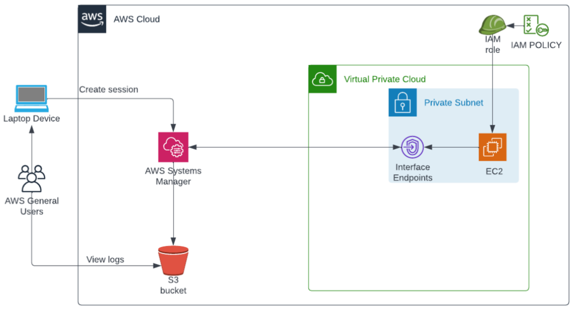


SSH Logging and Session Management Using AWS SSM and VPC Endpoint

Ravindra Singh
DevOps Engineer at Coditas | AWS Community Builder

2 articles + Follow

July 24, 2022

Open Immersive Reader

AWS PrivateLink restricts all network traffic between your managed instances, Systems Manager, and Amazon EC2 to the Amazon network. This means that your managed instances that don't have access to the Internet. If you use AWS PrivateLink, you don't need an internet gateway, a NAT device, or a virtual private gateway.

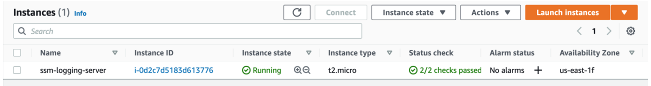
> No need to open the SSH Port(22) in the security group.

The **OS** is Amazon Linux 2, because by default it comes with AWS Systems Manager Agent (SSM Agent) installed.

EC2 and IAM

Launching an EC2 instance is normally fairly easy, but there’s one key task that must be done during launch, We need to attach an IAM role to our instance, otherwise, we won’t be able to achieve the expected results detailed at the end of this article.

The IAM role we associate with our EC2 instance must have the built-in **AmazonSSMManagedInstanceCore** and **AmazonS3FullAccess** policy(you can create your inline policy as well)



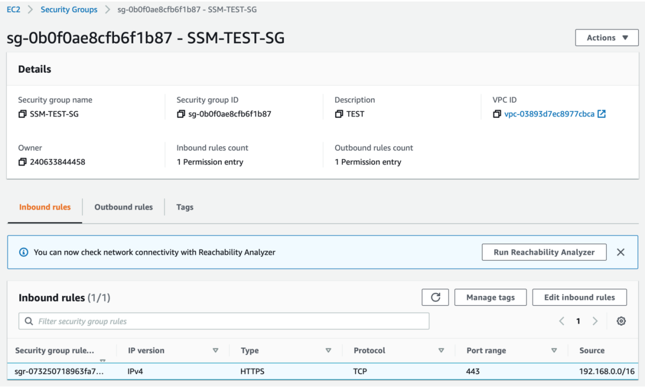
☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
☐	ssm-logging-server	i-0d2c7d5183d613776	Running	t2.micro	2/2 checks passed	No alarms +	us-east-1f

VPC Endpoints

AWS VPC ENDPOINTS enables private connection between your VPC and supported AWS Services and VPC Endpoints powered by AWS Private link.

- We need a VPC Endpoint that will help us to take the SSH of instances using AWS System manager and flow the traffic within the AWS Network because we are not using an Internet gateway, a NAT device, or a virtual private gateway.

> Instances must also allow HTTPS (port 443) outbound traffic to the following endpoints:


EC2 > Security Groups > sg-0b0f0ae8cfb6f1b87 - SSM-TEST-SG
Actions ▼
Inbound rules
Outbound rules
Tags
Run Reachability Analyzer
Manage tags
Edit inbound rules
Filter security group rules
1

sg-0b0f0ae8cfb6f1b87 - SSM-TEST-SG

Details

Security group name: SSM-TEST-SG
Security group ID: sg-0b0f0ae8cfb6f1b87
Description: TEST
VPC ID: vpc-03893d7ec8977cbca
Owner: 240633844458
Inbound rules count: 1 Permission entry
Outbound rules count: 1 Permission entry

