Novell iManager
Keeping eDirectory Management Simple

by Linda Kennard

This year, like last year and the year before, Network Magazine selected Novell eDirectory as the Product of the Year for the best directory service. In its May 2002 Product-of-the-Year issue, Network Magazine praises eDirectory for being a scalable, cross-platform, standards-based directory service, and concludes that “despite eDirectory’s maturity and the network infrastructure’s changing circumstances, Novell continues to increase its flagship product’s power and applicability.” (You can find this article at www.networkmagazine.com/article/NMG20020429S0003.)

Network Magazine editors made this statement based on the enhancements, technical ingenuity, and significance to readers that they noted in eDirectory 8.6.1. However, the upcoming release of eDirectory 8.7 equally supports the editors’ claim. Naturally, only time will tell whether eDirectory 8.7 will be awarded the Product of the Year award for the fourth consecutive year, but one thing is certain: With eDirectory 8.7, Novell continues to increase the power and applicability of its flagship product.

Available in closed beta since May and due to be released later this year, eDirectory 8.7 features a number of new enhancements. Among the more notable of these new features is web-based management of your eDirectory tree made possible through a new management interface: Novell iManager 1.5.

Fuelled by Novell’s goal to simplify access to and management of eDirectory, Novell iManager enables you to use a browser and, in some cases, a handheld device to manage your company’s eDirectory tree. Using Novell iManager, you can access this eDirectory tree over wired or wireless connections to an intranet, an extranet, or the Internet.

In addition to enabling wired and wireless eDirectory administration, Novell iManager also enables role-based (or delegated) administration. In essence, what this means is that using Novell iManager, you can farm out specific sets of eDirectory administrative tasks to users. These users, in turn, can access eDirectory to complete these tasks—and they don’t need a thorough understanding of the directory to do so.

BRINGING TIERS TO THE ...

Novell iManager ships on one of two eDirectory 8.7 CDs. One CD contains the traditional eDirectory components and includes ConsoleOne. The other CD, referred to as the web application CD, includes Novell iManager and Novell eGuide.

You can install the traditional eDirectory 8.7 components, as well as Novell iManager, on one server. However, Novell expects that most customers will prefer to run eDirectory on back-end servers and to run Novell iManager on web servers. This setup reflects the common three-tiered architecture on which Novell iManager is based:

- Tier one is the browser or handheld device.
- Tier two is the middleware server, which, in this case, is the web server running Novell iManager.
- Tier three is the backend server, which, in this case, is running eDirectory.

Tier One

Novell iManager enables you (and users to whom you assign rights) to access your company’s eDirectory tree using the following browsers:

- If you are running Windows NT, 2000, 98, or 95, you can use Microsoft Internet Explorer 5.5 with Support Pack 2 and above and Netscape 6.2 and above.
- If you are running Windows XP, you can use Microsoft Internet Explorer 6.0 (which ships with XP).
- If you are running Solaris, you can use Netscape 6.1.
- If you are running AIX, you can use Netscape 4.6.

Note. You can access Novell iManager using Netscape 4.6 and 4.7 on a Windows platform. However, when you use Netscape 4.6 (on Windows or AIX) and Netscape 4.7 (on Windows), Novell iManager automatically opens in Simple mode. Novell iManager provides the same functionality in Simple mode as it does in its regular mode but has a more basic interface in this mode.

You can also use Novell iManager to access eDirectory 8.6 and 8.7 trees from some handheld devices, namely Windows CE and...
Pocket PC devices. Novell plans to develop a Novell iManager web-clipping application for Palm OS devices and is working on enabling you to use Novell iManager from cell phones.

**Tier Two**

Novell iManager supports any of the following web server platforms:

- A pache 1.3.20 web server or higher. (You can download at no cost the latest version of the Apache web server from the Apache Software Foundation web site at http://httpd.apache.org/dist.)
- Tomcat 3.2.3 or higher. (You can download the latest version of Tomcat web server from the Jakarta Project web site at http://jakarta.apache.org.)
- Microsoft Internet Information Server (IIS) 4.0 on Microsoft Windows NT or IIS 5.0 on Microsoft Windows 2000.

