Improve the performance of CA Identity Manager

Alan Baugher, CA Sr. Principal Architect

2015-09-10

Checklist

Basic / Quick Tactical Wins

Effort = < 1 - 2 hour(s) per objective

19 objectives

- TP cleanup
- Screen Indexes
- IM -> IMPS mappings
- JIAM Cache
- InMemoryEvaluation
- IMPS Logging reductions
- User Sync Options
- Tuning JVM guidelines
- SM LDAP Directory Operations
- IMPS Tier Virtual Association 1:1
- CA Directory DSA Resizing
- Linux Entropy (SM/JCS/WebAppServer)
- ADS/Exchange Timeout
- Validate Load Balancing
- AV Exclusion
- Disable IMPS NT Services
- Load Balance IAMCS for JCS/CCS connectors
- Use all CPUs for CA Directory
- Remove Unused Endpoint Screens/Tasks

Advance / Strategic Planning Tasks

Effort = 1 day – 2 weeks per objective

19 objectives

- X64 architecture
- Dynamic logger
- Load balance routers
- Separate IM databases
- Database connection pool
- JMS Event Message Driven Bean pool
- JMS JDBC Store
- Two (2) independent web application clusters
- High-volume TP cleanup
- Parallel bulk / feed tasks
- Transactional Feed process
- Common install issues
- PX business logic streamlining
- CA APM (Wily Introscope) / IM & SM
- …

Managing & Correcting Error Messages

Effort = 1 day – 2 weeks for all areas

3 areas

- Web Application Server Logs
- IMPS Server Logs
- SM & Directory Logs

Advance Training

Effort = 1-4 week(s)

2 objectives

- Sandbox Lab
- OJT expansion of solution & training sessions

Document Business Logic in PX/IdentityPolicies/Provisioning

BASIC / QUICK TACTICAL WINS

BASIC / QUICK TACTICAL WINS 01

- **Impact: High value/minimal effort to implement**

- Description: Clean up the task persistence database / tables
  - Do NOT let this table go for weeks/months without clearing out the old data.
  - Every time a user logins in or performs an action, IM reads this database & associated tables
  - When the records are over a million plus rows, degradation of performance will result.
  - There is an OOTB IM task made for to address this issue.
  - Decide on how much data must to be kept for active usage of the IM solution.
    - Most clients will retain a minimum of three (3) to four (4) weeks of data
    - Why? Because if there are any workflow events; anyone who goes on vacation for two (2) weeks, will see the approval request when they get back. This assumes the workflow remains active; and has not already been delegated or has a built-in SLA to advance to another approver.
  - Decide if information is to be retains for audits or reports
    - Check box on the “Clean up task” allows for data to be “moved” instead of deleted, to an archive task persistence table.
    - Few clients leverage this, as there is an audit table in place for long term data to be retained.
      - Task audit checkbox MUST be turned on to leverage.
  - If possible, perform a database row count on the table tasksession12_5, before and after clean up task has executed. This will give the admin a reasonable metric how long a clean up operation will take to move from millions of rows to a goal of 100,000 of rows. Confirm that tasksession_id is a GUID entry. Perform an unique check on tasksession_id between TP and TPA using SQL compare of the tasksession_id columns.
  - Advance note: If this site has more data coming into the IM solution via external TEWS calls than can be managed by daily OOTB clean-up task, see the advance section.

- Actions: Login to IM User Console as a system admin; and schedule the TP clean up on a daily scheduled basis to remove any non-active task older than 14-21+ days.

- Reference:
  - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?1031429.html?
  - https://communities.ca.com/web/ca-identity-and-access-mgmt-distributed-global-user-community/message-board/-/message_boards/view_message/97528088;jsessionid=FB13691C0CC99A77451A23602B8A869C.usilap722?&#p_19

ca technologies

BASIC / QUICK TACTICAL WINS 02

- **Impact: High value/Requires DBA skill set to implement**

- Description: Add Indexes to high usage IM screen tables
  - *Post-install task;* Only run AFTER an IME is created.
  - Object store tables IM_SCREEN_LD & IM_SCREEN_FIELD_LD
  - Pre-built Scripts included in the IM Tools Folder under samples
    - /opt/CA/IdentityMinder/IAM_Suite/IdentityManager/tools/samples/ObjectStore/
  - Requires a DBA or access to the IM tables as the db owner to execute scripts
  - Improve usability of screens loading & Loading of IME (between steps 5 & 6)
    - From 10's seconds to less than 5 seconds

- Actions: Login to IM Database GUI or CLI Console; execute IM scripts; log off IM Database GUI or CLI Console; done.
  - Example with Oracle XE DB:
    - su - oracle
    - sqlplus idmdba001/Password01
    - SQL> @/opt/CA/IdentityMinder/IAM_Suite/IdentityManager/tools/samples/ObjectStore/objectstore_db_oracle.sql
    - SQL> exit

- Reference:
  - /opt/CA/IdentityMinder/IAM_Suite/IdentityManager/tools/samples/ObjectStore/readme.txt
  - http://www.ca.com/us/support/ca-support-online/product-content/knowledgebase-articles/tec1500343.aspx

BASIC / QUICK TACTICAL WINS 03

- **Impact: Medium value/minimal effort to implement**

- Description: Remove unnecessary default corporate to provisioning mappings
  - OOTB mappings of IM Well-Known User attributes are:
    - %ADMIN_OF%
    - %ADMIN_ROLE_CONSTRAINT%
    - %CERTIFICATION_STATUS%
    - %DELEGATORS%
    - %IDENTITY_POLICY%
    - %LAST_CERTIFIED_DATE%
    - %PASSWORD_DATA%
    - Note:
      - These default settings were retained for a few clients that were moving from an pure provisioning deployment model to a corporate store model+ provisioning deployment model, to avoid issues during upgrades with any custom business logic.
      - This will remove unnecessary sync operations and corresponding IM call back operations for these attributes.
      - These setting are not required for new deployments.
  - Reduce impact for * queries that may impact other users and processes
    - By default, the value for maximum rows and page size is unlimited for existing directories. For new directories, the value for maximum rows is unlimited and the value for page size is 2000.

- Actions:

- Login to the IME Management console; Select the IME; select Advance Settings\Provisioning; under the section “Attribute Mappings”; remove the selected well-known attributes defined above.

- Update Directory.xml settings

BASIC / QUICK TACTICAL WINS 04

- **Impact: Medium value/minimal effort to implement**

- Description: Enabled IMPS Cache
  - Improve performance when look-ups are required, as a part of an IM task, to query the provisioning server for a user.
  - Reduce network overhead & false negative message in WAS logs about missing ID from cache

- Actions: Login to the IME Management console; Select the IME; select Advance Settings\Miscellaneous
  - Create two (2) tokens/properties with the following values:
    - *JIAMCache=true*
    - *JIAMCacheTTL=86400*

- Reference:
  - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?384757.html?

BASIC / QUICK TACTICAL WINS 05

- **Impact: Medium value/minimal effort to implement**

- Description: Enabled IM Memory Evaluation for login authorizations
  - Improve performance during & after login, when IM queries on a user's IM access from the IM corporate user store.
  - Reduce sequential ldap queries by using case sensitive cache feature.
    - If the setting of value =1 causes issue in the IME; use the other value to set non-case sensitive caching, value =3.
- Actions: Login to the IME Management console; Select the IME; select Advance Settings\Miscellaneous
  - Create a token/property with the following value:
    - *UseInMemoryEvaluation =1*
- Reference:
  - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?592744.html?

BASIC / QUICK TACTICAL WINS 06

- **Impact: High value/minimal effort to implement**

- Description: Disable excessive logging at the mid-tier components, e.g. Provisioning Server (IMPS)
  - Default logging level for transactions is set to level = 7 upon initial install
    - This log level captured all searches as well as update to the IMPS server and to endpoint managed by the IMPS server in the etatrans* logs.
    - Most client only require monitoring of create/update/delete transactions
    - CA support requests and requires that when support tickets are open, that a use-case is executed when the log level is set to level =7.
    - Recommendation is to lower the log level to **level =3** unless actively working a CA support ticket or attempting to isolate an issue.
    - Improve I/O performance and lower disk usage of IMPS etatrans* logs.
    - Improve IM performance when any IM task requires communication to the IMPS server and/or managed endpoints.

- Actions: Login to the IM Provisioning Manager GUI; Select System Tab; Select Domain Configuration button; Select Transaction Log; Select Level; Modify default value from 7 to 3; click apply; done. (no need to bounce services)

- Reference:
  - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?237642.html

BASIC / QUICK TACTICAL WINS 07

- **Impact: High value/minimal effort to implement**

- Description: Disable user sync for select IM tasks
  - Task User Sync Option has three (3) settings:
    - **On Task Completion**
      - Mandatory sync of all delta user attributes between IMCD and IMPS/PD when task completes (aka “Self-Healing”)
    - **On Every Event**
      - Only sync the delta attributes in task/profile, but executes multiple times until the task completes.
    - **Off**
      - This task will not trigger user synchronization.
      - Used for tasks that do NOT required to be pushed/sync to IMPS, e.g. update questions.
  - OOTB IM tasks for create/modify/delete use-cases will have the default user sync option enabled to run “On Task Completion”
    - Recommend disable user sync option for default self-service task to update security questions and answers.
      - Improve performance of submission of questions/answers by preventing IM from trying to sync user’s attributes that are not manage of this self-service task.
    - Use “OnEveryEvent” to limit use-case of task to only sync user attributes within the task’s profile.
    - Other Tasks that may be adjusted: Prov Modify User, Prov Create User and Prov Delete User

- Actions: Login to the IM User Console; select Roles and Tasks; select Modify Task; select the IM Task by name; under Profile select User Synchronization; set to Off; test use-cases; ensure no issues or unexpected behavior; done.

- Reference:
  - https://supportcontent.ca.com/cadocs/0/CA%20IdentityMinder%2012%206%202-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?599193.html
  - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?AdminTaskProcessing.html
  - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?ConfigureAutomaticUserSynchronization.html

BASIC / QUICK TACTICAL WINS 08

- **Impact: High value/minimal effort to implement**

- Description: Update JVM options to improve memory, garbage collection, and ldap/s call performance.

- JVM Tuning {Aimed at JBOSS web application server; review for WebSphere & WebLogic frameworks}. Consider and fine tune the following JVM setup parameters :
  - # Memory Tuning for x64 / *– if using a 64 bit JVM, start at 2048m minimum and add the –d64 switch for linux/unix os (Note: IM Web App uses about 800MB when it starts)*
    JAVA_OPTS="$JAVA_OPTS –Xms2048m –Xmx4096m“
  - # Used to address performance with a WAS's JVM communicating to LDAP over SSL. Known issue with all WAS (JBOSS/WebLogic/WebSphere) / May impact BLC. (If IM version is greater than r12sp14; then this issue has been addressed)
  - JAVA_OPTS="$JAVA_OPTS -Dcom.sun.jndi.ldap.connect.pool.protocol=plain\tssl Dcom.sun.jndi.ldap.connect.pool.debug=fine -Dcom.sun.jndi.ldap.connect.timeout=5000 -Dcom.sun.jndi.ldap.connect.pool.maxsize=300 -Dcom.sun.jndi.ldap.connect.pool.prefsize=10"
  - # Garbage collection is important. These are good baseline settings but will need to be tuned
  - JAVA_OPTS="$JAVA_OPTS -Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000 -XX:+AggressiveOpts -XX:+AggressiveHeap -XX:+UseParallelGC"
  - # The below options are great for applications with a lot of looping code (such as IM)
  - JAVA_OPTS="$JAVA_OPTS -XX:CompileThreshold=10000 -XX:+UseOnStackReplacement"
  - # The below is good for applications with many classes and intensive bootstraps
  - JAVA_OPTS="$JAVA_OPTS -XX:PermSize=128m -XX:MaxPermSize=256m -XX:ReservedCodeCacheSize=128m"
  - # The below dictates how the JVM will page in it's heap. Use 4m or 16m pages in winOS, 256m for Linux. Ensure that the heap size is evenly divisible by the page size. WinOS may require GPO to be updated to allow service account to use “LargePages” memory feature.
  - JAVA_OPTS="$JAVA_OPTS -XX:+UseLargePages -XX:LargePageSizeInBytes=16m“
  - # The below address entropy challenge on headless/virtualized servers where entropy may be depleted and appears to halt the web app server
  - JAVA_OPTS=“$JAVA_OPTS -Djava.security.egd=file:/dev/./urandom“
  - # If OS is Solaris AND No Hardware/Software tokens nor SSL accelerators nor extended encryption modules are used; it is possible to use this setting.
  - JAVA_OPTS=“$JAVA_OPTS -Dsun.security.pkcs11.enable-solaris=false”
  - # Be Alert to OUT OF MEMORY errors for IM and the IAMCS [-XX:OnOutOfMemoryError="mail -s 'OOM on `hostname` at `date`' whoever@example.com]
  - JAVA_OPTS="$JAVA_OPTS -XX:OnOutOfMemoryError=“XMX_MEMORY_LIMIT_NEEDS_TO_BE_INCREASED“ OR an alternative (-XX:OnOutOfMemoryError='"kill -9 %p"')


