Novell’s iChain

A Secure Foundation for Integrating e-Business Activities by Sandy Stevens

With the evolution of the Internet over the last few years, e-business has become more than just a buzzword: It has become one of the most important strategic issues companies face today. In fact, industry analysts are predicting that e-business is the future of business. For example, International Data Corp. (IDC) predicts that the amount of commerce conducted over the Internet will exceed U.S. $3 trillion by the year 2003. The number of users who make purchases over the web will jump from 31 million in 1998 to more than 183 million by 2003.

To succeed in the emerging digital economy, companies need a coherent e-business strategy. However, putting your company’s business online is no easy task. Transforming your company into an effective e-business presents technical, operational, and human challenges that are far greater than you ever imagined.

If you are grappling with the issues of building an e-business, Novell’s latest Novell Directory Services (NDS) based e-business solution, iChain, can help you expand your company’s current network to connect the people and organizations with which your company does business. If your company has launched an e-business effort and is struggling to survive in this competitive economy, iChain can also help you integrate your company’s existing web sites and manage your company’s business-to-business and customer relationships. Scheduled for general release later this year, iChain enables you to build strong, secure, and manageable connections with your company’s customers, partners, suppliers, and employees.

The primary issue in building an e-business network is security. To conduct e-business with your company, partners, suppliers, and customers need to access applications and data on your company’s network. Often, your company’s employees need to access these same applications and data. For security reasons, however, you obviously can’t give external people access to your company’s entire internal network.

As you know, companies currently participating in e-business have created two separate networks to solve this problem: an intranet that connects the internal people to the applications and data they need and an extranet that connects external people to the applications and data they need. These companies then use firewalls to isolate external people from the internal network and to isolate unauthorized Internet users from the extranet.

Although firewalls provide a good method of controlling access to a particular network segment, they do not provide granular security to control the level of access a user has. For example, a company may want to grant a customer access to an inventory application so that the customer can view quantities in stock. However, the company may not want the customer to access the cost-of-goods information. Because most firewalls do not provide this kind of granular security, companies must implement other security mechanisms.

E-business also presents data privacy issues. When your company conducts online business with its customers, partners, and suppliers, information sent over the Internet can pass through several intermediary computers before it reaches its destination.
In a perfectly honest world, these intermediary computers would simply route the traffic without monitoring it. Unfortunately, the world isn’t perfectly honest. If given the opportunity, someone can and will eavesdrop on private transmissions. Eavesdroppers can intercept data and even modify it, replacing your information with their own. Even worse, eavesdroppers can intercept credit card numbers during online transactions. Eavesdroppers can intercept data and even modify it, replacing your information with their own. Even worse, eavesdroppers can intercept credit card numbers during e-commerce transactions.

As you may know only too well, e-business can also substantially increase the workload for network administrators. Expanding your company's network to include not only employees but also customers, partners, suppliers, and everyone else your company does business with can result in a massive administration burden. E-business networks can easily grow to include thousands, if not tens-of-thousands, of people. Imagine the size of the staff that you would require to create user accounts and manage network access for a network that size!

There is also the issue of managing the multitude of web sites and web applications that companies have implemented as they have evolved their networks toward e-business. Companies often run their web sites and related applications on a variety of dissimilar systems. Unfortunately, each application provides its own authentication, its own security, its own access control, its own e-commerce engine, and its own storage of usernames and profiles.

A s a result, companies have a difficult time managing overlapping technologies, security is reduced to the lowest common denominator, and users must log in to several applications as if they are accessing networks at different companies. In addition, the capability of data mining and cross selling is significantly lower. This web architecture makes managing and accessing web sites complex and costly.

**NOVELL’S SOLUTION**

iChain provides a platform for building and managing a secure e-business network. Rather than managing multiple web sites, intranets, and extranets as separate entities, you can manage your company's entire infrastructure as one cohesive network. iChain serves as a central point of administration and provides a common method of authentication, security, and access control. As a result, users log in only once and receive seamless access to all web sites and applications integrated by iChain. (The iChain architecture in Figure 1 shows the services iChain provides.)

**NDS eDirectory**

Not surprisingly, the heart of iChain is NDS eDirectory. When it comes to managing complex networks, NDS eDirectory is truly in a class by itself: NDS eDirectory's simplified management, along with its proven security, reliability, and scalability, make it the ideal foundation for e-business.

With NDS eDirectory's cross-platform capabilities, you do not have to maintain numerous parallel directories. Instead you can create one global identity for each user, and the user can then access network services and applications on multiple platforms with a single login.

