How to choose a good corporate user store for the CA IM solution

Alan Baugher

12/05/2013

Ref: https://support.ca.com/cadocs/0/CA%20IdentityMinder%2012%206%202-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?267323.html

Requirements

- Security / Audit / Governance
- Cost
- Schema
  - See Samples/Examples under installed folder of CA IAM Suite
- Authentications
- Authorization
- Provisioning
- Performance
  - Corporate User Store Load-Balancing
- Scalability / High-Availability

Security/Audit/Governance Requirements

- Client Security policies, PCI, SOX tend to emphasize limited exposure to IM administration functionality.
- The userstore should have well defined administration processes that limit updates to the userstore via the IdentityMinder solution and audit the processes.
- Direct access to the userstore should be avoided and not allowed except as part of select approved administrative functions as backup, recovery, bulk loading.
  - Ensure that Directory ACL exist and are enforced for service and administrative ID with the Directory solution itself. (see example at end of deck)
- Exposure of the userstore outside of the IdentityMinder solution allows for
  - Compromise of the IM authorizations
    - e.g. userstore could be manipulated to grant excessive authority by updating a user’s attribute used as a part of implicit role access or directly update IM Well-Known attributes to adjust access, with no audit trail except userstore’s directory logging.
  - Exposure of sensitive business data/logic.
- Existing userstores may have exposure due to pre-existing processes, access, or direct updates to the ldap userstore.
  - Active Directory has this exposure due to the access of the Administrators and other administrative groups that grant access to users’ profiles on the userstore.
  - Active Directory allow ALL domain users to have full access to non-sensitive attributes in Active Directory domain for users & groups. Any user can execute MS tools CSVDE/LDIFDE to dump the AD userstore to their workstation.
    - `csvde -f ADS_Export_Users.csv  -s  %LOGONSERVER%   -d %USERDOMAIN%   -p subtree  -r   "(&(objectCategory=person)(objectClass=User)(displayName=*))"`
    - `ldifde -f ADS_Export_Users.ldif  -s  %LOGONSERVER%   -d %USERDOMAIN%   -p subtree  -r   “(&(objectCategory=person)(objectClass=User)(displayName=*))"`
      - Where LOGONSERVER is the user Active Directory DC and USERDOMAIN is the Active Directory domain; both value may be viewed on a workstation with the windows command line window and the **set** command.
      - Note: If coping from PPT to windows cmd; replace the minus and the double quote characters; otherwise windows cmd will complain.

Cost Requirements

- Lower cost through existing x500/ldap directory assets
  - If an current LDAP Directory infrastructure exists and meets the other requirements, this will be one of the lower TCO solutions from a in-house supportability versus userstore cost.
- Lower cost using the CA Directory, that is included in the IM solution as an embedded license; and is fully supported by CA IM support team.
  - Utilize the ability of CA Directory to run on existing physical assets or co-locate with the J2EE platform.
  - Utilize the ability of scalability of CA Directory and Directory router for performance; no H/W LB needed!!!
  - Utilize the client IdM team knowledge of CA Directory (as it is embedded within in the CA IdentityMinder Provisioning Server as the Provisioning Directory)
  - Utilize the open schema process to rapidly convert other vendor directories data/LDIF to CA Directory.
  - Note:
    - Check with your local CA Sales team to ensure licensing has not changed; as this document may get dated.
    - If CA Directory functionality is expanded beyond CA IM; then CA Directory would need to be licensed separately.

Schema Requirements

- The corporate user store is recommended to support InetOrg schema attributes or similar to maintain information for:
  - User’s profile attributes [Mandatory]
    - Userid
    - FirstName (givenName)
    - LastName (sn)
    - Login ID (if different than Userid)
    - memberOf
    - Etc. {may be 20-100’s}
  - Group attributes <u>[Optional]</u>
    - If business requirements indicate a need to manage scope via groups in corporate user store.
    - Ensure referential integrity is maintained for group-user management.
  - Organization <u>[Optional]</u>
    - If business requirements indicate a need to manage scope via organization units in corporate user store.
    - Recommend using FLAT user-store (no Org Structure), unless using OU for scoping/SOD rules or if userstore is expected to be a size beyond 8GB.
  - CA Identity Minder/SiteMinder attributes
    - Expansion of existing user stores will be required to add in required attributes for the CA IM / SM solutions, e.g. 10-15 attributes
    - Expansion of additional attributes to manage client IM business logic, e.g. 20 single-value + 20 multi-value attributes
    - <u>If the corporate user store is **not** owned by the client IM team</u>, they will need to manage the relationship with the client userstore team to expand the schema and SLA requirements. This is typically process if using Active Directory as a userstore.
- Indexing
  - All objects that can be searched on by a user or internal IM/SM processes will need to be indexed.
    - Example: userid, lastname, businessunit, IM Well-Known, groupnames, etc.
- Maintenance cycle
  - Update to the corporate user store should be planned once a quarter to apply any vendor release patches and/or add in additional schema.
  - Determine if directory architecture will allow for phased migration of updates or if entire IM solution will need to be stopped.
- IMPS as a user store - Not recommended
  - IMPS (IMPD) was used as userstore for earlier IM solutions but had challenges as it was a fixed schema and no updates were allowed to prevent impact during upgrades; and has challenges with scalability, as no load-balancer may be placed in-between the IMWA::IMPS interface, due to possible RACE scenarios, typically seen with bulk loads of create and modify operations that may be sent to different IMPS servers; where the modify operation occurs prior to the create operation; and thus fails; requires a re-submit of the mod.
  - Note: With the use of AUX classes, the IMPS userstore (IMPD) may be expanded as needed for additional/unlimited custom fields. These fields would be managed via 1:1 mapping in the IME and accessible via Jxplorer. The IMPS GUI (Provisioning Manager) would not have a view into these additional custom fields.

