How to perform a NIS to LDAP Migration – with CA Directory

CA Services
2012

Agenda

- Standard Project overview
- Opportunities
- Logistics
- Resource Expectations
- Define Current State Operations
- Future State Operations
- Functional Requirements
- Solution Requirements
- Project Risks
- Design
- Overall Solution Review
- PAM Client Migration Processes
- Take-away / Lessons Learned

Standard Project Overview

- Migrate XYZ NIS environment to LDAP technology
  - NIS has been long discontinued by SUN (Oracle)
  - NIS technical capacity reached
    - netgroup map primary problem area
    - netgroup dbm files are filling up
    - character limit
  - Management of external non-NIS data
    - sudoers data
  - Roll out of migration may be as quick or as slow as the customer requires
    - Deploy client configurations in batches or single instances.
    - Retire NIS environment after full migration has occurred.

- Manage Password Reset Use-Case between legacy NIS clients and CA Directory during migration period
  - Two (2) options:
    - Integration with CA Identity Minder via Connector Xpress
    - Use PADL NIS/LDAP Gateway solution
      - http://www.padl.com/Products/NISLDAPGateway.html
        - Additional purchase option from PADL

Opportunities

- CA has validated that CA Directory has the ability to manage NIS environment data and would exceed reliability & performance expectations.
- CA can provide guidance that XYZ would be able to expand management over new NIS LDAP (CA Directory) with an existing CA Identity Minder solution for password reset and CRUD use-cases to meet.
- Client able to leverage internal resource SME knowledge of CA Directory & LDAP structures; due to any existing CA Identity Minder solution.
- Integration with CA Identity Minder would address password reset use-case & requirement to both legacy NIS clients (10000+) and new CA Directory during migration period.

Logistics

- Use of in place HW
  - No additional HW cost for CA Directory; use existing HW resource
  - RAM usage dependency is on size of NIS data
    - Assume 512 MB to 1 GB as high ball park limits
      - This would be free memory reserved for the CA Directory DSA.
      - Expect initial usage to be 128 MB or less
  - Disk space usage: 5 x RAM size to allow for offline copy of data to be retained & logs to grow.
- Staffing / allotted time
  - Use current CA Directory SME resources
- Remote engagement

Resource Expectations

- Challenge:
  - SME resources with experience in multiple NIS>LDAP conversions are not readily available, as this process is not an everyday occurrence.
  - Use a mix of resources/skill-sets to address this challenge.

- Expect to assign the following resources:
  - Assistance with initial migration process:
    - CA Directory Architect - document directory migration/DIT structure
    - PADL Support resource – to assist with migration scripts
    - Client Directory resource – deploy and test migration process
  - UNIX/Linux authentication/authorization client configurations
    - Client Directory resource – define and test AN/AZ processes
    - Client UNIX/Linux resource – configure and deploy client PAM modules
  - CA IM ConnectorXpress connector to manage new LDAP user store
    - Client or CA IM resource – configure and deploy new IM connector

Define Current State Operations

- New NIS accounts via Identity Minder
  - cannot provision netgroup or group information because no roles defined within IdM (RCM)
  - <10% provisioning due to roles deficiency
- Manual NIS account provisioning
  - new account information via workflow
  - Account created via custom script
    - yp make
    - yppush to slaves in real time
- Password change
  - Managed through Identity Minder Password Services
    - One way push
    - User can still change password at unix level (passwd)
    - Local custom script runs to notifiy user of password expiration
      - Reads passwd file (shadow file)

Future State Operations

- ‘YP’ commands need to be replaced by equivalent LDAP commands
  - ypcat, ypmatch, ypwhich, ??
- Current custom script to notify users of password expiration must be modified to read directory entries for password expiration information
- Custom script for telephone number lookups must be modified to access directory
  - 411 tool
- Customizing of synchronization between NIS databases and directory during migration phase
  - Not required if CA Identity Minder can provision to NIS replacement directory when ready for production
  - Not required if PADL NIS2LDAP gateway used during migration.

