During the many years I have spent consulting, teaching, and writing about NetWare and Novell Directory Services (NDS), there is one question people ask me most often: “Does NetWare provide a simple way to find out when an unauthorized user has been given administrative access to my company’s network?” My answer has always been the same: “Simple? No, but there are ways to find out...” I then launch into a lengthy discussion of the time-consuming methods of finding this information: “You can check each user’s Access Control List (ACL), inherited rights, group memberships, security equivalences, occupational roles, audit logs...” Usually the person’s eyes will glaze over about halfway through my answer.

If you have asked this question or faced this dilemma in the past, I have great news for you: With NetVision’s DirectoryAlert 2.5, you can be instantly notified when someone grants a user unauthorized access to your company’s network. You can also find out who granted the access and even from what station the access was granted. With DirectoryAlert, you catch NDS security violations when they occur, instead of after real damage has been done.

WHO HAS ACCESS TO YOUR COMPANY’S NETWORK?

Tracking the level of access users have to your company’s network is a daunting task. This task becomes especially difficult if your company has expanded its network to the Internet. In this case, your company’s user base may now include employees, customers, suppliers, and other business partners.

More often than not, network security breaches are caused by authorized users performing unauthorized tasks. These users have valid user accounts but have somehow acquired more rights than they should have. For example, suppose Jeff discovered that the network administrator had logged in to the network and left his workstation unattended. With little effort, Jeff could grant himself ADMIN rights to the entire network. With complete access to the network, Jeff could access sensitive company information and could perform any type of malicious act on the network.

In addition to monitoring authorized users, you must monitor the products that authenticate to the network through non-User object classes. These products extend the NDS schema and then authenticate to the network using a product-specific object. How do you know if these products pose a potential security breach?

With DirectoryAlert, you can address these security issues in a proactive manner by monitoring NDS event activity you consider unusual or suspicious. DirectoryAlert then sends reports that contain information about this event activity to the sources you identify.

You can configure DirectoryAlert to report event activity to text files, Extensible Markup Language (XML) files, LDAP Data Interchange Format (LDIF) files, pager, Open Database Connectivity (ODBC) compliant databases, NDS objects, and e-mail addresses. When DirectoryAlert reports an event, it includes information such as who changed an object, when the object was changed, and what change was made.

You can also configure DirectoryAlert to include information about the value of an attribute before the change was made and the new value. You can then use this information to reset an attribute if necessary.

MONITORING NDS ACTIVITY

With DirectoryAlert, you can monitor NDS events such as schema changes, logins and logouts, attribute changes, object creations, deletions, moves, and renames. (See Figure 1 on p. 40.) The following sections give some examples of the NDS events you can monitor with DirectoryAlert.

ACL Changes

By monitoring changes made to any object’s ACL, DirectoryAlert can notify you if someone grants a user additional NDS object or property rights or if someone grants a user inappropriate rights. For example, DirectoryAlert can immediately notify you when someone grants a user administrative access to your company’s network. This immediate notification allows you to verify that the person receiving the rights is an authorized individual, rather than a disgruntled employee with malicious intentions.

Monitoring ACL changes is also one way to monitor non-User object classes for inappropriate access.

To ensure that no one grants a user inappropriate rights through that user’s ACL, you can configure DirectoryAlert to monitor ACL changes such as the following:
• Granting the Supervisor right or granting all rights except the Supervisor right to NDS objects or properties
• Granting the Write or Add Self property right to certain object properties such as membership lists
• Changing the ACL of the [Root] object
• Changing the ACL of a Country, Locality, Organization, or Organizational Unit (OU) object

Group Membership Changes
By monitoring changes to the membership list of any Group object, DirectoryAlert can notify you when users are added to the membership lists of sensitive NDS Group objects. To ensure that no one has received inappropriate network access through group memberships, you may want DirectoryAlert to monitor the following types of Group objects:

• Group objects that have Supervisor rights
• Group objects that have ADMIN equivalences
• Group objects that have access to confidential company information such as payroll information

Security Equivalence Changes
By monitoring the Security Equal To attribute of any NDS object, DirectoryAlert can notify you when a user receives inappropriate rights by being made security equivalent to another object in the NDS tree. For example, suppose User A has Supervisor rights to the [Root] object in the NDS tree and User A makes User B security equivalent to User A. Because User B then has all of the rights and privileges that User A has, User B has Supervisor rights to the [Root] object of the NDS tree.

To ensure that no one receives inappropriate access to the network by being made security equivalent to another user, you may want DirectoryAlert to monitor the following:

• The Security Equal To attribute of an object with Supervisor rights anywhere in the NDS tree
• The Security Equal To attribute of the ADMIN user
• The Security Equal To attribute of any object that is security equivalent to the ADMIN user
• The Security Equal To attribute of Organizational Roles

By monitoring the Security Equal To attribute of any object, you can detect when a user is added to the Security Equal To list of any object that has the rights listed above.

