ZEROPIU
Difference as value

RBAC on Samba Environment

Fabrizio Manfredi Furuholmen

April 2008

Agenda

Introduction

RBAC Overview

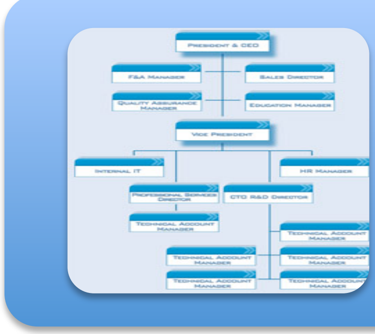
Solution

Implementation with Samba native methods

Implementation with custom Samba VFS

Conclusion

Introduction


President & CEO
F&A Manager
Sales Director
Quality Assurance Manager
Education Manager
Vice President
Internal IT
HR Manager
Professional Services Director
CTO R&D Director
Technical Account Manager
Technical Account Manager
Technical Account Manager
Technical Account Manager
Technical Account Manager
Technical Account Manager

"Within an organization, roles are relatively stable, while users and permissions are both numerous and may change rapidly"

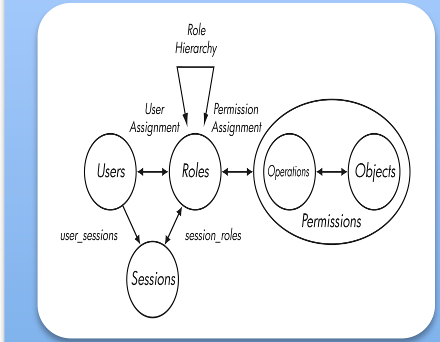
Controlling all access through roles simplifies

