Netsurion™ | EventTracker

Behavior Group Level & Other Enhancements

Update Document

Publication Date: October 23, 2018

Abstract

This document will guide the users with the Behavior group level handled by EventTracker. It also includes detail information about the other enhancements in this update

Audience

User(s) who wish to monitor Behavior and set it at different group level.

Table of Contents

Process to be followed after applying the update

Behavior Group Level

This new feature processes and analyzes behavior data on group level.

For Example: IP activity in two group

Group- 1- TOONS

Group- 2- SIEM

So, if IP activity for an IP "192.168.X.XX" is found in TOONS group than a new activity gets generated for TOONS group only and the next occurrence activity count gets increased for the same IP.

On the otherhand, if IP activity for "192.168.X.XX" is found in SIEM group than a new activity gets generated for SIEM group only and the next occurrence activity count will get increased for the same IP.

1. Once the update is applied, login to EventTracker web; navigate to **Admin** and then **Behavior Correlation Settings**.

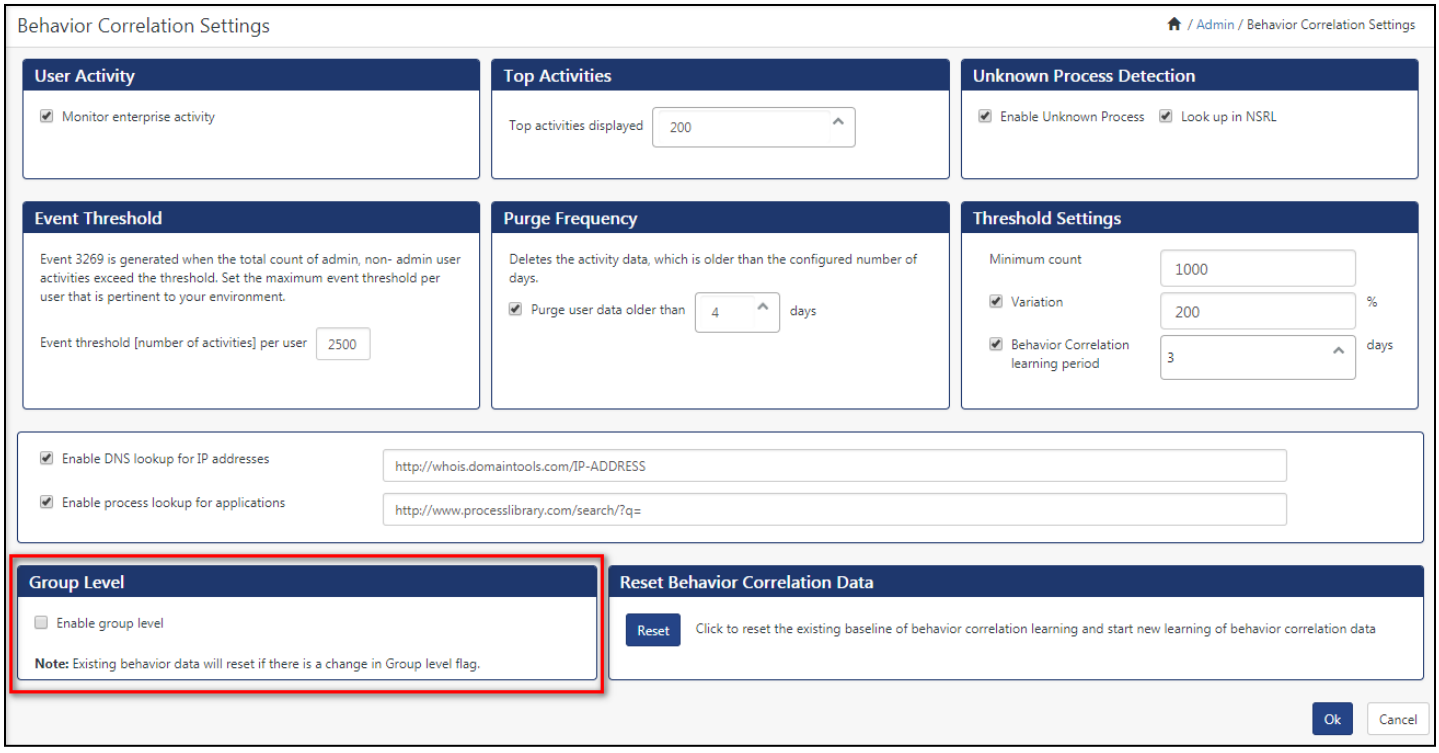

Figure 1

2. Scroll-down and you can see a Group-Level pane.
3. Select the "**Enable Group Level** "checkbox, which will reset the existing behavior data.

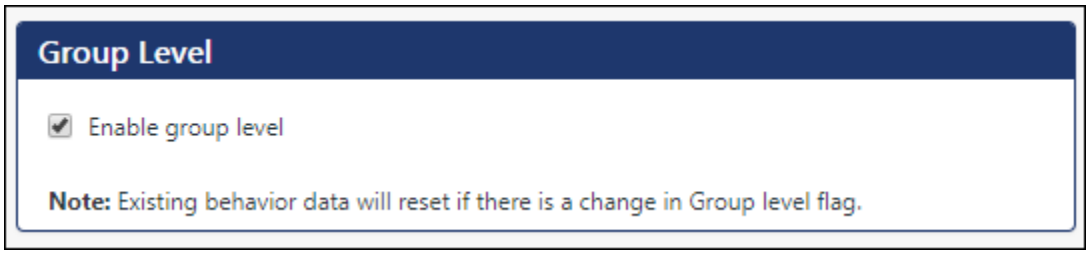

Figure 2

4. Click **OK** to **Save** the changes.

Once the group level gets enabled, you can see the changes in the different EventTracker modules.

A. BEHAVIOR CORRELATION

In **Behavior Correlation**, you can see the **Group** field gets added which will display all the available groups in the drop down list.

