

IPWorks Security Log Management Guide

USER GUIDE

Copyright

© Ericsson AB 2017, 2018. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing.

Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
1.1	Related Information	1
2	Prerequisite	2
3	Configuring Security Log	3
3.1	Store Security Logs as Local File	4
3.2	Configuring Syslog Client	6
4	Configuring Remote Syslog Server	8
4.1	Configuring Syslog Server Using UDP Connections	8
4.2	Configuring Syslog Server Using TCP Connections	9
5	Appendix	16
5.1	Installing Rsyslog TLS	16
	Reference List	17





1 Introduction

This document describes how to configure the security log for IPWorks.

The security log provides records of security events related to the following processes:

- DNS
- ENUM
- Storage Server (SS)

Figure 1 shows the security log architecture.

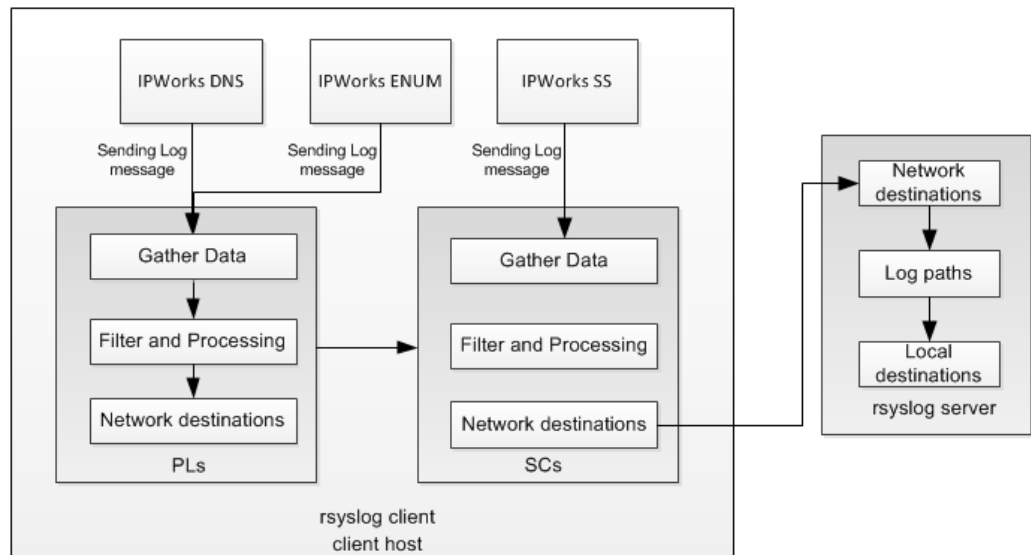


Figure 1 Security Log Architecture

1.1 Related Information

Trademark information, typographic conventions, and definition and explanation of abbreviations and terminology can be found in the following documents:

- Trademark Information
- Typographic Conventions
- Glossary of Terms and Acronyms



2 Prerequisite

- The syslog `rsyslog` has been installed on a platform that is used as the remote server.

For how to install the `rsyslog` on the remote server, refer to the online reference [Newbie guide to rsyslog](#).

- If IPv6 address is needed, first do the configuration according to the section [Configuring IPv6 OAM/Provision Network in IPWorks Initial Configuration](#), then use IPv6 address in the above configure process instead of IPv4 address.



3 Configuring Security Log

The security log configuration command `ipwsyslog` is located in the directory `/opt/ipworks/ipwsyslog/script`.

To configure the security log by using the `ipwsyslog` command, do the following:

1. Run the command on both System Controller (SC) boards (SC-1 and SC-2).

```
SC-1:~ # ipwsyslog
```

2. Select one number from the script prompted information:

```
Backup the current conf.... /etc/rsyslog.conf.backup
```

```
Where would like to store the ipworks logs? a local file or a
remote server?
```

- ```
1) local
2) remote
3) tls
```

3. Follow the instructions in Table 1 to continue based which option you selected in Step 2.

**Note:**

- After the configuration, `ipwsyslog` only works on the active SC, the other is in standby.
- The configuration from `ipwsyslog` covers the configuration in `/etc/rsyslog.conf`. For example, if you previously configure the log rotation in `/etc/rsyslog.conf`, and then you use `ipwsyslog` to do some configuration, you must re-configure the log rotation in `/etc/rsyslog.conf` again. The previous configuration in the file is stored in `/etc/rsyslog.conf.backup`.

