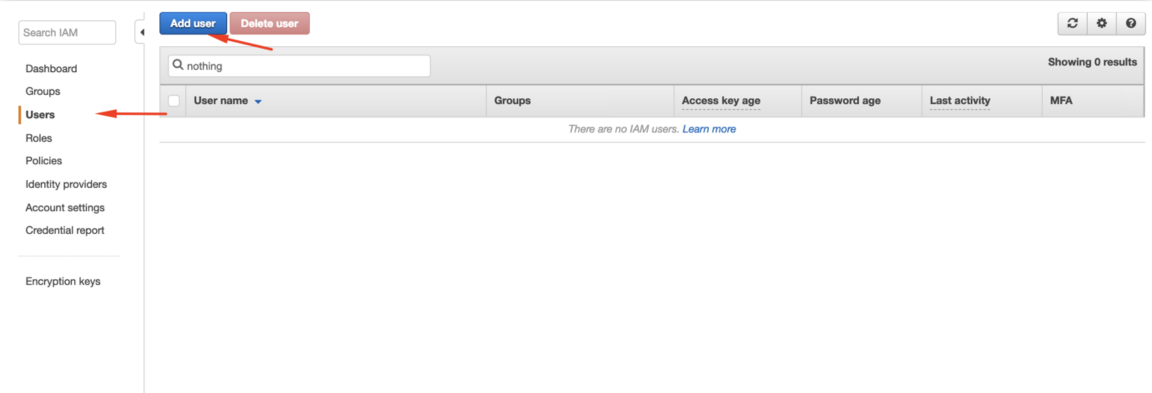
Integrating AVANAN with AWS S3 for Splunk logs - Part One

Step-1:

- Go to AWS IAM: https://console.aws.amazon.com/iam/home#/home

Step-2:

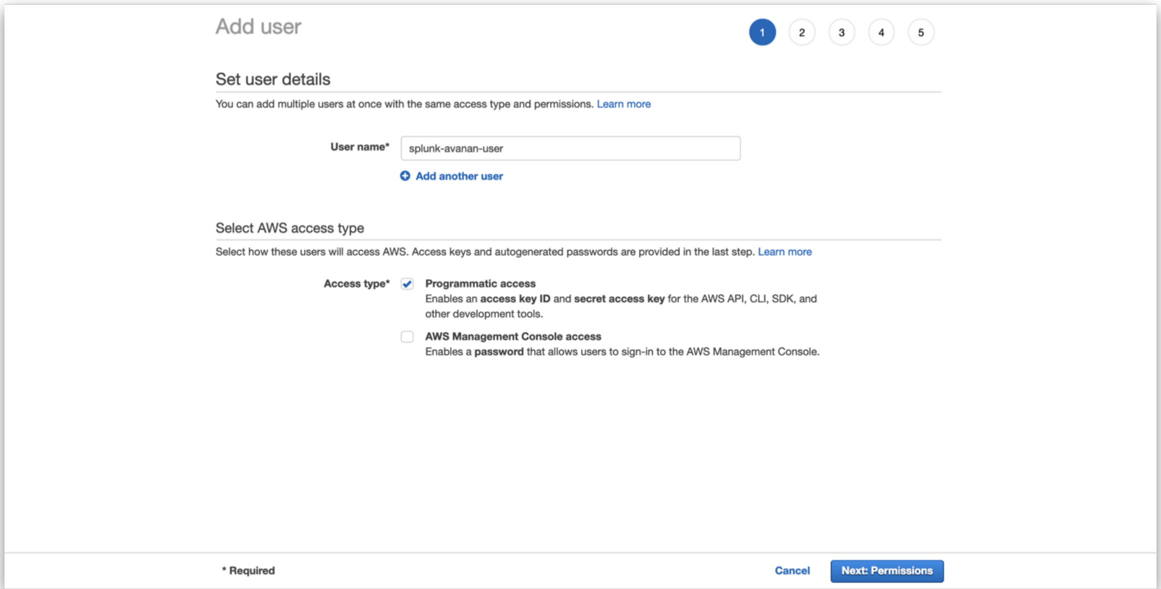
- Click on Users > Add user



There are no IAM users. Learn more

Step-3:

- Select a name and enable “Programmatic access”, click “Next: Permissions”



Add user

Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* splunk-avanan-user

Add another user

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

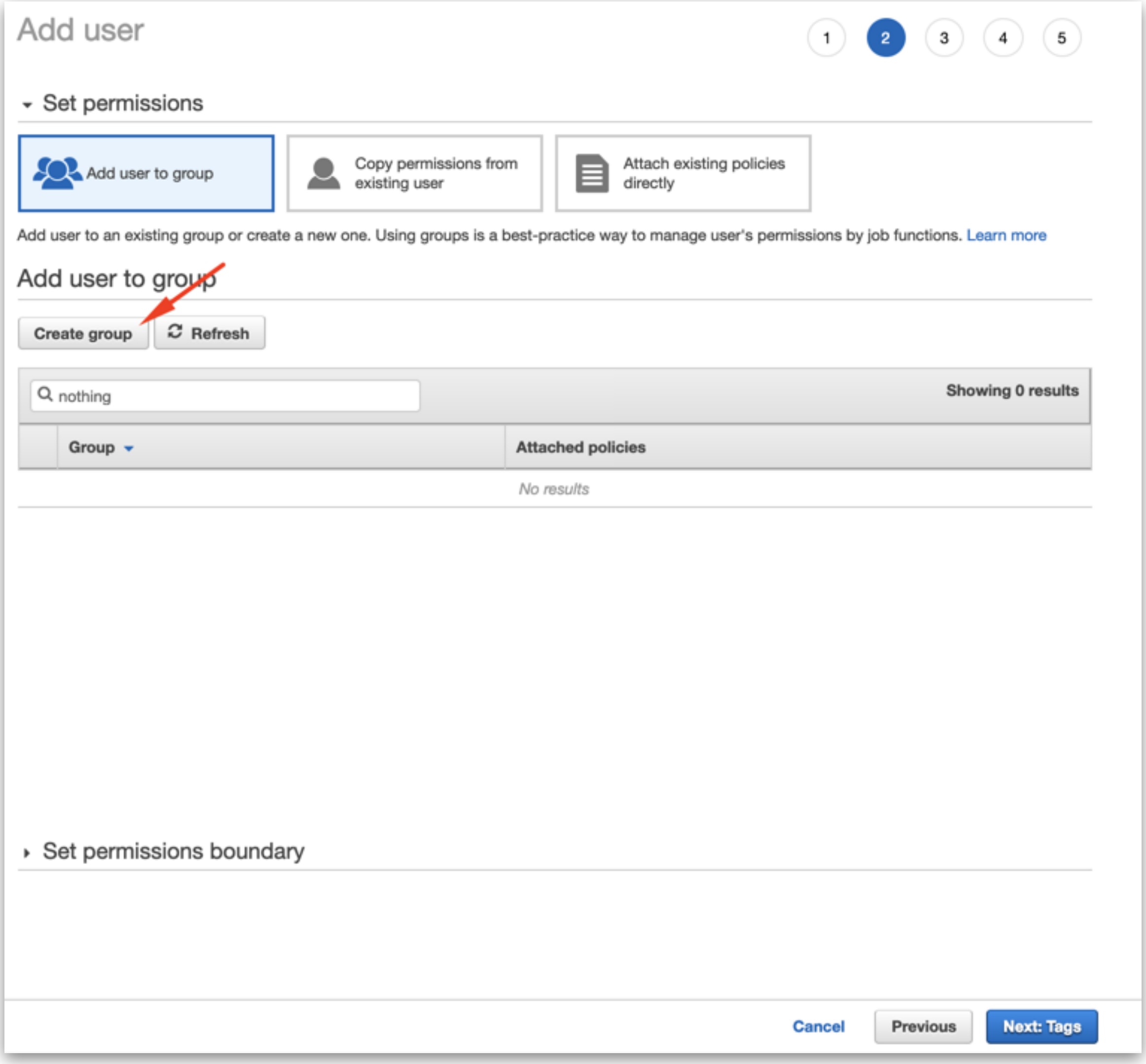
Access type* ☑ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

□ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

* Required

Step-4:

- Click on “Create group” (or the right group if already created)



Add user

Set permissions

Add user to group
Copy permissions from existing user
Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Add user to group

nothing

Showing 0 results

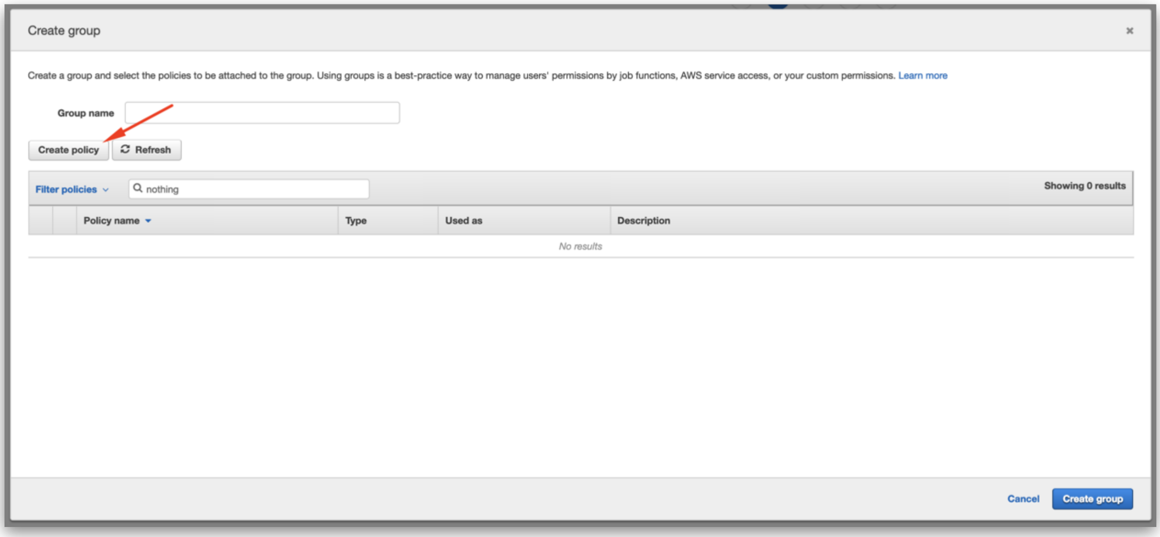
Group	Attached policies
No results	

Set permissions boundary

Cancel
Previous
Next: Tags

Step-5:

- Click on “Create policy” (or select the right policy if already created)



Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Learn more

Group name

Filter policies: nothing

Showing 0 results

	Policy name	Type	Used as	Description

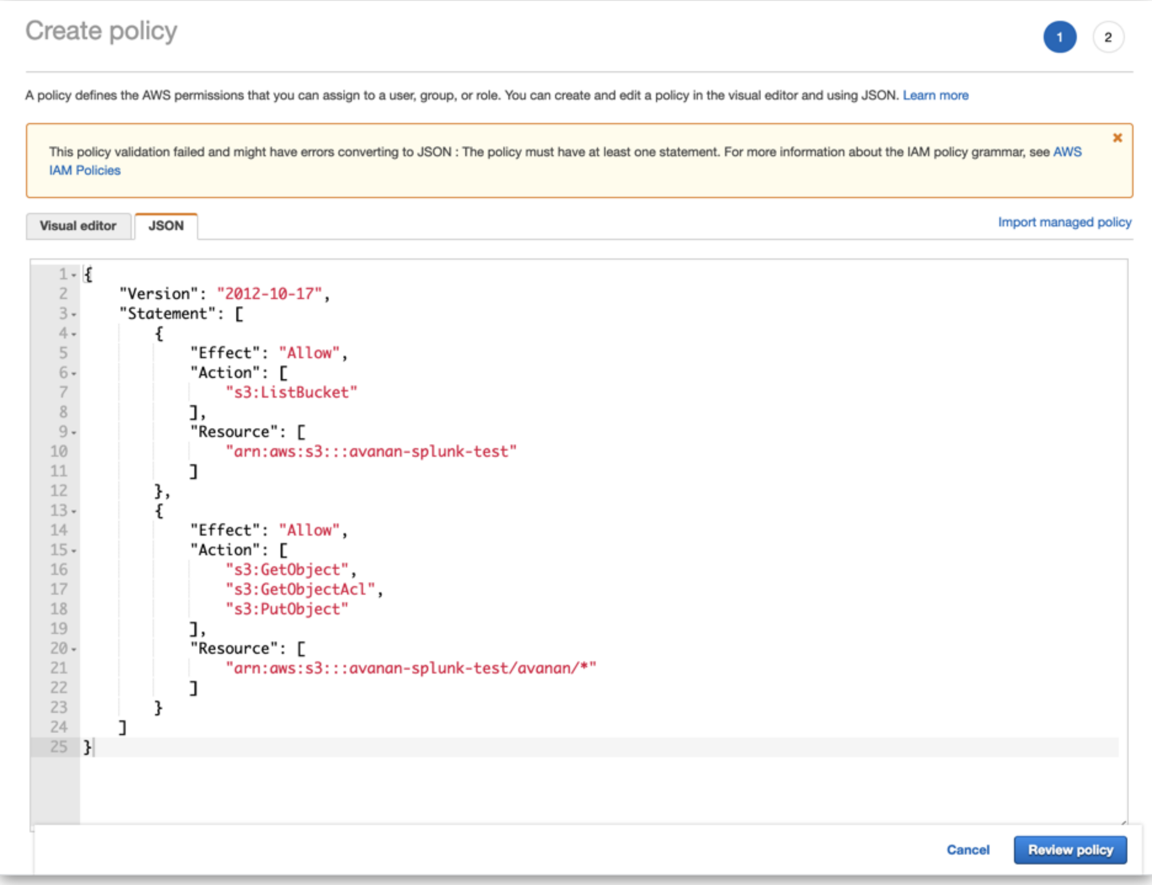
No results

Step-6:

- On the new tab, click on JSON and copy this over:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::YOUR_S3_BUCKET"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::YOUR_S3_BUCKET/THE_LOG_FOLDER_IF_ANY/*"
      ]
    }
  ]
}
```

- For example:



Create policy

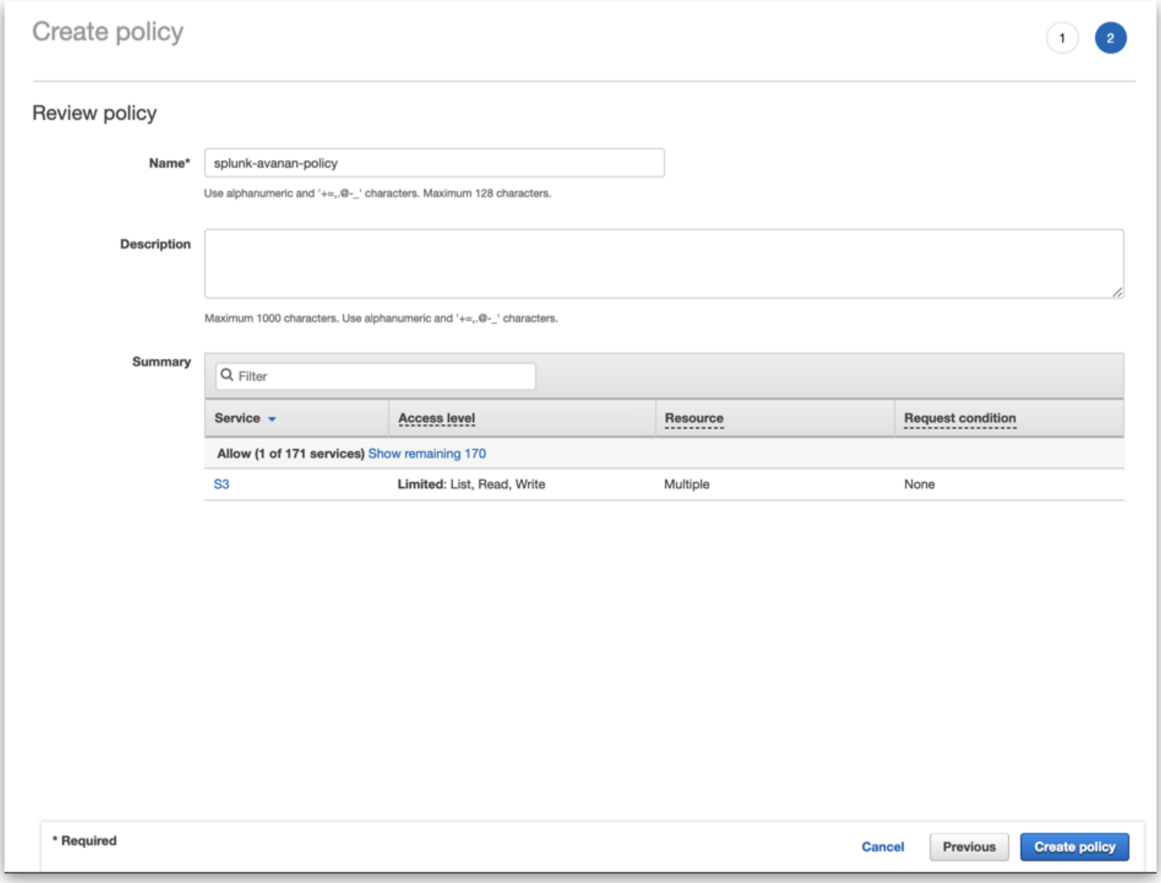
A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

This policy validation failed and might have errors converting to JSON : The policy must have at least one statement. For more information about the IAM policy grammar, see AWS IAM Policies

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::avanan-splunk-test"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::avanan-splunk-test/avanan/*"
            ]
        }
    ]
}
```

