HP Enterprise Security

HP Enterprise Security Products User Group 2014

Learn. Network. Share.

Checkpoint Connector Troubleshooting

Salvatore Alba

TAM Premier Support

Frankfurt – 03 April 2014

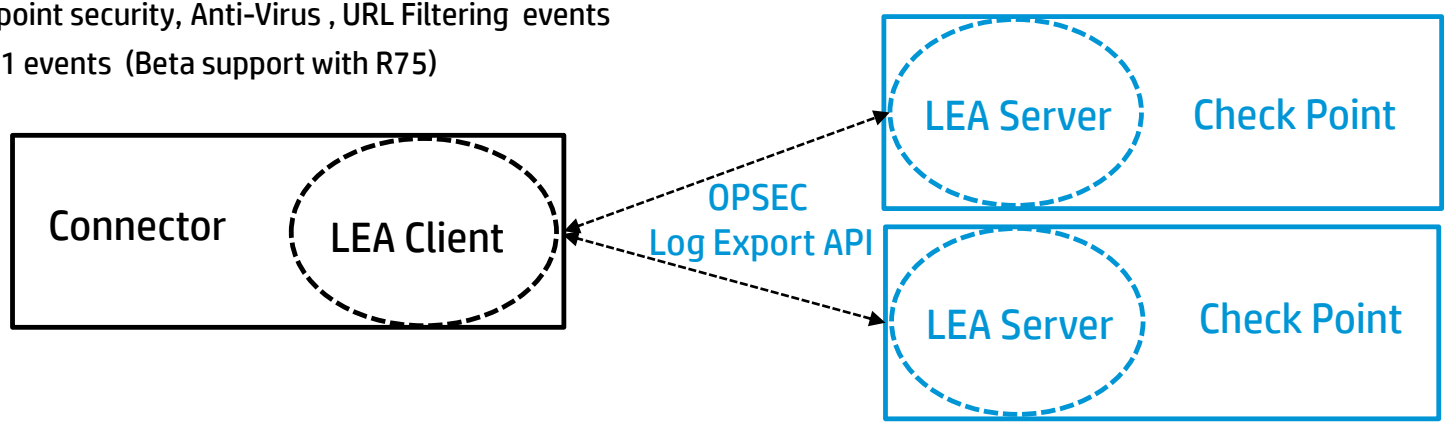
Agenda

- Introduction
- Device and Connector Configuration
- Connector Operation
- Common Problems and Troubleshooting
- Recommendations

Checkpoint Connector Troubleshooting

Introduction

- **Retrieves log data from Checkpoint devices such as**
  - Checkpoint FW1/VPN1, Checkpoint Provider-1
- **Versions supported**
  - R65, R70, R71, R75, and R76
- **Supported on platforms**
  - Windows, Linux, Solaris (Solaris 11 x86 not supported)
- **Uses Checkpoint OPSEC Log Export API to retrieve the following types of events**
  - Endpoint security, Anti-Virus , URL Filtering events
  - IPS-1 events (Beta support with R75)



Checkpoint Connector Troubleshooting

Device and Connector Configuration

- **Choose the Connection Type**
  - sslca (default and preferred)
  - ssl_opsec (not supported on connector appliance)
  - clear
- **Configure the Checkpoint**
  - Edit fwopsec.conf for the lea server port, authentication type and authentication port (**all connection types**)
  - Configure a new OPSEC application object and note down the activation key (**sslca , ssl_opsec**)
  - Obtain and note down the OPSEC SIC Name and OPSEC Entity SIC Name (**sslca, ssl_opsec**)
  - Establish an authentication key (**ssl_opsec**)
- **Configure the Lea Client on Connector**
  - Add "$ARCSIGHT_HOME/bin/agent/checkpoint/OPSECAD/linux " to LD_LIBRARY_PATH (**on linux only)**
  - Pull the certificate from lea server using the activation key (**sslca**)
  - Pull the authentication key from lea server using activation key (**ssl_opsec**)

