

**Role Creation and Use for BMC Discovery access via AWS Organizations, Stacks and Stack Sets.**

The purpose of this document is to outline the Stack and StackSet deployment steps necessary for BMC Discovery to assume a role to member accounts.

The attached CloudFormation template has two distinct parts. The first part should be deployed as a Stack on the Management account and will create the necessary local User Group, Local User, inline policy and attach AWS managed policies as necessary for Discovery to connect and assume a role to the targeted Member accounts. Once created you’ll need to create the needed Access and Secret Keys.

The second portion of the CFN Template should be deployed as a StackSet from the Management account and this will create the necessary Role, trusting the aforementioned Management account ID (you’ll have the opportunity to specify this during deployment. During deployment you can target a specific OU or deploy the role to every account within the organization. Its recommended to create a test OU with a test account to build familiarity and confidence in the deployment process before applying the template to production accounts.

A critical requirement is to enable all features in the organization. See link and screenshot below:

This must be enabled for the Management account to interact with the Member accounts. <https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_org_support-all-features.html>.



Glossary of Terms:

* OU = Organization Unit.
* CFN = CloudFormation.
* Stack = In this context we’re deploying a Stack on the Management account to create the local user which Discovery will use to connect to the account. <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacks.html>
* StackSet = This StackSet will deploy a role and attach policies on the selected Member Account. <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/what-is-cfnstacksets.html>
* Management and Member account = Management accounts contains member accounts and organization and consolidated billing for all members. <https://docs.aws.amazon.com/organizations/latest/userguide/orgs_best-practices_mgmt-acct.html> and <https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts.html>

Prerequisites:

* Organization ID
	+ https://console.aws.amazon.com/organizations/v2/home/settings
* OU ID if deploying to an OU and not the complete organization.
	+ <https://console.aws.amazon.com/organizations/v2/home/accounts>
	+ Currently all accounts within the OU and sub OUs will be targeted.
	+ It’s a good practice to create a new OU with a single account to test StackSet deployment. Keep in mind that once the account is moved from the test OU the Stack will be uninstalled.
* Master account ID
* Basic understanding of the IAM console, roles, and stacks/stackSets.

Helpful links.

* What are CFN stacksets
	+ <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/what-is-cfnstacksets.html>
* How to deploy stack sets.
	+ <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacks.html>

Feel free to change the key names in the YAML to reflect your corporate standards; IAM User, Group, Role and Policy names.

StackSet YAML in separate file as well as at bottom of this doc.

**Deploy the Stack on the Master account.**

This will create an IAM user group, needed policies, a user and attach the user and policies to the user group. You will need to manually create the Access Key and Secret Key after creation.

<https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html>

Create a new stack in Cloud Formation:

Navigate to Cloud Formation and select “Stacks” on the left menu.



Then select “Create New Stack”, “With new Resources”.



Next select “Template is ready”, “Upload a template file”, browse and select the YAML file. Click “Next”.



Create a memorable Stack Name and enter the AWS Master Account ID and Organization ID.



Its ok to leave the defaults in the next page and click Next. Review the next page and check the “Acknowledge…” and click “Create Stack”.



You should now validate that the User Group, attached policies User have been created in the IAM console.

**IAM CONSOLE**: [https://console.aws.amazon.com/iam/home?#/home](https://console.aws.amazon.com/iam/home#/home)

Open the “Security Credentials” tab in the newly created user and click “Create Access Key”.



**Deploy the StackSET from the Master account to the member account(s).**

From the Master Cloud Formation console, select “StackSets” and “Create StackSet.”



Next leave default “Template is ready”, select “Upload a template file” and browse to the template.



Create a stackSet name and add the Master/Management account ID and organization ID. This is used for the role trust and the organization ID is used to as an extra security check.



Leave default “Service-managed permissions” and select “next”.



Select “Deploy to organizational units” and input the OU ID. The StackSet will deploy on all member accounts within that OU.



If you move an account out of that OU the StackSet will be removed and the resources (role) removed.

To change this select “retain stacks” in “Account removal behavior”



You must specify a region. IAM resources are not region specific.

Change any deployment options as necessary or leave defaults as desired.



Review the next page and check the “Acknowledge…” and click “Create Stack”.



The stack will deploy to the member accounts in the OU specified. Verify the role created successfully, if necessary, directly on the member account.

TEMPLATE YAML.

AWSTemplateFormatVersion: 2010-09-09

Description: This template creates required cross-account role permissions for BMC

 Helix Discovery to scan account resources. Supports both use of AWS Organizations

 and non-AWS Organization environments account. \*\*WARNING\*\* This template creates

 AWS resources. You will be billed for the AWS resources used if you create a stack

 from this template. Use at your own risk.