Login and Password Violations
By monitoring user login restrictions, user password restrictions, and intruder lockouts, DirectoryAlert can notify you of potential security breaches caused by login and password violations. DirectoryAlert can also monitor user logins and logouts and notify you of suspicious logins. For example, DirectoryAlert can notify you if a user who is ADMIN equivalent logs in to the network at 2 a.m. on Saturday.

• User accounts that are enabled or disabled
• User accounts that are locked out because of incorrect login attempts
• Passwords that are enabled or disabled
• Password expiration
• User accounts that do not require passwords
• Modifications to the date and time of password expiration
• Modifications of concurrent connection limits
• Last login times

NDS User Template Changes
By monitoring the changes made to User Template objects or the creation of User Template objects, DirectoryAlert can notify you if User objects created with a template have inappropriate access to the network. Because a User Template object defines the attributes NDS uses to create User objects, you should monitor User Template objects

Please visit our advertiser
Biscom
http://www.biscom.com/cd_offer

For more information, visit http://www.nwconnection.com/advertise.html.
for changes in all the areas identified previously. For example, to ensure that no security breaches occur through User Template objects, you should use DirectoryAlert to detect the following:

- Suspicious ACL rights
- Suspicious Group memberships
- Suspicious Security Equal To assignments
- Password violations

NDS Schema Modifications

By monitoring changes to the NDS schema, DirectoryAlert can notify you when a new object class is added to the schema or when an attribute is added or modified. In this way, you will know all of the non-User objects that are logging in to the NDS tree and the level of access these objects have.

DIRECTORYALERT COMPONENTS

Surprisingly, four relatively simple components perform all of DirectoryAlert’s sophisticated monitoring capabilities:

- Global Event Services Broker
- DirectoryAlert Service Agent
- Event Consumers
- Snap-in module for the NetWare Administrator (NWADMIN) utility

GLOBAL EVENT SERVICES BROKER

The main component of DirectoryAlert is the Global Event Services Broker, which runs as a NetWare Loadable Module (NLM) on NetWare 4.1 or above servers. (This NLM is called NVGES.NLM.) The Broker’s sole function is to globally monitor NDS events across the entire network. The Global Event Services Broker can monitor both predefined NDS events and user-defined custom events.

The Global Event Services Broker monitors the NDS events that you specify when you configure DirectoryAlert. If one of these NDS events occurs, the Global Event Services Broker reports the event to the DirectoryAlert Service Agent in real time.

When you install DirectoryAlert, the installation program creates a container object, called the NetVision Global Event Service object, in the [Root] object of the NDS tree. This container object holds all of the NDS event types supported by DirectoryAlert. (See Figure 2 on p. 42.)

Typically, you must write an application to manage custom events. To help you create such an application, NetVision provides the Global Event Services application programming interface (API).

Monitor Settings

As mentioned earlier, to enable NDS event monitoring on your company’s network, you identify the NDS events that you want DirectoryAlert to monitor and report. You can define multiple monitor settings, with each setting acting on different events in the NDS tree.

You define monitor settings by selecting the DirectoryAlert Server object in the NWADMIN utility and selecting Details. You can then select the Monitor Settings Tab, select New, and then select a Monitor Template. (See Figure 1.)

Monitor Templates are simply groups of events that perform specific monitoring functions (such as monitoring ACL changes at the [Root] of the NDS tree). You can add or remove events from the Monitor Templates, or you can define your own Monitor Templates.

GLOBAL EVENT SERVICE ADMINISTRATOR

To monitor and report NDS activity, the Global Event Services Broker logs in to NDS as a special User object called the Global Event Service Administrator. The DirectoryAlert installation program automatically creates this User object in the

Figure 1. Using DirectoryAlert, you can monitor specific NDS events. The Monitor Template enables you to configure which NDS events you want to monitor.
NetVision Global Event Service object and grants the User object the Supervisor object right to this container object. To give you administrative access to this container object and the types of the NDS events that can be monitored, the DirectoryAlert installation program prompts you to assign a password to the Global Event Service Administrator object.

**Modes of Operation**

The DirectoryAlert installation program installs the Global Event Services Broker on the servers you select. You can manually load the NLM on these servers or have the DirectoryAlert installation program automatically load the NLM.

How do you determine which servers should run the Global Event Services Broker? You must first choose the “mode” in which you want to run the Global Event Services Broker. The Broker can run in one of three modes, and you choose the mode when you load this NLM:

- **Mode 1.** When the Global Event Services Broker runs in Mode 1, DirectoryAlert can provide real-time monitoring of NDS changes, regardless of on which replica the change is made. Mode 1 requires you to run the Global Event Services Broker on every NetWare server that holds a read-write replica of partitions that you want to monitor. If you choose Mode 1 and you make changes to an NDS replica on a server that is not running the Global Event Services Broker, the events are not reported.