Note: 1) See the configuration guide for the specific details

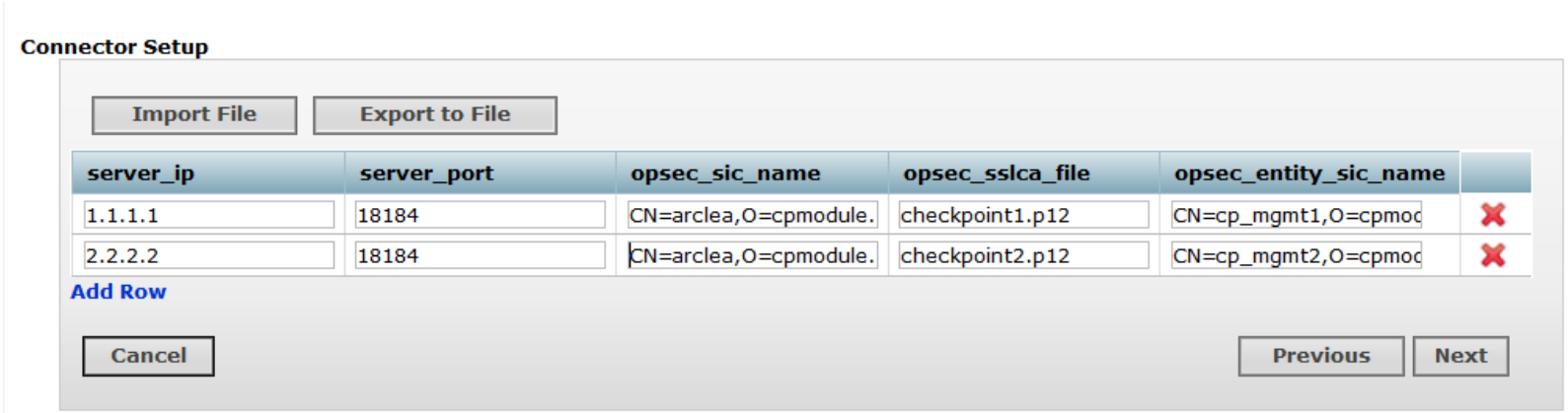
2) $ARCSIGHT_HOME refers to /<Connector Installation Folder>/current

Checkpoint Connector Troubleshooting

Device and Connector Configuration

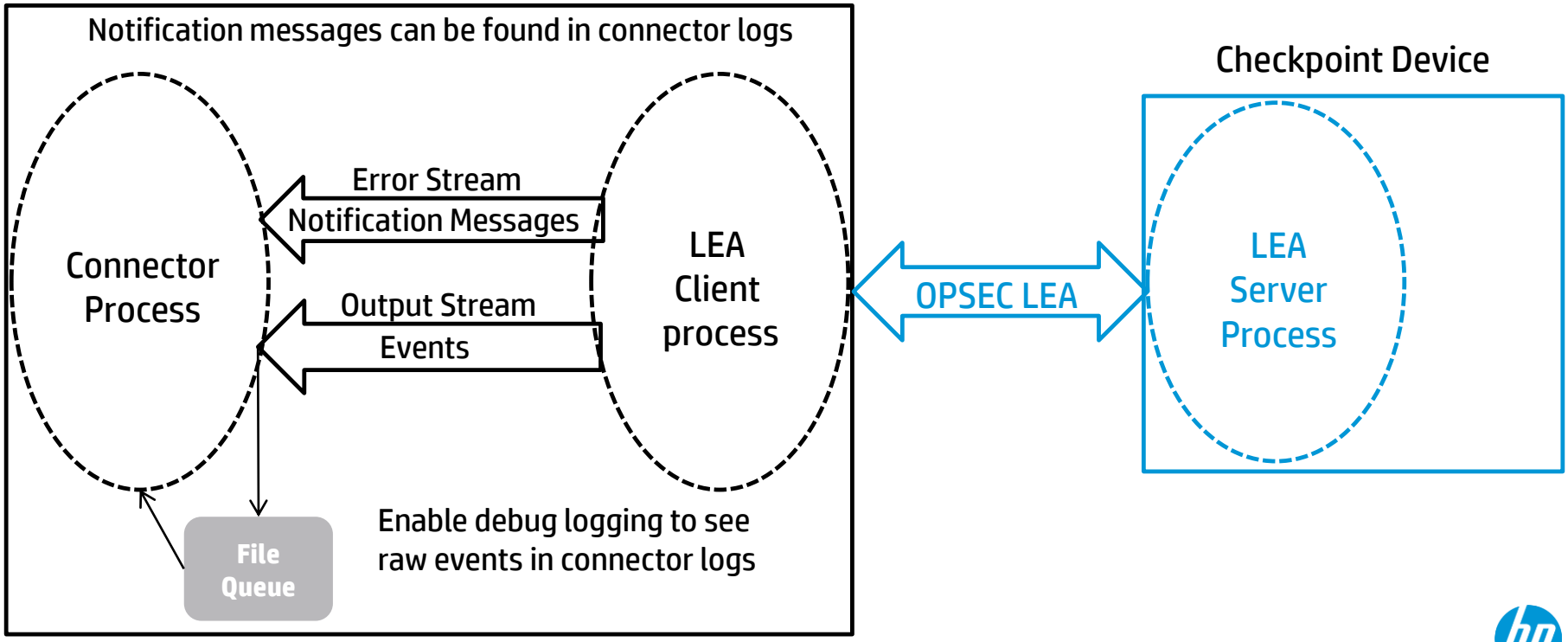
- **Follow up configuration on Checkpoint**
  - Make sure that a trust has been established between lea client and lea server
  - Install firewall policy to allow the connector to communicate with the checkpoint server
- **Configure the Connector**
  - Configure the connection type
  - Add a row for each of the Checkpoint Servers with the information noted on the previous slide

