

AWS Organizations Use Case

In the Management account:

1. (Pre-Req): In the [AWS Organizations](#) Console:
 - a. Take note of the Organization ID
 - b. In the 'Trusted access for AWS services' section, ensure that '[AWS CloudFormation StackSets](#)' is enabled.

The screenshot shows the AWS Organizations console. The top navigation bar includes the AWS logo, a 'Services' dropdown, and a search bar. Below the navigation bar, the 'AWS Organizations' header is visible, followed by tabs for 'Accounts', 'Organize accounts', and 'Policies'. The main content area is divided into two sections: 'Organization details' and 'Trusted access for AWS services'.

Organization details

Organization ID: o- a

Management account name: org-master

Management account email: [\[redacted\]@amazon.com](#) (verified)

Feature set: Your organization has all features enabled. This allows you to apply service control policies (SCPs) to limit what the accounts in the organization can do, enable trusted AWS services to have access to your organization and accounts, and create, manage and pay for the organization's accounts through consolidated billing. [Learn more](#)

[Delete organization](#)

Trusted access for AWS services

Allow other AWS services to perform actions in your organization. A trusted service can access information about the accounts, root, OUs, and policies for your organization. [Learn more](#)

Note: We recommend that you use the trusted service's console to enable and disable trusted access to AWS Organizations. This allows the other service to perform any supporting tasks needed to enable or disable access with Organizations. For more information, see the documentation for the specific trusted service.

AWS service	Status	Action
Tag policies [external link] Policies that can help you standardize tags across resources in your organization's accounts. Learn more	Disabled	Enable access
AWS Artifact [external link] A service that provides on-demand downloads of AWS security reports such as ISO and PCI reports. Learn more	Disabled	Enable access
AWS Backup [external link] A service that enables you to schedule automatic backups of your AWS resources. You can create policies that automatically apply your backup plans to resources across your organization's accounts. Learn more	Disabled	Enable access
AWS CloudFormation StackSets [external link] An extension of AWS CloudFormation stacks functionality that enables you to create, update, or delete stacks across multiple accounts and regions with a single operation. Learn more	Enabled ✔	Disable access

b

- c. [Deploy an AWS CloudFormation stack](#) using the provided template `bmcDiscoveryXARSetup.yaml`.

- i. For consistency, it's recommended you name the stack 'bmcDiscoveryXARSetup'
- ii. Provide the AWS Account ID for this current management account
- iii. Provide the AWS Organization ID

Specify stack details

Stack name

Stack name *i*

bmcDiscoveryXARSetup

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

MgmtAccountid *ii*

The 12 digit AWS account number to grant access to.

16

OrganizationId *iii*

When using AWS Organizations and run in the management account, provide the AWS Organization ID

0-

Cancel Previous Next

- iv. Wait for the stack to successfully complete

- d. Go to IAM | Users and select the new 'discoveryoutpost' user:

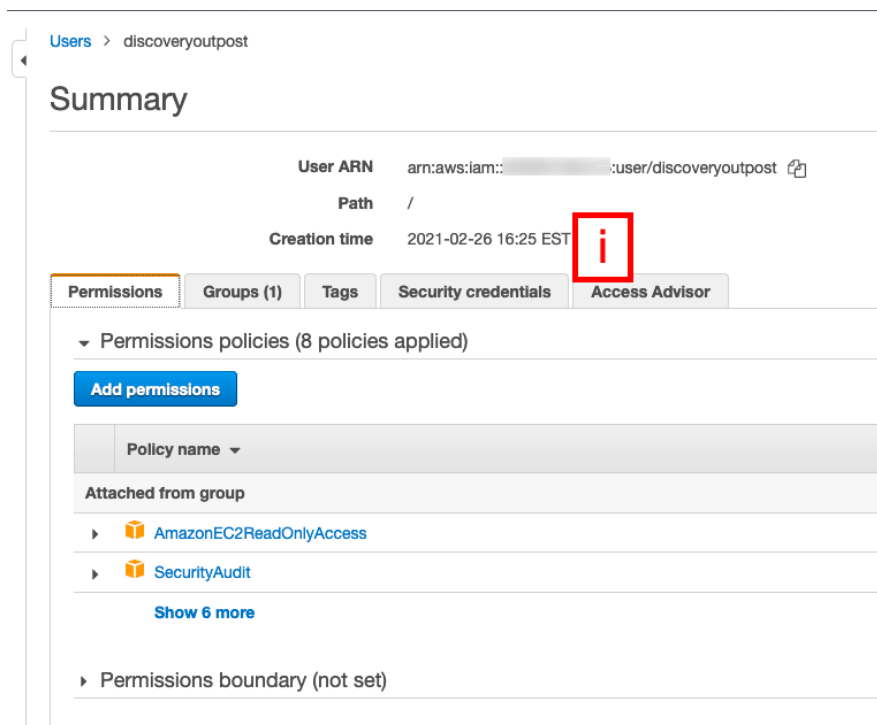
Add user Delete user

Find users by username or access key

User name

discoveryoutpost

- i. On the 'Security credentials' tab, create a new access key. Record or download the Access key ID and Secret access key. These will be used to configure the BMC Helix Discovery Outpost to perform its scan across your AWS Organization accounts:



