

Instalação de agente de segurança com SystemManager AWS

Criar IAM role SSMtoSNS com a Policy : AWSSNSFullAccess

Selecione SystemManager

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

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

Access reports

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

Step 2

Add permissions

Step 3

Name, review, and create

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

Allows 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.

Search system

Systems Manager

Choose a service to view use case

Cancel

Next

Procure por SystemManager e Next

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

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

Access reports

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

Step 2

Add permissions

Step 3

Name, review, and create

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

Allows 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:

Systems Manager

☒ Systems Manager

Allows SSM to call AWS services on your behalf

☐ Systems Manager - Inventory and Maintenance Windows

Allow AWS Systems Manager to call AWS resources on your behalf.

Procure a role AmazonSNSFullAccess e selecione

Identity and Access Management (IAM)

Search IAM

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)

Step 2Add permissions

Step 3Name, review, and create

Permissions policies (Selected 1/772)

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

Filter policies by property or policy name and press enter

5 matches

sns

Clear filters

	Policy name	Type	Description
<input type="checkbox"/>	AmazonSNSReadOnlyAccess	AWS m...	Provides read only access to Amazon SNS via the AWS Manageme...
<input type="checkbox"/>	AmazonSNSRole	AWS m...	Default policy for Amazon SNS service role.
<input checked="" type="checkbox"/>	AmazonSNSFullAccess	AWS m...	Provides full access to Amazon SNS via the AWS Management Con...
<input type="checkbox"/>	AWSIoTDeviceDefenderPublishFindingsT...	AWS m...	Provides messages publish access to SNS topic for execution of PU...
<input type="checkbox"/>	AWSElasticBeanstalkRoleSNS	AWS m...	(Elastic Beanstalk operations role) Allows an environment to enable ...

Set permissions boundary - optional

Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

Cancel

Previous

Next

De nome a sua role “sujestão” SSMtoSNS e clique em Create role

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

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

Access reports

- Access analyzer
 - Archive rules
- Analizers
- Settings
- Credential report

IAM > Roles > Create role

Step 1Select trusted entity

Step 2Add permissions

Step 3Name, review, and create

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

SSMtoSNS

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

Description

Add a short explanation for this policy.

Allows SSM to call AWS services on your behalf

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

Step 1: Select trusted entities

Edit

Confira e seguimos para criar um tópico de notificação

Identity and Access Management (IAM)

Search IAM

Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)

SSMtoSNS

Allows SSM to call AWS services on your behalf

Summary

Creation date

May 05, 2022, 15:24 (UTC-03:00)

Last activity

None

ARN

arn:aws:iam::721859630063:role/SSMtoSNS

Maximum session duration

1 hour

Permissions

Trust relationships

Tags

Access Advisor

Revoke sessions

Permissions policies (1)

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter

Policy name

Type

Description

AmazonSNSFullAccess

AWS managed

Provides full access to Amazon SNS via the AWS Management Console.

Acesse pagina do AWS Simple Notification Service

Crie um novo tópico após crie uma nova subscription escolha a opção de e-mail para receber as notificações e insira seu email após criada a sub confirme a inscrição no seu e-mail e salve a arn do tópico

Amazon SNS

×

Dashboard

Topics

Subscriptions

▼ Mobile

Push notifications

Text messaging (SMS)

Origination numbers

Amazon SNS > Topics

Topics (0)

EditDeletePublish messageCreate topic

🔍 Search

< 1 > ⓘ

Name▲	Type▼	ARN▼
No topics To get started, create a topic. Create topic		

De nome ao tópico e clique em Create topic e salve a arn: do tópico

Amazon SNS

×

Dashboard

Topics

Subscriptions

▼ Mobile

Push notifications

Text messaging (SMS)

Origination numbers

Amazon SNS > Topics > Create topic

Create topic

Details

Type

Info

Topic type cannot be modified after topic is created

☐ FIFO (first-in, first-out)

- Strictly-preserved message ordering
- Exactly-once message delivery
- High throughput, up to 300 publishes/second
- Subscription protocols: SQS

☒ Standard

- Best-effort message ordering
- At-least once message delivery
- Highest throughput in publishes/second
- Subscription protocols: SQS, Lambda, HTTP, SMS, email, mobile application endpoints

Name

NotificationSNS

Maximum 256 characters. Can include alphanumeric characters, hyphens (-) and underscores (_).