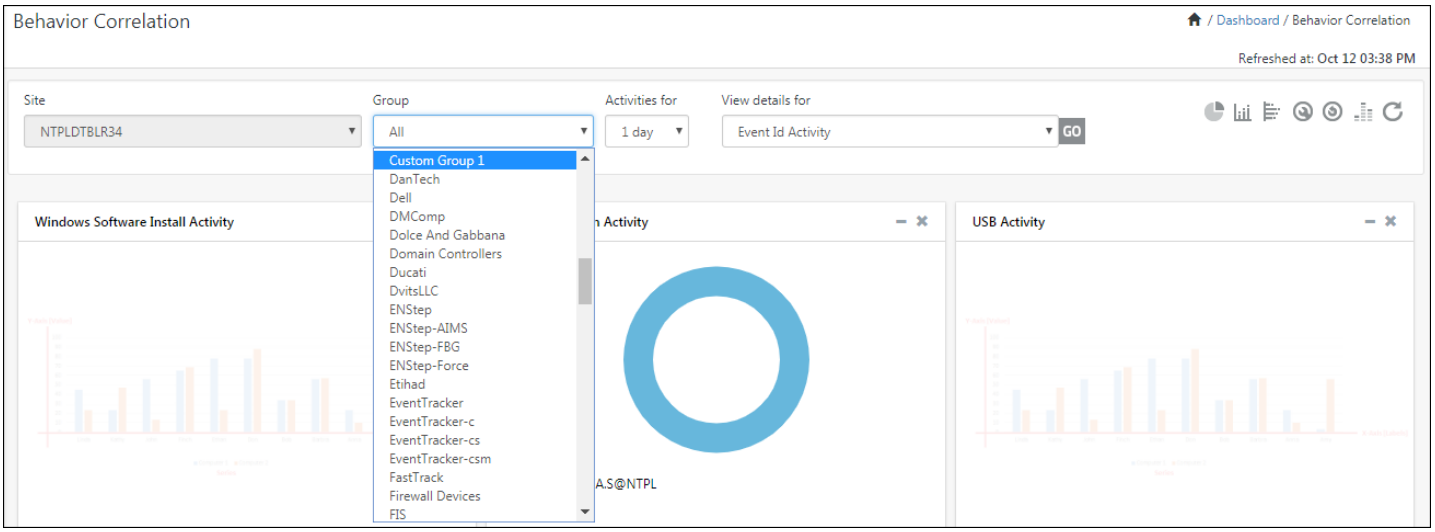

Figure 3

- You can select the desired group and view the details for any Behavior activity.
- It will list the unique event ids for that particular group.

Example 1
Group: **Custom Group 1**
Rule: **Event ID Activity**

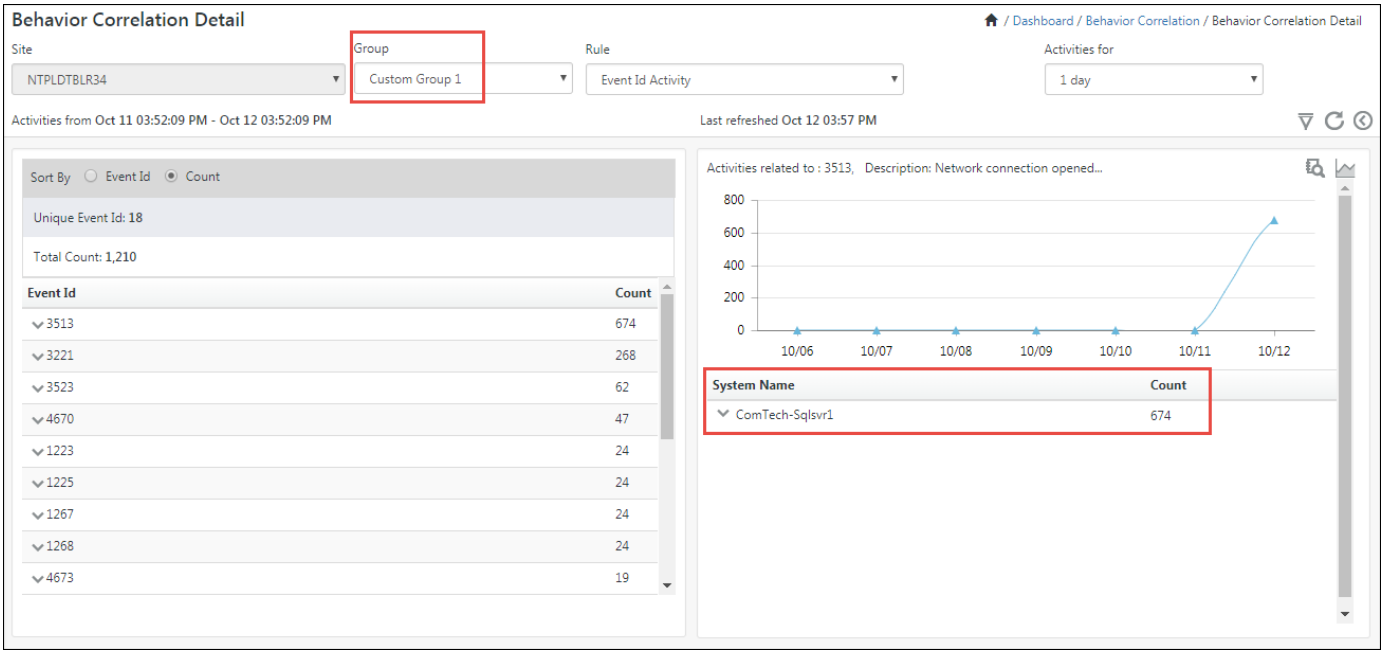

Figure 4

For Windows Applications Activity, it will list the unique application name for that particular group

Example 2

Group: **Custom Group 2**

Rule: **Windows Applications Activity**

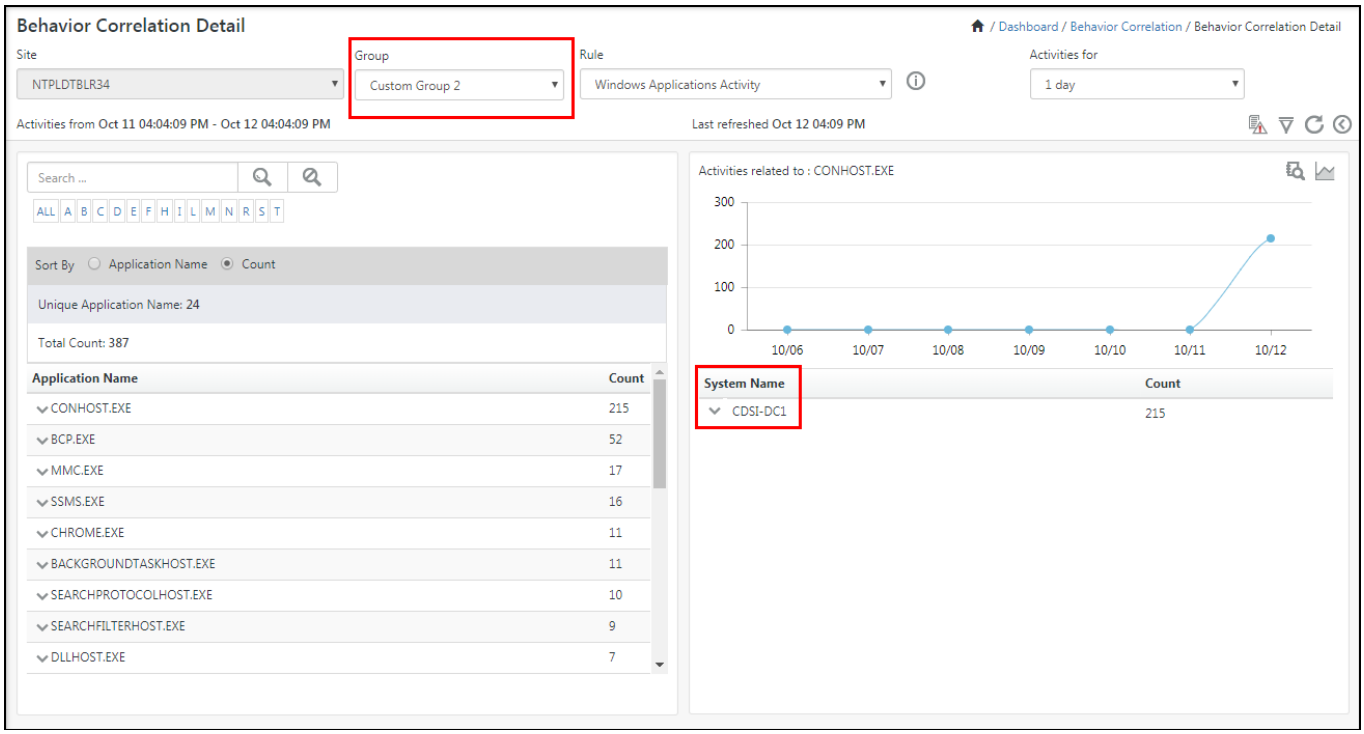

Figure 5

The same functionality applies for the below Modules.