You can now check network connectivity with Reachability Analyzer

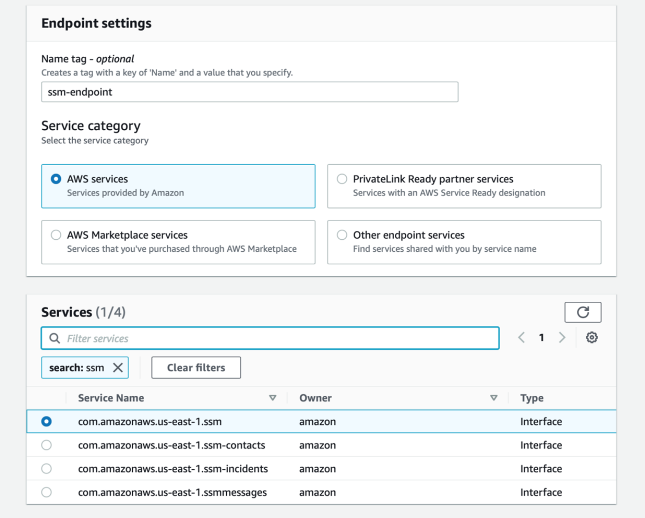
Inbound rules (1/1)

Security group rule...	IP version	Type	Protocol	Port range	Source
sgr-073250718963fa7...	IPv4	HTTPS	TCP	443	192.168.0.0/16

We need to create these VPC Endpoints. so that I can use Systems Manager to manage private EC2 instances without internet access.

1. ssm.region.amazonaws.com
2. ssmmessages.region.amazonaws.com
3. ec2messages.region.amazonaws.com
4. com.amazonaws.us-east-1.ec2
5. com.amazonaws.us-east-1.s3

Lets, Create a VPC endpoint for the AWS System manager.



Endpoint settings

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
ssm-endpoint

Service category
Select the service category

● AWS services
Services provided by Amazon

○ PrivateLink Ready partner services
Services with an AWS Service Ready designation

○ AWS Marketplace services
Services that you've purchased through AWS Marketplace

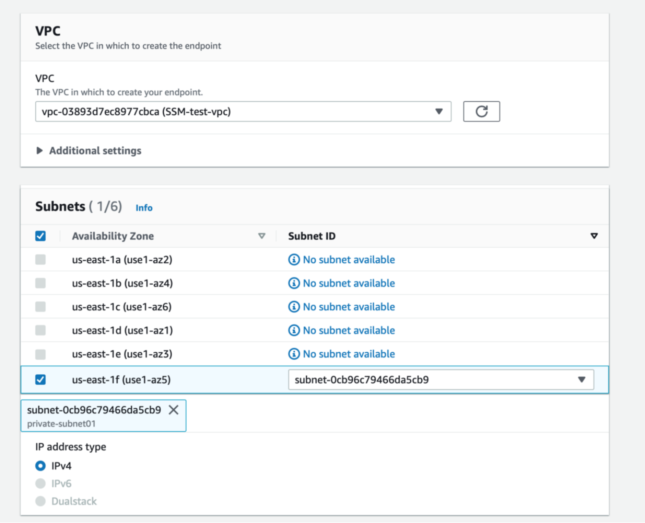
○ Other endpoint services
Find services shared with you by service name

Services (1/4)

search: ssm

	Service Name	Owner	Type
●	com.amazonaws.us-east-1.ssm	amazon	Interface
○	com.amazonaws.us-east-1.ssm-contacts	amazon	Interface
○	com.amazonaws.us-east-1.ssm-incidents	amazon	Interface
○	com.amazonaws.us-east-1.ssmmessages	amazon	Interface

For VPC, choose the VPC ID for your instance.



