CSN32: Are You a Smart Connector?

Mark Ulmer

Apollo Group Inc. | IT Services

Sr. Security Systems Engineer

September 13th, 2011

The Apollo Group

Our Challenge

Apollo Group is a publicly traded parent company that owns the University of Phoenix and a number of other subsidiaries in the education arena. With 300 physical locations in six countries, 500,000 students, 50,000 faculty and 22,000 employees, Apollo Group has a formidable challenge in securing all its systems, data and endpoints.

Reference:
http://www.arcsight.com/collateral/case_studies/ArcSight_CaseStudy_Apollo.pdf

Audience

- Who is this talk for?
  - ArcSight administrators
  - Those who need to keep ArcSight well fed
  - Focus on ArcSight SmartConnector software for Windows & Unix/Linux
- ArcSight SmartConnector version
  - We assume version 5.0.x
- Participation
  - I don't mind questions, yet please be mindful of time
  - There's always the hallways and email

Agenda

Why software connectors?

Basics

- Connector installs
- Anatomy of a connector folder
- Running as a service
- Config files
  - agent.properties file
  - agent.default.properties file
- Log files
  - Reading the agent.log
  - Reading the agent.out.wrapper.log

Tuning

- Logging levels
- Connector JVM memory

Analysis

- Running RegEx
- Running LogFu on connector logs
- Reading connector-status.log file

Tips

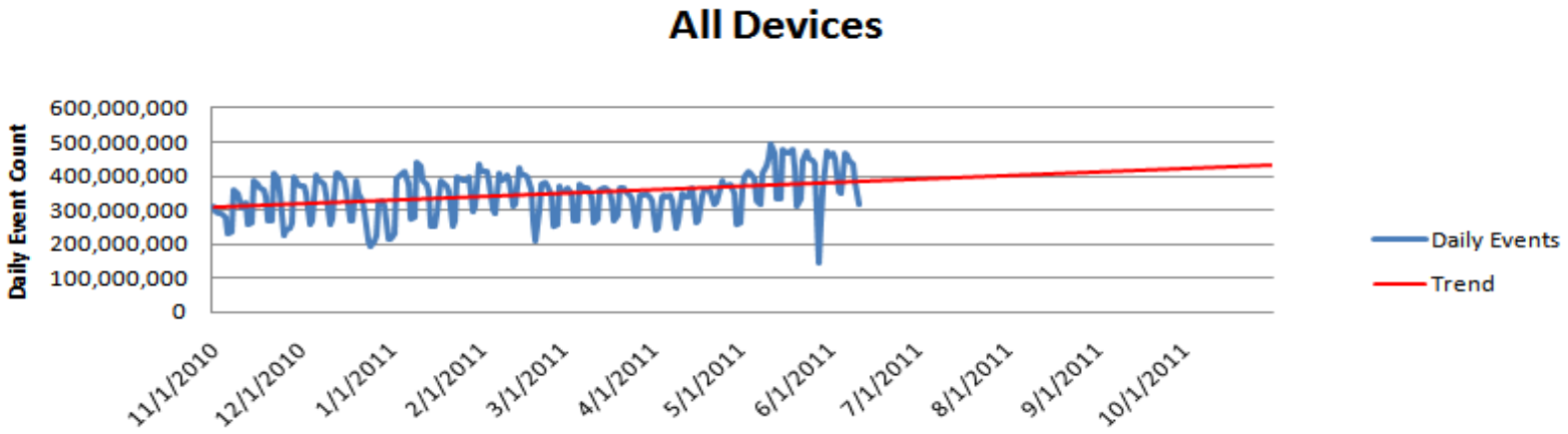
- Command line 'Get Status'
- KB Articles
- Silent Install headaches
- Connector removal
- Clean up time

Q & A

Why software based SmartConnectors?

Problem statement:

- Apollo has 400M daily events.
- Unix syslog connector alone peeks at Max E/s 2,500.
- A Connector Appliance model C5100 | Rated for ~5000 E/s

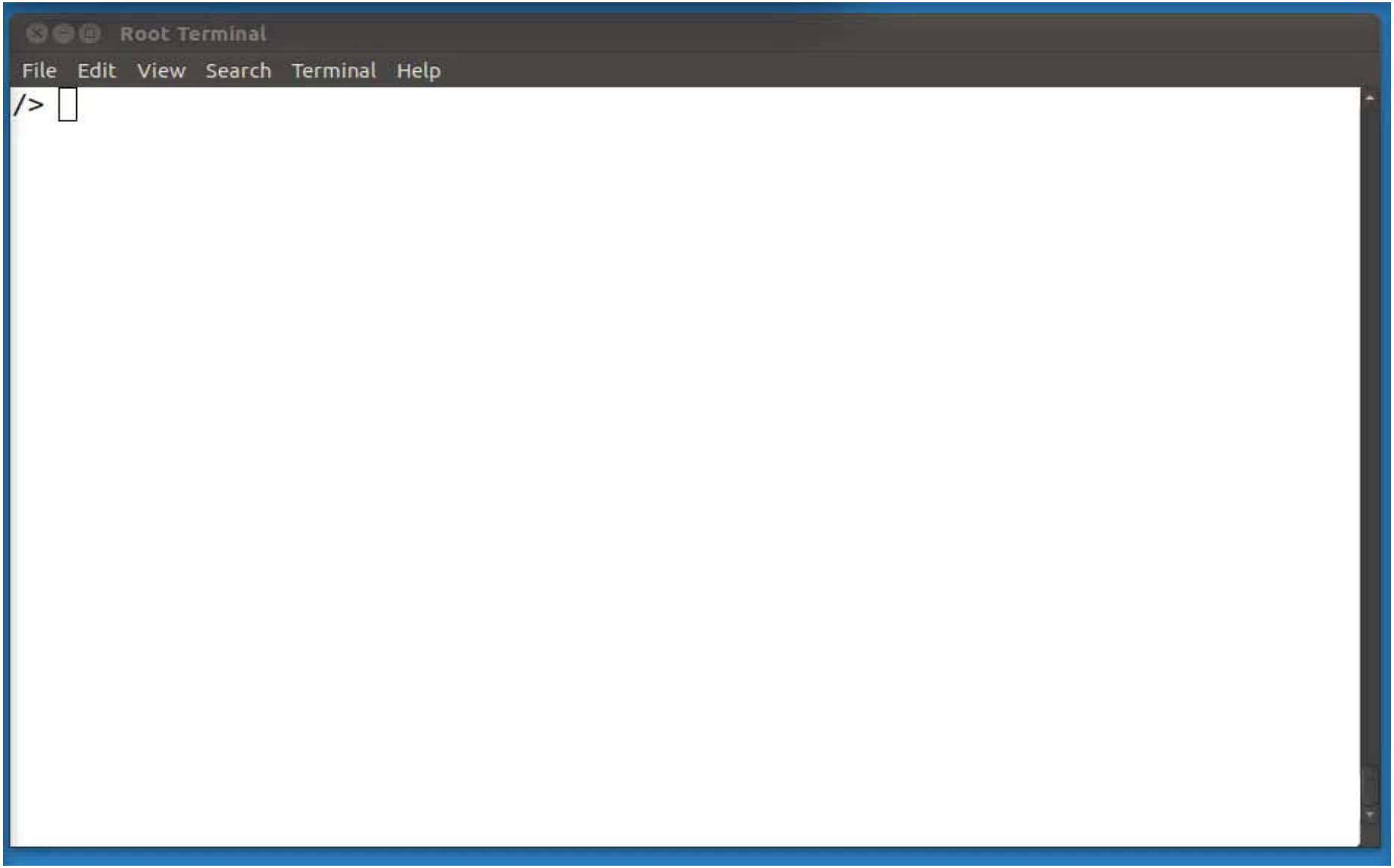


Answer (for us):

Hardware, Memory and Software Connectors provide flexible, performance and growth options.