B. THREATS

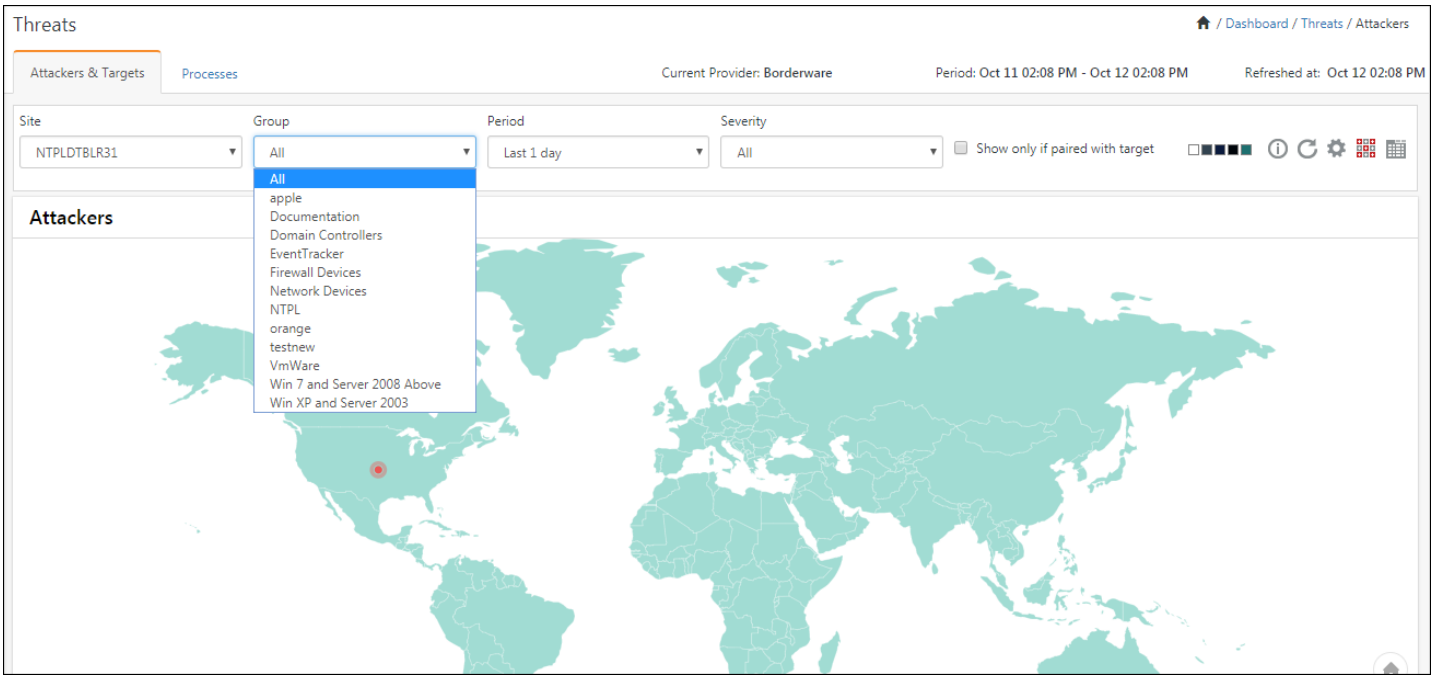

Figure 5

C. UNKNOWN PROCESSES

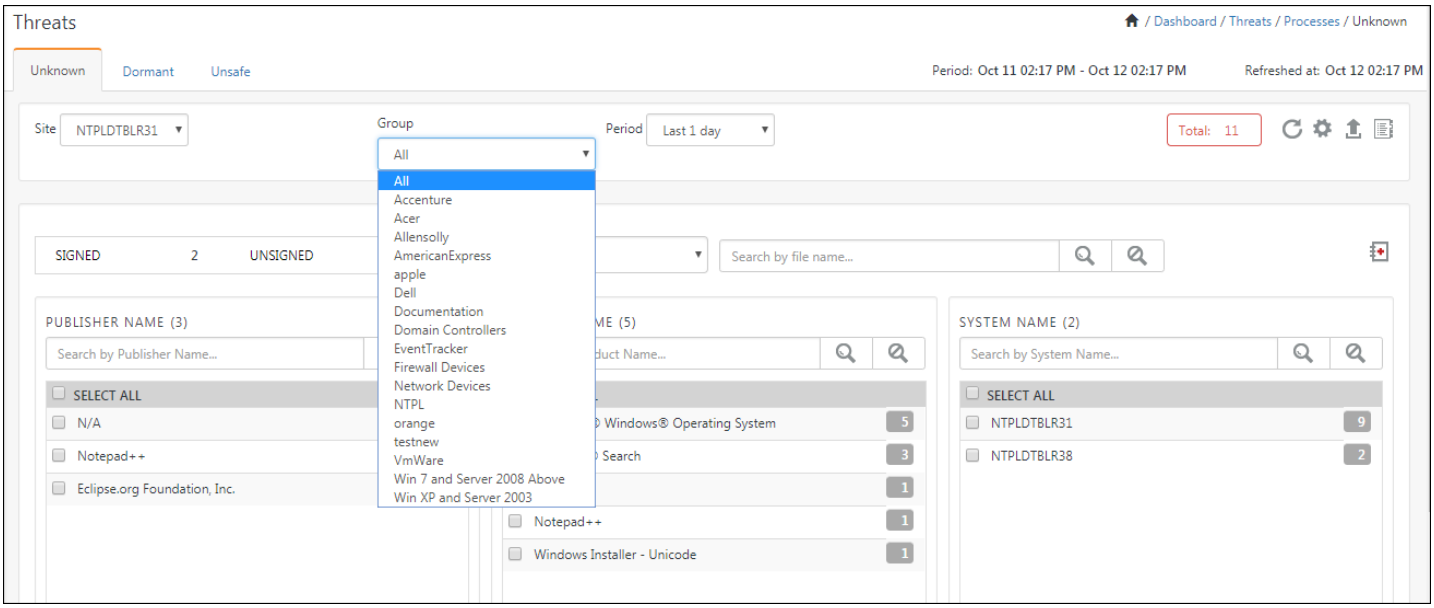

Figure 6

D. SYSTEMS

- In **Admin->Systems, Behavior Correlation** is not considered for the **Default** Group**.**