VPC
Select the VPC in which to create the endpoint

VPC
The VPC in which to create your endpoint.
vpc-03893d7ec8977cbca (SSM-test-vpc)

Additional settings

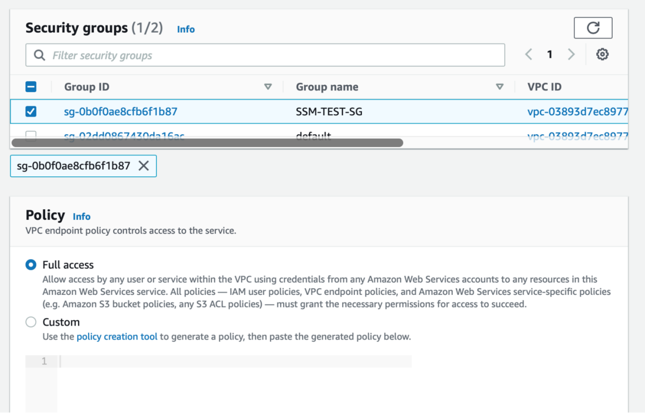
Subnets (1/6) Info

☑	Availability Zone	Subnet ID
□	us-east-1a (use1-az2)	No subnet available
□	us-east-1b (use1-az4)	No subnet available
□	us-east-1c (use1-az6)	No subnet available
□	us-east-1d (use1-az1)	No subnet available
□	us-east-1e (use1-az3)	No subnet available
☑	us-east-1f (use1-az5)	subnet-0cb96c79466da5cb9

subnet-0cb96c79466da5cb9
private-subnet01

IP address type
● IPv4
○ IPv6
○ Dualstack

For the Security group, select an existing security group, or create a new one. The security group must allow inbound HTTPS (port 443) traffic from the resources in your VPC that communicate with the service.



Security groups (1/2) Info

	Group ID	Group name	VPC ID
☑	sg-0b0f0ae8cfb6f1b87	SSM-TEST-SG	vpc-03893d7ec8977
□	sg-02dd0867430da16ac	default	vpc-03893d7ec8977

sg-0b0f0ae8cfb6f1b87

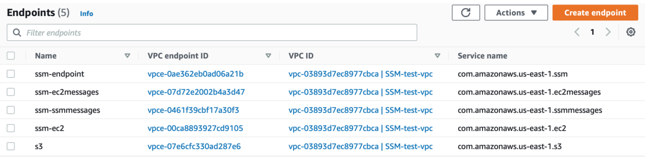
Policy Info
VPC endpoint policy controls access to the service.

● Full access
Allow access by any user or service within the VPC using credentials from any Amazon Web Services accounts to any resources in this Amazon Web Services service. All policies — IAM user policies, VPC endpoint policies, and Amazon Web Services service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed.

○ Custom
Use the policy creation tool to generate a policy, then paste the generated policy below.

> Repeat above steps to create other VPC endpoints.

You will see all the above Endpoints in the list.

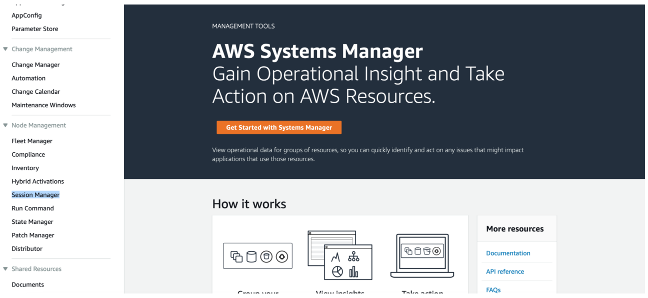


□	Name	VPC endpoint ID	VPC ID	Service name
□	ssm-endpoint	vpce-0ae362eb0ad06a21b	vpc-03893d7ec8977cbca | SSM-test-vpc	com.amazonaws.us-east-1.ssm
□	ssm-ec2messages	vpce-07d72e2002b4a3d47	vpc-03893d7ec8977cbca | SSM-test-vpc	com.amazonaws.us-east-1.ec2messages
□	ssm-ssmmessages	vpce-0461f39cbf17a30f3	vpc-03893d7ec8977cbca | SSM-test-vpc	com.amazonaws.us-east-1.ssmmessages
□	ssm-ec2	vpce-00ca8893927cd9105	vpc-03893d7ec8977cbca | SSM-test-vpc	com.amazonaws.us-east-1.ec2
□	s3	vpce-07e6cfc330ad287e6	vpc-03893d7ec8977cbca | SSM-test-vpc	com.amazonaws.us-east-1.s3

AWS Systems Manager Session Manager

This is the final key step, where we configure secure access to our Linux machine for SSH session monitoring and logging. We'll start with the Session Manager dashboard.

