

Task 3: ECS Exec Role

The image shows two screenshots of the AWS IAM console. The top screenshot displays the 'ecs:ListAccountSettings' policy details. The policy description states: 'Grants permission to list the account settings for an Amazon ECS resource for a specified principal'. The 'Access level' section shows 'List (7 selected)' and 'Read (2 selected)' permissions. The 'Manual actions' section lists various actions, with 'DescribeServices', 'DescribeTaskSets', 'DescribeTaskDefinition', 'DescribeTasks', 'ListAccountSettings', and 'ListTagsForResource' being selected. The bottom screenshot shows the 'Select trusted entity' step in the 'Create role' wizard. The 'Trusted entity type' section has 'AWS service' selected. The 'Use case' section has 'Elastic Container Service' selected. The bottom of the image shows a macOS dock with various application icons.

Policy Details: ecs:ListAccountSettings

Description: Grants permission to list the account settings for an Amazon ECS resource for a specified principal. [Learn more](#)

Access level: List (7 selected), Read (2 selected)

Manual actions (add actions):

- ☐ All Elastic Container Service actions (ecs:*)

Access level: List (7 selected), Read (2 selected)

Manual actions (add actions):

- ☐ DescribeCapacityProviders
- ☒ DescribeServices
- ☒ DescribeTaskSets
- ☐ DescribeClusters
- ☐ DescribeTaskDefinition
- ☐ ListAccountSettings
- ☐ DescribeContainerInstances
- ☐ DescribeTasks
- ☐ ListTagsForResource

Tagging:

- ☐ TagResource
- ☐ UntagResource

Write:

- ☐ CreateCapacityProvider
- ☐ DiscoverPollEndpoint
- ☐ StopTask
- ☐ CreateCluster
- ☐ ExecuteCommand
- ☐ SubmitAttachmentStateChanges
- ☐ CreateService
- ☐ Poll
- ☐ SubmitContainerStateChange
- ☐ CreateTaskSet
- ☐ PutAccountSetting
- ☐ SubmitTaskStateChange
- ☐ DeleteAccountSetting
- ☐ PutAccountSettingDefault
- ☐ UpdateCapacityProvider
- ☐ DeleteAttributes
- ☐ PutAttributes
- ☐ UpdateCluster
- ☐ DeleteCapacityProvider
- ☐ PutClusterCapacityProviders
- ☐ UpdateClusterSettings

Trusted entity type:

- ☒ AWS service: Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ☐ AWS account: Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ☐ Web identity: Allow users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ☐ SAML 2.0 federation: Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ☐ Custom trust policy: Create a custom trust policy to enable others to perform actions in this account.

Use case: Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases:

- ☐ EC2: Allows EC2 instances to call AWS services on your behalf.
- ☐ Lambda: Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:

Elastic Container Service

Chrome File Edit View History Bookmarks Profiles Tab Window Help

Amazon Web Services (AWS) x IAM Management Console x IAM Management Console x Amazon ECS components - Amazon x IAM roles for tasks - Amazon x

us-east-1.console.aws.amazon.com/iamv2/home?region=us-west-2#/roles/create?step=selectEntities

Services Search for services, features, blogs, docs, and more [Option+S]

Global developers/asingh4@nrel.gov

☐ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases

☐ EC2
Allows EC2 instances to call AWS services on your behalf.

☐ Lambda
Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:

Elastic Container Service

☒ Elastic Container Service
Allows ECS to create and manage AWS resources on your behalf.

☐ Elastic Container Service Autoscale
Allows Auto Scaling to access and update ECS services.

☐ Elastic Container Service Task
Allows ECS tasks to call AWS services on your behalf.

☐ EC2 Role for Elastic Container Service
Allows EC2 instances in an ECS cluster to access ECS.

Cancel Next

Feedback Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Chrome File Edit View History Bookmarks Profiles Tab Window Help

Amazon Web Services (AWS) x IAM Management Console x IAM Management Console x Amazon ECS components - Amazon x IAM roles for tasks - Amazon x

us-east-1.console.aws.amazon.com/iamv2/home?region=us-west-2#/roles/create?selectedService=EC2ContainerService&selectedUseCase=EC2ContainerSer...