Functional Requirements Summary

- NIS mappings to LDAP
  - Standard mappings
  - Non-standard
    - auto.aix
    - auto.compile
    - auto.linux
    - auto.linux8
    - auto.direct
    - auto.home
    - auto.master
    - ipphones
    - printers
    - termserv
    - ipnodes
    - netmasks
    - timezones
  - Automount maps

Functional Requirements cont’d

- Password management (aging, complexity, changes)
  - Current custom script needs to be modified to get password last change from directory
- Phased client migration
- Hardware reuse
- Netapp (OS=ontap) – queries user/group information for user authorization; query netgroup for host authorization
- DR Strategy (site failover)
- HA strategy (client failover)
- Environment resiliency
- SSL between client and directory and within directory layer
- Output of yp commands needs to be same or similar
- Unix user authentcation/authorization via LDAP
- SUDO authorization via LDAP
- NFS Appliance mounts (Keep both legacy and CA Directory account in sync with CA IM ETC/NIS UNIX agent)

Solution Requirements

Identifier	Solution Requirement	Business/IT Initiative Cross-reference
SR-01: Consolidate NIS/SUDOER Information	The directory shall provide for the necessary data so that the current NIS/SUDOER services/functionalities that are based off of unix file structures (i.e. netgroups) and/or databases work from directory centric services/information. .	BD-01: Technology Improvement
SR-02: All NIS clients using native OS LDAP	Configuration of the NIS client machines such that all users will be authenticated and authorized via the directory using the native OS LDAP client configurations.	BD-01: Technology Improvement
SR-03: SUDOER using LDAP	Configuration of the NIS client machines such that all SUDOERs will be authorized through the directory.	BD-01: Technology Improvement
SR-04: Provide Core Directory Services	Provide yellow and white page searches and rapid retrieval of information capable of supporting the NIS and SUDOER user populations.	BD-01: Technology Improvement
SR-05: Stronger Authentication	The solution needs to provide password aging and complexity to support the unix level change password functionality. The password complexity rules should be based on the current unix password complexity rules.	BD-01: Technology Improvement
SR-06: Restrict Directory Access	Provide fine grained controls on who is allowed to perform an operation on information in the directory.	BD-01: Technology Improvement
SR-07: Enhanced performance and service availability to provide increase in customer satisfaction	Provide a high performance solution with equally optimized read and write operations, able to support tens of thousands of simultaneous authorization events with high availability.	BD-01: Technology Improvement
SR-08: Central administration and monitoring	Provide a flexible, graphical, web-based administrative interface that supports central system configuration with global polices, system status, and event and process monitoring where the administrator can manage all directory instances from a single console view.	BD-01: Technology Improvement

