Enhancements in syslog Configuration, E-mail Incidents & syslog over TLS

Detailed Document

Publication Date: April 10, 2019
Abstract

This document provides enhancements related to syslog Configuration, E-mail Incidents and syslog over TLS in EventTracker v9.1.

Audience

EventTracker v9.1 user(s) who wish to configure syslog, use the E-mail Incident option and configure syslog over TLS in EventTracker v9.1.
Table of Contents

Abstract ................................................................................................................................. 1
Audience ............................................................................................................................... 1

Support for Multiple Device Extraction ........................................................................... 3
  Allowing multiple Device ID/Name extraction using multiple regular expressions per VCP  ....................................................................................... 3
  Ignore syslog Message if Regular Expression does not match .................................... 5
  Not to Resolve the Sender’s IP Address to Hostname .................................................. 7

E-mail Incident .................................................................................................................... 10

Configure syslog over TLS .............................................................................................. 13
  Pre-requisites .................................................................................................................. 13
  How to create a Client certificate? .................................................................................. 13
  How to generate a Server Certificate? .......................................................................... 15
  How to Configure TLS in the Server Machine? ............................................................ 17
  Rsylog Configuration to forward data from Client to server using certificate .......... 19
  Syslog-ng configuration to forward data from Client to server using certificate .......... 20
Support for Multiple Device Extraction

Allowing multiple Device ID/Name extraction using multiple regular expressions per VCP

An enhancement has been provided for extracting the device ID from syslog device while it is relaying. It will extract multiple device ids or device names that are reporting to the same Virtual Collection Point (VCP) by using multiple regular expressions.

- Login to the EventTracker web console. Navigate to Admin and then Manager.
- Click on syslog/Virtual Collection Point tab.
- Here, you can view the gear icon for each VCP port.

To extract device id/name, provide the regular expression by clicking the gear icon.
- Provide the regular expression and a token name and check the Active option.

Please note that the token name must be same as Named Capture Group.

For example: For this regular expression,

```
.*devid=(?P<Computer>\w-]+).*
```

The token name is “Computer”.

![Figure 1](image.png)
Once you click Add, it gets added. Click the Close button and Save it in Manager Configuration page.

**Figure 2**

<table>
<thead>
<tr>
<th>Regular expression</th>
<th>Token name</th>
<th>VCP port</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>.devid=([P&lt;Computer&gt;[:-]+]</td>
<td></td>
<td></td>
<td>514</td>
</tr>
</tbody>
</table>

**Figure 3**
Once the syslog device starts forwarding the data, the respective device id/name will be extracted based on the provided regular expression.

**In a similar way, you can configure multiple regular expressions for a single/multiple VCP ports.**

Figure 4

Once the device id is extracted, you can see it in the following format.

For example: **FG1K5D3I1480221-syslog**

**Ignore syslog Message if Regular Expression does not match**

1. **In case the** device ID could not be extracted from multiple regular expressions, you can select the checkbox “**Ignore syslog message if regular expression does not match**”, which will ignore the events. You will also not see the device id/name entry in the “System” module.
NOTE: Please note that if you enable “Ignore syslog message if regular expression does not match”, it will consider for all the regular Expression configured for that particular VCP port.
Not to Resolve the Sender’s IP Address to Hostname

1. If the regular expression fails to extract the device id, then if you do not wish to resolve the sender’s IP address to host name, enable the option “Do not resolve sender’s IP address to host name”. By disabling the same option, the IP address will get resolved to host name. You will see the IP Address or Hostname entry in the “System” module depending upon enabling or disabling this option.

2. Even at the VCP level, you can resolve the Sender’s IP Address to hostname. To do this, select the syslog port and click Edit. By default, it will be “Use Global” option under Resolve Hostname.
When you select the “Use Global” option, it will consider the globally enabled or disabled “Do not resolve sender’s IP address to host name” option.

If you select “Resolve IP to Hostname”, it will consider resolving the sender IP to Hostname.

**NOTE:** If the “Resolve IP to Hostname”, is selected at the VCP level and globally you have also selected “Do not resolve sender’s IP address to host name”, it will consider the option selected at the VCP level.
If you select “Do not Resolve IP to Hostname”, it will not resolve the sender IP to Hostname. It will remain as an IP address only.

**NOTE:** If the “Do not Resolve IP to Hostname”, is selected at the VCP level and globally you have also selected “Do not resolve sender’s IP address to host name”, it will consider the option selected at the VCP level.
You will see the IP Address or Hostname entry in the “System’ module depending upon enabling or disabling the option.

E-mail Incident

In this update, enhancement has been provided in the E-mail Incident option under Incident module.

In the e-mail Incident option, the email-ids of those users will be displayed who are having permission to that particular system/group.

From the Incidents Dashboard, click the Email Incident option.
The E-mail Incident window will get displayed.

Clicking the Add icon will display the e-mail ids of the users who have permission to this system/group.

Select the email ids and click OK.
You can also select an E-mail Template from the dropdown options.

**NOTE:** For Collection Point site, only the email-ids of those users will be displayed, who has permission to the Collection Point site/group.
Configure syslog over TLS

Pre-requisites

- Ensure to install the GnuTLS-utils for using the Certtool.

***IMPORTANT: TLS will only support for TCP mode.

How to create a Client certificate?