Users > discoveryoutpost

Summary

User ARN: arn:aws:iam::[redacted]:user/discoveryoutpost

Path: /

Creation time: 2021-02-26 16:25 EST

Permissions Groups (1) Tags Security credentials Access Advisor

Permissions policies (8 policies applied)

Add permissions

Policy name

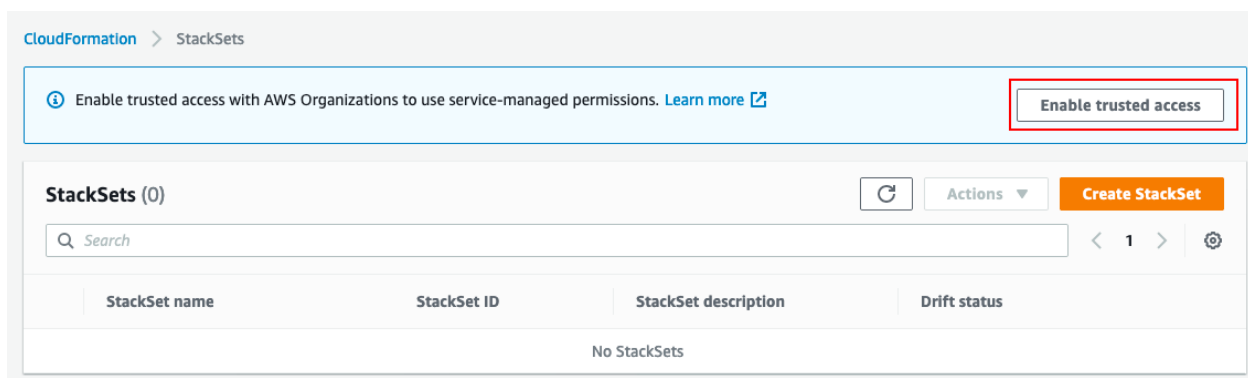
Attached from group

- AmazonEC2ReadOnlyAccess
- SecurityAudit

Show 6 more

Permissions boundary (not set)

- e. Go to the CloudFormation console | StackSets.
 - i. Click 'Enable trusted access' if not already enabled.



CloudFormation > StackSets

Enable trusted access with AWS Organizations to use service-managed permissions. [Learn more](#)

Enable trusted access

StackSets (0)

Search

StackSet name StackSet ID StackSet description Drift status

No StackSets

- ii. Click 'Create StackSet'
- iii. On the 'Choose a template' page,
 - 1. Provide the S3 URL if you uploaded the provided template bmcDiscoveryXARSetup.yaml to an S3 bucket as described earlier, otherwise, upload the template on this page.
 - 2. Click 'Next'
- iv. On the 'Specify StackSet details' page,
 - 1. Provide a StackSet name. For consistency, we recommend using the name 'bmcDiscoveryXARSetup'
 - 2. Provide the AWS Account ID for this current management account

3. Provide the AWS Organization ID you copied in the earlier step.
4. Click 'Next'

Specify StackSet details

StackSet name

StackSet name

bmcDiscoveryXARSetup

Must contain only letters, numbers, and dashes. Must start with a letter.

StackSet description

You can use the description to identify the stack set's purpose or other important information.

StackSet description

This template creates required cross-account role permissions for BMC Discovery account.

Parameters (2)

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

MgmtAccountId

The 12 digit AWS account number to grant access to.

OrganizationId

When using AWS Organizations and run in the management account, provide the AWS Organization ID

o-

Cancel

Previous

Next

- v. On the 'Configure StackSet options' page,
 1. Provide any tags if applicable
 2. Make sure the 'Service-managed permissions' option is selected
 3. Click 'Next'

Configure StackSet options

Tags

You can specify tags (key-value pairs) to apply to resources in your stack. You can add up to 50 unique tags for each stack.

