
Deploying a Global Identity Infrastructure
Anton Shmagin, UNDP

UNDP Overview

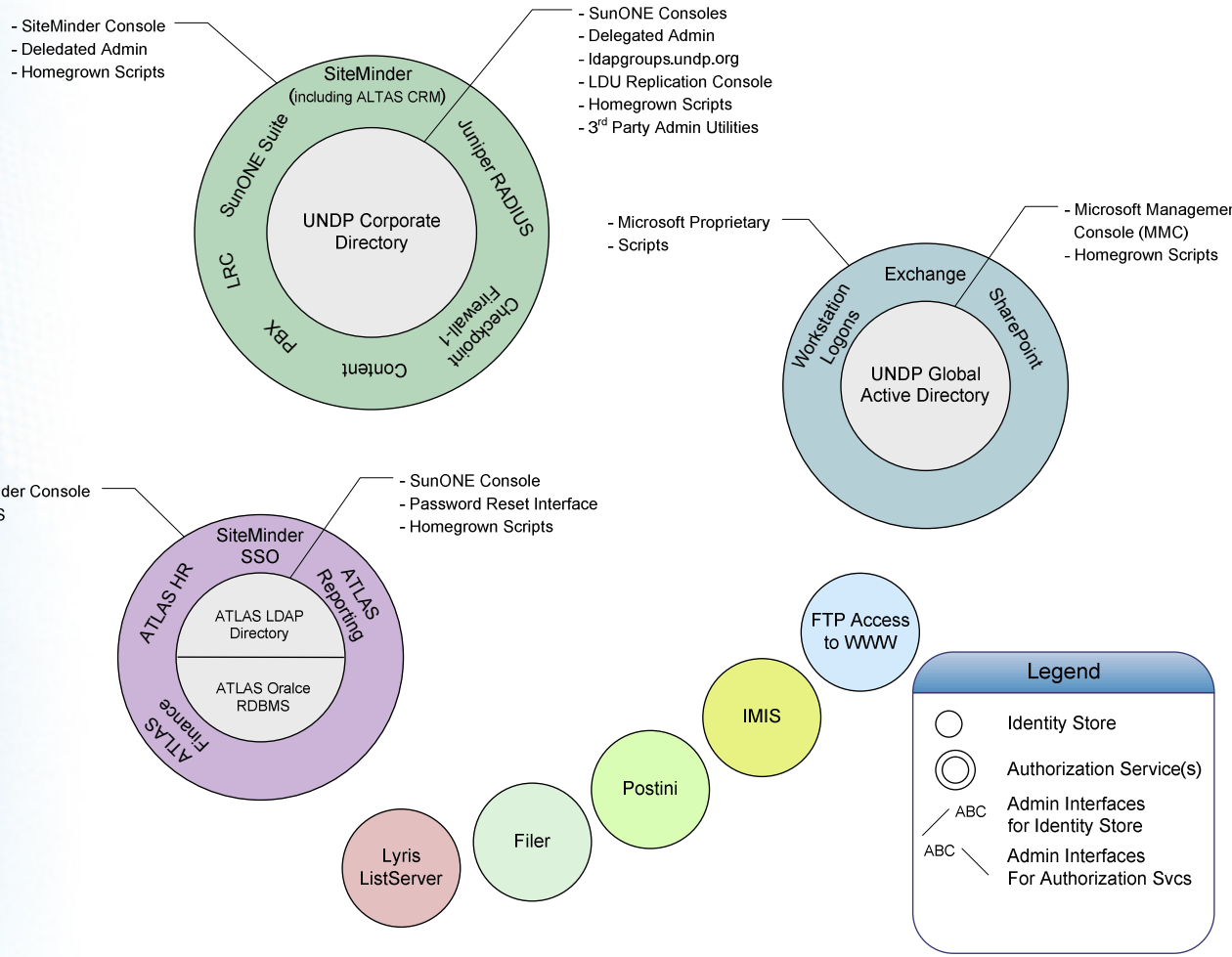
UNDP is the UN's global development network, advocating for change and connecting countries to knowledge, experience and resources to help people build a better life.