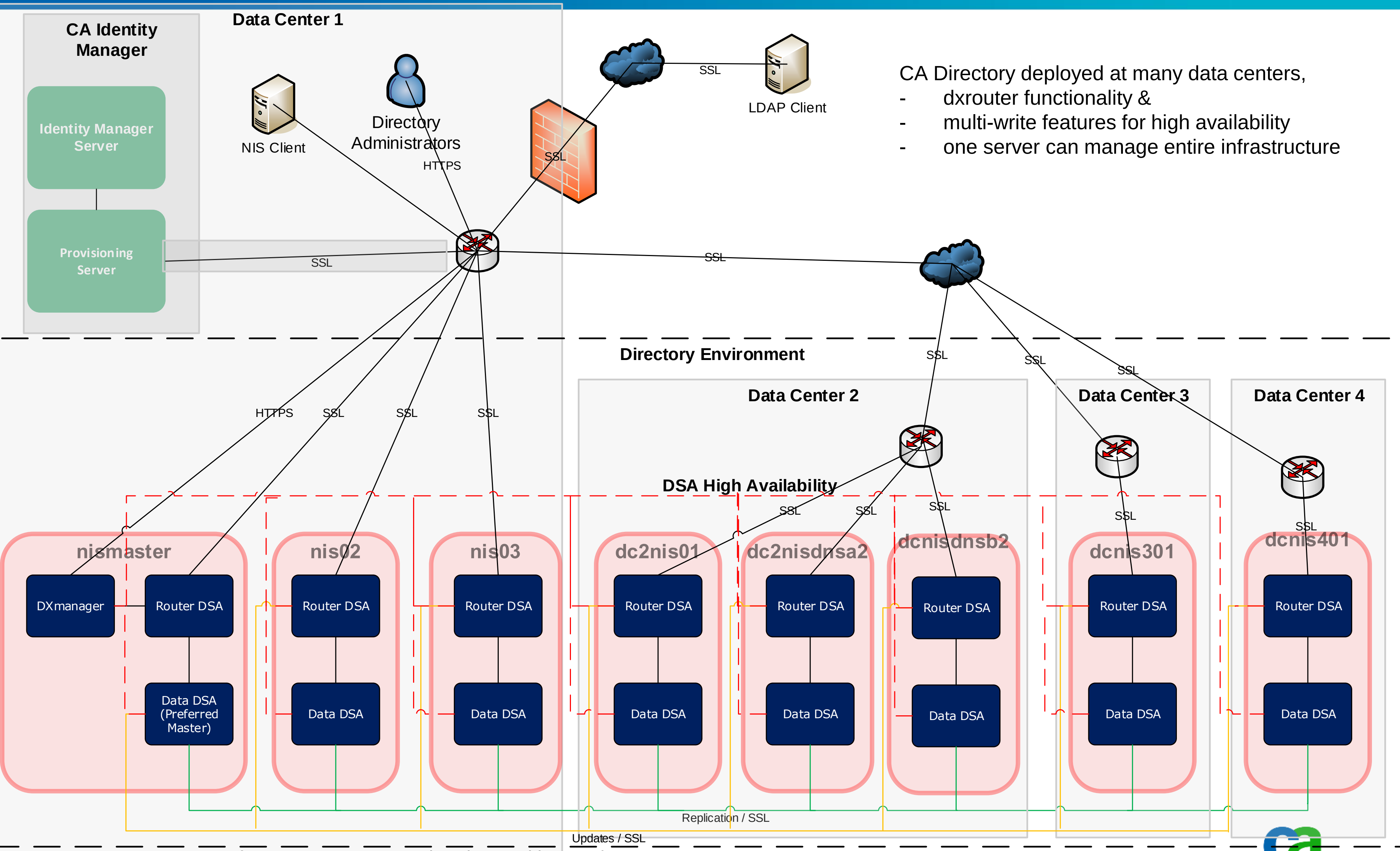
Project Risks

- Resources:
  - NIS > LDAP conversion process skill set is limited.
  - Client resources will manage NIS client tasks to move from NIS to LDAP for AN/AZ
  - CA / PADL resource will manage migration of data and design architecture
  - Acquire PADL / SYMAS support contract to assist with initial migration using their scripts.
- Technical:
  - Use of native PAM and NSS LDAP modules
    - Challenge:
      - Each platform type (OS version) implement PAM/NSS differently
      - Not all platforms types are of the same level for PAM and NSS modules (schema rfc2307 vs. schema rfc2307bis)
      - SSL configuration steps complexity
  - Synchronization process of LDAP and NIS userstores
    - Use either CA Identity Minder and/or PADL NIS2LDAP Gateway for both user data & password migration.
  - Non standard NIS mappings
    - See Functional Requirements for list
  - Password management (aging, complexity, changing)
    - last update time to directory if changed at unix level)
  - Data cleanliness
    - Data massaging for input to the migration scripts
    - GECOS fields are typically “messy”
  - Migration scripts
    - New development for non-standard mappings
    - Support and use of open source scripts
- Architecture:
  - Capture current metrics for NIS client accesses and traffic to current NIS servers (intended directory servers)
  - Outdated/Experimental RFC (draft-howard-rfc2307bis-02.txt) expired in 2/10/2010; even though it is used by many vendors.

Design

- Rfc2703bis guidelines
  - One subtree / NIS domain
- Incorporate SUDO users
- Incorporate auto_home, auto_direct and auto_master
- Incorporate netgroups
- CA partner(s)
  - PADL www.padl.com
  - SYMAS http://symas.com/

