Restart and View the Status of Service Engines Enabled on ESA/CES

Contents

Introduction

This document describes how to restart and view the status of service engines on an Email Security Appliance (ESA) or Cloud Email Security (CES).

Background Information

Starting Async OS 11.1.x and above, ESA allows for users with administrative access to SSH of the appliance to view and restart certain services when needed. Please refer to the release notes [here](#).

> **Caution**: The services should only be restarted as part of troubleshooting specific known issues, when in doubt please contact Cisco TAC.

Prerequisites

Requirements

- ESA running Async OS 11.1 or higher
- Administrative SSH access to the appliance
- Familiarity with executing commands via Secure Shell (SSH)

Components Used

The information in this document is based on all supported ESA hardware models and virtual appliances running Async OS 11.x or higher.

In order to verify version information of the appliance from the CLI, enter the **version** command. In the GUI, select **Monitor > System Status**.

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Restart and View the Status of Service Engines Enabled on ESA/CES

1. Connect to the ESA with the use of SSH.

2. Enter command **diagnostic** followed by sub-command **services**

3. Select one of the listed services by typing in its name (not case-sensitive).

4. Some services may have sub-commands to select specific service depending on installed device licenses (such as McAfee/Sophos for antivirus).

5. Enter command **status** in order to view the status of the service, or command **restart** to restart the service.

Sample output for reference:

```
lab.esa.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility. - DISK_USAGE - Check Disk Usage. - NETWORK - Network Utilities. -
REPORTING - Reporting Utilities. - TRACKING - Tracking Utilities. - RELOAD - Reset configuration
to the initial manufacturer values. - SERVICES - Service Utilities. []> services

Choose one of the following services:
- ANTISPAM - Anti-Spam services
- ANTIVIRUS - Anti-Virus services
- DLP - Cisco Data Loss Prevention services
- ENCRYPTION - Encryption services
- GRAYMAIL - Graymail services
- REPORTING - Reporting associated services
- TRACKING - Tracking associated services
- EUQWEB - End User Quarantine GUI
- WEBUI - Web GUI
- SMART_LICENSE - Smart Licensing Agent
- ETF - External Threat Feeds
- SDR - Sender Domain Reputation
- IP_REP_CLIENT - Sender IP Reputation Client
- URL_REPUTATION_CLIENT - URL Reputation Client
- SERVICE_LOG_CLIENT - Service Log Client
[]> antispam

Choose one of the following type of scanners:
- CASE - CASE
- IMS - Intelligent Multi Scan
[]> case

Choose the operation you want to perform:
- RESTART - Restart the service
- STATUS - View status of the service
[]> status
```

CASE has been up for 38m 38s.

Choose one of the following type of scanners:
- CASE - CASE
- IMS - Intelligent Multi Scan
[]> **case**

Choose the operation you want to perform:
- RESTART - Restart the service
- STATUS - View status of the service
[]> **restart**

Restart command processed. The service CASE should be up in a moment.

Choose one of the following type of scanners:
- CASE - CASE
- IMS - Intelligent Multi Scan
[]> **case**

Choose the operation you want to perform:
- RESTART - Restart the service
- STATUS - View status of the service
[]> **status**

CASE has been up for 13s.

Choose one of the following type of scanners:
- CASE - CASE
- IMS - Intelligent Multi Scan
[]>

Related Information

- **[Cisco Email Security Appliance End-User Guides](#)**
- **[Cisco Email Security Appliance Release Notes and General Information](#)**
- **[Technical Support & Documentation - Cisco Systems](#)**