- Presence in 148 countries
- Global ERP implementation
- 90% of all business processes web-enabled
- Broadband network in each office
- Global LDAP replication
- Almost all infrastructure components are LDAP centric

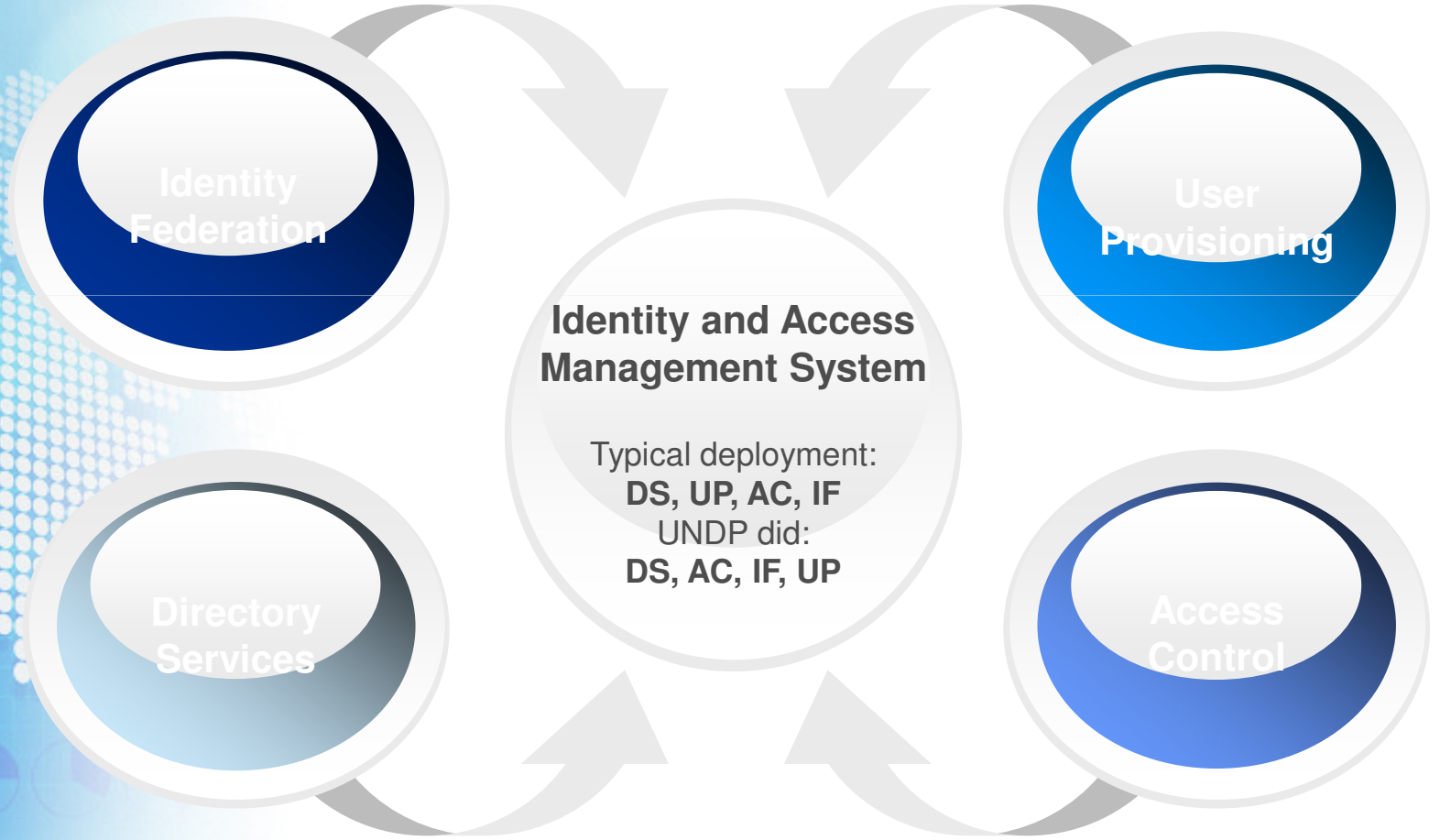
UNDP Overview

- 12 functional systems use LDAP (more than 60 servers)
- Mail (Sendmail + Sun Messaging Servers)
- Calendar
- RADIUS
- PBX Billing
- Firewall VPN
- SiteMinder SSO
- iPass
- SITA
- File/Print services
- etc

