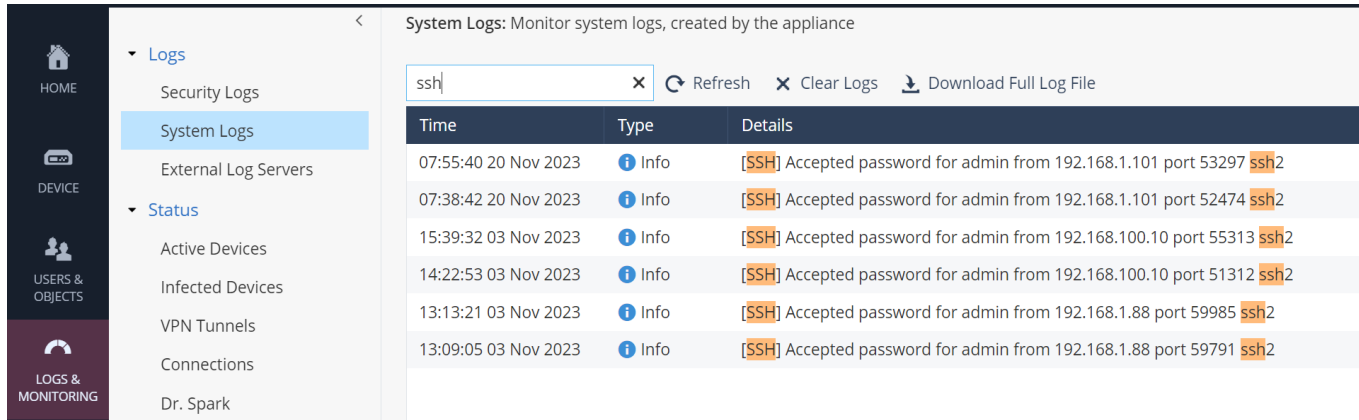


Working with Embedded GAIA System Audit Logs

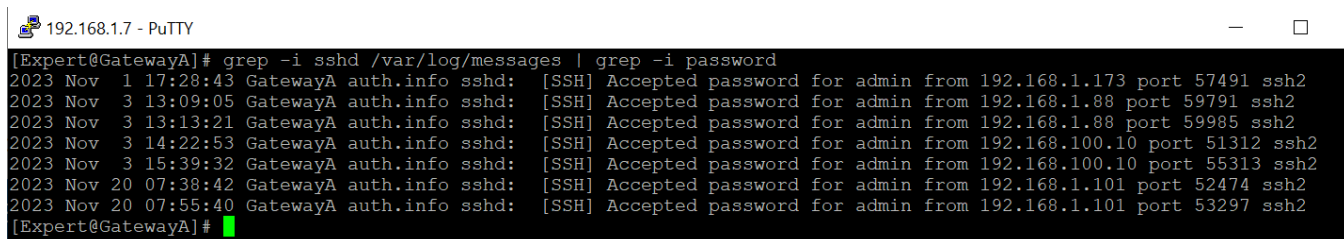
Chris Keith
Security Engineer-Heartland
November 20, 2023

Background: During a customer’s pen test, it was believed the tester was able to successfully log into one of the customer’s Spark appliances via SSH. The customer wanted to review the system audit logs to verify rather or not the tester successfully logged in. The customer had recently rebooted the appliance, so the messages file had rotated and the past audit logs were not included in the system log in the WebUI. The customer was able to use the steps below to verify the pen tester had not successfully log in.

1. On Spark appliances, the audit events are written to the active messages file in /var/log. After a reboot, a new messages file is created and the previous file is backed up in /logs.
 - a. To view SSH login events in the active messages file via the WebUI, navigate to “Logs & Monitor” and click on “System Logs”.
 - b. In the filter, type “ssh”. The successful SSH logins are displayed.




- c. To view SSH login events in the active message file via command line, log into the appliance in Expert mode.
 - d. Type “grep -i sshd /var/log/messages | grep -i password”. The successful SSH logins are displayed.



2. On Spark appliances, only the active messages file is stored in /var/log. Previous messages files are compressed and stored in /logs.