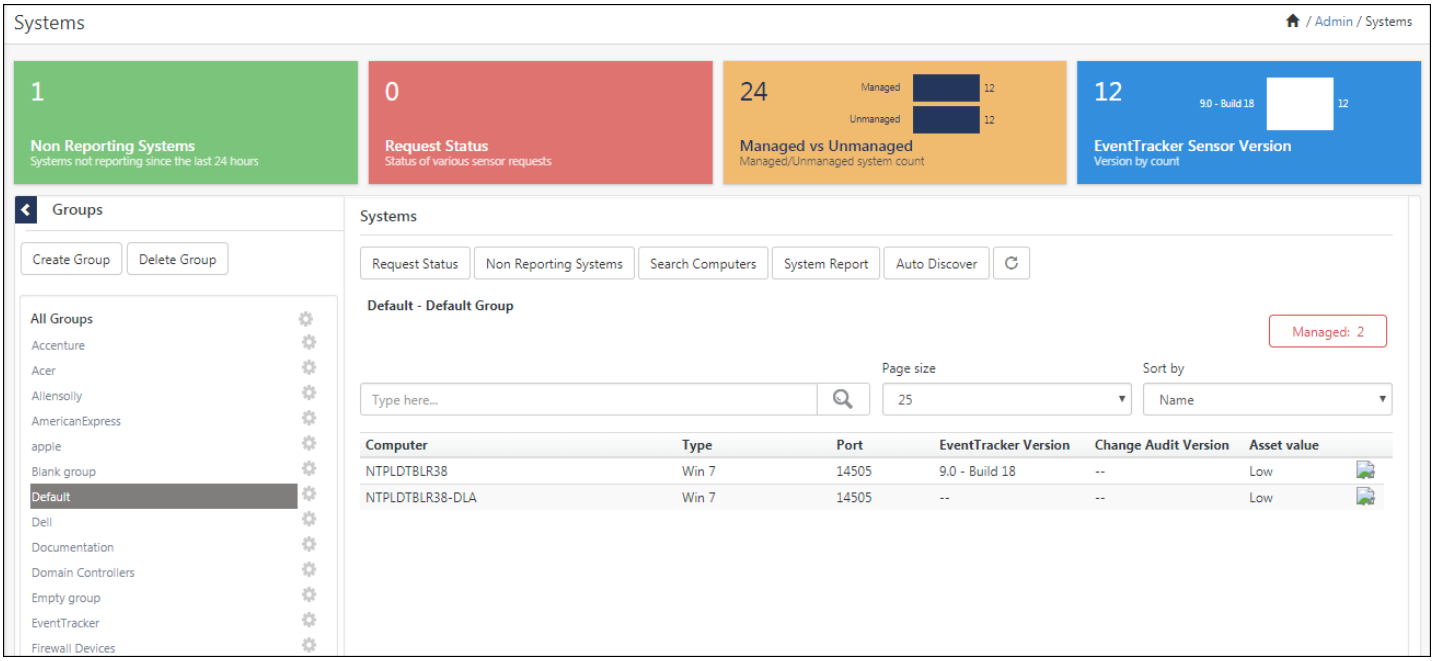

Figure 7

- For any custom group, if you do not wish to consider for behavior correlation,
  - ✓ Click on **Create Group** or modify the existing group by clicking the gear icon and selecting **Edit**.

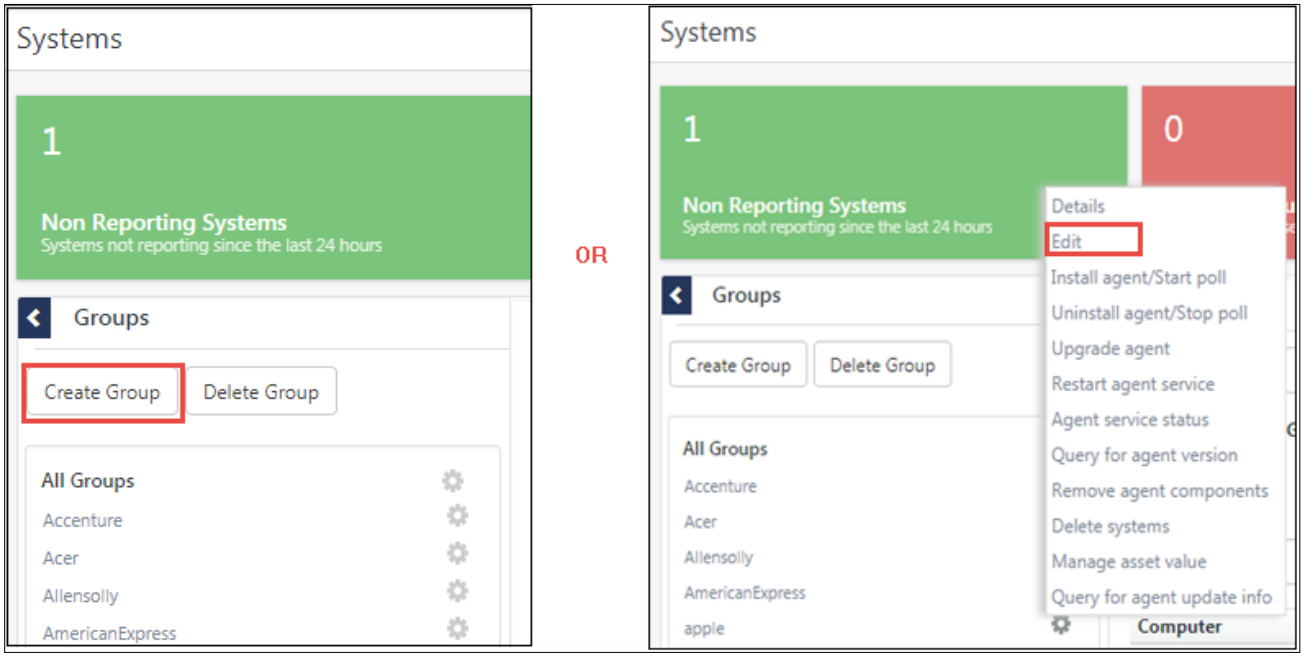

Figure 8

✓ Enable "**Do not consider for behavior correlation**" checkbox.