Table 1 Log Storage and Configuration Instructions

| Log Storage   |                                                   | Configuration Instructions                                                                                                                                                                    | Instructions          |
|---------------|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| local file    |                                                   | Select 1 and specify the file path to store the log. The log must be stored in <code>/var/log/</code> , and you can specify the log file name. The default name is <code>ipworks.log</code> . | Section 3.1 on page 4 |
| syslog client | syslog client using UDP connections               | Select 2 and then 1. Specify the remote server's IP address and listening port to receive logs.                                                                                               | Section 3.2 on page 5 |
|               | syslog client using TCP connections (without TLS) | Select 2 and then 2. Specify the remote server's IP address and listening port to receive logs.                                                                                               |                       |



| Log Storage          |                                     | Configuration Instructions | Instructions                                                                                    |
|----------------------|-------------------------------------|----------------------------|-------------------------------------------------------------------------------------------------|
| remote syslog server | syslog server using UDP connections |                            | Select 2 and then 1. Specify the remote server's IP address and listening port to receive logs. |
|                      | syslog server using TCP connections | without TLS                | Select 2 and then 2. Specify the remote server's IP address and listening port to receive logs. |
|                      |                                     | with TLS                   | Select 2 and then 2. Specify the remote server's IP address and listening port to receive logs. |

## 3.1 Store Security Logs as Local File

If you choose to store security logs as a local file, set the log file by following the steps below:

1. Log on to the machine where IPWorks is installed.
2. Log on to the active SC and then execute the `ipwsyslog` command:

```
#ipwsyslog
```

```
Backup the current conf...../etc/rsyslog.conf.backup
Where would you like to store the ipworks logs?
a local file or a remote server?
1) local
2) remote
3) tls
#?
```

3. Select `local` by entering 1:

**Note:** You need to input the file name manually. The default file name is `/var/log/ipworks.log` if you don't input the file name.

For example:

```
#? 1
The IPWorks logs will be stored in local path (/var/log)
Which file you need to store the ipworks log?
Please enter file name (default file: ipworks.log)
/var/log/ipworks.log
```

4. Configure the maximum size of the log file:

**Note:** You need to input the size of log file (Range: 1-20M) manually. The default size is 2M if you don't input the size.

For example:





Please configure maximum size of log file [default size: 2048 (unit: K)]: **2048**

5. Configure the maximum number of retained log files:

**Note:** You need to input the number of retained log files (Range: 5-20) manually. The default number is 20 if you don't input the number.

For example:

Please configure maximum number of retained log files [default number: 20]: **20**

**Note:** You need to re-enter the size and number if the disk space required for the configuration is greater than eighty percent of the rest in the configuration directory.

6. Enable the security logging on the IPWorks Server.

**Note:** Currently IPWorks supports the security logging for DNS, ENUM, and Storage Server. The following table lists the respective DN of security logging:

| Service        | DN                                                                                           |
|----------------|----------------------------------------------------------------------------------------------|
| DNS            | ManagedElement=<Node Name>,IpworksFunction=1,IpworksDnsRoot=1,DnsServer=1,BindService=1      |
| ENUM           | ManagedElement=<Node Name>,IpworksFunction=1,IpworksDnsRoot=1,IpworksEnumRoot=1,EnumServer=1 |
| Storage Server | ManagedElement=<Node Name>,IpworksFunction=1,IpworksCommonRoot=1,StorageServer=1             |

Following is an example of enabling the security logging for DNS Server:

```
#/opt/com/bin/cliss
```

```
> ManagedElement=<Node Name>,IpworksFunction=1,IpworksDnsRoot=1,DnsServer=1,BindService=1
```

```
(BindService=1)>configure
```

```
(config-BindService=1)>securityLog=true
```

```
(config-BindService=1)>commit
```

**Note:** The Step 3 and Step 4 are for log file rotation implement. When the maximum size of log file is reached, the log file is rotated. By default, the maximum log file size is 2M, the maximum number of retained log files are 20. Ring buffer is used, for example, when all the available log files are full, the oldest one is overwritten.



