

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 sylog 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.

The information contained in this document represents the current view of Netsurion. on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2019 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



Table of Contents

	Abstract	1
	Audience	1
Su	pport for Multiple Device Extraction Allowing multiple Device ID/Name extraction using multiple regular expressions per VCP	3 3
	Ignore syslog Message if Regular Expression does not match	5
	Not to Resolve the Sender's IP Address to Hostname	7
E-I	mail Incident	10
Co	onfigure syslog over TLS Pre-requisites	13 13
	How to create a Client certificate?	13
	How to generate a Server Certificate?	15
	How to Configure TLS in the Server Machine?	17
	Rsyslog Configuration to forward data from Client to server using certificate	19
	Syslog-ng configuration to forward data from Client to server using certificate	20

Netsurion... EventTracker

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.

М	anager 🏦 / Admin / Manager							
	Configuration Systed / Virtual Collection Point Direct Log Archiver Agent Settings E-mail Collection Master Ports Elasticsearch							
	ayabag							
☑ Enable syslog receiver 🔲 Do not resolve sender's IP address to host name			Total available: Unlimited					
	Port number	Description	Cache path	Purge frequency (days)	Archive path			
	514	All Syslog Systems (UDP)	C:\Program Files (x86)\Prism Microsystems\EventTracker\Cache	0	C\Program Files (x86)\Prism Microsystems\EventTracker\Archives	\$		
	515	Custom syslog port	C:\Program Files (x86)\Prism Microsystems\EventTracker\Cache	1	C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives	0		
						Add Edit Remove		



- 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".

Netsurion. EventTracker

Extract device id from syslog device	25		>
Port number: 514 Note: Adding multiple Regular Expression for extra	cting device id or name may cause the Ever	ntTracker Receiver performance o	legradation.
Regular expression	Token name	VCP port	Active
			Delete
Regular expression (i)			
.*devid=(?P <computer>[\w\-]+).*</computer>			
Token name 🛈			
Computer	Active Igna	ore syslog message if regular ression does not match	
			Add Clear Close

Figure 2

Once you click Add, it gets added. Click the Close button and Save it in Manager Configuration page.

Token name	VCP port	Active
Computer	514	V
		Delete
	Computer	Computer 514

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.

ort number: 514 ote: Adding multiple Regular Expression for extra	cting device id or name may cause the Eve	ntTracker Receiver performance d	egradation.
egular expression	Token name	VCP port	Active
devid=(?P <computer>[\w]+).*</computer>	Computer	514	
devname=(?P <system>[\w\-]+).*</system>	System	514	
logid=(?P <computer>[\w]+).*</computer>	logid	514	<i>«</i>
			Delet
Regular expression (i)			

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

 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.

Netsurion... EventTracker

ort number: 514 ote: Adding multiple Regular Expression for extr	acting device id or name may cause the Even	tTracker Receiver performance d	egradation.
egular expression	Token name	VCP port	Active
devid=(?P <system>[\w\-]+).*</system>	System	514	
			Delet
.*devid=(?P <system>[\w\-]+).*</system>			
oken name (j)			

Figure 5

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.



		-graaten -
Token name	VCP port	Active
Computer	514	
System	514	Image: A start of the start
logid	514	
		Delet
		Delet
		Delet
	Computer System logid	Computer 514 System 514 logid 514



Not to Resolve the Sender's IP Address to Hostname

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.

Μ	Aanager 🔶 🛧 / Admin / Manager						
	Configuration syslog /	Virtual Collection Point Direct Log	Archiver Agent Settings E-mail Collection Master Ports Ela	asticsearch			
	syslog						
		s to host name			Total available: Unlimited		
	Port number	Description	Cache path		Purge frequency (days)	Archive path	
	514	All Syslog Systems (UDP)	C:\Program Files (x86)\Prism Microsystems\EventTracker\Cache		0	C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives	\$
	515	Custom syslog port	C:\Program Files (x86)\Prism Microsystems\EventTracker\Cache		1	C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives	\$
							Add Edit Remove



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.