<input type="text" value="Key"/>	<input type="text" value="Value"/>	<input type="button" value="Remove"/>
----------------------------------	------------------------------------	---------------------------------------

Permissions

Choose an IAM role to explicitly define how CloudFormation will manage your target accounts. If you don't choose a role, CloudFormation uses permissions based on your user credentials. [Learn more](#)

☒ **Service-managed permissions**

StackSets automatically configures the permissions required to deploy to target accounts managed by AWS Organizations. With this option, you can enable automatic deployment to accounts in your organization

☐ **Self-service permissions**

You create the execution roles required to deploy to target accounts

- vi. On the 'Set deployment options' page,
 1. Select the appropriate options for your environment/needs.
 2. Note that it is recommended that you enable 'Automatic Deployment', as this will result in BMC Helix Discovery gaining access to scan new accounts as soon as they join the Organization without manual intervention.
 3. Click 'Next'

Set deployment options

Deployment targets

StackSets deploys stack instances to all accounts in the target organization or organizational units (OUs). If you add a parent OU as a target, StackSets also adds any child OUs as targets [Learn more](#)

☒ Deploy to organization

☐ Deploy to organizational units (OUs)

Automatic deployment

With automatic deployment enabled, if an account is added to an OU, StackSets automatically deploys additional stack instances to this account. If an account is removed from an OU, StackSets automatically deletes stack instances in this account.

☒ Enabled

☐ Disabled

Account removal behavior

When an account is removed from a target OU, should stack instances in the account be deleted or retained?

☒ Delete stacks

☐ Retain stacks

Specify regions

Choose the regions in which you want to deploy stacks. Stacks are deployed in these regions in the order that you specify. Note that during stack set operations, administrator and target accounts exchange metadata regarding the accounts themselves, as well as the stack set and stack set instances involved. [Learn more](#)

^

v

Remove

Add all regions

Remove all regions

Deployment options

Maximum concurrent accounts - optional

Number of accounts per region to which you can deploy stacks at one time. The higher the number, the faster the operation

Number

1

Failure tolerance - optional

Number of account, per region, for which stacks can fail before CloudFormation stops the operation in that region. If the operation is stopped in one region, it does not continue in other regions. The lower the number the safer the operation.

Number

0

Cancel

Previous

Next

- vii. On the 'Review' page,
 1. Review the selections made
 2. Check the 'I acknowledge the AWS CloudFormation might create IAM resources with custom names' checkbox
 3. Click 'Submit'
- viii. On the CloudFormation | StackSets page, you should now see the created StackSet in the Operations tab with a status of 'SUCCEEDED'

Page 6 of 12

This completes the steps of setting up [AWS IAM Cross Account roles](#). The StackSet will begin deploying the 'bmcDiscoveryXARSetup' template into the respective member accounts based on the options you selected in 'Deployment options' page. Depending on the size of your AWS Organization, this could take some time.

Additionally, if you enabled '[Automatic Deployment](#)', when you add a new account to your AWS Organization, StackSets will initiate deployment of the 'bmcDiscoveryXARSetup' template into the new member account automatically. Conversely, if the account is removed from the AWS Organization, StackSets will initiate deletion of the deployed 'bmcDiscoveryXARSetup' stack automatically.

Non- AWS Organizations Use Case

In the 'Parent' account:

1. (prereq, optional): Because the template needs to be run in every linked account, to simplify the deployment it's recommended to:
 - a. Copy the template, bmcDiscoveryXARSetup.yaml, to an S3 bucket with sufficient permissions that the admins for each of the linked accounts can open and execute the template.
 - b. Construct a quick-create link to which includes the master account ID and provide that to the linked account admins to execute rather than having them launch a stack manually.

For example, with the template in an S3 bucket 'acmecorp-discoveryassets', and a master account ID of '111111111111', the following quick-create link when opened

https://console.aws.amazon.com/cloudformation/home?region=us-east-1#/stacks/quickcreate?templateUrl=https%3A%2F%2Facmecorp-discoveryassets.s3.amazonaws.com%2FbmcDiscoveryXARSetup.yaml&stackName=bmcDiscoveryXARSetup¶m_MgmtAccountId=111111111111¶m_OrganizationalId=

CloudFormation > Stacks > Create stack

Quick create stack

Template

Template URL
https://acmecorp-discoveryassets.s3.amazonaws.com/bmcDiscoveryXARSetup.yaml

Stack description
This template creates required cross-account role permissions for BMC Discovery account.

Stack name

Stack name
bmcDiscoveryXARSetup

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

MgmtAccountId
The 12 digit AWS account number to grant access to.
111111111111

OrganizationId
When using AWS Organizations and run in the management account, provide the AWS Organization ID

Capabilities

The following resource(s) require capabilities: [AWS::IAM::Policy, AWS::IAM::Role]

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. [Learn more](#)

☒ I acknowledge that AWS CloudFormation might create IAM resources with custom names.

