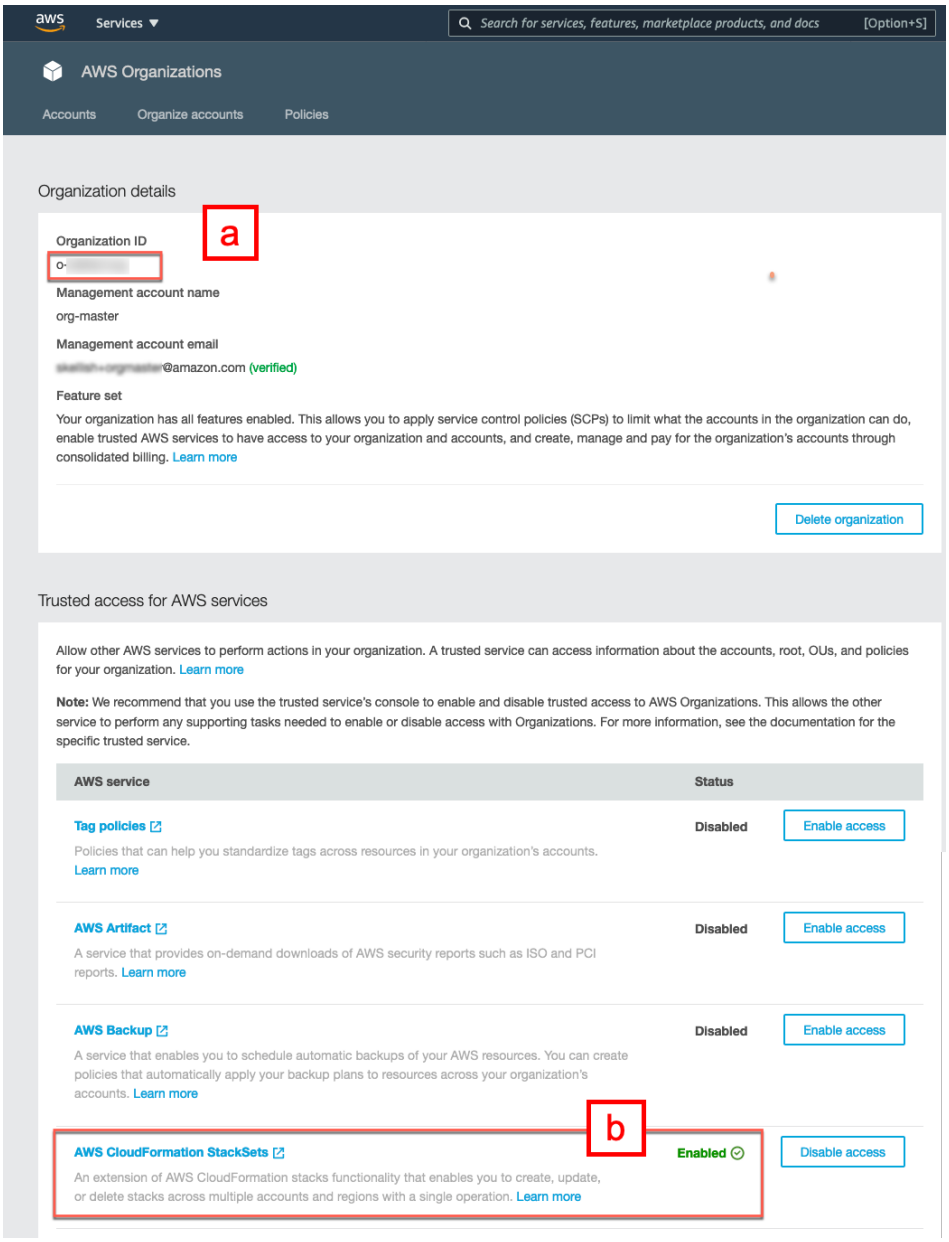
AWS Organizations Use Case

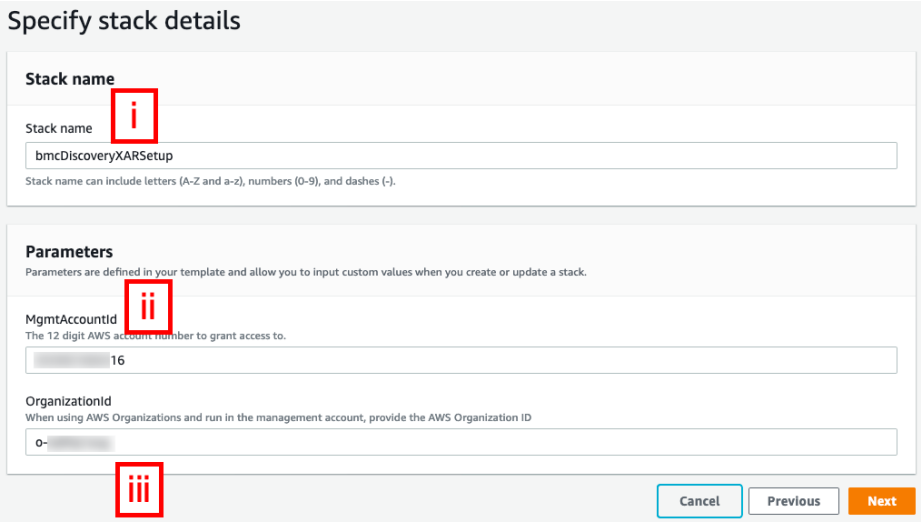
In the Management account:

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.



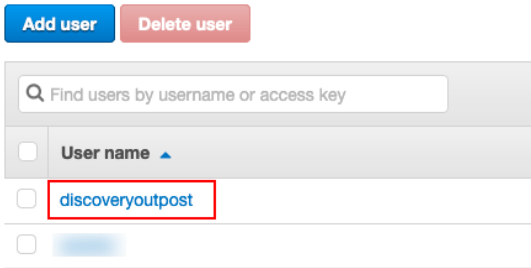
    c. Deploy an AWS CloudFormation stack using the provided template bmcDiscoveryXARSetup.yaml.