**Tier Three**

Novell iManager enables you to manage eDirectory 8.7 backend servers. You can also manage eDirectory 8.6 servers. However, you can complete more administrative tasks on an eDirectory 8.7 server than you can complete on an eDirectory 8.6 server.

Specifically, using Novell iManager, you can run traditional eDirectory utilities, such as DSREPAIR, only on eDirectory 8.7 servers. The reason for this is simple: eDirectory 8.6 servers do not include eDirectory Management Box, or eM Box (pronounced em-box), a new eDirectory 8.7 component.

Written in C and C++, eM Box basically wraps and puts a common set of application programming interfaces (APIs) on the traditional eDirectory utilities. These APIs enable you to access the utilities' functionality from a browser or, depending on the utility, a handheld device. The subcomponents of eM Box are the traditional eDirectory utilities, which in this context Novell collectively refers to as eM Tools. eM Box runs as part of NetWare 6 or part of the Directory Host (Dhost) on non-NetWare platforms. (For more information about eM Box, see the "When eM Box Gets Involved" section on p. 16.)

WHAT CAN YOU DO FROM A BROWSER?

Which administrative tasks can you complete or enable users to complete using Novell iManager? When you or users use Novell iManager to access an eDirectory 8.7 or 8.6 tree from a browser, you can complete all of the eDirectory operations that you can complete using ConsoleOne (assuming you have the necessary rights), with two exceptions: You cannot manage NetWare server resources from Novell iManager (although you can launch NetWare Remote Manager), and you do not have reporting capabilities.

Aside from these two exceptions, you can complete every eDirectory operation—and more—using Novell iManager that you complete using ConsoleOne. (To view a list of the types of administrative tasks you can complete using Novell iManager from a browser, see the left window in Figure 1 on p. 8.)

More specifically, with the appropriate rights, you can use Novell iManager from a browser to perform the following administrative functions:

---

Please visit our advertiser **St. Bernard Software**

On eDirectory 8.6 Servers
• You can create and modify dynamic groups. (For more information about dynamic groups, see “Get a Group” on p. 10.)
• You can create, delete, and modify static groups.
• You can create, copy, move, rename, delete, and modify eDirectory objects.
• You can create new User accounts, clear lockouts, and reset passwords for existing User accounts.
• You can create and delete Lightweight Directory Access Protocol (LDAP) objects.
• You can manage Novell Modular Authentication Service (NMAS) users, login sequences, and login methods.
• You can create, move, and merge partitions and view partition information.
• You can manage replicas.
• You can create filtered replicas by using the Filtered Replica Wizard.
• You can manage passwords.
• You can manage public key infrastructure (PKI) certificates, including creating user certificates, server certificates, and certificate authorities; issuing certificates; and creating trusted roots, among other things.
• You can modify trustees, inherited rights filters, and trustees' rights to other objects.
• You can manage the directory schema (by creating and deleting attributes and classes, among other things).
• You can launch NetWare Remote Manager.
• You can create and delete Lightweight Directory Access Protocol (SNMP) objects.
• You can manage passwords.
• You can manage public key infrastructure (PKI) certificates, including creating user certificates, server certificates, and certificate authorities; issuing certificates; and creating trusted roots, among other things.
• You can modify trustees, inherited rights filters, and trustees' rights to other objects.
• You can manage the directory schema (by creating and deleting attributes and classes, among other things).
• You can launch NetWare Remote Manager.
• You can create and delete Lightweight Directory Access Protocol (SNMP) objects.
• You can manage passwords.

On eDirectory 8.7 Servers
• You can complete all the tasks you can complete on eDirectory 8.6 servers.
• You can run the new backup and restore utility, Backup eM Tool. (For more information on Backup eM Tool, see “Some Like It Hot: Backing Up Novell eDirectory 8.7” on p. 18.)
• You can run the DSMERGE utility.
• You can run the DSREPAIR utility.

WHAT CAN YOU DO FROM A HANDHELD DEVICE?
Using Novell iManager from a Windows CE or Pocket PC device, you can complete a limited number of administrative tasks, assuming you have the necessary rights. Novell engineers enabled fewer tasks from handheld devices simply because they believe customers will want to perform fewer tasks from such devices.

For example, says James Whitchurch, Novell director of software engineering for eDirectory, “we don’t believe customers will want to do partition management from a handheld.” Tasks such as resetting passwords and running repairs are better suited for the handheld interface. Whitchurch adds. However, Novell is awaiting word from its customers regarding which, if any, additional tasks they’d like to see on their handhelds.