Authentication (AN) Requirements

- The corporate user store may or may not be the authentication source.
- The reference architecture for the CA IM solution uses the corporate user store as the authentication source.
- Modification of the reference architecture for CA IM solution is allowed in two (2) cases
  - Use of a CA Global Delivery module to allow redirect of J2EE/IME application authentication for internal users to a client's Active Directory environment.
    - Corporate User Store UserID must match the ActiveDirectory samAccountName
  - Use of CA SiteMinder integrated with CA IM to allow any directory/database source to be mapped one to one to the corporate user store for authentication.
    - Mapping between Corporate Store UserID and other authentication source is flexible; and only limited to directory/database configuration supported by SiteMinder.
    - Siteminder with MS IIS may be leveraged for use of IWA (integrated windows authentication) to provide for a seamless SSO user experience from the user's workstation to the IM application or other SSO protected apps.

Authorization (AZ) Requirements

- The corporate user store is the authorization source.
- Authorizations are managed by the IM Admin Roles for access with the IM User Console (IME=IM Environment).
- Authorization are managed by the IM Provisioning Roles for access to managed endpoints.
  - The Provisioning Roles are attached to Account Templates, which define endpoint specific policies/entitlements to create and manage access on the endpoints.
  - Endpoint is a reference to managed userstores: Active Directory, Exchange, Oracle Databases, SQL Databases, LDAP, Lotus Notes, AS/400, ACF2/TSS/RACF, UNIX, NIS, Salesforce, Google Apps, etc.   See IM bookshelf for complete list.
- Implicit scoping of access to IM Admin Roles may be managed via corporate user store groups or corporate user store organizations or attribute from a user’s profile.
  - Authorization by group or OU must be done via implicit scoping within the IM Admin Roles.
  - Or via implicit granting of the IM Admin Role via IM business logic with Identity Policies or PolicyXpress rules using group membership or OU location.