## 3.2 Configuring Syslog Client

This section describes procedures on how to configure the syslog client using UDP and TCP (without TLS) connections.

Here is an example of the configuration parameters that are applied to the syslog client:

| Protocol          | Assigned IP Address                                 |
|-------------------|-----------------------------------------------------|
| UDP               | syslog server IP: 192.168.0.1<br>syslog port: 514   |
| TCP (without TLS) | syslog server IP: 192.168.0.1<br>syslog port: 10514 |

1. Log on to the machine where IPWorks is installed.

2. Make sure that the port is available. For example:

```
netstat -nap|grep "514"|grep "udp"
```

3. Log on to the active SC and then use the ipwsyslog command:

```
#ipwsyslog
```

```
Backup the current conf...../etc/rsyslog.conf.backup
```

```
Where would you like to store the ipworks logs? a local file
or a remote server?
```

```
1) local
```

```
2) remote
```

```
3) tls
```

```
#?
```

4. Select remote by entering 2:

```
#?2
```

```
which protocol are you going to use to transfer the ipworks
logs? tcp or udp?
```

```
1) udp
```

```
2) tcp
```

```
#?
```

5. Select udp by entering 1, and configure the IP and port of the remote server:



**Note:** For TCP (without TLS), enter **2**, the procedures for TCP (without TLS) and UDP are similar. The only difference is the port number.

For example:

```
#? 1
```

```
What is the remote server's ip address(multi addresses
separated by comma):192.168.0.1
```

```
What is the remote server's listening port to receive
logs(multi ports separated by comma):514
```

6. After the configuration is finished successfully, check the connection between the syslog client and server:

For example:

```
netstat -anp |grep 192.168.0.1
```

```
udp 0 0 192.168.0.2:40930 192.168.0.1:514 8092/rsyslogd
```



## 4 Configuring Remote Syslog Server

This section provides examples of configuring the remote syslog server using UDP and TCP connections.

For more information on how to configure syslog server, refer to [Guides for rsyslog](#), Reference [6].

The syslog configuration file is located in `/etc/rsyslog.conf`.

### 4.1 Configuring Syslog Server Using UDP Connections

1. Log on to the syslog server.
2. Use `vi` or any editor to open the syslog configuration file `rsyslog.conf`.

Add below contents in `rsyslog.conf`:

```
module(load="imudp")
input(type="imudp" port="514")

if $fromhost-ip == '192.168.0.1' then {
 action(type="omfile" file="/var/log/remotefile02")
 stop
}
```

**Note:**

- Here, the IP address is the syslog client IP, and it must be the same as the IP that is configured in Section 3.2 on page 5.
- The port number must be unique and the same as the port that is configured in Section 3.2 on page 5.

3. Check whether the UDP port 514 is occupied by a server or application:

```
#netstat -nap|grep "514"|grep "udp"

udp 0 0 192.168.0.1:514 0.0.0.0:* 7945/rsyslogd
```

4. Restart the syslog service to make the configuration take effect.

```
service rsyslog restart
```

5. Enable security logging on the IPWorks Server.

Currently IPWorks supports security logging for DNS, ENUM, and Storage Server. You can enable the security logging by using ECLI. For details, see Section 3.1 on page 4.