Step-7:

- Click on Review Policy
- On the next screen, select a policy name and click on “Create Policy”



Create policy

Review policy

Name* splunk-avanan-policy

Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.

Description

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

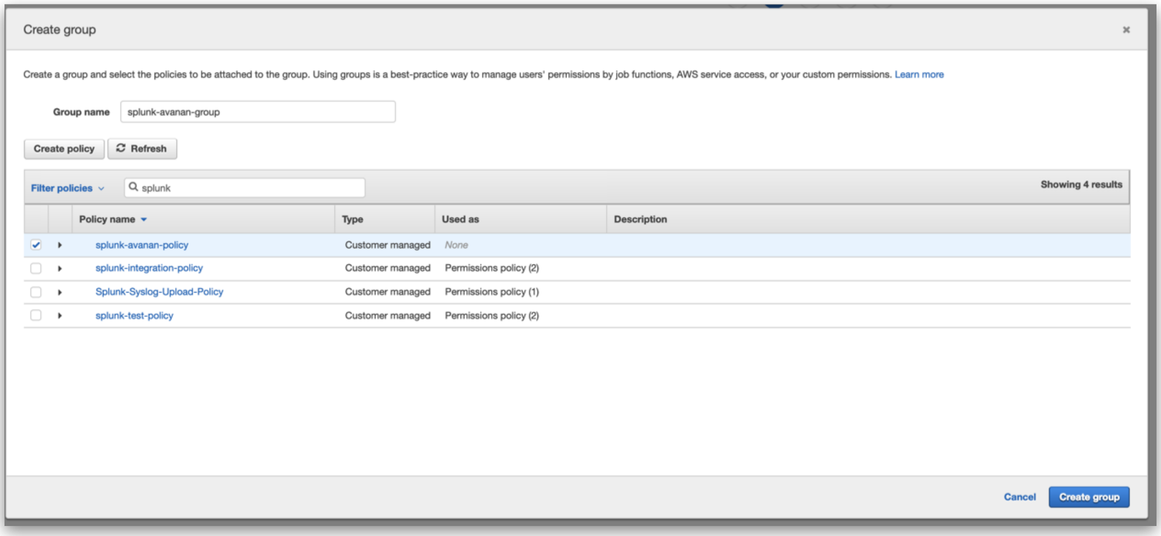
Summary

Service	Access level	Resource	Request condition
Allow (1 of 171 services) Show remaining 170			
S3	**Limited:** List, Read, Write	Multiple	None

* Required

Step-8:

- After the policy is created, go back to the previous tab and click “Refresh”
- Select the policy you just created, give the group a name and click on “Create group”



Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Learn more

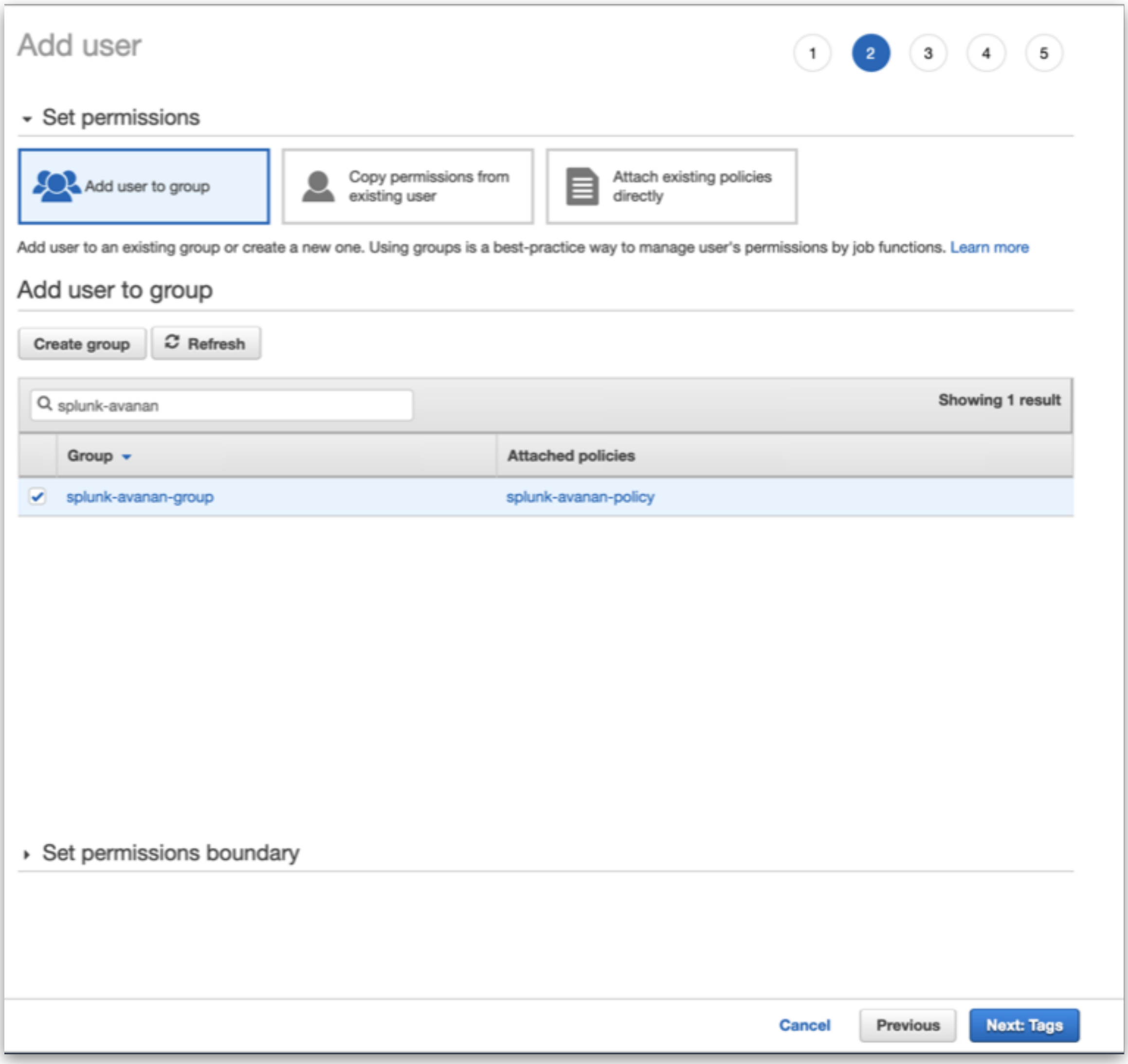
Group name: splunk-avanan-group

Filter policies: splunk — Showing 4 results

		Policy name	Type	Used as	Description
☑	▸	splunk-avanan-policy	Customer managed	*None*	
□	▸	splunk-integration-policy	Customer managed	Permissions policy (2)	
□	▸	Splunk-Syslog-Upload-Policy	Customer managed	Permissions policy (1)	
□	▸	splunk-test-policy	Customer managed	Permissions policy (2)	

