NFS Version 4 Requirements at Sandia National Laboratories

Connectathon 2003

March 04, 2003

Daniel Wachdorf
drwachd@sandia.gov

Sandia National Laboratories

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy under contract DE-AC04-94AL85000.

Sandia National Laboratories

Overview

- As part of the ASCI (Advanced Simulated and Computing Program) we are looking to develop and deploy a common security infrastructure and a common distributed file system that meets the needs of ASCI.
- We plan on transitioning from IBM DCE/DFS to a Microsoft Active Directory, LDAP, and NFSv4 environment

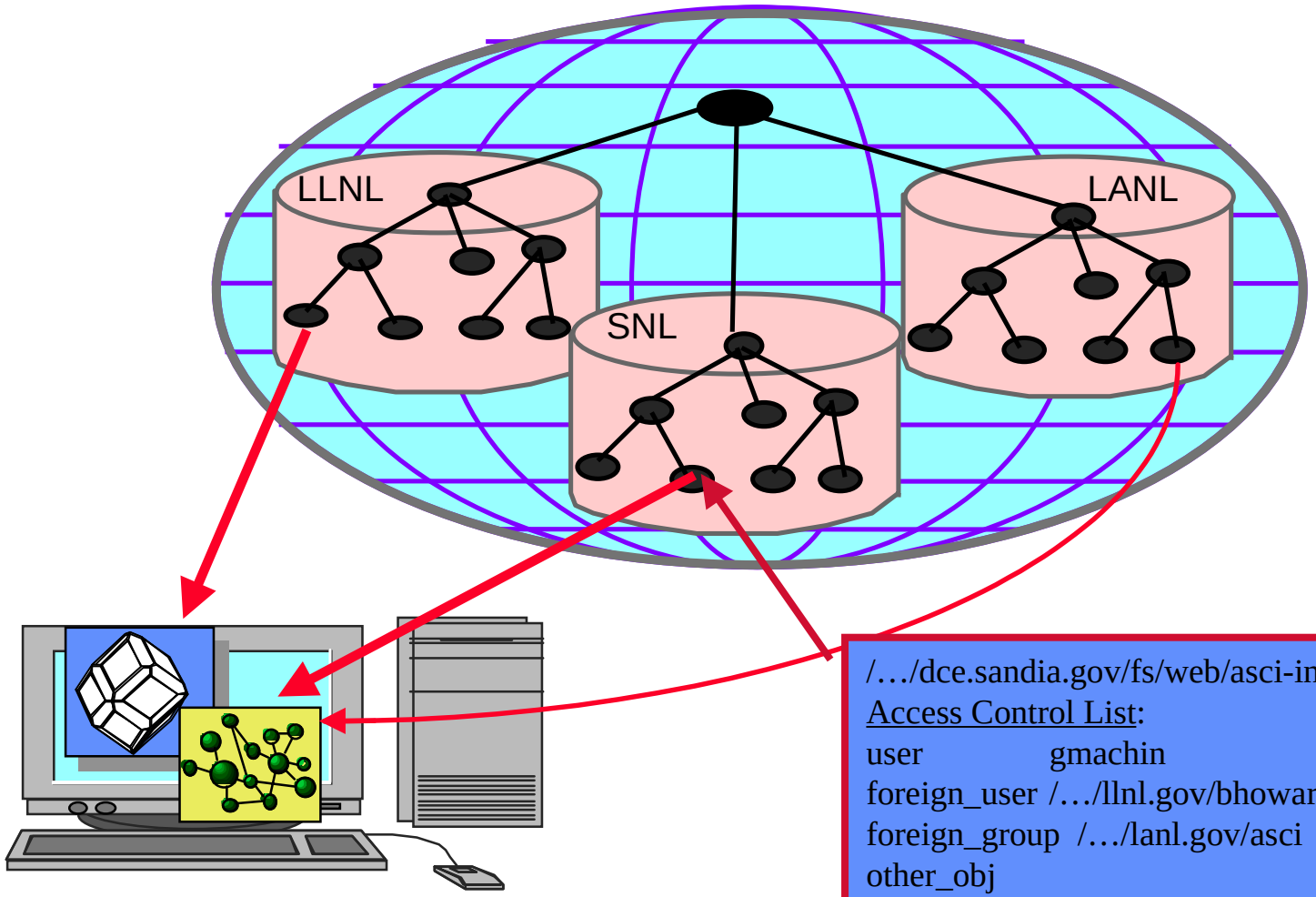
Sandia National Laboratories

Current Environment

- **Many Platforms – Microsoft, Sun, IBM, HP, SGI, and Linux**
- **Authentication – IBM DCE (Kerberos 5) and Windows Authentication (NT MD)**
- **Directory Service – IBM Cell Directory Service and Active Directory**
- **Network File System – IBM DFS**