 192.168.1.7 - PuTTY

```
[Expert@GatewayA]# pwd
/var/log
[Expert@GatewayA]# ls -la messages*
-rw-r--r--  1 root  root           51741 Nov 20 08:15 messages
[Expert@GatewayA]# █
```

 192.168.1.7 - PuTTY

```
[Expert@GatewayA]# pwd
/logs
[Expert@GatewayA]# ls -la messages*
-rw-r--r--  1 root  root           9634 Nov  1 16:40 messages-1698874827.gz
-rw-r--r--  1 root  root           1367 Nov  1 16:52 messages-1698875532.gz
-rw-r--r--  1 root  root           1496 Nov  1 17:06 messages-1698876378.gz
-rw-r--r--  1 root  root           1892 Nov  1 17:25 messages-1698877529.gz
[Expert@GatewayA]# █
```

- a. To view audit logs in a previous messages file, the file should be copied to a different directory and uncompressed.
 - i. Log into the appliance in Expert mode. Locate the backed-up messages file in /logs that will include the audit events for the date and time you are investigating.
 - ii. Copy the backup-up messages file to /tmp using the “cp <filename.gz> /tmp” command.

 192.168.1.7 - PuTTY

```
[Expert@GatewayA]# cd /logs
[Expert@GatewayA]# pwd
/logs
[Expert@GatewayA]# ls -la messages*
-rw-r--r--  1 root  root           9634 Nov  1 16:40 messages-1698874827.gz
-rw-r--r--  1 root  root           1367 Nov  1 16:52 messages-1698875532.gz
-rw-r--r--  1 root  root           1496 Nov  1 17:06 messages-1698876378.gz
-rw-r--r--  1 root  root           1892 Nov  1 17:25 messages-1698877529.gz
-rw-r--r--  1 root  root           4829 Nov 20 15:26 messages-1700515573.gz
[Expert@GatewayA]# cp messages-1700515573.gz /tmp
[Expert@GatewayA]# █
```

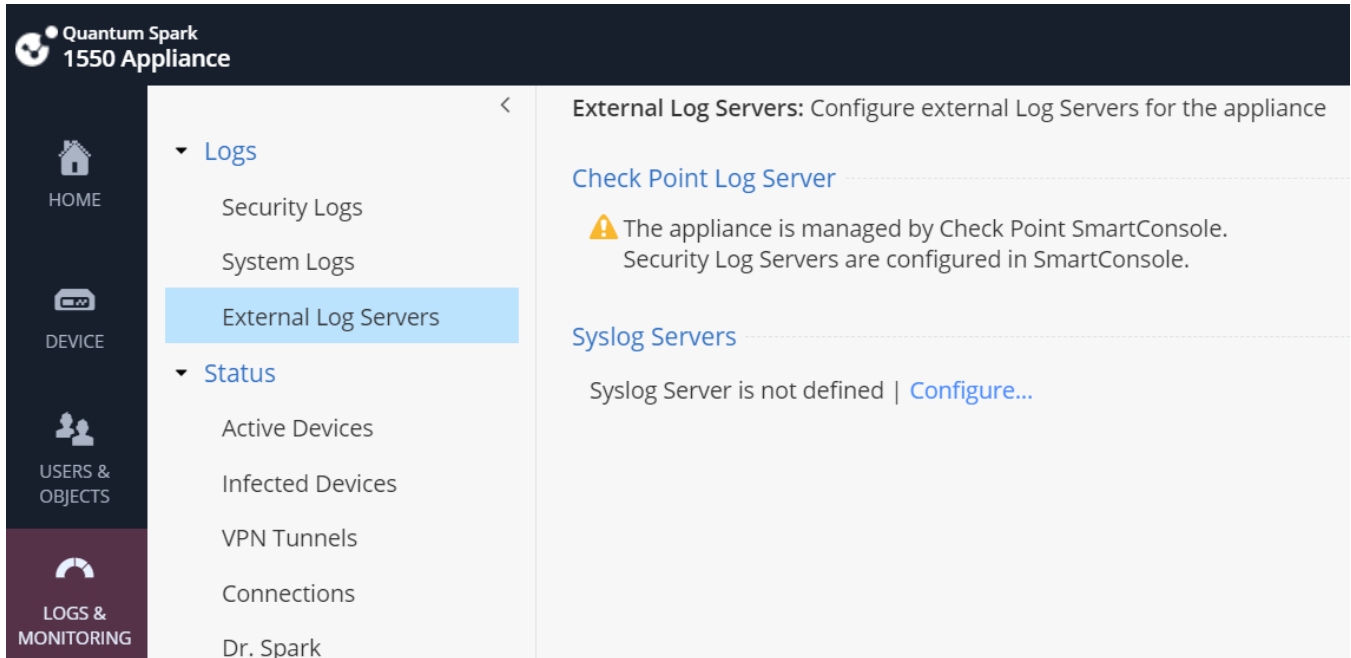
- iii. Change into the /tmp directory and uncompress the file using the “gzip -d <filename.gz>” command.

```
192.168.1.7 - PuTTY
[Expert@GatewayA]# cd /tmp
[Expert@GatewayA]# pwd
/tmp
[Expert@GatewayA]# ls -la messages*
-rw-r--r-- 1 root root 4241 Nov 20 16:28 messages
-rw-r--r-- 1 root root 4829 Nov 20 16:32 messages-1700515573.gz
[Expert@GatewayA]# gzip -d messages-1700515573.gz
[Expert@GatewayA]# ls -la messages*
-rw-r--r-- 1 root root 4241 Nov 20 16:28 messages
-rw-r--r-- 1 root root 5543 Nov 20 16:33 messages-1700515573
[Expert@GatewayA]# █
```

