

eProvisioning

by Cheryl Walton

Get Your Business in Hand

Does the word *eProvisioning* mean anything to you yet? In its simplest sense, eProvisioning is a technology—or more accurately, an intersection of technologies—designed to provide your company's employees, business partners, suppliers, and customers with precisely what they need precisely when they need it.

eProvisioning automates business processes to dramatically reduce the amount of time it takes a user to acquire the tools and network access needed to ply his or her trade. This user can be an employee or anyone with whom your company wants to do business. The tools this user needs can include anything from an e-mail account to a PC to a corporate credit card.

To automate business processes, eProvisioning systems integrate electronic systems that currently cannot share information. For example, an eProvisioning system can integrate your company's customer relationship management (CRM) system with its supply chain management (SCM) system. The CRM system can then notify the SCM system about how many products customers have ordered. (By integrating these two systems, your company can automate the process of purchasing production materials based on customer orders.)

eProvisioning systems can also automate manual processes such as the process of authorizing employee credit cards. Automating electronic and manual business processes can give your company a competitive advantage. For example, an eProvisioning system can cut the amount of time your company takes to make a newly hired employee productive from a matter of hours (or even days or weeks) to a matter of minutes.

Decreasing the amount of time it takes to make new employees productive can result in "a huge return on investment" for companies that implement eProvisioning systems, explains Phil Schacter, a network strategy service director for The Burton Group. (The Burton Group specializes in networking analysis, research, and consulting. For more information about The Burton Group, visit www.tbg.com.)

eProvisioning systems also reduce the burden and cost of managing a host of business systems separately. For example, an eProvisioning system can use the information in a human resource management (HRM) system to create user accounts in an e-mail system. Because eProvisioning systems can automate the process of creating user accounts in various systems, your company can potentially pay only one person to enter and maintain user information in one place.

As you may expect, the more users your company adds to its network, the greater the payoff your company can expect from implementing an eProvisioning

system. In fact, large companies may need to implement eProvisioning systems just to stay competitive.

If you work for a large company or if your company plans to add a large number of customers, suppliers, or partners to its network, your future as an IT professional may include managing an eProvisioning system. In this eventuality, the bad news is that you may be responsible for information that is currently someone else's responsibility. The good news is that if your company implements Novell's eProvisioning Solution Framework, managing this eProvisioning system probably won't increase your workload. In fact, Jack Mullins, a service line manager for Novell Consulting, says that implementing Novell's eProvisioning Solution Framework may actually decrease your workload.

THE FIRST STEP TO SUCCESS

Novell's eProvisioning Solution Framework is a customized



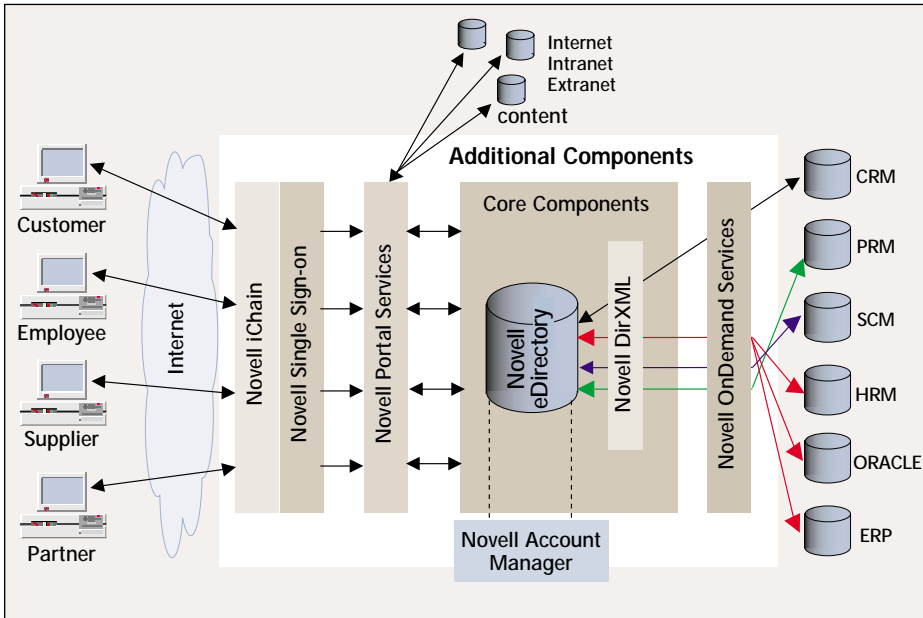


Figure 1. Novell eDirectory and Novell DirXML are at the core of every implementation of Novell's eProvisioning Solution Framework. Depending on your company's particular eProvisioning needs, Novell Consulting builds upon this core by adding additional components.

eProvisioning solution that includes Novell and partner software and Novell and partner consulting. Because Novell's eProvisioning Solution Framework is not a red-box product, it is available only through your company's Novell representative, Novell Consulting, or Novell partner consulting firms such as Cambridge Technology Partners (www.ctp.com), Cap Gemini Ernst & Young (www.cgey.com), and Deloitte Touche Tohmatsu (www.deloitte.com). (Cambridge Technology Partners, a Novell subsidiary, is a business management consulting and systems integration firm. Cap Gemini Ernst & Young is a management and IT consulting firm. Deloitte Touche Tohmatsu is a business assurance and advisory, tax, and consulting firm.)