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

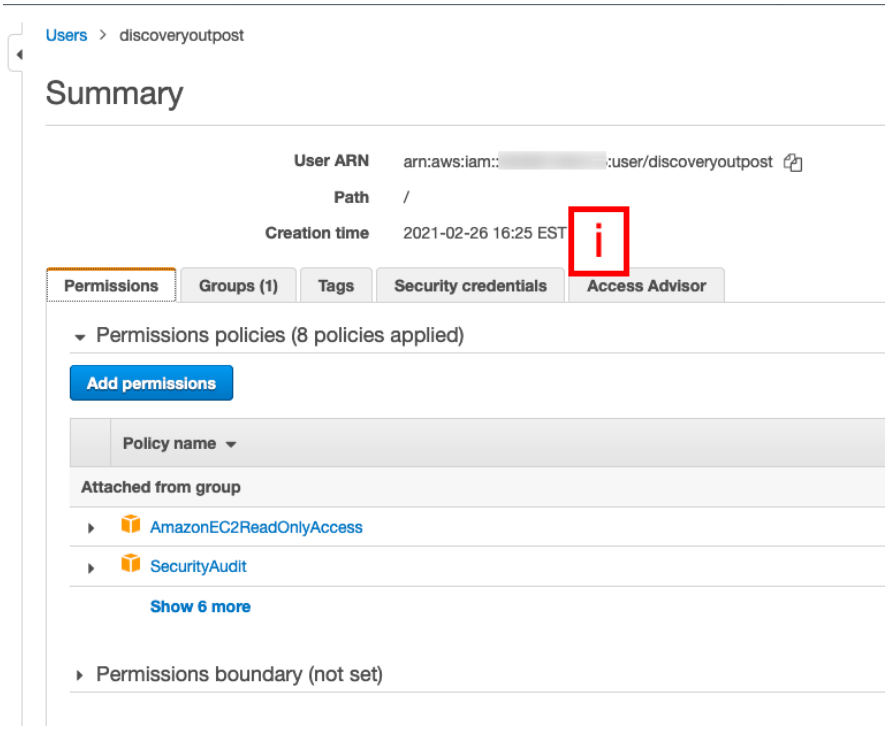


iv. Wait for the stack to successfully complete

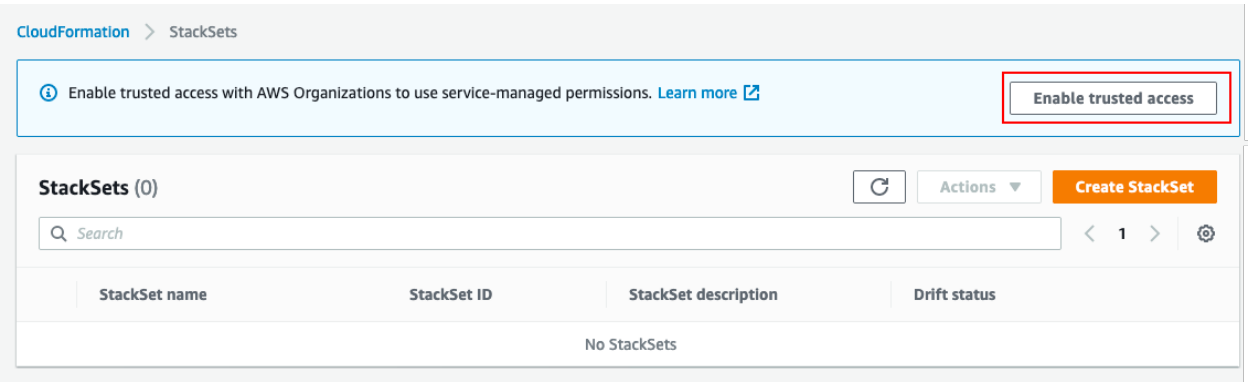
d. Go to IAM | Users and select the new 'discoveryoutpost' user:



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:

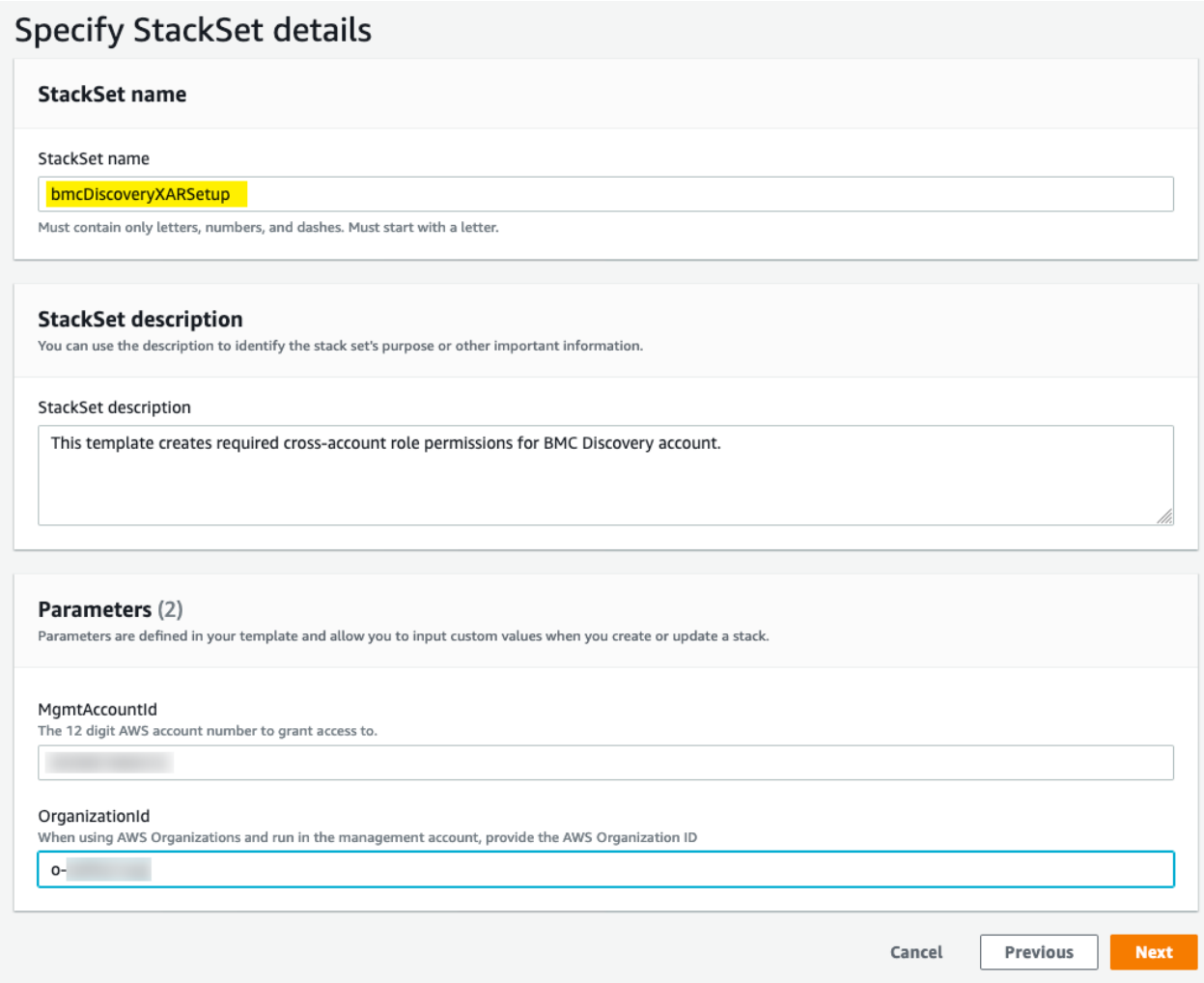


e. Go to the CloudFormation console | StackSets.
   i. Click 'Enable trusted access' if not already enabled.

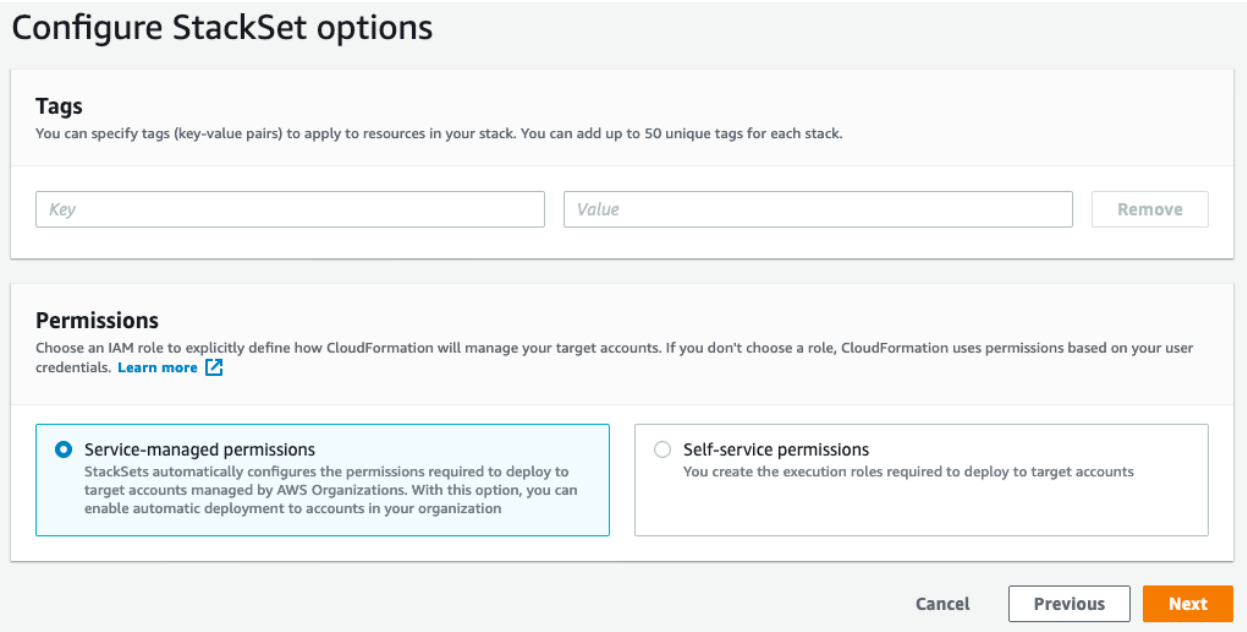


   ii. Click 'Create StackSet'
   iii. On the 'Choose a template' page,
      1. Provide the S3 URL if you uploaded the provided template bmcDiscoveryXARSetup.yaml to an S3 bucket as described earlier, otherwise, upload the template on this page.
      2. Click 'Next'
   iv. On the 'Specify StackSet details' 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