Management

Review of access controls

Enforce enterprise-specific security policies

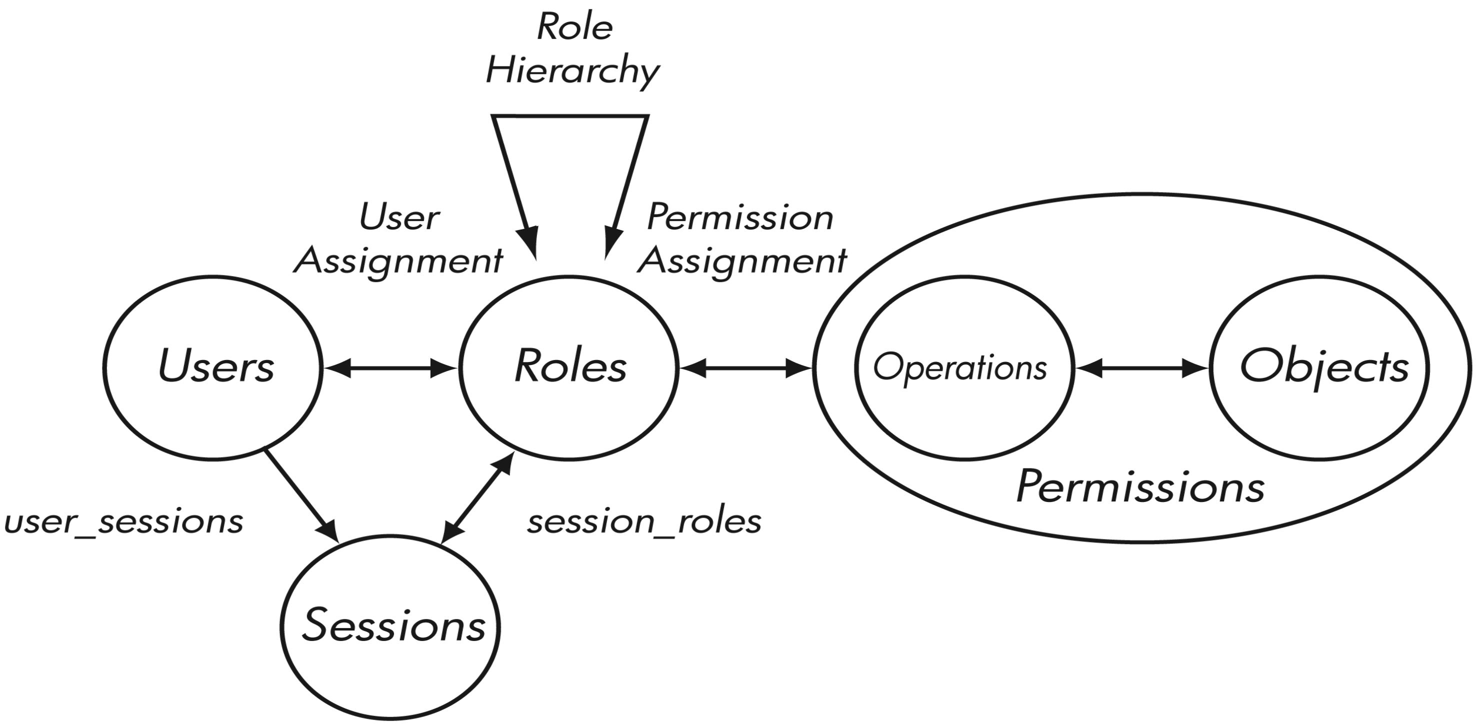
Overview: RBAC



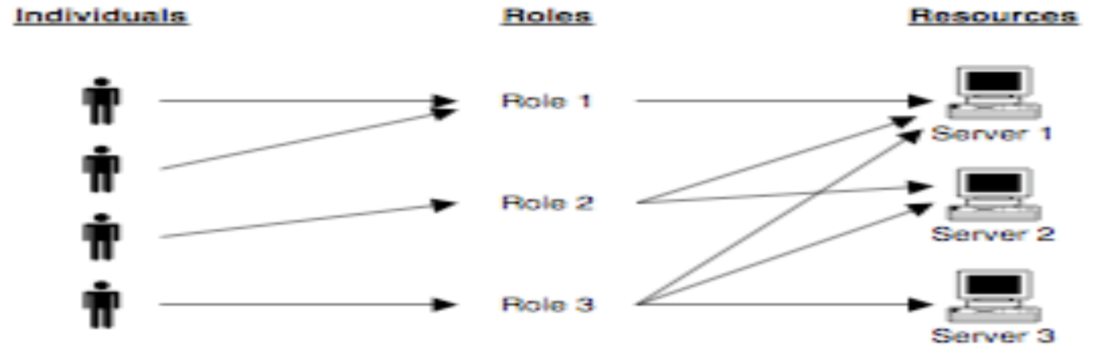
A general-purpose role based access control model was proposed in 1992 by Ferraiolo and Kuhn

- A key feature of this model is:
  - All access is through roles
  - A role is essentially a collection of permissions
  - All users receive permissions only through the roles to which they are assigned, or through roles they inherit through the role hierarchy

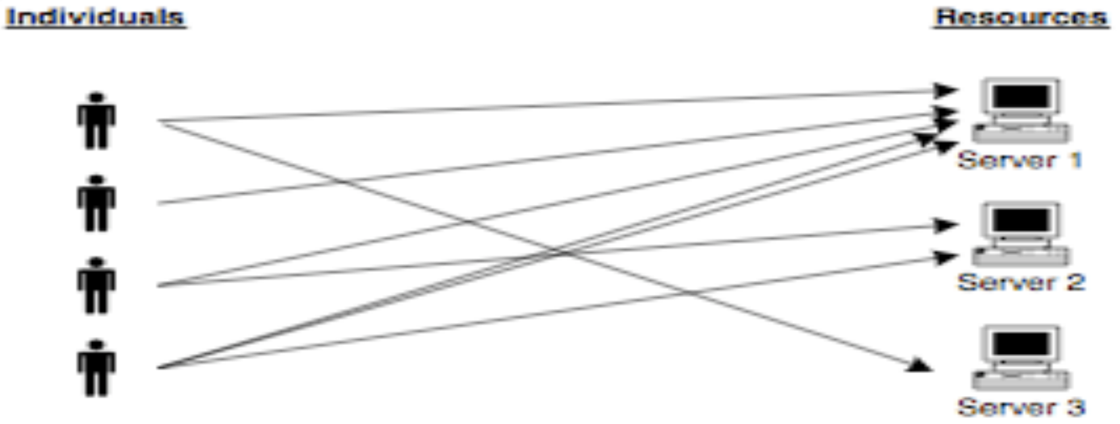
Overview: Model



Overview: RBAC vs ACL



a) Role-Based Access Control



b) Discretionary Access Control Using Access Control Lists

Introduction: Windows

Application

- namespace for roles, tasks, and operations.

Scope

- collection of resources in which each resource of similar type has the same authorization policy.

Role

- Usually corresponds to a job category or responsibility (for example, purchaser or hiring manager) and is a collection of tasks that a user must have to do that job.

Task

- collection of operations and sometimes other tasks.

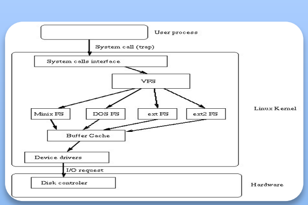
Operation

- set of permissions that are associated with system-level or API-level security procedures.

Business Rule

- script that is associated with a task. A rule allows access decisions to be based on any run-time condition that a script can test.