Note: See the configuration guide for the specific details

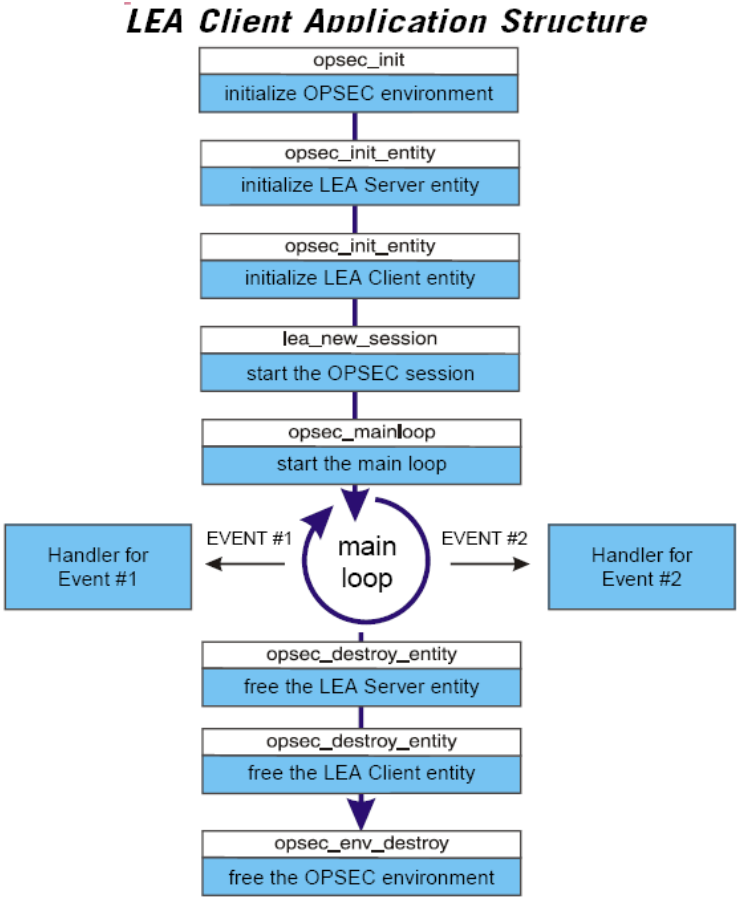


Checkpoint Connector Troubleshooting

Basic Connector operation



Checkpoint Connector Troubleshooting



- Creates two sessions
  - Audit log session
  - Security log session

Checkpoint Connector Troubleshooting

Notification Messages – Meaning and Processing

Message	Meaning and Processing
MSG13	All sessions created and LEA client entered OPSEC main loop. Connector sets the state for all the devices to be up
MSG17	Lea client got the first checkpoint event
MSG18	Log file has ended in one of the sessions
MSG19	Log file has been switched in one of the sessions
MSG25	One of the sessions of an lea server has ended. Connector sets the device state to be down
MSG29	Lea client re-established the session of an lea server. Set the device state to be up
MSG16	Lea client got no response from one of the lea servers for a scheduled ping
MSG15	Trying to reconnect with an Lea Server. Restart connector if no. of reconnects > checkpoint.reconnect (default=30)
MSG14	OPSEC main loop ended