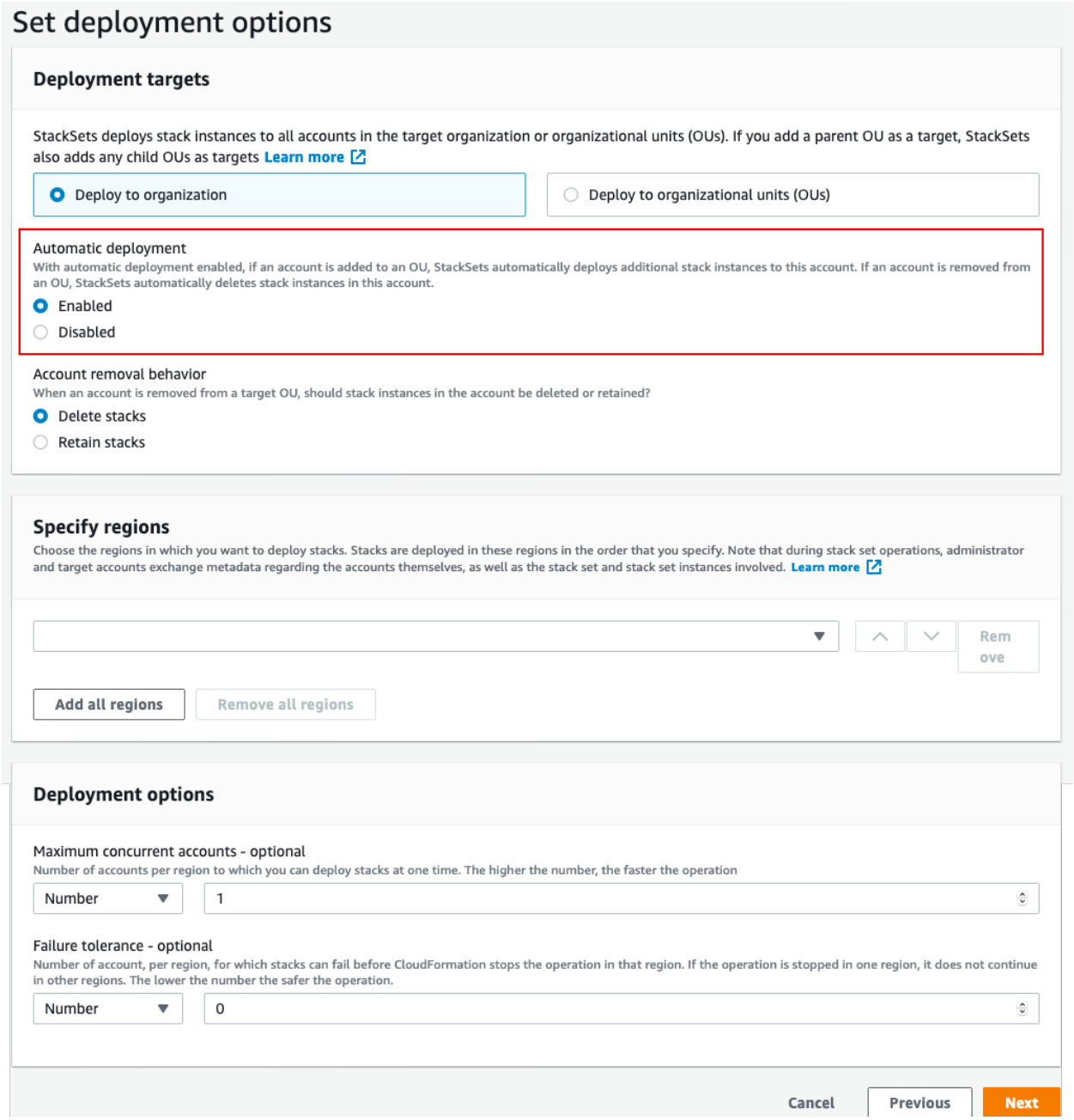
3. Provide the AWS Organization ID you copied in the earlier step.
4. Click 'Next'



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'



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’



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'

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.