For now, you can complete the following tasks using Novell iManager from a handheld device:

Figure 1. Novell iManager enables you to manage eDirectory using a browser or, in some cases, a handheld device. When you log in, you choose the administrative task (from the list on the left) you want to complete.

Figure 2. Novell iManager supports role-based services, which enable you to assign particular users one or more roles. You associate each role with one or more specific administrative tasks. When these users log in to iManager, they see only the administrative task or tasks you’ve associated with this role.
On eDirectory 8.6 Servers
• You can reset passwords.
• You can access and use Service Manager, which allows you to stop and start eDirectory services such as LDAP.

On eDirectory 8.7 Servers
• You can complete all the tasks you can complete on eDirectory 8.6 servers.
• You can run unattended and local repairs.
• You can run Backup eM Tool.

DIRECTORY COMPLEXITY: NOW YOU SEE IT, NOW YOU DON’T
Whether you access Novell iManager from a browser or a handheld device, when you log in to Novell iManager, you will immediately notice that the interface takes a whole new approach to eDirectory. Rather than opening to the hierarchical structure of the tree, Novell iManager opens to a simple list of roles, which you can click to reveal tasks. (See Figure 1.) Reducing and simplifying eDirectory management is one of Novell’s long-term goals, toward which Novell iManager takes a giant step.

This goal to simplify eDirectory management stems in part from Novell’s understanding of an emerging class of eDirectory users. Traditional eDirectory users are administrators, like you, who thrive on technical detail and have what you might call a geek’s love of the guts of eDirectory.

The emerging class of eDirectory users does not have such a love. Who are these less directory-savvy users? These are the users to whom you grant a few administrative rights in an attempt to distribute the burden of managing your company’s network. For example, you may want the supervisor of a particular department to be responsible for resetting passwords (as necessary) for the users within this department. These pseudo administrators have only a superficial understanding of the directory—if any understanding at all.

Unfortunately, using today’s eDirectory management interface, ConsoleOne, requires more than a superficial understanding of the directory. In fact, using ConsoleOne requires an intimate understanding of eDirectory trees, trustees, access control lists, and other directory-specific details. In other words, using ConsoleOne, says Whitchurch, requires a “carnal knowledge of the directory.” (This phrase “makes people cringe,” Whitchurch admits. “But it gets their attention.”)

Pass Out the Roles
With Novell iManager, Novell has hidden the complexity of the directory through role-based services. In a nutshell, role-based services enable you to assign particular users one or more roles. For each role you create, you associate one or more administrative tasks. When users log in to the directory using the password associated with their assigned role, they see only the tasks associated with this role.

Whitchurch offers this example. Suppose user James has two roles: one role as an administrator and one role as a password-only administrator. When James logs in to the tree as ADMIN, he sees a full set of tasks—the tasks assigned to his role as ADMIN. (See Figure 1.) When James logs in to the tree as James (the password-only administrator), he sees only one task in the left window of the Novell iManager interface: Password Management. (See Figure 2.)

Role-based services serve a two-fold purpose: First, they reduce eDirectory management by giving you control over who does what administratively in eDirectory. Second, they reduce the complexity of the directory for users.

Sound Familiar?
As you may know, Novell has offered flavors of role-based services in the past. For example, using ConsoleOne to access eDirectory 8.6.1, you can configure role-based services that are accessible through ManageWise. However, as Whitchurch points out, these previous variations of role-based services were specific to a product. In other words, you created roles (using ConsoleOne) for certain users who could then use a product, such as ManageWise, to perform administrative tasks relevant to that product.

With Novell iManager and eDirectory 8.7, in contrast, Novell has taken role-based services to the directory. In other words, using Novell iManager, you create roles for certain users, who can then use Novell iManager to perform administrative tasks in eDirectory.

Please visit our advertiser Biscom at www.biscom.com.
ConsoleOne does not lend itself, as does Novell iManager, to using role-based services. Despite the rights or lack thereof that you've assigned a particular user, when he or she logs in to the tree using ConsoleOne, that user sees more than the specific tasks he or she has been assigned.

