IBM Z HMC (Hardware Management Console) 2.15.0 Remote Syslog Server

April 15, 2021

Client Update

Brian Valentine
HMC/SE Development
File Updated: 04-15-21

IBM Z

Z Exchange

Audit Mgmt offload support to Remote Syslog

Goals and Approach

- Goals
  - **Consolidation** of key HMC/SE log information to new log entries as a supplement to existing logs (i.e. no current logs are being removed)
  - Customizable **forwarding** of selected consolidated log entries to a customer-controlled centralized gathering point or points
- Approach
  - Leverages syslog capability
    - syslog is a logging component and protocol
    - HMC/SE will utilize a standard rsyslog component within its environment
    - rsyslog supports forwarding to syslog servers for log consolidation and analysis
    - Commonly used syslogging tools (such as rsyslog itself) and products (such as ***Splunk Enterprise***) are capable of acting as syslog servers

Consolidation

Types of logs being consolidated

- Audit logs
- Security logs
- Console events
- Hardware messages
- Web Services API request logs
- BCPii logs

Consolidation approach

- Summary information is captured and formatted at the existing logging points and syslogged

- For remote consolidation
  - New HMC task
    - Configure rsyslog to forward selected consolidated syslog entries from the HMC or managed SEs to customer-controlled syslog servers

Sample consolidated log entries

```
Apr  3 10:02:24 HMC0318A zHMC.HMC0318A.SecurityLog: The user browser logged into the
underlying console operating system platform.

Apr  3 10:02:29 HMC0318A zHMC.HMC0318A.AuditLog: A device monitor event occurred; Device
Type: usb, Action: discovered at startup, Vendor: QEMU, Model: QEMU USB Tablet, Serial:
42

Apr  3 10:03:13 HMC0318A zHMC.HMC0318A.HwMsgLog: AttentionID: 38b59cc0-5619-11e9-a82d-
fa163e302a96 Creation Date: Wed Apr 03 10:03:13 EDT 2019 Description: ACT04320I Device
Monitor. Device Type: usb, Action: discovered at startup, Vendor: QEMU, Model: QEMU USB
Tablet, Serial: 42

Apr  3 10:03:14 HMC0318A zHMC.HMC0318A.EventLog: The console application was
initialized.
```