Novell Consulting works with partner consulting firms to design an eProvisioning solution that meets your company's particular needs. To design this customized solution, these partner firms and Novell Consulting first assess and document the business processes and practices in which your company is currently engaged.

This assessment is the first step toward implementing your company's eProvisioning Solution Framework. Hence, Novell's consulting partners are "a very critical component" in Novell's solution, Tyler Crowder, a Net solutions campaign manager for Novell, explains. (For more information about the role Novell partner

consulting firms play in Novell's eProvisioning solution, see "Novell Consulting Consults the Consultants" on p. 10.)

AN EPROVISIONING SOLUTION THAT LETS YOU PICK AND CHOOSE

The second step toward implementing your company's eProvisioning Solution Framework is deploying the solution. With Novell's eProvisioning Solution Framework, you can plan and then deploy this solution in stages, rather than having to plan and deploy a full-blown eProvisioning system all at once. Depending on your needs, you can begin implementing one or more of the following types of Novell eProvisioning implementations:

- Employee implementation
- Customer implementation
- Partner implementation
- Supplier implementation

An Employee Implementation

An employee implementation of Novell's eProvisioning Solution Framework is an infrastructure that automates the process of creating, deleting, and synchronizing employee information across your company's systems and applications. For example, an employee implementation can automate the process of creating, deleting, and synchronizing user accounts across your company's directories such as

Novell eDirectory, Windows domains, Active Directory, and directories running on Linux and Solaris servers. An employee implementation can also automate user-account processes in your company's e-mail system and the applications employees need on the job.

An employee implementation can also automate manual processes or tasks, such as the process of providing new employees with a telephone, PC, mobile phone, and badge. To automate manual processes, Novell Consulting incorporates these processes into a workflow system, such as Metastorm e-work. (Metastorm e-work is a business process automation tool. For more information about e-work, see the flash demonstration at www.metastorm.com/products/overview_index.asp. For more information about how Novell's eProvisioning Solution Framework uses e-work, see "e-work Your Business Processes" on p. 16.) By automating these processes, an employee implementation can increase worker productivity.

In addition, an employee implementation can strengthen security. With an employee implementation, your company's employees have access to all of the information and applications that they need the moment they report for their first day on the job. Conversely, an employee implementation revokes this access the moment your company terminates this employee's employment (and thus disables this employee's user account in eDirectory).

A Customer Implementation

A customer implementation of Novell's eProvisioning Solution Framework is an infrastructure that automates the process of providing customers with the information and services that they need when they need them. For example, a customer implementation can provide a customer with up-to-the-minute tracking information on his or her account balance.

A customer implementation can also customize the presentation of information and services based on customer preferences. For example, Novell and its partners created a customer eProvisioning solution that enables CNN Interactive's visitors to indicate the types of news and events that interest them most. The solution then uses this information to create a personalized version of the news for each visitor.

Novell Consulting Consults the Consultants

To ensure that your company's eProvisioning solution is exactly what your particular company needs, Novell relies on partner consulting, advisory, and IT services firms such as Cambridge Technology Partners (www.ctp.com), Cap Gemini Ernst & Young (www.cgey.com), Deloitte Touche Tohmatsu (www.deloitte.com), KPMG (www.kpmg.com), and PricewaterhouseCoopers (www.pricewaterhousecoopers.com). These partner companies play a crucial role in designing Novell's eProvisioning Solution Framework by documenting the business processes in which your company is currently engaged. For example, if your company needs an employee implementation, a Novell partner company may document and assess the steps that your company takes to recruit, hire, and then provision new employees.

Novell partner companies "go through all of the different business rules and document what those rules are," Jack Mullins, a service line manager for Novell Consulting, explains. The partner companies then turn these business rules over to Novell consultants, who use these rules to customize Novell DirXML drivers,

which can help automate the processes that the business rules describe. (For more information about the role DirXML plays in Novell's eProvisioning Solution Framework, see the "DirXML: Because Cyberspace Is Not a Perfect Place" section on p. 12 of the main article.)

Novell partner companies are also often experts in business software and use this expertise to help Novell implement key parts of its eProvisioning Solution Framework. For example, Deloitte Touche Tohmatsu used its PeopleSoft expertise to help Novell Consulting build a large banking firm's employee implementation. (To view the eProvisioning success stories of other Novell customer companies, visit http://developer.novell.com/nss/nss_esolution.jsp?solutionKey=7464.)

Specifically, Deloitte Touche Tohmatsu configured the PeopleSoft message agent to queue specific types of employee information, which the DirXML Driver for PeopleSoft then pushes to the banking firm's eDirectory identity management tree. (For more information about PeopleSoft, visit www.peoplesoft.com.) This eDirectory identity management tree serves as an identity vault for users on the banking firm's network. ●

Partner and Supplier Implementation

A partner implementation of Novell's eProvisioning Solution Framework is an infrastructure that can automatically provide your company's business partners with information and services that partners need. Similarly, a supplier implementation of Novell's eProvisioning Solution Framework can provide your company's suppliers with information and services they need.

For example, if your company manufactures automobiles, a partner implementation can provide the automobile dealerships that sell these automobiles with access to information about automobile availability and price. With a supplier implementation, your company can also provide parts manufacturers with its latest production schedules. These manufacturers can then deliver parts where and when your company needs them.

The infrastructures for these implementations have at least two quintessential examples of Net services software in common—Novell eDirectory and Novell DirXML.