Services Search for services, features, blogs, docs, and more [Option+S]

Global developers/asingh4@nrel.gov

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
ECSExecSpecificRole
Maximum 64 characters. Use alphanumeric and '+', '=', '@', '-' characters.

Description
Add a short explanation for this role.
Allows ECS to create and manage AWS resources on your behalf.
Maximum 1000 characters. Use alphanumeric and '+', '=', '@', '-' characters.

Step 1: Select trusted entities

Edit

```
1- {  
2-   "Version": "2008-10-17",  
3-   "Statement": [  
4-     {  
5-       "Sid": "",  
6-       "Effect": "Allow",  
7-       "Principal": {  
8-         "Service": "ecs.amazonaws.com"  
9-       },  
10-    ]  
11- }
```

Chrome File Edit View History Bookmarks Profiles Tab Window Help

Amazon Web Services (AWS) x IAM Management Console x IAM Management Console x Amazon ECS components - Amazon x IAM roles for tasks - Amazon x

us-east-1.console.aws.amazon.com/iamv2/home?region=us-west-2#/roles/details/ECSExecSpecificRole?section=permissions

Services Search for services, features, blogs, docs, and more [Option+S]

Global developers/asingh4@nrel.gov

Identity and Access Management (IAM)

Unable to load search
Dashboard

▼ Access management

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings

▼ Access reports

- Access analyzer
- Archive rules
- Analizers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

ECSExecSpecificRole

Allows ECS to create and manage AWS resources on your behalf.

Summary

Creation date: October 14, 2022, 09:35 (UTC-05:00)
Last activity: None

ARN: `arn:aws:iam::246460460343:role/ECSExecSpecificRole`
Maximum session duration: 1 hour

Permissions Trust relationships Tags Access Advisor Revoke sessions

Permissions policies (1) Info

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter.

Policy name	Type	Description
<input type="checkbox"/> AmazonEC2ContainerServiceRole	AWS managed	Default policy for Amazon ECS service role.

https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-west-2#

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Chrome File Edit View History Bookmarks Profiles Tab Window Help

Amazon Web Services (AWS) x IAM Management Console x IAM Management Console x IAM Management Console x Amazon ECS components - Amazon x IAM roles for tasks - Amazon x

us-east-1.console.aws.amazon.com/iam/home#/policies/new?step=edit

Services Search for services, features, blogs, docs, and more [Option+S]

Global developers/asingh4@nrel.gov

Documentation

Service Elastic Container Service

Actions Specify the actions allowed in Elastic Container Service

Filter actions

Manual actions (add actions)

☐ All Elastic Container Service actions (ecs:*)

Access level

Expand all Collapse all

☒ List (7 selected)

- ☒ ListAttributes
- ☒ ListClusters
- ☒ ListContainerInstances
- ☒ ListServices
- ☒ ListTaskDefinitionFamilies
- ☒ ListTaskDefinitions
- ☒ ListTasks

☒ Read (9 selected)

- ☒ DescribeCapacityProviders
- ☒ DescribeClusters
- ☒ DescribeContainerInstances
- ☒ DescribeServices
- ☒ DescribeTaskDefinition
- ☒ DescribeTasks
- ☒ DescribeTaskSets
- ☒ ListAccountSettings
- ☒ ListTagsForResource

