Splunk® Supported Add-ons
Splunk Add-on for AWS released

Configure AWS permissions for the Splunk Add-on for AWS

Generated: 5/16/2020 5:57 pm
Configure AWS permissions for the Splunk Add-on for AWS

Before installing the Splunk Add-on for AWS, configure AWS permissions for your Amazon Web Services accounts.

Before you can configure Splunk to work with your AWS data, you must set up accounts in Amazon Web Services.

Configure AWS accounts and permissions

To configure AWS accounts and permissions, you must have administrator rights in the AWS Management Console. If you do not have administrator access, work with your AWS admin to set up the accounts with the required permissions.

- To let the Splunk Add-on for Amazon Web Services access the data in your AWS account, you assign one or more AWS accounts to an IAM (AWS Identity Account Management) role. You then grant those roles the permissions that are required required by the AWS account.

- If you run this add-on on a Splunk platform instance in your own managed Amazon EC2 (Elastic Compute Cloud), then assign that EC2 to a role and give that role the IAM permissions listed here.

Manage IAM policies

There are three ways to manage policies for your IAM roles:

- Use the AWS Policy Generator tool to collect all permissions into one centrally managed policy. You can apply the policy to the IAM group that is used by the account(s) or the EC2s that the Splunk App for AWS uses to connect to your AWS environment.
- Create multiple different users, groups, and roles with permissions specific to the services from which you plan to collect data.
- Copy and paste the sample policies provided on this page and apply them to an IAM Group as custom inline policies. To further specify the resources to which the policy grants access, replace the wildcards with the exact ARNs (Amazon Resource Names) of the resources in your environment.

For more information about working with inline policies, see the AWS documentation.

Create and configure roles to delegate permissions to IAM users

The Splunk Add-on for AWS supports the AWS Security Token Service (AWS STS) AssumeRole API action that lets you use IAM roles to delegate permissions to IAM users to access AWS resources.

AssumeRole returns a set of temporary security credentials (consisting of an access key ID, a secret access key, and a security token) that an AWS account can use to access AWS resources that it might not normally have access to.

To assume a role, your AWS account must be trusted by the role. The trust relationship is defined in the role’s trust policy when the role is created. That trust policy states which accounts are allowed to delegate access to this account's role.

The user who wants to access the role must also have permissions delegated from the role’s administrator. If the user is in a different account than the role, then the user's administrator must attach a policy that allows the user to call AssumeRole on the ARN of the role in the other account. If the user is in the same account as the role, then you can either attach a policy to the user (identical to the previous different account user), or you can add the user as a principal directly in the role’s trust policy.
To create an IAM role, follow the instructions in the AWS documentation:

After creating the role, use the AWS Management Console to modify the trust relationship to allow the IAM user to assume the newly created role. The following example shows a trust relationship that allows a role to be assumed by an IAM user named johndoe:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/johndoe"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Next, grant your IAM user permission to assume the role. The following example shows an AWS Identity and Access Management policy that allows an IAM user to assume the s3admin role:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::123456789012:role/s3admin"
        }
    ]
}
```

Configure one policy containing permissions for all inputs

The following sample policy provides the necessary permissions for all ten inputs included in the Splunk Add-on for AWS. See the remaining sections for separate policies that break out the permissions for each service.

Sample inline policy:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
        }
    ]
}
```
"s3:GetObject",
"s3:GetBucketLocation",
"s3:ListAllMyBuckets",
"s3:GetBucketTagging",
"s3:GetAccelerateConfiguration",
"s3:GetBucketLogging",
"s3:GetLifecycleConfiguration",
"s3:GetBucketCORS",
"config:DeliverConfigSnapshot",
"config:DescribeConfigRules",
"config:DescribeConfigRuleEvaluationStatus",
"config:GetComplianceDetailsByConfigRule",
"config:GetComplianceSummaryByConfigRule",
"iam:GetUser",
"iam:ListUsers",
"iam:GetAccountPasswordPolicy",
"iam:ListAccessKeys",
"iam:GetAccessKeyLastUsed",
"autoscaling:Describe*",
"cloudwatch:Describe*",
"cloudwatch:Get*",
"cloudwatch:List*",
"sns:Get*",
"sns:List*",
"sns:Publish",
"logs:DescribeLogGroups",
"logs:DescribeLogStreams",
"logs:GetLogEvents",
"ec2:DescribeInstances",
"ec2:DescribeReservedInstances",
"ec2:DescribeSnapshots",
"ec2:DescribeRegions",
"ec2:DescribeKeyPairs",
"ec2:DescribeNetworkAcls",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeVolumes",
"ec2:DescribeVpcs",
"ec2:DescribeImages",
"ec2:DescribeAddresses",
"lambda:ListFunctions",
"rds:DescribeDBInstances",
"cloudfront:ListDistributions",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeInstanceHealth",
"elasticloadbalancing:DescribeTags",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"elasticloadbalancing:DescribeListeners",
"inspector:Describe*",
"inspector:List*",
"kinesis:Get*",
"kinesis:DescribeStream",
"kinesis:ListStreams",
"kms:Decrypt",
"sts:AssumeRole"
],
"Resource": [ ]
}
Configure AWS Config permissions