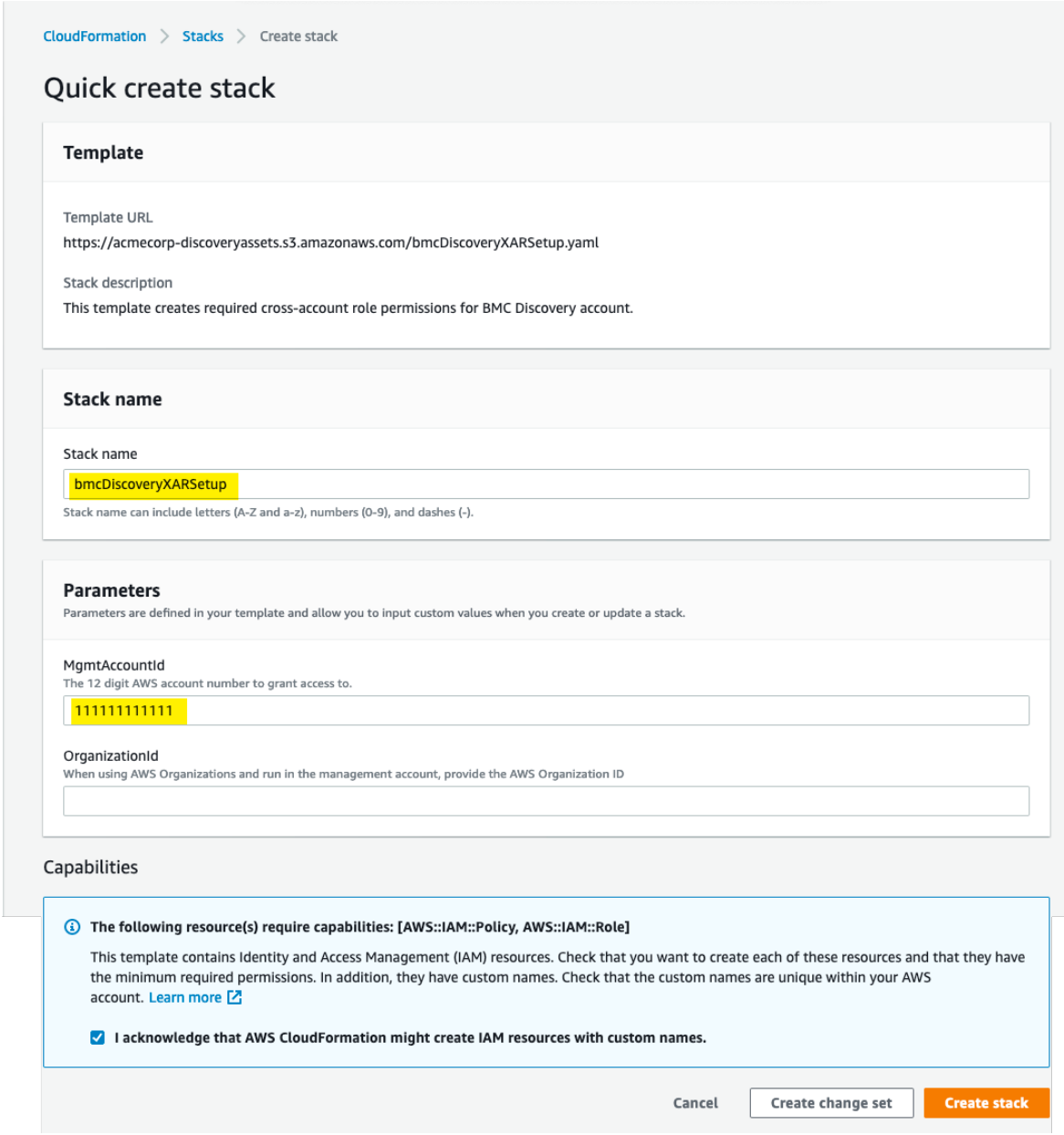
Non- AWS Organizations Use Case

In the 'Parent' account:

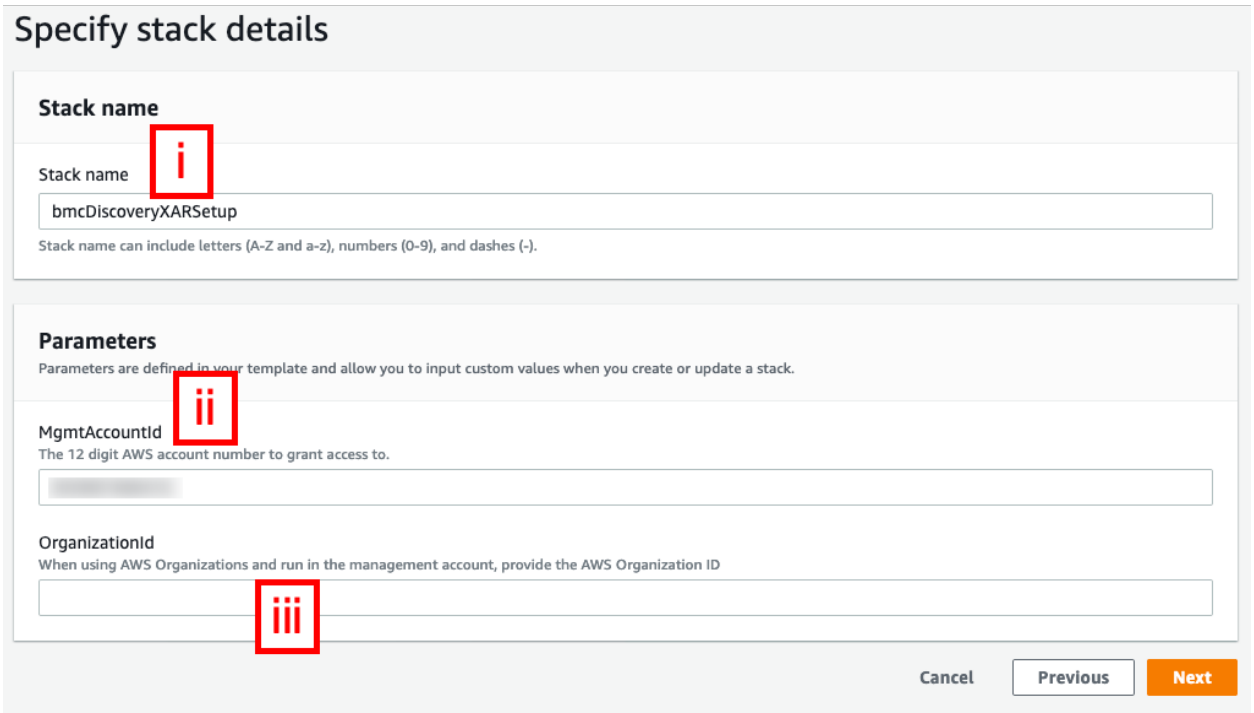
1. (prereq, optional): Because the template needs to be run in every linked account, to simplify the deployment it's recommended to:
    a. Copy the template, bmcDiscoveryXARSetup.yaml, to an S3 bucket with sufficient permissions that the admins for each of the linked accounts can open and execute the 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&param_MgmtAccountId=111111111111&param_OrganizationId=

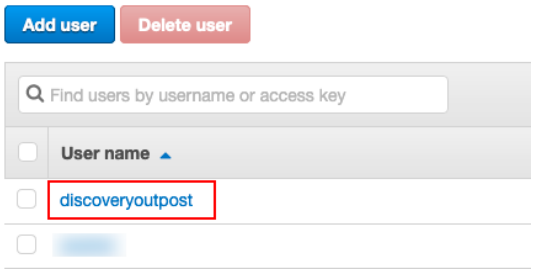


c. Deploy a CloudFormation stack using the provided template bmcDiscoveryXARSetup.yaml.
   i. For consistency, it's recommended you name the stack ‘bmcDiscoveryXARSetup’
   ii. Provide the AWS Account ID for this current ‘master’ account.
   iii. Leave the AWS Organization ID parameter empty.

