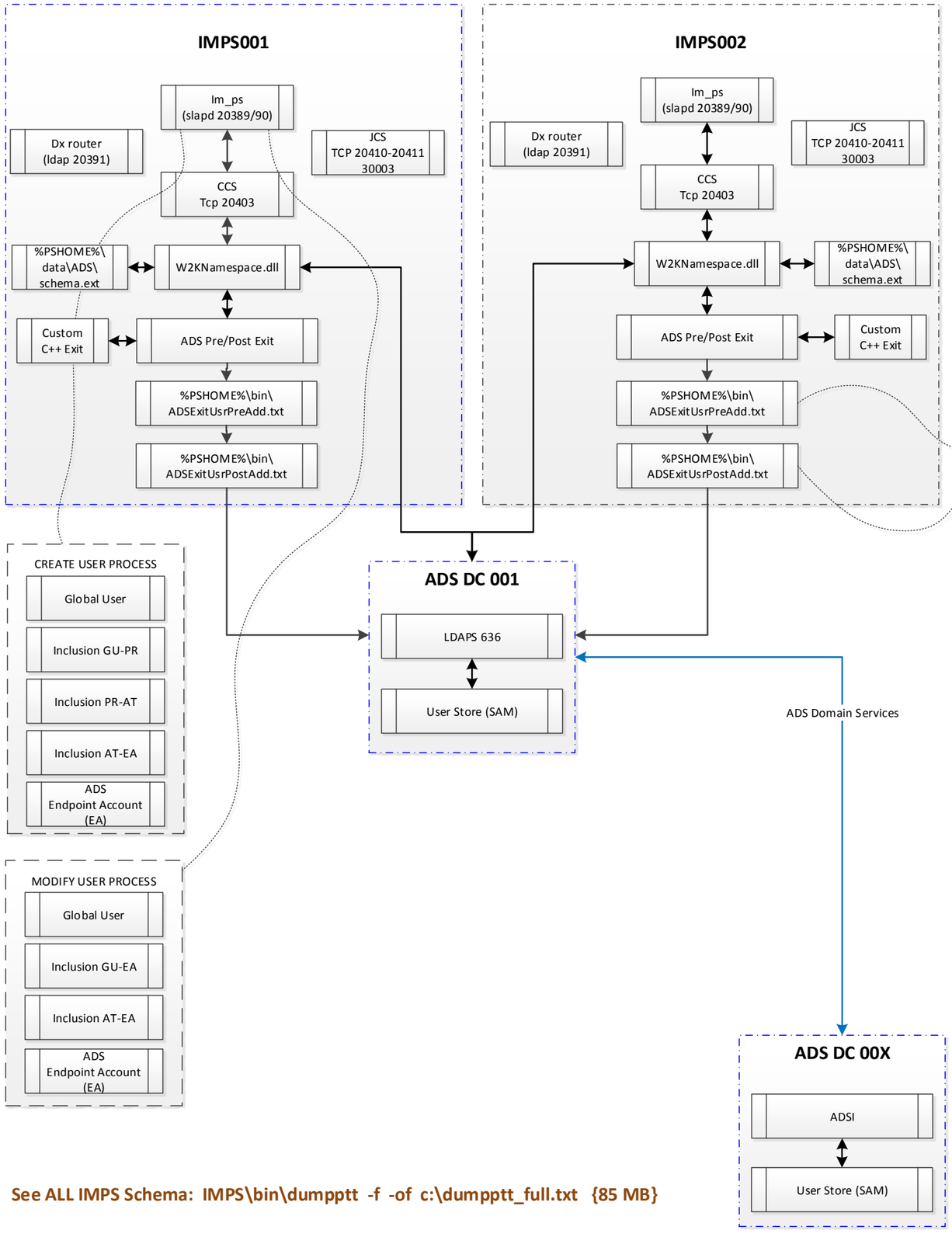
Communication from the IMPS Server to ADS (636) & Log Locations



- %IMPS%\log\im_ps.log IM Provisioning Log; minimal use until debugging is required & enabled
- %IMPS%\log\etatrans.date.log IM Transaction Log (typically set to level=7; may be reduced to level 3 to reduce I/O)
- %IMPS%\log\satrans.date.log SuperAgent Transaction Log creation/modify log
- %IMPS%\data\ADS\schema.ext Used to extend the default IMPS ADS schema to match customer AD Endpoint attributes that are NOT already includes in W2KNamespace.dll (see dumpptt.exe at bottom of screen). This will store data in the eTPayLoad attribute under the EA (endpoint account) object. Do NOT correlate on any attribute defined on schema.ext; as these are fixed base length attributes; and may not return just a single attribute value.
- %IMPS%\log\ADS\hostname.log ActiveDirectory creation/modify log

Useful commands from MS that may be used with IMPS ADS Batch Process

1) dsquery user –samid %SAMID% {Query on existing user by sAMaccountName}

2) dsmod user –samid %SAMID% {Modify user by samAccountName}

3) Netdom query dc {Identify ALL DC in domain}
4) netdom query pdc {Identify the PDC emulator DC/ Recommended as primary DC for IMPS to avoid issues with password reset}

5) Csvde /ldifde {Tools to export ADS User objects}

Limitations of the ADS CLI Pre/Post Batch process.