Metadata:

 AWS::CloudFormation::Interface:

 ParameterGroups:

 - Label:

 default: Discovery Parameters

 Parameters:

 - MgmtAccountId

 - IAMUserName

 ParameterLabels:

 MgmtAccountId:

 default: Management/Master Account ID

 IAMUserName:

 default: Discovery IAM user name

Parameters:

 MgmtAccountId:

 AllowedPattern: '[0-9]+'

 Description: The 12 digit AWS account number to grant access to.

 MaxLength: '12'

 MinLength: '12'

 Type: String

 IAMUserName:

 Description: Name of IAM user to be used to switch roles

 Type: String

 Default: discovery

Conditions:

 IsMgmtAccount: !Equals

 - !Ref 'MgmtAccountId'

 - !Ref 'AWS::AccountId'

Resources:

 # Group to consolidate the Discovery scan permissions as a best practice, even though we only have one

 # user 'discovery' in the group

 bmcDiscoveryROScanIAMGroup:

 Condition: IsMgmtAccount

 Type: AWS::IAM::Group

 Properties:

 ManagedPolicyArns:

 - arn:aws:iam::aws:policy/ReadOnlyAccess

 - arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess

 Policies:

 - PolicyName: bmcDiscoveryROScanAssumeRolePolicy

 PolicyDocument:

 Version: 2012-10-17

 Statement:

 - Effect: Allow

 Action:

 - sts:AssumeRole

 Resource:

 - arn:aws:iam::\*:role/bmcDiscoveryROScanTrustRole

 bmcDiscoveryOutpostUser:

 Condition: IsMgmtAccount

 Type: AWS::IAM::User

 Properties:

 UserName: !Ref 'IAMUserName'

 Groups:

 - !Ref 'bmcDiscoveryROScanIAMGroup'

 bmcDiscoveryROScanTrustRole:

 Type: AWS::IAM::Role

 Metadata:

 cfn-lint:

 config:

 ignore\_checks:

 - W28

 cfn\_nag:

 rules\_to\_suppress:

 - id: W28

 reason: "Explicit name defined to allow BMC Discovery to reference a known value across all customer environments"

 Properties:

 RoleName: bmcDiscoveryROScanTrustRole

 AssumeRolePolicyDocument:

 Version: 2012-10-17

 Statement:

 - Action: sts:AssumeRole

 Effect: Allow

 Principal:

 AWS: !Sub

 - 'arn:aws:iam::${MgmtAccountId}:user/${DiscoveryUserName}'

 - DiscoveryUserName: !If

 - IsMgmtAccount

 - !Ref bmcDiscoveryOutpostUser

 - !Ref IAMUserName

 Path: /

 ManagedPolicyArns:

 - arn:aws:iam::aws:policy/ReadOnlyAccess

 bmcDiscoveryAdditionalROScanPolicy:

 Type: AWS::IAM::Policy

 Metadata:

 cfn-lint:

 config:

 ignore\_checks:

 - W12

 cfn\_nag:

 rules\_to\_suppress:

 - id: W12

 reason: "Wildcard used to allow BMC Discovery to find all resources."

 Properties:

 PolicyName: bmcDiscoveryAdditionalROScanPolicy

 PolicyDocument:

 Version: 2012-10-17

 Statement:

 - Effect: Allow

 Action:

 - lakeformation:List\*

 - sdb:DomainMetadata

 Resource: '\*'

 Groups:

 - !If

 - IsMgmtAccount

 - !Ref 'bmcDiscoveryROScanIAMGroup'

 - !Ref 'AWS::NoValue'

 Roles:

 - !Ref 'bmcDiscoveryROScanTrustRole'

 bmcDiscoverySessionManagerScanPolicy:

 Type: AWS::IAM::Policy

 Metadata:

 cfn-lint:

 config:

 ignore\_checks:

 - W12

 cfn\_nag:

 rules\_to\_suppress:

 - id: W12

 reason: "Wildcard used to allow BMC Discovery to find all resources."

 Properties:

 PolicyName: bmcDiscoverySessionManagerScanPolicy

 PolicyDocument:

 Version: 2012-10-17

 Statement:

 - Effect: Allow

 Action:

 - ssm:StartSession

 Resource: arn:aws:ec2:\*:\*:instance/\*

 - Effect: Allow

 Action:

 - ssm:ResumeSession

 - ssm:TerminateSession

 Resource: '\*'

 Groups:

 - !If

 - IsMgmtAccount

 - !Ref 'bmcDiscoveryROScanIAMGroup'

 - !Ref 'AWS::NoValue'

 Roles:

 - !Ref 'bmcDiscoveryROScanTrustRole'

Outputs:

 RoleARN:

 Description: The ARN of the role that can be assumed by the other account.

 Value: !GetAtt 'bmcDiscoveryROScanTrustRole.Arn'