With ConsoleOne, you get "the full meal deal," W hitchurch explains. "Even if you don't have rights to do certain things in the directory—for example, to manage DirXML—the snap-ins for those functions are loaded, and you are presented with a huge number of things that you have to sort through in order to find the assignments that you have rights to do."

The availability of role-based services for eDirectory management may be particularly exciting to you, depending on how you've attempted to delegate eDirectory administration in the past. W hitchurch cites an example of one Novell customer who attempted to delegate administration by removing different sets of snap-ins from ConsoleOne to create customized ConsoleOne packages for various users. The point of creating these packages was to minimize the complexities of the directory for these users. Novell iManager automatically minimizes (in fact, arguably eliminates) these complexities based on the roles that you assign users.

**Plugging in Tasks**  
When you install Novell iManager (as part of eDirectory 8.7), several roles are created by default—for example, eDirectory Administration and Schema Management. (For a complete list of the default roles, see the left window in Figure 1 on p. 8.) These roles are represented in the eDirectory tree as rbsRole objects.

Tasks associated with the eDirectory Administration role, like all other Novell iManager roles, are exposed through Novell iManager plug-ins. Novell iManager plug-ins are software packages that provide users with an interface for completing

---

**Get a Group**

Have you heard about or perhaps experimented with dynamic groups in Novell eDirectory? The dynamic group feature was first available in eDirectory 8.6.1. However, because ConsoleOne was not aware of dynamic groups, you could manage dynamic groups only programmatically using Lightweight Directory Access Protocol (LDAP). (For more information about managing dynamic groups using LDAP see "How to Manage and Use Dynamic Groups in Novell eDirectory" Novell AppNotes, Apr. 2002. You can download this article from http://developer.novell.com/research/appnotes/2002/April/05/a020405.htm.)

With the release of eDirectory 8.7, managing the dynamic group feature is significantly easier: Novell iManager provides an interface for managing dynamic groups.

What are dynamic groups? In terms of their purpose, dynamic groups are the same as the static groups to which you've grown accustomed. That is, in eDirectory, you can create Group objects and make other eDirectory objects members of this group for the purpose of easing administrative tasks.

For example, you may have created an Accounting Group object, which includes as its members only User objects representing the accounting employees within your organization. Perhaps you created this group to control access to a particular facility or room. Because your organization has multiple accounting employees—maybe as many as 50 employees—using a Group object to control access rights to this facility or room is easier than assigning rights individually to each of the Group object’s 50 members.

The Group object concept is useful, but traditional static groups have a few problems. For example, suppose an accounting employee gets hired in a different department. Not only do you have to change the department attribute in this employee’s User object, but you also have to remove this User object from one Group object and add it to another Group object. Of course, making these changes isn’t difficult. It’s just a nuisance—and the more groups an employee belongs to, the bigger the nuisance. Enter dynamic groups. Unlike static groups, membership lists for dynamic groups are computed on-the-fly, based on a set of search criteria rather than a pre-established list. When you create a dynamic group, you specify members by using a search filter that defines which object attributes members of this group have in common. You also have the option to modify the membership list by manually excluding or including particular objects.

For example, suppose you replaced the static Marketing group with a dynamic Marketing group. The dynamic Group object would specify that members of the Marketing group should include all employees that have “marketing” in their department attribute. eDirectory would then compute the membership list for the Marketing group when (and only when) eDirectory or other applications access this group. As a result, you no longer have to manually add and delete members to and from a Group object. You simply specify the search criteria, and eDirectory generates an always-current membership list on an as-needed basis.

Not only that, but when you create or delete User objects, you no longer have to open each Group object to which an individual User object belongs or should belong. Furthermore, because dynamic membership lists aren’t stored, dynamic groups with large membership lists consume less storage.

Synchronizing dynamic groups rather than static groups is a bit more efficient a well: After all, with a dynamic group, eDirectory servers only need to transfer the search filter. With a static group, in contrast, eDirectory servers need to transfer each individual member.