- **Mode 2.** If you choose Mode 2, you must load the Global Event Services Broker on at least one server that holds replicas of all of the partitions you want to monitor. When you run the Global Event Services Broker in this mode, monitoring the entire network is dependent on NDS synchronization, which may adversely affect DirectoryAlert’s performance. (Depending on the design and size of your company’s network, NDS synchronization may take some time. As a result, events may not be reported as quickly.)

- **Mode 3.** If you run the Global Event Services Broker in Mode 3, DirectoryAlert monitors only a single partition in the NDS tree. If you choose Mode 3, you must load the Global Event Services Broker on one or more servers that contain a read-write replica of the partition you want to monitor. In Mode 3, the Global Event Services Broker does not communicate with other Global Event Services Brokers that may be running on the network.

**Managing the Global Event Services Broker**

When you run the Global Event Services Broker on a server, you can monitor and manage the Global Event Services system from the console of that server. For example, you can view information such as the server memory being used by the Global Event Services Broker. You can also view general information about that server, such as user connection information and Server SET commands that relate to the Global Event Services Broker. You can also configure the Global Event Services Broker on that server. Changes made to the Global Event Services Broker on one server do not

---

For more information, visit [http://www.learnkey.com](http://www.learnkey.com)

---

**PRODUCTS**

DirectoryAlert 2.5

For more information, visit [http://www.nwconnection.com/advertise.html](http://www.nwconnection.com/advertise.html).
affect the Global Event Services Brokers on other servers on the network.

**DIRECTORYALERT SERVICE AGENT**

The DirectoryAlert Service Agent runs as a service on a Windows NT or Windows 2000 server or workstation. When you start the DirectoryAlert Service Agent, it registers with the Global Event Services Broker. Then when a change is made in NDS and that change triggers an NDS event that you want monitored, the Global Event Services Broker notifies the DirectoryAlert Service Agent. The DirectoryAlert Service Agent, in turn, reports the information to an Event Consumer.

**EVENT CONSUMERS**

Event Consumers provide the reports of monitored events that occur in NDS. Event Consumers can send reports to the following sources:

- Text files
- XML files
- LDIF files
- E-mails
- Pagers
- ODBC-compliant databases
- NDS objects
- Simple Network Management Protocol (SNMP) alerts

To install Event Consumers, you launch the NWADMIN utility, select the Details page of the DirectoryAlert object, and then select Installed Event Consumers. When you install Event Consumers, you determine the Event Consumers DirectoryAlert will use for reporting NDS events. You assign Event Consumers to specific monitored events when you create the monitor settings.

**NWADMIN SNAP-IN MODULES**

DirectoryAlert includes two snap-in modules for the NWADMIN utility: the DirectoryAlert snap-in module and the Global Event Services snap-in module. These snap-in modules add functionality to the NWADMIN utility, enabling you to define and to configure event monitoring on your company's NDS tree.

The Global Event Services snap-in module allows you to globally manage and configure Global Event Service Brokers on your company's network. The changes you make using the NWADMIN snap-in affect all of the Global Event Service Brokers running on your company's network. (If you want to make changes to only one Global Event Service Broker, you can make changes at the console of the server on which that Broker is running.)

DirectoryAlert includes snap-in modules for Windows 95, Windows NT, and the common 32-bit version of the NWADMIN utility.

**PUTTING IT ALL TOGETHER**

After you install DirectoryAlert and the Global Event Services on your company's network, you load the Global Event Services Broker on the appropriate servers. You then create monitor settings using the NWADMIN utility to define the various NDS events you want DirectoryAlert to monitor. DirectoryAlert registers the events you have defined with the Global Event Services Broker.

When a registered event occurs, the Global Event Services Broker notifies the DirectoryAlert Service Agent. The DirectoryAlert Service Agent sends the event to the Event Consumer specified for that monitor setting. The Event Consumer then reports the event to you in the manner you have defined: e-mail, pager, log file, and so on.

**DSMEDIC**

DirectoryAlert also includes a set of diagnostic tools called DSMedic. Using DSMedic, you can check connection information, check for Global Event Services coverage, and test the status of the Global Event Services on the network.

When you install DirectoryAlert, the installation program automatically installs DSMedic and places a DSMedic option in the Start Menu of your workstation. To access DSMedic from your Start Menu, select Programs/DirectoryAlert, and then select DSMedic.

**CONCLUSION**

If you want to stay on top of what is happening on your company's network at all times, NetVision's DirectoryAlert is exactly the product you need. With DirectoryAlert, you can proactively monitor NDS activity on the network. As a result, you can prevent network security breaches by acting on unusual or suspicious activity when it happens rather than after real damage has been done to the network.

If you would like to test drive DirectoryAlert, you can download a free 30-day trial version from NetVision's web site at http://www.netvision.com.

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