- Only for create user use-case (will not be called for mod or term)
- Only certain fields are exposed (see the ADS log file for the attributes that are exposed) { you can get around this limitation once you get the GU to perform a 2nd operation in your script to query IMPS}
- Script must be OS compatible with provisioning server OS {if ps is on windows, use VB or powershell or java}

Example: Reset user home folder permissions
cmd /c "ICACLS.EXE \\hostname01\Homefolders\%sAMAccountName% /reset"
cmd /c "ICACLS.EXE \\hostname01\Homefolders\%sAMAccountName% /grant %userPrincipalName%:(OI)(CI)M /T /C"

Examples: Enable Account / Discover mail Server / Set AD Groups
dsquery user -s %active_directory_DC_hostname% -samid %1 | dsmod user -s %active_directory_DC_hostname% -disabled no >> %LogHome%\%LogName%
dsquery * "%BaseOU%" -filter "(sAMAccountName=%1)" -attr msExchHomeServerName
dsquery user -samid %samfromuser%|dsget user -memberof|dsmod group -s %active_directory_DC_hostname% -c -addmbr %touser%

- Windows Event Viewer Minimal use unless debugging

- Windows Event Viewer Minimal use unless debugging

See ALL IMPS Schema: IMPS\bin\dumpptt -f -of c:\dumpptt_full.txt {85 MB}

:: Use MS ADS Resource Kit tool, ldifde and csvde to export ADS data
:: SNAPSHOT BEFORE / AFTER IM DEPLOYMENT
:: to LIDF and CSV formatted files

:: Before running this command replace the two (2) variables below
:: Replace Hostname of an Active Directory Domain Controller Hostname if %USERDOMAIN% does not resolve.
:: Replace ADSDOMAIN with the correct base DN syntax, e.g. "DC=corp,DC=company,DC=com"
:: This program may be execute as any Active Directory User to pull public AD data on TCP Port 389.

set HOSTNAME=%USERDOMAIN%
set ADSDOMAIN="DC=corp,DC=company,DC=com"

:: Reorder Date field for use with filenames
FOR /F "tokens=1-5 delims=/: " %%J IN ('DATE/T') DO (SET newdate=%%M%%K%%L)
:: Reorder Time
FOR /F "tokens=1-5 delims=/: " %%J IN ('TIME/T') DO (IF "%%L"=="PM" (SET /A newtime=%%J*100+1200+%%K)
ELSE (SET newtime=%%J%%K))
set ts=%newdate%_%newtime%