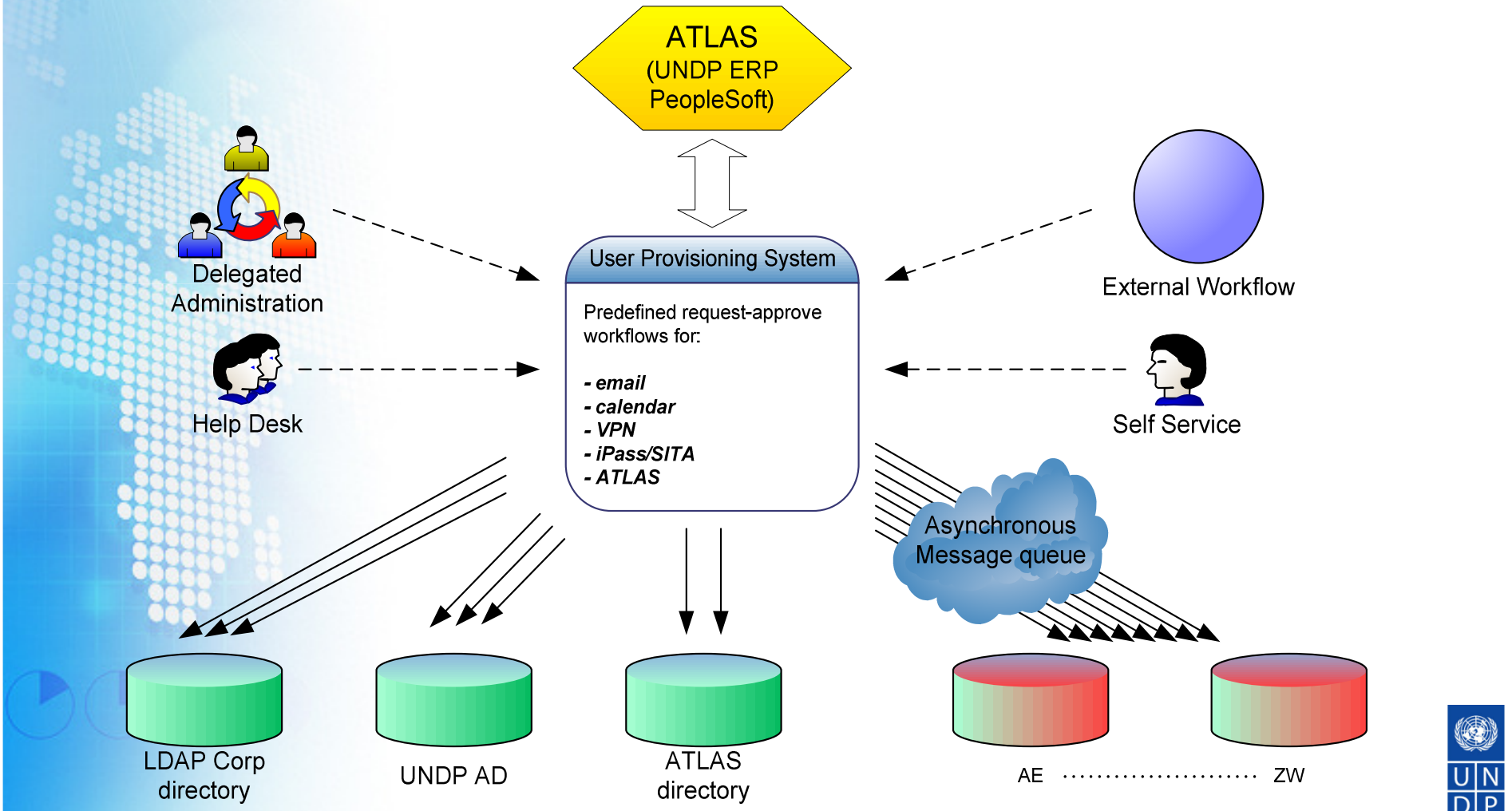
UNDP Overview



UNDP IAM System



Provisioning



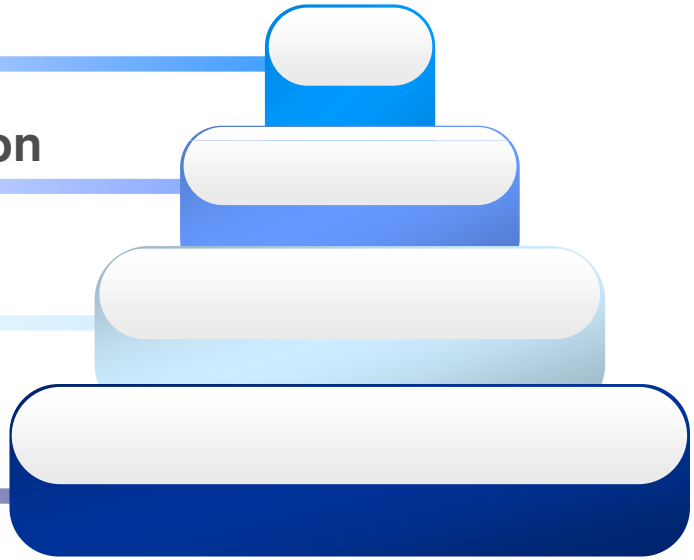
Why Virtual Directory ?

