Managing Enterprise Services

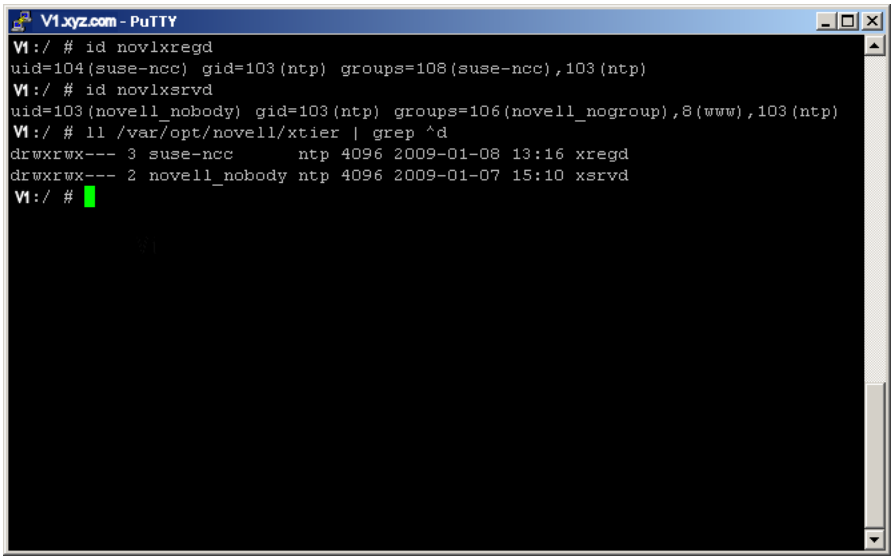
Spanning a Linux User Management configuration

This chapter sample describes key components of the Novell Linux User Management (LUM) service that may require implementation and management standards in an enterprise environment. In a nutshell LUM brings the eDirectory feature set to the Linux account management realm. This includes provisioning, authentication, authorization, and even password policy support to name but a few.

One key behavior to be aware of when architecting and managing your LUM implementation is the fact that local UID and GID values are given preference in the event of a conflict with accounts stored in eDirectory. For example, a conflict occurs when a LUM based account is presented to a local server and the UID or GID value stored in eDirectory is the same as the local account. In this scenario the eDirectory based account will assume the identity of the local account that is assigned the conflicting UID or GID value on that server.

One possible end result of this behavior could be that LUM enabled accounts used for OES services on a given server could have their file permissions aligned with the local entity that shares the UID or GID.

Consider the following:



When this scenario occurs with key OES Linux system users there is a chance that hosted services may not function predictably or even at all. It is even possible that the security of the service, and other services, may be compromised if it's local UID or GID assignment is shared with another user or group. This is the case in the example given for the NetStorage service.

One possible solution for large scale LUM deployments would be to architect a LUM infrastructure. The design goals for this infrastructure would be that it scale easily, be flexible enough to meet operational needs of the organization, and allow groups of servers to share a common configuration. By utilizing eDirectory object placement, naming, and uidNumber/gidNumber attribute standards a LUM infrastructure could be designed to satisfy those design goals.

Another key component in managing such an infrastructure will be developing procedures for mitigating and correcting instances where these inconsistencies can and do occur.

Linux User Management service details examined

Linux User Management allows OES Linux users to be created, managed, authenticated, and authorized using eDirectory. Some Novell services require LUM components to enable them to consume both eDirectory and local OES Linux resources and services.

For example, when Novell Storage Services (NSS) is installed on the Linux server, some system users are removed from the local Linux user store and re-created as LUM-enabled users in eDirectory. This is required because these users must have access to NSS data, and all NSS access is controlled through eDirectory. A list of common OES Linux applications and their respective system user is listed below.

Application	Runs as		Service can utilize LUM
Apache	wwwrun		Yes
iFolder 2	wwwrun		Yes
iFolder 3	wwwrun		Yes
iPrint	iprint		
OpenWBEM	novell_nobody		
Tomcat 4	novlwww		Yes
Tomcat 5	tomcat		
eGuide	novlwww, tomcat	** Dependant on OES Linux version	Yes
Quickfinder	wwwrun		Yes
iManager	novlwww, tomcat	** Dependant on OES Linux version	Yes
NetStorage	wwwrun		Yes
Virtual Office	novlwww, tomcat	** Dependant on OES Linux version	Yes

** NetStorage uses the xTier middle-tier server for authentication and session management. XTier consists of two daemons, novlxsrvd (Novell Xtier Service daemon) and novlxregd (Novell xTier Registry daemon) who have their own users and group. These are named novlxsrvd, novlxregd, and novlxtier respectfully.

** User novlxsrvd is in the www group because it needs access to an Apache domain socket

** QuickFinder requires that all users who manage the service, including the eDirectory Admin user, belong to the www group.

Novell Registry Access Control

Access control to the registry is usually enforced by the operating system.

On Windows, each branch of the registry can have its own access control list (ACL). Windows checks to see if the calling thread has permissions to read/write/modify the registry entry being accessed, and returns status appropriately.

On NetWare, local access to the registry is a trusted operation, and any NLM running on the server is allowed access.

On Linux, Novell XTier has implemented its own registry based on XFLAIM and access to this database is via UNIX domain sockets. Only XTier's LUM enabled registry user (novlxregd) and group (novlxtier) have access to these domain sockets, and access control is enforced via file system permissions. For any process to access the Novell registry on OES Linux servers, the user associated with the process must be a member of the LUM enabled novlxtier group.

WARNING: Do not store security-sensitive information in the registry. Sensitive information such as passwords should not be stored in the registry unless it is protected by strong encryption.

LUM command line utility notes:

Managing LUM users is usually accomplished in iManager or by using the namx commands from the command line **(namuseradd**, **namgroupadd**, etc).

It is often useful to know what users can currently access a server or workstation. One option is to use **namuserlist**. For example, running **namuserlist** with the context o=novell yields the following:

namuserlist -x o=novell
admin:x:600:600::/home/admin:/bin/bash
jbrown:x:603:600::/home/jbrown:/bin/bash

The only limitation with **namuserlist** is needing to know the context to look for user objects. **namuserlis**t also only lists the users in eDirectory. The command **getent** will display all the local and eDirectory users the system knows about.

The **getent** command can also display known user information. Running **getent passwd or getent group** displays all of the users and groups on the system including those that are LUM enabled.