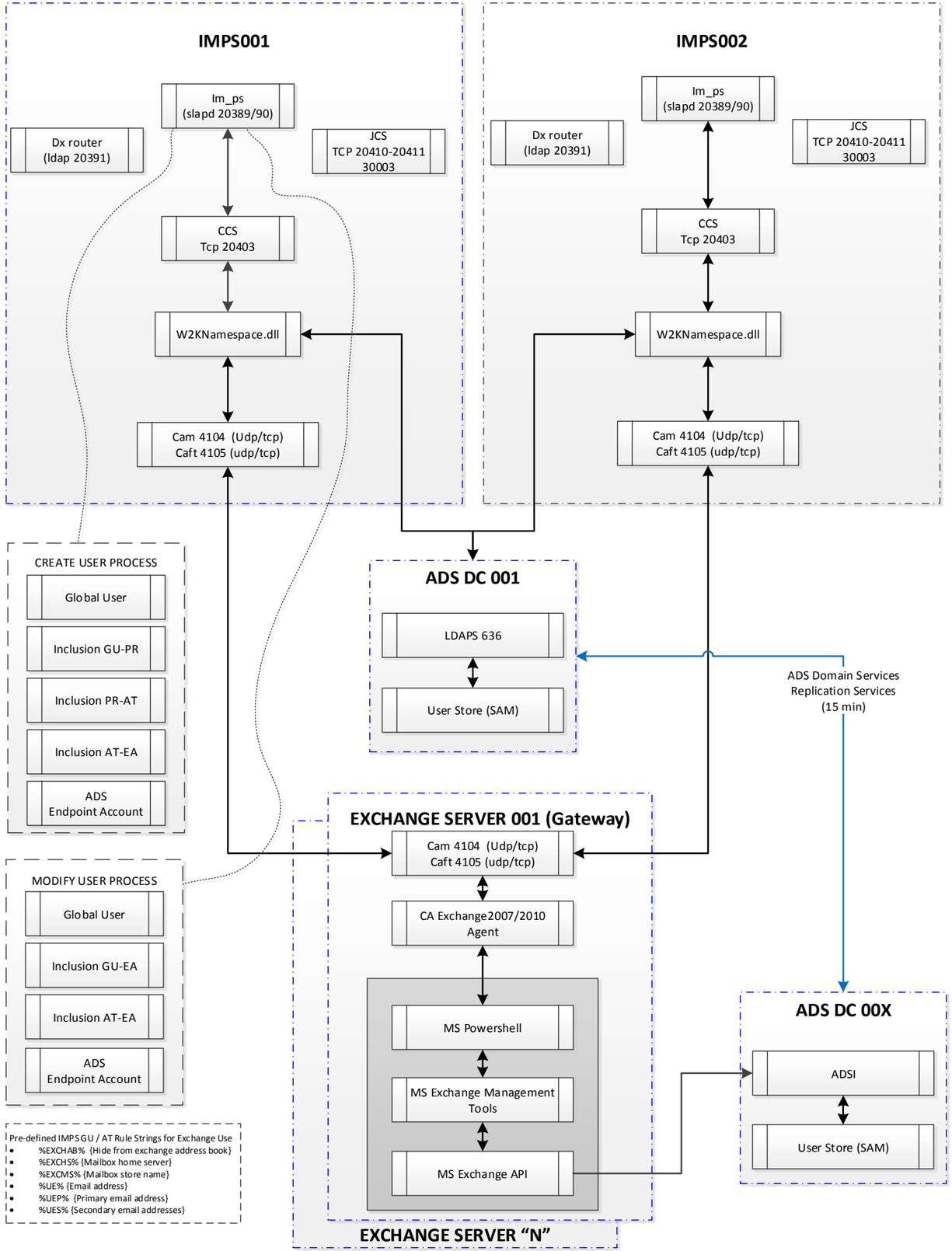
:: CSV Extract
csvde -f %ts%_ADS_Export_Users.csv -s %HOSTNAME% -d %ADSDOMAIN% -p subtree -r
"(&(objectCategory=person)(objectClass=User)(displayName=*))"

@echo Full CSV Extract of AD Users Complete

:: LDIF Extract
ldifde -f %ts%_ADS_Export_Users.ldif -s %HOSTNAME% -d %ADSDOMAIN% -p subtree -r
"(&(objectCategory=person)(objectClass=User)(displayName=*))"

@echo Full LDIF Extract of AD Users Complete

Communication from the IMPS Server to the MS Exchange Server(s) via ADS & CA Exchange Agent & Log Locations



- %IMPS%\log\im_ps.log IM Provisioning Log; minimal use until debugging is required & enabled
- %IMPS%\log\etatrans.date.log IM Transaction Log (typically set to level=7;
  may be reduced to level 3 to reduce I/O but still capture create/mod/term use-cases operations)

- %IMPS%\log\satrans.date.log SuperAgent Transaction Log creation/modify log

- %IMPS%\log\ADS\hostname.log ActiveDirectory creation/modify log
- %IMPS%\log\ADS\Exchange.%id%.txt Output File from IMPS to CAM/CAFT to be sent to Exchange Server CAM/CAFT & Exchange Agent
- %IMPS%\log\ADS\Exchange.out.id.txt Data returned from Exchange Server to be used by IMPS server. This output file may not show if the Service account does NOT have full Exchange Admin permission to view mailbox rights for a user.
- %IMPS%\log\ADS\Exec.out.id.txt Error Code returned from Exchange Server to be used by IMPS server.

- %CAM%\ftlogs CAFT Logs; Minimal use unless debugging
- %CAM%\logs CAM logs: Minimal use unless debugging is enabled to identify issue with communication or encryption

- Windows Event Viewer Minimal use unless debugging

Issue: Exchange 2010 has new throttle limits
IM solution OOTB has uses a service account for IM on the Exchange server with 18 max concurrent login to create/modify Exchange accounts.
Recommendation #1: Increase the throttle sessions to 100 to accommodate IM bulk feeds that are sent in batches with a batch switch of 100.