However, be advised that dynamic groups are not without disadvantages. For example, because a query must take place to generate a membership list, dynamic group operations are performed slower than static group operations. Also, the NetWare file system and bindery aren’t yet aware of dynamic groups, so you can’t use dynamic groups to simplify the task of controlling rights to NetWare volumes.
Please visit our advertiser **Visual Click** at www.visualclick.com.
various tasks. For example, Novell engineers created plug-ins for the traditional eDirectory utilities, such as the eDirectory Repair plug-in. The eDirectory Repair plug-in (like the plug-ins for other traditional eDirectory utilities) installs automatically with eDirectory 8.7. This plug-in exposes a total of seven tasks, which map to the options that are available in the command-line DSREPAIR utility:

- Basic Repair
- Repair via iMonitor
- Replica Repair
- Replica Ring Repair
- Schema Maintenance
- Server Repair
- Sync Repair

Novell engineers associated these tasks, as well as the tasks exposed through other eDirectory utility plug-ins, with a role called eDirectory Maintenance Utilities. Hence, if you assign a user the eDirectory Maintenance Utilities role (one of Novell iManager’s default roles), this user will see all of the tasks associated with that role, which include not only the DSREPAIR tasks listed above but also the tasks exposed through the DSMERGE and Backup eMTool plug-ins.

The eMFrame SDK

Novell iManager ships with the following plug-ins:

- DSREPAIR plug-in
- DSMERGE plug-in
- Backup eMTool plug-in
- Information and Content Exchange (ICE) plug-in
- LDAP plug-in
- Schema Manager plug-in

Each iManager plug-in provides users with an interface to complete a specific task or set of tasks in eDirectory. For example, the Backup eMTool plug-in provides users with an interface to run this new backup and restore utility. Similarly, the Schema Manager plug-in provides users with an interface for managing the eDirectory schema.

To develop these and other plug-ins, Novell engineers used the eDirectory Management Framework or eMFrame (pronounced em-frame) software development kit (SDK). As you would expect, you can use the eMFrame SDK to write your own iManager plug-ins. The eMFrame SDK enables you to write a Novell iManager plug-in using any of the following languages:

- Java
- Java Script
- HTML

Alternatively, you can use Novell iManager’s plug-in wizard, which is referred to as the Task Builder. This wizard generates an HTML file based on your input without requiring you to write any code. In addition to generating this interface, the Task Builder prompts you to associate this interface with a task and to assign that task to a user. “In five minutes,” Whitchurch claims, “you can effectively have a task that people could access to get to information and to read and write to eDirectory.”

Figure 3. Novell iManager is based on the eDirectory Management Framework (eM Frame). eM Frame runs on your web server and includes plug-ins that access either the eDirectory Management Toolbox (eM Box) or the eDirectory database directly via various SDKs, including the eM Box, LDAP, and eDirectory SDKs.

Figure 4. When the eM Box SOAP service receives an event from eM Frame, it publishes that event on an event bus. The eM Tool that subscribed to the event receives the event and performs the requested action.
Getting Things Role-ing

You can simply use the default roles and their associated tasks as is, or you can customize the roles. For example, you can add to or delete from the list of tasks associated with each role. You can also create new roles with your own custom set of tasks.

Whether you use the default roles or create roles of your own, to delegate administration, you need to assign members to roles. Members can be all of the users in a particular container or group object, or they can be individual user objects. For each member, you also need to specify the scope of this role—that is, the area of your eDirectory tree where you want this member to perform this task.

For example, suppose you wanted to enable user Fred to perform Backup Configuration, Backup, and Restore tasks on the servers in your company's Tokyo office. To do so, you would create a role called Backup Administration. To create a role, you would log in to Novell iManager and click the Configure icon. (The Configure icon is the picture of the person behind a desk near the middle and at the top of the Novell iManager window. See Figure 1 on p. 8.)

When you click the Configure icon, you see the configuration options for role-based services in the left window. To create this new role for Fred, you would click the Role Configuration option, and from the newly exposed list, you would click Create Novell iManager Role. To finish creating the role, you would complete these steps:

1. Name the role (in this case, Backup Administration), and specify the rbsCollection object (for example, Role Based Service.xyzcorp) where this role will be stored. rbsCollection objects are container objects that store role-based services objects. (For more information about collections, see “RBS Objects” on p. 16.) Click Next.
2. Click to select tasks from the list of those available to associate Backup Configuration, Backup, and Restore tasks with the Backup Administration role. Click Next.
3. Enter the name of the container, group, or user object you want to be a member of this role. In this case, you could click the Browse button, click Search, and then find and click user.Fred.
4. For each role member, specify the context of the eDirectory tree where you want this member to perform the Backup Administration role. In this case, you would click the Browse button, click search, and then find and click the Tokyo container.

