Directory Agnostic ID Broker for Multi-protocol NAS

Manoj Dahal
Manoj.Dahal@microfocus.com
Sridhara Jaganath
Sridhara.Jagannath@microfocus.com

Agenda

- Introduction
- Open Enterprise Server (OES), a Multiprotocol NAS
- Fine-grain Access Control List (aka Trustee-rights) in OES
- Need of an ID Broker
- ID Broker Architecture
- Summary

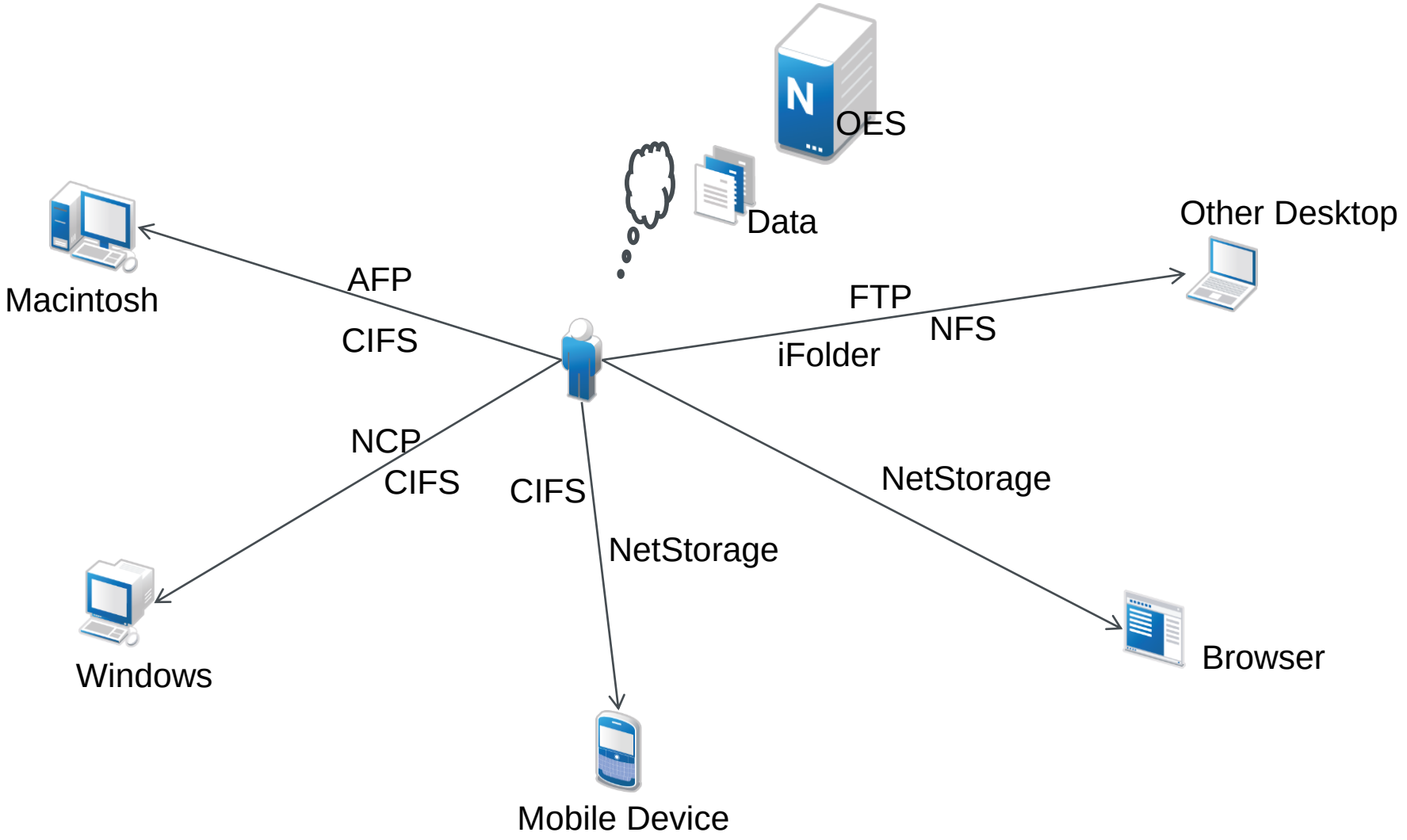
Introduction

- In 90’s we saw the dominance of File Service market by NetWare
- Had almost 80% market share
- The next-generation file server Open Enterprise Server (OES) was born in 2005
- OES is built on SUSE Linux Platform
- Over the last decade it has become a solid Multi-protocol NAS Box
- Has own home grown file system - NSS
- Supports POSIX file systems as well
- Includes clustering capability for failover of nodes
- Distributed File Service is supported by means of Junctions

OES- A Multiprotocol NAS

- OES provides File Access using following protocols
  - CIFS (aka SMB)
  - AFP – Apple File Protocol
  - NCP – NetWare Core Protocol
  - FTP
- Linux NFS server can export an OES Share
- File services are layered over it’s dir cache down to file system
- POSIX system calls or native APIs (called zAPI) are used
- Varieties of clients can connect OES viz. Windows, Linux, Mac
- AD/eDir as Identity Store

What does File Access Means in OES?