Business Applications

Business Process Integration

Business Infrastructure

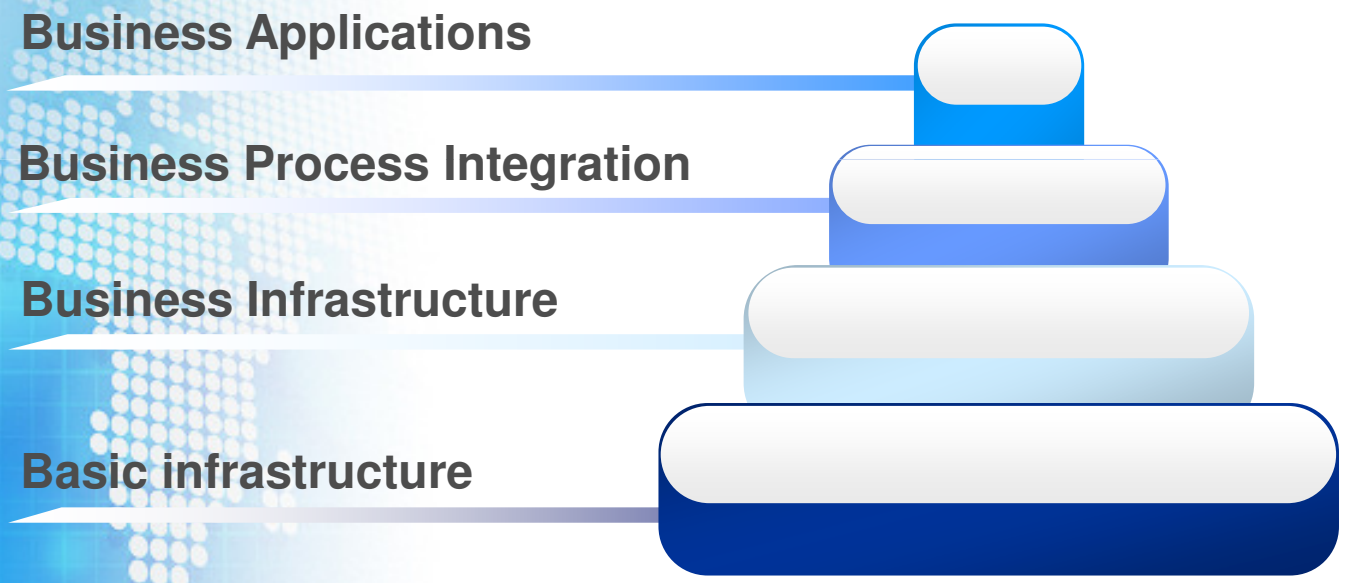
Basic infrastructure



Basic Infrastructure

- Servers
- Network
- OS
- Transport Services

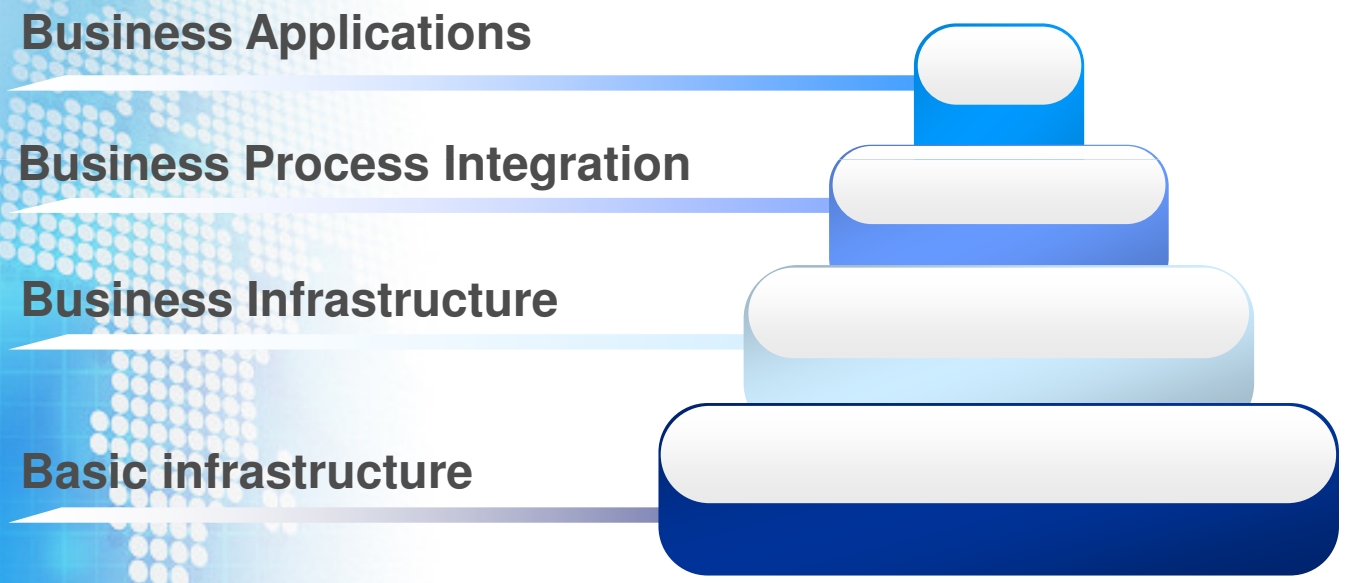
Why Virtual Directory ?