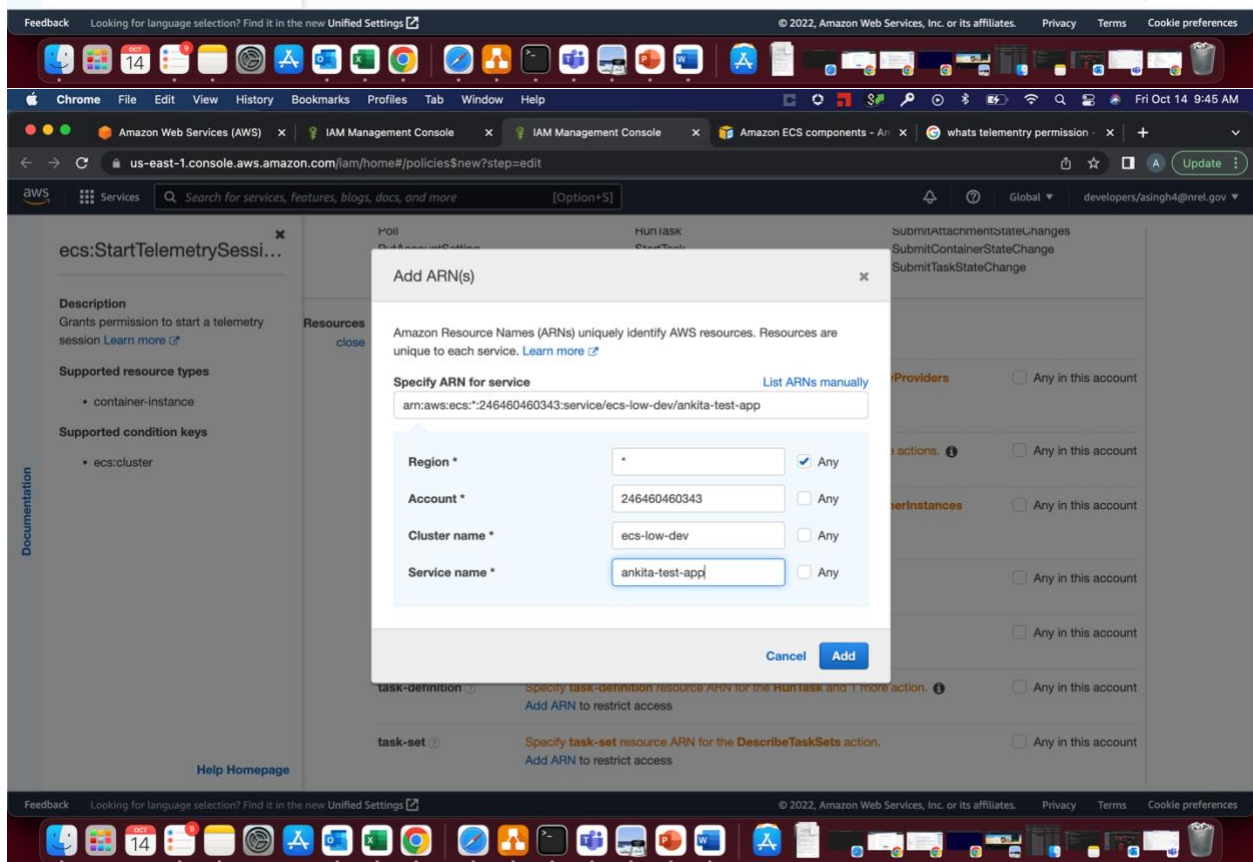
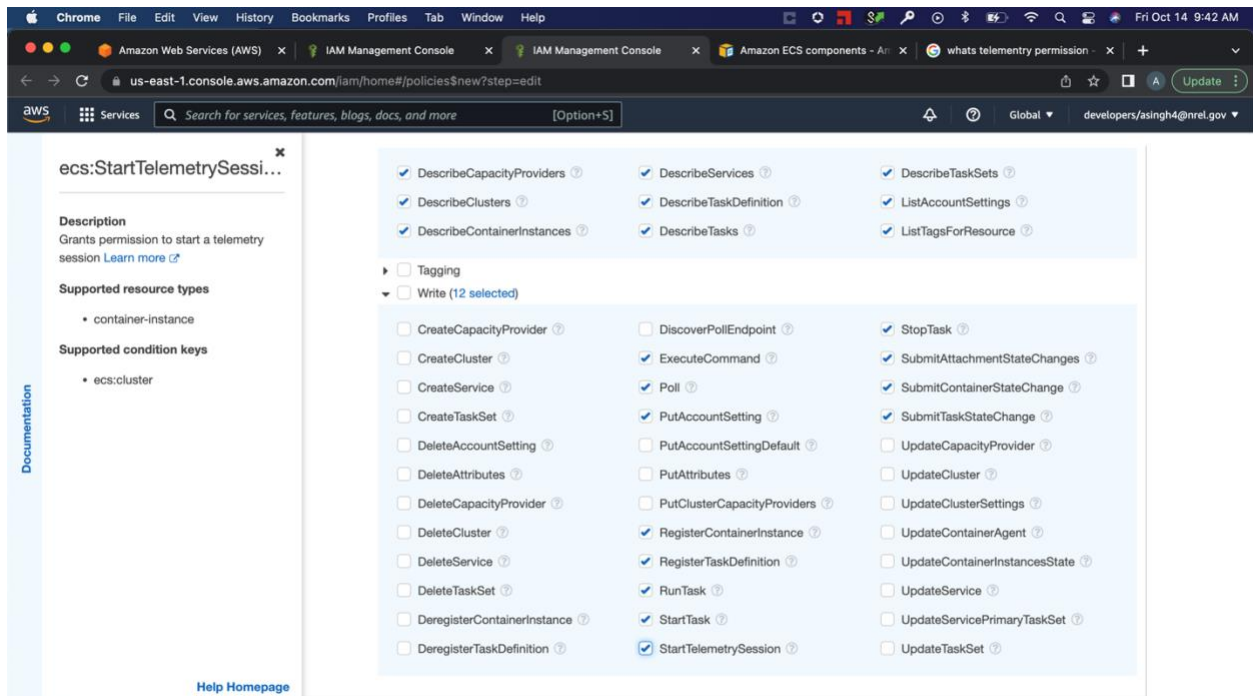
☐ Tagging

