Mandiant

DISASTER RECOVERY INFORMATION

Having a functional Validation Platform may be one of the items you include in your Disaster Recovery plans. To help you with your planning, we've compiled some recommendations and helpful hints.

General backup requirements

Regardless of how your platform is installed, we recommend you maintain copies of the following so they are available if you have to go through your Disaster Recovery process.

- Your license
- If Integrations required any customization of the integration itself, a copy of that customization / integration state (or the information required to recreate the changes)
- A list of items you had to add to your Allow list to allow the platform to communicate correctly
- A copy of the appliance or software for your existing versions of the Actor
- A copy of the appliance or software for your existing version of the Protected Theater
- A copy of any certs applied to Actors

> **TIP:** Existing certs can be applied to Actors but not Directors. If you don't use a backup that includes the SSL certificate, you need to create, sign, and apply a new cert to the Director.

Since you need to use the same version across Security Validation components, we recommend keeping copies of your Actor and Protected Theater appliances or software in case you also have to recover those components.

MSV (on-prem) systems

Director

If you are taking a snapshot of system the Director is located, we recommend shutting down the system completely before taking the snapshot or making the full backup.

> **NOTE:** If the Machine Identifiers changed on the snapshot or backup you use to restore your Security Validation components, you may be required to run `vreset` on your Actors and Protected Theaters and then re-registering them.

If you are not taking a snapshot of the system and instead plan on installing the Director from scratch, we recommend you maintain copies of the following:

- A copy of the appliance or software for your existing version of the Director
- A backup of the Director database

> **TIP:** Create these backups as frequently as necessary. We suggest creating a backup any time you make configuration changes and as frequently as necessary, based on your company's loss tolerance.

- Your system-level configuration details
  - Interface configuration
  - Routing information
  - Custom iptables rules

Actors

Actors do not contain data, so it is not as important to back them up. If you have the appliance or software to install them again, you can register them using the same configuration as previously. If you added a cert to them and kept the cert,

you can just reapply the cert.

Protected Theater and Protected Actor

We recommend taking a snapshot / full backup of your Protected Theater for Disaster Recovery purposes. That will reduce the time required to restore your Validation Platform. There are a few important things to consider if you do have to restore the platform:

- Your Protected Theater and Protected Actor should work automatically with no additional configuration in the following instances:
  - If you restore your Director from a backup that's on the same IP and use an existing PT
  - If you restore both your Director and Protected Theater from backups and no networking changes (IP addresses stay the same, etc)
- If you keep an existing Protected Theater, you will need to run `vreset`, add both the Protected Theater and Protected Actor to the Director via the UI, and then register them in the following instances:
  - If you add a new Director and don't apply a backup
  - If restore the Director with a new IP
  - If your backup didn't include the Protected Theater

Cloud systems

If your environment is hosted in a cloud system you maintain, you should have the ability to take regular snapshots / backups of your Director and Actors. These can be maintained in a separate system and used to restore your platform.

Depending on how you create your backup, you may need to complete one or more of the following configuration steps:

- Create and apply a certificate

  > **NOTE:** If your backup does not include the SSL certificate, you will need to generate a new SSL CSR, get it signed, and apply it

- Configure network interfaces
- Verify services are running
- Re-register or rebuild your Actors
- Re-register or rebuild your Protected Theater

Hosted systems

We take nightly backups of our Directors in the form of AMIs. Backups AMIs are stored and retained for 7 days in the same region as the Director for fast recovery. In addition, a duplicate copy is made in a separate region for Disaster Recovery purposes and is retained for 30 days.

No data is stored on the Actor. You can remove and reregister the Actor in the Director.