D:\vmware\jvm.txt


D:\run.bat

-XX:+HeapDumpOnOutOfMemoryError -XX:OnOutOfMemoryError="kill -3 pid > threaddump.txt" -XX:HeapDumpPath=/disk2/dumps

ca technologies

BASIC / QUICK TACTICAL WINS 08B

Impact: High value/minimal effort to implement

- Description: Update JVM options to improve memory, garbage collection, and ldap/s call performance.
- JVM Tuning {Aimed at JBOSS web application server; review for WebSphere & WebLogic frameworks}. Consider and fine tune the following JVM setup parameters :
  - # Garbage collection is important. These are good baseline settings but will need to be tuned
  - JAVA_OPTS="$JAVA_OPTS -Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000 -XX:+AggressiveOpts -XX:+AggressiveHeap -XX:+UseParallelGC"
- #Added by Amit
- JAVA_OPTS="$JAVA_OPTS -XX:+HeapDumpOnOutOfMemoryError"
- JAVA_OPTS="$JAVA_OPTS -verbose:gc -Xloggc:gc.log -XX:+PrintGCDetails -XX:+PrintGCTimeStamps"

BASIC / QUICK TACTICAL WINS 08C

Impact: High value/minimal effort to implement

- Description: Update JVM options to improve memory, garbage collection, and ldap/s call performance.
- #Reported by Itamar for WebSphere 7 ; https://communities.ca.com/thread/105855683
- JAVA_OPTS = "$JAVA_OPTS -Xgcpolicy:gencon -Dsun.reflect.inflationThreshold=0 -Xdump:none -Dcom.sun.jndi.ldap.connect.pool.protocol=plain\tssl -Dcom.sun.jndi.ldap.connect.pool.debug=fine -Dcom.sun.jndi.ldap.connect.timeout=5000 -Dcom.sun.jndi.ldap.connect.pool.maxsize=300 -Dcom.sun.jndi.ldap.connect.pool.prefsize=128"

Note:

In 12.6 SP4+, may increase the # of threads assign to the object feeder event (used by IM BLC and Bulk Loader IM Task. The default was previously hard coded to 30

Select	Name	Description	Minimum Size	Maximum Size
You can administer the following resources:				
☐	Default		20	20
☐	ORB.thread.pool		10	50
☐	SIBFAPInboundThreadPool	Service integration bus FAP inbound channel thread pool	4	50
☐	SIBFAPThreadPool	Service integration bus FAP outbound channel thread pool	4	50
☐	SIBJMSRAThreadPool	Service Integration Bus JMS Resource Adapter thread pool	35	128
☐	TCPChannel.DCS		5	20
☐	WMQCommonServices	WebSphere MQ common services thread pool	1	40
☐	WMQJCAResourceAdapter	wmqJcaRaThreadPoolDescription	5	25
☐	WebContainer		50	120
☐	server.startup	This pool is used by WebSphere during server startup.	1	3
Total 10				

BASIC / QUICK TACTICAL WINS 09

- **Impact: High value/minimal effort to implement**

- Description: IM when integrated with SM, has all user directory authentication operations routed through SM. Update SM pool of Directory connections to increase number of fixed connections to improve performance for LDAP calls
- Within the SiteMinder WAM UI or FSS UI, select the User Directory
  - Edit the LDAP Directory Failover and Load Balancing Setup
  - Add the SAME LDAP server multiple times to the dialog box.
    - If using CA Directory start with 10 connections before starting performance query with CA IME.
      - Use the IM task for View or Modify User to see a difference
        - Combined with the Screen Index Update, there will be a noticeable difference.

- Ref: https://supportcontent.ca.com/cadocs/0/CA%20IdentityMinder%2012%206%202-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?268042.html
- Additional Ref. for setting page limits:
- https://supportcontent.ca.com/cadocs/0/CA%20IdentityMinder%2012%206%202-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?268090.html

BASIC / QUICK TACTICAL WINS 10

- **Impact: High value/minimal effort to implement**

- Description: IMPS (provisioning servers) tier may have many servers, but within the current IM reference architecture, there is only FAILOVER and no LOAD BALANCING features for IMWA (web app) to communicate to IMPS.
  - If there were N+1 IMPS servers, 100% of traffic to the IMPS tier ALWAYS goes to the first IMPS server. Research with using CA Directory routers, to introduce LOAD BALANCING has been reported to cause a race condition, when the router redirect IMPS traffic to multiple IMPS server, that should stay on one IMPS server until the entire transaction is complete. To adhere to that requirement and still offer a better solution to leverage the full IMPS architecture, the proposed process will keep the existing FAILOVER process, but introduce a tighter integration between components in the same virtual stack between IMWA (web app) and it's IMPS using local host files.
  - This process emulates how CA integrates the Insession Workpoint solution. Workpoint configuration files use "localhost" to enforce the Workpoint engine to be tightly integrated with each IM Web Application Server.
  - **WARNING:** **This is a FIELD DEVELOPED NETWORK PROCESS** and is below CA component management awareness. This will be supported and managed by the Client's IM team .

- Design: "STATIC LOAD BALANCING" {X increase in performance based on number of nodes}
  - Designate the hostnames: imps001, imps002, imps003, imps004, imps0XX, etc.
    - IMPS001 will always be the IMPS IP address associated with the IMWA server within the same logical stack. Therefore this IP will be different on each IMWA server.
    - IMPS002 will be the IMPS IP address associated with the 2nd IMWA server within the same DATA CENTER.
    - IMPS003 / IMPS004 will be the IMPS IP address associated with the 2nd Data Center architecture.
  - The process above will keep traffic originating from IMWA001 with IMPS001, IMWA002 with IMPS002, etc.
  - If FAILOVER is required, it will first be with the IMPS servers within the same data center, then failover, if needed, to the IMPS servers in the 2nd data center.
  - This process will still allow a client to perform in-place upgrades of service packs (that upgrade binaries and not directory schema) without impact to the uptime of the solution.
  - **WARNING:** This design may introduce a possible "RACE" conditions when used with J2EE load balancers. If a create user operation is submitted with a Modify User operation to two different JVM with provisioning to an endpoint's same account; the possibility that the modification operation may begin first is a possibility, though unlikely.
    - How to engage CA Support for this design:
      - If this issue is suspected; client would roll-back solution to correct IMPS IP addresses, re-execute the use-case; if the issue is re-created; then client would open a CA support call and work the issue.
    - If RACE condition occurs;
      - The resolution would be for the client would resubmit the creation record first; then the modification update.

- Action:
  - Edit the local host file on the IMWA servers (windows/unix/linux) to reflect the rules above.
  - Validation: Perform any action within IM user console using the direct Web App port, and validate any provisioning action occurs on the correct IMPS server. E.g. Query users's endpoint accounts; add a provisioning role to a user; execute an Explore and Correlate process.

ca technologies

BASIC / QUICK TACTICAL WINS 11

Impact: Med value/minimal effort to implement

- Description: CA Directory's DSA for IMPD / IMCD / Siteminder PolicyStore/KeyStore/SessionStore are typically setup with large memory sizes to accommodate expected or estimated (SWAG) growth.
- Sometimes the sizes used are an order of magnitude too large.
  - The process time that CA directory uses to manage the memory space and write to disk more excessive than is required.
  - The RAM space may be better used for other DSA on the server that need the space to grow.
  - The below process discuss how to identity the correct data size of the DSA and how to decrease or increase as needed.
- Design:
  - Review the DSA sizes defined in the DXHOME\config\servers*.dxi file
  - Perform a dump of the DSA data using dxdumpdb command for each DSA on a server.
    - dxdumpdb -f DSA_output.ldif DSA_Name
  - Review the size of the DSA's LDIF
    - This will give a good estimate of what the memory size is being used currently, as this size will be used as a base to estimate resizing needs.
    - DSA guideline for sizing should be roughly a minimal of 2.5x times the size of the LDIF file:
      - DSA's LDIF = 10 MB => DSA size = 25 MB => System needs 1 GB of RAM
      - DSA's LDIF = 2000 MB => DSA size = 5000 MB => System needs 8 GB of RAM, as 4 GB RAM would not be enough to allow the DSA to start.
    - If the DSA LDIF is near the current size of the DSA or within the 2.5x sizing guideline, then the DSA should be resize "upward" for growth.
      - Update the DXI file with new size; then stop DSA; Use the command: dxextenddb dsaname; restart DSA; They system will auto-resize the DSA data file.
      - https://supportcontent.ca.com/cadocs/0/CA%20Directory%20r12%200%20SP11-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?917385.html
- Action:
  - Downsizing a DSA's datastore:
    - 1. stop the DSA {dxserver stop dsaname}
    - 2. Dump the datastore to LDIF: "dxdumpdb -f {filename.ldif} dsaName"
      - example: dxdumpdb -f democorp.ldif democorp
    - 3. Edit the DSAs initialization file to edit the "dxgrid-db-size" to reduce it to the new size, and save the file {$DXHOME\dxserver\config\servers\dsaname.dxi}
    - 4. Reload the data using DXloaddb - "dxloaddb -s dsaName ldif-filename.ldif"
      - example: dxloaddb -s democorp democorp.ldif
    - 5. Start the DSA. {dxserver start dsaname}

ca technologies

BASIC / QUICK TACTICAL WINS 12

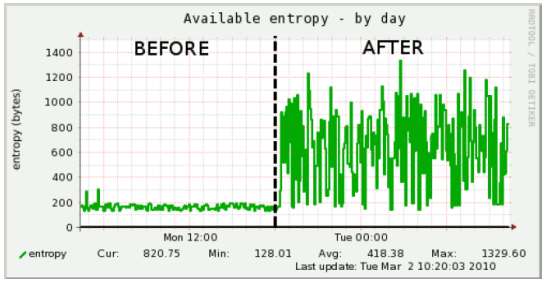
- **Impact: High value/minimal effort to implement**

- Description: Web App Servers (JBOSS/Weblogic/Websphere), IM w/FIPS, IM JCS service, CA Siteminder, & CA Directory may be deployed on RHEL/Linux; and performance for startup of services or connection to LDAP/S userstore may be lengthy due to low entropy on “headless virtual servers”.

- Background:
  - Encryption solutions need to have an random pool available from an OS to ensure the cryptography seed routines are secure.
  - Web Server with SSL server certificates, Client certs used between solution components, or any other solution that performs encryption.
  - Solutions that perform encryption on-the-fly are greatly affected by a low random noise pool.
  - Physical system can “fill” the entropy pool by direct interaction (mouse/keyboard), but on a headless server or virtual server with SSL/encryption traffic, the entropy pool can be drained faster than the system can replenish the data.

- Action: (SEE ENTROPY NOTES AT BACK OF DECK)
  - DEV/TEST/QA (NON-PROD)
  - Use Software fix to address by replacing the device driver with the pseudo device driver
    - LINUX: **#watch -n 1 cat /proc/sys/kernel/random/entropy_avail**
    - SOLARIS: **#echo ::rnd_stats | mdb -k**
    - Test: mv /dev/random /dev/random.org & ln -s /dev/urandom /dev/random
    - Rngd Toolset / Config Fix: vi /etc/sysconfig/rngd to contain:
      - # Add extra options here
      - EXTRAOPTIONS="-r /dev/urandom“
      - service rngd start & chkconfig rngd on
    - For JVM only
      - -Djava.security.egd=file:/dev/./urandom
      - -Dsun.security.pkcs11.enable-solaris=false {if requirement don’t require this}
  - PROD
    - Review adding hardware entropy generators + RNGD service.
    - Use HAVEGED entropy generator (processes/clock as input)

dd if=/dev/random of=/dev/null count=8192



Reference:

https://support.ca.com/cadocs/0/CA%20SiteMinder%20r12%205-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?1865112.html?zoom_highlight=random
http://en.wikipedia.org/wiki/Entropy_(computing)
http://tuxhelp.org/doku.php%3Fid=redhat:rngd:rgnd_init_script.html
http://www.linuxfromscratch.org/hints/downloads/files/entropy.txt

ca technologies

BASIC / QUICK TACTICAL WINS 13

Impact: High value/minimal effort to implement

- Description: CA IM with provisioning may experience performance delays when provisioning AD accounts with Exchange mailboxes due to the OOTB limit of eighteen (18) concurrent sessions to Exchange via Powershell APIs; and if the delay is longer than the CA IM's CAM component timeout setting, the AD account will fail to be created.