Business Infrastructure

- RDBMS
- LDAP
- PKI
- Messaging
- PBX/VoIP
- Web Services

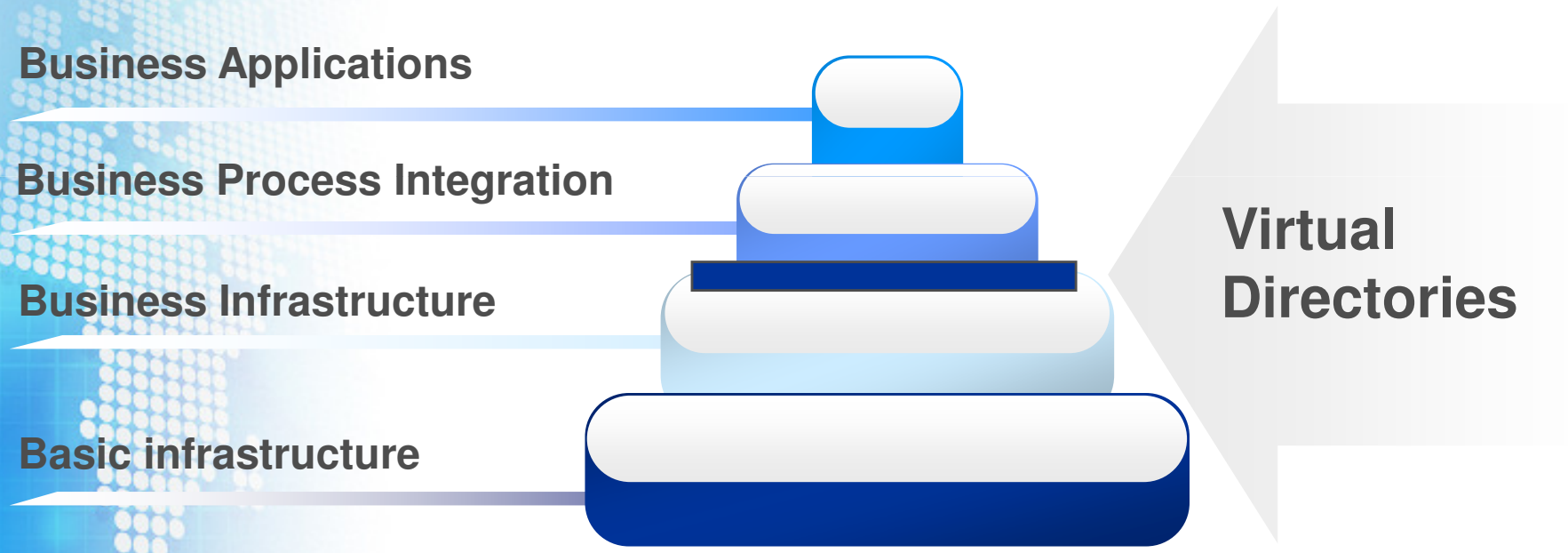
Why Virtual Directory ?



Business Process Integration

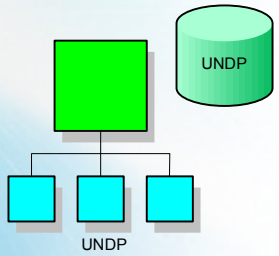
- User Provisioning
- Authentication
- Authorization
- Federation
- Custom Integration

Why Virtual Directory ?



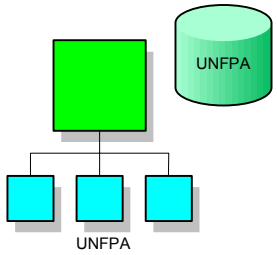
Traditional Use Cases implemented

- Flexible abstraction layer for organization's directory services
- Smart load-balancing and fail-over proxy
- Client's connections optimization through connection pooling
- Translated non-LDAP sources to LDAP
- Unified security policies for multiple directories
- SSL termination point



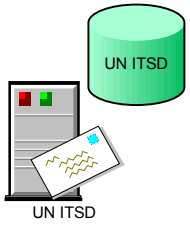
SunONE Directory Server

dn: uid=firstname.lastname,ou=xx,ou=undp,o=un
objectClass: person
objectClass: top
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: mailRecipient
telephoneNumber: +nn (nnn) nnnnnnnn
cn: Firstname Lastname
mailHost: inet01.xx.undp.org
sn: Lastname
givenName: Firstname
mail: firstname.lastname@undp.org
uid: firstname.lastname



