

Novell iChain

How One Company Found Its e-Business Solution

Sandy Stevens-Marymee

If your company delivers content over the web, you know that today's Internet users expect more for less: more features, more services, and more entertainment—all in less time, with less effort. If your company's web site is slow or difficult to use, potential customers will click to the next site faster than they can read your company name.

How do you build a secure web site that provides the transparency, ease-of-use, and fast response times that today's savvy Internet users demand? This article explains how Essentialtalk Network, an Internet-based communications company, is using Novell iChain to build a fast, easy-to-use web site.

ESSENTIALTALK NETWORK OPTIMIZES COMMUNICATIONS

Essentialtalk Network provides an interactive communications network that enables individuals and organizations to communicate across time zones and geographical boundaries. Using Essentialtalk Network's Internet-based venue, companies can communicate with employees, customers, and partners via high-quality audio, video, and text.

For example, a company can leverage the Essentialtalk Network to conduct internal and external training (both live and pre-produced); to hold meetings, seminars, and conferences; and to improve corporate and marketing communications. Participants in these events can share their opinions or ask questions by simply posting messages on the Essentialtalk Network web site.

In addition, Essentialtalk Network can archive any event for those who cannot participate in the live event. For example, suppose you are unable to attend an important corporate training session because you are on an airplane. When you reach your destination, you can log in to the Essentialtalk Network web site and view the event at your convenience.

You can also post questions and comments regarding the event. Essentialtalk Network will forward these comments to the event moderator or instructor who can then post the response on the Essentialtalk Network web site.

Essentialtalk Network also provides talk-radio capabilities

that enable companies to broadcast regularly scheduled "radio" programs via the Internet. In addition, Essentialtalk Network provides online talk forums where individuals can discuss a variety of personal issues from culture and current affairs to family, health, personal finance, politics, sports, and technology.

THE CHALLENGE

When Essentialtalk Network set out to design a web architecture that would support the concept of relationship-based knowledge exchange and communication, the company faced a number of challenges. First and foremost, the company needed a highly secure solution that enabled it to support a rapidly growing number of Internet participants throughout the world.

Essentialtalk Network also wanted a flexible solution that would give it the freedom to choose the operating system platform and applications that best met the company's present and future needs.

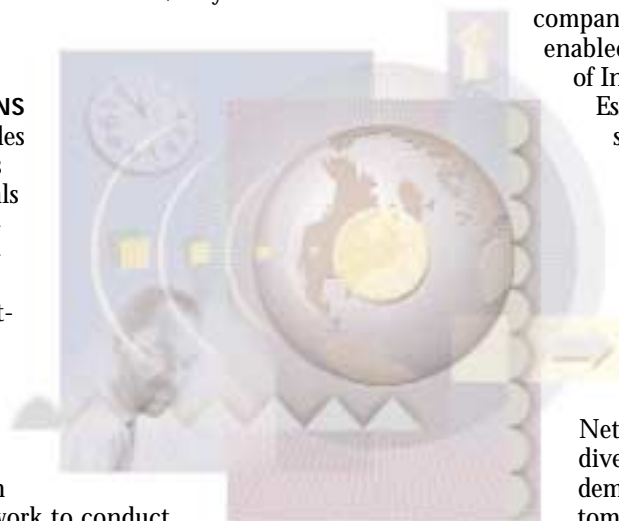
"We needed to design an architecture that could handle literally tens of thousands to hundreds of thousands of customers," Lorand Szojka, CIO of Essentialtalk Network, explains. According to Szojka, Essentialtalk

Network not only needed to authenticate diverse users but also to "provide them with demographically and geographically customized content."

THE ICHAIN SOLUTION

When the Essentialtalk Network team began looking for products that would meet its requirements, the evaluation process was very short. "Because we didn't have legacy systems, we were able to truly look at the technologically superior products and look at what products best met our needs," says Szojka. "We knew that we needed a scalable solution, and we knew that we wanted to base our architecture on directory-enabled tools. If you look out in the marketplace, there are very few true directories to choose from."