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

Justification: Scenario: 2000 creations from IME BLC. Exchange able to create user mailbox in 20 seconds. Timeouts bumped to 600 seconds
18 session pool: 2000 * 20 / 18 = 40,000 seconds / 18 = 2222 seconds = < 40 minutes (Expect 5-10% failure due to timeout over 600 seconds)
100 session pool: 2000 * 20 / 100 = 40,000 seconds / 100 = 400 seconds = < 5 minutes [Expect no faliures]

- %CAM%\ftlogs CAFT Logs; Minimal use unless debugging
- %CAM%\logs CAM logs: Minimal use unless debugging is enabled to identify issue with communication or encryption
- %CAM%\E2K7PS_date.log CA Exchange Agent log; Exchange creation/modify log
  Details can be increased using the EXCTraceLevel in Windows Registry
  Pull exact E2KSAUTIL.exe command from this log, to validate Exchange Server's Performance for 1 ID.
- %IMPS%\Exchange.%id%.txt Output File from IMPS to CAM/CAFT sent to Exchange Server CAM/CAFT then Exchange Agent
- %IMPS%\Exchange.out.id.txt Data returned from Exchange Server to be sent & used by IMPS server. This file may not be created if the NT service account does NOT have full Exchange Admin to view the user's mailbox rights.
- %IMPS%\Exec.out.id.txt Return Code from Exchange Server Agent to IMPS server

- Windows Event Viewer Minimal use unless debugging
- Windows Event Viewer - Exchange Server – Minimal use unless debugging

RunBook Notes:
1) CAM/CAFT Disk space; the agent tried to install on Drive C. If the OS is Windows 2008, use MS tool, mklink to move install to drive D:
mklink /j <sourceDir> <destDir>

2) A daily "clean up" script is required to be built by CA or client to ensure the logs don't fill up the disk and to improve performance.
Use "forfiles.exe" (ships with Win2k3 and Win2k8) in a nightly scheduled batch job to remove the CAM/CAFT .txt files
forfiles /s /m <pathToCamCaftFiles>*.txt /d -1 /c "cmd /c del @file"

3) "Gateway" Exchange server should "live" nearby the primary Active Directory endpoint to avoid issues with replication periods, e.g. , intra-site replication period = 5min; inter-site replication period = 15min. Review bookshelf for latest registry/environmental settings to assist.

4) If "Gateway" Exchange server(s) do/does not show up, then there is a permission issue with the AD proxy ID. Re-Explore AD directory with a solid check mark in the top box. Or run this command: ldapsearch %HOST% -p 20389 -D "eTGlobalUserName=%USER%,eTGlobalUserContainerName=Global Users,eTNamespaceName=CommonObjects,dc=%DOMAIN%,dc=eta" -w %PWD% -b "eTADSDirectoryName=%ADS%,eTNamespaceName=ActiveDirectory,dc=%DOMAIN%,dc=eta" -s base "(objectclass=eTADSDirectory)" eTADSexchangeStores eTExploreUpdateEtrust

5) To avoid Windows 2008 UAC impacting cafthost command; Set the environment variable **CAI_Admin_Check=2**, then, re-run **cafthost -l** to test

6) Tactical Fix for Timeout: Bump timeouts from 2-5 minutes to 10 minutes
On Exchange server: Increase timeout of HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Identity Manager\Ex2k7AgentTimeout 600 seconds
On IMPS servers(all): Set the environmental variables, then bounce the im_ccs service. ADS_E2K_SEND_DC=1 & ADS_CONFIRM_MAILBOX 600 seconds

- Exchange 2007/2010 Agent Trace
  [HKLM\...\Identity Manager]
  "EXCTraceLevel"=dword:00000002