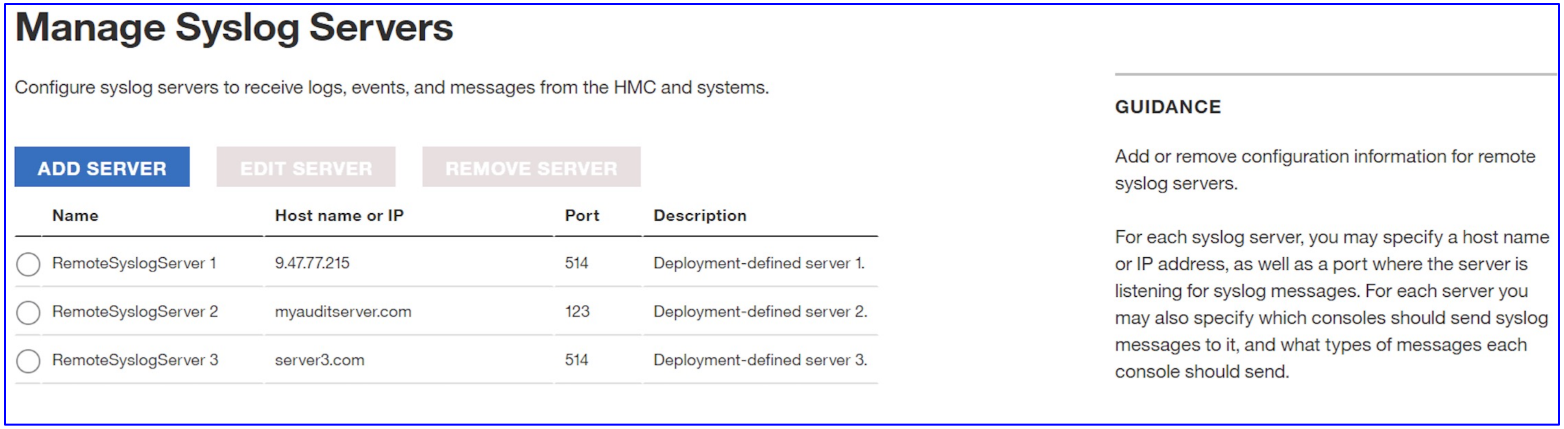
Forwarding

- New HMC *Manage Syslog Servers* task
  - allows specification of a list of remote syslog servers as targets for
    - the HMC itself as well as for any managed CPC (SE) (2.15.0 or newer)
  - **Note:**
    - Currently must configure each additional HMC uniquely
      - Or recommend using HMC Data Replication and configure one HMC/replicate
    - When configuring a 2nd HMC, any previous CPC (SE) configurations will be shown with the previous customization settings
      - which can also be altered further

- For each remote syslog server you must specify:
  - The server
  - The port where the server is listening for syslog messages
  - Which of the 6 supported logs types should be forwarded
    - For each server you may select any mix of the 6 log types,
      - from a single type to all types

- The task configures rsyslog to do the forwarding.

Manage/Add Syslog Servers



Manage Syslog Servers

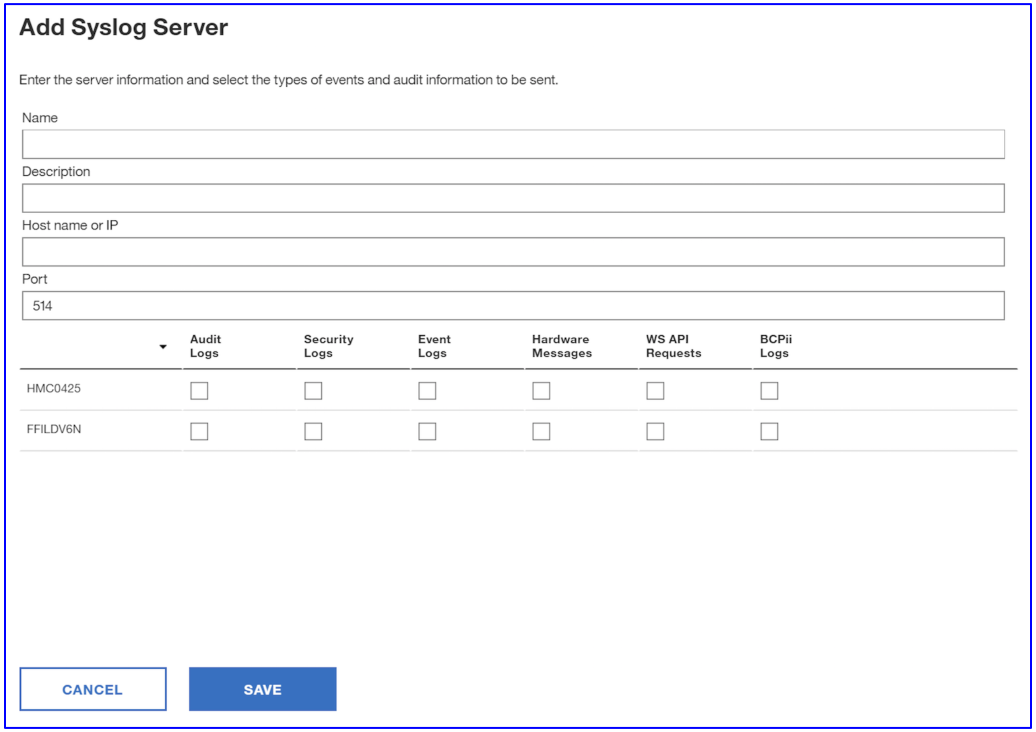
Configure syslog servers to receive logs, events, and messages from the HMC and systems.

	Name	Host name or IP	Port	Description
○	RemoteSyslogServer 1	9.47.77.215	514	Deployment-defined server 1.
○	RemoteSyslogServer 2	myauditserver.com	123	Deployment-defined server 2.
○	RemoteSyslogServer 3	server3.com	514	Deployment-defined server 3.