syslog Receiver Port	×			
Port Number				
514				
Description				
All Syslog Systems (UDP)				
Cache Path				
C:\Program Files (x86)\Prism Microsystems\EventTracker\Cache Browse				
Note: Configuring cache path on different disk drive(s) would help in enhancing the application performance.				
Purge archives older than 0 days				
Enable TLS				
Resolve Hostname				
Use global 🔻				
Raw syslog forward:				
Select a destination and port to which all the incoming events will be forwarded as raw syslog messages.				
Trap Destination (IP Address or host name)				
Mode: UDP TCP				
UDP Port				
Save				



• 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.

syslog Receiver Port	\times				
Port Number					
514					
Description					
All Syslog Systems (UDP)					
Cache Path					
C:\Program Files (x86)\Prism Microsystems\EventTracker\Cache Browse					
Note: Configuring cache path on different disk drive(s) would help in enhancing the application's performance.					
Purge archives older than 0 days					
Enable TLS					
Resolve Hostname					
Resolve IP to Hostname 🔻					
Raw syslog forward:					
Select a destination and port to which all the incoming events will be forwarded as raw syslog messages.					
Trap Destination (IP Address or host name)					
Mode: UDP TCP					
UDP Port					
Save					



 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.



syslog Receiver Port
Port Number
514
Description
All Syslog Systems (UDP)
Cache Path
C:\Program Files (x86)\Prism Microsystems\EventTracker\Cache Browse
Note: Configuring cache path on different disk drive(s) would help in enhancing the application's performance.
Purge archives older than 0 days
Enable TLS
Resolve Hostname Do not Resolve IP to Hostname
Raw syslog forward: Select a destination and port to which all the incoming events will be forwarded as raw syslog messages.
Trap Destination (IP Address or host name)
Mode: UDP TCP
UDP Port
Save Cancel



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.



Incidents					🕈 / Dashboard / Incidents / Tabula
Updated: Apr	09 02:12 PM	Incidents from	: Apr 08 02:12 PM - Apr 09 02:12 PM	٥	Total: 1 Duration Last 1 day 🔻
Dashboard	Graph Tabular Tile				
Site ()		Group		Sort By Flag	Show
R1S5-VM	M11[172.28.9.145]	• All	•	Time • All	▼ Unacknowledged ▼
< 1	of 1 💊 GO				Q, Ack
+	Date/Time	Event Id	Site/Computer	Incident Name	Ack
+	Apr 09 01:01:30 PM	♥ 3201	√R155-VM11[172289.145] / <mark>R155-VM11</mark>	Disk space is critically low on EventTracker server	Copy to notepad Add to casebook Add notes



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.

Send Incider	nt via e-mail	
To:		⊕ Ü
Cc:		⊕ 🗓
	-Use comma(,) to separate multiple e-mail recipients.	
Subject:	Alert from NTPLDTBLR81 - EventTracker: New Unique Process Hash A	
Message:	Date: Apr 09 01:24:15 PM Incident No: 201904011369 Acknowledge status: Unacknowledged Notes: Event Id: 2040 System: NTPLDTBLR81 Source: EventTracker User: SYSTEM	
Email template:	AlertEmailTemplate-Short.htm	
	Send Close	

Figure 12

Select the email ids and click OK.



Email addresses		×
Search email address	Q	Q
 test@eventtracker.com Test2@eventtracker.com 		
< Page 1 of 1 >		
		Ok



You can also select an E-mail Template from the dropdown options.

Send Incider	nt via e-mail	
		0.5
To:		(+)
Cc:		🛨 🗓
	-Use comma(,) to separate multiple e-mail recipients.	
Subject:	Alert from NTPLDTBLR81 - EventTracker: New Unique Process Hash A	
	Date: Apr 09 01:24:15 PM	
	Incident No: 201904011369	
	Notes	
Message:	Event Id: 2040	
	System: NTPLDTBLR81	
	Source: EventTracker	
	User: SYSTEM	
Email template:	AlertEmailTemplate-Short.htm	R
	None	15
	AlertEmailTemplate-Short.htm	
	DefaultAlertEmailTemplate.htm	