Display name - optional

To use this topic with SMS subscriptions, enter a display name. Only the first 10 characters are displayed in an SMS message. Info

My Topic

Maximum 100 characters.

Agora vamos criar subscription

Amazon SNS

×

Dashboard

Topics

Subscriptions

▼ Mobile

Push notifications

Text messaging (SMS)

Origination numbers

Amazon SNS > Topics > NotificationSNS

NotificationSNS

EditDeletePublish message

Details

Name

NotificationSNS

Display name

-

ARN

arn:aws:sns:sa-east-1:721859630063:NotificationSNS

Topic owner

721859630063

Type

Standard

Subscriptions

Access policy

Delivery retry policy (HTTP/S)

Delivery status logging

Encryption

Tags

Subscriptions (0)

EditDeleteRequest confirmationConfirm subscriptionCreate subscription

Selecione email e insira seu email

Amazon SNS

×

Dashboard

Topics

Subscriptions

▼ Mobile

Push notifications

Text messaging (SMS)

Origination numbers

Create subscription

Details

Topic ARN

Qarn:aws:sns:sa-east-1:721859630063:NotificationSNSX

Protocol

The type of endpoint to subscribe

Email▼

Endpoint

An email address that can receive notifications from Amazon SNS.

att@wefixit.inf.br

Acesse seu email e confirme a inscrição

Amazon SNS

×

Dashboard

Topics

Subscriptions

▼ Mobile

Push notifications

Text messaging (SMS)

Origination numbers

Details

Name

NotificationSNS

ARN

arn:aws:sns:sa-east-1:721859630063:NotificationSNS

Type

Standard

Display name

-

Topic owner

721859630063

Subscriptions

Access policy

Delivery retry policy (HTTP/S)

Delivery status logging

Encryption

Tags

Subscriptions (1)

Edit

Delete

Request confirmation

Confirm subscription

Create subscription

QSearch

<1>⚙

	ID	Endpoint	Status	Protocol
<input type="radio"/>	Pending confirmation	att@wefixit.inf.br	⌚ Pending confirmation	EMAIL

Após confirmar seu email e verificar o status deve estar confirmado

Amazon SNS

×

Dashboard

Topics

Subscriptions

▼ Mobile

Push notifications

Text messaging (SMS)

Origination numbers

Details

Name

NotificationSNS

ARN

arn:aws:sns:sa-east-1:721859630063:NotificationSNS

Type

Standard

Display name

-

Topic owner

721859630063

Subscriptions

Access policy

Delivery retry policy (HTTP/S)

Delivery status logging

Encryption

Tags

Subscriptions (1)

Edit

Delete

Request confirmation

Confirm subscription

Create subscription

QSearch

<1>⚙

	ID	Endpoint	Status	Protocol
<input type="radio"/>	9ea5380d-0d8f-4afa-8ddb-d8fa800cc0b5	att@wefixit.inf.br	✅ Confirmed	EMAIL

Acesse pagina do AWS SystemManager quick setup e clique em Get Started

AWS Systems Manager

Quick Setup

▼ Operations Management

Explorer

OpsCenter

CloudWatch Dashboard

Incident Manager

▼ Application Management

Application Manager

AppConfig

Parameter Store

▼ Change Management

Change Manager

Automation

Change Calendar

Maintenance Windows

▼ Node Management

MANAGEMENT TOOLS

AWS Systems Manager

Gain Operational Insight and Take Action on AWS Resources.

Get Started with Systems Manager

View operational data for groups of resources, so you can quickly identify and act on any issues that might impact applications that use those resources.