6. Check whether the configuration works in the file `/var/log/ipworks.log` if you use the default value.

## 4.2

### Configuring Syslog Server Using TCP Connections

1. Log on to the syslog server.
2. Use `vi` or any editor to open the syslog configuration file `rsyslog.conf`.

Add below contents in `rsyslog.conf`:

```
module(load="imtcp")
input(type="imtcp" port="10514")

if $fromhost-ip == '192.168.0.1' then {
 action(type="omfile" file="/var/log/remotefile02")
 stop
}
```

**Note:**

- Here, the IP address is the syslog client IP, and it must be the identical to the IP configured in Section 3.2 on page 5.
- The port number must be unique and the same as the port that is configured in Section 3.2 on page 5.

3. Check whether the TCP port 10514 is occupied by a server or application:

```
#netstat -nap|grep "10514"|grep "tcp"

tcp 0 0 0.0.0.0:10514 0.0.0.0:* LISTEN 10539/rsyslogd
```

4. Restart the syslog service to make the configuration take effect.

```
#service rsyslog restart
```

If you need to secure logging using TLS, see Section 4.2.1 on page 10.

5. Enable security logging on the IPWorks Server.

Currently IPWorks supports security logging for DNS, ENUM, and Storage Server. You can enable the security logging by using ECLI. For details, see Section 3.1 on page 4.

6. Check whether the configuration works.

For example,

```
tailf /var/log/ipworks.log
```



```
Feb 18 06:42:58 SC-1 rsyslogd: [origin software="rsyslogd"
swVersion="8.4.0" x-pid="6514" x-info="http://www.rsyslog.com"]
exiting on signal 15.
```

```
Feb 18 06:42:58 SC-1 rsyslogd: [origin software="rsyslogd"
swVersion="8.4.0" x-pid="8935" x-info="http://www.rsyslog.com"]
start
```

```
Feb 18 06:42:58 SC-1 systemd[1]: Starting System Logging
Service...
```

```
Feb 18 06:42:58 SC-1 systemd[1]: Started System Logging
Service.
```

### 4.2.1 Security Logging Using TLS

To configure the security logging using TLS, do the following:

For more information about security logging using TLS, refer to [Encrypting Syslog Traffic with TLS \(SSL\)](#).

To use TLS for the security logging, make sure that the required RPM packages are installed, for details, see Section 5.1 on page 16.

Perform Step 1 to Step 8 on the syslog server:

1. Create a configuration file `openssl.cnf` in a directory (for example `/etc/rsyslog/protected/`). An example of the configuration file is shown in Example 1.

**Note:** Make sure that the information in the `[ root_ca_distinguished_name ]` section is correct.

2. Clear up the commands if they have been executed previously.

```
rm -rf crl newcerts private *.pem *.info serial index
```

3. Prepare the directories and files for the following commands.

```
mkdir crl newcerts private
```

```
chmod go-rwx private
```

```
echo '01' > serial
```

```
touch index
```

4. Create a CA with a key and generate a certificate request.

```
openssl req -new -config openssl.cnf -keyout private/cakey.p
em -out careq.pem
```

5. Create a certificate for the CA by using the above key and self-sign it.



```
openssl ca -config openssl.cnf -create_serial -out cacert.pem
-batch -keyfile private/cakey.pem -selfsign -extensions v3_ca
-infiles careq.pem
```

6. Create server private key and generate a server certificate request.

```
openssl req -nodes -new -keyout server-key.pem -out
server-cert-req.pem -config openssl.cnf
```

7. Create a certificate for the server by using the above server certificate request and sign it with the CA certificate.

```
openssl ca -config openssl.cnf -out server-cert.pem -batch
-infiles server-cert-req.pem
```

8. Copy cacert.pem, server-cert.pem and server-key.pem to a directory (for example, /etc/rsyslog/protected/), edit the /etc/rsyslog.conf configuration file, remove "module(load="imuxsock")".

```
module(load="imuxsock") #remove this line

$ModLoad imuxsock # local messages
$ModLoad imtcp # TCP listener

make gtls driver the default
$DefaultNetstreamDriver gtls

certificate files
$DefaultNetstreamDriverCAFile /etc/rsyslog/protected/cacert.pem
$DefaultNetstreamDriverCertFile /etc/rsyslog/protected/server-cert.pem
$DefaultNetstreamDriverKeyFile /etc/rsyslog/protected/server-key.pem

$InputTCPServerStreamDriverMode 1 # run driver in TLS-only mode
$InputTCPServerStreamDriverAuthMode anon # client is NOT authenticated
$InputTCPServerRun 10514 # start up listener at port 10514
```