EDIRECTORY SUITS EPROVISIONING TO A T

Directory-based eProvisioning systems—particularly Novell's eProvisioning Solution Framework—have clear advantages over eProvisioning systems that are not directory based. By storing and managing user identities, directory-based eProvisioning systems can put users at the

center of your e-business strategy. You can then use these identities to control users' access to your company's network.

That is, directory-based eProvisioning systems can provide role-based, rules-based access to your company's network. With non-directory-based eProvisioning systems, on the other hand, you may need to manage user access to these systems through other, less efficient means such as access control lists (ACLs).

Of course, not all directories are equally capable of providing a foundation for an eProvisioning system. For example, according to a Gartner Group report called "Directory, Security and Provisioning Services: Foundation for E-Business," directories that support Lightweight Directory Access Protocol (LDAP) provide a better foundation for eProvisioning systems than directories that don't support LDAP. (Novell commissioned this report from Gartner Consulting. For more information about Gartner, visit www.gartner.com.)

LDAP directories store identity information that LDAP-enabled applications can access directly. Because these applications can access LDAP-compliant directories natively, an eProvisioning system that is based on an LDAP-compliant directory doesn't require specialized code to enable that access. Using an LDAP-compliant directory and LDAP-compliant applications can therefore simplify and accelerate the process of implementing an eProvisioning system.

In addition, directories that can accommodate a large number of objects—such as 100,000 or more objects—provide stronger foundations for eProvisioning systems than directories that can handle only a small number of objects. After all, an implied reason for implementing an eProvisioning system is to provide the scalability to conduct e-business. The more business partners, suppliers, customers, and employees your company adds to its network, the more your company benefits from automating the processes that provide these users with the tools they need.

Assuming that you are familiar with eDirectory, you probably know that it fits the definition of an eProvisioning-capable directory to a T. That is, eDirectory is fully compliant with LDAP 3, the most recent version of the LDAP standard. In addition, eDirectory can accommodate millions—even billions—of objects.

eDirectory also has an extensible schema: You can add objects and attributes that enable eDirectory to manage complex user identities. As a result, eDirectory can distinguish important differences between users. For example, eDirectory can distinguish the difference between users who are employees and users who are suppliers. eDirectory can then grant these users access to network resources accordingly.

In addition, eDirectory is cross-platform, so you can run the eDirectory tree that lies at the heart of Novell's

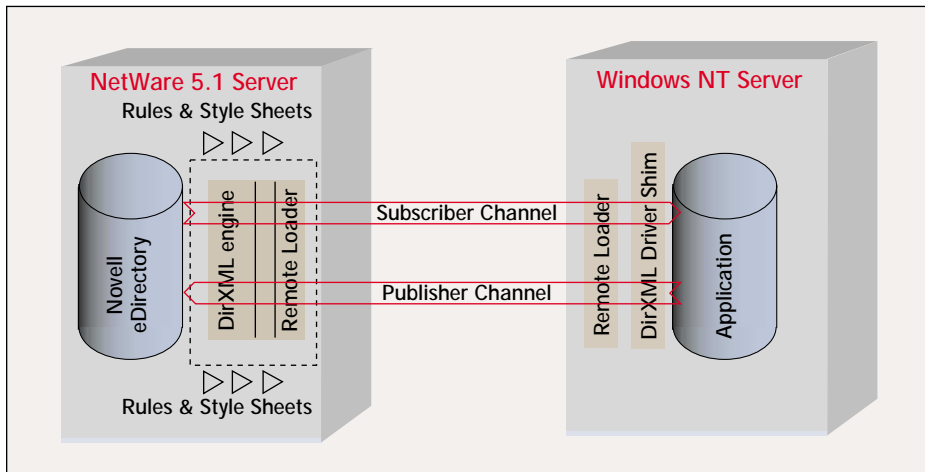


Figure 2. DirXML 1.1 will include a remote loader, which gives you the option of running the DirXML engine and Novell eDirectory on any server that eDirectory supports, regardless of a particular application's API restrictions.

eProvisioning Solution Framework on virtually any platform that makes sense for your particular company. Novell Consulting creates this eDirectory tree to function as a “separate identity vault” that stores “all sorts of user information,” Mullins explains. (eDirectory 8.5—the version of eDirectory upon which Novell currently bases its eProvisioning Solution Framework—runs on NetWare 5.1, Windows 2000 and NT, Linux, Solaris, Tru64 UNIX, and AIX. For more information about eDirectory, visit www.novell.com/products/nds.)

DIRXML: BECAUSE CYBERSPACE IS NOT A PERFECT PLACE

In a perfect world, all applications would be LDAP enabled and all directories would be both LDAP enabled and cross-platform. Novell could simply use a dedicated eDirectory tree to manage user access for its entire eProvisioning Solution Framework, and every application could use eDirectory as its authoritative source for user authentication and authorization. You would create only one user account to give a particular user access to every application that he or she needs. In other words, if the computing world were a perfect place, using standards-based software alone would enable you to provision users with the electronic information and applications they need.

Precisely because the world of network computing is far from perfect, the other core component of Novell's eProvisioning Solution Framework is Novell DirXML. DirXML is a data-sharing tool that—as its name implies—uses eXten-

sible Markup Language (XML) and eDirectory to synchronize common data that reside in the directories and applications across your company's network. For example, DirXML can push a user's updated job title from your company's HRM application to the eDirectory identity management tree. (The eDirectory identity management tree is an eDirectory tree that is dedicated to managing the eProvisioning solution.)