MSG22	Lea client ended abnormally

Checkpoint Connector Troubleshooting

Event Collection and Parsing

- **Lea Client**
  - OPSEC main loop calls Lea Client's callback function LeaRecordHandler
  - Constructs a log line consisting of key value pairs from the fields and values inside the Lea Record
  - Sends the constructed log line out on its standard output stream to connector process

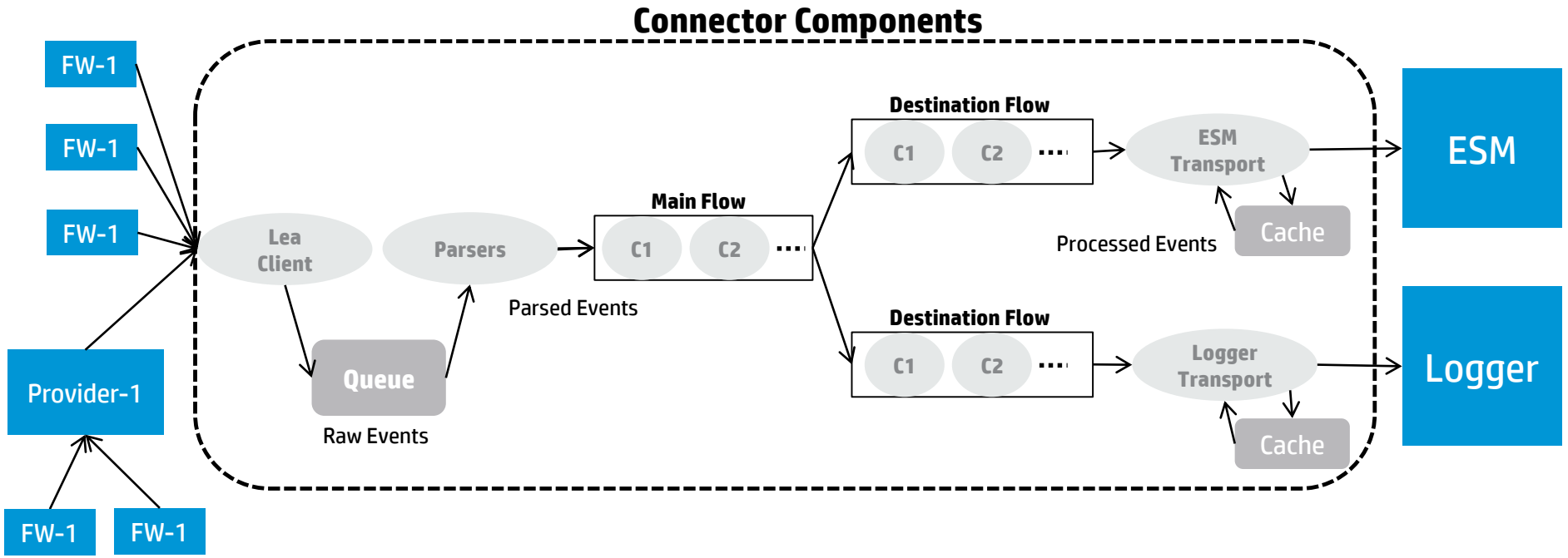
```
<A>time@= 3Jul2004  1:29:04@&action@=accept@&orig@=167800760@&i/f_dir@=outbound@&has_accounting@
=0@&product@=SmartView Reporter Log Consolidator@&Operation@=Log Out@&Administrator@=localhost@&
Machine@=host184@&Subject@=Administrator Login@&Operation Number@=9

<S>time@= 2Jul2004 14:36:56@&action@=accept@&orig@=167800760@&i/f_dir@=inbound@&i/f_name@=EL90BC
6@&has_accounting@=0@&product@=VPN-1 & FireWall-1@&__policy_id_tag@=product=VPN-1 & FireWall-1[d
b_tag={2F7841A0-5A83-4E52-BB04-57F674692064};mgmt=host184;date=1088126102;policy_name=defaultfil
ter]@&src@=3232240868@&s_port@=3107@&dst@=167800760@&service@=FW1_lea@&proto@=tcp@&rule@=1
```