- Background:
  - When an AD account is created, it is two (2) separate processes that occur very quickly, but may not be replicated as quickly. The AD account is first created with it's profile in a suspended state, then immediately after the account is created, AD then activates the account.
  - When creating an Exchange mailbox, the Exchange server has it's own list of AD Domain Controllers that it communicates to. These are the DC that Exchange uses to search for an AD account upon creation of the mailbox. If the AD account does not exist or is in a suspended status, the Exchange creation process will fail.
  - The CA IM AD Exchange Agent process, called by a AD service account, has default timeout settings set to create an Exchange mailbox. The IM agent on the Exchange server will use the Exchange APIs to check if the AD account exists and is in an active status before sending the create process to the Exchange server. If the AD account does not appears or show as active in the default timeout window, then the process will fail.
  - To address this issue and improve performance and reliability, the following changes are recommended.

- Actions:
  - On Exchange Server
    - Service account used to create Exchange mailbox has "Exchange Organization Administrator" Group assigned.
      - The CA CAM NT service should be setup to run under this ID
    - Increase the throttle sessions to 100 to accommodate IM bulk feeds that are sent in batches with a batch switch of 500.
      - 1. Exchange Admin may create a new Throttling policy to be used by select user accounts: Example: New-ThrottlingPolicy MaxPowershell -PowerShellMaxConcurrency 100
      - 2. Exchange Admin would then apply this new throttling policy for the IM service account on the Exchange server.: Example: Set-Mailbox "User Name" -ThrottlingPolicy MaxPowershell
      - Update Windows Registry Key for CA IM Exchange Agent from default of 60 seconds to 600 seconds: HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Identity Manager\Ex2k7AgentTimeout
    - Add the environmental variable **eTrustIM_RUS_Delay_Seconds** and add a value of **3** (seconds) [5x = 15 seconds]
  - On IMPS (IM Provisioning Server with CCS service)
    - Add the environmental variable **ADS_CONFIRM_MAILBOX = 600** (seconds)
    - Add the environmental variable of **ADS_E2K_SEND_DC** = **1** (on).
    - Add the environmental variable of **ADS_FAILOVER** = **1** (on) & pick only FAST DC on the ADS Endpoint Failover TAB
      - Note: we ALWAYS want the primary ADS DC endpoint to be the "PDC emulator" (this addresses password replication challenges within the AD domain)

BASIC / QUICK TACTICAL WINS 14

- **Impact: High value/minimal effort to implement**

- **Description:** The IM solution may be deployed in an high availability configuration with J2EE clustering with supported web servers that integrate with the J2EE web application servers; and with hardware load balancers. If the configurations are not correct, only a single stack may be used, and therefore the solution would not scale as expected. Typically, the J2EE platforms will be configured with “round-robin” as the load balancing feature for each transaction.

- The other tier to check for proper load balancing is the data tier: Directory for the corporate user store & Database for the IM object/TP store.

- **Actions:**
  - Monitor on each J2EE JVM the “used memory”, when a bulk task is executed.
    - If the configuration is correct, then each transaction will be load balanced between each J2EE JVM; and reflected in the memory used of the JVM. If not configured correctly, only the first JVM will show activity.
    - To assist with analysis, a PX rule may be created to monitor the CREATE USER task, to write out to the web app log, with a notification message about the new userid. These results can be pulled from each web app server, to validate the load is being properly load balance by number of creations.
  - Monitor the queries to the directory to ensure that all directory servers are being utilized during login events and when data needs to be pulled or compared.
    - For updates, validate that one or selected directory servers, “designated as updated servers” are responsive enough to scale for password changes and other use-cases.
  - Monitor the database(s) used by IM solution
    - Using native or 3rd party tools, ensure that no query or update takes longer than 100 msec.
    - Ensure that the prior tactical suggestion of adding indexes to the IM SCREEN tables has been accomplished.
    - Validate underlying disc and NICs of the database servers are not a bottle neck for performance for database while it replicates data across a LAN or WAN for the remote database clusters.

BASIC / QUICK TACTICAL WINS 15

- **Impact: High value/minimal effort to implement**

- **Description:** The IM solution may be deployed on an OS with AntiVirus. The AntiVirus solution may be causing a performance hit to IM processes and folders during runtime.

- The IM processes and log folders are well known; and may be scanned on a daily basis, the business risk is minimal to exclude these processes and log folders from the RealTime AV Monitor.

- Use Microsoft SysInternal Tool, Process Explorer, to identify all IM processes on Windows OS

- **Actions:**
  - Update AV exclusion for IM processes and IM log folders

- IMPS Server
  - Processes
    - im_ps.exe
    - im_ccs.exe
    - jcs.exe
    - Javaw.exe
    - dxserver.exe
    - cam.exe
    - caft.exe
    - etadmin.exe
- IMWA Server
  - Processes
    - Java.exe
    - W3wwp.exe (MS IIS)
    - LLAWP.exe (SM WA)
    - Dxserver.exe
- IMCD/IMPD
  - Processes
    - Dxserver.exe
    - Dxadmind.exe
- SMPS
  - Processes
    - Smpolicysrv.exe
    - Service_policysrv.exe
    - Java.exe
    - Service_monsrvr.exe
    - Dxserver.exe

- IMPS Server
  - Log Folders
    - D:\Program Files (x86)\CA\IdentityManager\ProvisioningServer\logs
    - D:\Program Files (x86)\CA\Identity Manager\Connector Server\logs
    - D:\Program Files\CA\Directory\dxserver\logs
- IMWA Server
  - Processes
    - Web Application Server Logs
    - Web Server Logs
    - Web Agent Logs
    - D:\Program Files\CA\Directory\dxserver\logs
- IMCD/IMPD
  - Processes
    - D:\Program Files\CA\Directory\dxserver\logs
- SMPS
  - Processes
    - D:\Program Files\CA\siteminder\log
    - D:\Program Files\CA\Directory\dxserver\logs

BASIC / QUICK TACTICAL WINS 16

- **Impact: Low value/minimal effort to implement**

- **Description:** The IM solution provides a centralized log forwarding process for the IMPS tier. This centralized forwarding of log events may be sent via SNMP to a centralized console.

- If no SNMP forwarding is enabled, then the five (5) NT services for this service may be changed from auto-start to manual or disabled. The performance gain is slight, but as this component defaults its installation to the primary OS drive "C:\", this will offer relief for OS I/O operations.

- **Actions:**
  - Update Windows NT services for the five (5) CA Enterprise Common Services used for centralized logging to SNMP consoles. Reset from auto-start to manual or disabled.
    - Enterprise Common Services (Transport)
    - Enterprise Common Services GUI Framework
    - Enterprise Common Services Log Daemon
    - Enterprise Common Services Store-And-Forward Manager
    - Enterprise WorldView

BASIC / QUICK TACTICAL WINS 17

Impact: High value/minimal effort to implement

- **Description:** The IM r12.6.x solution provides a load balancing IAM Connector Server that can front-end the legacy CCS connector. This process allows round-robin load balancing between known connectors and use of routing rules by namespace type.
- A single CCS service with direct feed from the IMPS server; may be expected to have 15-17 updates/second to Active Directory; depending on the endpoint/userstore response.
- A load-balance IAM CS (JCS) with two (2) CCS services; may be expected to have 25-28 updates/second to Active Directory; depending on the endpoint/userstore response.
  - This is almost a 2x increase in performance.
  - Additional CCS may be added to the environment.
  - 10,000 update / 25 = 400 seconds < less than 7 minutes for 10K updates with LB x 2 CCS.
- **Actions:**
  - When installing the IAM CS (JCS) Connector Server; select manage remote CCS services or manage a local service.
  - Do not accept the default / legacy setting of IMPS + CS configuration.
  - Manage the Connectors (IAM CS and CCS) with Connector Xpress
    - Ensure JCS is the default connector; and neither of the CCS
  - Use Jxplorer to view the IAM CS routing rules in the IMPD.
  - Use Connector Xpress to change the CS routing rules for each endpoint.

BASIC / QUICK TACTICAL WINS 18

Impact: High value/minimal effort to implement

- Description: CA Directory's DSAs for IMPD / IMCD / Siteminder PolicyStore/KeyStore/SessionStore are typically setup with default MAX thread CPU count of eight (8).

- If the Server where CA Directory is installed has additional CPU or Hyperthreading, it will be beneficial to increase the MAX thread count for CA Directory. Use a value of 2-4 times the number of available CPUs. Monitor and adjust for the best responses. Use a tool like Jmeter.org or CA Directory dxsoak to monitor for performance metrics.

- Action:
  - Use Dxconsole to set immediately or add a token to the DSA settings DXC file, then either restart or re-init the DSAs.
    - set user-threads = 16; {use a value of 16-32 for a 8 CPU server; start with 16 and then increase until performance is not affected}
    - get user-threads; {Use to view current value}

- References:
  - https://supportcontent.ca.com/cadocs/0/CA%20Directory%2012%20SP13-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?set_user-threads_command.htm
  - https://supportcontent.ca.com/cadocs/0/CA%20Directory%2012%20SP13-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?set_user-threads_command.htm

BASIC / QUICK TACTICAL WINS 19

Impact: High value/minimal effort to implement

- Description: Importing un-needed IM Screens/Tasks for Endpoints that are NOT being managed is a area that can have impact on the startup performance of the J2EE platform, which can be directly observed with the log4j enabled for ims=DEBUG.
- Between these two (2) steps, every endpoint screens/tasks will add roughly 20-30 seconds of delay, as the J2EE platform communicates with the database.
  - [ims.default] - * Startup Step 5 : Attempting to start SecretKeyStore
  - [ims.default] - * Startup Step 6 : Attempting to start CacheManagerService
- Action:
  - While solution is in use: Use IM User Console to remove endpoint screens/tasks. As there is a large number for each endpoint, this will take some time.
    - May view samples of imports to help identify the screens/tasks
  - With the use of a maintenance window
    - Use IM Management console to export the environment; remove the unneeded screens/tasks, save this file, then re-import this new IME
- References:

BASIC / QUICK TACTICAL WINS 20

Impact: High value/minimal effort to implement

- Description: In a default installation of JBoss 4/5/6/7, the JBoss hot deployment scanner runs every 5 seconds, which affects JBoss performance. You can disable this feature, if it is not needed, or change how often it runs.
- Action:
  - On JBoss AS 4/5/6 you can disable JBoss hot deployment's feature through the the conf/jboss-service.xml file. Find the following line:
    - <!-- A flag to disable the scans -->
    - <attribute name="ScanEnabled">true</attribute>
  - Simply change to false and hot deployment will be disabled. If on the other hand you simply want to reduce scan polling time, look for a few lines before:
    - <!-- Frequency in milliseconds to rescan the URLs for changes -->
    - <attribute name="ScanPeriod">5000</attribute>
  - This will set the scan time (in milliseconds)
  - JBOSS 7
    - [standalone@localhost:9999 /] /subsystem=deployment-scanner/scanner=default:write-attribute(name=scan-enabled,value=false)
- References:
  - https://wiki.ca.com/display/CIM1265/Runtime+Components+Tuning
  - http://www.mastertheboss.com/jboss-server/jboss-deploy/how-to-configure-jboss-to-disable-hot-deployment

BASIC / QUICK TACTICAL WINS 21

Impact: High value/minimal effort to implement

- Description:. During startup of JBOSS servers jakarta would prematurely send web requests to jboss before the server had finished starting, resulting in a jboss 404 error
- Action:
  - Red hat support provided the following flag to place in the standalone.bat startup options. It is only available in jboss eap 6.2+, now the service seems to behave in a much more user friendly manner. Since there is no mod_cluster option for IIS web servers.
    - -Dorg.apache.catalina.connector.WAIT_FOR_BEFORE_START=/castylesr5.1.1,/idmmanage,/iam/immanage,/idm,/iam/im
- References:
  - https://communities.ca.com/message/241780544#241780544