Step-9:

- Back to the “Add user” screen, confirm that the group you just created is selected and click on “Next: Tags”



Add user

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Add user to group

splunk-avanan

Showing 1 result

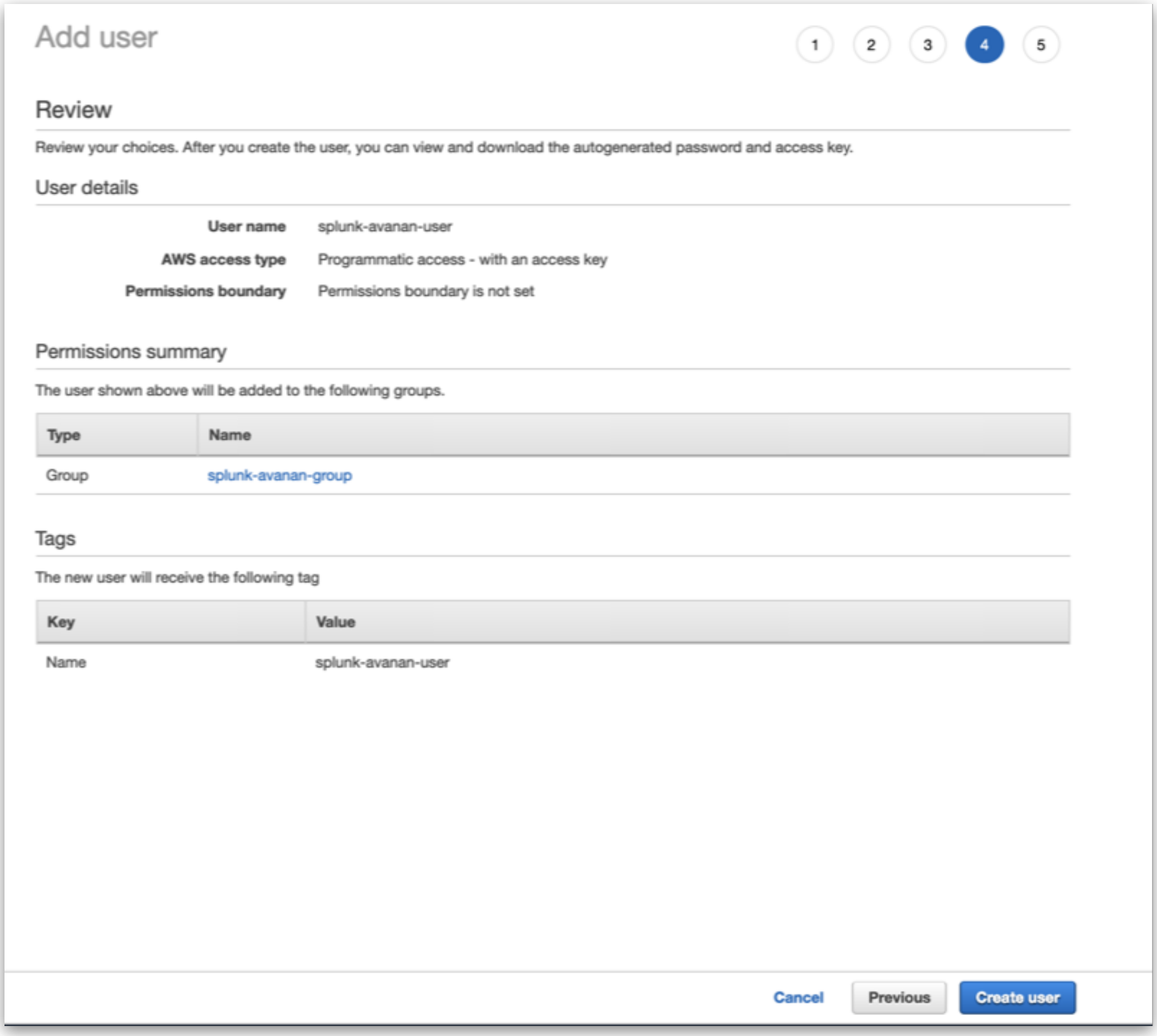
	Group	Attached policies
☑	splunk-avanan-group	splunk-avanan-policy

Set permissions boundary

1
2
3
4
5
Add user to group
Copy permissions from existing user
Attach existing policies directly
Create group
Refresh
Cancel
Previous
Next: Tags

Step-10:

- Add the necessary Tags (in accordance with your environment directives) and click on "Next: Review"
- Confirm all the configurations and click on "Create user"



Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	splunk-avanan-user
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	splunk-avanan-group

Tags

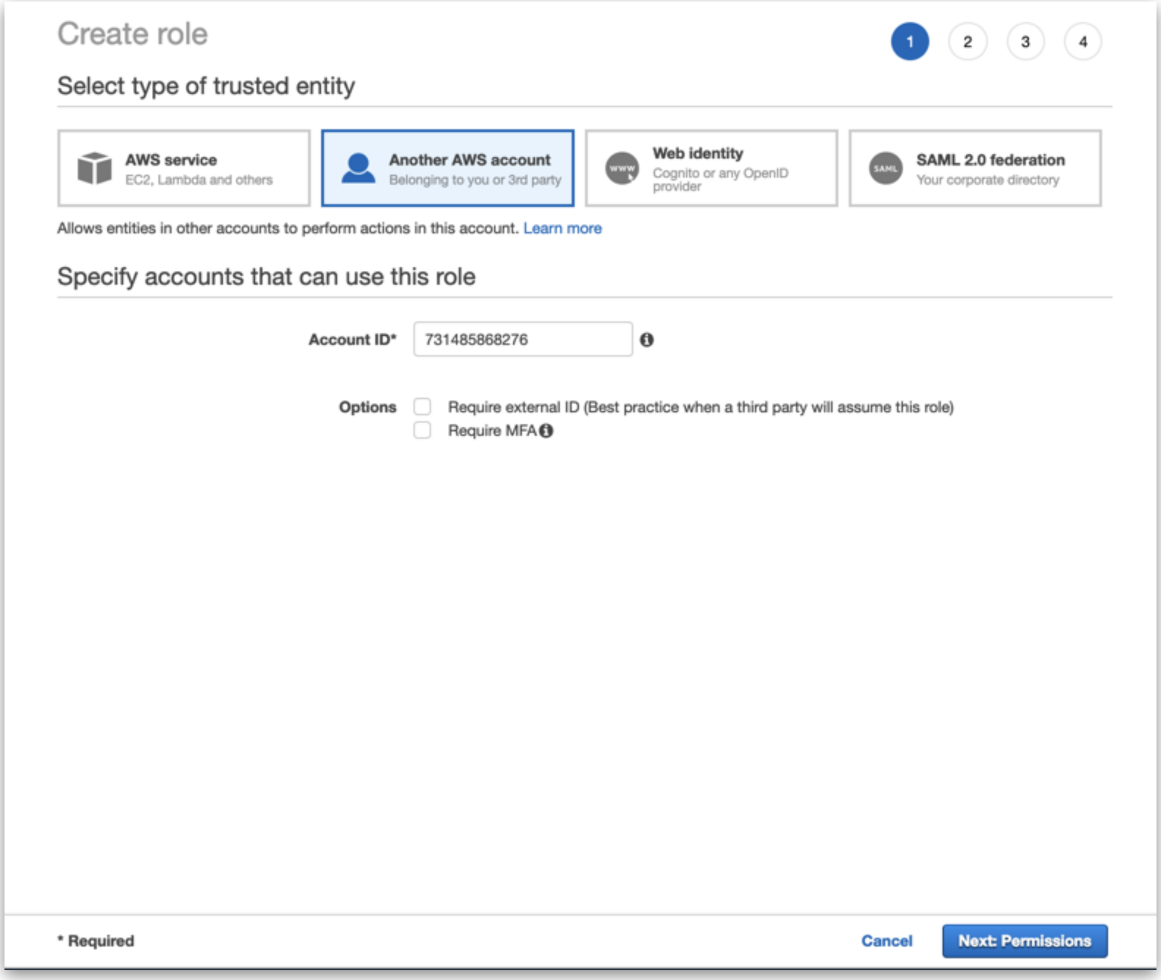
The new user will receive the following tag

Key	Value
Name	splunk-avanan-user

- ***Download the CSV or copy the Access Key and Secret access key somewhere safe. This information won't be available again.**
- Close.