- **Connector**
  - Receiver thread receives the log line and dumps it at the end of the file queue
  - Reader thread reads a log line from the beginning of the file queue
  - If the log line starts with <A>, it is passed to the audit log parser
  - If the log line starts with <S>, it is passed to the security log parser
  - Parsers normalize the logline and produce an ArcSight security event

Checkpoint Connector Troubleshooting

Event Flow



Checkpoint Connector Troubleshooting

Event Flow

Event Reception	Event Queuing	Event Parsing	Event Processing	Event Transport
• Lea client collects the Lea Records from Lea server • Lea client converts the Lea Records into log lines of key value pairs • Lea client prints the log lines to standard output stream	• Connector receives log lines from lea client • Writes them to a queue of files on the file system in the order in which they are received	• Connector picks up the log lines from the file queue in a FIFO manner and parses them • Checkpoint key value pairs are normalized into Arcsight event	• Normalized events are categorized and processed in many ways useful for correlation and asset modeling • Events are batched, filtered or aggregated as required for efficiency	• Enriched ArcSight events are sent to ESM/Logger destination • Events cached when destinations are down and resent when they are back up

Checkpoint Connector Troubleshooting

Common Problems

Common problems encountered fall into one of these areas

- Configuration problems
- Connectivity loss
- Parsing and mapping issues
- Performance issues

Checkpoint Connector Troubleshooting

Port Configurations

- **Problem**
  - Connector unable to connect with checkpoint due to mistakes done in port configuration
- **Solution**
  - The lea server port and authentication ports differ based on the connection type
  - The following parameters should be present in **fwopsec.conf** file based on the connection type

Connection Type	Configuration
clear	*lea_server port 18184* *lea_server auth_port 0*
ssl_opsec	*lea_server auth_port 18184* *lea_server port 0* *lea_server auth_type ssl_opsec*
sslca	*lea_server auth_port 18184* *lea_server port 0* *lea_server auth_type sslca*

Note: Any changes done to the **fwopsec.conf** file will require the firewall service be restarted using **cpstart/cpstop** command

Checkpoint Connector Troubleshooting

SIC Activation Key

- **Some tips related to the SIC activation key**
  - SIC Activation Key needs to be initialized before pulling the cert from the LEA Client.
  - It must be initialized with one time password and Trust state appears as “Initialized but trust not established”.
  - Once the cert is pulled successfully, the Trust state will change to “Trust established”.
  - It is not possible to pull the cert again when the Trust state is already in “Trust established” state.
  - If the cert in the LEA client has been deleted, the Object SIC Communication Activation Key will need to be reset again using the same process.

Initial state when password is entered. Click on the “Initialize”

State when it is initialized but cert has not been pulled

State when cert has been pulled successfully

Checkpoint Connector Troubleshooting

Certificate Location

- **Problem**
  - Certificates are pulled to the wrong location
  - The ‘opsec_pull_cert’ utility is located in **$ARCSIGHT_HOME/bin/agent/checkpoint/OPSECAD/<platform>** folder
  - When the utility is executed from this location, it is very common to see the certificate pulled in to the same location

- **Solution**
  - Connector and the lea client expect the certificate to be present under **$ARCSIGHT_HOME/user/agent/checkpoint** folder
  - The certificate needs to be manually copied to this location or pulled into the right place by specifying the complete path