How it works

More resources

[Documentation](#)

[API reference](#)

[FAQs](#)

Selecione Host Management e clique em Create

AWS Systems Manager

Quick Setup

▼ Operations Management

Explorer

OpsCenter

CloudWatch Dashboard

Incident Manager

▼ Application Management

Application Manager

AppConfig

Parameter Store

▼ Change Management

Change Manager

Automation

Change Calendar

Quick Setup

Library | Configurations

Configuration types

Filter below results

Host Management

Powered by Systems Manager

Configuration status

1 configured

Description

Configures IAM roles and enables commonly used Systems Manager capabilities to securely manage your Amazon EC2 instances.

Create | View 1 configuration

Config Recording

Powered by AWS Config

Configuration status

No configurations

Description

Enables the tracking and recording of changes to the AWS resource types you choose. Configures delivery and notifications options for the recorded data.

Create

Conformance Packs

Powered by AWS Config

Configuration status

No configurations

Description

Deploys conformance packs provided by AWS Config. Conformance packs are collections of AWS Config rules and remediation actions that can be deployed as a single entity.

Create

Mantenha as opções selecionadas

AWS Systems Manager

Quick Setup

▼ Operations Management

▼ Application Management

▼ Change Management

Explorer

OpsCenter

CloudWatch Dashboard

Incident Manager

Application Manager

AppConfig

Parameter Store

Change Manager

Automation

Change Calendar

Maintenance Windows

Systems Manager > Quick Setup > Create configuration

Customize Host Management configuration options

Configuration options

Quick Setup configures the following Systems Manager components based on best practices. Select the check boxes for actions you want to schedule. [Learn more](#)

Systems Manager

☒ Update Systems Manager (SSM) Agent every two weeks.

☒ Collect inventory from your instances every 30 minutes.

☒ Scan instances for missing patches daily.

Amazon CloudWatch

☐ Install and configure the CloudWatch agent.

☐ Update the CloudWatch agent once every 30 days.

If you run this configuration, [Systems Manager Explorer](#) is enabled.

Learn more about the metrics included in [the CloudWatch agent's basic configuration](#) and Amazon CloudWatch [pricing](#).

Abaixo em Targets marque Current account > Current Region > Manual e selecione as Instâncias criadas com Terraform e clique em Create pode levar de 5 a 10 para finalizar

AWS Systems Manager

Quick Setup

▼ Operations Management

▼ Application Management

▼ Change Management

Explorer

OpsCenter

CloudWatch Dashboard

Incident Manager

Application Manager

AppConfig

Parameter Store

Change Manager

Automation

Change Calendar

Maintenance Windows

Targets

Targets determine where this configuration is deployed.

Choose the accounts and Regions you want to deploy this configuration to.

☐ Entire organization

☐ Custom

☒ Current account

Deploys your configuration to all OUs and Regions in your organization.

Choose the OUs and Regions you want to deploy this configuration to.

Choose the Regions to deploy this configuration to within the currently signed in account.

Choose between deploying to the current Region or a custom set of Regions.

☒ Current Region

☐ Choose Regions

Deploy configuration to the current Region.

Choose the Regions you want to deploy this configuration to.

Choose how you want to target instances

☐ All instances

☐ Specify instance tag

☐ By Resource Group

☒ Manual

Deploy your configuration to all instances in the target account and Regions.

Specify a tag key-value pair to select instances that share that tag.

Specify a resource group. Only instances in that group will be configured.

Manually specify the instances you want to configure.

Instances

<input checked="" type="checkbox"/>	Name	Instance ID	Instance type	Instance state	Availability zone	IAM Instance profile name
<input checked="" type="checkbox"/>	webserver2	i-026dbdff130398bbb	t2.micro	running	sa-east-1a	-
<input checked="" type="checkbox"/>	webserver1	i-0a8c85c06a3e970bd	t2.micro	running	sa-east-1a	-

AWS Systems Manager

Quick Setup

▼ Operations Management

Explorer

OpsCenter

CloudWatch Dashboard

Incident Manager

▼ Application Management

Application Manager

AppConfig

Parameter Store

▼ Change Management

Change Manager

Automation

Change Calendar

Maintenance Windows

Filter by

► Regions

► Deployment status

► Association status

Configuration deployment status

The status of your configuration's deployment to its targets.

