Can I backup tracking, reporting and quarantined dataset from the Security Management Appliance (SMA)?

Contents

Question

Can I back up tracking, reporting and quarantined dataset from the Security Management Appliance (SMA)?

Answer

The Cisco Security Management Appliance (SMA) allows an administrator to copy the active datasets (tracking, reporting and ISQ database) from the "source" SMA to a "target" SMA via the **backupconfig** command on the CLI.

The backup process is executed in two phases:

Phase 1

The backup process starts with the data transfer between the source and target appliances. During data transfer, services on the source appliance remain running, therefore data collection can still continue. Services though are shut down on the target appliance. Once the data transfer is complete from the source to target appliance, Phase 2 begins.

Phase 2

When Phase 2 begins, services on the source appliance are shut down. Any differences that have collected during the data transfer between the source and target appliance since the initial shutdown are copied to the target appliance and the service is brought back up for both the source and the target. This allows for maximum uptime on the source appliance and no data loss for either appliance.

There are two types of scheduled backups that you can perform on the SMA:

Periodic Backups: Periodic backups consist of continual backups that can be scheduled for a predetermined time, or for a single backup that occurs at a predetermined time.

Instant Backups: Instant backups occur immediately when the user initiates the backupconfig command on the CLI.

Additionally, you can view or cancel scheduled and ongoing backups, check the status of a backup, or verify if a backup can be scheduled onto a remote machine.