At the foundation of iChain is NDS eDirectory 8.5—a full service, platform-independent directory. As the user information repository for iChain, NDS eDirectory provides the scalability to handle a site's growth to potentially tens of thousands of users and tens of thousands of hits per minute. What's more, with eDirectory's redundant fail-over capabilities, no single



What's New in iChain 2.0

Novell's next version of iChain, iChain 2.0, is scheduled for release this month. This version adds new functionality and enhances the manageability, scalability, and performance of iChain.

The following list is an overview of what you can expect to find in iChain version 2.0:

- **Token Authentication.** iChain 2.0 adds token-based authentication for companies that want to use a strong authentication method. With token authentication enabled, companies can require users to have additional factors to successfully authenticate—something they know, such as a personal identification number (PIN) and something they have, such as a token device. iChain 2.0 supports ActivCard, RSA SecureID, and Vasco tokens.
- **XML-Based Form-Fill Authentication.** iChain 2.0 adds a form-fill feature to the existing single sign-on capabilities. This feature supports web applications that use forms to authenticate users. For example, when a user enters form data to authenticate to a web application, iChain captures the data and uses Novell Secret Store to securely store the user's credentials. The next time the user accesses the web site, iChain automatically fills in the form data necessary to authenticate the user.
- **Strong Encryption.** To ensure the highest levels of encryption, iChain 2.0 can require a similar strength of

encryption for both the browser and the iChain proxy server. If the browser has a lower level of encryption than is required by the iChain proxy server, a communication link is not established.

- **Configuration Wizard.** iChain 2.0 adds a new configuration wizard that simplifies the configuration of iChain. This wizard queries the user and automatically creates a configuration file based on the user's responses.
- **Performance.** iChain 2.0 has two enhancements that increase overall system performance: improved acceleration of numerous core components and reduced access control processes through the use of public pages and URL exceptions.
- **Scalability.** Companies can now link several iChain 2.0 servers to balance the load created by potentially millions of authentication requests.
- **Fault Tolerance.** iChain 2.0 adds additional levels of fault tolerance to the iChain authentication, access control and Object Level Access Control (OLAC). To provide this fault tolerance, iChain 2.0 enables you to link multiple iChain servers together. If, for some reason, one of the iChain servers goes down, the other iChain servers automatically assume the responsibilities of that server without requiring users to log in again.
- **Custom-Logging Pages.** iChain 2.0 allows companies to present different identities by specifying custom login pages for each defined accelerator. This feature is ideal for web-hosting services.

point of failure exists that ensures the iChain user repository is available at all times.

Using eDirectory, iChain can unify a company's heterogeneous network environment with a single point of administration. In addition, eDirectory's native Lightweight Directory Access Protocol (LDAP) support provides compatibility with other LDAP-based applications.

With eDirectory as the clear choice of directories, Essentialtalk Network brought in Novell Consulting to help it design an eDirectory-enabled infrastructure that would meet its needs. The recommended solution was iChain, Novell's eDirectory-based security and management infrastructure.

Using iChain 1.0 as the foundation for web security, Essentialtalk Network officially launched its web site on October 2, 2000. In December 2000, Essentialtalk Network upgraded to iChain 1.5. According to Szojka, Essentialtalk Network "is very interested" in the new features of iChain 2.0. (iChain 2.0 is scheduled to be released this month. For more information about iChain 2.0, see "What's New in iChain 2.0.")

Essentialtalk Network currently implements the following three iChain 1.5 components:

- iChain proxy server
- iChain authorization server
- eDirectory 8.5

The remainder of this article explains how Essentialtalk Network is using these iChain components to deliver services to its clients.

ICHAIN PROXY SERVER

Figure 1 illustrates Essentialtalk Network's iChain architecture. As you can see, iChain proxy server provides secure access to the Essentialtalk Network web site, and all of the users' authentication and access information is stored in eDirectory.

iChain proxy server provides the initial point of access to the Essentialtalk Network. When a user wants to access a secure area of the Essentialtalk Network web site, that user must log in via the iChain proxy server. The iChain proxy server then communicates with the iChain authorization server, which accesses the information stored in eDirectory to determine the user's access privileges.

iChain proxy server is a web accelerator that uses an enhanced version of Volera Excelerator's reverse proxy technology. (Volera Excelerator was formerly called *Novell Internet Caching System*.) As a reverse proxy, the iChain proxy server increases the speed at which Essentialtalk Network can deliver content to users.

