

Centralized Web Application Authentication and Authorization

Lawrence Kearney

Systems Support Specialist
Medical College of Georgia

Jack Evans

Web Content Administrator
Medical College of Georgia

Novell.[®]

Session Resources

- Contact Information:
 - > Lawrence Kearney, Systems Support Specialist
 - » lkearney@mcg.edu
 - > Jack Evans, Web Content Administrator
 - » jaevans@mcg.edu

The background of the slide is a solid blue color with a pattern of white diagonal lines. These lines originate from the right edge and fan out towards the left, creating a sense of motion or depth. The lines vary in thickness and opacity, with some being more prominent than others.

Background

Challenge

- Migrate university web presence from the Microsoft IIS platform to an alternate platform
 - Tens of thousands of pages and documents
 - Lack of internal web server application development and support resources
 - Dozens of publishers
 - > Mac
 - > PC
 - Local accounts for publishing access
 - > Not synchronized to our directory system

Goals

- Update web server to current technology standards
- Improve web server support “ability”
- Improve web server scalability
- Improve web server security
- Improve web server performance
- Improve web server availability
- Minimize internal support overhead
- Minimize content management overhead

Content Management Environment

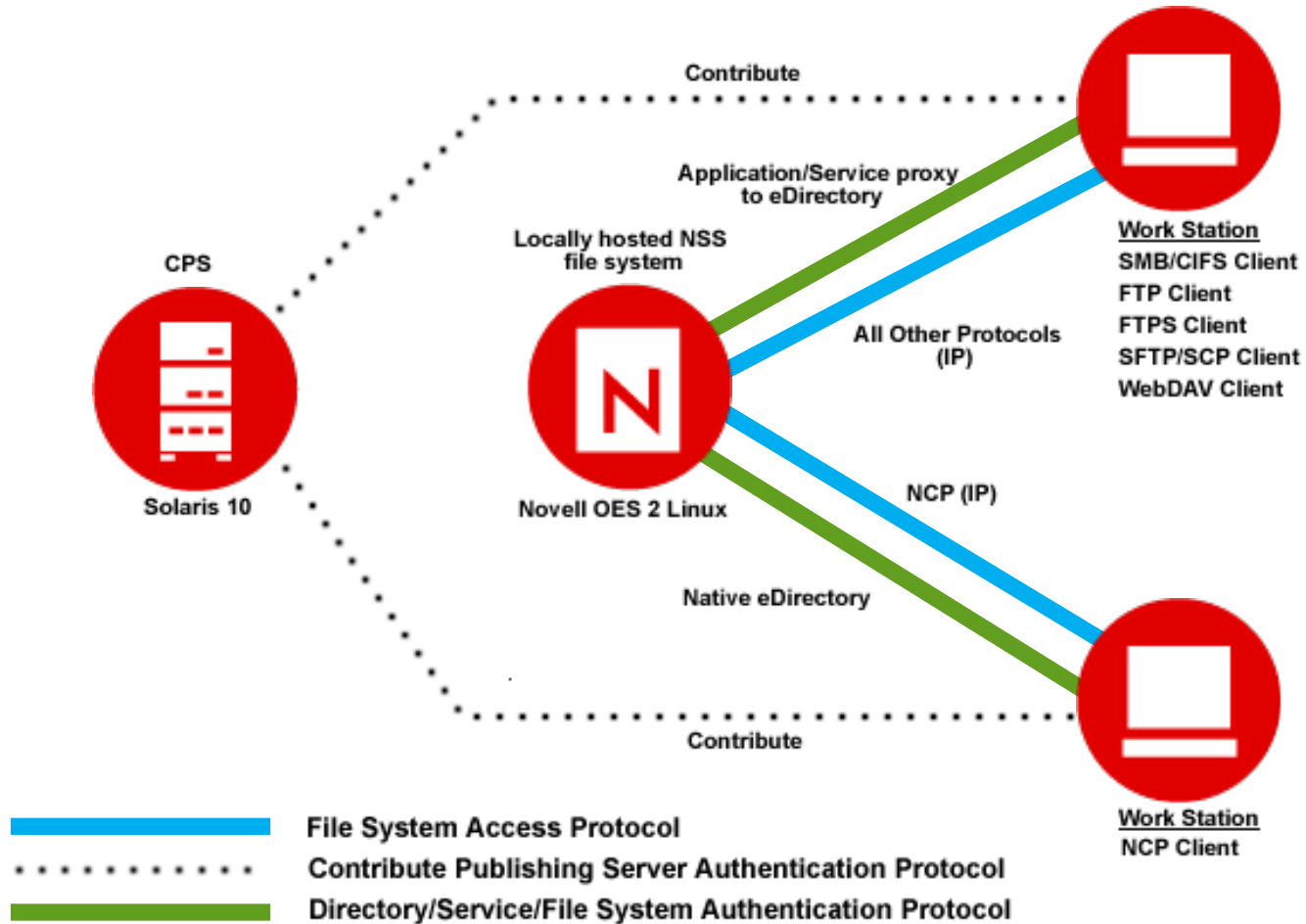
- Adobe Contribute Publishing Server
 - “Less Invasive”
 - Plays well with eDirectory™
 - Control over user permissions
 - Workflow management
 - User activity tracking
- Adobe Contribute
 - WYSIWYG client puts web publishing within easy reach of our average business users
- Adobe Dreamweaver
 - Preferred client for our intermediate and advanced users

