Pls link to this from:

1. http://www.likewise.com/resources/documentation_library/#case

2. http://www.likewise.com/resources/case_studies/index.php With this desc:

This case study describes how a company deployed Likewise Enterprise to integrate IBM AIX and Red Hat Linux machines with Windows computers and Active Directory.

3. http://www.likewise.com/products/likewise_enterprise/Linux-Active-Directory-Integration.php

as

Learn more about AIX Active Directory integration.

==========
KEYWORDS:
Red Hat Windows integration,
RHEL Windows integration,
AIX Active Directory,
AIX Windows integration,
logon rights group policy,
AIX group policy,
identity management system

DESC:
This case study describes how a company deployed Likewise Enterprise to integrate IBM AIX and Red Hat Linux machines with Windows computers and Active Directory.

<link rel="schema.DC" href="http://purl.org/dc/elements/1.1/">
<meta name="DC.title" content="Case Study: Integrating Red Hat and AIX with Windows and Active Directory">
<meta name="DC.description" content="This case study describes how a company deployed Likewise Enterprise to integrate IBM AIX and Red Hat Linux machines with Windows computers and Active Directory.">
<meta name="DC.subject" content="AIX Active Directory,
AIX Windows integration,
logon rights group policy,
red hat windows integration,
rhel windows integration,
identity management system">
<meta name="DC.language" scheme="ISO639-1" content="en">

TITLE:

Case Study: Energy Company Achieves Red Hat Windows Integration

SUBTITLE:

Likewise Connects RHEL and IBM AIX with Active Directory

PROFILE
The company, a large producer of natural gas, focuses on developmental drilling and property acquisitions in several regions of the United States. The company uses hundreds of computers running Red Hat Enterprise Linux versions 3, 4, and 5 as well as a number of large IBM AIX servers with 15-plus network cards each. In addition, many of company's 4,300 employees work on Microsoft Windows computers managed with Microsoft Active Directory.

SITUATION
On its Red Hat machines, the company had standardized user names but had not standardized user IDs (UIDs). Each Linux user was authenticated locally by using the /etc/passwd file on the machine. Accounts on local machines were created as needed. Because each user did not have an account on each Linux computer, system administrators had to run the local useradd utility every time a user needed to access a machine on which the user did not have an account. The local utility was used to create the user's name, home directory, shell, and password in the /etc/passwd file.

NO CONSISTENCY ACROSS PLATFORMS
Authenticating users with the /etc/passwd file meant that each Linux computer was in effect running its own identity management system: Users who have access to multiple computers must maintain their passwords on each computer. When they have to change passwords, they must do so on every computer -- a time-consuming, error-prone process that can leave security holes. More: Every time a user joins or leaves the company, the user must be manually added to or removed from every Linux computer. Meantime, to bypass the burdensome task of maintaining their passwords, some administrators used the root account, an insecure practice that runs counter to accepted security standards and regulations.

Administrators who did not have root access and had not already been provisioned with user access to a server were at a loss when they had to troubleshoot an emergency issue -- they had to first get someone with root access to provision them with an account.

On the company's AIX servers, the situation was slightly different. The users had standardized IDs, but because of the default 8-character AIX limit on user names, user names consisted of only the first 8 characters of each user's full Windows user name -- discrepancies that posed major problems in migrating to a system with uniform user names and IDs.

MOTIVATION FOR USING LIKEWISE ENTERPRISE
The result of managing user access to hundreds of Linux and AIX machines on an ad hoc, computer-by-computer basis with /etc/passwd files can be summed up in one word: drudgery. Administrators were overwhelmed trying to keep it all working properly and securely. In implementing Likewise Enterprise, management's objective was straightforward: To make their system administrators happy.

SOLUTION

The company deployed Likewise Enterprise to all their IBM AIX and Red Hat Linux machines and joined them to Active Directory. The company hired Likewise Professional Services to migrate the machines to Active Directory, consolidate UIDs for the Red Hat machines, and provide user training. Likewise documentation explained how to extend the AIX user names beyond 8 characters so that the user names for AIX could match those of Windows.

In Active Directory, the company used Likewise cell technology to create two cells, one for its city headquarters and another for a town where it has operations. Each cell contains a test, development, and production environment. And each environment contains cells for each type of the company's application servers -- Oracle, PeopleSoft, etc. With these Likewise cells, the company can now manage its servers not only by location and environment but also by application.

To control access to the Linux and AIX servers, the company deployed Likewise's allow_logon_rights group policy. The policy includes the groups that are allowed to access servers by location, environment, and type.

The tyranny of managing hundreds of /etc/passwd files on an ad hoc, computer-by-computer basis was over: By using Likewise to join Linux and Unix computers to Active Directory, the company could now centrally manage user names and IDs in Active Directory in a uniform and consistent way. Local user accounts on Red Hat and AIX were retired.

The need for root access was reduced. Instead of letting system administrators use root, the Likewise group policy for sudo delegated authority to system administrators so they could run root commands without logging in as root.

The company also used a Likewise group policy to display a message giving users a phone number to call for help when their logon rights were denied. Another Likewise group policy warned users 14 days before their passwords expired.

BENEFITS

In general, implementing Likewise Enterprise improved security and saved the time and resources of system administrators. The company benefited in a number of concrete ways, including the following:

*Migrating /etc/passwd files to Active Directory centralized the management of user names and passwords, freeing system administrators from the time-consuming burden of managing user names and passwords on a computer-by-computer basis.
*Joining machines to Active Directory made each user's name, ID, and password consistent across Linux, AIX, and Windows computers, making it easier to manage users and control access.
*Using Likewise cells and group policies improved access control and security.
*Deploying Likewise's sudo group policy improved security and regulatory compliance by eliminating the need for system administrators to log on with root accounts.
*Using a Likewise group policy to display a message before passwords expired reduced calls to the help desk for password resets.