Two things happen when members are assigned to a role: Members see this role and its associated tasks when they log in to Novell iManager, and they also receive the rights necessary to complete these tasks. Thus, when user Fred logs in to Novell iManager, he will see in the left window the Backup Administration role (and any other role that he's been assigned). When he clicks this role, he will see the Backup Configuration, Backup, and Restore tasks you associated with this role. He will then be able to perform these tasks only on servers in the Tokyo container.

Novell iManager in Action

Suppose that user Fred wants to run a backup on Server_A in the Tokyo container and that Server_A is a Windows NT server running eDirectory 8.7. When Fred enters the URL in his browser for his network's Novell iManager server, a Novell iManager servlet intercepts the request and informs the web server that...
Please visit our advertiser Novell Inc. at www.novell.com.
Please visit our advertiser Novell Inc. at
the request from Fred's browser is intended for Novell iManager. When Novell iManager receives the request, it creates a sort of note-to-self in cache, indicating the type of device (in this case, a browser) this request came from.

Novell iManager next returns the login screen to Fred's browser. Fred enters his credentials and clicks Log In. Novell iManager passes Fred's credentials to the eDirectory 8.7 server. This server compares the entered credentials against what is stored in the database and returns, in this case, a message indicating that Fred has the necessary rights. The message also indicates that Fred has rights to see the backup and restore tasks associated with this role in the Tokyo container.

Novell iManager accordingly not only authenticates Fred but also loads the Backup and Administration role, enabling Fred to see only the Backup and Administration role and the Backup Configuration, Backup, and Restore tasks associated with this role. Fred clicks Backup and, on the first screen, is prompted to enter the name of the server on which he wants to run the backup. In this case, Fred either enters Server_A or, if Fred can't remember the name of the server, clicks the Browse button. When Fred clicks the Browse button, he opens the Object Selector box, which enables him to search the Tokyo branch of the eDirectory tree. Fred completes the remaining fields and ultimately clicks Start to initiate the backup procedure.

When eMBox Gets Involved

When Fred clicks Start, the Backup eMTool plug-in on the Novell iManager server turns Fred's request into an HTTP post bound for eMBox on Server_A. Next Novell iManager forwards Fred's request via the eMBox SDK to the HTTP stack within Directory host (Dhost) on Server_A. (See Figure 3 on p. 12.)

The stack, in turn, forwards the request to the Simple Object Access Protocol (SOAP) service running on the Dhost as part of eMBox. SOAP specifies exactly how to encode an HTTP header and an XML file so that a program on one computer can call a program on another computer running the same or a different operating system and pass that program information. SOAP also specifies how the called program can return a response. (For the latest version of the SOAP specification, visit www.w3.org/TR/soap12-part1.)

The SOAP service opens the request and basically posts the request as an event on the event bus, to which every eMTool register interest in specific types of events. (See Figure 4 on p. 12.) A listener on the event bus, eMTools hear about new events. Because the request was for a Backup, Backup eMTool hears and retrieves this event, performs the requested action, and sends the result to the SOAP service.

KEEPING THINGS SIMPLE

Novell iManager reduces and simplifies eDirectory administration in several ways. For one thing, Novell iManager reduces eDirectory management by enabling you to distribute the management burden: You can assign users roles, which are associated with one or more administrative tasks.

For users, Novell iManager simplifies the potential complexity of the eDirectory tree. Users with assigned roles access the eDirectory tree from their browser or handheld device (depending on the task they need to complete) and see only their assigned role or roles and associated tasks.

Novell iManager further simplifies eDirectory management for you by enabling you to access eDirectory from virtually anywhere and to complete several administrative tasks, including running traditional eDirectory utilities.

Of course, if you're a techno-geek, reduced complexity might strike you as bad news. If this is the case, you may be relieved to learn that Novell iManager continues to support command-line access, which it now enables both locally and remotely. Techno-geek or no techno-geek, you (like all network administrators) appreciate tools that simplify your work—and Novell iManager does precisely that.

Linda K. Ennard works for Niche Associates, which is located in Sandy, Utah.