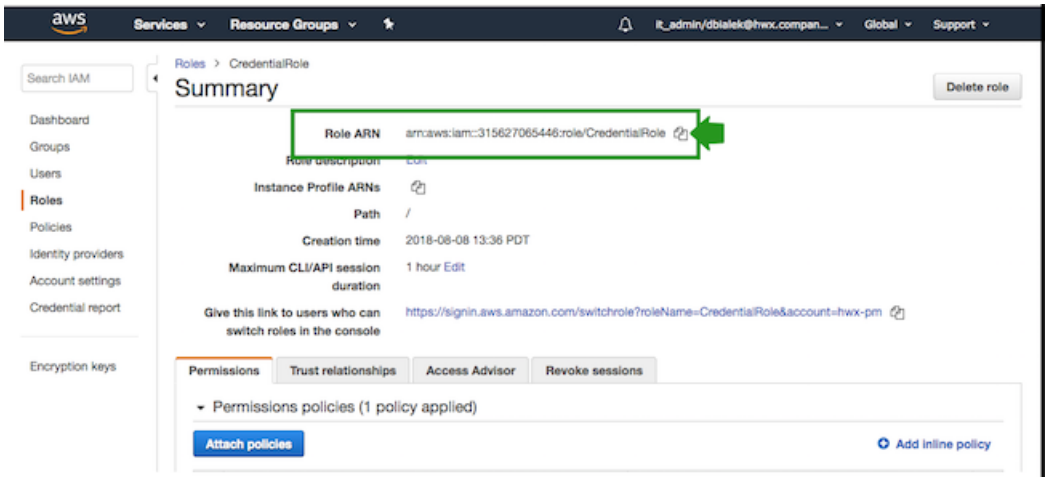
To perform these steps, you must know the IAM Role ARN corresponding to the CredentialRole configured as part of the prerequisites.

Steps

1. In the Cloudbreak web UI, select Credentials from the navigation pane.
2. Click Create Credential.
3. Under Cloud provider, select “Amazon Web Services” or "AWS GovCloud".
4. 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.
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.

5. You can obtain the IAM Role ARN from the IAM console on AWS > Roles by click on your IAM role to navigate to its summary and then copying the Role ARN:



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

Now that you have created a Cloudbreak credential, you can start creating clusters.