z/OS 3.1 IBM Education Assistant

Solution Name: SYSLOGD support for logging over TCP

Solution Element: z/OS Communications Server

July 2023

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.

Agenda

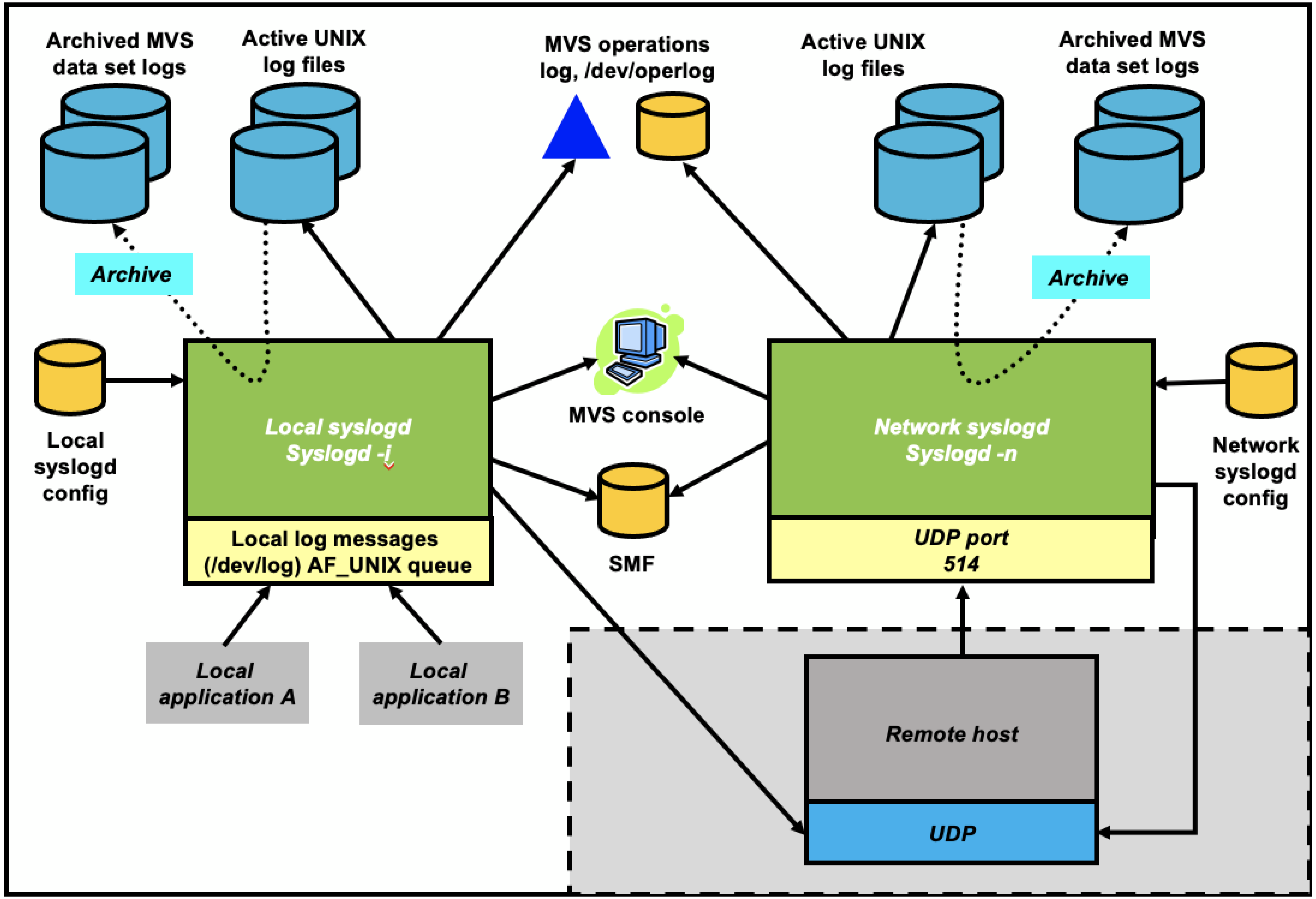
- Trademarks
- Objectives
- Overview
- Usage & Invocation
- Diagnostics
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Installation & Configuration
- Appendix

Objective

- Who
  - z/OS System Administrator
- What
  - Support added to the z/OS syslog daemon to send and receive message over the network using TCP. Only UDP was supported before.
- Wow
  - TCP can be secured with TLS. An IPsec VPN was required to secure with UDP.
  - TCP is a reliable protocol unlike UDP which provides no guaranteed delivery.
  - Interoperability with other syslogd implementations that only support TCP, or prefer TCP support protected by TLS