Set the following permissions in your AWS configuration:

- **For the S3 bucket that collects your Config logs:**
  - `GetObject`
  - `GetBucketLocation`
  - `ListBucket`
  - `ListAllMyBuckets`

- **For the SQS subscribed to the SNS Topic that collects Config notifications:**
  - `GetQueueAttributes`
  - `ListQueues`
  - `ReceiveMessage`
  - `GetQueueUrl`
  - `SendMessage`
  - `DeleteMessage`

- **For the Config snapshots:** `DeliverConfigSnapshot`

- **For the IAM user to get the Config snapshots:** `GetUser`

Sample inline policy:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "sqs:ListQueues",
        "sqs:ReceiveMessage",
        "sqs:GetQueueAttributes",
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
        "sqs:DeleteMessage"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```
For more information and sample policies:

- For S3: http://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html

Configure CloudTrail permissions

Required permission for the S3 bucket that collects your CloudTrail logs: Get*, List*, Delete*

Granting the delete permission is required to support the option to remove log files when you are done collecting them with the add-on. If you set this parameter to false, you do not need to grant delete permissions.

Required permission for the SQS subscribed to the S3 bucket that collects CloudTrail logs: GetQueueAttributes, ListQueues, ReceiveMessage, GetQueueUrl, DeleteMessage

In the Resource section of the policy, specify the ARNs of the S3 buckets and SQS queues from which you want to collect data.

Sample inline policy:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ReceiveMessage",
        "sqs:GetQueueUrl",
        "sqs:DeleteMessage",
        "s3:Get*",
        "s3:List*",
        "s3:Delete*"
      ],
      "Resource": ["*"
    }
  ]
}
```
For more information and sample policies, see:

- S3 information and sample policies: http://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html

**Configure CloudWatch permissions**

Required permissions for CloudWatch: Describe*, Get*, List*

Required permissions for Autoscaling: Describe*

Required permissions for EC2: Describe*

Required permissions for S3: List*

Required permissions for SQS: List*

Required permissions for SNS: List*

Required permissions for Lambda: List*

Required permissions for ELB: Describe*

Sample inline policy:

```json
{
    "Statement": [{
        "Action": [
            "cloudwatch:List*",
            "cloudwatch:Get*",
            "autoscaling:Describe*",
            "ec2:Describe*",
            "s3:List*",
            "sqs:List*",
            "sns:List*",
            "lambda:List*",
            "elasticloadbalancing:Describe*"
        ],
        "Effect": "Allow",
        "Resource": "*"
    }],
    "Version": "2012-10-17"
}
```

For more information and sample policies, see:
Configure CloudWatch Logs (VPC Flow Logs) permissions

Required permissions for logs: DescribeLogGroups, DescribeLogStreams, GetLogEvents

Sample inline policy:

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Action": [
            "logs:DescribeLogGroups",
            "logs:DescribeLogStreams",
            "logs:GetLogEvents"
         ],
         "Effect": "Allow",
         "Resource": "*"
      }
   ]
}
```

