

**MDR – SmartConnector Best Practices Document**

MDR – SmartConnector Best Practices & Optimization Parameters Document



TABLE OF CONTENTS

[1. Executive Summary 3](#_Toc5011667)

[2. Standard SmartConnector Parameters 3](#_Toc5011668)

[2.1 Field Based Aggregation (Section – 1) 4](#_Toc5011669)

[a) Checkpoint Firewall (SYSLOG Based Forwarding) 4](#_Toc5011670)

[b) Oracle Database 4](#_Toc5011671)

[c) All Firewalls (SYSLOG Based Forwarding) 4](#_Toc5011672)

[d) All IPS (SYSLOG Based Forwarding) 4](#_Toc5011673)

[e) Microsoft IIS (Web Servers) 5](#_Toc5011674)

[f) FTP Servers 5](#_Toc5011675)

[g) Microsoft Windows Servers 5](#_Toc5011676)

[h) Microsoft SQL Database 5](#_Toc5011677)

[2.2 Filters (Section - 2) 5](#_Toc5011678)

[a) Microsoft Windows Servers 5](#_Toc5011679)

[b) Checkpoint Firewall (SYSLOG Based Forwarding) 5](#_Toc5011680)

[c) Cisco ASA (SYSLOG Based Forwarding) 5](#_Toc5011681)

[d) Fortigate Firewall (SYSLOG Based Forwarding) 6](#_Toc5011682)

[e) Palo Alto Firewall (SYSLOG Based Forwarding) 6](#_Toc5011683)

[f) SonicWall Firewall (SYSLOG Based Forwarding) 6](#_Toc5011684)

[3. Additional Configurations 6](#_Toc5011685)

1. Executive Summary

The document provides details and standard parameters which as part of our best practices and optimization configuration which needs to be configured on the SmartConnectors across different deployment models. And the configurations are only applicable for ArcSight Logger destinations and not applicable to ArcSight ESM

1. Standard SmartConnector Parameters

Before you install and configure any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger) and the connectivity is established. After installing the connectors to communicate with Logger, you can set up their properties through the connector Configuration Wizard, proceed with the next steps as per below

1. Using the $ARCSIGHT\_HOME\current\bin\runagentsetup script, run the connector configuration program.
2. After running the wizard, **Modify Connector** is selected by default. Do not change this selection.
3. Click **Next**. On the window displayed, select **Add, modify, or remove destinations**.
4. Make sure your destination is selected and click **Next**.
5. Select **Modify destination settings** to configure the following parameters:
6. Modify the parameters for each destination as per below table

|  |  |  |
| --- | --- | --- |
| **Main Parameter** | **Sub Parameter** | **Values** |
| **Cache** | Cache Size | 5 GB |
| **Network** | Enable Name Resolution | No |
| Name Resolution Domain from email | No |
| Clear hostname as IP address | No |
| Address-Based Zone Population Defaults Enabled | No |
| Zone Population Mode | No Zoning (clear) |
| Customer URI | Enter <customerName> |
| **Field Based Aggregation** | Time Interval | 1 minute |
| Event Threshold | 100 events |
| Field Name | Refer to Section 1 for aggregation fields with respective to the log sources |
| Preserve common fields | Yes |
| **Processing** | Enable Device Status Monitoring (in millisec) | 900000 |
| **Filters** | Filter Out | Refer to Section 2 for filtering queries with respective to the log sources |

***Note:*** *Incase of “Customer Name”, make sure the appropriate customer names are inputted which is received from the ADR Team incase of MDR on Cloud Customers and for On-Prem customers the customer name should be configured by the implementation team and inputted in the above parameter.*

* 1. Field Based Aggregation (Section – 1)

1. Checkpoint Firewall (SYSLOG Based Forwarding)

deviceAddress,deviceVendor,deviceProduct,deviceEventClassId,deviceSeverity,sourceAddress,destinationAddress,destinationPort,name,message,sourceUserName,destinationUserName,fileName,deviceCustomString1,deviceCustomString2,deviceCustomString3,deviceHostName,sourceHostName,destinationHostName,sourceTranslatedAddress,destinationTranslatedAddress,agentAddress

1. Oracle Database

deviceAddress,deviceVendor,deviceProduct,deviceEventClassId,deviceSeverity,agentAddress,agentSeverity,sourceAddress,destinationAddress,destinationPort,name,destinationUserName,fileName

1. All Firewalls (SYSLOG Based Forwarding)

deviceAddress,deviceVendor,deviceProduct,deviceEventClassId,deviceSeverity,agentAddress,sourceAddress,destinationAddress,destinationPort,name,message,sourceUserName,destinationUserName,fileName,deviceCustomString1,deviceCustomString2,deviceCustomString3,deviceHostName,sourceHostName,destinationHostName,deviceAction

1. All IPS (SYSLOG Based Forwarding)

deviceAddress,deviceVendor,deviceProduct,deviceEventClassId,deviceSeverity,agentAddress,sourceAddress,destinationAddress,destinationPort,name,message,sourceUserName,destinationUserName,fileName,deviceCustomString1,deviceCustomString2,deviceCustomString3,deviceCustomString4,deviceCustomString5,deviceCustomString6,deviceHostName,sourceHostName,destinationHostName

1. Microsoft IIS (Web Servers)

deviceAddress,deviceVendor,deviceProduct,deviceEventClassId,deviceSeverity,agentAddress,sourceAddress,destinationAddress,destinationPort,name,message,sourceUserName,destinationUserName,fileName,deviceCustomString1,deviceCustomString2,deviceCustomString3,deviceHostName,sourceHostName,destinationHostName