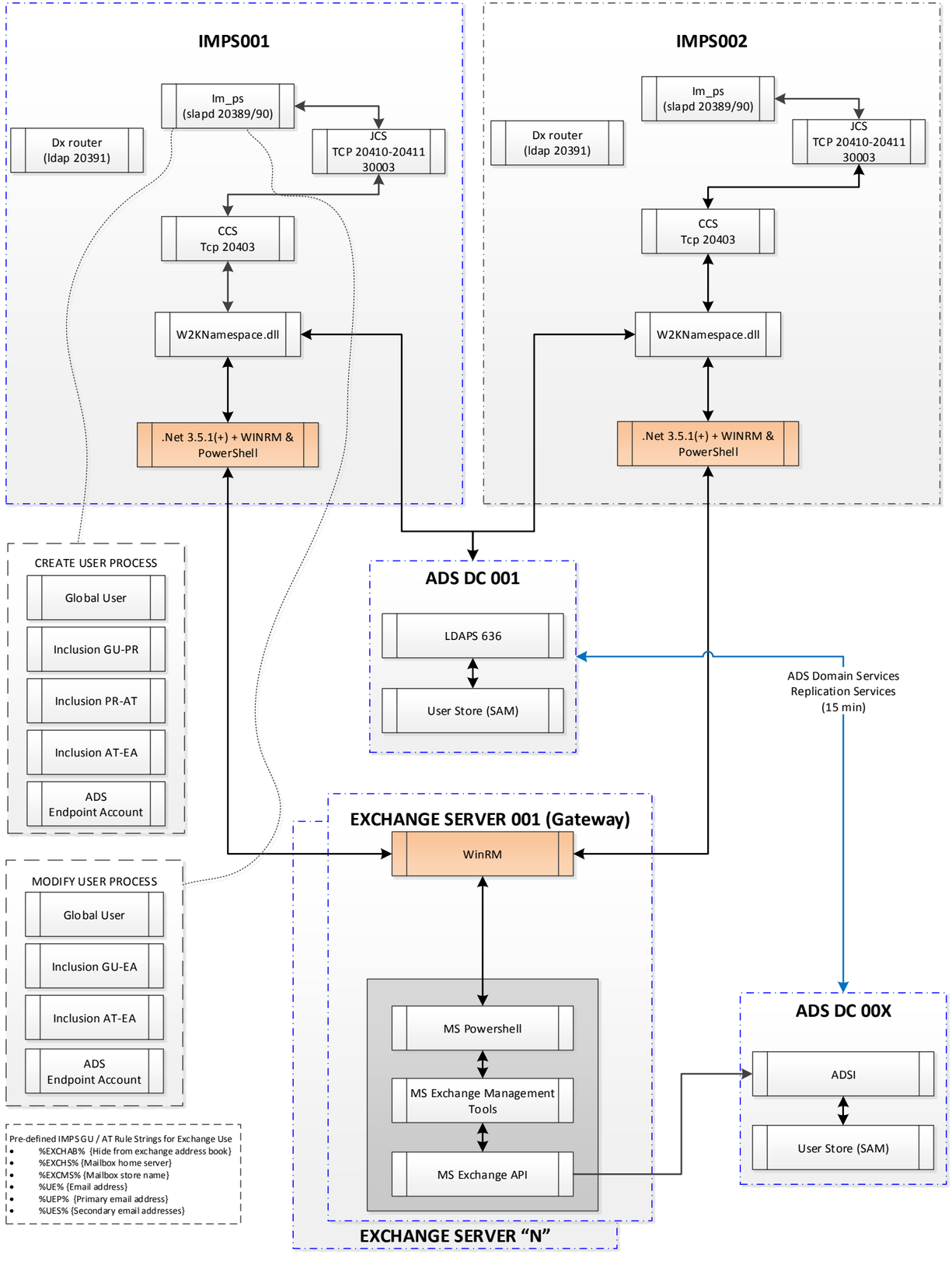
PRO:
- Default / Failover for ADS.
- Exchange provisioning/de-provisioning is integrated with ADS & CPP connector
- Exchange provisioning may be load-balanced as client dictates by round-robin via an attribute stored on GU attributes for Exchange Server & MailStore
- Able to Use ADS Account Templates for ADS attributes & extended attributes for Exchange.

CON:
- ADS payload outgoing only (incoming requires fixed & populated values for correlation use).
- Mixed Exchange environments require latest Exchange agent deployed on ALL exchange servers for Exchange 2010/2007.
- Exchange Provisioning use-cases: ADD/DEL/MOVE
- Performance impacted by three (3) files created for every query to Exchange server.
- Updates to ADS user record to query manager DN and/or password appears to call Exchange Agent
- Exchange agent may query an AD DC that is NOT the same as the IMPS server communicates to.

Requires:
- No Additional Software Required.
- CAM NT Service must be execute by an ADS Domain Account with Exchange Privileges (See bookshelf)
- CAFTHOST must be defined on both Exchange and IMPS servers

Tools:
- **Cafthost -l** {to view IP/hostnames that are allowed; otherwise error message access denied will appear.
- **Cafthost -a** {to add IP/hostnames}
- **Camping** IP/hostname {view comm. over CAM UDP/TCP}
- **Camstat** {to view cam comm.}
- **camconfig save** {config file **cam.cfg**}
  Use Notepad to inspect file
  Ensure no "forwarding" lines exist in this file
- **cam start** or **camclose** {start/stop}
- **cam –d start** {Debug cam}
- **camcheck** {validate installation}
- **camconfig audit on; camconfig trace=all; cam stop; cam start** {full trace debugging}

Communication from the IMPS Server to the MS Exchange Server(s) via ADS & CA Exchange Agent & Log Locations



Pre-defined IMPS GU / AT Rule Strings for Exchange Use
- %EXCHAB% {Hide from exchange address book}
- %EXCHS% {Mailbox home server}
- %EXCMS% {Mailbox store name}
- %UE% {Email address}
- %UEP% {Primary email address}
- %UES% {Secondary email addresses}

- %IMPS%\log\im_ps.log IM Provisioning Log; minimal use until debugging is required & enabled
- %IMPS%\log\etatrans.date.log IM Transaction Log (typically set to level=7; may be reduced to level 3 to reduce I/O but still capture create/mod/term use-cases operations)

- %IMPS%\log\satrans.date.log SuperAgent Transaction Log creation/modify log

- %IMPS%\log\ADS\hostname.log ActiveDirectory creation/modify log
- %IMPS%\log\ADS\Exchange.%id%.txt Output File from IMPS to CAM/CAFT to be sent to Exchange Server CAM/CAFT & Exchange Agent
- %IMPS%\log\ADS\Exchange.out.id.txt Data returned from Exchange Server to be used by IMPS server. This output file may not show if the Service account does NOT have full Exchange Admin permission to view mailbox rights for a user.
- %IMPS%\log\ADS\Exec.out.id.txt Error Code returned from Exchange Server to be used by IMPS server.