The path to Open Enterprise Server 2

Logical Steps

- Research
 - Will Apache use NSS?
- Research
 - Will Apache use eDirectory™ and LDAP for all authentication and authorization requests?
- Research
 - Are the publishing applications compatible with above?
- Plan system architecture and perform feasibility study
- Plan implementation and deploy

Basic Architecture



OES 2 key configuration steps

- Novell® Core Protocol (NCP)
- Novell Storage Services™ (NSS)
- Novell Cluster Services™ (NCS)
- Novell Storage Management Services (SMS)
- Novell Linux User Management (LUM)
- File system access protocol (samba, SFTP, FTPS,webdav) configuration and enterprise optimization
- Novell services (NetStorage and Quickfinder server)
- Apache and Tomcat (LUM configuration, service customization, and enterprise optimization)
- Specialized eDirectory™ components (customized from defaults)
- Clustering applications and services
- Benchmarking and testing

The background is a solid blue color with a pattern of diagonal lines in various shades of blue, creating a sense of movement and depth. The lines are most prominent on the right side and fade towards the left.

Power to the people

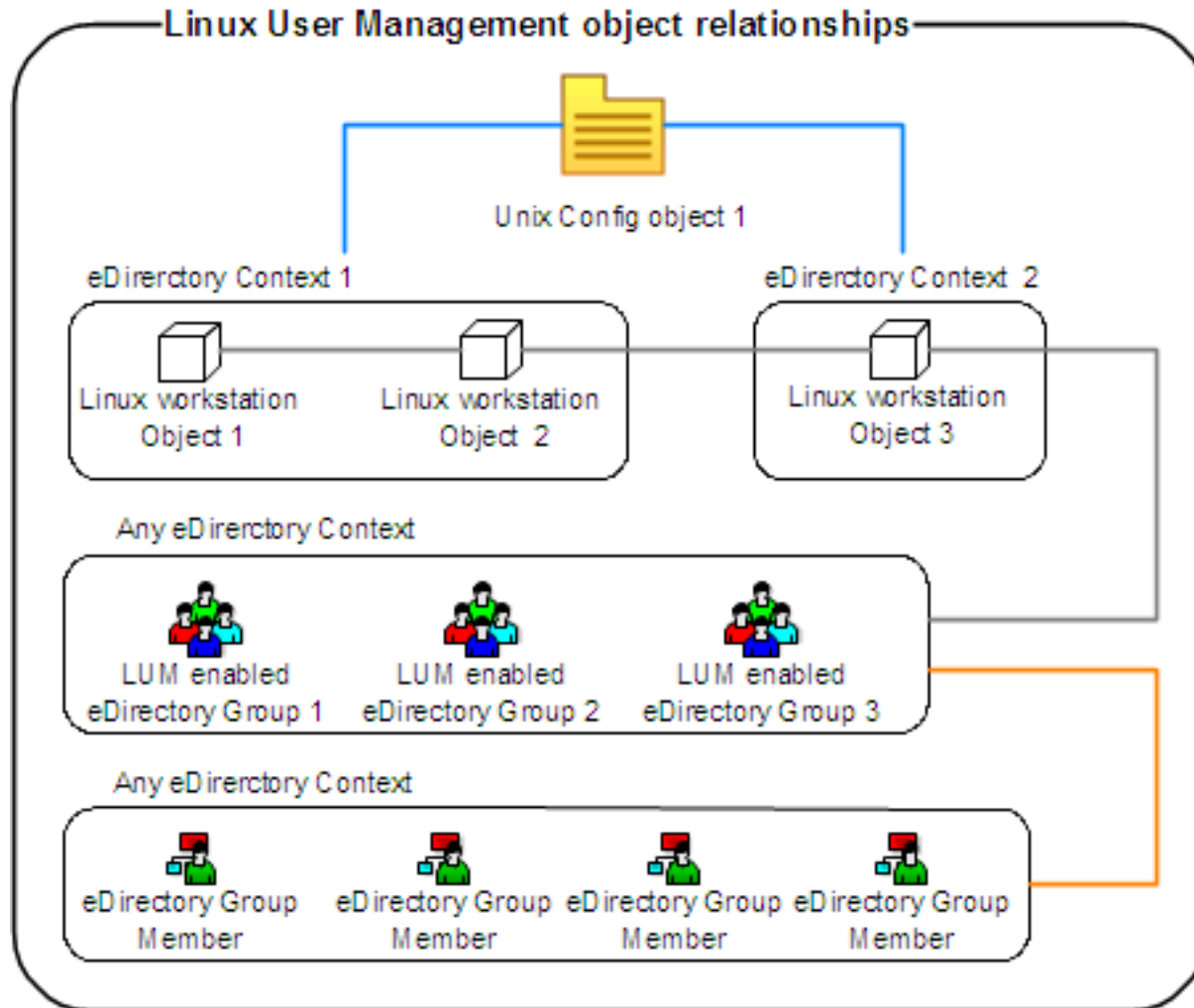
Provisioning Publishing Users

- Prerequisites
 - User must have an eDirectory™ account in the eDirectory tree hosting the target services
 - User must have file system rights to the volume(s) containing managed published content
 - User's eDirectory account must be LUM, and possibly samba, enabled
 - > Adds POSIX and samba attributes and values
 - » Allows eDirectory authentication credentials to be used to access OES Linux server resources
 - » Common primary group injects role based service like access control

Linux User Management - LUM

- Directory-enabled application which centralizes the storage and management of Linux user accounts
 - Uses eDirectory™ for the back-end repository of users
 - Benefits from the security, scalability and reliability that eDirectory users have come to expect.
 - > Unique UIDs and GIDs across the LDAP tree, or LUM domain
 - > Advanced server access control based on LDAP access control lists (ACLs) in eDirectory
 - > Refined LDAP searches offering a more effective integration with eDirectory

Linux User Management - LUM



The background of the slide is a solid blue color with a pattern of diagonal lines in various shades of blue, creating a sense of motion and depth. The lines are most prominent on the right side and fade towards the left.

Who's in the band?

File system access configuration (authorization included.. no charge)

- In Band

- Any file system access protocol used to write to the web file system that honors our publishing workflow system (CPS) and the file system ACL model is considered to be in band.

