Abstract

This document provides information related to syslog over TLS configuration in EventTracker v9.1 and above.

Audience

EventTracker v9.1 and above user(s) who wish to configure syslog over TLS.
# Table of Contents

1. Configuring syslog over TLS using Self Signed Certificate
   1.1 Generating a Certificate on Windows Server
   1.2 Exporting the Certificate
   1.3 Configuring TLS in the Server Machine

2. Configuring syslog over TLS using certificate issued by trusted CA
   2.1 Pre-requisites
   2.2 Creating a Client Certificate
   2.3 Generating a Server Certificate
   2.4 Configuring TLS in the Server Machine
   2.5 Rsyslog Configuration to forward data from Client to server using Certificate
   2.6 Syslog-ng configuration to forward data from Client to server using Certificate
1. Configuring syslog over TLS using Self Signed Certificate

1.1 Generating a Certificate on Windows Server

1. Open the Windows powershell in the Admin mode
   
   (To do that right click on the powershell icon and choose run as administrator)
   
   The powershell window appears.

2. Execute the following command.
   
   ```powershell
   New-SelfSignedCertificate -dnsname "Full name of Manager/Server" -CertStoreLocation cert:\LocalMachine\My
   
   (Example: New-SelfSignedCertificate -dnsname "ETTVMBLR22012-3.ntpl.local" -CertStoreLocation cert:\LocalMachine\My)
   ```

   ![Figure 1](image)

   **Note:** Save the subject name (marked in the above figure) after executing. This subject name is used while configuring syslog over TLS in the server machine.

3. Open **Run** (Click clt + R)
4. Type in **mmc** and Click **OK**.

   **Console1 – [Console Root] window opens.**

   **Note:** If the **User Access Control pop up** appears click yes to proceed.
5. Click **File→Add/Remove Snap-in**

![Figure 3](image-url)
6. **Add/Remove Snap-ins** window opens. Choose Certificates from the **Available snap-ins** and click **Add**.

![Figure 4](image)

7. **Certificates snap-in** window appears. Choose Computer account option and click **Next**.

![Figure 5](image)
8. **Select computer** window appears, Local computer option is selected by default. Click **Finish**.

   ![Figure 6](image)

9. Certificates is added to the Selected snap-ins, Click **Ok**.

   ![Figure 7](image)
10. You will see Certificates icon in the Console1 window. Double click the Certificates icon.

Figure 8

11. Double click on personal folder.

Figure 9
12. Under **Console Root Folder** in the **Left pane**. Click to expand **Personal folder** and choose **Certificate folder**. The certificates are seen in the **Right pane**.

![Figure 10](image)

### 1.2 Exporting the Certificate

1. Right click on the certificate which was created after executing the **PowerShell** command.
2. Choose All Task-> Export.

![Figure 11](image)
3. Certificate Export Window appears. Click **Next**

![Certificate Export Wizard](image1)

*Figure 12*

4. Choose the option “Yes, Export the private key” to export the private key and click **Next**.

![Certificate Export Wizard](image2)

*Figure 13*
5. Click Next on the default settings

![Certificate Export Wizard](image1.png)

Figure 14

6. Enable the check box password, enter the password
7. Click Next.

**Note:** While configuring the syslog over TLS on the server side, provide the password set.

![Certificate Export Wizard](image2.png)

Figure 15
8. Click **Browse** to browse the location where you want to export the certificate and Click **Save**.

![Figure 16](image)

9. **Completing the Certificate Export** Wizard appears. Click **Finish**.

![Figure 17](image)
10. The Export was Successful message appears. Click Ok.

![Certificate Export Wizard]

Figure 18

1.3 Configuring 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 subject name of the server certificate. This should be same as what is provided in section 1.1 as subject name.
6. Browse the path for the pfx certificate file.
7. Provide the password, which was used while exporting the certificate.
8. Click **Save**.
2. Configuring syslog over TLS using certificate issued by trusted CA

2.1 Pre-requisites

The GnuTLS-utils should be installed, for using the Certtool.