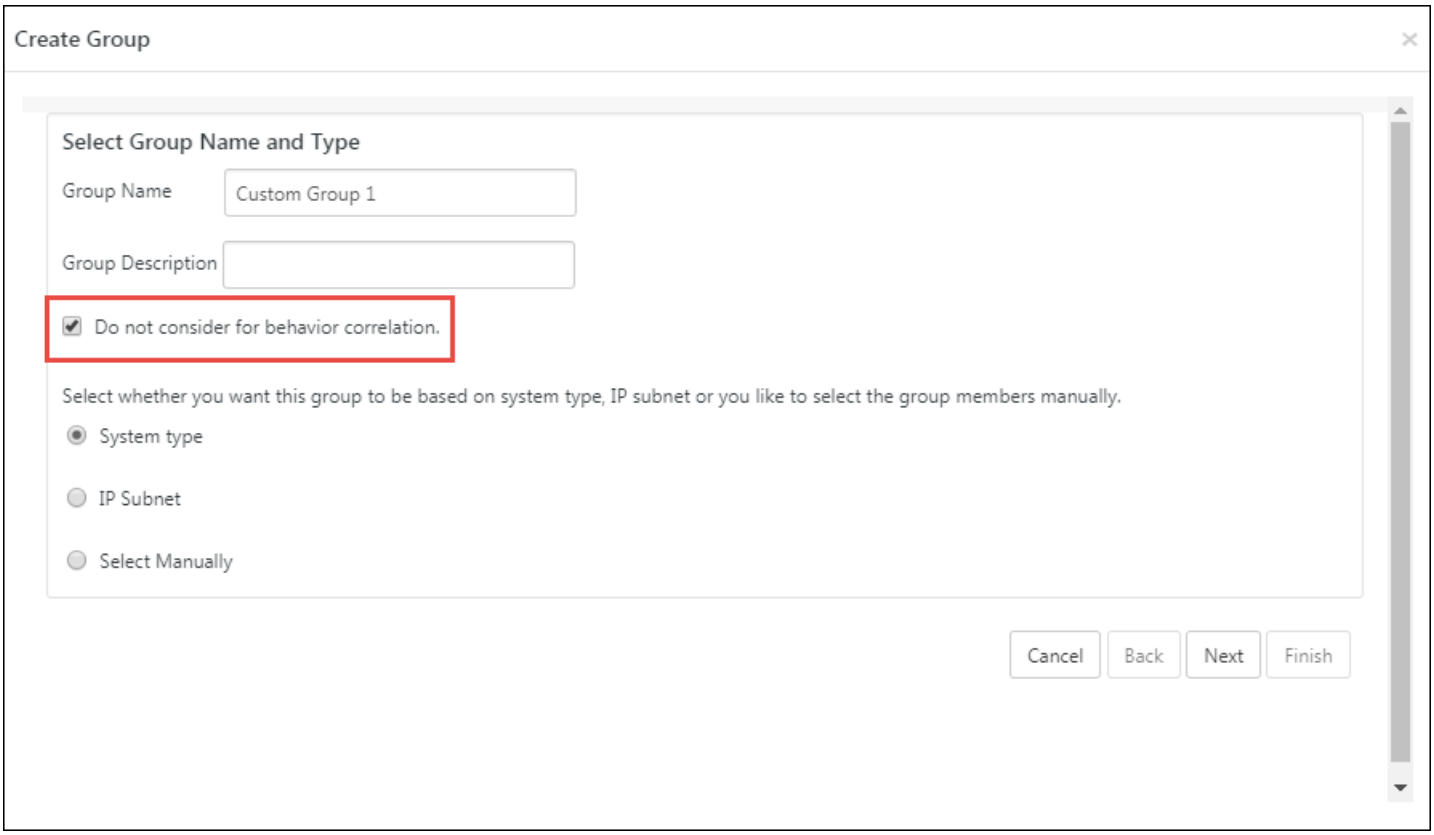

Figure 9

The particular group will not be considered for the Behavior Correlation.

Allow the user to configure the Risk calculation based on Threat Level

Earlier the EventTracker Risk calculation was based on **(TVA) T**hreat, **V**ulnerability, and **A**sset value.

In this update, an option is provided which, if enabled will consider only the **T**hreat level to calculate the risk.

Login to EventTracker web and navigate to **Admin**-> **Manager**.

Under the Alert Events pane, an option has been provided "**Generate alert based only on threat level**". If this particular option is enabled, the risk of an alert will only be considered based on the threat level. Disabling this option will take the earlier behavior into consideration and calculate the risk based on TVA.

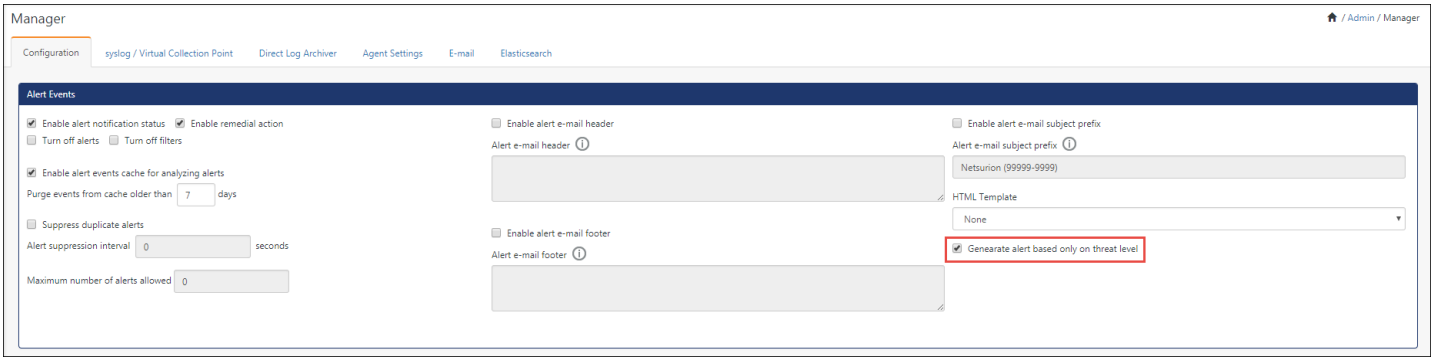

Figure 10

Tile Dashboard: View the tile by risks

In the Tile Dashboard, an option is provided to filter tiles based on risks. The user can select the Risk options available from the dropdown list and get only those tiles in the dashboard.

- Navigate to **Incidents**-> **Tile** View.
- A new option field "**Risk**" is added.

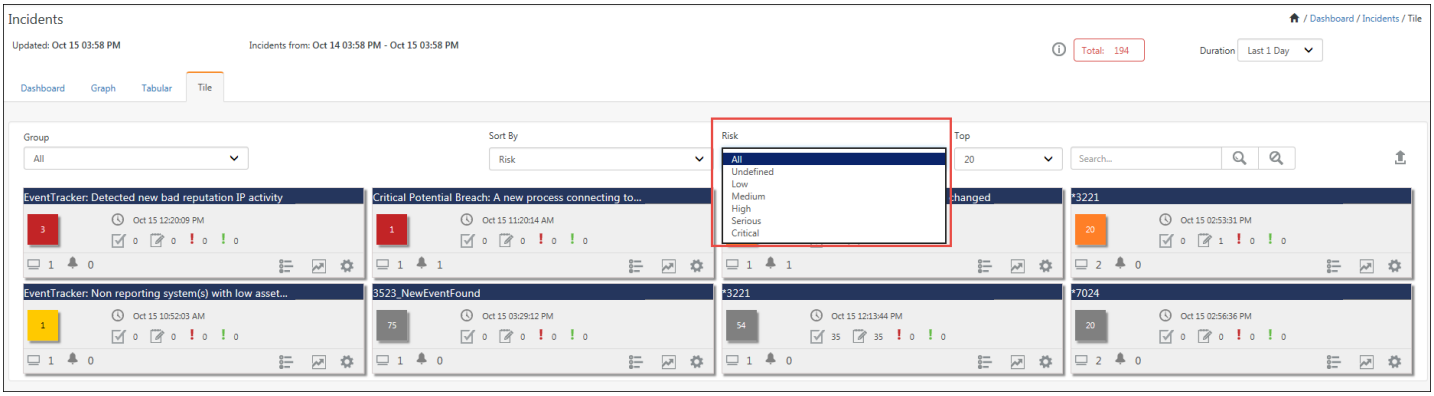

Figure 11

- Select the severity from the dropdown list and it will display only those tiles.