Step-11:

- Click on Roles and on “Create role”
- Select Another AWS Account
- Insert the 12 digit number of the user you just created click on “Next: Permissions”



Create role

Select type of trusted entity

Another AWS account
Belonging to you or 3rd party

Allows entities in other accounts to perform actions in this account. Learn more

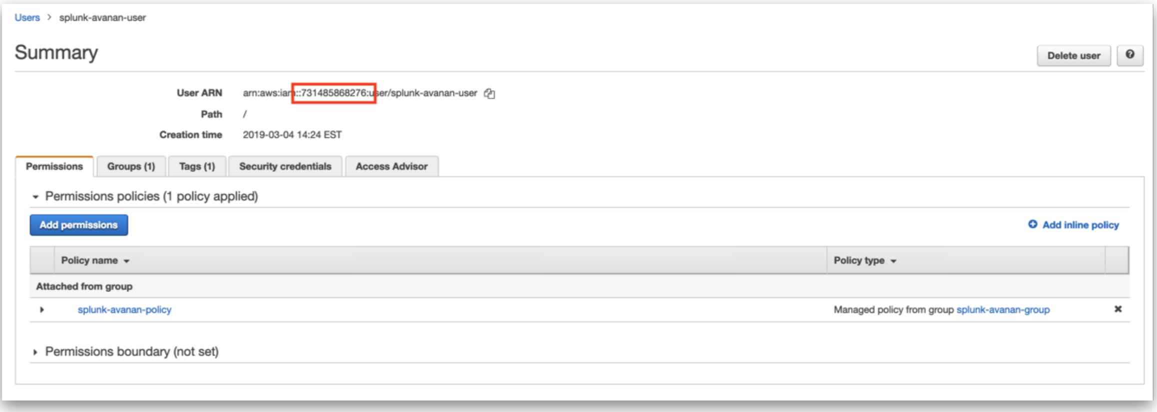
Specify accounts that can use this role

Account ID* 731485868276

Options
□ Require external ID (Best practice when a third party will assume this role)
□ Require MFA

* Required

- Note: to find the 12 digit number, open the user on another screen:



Users > splunk-avanan-user

Summary

User ARN arn:aws:iam::731485868276:user/splunk-avanan-user

Path /

Creation time 2019-03-04 14:24 EST

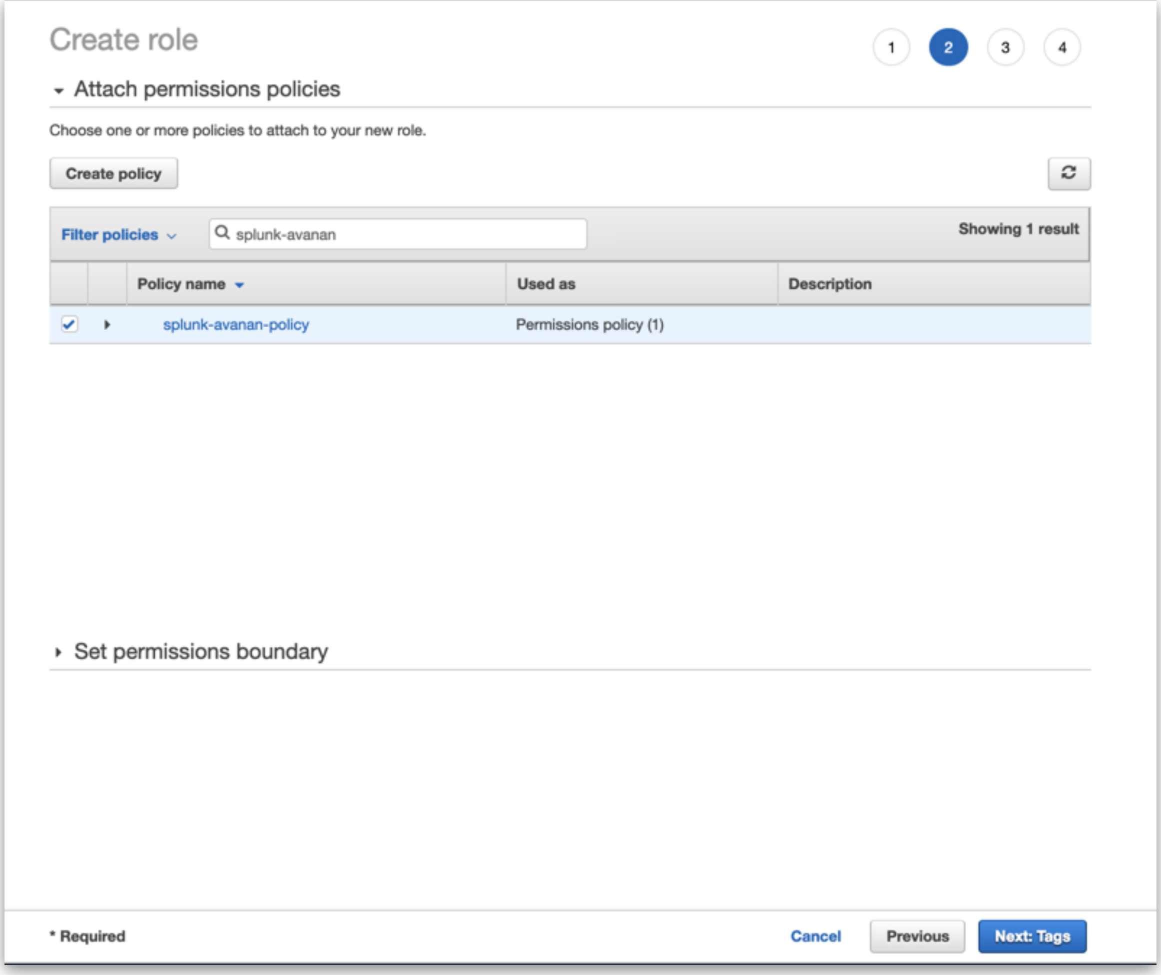
Permissions policies (1 policy applied)

Policy name	Policy type
Attached from group	
splunk-avanan-policy	Managed policy from group splunk-avanan-group

Permissions boundary (not set)

Step-12:

- Select the policy you created, click on Next: Tags



Create role

Attach permissions policies

Choose one or more policies to attach to your new role.