- %CAM%\ftlogs CAFT Logs; Minimal use unless debugging
- %CAM%\logs CAM logs: Minimal use unless debugging is enabled to identify issue with communication or encryption

- Windows Event Viewer Minimal use unless debugging

Issue: Exchange 2010 has new throttle limits
IM solution OOTB has uses a service account for IM on the Exchange server with 18 max concurrent login to create/modify Exchange accounts.
Recommendation #1: Increase the throttle sessions to 100 to accommodate IM bulk feeds that are sent in batches with a batch switch of 100.

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

Justification: Scenario: 2000 creations from IME BLC. Exchange able to create user mailbox in 20 seconds. Timeouts bumped to 600 seconds
18 session pool: 2000 * 20 / 18 = 40,000 seconds / 18 = 2222 seconds = < 40 minutes (Expect 5-10% failure due to timeout over 600 seconds)
100 session pool: 2000 * 20 / 100 = 40,000 seconds / 100 = 400 seconds = < 5 minutes [Expect no failures]

https://docops.ca.com/ca-imag-connectors/1-0/EN/microsoft-active-directory-microsoft-exchange-and-microsoft-lync/how-to-connect-to-exchange-2010-and-2013-agentless

- %IMPS%\Exchange.%id%.txt Output File from IMPS to CAM/CAFT sent to Exchange Server CAM/CAFT then Exchange Agent
- %IMPS%\Exchange.out.id.txt Data returned from Exchange Server to be sent & used by IMPS server. This file may not be created if the NT service account does NOT have full Exchange Admin to view the user's mailbox rights.
- %IMPS%\Exec.out.id.txt Return Code from Exchange Server Agent to IMPS server

- Windows Event Viewer Minimal use unless debugging
- Windows Event Viewer - Exchange Server – Minimal use unless debugging

RunBook Notes:
~~1) CAM/CAFT Disk space; the agent tried to install on Drive C. If the OS is Windows 2008, use MS tool, mklink to move install to drive D:~~
~~**mklink /j <sourceDir> <destDir>**~~

~~2) A daily "clean up" script is required to be built by CA or client to ensure the logs don't fill up the disk and to improve performance.~~
~~Use "forfiles.exe" (ships with Win2k3 and Win2k8) in a nightly scheduled batch job to remove the CAM/CAFT .txt files~~
~~**forfiles /s /m <pathToCamCaftFiles>*.txt /d -1 /c "cmd /c del @file"**~~

3) "Gateway" Exchange server should "live" nearby the primary Active Directory endpoint to avoid issues with replication periods, e.g. , intra-site replication period = 5min; inter-site replication period = 15min. Review bookshelf for latest registry/environmental settings to assist.

4) If "Gateway" Exchange server(s) do/does not show up, then there is a permission issue with the AD proxy ID. Re-Explore AD directory with a solid check mark in the top box. Or run this command: ldapsearch %HOST% -p 20389 -D "eTGlobalUserName=%USER%,eTGlobalUserContainerName=Global Users,eTNamespaceName=CommonObjects,dc=%DOMAIN%,dc=eta" -w %PWD% -b "eTADSDirectoryName=%ADS%,eTNamespaceName=ActiveDirectory,dc=%DOMAIN%,dc=eta" -s base "(objectclass=eTADSDirectory)" eTADSexchangeStores eTExploreUpdateEtrust

~~5) To avoid Windows 2008 UAC impacting cafthost command, Set the environment variable **CAI_Admin_Check=2**, then, re-run **cafthost -l** to test~~

6) Tactical Fix for Timeout: Bump timeouts from 2-5 minutes to 10 minutes
~~On Exchange server: Increase timeout of HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Identity Manager\Ex2k7AgentTimeout 600 seconds~~
On IMPS servers(all): Set the environmental variables, then bounce the im_ccs service. ADS_E2K_SEND_DC=1 & ADS_CONFIRM_MAILBOX 600 seconds

- Exchange 2007/2010 Agent Trace
  [HKLM\...\Identity Manager]
  "EXCTraceLevel"=dword:00000002