ADVANCE / STRATEGIC PLANNING TASKS

ADVANCE / STRATEGIC PLANNING 01

Impact: High Value / medium difficulty

- Description: Move to x64 bit architecture with 2-4 CPU cores
  - If available and supported by client; chose an IM supported Unix/Linux as OS for Web Application Server(s)
  - Web Application Servers use Java for the IM JVM
    - The bit level of Java is important to the amount of memory that is available for the IM JVM to use.
    - IM default memory usage upon startup of the IME is typically 300-400 MB
    - Most clients set initial JVM to 512 MB and maximum JVM (on 32bit) to 1024 MB
    - 32bit Java forces the maximum memory to be less than 2.2 GB of RAM accessible
      - Out of memory error message may occur for long running / detailed reports.
    - 64bit Java allow memory to be increased dramatically.
    - Recommend setting initial memory to 2048 MB and maximum to 4096 MB (-Xms2048M –Xmx4096M -d64)
      - Don't set the initial setting too unnecessarily high, as the "memory garbage collection" routine may impact performance
      - For additional information about web application tuning, see the vendor guides
      - See JVM tweaks further down in this document for additional options.
- **Actions:** Deploy IM in 64bit mode for new environments. For upgrades, deploy IM in a side-by-side configuration; and perform migration tasks; instead of upgrade in-place tasks. Set JVM values as recommend above.
- Reference:
  - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?1988666.html?
  - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?1999277.html
  - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?478644.html

ADVANCE / STRATEGIC PLANNING 02

- **Impact: High Value / low difficulty**

- Description: Do NOT let the user store be the bottleneck in your IM environment
  - Use CA Directory as the Corporate User Store of Identity Minder, if possible.
    - CA Directory has a LOAD BALANCE ROUTER included (see A/SP #04)
      - Achieve five nines (99.99%) Uptime
      - Performance scale the solution to 1 Billion entries or more.
    - CA Directory uses the DXGrid technology.
    - All attribute are INDEXED
      - FAST, FAST RESPONSE
      - This solves a typical performance challenge if any attribute this is heavily referenced, is not indexed.
    - All data is in MEMORY
      - FAST, FAST REPONSE
      - NOT CACHE DATA BUT ALL DATA
    - Configurations may be done on the fly
      - Re-init after a change
    - Validate FAST response
      - Use the dxsoak command under samples folder to validate fast responses or any other LDAP query tool.
    - Update Replications are Synchronized before a response is returned
      - If the peer directory servers do NOT respond within an expected timeframe, the updated record is queue, and then forwarded when that server responds or if down, becomes available.
        - Only seen in large distance geographical separated data centers, DNS issue or network connectivity challenges.
  - If not using CA Directory;
    - Ensure all attributes that are used in queries, are INDEXED!!!
    - Ensure directory cache features and routing for load balancing are enabled.
      - IF the Directory does NOT have load balancing, then purchase a hardware load balancer (F5/BIGIP)
      - If using existing directory, ensure ACLs are used to limit exposure to access outside of IM solution to avoid impact to business logic and defendable compliance.

- Actions: Install CA Directory; create a corporate DSA; load data via LDIF or CSV (via csv2ldif); start DSA; validate data via LDAP query tools (ldapsearch;jxplorer;SoftTerra LDAPbrowser/admin;Apache LDAP admin); validate performance with dxsoak or other tools to compare number of queries/second & number of updates/second. Create multiple peer DSA with load balance router to scale the solution.

ADVANCE / STRATEGIC PLANNING 03

- **Impact: High Value / medium difficulty**

- Description: Add dynamic logger to IM environment to assist with troubleshooting performance challenges.
  - Requires services to be restarted/bounced for web application server
  - Allows for debug viewing of im and ims loggers to be leveraged to isolate IM business logic & configuration challenges
  - Allows for debug viewing of database connections and pooling with jdbc loggers.
  - Useful for tracking IM business logic from feed to PX rules
    - i. Im.feeder = DEBUG {Must be added in Edit box}
      ii. Ims.policyxpress = DEBUG
      iii. Ims.tasktrack.custom = DEBUG {Must restart IME to fully capture debug at startup of IME}
  - Included under the CA IM tool
    - ..\Identity Manager\tools\samples\Admin\readme.txt
    - Folder will copy the existing JSP stubs that are in place.
    - Web application security may be added for non-development environments
- Actions: Install the dynamic logger tool; follow instructions within the readme under ..\Identity Manager\tools\samples\Admin\readme.txt; bounce the web application services; validate dynamic logger updates the web application logs
  - Additional advance step: Create 2nd log4j file for only IM tasks and debuggers to isolate web application server non-IM messages.
- Reference:
  - ..\Identity Manager\tools\samples\Admin\readme.txt

ca technologies

ADVANCE / STRATEGIC PLANNING 04

Impact: High Value / medium difficulty

- Description: Add CA Directory routers to provide load balancing to user stores
  - Communication from the IM Web Application server to the IM Corporate User Store and the IM Provisioning User Store is typically setup in fail-over mode.
    - If multiple stacks of IM are available, this configuration does not get the best performance, as most queries and updates will be managed by the first stack that is configured as the IM user store directory.
  - IM solution includes an enterprise directory (CA Directory) that is used for the embedded provisioning user store and as well as a high available and load balance router between the provisioning server and the provisioning directory, to allow the solution to scale.
  - The same functionality of the software router may be introduced at the web application server to provide a high available and load balance router to the corporate user store; ~~and to the provisioning server.~~ (Per CA Support, the router is not supported in this configuration for the provisioning server due to possible race issue where mod ops may occur prior to create ops via use of PX rules during create user operation at the IMPS tier, but still may be used for the corporate user store.)
  - Requires:
    - installation of CA Directory on the IM Web Application Server(s) & SM Policy Servers (if using SiteMinder)
    - a configured software router using “localhost” & defined available port
    - a copy of the knowledge files of the corp/provisioning user stores & schemas.
      - Assumption: Corporate user store solution is CA Directory
- Actions: Install CA Directory on IM Web Application servers (and SM servers); use the text editing tool to create the router configuration file; copy over the CA Directory corp/prov schemas and knowledge files; update the IME’s directories settings; bounce the IME; perform use-case testing; done.
- Reference:
  - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?844176_1.html?
  - https://supportcontent.ca.com/cadocs/0/CA%20Directory%20r12%200%20SP10-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?example-how_routing_works.htm
  - https://supportcontent.ca.com/cadocs/0/CA%20Directory%20r12%200%20SP10-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?

ADVANCE / STRATEGIC PLANNING 05

- **Impact: Medium Value / medium difficulty / Requires DBA assistance**

- Description: Separate IM Databases
  - Workflow & Auditing & Task Persistence & Object Store & Snapshots (reporting) & Archive (task persistence archive)
  - Out of the box install of IdentityMinder, will install all IM database tables within the IM objectstore.
    - This configuration is fine for small size clients and/or limited use-case, e.g. self-service password reset only
  - Improve I/O performance by installation and separating the IM database(s), if possible on different SAN disks
    - Active databases
      - ObjectStore & Task persistence & Workflow & Auditing
    - Scheduled Peak usage databases
      - Snapshots (reporting) & Archive
  - Requires DBA or db owner access to IM database.
  - IMPORTANT FOR DAR SCENARIOS:
    - IM Databases may grow from 50GB to 200GB.
    - DAR scenarios may cause outage fro 12-16 hours to recovery just DB data from online/tape.
      - Reduce impact of LARGE databases from being needed for DAR, e.g. TPA and SNAPSHOTS/REPORTS from ACTIVE DBs needed for IM ObjectStore.

- Actions: Plan location of databases and sizing required, e.g. 100 GB or (5-10GB with growth allowed) for each. Create the databases prior to the installation of CA IM per bookshelf and the included SQL scripts under the IM tools. Install and start IM and monitor the web application logs for errors; perform use-case testing; done.

- Reference:
  - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?477117.html
  - https://communities.ca.com/web/ca-identity-and-access-mgmt-distributed-global-user-community/message-board/-/message_boards/message/78458009?&#p_19
  - SQL scripts under:
    - ..\Identity Manager\tools\db
    - ..\Identity Manager\tools\Workpoint\database
    - ..\Identity Manager\tools\imrexport\db

ADVANCE / STRATEGIC PLANNING 06

- **Impact: Medium Value / medium difficulty / Requires DBA assistance**

- Description: Update IM Database Connection Pool Settings
  - OOTB IM Connection pool is setup with six (6) JDBC connections with default of initial connection = **5** to maximum connections = **200** number of physical connection within WebLogic Application Server.
  - The Web Application Server manages the JDBC connections to Oracle Database. These value may be viewed in the IM configuration files for the JDBC connections.
  - Example:
    - /opt/weblogic/weblogic1036/Middleware/user_projects/domains/base_domain/config/jdbc/
      - iam_im_DataSource-archive-jdbc.xml
      - iam_im_DataSource-audit-jdbc.xml
      - iam_im_DataSource-os-jdbc.xml
      - iam_im_DataSource-rs-jdbc.xml
      - iam_im_DataSource-tp-jdbc.xml
      - iam_im_DataSource-wf-jdbc.xml
  - **Calculations:**
    - **Per WebLogic Server**
      - Minimal connections per server is: 6 x 5 = 30 connections
      - Maximum connection per server is: 6 x 200 = 1200 connections
    - **Per WebLogic Cluster:** (Four (4) weblogic servers in the weblogic cluster)
      - Minimal connections per cluster is: 4 x 6 x 5 = 120 connections
      - Maximum connection per cluster (with 4 servers): 4 x 6 x 200 = 4800 connections
  - Default are fine for most sites; work with client's DBA team to monitor connectivity during use-case testing; to ensure number of connections are sufficient.

- Actions: Work with DBA to monitor DB connection during use-case testing; adjust initial & max connections to load balance between the six (6) databases, e.g. lower workflow (wf), report (rs), and archive connections and increase objectstore (os), task presistence (tp), and audit, as needed; bounce services & retest use-cases.

ADVANCE / STRATEGIC PLANNING 07

Impact: Medium Value / medium difficulty

- Description: Tune JMS setting for IM databases
  - IM uses JMS to manage events transaction state
    - IM creates a JMS message containing the event ID and posts that message to the Event Message Queue.
    - Upon receiving the message, JMS then invokes an instance of the Event Message Driven Bean, which is an implementation of the Event Controller.
    - The Event Controller uses the event ID in the message to retrieve the event from the task persistence database, and executes the actions for the event's current state.
    - Upon completion of that state, the event is set to the next state, persisted in the task persistence database, and a new JMS message is posted for processing the next state.
  - Default values of 128 for the IM's Event Message Driven Bean pool size is fine for majority of client sites.
    - Monitor IM web application logs to identify any error messages related to JMS queue or event message driven bean pool size
    - Increase to 2x, e.g. 256, if error message are noted above.
- Actions: Review IM install documentation; Update IM configuration files (xml) to change default values for higher maximum value by 2x.; bounce services and validate unit and use-case testing for IM use-cases
- Reference:
  - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?613192.html?