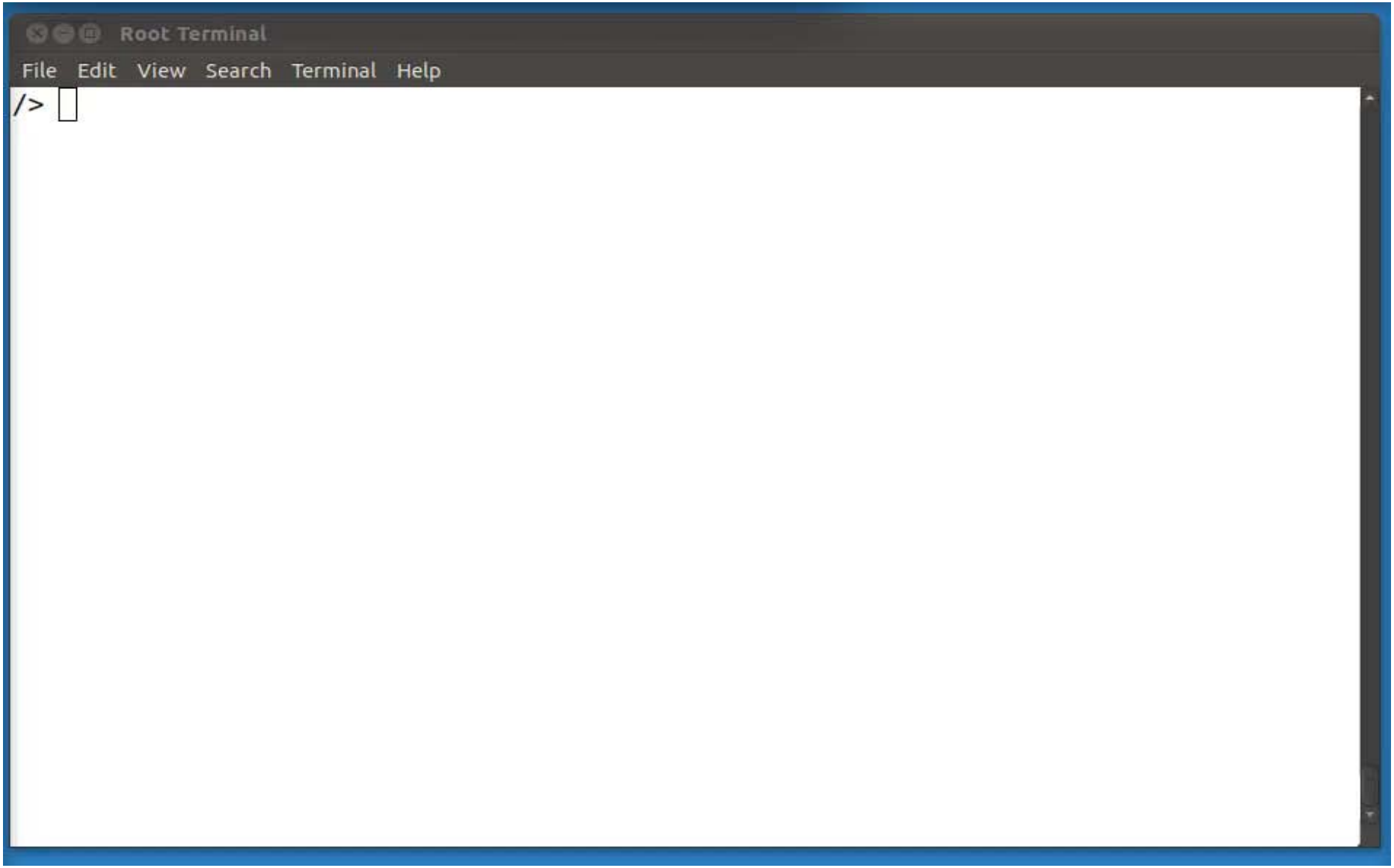
The basics –

Installing a connector (this will be quick)