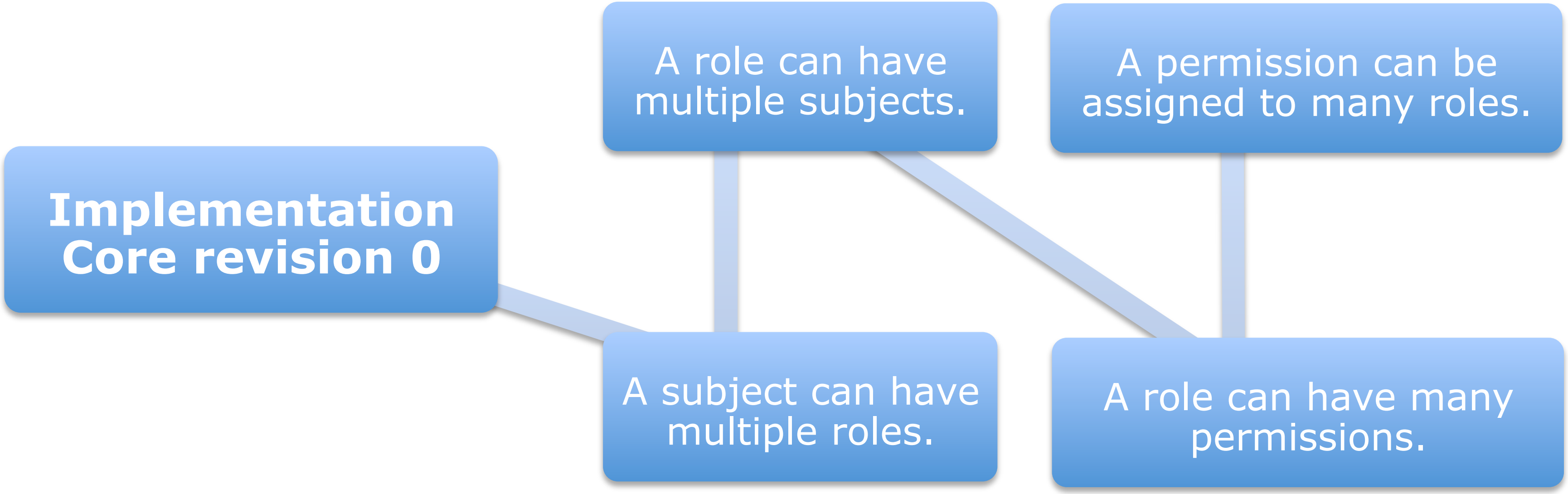
Implementation Steps



Steps

- **Role analysis**
- Identify Resources
- RBAC object map
- Samba implementation

Implementation



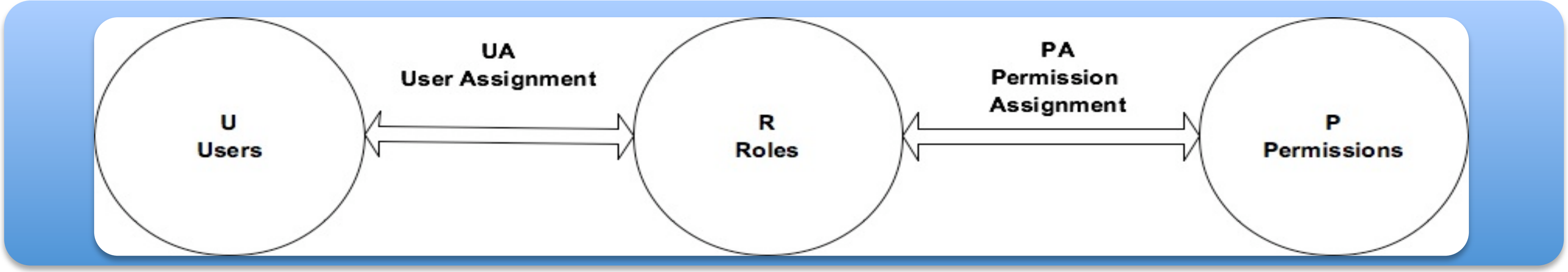
Implementation Core revision 0

A role can have multiple subjects.

A permission can be assigned to many roles.

A subject can have multiple roles.

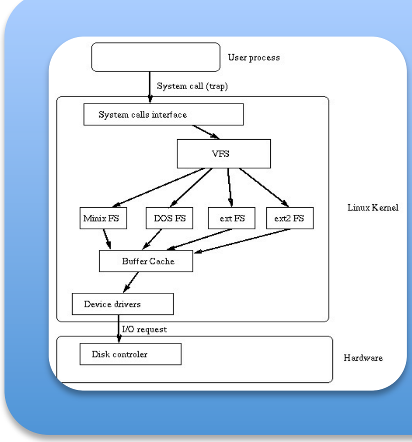
A role can have many permissions.



Samba Implementations

Usage Native methods

- Share
- Groups



VFS Module

- Custom Module
- Directory Server

Native Methods : Mapping

U
Users

Samba User

R
Roles

Group

- With specific prefix Role_[Role name]

P
operations

Group

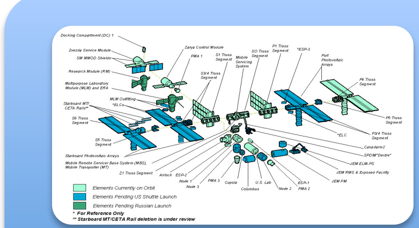
- RO Group prefix OBJECTNAME_RO with read only permission
- RW Group prefix OBJECTNAME_RW with read write permission
- OWNER Group prefix OBJECTNAME_OWNER with complete permission

P
Objects

Shares

- Minimal element Windows share
- Windows share name = operation group name

Native Methods: smb.conf

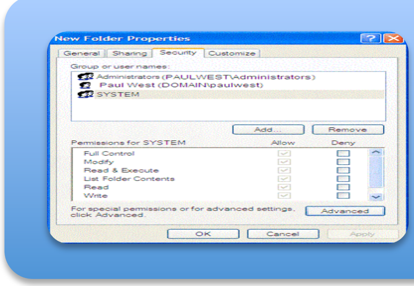


Conf

- Winbind nested groups
- Local group as permission
- Domain group as role
- Force group creation

Share

- *valid user ..*



Group or user names:

Administrators (PAULWEST\Administrators)
Paul West (DOMAIN\paulwest)
SYSTEM

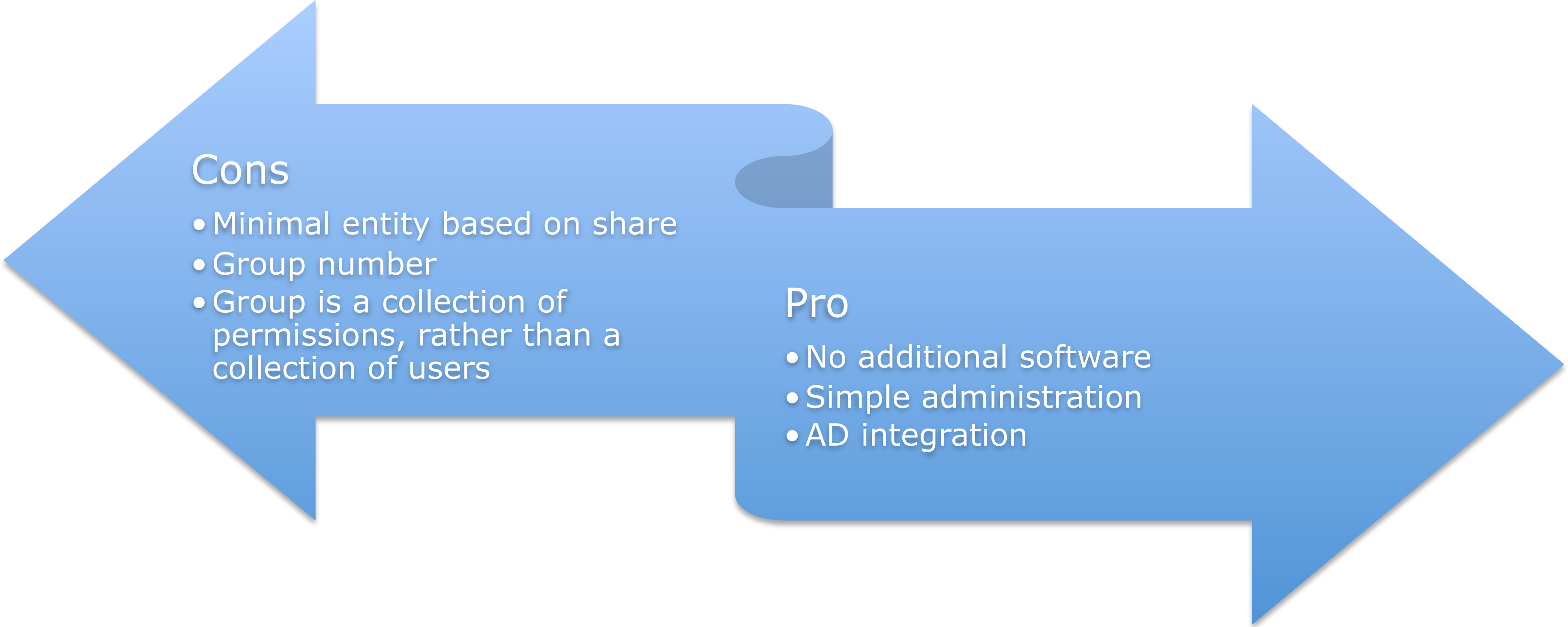
Permissions for SYSTEM	Allow	Deny
Full Control	☑	☐
Modify	☑	☐
Read & Execute	☑	☐
List Folder Contents	☑	☐
Read	☑	☐
Write	☑	☐

For special permissions or for advanced settings, click Advanced.