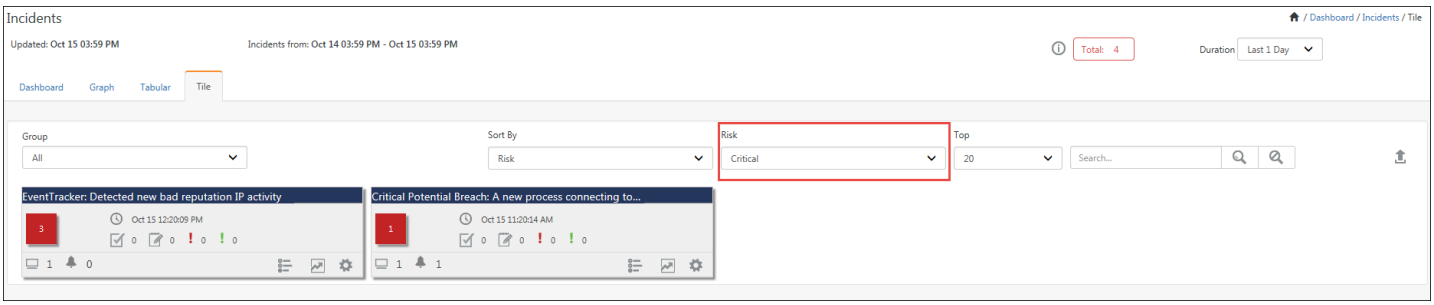

Figure 12

Enable/ Disable Syslog Relay

Earlier, if the EventTracker agents are running with syslog relay configuration then there was no indication in the Manager machine.

To avoid this, now in the System Manager the particular managed agent running with syslog relay configuration displays in green color. This helps the Admin to identify the managed agents with the syslog relay, easily.

Now, the Admin can even configure the syslog relay for any target machine from the System Manager.

- Login to EventTracker and navigate to **Admin**> **Systems.**
- Click the gear icon beside the target system and select "Enable syslog relay" from the dropdown list.

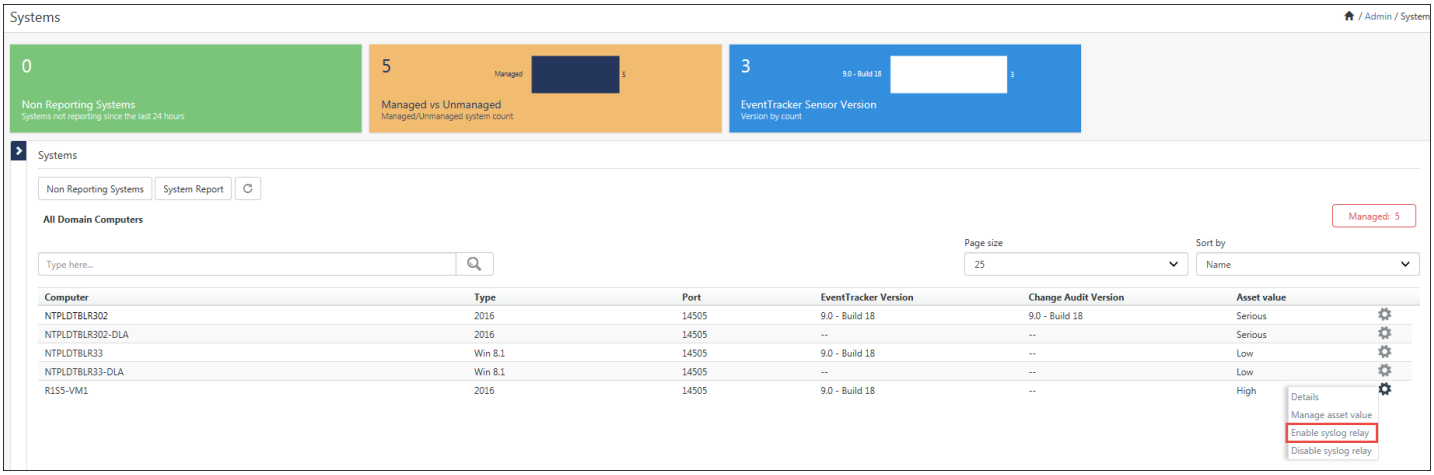

Figure 13

In the Enable syslog relay dialog box, provide the **Regular Expression**, **Protocol** and **Port** and click **OK**.