NDS eDirectory enables you to establish relationships between people, applications, information, and devices on your e-business network. Using ConsoleOne, which is included with iChain, you can grant users rights based on their relationship to the company and their role in that relationship. NDS eDirectory minimizes the complexity of establishing these relationships through centralized administration, policy-based management, and object inheritance.

**Delegation of Authority**

As your company’s e-business network grows into a huge intermixed web of people, organizations, and services all linked together, it will be virtually impossible for one person or organization to manage this network. iChain allows you to delegate the management of the e-business network to participating business partners. You can simply create subadministrators and grant them the rights to manage their portion of the network. This way, each company can assume responsibility for managing its own portion of the e-business network.

**LDAP Support**

NDS eDirectory natively supports Lightweight Directory Access Protocol (LDAP) 3, which has become the standard that Internet-based applications use to access directory information. Because NDS eDirectory supports LDAP 3, users can use any LDAP-based application, browser, or client to access the NDS information to which they have rights.

**ICHAIN SECURITY**

iChain incorporates several security mechanisms that ensure the privacy of data sent over the Internet. For example, iChain supports the use of Secure Sockets Layer (SSL) to ensure privacy when data is transmitted between your company’s web site and a user’s browser. (Today’s browsers support SSL.) SSL is a communication system that encrypts information before sending it over the Internet.

SSL ensures the confidentiality of data and the integrity of data. If a third-party intercepts data being transmitted between SSL-enabled devices, that data will be unreadable. If a third-party attempts to alter the data being transmitted, the...
recipient will know because the data won’t decrypt properly.

To identify users and to verify their access privileges, i-Chain provides a variety of authentication mechanisms. For example, i-Chain supports authentication methods such as passwords, token cards, and smart cards. i-Chain can also use X.509 certificates for authentication, no matter whether the certificates are minted by Novell Certificate Server or by another certificate authority. (For more information about X.509 certificates, see “Novell Certificate Server 2.0: Is Your Network Certifiably Secure?” NetWare Connection, Jan. 2000, pp. 6–20. You can download this article from http://www.nwconnection.com/past.)

To secure access to your company’s network, the i-Chain Authentication Proxy functions as the primary access point for your company’s network infrastructure. When a user tries to authenticate to your company’s network, the Authentication Proxy checks the NDS eDirectory policies defined for that user or for that user’s community and determines the user’s access rights. Based on the user’s profile and access rights, the i-Chain Authentication Proxy then authenticates the user to all of the web servers and web applications that the user is authorized to use.

Because the i-Chain Authentication Proxy supports today’s most popular web servers and applications, you can integrate your company’s existing web infrastructure and present users with a cohesive unified web experience. With i-Chain, users have one web identity for your company’s network. By logging in with one username and password, a user can automatically access a multitude of web sites and applications that require authentication. (See Figure 2.)

In addition, when you add a new web site that requires authentication, you can simply grant a user access to that web site. This user can then continue using his or her original username and password, logging in to the network only once.

ICHAIN DIGITAL COMMUNITIES

When you install i-Chain, the installation program adds new object classes to your company’s NDS schema. For example, these new object classes enable you to create objects that represent i-Chain Communities, i-Chain Services, and i-Chain Servers.

The purpose of a digital community is to reflect frequent changes in an environment with numerous users. Novell has optimized the i-Chain digital communities to reflect dynamic common properties (such as suppliers that have a maximized credit balance).
You can use ConsoleOne to create iChain Communities in the Organizational Unit (OU) object. You can then use the iChain Communities to grant groups of people access to the information that they need on your company's network. Using ConsoleOne, you can grant access to content, web pages, and applications on a community basis rather than on an individual user basis.

When you configure an iChain Community, you can define the following properties:

- Updates, which enable you to write HTML code directly into the Community object. You will typically use updates to include simple text messages, although the HTML code can include other objects.
- Links, which refer to URLs the community has access to. Users cannot surpass the iChain Authentication Proxy to access a URL they do not have rights to access.
- Documents, which allow you to define which documents the community members can see or publish, depending on their access rights.

To help you manage digital communities, iChain lets users join communities on their own, without requiring administrator intervention. When a user joins a community, iChain automatically creates a User object in NDS eDirectory and provides that user with a set of basic services.

You can configure the self-registration process to occur automatically or through an approval process, where iChain notifies you of the registration. You can then grant the user additional access if desired. This self-registration is an elegant solution for managing communities because it minimizes your administration burden while providing users with the appropriate level of access to your company's resources.

Self-registration is an optional feature. If you are uncomfortable with people self-registering on your company's network, you can disable this feature.

