Mandiant

USING AWS SYSTEM MANAGER WITH SECURITY VALIDATION

If you are running a Mandiant Advantage Security Validation Actor or Director in AWS, you can use the AWS System Manager to manage the instances. This requires installing the AWS Systems Manager Agent (SSM Agent) an the instance.

For full details on AWS System Manager and the SSM Agent please refer to the AWS documentation:
https://docs.aws.amazon.com/systems-manager/latest/userguide/what-is-systems-manager.html

Installing the SSM Agent

Requirements vary based on how you deployed your Actor and Director and what version it is.

Version 4.5.3.2 and new AMIs:

The AWS Systems Manager Agent (SSM Agent) is included in the Mandiant Advantage Security Validation's AMIs. This means the Agent will automatically start when you deploy a new Actor or Director using the AMI.

Pre 4.5.3.2 Appliances (OVAs, AMIs):

If you already have an Actor or Director that was created from our AMI, you can manually add the AWS Systems Manager Agent to it. To do so, you will need to SSH into the system and run the following commands:

```
sudo yum install https://s3.us-east-1.amazonaws.com/amazon-ssm-us-east-1/latest/linux_amd64/amazon-ssm-agent.rpm
sudo systemctl enable amazon-ssm-agent
sudo systemctl start amazon-ssm-agent
```

This will install and start the agent for you, so it's ready to be connected to your AWS System Manager.

Actors & Directors installed from Software

If you have an Actor or Director in AWS that was not created from our AMI, you can manually add the AWS Systems Manager Agent to it. To do so, you will need to SSH into the system and run a set of OS-specific commands. See **https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-manual-agent-install.html** to get the commands for your operating system.

When you run the commands, the agent will install and start, so it's ready to be connected to your AWS System Manager.

Useful Requirement information

- The SSM Agent reaches out to an Amazon endpoint to check-in and communicate with the console.
  - It is possible that you will have firewall rules in place that could block this communication.
  - There may be some scenarios with VPCs where routes or networking to the endpoint won't be available.
- AWS instances have to be associated with a IAM role that allows them privileges to do what they need to do in AWS Session Manager.