AlienVault Unified Security Management™ Solution

Complete. Simple. Affordable

Device Integration: Citrix NetScaler

CONTENTS

1. INTRODUCTION

The objective of this document is to explain how to configure a Citrix NetScaler device to send log data to AlienVault USM.

This document is related to the AlienVault document "Data Source Plugin Management". The explanation about how to enable plugins can be found in that document.

2. CITRIX NETSCALER INFORMATION

Device Name	NetScaler
Device Vendor	Citrix
Device Type	Load Balancer
Data Source Name	citrix-netscaler
Connection Type	syslog
Data Source ID	1678

3. CONFIGURING CITRIX NETSCALER TO SEND LOG DATA TO ALIENVAULT

Citrix NetScaler must be configured to send log data to an AlienVault Sensor over the Syslog protocol.

1. Log on to the Citrix NetScaler web console with administrator credentials.
2. From the top menu, click **Configuration**.
3. In the System Configuration window, select a configuration utility.
4. In the navigation panel, expand the **System** folder.
5. Click the **Auditing** folder.
6. In the **Settings** section of the Auditing window, click **Change global auditing settings**.
7. In the Configure Auditing Parameters window, complete the fields as follows:

Field	Action
Auditing Type	From the drop-down list, select SYSLOG
IP Address	Enter the IP address of an AlienVault Sensor.
Port	Type 514
Log Levels	Select All
Log Facility	Select the appropriate log facility fro the drop-down list
Date Format	Select MMDDYYY
Time Zone	Select GMT
TCP Logging	Select TCP Logging
ACL Logging	Select ALC Logging

8. Above the top menu, click **Save**.
9. Click **Yes** to save configuration settings.

4. CONFIGURING ALIENVAULT TO RECEIVE LOGS FROM CITRIX NETSCALER

Devices that send log data via Syslog require configuration of the Syslog service to process those incoming logs into a unique file destination.

1. Open the console on the AlienVault Appliance, or log in over Secure Shell (SSH) as the "root" user.
2. Select and accept the "Jailbreak this Appliance" option to gain command line access.
3. Create a new configuration file to save incoming logs:

```
nano -w /etc/rsyslog.d/citrix-netscaler.conf
```

4. Add the following line to the file, one for each Citrix NetScaler device you are sending logs from:

```
if ($fromhost-ip == 'IP_Address') then /var/log/citrix-netscaler.log
```

IP_Address refers to the Citrix NetScaler IP Address.

5. End the file with this line:

```
& ~
```

6. Press **Crtl+W** to save the file and **Ctrl+X** to exit the editor.

7. Restart the Syslog Collector:

```
/etc/init.d/rsyslog restart
```

5. CONFIGURING LOG FILE EXPIRATION

Incoming logs will be processed by the Sensor and passed on to the SIEM Service. Keeping the raw log files on the sensor for more than a few days is unnecessary and they should be purged to maintain adequate free filesystem capacity.

1. Create a new log rotation configuration file.

```
nano –w /etc/logrotate.d/citrix-netscaler
```

2. Add the follows content to the file:

```
/var/log/citrix-netscaler.log
{
 rotate 4 # save 4 days of logs
 daily # rotate files daily
 missingok
 notifempty
 compress
 delaycompress
 sharedscripts
 postrotate
 invoke-rc.d rsyslog reload > /dev/null
 endscript
}
```

6. HOW TO ENABLE THIS PLUGIN

This plugin is already configured, but it is necessary to enable it, through console or through the web interface. The instructions about how to enable this plugin can be found in the AlienVault document "Data Source Plugin Management".