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:

```
estuser1@R1S6-VM3:~$ sudo certtool -s --load-privkey ca.key.pem --outfile ca.cr
Generating a self signed certificate...
Please enter the details of the certificate's distinguished name. Just press ent
er to ignore a field.
common name: centos
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: 6668512171081630735):
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 IPsec IKE operations? (y/N): y
Is this a TLS web server certificate? (y/N): y
Enter a dnsName of the subject of the certificate:
Enter a URI of the subject of the certificate:
Enter the IP address of the subject of the certificate:
Will the certificate be used for signing (DHE ciphersuites)? (Y/n): y
Will the certificate be used for encryption (RSA ciphersuites)? (Y/n): y
Will the certificate be used to sign OCSP requests? (y/N): y
Will the certificate be used to sign code? (y/N): n
Will the certificate be used for time stamping? (\gamma/N): n
Will the certificate be used for email protection? (\gamma/\mathbb{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 ciphersuites)? (Y/n): n
```

```
CRL distribution point
       the URI of
.509 Certificate Information:
        Version: 3
        Serial Number (hex): 5c8b507d01b0840f
        Validity:
                Not Before: Fri Mar 15 07:13:01 UTC 2019
                Not After: Sun Jun 23 07:13:29 UTC 2019
        Subject: CN=centos
        Subject Public Key Algorithm: RSA
Algorithm Security Level: High (3072 bits)
                Modulus (bits 3072):
                        00:c8:a2:3d:a3:8e:16:88:ea:fa:bb:a4:99:d8:65:73
                         29:d2:ea:06:08:9e:74:d1:81:d9:8c:38:91:11:04:b2
                         4e:49:e7:59:5a:bd:16:08:0a:62:fe:7c:d9:3f:59:b1
                         92:fa:70:f4:c6:18:4c:4b:bd:bc:ed:28:54:3f:17:cc
                         ld:f6:fc:b5:62:73:6d:75:a8:99:20:6f:72:38:1a:ed
                         b1:fd:17:b1:a0:48:5f:74:bc:1b:57:ae:61:2e:2c:9d
                         28:62:5d:51:bb:3a:aa:3d:30:bd:ed:46:db:bd:22:17
                         a7:1b:10:e6:d8:b9:8d:d9:0c:d6:a7:74:b5:fc:c6:c7
                         92:df:d1:c2:83:b9:fe:18:dc:22:95:79:eb:62:c7:3d
                Exponent (bits 24):
                        01:00:01
        Extensions:
                Basic Constraints (critical):
                        Certificate Authority (CA): TRUE
                Key Purpose (not critical):
                        TLS WWW Client.
                         TLS WWW Server.
                        Ipsec IKE.
                        OCSP signing.
                Key Usage (critical):
                        Digital signature.
                        Non repudiation.
                        Key encipherment.
                        Certificate signing.
                Subject Key Identifier (not critical):
                         68c405e1b3bad5401735d171866f19cf3636acf3
Other Information:
        Public Key ID:
                sha1:68c405e1b3bad5401735d171866f19cf3636acf3
                sha256:7c76087403747884bffb9dfe2665aec8e42f7758f92eb465c7b101bcd
936c89
        Public Key PIN:
                pin-sha256:fHYIdAN0eIS/+53+JmWuy0Qvd1j5LrRlx7EBvNyTbIk=
        Public key's random art:
                +--[ RSA 3072]---
                       = S
s the above information ok? (v/N): v
Signing certificate.
```

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:

ls

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:

certtool -p --outfile ntpldtblr300.key.pem

• 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

- 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



```
Certificate Information
        Version: 3
        Serial Number (hex): 5c8b545a09bc49c9
        Validity:
                 Not Before: Fri Mar 15 07:29:30 UTC 2019
        Subject: CN=ntpldtblr300
        Subject Public Key Algorithm: RSA
                 Modulus (bits 3072):
                          00:f1:6f:33:49:20:01:2b:68:20:46:ae:30:94:66:f6
                           f6:b7:67:9e:ce:7b:77:bd:c0:98:f8:ef:04:b9:18:3c
1b:24:37:e7:d2:81:68:b4:36:ee:55:67:17:2a:87:13
                           fd:c0:30:ec:66:f6:db:68:86:d9:1c:60:3c:5c:af:b1
                           02:60:32:c6:69:6b:5a:4a:16:c8:14:2f:af:15:22:f5
                           00:08:b4:c8:a5:1a:59:ea:c4:8f:71:97:d6:b1:f4:4a
                           cb:7c:f6:6c:1f:ff:21:76:ca:02:a8:ab:81:a8:d0:34
                           cc:33:e6:60:08:4d:df:6a:70:f9:20:69:d7:1f:a1:c9
                           c6:4c:9e:58:a6:68:6e:4e:6a:82:cc:6c:e3:b7:4f:7c
                           1a:67:9d:c9:d3:32:5e:7e:92:e1:0b:13:63:f7:79:c7
bd:be:2a:78:29:c8:09:fd:d7:a5:0d:ec:97:62:ef:36
                           ab
                 Exponent (bits 24):
        Extensions:
                 Basic Constraints (critical):
                 Certificate Authority (CA): TRUE Key Purpose (not critical):
                           TLS WWW Server.
                           Ipsec IKE.
                           OCSP signing.
                 Subject Alternative Name (not critical):
IPAddress: 172.28.100.43
                 Key Usage (critical):
Digital signature.
                 Key encipherment.
Certificate signing.
Subject Key Identifier (not critical):
                 Authority Key Identifier (not critical):
68c405e1b3bad5401735d171866f19cf3636acf3
ther Information:
                 sha1:719b5d5c36d6a91363177d1547000b3df7374685
                 sha256:da251dec03a8cd05844e23631b28ac08f2ffe0cb916566b31fec1bd8f
12bcbb
                 pin-sha256:2iUd7AOozQWETiNjGyisCPL/4MuRZWazH+wb2P4SvLs=
       Public key's random art:
                  +--[ RSA 3072]----+
                               .0*E**
                            • + + ••
                            S o . o o
s the above information ok? (y/N): y
        certificate
```

Figure 17

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



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

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:

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.



syslog Receiver Port		×
	Port Number	
	555	
	Description	
	Cache Path	
	D:\ETv9.1\EventTracker\Cache Browse	
	Note: Configuring cache path on different disk drive(s) would help in enhancing the application's performance.	
	Purge archives older than 0 days	
	✓ Enable TLS	
	Certificate subject name	
	ntpldtblr300	
	Certificate path	
	D:\certificate\ntpldtblr300.pfx Browse	
	Password	
	•••••	
	Ignore syslog message if regular expression does not match	
	Do not resolve IP address to host name	
	Raw syslog forward:	
	Select a destination and port to which all the incoming events will be forwarded as raw syslog messages.	
	Trap Destination (IP Address or host name)	
	Mode: UDP TCP	
	UDP Port	
	Save Cancel	

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

vi /etc/rsyslog.conf

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

```
DefaultNetstreamDriverCAFile /etc/rsyslog.d/keys/ca.crt

#$DefaultNetstreamDriverCertFile /etc/rsyslog.d/keys/ca.d/79.crt

#$DefaultNetstreamDriverCertFile /etc/rsyslog.d/keys/ca.d/9227.crt

$DefaultNetstreamDriver gtls # use gtls netstream driver

$ActionSendStreamDriverMode 1 # require TLS for the connection

$ActionSendStreamDriverAuthMode anon # server is NOT authenticated

#$ActionSendStreamDriverAuthMode x509/certvalid

#$ActionSendStreamDriverAuthMode x509/name
```

```
Figure 20
```

• Please enable the following commands to communicate through TLS.

\$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

• 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:

. @@remote-host:514
start forwarding rule 1
<pre>\$ActionQueueType LinkedList # use asynchronous processing</pre>
\$ActionQueueFileName srvrfwd1 # set file name, also enables disk mode
<pre>\$ActionResumeRetryCount -1 # infinite retries on insert failure</pre>
<pre>\$ActionQueueSaveOnShutdown on # save in-memory data if rsyslog shuts down</pre>
. @@172.28.100.43:529
<pre># end forwarding rule 1</pre>
start forwarding rule 2
\$ActionQueueType LinkedList # use asynchronous processing
<pre>\$ActionQueueFileName srvrfwd1 # set file name, also enables disk mode</pre>
<pre>\$ActionResumeRetryCount -1 # infinite retries on insert failure</pre>
\$ActionQueueSaveOnShutdown on # save in-memory data if rsyslog shuts down
. @@172.28.9.145:520
end forwarding rule 1

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

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:

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





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

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