OES Architecture

Identity

- **eDirectory**
- **Active Directory**

Access Protocols

- NCP
- AFP
- FTP
- SMB v1 & v2

Data Management Services

- DFS
- DST
- SMS
- Migration

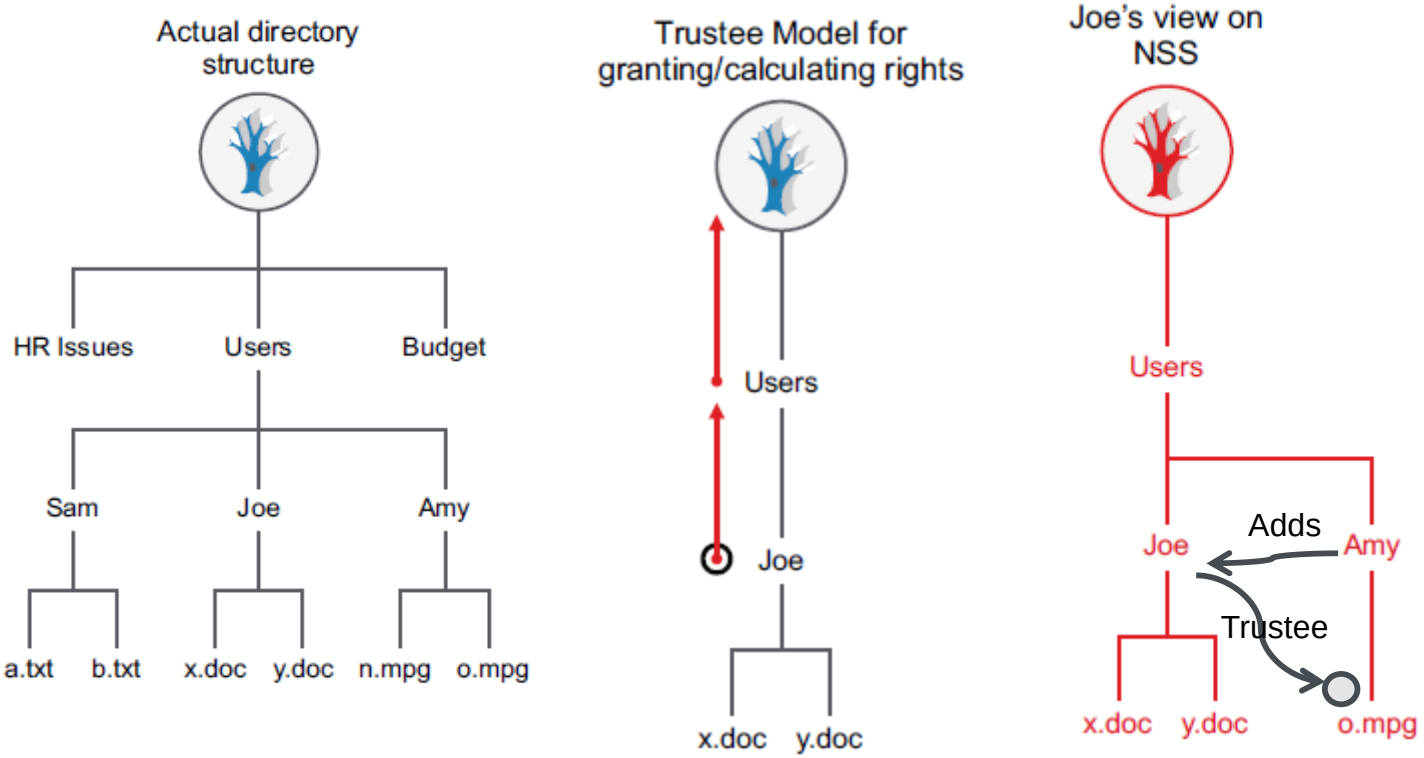
File System

- NSS > 8 TB
- NLVM
- RAID

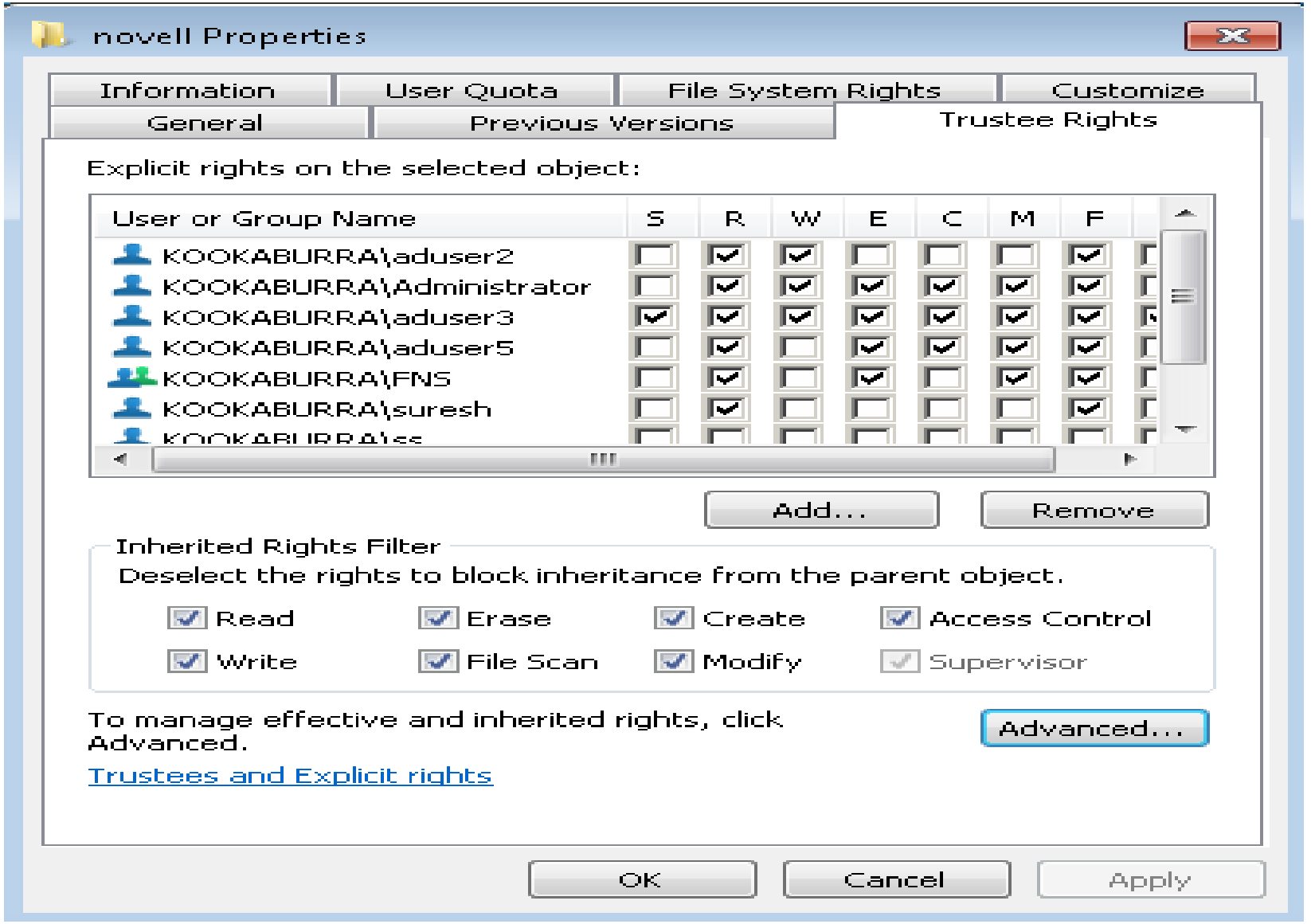
Clustering

- NCS

Fine-grain ACLs (aka Trustee-rights) in OES



- Granting Rights (e.g. to Joe)
  - Inheritance and visibility
- Sharing with (e.g. Joe to Amy)
- Very much scalable on trustee settings
  - No stamping on every object


novell Properties
Information
User Quota
File System Rights
Customize