Perform Step 9 to Step 12 on the client machine:

9. Copy the cacert.pem to client directory (for example, /etc/rsyslog/protected/).

10. Create a configuration file named openssl.cnf as shown in Example 1.

**Note:** Make sure the information in the [ root\_ca\_distinguished\_name ] section is correct.

11. Create client private key and generate a client certificate request.

```
openssl req -nodes -new -keyout client-key.pem -out
client-cert-req.pem -config openssl.cnf
```

12. Copy the client-cert-req.pem to the directory /etc/rsyslog/protected/ on the syslog server.

13. On the syslog server, create a certificate for the client by using the above client-cert-req.pem and sign it with the CA certificate.



```
openssl ca -config openssl.cnf -out client-cert.pem -batch
-infiles client-cert-req.pem
```

14. On the syslog server, copy client-cert.pem to the directory /etc/rsyslog/protected/ on the client machine.

15. On the client machine, edit /etc/rsyslog.conf as below:

```
make gtls driver the default
$DefaultNetstreamDriver gtls

certificate files
$DefaultNetstreamDriverCAFile /etc/rsyslog/protected/cacert.pem
$DefaultNetstreamDriverCertFile /etc/rsyslog/protected/client-cert.pem
$DefaultNetstreamDriverKeyFile /etc/rsyslog/protected/client-key.pem

Use default timestamp format
$ActionSendStreamDriverMode 1 # run driver in TLS-only mode
$ActionSendStreamDriverAuthMode anon # server is NOT authenticated
```

16. On the syslog server, restart the rsyslog service to make the configuration take effect.

```
service rsyslog restart
```

17. On the client machine, restart the rsyslog service to make the configuration take effect.

```
service rsyslog restart
```

```
#
OpenSSL configuration file for custom Certificate Authority. Use a
different openssl.cnf file to generate certificate signing requests;
this one is for use only in Certificate Authority operations (csr ->
cert, cert revocation, revocation list generation).
#
Be sure to customize this file prior to use, e.g. the commonName and
other options under the root_ca_distinguished_name section.
#
```

```
HOME = .
RANDFILE = $ENV::HOME/.rnd
```

```
[ca]
default_ca = CA_default
```

```
[CA_default]
dir = .
unused at present, and my limited certs can be kept in current dir
#certs = $dir/certs
new_certs_dir = $dir/newcerts

crl_dir = $dir/crl
database = $dir/index
```





```

certificate = $dir/cacert.pem
serial = $dir/serial
crl = $dir/cakey.pem
private_key = $dir/private/cakey.pem
RANDFILE = $dir/private/.rand

x509_extensions = usr_cert

Make new requests easier to sign - allow two subjects with same name
(Or revoke the old certificate first.)
unique_subject = no

Comment out the following two lines for the "traditional"
(and highly broken) format.
name_opt = ca_default
cert_opt = ca_default

default_crl_days= 30
default_days = 3650
pick a stronger hash, if possible
default_md = sha1
MSIE may need following set to yes?
preserve = no

A few difference way of specifying how similar the request should look
For type CA, the listed attributes must be the same, and the optional
and supplied fields are just that :-)
policy = policy_match

For the CA policy
[policy_match]
countryName = match
stateOrProvinceName = match
organizationName = match
organizationalUnitName = optional
commonName = supplied

emailAddress = optional

For the 'anything' policy
At this point in time, you must list all acceptable 'object'
types.
[policy_anything]
countryName = optional
stateOrProvinceName = optional
localityName = optional
organizationName = optional
organizationalUnitName = optional
commonName = supplied
emailAddress = optional