To determine exactly what information gets pushed from a particular application to eDirectory (or vice versa), you create filters on the publisher and subscriber channels for application-specific DirXML drivers. These filters are XML documents that describe the data that can flow from the application to eDirectory and the data that can flow from eDirectory to the application. (For more information about XML, visit www.w3c.org/xml.)

For example, you can create a filter that includes an attribute for job titles. You create this filter on the publisher channel for the HRM DirXML driver. If a job title changes in the HRM application, the HRM DirXML driver then pushes that change to the eDirectory identity management tree.

Similarly, you can create a filter for telephone numbers. You create this filter on the subscriber channel for the HRM DirXML driver. When someone updates a telephone number in the eDirectory identity management tree, the HRM DirXML driver then pushes this change to the HRM application.

DirXML drivers also include application-specific shims, which use an applica-

tion's native application program interface (API) to receive changes from that application through the publisher channel. In addition, DirXML uses these shims to push changes in eDirectory to the application through the subscriber channel.

With DirXML 1.0, if an application includes an API set that you cannot access remotely, you must run a DirXML driver on the same computer that is running the application. For example, PeopleSoft systems run on Windows 2000 or NT servers. Likewise, the PeopleSoft PeopleTools API set can run only on Windows 32-bit servers. As a result, you must run the DirXML driver for PeopleSoft systems on the same Windows 2000 or NT computer that is running the PeopleTools API set. (PeopleTools is an application development environment and API set through which you can access or make changes to PeopleSoft systems. For more information about PeopleSoft, visit www.peoplesoft.com.)

Furthermore, you must run these drivers on a machine that is also running eDirectory and the DirXML engine. In other words, if you want to use DirXML 1.0 to synchronize information between your company's PeopleSoft HRM system database and the eDirectory identity management tree, that tree must be running on the Windows 2000 or NT server that is running PeopleTools.

Note: This server does not need to hold the root partition of the eDirectory tree. This server can hold the master replica or a read-write replica of the eDirectory tree.

The next release of DirXML (version 1.1) enables you to run eDirectory and the DirXML engine on any platform eDirectory supports, regardless of API restraints that certain applications impose. See Figure 2. (DirXML 1.1 will be released soon. For more information, see “DirXML 1:1: Synching With Style,” on p. 40.) In other words, if you use DirXML 1.1 to synchronize information between PeopleSoft and eDirectory, you can run PeopleSoft on a Windows NT server and the eDirectory engine on an entirely different server, such as a NetWare 5.1 server. (For more information about DirXML, see “Too Many Directories? Synch 'Em With DirXML” and “Check Out That DirXML Engine,” *Novell Connection*, May 2000. You can download these articles from www.ncmag.com/past.)

NDS SPREAD
NEW ELECTRONIC FILE

e-work Your Business Processes

Novell Consulting uses Novell eDirectory, Novell DirXML, and other Novell products to provision users with IT-based information and services. If this information and these services require prior authorization, however, Novell Consulting will probably use Metastorm e-work to automate the authorization process.

“DirXML can do very, very well with automating at a system level as long as there are no specific manager approvals that exist within” the business process that needs to be automated, Tyler Crowder, Novell Net solutions campaign manager, explains. “Metastorm e-work comes into play to help automate approval-oriented business processes.”

Novell Consulting also uses e-work to automate other, non-IT-based manual business processes, such as the process of getting approvals to open a job requisition or providing new employees with a desk, mobile phone, and PC. For example, Novell uses e-work in Zero-Day Start (which is Novell’s internal employee implementation of the eProvisioning Solution Framework) to automate the process of hiring new employees.

As Mark Reed, senior business development manager for Metastorm, explains, “e-work is a business process automation tool or workflow tool” that includes the e-work Designer. The e-work Designer, which is a graphical tool for mapping business processes, includes a forms creation tool for creating business forms. You use these tools to create applications that can automate your company’s particular manual business processes. In other words, Reed adds, e-work is “primarily a rapid application development platform. It doesn’t necessarily do anything out of the box.”

e-work runs on Windows 2000 and NT and integrates with Novell eDirectory via Novell DirXML or Metastorm’s data extraction utility. e-work works with NDS 8.0 or above. The integration between e-work and eDirectory allows companies to manage the users and roles within e-work. In addition, e-work can prepopulate business forms with identity information that is stored in eDirectory. e-work also integrates with Novell GroupWise 5.5 or above and Microsoft Outlook 98 or above.

FOR EXAMPLE?

The following example demonstrates how Novell Consulting may deploy an e-work application to automate the task of requesting and granting leave time:

Novell Consulting or a partner consulting company documents the company’s leave-time procedures and policies. Novell Consulting then uses the e-work Designer to create a process map. This map reflects the business rules that determine how this leave-time information will progress through the e-work applica-

tion when a user submits a request for leave.

Novell Consulting uses the Designer’s forms creation tool to create a leave request form that pulls information from an eDirectory identity vault to prepopulate selected fields on this form. After Novell Consulting creates this map and the leave request form, Novell Consulting publishes the resulting e-work procedure, which automatically creates the new e-work leave request application.