Provisioning (PR) Requirements

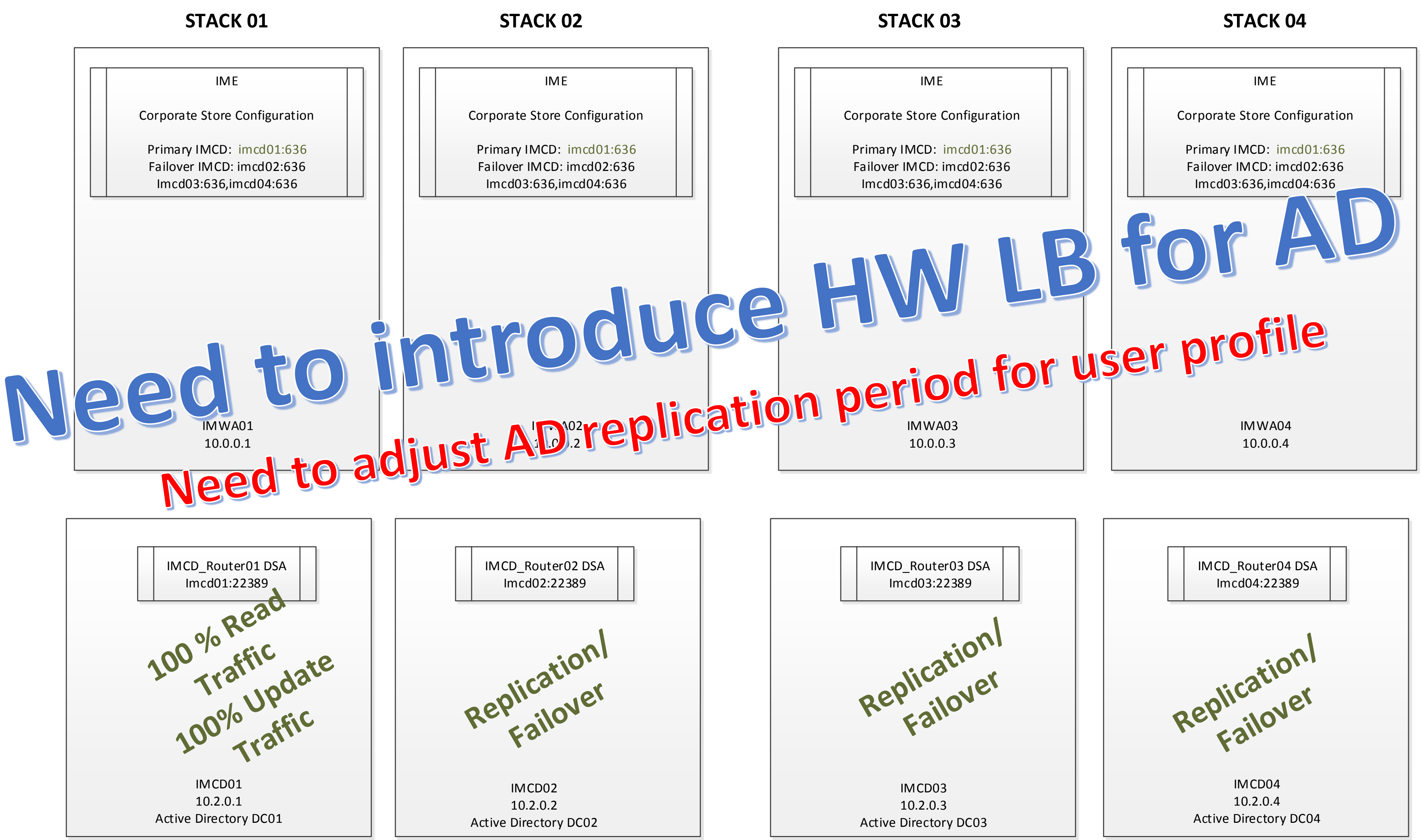
- CA Identity Minder Reference Architecture allow for two (2) major provisioning architectures
  - IM Web Architecture (no endpoint provisioning/no provisioning server)
    - Typically used to manage external customers and external applications that use the corporate user store and/or IM web services.
    - Also the basis for CA CloudMinder (IM/SM/AM integrated platform)
  - IM with endpoint provisioning.
    - Typically used to manage ANY provisioning requirements to a supported endpoint for internal/external users.
    - May be used with CA CloudMinder with onsite/onpremise mid-tier component to manage client's hosted endpoints.
- The reference architecture of the CA IM solutions defines two types of provisioning.
  - Provisioning of the identity (user object), group, or OU within the IME (top tier)
  - Provisioning of the identity (user object) to managed endpoints.
    - The IM Provisioning Server has no open API or processes to allow for endpoint Group provisioning (create/mod/del groups)
    - The IM Provisioning Server has no open API or processes to allow for endpoint OU provisioning (create/mod/del OU)
    - The IM Provisioning does perform the following with regards to endpoint groups/OU
      - Provisioning of the identity to endpoint, and update memberOf attribute for endpoint Group membership and/or placement of the identity within the correct OU location for create/mod
  - To expand IM Provisioning functionality to non-identities objects within endpoints; clients may leverage the IM SDK to build custom JSP page with remote endpoint calls to meet any endpoint requirement. If the endpoint requirements are limited, e.g. create group, a client may leverage the IM PX framework to call a custom Java module to update endpoints, example: Create AD groups/OU with an associated screen.
- Data flow Requirements
  - The creation of a user object with provisioning to endpoints process flow:
    - User object is create in IM corporate user store (with IM business logic to update or transform attributes);
    - User object is attached to a IM provisioning role;
    - User object is created in the IM Provisioning Server/Directory user store (mid-tier/provisioning engine for managed endpoints)
    - User object is created in management endpoint with defined policy/entitlements as prescribed in IM Account Template associated with Provisioning Role
      - If endpoint user account already exist, then the create process will fail; and no entitlement will be updated,
      - For AD, this also means that no AD account and no Exchange mailbox will be created.
- No Challenges/Concerns for "IM Web Architecture" for any userstore.
- Challenges/Concerns to avoid or manage:
  - Any requirement for "IM with endpoint provisioning"
    - where there is any expectations of current or future endpoint provisioning to the corporate user store as a managed endpoint
    - This is a warning flag, due to data flow requirements with "collision" of use-cases for create/mod/term.
  - Typically, this usually includes Active Directory.
    - A way to manage this challenge is to avoid management of AD as an endpoint within the IMPS server; which includes NO acquiring AD as an endpoint; NO E&C; ProvRoles/AccountTemplates/ReverseSync; but this also eliminates the ability to manage AD/Exchange with IM business logic in IdentityPolicies and PolicyXpress

Performance Requirements

- CA Identity Minder Reference Architecture provides for failover to the corporate and provisioning user store
  - Defined in the IM Management Console with a primary userstore and a list of failover userstores (hostname:port)
  - With SM integration,
    - The IM Management Console will “clone” the IM Directory objects to the SM Policy Store and create two (2) objects:
      - SMobject User Directory
      - SM-IMSobject User Directory.
    - SiteMinder must have the same network path to the corporate user store and provisioning user stores that the J2EE (Jboss/weblogic/websphere) have.
- Performance between different vendor LDAP directories are on par with each other using memory cache features or loading the entire directory into memory when using the same hardware: CPU/RAM.
  - CA Directory uses DXGrid process, to load and index the ensure user store for 2-3x faster response than other directories.
  - Indexing is VERY important of all IM Well-Known objects
- To achieve a factor of 2x-100x faster response for the corporate user store, it is necessary to introduce “load balancing” functionality between the J2EE platform (and SiteMinder Policy Server) and the supported user stores. “
  - **Static Load Balancing** is a concept to address **active/passive** userstore architecture. [X faster depend on number of nodes]
    - This concept will leverage “host aliases” to improve userstore architecture data flow.
    - Requirement: Two (2) or more nodes of IM solution exist at J2EE tier; two (2) or more nodes of corporate user store exists.
    - How: Update J2EE servers’ host file to use host file aliases for corporate user stores 1 & 2; Flip IP between J2EE hosts to enforce J2EE #1 uses UserStore #1 and J2EE #2 uses UserStore#2
    - Challenge/Concern: Typically update operations for LDAP is sent to one primary LDAP server and allowed to replicate via LDAP vendors internal mechanism. Possible race condition if two (2) updates are sent to the same user object for the same attribute on both IME. Very unlikely, but client must be aware of concern and monitor for this process.
    - If client suspects concern, client would roll-back the host aliases to correct Ips, reperform use-case, if issue still exists, then client would open a CA support ticket to work the issue.
  - **Dynamic Load Balancing** is a concept that managed the rule-of-thumb estimate: 90% of LDAP activity/traffic are queries. [4-10x + faster]
    - This concept will leverage true load balancers, either hardware or software smart routers.
    - These routers would leverage ALL userstore services to provide **active/active** usestore architecture.
    - Theses routers would NOT impact the userstore update process. No race condition concerns.
    - Examples:
      - Hardware: F5/BIGIP smart hardware router to load balance queries and if user store is large & spilt to multiple DSA by OU, a redirect of updates to the correct DSA.
      - Software: CA Directory Router, load-balance queries and send updates to the correct DSA if DSA are split by OU.
    - Scalability built-in; add additional nodes as needed
    - With monitor process; possible to leverage five nine (99.999%) architecture for user store will this model, across WAN connections.
- Replication between directory nodes must be millisecond response times for the entire user’s profile
  - Typically, this is an issue for Active Directory with a default replication time of 15 minutes between local nodes for the full user profile.