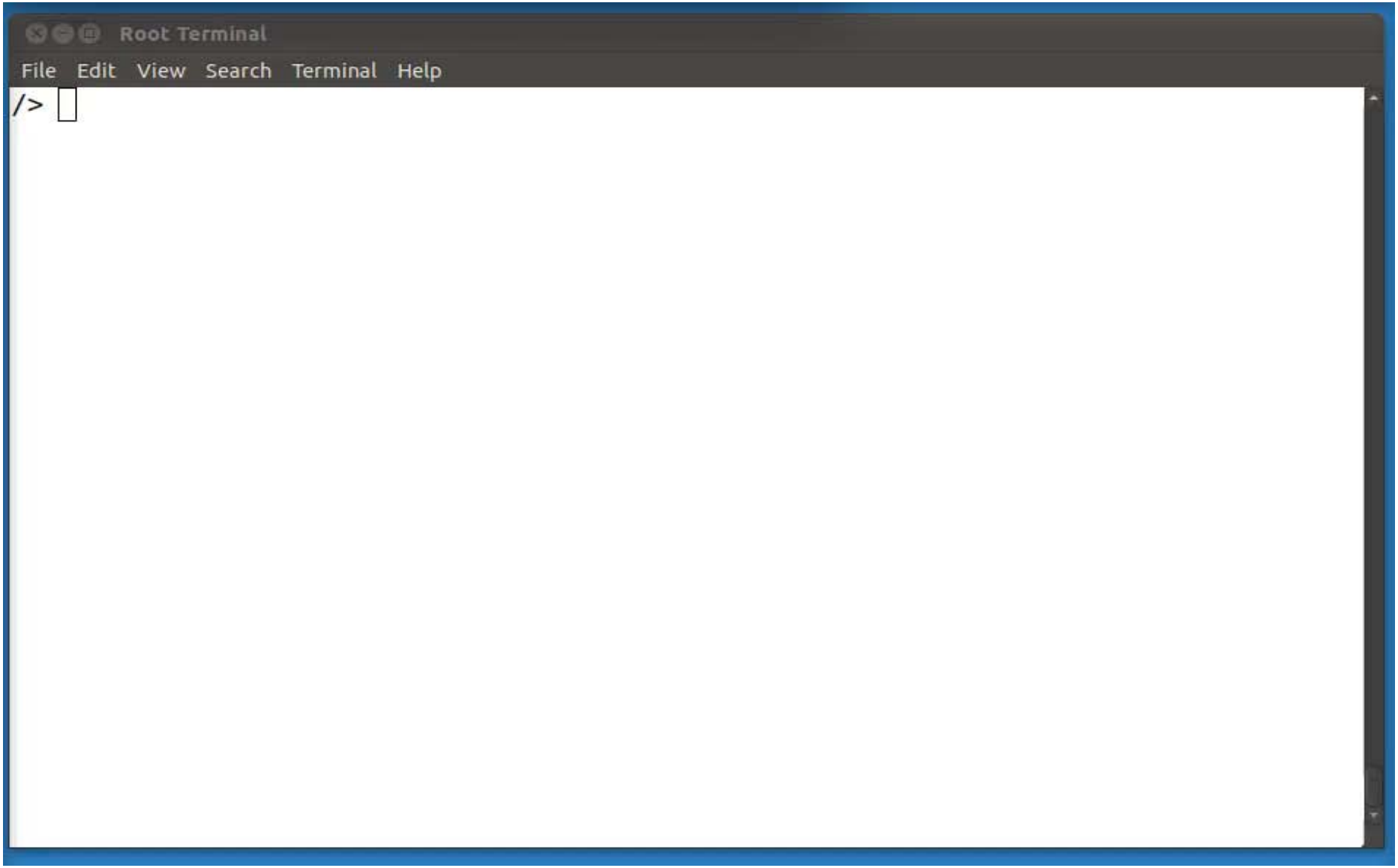
The basics –

Installing a connector from command line



The basics –

Anatomy of a connector



Anatomy of a connector

/opt/arcsight/connectors/syslog/

/opt/arcsight/connectors/bluecoat/

|-A5717/

|-current/

|-bin/

|-scripts/

|-config/agent/

|-jre/lib/security/

|-logs/

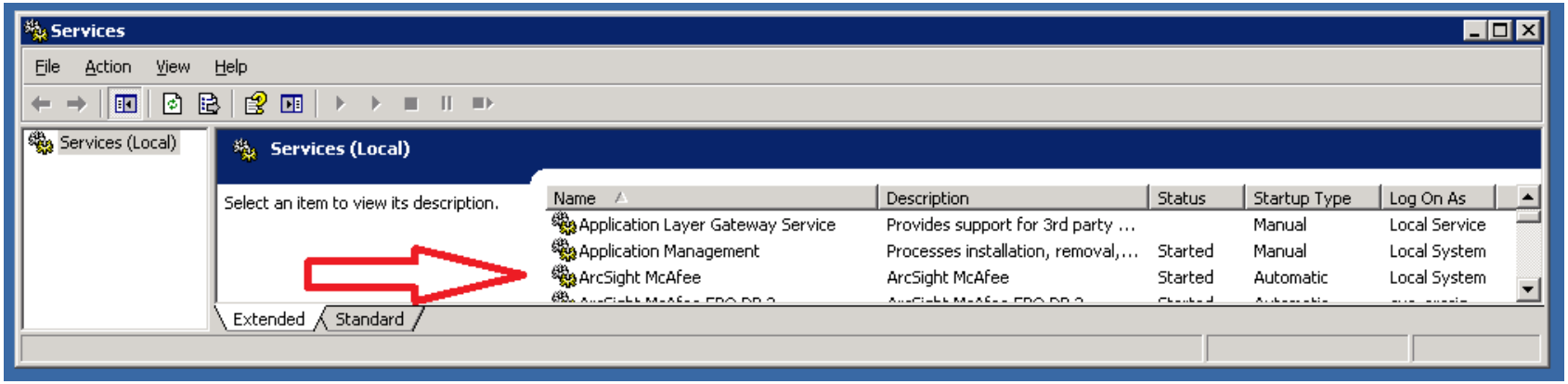
|-user/agent/

|-agentdata/

tree.txt

Connector running as a service

Windows



Linux

/etc/init.d/arc_syslog

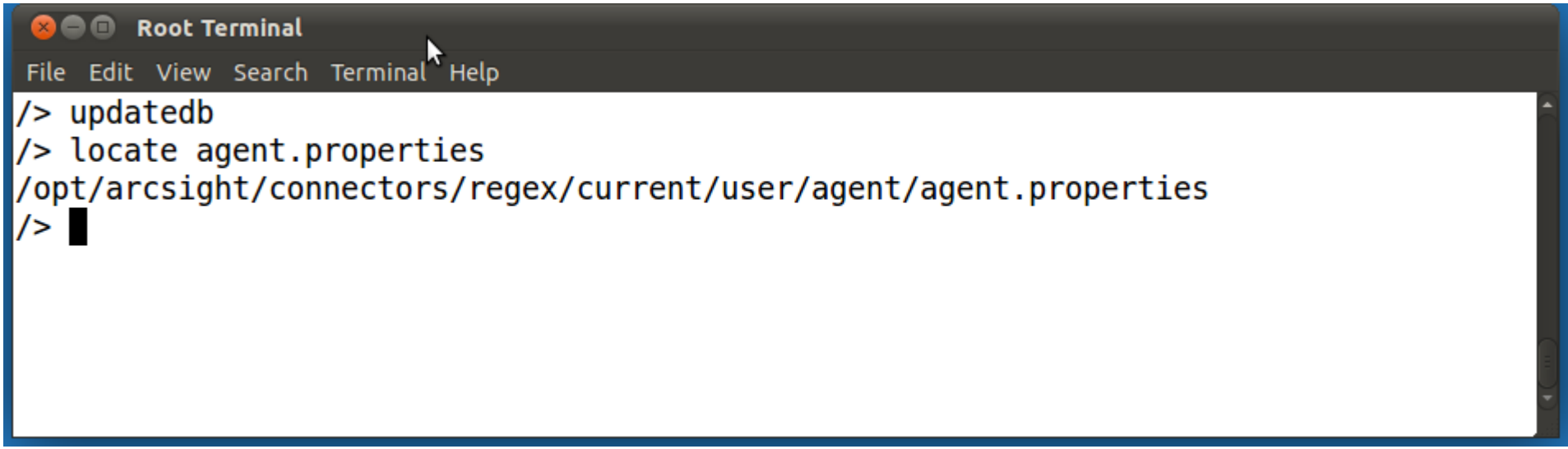
/etc/init.d/arc_bluecoat_file

Linux command line: service arc_bluecoat_file stop |start | restart

Linux Tip: the locate command

From Wikipedia, the free encyclopedia

locate is a Unix utility first created in 1983 used to find files on filesystems. It searches through a prebuilt database of files generated by **updatedb** or a daemon and compressed using incremental encoding. It is significantly faster than **find**, but requires the database to be updated regularly.



Agenda

Why software connectors?

Basics

- Connector installs
- Anatomy of a connector folder
- Running as a service
- Config files
  - agent.properties file
  - agent.default.properties file
- Log files
  - Reading the agent.log
  - Reading the agent.out.wrapper.log

Tuning

- Logging levels
- Connector JVM memory

Analysis

- Running RegEx
- Running LogFu on connector logs
- Reading connector-status.log file

Tips

- Command line 'Get Status'
- KB Articles
- Silent Install headaches
- Connector removal
- Clean up time

Q & A

Connector **agent.properties**

- Become familiar with your <ArcSight_home>\user\agent\agent.proerties file.
- **These are your configuration choices** made during installation.
- Backup this file.

```
#ArcSight Properties File
#Tue Jun 07 17:41:02 MST 2011
agents.maxAgents=1
agents[0].destination.count=1
agents[0].destination[0].agentid=3Pcgee7658ABCWV7H6JabdPw\=\=
agents[0].destination[0].params=<?xml version\="1.0" encoding\="UTF-
8"?>\n<ParameterValues>\n    <Parameter Name\="port" Value\="8443"/>\n
<Parameter Name\="filterevents" Value\="false"/>\n    <Parameter Name\="host"
Value\="esm-manager.companyname.com"/>\n    <Parameter Name\="aupmaster"
Value\="false"/>\n    <Parameter Name\="fipsciphers"
Value\="fipsDefault"/>\n</ParameterValues>\n
agents[0].destination[0].type=http
agents[0].enabled=true
agents[0].entityid=3Pcgee7658ABCWV7H6JabdPw\=\=
agents[0].foldertable[0].configtype=sdkfilereader
agents[0].foldertable[0].folder=C\:\\temp\\bluecoat5\\
agents[0].foldertable[0].logfiletype=main
agents[0].foldertable[0].maxretries=3
```

agent.properties (continued)

```
agents[0].foldertable[0].logfiletype=main
agents[0].foldertable[0].maxretries=3
agents[0].foldertable[0].mode=RenameFileInTheSameDirectory
agents[0].foldertable[0].modeoptions=processed
agents[0].foldertable[0].usenonlockingwindowsfilereader=false
agents[0].foldertable[0].usetriggerfile=false
agents[0].foldertable[0].wildcard=SG_main*gz
agents[0].type=bluecoat_ng_file
server.base.url=https\://esm-manager.companyname.com\:8443
server.registration.host=esm-manager.companyname.com

# Added by me on 6/9/2011 to reduce logging messages.
# 0 = Debug, 1 = Info, 2 = Warn, 3 = Error, 4 = Fatal
log.channel.file.property.package.com.arcsight=2
```