This e-work application may enable the following process:

1. A user opens GroupWise and selects the e-work Forms folder from the GroupWise navigation bar or toolbar. e-work displays a list of forms that are available to the user, based on that user’s identity in the eDirectory identity management tree.
2. The user requests the Leave Request form. e-work then displays that form, which includes fields that are prepopulated with identity information, such as the employee’s name and job title.
3. e-work uses Open Database Connectivity (ODBC) to query a PeopleSoft human resource management (HRM) system for the employee’s available leave time. e-work then populates the Available Leave Time field of the Leave Request form with this information.
4. The employee requests leave from October 29 to October 31 and submits the Leave Request form.
5. e-work then routes this form to the employee’s supervisor for approval. This form then appears on the supervisor’s e-work To Do List.
6. The supervisor opens the form, reads it, and approves the leave request by clicking the Submit button.
7. e-work sends a message to the employee’s GroupWise e-mail box, explaining that the employee’s leave request has been approved. e-work also routes the approved Leave Request form to an HR department clerk’s e-work To Do list.
8. This clerk opens and reads the form.
9. The clerk then deletes 24 hours from the employee’s available leave in the PeopleSoft HRM database. (If the company’s policies allowed it, e-work could automatically delete the time from the PeopleSoft database, without this clerk’s intervention.)

e-work also has tracking capabilities that enable you to see exactly how a particular business process is progressing. You can also configure e-work to escalate a task—that is, route the task to another person—if the person to whom this task is assigned does not complete the task in a specified amount of time. (For another example of how you can use e-work to automate business processes, see the flash demonstration at www.metastorm.com/products/overview_index.asp.) ●

THE WAY THEY DO THE THINGS THEY DO

Novell’s eProvisioning Solution Framework uses DirXML to automate the process of creating user accounts. For example, DirXML automates user account creation for Freddie Mac. Novell Consulting and its partners created an employee implementation of Novell’s eProvisioning Solution Framework for Freddie Mac. As

part of this implementation, DirXML automated user account creation based on Freddie Mac’s own business rules and practices. (Of course, consultants from Deloitte Touche Tohmatsu documented Freddie Mac’s business rules and processes as the first step in creating the employee implementation.)

Specifically, based on information that Freddie Mac’s HR department enters into

its PeopleSoft database, DirXML creates new employees in the company’s eDirectory identity management tree. DirXML also creates accounts in the company’s NetWare user directory tree and its Lotus Notes system. The NetWare user directory tree gives users access to information and applications running on Freddie Mac’s NetWare servers. (For more information about Freddie Mac, visit www.

freddiemac.com. For more information about this account creation process, see “Go With the DirXML Flow” on p. 20.)

More importantly, at least from a security perspective, Novell’s eProvisioning Solution Framework uses DirXML to synchronize user information and delete accounts. According to The Burton Group, one-third of the user-related information in the networks of large companies is incorrect. “It’s incredible how much bad data there is out there,” Schacter asserts.

This bad data could conceivably give users access to information and applications that these users should not be able to access. For example, suppose your company hires a new manager and, months later, determines that this manager isn’t capable of performing managerial tasks. Rather than firing this manager, your company offers the manager a demotion, which the manager accepts.

When this employee was a manager, your company’s eProvisioning system automatically granted his or her rights to confidential information, such as employee salaries and bonuses. If your company’s eProvisioning system cannot automatically revoke these rights, this ex-manager may have access to this confidential information for weeks or even months, depending on who is responsible for revoking access to this information and how busy that person is. If the manager were fired and your company’s eProvisioning system couldn’t delete or disable all of his or her accounts, this manager could possibly use those accounts for an extended period of time to undermine the entire company.

By automatically synchronizing your company’s user information across the entire network, DirXML can eliminate the problems bad or outdated data can cause. DirXML can also save your company the cost of hiring extra employees just to synchronize your company’s user data. As Glen Knutti, Novell consultant, says, DirXML is “a money-saving move to keep your data clean and synchronized.”

FLESHING OUT THE BONES

The employee implementation for Freddie Mac also includes Novell eGuide, a web-based application through which users can query and display information from LDAP-compliant directories. eGuide enables Freddie Mac’s 12,000 employees to use a web browser to access selected information (such as names, office extensions, and pager numbers) about their colleagues.

eGuide accesses the eDirectory identity management tree to retrieve this information, which is always as current as the information in Freddie Mac’s PeopleSoft system. The PeopleSoft system is the authoritative source for employee data.

In an employee implementation for a large banking firm, Novell Consulting configured the eDirectory identity management tree as the authoritative source for selected user data. This employee implementation (which automatically provisions resources for the firm’s 30,000 employees) uses DirXML drivers for PeopleSoft to coordinate information from three separate PeopleSoft HRM

By automatically synchronizing your company’s user information across the entire network, DirXML can eliminate the problems bad or outdated data can cause.

systems. In most cases, these PeopleSoft systems provide the authoritative data source for this firm’s eDirectory identity management tree.

However, this banking firm decided that in some cases, the users themselves are the most logical source for authoritative data. “[The banking firm] decided that since users are the best source for their pager numbers and cell phone numbers, the best way to update that information was to let the users do it themselves,” explains John Hartmus, a Novell consultant who worked on this employee implementation.

eGuide can use LDAP calls to write information to directories as well as to read information from directories. Novell Consulting configured eGuide to enable employees to update this information in the eDirectory identity management tree. Novell Consulting then configured DirXML to make the eDirectory identity management tree the authoritative source for this information. (For more information about eGuide, see www.novell.com/products/eguide.)

Enabling users to update their own information makes good economic sense for this company, which spans several countries and includes thousands of users. This decision will make even better economic sense when the banking firm implements the second stage of its eProvisioning solution. The second stage is a customer implementation that expands the company’s network to include more than 6 million users.