- > Remember, PC, Mac, and Linux

- Out of Band

- Any other file system protocol used to write to the web file system is considered out of band, even if the file system ACL model is honored

- > Useful to quickly correct or mitigate content issues resulting from publishing errors, attacks that impact web content, or even allow key users to respond to publishing needs for absentee publishers.

Who's in our bands?

- In
 - SFTP
 - FTP (But we don't let him play)

- Out
 - Local/Network (Novell client access (NCP))
 - > Technically still out of band, but this method does honor the document “check in” and “check out” features native to the web publishing client. Its use is limited to select users and admins. This access method is not advertised to other users.
 - NetStorage (WebDAV), FTPS, SCP, and Samba
 - > The use of these access methods is limited to select users and admins. This access method is also not advertised to other users.

Band photo

File transfer protocol access model

"In band" Publishing	
<u>File transfer protocol</u>	<u>Clients</u>
Local network	Dreamweaver
FTP	Dreamweaver Contribute
SFTP	Dreamweaver Contribute
"Out of band" Publishing	
<u>File transfer protocol</u>	<u>Clients</u>
Local network	Dreamweaver Novell Client
WebDAV	Dreamweaver /WebDrive NetStorage
FTPS	Dreamweaver /WebDrive Most FTP clients
SCP	Most SSH clients
Samba/CIFS	Dreamweaver Microsoft Windows Macintosh 10.x Linux

- Honors CPS work flow and file systems ACLS
- Honors file systems ACLS

Summary and Questions

- What we learned about OES Linux evolution, interoperability, and support services.
- What we saved in administrative, implementation, operational, and management resources.
- What the university gained in web services, web based promotion, and web service reliability.
- Solution may be implemented at other campus'.
- Questions....

Novell.[®]

Unpublished Work of Novell, Inc. All Rights Reserved.

This work is an unpublished work and contains confidential, proprietary, and trade secret information of Novell, Inc. Access to this work is restricted to Novell employees who have a need to know to perform tasks within the scope of their assignments. No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of Novell, Inc. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

General Disclaimer

This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. Novell, Inc. makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The development, release, and timing of features or functionality described for Novell products remains at the sole discretion of Novell. Further, Novell, Inc. reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All Novell marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.