Mode options **
- None
- RenameFileInTheSameDirectory
- DeleteFile

Hey what is this?

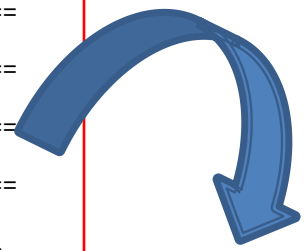
Ref: https://arcsight.custhelp.com/cgi-bin/arcsight.cfg/php/enduser/std_adp.php?p_faqid=2186

Connector **agent.default.properties**

To review and understand the connector settings and defaults you can VIEW the <ArcSight_home>\config\agent\agent.default.properties file.

- **DO NOT EDIT THIS FILE.**
- Copy a property line you want modify over to your agent.properties file.
- E.g. Number of agent.log backup files is 10 by default. Let's make it 20.

```
# ============================================================
# ArcSight Smart Agent default properties
# ============================================================

# ============================================================
# Log configuration.
# ============================================================

# The loglevel for the default package. Anything with a level
# >= the one specified will be logged.
# 0 = Debug, 1 = Info, 2 = Warn, 3 = Error, 4 = Fatal
log.channel.file.property.package.com.arcsight=1

# The path and name of the log file.
log.channel.file.property.path=agent.log

# The maximum size of the log file before it will be rolled over.
log.channel.file.property.maxsize=10MB

# The maximum number of backup files to create for rolling over.
log.channel.file.property.maxbackupindex=10
```



```
#ArcSight Properties File
#Tue Jun 07 17:41:02 MST 2011

.
.
.


# Added by me on --DATE-- to have more logging history.
# The maximum number of agent.log backup files
log.channel.file.property.maxbackupindex=20
```

Agenda

Why software connectors?

Basics

- Connector installs
- Anatomy of a connector folder
- Running as a service
- Config files
  - agent.properties file
  - agent.default.properties file
- Log files
  - Reading the agent.log
  - Reading the agent.out.wrapper.log

Tuning

- Logging levels
- Connector JVM memory

Analysis

- Running RegEx
- Running LogFu on connector logs
- Reading connector-status.log file

Tips

- Command line 'Get Status'
- KB Articles
- Silent Install headaches
- Connector removal
- Clens up time

Q & A

Reading the **agent.log** file

<CODE MAP: 'SYSTEM'>

<ArcSight Version: 5.1.3.5870.0>

[2011-07-24 14:54:12,413][INFO][default.com.arcsight.agent.hh][logStatus] {C=0, ET=Up, HT=Up, N=Unix, S=241314, T=70.96666666666667}

[2011-07-24 14:54:12,428][INFO][default.com.arcsight.agent.hh][logStatus] Other status:

[2011-07-24 14:54:12,428][INFO][default.com.arcsight.agent.hh][logStatus] {Last Start Time=1311541749532, Uptime=2702}

[2011-07-24 14:54:13,068][WARN][default.com.arcsight.agent.zc.d][hostNameUnknownForIp] Unknown IP [10.12.57.12] can not be resolved. Removed it from queue

[2011-07-24 14:54:13,069][WARN][default.com.arcsight.agent.zc.d][hostNameUnknownForIp] Unknown IP [10.12.21.30] can not be resolved. Removed it from queue

[2011-07-24 14:54:13,069][WARN][default.com.arcsight.agent.zc.d][hostNameUnknownForIp] Unknown IP [10.12.15.52] can not be resolved. Removed it from queue

[2011-07-24 14:54:13,070][WARN][default.com.arcsight.agent.zc.d][hostNameUnknownForIp] Unknown IP [10.12.12.42] can not be resolved. Removed it from queue

[2011-07-24 14:54:15,050][ERROR][default.com.arcsight.agent.loadable.agent._SyslogFileNameFollower][parseAndSend] Unable to process Syslog aggregated alert

from [10.12.173.104] message [last message repeated 4 times] cache size [1000])

[2011-07-24 14:54:15,123][WARN][default.com.arcsight.agent.zc.d][hostNameUnknownForIp] Unknown IP [10.12.4.33] can not be resolved. Removed it from queue

[2011-07-24 14:54:15,133][WARN][default.com.arcsight.agent.sdk.a.o][parseValues] No empty message id submessage defined and no submessage description found

for messageid [DAEMON-3-SYSTEM_MSG] message [ntp:sendto(10.12.12.219): No route to host - ntpd[2883]]

[2011-07-24 14:54:15,208][WARN][default.com.arcsight.agent.zc.b][lookupByName] Cannot find information for [cc:b9:cc:89:87:79]

[2011-07-24 14:54:15,208][WARN][default.com.arcsight.agent.zc.d][ipUnknownForHostName] Unknown host name [cc:b9:cc:89:87:79] can not be resolved. Removed it from queue

agent.log (file continued)

[2011-07-24 14:54:18,965][INFO][default.com.arcsight.agent.loadable._EventCounter][processSingleAlert] First event from [Unix|Unix||10.12.18.27] received.

[2011-07-24 14:54:18,977][INFO][default.com.arcsight.agent.loadable._DeviceEventCounter][processSingleAlert] New device found [cc34cc0ac8.company.com|10.12.18.27|Unix|Unix]. Starting counters.

…

[2011-07-24 15:19:33,782][WARN][default.com.arcsight.agent.wf.i][run] Unable to find subagent for with message :.. Warnings logged [15560]

[2011-07-24 15:19:33,782][WARN][default.com.arcsight.agent.wf.i][run] Subagent not found for message []. Warnings logged [15561]

[2011-07-24 15:19:33,782][ERROR][default.com.arcsight.agent.wf.k][processMsg]

java.lang.NumberFormatException: For input string: "/tr"

at java.lang.NumberFormatException.forInputString(NumberFormatException.java:48)

at java.lang.Integer.parseInt(Integer.java:449)

at java.lang.Integer.parseInt(Integer.java:499)