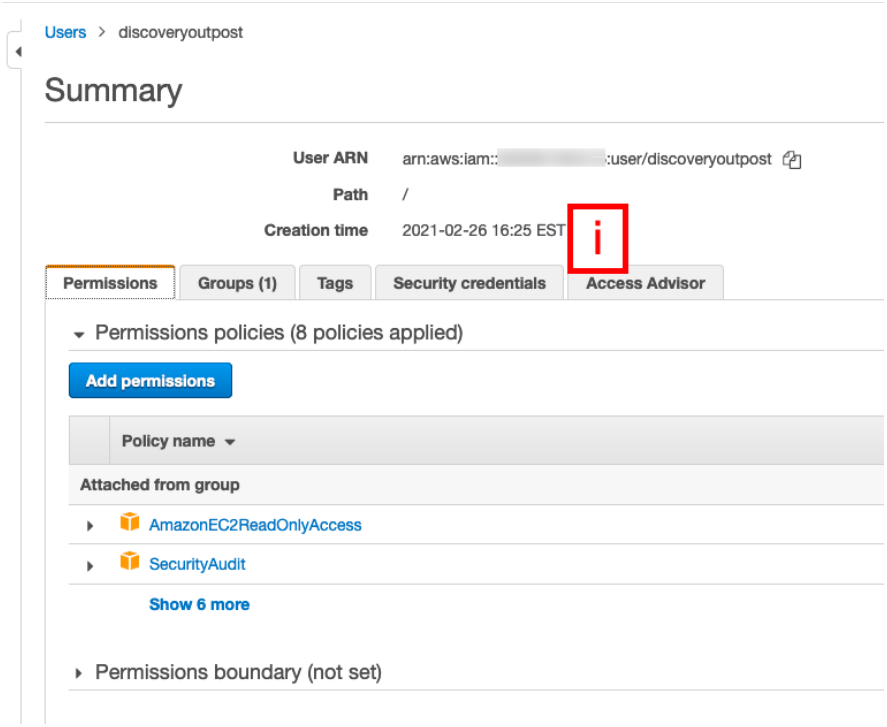


iv. Wait for the stack to successfully complete

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



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:

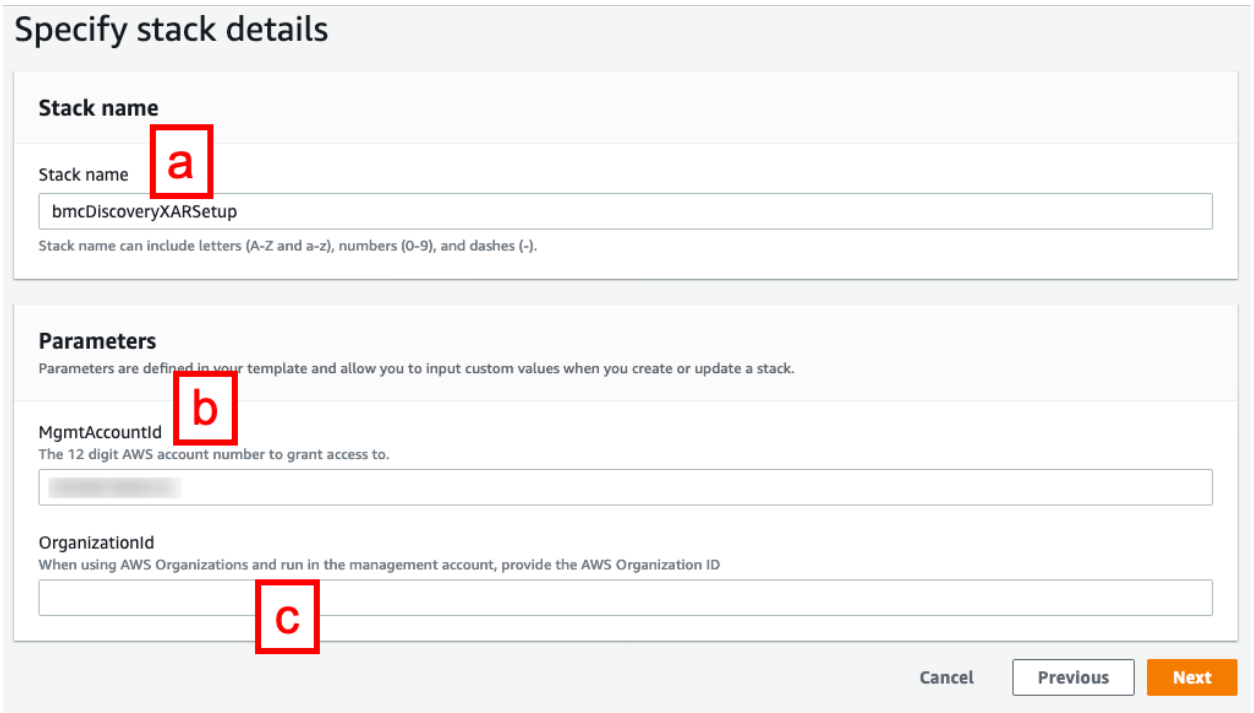


In each linked account:

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.



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.

```
[profile discoveryoutpostM]
aws_access_key_id=
aws_secret_access_key=
region=us-east-1

[profile discoveryoutpostC1]
region=us-east-1
role_arn=arn:aws:iam::222222222222:role/bmcDiscoveryROScanTrustRole
source_profile=discoveryoutpostM

[profile discoveryoutpostC2]
region=us-east-1
role_arn=arn:aws:iam::333333333333:role/bmcDiscoveryROScanTrustRole
source_profile=discoveryoutpostM
```

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"
                }
            ]
        ]
    ]
]
$
```