11 Ways to Perform Single Sign-On Monitoring

Steve Lavoie
Aaron Berman

May 7 2015

Agenda

1 WHY MONITOR

2 ARCHITECTURAL MONITORING TECHNIQUES

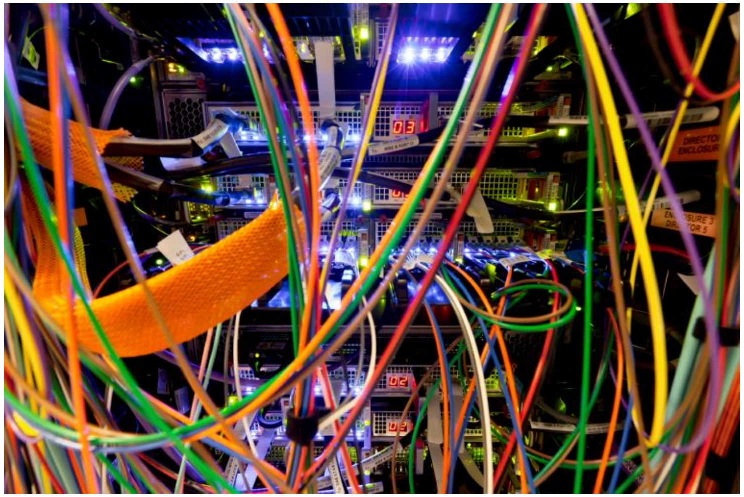
3 COMMAND LINE MONITORING TECHNIQUES

4 TOOLS FOR COLLECTING SINGLE SIGN-ON MONITOR DATA

5 QUESTIONS

Single Sign-On is mission critical

- Single Sign-On touches many applications across the enterprise
  - Both internal employee and Consumer transactions
- If Single Sign-On stops, the applications stop as well
- When a problem occurs and why so action can be taken
  - Need to identify problems that are intermittent
  - Need to identify possible problems before they cause outages



Organizations need to identify problems quickly

- Single Sign-On can cross many organizations
  - Application teams
  - Directory teams
  - Single Sign-On teams
- When a problem occurs we tend to play organizational blame games
- Since Single Sign-On touches many components it often gets blamed even if it is not at fault

Many different ways to “Monitor”

- “Monitor” can mean many different things
  - Components Up / Down
  - System “health”
    - Total Throughput
    - Latency of Requests
  - User activity

- No single solution for everything

Architectural Monitoring

Monitoring Technique 1 - Synthetic Transactions

- Tools to Automatically “login” and access a page
- Sees the site from a and user perspective
- Wide variety of tools
  - Even seen load testing tools be used for this purpose

Monitoring Technique 1 - Synthetic Transactions

- What it tells you
  - Is your website responding to logins
  - Login times
- Benefits
  - Looks across entire site
- Drawbacks
  - Unknown what the path is for the transaction
    - Failover, round robin, internal component failures are hidden
  - Creates extra load on system
- Tip: a single website on each policy server with a single agent that only communicates to that policy server

Monitoring Technique 2 – ServerErrorFile ACO Setting

- Existing ACO setting to either display a friendly HTML page or redirect on a WebAgent Error
- Introduced prior to SM 12.0
- Use the redirect ability to redirect users to a friendly page on a separate web server
  - Create a separate log for errors for all agents in a single spot
  - Collect the error code (Querystring)
  - Collect the referrer (HTTP headers)
- Possibly take actions

Monitoring Technique 2 – ServerErrorFile ACO Setting

- What it tells you
  - Has a Web Agent encountered an error
    - What the error code is
    - Which website
- Benefits
  - Real time information – can trigger an alert
  - Useful in calculating intermittent issues
  - Can also display a friendly error page
- Drawbacks
  - Requires some scripting to collect and save the data

Monitoring Technique 3 - CA Application Delivery Analysis (ADA)

- Network Layer Monitoring tool
- Plugs into network switches and looks at TCP Traffic
- Can examine communications to/from multiple systems and understand latency of these components

Monitoring Technique 3 - CA Application Delivery Analysis (ADA)

- What it tells you
  - Latency of communications between multiple components
- Benefits
  - Can quickly identify component have trouble
  - Can identify if it is the network or the application
- Drawbacks
  - Not included in Core Single Sign-On License
  - Not a Single Sign-On specific solution