ACL

- ACL support on File system
- ACL inherits

Native Methods : result



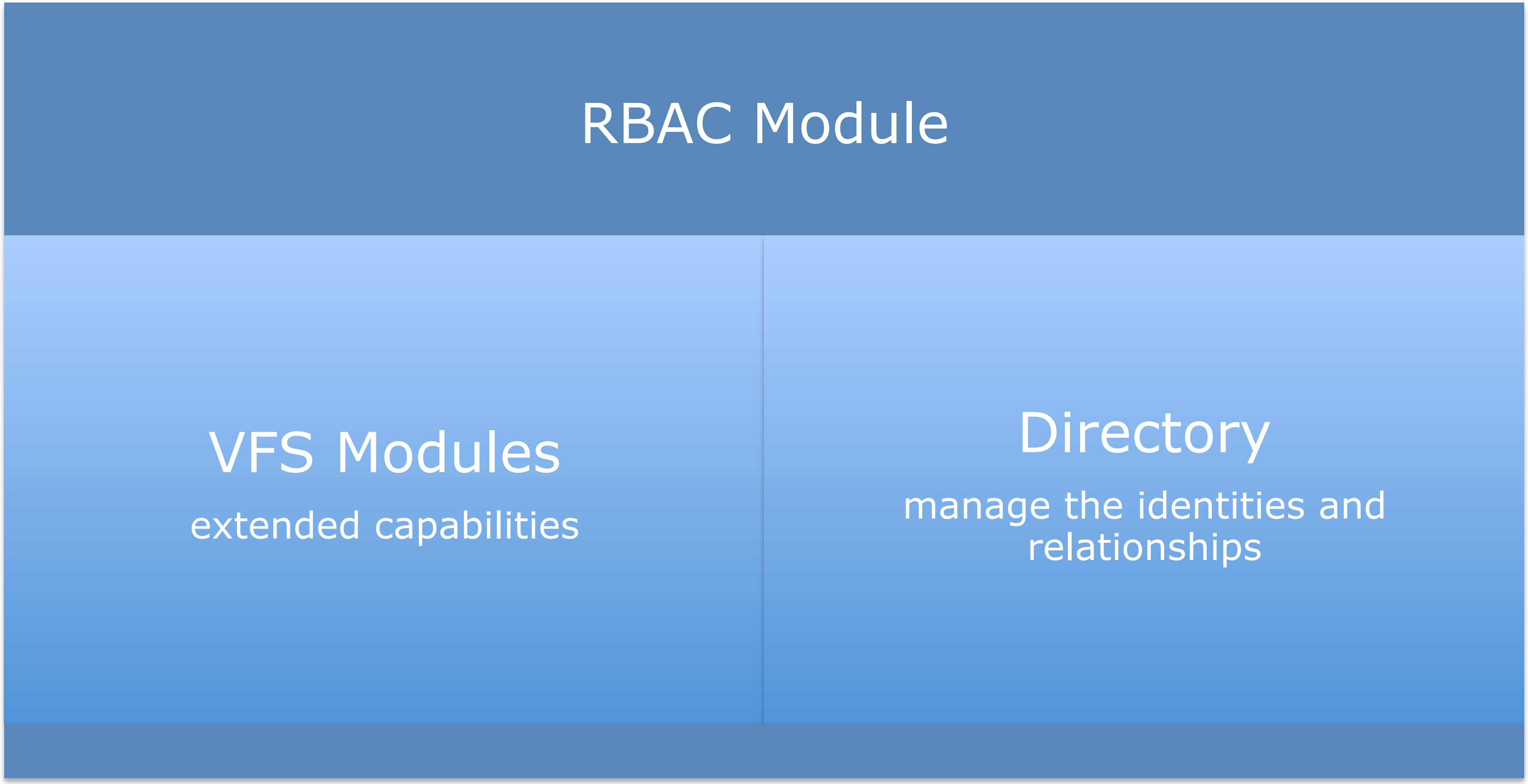
Cons

- Minimal entity based on share
- Group number
- Group is a collection of permissions, rather than a collection of users

Pro

- No additional software
- Simple administration
- AD integration

VFS Module: introduction



RBAC Module

VFS Modules

extended capabilities

Directory

manage the identities and relationships

VFS Module : Mapping

U
Users

Samba User

R
Roles

New entity

- New branch in Directory server
- New objectclass

P
Operations

VFS layer

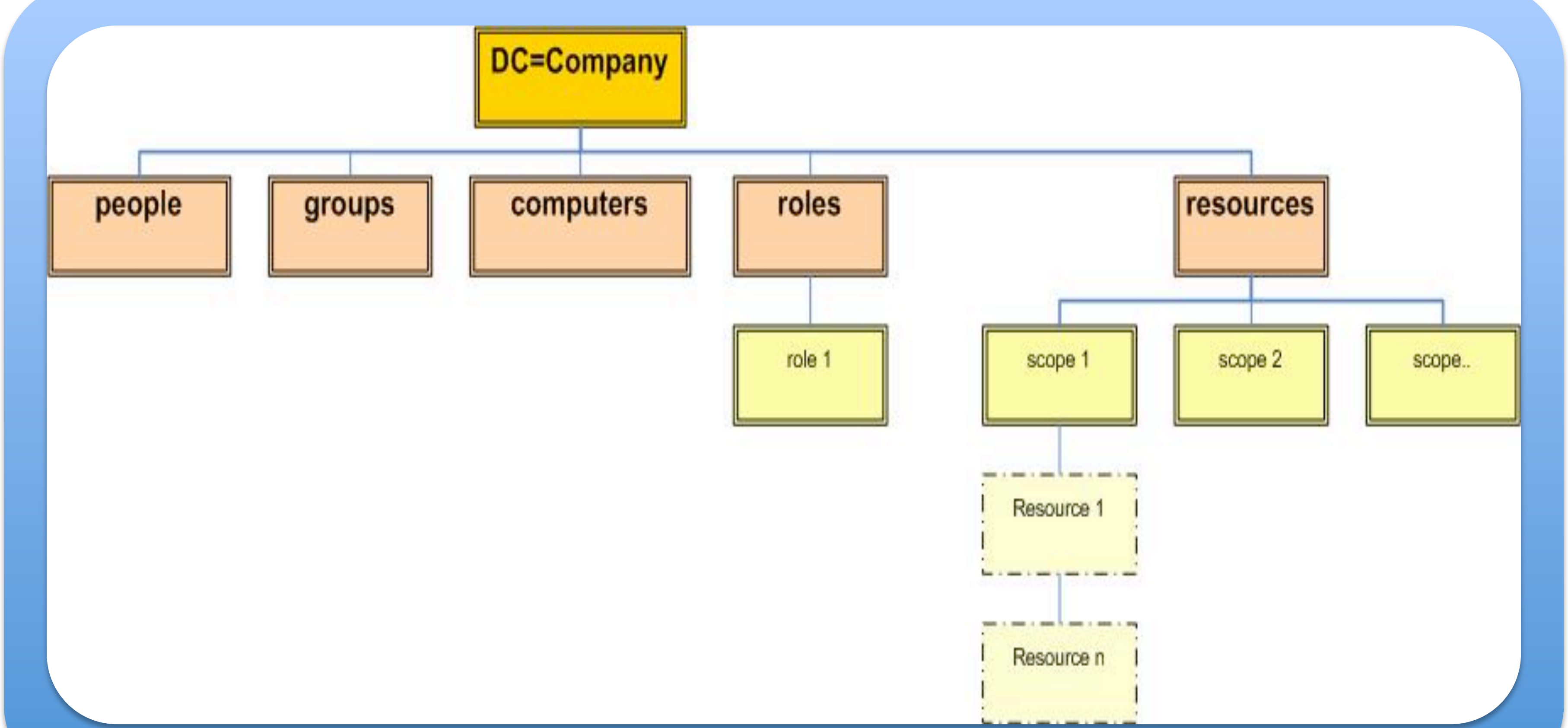
- Operation handle by vfs ()
- Attribute in object level