- iv. To view the successful SSH logins, use the “grep -i sshd <filename> | grep -i password” command.

```
192.168.1.7 - PuTTY
[Expert@GatewayA]# pwd
/tmp
[Expert@GatewayA]# ls -la messages*
-rw-r--r-- 1 root root 4241 Nov 20 16:28 messages
-rw-r--r-- 1 root root 5543 Nov 20 16:33 messages-1700515573
[Expert@GatewayA]# grep -i sshd /var/log/messages-1700515573 | grep -i password
2023 Nov 1 17:28:43 GatewayA auth.info sshd: [SSH] Accepted password for admin from 192.168.1.173 port 57491 ssh2
2023 Nov 3 13:09:05 GatewayA auth.info sshd: [SSH] Accepted password for admin from 192.168.1.88 port 59791 ssh2
2023 Nov 3 13:13:21 GatewayA auth.info sshd: [SSH] Accepted password for admin from 192.168.1.88 port 59985 ssh2
2023 Nov 3 14:22:53 GatewayA auth.info sshd: [SSH] Accepted password for admin from 192.168.100.10 port 51312 ssh2
2023 Nov 3 15:39:32 GatewayA auth.info sshd: [SSH] Accepted password for admin from 192.168.100.10 port 55313 ssh2
2023 Nov 20 07:38:42 GatewayA auth.info sshd: [SSH] Accepted password for admin from 192.168.1.101 port 52474 ssh2
2023 Nov 20 07:55:40 GatewayA auth.info sshd: [SSH] Accepted password for admin from 192.168.1.101 port 53297 ssh2
2023 Nov 20 09:22:01 GatewayA auth.info sshd: [SSH] Accepted password for admin from 192.168.1.101 port 55738 ssh2
[Expert@GatewayA]# █
```

3. Customers can also choose to send the System Logs to a Syslog server, allowing them to view the audit events within their Syslog server.
 - a. Within the WebUI, navigate to “Logs & Monitoring”.
 - b. Click “External Log Servers”.
 - c. Click “Configure” under “Syslog Servers”.



The screenshot displays the Check Point Quantum Spark WebUI for a 1550 Appliance. The left sidebar contains navigation options: HOME, DEVICE, USERS & OBJECTS, and LOGS & MONITORING. The main content area is titled "External Log Servers: Configure external Log Servers for the appliance". It features a "Check Point Log Server" section with a warning icon and the text: "The appliance is managed by Check Point SmartConsole. Security Log Servers are configured in SmartConsole." Below this is a "Syslog Servers" section with the text: "Syslog Server is not defined | [Configure...](#)".