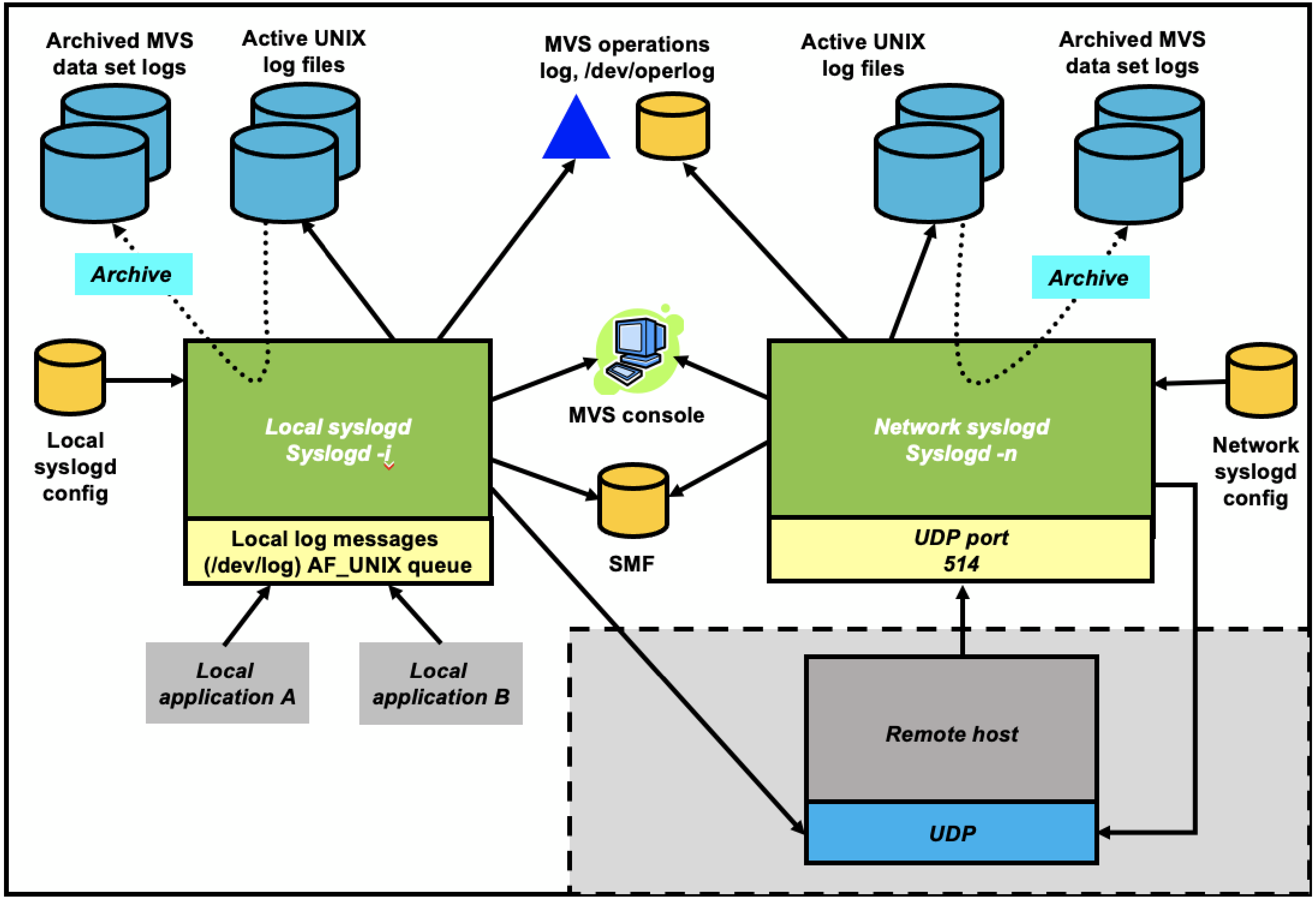
Overview – existing syslogd support (1 of 2)

- Processes local and remote messages and logs them to various destinations:
  - MVS console
  - UNIX log files
  - SMF
  - operlog log stream (operlog)
  - Users
  - Remote hosts
- Uses a configuration file made up of rules to control where messages are logged.



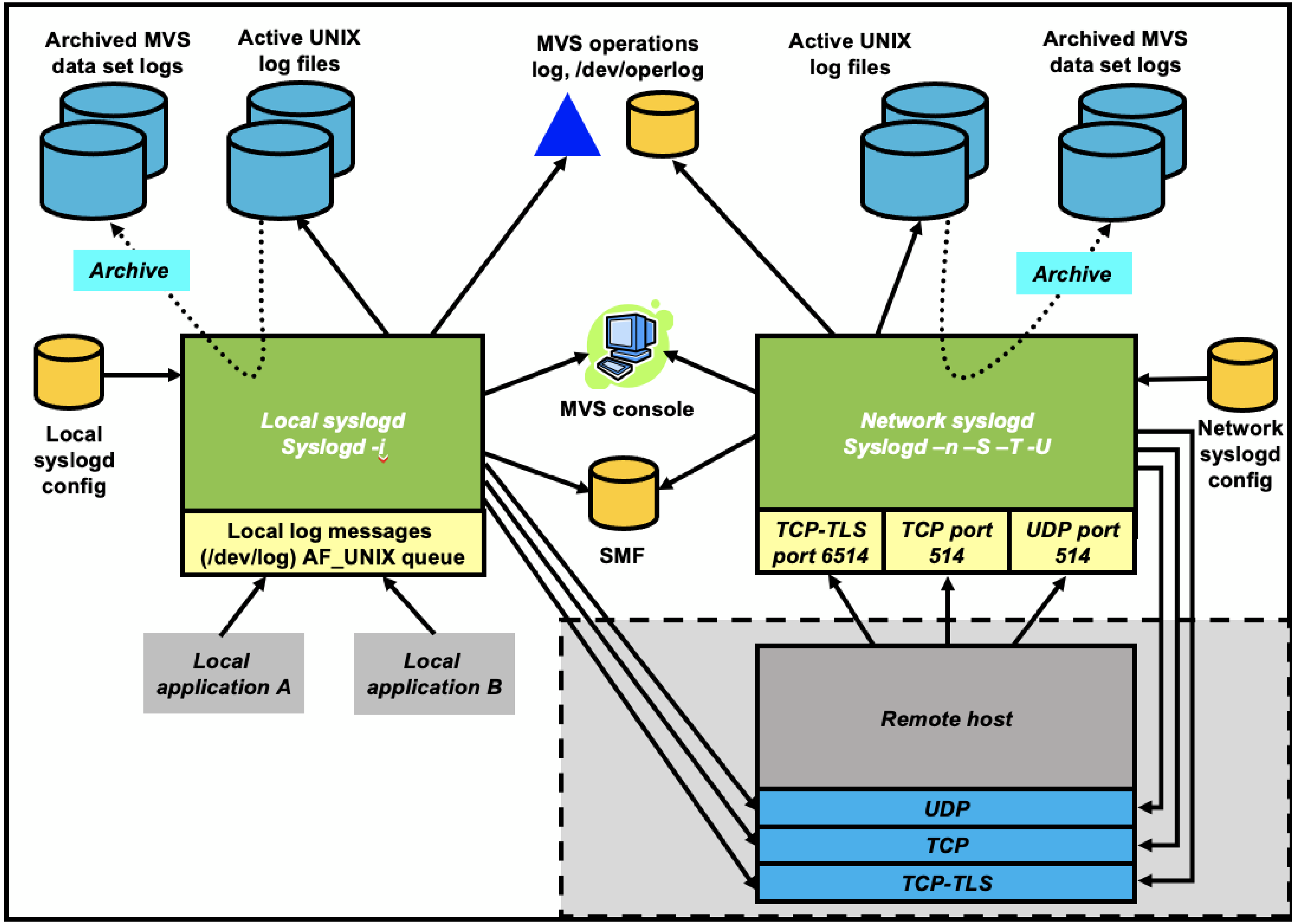
Overview – existing syslogd support (2 of 2)