Reading the **agent.out.wrapper.log** file


```
INFO   | jvm 1    | 2011/07/24 09:10:03 | [Sun Jul 24 09:10:03 MST 2011] [INFO ] First event from [Unix|Unix||10.12.32.37]
       received.
INFO   | jvm 1    | 2011/07/24 09:10:03 | [GC 396143K->267670K(523200K), 0.0027590 secs]
INFO   | jvm 1    | 2011/07/24 09:10:03 | [GC 396502K->267806K(523136K), 0.0031070 secs]
INFO   | jvm 1    | 2011/07/24 09:10:04 | [GC 396638K->268152K(523200K), 0.0030310 secs]
INFO   | jvm 1    | 2011/07/24 09:10:04 | [GC 397048K->269146K(523200K), 0.0046280 secs]
INFO   | jvm 1    | 2011/07/24 09:10:04 | [GC 398042K->269274K(522560K), 0.0024620 secs]
INFO   | jvm 1    | 2011/07/24 09:10:04 | [GC 397530K->269970K(522688K), 0.0029620 secs]
INFO   | jvm 1    | 2011/07/24 09:10:04 | [GC 398223K->271107K(522496K), 0.0028250 secs]
INFO   | jvm 1    | 2011/07/24 09:10:05 | 2011-07-24 09:10:05
INFO   | jvm 1    | 2011/07/24 09:10:05 | Full thread dump Java HotSpot(TM) Server VM (16.3-b01 mixed mode):
INFO   | jvm 1    | 2011/07/24 09:10:05 |
INFO   | jvm 1    | 2011/07/24 09:10:05 | "ThreadLocalWorker #3 for Post-Aggregation Batching[3y+Fm7SoBABDkq9Sa8vl-
       4A==]" prio=10 tid=0x09e65400 nid=0x5b5d waiting on condition [0xacc7d000]
INFO   | jvm 1    | 2011/07/24 09:10:05 |    java.lang.Thread.State: TIMED_WAITING (sleeping)
INFO   | jvm 1    | 2011/07/24 09:10:05 |             at java.lang.Thread.sleep(Native Method)
INFO   | jvm 1    | 2011/07/24 09:10:05 |             at com.arcsight.agent.pe.j$c_$a_.run(j$c_$a_.java:875)
INFO   | jvm 1    | 2011/07/24 09:10:05 |
```

Agenda

Why software connectors?

Basics

- Connector installs
- Anatomy of a connector folder
- Config files
  - agent.properties file
  - agent.default.properties file
- Logs
  - Reading the agent.log
  - Reading the agent.out.wrapper.log

Tuning

- Logging levels
- Connector JVM memory

Analysis

- Running RegEx
- Running LogFu on connector logs
- Reading connector-status.log file

Tips

- Command line ‘Get Status’
- KB Articles
- Silent Install headaches
- Connector removal
- Clean up time

Q & A

Tuning the **agent.log** file

Too many logs. What can I do…

The default logging level for a connector is Info. Change this only when you decide Info messages are too much to review.

With some connector types the logs will rollover very fast.

Solution: Add the following lines to agent.properties file. This will take precedence over the default setting in the agent.default.properties file. A connector restart will be required.

```
# Changed from 1 to 2 by me on 4/13/2011 to reduce logging messages.
# 0 = Debug, 1 = Info, 2 = Warn, 3 = Error, 4 = Fatal
log.channel.file.property.package.com.arcsight=2
```

Caution: Change this back when sending logs to support. Full detail may be needed.


agent.properties


WARN_agent.log

Tuning the **Connector Java memory settings**

Java heap is divided into generations

Minor GC

- Only collects young generation
- May expand to entire heap, and become a major collection

```
[GC 338,279K->214,397K(520,640K), 0.0037640 secs]
```

Major GC or Full GC

- Collects both young generation and tenured generation

```
[Full GC 393,785K->75,819K(520,576K), 0.3965000 secs]
```

Tuning the **Connector Java memory settings**

Minor GC pause ("[GC …]")

- Should be under 1 sec

Major GC pause ("[Full GC ….]")

- Actual time depends on hardware
- Estimate: ~1 sec every 200 MB Heap

```
[Full GC
932,135K->542,955K(1,036,928K), 3.9721866 secs]
```

Working Set is defined as the memory that is in actual use and has no garbage

- Working set of the JVM can be found as above, immediately after a "Full GC"

Changing Memory Allocation for SmartConnector JVM

Support Knowledge Base article: **3430**

Q: How do I change the **memory** allocation for the SmartConnector JVM?

Disclaimer: The greater the size of the JVM **memory**, the greater is the time required to run full garbage collection when **memory** runs low. In other words, there is a trade-off between the size of the JVM **memory** and the system performance.

1. Edit the <ArcSight_home>**/current/user/agent/agent.wrapper.conf** file
2. Modify the following properties in agent.wrapper.conf to change the value of **minimun** and **maximum** memory used in Mb:

   wrapper.java.initmemory=256

   wrapper.java.maxmemory=256

   Example of the modified property:

   wrapper.java.initmemory=512

   wrapper.java.maxmemory=1024

Ref: https://arcsight.custhelp.com/cgi-bin/arcsight.cfg/php/enduser/std_adp.php?p_faqid=3430

Tuning the Console Java memory settings

Support Knowledge Base article: **1355**

- Question How to change java heap size for the ESM Console?
- Answer Use the following steps to change Console's Heap Size:

  1. Edit <*ARCSIGHT_HOME*>*current**bin**scripts**console.bat* file.

  Modify the following property:

  2. set ARCSIGHT_JVM_OPTIONS=-Xms64m -Xmx256m -XX:-UseThreadPriorities -XX:+HeapDumpOnOutOfMemoryError -Dsun.java2d.noddraw=true

  For example to set the Console to use 1 GB of memory set *-Xmx* as following*:*

  3. set ARCSIGHT_JVM_OPTIONS=-Xms64m -Xmx1024m -XX:-UseThreadPriorities -XX:+HeapDumpOnOutOfMemoryError -Dsun.java2d.noddraw=true

Ref: https://arcsight.custhelp.com/cgi-bin/arcsight.cfg/php/enduser/popup_adp.php?p_faqid=1355

Agenda

Why software connectors?

Basics

- Connector installs
- Anatomy of a connector folder
- Running as a service
- Config files
  - agent.properties file
  - agent.default.properties file
- Logs
  - Reading the agent.log
  - Reading the agent.out.wrapper.log

Tuning

- Logging levels
- Connector JVM memory

Analysis Tools

- Running RegEx
- Running LogFu on connector logs
- Reading connector-status.log file

Tips

- Command line ‘Get Status’
- KB Articles
- Silent Install headaches
- Connector removal
- Clean up time

Q & A

TIP: Keep connector guides handy

Download Connector Guides

SmartConnectorConfigGuides-5.1.4.5933.zip

- You need the SmartConnector Guides for hour and hours of fun reading. ☺

- Did you know you have options?
  - See KBA 788 - Mapping additional data values

Adobe Acrobat Document

Adobe Acrobat Document

Ref: https://arcsight.custhelp.com/cgi-bin/arcsight.cfg/php/enduser/std_adp.php?p_faqid=788

