NDS-Enabled Products

Ted Lloyd

Because directory services are becoming a foundation technology for both corporate networks and the Internet, more and more developers are making their products directory enabled. And because Novell has the leading directory service, these developers are particularly interested in enabling their products to work with Novell Directory Services (NDS).

Of course, this is good news for you, the consumer. NDS-enabled products offer several benefits. For example, by purchasing NDS-enabled applications, you can minimize the number of times users have to enter a username and password to access the information and the resources they need. You can also control users’ rights to access applications through NDS.

In addition, you can manage NDS-enabled products from a central location. For example, you can create an object for each NDS-enabled application, and you can then use Novell's NWADMIN utility to manage the application. You can also grant users rights to access that application, just as you grant users rights to access other network resources. Because NDS-enabled products can use NDS for authentication and centralized management, these products are easier to manage than products that are not NDS enabled.

To help you identify and purchase products that support NDS, Novell offers a new Directory Enabled logo. If a company's product passes Novell's compatibility testing, the company can use the Directory Enabled logo to verify that the product supports NDS.

Literally hundreds of products and applications are NDS enabled. Since we cannot feature all of these products in this article, we have selected a few that are particularly interesting. Most of the products featured provide security services for your company's network or for its web site. For more information about Novell certification testing or for a list of the NDS-enabled products that have been Novell certified, visit http://developer.novell.com/sitemaps/yes.html.

INTRUDER ALERT 3.0.1 FOR NETWARE

Intruder Alert 3.0.1 for NetWare is from AXENT Technologies Inc. is a real-time, rules-based centralized host detection system. To keep you one step ahead of hackers, Intruder Alert 3.0.1 combines three standard intrusion-detection methodologies to protect your company’s network:

• 24-by-7 real-time, device-level activity monitoring
• Post-event audit trail review
• Packet/segment monitoring

To help you determine what events should be monitored, Intruder Alert 3.0.1 provides Drop and Detect security policies. Intruder Alert 3.0.1 monitors NetWare file system events, operating system events, and NDS events and compares these events against the Drag and Drop security policies. If Intruder Alert 3.0.1 detects a problem, it notifies you immediately.

To ensure that your company is protected against the latest types of network attacks, AXENT periodically updates its Drag and Drop security policies and posts these updates on its web site. You can also use Intruder Alert 3.0.1 to create customized security policies to meet the needs of your particular company.

Intruder Alert 3.0.1 supports NetWare 5, 4.2, 4.11, 3.2, and 3.12. For more information about Intruder Alert 3.0.1, visit http://www.axent.com. To find a sales office in your area, visit http://www.axent.com/Axent/Resellers. You can also call 1-301-258-5043 or 1-888-44-AXENT.

SITEMINDER 3.6

SiteMinder 3.6 from Netegrity Inc. enables you to define rules and policies that determine who can access the applications running on your company’s web site. With SiteMinder 3.6, you can also delegate administrative tasks to particular web masters. For example, you can assign one web master administrative rights to manage all of the partners that access your company's web site.

In addition, SiteMinder 3.6 provides single sign-on to all of the applications running on your company's web site. SiteMinder 3.6 stores users' credentials, or identity, in an encrypted cookie. If an authenticated user tries to access another application or even another web server on your company's web site, SiteMinder 3.6 uses these credentials to authenticate the user.

SiteMinder 3.6 also allows you to add authentication services to your company's web site. SiteMinder 3.6 supports a wide range of authentication methods, including passwords, token cards, X.509 public-key certificates, custom forms, or a combination of these methods.

SiteMinder 3.6 takes advantage of your company's existing NDS tree. For example, SiteMinder 3.6 uses NDS to extract information about users and their group membership, rather than using its own separate database. As a result, you only need to manage information in one database.

SiteMinder 3.6 supports NetWare 4.11. For more information about SiteMinder 3.6, visit http://www.netegrity.com. You can also call 1-800-325-9870 or 1-781-890-1700.
WEBCONSOLE 3.0

WebConsole 3.0 from PatchLink.com Corp. (formerly called HiTecSoft Corp.) is a standalone, remote management product. With WebConsole 3.0, you can use a web browser to manage NetWare 5, 4, and 3 servers via the Internet or your company’s intranet.