- Processes local messages over an AF_UNIX socket.
- Sends and receives messages remotely using the UDP protocol
- UDP does not guarantee delivery of a message and the only way to secure a connection is with a VPN using IPSec.



Overview – new syslogd support for TCP

- Syslogd now supports sending and receiving messages over:
    - UDP
    - An unprotected TCP connection
    - A TCP connection protected by TLS
- Support for TCP allows reliable transport and data security provided by TLS

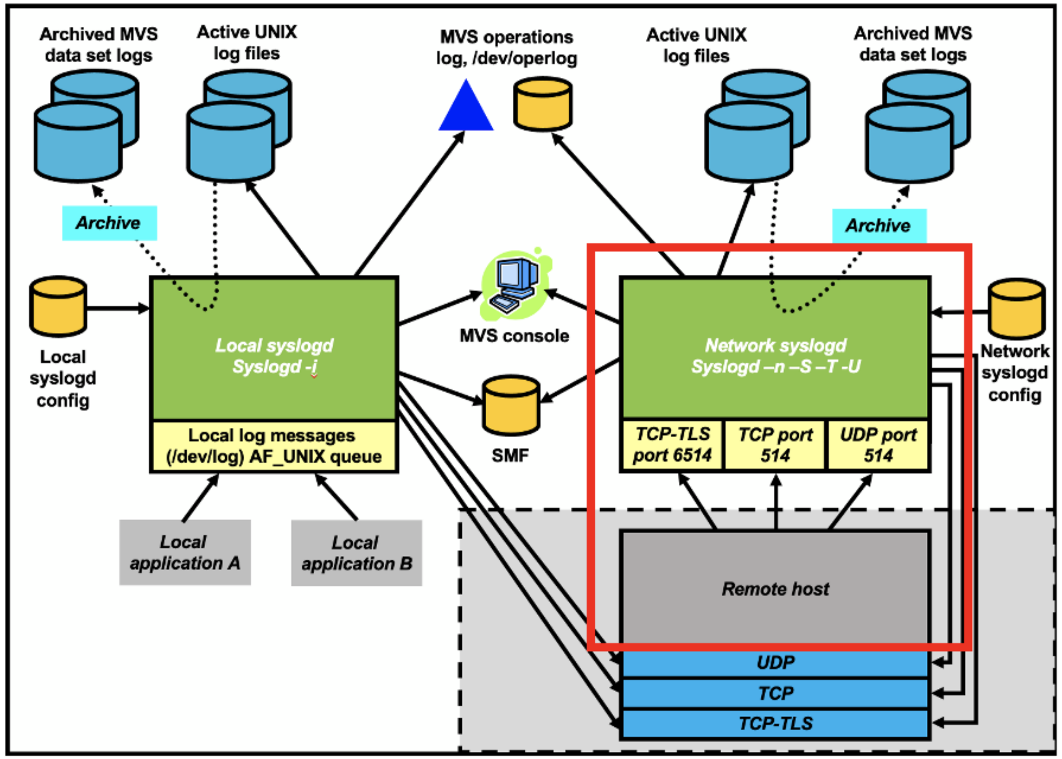


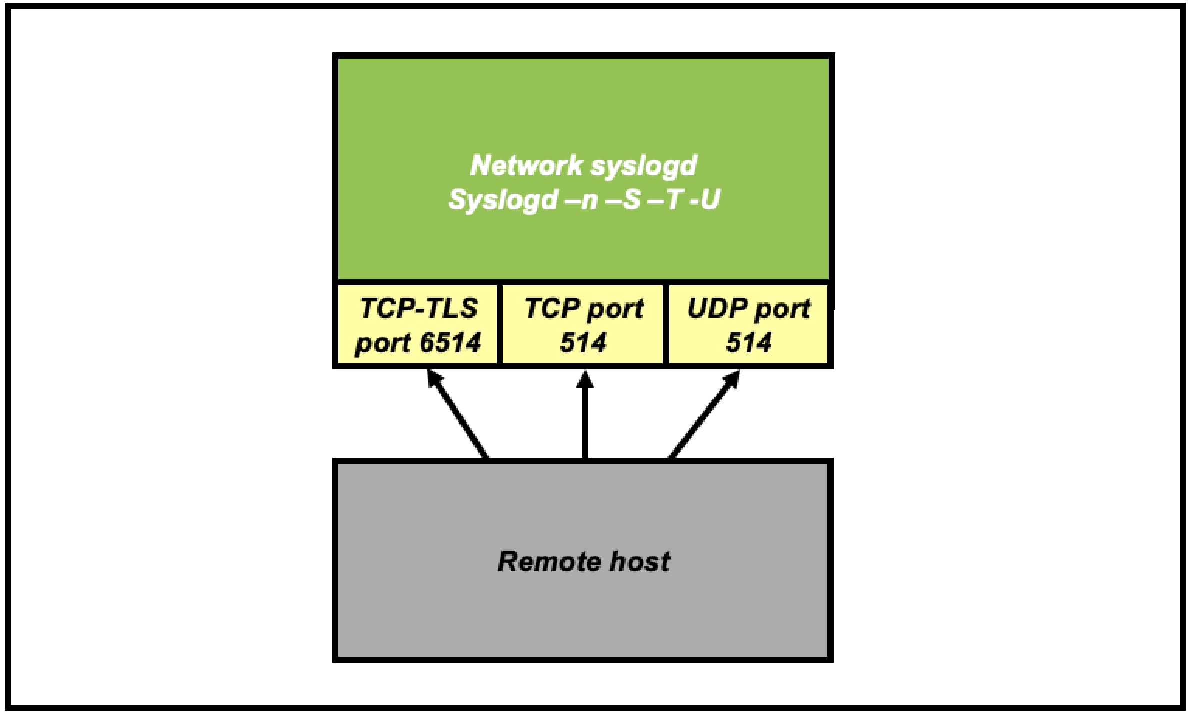
Overview – existing syslogd start options