Depending on the company’s particular needs, Novell Consulting or its partners will add other Novell products or partner products to this company’s eProvisioning Solution Framework. (See Figure 1 on p. 8.) Novell Consulting may use the following products to expand the capabilities of the company’s present eProvisioning Solution Framework:

- Novell Account Management
- Novell iChain
- Novell SecureLogin
- Novell Modular Authentication Service (NMAS)
- Novell Portal Services
- Novell OnDemand Services

Although a detailed discussion of these products is beyond the scope of this article, a brief description of each product follows.

Novell Account Management: When You Can’t See the Forest for the Trees

In Freddie Mac’s employee implementation, Novell Consulting used a DirXML Driver for eDirectory to push selected information from the eDirectory identity management tree to the NetWare user directory tree. Suppose, however, that Freddie Mac also wanted to synchronize this information with its Windows 2000 and NT servers. Also suppose Freddie Mac wanted to automatically provision accounts on Solaris or Linux servers.

In this case, Novell Consulting could do one of the following two things:

- Novell Consulting could configure the DirXML driver for NT Domain to provision accounts on the company’s Windows NT servers. Novell Consulting could then configure the DirXML driver for LDAP to provision accounts on Linux and Solaris servers that use LDAP-compliant directories for local authentication. Finally, Novell Consulting could create a customized DirXML

Go With the DirXML Flow

As a first step to setting up an employee implementation for Freddie Mac (www.freddiemac.com), consultants from Deloitte Touche Tohmatsu (www.deloitte.com) documented Freddie Mac's business rules and processes. Based on these rules and processes, Novell Consulting used DirXML and Novell eDirectory to automate the process of creating accounts for newly hired Freddie Mac employees. The following is a step-by-step description of the process of creating accounts:

1. The personnel department adds information about a new employee into Freddie Mac's PeopleSoft 7.5 human resource management (HRM) system database. This PeopleSoft system is running on a Windows NT 4 server with Service Pack 6.
2. The PeopleSoft message agent places information about the new employee into a queue, which the DirXML Driver for PeopleSoft regularly polls to find changes to the PeopleSoft database.
3. The DirXML Driver for PeopleSoft, which is running on the same Windows NT 4 server, uses this information (such as the employee's name, date of birth, and job title) to create the user in the Active container in Freddie Mac's eDirectory identity management tree. This identity management tree, which is also running on the same Windows NT 4 server, is an eDirectory 8.5 directory tree that serves as a user identity vault. This identity management tree includes two container objects—an Active container object for current employees and an Inactive container object for employees who have been fired, laid off, or who are on extended leave. Creating an account for the new employee in this identity management tree activates a DirXML Driver for NDS

eDirectory, which is also running on the Windows NT 4 server.

4. The DirXML Driver for NDS eDirectory pushes selected information to the NetWare user eDirectory tree, which is running on Freddie Mac's NetWare 5.1 servers. Only certain parts of the [new employee's] information need to go into the [NetWare user] eDirectory tree," Glenn Knutti, a Novell consultant who worked on Freddie Mac's eProvisioning system, explains. For example, the new employee's office location goes into the NetWare user tree. In fact, this office location determines the container object in which DirXML creates the new employee's account. On the other hand, the new hire's date of birth does not go into this NetWare user eDirectory tree.

After the DirXML Driver for NDS creates an account for the new employee in this NetWare user eDirectory tree, he or she then has access to information and applications on Freddie Mac's network.

5. Creating an account for the new employee in the identity management tree also activates a DirXML Driver for Lotus Notes, which is also running on the Windows NT 4 server.
6. The DirXML Driver for Lotus Notes then creates a place holder in the Lotus Notes name and address book. "All that's created is a record that has the employee number that is created in PeopleSoft when the [new employee] is created in PeopleSoft," Knutti explains. This process activates an internal application that queries PeopleSoft for information that the application then uses to complete the new hire's Lotus Notes account.

Note: Freddie Mac could have used the DirXML Driver for Lotus Notes to create the complete user account in Lotus Notes. The company chose to create Lotus Notes accounts using the method described above. ●

driver to provision user accounts on Freddie Mac's Windows 2000 servers.

As you can imagine, building this solution could be a costly process. Before configuring and creating the DirXML drivers, Novell Consulting and its partners would first need to analyze and document the business rules and processes that define how and when user accounts are created on each platform.

- Novell Consulting could deploy Novell Account Management, which enables you to create and manage user accounts on Windows 2000 and NT, Solaris, and Linux through your company's eDirectory tree. With Novell Account Management, you enter user information once in eDirectory, and Account Management uses that information to create and update user accounts on Windows 2000 and NT, Solaris, and Linux.

By deploying only the DirXML Driver for NDS and Novell Account Management, Freddie Mac could automatically provision user accounts on its NetWare, Windows 2000 and NT, Linux,

and Solaris servers. Specifically, the DirXML Driver for NDS could provision user accounts in Freddie Mac's NetWare user eDirectory tree. Novell Account Management would then use that information to provision user accounts on Windows 2000 and NT, Linux, and Solaris servers. (For more information about Novell Account Management, visit www.novell.com/products/nds/accountmanagement.)

iChain: Law Enforcement for the Net

iChain is a directory-based management product. You can use iChain to enable users to securely access your company's network over the Internet using HTTP. You do not need to set up a virtual private network (VPN). Because iChain is based on eDirectory, iChain also provides granular control over user access to your company's applications and information.

