

Adding a user to an existing role

In the sub-account (ex: Su2c AWS account) create a new role, “For another AWS account” and then enter the Master VAI account ID (ex: 639677452477) to give access to. Choose the privileges (ex: [AdministratorAccess](#)) for the role and give it a name (ex: su2cadmin)

Search IAM

Roles > su2cadmin

Summary

Delete role

Role ARN: arn:aws:iam::197833163604:role/su2cadmin

Role description: this the the admin role for the su2c

Instance Profile ARNs

Path: /

Creation time: 2018-01-19 15:24 EST

Give this link to users who can switch roles in the console: <https://signin.aws.amazon.com/switchrole?roleName=su2cadmin&account=197833163604>

Permissions Trust relationships Access Advisor Revoke sessions

You can view the trusted entities that can assume the role and the access conditions for the role. [Show policy document](#)

Edit trust relationship

Trusted entities

The following trusted entities can assume this role.

Trusted entities

The account 639677452477

Conditions

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

There are no conditions associated with this role.

Now any admin user from the master VAI account can switch roles into the Su2c account admin role.

If we want to further limit access to SU2C within Master VAI to non-admins using policies and apply to a group

Create policy



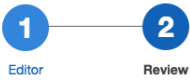
A policy defines the AWS permissions that can be assigned to a user, group, role, or resource. You can construct a policy using the visual editor or create a policy document using the JSON editor.

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](#)

Visual editor JSON Import managed policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "sts:AssumeRole",
7       "Resource": "arn:aws:iam::197833163604:role/su2cadmin"
8     }
9   ]
10 }
```

Create policy



Review policy

Before you create this policy, provide the required information and review this policy.

Name*

becomeSU2CAdmin

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

Description

this policy allows users to become an su2c admin

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

Summary

Filter

Service	Access level	Resource
Allow (1 of 128 services) Show remaining 127		
STS	Limited: Write	RoleName string like su2cadmin

aws

Services

Resource Groups

awszackr @ 6396-7745-2477

Global

Support

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

IAM > Groups > VAI_SU2C_admins

Summary

Group ARN:

arn:aws:iam::639677452477:group/VAI_SU2C_admins

Users (in this group):

3

Path:

/

Creation Time:

2018-01-22 11:08 EST

Users

Permissions

Access Advisor

Managed Policies

The following managed policies are attached to this group. You can attach up to 10 managed policies.

Attach Policy

Policy Name	Actions
becomeSU2CAdmin	Show Policy Detach Policy Simulate Policy

Inline Policies

Then add users to the group who can access this external role:

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

[IAM](#) > [Groups](#) > [VAI_SU2C_admins](#)

Summary

Group ARN:

arn:aws:iam::639677452477:group/VAI_SU2C_admins

Users (in this group):

3

Path:

/

Creation Time:

2018-01-22 11:08 EST

Users




Permissions

Access Advisor

This view shows all users in this group: 3 Users

Remove Users from Group

Add Users to Group

User	Actions
 awszackr	Remove User from Group
 awsjasonk	Remove User from Group
 awsanthonyw	Remove User from Group