- d. Enter the configuration information for the Syslog Server. Check the boxes next to “Show obfuscated fields” and “System logs”.
- e. Click “Apply”.

NEW SYSLOG SERVER ✕

Protocol:

Name:

IP address:

Port:

Enable log server

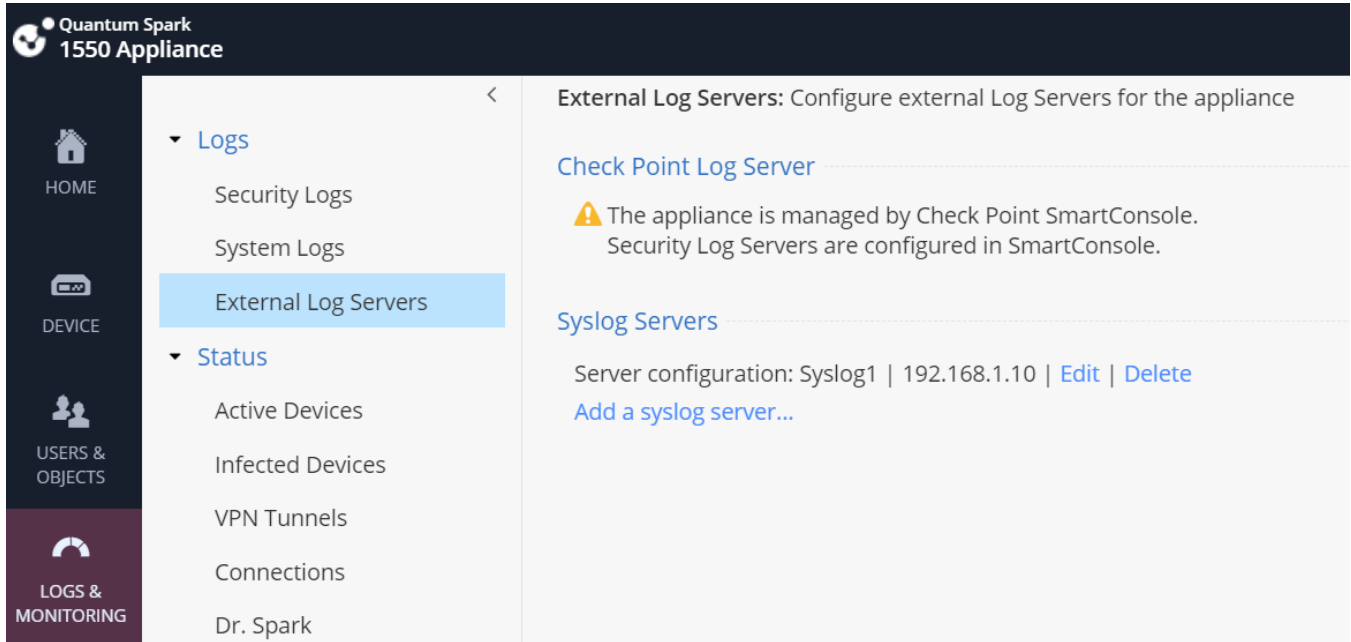
Show obfuscated fields

Forwarded logs:

System logs

Security logs

- f. The newly added Syslog server will now show up under “Syslog Servers” and system events should be forwarded to the Syslog server..



The screenshot shows the configuration page for External Log Servers on a Quantum Spark 1550 Appliance. The left sidebar contains navigation options: HOME, DEVICE, USERS & OBJECTS, and LOGS & MONITORING. The main content area is titled "External Log Servers: Configure external Log Servers for the appliance". It features a "Check Point Log Server" section with a warning icon and text: "The appliance is managed by Check Point SmartConsole. Security Log Servers are configured in SmartConsole." Below this is a "Syslog Servers" section showing a configuration for "Syslog1" at IP address "192.168.1.10" with "Edit" and "Delete" links, and an "Add a syslog server..." link. A central menu lists "Logs" (Security Logs, System Logs, External Log Servers) and "Status" (Active Devices, Infected Devices, VPN Tunnels, Connections, Dr. Spark).