1

Total

Success

1

Failed

0

Pending

0

Configuration association status

The status of the State Manager associations created by your configuration.

5

Total

Success

5

Failed

0

Pending

0

Configuration details

The status of each configuration deployment.

Last updated: just now
Configuration progress updated every 30 seconds.

Q

Search account ID

<

1

>

	Account	Region	Configuration deployment status	Configuration status	Drift status
<input type="radio"/>	721859630063	sa-east-1	✔ Success	✔ 5 Success	None

Vamos testar a conexão com Instâncias na seção Session Manager clique Start Session

▼ Change Management

Change Manager

Automation

Change Calendar

Maintenance Windows

▼ Node Management

Fleet Manager

Compliance

Inventory

Hybrid Activations

Session Manager

Run Command

State Manager

Patch Manager

Distributor

AWS Systems Manager > Session Manager

Session Manager

Sessions

Session history

Preferences

Sessions

Q

Terminate

Start session

<

1

>

Session ID	Owner	Instance ID	Document name	Reason	Start date	Status
There are no active sessions at the moment. Click Start session to connect to an instance or choose the Session history tab to view details about terminated sessions.						

Selecione a Instância e clique em start

▼ Change Management

Change Manager

Automation

Change Calendar

Maintenance Windows

▼ Node Management

Fleet Manager

Compliance

Inventory

Hybrid Activations

Session Manager

Run Command

State Manager

Patch Manager

Distributor

AWS Systems Manager > Session Manager > Start a session

Start a session

Select the instance that you would like to start a session on

Reason

Reason for session – optional

The reason for connecting to the instance. This value is included in the details of the event created by AWS CloudTrail when you start the session. The value can have up to 256 characters.

Enter reason

Target instances

Q Filter instances

< 1 >

	Instance name	Instance ID	Agent version	Instance state	Availability zone	Platform
<input checked="" type="radio"/>	webserver1	i-0a8c85c06a3e970bd	3.1.1374.0	✔ running	sa-east-1a	Ubuntu
<input type="radio"/>	webserver2	i-026dbdff130398bbb	3.1.1374.0	✔ running	sa-east-1a	Ubuntu