The iChain proxy server speeds delivery by intercepting inbound content requests and, when possible, delivering the content from a local cache. On average, iChain proxy server can cache approximately 85 percent of a web server's content. According to Szojka, Essentialtalk Network's "web servers are sitting there at 20 percent utilization at best—and that indicates that the proxy server is doing its job really well."

Multihoming

The iChain proxy server adds two multihoming techniques to a typical reverse proxy:

- **Multihoming.** Multihoming enables you to use a single public IP address to handle requests made to multiple back-end web servers.
- **Path-Based Multihoming.** Path-based multihoming enables you to use one Domain Naming System (DNS) name with multiple suffixes. iChain proxy server will then redirect requests to different web servers based

on the suffix. For example, iChain proxy server would direct requests for www.essentialtalk.com/web1 to one web server and requests for www.essentialtalk.com/web2 to a different web server.

Essentialtalk Network uses path-based multihoming to provide transparency for its customers. For example, a company that uses Essentialtalk Network to broadcast a radio program for employees can provide a link on the company's web site for that radio program. The link may include a suffix. For example, the URL may look like www.essentialtalk.com/webradio. When a user clicks on this link, the iChain proxy server will transparently deliver the content from the web server on the Essentialtalk Network site that hosts the radio program.

"Multihoming is exactly why we think this [technology] is so powerful. Our objective is to solve communication problems for organizations and between people so we want to be transparent. Multihoming makes us transparent."

Secure Access

The iChain proxy server also supports Secure Sockets Layer (SSL). As a result, Essentialtalk Network can provide data confidentiality. By enabling the Secure Access feature included with the iChain proxy server, Essentialtalk Network can send web pages securely to browsers. All data exchanged between the proxy server and a user's browser are encrypted via SSL. Encryption creates a secure 'tunnel' between the two, which prevents any unauthorized system from reading the data.

For example, suppose a company wants to sell seminars or other events that are archived on the Essentialtalk Network web site. When a user purchases an archived event, the Secure Access feature will enable web pages and confidential information, such as credit card numbers, to be transmitted via a secure connection.

Another benefit that the Secure Access feature provides is offloading processor-intensive SSL encoding and decoding. Because SSL encryption tasks are offloaded from the Essentialtalk Network web servers, the web servers are freed up to do what they do best—serve content.

To further facilitate delivering digital content to its customers, Essentialtalk Net-

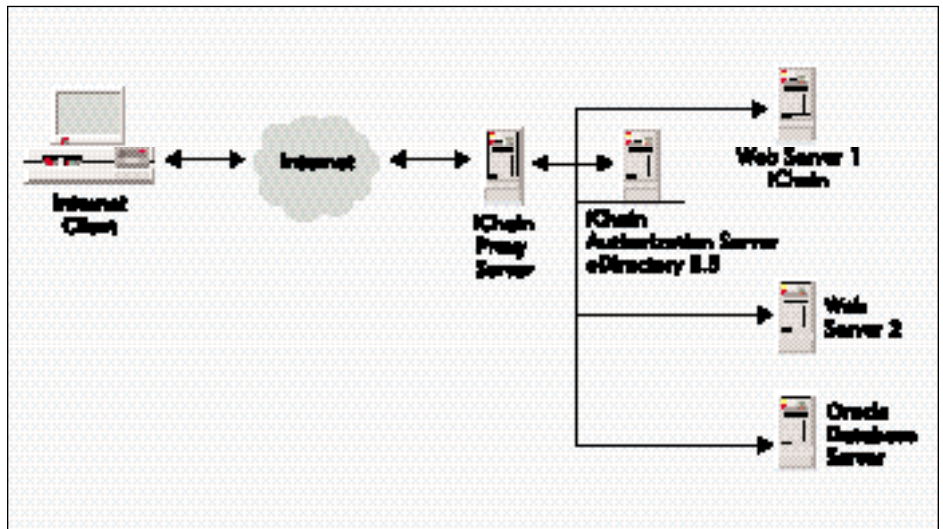


Figure 1. Essentialtalk Network uses an iChain proxy server to provide secure access to the Essentialtalk Network web site. All of the users' authentication and access information is stored in eDirectory.

work recently implemented Novell On-Demand Services. OnDemand Services is Novell's application and content-provisioning solution. With OnDemand Services, Essentialtalk Network can securely deliver seminars or other archived events to customers. OnDemand helps Essentialtalk Network provision which events customers can purchase, lease, or freely access on the Essentialtalk Network web site.