P
Objects

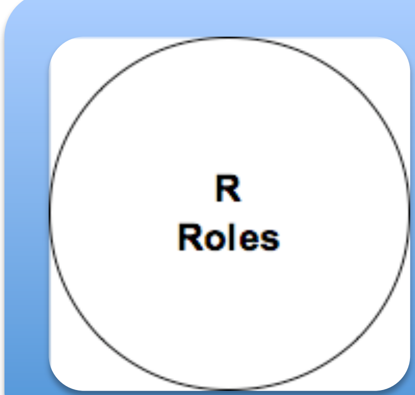
New entity

- New branch in Directory server
- New objectclass

VFS Module: DIT

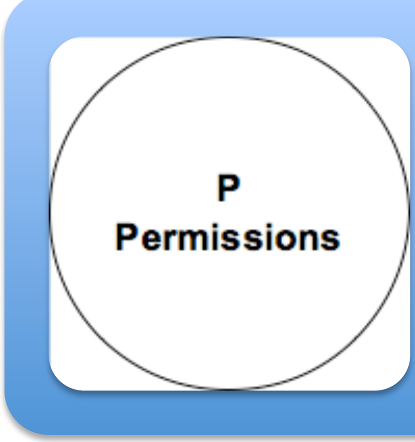


VFS Module: DIT



Role Object

- userMemberID
- roleName
- adminUser

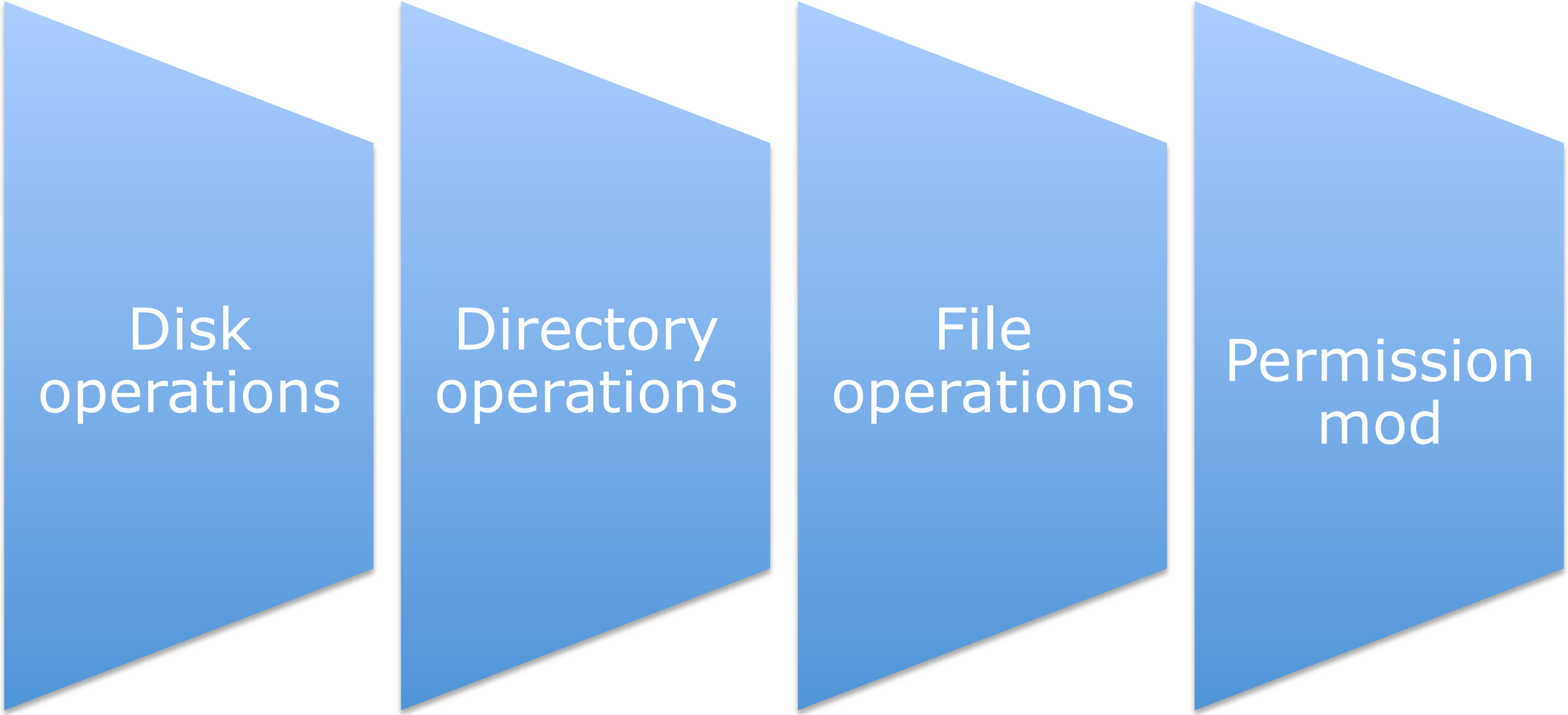


Resources Object

- objectName
- URL
- Operations
- Role

VFS Module: implementation

Check Role/Permission on: Write/Read/Administration



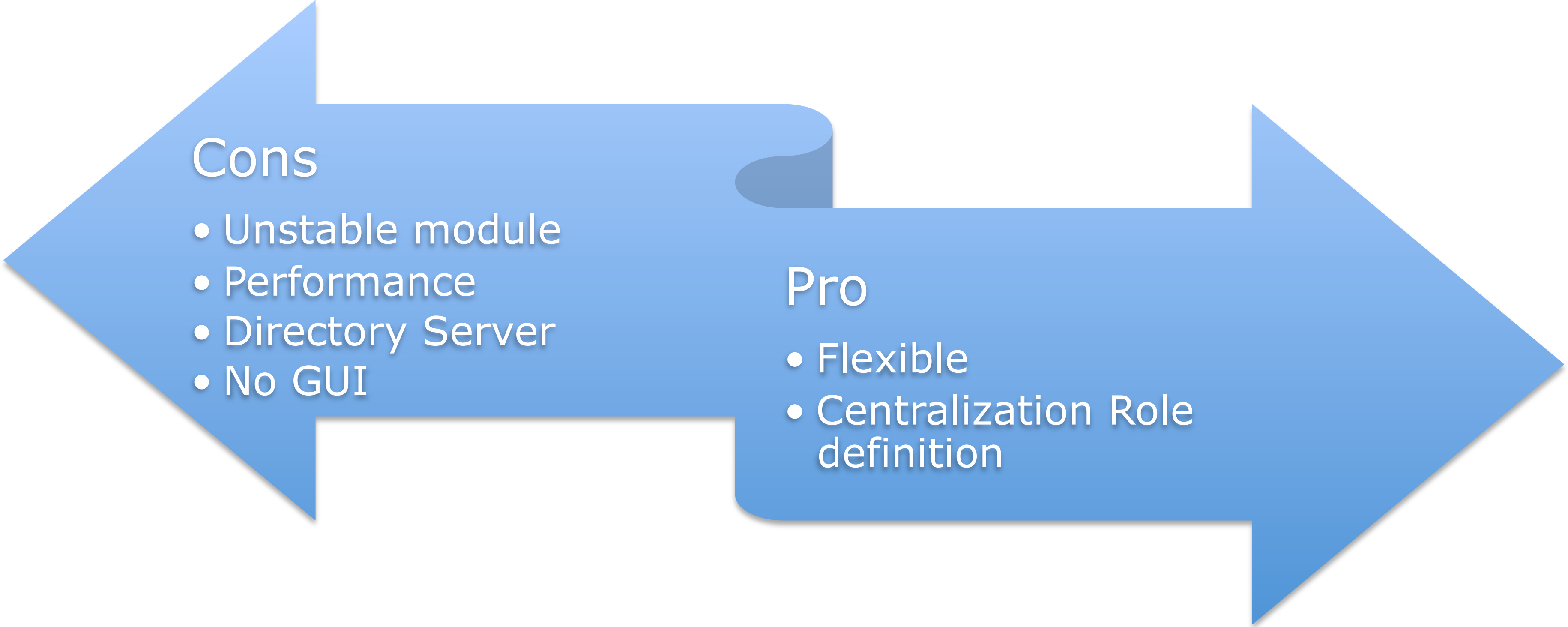
Disk operations

Directory operations

File operations

Permission mod

VFS Module: result



Cons

- Unstable module
- Performance
- Directory Server
- No GUI

Pro

- Flexible
- Centralization Role definition

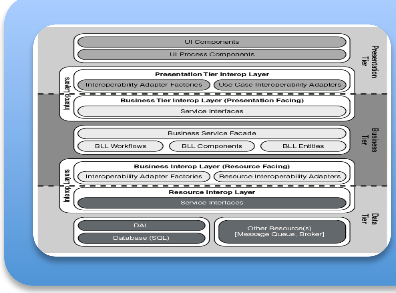
Common Errors

Wrong Usage

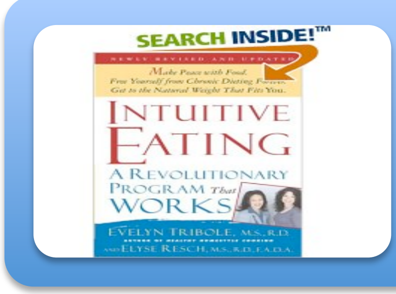
- Unstable organization
- Many cross function user
- Usage RBAC as ACL
- Security Enforcement

Benefit

Multi-user systems


UI Components
UI Process Components
Presentation Tier
Presentation Tier Interop Layer
Interoperability Adapter Factories
Use Case Interoperability Adapters
Interop Layers
Business Tier Interop Layer (Presentation Facing)
Service Interfaces
Business Service Facade
BLL Workflows
BLL Components
BLL Entities
Business Tier
Business Interop Layer (Resource Facing)
Interoperability Adapter Factories
Resource Interoperability Adapters
Interop Layers
Resource Interop Layer
Service Interfaces
DAL
Database (SQL)
Other Resource(s) [Message Queue, Broker]
Data Tier

Multi-application systems


SEARCH INSIDE!™
NEWLY REVISED AND UPDATED
Make Peace with Food.
Free Yourself from Chronic Dieting Forever.
Get to the Natural Weight That Fits You.
INTUITIVE EATING
A REVOLUTIONARY PROGRAM That WORKS
EVELYN TRIBOLE, M.S., R.D.
AND ELYSE RESCH, M.S., R.D., F.A.D.A.