ADVANCE / STRATEGIC PLANNING 08

- **Impact: Low-Medium Value / medium difficulty**

- Description: Move Web Application Server JMS queue from defaults of filestore or embedded Hypersonic database to an enterprise database
  - Requires Web Application Server knowledge/skillset
  - Post install task
  - Increases reliability and performance
  - Common challenge at sites that have issues with JMS queue not setup correctly between members of a web application server cluster
    - Action on one cluster member is not viewable on another cluster member (unless servers are bounced and forced to re-read the database objectstore)
  - Requires services to be restarted/bounced for web application server
  - You may use the IM objectstore as the JDBC database for the JMS queue for the IM application.
- Actions: Review IM install documentation; Review WAS documentation; modify JMS queue to use JDBC; bounce services and validate unit and use-case testing for IM use-cases
- Reference:
  - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?1701130.html

ADVANCE / STRATEGIC PLANNING 09

Impact: Medium Value / High Difficulty

- Description: Create two (2) independent Web Application Server(s)/Cluster's JMS queues
  - Declare one Cluster to be used for **User Interaction** and the other for **Batch processes**
  - Isolate high impact hourly or ad-hoc batch processes or TEWS queries from impacting the user experience for delegated administrators and/or self-service administration use-cases.
  - Pro:
    - Both clusters will use the same IM databases for queries and updates
    - JMS queue and memory usage will be isolated to those tasks that are exposed to the defined Web Application Cluster
  - Con:
    - Tasks that perform updates to the common IM database will not alert the other independent cluster of the update.
    - Cluster need to be refreshed to be aware of updates made by the other cluster if the Web Application Server does NOT supports letting the cache be configured to flush itself on a periodic basis or at a preset time.
  - Requires Web Application Server knowledge/skillset
  - Requires additional h/w footprint
  - Post install task
  - Increases reliability and performance
  - Requires services to be restarted/bounced for web application server
- Actions: Review IM install documentation; Review WAS documentation; install 2nd Web Application Cluster with new Cluster name; bounce services and validate unit and use-case testing for IM use-cases
- Ref: https://supportcontent.ca.com/cadocs/0/CA%20IdentityMinder%2012%206%202-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?856429.html?

ca technologies

ADVANCE / STRATEGIC PLANNING 10

- **Impact: High Value / High Difficulty / Requires DBA assistance**

- Description: Task Persistence Schedule Clean Task Can NOT keep up with data cleanup.
  - Client architecture using the IME ability to expose tasks and business functionality into consumable web services.
    - Updates to IME may exceed a certain point where more data flows into the tasksession12_5 tables than the OOTB IM cleanup task can manage.
    - Validate with daily row counts of this table, before and after each clean-up effort to determine if this is an issue for your environment. Check that tasksession_id is GUID and unique between TP and TPA
    - Reach out to CA support for the latest processes to help assist
    - Scheduled weekly/bi-weekly maintenance periods to:
      - Offline IM solution to run scheduled SQL jobs to
        - Delete all data older than 2-4 weeks
        - Move all data older than 2-4 weeks into the Task Persistence Archive DB
    - Requires DBA assistance / knowledge/skillset
    - Requires downtime for solution; service interruption
    - Increases reliability and performance
    - Requires services to be restarted/bounced for web application server
    - DBA Assistance
      - Use Garbage Collection script under IAM Suite/Tool to remove older data from database (complete remove)
      - Use Reset Status of "In Progress Tasks" > 30 days to Audit Status to allow TP to clean up. See script under IAM Suite/Tool for example.

- Actions: Review IM install documentation; Work with client's DBA team; Schedule back up and dba clean up tasks; bounce services and validate unit and use-case testing for IM use-cases

ca technologies

ADVANCE / STRATEGIC PLANNING 11

- **Impact: Medium Value / Low Difficulty**

- Description: Lower duration for Bulk Load or Bulk Feeder Processes
  - Challenge: Bulk Load or the Bulk Loader (Feeder) are executed sequentially for rows of data
  - Assumption: Direct transaction is NOT being used to TEWS from authoritative source
  - Increase performance by splitting the import data file into two (2) -ten (10) parallel sections; and feed each new file into multiple Bulk Load Task(s) or Bulk Loader (Feed)
    - Job duration will decrease by a linear factor until JVM memory is consume
    - Works well for scheduled feeds, where the pre-processing business logic will split the data file, with the following assumptions
      - Sort all create use-case data from modify user data
      - Pair modify use-case transactions with create use-case for same identity, if possible
      - Spilt file and keep pairs equal weighted between new data files.
  - Alternative: Copy BLC client (java components) into new folder and use as 2nd+ BLC client to parallel feed processes
- Actions: Review IM install documentation for IM Bulk Loader (Feed); Work with client's scripting teams or CA GD development for pre-processing business logic module; that will either use the IM Bulk Loader (feed client) or TEWS; bounce services and validate unit and use-case testing for IM use-cases

ADVANCE / STRATEGIC PLANNING 12

- **Impact: High Value / High Difficulty / Java & Web API coding required**

- Description: Move feed process from scheduled to transactional
  - When the amount of incoming feed data overwhelms a hourly scheduled feed process, clients should review moving the feed process to a new architecture.
    - Client or CA GD services would create a web transactional service bus that would consume authoritative data as it is submitted, then apply pre-processing business logic, as needed, to determine if the record is a new user use-case or modify user use-case,
    - As well, as business logic for employee type
    - Requires web development experience
- Actions: Review IM SDK & TEWS documentation. Review authoritative source information (HR/PeopleSoft/SAP/etc.); validate unit and use-case testing for IM feed use-cases

ADVANCE / STRATEGIC PLANNING 13

- **Impact: Medium Value / medium difficulty**

- Description: Misc. tweaks
  - Web Servers
    - Leverage a properly configured Apache mod_proxy_ajp;
  - JBOSS Tuning
    - Configure JBOSS to bind to a specific IP rather than all IPs;
    - Disable the hot deployment scanner;
      - https://supportcontent.ca.com/cadocs/0/CA%20IdentityMinder%2012%206%202-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?1782017.html?
    - Move JMS off of hypersonic;
  - Membership / Administrator Policies for Roles
    - Avoid using groups in membership policies as they are not subject to in-memory-evaluation
    - Recommend using IM Admin Roles for membership policies for any Use-Case with SOD or Workflows Approval Groups
  - JVM Tuning: Moved to Tactical #8

- Actions: Review miscellaneous tweaks to determine if these will assist in your IME environment.

ADVANCE / STRATEGIC PLANNING 14

- **Impact: Low Value / low difficulty**

- Description: Review common issues during installs & upgrades
  - DNS
    - IP v4 versus IP v6
    - Windows 2008 servers, default installations, attempt to use IP v6.
      - May see communication issues if any component is not setup to understand IPv6.
      - If an issue, update components, adjust component configurations, or disable IPv6 on NICs
  - Firewall ports
    - Ensure connectivity exist bi-directional
      - Use any TCP tool to test
        - telnet hostname port
        - ftp hostname port
        - Ssh hostname port
      - If a connection is made, a window will appear and hold open the connection; otherwise the connection will drop if the port is not open or incorrect.
  - Anti-Virus
    - AV will scan the MS cab files for installation on Windows. The scan process will greatly increase the install duration; and may fail the install.
    - Recommend AV be disabled temporarily until after the installations have completed.
  - OS and/or Web Application Server Permissions
    - Ensure the account used to install the IM components has access to create files and folders under the OS and under the Web Application Server folders.
  - Database permissions
    - Ensure the database id (schema account) has permissions to create tables as a db owner for the IM installation and startup.

ADVANCE / STRATEGIC PLANNING 15

- **Impact: Mixed Value / medium difficulty**

- Description: Understand & streamline business logic within IM's Policy Xpress framework
  - Build data process flows from IME_environment_roles.xml
    - Create table of each IM task name defined for each use-case
    - Columns for each IM task
      - STEP order
      - PX & MX attached to each STEP {With priority number within the step}
      - Data Elements (attributes) updated in each PX Action Rule(s)
      - Recommendations/Notes: Retire/combine or move PX rules
        - Note: Avoid using ModifyUserEvent when possible, to avoid inadvertent looping
      - Include workflow events with user interaction
      - Include update of corporate user store (ldap update)
    - Build visual flow charts of process, in step order, for each task
    - Estimate 2-4 hours effort per PX rule, e.g. 100 PX rules = 400 hours to document & flowchart for analysis

- Actions: Read & research IM Wiki on https://communities.ca.com/web/ca-identity-and-access-mgmt-distributed-global-user-community/ to assist.

ADVANCE / STRATEGIC PLANNING 16

Impact: Medium Value / low difficulty

- Description: Understand & streamline business logic within IM's Identity Policies, Roles, and Tasks' as they are evaluated
  - Optimize Roles
    - Manage Role Evaluation Impact at Login; Use InMemoryEvaluation
      - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?586890.html
    - A single rule with a complex expression is more efficient than multiple rules with simple expressions.
      - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?586890.html
      - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?598903.html
  - Optimize Tasks
    - Manage Task Scope Impact
      - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?586890.html
    - Manage TABs impact within Tasks by removing extra TABS that have no value on the use-case or the TASK
      - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?586892.html
      - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?598858.html
  - Optimize Group membership and management
    - Use User Well-knowns of %MEMBER_OF% AND %ADMINISTRATOR_OF%
      - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?599186.html
  - Optimize Identity policies
    - How Users and Identity Policies Are Synchronized;
      - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?270909.html
- Actions: Research existing Identity Policies, Tasks, Role scoping / evaluation logic; and schedule effort to refine business logic

ca technologies

ADVANCE / STRATEGIC PLANNING 17

- **Impact: Medium Value / low difficulty**

- Description: Isolate & Improve load-balancing of Explore & Correlate Processing
  - Challenge:
    - Current scheduled tasks of explore and correlate processing within the IME, may be executed on any of the IMPS servers.
    - As no load-balancing feature currently exists, the scheduled tasks may end up running simultaneously on the same IMPS server(s)
  - Proposal:
    - Identity IMPS servers that are not heavily CPU bound OR horizontal scale & add a new virtual IMPS server to designate for E&C processes.
    - Create a new IMPS account for batch jobs;(for audit requirements to isolate which service account updated IM accounts.)
    - Create windows or UNIX batch/script that call the IM CLI tool of etautil/ldapsearch to perform the explore and correlation processes
      - If any one of the E&C processes to an endpoint takes more than 2 hours; research a process to split the explore operation into two or more processes than may be executed simultaneously for the same endpoint, e.g.
        - Explore AD by Ous that start with A-M within one batch/script & N-Z within another batch/script
        - Explore LDAP/Mainframe (ACF2/TSS/RACF) with direct LDAP connection using ldapsearch; and update IMPS “pointer” account objects with etautil
        - Use TCP 20389 or 20390
        - Use etautil ability to load password or password hash from file & use OS’ ACLs to lock down access to file.
    - See tactical task where IMPS is tied to IMWA server via host files as alternative solution.

- Actions: Research IMPS CLI tools of etautil/ldapsearch; & scheduler tools of OS (win scheduler / UNIX/Linux crontab)

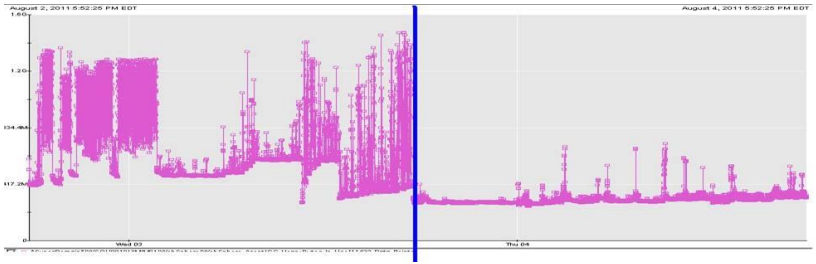
ADVANCE / STRATEGIC PLANNING 18

- **Impact: Medium Value / low difficulty**

- Description: Reduce impact of initial E&C or lengthy E&C processes in IME
  - Challenge:
    - If the initial E&C operation is lengthy, the IMPS call back / notify DSA will be queue to forward events to the IM servers. If this data serves no audit purpose, then the IMPS call back feature may be temporarily disabled.
    - If the E&C operations is execute with the UPDATE feature, where an endpoint attribute is authoritative, e.g. email, telephone, then do NOT disable the IMPS call back feature.
  - Proposal:
    - Temporarily Disabled IM Callback
- Actions: See Help Guide on the Identity Manager Provisioning Server for details to disable IM callback process.

ADVANCE / STRATEGIC PLANNING 19

- **Impact: Medium Value / low difficulty**
- Description: Add CA Wily Tool set to monitor the J2EE platform and Siteminder.
  - Challenge:
    - If performance issues still exist, it make a take a deeper look or observation over a long duration. The CA Wily Toolset is design for continuous monitoring of the JVM and GC (Garbage Collection) for any web application server.
    - It has also been expanded to monitor SiteMinder Agents to improve their performance as well.
  - Proposal:
    - Acquire and Deploy CA Wily for Web Application Server and SiteMinder
- Actions: Monitor performance with CA Wily



MANAGING & CORRECTING ERROR MESSAGES

MANAGING & CORRECTING ERROR MESSAGES - 01

- **Impact: High Value / Medium Difficulty**

- Description: Create Goal for **No Error Message(s)** in Web Application Logs
  - This is the hidden performance challenge
  - After the install or anytime, pull the current full workday log from all web application servers of the cluster.
  - Edit the logs to ensure the server hostname, if missing, is added to the logs, after the date-time stamp
  - Join these files together into one new large file & sort by time stamp
  - Assumption: No common error console currently exist to be leveraged, instead.