Checkpoint Connector Troubleshooting

Missing .DLL files in Windows Environment

- **Problem**
  - In some Windows environments, the Lea client fails to run because of the following .DLL files missing

    msvcp71.dll

    msvcr71.dll

- **Solution**
  - Download and copy the missing .DLL files into one of the following locations

    C:\Windows\SysWOW64 (On 64 bit Windows)

    C:\Windows\System32 (On 32 bit Windows)

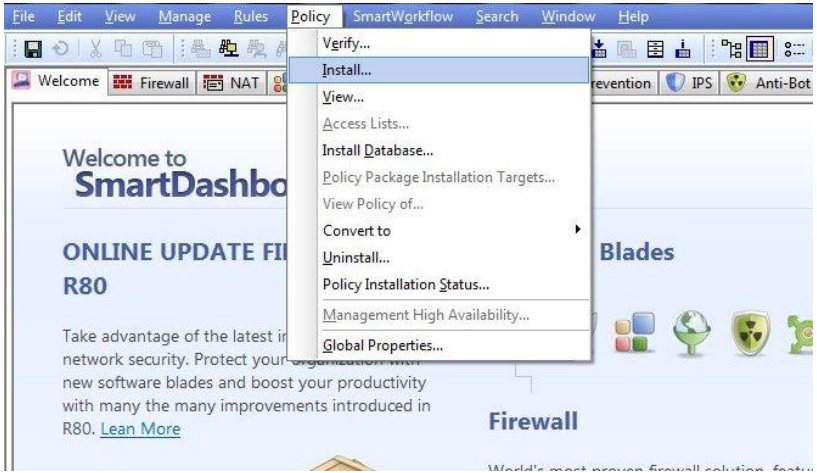
  - If the .DLL files still cannot be found by the Lea client, then copy them to the following folder

    $ARCSIGHT_HOME\bin\agent\checkpoint\OPSECAD\win32

Checkpoint Connector Troubleshooting

Policy Installation

- **Problem**
  - After creating the object on the Checkpoint SmartDashboard to allow the connector to communicate with it, it is often forgotten to install the policy
- **Solution**
  - This can be easily achieved by going to the Checkpoint SmartDashboard, selecting the Policy in the main menu and then select “Install..”



Checkpoint Connector Troubleshooting

Enabling Debug Logging

- Can be useful for troubleshooting problems where normal logging does not reveal the root cause
- Produces more verbose output in the connector logs, not recommended in production as it affects performance
- Log files rotate and wrap up faster because of significantly higher amount of logging
- Log file size and count may need to be increased to prevent losing information

Connection Type	Configuration
Enable debug logging	Add the following properties into **user/agent/agent.properties** *log.global.debug=true* *log.channel.file.property.package.com.arcsight=0*
Increase log file and size	Add the following properties into **user/agent/agent.properties** *log.channel.file.property.maxsize=20MB* *log.channel.file.property.maxbackupindex=20*
Increase the wrapper log file and size	Add the following properties into **user/agent/agent.wrapper.conf** *wrapper.logfile.maxsize=20m* *wrapper.logfile.maxfiles=20*

Note: Any changes done to **agent.properties** or **agent.wrapper.conf** file will require a connector restart