GUIDANCE

Add or remove configuration information for remote syslog servers.

For each syslog server, you may specify a host name or IP address, as well as a port where the server is listening for syslog messages. For each server you may also specify which consoles should send syslog messages to it, and what types of messages each console should send.



Add Syslog Server

Enter the server information and select the types of events and audit information to be sent.

Name

Description

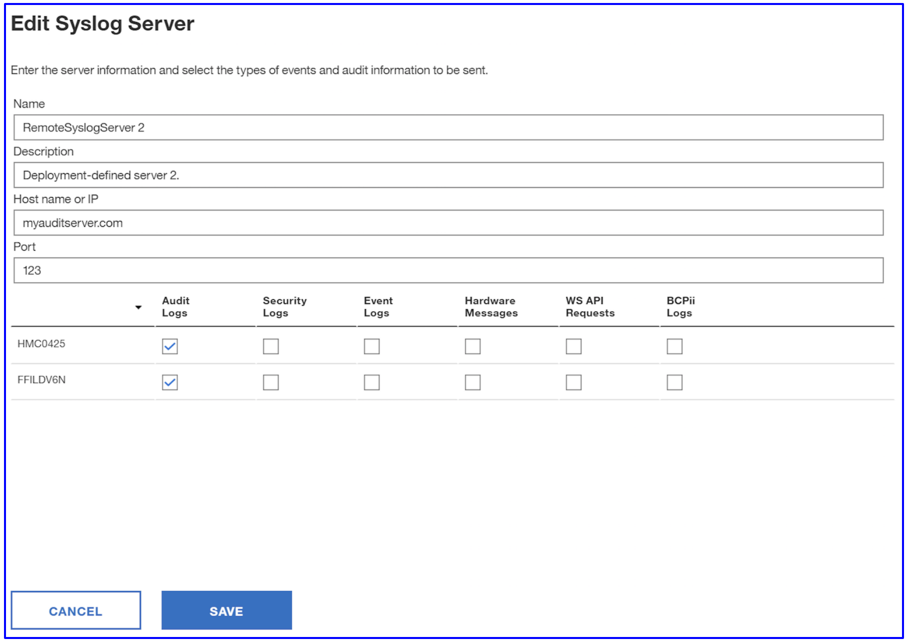
Host name or IP

Port

514

	Audit Logs	Security Logs	Event Logs	Hardware Messages	WS API Requests	BCPii Logs
HMC0425	□	□	□	□	□	□
FFILDV6N	□	□	□	□	□	□

Edit/Remove Syslog Servers



Edit Syslog Server

Enter the server information and select the types of events and audit information to be sent.

