Mandiant

TROUBLESHOOTING SECURITY VALIDATION IN AWS

Mandiant Advantage Security Validation (MA-SV) Actors and Directors hosted on AWS have specific configuration requirements to ensure communication. If the Security Validation team is hosting the component for you, there may be additional configuration requirements.

Issues generally fall into one of the following categories:

- AWS specific configuration
- Disk
- Environment's security technology configuration
- Actor / Director configuration

Before submitting a support ticket, review the common issues to verify your configuration is correct. While this document does not provide step-by-step instructions, it does give you a starting point.

AWS Configuration

- Security Groups not created
- Security Group not assigned to all interfaces of an Actor
- Security Group not assigned to the instance
- Incorrect or incomplete IP addresses in the Security Groups
- T2 to T3 instance type conversion interface issue
  - The ethernet interface configuration is incorrect when you boot an instance that was changed from T2 to T3
- Instance type isn't sized correctly
  - Occurs with Directors that are resource heavy / have multiple integrations (rare)

Can be remedied by enabling unlimited CPU credit or increasing instance size.

Disk

- Disk undersized
- Incorrect partition size

Environment's Security Technology Configuration

- Firewall blocking Actor / Director traffic
  - Happens most frequently with PAN firewalls
- Proxy file size limits
- Proxy blocking specific types of Actor to Director communication (the Allow list needs to be updated)

Actor / Director Configuration

- Actors are registered to Directors using the IP and not DNS.
  - Causes issues with specific Actions
  - Causes issues with specific network paths
- Actor configured using proxies
- Issue caused by `vsetnet` configuration
  - DNS info in `/etc/resolv.conf` is not correct
  - Information entered using `vsetnet` was incorrect