Overall Solution – Topology – 99.999%

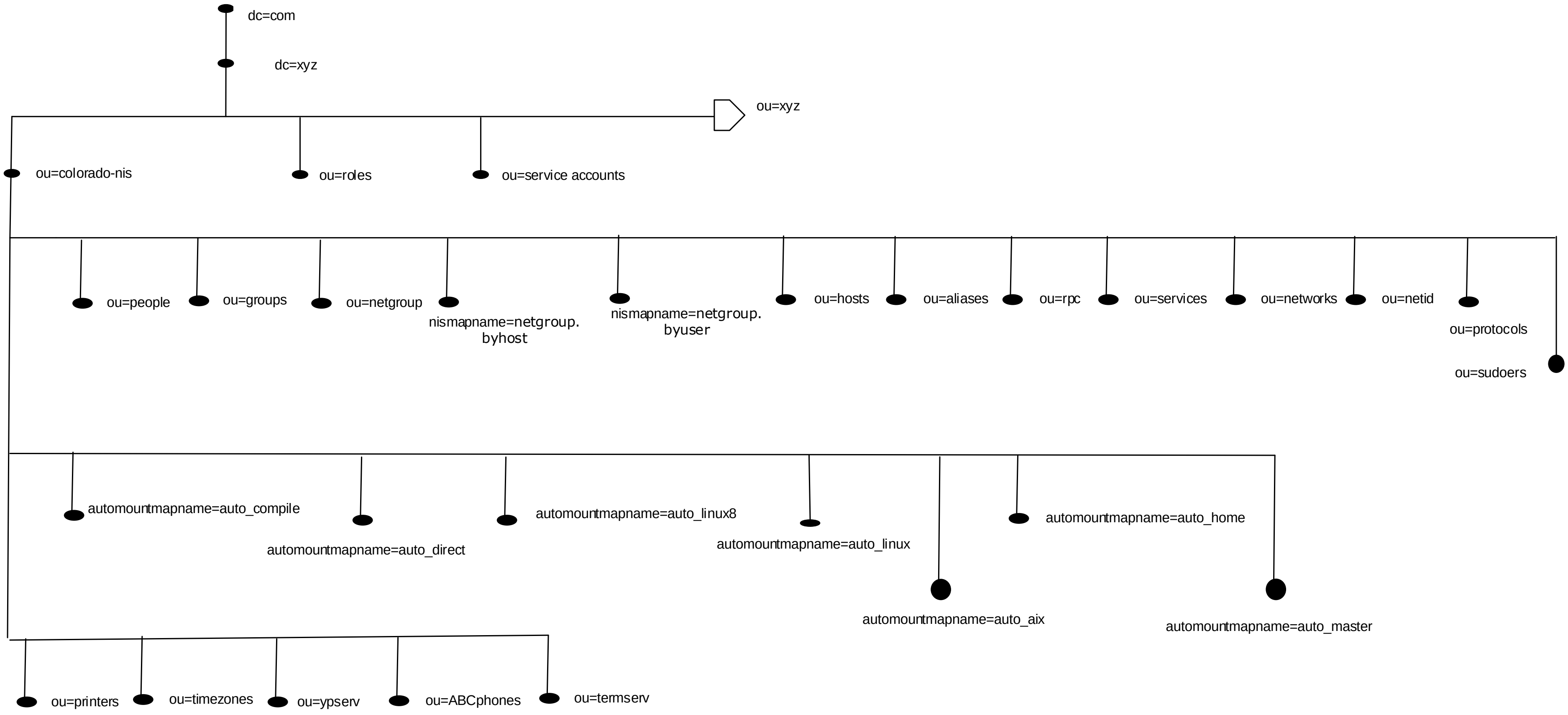


CA Directory deployed at many data centers,

- dxrouter functionality &
- multi-write features for high availability
- one server can manage entire infrastructure