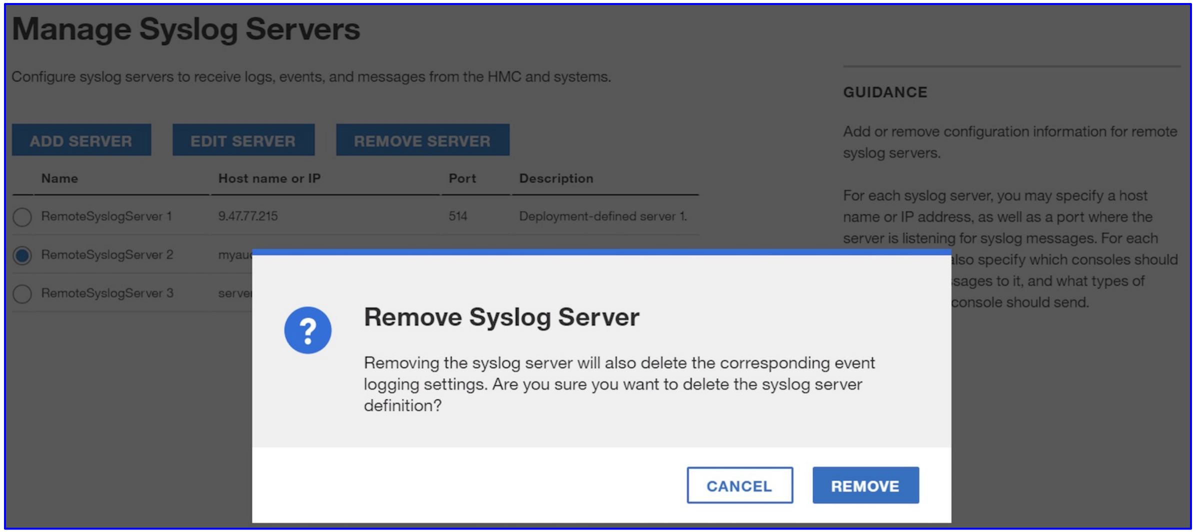
Name: RemoteSyslogServer 2

Description: Deployment-defined server 2.

Host name or IP: myauditserver.com

Port: 123

	Audit Logs	Security Logs	Event Logs	Hardware Messages	WS API Requests	BCPii Logs
HMC0425	☑	☐	☐	☐	☐	☐
FFILDV6N	☑	☐	☐	☐	☐	☐



Manage Syslog Servers

Configure syslog servers to receive logs, events, and messages from the HMC and systems.

	Name	Host name or IP	Port	Description
○	RemoteSyslogServer 1	9.47.77.215	514	Deployment-defined server 1.
●	RemoteSyslogServer 2	myau		
○	RemoteSyslogServer 3	serve		

GUIDANCE

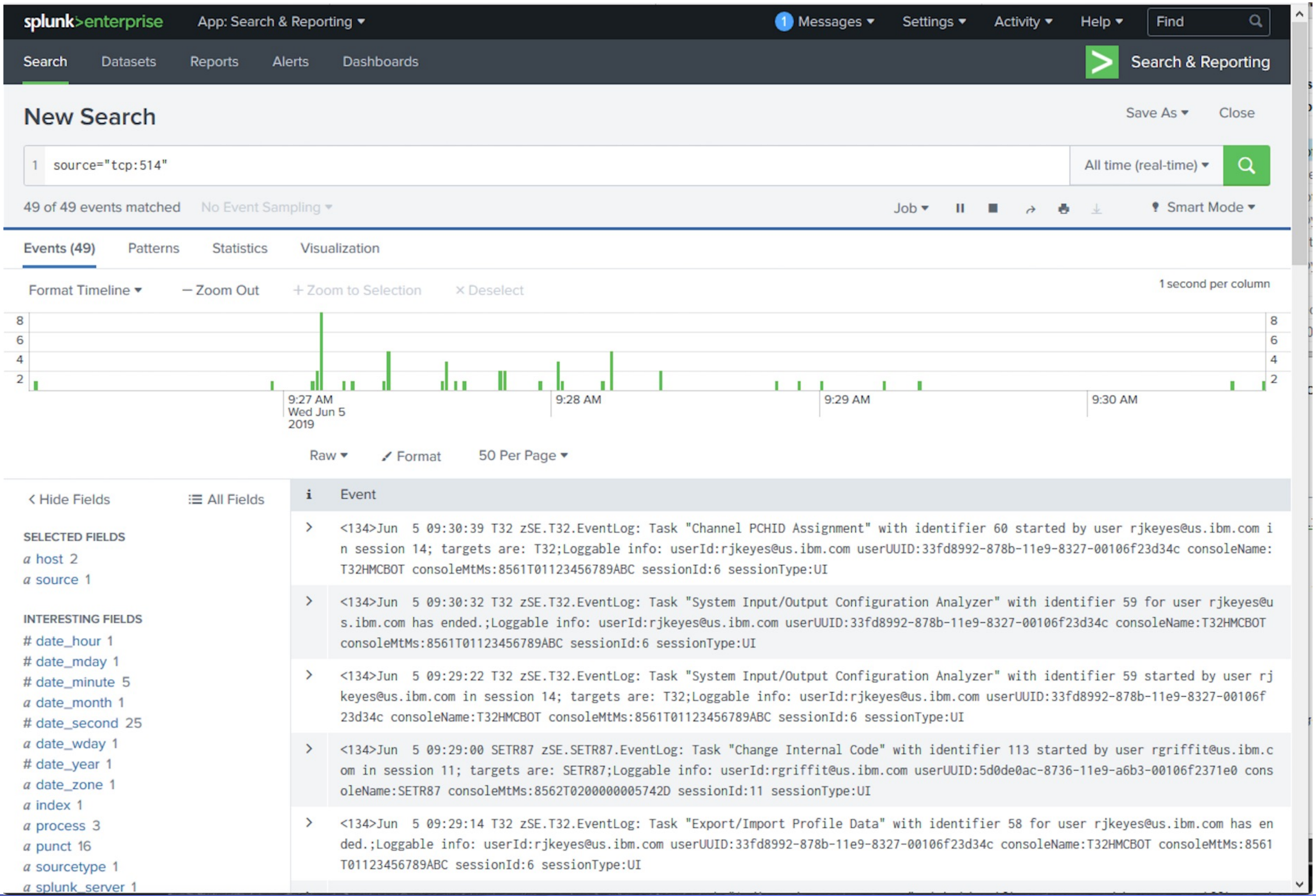
Add or remove configuration information for remote syslog servers.