Scalability / High-Availability Requirements

- Scalability Requirements
  - User store scalability typically refers to horizontal-scalability
    - A requirement to expand the number of userstore nodes (servers) so that IM performance is not impacted with regards to queries, as solution grows.
  - This is typically not a concern for many LDAP solutions.
    - Replication of user's profile must be on millisecond response time between horizontal nodes.
    - This is typically an issue for Active Directory replications default periods for the entire user profile.
      - Default replication time between AD domains near geographical is typically 15 minutes
      - Default replication time between AD domains far geographical is typically 15min-720min
  - The other type of scalability is vertical-scalability, which has an impact on server costs with regards to CPU/RAM.
    - If the corporate user store has grown to include binary data, e.g. biometrics, photos, audio voiceprints, or the number of users has expanded the solution to greater than 8GB (validated by LDIF extract), then server cost for RAM will need to expand to manage current use of RAM for OS & any temporary use of RAM for re-indexing.
    - Determine if the LDAP solution has the ability to provide by itself or in conjunctions with a load balancer, the ability to spilt the LDAP userstore into two or more parts, so that any sub-section of the LDAP tree is less than hardware requirements of the servers; place the other sub-sections on additional servers.
      - A router will be update to redirect queries/updates to the correct sub-section of the LDAP tree.
- High Availability Requirements
    - LDAP solution should be able to support two (2) or more nodes to meet the minimal HA requirements.
    - LDAP solution should be able to support three (3) or more nodes (servers) to achieve 99.9% uptime.