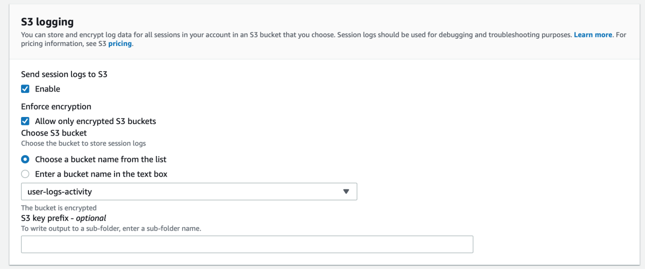
- Click on session manager from the left panel and it will take up you to the new screen.



AWS Systems Manager
Gain Operational Insight and Take Action on AWS Resources.

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.

- On the Preferences page, we will find multiple options that we could explore, but we will be focusing on streaming SSH session logs to the S3 bucket.



S3 logging

You can store and encrypt log data for all sessions in your account in an S3 bucket that you choose. Session logs should be used for debugging and troubleshooting purposes. Learn more. For pricing information, see S3 pricing.

Send session logs to S3
☑ Enable

Enforce encryption
☑ Allow only encrypted S3 buckets

Choose S3 bucket
Choose the bucket to store session logs
● Choose a bucket name from the list
○ Enter a bucket name in the text box

user-logs-activity ▼
The bucket is encrypted

S3 key prefix - *optional*
To write output to a sub-folder, enter a sub-folder name.

Once SSH logging is configured, we can SSH into our Linux machine and execute some commands to see if the activity is getting captured or not.

Let's Login to the instance using SSM:

We can use the **CLI** and **GUI** to command to connect the instance through the SSM

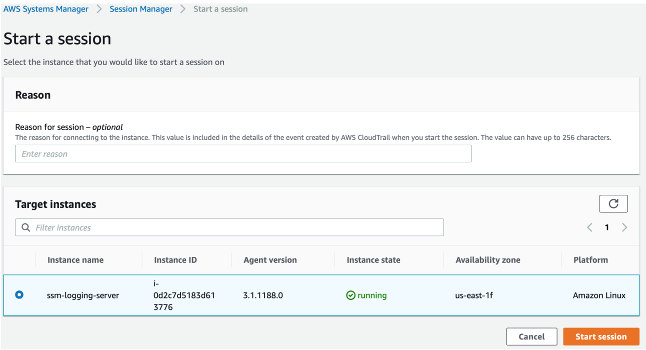
CLI Command:

```
aws ssm start-session --target <instance-id>  --regi
```

GUI:

So, let's start a session. On the same page, we will find a "Sessions" tab where we can start a session. Clicking the

“Start Session” button will give us a list of EC2 machines on which we can initiate a session:



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.

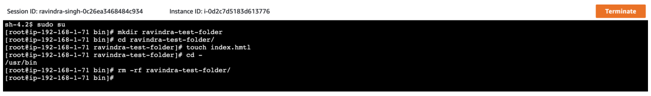
Enter reason

Target instances

Filter instances

	Instance name	Instance ID	Agent version	Instance state	Availability zone	Platform
●	ssm-logging-server	i-0d2c7d5183d613776	3.1.1188.0	✓ running	us-east-1f	Amazon Linux

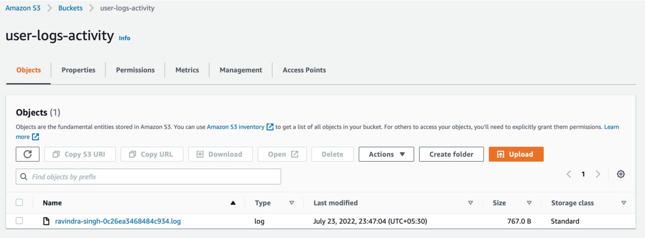
Let's Execute a few commands to log user session activity



