MVision for AWS

# Integration Pre-requisites

This document lists the pre-requisites necessary for the deployment of MVision for AWS solution. It has been organized as per the use cases of the customer for this product and the pre-requisites necessary to implement the related feature.

If a test/sandbox/lower environment is in scope for a specific use case, the same pre-requisites are applicable, and separate for the lower environment as well, unless specifically mentioned otherwise.

As part of the engagement, once deployment is completed, we will be handing it off to Support and support team will be helping out on any product issues, monitoring etc. For support team to be able to help out, they will occasionally need to login into tenant and they will reach out to designated customer contact to take permission. Please provide contact email address for support to reach out.

**Customer Contact Details:**

|  |  |  |
| --- | --- | --- |
| **Name** | **Email** | **Phone Number** |
|  |  |  |
|  |  |  |

***Please check the check box (**) against each item to indicate readiness of the specific pre-requisites.***

*Links to McAfee-MVision Help portal have been provided under some of the Use Cases below, for reference for additional information about the use case. These links are accessible once you navigate to the Help portal after logging into the MVision-MVision Dashboard.*

1. AWS MVision Integration for User Activity Monitoring and Configuration Audit

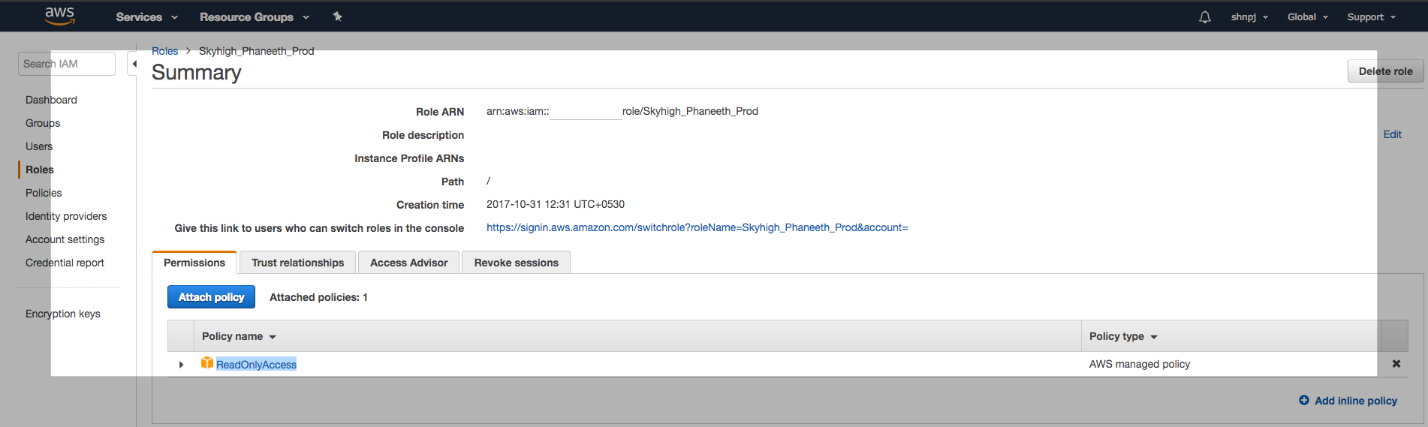
MVision for AWS provides audit compliance policies that help you monitor AWS and your AWS configuration. These policies cover all of CIS Benchmark recommended policies listed at <https://learn.cisecurity.org/benchmarks>. In addition, they also have a list of MVision Recommended best practices for AWS configuration.

**NOTE:**The availability of policies may differ depending on the AWS services your organization is using.

More info on Setting up [MVision for AWS here](https://success.myshn.net/IaaS/Skyhigh_for_AWS).

**IAM role in your AWS account(s) with the standard AWS** [**ReadOnlyAccess**](https://console.aws.amazon.com/iam/home?region=us-east-1#/policies/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FReadOnlyAccess)

**Role assigned to MVision Account and External ID**



MVision for AWS can import user activity logs generated by AWS CloudTrail and process them using the Behavior Analytics Engine to look for access anomalies and potential threats.