Command Line Monitoring

Monitoring Technique 4 - "Stats" or "Publish" commands

- There are two command line tools to dump out Single Sign-On policy server data to log files.
  - "smpolicysrv –stats"
  - "smpolicysrv –publish"
- Some organization will programmatically run these commands every 5 – 15 minutes just so they have the data in their logs.
- Provide Key data
  - Thread status
  - Queue depth
  - Agent connection status

SmPolicyServ – Stats Example

```
[4308/4976][Tue Apr 14 2015 16:11:36][CServer.cpp:4623][INFO][sm-Server-02000] System Statistics

[4308/4976][Tue Apr 14 2015 16:11:36][CServer.cpp:4640][INFO][sm-Server-02020] Thread pool limit: 8

[4308/4976][Tue Apr 14 2015 16:11:36][CServer.cpp:4661][INFO][sm-Server-02030] Thread pool: Msgs=680 Waits=680 Misses=304 Max HP Msg=1 Max NP Msg=1 Current Depth=0 Max NP Depth=1 Current High Depth=0 Current Norm Depth=0 Current Threads=8 Max Threads=8 Busy Threads=0

[4308/4976][Tue Apr 14 2015 16:11:36][CServer.cpp:4669][INFO][sm-Server-02040] Connections: Current=1 Max=3 Limit=256 Exceeded limit=0
```

Monitoring Technique 4 - “Stats” or “Publish” commands

- What it tells you
  - Internals to Single Sign-On policy server (threads, Queues)
  - Agents that are connected (publish only)
- Benefits
  - Command line tool can be scripted
  - Data flows to SMPS Log, can be log scraped
- Drawbacks
  - Moment in time
  - Since threads do not close after they are opened, thread count can be misleading

Monitoring Technique 4 - “Stats” or “Publish” commands

- **SERVER**
  - Short_Name
  - Full_name
  - Product
  - Version
  - Platform
  - TCP ports
  - ThreadPool
    - MSGS
    - Max High Depth
    - Max Nrom Depth
    - Max Msg Depth
    - Current High Depth
    - Current Message Depth
    - Thread Limit
    - Thread Max
    - Threads Current
    - Threads Busy
  - Key Management
    - Generation: {Enabled/Disabled}
    - Update : {Enabled/Disabled}
  - Journal Refresh and Flush
  - Policy Store Cache
  - UserAZCache

- **REPORTS**
  - Thread Count
  - Pending Logs Entries
  - Auth Events
  - AZ Events
  - Admin Access Events
  - Affilitate Events
  - Adminitrative Events
  - Output type (TXT or ODBC)

- **AUDITLOG_STORE**
  - Name
  - File/DSN
  - Log Retentions Settings

- **STORE DATA**
  - **Policy Store**
  - **Key Store**
  - **Token Store**
    - **Connection Properties**
    - **Versions**
    - **Connections Statistics**

- **Agent Connection Manager**
  - CURRENT
  - MAX
  - DROPPED
  - IDLE_TIMEOUT
  - ACCEPT_TIMEOUT
- **User Directories**
  - **Connection Properties**

- **Event Handlers**

Monitoring Technique 5 – Command Line Tools

- Count the number of WebAgent connections to a Policy Server
- Grep – i –n | ESTABLISHED | 44443 | wc –l
- Agent connections do not mean the policy server is processing requests for that agent
  - Number of agent connections will outnumber number of Policy Server threads
  - Timeouts
  - Policy Server Queue

Monitoring Technique 5 – Command Line tools

- What it tells you
  - Numbers of agent connections if numbers of connections are increasing, either load is increasing or policy server is slowing down
  - If Number of connections equals MAX Connections, the system is no longer taking new requests
- Benefits
  - Quick and easy way to identify number of agents making requests
- Drawbacks
  - Moment in time
  - Agent API developers can skew this number
  - Connections remain established until timed out

Monitoring Technique 6 – SMPS & SMEXEC Log

- Administrative log
- Errors
- Server startups and shutdowns
- Bad connections to directories / databases
- SM Exec will try to restart Policy Server automatically after a crash

Monitoring Technique 6 – SMPS & SMEXEC Log

- What it tells you
  - When Policy servers startup, how long they take to startup
  - If there is intermittent crashing of Policy Server
- Benefits
  - Sometimes administrators don’t even know a process restarted
  - Can log occasional errors before they turn into big problems
- Drawbacks
  - No root cause defined in the log
  - Log that has to be separately read and examined