STACK 01

IME

Corporate Store Configuration

Primary IMCD: imcd01:636
Failover IMCD: imcd02:636
Imcd03:636,imcd04:636

IMWA01
10.0.0.1

IMCD_Router01 DSA
Imcd01:22389

100 % Read Traffic
100% Update Traffic

IMCD01
10.2.0.1
Active Directory DC01

STACK 02

IME

Corporate Store Configuration

Primary IMCD: imcd01:636
Failover IMCD: imcd02:636
Imcd03:636,imcd04:636

IMWA02
10.0.0.2

IMCD_Router02 DSA
Imcd02:22389

Replication/ Failover

IMCD02
10.2.0.2
Active Directory DC02

STACK 03

IME

Corporate Store Configuration

Primary IMCD: imcd01:636
Failover IMCD: imcd02:636
Imcd03:636,imcd04:636

IMWA03
10.0.0.3

IMCD_Router03 DSA
Imcd03:22389

Replication/ Failover

IMCD03
10.2.0.3
Active Directory DC03

STACK 04

IME

Corporate Store Configuration

Primary IMCD: imcd01:636
Failover IMCD: imcd02:636
Imcd03:636,imcd04:636

IMWA04
10.0.0.4

IMCD_Router04 DSA
Imcd04:22389

Replication/ Failover

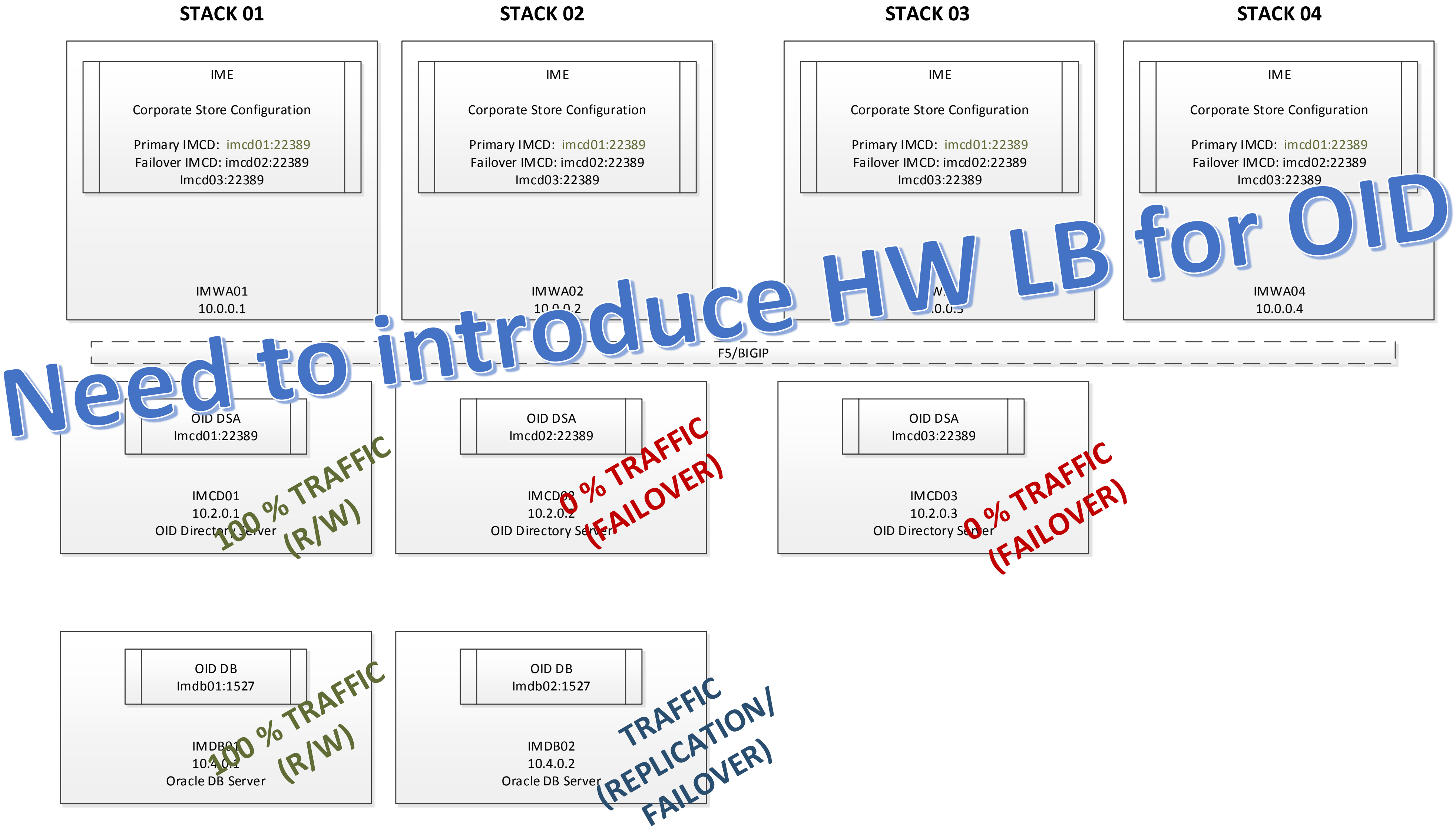
IMCD04
10.2.0.4
Active Directory DC04

Need to introduce HW LB for AD

Need to adjust AD replication period for user profile

IMWA:IMCD (IM Corporate User Store)
AD – No LB - Different Nodes

If IM/SM integration exists; no changes need to be made to SiteMinder Policy Servers.



STACK 01

IME
Corporate Store Configuration
Primary IMCD: imcd01:22389
Failover IMCD: imcd02:22389
Imcd03:22389

IMWA01
10.0.0.1

STACK 02

IME
Corporate Store Configuration
Primary IMCD: imcd01:22389
Failover IMCD: imcd02:22389
Imcd03:22389

IMWA02
10.0.0.2

STACK 03

IME
Corporate Store Configuration
Primary IMCD: imcd01:22389
Failover IMCD: imcd02:22389
Imcd03:22389

IMWA03
10.0.0.3

STACK 04

IME
Corporate Store Configuration
Primary IMCD: imcd01:22389
Failover IMCD: imcd02:22389
Imcd03:22389

IMWA04
10.0.0.4

F5/BIGIP

OID DSA
Imcd01:22389

IMCD01
10.2.0.1
OID Directory Server

OID DSA
Imcd02:22389

IMCD02
10.2.0.2
OID Directory Server

OID DSA
Imcd03:22389

IMCD03
10.2.0.3
OID Directory Server

OID DB
Imdb01:1527

IMDB01
10.4.0.1
Oracle DB Server

OID DB
Imdb02:1527

IMDB02
10.4.0.2
Oracle DB Server

Need to introduce HW LB for OID

100 % TRAFFIC (R/W)

0 % TRAFFIC (FAILOVER)

0 % TRAFFIC (FAILOVER)

100 % TRAFFIC (R/W)