Sandia National Laboratories

DFS Cross Cell Trust



/…/dce.sandia.gov/fs/web/asci-info.html

Access Control List:

user	gmachin	rwxc
foreign_user	/…/llnl.gov/bhoward	rw
foreign_group	/…/lanl.gov/asci	r
other_obj		r

Impetus for Change

- **IBM announces end of life for DCE/DFS support at the end of 2004**
- **Microsoft Active Directory enables Kerberos and LDAP support**
- **Expanding use of secure WAN file system not only for ASCI Labs (Sandia, LANL, and LLNL), but other Labs and Plants as well (Pantex, Y12, . .)**

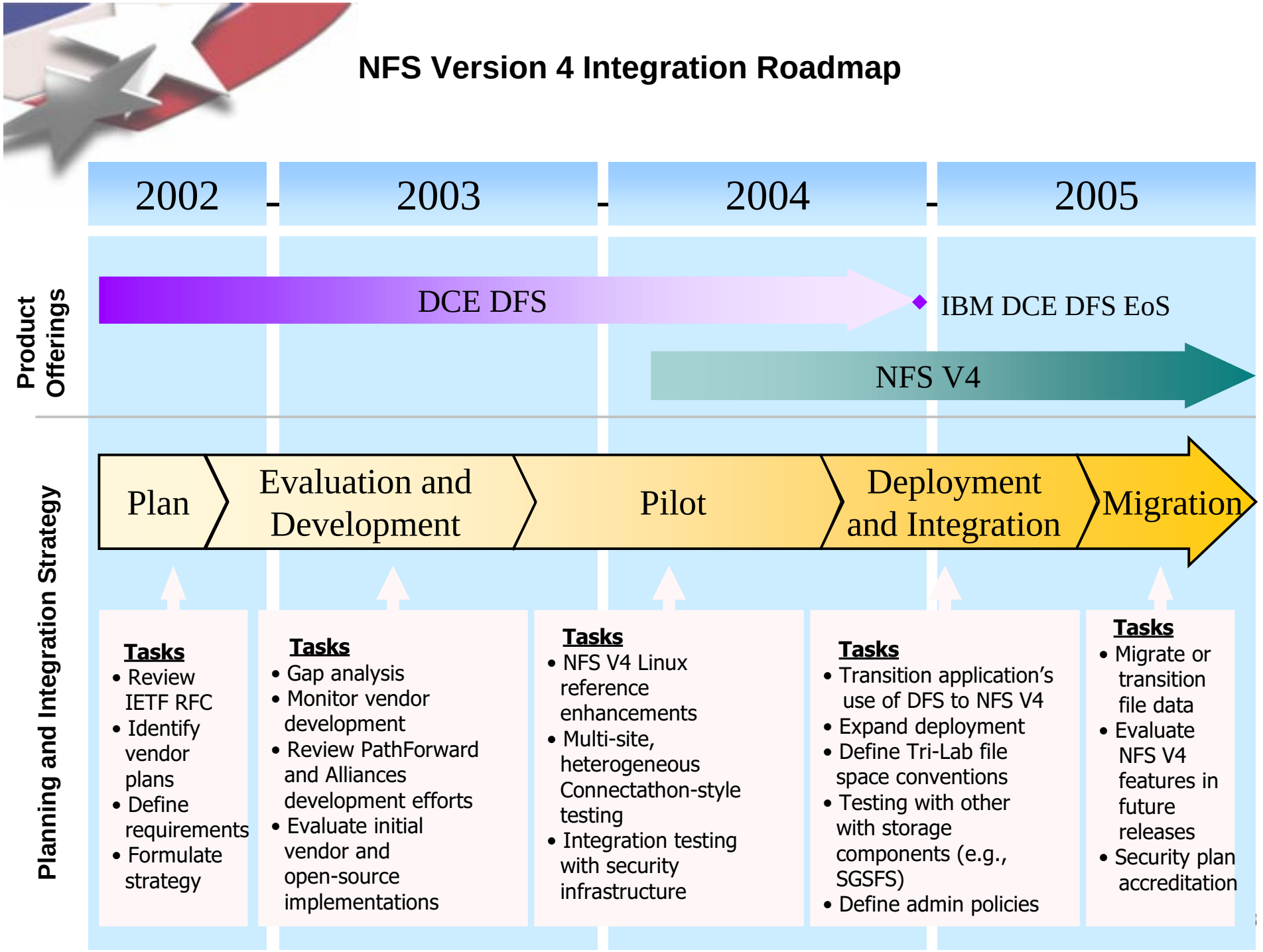
Sandia National Laboratories

Future Environment

- Still many Platforms
- Authentication – Kerberos V (GSSAPI and Active Directory)
- Directory Service – LDAP
- Network File System – NFS Version 4 (?)
- Operation across multiple security Realms

Sandia National Laboratories

NFS Version 4 Integration Roadmap



NFSv4 Implementation Requirements

- TCP
- Kerberos 5 Authentication (RPCSEC_GSS)
- Seamless integration with Windows and Unix systems.
- Robust Access Control Lists – specific access for local users and groups and remote users and groups.

Sandia National Laboratories

Concerns with NFSv4 Implementations

- User to UID/GID mapping
- Group Information
- Access Control List processing

Sandia National Laboratories

User to UID/GID mapping

- **Must handle cross realm users ie -** `john@sandia.gov` **and** `john@lanl.gov` **must be different.**
- **Don’t want to create a local account for each local and foreign user.**
- **Don’t want foreign users/groups mapped to local UID/GID.**

Sandia National Laboratories

Idea – Separate File systems

- For POSIX systems, separate local permissions and network file permissions.
- Have files be locally owned by user nfsd, then export those with permissions based on ACL.
- Local users can not access files through local file system
- Local users would just mount the directory using NFS to have access to files they own.
- Problem - Where are ACL stored?

Sandia National Laboratories

User's Group Information

- Would like to see NFSv4 use LDAP to obtain local group information for local users.