- Syslogd recognizes the following start options:
  - **-f** - Specify configuration file name.
  - **-d** - Run syslogd in debugging mode.
  - **-c** - Create log files and directories automatically.
    - **-D** - Specify the global access permissions when creating directories.
    - **-F** - Specify the global access permissions when creating log files.
  - **-i** - Start in local-only mode.
  - **-n** - Start in network-only mode.

Overview – new start options for receiving messages

- Additional start options for receiving over the network:
  - **-U** – receive messages over UDP. Default port is 514.
  - **-T** – receive messages over unprotected TCP. Default port is 514.
  - **-S** – receive messages over TCP protected by TLS. Default port is 6514.

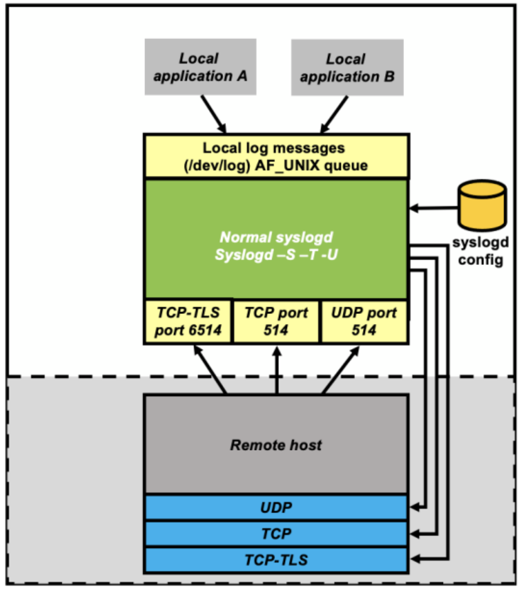




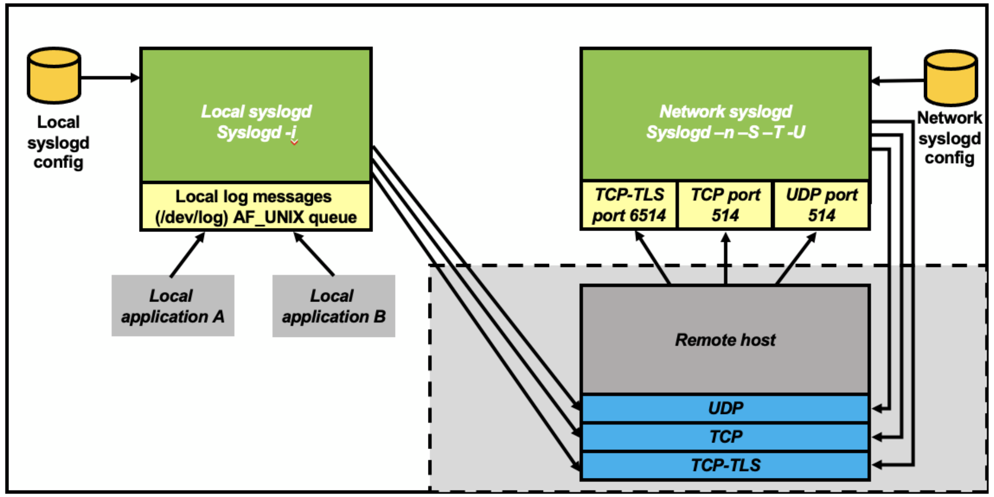
Overview – syslogd instances

- A syslogd instance can start in one of three modes:
  - **Normal mode**
    - Processes messages from local applications.
    - Processes messages received over the network by a remote system.
    - Only one syslogd instance on a system in this mode.
  - **Local-only mode (-i)**
    - Only processes messages from local applications.
    - Can not be configured with the new start options **-U, -T, -S**.
  - **Network-only mode (-n)**
    - Only processes messages received over the network by a remote system.