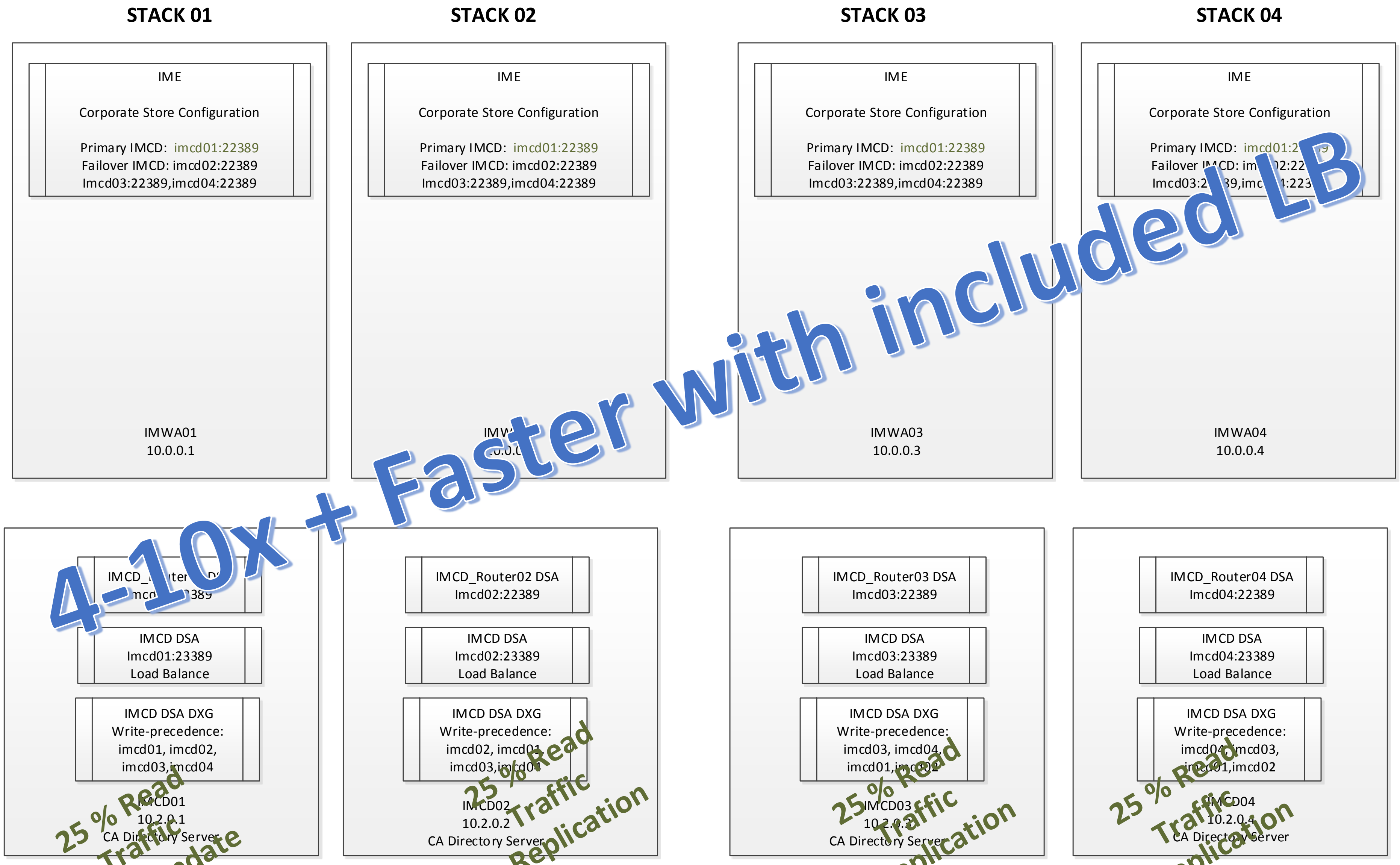
TRAFFIC (REPLICATION/ FAILOVER)

IMWA:IMCD OID Model

No Load Balancing

Hardware (F5/BIGIP) Load Balancer(s) may be added between IMWA / SMPS servers and the OID Directory servers.

Inventory: 5 Server(s) + 1-2 F5/BIGIP LB for ProdEnv (similar for dev/test env.)



STACK 01

IME
Corporate Store Configuration
Primary IMCD: imcd01:22389
Failover IMCD: imcd02:22389
Imcd03:22389,imcd04:22389

IMWA01
10.0.0.1

IMCD_Router DSA
Imcd01:22389

IMCD DSA
Imcd01:23389
Load Balance

IMCD DSA DXG
Write-precedence:
imcd01, imcd02,
imcd03,imcd04

IMCD01
10.2.0.1
CA Directory Server

STACK 02

IME
Corporate Store Configuration
Primary IMCD: imcd01:22389
Failover IMCD: imcd02:22389
Imcd03:22389,imcd04:22389

IMWA02
10.0.0.2

IMCD_Router02 DSA
Imcd02:22389

IMCD DSA
Imcd02:23389
Load Balance

IMCD DSA DXG
Write-precedence:
imcd02, imcd01
imcd03,imcd04

IMCD02
10.2.0.2
CA Directory Server

STACK 03

IME
Corporate Store Configuration
Primary IMCD: imcd01:22389
Failover IMCD: imcd02:22389
Imcd03:22389,imcd04:22389

IMWA03
10.0.0.3

IMCD_Router03 DSA
Imcd03:22389

IMCD DSA
Imcd03:23389
Load Balance

IMCD DSA DXG
Write-precedence:
imcd03, imcd04,
imcd01,imcd02

IMCD03
10.2.0.3
CA Directory Server

STACK 04

IME
Corporate Store Configuration
Primary IMCD: imcd01:22389
Failover IMCD: imcd02:22389
Imcd03:22389,imcd04:22389