For each syslog server, you may specify a host name or IP address, as well as a port where the server is listening for syslog messages. For each
also specify which consoles should
sages to it, and what types of
console should send.

Remove Syslog Server

Removing the syslog server will also delete the corresponding event logging settings. Are you sure you want to delete the syslog server definition?

Splunk Example Data



New Search

```
1  source="tcp:514"
```

All time (real-time) ▾

49 of 49 events matched   No Event Sampling ▾

SELECTED FIELDS

a host 2
a source 1

INTERESTING FIELDS

date_hour 1
date_mday 1
date_minute 5
a date_month 1
date_second 25
a date_wday 1
date_year 1
a date_zone 1
a index 1
a process 3
a punct 16
a sourcetype 1
a splunk_server 1

```
<134>Jun  5 09:30:39 T32 zSE.T32.EventLog: Task "Channel PCHID Assignment" with identifier 60 started by user rjkeyes@us.ibm.com in session 14; targets are: T32;Loggable info: userId:rjkeyes@us.ibm.com userUUID:33fd8992-878b-11e9-8327-00106f23d34c consoleName:T32HMCBOT consoleMtMs:8561T01123456789ABC sessionId:6 sessionType:UI

<134>Jun  5 09:30:32 T32 zSE.T32.EventLog: Task "System Input/Output Configuration Analyzer" with identifier 59 for user rjkeyes@us.ibm.com has ended.;Loggable info: userId:rjkeyes@us.ibm.com userUUID:33fd8992-878b-11e9-8327-00106f23d34c consoleName:T32HMCBOT consoleMtMs:8561T01123456789ABC sessionId:6 sessionType:UI

<134>Jun  5 09:29:22 T32 zSE.T32.EventLog: Task "System Input/Output Configuration Analyzer" with identifier 59 started by user rjkeyes@us.ibm.com in session 14; targets are: T32;Loggable info: userId:rjkeyes@us.ibm.com userUUID:33fd8992-878b-11e9-8327-00106f23d34c consoleName:T32HMCBOT consoleMtMs:8561T01123456789ABC sessionId:6 sessionType:UI

<134>Jun  5 09:29:00 SETR87 zSE.SETR87.EventLog: Task "Change Internal Code" with identifier 113 started by user rgriffit@us.ibm.com in session 11; targets are: SETR87;Loggable info: userId:rgriffit@us.ibm.com userUUID:5d0de0ac-8736-11e9-a6b3-00106f2371e0 consoleName:SETR87 consoleMtMs:8562T0200000005742D sessionId:11 sessionType:UI

<134>Jun  5 09:29:14 T32 zSE.T32.EventLog: Task "Export/Import Profile Data" with identifier 58 for user rjkeyes@us.ibm.com has ended.;Loggable info: userId:rjkeyes@us.ibm.com userUUID:33fd8992-878b-11e9-8327-00106f23d34c consoleName:T32HMCBOT consoleMtMs:8561T01123456789ABC sessionId:6 sessionType:UI
```