splunk-avanan

Showing 1 result

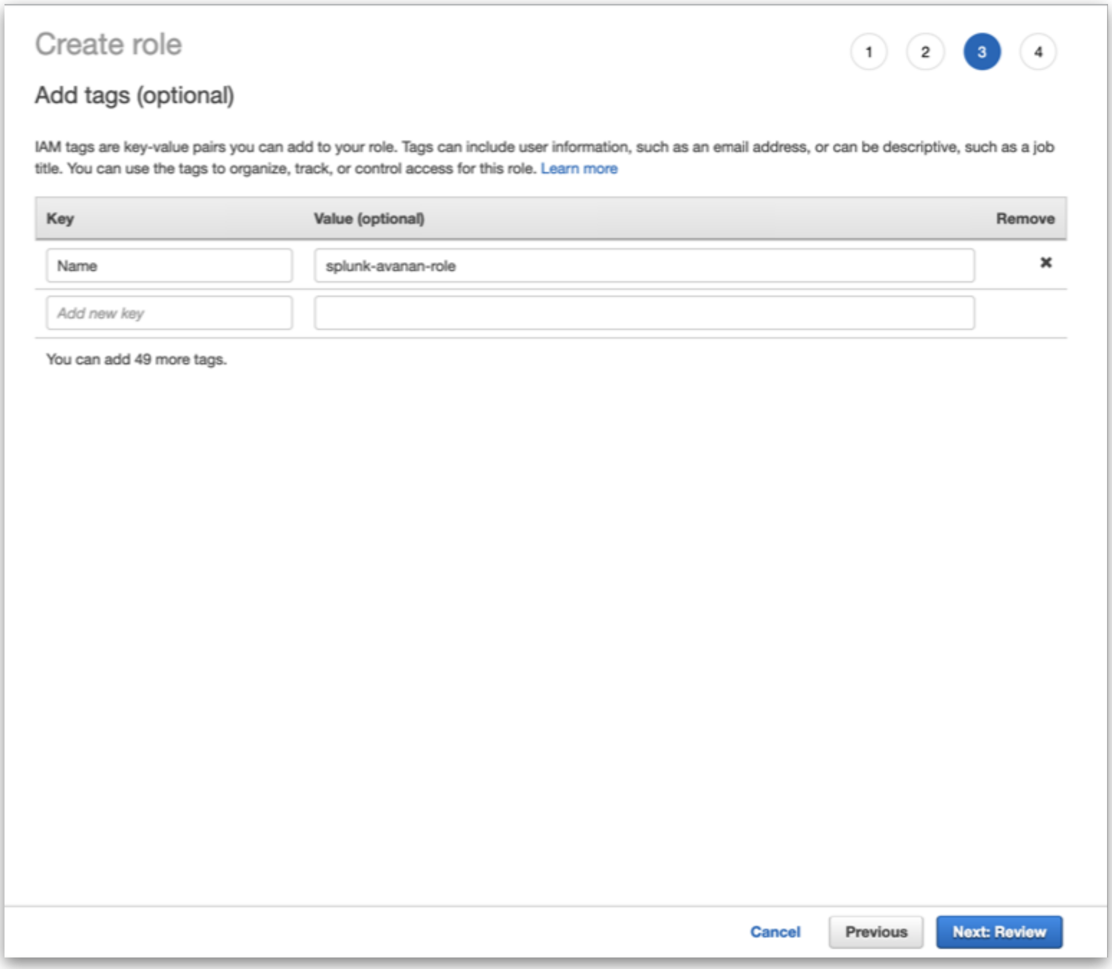
		Policy name	Used as	Description
☑	▸	splunk-avanan-policy	Permissions policy (1)	

Set permissions boundary

* Required

Step-13:

- Add the necessary Tags (in accordance with your environment directives) and click on Next: Review



Create role

Add tags (optional)

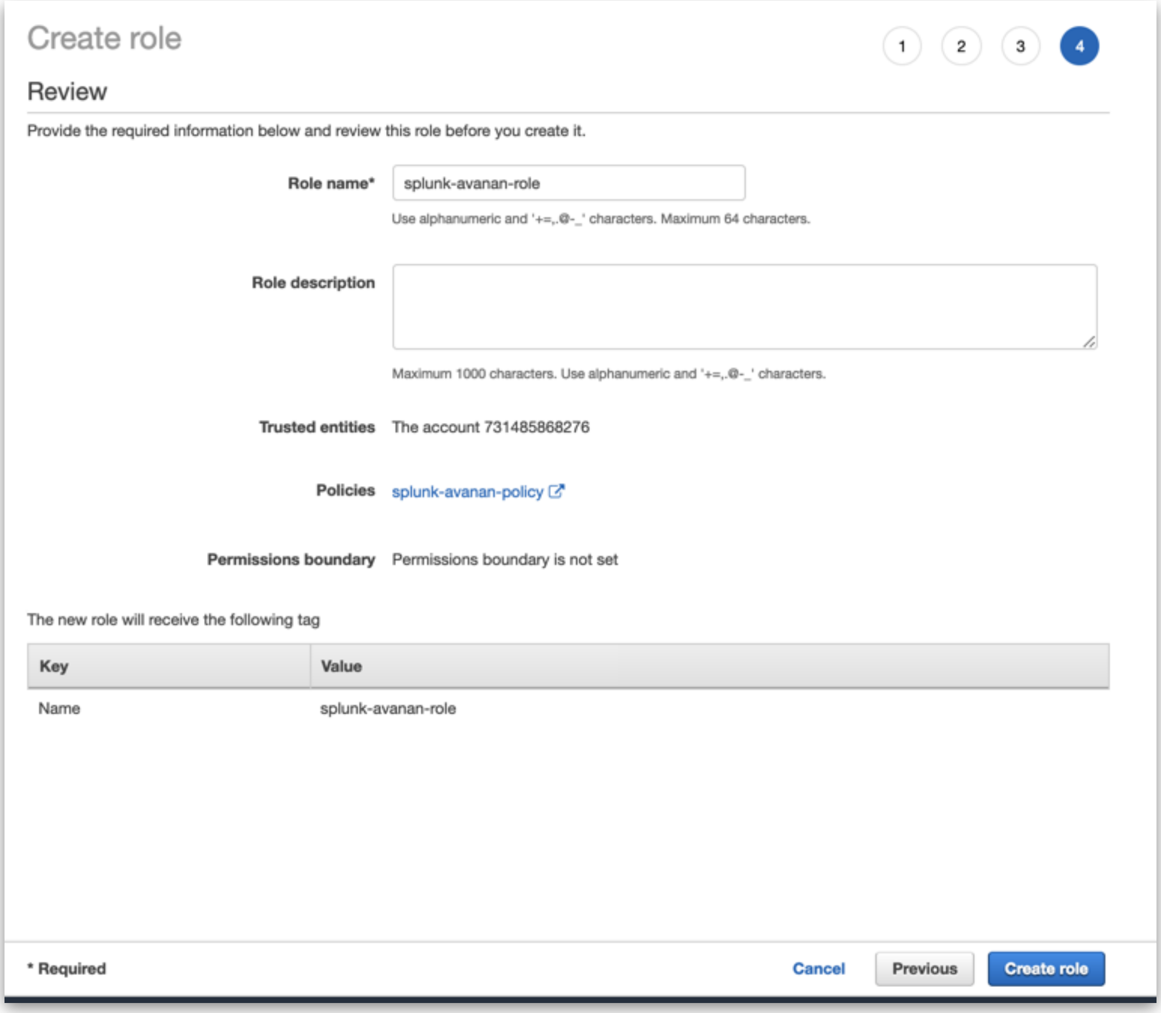
IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. Learn more

Key	Value (optional)	Remove
Name	splunk-avanan-role	✖
Add new key		

You can add 49 more tags.

Step-14:

- Select a role name and click on Create Role



Review

Provide the required information below and review this role before you create it.

Role name* splunk-avanan-role

Use alphanumeric and '+=,.@-_' characters. Maximum 64 characters.

Role description

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Trusted entities The account 731485868276

Policies splunk-avanan-policy

Permissions boundary Permissions boundary is not set

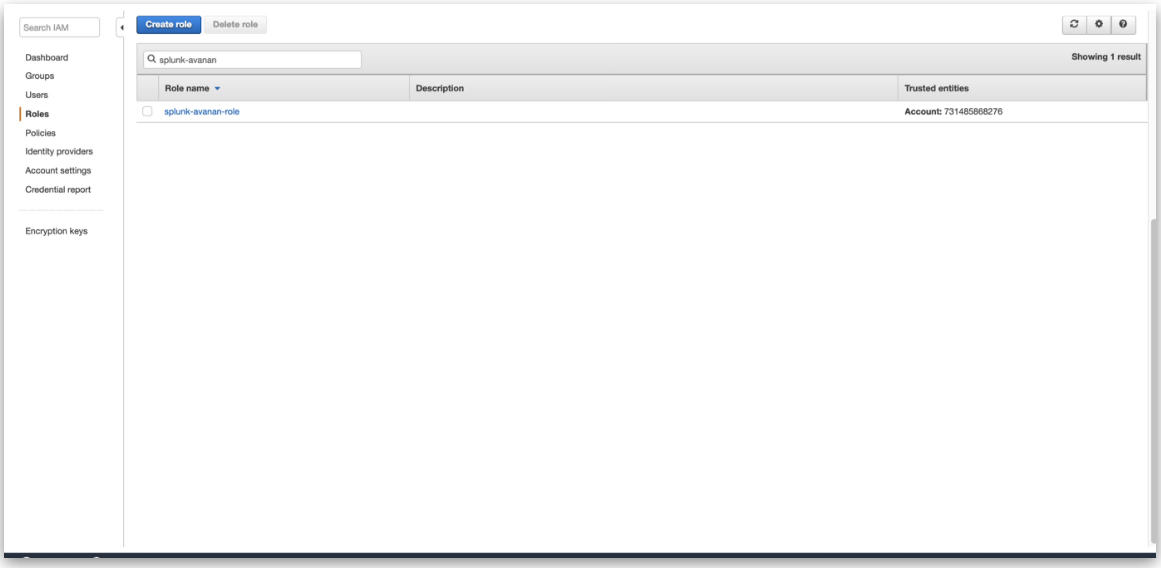
The new role will receive the following tag

Key	Value
Name	splunk-avanan-role

* Required

Step-15:

- Search for the role you just created, click on its name.