- Actions:
  - Identify all error messages, e.g. strings with “ERROR”
  - Categorize and count error messages
    - Infrastructure, e.g. OS, Java, Database, Network
    - Product, e.g IM support with version of Infrastructure
    - Business Logic, e.g. PX Rules/Identity Policies/Custom BLTH/LAH/EL
  - Triage & determine which errors require CA Support Tickets or 3rd party vendor for product or unknown issue. Spend no more than 10 minutes on each issue to triage.
  - Open internal tracking list for CA and non-CA support Tickets
    - Assign resources to issue to resolve or work the issue
    - Tickets should be
      - Resolved (date of fix and deployment to QA/Stage/Model Env. and then when to production Env.),
      - Postponed (low impact),
      - Marked for resolution in confirm service pack (low-medium impact)
      - Escalated for CA support if CA Support ticket resolution not feasible in project time (high impact)
      - Escalated for internal management if internal resources resolution not feasible in project time (high impact)
  - Active Monitoring of Web Application Logs
    - May update log4j to separate IM application events from Web Application Server events
    - May use IM dynamic logging.jsp page to assist with debugging business logic

MANAGING & CORRECTING ERROR MESSAGES - 02

Impact: High Value / Medium Difficulty

- Description: Create Goal of No Error Message(s) in Provisioning Server (eta), IAM CS (log4j) & Endpoint Logs (sa & ADS)
  - This is the hidden performance challenge
    - After the install or anytime, pull the current full work day ETA logs from all provisioning servers
    - Edit the logs to ensure the server hostname, if missing, is added to the logs, after the date-time stamp
    - Join these files together into one new large file & sort by time stamp
    - Assumption: No common error console currently exist to be leveraged, instead.

- Actions:
  - Identify all error messages, e.g. strings with “ERROR”
  - Categorize and count error messages
    - Infrastructure, e.g. OS, Java, Database, Network
    - Product, e.g IM support with version of Infrastructure
    - Business Logic, e.g. IMPS Account Templates, IMPS Proxy Accounts permissions, IMPS Connectors and API access, CX con configuration files, CX Bindings (javascript)
  - Triage & determine which errors require CA Support Tickets or 3rd party vendor for product or unknown issue. Spend no more than 10 minutes on each issue to triage.
  - Open internal tracking list for CA and non-CA support Tickets
    - Assign resources to issue to resolve or work the issue
    - Tickets should be
      - Resolved (date of fix and deployment to QA/Stage/Model Env. and then when to production Env.),
      - Postponed (low impact),
      - Marked for resolution in confirm service pack (low-medium impact)
      - Escalated for CA support if CA Support ticket resolution not feasible in project time (high impact)
      - Escalated for internal management if internal resources resolution not feasible in project time (high impact)
  - Active Monitoring of Provisioning Servers (eta), IAM CS (log4j), & Endpoint Logs (sa & ADS)

MANAGING & CORRECTING ERROR MESSAGES - 03

- **Impact: High Value / Medium Difficulty**

- Description: Create Goal of No Error Message(s) in SiteMinder Policy Server logs; SiteMinder Web Agent Logs; CA Directory router and DSA logs.

- Actions:
  - Identify all error messages, e.g. strings with “ERROR”
  - Categorize and count error messages
    - Infrastructure, e.g. OS, Java, Database, Network
    - Product, e.g IM support with version of Infrastructure
    - Business Logic, e.g. Web Access Logs; DSA/Router logs
  - Triage & determine which errors require CA Support Tickets or 3rd party vendor for product or unknown issue. Spend no more than 10 minutes on each issue to triage.
  - Open internal tracking list for CA and non-CA support Tickets
    - Assign resources to issue to resolve or work the issue
    - Tickets should be
      - Resolved (date of fix and deployment to QA/Stage/Model Env. and then when to production Env.),
      - Postponed (low impact),
      - Marked for resolution in confirm service pack (low-medium impact)
      - Escalated for CA support if CA Support ticket resolution not feasible in project time (high impact)
      - Escalated for internal management if internal resources resolution not feasible in project time (high impact)
  - Active Monitoring of SiteMinder Policy Server;SiteMinder Web Agent; CA Directory Router & DSA logs.

ADVANCE TRAINING

ADVANCE TRAINING - 01

- **Impact: High Value / Medium Difficulty**
- Description: Create a goal of building an IM Sandbox Environment for self-training and validation of use-cases by each business / technical analyst
- Actions:
  - Recommend client invest in and expand client's technical and business knowledge. Client's IM personnel will need to perform OJT (on-the-job-training) with a sandbox environment that emulates client's production environments on the user's laptop to gain further expertise with complex and integrated solutions.
    - Demonstrate the solutions;
    - Perform internal self-training on production use-cases;
    - Validate configurations prior to dev/production rollout;
    - Build documentation for upgrades.
    - Manage complexity integration testing
    - Achieve advance subject matter expertise that is not provided by current vendor training
  - Recommended specs for laptops to support virtualized sandbox images:
    - Laptop Specs - Minimal:
      - Architecture: x64 bit Dual Processor w/ Hyper-threading {either Intel i5/i7 or AMD comparative}
      - BIOS: Support VT (Virtualization Technology)
      - RAM: 8 GB RAM
      - OS: 64bit OS (Windows Server 2008 Standard / Windows 7 or 8 / Linux – Suse or CentOS or Ubutu)
      - Hard Drive: 2 x 500 GB 7200 RPM HDD {one drive for os/programs; other drive for vmware images/snapshots}
      - Video: Standard / As-Is
      - Network: Standard / As-Is (LAN/WiFi)
      - DVD-Rom: Standard / USB version plug-in
  - Laptop Specs - Recommended:
    - Architecture: x64 bit Quad Processor w/ Hyper-threading {either Intel i5/i7 or AMD comparative}
    - BIOS: Support VT (Virtualization Technology)
    - RAM: 16 GB RAM
    - OS: 64bit OS (Windows Server 2008 Standard / Windows 7 or 8 / Linux – Suse or CentOS or Ubutu)
    - Hard Drive: 1 x 500 GB SSD Drive + 1 x 1 TB GB 7200 RPM HDD {one drive for os/programs; other drive for vmware images/snapshots}
    - Video: Standard / As-Is
    - Network: Standard / As-Is (LAN/WiFi)
    - DVD-Rom: Standard / USB version plug-in

ADVANCE TRAINING - 02

- **Impact: High Value / Medium Difficulty**
- Description: Create process to cross training staff with broad base knowledge

Actions:

- Recommend 2-3 day courses (online) for databases (MS SQL/Oracle)
  - Command Line Interfaces (CLI) & Web Administration Console
  - 3rd party tools - Dbvisualizer
- Recommend 2-3 day course (online) for LDAP/X500 Directories (Open LDAP/CA Directory)
  - LDAP CLI (ldapsearch/ldapmod) & LDAP Administrations tools
  - LDIF Format
  - 3rd party tools – Jxplorer, SoftTerra LDAPBrowser/Admin, Apache LDAP
- Recommend 2-3 day course (online) for Web Application Servers (Jboss/WebSphere/WebLogic)
  - Community version Jboss
  - Developer edition WebSphere
  - Developer edition WebLogic
- Recommend 1 day course (online) for building SSL certificates
  - Host based
    - Active Directory certs (TCP 636) / Web Server certs (HTTPS) / LDAPS certs (LDAPS)
- Recommend 1 day course (online) for Log4J configurations and understanding logs
  - Log4J properties / xml files
- Recommend 5 day course (online) for Java coding/decoding
  - JDGui tool to decompile Java class files
  - Build LAH/BLTH/EL
- Recommend 3-4 day course (OJT) for CX connector / operational bindings
  - XML mapping to database / directory
  - Javascript coding for CX operational bindings
- Endpoint knowledge
  - Build own Active Directory Domain/Forest with users/groups
  - Build own Exchange 2010 Mail Server with mailboxes
  - Build own LDAP directory with users/groups
  - Build own database tables with users/groups
  - Build own Linux/Unix server with users/groups
  - Research & Review SAP Modules (ECC/HR/GR); ACF2/RACF/TSS security; Lotus Notes; AS/400; HP-Non Stop; GoogleApps & SalesForce; Oracle Financials (Oracle Applications)

SM PS PERFORMANCE HINTS

SM PERFORMANCE NOTES

- Use of CA Directory for SM policy store. Used at clients for five nines (99.999%)
  - Separate the keystore from the policy store (allows for stepped-up upgrades/migrations)
  - Separate the session store. (CA Directory is the only support LDAP for session store)
- On Vmware with Linux
  - Add hardware devices to improve entropy or add entropy devices to ESX servers
    - Some software solutions exist but they reduce the security by using pseudo entropy
  - Will impact encryption/decryption performance of SMPS
    - Install / Startup
- On RHEL Linux
  - Ownership of files under SiteMinder Policy Server under it's home folder & files under /tmp
    - CPU usage will be reduce from 80%+ -> 5%
  - Update selinux security for SMPS daemons
- JVM tweaks for SM WAMUI
  - Similar to IM JVM tweaks
- Use perl script (various versions exist) to create alternative UI; with FSSUI
  - Will create a 4xagent to be used only by FSSUI to jumpstart an admin ui without deployment of SM WAMUI.
  - Needs a webserver (apache) to allow use of applet.

SM PERFORMANCE NOTES – ADDITIONAL

- SMPS User Directories
  - Similar to IM note; increase the number of entries for the SAME userstore.
  - If you think your directory server can handle (most cannot), you can open more connections to the directory server by doing this trick of editing the local host file.
  -

    /etc/hosts
    10.0.0.1 MyRealLDAPHostname
    10.0.0.1 ldap1
    10.0.0.1 ldap2
    10.0.0.1 ldap3

    When you define your user directory definition, do not use the IP, use the dummy hostnames in a load balanced configuration. With this simple trick you can increase your throughput to the directory server. Note:(As an aside, using the same IP address listed multiple times might work, but there is internal code on when SMPS will mark a connection as bad and remove all IPs. So if there are three IPs listed that are all the same, and have a blip with the directory server, all connections would be marked as bad. Using difference hostnames (which map to the same IP) circumvents this problem.)
  - Ensuring that directory response times are under 10ms (queries are under 1ms and updates are ~3ms avg)
  - Use CA Directory (dxgrid/memory based/ fully indexed/embedded license if used for SM Policy Store)
  - Ref: https://communities.ca.com/web/ca-identity-and-access-mgmt-distributed-global-user-community/message-board/-/message_boards/view_message/98358658?&#p_19
- Use CA wily for monitoring of infrastructure.
  - JVM
  - Directory
- Use the SM Policy Trace tool for performance bottleneck observation/research
  - http://tiny.cc/SMTraceAnalysisTool
- Sepmaphore Memory – SM Web Agents
  - LLAWP process takes extra few seconds to die, even after apache is dead.
  - Use apache restart (not stop/start); as restart has a built in sleep of 10 seconds versus 2 seconds or so if executed manually.

SM PERFORMANCE NOTES – FIVE FREQUENTLY OVERLOOKED ITEMS

Rarely does one ever state, "My SiteMinder rollout is complete". There is usually another application to secure, the need to rewrite policies for finer grained access control, or servers to upgrade or operating systems needing a hotfix. As a result, some fine tuning is often overlooked. The following list contains examples of items that are often overlooked. These particulars range from individual settings to overall solutions; however in the implementations where these are properly addressed, a greater level of ROI and ease of use have resulted with regularity.

1. Tuning Policy Server Threads

Out of the box the SiteMinder Policy server ships pre-configured to run the policy server within 8 threads. This was intentionally kept low over the years for concerns related to context switching and overall resource allocation on mixed servers, but for today's modern hardware that can execute 32, 64 or higher number of threads simultaneously, the default is normally set too low. By setting the number of threads to an exceptionally low number you have intentionally inserted a potential bottleneck into the policy server. To understand how this works, it is important to realize that once the agent sends a request to the policy server, a worker thread is assigned to the request, and that thread remains executing that request until completion. Once complete, the thread becomes available for the next request. Based on this threading model, the number of threads in the policy server is equal to the number of concurrent requests the policy server can ever serve. With a default of 8 threads, if a 9th request is sent from any webagent to the policy server, it will be queued until one of the other 8 requests currently being processed has completed. A symptom of this is a policy server where the CPU utilization never reaches past a set point, even though additional requests are becoming queued. Increasing the number too high may result in resource contention, but users have successfully leveraged between 32 to even 256 threads on a single policy server without problematic issues.

2. IgnoreQueryData Agent Setting

The Ignore query Data Agent configuration object does exactly what it's name sounds like, it tells the webagent and the policy server only to examine the URL up to the "?" in the URL. Most SiteMinder environments do not use data in the querystring (after the "?") as part of their SiteMinder rules, and in the ones that do, it is typically only for a subset of applications within the environment. By telling web agents that are not examining the querystring, the web agent resource and session caches can become much better utilized, and in some cases tuned down to save additional shared memory on the web server. This increased cache utilization on the WebAgent can result in a significant decrease of "isProtected" and "IsAuthorized" requests to the policy server resulting in the policy server getting fewer requests.