Session ID: ravindra-singh-0c26ea3468484c934   Instance ID: i-0d2c7d5183d613776

```
sh-4.2$ sudo su
[root@ip-192-168-1-71 bin]# mkdir ravindra-test-folder
[root@ip-192-168-1-71 bin]# cd ravindra-test-folder/
[root@ip-192-168-1-71 ravindra-test-folder]# touch index.hmtl
[root@ip-192-168-1-71 ravindra-test-folder]# cd -
/usr/bin
[root@ip-192-168-1-71 bin]# rm -rf ravindra-test-folder/
[root@ip-192-168-1-71 bin]#
```

After executing a few commands, let’s navigate to our S3 bucket and confirm whether the activity is being recorded or not?



Amazon S3 > Buckets > user-logs-activity

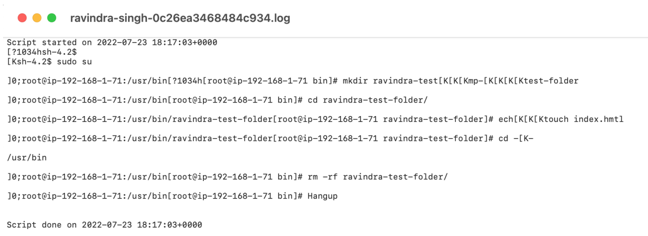
user-logs-activity Info

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you’ll need to explicitly grant them permissions. Learn more

□	Name	Type	Last modified	Size	Storage class
□	ravindra-singh-0c26ea3468484c934.log	log	July 23, 2022, 23:47:04 (UTC+05:30)	767.0 B	Standard

Download the log file to see the user session activity.



ravindra-singh-0c26ea3468484c934.log

```
Script started on 2022-07-23 18:17:03+0000
[?1034hsh-4.2$
[Ksh-4.2$ sudo su

]0;root@ip-192-168-1-71:/usr/bin[?1034h[root@ip-192-168-1-71 bin]# mkdir ravindra-test[K[K[Kmp-[K[K[K[Ktest-folder

]0;root@ip-192-168-1-71:/usr/bin[root@ip-192-168-1-71 bin]# cd ravindra-test-folder/

]0;root@ip-192-168-1-71:/usr/bin/ravindra-test-folder[root@ip-192-168-1-71 ravindra-test-folder]# ech[K[K[Ktouch index.hmtl

]0;root@ip-192-168-1-71:/usr/bin/ravindra-test-folder[root@ip-192-168-1-71 ravindra-test-folder]# cd -[K-

/usr/bin

]0;root@ip-192-168-1-71:/usr/bin[root@ip-192-168-1-71 bin]# rm -rf ravindra-test-folder/

]0;root@ip-192-168-1-71:/usr/bin[root@ip-192-168-1-71 bin]# Hangup


Script done on 2022-07-23 18:17:03+0000
```

We now have a setup, with at-rest encryption enabled, recording every command fired in our Linux machine and storing it in our S3 bucket.

!!

> Any secrets provided or generated during the session will be recorded in CloudWatch or S3 and can be seen by anyone who has the required permissions. To prevent that, we can use **stty -echo; read passwd; stty echo;** for each secret we need to provide during the session.

Thank you

References:

https://aws.amazon.com/premiumsupport/knowledge-center/ec2-systems-manager-vpc-endpoints/

Report this

Published by

Ravindra Singh
DevOps Engineer at Coditas | AWS Community Builder 2 articles + Follow
Published • 1y

How to log SSH activity—minus sensitive input, like passwords, commands — occurring in Linux AWS EC2 instances to the S3 buckets. #logging #aws #SSM #endpoints #linux

Like Comment Share 27

Reactions

+15

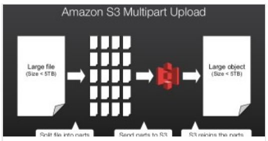
0 Comments

Add a comment...

Ravindra Singh
DevOps Engineer at Coditas | AWS Community Builder

+ Follow

More from Ravindra Singh



AWS S3 Multipart Upload using AWS CLI

Ravindra Singh on LinkedIn