Administrators you need a connector installed on your workstation

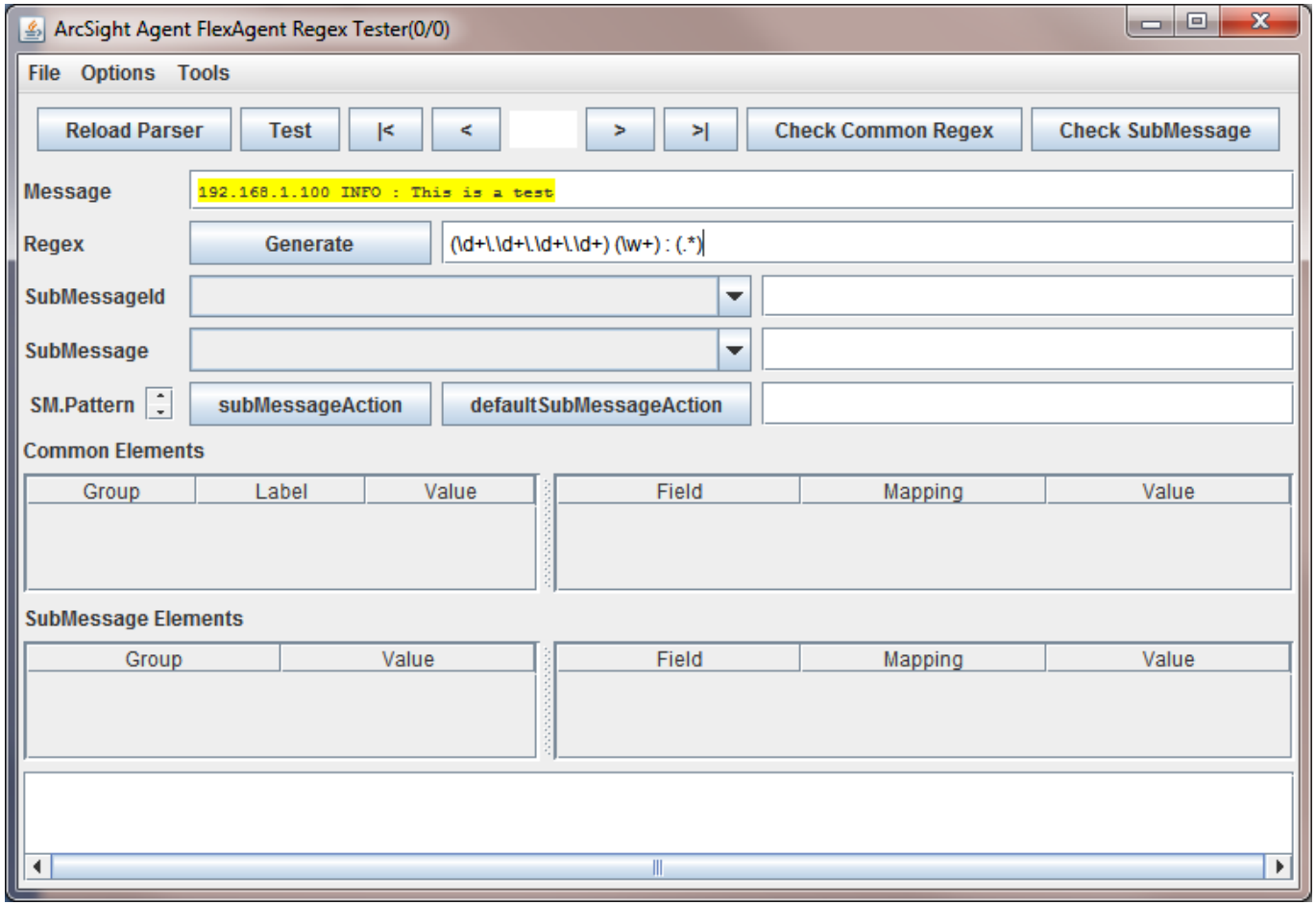
Why?

- Connector install is needed for **RegEx** and **LogFu**
- These tools are not in the console package
- Test SmartConnector upgrade local.

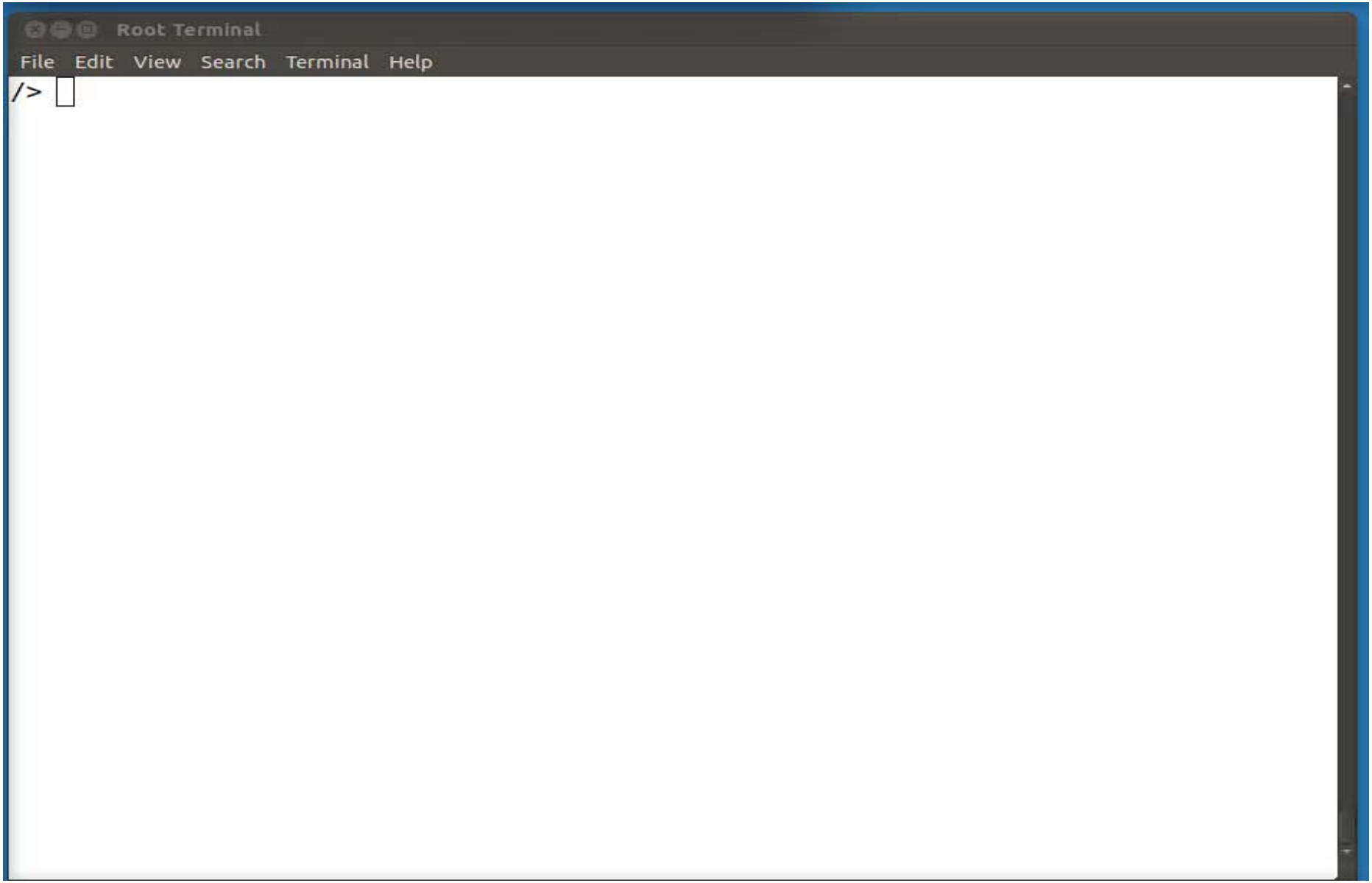
Running RegEx on workstation

Invoke the RegEx script by executing the following commands:

- cd <ARCSIGHT_HOME>\current\bin
- arcsight regex



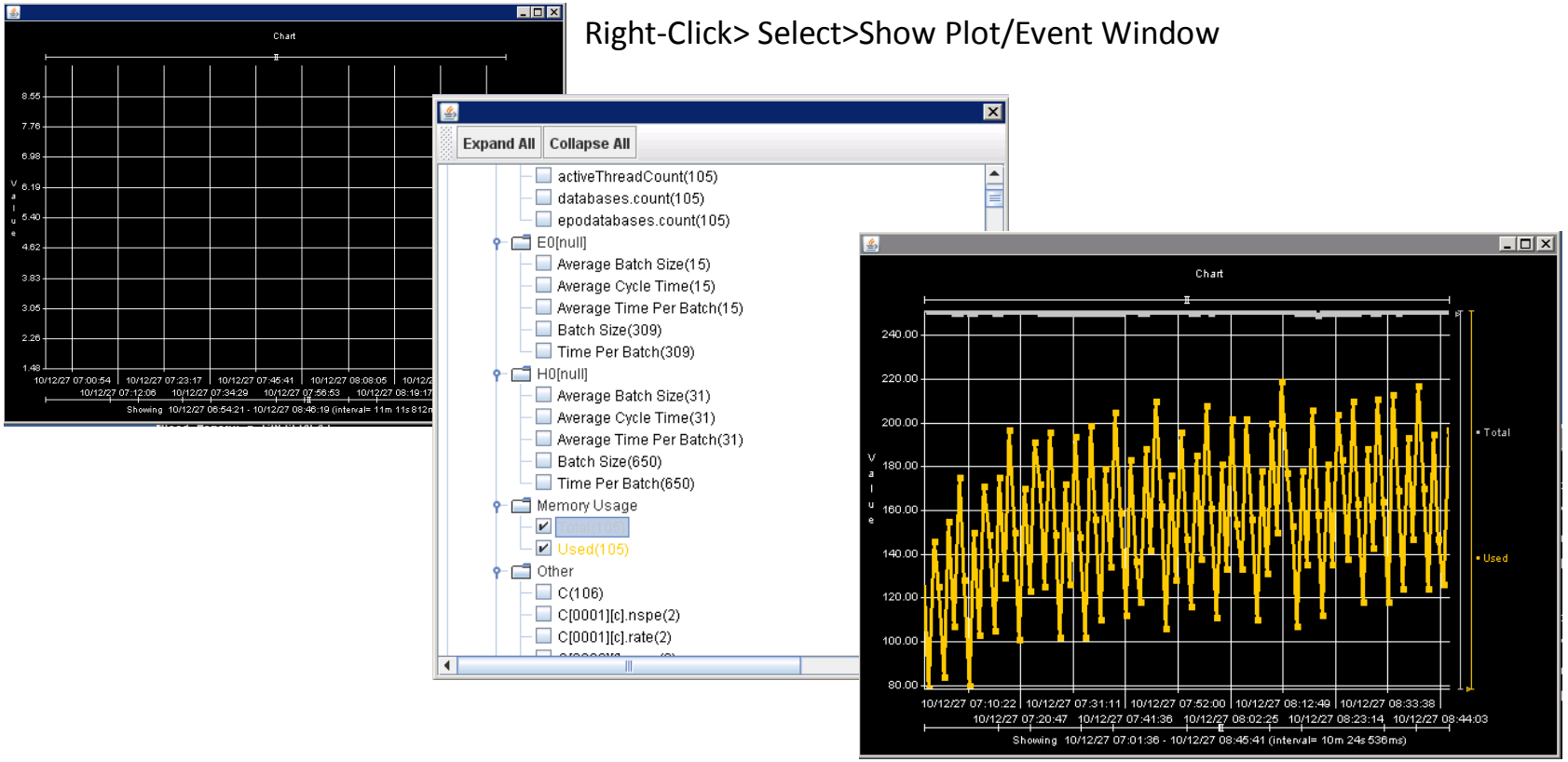
RegEx Demo



Running LogFu on connector logs

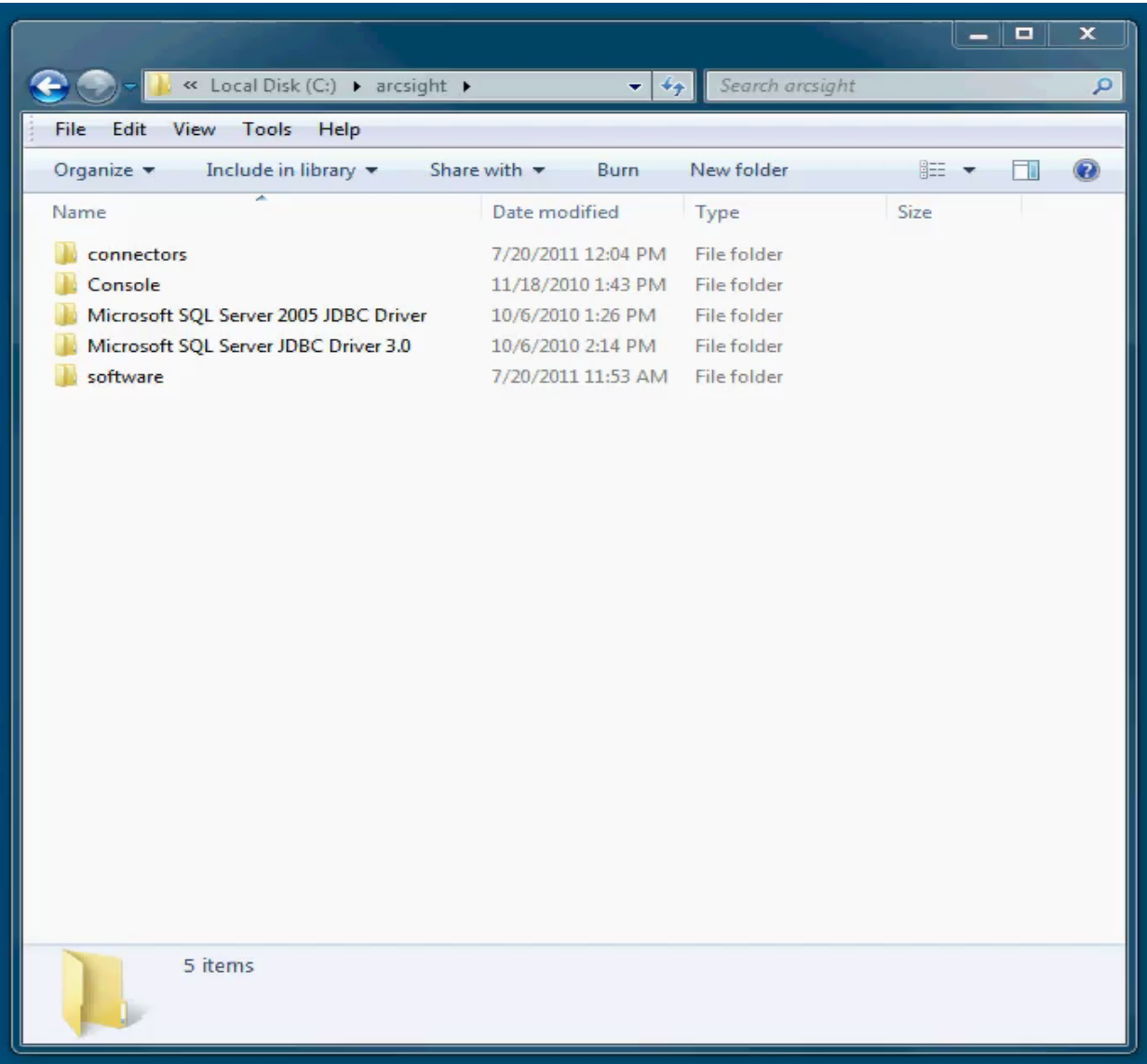
Invoke the LogFu script by executing the following commands:

- cd <ARCSIGHT_HOME>\current\logs\
- ..\bin\arcsight agent logfu -a



Right-Click> Select>Show Plot/Event Window

LogFu Demo


« Local Disk (C:) ▸ arcsight ▸
Search arcsight
File Edit View Tools Help
Organize Include in library Share with Burn New folder
Name Date modified Type Size
connectors 7/20/2011 12:04 PM File folder
Console 11/18/2010 1:43 PM File folder
Microsoft SQL Server 2005 JDBC Driver 10/6/2010 1:26 PM File folder
Microsoft SQL Server JDBC Driver 3.0 10/6/2010 2:14 PM File folder
software 7/20/2011 11:53 AM File folder
5 items

Agenda

Why software connectors?