Normal mode



Local-only and network-only mode



Overview – syslogd configuration file

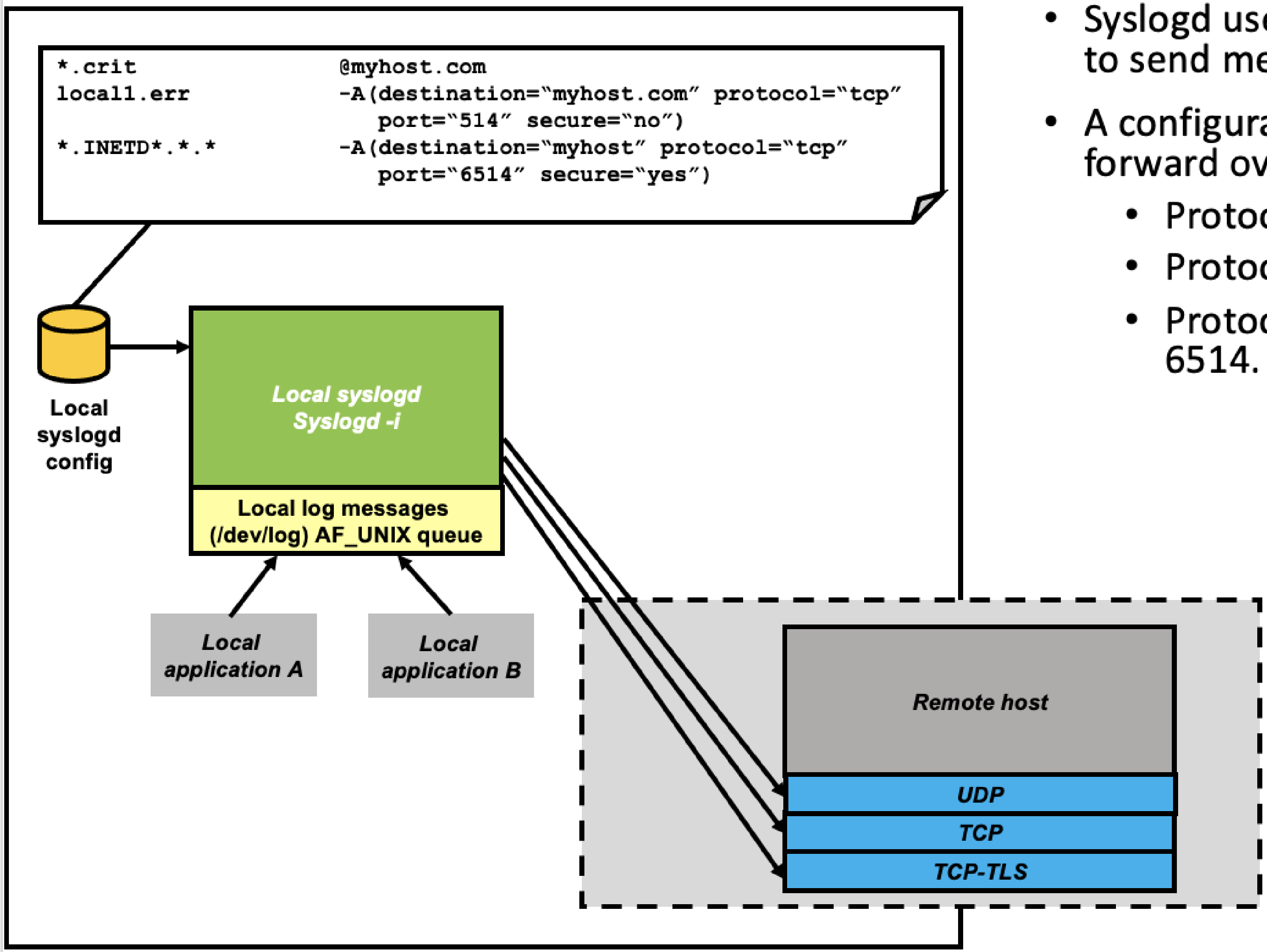
- There are a few ways syslogd will point to a configuration file:
  1. Using the **–f** start option
  2. Environment variable - SYSLOGD_CONFIG_FILE
  3. Defaulting to /etc/syslog.conf

- A configuration file defines logging **rules** that require a source and a destination.
  - The source is made up of criteria such as a facility and priority. This defines which messages will be processed for a rule.

	Source	Destination
Local Source	USERID.JOBNAME.FACILITY.PRIORITY	$SMF
Remote Source	(HOSTNAME/IP-ADDRESS).FACILITY.PRIORITY	/var/local.log
Local and Remote Source	FACILITY.PRIORITY	@192.168.0.1

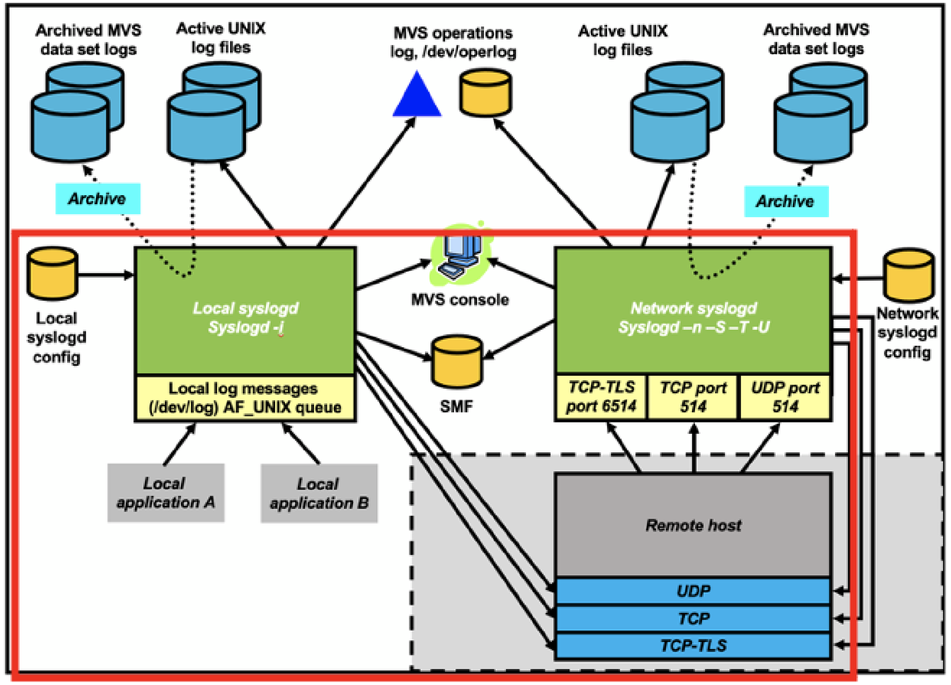
- Any changes made to the configuration file require syslogd to reread it. To force syslogd to reread its configuration file:
  - Issue the MODIFY *procname*, RESTART command
  - Send a SIGHUP signal with a kill command (kill –s HUP *processID)*