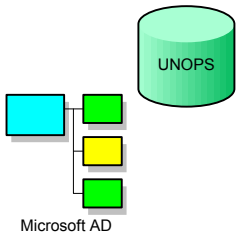
SunONE Directory Server

dn: uid=lastname,ou=People,o=UNFPA
objectClass: person
objectClass: top
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: mailRecipient
telephoneNumber: +nn (nnn) nnnnnnnn
cn: Firstname Lastname
mailHost: mail.unfpa.org
sn: Lastname
givenName: Firstname
mail: lastname@undp.org
uid: lastname



Lotus Domino

dn: uid=lastnamefirstinitial,ou=People,o=UN
objectClass: person
objectClass: top
objectClass: organizationalPerson
objectClass: inetOrgPerson
telephoneNumber: +nn (nnn) nnnnnnnn
cn: Firstname Lastname
mailHost: mailhost.un.org
sn: Lastname
givenName: Firstname
mail: lastnamefirstinitial@un.org
uid: lastnamefirstinitial

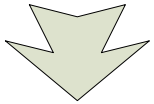


Microsoft Active Directory

dn: CN=Firstname Lastname,DC=unops,DC=org
cn: Firstname Lastname
c: US
displayName: Firstname Lastname
mail: firsinitiallastname@unops.org
givenName: Firstname
distinguishedName: CN=Firstname Lastname,DC=unops,DC=org
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
name: Firstname Lastname
sn: Lastname
telephoneNumber: +nn (nnn) nnnnnnnn