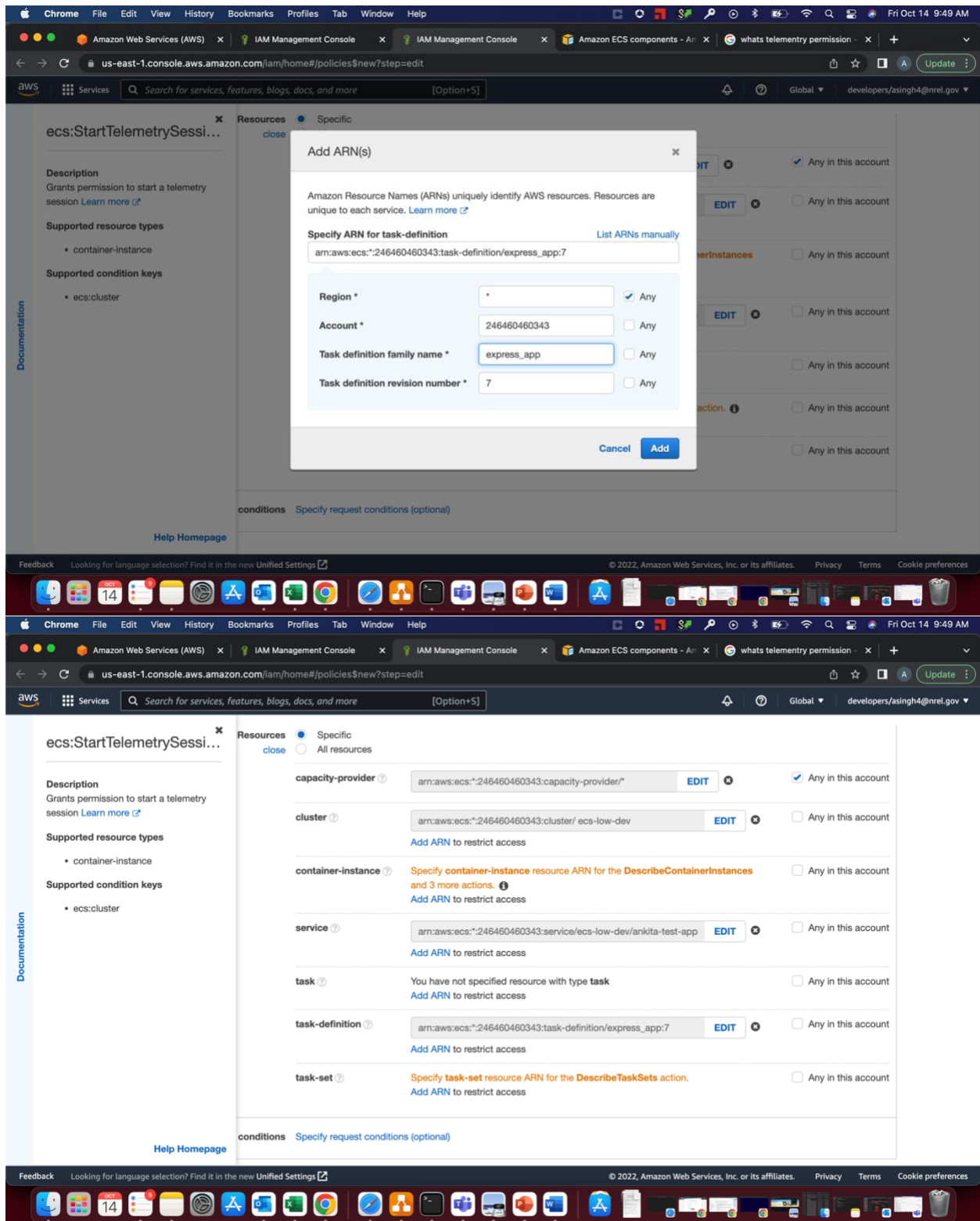
☐ Write (9 selected)