Overview – forwarding messages over the network (1 of 2)



```
*.crit              @myhost.com
local1.err          -A(destination=“myhost.com” protocol=“tcp”
                       port=“514” secure=“no”)
*.INETD*.*.*        -A(destination=“myhost” protocol=“tcp”
                       port=“6514” secure=“yes”)
```

- Syslogd uses a configuration rule forwarding action to send messages over the network.
- A configuration rule can now be configured to forward over:
  - Protocol UDP. Default to port in /etc/services.
  - Protocol TCP. Default port 514.
  - Protocol TCP protected by TLS. Default port 6514.



Overview – forwarding messages over the network (2 of 2)

- Syslogd configuration rules use the following forwarding action to send messages using only UDP:

```
@hostname/ipAddress
```

  - **Hostname**: myhost.com
  - **IP address**: 192.168.2.1

```
@myhost.com
@192.168.2.1
```

- Configuration rule –A(…) forwarding action for sending messages over UDP and TCP:

```
-A(destination=“value” protocol=“value” port=“value” secure=“value”)
```

  - **destination** parameter (required)
    - Hostname: myhost.com
    - IP address: 192.168.0.1
  - **protocol** parameter (required)
    - UDP
    - TCP

```
-A(destination=“myhost.com” protocol=“udp” port=“514”)
-A(destination=“192.168.0.1” protocol=“tcp” port=“514” secure=“no”)
-A(destination=“myhost.com” protocol=“tcp” secure=“yes”)
-A(destination=“192.168.0.1” protocol=“tcp” secure=“yes” port=“6514”)
```

  - **port** parameter (optional)
    - Any valid port number. This value should be configured based on the listening port for the remote syslogd.
  - **secure** TCP parameter (optional)
    - Yes - Secure the data being forwarded over the TCP socket with TLS.
    - No – Do not secure the data being forwarded over the TCP socket.

Usage & Invocation – receiving messages over TCP (1 of 3)

- **Setup tasks to receive syslogd messages over the network using TCP**
  - Specify syslogd –T start option (syslogd can be in normal mode or network only mode)
  - If syslogd messages can also be received over the network using UDP, specify the –U start option
  - Specify the TCP port for receiving syslogd messages in /etc/services
  - Reserve the TCP port in the TCP/IP profile for syslogd
  - Setup remote system to send syslogd messages

- **Setup tasks to receive syslogd messages over the network using TCP protected by TLS**
  - Specify syslogd –S start option (syslogd can be in normal or network only mode)
  - If syslogd messages can also be received over the network using UDP, specify the –U start option
  - Specify the secure TCP port for receiving syslogd messages in /etc/services
  - Reserve the secure TCP port in the TCP/IP profile for syslogd
  - Implement an AT-TLS syslogd server rule
    - The rule should be configured with ApplicationControlled off. Syslogd will be an AT-TLS aware application verifying that a successful TLS session has been negotiated before processing received data.
  - Obtain a server certificate and private key for the syslogd server and connect it to the SAF keyring or key database referenced by the AT-TLS rule.
  - Setup remote system to send syslogd messages using TLS protection

Usage & Invocation – receiving messages over TCP (2 of 3)

- Scenario 1: Start a syslogd instance in normal mode to process local and remote messages, but only receive messages over an unprotected TCP socket and TCP socket protected by TLS.

Start procedure:

```
//CONFHFS EXEC PGM=SYSLOGD,REGION=0M,TIME=NOLIMIT,
//         PARM='ENVAR("_CEE_ENVFILE_S=DD:STDENV")/-c –T -S'
//*
//STDENV   DD DUMMY
//SYSPRINT DD SYSOUT=*
//SYSIN    DD DUMMY
//SYSERR   DD SYSOUT=*
//SYSOUT   DD SYSOUT=*
//CEEDUMP  DD SYSOUT=*
```

Shell:

```
===> _BPX_JOBNAME=SYSLOGD syslogd -c –T –S &
```

- Scenario 2: Start a syslogd instance in network-only mode to process only remote messages, but only receive messages over a UDP socket and TCP socket protected by TLS.

Start proc:

```
//CONFHFS EXEC PGM=SYSLOGD,REGION=0M,TIME=NOLIMIT,
//         PARM='ENVAR("_CEE_ENVFILE_S=DD:STDENV")/-c -n –U -S'
//*
//STDENV   DD DUMMY
//SYSPRINT DD SYSOUT=*
//SYSIN    DD DUMMY
//SYSERR   DD SYSOUT=*
//SYSOUT   DD SYSOUT=*
//CEEDUMP  DD SYSOUT=*
```

