WSA Log Transfer to a Remote SCP Server

Document ID: 118074

Contributed by Handy Putra, Cisco TAC Engineer.
Aug 26, 2014

Contents

Introduction

This document describes how to transfer logs from the Cisco Web Security Appliance (WSA) to a remote Secure Copy (SCP) server. You can configure the WSA logs, such as access and authentication logs, so that they are forwarded to an external server with SCP protocol when the logs roll−over or wrap.

The information in this document describes how to configure the log rotation rules as well as the Secure Shell (SSH) keys that are required for a successful transfer to an SCP server.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

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.

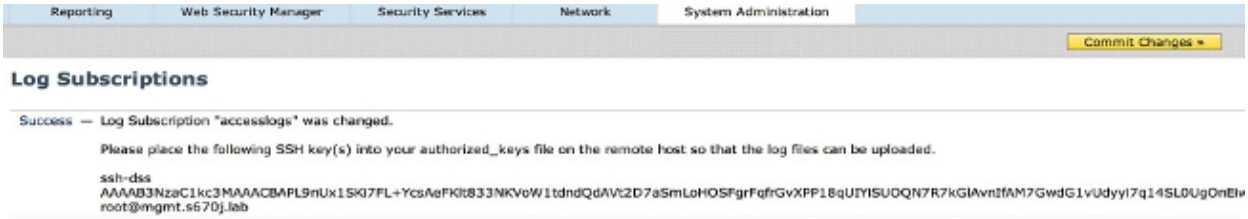
Configure

Complete these steps in order to configure the WSA logs so that they can be retreived with SCP on a remote server:

1. Log into the WSA web GUI.
2. Navigate to ***System Administration*** > ***Log Subscriptions***.
3. Select the name of the log(s) for which you desire to configure this retrieval method, such ***as access logs***.

4. In the Retrieval Method field, choose ***SCP on Remote Server***.
5. Enter the SCP host name or the IP address of the SCP server.
6. Enter the SCP port number.

   Note: The default setting is ***port 22***.
7. Enter the full path name of the SCP server target directory to which the the logs will be transfered.
8. Enter the username for the SCP server authenticated user.
9. If you want to automatically scan the host key or manually enter the host key, then enable ***Host Key Checking***.
10. Click ***Submit***. The SSH key that you will place into the SCP server ***authorized_keys*** file should now appear near the top of the ***Edit Log Subscription*** page. Here is an example of a successfulmessage from the WSA:



11. Click ***Commit Changes***.
12. If the SCP sever is a Linux or Unix server or a Macintosh machine, then paste the SSH keys from the WSA into the ***authorized_keys*** file located in the SSH directory:

    A. Navigate to the ***Users*** > <***username***> > ***.ssh*** directory.

    B. Paste the WSA SSH key into the ***authorized_keys*** file and save the changes.

    Note: You must manually create an ***authorized_keys*** file if one does not exist in the SSH directory.

Verify

Complete these steps in order to verify that the logs are successfully transferred to the SCP server:

1. Navigate to the WSA ***Log Subscriptions*** page.
2. In the ***Rollover*** column, choose the log that you configured for SCP retrieval.
3. Locate and click ***Rollover Now***.
4. Navigate to the SCP server folder that you configured for log retrieval and verify that the logs are transferred to that location.

Complete these steps in order to monitor the log transfer to the SCP server from the WSA:

1. Log into the WSA CLI via SSH.

2. Enter the ***grep*** command.

3. Enter the appropriate number for the log that you want to monitor. For example, enter ***31*** from the grep list for the ***system_logs***.

4. Enter ***scp*** at the *Enter the regular expression to grep* prompt in order to filter the logs so that you can monitor only the SCP transactions.

5. Enter ***Y*** at the *Do you want this search to be case insensitive?* prompt.

6. Enter ***Y*** at the *Do you want to tail the logs?* prompt.

7. Enter ***N*** at the *Do you want to paginate the output?* prompt. The WSA then lists the SCP transactions in real−time. Here is an example of successful SCP transactions from the WSA system_logs:

```
Wed Jun 11 15:06:14 2014 Info: Push success for subscription <the name of the log>:
Log aclog@20140611T145613.s pushed to remote host <IP address of the SCP Server>:22
```

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Updated: Aug 26, 2014 Document ID: 118074