Basics

- Connector installs
- Anatomy of a connector folder
- Running as a service
- Config files
  - agent.properties file
  - agent.default.properties file
- Logs
  - Reading the agent.log
  - Reading the agent.out.wrapper.log

Tuning

- Logging levels
- Connector JVM memory

Analysis

- Running RegEx
- Running LogFu on connector logs
- Reading connector-status.log file

Tips

- Command line 'Get Status'
- KB Articles
- Silent Install headaches
- Connector Removal
- Clean up time

Q & A

Command line 'Get Status'

Support Knowledge Base article: **1877**

- Question How can I view the SmartConnector status?
- Answer information received by using the Console's GetStatus command, There is a command to obtain the same however the command is un-documented and hidden.

- To use this command:
  - Navigate to the **<**ARCSIGHT_HOME**>/current/bin** directory on the SmartConnector host and execute the following command:
  - *arcsight* ***agentcommand*** *-c status*

    or
  - *arcsight* ***agentcommand*** *-c status* > ../logs/connector-status.txt

connector-status.txt

SmartConnector **Silent Install**

On Windows

ArcSight--<x.x.x.xxxx>.0-Connector-Win.exe –i console

On Linux/Unix

chmod 755 ArcSight-<x.x.x.xxxx>.0-Connector-Linux.bin

ArcSight--<x.x.x.xxxx>.0-Connector-Linux.bin –i console

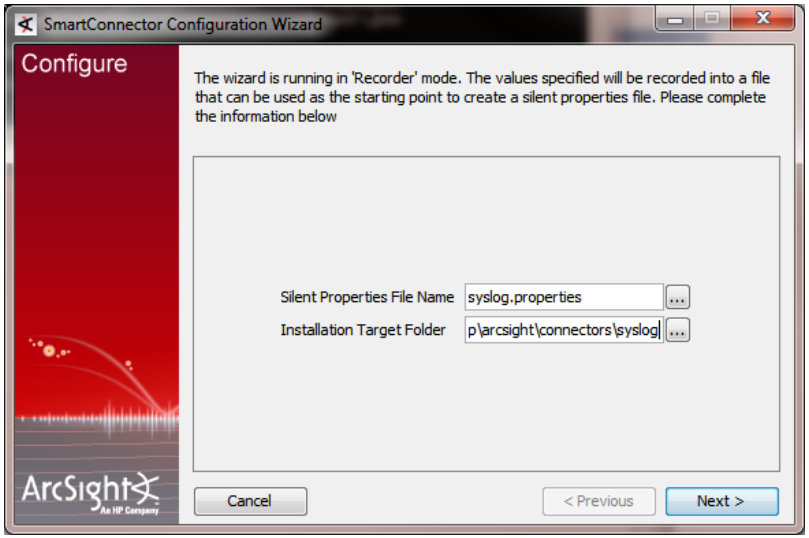
Wait! What? That requires a connector to be installed first.

runagentsetup.bat -i recorderui –g (Generates a sample slient install properties file).

SmartConnector **Silent Install**

- From a command prompt window (from the <ARCSIGHT_HOME>\current\bin\ directory)
- Enter the following command to launch the SmartConnector Configuration Wizard in record mode: runagentsetup.bat -i recorderui

Problem: Only works with demo certificate



Could be useful in the future.

TIP: Removal of a Connector

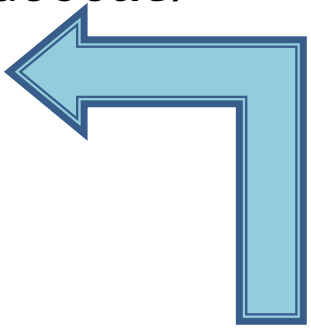
Remove server service first!

Connector Console Mode (Non-GUI):

1. Invoke the setup wizard by executing the following command from:
   - cd <ARCSIGHT_HOME>\current\bin
   - ./runagentsetup.sh or ./arcsight agentsetup -i console -w
2. Select:
   - I want to change SmartConnector service settings.
   - Yes, I want to remove the SmartConnector service.

TIP: Clean up old connector versions to get some space back.

```
/opt/arcsight/connectors/bluecoat/
                |-A5717/
                |-5.0.1.5594.0
                |-5.1.1.5782.0
                |-current/
```



If every thing is working you can just remove the old folders with a simple **delete**.

Caution: Don't delete current
TIP: Leave the last previous, just in case.

Summary

I suggest the following:

- Software connectors have potential for greater flexibility and higher event rates
- Install connector on the admin workstation for RegEx and LogFu
- Perform upgrades in a workstation first
- Know the connector structure and key files
- Know your configuration files
- Know your logs
- Know your status
- Learn memory tuning steps
- Knowledge base articles are there, just hard to find
- Keep your connector guides handy
- Don’t be afraid to explore; it’s all just 1s and 0s ☺

Agenda

Why software connectors?

Basics

- Connector installs
- Anatomy of a connector folder
- Running as a service
- Config files
  - agent.properties file
  - agent.default.properties file
- Logs
  - Reading the agent.log
  - Reading the agent.out.wrapper.log

Tuning

- Logging levels
- Connector JVM memory

Analysis

- Running RegEx
- Running LogFu on connector logs
- Reading connector-status.log file

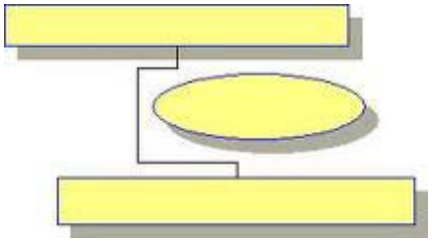
Tips

- Command line 'Get Status'
- KB Articles
- Silent Install headaches
- Connector Removal
- Clean up time

Q & A

Q & A

John writes: What colors do smart connectors come in?



[Extra] Glossary from ArcSight

Base events

- Base **events** are **events** that have been processed and normalized by the SmartConnector and sent to the Manager.

Aggregated events

- Aggregated **events** are normalized **events** that have been aggregated (summarized and consolidated), either by the SmartConnector or by the Manager's correlation engine.

Correlated events

- Correlated **events** are a series of normalized **events** which together cause the conditions of a rule or correlation data monitor to be met.

Correlation events

- A correlation event is created when all conditions and thresholds are met in the correlation engine (rule or data monitor), or by a condition set at the SmartConnector. Correlation **events** are sent through the event lifecycle as new **events** so they can themselves be evaluated by filters, active channels, rules, data monitors, active lists, Pattern Discovery, and reports.

SLC

- SLC means something like Since Last Check or Count. I don't know if that's the official abbreviation, but it's the delta since the last time this stat was reported. (ref: Protect 724)