1. FTP Servers

deviceAddress,deviceVendor,deviceProduct,deviceEventClassId,deviceSeverity,agentAddress,sourceAddress,destinationAddress,destinationPort,name,message,sourceUserName,destinationUserName,fileName,deviceCustomString1,deviceCustomString2,deviceCustomString3,deviceHostName,sourceHostName,destinationHostName

1. Microsoft Windows Servers

deviceAddress,deviceVendor,deviceProduct,deviceEventClassId,deviceSeverity,agentAddress,sourceAddress,destinationAddress,destinationPort,name,message,sourceUserName,destinationUserName,fileName,deviceCustomString1,deviceCustomString2,deviceCustomString3,deviceHostName,sourceHostName,destinationHostName,deviceCustomString4,deviceCustomString5,deviceCustomString6,flexString1,flexString2

1. Microsoft SQL Database

deviceAddress,deviceVendor,deviceProduct,deviceEventClassId,deviceSeverity,deviceInboundInterface,agentAddress,agentSeverity,sourceAddress,destinationAddress,destinationPort,name

* 1. Filters (Section - 2)

1. Microsoft Windows Servers

( deviceVendor EQ "Microsoft" And ( deviceEventClassId EQ "Microsoft-Windows-Security-Auditing:594" Or deviceEventClassId EQ "Microsoft-Windows-Security-Auditing:4656" Or deviceEventClassId EQ "Microsoft-Windows-Security-Auditing:4658" Or deviceEventClassId EQ "Microsoft-Windows-Security-Auditing:4662" Or deviceEventClassId EQ "Microsoft-Windows-Security-Auditing:5140" Or deviceEventClassId EQ "Microsoft-Windows-Security-Auditing:4768" Or deviceEventClassId EQ "Microsoft-Windows-Security-Auditing:5156" Or deviceEventClassId EQ "Microsoft-Windows-Security-Auditing:4769" ) )

1. Checkpoint Firewall (SYSLOG Based Forwarding)

( deviceProduct EQ "VPN-1 & FireWall-1" AND deviceAction EQ "Accept" )

1. Cisco ASA (SYSLOG Based Forwarding)

( deviceProduct EQ "ASA" And ( name StartsWith "FTP connection from" Or name StartsWith "No matching connection" Or name StartsWith "Deny inbound (No xlate) tcp" Or name StartsWith "Teardown" Or name StartsWith "Built" ) )

1. Fortigate Firewall (SYSLOG Based Forwarding)

( deviceVendor EQ "Fortinet" And ( deviceAction EQ "accept" Or deviceAction EQ "close" ) )

1. Palo Alto Firewall (SYSLOG Based Forwarding)

( deviceVendor EQ "Palo Alto Networks" And name = “TRAFFIC” And deviceAction EQ "allow" )

1. SonicWall Firewall (SYSLOG Based Forwarding)

( deviceVendor EQ SonicWall And name EQ "Connection Opened" )

***Note:*** *Incase the logs from different log sources are being received in a single Syslog Connector, validate the combination of the above filters in the Logger first and then apply accordingly on the SmartConnector.*

1. Additional Configurations

Below are the additional configurations which needs to be configured on every SmartConnector installed based on the criteria’s defined below

|  |  |
| --- | --- |
| **Received EPS (Per Connector)** | **Additional Configurations Involved** |
| < 150 | Connector JVM – **256 MB**  Multi-Threading – **No** |
| 150 - 300 | Connector JVM – **512 MB**  Multi-Threading – **No** |
| 300 - 1000 | Connector JVM – **1 GB**  Multi-Threading – **Yes** |
| > 1000s | Connector JVM – **2 GB**  Multi-Threading – **Yes** |

***Note:*** *EPS beyond 1000 on a single SmartConnector, both filtering and aggregation must be relooked and accordingly optimize the EPS.*

Below are the steps mentioned on how to configure the JVM and Multi-Threading on the SmartConnector

1. **JVM Configuration**
2. Navigate to following path ***$ARCSIGHT\_HOME\current\user\agent\*** and open the file agent.wrapper.conf in your selected file editor and modify the **“initmemory”** & **“maxmemory”** values highlighted in Yellow with the values as per the criteria’s defined above

# Java Additional Parameters (additional parameters will now be written programmatically)

# wrapper.java.additional.1=

# Initial Java Heap Size (in MB)

wrapper.java.initmemory=1024

# Maximum Java Heap Size (in MB)

wrapper.java.maxmemory=2048

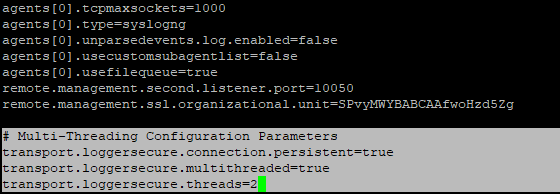
1. **Multi-Threading Configuration**
2. Navigate to following path ***$ARCSIGHT\_HOME\current\user\agent\*** and open the file agent.properties in your selected file editor and add the below mentioned lines at the end of the file as per the criteria’s defined above (Refer snapshot below for better clarity)

# Multi-Threading Configuration Parameters

transport.loggersecure.connection.persistent=true

transport.loggersecure.multithreaded=true

transport.loggersecure.threads=2





**Head Office:** 11480 Commerce Park Drive, Suite 210, Reston, VA 20191 USA. Ph: +1-703-8713934

**Bangalore:** +91-80-42543444, **Doha:** +97433559018, **Dubai:** +971-4-2595526, **Kuala Lumpur:** +60-3-7660-4988, **London:** +44(0)2071487475, **Mumbai:** +9102233655151, **Yes:** +966(0)114725163, **Toronto:** +1-416-273-5004, **Virginia:** +1-703-8713934

sales@paladion.net | www.paladion.net