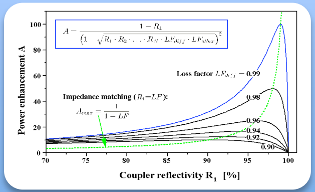
Intuitive

- competency, authority and responsibility

Result

Deploy

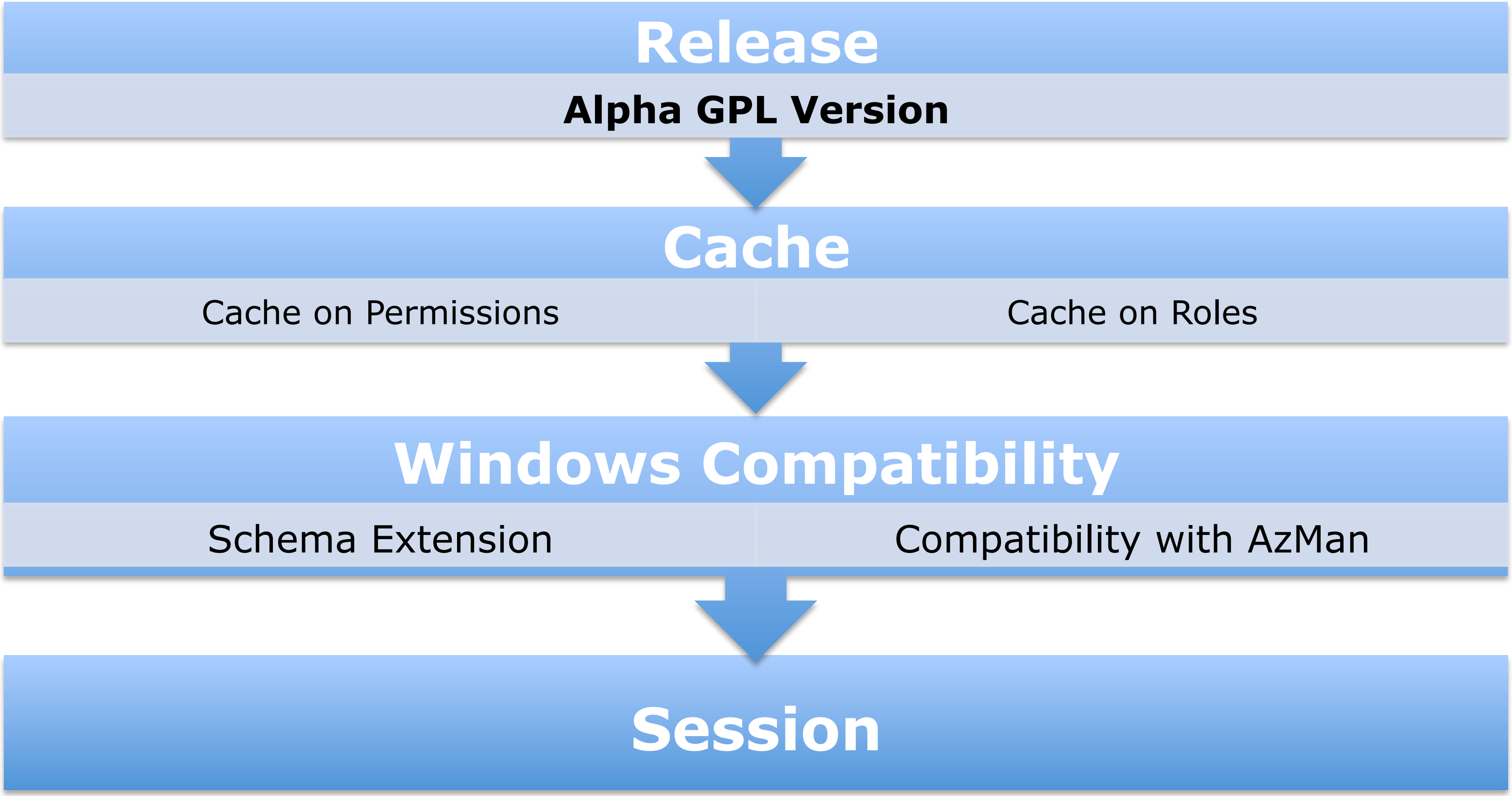
- 400 people
- 20 roles
- 100 shares
- 7 servers



Enhancement

- Reduction provisioning time 70%
- Simplify security audit

VFS Module: next



Release

Alpha GPL Version

Cache

Cache on Permissions

Cache on Roles

Windows Compatibility

Schema Extension

Compatibility with AzMan

Session

Reference

- For Further Questions:
- Fabrizio Manfredi
- fabrizio.manfredi@gmail.com manfred@freemails.ch
- http://www.beolink.org