Support for eDirectory and other security features makes iChain "very much a web security system," Crowder ex-

plains. For example, iChain supports Secure Sockets Layer (SSL), allowing you to encrypt data as that data traverses the Internet from your company's network to users' browsers.

You can also configure iChain as an application-level proxy server. As a proxy server, iChain can deliver content—such as applications and information—to Internet users without giving those users access to your company's network. For example, Novell Consulting plans to use iChain when it implements the second stage of the large banking firm's customer implementation. In fact, Novell Consulting plans to configure iChain as a proxy server that delivers all of the applications and information (such as account information) that the banking firm plans to make available to its customers.

To authenticate external users, this proxy server will access an external eDirectory tree running within the company's demilitarized zone (DMZ). (A DMZ can include a server or small

network that exists between a company's internal network and a public network, such as the Internet.) This external eDirectory tree will contain the minimum amount of user information required to provide granular access control to the information and applications that will be available to the bank's six million customers. iChain will then grant authenticated users access to internal information or applications based on those users' profiles in eDirectory.

Through a DirXML driver for NDS, the external eDirectory tree will receive user information from an eDirectory identity management tree that contains a complete store of user information. This eDirectory identity management tree lies inside the company's firewall.

Novell Consulting will then configure the company's firewall so that only the IP address of the iChain server is allowed to access the company's internal network. By using this configuration, the company only needs to create "one hole in the firewall rather than creating holes for six million users," Mullins explains.

(For more information about using iChain, see "Novell iChain: How One Company Found Its e-Business Solution," *Novell Connection*, Aug. 2001, pp. 14-22. You can download this article from www.ncmag.com/past.)

iChain can also give users single sign-on access to web-based applications and services. After a user authenticates to iChain through eDirectory, he or she can access web-based applications and services that require additional identity or authentication information without having to log in to these applications and services separately. When an authorized user accesses such an application or service, iChain automatically retrieves the user's credentials from eDirectory and passes those credentials to the requested application or service.

iChain 2.0 (the latest version of iChain) also supports XML-based form-fill authentication, which extends iChain's single sign-on capabilities to web-based applications that use forms to authenticate users. XML-based form-fill authentication enables iChain to provide authentication

via digital certificates, tokens, and other means that are stored in LDAP-accessible fields in eDirectory. (For more information about iChain, visit www.novell.com/products/ichain.) To see how one company used iChain, see "Novell Products at Work" on p. 22.

Novell SecureLogin: Create a Singular Sensation

To give users single sign-on access to virtually all of the applications running on your company's network, you can add Novell SecureLogin to your company's eProvisioning Solution Framework. SecureLogin is password-management software that you install on Windows 2000, 98, 95, ME, and NT 4.0 workstations that are running Novell client software.

SecureLogin extends NDS and eDirectory User objects to include an attribute that can store encrypted usernames and passwords. (SecureLogin supports NDS 5.0 and above and eDirectory.) Using the login credentials stored in this attribute, SecureLogin can provide users with single sign-on access to a wide

**Please visit our advertiser Airous Networks
online at www.airous.com.**

Novell Products at Work

Finding out about a new product is great, but you probably also want to know which companies are using the product and how they are using it. The following briefly explains how one company is using Novell eDirectory and Novell iChain.

THE CLIENT

Noridan Mutual Insurance Company—Blue Cross Blue Shield of North Dakota, a not-for-profit health care coverage provider

THE PROBLEM

Noridan's dial-in customer service center was consistently overwhelmed. To alleviate the congestion at call centers, Noridan wanted to develop a single, cross-platform solution that would offer users a quick way to find information about their health care coverage. In addition, this solution needed to be highly secure in order to comply with the U.S. government's new security and privacy regula-

tions (the Health Insurance Portability and Accountability Act [HIPAA]).

THE TOOLS

- Novell eDirectory
- Novell iChain

THE SOLUTION

Using eDirectory and Novell iChain, Noridan effectively merged all of its web applications into a centralized infrastructure. Novell iChain enables Noridan users to self-register on the Noridan web site. Subsequently, users are sent a username and password via e-mail, which they can then use to securely access their personal health care information.

THE RESPONSE

"Our previous solution did not offer the flexibility and security we needed. Novell eDirectory, together with Novell iChain, was the only solution that would allow us to meet HIPAA standards," says Troy Aswege, Noridan assistant vice president of IS. ●

variety of applications, including the following applications:

- Windows 32-bit applications
- E-mail applications such as GroupWise, Lotus Notes, and Outlook
- IBM and UNIX mainframe applications

SecureLogin can also provide single sign-on access to Telnet sessions, Citrix terminal sessions, terminal emulators, and web applications.

To provide this single sign-on access, SecureLogin listens for and responds to authentication requests from users' applications. When a user launches an application for the first time after you install SecureLogin, he or she must log in to that application as usual. SecureLogin then captures the user's login credentials and stores these credentials, encrypted, in the user's User object.

Henceforth, when this user launches this application, SecureLogin automatically retrieves these login credentials from eDirectory and provides them to the application on the user's behalf.

SecureLogin can also handle password changes. If a user's password expires, SecureLogin can automatically generate a new password that is based on your company's password policy.

By eliminating the need to remember multiple username and password combinations, SecureLogin can reduce the number of password-related calls that your company's help desk receives. Because each help-desk call can cost your company an estimated U.S. \$25–50, SecureLogin can save your company "up to millions of dollars a year in help-desk costs," Mullins explains.