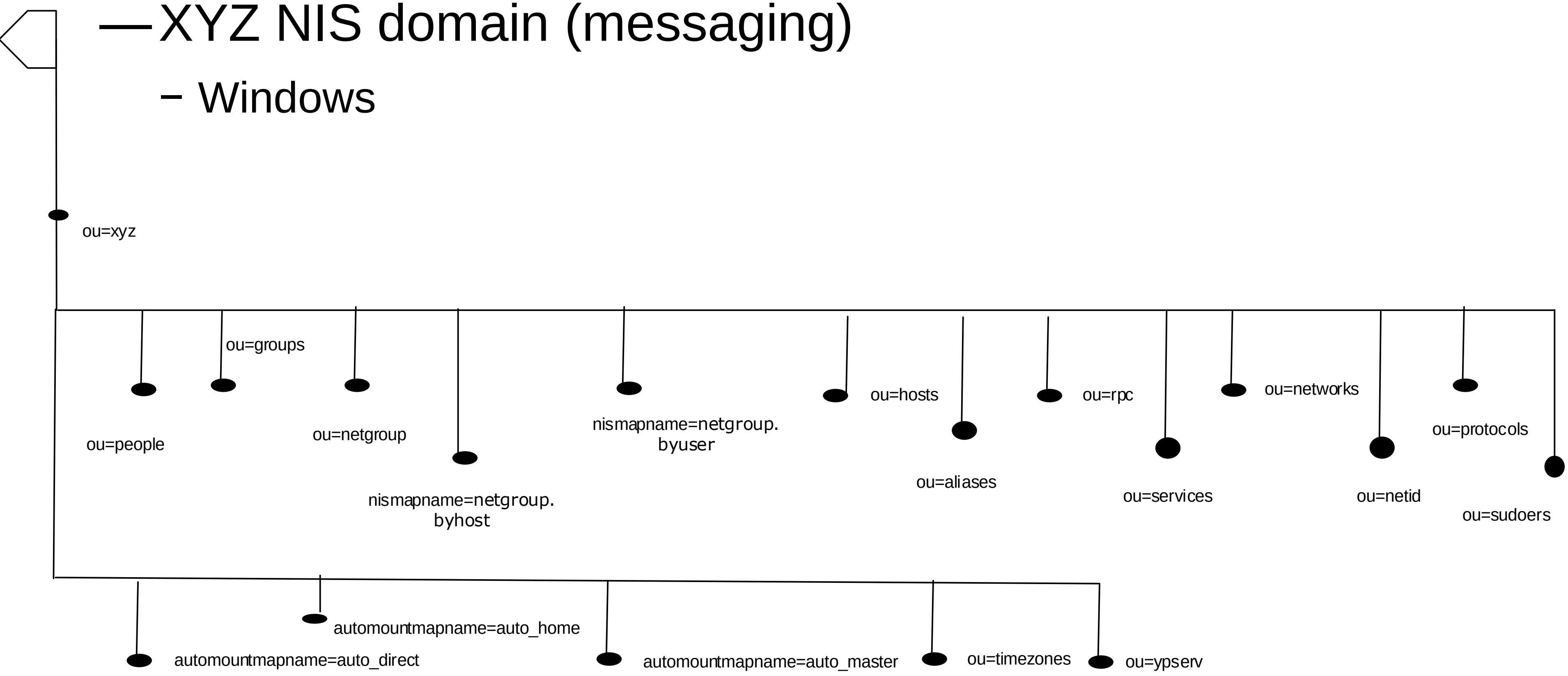
Overall Solution - XYZ NIS DIT

—XYZ NIS domain

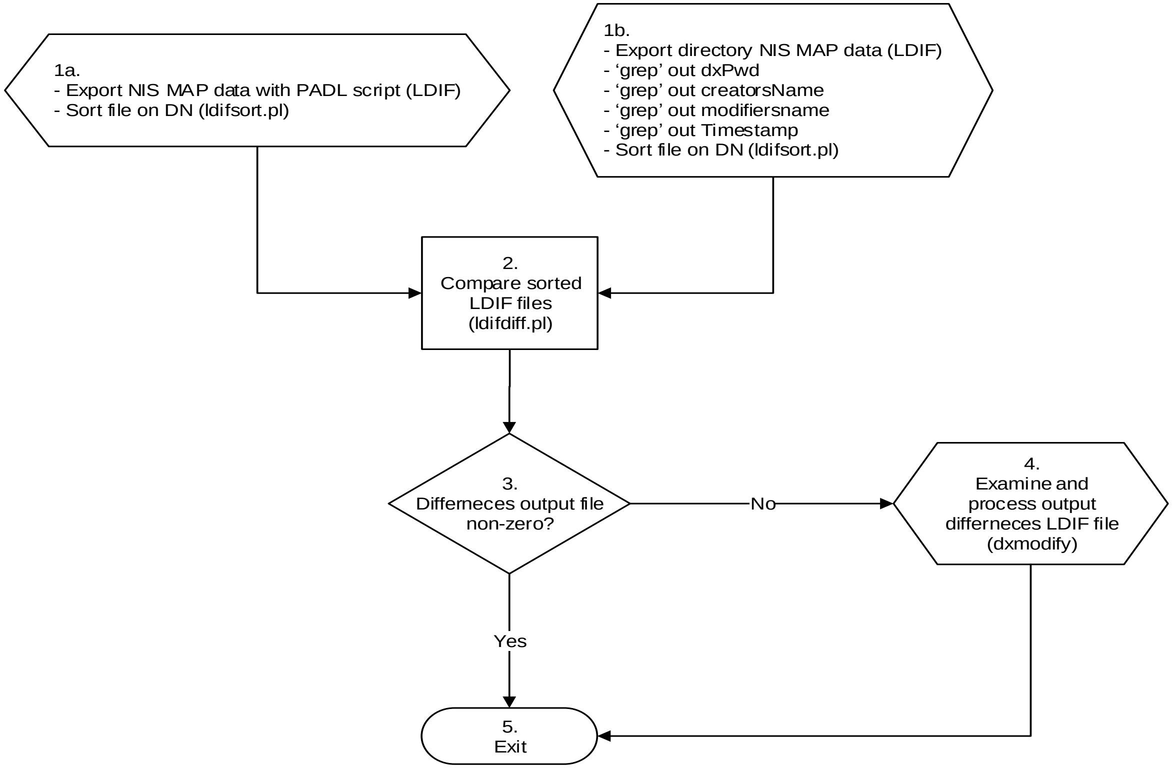


Overall Solution - XYZ NIS DIT Cont'd

- XYZ NIS domain (messaging)
  - Windows


ou=xyz
ou=groups
ou=people
ou=netgroup
nismapname=netgroup.byhost
nismapname=netgroup.byuser
ou=hosts
ou=aliases
ou=rpc
ou=services
ou=networks
ou=netid
ou=protocols
ou=sudoers
automountmapname=auto_home
automountmapname=auto_direct
automountmapname=auto_master
ou=timezones
ou=ypserv

NIS / LDAP sync Process



1a.
- Export NIS MAP data with PADL script (LDIF)
- Sort file on DN (ldifsort.pl)

1b.
- Export directory NIS MAP data (LDIF)
- ‘grep’ out dxPwd
- ‘grep’ out creatorsName
- ‘grep’ out modifiersname
- ‘grep’ out Timestamp
- Sort file on DN (ldifsort.pl)

2.
Compare sorted LDIF files (ldifdiff.pl)

3.
Differneces output file non-zero?

4.
Examine and process output differneces LDIF file (dxmodify)

5.
Exit

Tools used

- CA Directory tools
  - Dxtools reference guide
- Standard UNIX binaries
  - grep, diff
- PERL based tools
  - PADL migration scripts – These scripts will produce an LDIF representation of the current NIS database for the respective mapping.
  - CPAN PERL
    - sudoers2ldif.pl – This perl script will produce an LDIF representation of the current SUDOERs database.
    - ldifsort.pl – This perl script is supplied by CPAN PERL website and sorts the LDIF files according to the key fields as entered.
    - ldifdiff.pl – This perl script is supplied by CPAN PERL website and will compare the sorted LDIFs between the NIS MAP data and directory NIS MAP data and produce an output LDIF file of differences which can then be applied to the directory.

PAM Client Migration Processes

- Migrate internal community first, then external
- PAM client configurations
- Use scripts provided by PADL and Internet communities for data conversions
  - Some scripts will need modifications due to customer environment