After authenticating to NDS, you select the type of management task you want to perform from a task bar on WebConsole 3.0’s main screen. WebConsole 3.0 then enables you to perform management tasks such as the following:

- View and error log, enter server-console commands, and generate reports (via a Java-based RCONSOLE screen)
- Reboot servers
- Load and unload NetWare Loadable Modules (NLMs)
- Mount and dismount volumes
- View statistics about server connections, including address information, a list of open files, and login and logout times
- Edit server configuration files
- Clear unwanted server connections
- Edit boot sequence files
- Edit text files
- View, create, and delete file and directory information
- Modify file trustee rights

WebConsole 3.0 supports NetWare 5, 4, and 3. For more information about WebConsole 3.0, visit PatchLink.com’s web site (http://www.patchlink.com). You can also call 1-888-970-1025 or 1-602-970-1025.

SECURECONSOLE 3.11B FOR NETWARE

SecureConsole 3.11b for NetWare from Protocom Development Systems Ltd. enables you to control and monitor users’ access to NetWare server consoles. With SecureConsole 3.11b, you can grant certain users or groups rights to access a server console, and you can limit these users or groups to using certain commands or applications.

Because you can grant different levels of access to individual users, you can delegate administrative tasks and continue to maintain tight security. For example, you can limit a tape backup administrator to using only tape backup commands and applications. SecureConsole 3.11b would then prevent this user from using other commands and applications at the server console.

SecureConsole 3.11b acts as a screen saver at the server console, prompting users to enter their NDS username and password. SecureConsole 3.11b then verifies these usernames and passwords through NDS or bindery emulation.

If a user is authorized to access the server console, SecureConsole 3.11b unlocks the server console and then verifies the user’s actions against a list of commands and applications that you have authorized this user to use. SecureConsole 3.11b also maintains a log that contains every authorized and unauthorized command that is entered by each user who logs in to the server console.

In addition, you can configure SecureConsole 3.11b to send an alert to any network management console that
supports the Simple Network Management Protocol (SNMP) if an unauthorized user tries to access the server console.

In addition, SecureConsole 3.11b now includes SecureRemote, which secures remote server sessions. To prevent hackers from stealing passwords and other sensitive information, SecureRemote encrypts remote access server sessions. (SecureRemote supports both IP and IPX.) SecureConsole 3.11b supports NetWare 5 and 4. For more information about SecureConsole 3.11b, visit Protocom's web site (http://www.serversystems.com). You can also call 1-800-581-3502 (in the United States and Canada), 2-6208-4888 (in Australia), or 01454-777-654 (in the United Kingdom).

BINDVIEW EMS

BindView Enterprise Management System (EMS)/NOSadmin 6 from BindView Development Corp. is a client-server utility that allows you to manage the security and integrity of your company's network from a Windows NT, 98, 95, or 3.x workstation. You can also use BindView EMS/NOSadmin 6 to isolate and troubleshoot security risks and configuration problems on your company's network.

With BindView EMS/NOSadmin 6, you can conduct a complete security assessment of the entire network, analyzing passwords, users' rights, network administrators' rights, and the NDS tree. For example, you can determine which users have rights to access mission-critical data. You can also determine how these rights flow down the NDS tree. You can then revoke these rights for users who do not need to access the data.

In addition, you can use BindView EMS/NOSadmin 6 to analyze configuration issues, such as SET parameters and the usage of hard drive space. You can also compare the configuration of each server against your company's standards, and you can add, delete, or update NLMs or other files on multiple servers. You can even use the configuration tools that come with BindView EMS/NOSadmin 6 to deploy Novell's AUDITCON utility, and you can generate query- and presentation-level reports based on the information the AUDITCON utility gathers.

BindView EMS/NOSadmin 6 supports NetWare 5 and 4. For more information about BindView EMS/NOSadmin 6, visit BindView Development's web site (http://www.bindview.com). You can also call 1-800-749-8439 or 1-713-881-9100.

CONCLUSION

More and more developers are making their applications NDS enabled. And of course, the more NDS-enabled applications that developers create, the more NDS-enabled applications you have to choose from.

Novell rewards the most innovative developers through its ongoing Novell Developers' Contest. To check out the most recent winners of this contest, visit Novell's DeveloperNet web site (http://developer.novell.com/contest/spotlight.htm). We will also feature the winning products in a future issue.