The checkallsslcerts Script

Overview

In the past, cPanel & WHM services used a self-signed certificate. Now all cPanel & WHM services use a cPanel-signed hostname certificate with a Comodo® trust chain. This document explains how the system installs a cPanel-signed hostname certificate and how to disable the automatic installation of a cPanel-signed hostname SSL certificate if you do not wish to use it.

The `/usr/local/cpanel/bin/checkallsslcerts` script

The system runs the `/usr/local/cpanel/bin/checkallsslcerts` script during the nightly cPanel & WHM update (`upcp`) process. This script performs the following actions:

- Installs a cPanel-signed hostname certificate on the server, if one does not exist.
- Updates the SSL certificate for all cPanel & WHM services.
- Issues a Comodo-signed SSL certificate on any server with a self-signed, expired, or soon-to-expire certificate.

> **Note:**
> A soon-to-expire certificate means that the SSL certificate expires in three days or fewer.

To execute these actions, the script performs the following steps:

1. The system creates a Domain Control Validation (DCV) file, which resembles the following example:

```
4221C402112E4831C72C2E004614C47C.txt
```

> **Notes:**
> - Systems that use EasyApache 3 store this file in the `/usr/local/apache/htdocs/.well-known/pki-validation/` directory.
> - Systems that use EasyApache 4 store this file in the `/var/www/html/.well-known/pki-validation` directory.

2. The system performs a DNS lookup for the hostname's IP address on the root nameservers. To do this, it runs the following command:

```
dig =trace hostname.example.com
```

> **Notes:**
> - If the `dig` command returns multiple IP addresses, the system uses the first IP address that the command returns.
> - In this example, `hostname.example.com` represents the server's hostname.

3. The system uses the hostname's IP address to confirm that it can access the Domain Control Validation (DCV) file. To do this, it runs the following command:

```
curl 192.0.2.0/AFAA5C66A1EEF5812703A46C21C013B4.txt
```

> **Note:**
> In this example, `192.0.2.0` represents the primary IP address, and `AFAA5C66A1EEF5812703A46C21C013B4.txt` represents the DCV file.

4. When the local DCV check passes, the system sends a request to the cPanel Store API for the new SSL certificate.
   - If a valid SSL certificate exists and matches the DCV file, the system does not perform any action.
   - If the system must issue a new SSL certificate, the systems sends a request to Comodo.
   - Comodo validates the DCV file from the following IP addresses:

> **Important:**
> Comodo uses these IP addresses to attempt to access the cPanel server. You **must** whitelist these IPs in the server firewall. For more information, read our How to Configure Your Firewall for cPanel Services documentation.

```
178.255.81.12
178.255.81.13
91.199.212.132
199.66.201.132
```

5. The system logs the Comodo requests in the `/etc/apache2/logs/access` file. It also contains user agent strings that show who accesses the DCV file. These user agent strings resemble the following examples:

cPanel user agent strings Comodo user agent strings

```
192.0.2.0 - - [16/Jun/2016:16:16:16 -0500]  "GET
/4221C402112E4831C72C2E004614C47C.txt HTTP/1.1" 200 53  "-"
"Cpanel-HTTP-Client/1.0"
192.0.2.0 - - [16/Jun/2016:16:16:16 -0500]  "GET
/4221C402112E4831C72C2E004614C47C.txt HTTP/1.1" 200 53  "-"
"Cpanel-HTTP-Client/1.0"
```

```
199.66.201.132 - - [16/Jun/2016:16:18:46 +0000]  "GET
/4F571E4CB76F46E37B8118CEA1DB42BA.txt HTTP/1.1" 200 53  "-" "COMODO
DCV"
199.66.201.132 - - [16/May/2016:16:18:46 +0000]  "GET
/4F571E4CB76F46E37B8118CEA1DB42BA.txt HTTP/1.1" 200 53  "-" "COMODO
DCV"
```

Optional command line flags

The `/usr/local/cpanel/bin/checkallsslcerts` script includes the following optional flags:

Optional CLI Switches	Description

`--verbose`	Adjusts output to include messages that resemble the following: • The system will attempt to replace the self-signed certificate for the “cpanel” service with a signed certificate from the cPanel Store. • The system will attempt to replace the self-signed certificate for the “dovecot” service with a signed certificate from the cPanel Store. • The system will attempt to replace the self-signed certificate for the “exim” service with a signed certificate from the cPanel Store. • The system will attempt to replace the self-signed certificate for the “ftp” service with a signed certificate from the cPanel Store.
`--allow-retry`	If the cPanel Store continues the hostname certificate request, then the system checks the cPanel Store again in an hour. To do this, it runs the following command: Click to view... `/usr/local/cpanel/scripts/try-later --action '/usr/local/cpanel/bin/checkallsslcerts --no-retry' --check '/bin/sh -c exit 1' –delay 60 --max-retries 1 --skip-first` If the system must retry, an entry will apper in the `at` daemon (`atd`) job queue. Use the following arguments to view, execute, or remove a job: **Argument** / **Description** `atq` — Views queue at jobs. `at -c #` — Views contents of a specific job number. `at -c # | sh` — Manually executes a job. `atrm #` — Manually removes a job.

Disable a cPanel-signed hostname certificate.

To disable a cPanel-signed hostname certificate's installation, run the following command:

```
touch /var/cpanel/ssl/disable_auto_hostname_certificate
```

To disable the automatic replacement of all expired service certificates and disable notifications about expired or expiring service certificates, run the following command:

```
touch /var/cpanel/ssl/disable_service_certificate_management
```

Additional documentation

Suggested documentationFor cPanel usersFor WHM usersFor developers

- The checkallsslcerts Script
- Purchase and Install an SSL Certificate
- Manage Service SSL Certificates
- The set-tls-settings Script
- Generate an SSL Certificate and Signing Request

- SSL TLS Wizard
- Install and Manage SSL for your site HTTPS
- SSL TLS Status
- Manage Certificate Sharing
- Certificate Signing Requests - CSR

- The checkallsslcerts Script
- Purchase and Install an SSL Certificate
- Manage Service SSL Certificates
- The set-tls-settings Script
- Generate an SSL Certificate and Signing Request

- UAPI Functions - SSL::can_ssl_redirect
- UAPI Functions - SSL::toggle_ssl_redirects_for_domains
- cPanel API 1 Functions - SSL::deletecsr
- cPanel API 1 Functions - SSL::gencsr
- cPanel API 1 Functions - SSL::showcsr