3. User Store Performance

Regardless of if the user store is a LDAP directory, or a Database, there are usually some inherent delays while SiteMinder must contact the user store for authentication, authorization queries or to pull specific user attributes for HTTP responses. As discussed above in the thread section, a single thread is bound to a transaction until it completes, and that thread will wait on the user store until it responds to a query. If you take a case where there are 5 queries and each query takes 5ms, that is 25ms of possible wait time just on the request. If the latency of each user store call goes up to 15ms, that 25ms of total wait time increases to a compounded 75ms. This can potentially have a significant impact to each transaction, but can also reduce the total throughput of the policy server. Therefore, it is very important to monitor the user store response times and establish proper SLAs with the team managing the directory/database is use.

4. Audit Reporting

Too often large SiteMinder implementations are not setup, for whatever reason, to gather and analyze the data that can be collected about user habits. This vital function is not only important for future capacity planning and forensics in the event of a purported breach, but also provides the ability to easily report data to the business owners and the decision makers that originally chose to implement SiteMinder. These reports are not just limited to basic information, such as the number of successful / failed logins is very useful, but the ability extends beyond that to items such as the total number of unique daily visitors, as well the top users that repeatedly log into the applications. Users have been able to benefit from the variety of reports that SiteMinder can offer. User generated reports spawned from SiteMinder audit data have been used to identify things such as the top 10 or the least 10 accessed web applications, helping an organization to understand where to potentially focus their money, efforts, and time in the future. What is unique about SiteMinder logging is that it crosses over multiple web applications giving a total picture of what users accessed during their entire session.

5. ServererrorFile ACO Setting As A Monitor

Another great setting is the **ServerErrorFileACO** setting. This setting can tell the webagent what to do in the event some error occurs. Typically this is to display a particular HTML file or redirect the user to another page. Not only does this provide an improved experience for the site's users, as there will invariably be a time an HTTP 500 error message is returned from the webagent for one reason or another, but it can also indicate to site administrators what is happening. One popular idea is to setup a separate web server, which does not have a SiteMinder webagent installed. Then create a generic error message on a URL, for example "error.html". Next, configure all the webagents across the enterprise to use the newly created "error.html" page as an error redirect. Hereafter when an error occurs, the error code will be automatically placed into the querystring of the redirect to "error.html" and if the webserver is setup to log the referrer and this querystring data, the web server log can be used to detect problems. In some cases this could be built as a dynamic application that can log that information into a database or even send out alert messages to administrators. The options can be almost limitless and the configurations seemingly boundless.

Ref: https://communities.ca.com/web/ca-identity-and-access-mgmt-distributed-global-user-community/blog/-/blogs/siteminder-implementation:-five-frequently-overlooked-items

ca technologies

SITEMINDER BACKUP & SM POLICYREADER TOOL

- XPSExport smpolicystore-{datetimestamp}-xb.xml -xb -npass -vT {complete export;sm/ims objects; used for troubleshooting or DAR scenarios}
  - Note: ims objects will not all be exported if the ImsSmObjects.xdd was not previously deployed.
- XPSExport smpolicystore-{datetimestamp}-xa.xml -xa -npass -vT {env only; sm objects; used for migration; less noise}
- XA export (env only) does NOT show the following:
- · IMSEnviornment / IMSDirectory / IMSAdditionalPropertSet / AgentInstance / AgentType / Admin
- Use using XPSExplorer to delete the IMSobjects, if needed, then allowing them to be rebuilt.
- Using the ims=DEBUG, during the import process of a UserStore/IME in the IM Management Console, you can observe the “cloning” process to the SM Policy Store.
- http://tinyurl.com/SMPolicyReader

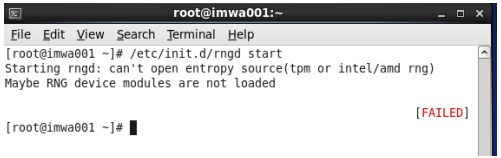
- BEST BACKUP STRATEGY: Use the Directory export process and create an LDIF

TUNING GUIDELINES FROM CA BOOKSHELVES

- Continually monitor the latest IM/SM/Dir/AM/RM bookshelves for new updates
  - Search on keywords of “tune”, “performance”, “pool”, “index”
  - Example:
    - Search of “tune”
      - Returned 13 results for IM r12.6sp2
      - Returned 12 results for SM r12.5
      - Returned 1 results for Dir r12.0sp11
      - Returned 10 results for AM 7.1/RM r3.1
    - Search of “performance”
      - Returned 14 results for IM r12.6sp2
      - Returned 107 results for SM r12.5
      - Returned 60 results for Dir r12.0sp11
      - Returned 61 results for AM 7.1/RM r3.1
    - Search of “pool”
      - Returned 36 results for IM r12.6sp2
      - Returned 18 results for SM r12.5
      - Returned 0 results for Dir r12.0sp11
      - Returned 86 results for AM 7.1/RM r3.1
    - Search of “index”
      - Returned 18 results for IM r12.6sp2
      - Returned 37 results for SM r12.5
      - Returned 16 results for Dir r12.0sp11
      - Returned 31 results for AM 7.1/RM r3.1

HIGH LEVEL NOTES OF ENTROPY

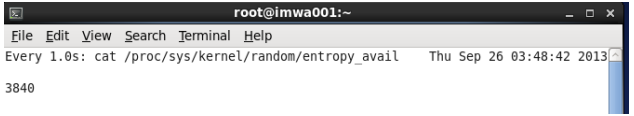
- IM r12.6 bookshelf mentions using rngd & rngd-tools to assist with increasing entropy.
  - This is mentioned to assist with FIPS encryption. Impacts IM JCS Service (IAMCS)
  - Impacts startup time of IM Web Application if integrated with Siteminder.
  - Impacts LDAPS connection performance if IM is integrated with Siteminder.



- SM r12.51 bookshelf mentions replacing the /dev/random driver with pseudo /dev/urandom device driver.
  - Impacts startup time of SMPS and connect to LDAPS
  - When using software replace process, LDAP connect drops from 90+ seconds to less than 1 second.
    - mv /dev/random /dev/random.org then ln –s /dev/urandom /dev/random

- Oracle documents for WebLogic mention replacing the /dev/random driver with pseudo /dev/urandom device driver in the JVM or via RNGD service.
  - Impacts startup time of WebLogic

- RNGD is a software solution used to integrate with hardware components to replenish the entropy pool.
  - The rngd daemon acts as a bridge between a Hardware TRNG (true random number generator) such as the ones in some Intel/AMD/VIA chipsets, and the kernel's PRNG (pseudo-random number generator).
  - It may also be used to connect to the pseudo random device driver, /dev/urandom. Better solution is to integrate RNGD with hardware, e.g. SSL Accelerator Cards. RNGD will pull HW introduced randomness from /dev/hwrandom and feed this to /dev/random.
  - 1) Edit /etc/sysconfig/rngd
    - # Add extra options here
      - EXTRAOPTIONS="-t 2 –W 2048"
    - If NO hardware exist or error is reported upon STARTUP, use these extra options:
      - EXTRAOPTIONS="-r /dev/urandom"
      - EXTRAOPTIONS="-i -o /dev/random -r /dev/urandom -t 10 -W 2048"
        - NOTE: Using –r /dev/urandom is NOT FIPS compliant
  - 2) Enabled rngd as a service : chkconfig rngd on
  - 3) Start Service : service rngd start
  - 4) Test Entropy : cat /dev/random | rngtest -c 1000



EXTRAOPTIONS="-i -o /dev/random -r /dev/urandom -t 0.01 -W 2048" will give a large pool of > 3000 to use; but at the expense of some CPU time
EXTRAOPTIONS="-i -o /dev/random -r /dev/urandom -t 10 -W 2048" will give a range from 130-1800 every few seconds. Very adequate.
EXTRAOPTIONS="-r /dev/urandom" will give a range from 50-180 which seems to work well on vmware image (other values are defaults)

- Monitor Entropy
  - watch -n 1 cat /proc/sys/kernel/random/entropy_avail && What programs are using Entropy: lsof | grep -E "/dev/[u]{0,1}random"

ENTROPY IMPACT: JVM/IM/SM

- BEST: (All environments) {Impact: All solutions + JVM}
  - Use hardware and the RNGD daemon to keep /dev/random populated. Existing hardware may be sufficient, so test this first.
  - Use HAVEGED daemon as the EGD process (input is from processor/clock)
- BETTER: (DEV/TEST/QA) {Impact: All solutions + JVM}
  - Use with RNGD service until hardware can be obtained (NOTE: Using –r /dev/urandom is NOT FIPS compliant)
    - rngd -r /dev/urandom -o /dev/random -t 10
      - {make the number lower to increase refresh of entropy pool}
    - Edit /etc/sysconfig/rngd
      - EXTRAOPTIONS="-i -o /dev/random -r /dev/urandom -t 10 -W 2048"
- GOOD: (DEV/TEST/QA environments) {Impact: JVM only}
  - Change the java configuration in a way that '/dev/urandom' is not mapping directly to '/dev/random'.
  - Change the file $JAVA_HOME/jre/lib/security/java.security:
    - securerandom.source=file:/dev/urandom into
    - securerandom.source=file:/dev/./urandom {/dev/urandom doesn't work due to unknown path issue; must use .}
- GOOD: (DEV/TEST/QA environments) {Impact: JVM only}
  - Add an Java option during startup of the JVM: (Oracle Recommendation)

    -Djava.security.egd=file:/dev/./urandom
    - {/dev/urandom doesn't work due to unknown path issue; must use .}
- Example: Add the Java parameter to setDomainEnv.sh:
  - if ["${USER_MEM_ARGS}" != ""] ; then
  - MEM_ARGS="${USER_MEM_ARGS}
  - export MEM_ARGS
  - fi
  - MEM_ARGS="${MEM_ARGS} -Djava.security.egd=file:/dev/./urandom"
- OK: (DEV/TEST/QA environments) {Impact: All solutions + JVM}
  - Use the pseudo device driver for all applications/system wide update:
    - mv /dev/random /dev/random.org
    - ln -s /dev/urandom /dev/random
- JUMP START Randomness pool: {All environments; add process to boot rc script of OS}
  - dd if=/dev/zero of=filename.iso bs=1G count=50 {where filename.iso is any large file}

IM LOGGING.JSP DEBUGGING 1 OF 2

Here are the list of loggers that I find very useful when debugging. (5 of the hundreds available) / I enabled all loggers for im=debug and ims=debug, exercised use-cases; and then sorted through the list. Note: If using parent loggers, there is the possibility of being “buried in the noise”.

These select loggers will provide the details of the business logic that has been created in IM. I have included some commentary and examples of what would be returned that has high value.

General

ims.tasktrack.custom=DEBUG

- Provides the start of the TASK or EVENT state:

- 2013-08-24 15:15:17,225 INFO [ims.tasktrack.custom] (http-0.0.0.0-8080-2) Entered execute for task ModifyIdentityPolicySet and step VALIDATION

- 2013-08-24 15:15:17,229 INFO [ims.tasktrack.custom] (http-0.0.0.0-8080-2) Exiting execute

- 2013-08-24 15:15:17,233 INFO [ims.tasktrack.custom] (http-0.0.0.0-8080-2) Entered execute for task ModifyIdentityPolicySet and step SUBMITTED

Bulk Loader / BLC / Feeder {View how the BLC or Bulk Load task loads data into IME}

im.feeder = DEBUG

PX Rules

ims.policyxpress = DEBUG

- Provides the complete trail of PX rules being executed

- On a quiet system, use this to document the process data flow between PX rules (combine with identity polices as needed)

ims.jdbc.JDBCManagedObjectProvider=DEBUG

- Provides the name of the PX Rule to # in DB

- Provides the event for PX_WHEN: SELECT "PX_WHEN"."UNIQUE_NAME", "EVENTNAME", "TYPE", "STEP", "POLICYUN" FROM "PX_WHEN" WHERE "TYPE"=? AND "STEP"=? AND "EVENTNAME"=? AND "ENV_OID"=? (6,16,ModifyUser,1)

IM LOGGING.JSP DEBUGGING 2 OF 2

Here are the list of loggers that I find very useful when debugging. (5 of the hundreds available) / I enabled all loggers for im=debug and ims=debug, exercised use-cases; and then sorted through the list. Note: If using parent loggers, there is the possibility of being “buried in the noise”.