- Would like support for obtaining group information for foreign users.
- NFSv4 should work seamlessly with Microsoft Active Directory.
- Optionally - Use Privilege Attribute Certificate from Microsoft Windows to obtain Group Information.

Sandia National Laboratories

Idea – Customizable Callbacks

- Have the implementation use a customizable callback to determine group information for foreign groups.
- This would allow modification to fit NFSv4 in operating situations that best suite our needs.
- For example, we want to decode the Microsoft PAC to determine group information, or we communicate with foreign LDAP server to determine group identity of foreign users.

Sandia National Laboratories

Order of Access Control List

- **Problem: RFC 3010 specifies no way in which Access Control Entry order is handled in a list. RFC just states “in order”.**
- **Access control list management creates enough problems for end users, now we have the following situation possible:**
  - **We have user `john@sandia.gov` who is a member of `users@sandia.gov`**
  - **We have a file we want `users@sandia.gov` to access, so we `acl +r users@sandia.gov file.`**
  - **We don’t want `john` to access the file, so we `acl –r john@sandia.gov file.`**
  - **The ACL is:**

```
ALLOW read users@sandia.gov
DENY read john@sandia.gov
```

  - **Unfortunately, we have granted `john` access to the file when we wanted to deny him access.**

Sandia National Laboratories

Idea – Processing Order

- **Solution: Process ACL entries in a specific order. ALLOW or DENY at each step.**
  - **First, check local user access.**
  - **Next, check foreign user access.**
  - **Next, check local group access.**
  - **Next, check foreign group access.**
  - **Lastly, check “others” access.**
- **This prevents ambiguity and provides an easier to understand method for processing ACL.**

Sandia National Laboratories

Sandia's Goals

- **Would like to work with Companies developing implementations.**
- **Participate in testing NFSv4 in cross realm environments.**

Sandia National Laboratories