If you like the idea of user self-registration but want a little more security, you can use digital certificates together with self-registration. Digital certificates provide trust when users self-register. If a user has a digital certificate to verify his or her identity, iChain automatically registers that user for the appropriate communities based on policies that you have defined.

ICHAIN PORTAL

To create customized solutions for users and to make it easier for users to access your company's network, iChain includes a secure portal. This portal is a web page that displays a set of applications and links (URLs) to web pages that are unique to each user. When a user logs in to your company's network, iChain dynamically builds this web page, which presents the network resources to which that user has rights in NDS eDirectory.

Novell is also working with vendors that specialize in portal software to integrate their solutions with iChain. The portal software will then handle the presentation logic while iChain concentrates on the back-end infrastructure of the solution. (For more information about the companies that have announced support for Novell's iChain, see “Novell's iChain Partners.”)

A COMMON DATA STORE

To help you integrate your company's e-business network with existing application databases and directories, iChain can use DirXML, which replicates information from dissimilar directories to NDS eDirectory. With DirXML, NDS eDirectory becomes a data store for common information, eliminating the need to enter the same information—such as names, e-mail addresses, and telephone numbers—multiple times in multiple databases.

With DirXML, you partition the NDS tree in a way that makes sense for the application. You can create custom replicas, known as virtual replicas, for applications that serve as connectors between NDS eDirectory and the applications' native database. In addition, because NDS eDirectory supports multiple writable replicas and NDS replication is bidirectional, both applications and network administrators...
can make changes to the data stored in NDS eDirectory. The normal NDS replication process then automatically updates those changes throughout the network.

To deliver NDS information to applications in their native format, DirXML uses integration drivers. Using the Extensible Markup Language (XML), the integration drivers eliminate the need for any NDS-specific coding. These drivers apply the appropriate filtering, data transformation, object mapping, and event mapping to NDS data before delivering the information to the application. Integration drivers can also receive data from applications and convert that data to NDS format using XML.

DIRCOMMERCE

iChain also includes DirCommerce, a directory-based transaction system that allows you to sell or temporarily lease NDS eDirectory objects. These objects can represent anything from durable goods, services, disk space, electronic content, to Virtual Private Network (VPN) connections, digital certificates, or community memberships.

In addition, DirCommerce provides enforcement and reporting capabilities, and it interfaces with popular payment-processing gateways. DirCommerce is a powerful foundation for e-business applications that provide e-commerce services. The NDS eDirectory integration allows DirCommerce to apply policies to the transaction process. As a result, you can base pricing options on users' community membership or on a certain event.

For example, a customer who has purchased U.S. $100 of merchandise in a three-month period of time may become a member of the Gold Club community and receive a 10 percent discount on all purchases made during the next month.

DirCommerce is particularly important in hosted environments. Many small companies are turning to service providers who can offer a complete e-business infrastructure for a monthly fee. Without spending millions of dollars on a network infrastructure that will support e-business, these small companies can then look and operate as if they were large companies.

However, using a service provider may not always be the best option. If a company needs a variety of customized services, it may be more economical for that company to implement its own e-business solution. DirCommerce enables any company to charge for online services and to provide customized services for customers.

BUSINESS-TO-BUSINESS

Many business-to-business solutions are offering sites that connect corporate buyers with corporate suppliers. Unfortunately, each participating company must trust the provider of these sites. In addition, these sites may host companies that compete with each other—making companies uncomfortable with this type of e-commerce solution.

Many companies want to maintain authority over their own data. With iChain, companies can implement business-to-business solutions that do not require a mediator. Each company retains full ownership and authority over its data and transactions. Each company can also determine the kind of relationship it has with another company—controlling the data and resources it shares.

CONCLUSION

Many companies are changing their web sites from information-only sites to sites that offer a variety of online services. These companies need to connect their customers, partners, and suppliers to information on the companies' internal network. In addition, companies want to combine their services with the online services that their partners provide to create new value propositions for their mutual customers.

To provide these services, companies must expose information and services to their customers and to partners across the Internet. Exposing this information presents many challenges, such as providing strong security, dealing with large numbers of new users, and keeping administration costs low. With iChain, Novell will deliver a powerful directory-enabled solution that addresses these issues. iChain could very well be the foot-in-the-door that Novell needs to break into the competitive world of e-business products.

Novell plans to release iChain later this year. For more information about iChain, visit http://www.novell.com/products/ichain. You can also call at 1-888-321-4272 or 1-801-228-4272.

Sandy Stevens is a freelance writer based in San Diego, California. Ms. Stevens is coauthor of Novell’s Guide to Integrating NetWare 5 and NT, Novell’s Guide to NetWare Printing, and Novell’s Guide to BorderManager.