IMPORTANT: TLS supports only TCP mode.

2.2 Creating a Client Certificate

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

   ```
   certuser@Belse-VMS:~# certtool -s --load-privkey ca.key.pem --outfile ca.crt
   Generating a self signed certificate...
   Please enter the details of the certificate's distinguished name. Just press enter to ignore a field.
   Common name: centos
   OID:
   Organizational unit name:
   organization name:
   locality name:
   State or province name:
   Country name (2 chars):
   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: 6668512171081630733):
   
   Activation/Expiration time.
   The certificate will expire in (days): 100
   
   Extensions.
   Does the certificate belong to an authority? (y/N): y
   Path length constraint (decimal, -1 for no constraint): -1
   Is this a TLS web client certificate? (y/N): y
   Will the certificate be used for IKE operations? (y/N): y
   Is this a TLS server certificate? (y/N): y
   Enter a name of the subject of the certificate:
   Enter the name of the subject of the certificate:
   Enter the IP address of the subject of the certificate:
   Will the certificate be used for signing (DHE cipher suites)? (y/N): y
   Will the certificate be used for encryption (RSA cipher suites)? (y/N): y
   Will the certificate be used to sign IKE requests? (y/N): y
   Will the certificate be used to sign IKE? (y/N): n
   Will the certificate be used for time stamping? (y/N): n
   Will the certificate be used for email protection? (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 (DHE cipher suites)? (y/N): n
   ```
Syslog over TLS Configuration

Figure 20
It will generate a client certificate with the name **ca.crt**

To verify, enter the command: `ls`

### 2.3 Generating a Server Certificate

1. 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:
   ```
   certtool -p --outfile ntpldtblr300.key.pem
   ```

2. To convert pem file to crt file, enter the below command:
   ```
   certtool -c --load-privkey ntpldtblr300.key.pem --load-ca-privkey ca.key.pem --load-ca-certificate ca.crt --outfile ntpldtblr300.crt
   ```

3. Enter the Common name, the certificate expiry date and the below fields as shown in the figure:

4. Mention the server IP Address in the highlighted field.

![Figure 21](image)
5. Now, to convert crt file to pfx file, enter the below command:

```bash
openssl pkcs12 -export -out ntpldtblr300.pfx -inkey ntpldtblr300.key.pem -in ntpldtblr300.crt
```
6. Enter the Export password to use the server certificate.
7. To verify, enter the command: `ls`

![Command output](image)

**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:

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

### 2.4 Configuring 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. Provide the password, which was used while exporting the certificate.
2.5 Rsyslog Configuration to forward data from Client to server using Certificate

1. Login to the CentOS or UBUNTU client machine.
2. Install rsyslog-gnutls
3. Type the below command to configure rsyslog
   ```
   vi /etc/rsyslog.conf
   ```
Syslog over TLS Configuration

4. Enter the password and the rsyslog configuration opens.
5. Enter the below commands to enable the TLS.

```bash
$DefaultNetstreamDriverCAFile /etc/rsyslog.d/keys/ca.crt
$DefaultNetstreamDriverCertFile /etc/rsyslog.d/keys/ca.d/78.crt
$DefaultNetstreamDriverConfigFile /etc/rsyslog.d/keys/ca.d/9277.crt
$DefaultNetstreamDriver gtls # use gtls netstream driver
$ActionSendStreamDriverMode 1 # require TLS for the connection
$ActionSendStreamDriverAuthMode anon # server is NOT authenticated
$ActionSendStreamDriverAuthMode x509/cert/valid
$ActionSendStreamDriverAuthMode x509/name
```

**Figure 25**

6. Enable the following commands to communicate through TLS.

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

7. 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 26**

### 2.6 Syslog-ng configuration to forward data from Client to server using Certificate

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

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

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

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

```
destination d_net {
    tcp("172.28.100.52" port(514)
    tls(peer_verify(optional-untrusted) ca_dir("/etc/rsyslog.d/keys/ca.crt")));
};
```

Figure 27

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

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