ICHAIN AUTHORIZATION AND AUTHENTICATION

Essentialtalk Network's authorization server is a NetWare 5.1 server running eDirectory 8.5. All access privileges for Essentialtalk Network users are stored in eDirectory.

Note. Although Essentialtalk Network uses eDirectory, iChain also supports the ability to store user authentication information in an LDAP directory.

When a user logs in to the Essentialtalk Network web site through the iChain proxy server, the proxy server sends the authentication information via LDAP to the iChain authorization server. The iChain authorization server accesses eDirectory to determine the appropriate access for the user. The iChain proxy server then enforces the access control policies for the user and presents a customized user interface for the user.

Web Single Sign-On

iChain gives users the convenience of single sign-on to multiple web serv-

ers and applications. iChain has several methods for enabling this single sign-on. For example, iChain can forward a user's authentication information using XML-based Form Fill in the query

Visit our advertiser
Wired Red at
www.wiredred.com.

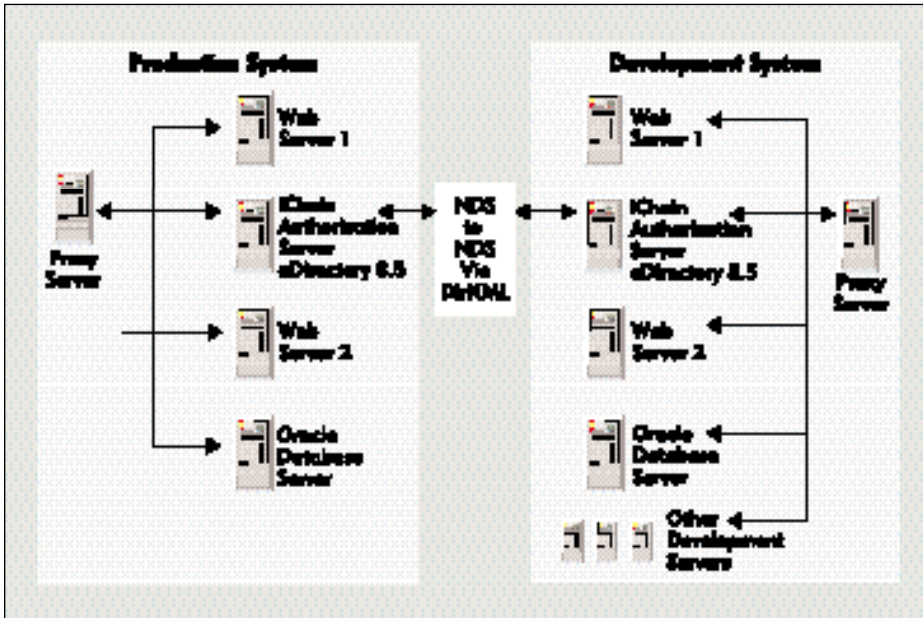


Figure 2. Essentialtalk Network uses Novell's DirXML to synchronize eDirectory account information between the production system and the development system.

string, in the custom header, or in the HTTP authentication header.

When a user who is authenticated to the Essentialtalk Network web site accesses a web resource that requires additional authentication, iChain transparently submits the user's authentication information to the web server. iChain automatically grants or denies the user access to the resource without requiring the user to provide his or her username and password a second time.

ICHAIN IDENTITY MANAGEMENT

iChain also includes the following two identity management features that help Essentialtalk Network provide customers with a customized experience:

- **Self-Registration.** This feature provides a web-based form that enables users to self-register and become part of an Essentialtalk Network event.
- **Self-Provisioning.** This feature allows the users to modify their identities.

According to Szojka, Essentialtalk Network originally used these features to create a talk-radio network. Users would self-register and become part of the digital group that had access to the discussion topics in which they were interested.

As Szojka explains, the real benefits of self-registration and self-provisioning be-

came evident when Essentialtalk Network began providing services to businesses. "Businesses have their own user bases. If you have a client such as Bell Intrigna that has employees who can self-register and administer their own data, who best does this than the clients themselves? We have about 40 clients at various stages of development, and each one will self-maintain their information."