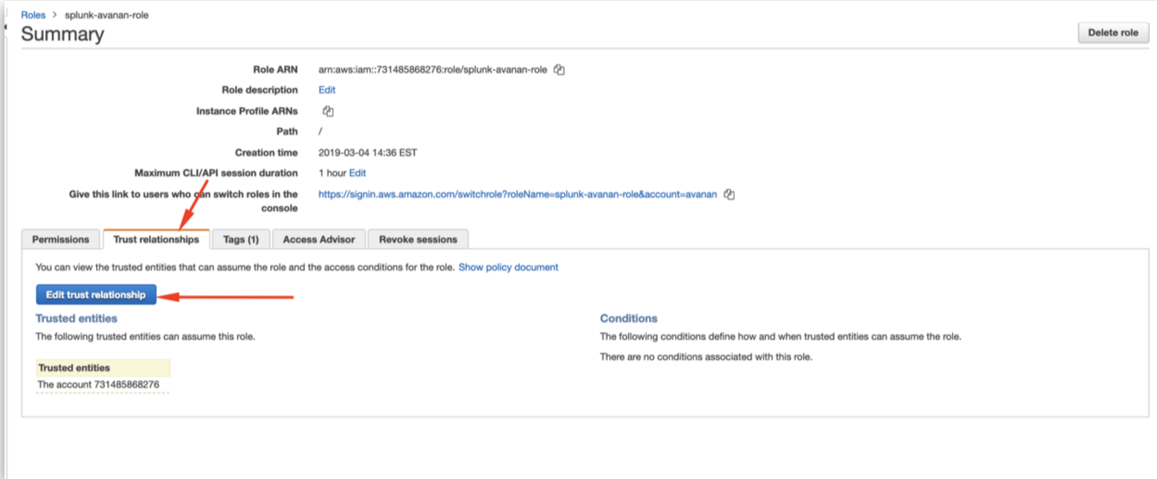
splunk-avanan

Showing 1 result

	Role name	Description	Trusted entities
□	splunk-avanan-role		Account: 731485868276

Step-16:

- Select “Trust relationships” and click on “Edit trust relationship”



Summary

Role ARN	arn:aws:iam::731485868276:role/splunk-avanan-role
Role description	Edit
Instance Profile ARNs	
Path	/
Creation time	2019-03-04 14:36 EST
Maximum CLI/API session duration	1 hour Edit
Give this link to users who can switch roles in the console	https://signin.aws.amazon.com/switchrole?roleName=splunk-avanan-role&account=avanan

You can view the trusted entities that can assume the role and the access conditions for the role. Show policy document

Trusted entities

The following trusted entities can assume this role.

Trusted entities
The account 731485868276

Conditions

The following conditions define how and when trusted entities can assume the role.

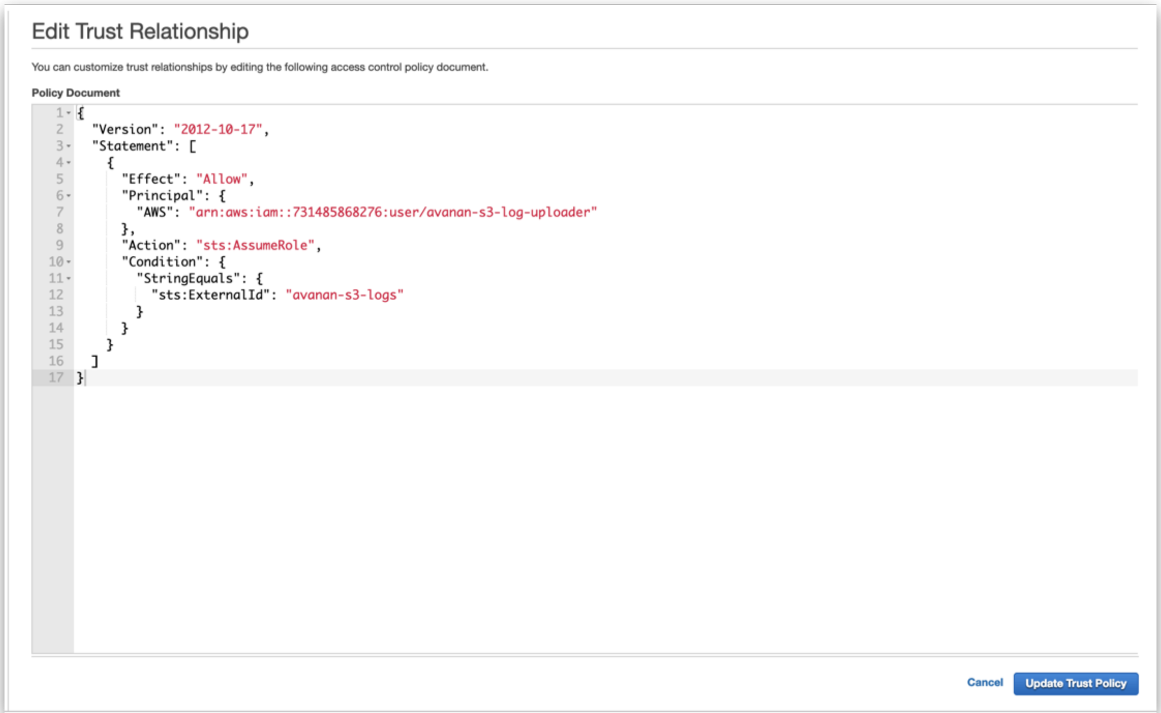
There are no conditions associated with this role.

Step-17:

- Copy the following over and click on “Update Trust Policy”

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::731485868276:user/avanan-s3-log-uploader"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "avanan-s3-logs"
        }
      }
    }
  ]
}
```

- For Example:



Edit Trust Relationship

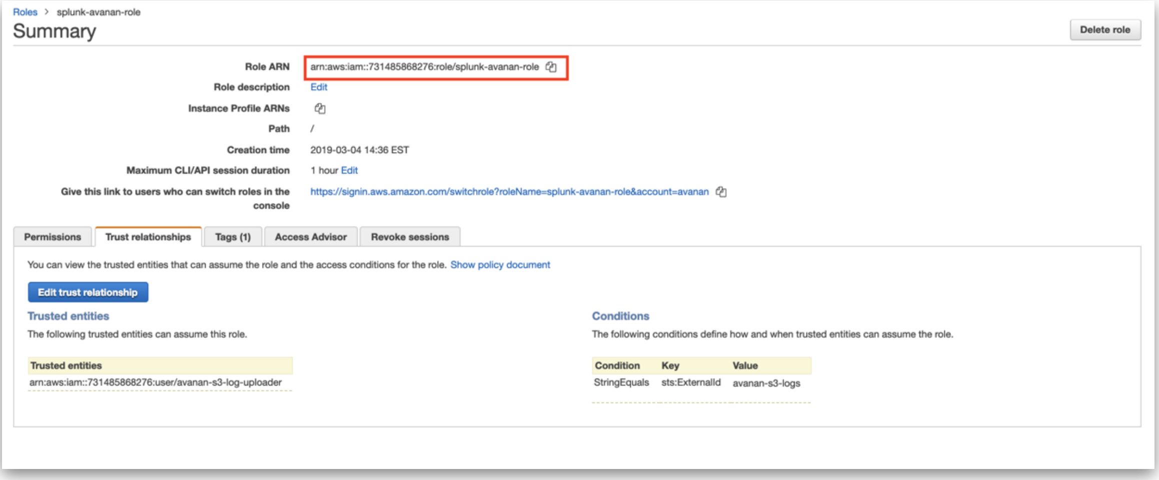
You can customize trust relationships by editing the following access control policy document.

Policy Document

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::731485868276:user/avanan-s3-log-uploader"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "avanan-s3-logs"
        }
      }
    }
  ]
}
```

Step-18:

- Copy the Role ARN to use on the Avanan side



Summary

Role ARN	arn:aws:iam::731485868276:role/splunk-avanan-role
Role description	Edit
Instance Profile ARNs	
Path	/
Creation time	2019-03-04 14:36 EST
Maximum CLI/API session duration	1 hour Edit
Give this link to users who can switch roles in the console	https://signin.aws.amazon.com/switchrole?roleName=splunk-avanan-role&account=avanan

You can view the trusted entities that can assume the role and the access conditions for the role. Show policy document

Trusted entities

The following trusted entities can assume this role.