```



```

[req]
default_bits = 2048
default_keyfile = ./private/ca-key.pem
pick a stronger hash, if possible
default_md = sha1

prompt = no
distinguished_name = root_ca_distinguished_name

x509_extensions = v3_ca

Passwords for private keys if not present they will be prompted for
input_password = secret
output_password = secret

This sets a mask for permitted string types. There are several options.
default: PrintableString, T61String, BMPString.
pkix : PrintableString, BMPString.
utf8only: only UTF8Strings.
nombstr : PrintableString, T61String (no BMPStrings or UTF8Strings).
MASK:XXXX a literal mask value.
WARNING: current versions of Netscape crash on BMPStrings or UTF8Strings

so use this option with caution!
string_mask = nombstr

req_extensions = v3_req

[root_ca_distinguished_name]
commonName = myhost
countryName = CN
stateOrProvinceName = ShangHai
localityName = ShangHai
0.organizationName = IPWorks
emailAddress = support@ericsson.com
[usr_cert]

These extensions are added when 'ca' signs a request.

This goes against PKIX guidelines but some CAs do it and some software
requires this to avoid interpreting an end user certificate as a CA.

basicConstraints=CA:FALSE

PKIX recommendations harmless if included in all certificates.
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer:always
```



```

nsCaRevocationUrl =
#nsBaseUrl
#nsRevocationUrl
#nsRenewalUrl
#nsCaPolicyUrl
#nsSslServerName

[v3_req]

Extensions to add to a certificate request

basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment

[v3_ca]

Extensions for a typical CA

PKIX recommendation.
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer:always

This is what PKIX recommends but some broken software chokes on critical
extensions.
#basicConstraints = critical,CA:true
So we do this instead.
basicConstraints = CA:true

[crl_ext]

CRL extensions.
Only issuerAltName and authorityKeyIdentifier make any sense in a CRL.

issuerAltName=issuer:copy
authorityKeyIdentifier=keyid:always,issuer:always

```

Example 1 openssl.cnf



## 5 Appendix

### 5.1 Installing Rsyslog TLS

---

---

#### Attention!

This section provides the Rsyslog TLS (version 1.2) installation in **SLES 12**.

---

---

1. Download the following RPM packages by searching the keyword **rsyslog-module-gtls** from the website <https://www.suse.com>.
  - libp11-kit0-0.20.3-1.6.x86\_64.rpm
  - libnettle4-2.7.1-5.20.x86\_64.rpm
  - libhogweed2-2.7.1-5.20.x86\_64.rpm
  - libtasn1-3.7-2.13.x86\_64.rpm
  - libtasn1-6-3.7-2.13.x86\_64.rpm
  - libgnutls28-3.2.15-1.8.x86\_64.rpm
  - rsyslog-module-gtls-8.4.0-2.2.x86\_64.rpm
2. Log on to the Linux Server with the Rsyslog installed.
3. Create an installation directory, for example, /home/install, and copy the downloaded packages into the directory.
4. Execute the following commands to install the RPM packages:

```
rpm -ivh libp11-kit0-0.20.3-1.6.x86_64.rpm libnettle4-2.7.1-5.20.x86_64.rpm libhogweed2-2.7.1-5.20.x86_64.rpm

rpm -ivh libtasn1-3.7-2.13.x86_64.rpm libtasn1-6-3.7-2.13.x86_64.rpm libgnutls28-3.2.15-1.8.x86_64.rpm rsyslog-module-gtls-8.4.0-2.2.x86_64.rpm
```



## Reference List

### IPWorks Documents

- [1] Trademark Information
- [2] Typographic Conventions
- [3] Glossary of Terms and Acronyms
- [4] IPWorks Initial Configuration, 5/1553-AVA 901 33/3

### Other Reference

- [5] [Novell AppArmor](#)
- [6] [Newbie guide to rsyslog](#)
- [7] [Guides for rsyslog](#)
- [8] [Encrypting Syslog Traffic with TLS \(SSL\)](#)