IMWA04
10.0.0.4

IMCD_Router04 DSA
Imcd04:22389

IMCD DSA
Imcd04:23389
Load Balance

IMCD DSA DXG
Write-precedence:
imcd04, imcd03,
imcd01,imcd02

IMCD04
10.2.0.4
CA Directory Server

4-10x + Faster with included LB

25 % Read Traffic
100% Update Traffic

25 % Read Traffic + Replication

25 % Read Traffic + Replication

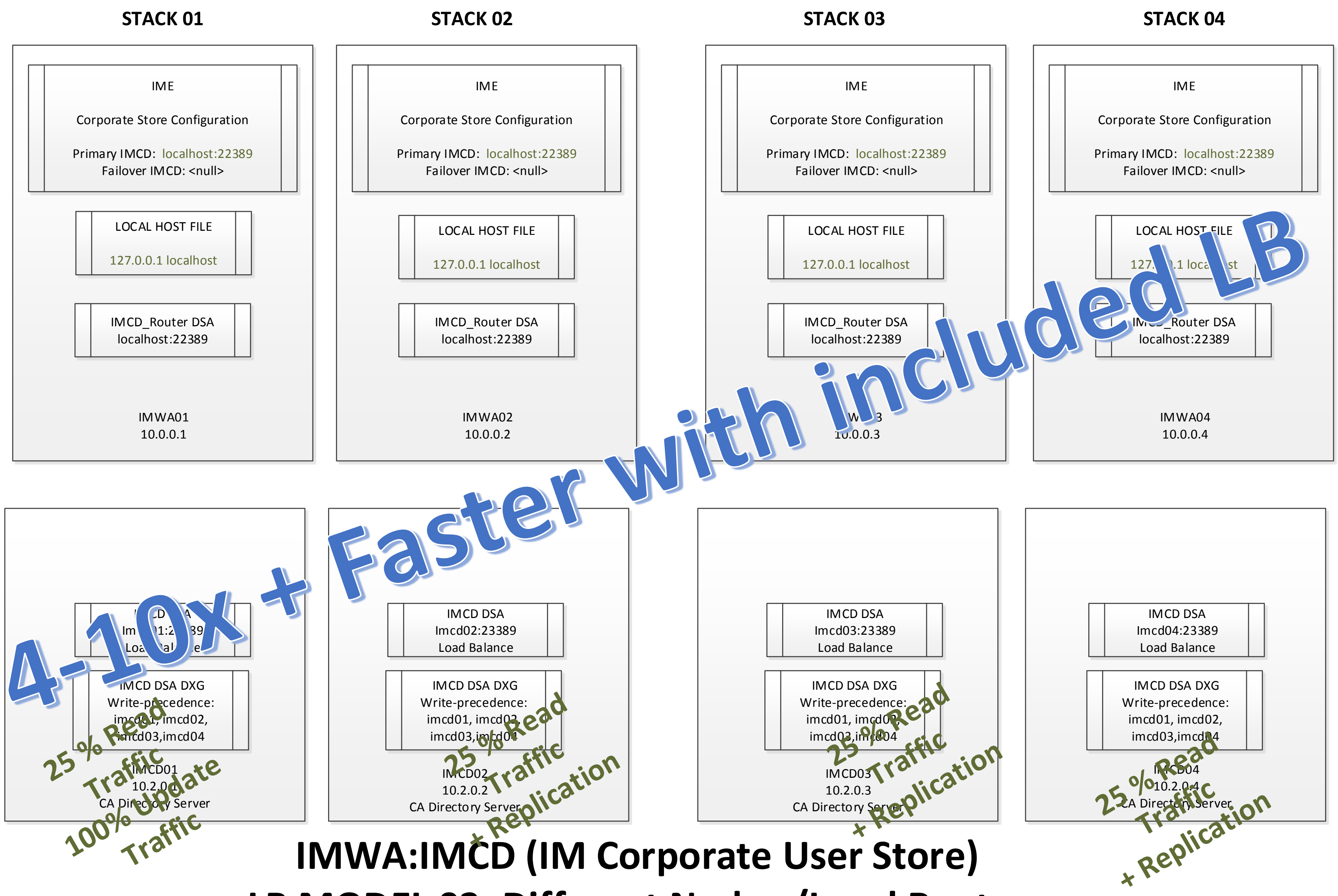
25 % Read Traffic + Replication

IMWA:IMCD (IM Corporate User Store)

LB MODEL 01: Different Nodes /Remote Router

Using CA Directory load balancing router to allow solution to scale

If IM/SM integration exists; no changes need to be made to SiteMinder Policy Servers.



STACK 01

IME
Corporate Store Configuration
Primary IMCD: localhost:22389
Failover IMCD: <null>

LOCAL HOST FILE
127.0.0.1 localhost

IMCD_Router DSA
localhost:22389

IMWA01
10.0.0.1

IMCD DSA
Imcd01:23389
Load Balance

IMCD DSA DXG
Write-precedence:
imcd01, imcd02,
imcd03,imcd04

IMCD01
10.2.0.1
CA Directory Server

STACK 02

IME
Corporate Store Configuration
Primary IMCD: localhost:22389
Failover IMCD: <null>

LOCAL HOST FILE
127.0.0.1 localhost

IMCD_Router DSA
localhost:22389

IMWA02
10.0.0.2

IMCD DSA
Imcd02:23389
Load Balance

IMCD DSA DXG
Write-precedence:
imcd01, imcd02,
imcd03,imcd04

IMCD02
10.2.0.2
CA Directory Server

STACK 03

IME
Corporate Store Configuration
Primary IMCD: localhost:22389
Failover IMCD: <null>