General
Previous Versions
Trustee Rights
Explicit rights on the selected object:
User or Group Name
S
R
W
E
C
M
F
KOOKABURRA\aduser2
KOOKABURRA\Administrator
KOOKABURRA\aduser3
KOOKABURRA\aduser5
KOOKABURRA\FNS
KOOKABURRA\suresh
Add...
Remove
Inherited Rights Filter
Deselect the rights to block inheritance from the parent object.
Read
Erase
Create
Access Control
Write
File Scan
Modify
Supervisor
To manage effective and inherited rights, click Advanced.
Advanced...
Trustees and Explicit rights
OK
Cancel
Apply

What is the Need of an ID Broker?

- In Linux/UNIX world there is concept of User Id
- Which is tightly coupled with Operating system and the file system
- In today's world data and identity are in separate stores
- Need a way to relate Linux/UNIX User Id to the Identity
- Scalability – e.g. number of users/DC/Forest etc.

- Seamlessly need to work with different Identity Stores
- Linux understands only UID
- NSS File System supports remote identity – GUID/SID
- Need a marriage between all UID/GUID/SID/Name
- GUID/SID History (ability to map same UID)
- That’s why ‘NIT’ was born

The ID Broker- NIT

- Single Point of Contact for eDirectory (eDir) and Active Directory (AD) identities