Checkpoint Connector Troubleshooting

Running the Lea Client in debug mode

- Notification messages from the lea client do not reveal communication problems between the lea client and server
- Enabling debug logging on the connector does not enable debug logging in lea client
- Lea client needs to be run separately in a terminal in debug mode for more advanced troubleshooting
  - `C:\>cd Connector\current\bin\agent\checkpoint\OPSECAD\win32`
  - `C:\Connector\current\bin\agent\checkpoint\OPSECAD\win32>set OPSEC_DEBUG_LEVEL=3`
  - `C:\Connector\current\bin\agent\checkpoint\OPSECAD\win32>lea_client -d on -m online -t clear -h 'LEA server IP Address' -p 18184 2>&1 output.txt`

```
Parsed Lea Client Input Parameters
CINFO server[0] type=sslca ip=10.248.0.111 port=18184 sic_name=CN=arcsight_lea,O=fw-mg-ccm.sede
sslca_file=opsec.p12 entity_sic_name=CN=cp_mgmt,O=fw-mg-ccm.sede.corp.sanpaoloimi.com.7n7tg4
MSG04 Created OPSEC environment
MSG06 Create OPSEC LEA client
MSG08 Created OPSEC LEA server entity
MSG26 Called LeaStartHandler : session( 137703632 )
MSG10 Created security log session
MSG26 Called LeaStartHandler : session( 137703824 )
MSG12 Created audit log session
SINFO server[0]ip= 10.248.0.111 security_log_session=137703632 audit_log_session=137703824
MSG13 Start OPSEC opsec_mainloop ...
MSG25 Ended session : One security/audit log session( 137703632 ) ends
MSG25 Ended session : One security/audit log session( 137703824 ) ends
MSG14 End OPSEC opsec_mainloop
MSG15 Try to connect LEA server again ...
```

Checkpoint Connector Troubleshooting

Connectivity Loss

- Lea client some times loses connectivity with one or more Lea servers
- After a few attempts to reconnect, the connector will forcefully restart
- In some scenarios, **it is possible that loss of connection is not even detected**
  - Event collection stops
  - Restarting the checkpoint server does not help
  - Only restarting the connector helps
  - Run the connector in debug mode and collect the logs
  - Run the lea client offline in debug mode and capture the output
  - If possible collect the Lea server logs too
  - Contact support

Checkpoint Connector Troubleshooting

Event delays and losses due to queuing

With high event volumes, file queue can build up faster leading to significant delays

- **When file queue becomes full, connector starts dropping events**
- Enable checkpoint parser multithreading (may need to follow up with memory increase if required)
- Increase the file queue size and/or file queue count

Parameter	Default	Recommendation
checkpoint.parser.multithreading.enabled	false	Set it to 'true' to enable multithreading
checkpoint.parser.threadcount	-1	Set it to a specific value or leave it at -1 for the connector to decide the number of threads based on number of cores in the CPU
checkpoint.parser.threadsperprocessor	-1	Takes effect only when the threadcount is set to -1. Total number of threads = number of processors * threadsperprocessor
filequeuemaxfilecount	100	Increases the number of files in the file queue
filequeuemaxfilesize	100000	Increases the size of each file in the file queue

Checkpoint Connector Troubleshooting

Event delays and losses due to caching

- Caching can occur due to problems with the destination or network latencies
- Excessive caching can cause event delays
- When the cache becomes full, connector overwrites the oldest events with newer events causing event loss
- If the root cause of caching is network latency, then enabling multithreading on the transport helps
- Increasing the cache size helps in holding the events for a longer period in cache without being overwritten

Parameter	Default	Recommendation
http.transport.threadcount	1	Set it to N (<= number of cores in the CPU)
transport.loggersecure.threads	1	Set it to N (<= number of cores in the CPU)

Checkpoint Connector Troubleshooting

Current Limitations and Recommendations

- Limitation
  - Most connectors run on a 32bit JVM even on 64bit platforms. This includes the Checkpoint connector. The LEA Client is currently 32bit too.
  - Maximum theoretical memory heap size is 4GB. But in practice this limit is much lower due to other constraints such as available swap, kernel address space usage, memory fragmentation, contiguously locatable memory on the operating system, JVM overhead and total available memory on the system versus the number of connectors and other processes running on the system. General guidelines for the heap size limits are as follows.
    - 1024MB on Connector Appliances
    - 1536MB Windows platform
    - 2048MB on Linux and Solaris operating systems

- Recommendation
  - The JVM memory limitation, this brings to the limitation of maximum EPS of 1500-1800. If the current connection of the connector is to Provider-1 which has consolidated firewall logs coming from various Firewall-1s, we would recommend to have multiple instance of Connectors, connecting directly to the Firewall-1. Alternatively, have multiple instances of Provider-1 with one connector connecting to each instance. This will help to distribute the load.

Q & A

Thank you