- Login to the Client Machine (CentOS or UBUNTU).
- Enter the below command:
  `certtool -p --outfile ca.key.pem`
- Enter the credentials to generate RSA private key.
- Next, enter the below command:
  `certtool -s --load-privkey ca.key.pem --outfile ca.crt`
- Next, enter the Common name, the certificate expiry date and the below fields as shown in the figure:

```
Generating a self signed certificate...
Please enter the details of the certificate's distinguished name. Just press enter to ignore a field.
Common name (CN): centos
State or province name (ST): 
Locality name (L): 
Country name (2 chars): US
Enter the subject's domain component (DC): 
This field should not be used in new certificates.
E-mail: 
Enter the certificate's serial number in decimal (default: 6668512171081630735):
```

Activation/Expiration time.
The certificate will expire in (days): 100

Extensions:
- Does the certificate belong to an authority? (y/N): y
- Path length constraints (decimal, -1 for no constraints): -1
- Is this a TLS web client certificate? (y/N): y
- Will the certificate be used for IPsec IKE operations? (y/N): y
- Is this a TLS web server certificate? (y/N): y
- Enter a dNname of the subject of the certificate:
- Enter a URN of the subject of the certificate:
- Enter the IP address of the subject of the certificate:
- Will the certificate be used for signing (DHKE ciphersuites)? (y/N): y
- Will the certificate be used for encryption (RSA ciphersuites)? (y/N): y
- Will the certificate be used to sign OSCP requests? (y/N): y
- Will the certificate be used to sign certificates? (y/N): n
- Will the certificate be used to sign other certificates? (y/N): y
- Will the certificate be used to sign CRLs? (y/N): n
- Will the certificate be used for signing (DHKE ciphersuites)? (y/N): n
Figure 15
It will generate a client certificate with the name `ca.crt`

To verify, whether it got generated or not, please enter the below command:

Is

### How to generate a Server Certificate?

- Enter the below command with your machine name. (Machine name is not mandatory)
  
  In our example, we have taken machine name as “ntpldtblr300”. To generate the RSA private key:

  ```bash
  certtool -p --outfile ntpldtblr300.key.pem
  ```

- To convert pem file to crt file, enter the below command:

  ```bash
  certtool -c --load-privkey ntpldtblr300.key.pem --load-ca-privkey ca.key.pem --load-ca-certificate ca.crt --outfile ntpldtblr300.crt
  ```

- Next, enter the Common name, the certificate expiry date and the below fields as shown in the figure:

- Please mention the server IP Address in the highlighted field.

![Figure 16](image-url)
Now, to convert crt file to pfx file, Enter the below command:

`openssl pkcs12 -export -out ntpldtblr300.pfx -inkey ntpldtblr300.key.pem -in ntpldtblr300.crt`
syslog Configuration, E-mail Incidents & syslog over TLS

- Enter the Export password to use the server certificate.
- To verify, whether the certificate got generated or not, please enter the below command:

```bash
ls
```

Figure 18

**NOTE:** Please export the certificate file (.pfx file) in the Server machine. If the user is not able to export the certificate file, give Read and Write permission to export the file as shown below:

```bash
chmod a+rw ntpldtblr300.pfx
```

### How to Configure TLS in the Server Machine?

1. Login to the EventTracker web and then navigate to Admin and then Manager Configuration.
2. Go to syslog/Virtual Collection Point tab.
3. In the syslog pane, click Add.
4. In syslog Receiver port window, enter the Port number and then Enable TLS.
5. Provide the common name of the server certificate and then browse the path for the pfx certificate file.
6. Give the password, which was provided while exporting the certificate.
Figure 19

7. Click on **Save**.
Rsyslog Configuration to forward data from Client to server using certificate

- Login to the CentOS or UBUNTU client machine.
- Install rsyslog-gnutls
- Type the below command to configure rsyslog

```bash
vi /etc/rsyslog.conf
```

- Enter the password and the rsyslog configuration will display.
- Enter the below commands to enable the TLS.

```bash
$DefaultNetstreamDriverCAFile /etc/rsyslog.d/keys/ca.crt
$DefaultNetstreamDriverCertFile /etc/rsyslog.d/keys/ca.d/79.crt
$DefaultNetstreamDriverCertFile /etc/rsyslog.d/keys/ca.d/927.crt
$DefaultNetstreamDriver gtls # use gtls netstream driver
$ActionSendStreamDriverAuthMode 1 # require TLS for the connection
$ActionSendStreamDriverAuthMode anon # server is NOT authenticated
$ActionSendStreamDriverAuthMode x509/certvalid
$ActionSendStreamDriverAuthMode x509/name
```

- Please enable the following commands to communicate through TLS.

```bash
$DefaultNetstreamDriver gtls # use gtls netstream driver
$ActionSendStreamDriverMode 1 # require TLS for the connection
$ActionSendStreamDriverAuthMode anon # server is NOT authenticated
```

- Now, provide the IP address of the server and the port number to forward the data from client to server. An example is shown below:

```bash
.* @@remote-host:514
```

Figure 20

Figure 21
Syslog-ng configuration to forward data from Client to server using certificate

- Login to the CentOs or UBUNTU client machine.
- Type the below command to configure syslog-ng

```bash
vi /etc/syslog-ng/syslog-ng.conf
```

- Now enter the password and the syslog-ng configuration will display.
- To forward data client to server, provide the IP address and the port number.
- For enabling TLS, enter the command shown below:

```bash
tls(peer_verify(optional-untrusted) ca_dir("/etc/rsyslog.d/keys/ca.crt"));
```

Figure 22

- To map the source configuration with destination, provide the below command:

```bash
log { source(s_src); destination(d_net);};
```