Trusted entities
arn:aws:iam::731485868276:user/avanan-s3-log-uploader

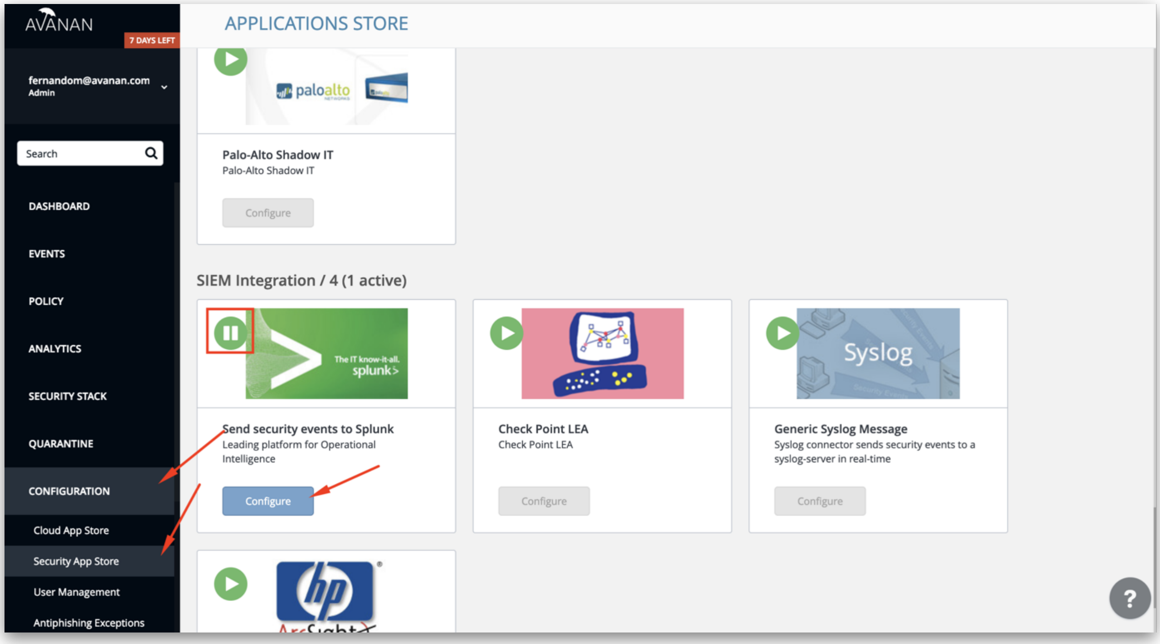
Conditions

The following conditions define how and when trusted entities can assume the role.

Condition	Key	Value
StringEquals	sts:ExternalId	avanan-s3-logs

Step-19:

- Back on Avanan, go to Configuration > Security App Store.
- Find Splunk on the list and click on Configure (if the button is grey out, the module is not enabled, click on the round "PLAY" button to enable it and refresh the page)



Palo-Alto Shadow IT
Palo-Alto Shadow IT

SIEM Integration / 4 (1 active)

Send security events to Splunk
Leading platform for Operational Intelligence

Check Point LEA
Check Point LEA

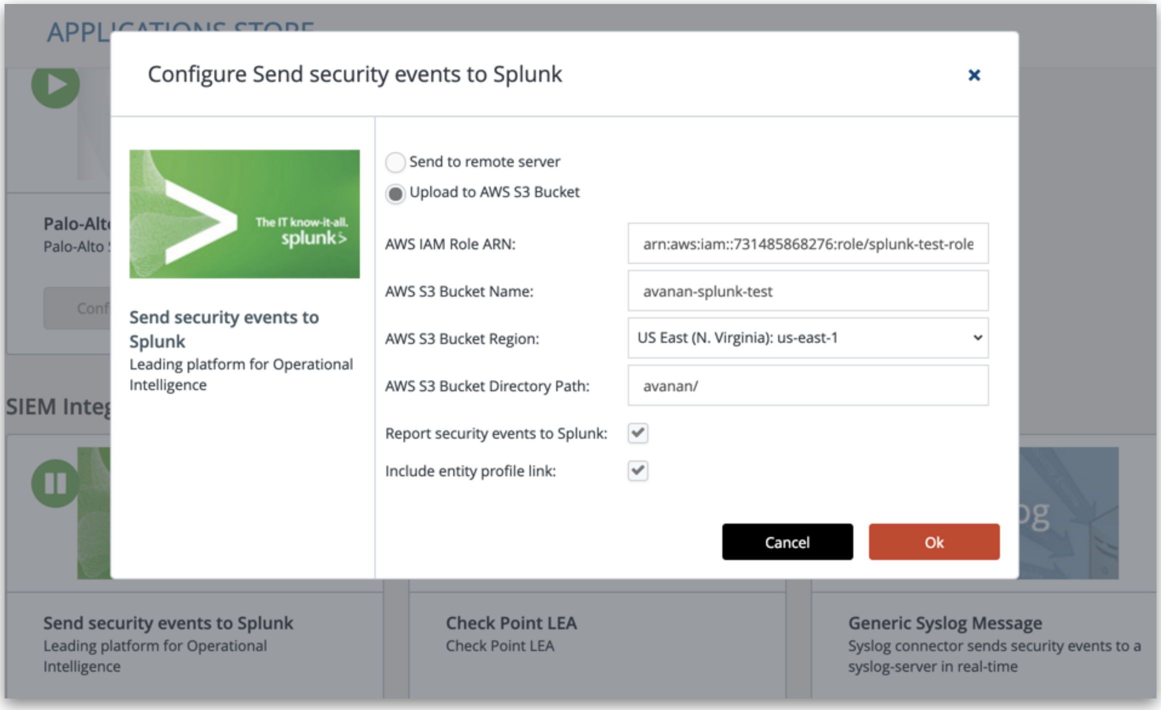
Generic Syslog Message
Syslog connector sends security events to a syslog-server in real-time

Step-20:

- Copy your Role ARN, bucket name, and select a region. Insert the subfolder you want the logs to be uploaded to, if any (they will be uploaded to the root directory if left empty).

  > Select "Report security events to Splunk" if you want all new security events to be uploaded (recommended).

  > Select "Include entity profile link" if you want to add a link to the entity profile on Avanan to the JSON logs.



Configure Send security events to Splunk

Send security events to Splunk

Leading platform for Operational Intelligence

○ Send to remote server

● Upload to AWS S3 Bucket

AWS IAM Role ARN: arn:aws:iam::731485868276:role/splunk-test-role

AWS S3 Bucket Name: avanan-splunk-test

AWS S3 Bucket Region: US East (N. Virginia): us-east-1

AWS S3 Bucket Directory Path: avanan/

Report security events to Splunk: ☑

Include entity profile link: ☑

×
The IT know-it-all.
splunk>
Cancel
Ok
APPLICATIONS STORE
Palo-Alto
SIEM Integ
Send security events to Splunk
Leading platform for Operational Intelligence
Check Point LEA
Check Point LEA
Generic Syslog Message
Syslog connector sends security events to a syslog-server in real-time

- Click on Ok to save. The Avanan-S3 side of the integration is done.