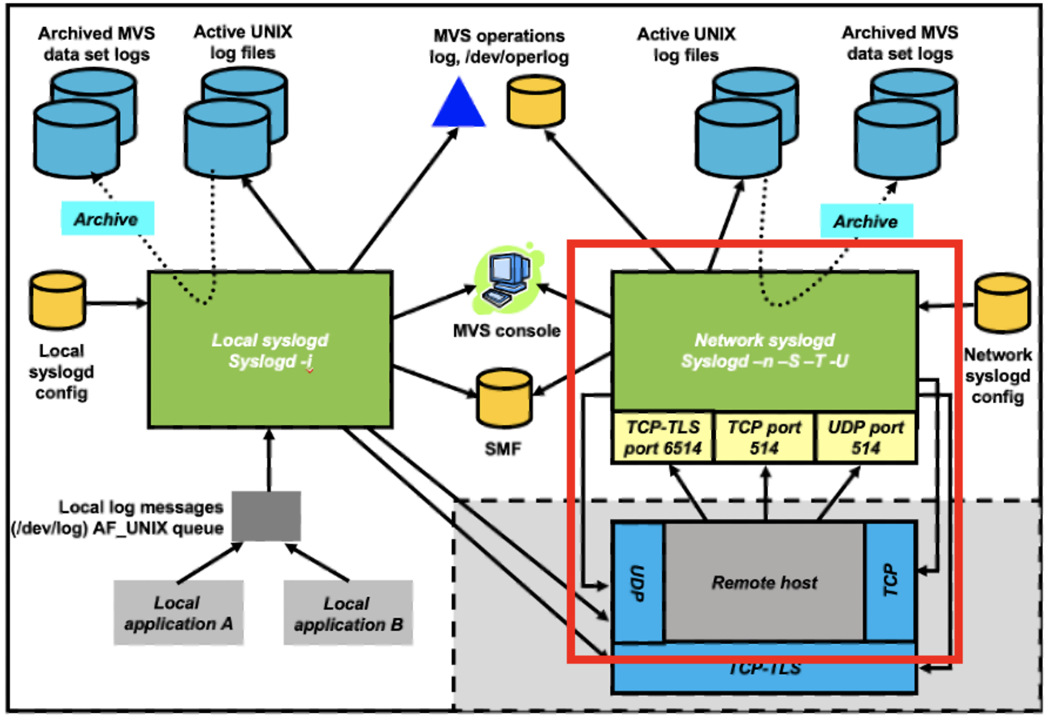
Shell:

```
===> _BPX_JOBNAME=SYSLOGD syslogd -c –n –U –S &
```

Usage & Invocation – receiving messages over TCP (3 of 3)

- Will search in /etc/services or ETC.SERVICES for a configured port number for receiving messages over the network.
    - *syslog portnumber/udp*
        - Default is port 514
    - *syslog portnumber/tcp*
        - Default is port 514
    - *syslog-tls portnumber/tcp*
        - Default is port 6514

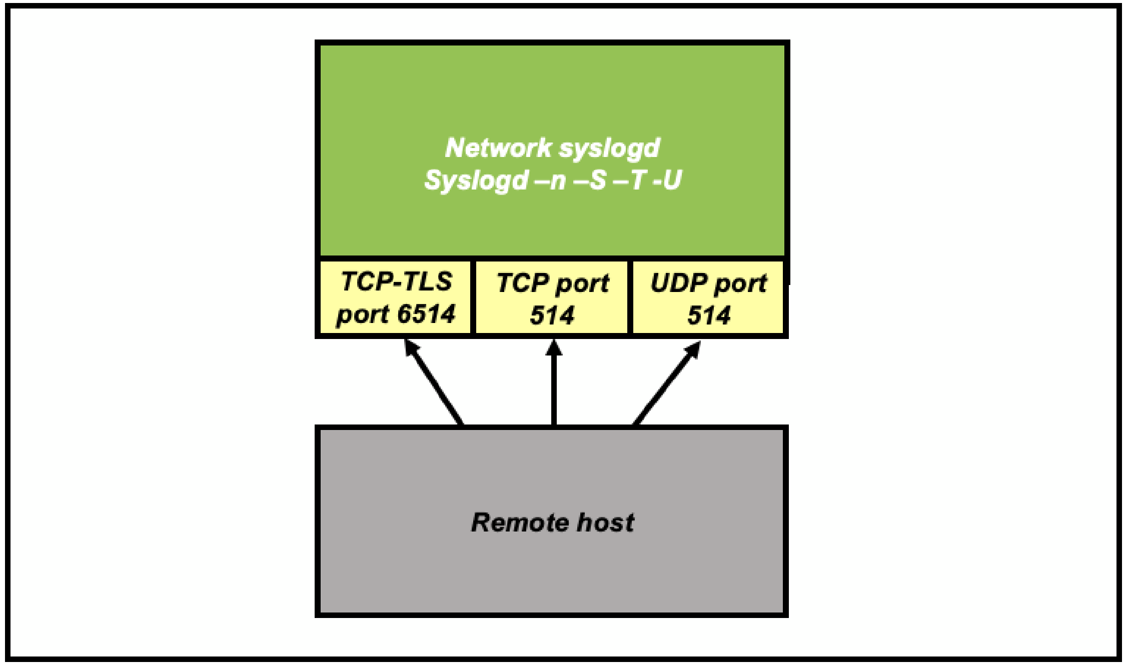
```
syslog          514/udp
syslog          514/tcp
syslog-tls      6514/tcp
```



- Port reservations in TCP/IP profile for receiving for messages over the network.

```
PORT
   514   TCP  SYSLOGD
   514   UDP  SYSLOGD
   6514  TCP  SYSLOGD
```

- IANA defines TCP port 6514 for the TCP with TLS service. There is no standard port defined by IANA for syslogd to receive messages over unprotected TCP. The z/OS syslogd uses TCP port 514 by default, but that port could be in use by another service.



Usage & Invocation – sending messages over TCP (1 of 2)

- **Setup tasks to send syslogd messages over the network using TCP**
  - Add rules in the syslogd configuration file using the –A(…) forwarding action to specify which syslogd messages should be sent remotely using TCP.
  - Setup remote system to receive syslogd messages.

- **Setup tasks to send syslogd messages over the network using TCP protected by TLS**
  - Add rules in the syslogd configuration file using the –A(…) forwarding action with secure="yes" to specify which syslogd messages should be sent remotely using TCP protected by TLS.
  - Implement an AT-TLS syslogd client rule, including a client certificate, if required.
    - The rule should be configured with ApplicationControlled off. Syslogd will be an AT-TLS aware application verifying that a successful TLS session has been negotiated before sending messages.
  - Setup remote system to receive syslogd messages using TLS protection.