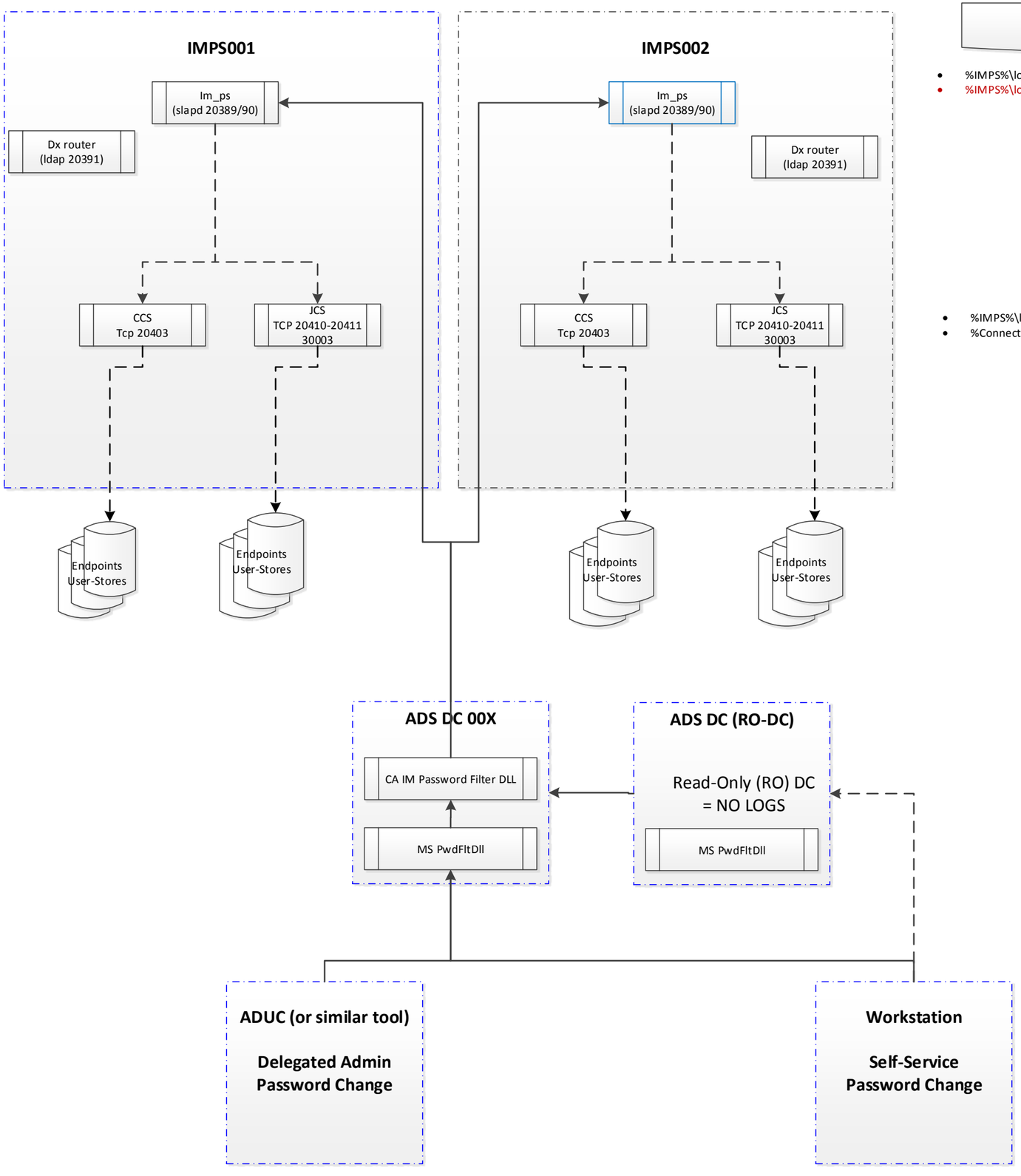
PRO:
- Default / Failover for ADS.
- Exchange provisioning/de-provisioning is integrated with ADS & CPP connector
- Exchange provisioning may be load-balanced as client dictates by round-robin via an attribute stored on GU attributes for Exchange Server & MailStore
- Able to Use ADS Account Templates for ADS attributes & extended attributes for Exchange.

CON:
- ADS payload outgoing only (incoming requires fixed & populated values for correlation use).
- Mixed Exchange environments require latest Exchange agent deployed on ALL exchange servers for Exchange 2010/2007.
- Exchange Provisioning use-cases: ADD/DEL/MOVE
- Performance impacted by three (3) files created for every query to Exchange server.
- Updates to ADS user record to query manager DN and/or password appears to call Exchange Agent
- Exchange agent may query an AD DC that is NOT the same as the IMPS server communicates to.