**AWS Cloud Trail Logs from all AWS accounts should be routed to the specified S3 bucket of one of the AWS accounts configured in MVision.**

[Link to AWS Help](http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-receive-logs-from-multiple-accounts.html)

|  |  |  |  |
| --- | --- | --- | --- |
| AWS Account | ARN Role | Preferred Name | AWS Bucket Name |
| AWS Account # 1 |  |  | <Name of S3 Bucket configured for CloudTrail logs> |
| AWS Account # 2 |  |  |  |
| AWS Account # 3 |  |  |  |

|  |  |
| --- | --- |
| MVision Account Details | Value (will be visible on the MVision Dashboard) |
| MVision AWS Account ID |  |
| External ID |  |

An alternate method is to have the AWS details in a CSV with the below format and upload to MVision Dashboard

role-arn, preferred-name, aws-bucket-name

role-arn, preferred-name, aws-bucket-name

1. Custom Configuration Audit Rules using Lambda Scripts

MVision allows building of custom Configuration Audit Policies based on Amazon Lambda scripts. This would require assigning additional permissions to the MVision IAM User.

More info on Custom rules using [lambda functions here](https://success.myshn.net/IaaS/Skyhigh_for_AWS).

Allow Lambda scripts Service to assume the MVision IAM user assigned Role

Editing the trust relationship:

1. Navigate to AWS: Roles > MVision\_for\_aws\_role > Trust relationships > Edit trust relationship
2. Add the following to the beginning of the JSON (just after Statement line).

*{*

*"Effect": "Allow",*

*"Principal": {*

*"Service": "lambda.amazonaws.com"*

*},*

*"Action": "sts:AssumeRole"  
 },*



Add an additional policy that has permissions to create and execute Lambda scripts to MVision Role in IAM

Adding the Policy:

1. Navigate to IAM and create a new policy called SHN\_Lambda
2. Select JSON and paste the following:

*{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "Stmt1510661968000",  
            "Effect": "Allow",  
            "Action": [  
                "lambda:CreateFunction",  
                "lambda:DeleteFunction",  
                "lambda:GetFunction",  
                "lambda:GetFunctionConfiguration",  
                "lambda:InvokeFunction",  
                "lambda:ListFunctions",  
                "lambda:UpdateFunctionCode",  
                "lambda:UpdateFunctionConfiguration",  
                "iam:PassRole"  
            ],  
            "Resource": [  
                "\*"  
            ]  
        }  
    ]  
}*

1. Attach this new policy to the existing MVision\_for\_aws\_role role.
2. Send Configuration Audit Policy incidents to AWS SNS Topics and SQS service

MVision integrates with AWS SNS and SQS by allowing configuration audit policy incidents to be sent to them. This is achieved on a per audit policy level and allows automatic remediation by having Lambda functions triggered via topics/messages.

Add an additional policy that has permissions to create and execute Lambda scripts to MVision Role in IAM

Adding the Policy:

1. Navigate to IAM and create a new policy called SHN\_SNS\_SQS
2. Select JSON and paste the following:

*{  
   "Version": "2012-10-17",  
   "Statement": [  
       {  
           "Effect": "Allow",  
           "Action": [  
               "sns:Publish",  
               "sns:Subscribe",  
               "sns:Unsubscribe",  
               "sqs:ListQueues",  
               "sqs:SendMessage",  
               "sns:GetTopicAttributes"  
           ],  
           "Resource": "\*"  
       }  
   ]  
}*

1. Attach this new policy to the existing MVision\_for\_aws\_role role.
2. AWS MVision Integration to perform On Demand Scan for DevOps templates and S3 buckets

MVISION performs On-Demand Scans provide Data Loss Prevention (DLP) protection to files stored in Amazon S3 Buckets and DevOps template scans.

* On-Demand Scans evaluate data protection policies for the content in S3 buckets and support targeted investigations on data in S3
* DevOps On-Demand Scans identify compliance issues and enforce remediation steps earlier in the cycle saving time and effort

Add an additional policy that has permissions to scan DevOps templates

Adding the Policy:

1. Navigate to IAM and create a new policy called SHN\_SNS\_SQS
2. Select JSON and paste the following:

{

    "Version": "2012-10-17",

    "Statement": [{

        "Sid": "VisualEditor0",

        "Effect": "Allow",

        "Action": [

            "s3:GetObject",

            "s3:ListBucket",

            "cloudformation:ValidateTemplate"

        ],

        "Resource": "\*"

    }]

}

1. Attach this new policy to the existing MVision\_for\_aws\_role