Cancel Create change set **Create stack**

- c. Deploy a CloudFormation stack using the provided template bmcDiscoveryXARSetup.yaml.
 - i. For consistency, it's recommended you name the stack 'bmcDiscoveryXARSetup'
 - ii. Provide the AWS Account ID for this current 'master' account.
 - iii. Leave the AWS Organization ID parameter empty.

Specify stack details

Stack name

i

Stack name

bmcDiscoveryXARSetup

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

ii

MgmtAccountId

The 12 digit AWS account number to grant access to.

iii

OrganizationId

When using AWS Organizations and run in the management account, provide the AWS Organization ID

Cancel

Previous

Next

iv. Wait for the stack to successfully complete

d. Go to IAM | Users and select the new 'discoveryoutpost' user:

Add userDelete user

Find users by username or access key

User name

discoveryoutpost

- i. On the 'Security credentials' tab, create a new access key. Record or download the Access key ID and Secret access key. These will be used to configure the BMC Helix Discovery Outpost to perform its scan across your AWS Organization accounts:

Users > discoveryoutpost

Summary

User ARN	arn:aws:iam::[redacted]:user/discoveryoutpost
Path	/
Creation time	2021-02-26 16:25 EST

i

Permissions

Groups (1)

Tags

Security credentials

Access Advisor

▼ Permissions policies (8 policies applied)

[Add permissions](#)

Policy name ▼
Attached from group
▶ AmazonEC2ReadOnlyAccess
▶ SecurityAudit
Show 6 more
▶ Permissions boundary (not set)

In each linked account:

2. Deploy a CloudFormation stack using the provided template `bmcDiscoveryXARSetup.yaml`.

As mentioned above, it's best practice to provide a quick-create link, which will prepopulate the stack name for consistency across accounts, and the master account ID.

- a. For consistency, it's recommended you name the stack 'bmcDiscoveryXARSetup'
- b. Provide the AWS Account ID for this current 'master' account.
- c. Leave the AWS Organization ID parameter empty.

Specify stack details

Stack name

Stack name

bmcDiscoveryXARSetup

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

MgmtAccountid

The 12 digit AWS account number to grant access to.

Organizationid

When using AWS Organizations and run in the management account, provide the AWS Organization ID

Cancel Previous Next

- d. Wait for the stack to successfully complete

Testing

The AK/SAK you generated for the 'discoveryoutpost' IAM user can now be used to query across the accounts where the template has been deployed.


For example, with a master account ID '111111111111' and two linked accounts, ID '222222222222' and ID '333333333333', with the [AWS Command Line Interface \(CLI\)](#) configured ([~/aws/config](#)):

This sets up a separate CLI profile to access each account. Note that AK/SAK created for the 'discoveryoutpost' IAM user are only provided for the master account profile.

The two linked account profiles:

1. use a '[source profile](#)' property pointing to the master account profile to obtain the same AK/SAK.
2. Use a '[role arn](#)' property containing the 'bmcDiscoveryROScanTrustRole' arn in the respective linked account which in turn has the trust relationship for the master account.

```
1 [profile discoveryoutpostM]
2 aws_access_key_id=
3 aws_secret_access_key=
4 region=us-east-1
5
6 [profile discoveryoutpostC1]
7 region=us-east-1
8 role_arn=arn:aws:iam::222222222222:role/bmcDiscoveryROScanTrustRole
9 source_profile=discoveryoutpostM
10
11 [profile discoveryoutpostC2]
12 region=us-east-1
13 role_arn=arn:aws:iam::333333333333:role/bmcDiscoveryROScanTrustRole
14 source_profile=discoveryoutpostM
15
```



Assuming there is an EC2 instance deployed in each account, the following depicts BMC Discovery scanning each account, with each [describe-instances](#) query returning the instance in the account corresponding to the profile used, as shown by the different instance ID and Tag/Name value.

```
$aws --profile discoveryoutpostM ec2 describe-instances --query 'Reservations[*].Instances[*].[InstanceId, Tags]'
[
  [
    [
      "i-0607b8974a542b896",
      [
        {
          "Key": "Name",
          "Value": "orgMaster-Instance"
        }
      ]
    ]
  ]
]
$aws --profile discoveryoutpostC1 ec2 describe-instances --query 'Reservations[*].Instances[*].[InstanceId, Tags]'
[
  [
    [
      "i-0c6a8107bc4ffb280",
      [
        {
          "Key": "Name",
          "Value": "orgChild1-Instance"
        }
      ]
    ]
  ]
]
$aws --profile discoveryoutpostC2 ec2 describe-instances --query 'Reservations[*].Instances[*].[InstanceId, Tags]'
[
  [
    [
      "i-09389259fe9d35eae",
      [
        {
          "Key": "Name",
          "Value": "orgChild2-Instance"
        }
      ]
    ]
  ]
]
$
```