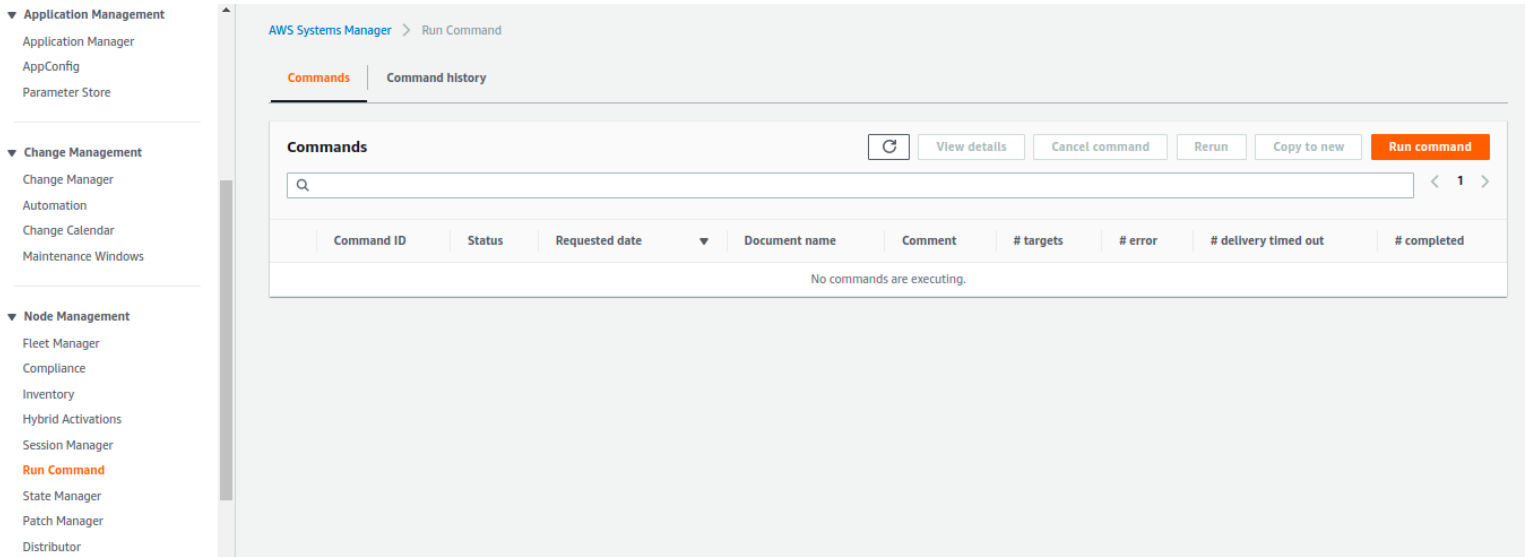
Cancel

Start session

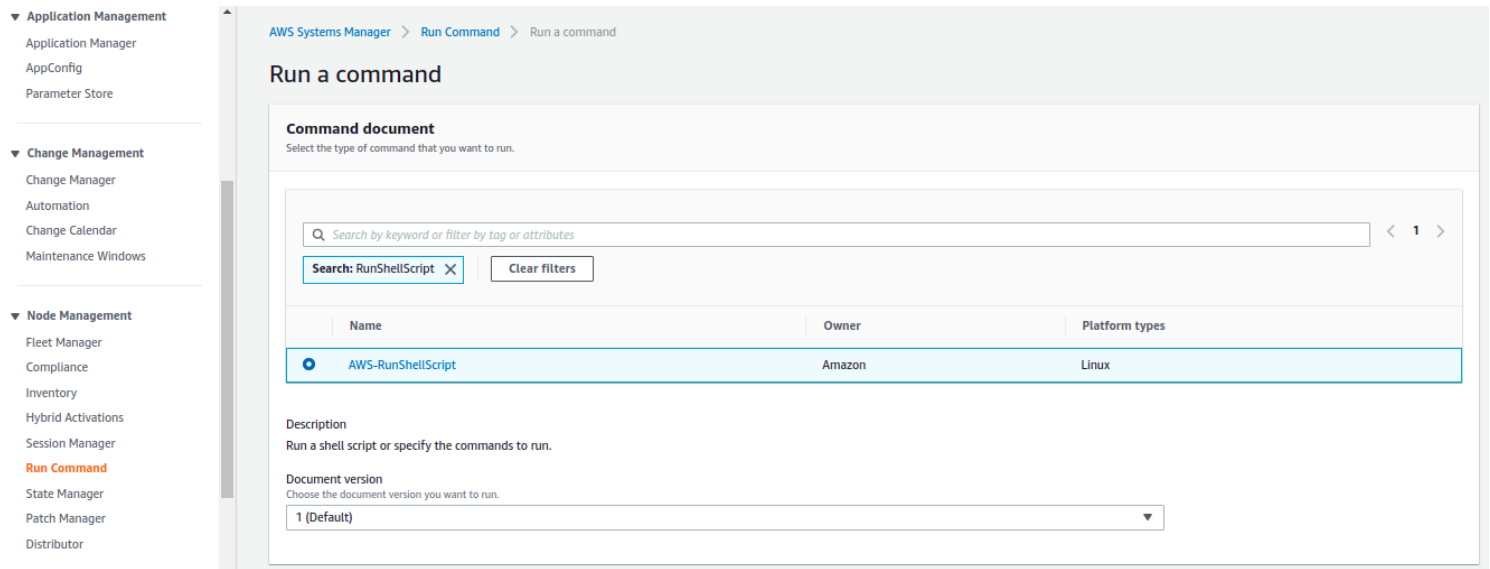
Execute o comando `ls -ltr /usr/bin/security_agent` a pasta estará vazia

```
$
$
$ ls -ltr /usr/bin/security_agent
ls: cannot access '/usr/bin/security_agent': No such file or directory
$
```