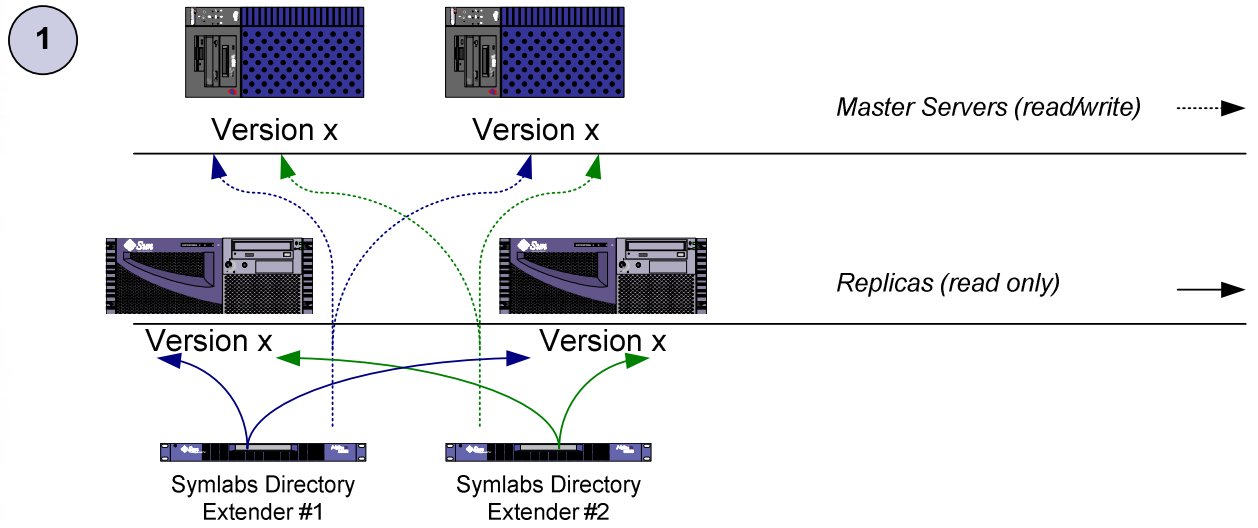
Symlabs Directory Extender #1

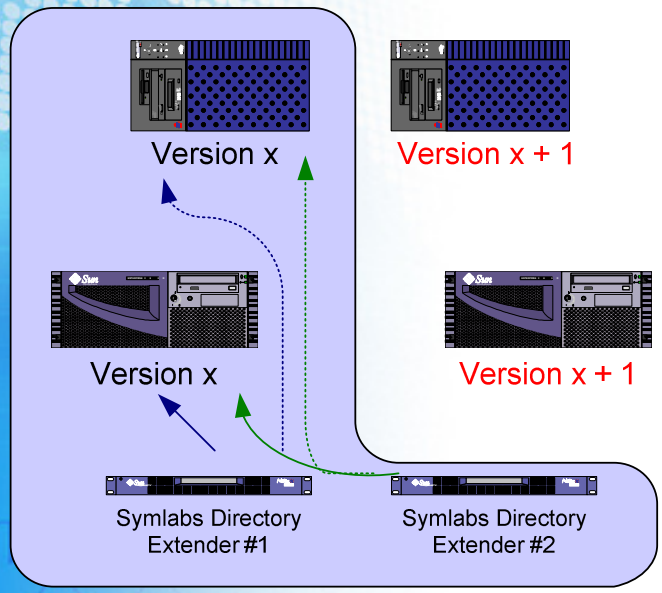
Symlabs Directory Extender #2

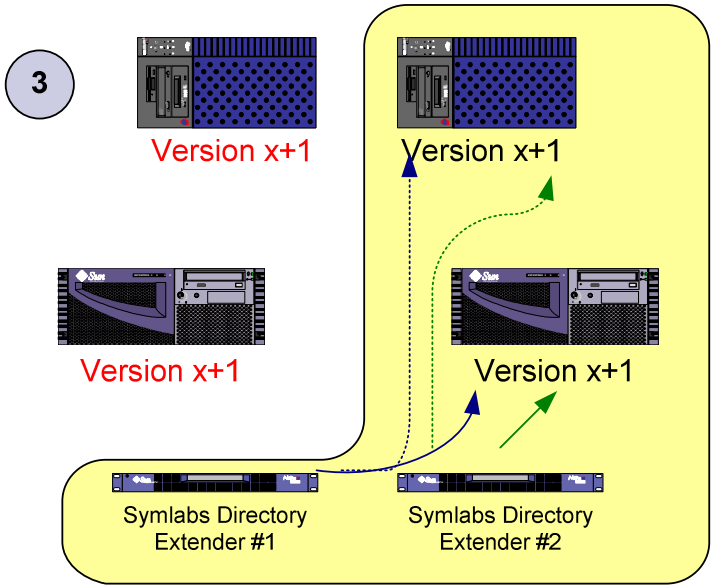


Unified Representattion

dn: uid=firstname.lastname@organization.org,o=un
objectClass: person
objectClass: top
objectClass: organizationalPerson
objectClass: inetOrgPerson
telephoneNumber: +nn (nnn) nnnnnnnn
cn: Firstname Lastname
sn: Lastname
givenName: Firstname
mail: firstname.lastname@organization.org
uid: firstname.lastname@organization.org
userpassword: <bind via SSL to organizational directory server or authentication database>


1
Version x
Version x
Master Servers (read/write)
Replicas (read only)
Version x
Version x
Symlabs Directory Extender #1
Symlabs Directory Extender #2


Version x
Version x + 1
Version x
Version x + 1
Symlabs Directory Extender #1
Symlabs Directory Extender #2


3
Version x+1
Version x+1
Version x+1
Version x+1
Symlabs Directory Extender #1
Symlabs Directory Extender #2

Non-traditional Use Cases implemented

- Protocol debugger (application integration)
- Support for legacy application
- Integration to custom API (Postini cHTML)
- Statistics and clean-up efforts

Challenges

- Executive buy-in
- Redesign of all audit processes
- All beneficiary systems have to be documented prior to deployment
- Backup options and troubleshooting guide
- Keep it simple

Achievements

- Non-intrusive deployment
- Reliability and performance increase
- Integration with Postini
- 0 downtime for backend upgrades
- Interfaces and API available
- Password services

Deployment strategy

Recommendation

- Coordination with Enterprise Architecture Plan
- Executive sponsorship
- “Visual” deliverables
- Build on success
- Document everything


Thank You!