You must also ensure that your role has a trust relationship that allows the flow logs service to assume the role. While viewing the IAM role, choose Edit Trust Relationship and replace the policy with this one:

Sample inline policy:

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "Service": "vpc-flow-logs.amazonaws.com"
         },
         "Action": "sts:AssumeRole"
      }
   ]
}
```

Configure Description permissions

Required permissions for EC2 resources: DescribeInstances, DescribeReservedInstances, DescribeSnapshots, DescribeRegions, DescribeKeyPairs, DescribeNetworkAcls, DescribeSecurityGroups, DescribeSubnets, DescribeVolumes, DescribeVpcs, DescribeImages, DescribeAddresses

Required permissions for Lambda: ListFunctions

Required permissions for RDS: DescribeDBInstances

Required permissions for CloudFront, if you are in a region that supports CloudFront: ListDistributions

Required permissions for ELB: DescribeLoadBalancers, DescribeInstanceHealth, DescribeTags, DescribeTargetGroups, DescribeTargetHealth

Required permissions for S3: ListAllMyBuckets, GetAccelerateConfiguration, GetBucketCORS, GetLifecycleConfiguration, GetBucketLocation, GetBucketLogging, GetBucketTagging
Sample inline policy:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeRegions",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcs",
        "ec2:DescribeImages",
        "ec2:DescribeAddresses",
        "lambda:ListFunctions",
        "rds:DescribeDBInstances",
        "cloudfront:ListDistributions",
        "iam:GetUser",
        "iam:ListUsers",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccessKeys",
        "iam:GetAccessKeyLastUsed",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeListeners",
        "s3:ListAllMyBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetBucketCORS",
        "s3:GetLifecycleConfiguration",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketTagging"
      ],
      "Resource": ["*"
    ]
  ]
}
```

Configure S3 permissions

**Required permissions for S3 buckets and objects:** ListBucket, GetObject, ListAllMyBuckets

**Required permissions for KMS:** Decrypt

In the Resource section of the policy, specify the ARNs of the S3 buckets from which you want to collect S3 access logs, CloudFront access logs, ELB access logs, or generic S3 log data.

Sample inline policy:
Configure SQS-based S3 permissions

Required permissions for SQS: GetQueueUrl, ReceiveMessage, DeleteMessage, GetQueueAttributes, ListQueues

Required permissions for S3 buckets and objects:GetObject

Required permissions for KMS:Decrypt

Sample inline policy:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "s3:GetObject",
        "kms:Decrypt"
      ],
      "Resource": "*"
    }
  ],
  "Resource": "*"
}
```

For more information and sample policies, see http://docs.aws.amazon.com/AmazonS3/latest/dev/using-iam-policies.html.

Configure permissions

Required permissions for for the S3 bucket that collects your billing reports: Get*, List*

In the Resource section of the policy, specify the ARNs of the S3 buckets that contain billing reports for your accounts.

Sample inline policy:
Configure Config Rule permissions

Required permission for Config: DescribeConfigRules, DescribeConfigRuleEvaluationStatus, GetComplianceDetailsByConfigRule, GetComplianceSummaryByConfigRule

For more information and sample policies, see http://docs.aws.amazon.com/config/latest/developerguide/example-policies.html

Configure Amazon Inspector permissions

Required permission for Amazon Inspector: Describe*, List*

For more information and sample policies, see http://docs.aws.amazon.com/config/latest/developerguide/example-policies.html
Configure Kinesis permissions

Required permission for Amazon Kinesis: Get*, DescribeStream, ListStreams

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["kinesis:Get*", "kinesis:DescribeStream", "kinesis:ListStreams"],
            "Resource": "*"
        }
    ]
}
```

Configure SQS permissions

Required permission for Amazon SQS: GetQueueAttributes, ListQueues, ReceiveMessage, GetQueueUrl, SendMessage, DeleteMessage

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Configure SNS permissions

Required permission for Amazon SNS: Publish, Get*, List*
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["sns:Publish", "sns:Get*", "sns:List*"],
      "Resource": "*"
    }
  ]
}

For more information, see http://docs.aws.amazon.com/streams/latest/dev/controlling-access.html.