When an Essentialtalk Network client hosts an event such as an online seminar or meeting, Essentialtalk Network creates a digital group and gives users in that digital group access to the resources associated with that event. For example, clients can access resources such as audio and video capabilities and supplemental documentation. Clients can also have the ability to post questions during the event and the ability to archive the event.

Essentialtalk Network then assigns an administrator over the digital group. This group administrator is frequently the instructor or moderator of the event. The group administrator then provisions resources for the users in the group.

"When you book a hotel room for a conference, for example, you provision items such as an overhead projector and a coffee machine. The instructor self-provisions the meeting environment and the attendees at that meeting can then self-register and administer themselves," explains Szojka.

A Custom Web Experience

Essentialtalk Network is currently evaluating and implementing additional technologies that will enable the company to further customize a user's web experience. For example, Essentialtalk Network is evaluating the Object Level Access Control (OLAC) feature of iChain.

OLAC injects dynamic data that is based on a user's identity into the HTTP header. As described earlier, this same technology allows iChain to provide single sign-on to web resources. However, OLAC is much more powerful than just providing web single sign-on; OLAC allows companies to customize a user's web experience by injecting personal information such as personal preferences, credit card information, and addresses. Although Essentialtalk Network has not used OLAC to its fullest capacity, the company is "very interested" in this technology.

Essentialtalk Network is also in the process of implementing Novell Portal Services, which will help the company provide users with the resources that they need for a particular event. According to Szojka, Novell Portal Services can provide gadgets, or tools, that represent the functions and resources that an instructor or moderator can allocate to a classroom or session. (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.)

iChain is the security that goes around it to make sure that users are given access to the proper resources such as the ability to support audio, visual, and supplemental documentation; the ability to post questions; the ability to archive and replay those archives; and the provisioning of channels to set a schedule.

Eliminating Downtime

For Essentialtalk Network, even the smallest amount of web site downtime is catastrophic and results in significant loss of revenue. To ensure the web site functions continuously, Essentialtalk Network operates with two mirrored systems—a production system and a development system. This solution, developed with

the help of Novell Consulting, virtually eliminates downtime of the Essentialtalk Network web site due to system failure, outside attacks, or system maintenance.

The Essentialtalk Network production and development systems are completely self-contained and are duplicates of each other with the exception of the web access IP address. (The development system also includes a few additional development servers that are not required in the production system.) The production system is online during normal operating conditions. The development system is a backup and development environment. Only internal personnel typically access this system.

Keeping It in Synch

Essentialtalk Network uses Novell's DirXML to synchronize eDirectory account information between the production system and the development system. (See Figure 2 on p. 20.) DirXML automatically copies any change that is made in eDirectory on the production system to the development system. As a result, the development system remains

up-to-date with all of the users' account information, including passwords. If the production system goes down due to system maintenance or failure, Essentialtalk Network can bring the development system online.

Easy Upgrade

When Essentialtalk Network upgraded from iChain 1.0 to 1.5 in December 2000, these two systems enabled the company to perform the upgrade with only six minutes of downtime. With the help of Novell Consulting, Essentialtalk Network upgraded its development system first and then used DirXML to transfer the users from the production system to the development system.

Essentialtalk Network was then able to bring the development system online while upgrading the production system. When the upgrade of both systems was completed, Essentialtalk Network brought the production system back online.

CONCLUSION

iChain has given Essentialtalk Network the flexibility to grow rapidly

without worrying about its security infrastructure. "I have a product that is independent of the operating system and the underlying hardware and the applications that I'm running. It simplifies the design of those very applications so if I find an application that runs best on a Linux box, then that's the application that I can plug in very transparently to our security infrastructure. [iChain] frees me up as a CIO to focus on what's best in every situation and gives me the flexibility in my future designs," says Szojka.

Szojka adds, "The software is transparent to what we're trying to achieve so it doesn't hinder us. It assists us. It's there all of the time where we forget about it because we know that it is there. A good analogy is: I need air to breathe; I expect that it will be there, and it is always there. I don't worry about [web security] so I can go about my task of running a communications company."

Sandy Stevens-Marymee is a technical writer for Technology Innovations Group Inc. She lives and works in San Diego, California. ●