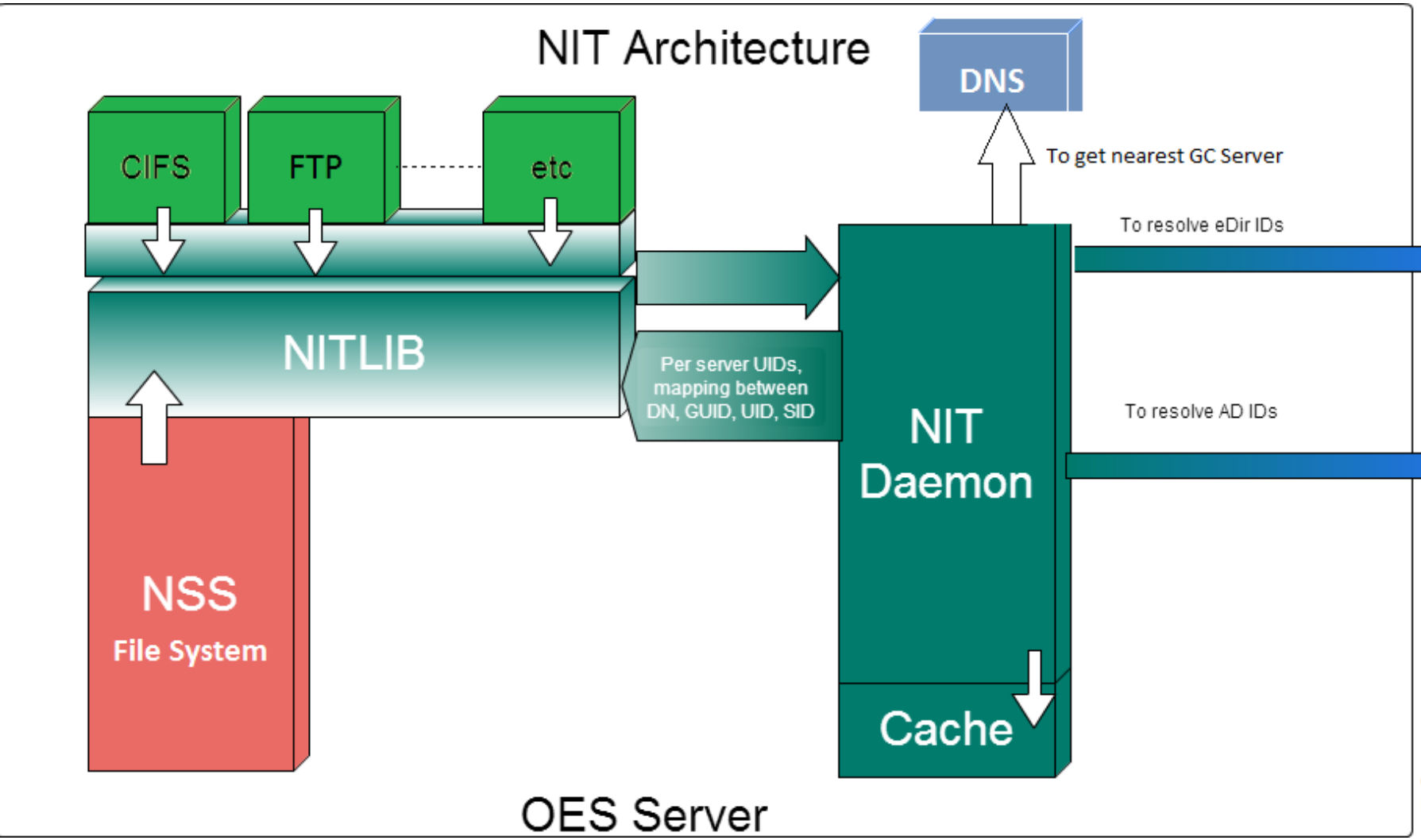
- Generates UID*
  - AD users need not necessarily have uidNumber attribute populated
  - Configure UID range appropriately

- Converts Identity attributes
  - GUID, UID, Name and SID (for AD alone)
  - Cache

- Fetches/calculates group memberships

**A user ID (UID) is a unique positive integer assigned by a Unix-like operating system to each user.*

NIT Architecture



UID Translation…

- CIFS
  - User Logins
  - Obtains Group Membership
  - GetUIDByName()
  - Setfsuid()

- NSS
  - Get UID from CIFS
  - GetUserInfoByUID
  - Receives GUID
  - Also asks Group Memberships from NIT

- ID Broker
  - Gets nearest GC from DNS
  - ldap binds with GC Server (port 3268)
  - Gets group memberships from AD/eDir
  - Maps between UID, GUID, SID & Name

Summary

- OES, a Multi-protocol NAS supports CIFS, NCP, AFP and FTP for file access
- An ID Broker has been introduced for mapping user id to identity residing in eDirectory and Active Directory
- The User Ids are mainly used for file authorization in OES
- We see immense future possibilities for it

Thank You

Q & A