Monitoring Technique 7: Policy Server Profiler Analysis

- Policy Server Profiler
  - Generates Policy Server Trace Logs
- Download Policy Server Trace Log Analysis Tool:
  - https://communities.ca.com/thread/97562407
- Generates PDF reports of one or more trace logs
- Includes useful graphs

Monitoring Technique 7: Policy Server Profiler Analysis

Report Categories

- Process Request
- Authrequest
- AzRequest
- HighPriorityConnectRequest
- LDAPRequest
- LDAPWait
- LDAPRequestPlusWait
- SQLRequest
- NormalQueueWaitTime
- HighPriorityQueueWaitTime
- LineCount
- ErrorCount
- SQL Connections
- Queue Depth
- Long Transactions: ProcessRequest
- Long Transactions: HighPriorityConnectRequest

Report Sub-Categories

- Summary ProcessRequest
- Graph ProcessRequest
- Table ProcessRequest
- SrcLine Graph ProcessRequest
- Concurrent_Process_request
- StartAndEnd_ ProcessRequest
- StartAndEndDelta_ ProcessRequest
- Lock Detect
- Lock Throughput

Single Sign-On Monitoring Data

Single Sign-On Monitoring Subsystem

- Single Sign-On has a internal monitoring subsystem that can be used to called various monitor data and provide the data to a variety of tools
- This system collects data, and there are a variety of techniques to view it

Monitoring Technique 8 – One View Monitor

- Part of core Single Sign-On
- Web UI that displays data from the Single Sign-On monitoring subsystem
- Can be for a single policy server or all events can be consolidated

Monitoring Technique 8 – One View Monitor

- What it tells you
  - Data from internal monitoring subsystem
- Benefits
  - Part of core Single Sign-On
- Drawbacks
  - Just a snapshot in time
    - No history or recording
  - Averages are only reset on server restart

Monitoring Technique 8 - CA APM (Wily) for Single Sign-On

- A version of CA's Application Monitoring Tool (Wily) specific for Single Sign-On
- Collects Policy Server and agent data collected through Single Sign-On Monitoring subsystem
- Has plugins for Policy Server, Web Agents and Secure Proxy Server

Monitoring Technique 9 - CA APM (Wily) for Single Sign-On

- What it tells you
  - Data from internal monitoring subsystem
- Benefits
  - Graphical charts of data
  - Historical comparison
  - Can be used for Policy server only (still get some agent data) or can also be used with agents
  - Can do alerting of metrics fall out of ranges
- Drawbacks
  - Not included in Core Single Sign-On License
  - Looks at Monitoring data – not end user activity

Monitoring Technique 10 - IdentityLogix (partner) SpyLogix for Single Sign-On

- 3rd party tool from IdentityLogix
- Collects Data from Single Sign-On monitoring subsystem
- Collects end user audit activity
- Can do alerting based on thresholds
- Helps an engineer to manage and find the data they are looking for in gigabytes of logs

Monitoring Technique 10 - IdentityLogix (partner) SpyLogix for Single Sign-On

- What it tells you
  - Data from internal monitoring subsystem
  - Audit data (authentications, authorizations)

- Benefits
  - Detailed transactional information
  - Also integrated with IdentityMinder
  - Planned integration with Directory

- Drawbacks
  - 3rd party product
  - Not included with Single Sign-On License

Monitoring Technique 11 - SNMP

- Collects Policy Server and agent data collected through Single Sign-On Monitoring subsystem
- Sends data to various SNMP monitoring tools
- Provided MIB for SNMP collector

Monitoring Technique 11 - SNMP

- What it tells you
  - Data from internal monitoring subsystem
- Benefits
  - Can have a centralized view of the environment
- Drawbacks
  - No tools to interpret data in the SNMP collector

Live Q&A

- Ask a question…
  - In the WebEx Q&A or Chat windows.
  - Press *6 or #6 to unmute your line.
  - Or… in the CA Security Community!

ca.com/talksecurity

???

Follow @CASecurity and @CA_Community on Twitter!

Aaron Berman
Steve Lavoie

Aaron.Berman@ca.com
Steve.Lavoie@ca.com

@CASecurity

slideshare.net/CAinc

linkedin.com/company/ca-technologies