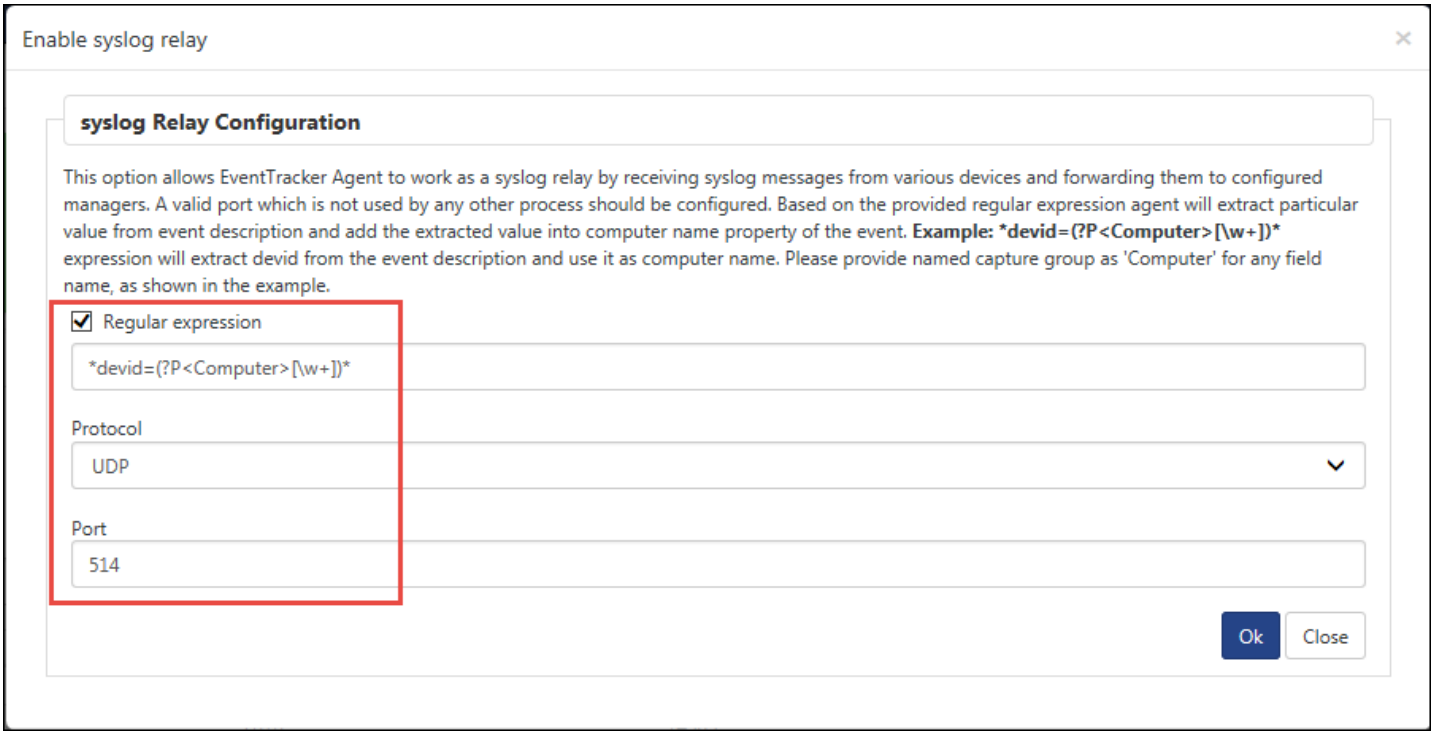

Figure 14

The Target system will turn “Orange” in color. This indicates that still syslog relay is not enabled on the target agent machine.

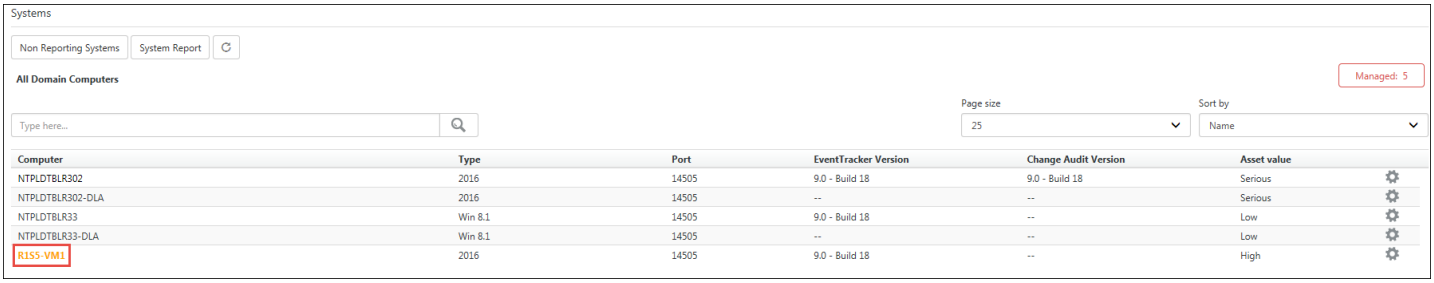

Figure 15

Once the target system turns “Green” in color, it indicates that the syslog relay configuration is successfully enabled on the target agent machine.

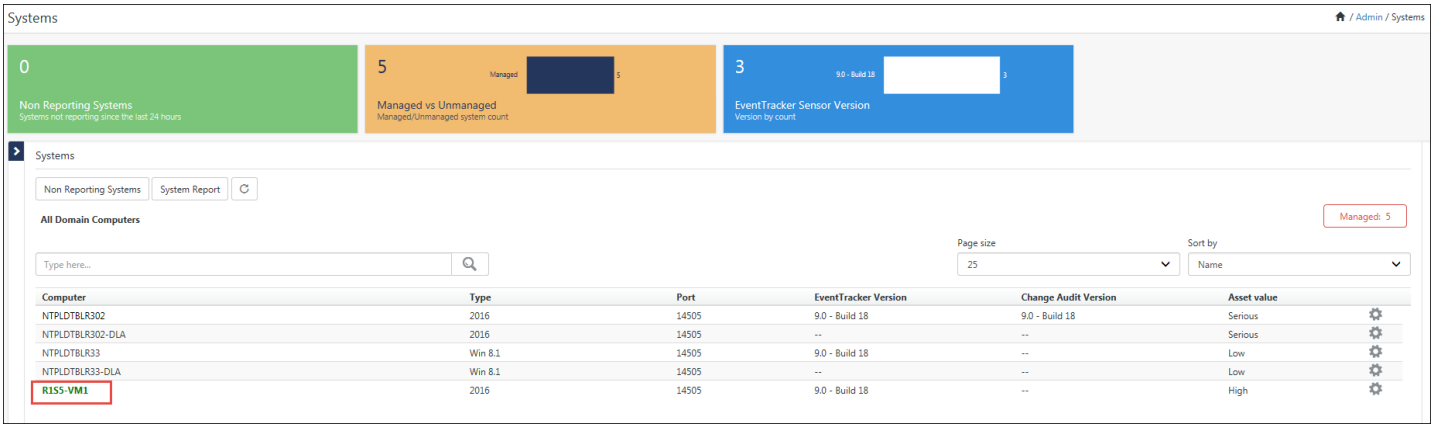

Figure 16

If at any point you wish to disable the syslog relay configuration option, click the gear icon beside the target system and select "**Disable syslog relay**" from the dropdown list.

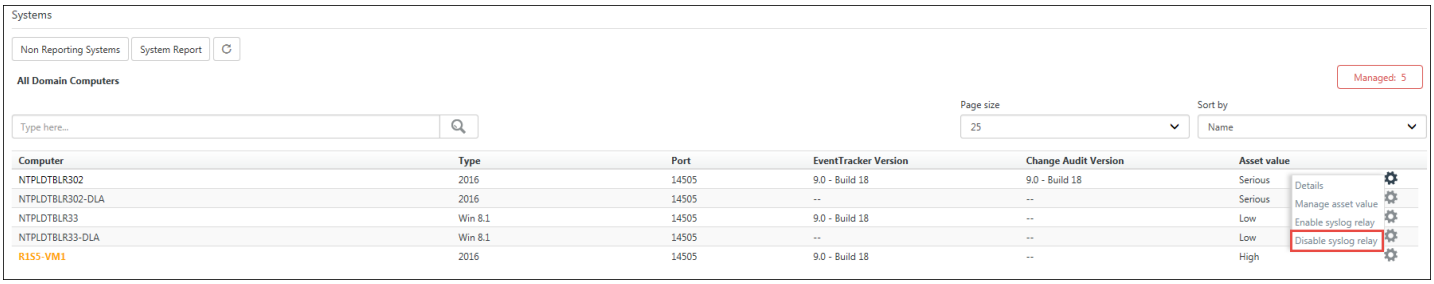

Figure 17

Enabling or Disabling TLS Versions in VMWare

Managing TLS Protocol Configuration with the TLS Configurator Utility

Starting with vSphere 6.7, only TLS 1.2 is enabled, by default. TLS 1.0 and TLS 1.1 are disabled by default. Whether you do a fresh install, upgrade, or migration, vSphere 6.7 disables TLS 1.0 and TLS 1.1. You can use the TLS Configurator utility to enable older versions of the protocol temporarily on vSphere 6.7 systems. You can then disable the older less secure versions after all connections use TLS 1.2.