Identity Policies

ims.jdbc.JDBCManagedObjectProvider=DEBUG {Same logger as above}

- Provides the name of Identity Policy: SELECT "IM_IDENTITY_POLICY_SET"."UNIQUE_NAME", "ENABLED", "DESCRIPTION", "CATEGORY", "FRIENDLYNAME", "MEMBERRULE", "CONTAINSCOMPLIANCE" FROM "IM_IDENTITY_POLICY_SET" WHERE "FRIENDLYNAME"=? AND "ENV_OID"=? (Test001,1)

- Provides the event for PX_WHEN: SELECT "PX_WHEN"."UNIQUE_NAME", "EVENTNAME", "TYPE", "STEP", "POLICYUN" FROM "PX_WHEN" WHERE "TYPE"=? AND "STEP"=? AND "EVENTNAME"=? AND "ENV_OID"=? (6,16,ModifyUser,1)

ims.llsdk.role.azengine=DEBUG

- Provides the name of the Identity Policy used for a user:

- 2013-08-24 15:15:46,741 DEBUG [ims.llsdk.role.azengine] (http-0.0.0.0-8080-1) PolicyEngine.getCurrentIdentityPolicySets - Found 1 matching policy sets for user uid=bugs,ou=people,o=DEMOCORP,c=AU

- 2013-08-24 15:15:46,780 DEBUG [ims.llsdk.role.azengine] (http-0.0.0.0-8080-1) PolicyEngine.getCurrentIdentityPolicies - Check for preventative identity policies. Identity policy set 'Test001' contains 1 policies

ims.llsdk.role.azcache.ridiculouslydetailed=DEBUG

- Provide detail on Identity Policy

- 2013-08-24 15:15:47,881 DEBUG [ims.llsdk.role.azcache.ridiculouslydetailed] (WorkManager(2)-37) Testing directory policy for user uid=bugs,ou=people,o=DEMOCORP,c=AU with rule [<MemberRule><AttributeExpression attribute="postalAddress" comparator="EQUALS" value="1"/></MemberRule>]

- 2013-08-24 15:15:47,888 DEBUG [ims.llsdk.role.azcache.ridiculouslydetailed] (WorkManager(2)-37) User uid=bugs,ou=people,o=DEMOCORP,c=AU matches directory rule [<MemberRule><AttributeExpression attribute="postalAddress" comparator="EQUALS" value="1"/></MemberRule>]

- 2013-08-24 15:15:47,888 DEBUG [ims.llsdk.role.azcache.ridiculouslydetailed] (WorkManager(2)-37) Finished calculating 1 directory policies for user bugs

JDBC (To see ALL jdbc calls, then the parent logger may be used.)

ims.jdbc =DEBUG ims.tmt.persistence.sql =DEBUG ims.llsdk6.directory.jdbc.sqlexec=DEBUG

ca technologies

DOCUMENT IM BUSINESS LOGIC 1 OF 2

- Goal: Documentation of IM business logic.

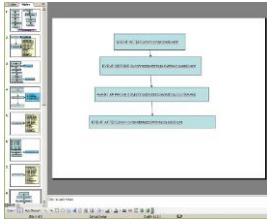
- Business logic may change during the lifecycle of the solution. And as it drifts from initial documentation, it can be a costly process for debugging or adding on new functionality without impacting current business. The process outline below will demonstrate a step by step process of how to capture business logic and then document within MS powerpoint or MS visio for a complete view of all uses cases.

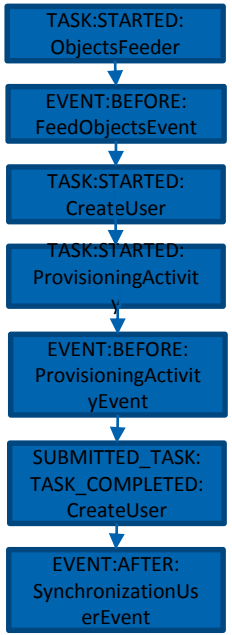
- This process may be time consuming and will require a pre-prod environment that has matching prod business logic.

- The pre-prod system MUST be quiet; which mean no other users or services acting upon the solution during this process; otherwise "noise" will defeat this exercise.

- **Actions:**

  - Deploy the IM logging.jsp process from the CA IM samples (IAM Suite / Tools) to ALL J2EE platforms.
    - Copy this file over the existing STUB jsp with the same name.
    - Recompile for JBOSS (Not required for WebLogic/WebSphere)
  - Launch the browser to the URI with logging.jsp to ALL J2EE servers (or just run one J2EE) (E.g http://imwa001.im.dom:7001/iam/im/logging.jsp)
  - Enabled the following
    - J2EE loggers to DEBUG state {be careful of spaces}
      - **ims.tasktrack.custom** {Used to monitor general start/exit transition for task/event/blth/lah}
      - **im.feeder** {View how the BLC or Bulk Load task loads data into IME}
      - **ims.policyxpress** {Provides the complete trail of PX rules being executed}
      - **ims.llsdk.role.azengine** {Provides the name of the Identity Policy used for a user}
      - **ims.llsdk.role.azcache.ridiculouslydetailed** { Provide detail on Identity Policies executed}
    - IMPS ETAtrans logs (loglevel=**3**) (IMPS\logs\etatrans{datestamp}.log)
    - IMPS ADS log (IMPS\logs\ADS\adshostname.log)
    - If needed; {IMPS Exchange Logs ((IMPS\logs\ADS\adshostname.log) + IMPS CAM Logs (CAM\logs*)
  - Note the time stamp before starting
    - Validate the J2EE logs are quiet
    - If other loggers are present, and are "noisy"; set that logger = WARN in logging.jsp during this exercise.



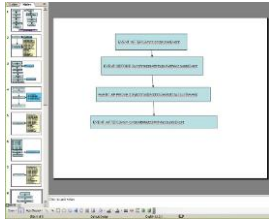


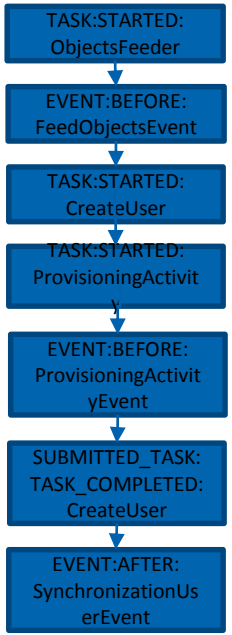
ca technologies

DOCUMENT IM BUSINESS LOGIC 2 OF 2

- Goal: Documentation of IM business logic.

- **Actions:**
  - Execute the beginning of the use-case
    - If using the IM Bulk Loader Client; execute that process for one (1) record pre use-case.
      - Do not use more than one; as this will add "noise" and make it difficult to map the business logic.
  - Monitor the progress of the use-case with IM View Submitted Task
    - When the task shows as "completed", view the J2EE log and ensure that all loggers are viewable, ensuring that they were entered correctly within the logging.jsp.
    - If all loggers are seen, copy this file to your desktop.
  - Open Visio or PowerPoint or any tool that will allow a capture of visual representation of the data flow.
    - Create a starting point with the 1st box; it will be labeled with the very first STEP of the [ims.policyxpress] logger. **TASK:STARTED:ObjectsFeeder**
    - Continue to the next STEP of the [ims.policyxpress] logger; add in arrows between the boxes of the serial data flow.
    - When a STEP has a PX rule executed; identify the step; then add another box (comment) to the side that captures the PX Rule's name
      - Additional information of the PX rule will need to wait, until we capture the entire serial data process flow.
    - This process will continue across multiple slides, as needed, don't crowd the data, as additional information will be added later, to fill out the business logic executed.
    - Create a new deck or visio TAB for each use-case.
    - After the process flow has been captured for each STEP, add in additional notes on PX Rule priorities & PX Action Rules.
      - PX Data Elements (with loops) + PX Action Rules will have their own data flow (Iterators)
      - Multiple PX Rule may exist for the SAME STEP, e.g. priority 10,20,30,40,…,999.
      - Capture the PX data flow on a new deck/visio.
    - If business logic is missing due to BLTH or other custom code; add in these loggers as needed, and re-execute the use-case.
  - Review of business logic
    - Follow PX Framework best practices (see the CA Community Site for the PX Wiki) to move any PX Rule trigger from an EVENT STEP to a TASK STEP.
    - Identify any IM Identity Policies that may be moved to PX Framework
    - Determine if any PX Rule may be adjusted with Data Entry Rule to prevent execution for use-cases that don't apply.
    - Remember to add the IMPS provisioning logs from ETA/ADS/Exchange/CAM to complete the data flow.





ca technologies

APACHE WEB SERVER SETTINGS

- Use best practices from Yahoo/Google Web Developers to increase web server performance
- Independent of solution.
- Focus on httpd.conf settings
  - Modify default eTAGS
  - Add in mod_expires, mod_deflate, mod_header entries.
  - Test with FireFox with Firebug & Yslow for grading scales and monitor any delay.

APACHE W.S. DEFLATE-EXPIRES-HEADERS.CONF

```
## Ensure this configuration is called by Apache 2.2.x httpd.conf

## and that LoadModule entries exist for deflate, expires, headers

## Used for CA IM/SM Bandwidth Performance gain over CPU usage

#### Enable GZIP

<ifmodule mod_deflate.c>

AddOutputFilterByType DEFLATE text/text text/html text/plain text/xml text/css application/x-javascript application/javascript

# Alternative full version

#SetOutPutFilter DEFLATE

# Address Netscape 4.x issue

BrowserMatch ^Mozilla/4 gzip-only-text/html

# Address Netscape 4.06-4.08 issues

BrowserMatch ^Mozilla/4\.0[678] no-gzip

# Address when MS IE masquerades as Netscape

BrowserMatch \bMSIE !no-gzip !gzip-only-text/html

# Don't compress images or select file types. Add fcc for SM

SetEnvIfNoCase Request_URI \

\.(?:gif|jpe?g|png|fcc)$ no-gzip dont-vary

# Make sure proxies don't deliver the wrong content

Header append Vary User-Agent env=!dont-vary

</ifmodule>
```

```
#### Expires Headers - 2678400s = 31 days

<ifmodule mod_expires.c>

 ExpiresActive On

 ExpiresDefault "access plus 1 seconds"

 ExpiresByType text/html "access plus 7200 seconds"

 ExpiresByType image/gif "access plus 2678400 seconds"

 ExpiresByType image/jpeg "access plus 2678400 seconds"

 ExpiresByType image/png "access plus 2678400 seconds"

 ExpiresByType text/css "access plus 518400 seconds"

 ExpiresByType text/javascript "access plus 2678400 seconds"

 ExpiresByType application/x-javascript "access plus 2678400 seconds"

</ifmodule>
```


```
#### Cache Headers

<ifmodule mod_headers.c>

 # Cache specified files for 31 days

 <filesmatch "\.(ico|flv|jpg|jpeg|png|gif|css|swf)$">

 Header set Cache-Control "max-age=2678400, public"

 </filesmatch>

 # Cache HTML files for a couple hours

 <filesmatch "\.(html|htm)$">

 Header set Cache-Control "max-age=7200, private, must-revalidate"

 </filesmatch>

 # Cache PDFs for a day

 <filesmatch "\.(pdf)$">

 Header set Cache-Control "max-age=86400, public"

 </filesmatch>

 # Cache Javascripts for 31 days

 <filesmatch "\.(js)$">

 Header set Cache-Control "max-age=2678400, private"

 </filesmatch>

</ifmodule>
```

ca technologies

Additional Tools JSTACK and Memory Analyzer

The best place to get started is to get a heapdump from the Java JVM that IM is running. JSTACK is a pretty good tool to get this output. Basically, you'll end up with a snapshot of all of the memory and threads in your application server.

Then use the IBM Memory Analyzer Tool to examine the heap. What you're looking for is high memory usage by specific IM classes, and then you can focus on what the bottleneck may be.

JSTACK tips and tricks are here:
How to take Thread Dumps from a JVM

IBM Memory Analyzer Tool is here:
developerWorks : IBM Monitoring and Diagnostic Tools for Java - Memory Analyzer Version 1.4

CA Support is happy to help you analyze the heap dumps.

There are two common types of IM performance issues.

The first is due to poor role rule evaluations. This will be the case if the logins take a very long time before displaying a user's tasks in the IM User Console. This is the link for our documentation on optimizing role evaluations.
Performance and Optimization - CA Identity Manager - 12.6.5 - CA Wiki

The second type is due to an enormous number of users in the task persistence database tables. To avoid this, garbage collection should scheduled on a regular basis.
Cleanup Submitted Tasks - CA Identity Manager - 12.6.5 - CA Wiki