  - Some scripts will need modifications due to directory standards (i.e. one structural OC)

Take Away

- Use PADL/SYMAS as springboards as required
  - Acquire support contract for 80-160 hours from PADL/SYMAS to support initial migration efforts from remote resources.
- Provide questionnaire specifically around NIS migration to help with SOW (i.e. number of NIS domains, number/types of PAM clients, PAM client migration ownership, etc.)
- Integration with CA IM and/or PADL NIS/LDAP GATEWAY to manage password reset use-case during migration to NIS clients
- Integrate with CA IM and CA IM ETC/NIS agent to manage NFS home folder shares requirements.
- Manage new LDAP user store with CA IM Connector Xpress to manage one to many structural class objects and the use of Operational Bindings (Javascript) to manage the CRUD Use-Cases.

LDAP Client Configuration Examples

This document details the various configuration files and settings for the different operating systems.

1) Confirm the ownership (root:sys) and permissions (see specifics below) on configuration files installed by BladeLogic

AIX Configurations

- **LDAP - Client Configuration**
- This document details the various configuration files and settings for the different operating systems.
- 1) Confirm the ownership (root:sys) and permissions (see specifics below) on configuration files installed by BladeLogic
- **AIX**
- BladeLogic pkg: AIX_LDAP_Client_CCB-PROD_files
- BladeLogic job: deploy_AIX_LDAP_Client_CCB-PROD_files Files installed by BladeLogic job Specifies
- clientsvc? Specifies
- CCB-PROD? Specifies LDAP servers? Specifies
- SUDO? SSL Perms
- /etc/security/ldap/2307aixuser.map 640
- /etc/irs.conf 600
- /etc/security/ldap/ldap.cfg Y Y Y Y 600
- /etc/security/ldap/ldapkeys.crl
- /etc/security/ldap/ldapkeys.kdb
- /etc/security/ldap/ldapkeys.rdb Y
- Y
- Y 640
- 640
- 640
- /etc/ldap.conf Y Y Y 644
- /etc/methods.cfg 644
- /etc/netsvc.conf 644
- /etc/pam.conf 600
- /etc/security/login.cfg 640
- /etc/security/ldap/mksecldap.ksh