LOCAL HOST FILE
127.0.0.1 localhost

IMCD_Router DSA
localhost:22389

IMWA03
10.0.0.3

IMCD DSA
Imcd03:23389
Load Balance

IMCD DSA DXG
Write-precedence:
imcd01, imcd02,
imcd03,imcd04

IMCD03
10.2.0.3
CA Directory Server

STACK 04

IME
Corporate Store Configuration
Primary IMCD: localhost:22389
Failover IMCD: <null>

LOCAL HOST FILE
127.0.0.1 localhost

IMCD_Router DSA
localhost:22389

IMWA04
10.0.0.4

IMCD DSA
Imcd04:23389
Load Balance

IMCD DSA DXG
Write-precedence:
imcd01, imcd02,
imcd03,imcd04

IMCD04
10.2.0.4
CA Directory Server

4-10x + Faster with included LB

25 % Read
Traffic
100% Update
Traffic

25 % Read
Traffic
+ Replication

25 % Read
Traffic
+ Replication

25 % Read
Traffic
+ Replication

IMWA:IMCD (IM Corporate User Store)

LB MODEL 02: Different Nodes /Local Router

Using CA Directory load balancing router to allow solution to scale

If IM/SM integration exists, then the localhost CA Directory router will need to exist on all SMPS servers.

CA Directory ACLS

- Lock down access to your data

CA Directory ACLs Example #1

```
# Define static/dynamic access controls
set access-controls = True;
set min-auth = clear-password;
set dynamic-access-control = false;
```

```
# Define Service admin accounts that will be able to update userstore via LDAP
# This may be the same accounts using for the IM/SM solutions
set group = {
   name    =   admins
   users   =   <dc com><dc im><ou internal><ou admins><uid idmadmin>,
               <dc com><dc im><ou internal><ou admins><uid idmpublic>,
               <dc com><dc im><ou internal><ou admins><uid idminbound>,
               <dc com><dc im><ou internal><ou admins><uid smadmin>,
               <dc com><dc im><ou internal><ou admins><uid smsuperuser>
};
```

```
# Grant service admin accounts access to tree
set admin-user admins= {
   group   = admins
   subtree = <dc com><dc im>
};
#Rule to allow all users full rights to own entry
set super-user self = {
   own-entry
};
```

Ref: https://supportcontent.ca.com/cadocs/0/CA%20Directory%20r12%200%20SP11-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?example_config_role-based_access_control_in_router_dsa.html

CA Directory ACLs Example #2

```
# Define static/dynamic access controls
set access-controls = True;
set min-auth = clear-password;
set dynamic-access-control = false;
```

```
#Enables the ability to use group assignment
set role-subtree =  <dc "com"><dc “im"><ou "groups">;
set use-roles = true;
```

```
#Superuser access
set super-user = { user = <dc com><dc im><ou internal><ou admins><uid idmadmin> };
```

```
#This sets the super admin access to the Security Admin group
set admin-user  = {
role = <dc "com"><dc “im"><ou "groups"><ou "security"><cn “admins">
subtree = <dc "com"><dc “im">
};
```

```
#This sets read access within the people branch to the Auditors group
set reg-user “auditors" = {
role = <dc "com"><dc “im"><ou "groups"><ou "security"><cn “auditors">
subtree = <dc "com"><dc “im"><ou "people">
};
#This sets read access to the entire DIT to the Auditors group
set reg-user “dit-auditors" = {
role=<dc "com"><dc "im"><ou "groups"><ou "security"><cn “dit-auditors">
subtree = <dc "com"><dc “im">
```

```
#The ACL settings allows the user to read self attributes and modify password
set reg-user "Self 1"= {
user-subtree = <dc com><dc im><ou people>
entry = <dc com><dc im><ou people>
attrs = ou
};
set reg-user "Self 2"= {
own-entry
subtree = <dc com><dc im>
};
set reg-user "Self 3"= {
   own-entry
   subtree = <dc com><dc im><ou people>
           attrs = userPassword
           perms = modify
};
```

Ref: https://supportcontent.ca.com/cadocs/0/CA%20Directory%20r12%200%20SP11-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?example_config_role-based_access_control_in_router_dsa.html

CA Directory ACLs Example #3

```
# Define static/dynamic access controls

set access-controls = True;

set min-auth = clear-password;

set dynamic-access-control = false;
```

```
#SiteMinder and Federation admin ACL for userstore plus DIT-ReadOnly

#Able to modify idmDisabledState, userpassword, idmPasswordData

set admin-user "SiteMinder - Federation" = {

role=<dc "com"><dc "im"><ou "groups"><ou "security"><cn “smfedmodify">

subtree = <dc "com"><dc "im">

attrs = idmDisabledState, userPassword, idmPasswordData

perms = modify

};

#Ability to add group membership for all objects under the application ou

set admin-user “groupmodify01"= {

  role = <dc "com"><dc "im"><ou "groups"><ou "security"><cn “addgroupsmembers01">

                subtree = <dc "com"><dc "im"><ou "groups"><ou "applications">

                attrs = member

  perms = modify

};

#Ability to modify the all App Groups attribute on the user object

set admin-user “groupmodify02"= {

  role = <dc "com"><dc "im"><ou "groups"><ou "security"><cn “addgroupmembers02">

    subtree = <dc "com"><dc "im"><ou "people">

    attrs = imAppGroups

  perms = modify

};
```