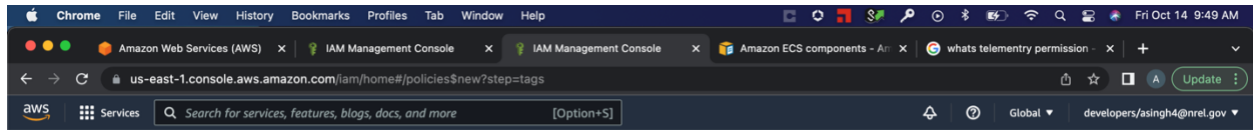
- ☐ CreateCapacityProvider
- ☐ DiscoverPollEndpoint
- ☒ StopTask

Feedback Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences







Create policy

1 2 3

Add tags - optional

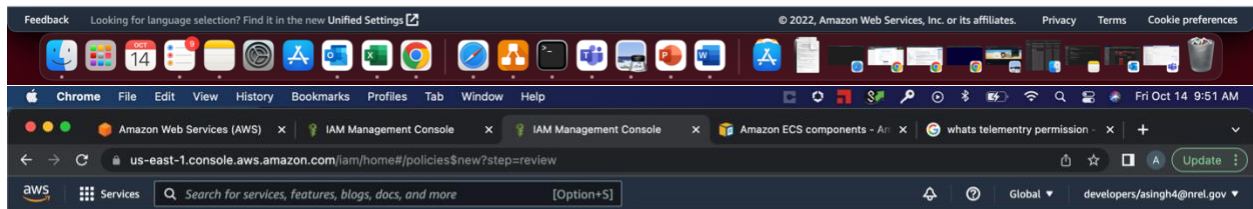
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add tag

You can add up to 50 more tags.

Cancel Previous Next: Review



Create policy

1 2 3

Review policy

Name* Anki_ECSExecSpecificPermission

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

Description Creating a specific policy to access ECS service with limited actions for the user

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

Summary

Filter			
Service	Access level	Resource	Request condition
Allow (1 of 335 services) Show remaining 334			
Elastic Container Service	Limited: List, Read, Write	Multiple	None

Tags

Key	Value
-----	-------

No tags associated with the resource.