No menu a esquerda do SystemManager acesse Run Command para provisionamento do "agente" clique em Run Command



Clique em Run e selecione AWS-RunShellScript



Abaixo em Command parameters insira o script

```
sudo wget -q https://bootcamp-aws.s3.amazonaws.com/install_security_agent.sh -P /tmp
sudo chmod +x /tmp/install_security_agent.sh
sudo /tmp/install_security_agent.sh
ls -ltr /usr/bin/security_agent
```

Na seção targets marque a opção Choose instances manually e selecione as instâncias

▼ Application Management

Application Manager

AppConfig

Parameter Store

▼ Change Management

Change Manager

Automation

Change Calendar

Maintenance Windows

▼ Node Management

Fleet Manager

Compliance

Inventory

Hybrid Activations

Session Manager

Run Command

State Manager

Targets

Targets

Choose a method for selecting targets.

☐ Specify instance tags

☒ Choose instances manually

☐ Choose a resource group

Specify one or more tag key-value pairs to select instances that share those tags.

Manually select the instances you want to register as targets.

Choose a resource group that includes the resources you want to target.

i-0a8c85c06a3e970bd

i-026dbdff130398bbb

Instances

< 1 >

⊞

<input checked="" type="checkbox"/>	Node ID	Source type	Source ID	Name	Ping status	Node state	Availability zone	Last ping time
<input checked="" type="checkbox"/>	i-0a8c85c06a3e970bd	-	-	webserver1	Online	running	sa-east-1a	5/5/2022 at 16:53:39 GMT-4
<input checked="" type="checkbox"/>	i-026dbdff130398bbb	-	-	webserver2	Online	running	sa-east-1a	5/5/2022 at 16:52:32 GMT-4

Na seção Output options desmarque a opção de S3

▼ Node Management

Fleet Manager

Compliance

Inventory

Hybrid Activations

Session Manager

Run Command

State Manager

▼ Output options

Write command output to an Amazon S3 bucket

Write all command output to an Amazon S3 bucket. Command output in the console is truncated after 2500 characters.

☐ Enable an S3 bucket

☒ Send command output to Amazon CloudWatch logs

You can stream and encrypt log data for all commands in your account to a CloudWatch Logs log group in your account. [Learn more](#)

☐ Enable CloudWatch logs

Na Seção SNS notifications em IAMrole selecione a role SSMtoSNS cole a arn do SNS topic e clique em RUN

▼ Change Management

Change Manager

Automation

Change Calendar

Maintenance Windows

▼ Node Management

Fleet Manager

Compliance

Inventory

Hybrid Activations

Session Manager

Run Command

State Manager

Patch Manager

Distributor

▼ SNS notifications

SNS notifications

Configure Systems Manager to send notifications about command statuses using Amazon Simple Notification Service.

☒ Enable SNS notifications

IAM role

Choose an IAM role to start SNS notifications

arn:aws:iam::721859630063:role/SSMtoSNS

SNS topic

Enter an SNS topic. An SNS topic is a communication channel to subscribe to notifications. [Learn more.](#)

arn:aws:sns:sa-east-1:721859630063:NotificationSNS

Event notifications

Choose the types of events you want to be notified about. [Learn more.](#)

All events

Change notifications

Choose when you would like to receive notifications about changes to Run Command.

☐ Command status changes

Notifies you when the status of a command changes.

☒ Command status on each instance changes

Notifies you when the command status of an instance changes.

Após retorne a sua instância e rode comando `ls -ltr /usr/bin/security_agent`

Você vai ver que o agente de segurança foi copiado para as Instâncias, em casos de muitas instâncias essa solução é perfeita para cópia e instalação

```
$
$
$ ls -ltr /usr/bin/security_agent
ls: cannot access '/usr/bin/security_agent': No such file or directory
$ ls -ltr /usr/bin/security_agent
-rwxr-xr-x 1 root root 250 Oct  5  2020 /usr/bin/security_agent
$
```