Requires:
- No Additional Software Required.
- CAM NT Service must be execute by an ADS Domain Account with Exchange Privileges (See bookshelf)
- CAFTHOST must be defined on both Exchange and IMPS servers

Tools:
- Winrm
- Powershell
- .NetFramework

Communication to/from the IMPS Server from ADS & Log Locations



- %IMPS%\log\im_ps.log IM Provisioning Log; minimal use until debugging is required & enabled
- %IMPS%\log\etatrans.date.log IM Transaction Log (typically set to level=7; may be reduced to level 3 to reduce I/O)

- %IMPS%\log\satrans.date.log SuperAgent Transaction Log creation/modify log
- %ConnectionServer%\log\jcs.log JCS Connector Service; Transaction logs log4j logging

- %CA_Password_Filter%\ads_pwd.log CA AD Password Filter agent; Very useful
- eta_pwdsync.conf
- Two (2) Loggers:
  logging_enabled=yes (DEFAULT)
  ldap_logging_enabled=no (DEBUG ONLY)

NOTE: Set these where the im_ccs service runs. Ensure these are SYSTEM environmental switches and NOT user environmental switches.

NEWER AGENTLESS

ADS_AGENTLESS_MODE: 1 [AB. High Value. Will force AGENTLESS connection to Exchange 2010 & UP]
ADS_AGENTLESS_AUTHMETHOD: 2 [AB. High Value. Default value = 2, Kerberos authentication]
ADS_AGENTLESS_MAXCONN: 100 [AB. High Value. Default value = 3. Increase to **100** and ALSO have Exchange Admin create a new quota for the service account used to create mailboxes. Default Exchange Powershell Quota is **18**. New-ThrottlingPolicy MaxPowershell -PowerShellMaxConcurrency 100 AND Set-Mailbox "ServiceAccountID" -ThrottlingPolicy MaxPowershell]
ADS_AGENTLESS_LOGLEVEL: 1 [AB. Monitor. Default value = 1. Error level ONLY, increase to level 3 for debugging]

OTHER ENV SWITCHES

ADS_CONFIRM_MAILBOX: 600 [AB. Medium Value. CCS service will wait 10 minutes for single account. Exchange Powershell Mailbox Quota of 18 and BLC with 1000's of users.]
ADS_DISABLE_DCSTATUS: 1 [AB. Low Value. Mask the AD Failover List in the IM Prov Manager UI]
ADS_DISABLE_PRIMARYGROUPNAME: 1 [AB. Low Value. Mask the viewing the default AD Primary Group in the IM Prov Manager UI]
ADS_E2K_SEND_DC: 1 [AB. High Value. Send the DC hostname to the Exchange server to query first instead of Exchange relying on its current pool]
ADS_FAILOVER: 1 [AB. High Value. Requires service account can view all alternatives DC. May limit failover DC via properties file.]
ADS_FORCELOG: 1 [AB. Monitor. Seems only valuable for debugging. Has performance hit.]
ADS_SIZELIMIT: 50000 [AB. Low Value. The IMPS service can page with lower limits. Impact if this value is > what AD default page limit size is.]
ADS_WTS_TIMEOUT: -1 [AB. Medium Value. Performance if Terminal Services attribute are NOT being managed, e.g. changed in Account Templates or PX rules.]

*** ***

REFERENCES:

ALL AGENTLESS TOKENS FOR EXCHANGE
https://wiki.ca.com/display/IMGC10/Configuration+Options+for+Exchange+in+Agentless+Mode
https://wiki.ca.com/pages/viewpage.action?pageId=120917462

ADS_CONFIRM_MAILBOX
http://cookbooks.ca.com/cagovernanceminder/2014/02/14/solution-for-microsoft-exchange-performance-problems/
https://supportcontent.ca.com/cadocs/0/CA%20Identity%20Manager%20r12%205%20SP15-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?1565452.html?zoom_highlight=ADS_CONFIRM_MAILBOX

ADS_E2K_SEND_DC
https://supportcontent.ca.com/cadocs/0/CA%20Identity%20Manager%20r12%205%20SP15-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?1826645.html?zoom_highlight=ADS_E2K_SEND_DC
https://wiki.ca.com/display/IMGC10/Known+Issues+for+Exchange

ADS_FAILOVER
http://www.ca.com/us/support/ca-support-online/product-content/knowledgebase-articles/tec449125.aspx
https://supportcontent.ca.com/cadocs/0/CA%20Identity%20Manager%20r12%205%20SP15-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?388312.html

ADS_FORCELOG
https://wiki.ca.com/display/IMGC10/Overwrite+the+Logging+Configuration+on+an+Active+Directory+Endpoint

ADS_SIZELIMIT
https://wiki.ca.com/display/IMGC10/Change+the+Page+Size+for+Paged+Searches

ADS_WTS_TIMEOUT
https://wiki.ca.com/display/IMGC10/Known+Issues+for+Active+Directory