In addition, SecureLogin integrates with NMAS to provide single sign-on access to applications that require graded authentication, including biometric, digital certificate, token, or smart-card authentication. (NMAS integrates with eDirectory and enables you to require graded authentication for applications and information. For more information about NMAS, see the following "NMAS: Authentication Services That Make the Grade" section.)

For example, suppose an application requires a username and password combination and a thumbprint scan (which is biometric authentication). When a user launches this application, SecureLogin automatically provides the user's username and password combination. SecureLogin then prompts the user to provide his or her thumbprint scan. (For more information about SecureLogin, visit www.novell.com/products/securelogin/details.html.)

NMAS: Authentication Services That Make the Grade

Your company may require more than a standard username-and-password combination for authentication. For example, your company may require a username-and-password combination and a digital certificate before users can access its financial database. Your company may also require a digital certificate and a biometric login credential (such as a thumbprint scan). In other words, your company may require graded authentication.

If your company is planning to allow certain external or internal users to access confidential information, you can use NMAS to provide graded authentication for that information. NMAS enables you to create authentication policies in eDirectory that require a sequence of one or more login factors. (Login factors come in three varieties: what you know, such as a username and password; what you have, such as an X.509 digital certificate; and what you are, such as your fingerprint.)

You can then assign these authentication policies to specific applications or to NetWare volumes. For example, before a user can access files that contain financial information, you can require that user to use two login factors: a username and password and a fingerprint scan.

To allow your company's business partners to access top-secret product formulas, on the other hand, you can require three login factors: a fingerprint scan, a digital certificate, and a username and password. (For more information about NMAS, see "NMAS: It's What Spy Movies Are Made Of," *Novell Connection*, Feb. 2000, pp. 6–21. You can download this article from www.ncmag.com/past/.)

Novell Portal Services: Their Space, Your Place

If you plan to make applications, information, or other resources available to users over the Internet, you may want to consider using Novell Portal Services to personalize these users' experience. Personalizing users' experience can help your company establish stronger ties with users—whether those users are customers, employees, suppliers, or partners.

Novell Portal Services is a directory-based portal framework that enables you to personalize the information and services that users access via the Internet using protocols such as HTTP and SSL. You can also personalize the way this information

and these services appear to users, based on the users' identity in eDirectory.

With Novell Portal Services, you can also enable users to customize their own information or applications. For example, with i-Login.net, Novell's in-house implementation of Novell Portal Services, users can customize the Stock Ticker gadget to display information about specific stocks. (Gadgets are services that can snap into the Novell Portal Services framework. For more information about Novell Portal Services, see "Novell Portal Services: A Better Way To Build a Desktop," *Novell Connection*, Dec. 2000, pp. 22-32 and "Novell Portal Services: The Tools You Need To Build a Better Desktop," *Novell Connection*, Jan. 2001, pp. 18-31. You can download these articles from www.ncmag.com/past.) For more information about other portal options, see "Novell Shouts Yahoo!" on p. 38.

Novell OnDemand Services: Directory-Based Thin Client Computing

Suppose your company employs salespeople who work on the road. If your

company wants to include this sales force in its employee implementation, you may need to make applications that handle sales-related information available to these salespeople via the Internet. If these applications happen to be Windows 32-bit applications, you can make them available over the Internet using Novell OnDemand Services.

Novell OnDemand Services can deliver Windows 32-bit applications over the Internet to any user who has a standard web browser. That is, with Novell OnDemand Services, users don't need to worry about installing and maintaining client software—and neither do you.

Novell OnDemand Services delivers these applications, which are running on your network, in real time. As a result, your company's sales force can arm itself with the latest information. "The beautiful thing about Novell's eProvisioning Solution Framework," Mullins explains, "is that it is based on real-time information."

Novell OnDemand Services also includes pricing schemes and use-tracking features. If your company provides ap-

plications to customers for a fee, it can implement a customer implementation that uses Novell OnDemand Services to deliver these applications. Because Novell OnDemand Services is directory-based, Novell OnDemand Services knows which users are salespeople who get their applications for free and which users are customers who pay for their applications.

In addition, Novell OnDemand Services is available as a gadget for Novell Portal Services, which enables you to integrate Novell OnDemand Services with the portal through which you provide other resources—such as information about your company's latest, greatest product. (For more information about Novell OnDemand Services, see "Novell OnDemand Services Simplifies the Delivery of eProvisions" on p. 27.)

CONCLUSION

If your company decides to implement an eProvisioning Solution Framework, Novell Consulting and its consulting partners can combine the products described above in many ways to create the particular implementation to fit your company. How seriously should your company be considering an eProvisioning solution?

That depends on how big your company is and how crucial it is that your company be able to put people to work fast. For example, Schacter cites a company that recently deployed an eProvisioning system. This company told Schacter that it hired three hundred temporary workers, and those workers were temporary because the company needed them immediately. Obviously, Schacter explains, "it was very important to that company to provision workers quickly."

If you work for a large company, analysts such as Schacter and Roberta Witty, a Gartner information security strategies research director, predict that your company may be in the process of implementing an eProvisioning system within the next five years. Since your company is probably already using Novell products, the eProvisioning system it implements could certainly be Novell's eProvisioning Solution Framework. After all, your company is probably already familiar with the power of Novell eDirectory, which is the centerpiece of Novell's eProvisioning Solution Framework.

Cheryl Walton works for Niche Associates, an agency that specializes in technical writing and editing. ●

**Please visit our advertiser Biscom
online at www.biscom.com.**