Usage & Invocation – sending messages over TCP (2 of 2)

- Configuration file rules for forwarding messages over the network

Local/Remote Source	Destination	Description
(192.168.0.6).*.CRIT	-A(destination=“192.168.1.9” protocol=“udp” port=“514”)	Process remote messages from host 192.168.0.6 with priority crit or higher and forward them to the remote UDP destination 192.168.1.9 on port 514
.FTPD..ERR	-A(destination=“abc.com” protocol=“tcp” secure=“no” port=“514”)	Process local messages with priority err or higher from applications with “FTPD” jobname and forward them to the remote TCP destination abc.com on port 514 over a non-secure TCP connection
.IKED..ERR	-A(destination=“192.168.1.9” protocol=“tcp” port=“6514” secure=“yes”)	Process local messages with priority err or higher from applications with “IKED” jobname and forward them to the remote TCP destination 192.168.1.9 on port 6514 over a secure TCP connection

Diagnostics (1 of 2)

- Syslogd will write messages with a priority of error when problems are encountered.
  - It is recommended to write local syslogd error messages to a local file.

configuration file rule:

```
*.SYSLOGD*.*.ERR         /var/log/syslogd.log
```

- Here is an example of error messages written to a local file:

```
Feb 20 8:12:49 SYS1 syslogd1: FSUM1277 recv tcp inet (myhost.com 198.2.1.6 514) closed due to timeout
Feb 20 9:04:42 SYS1 syslogd1: FSUM1282 An error was detected on the AF_INET or AF_INET6 TCP socket, syslogd will no longer
monitor the TCP socket
```

  - The first message is written when an inbound connection is closed because a message has not been received over a TCP connection for 15 minutes
  - The second message indicates that the syslogd TCP listening socket has been closed because the socket has been dropped with netstat

Diagnostics (2 of 2)

- Syslogd will write some error messages to the console
  - When errors occur before syslogd initialization has completed, error messages are written to the console
  - For a small number of error conditions (after initialization), messages are written to the console
  - For example, the following messages are written to alert the operator that syslogd is attempting to connect to a remote syslogd to send a message.

```
13.47.52 FSUM1284 SYSLOGD: TCP SOCKET (myhost 192.168.1.6 514): EDC5112I RESOURCE TEMPORARILY UNAVAILABLE. ERRNO/RSN=112/74B30296
15.18.21 FSUM1284 SYSLOGD: CONNECT (myhost 192.168.1.6 514): EDC8128I CONNECTION REFUSED. ERRNO/RSN=1128/76630291
```

  - The first message indicates that a local TCP socket cannot be obtained (typically the local TCP stack is down)
  - The second message indicates that an attempt to connect was rejected

Interactions & Dependencies

- Software Dependencies
  - None
- Hardware Dependencies
  - None
- Exploiters
  - None

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Plex must be at the new z/OS level: No
- No upgrade/coexistence considerations.

Installation & Configuration (1 of 2)

- Updated sample files:
  - Syslogd started proc sample: tcpip.SEZAINST(SYSLOGD)
  - Syslogd configuration file sample: /usr/lpp/tcpip/samples/syslog.conf
- Guidelines for configuring rules to send messages remotely over TCP
  - Identify specific messages that you want to send to an external collection point. For example:
    - All error messages for an application could be sent to a collection point for analysis
    - Audit messages for an application could be sent to a collection point to provide a single point for auditing
  - It is recommended that debug-level messages remain on the local system in a file.
- New environment variable:
  - By default, 128 TCP connections can be active with a syslogd server/receiver. Each of the connections has a thread assigned to it. Typically, there is no need to modify this default.
    - Environment variable SYSLOGD_TCPTHREADPOOL_SIZE can be used to reduce the number of threads allocated for inbound TCP connections. A value of 5 – 128 is accepted.
  - Note: The number of outbound TCP connections that can be established is limited by the number of output destination threads (250) that can be supported by syslogd.

Installation & Configuration (2 of 2)

- IPL automation considerations
  - z/OS syslog daemon is typically started early in the IPL to ensure that any messages written to syslogd can be captured
  - Syslogd configuration rules that forward messages over TCP can not be operational until the network is operational – the TCP/IP stack on this system is active and the receiving TCP/IP stack is active.
  - Syslogd configuration rules that include TLS protection for the TCP traffic will also need to have the AT-TLS infrastructure active, including policy agent
  - Messages can be queued until the network and AT-TLS infrastructure become active. If the message queues are flooded, messages will be dropped.
  - During IPL, ensure that critical messages are written to a local location for immediate awareness.
  - Tip: When using AT-TLS protection for syslogd connections (either –S option or rules specify secure="yes”), do not permit the syslogd user ID to the profile protecting the *EZB.INITSTACK.sysname.stackname* resource. This prevents the connections from being attempted before the AT-TLS infrastructure is active.
  - Tips: When AT-TLS protection is not used for syslogd connections, but messages are being sent or received over the network, consider permitting the syslogd user ID to the profile protecting the EZB.INITSTACK.*sysname.stackname* resource. This allows messages to be sent/received over the network without waiting for the AT-TLS infrastructure which is not needed. This reduces the potential for flooding syslogd's message queues.

Summary

- Syslogd will be able to receive and send messages over a TCP socket and protect a TCP connection with TLS.
  - New start options (-U, -T, -S) for receiving messages over the network.
  - The new –A(…) forwarding action that will allow a port and TCP protection to be specified on a rule for forwarding messages over the network.

- This function is also planned to be provided on z/OS V2R5 with APAR PH47666

Appendix

- Publications
  - z/OS Communications Server: IP Configuration Guide
    - Chapter 5. Configuring the syslog daemon
  - z/OS Communications Server: IP Configuration Reference
    - Chapter 15. Syslog daemon