As part of the process, you can disable TLS 1.0, and enable TLS 1.1 and TLS 1.2. Or, you can disable TLS 1.0 and TLS 1.1, and enable only TLS 1.2.

NOTE:

Starting with vSphere 6.7, the TLS Configurator utility is included in VCenter/VSphere.

You no longer have to download it separately.

If you are not able to find utility then use the below procedure:

Prerequisites

Ensure that the hosts and services that the vCenter Server manages can communicate using a version of TLS that remains enabled. For products that communicate only using TLS 1.0, connectivity becomes unavailable.

1. Login to the vCenter Server system with the username and password for administrator@vsphere.local, or as another member of the vCenter Single Sign-On Administrators group who can run scripts.

2. Go to the directory where the script is located.

Windows:

cd %VMWARE_CIS_HOME%\TlsReconfigurator\VcTlsReconfigurator

Linux:

cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator

3. Run the command, depending on your operating system and on which version of TLS you want to use.

   ✓ To disable TLS 1.0 and enable both TLS 1.1 and TLS 1.2, run the following command.

   Windows:

   directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.1 TLSv1.2

   Linux:

   directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.1 TLSv1.2

   ✓ To disable TLS 1.0 and TLS 1.1, and enable only TLS 1.2, run the following command.

   Windows:

   directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.2

   Linux:

   directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2

4. If your environment includes other vCenter Server systems, repeat the process on each vCenter Server system.

5. Repeat the configuration on each ESXi host and each Platform Service Controller.

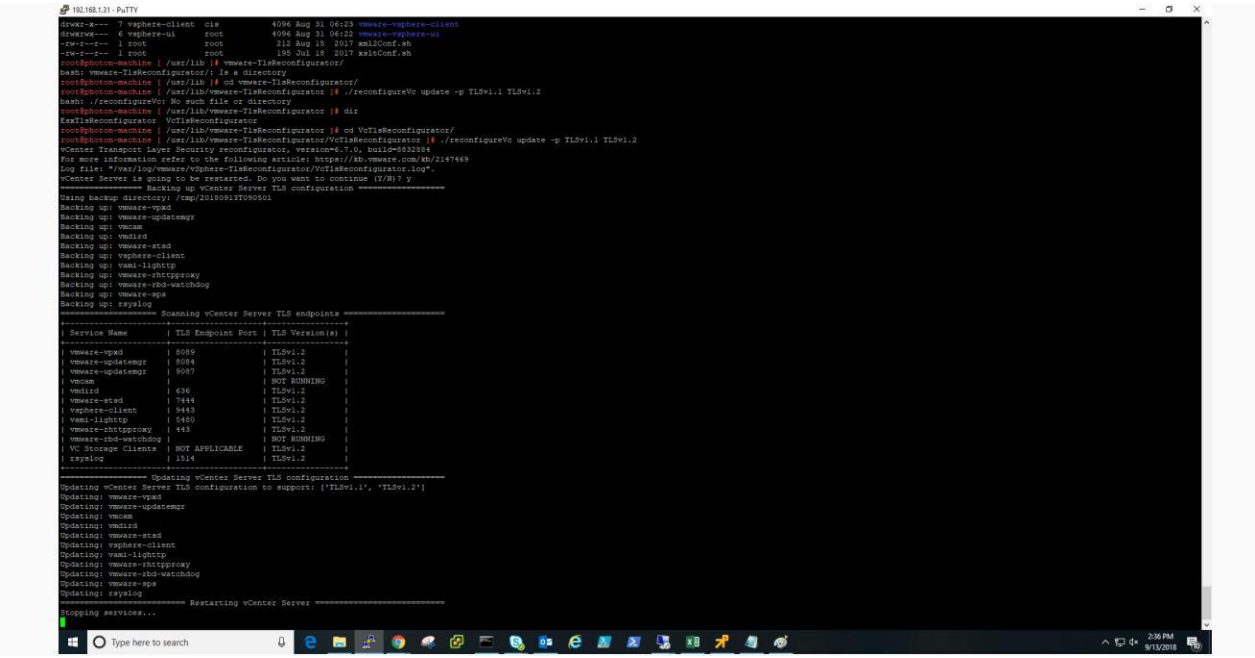

Figure 18 (Before updating TLS Version)

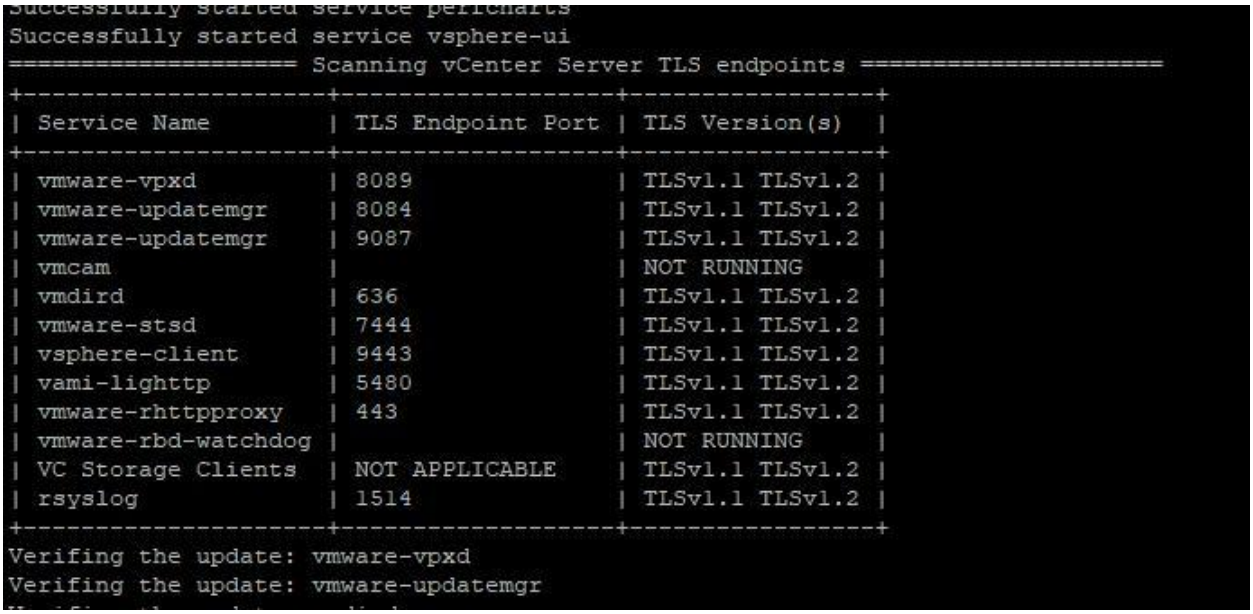

Figure 19 (After updating TLS Version)