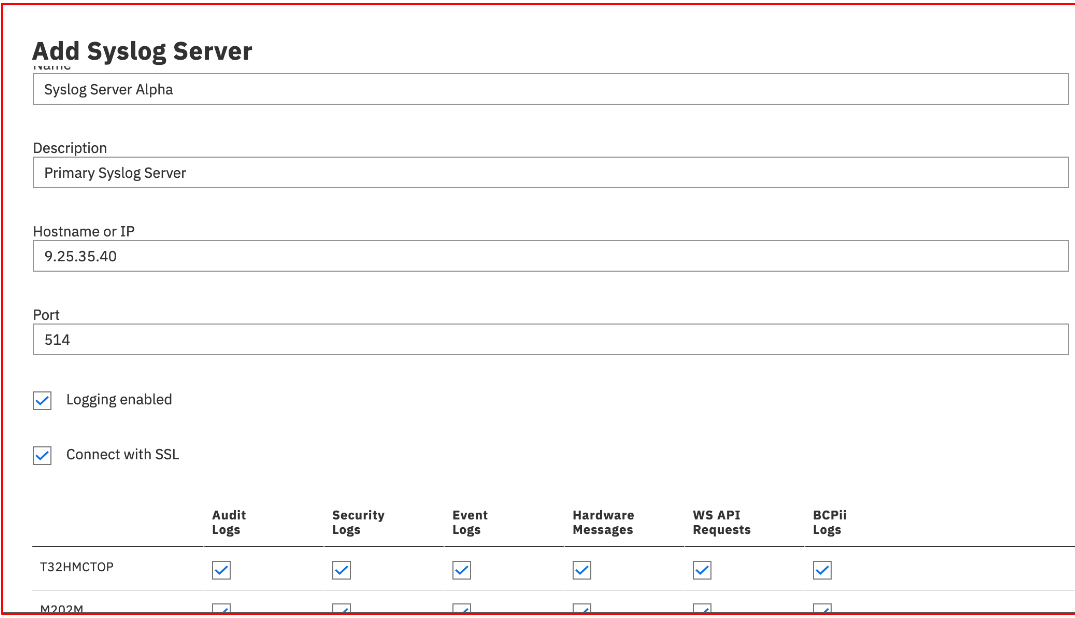
Forwarding connectivity

- **Recommendation:** HMC to SE network is isolated to HMC to SE/CPC network traffic
  - **Net result:** Forwarding from the HMC and SE work differently although they are configured in the same manner
    - *HMC:* For each configured remote syslog server, the HMC must have connectivity directly to the server.
    - *SE:* For each configured remote syslog server, there must be a managing HMC that has connectivity to that server.
      - **If there is such an HMC**, the SE will discover it automatically and proxy the forwarding through it.
        -- This is conceptually similar to SE tasks that support FTP today: the FTP traffic is automatically proxied through a capable discovered managing HMC.
      - **If an SE cannot locate an HMC** with connectivity, or if an **HMC does not have connectivity for its own logs**,
        - a rolling buffer of logs is kept for forwarding when connectivity is restored.
        - This exploits buffering capability built into rsyslog.

Remote Syslog Server enhancements

▶ z15 Initial Support

- Configure rsyslog to forward selected consolidated syslog entries from the HMC or managed SEs to customer-controlled syslog servers
  - Audit logs
  - Security logs
  - Console events
  - Hardware messages
  - Web Services API request logs
  - BCPii logs



Add Syslog Server

Name
Syslog Server Alpha

Description
Primary Syslog Server

Hostname or IP
9.25.35.40

Port
514

☑ Logging enabled

☑ Connect with SSL

	Audit Logs	Security Logs	Event Logs	Hardware Messages	WS API Requests	BCPii Logs
T32HMCTOP	☑	☑	☑	☑	☑	☑
M202M	☑	☑	☑	☑	☑	☑

▶ Enhancements

- z14 CPC support in addition to z15 CPC
- HMC Data Replication support
- Support of SSL connections between HMC and syslog server
- Support *IBM QRadar DSM for IBM Z Hardware Management Console*