

# Monitoring AD Changes

Randy Franklin Smith

(Reprinted from WindowsItPro Magazine)

Active Directory (AD) is the epitome of a mission-critical infrastructure system. Often, the highest-level AD object—a forest—corresponds to the enterprise itself. One mistake can cause an enterprisewide catastrophe. The more administrators you have, the greater the chance that "too many chefs can spoil the stew." Obviously, you need effective AD monitoring, and the need becomes even more evident when you take into account intrusion attempts from the outside and by disgruntled IT staff members.

Additionally, you can take advantage of AD's delegation-of-control features to empower local administrators and managers to assign group memberships and perform other simple maintenance tasks that you've always performed because you've been afraid of losing control over them. The ability to effectively monitor what the people you delegate authority to are doing with it helps you to assuage your fear and stay in command.

You can stay on top of what's happening in AD and who's changing what by using two audit categories: account management and directory service access. Account management auditing provides notification of high-level changes (i.e., creations, deletions, and other changes) to user accounts, computer accounts, and groups. Account management auditing also tracks some account policy-related changes.

Directory service access auditing provides low-level, field-by-field change notification. For any high-level change that account management auditing tracks, directory service access auditing generates several events, but when available, account management events are almost always easier to understand and are more informative. Therefore, the general rule of thumb is to use account management auditing when available and directory service access auditing for activity that account management auditing doesn't track. If you're interested in monitoring local users and groups on a member server, you can use account management auditing but not directory service access auditing.

## Account Management Auditing

To enable account management auditing, select Domain Controller Security Policy under Administrative Tools; maneuver to Security Settings, Local Policies, Audit Policy; and enable Audit account management for success and failure. Account management auditing provides discrete event IDs for creation of, deletion of, and changes to users, computer, and group accounts. Table 1 lists account management event IDs.

**TABLE 1: Account Management Event IDs**

Account	Created Event ID	Changed Event ID	Deleted Event ID
User	Event ID 624	Event ID 642	Event ID 630
Computer	Event ID 645	Event ID 646	Event ID 647
Local group	Event ID 635	Event ID 639	Event ID 638
Global group	Event ID 631	Event ID 641	Event ID 634
Universal group	Event ID 658	Event ID 659	Event ID 662

Account management creation events can help you keep AD clear of redundant or nonstandard users, computers, and groups. Cleaning up redundant or unneeded objects soon after their creation is much easier than doing so down the road when no one remembers what the object was intended for or why it was created. You can spot-check creation events and audit new users, groups, and computers' compliance with your organization's policies and procedures. A new computer account means that

## Monitoring AD Changes

Randy Franklin Smith

(Reprinted from WindowsItPro Magazine)

someone is rolling out a new workstation or server into your domain. You can verify event ID 645 against your new-computer provisioning process to make sure the computer being added is authorized. You can use event ID 624 to track new users being added to the domain. Verify that the new accounts are legitimate user accounts, and enforce any policies you might have for naming conventions, employee/contractor documentation, or shared or application accounts.

You can also watch for event IDs 631, 635, and 658 to enforce naming convention policies on groups and to make sure that each group has a clearly indicated owner who's responsible for approving member additions and removals. A good place to document the owner of a group is the Managed By tab on the group's Properties dialog box, which lets you link a group to an AD user account. Most other AD objects' Properties dialog boxes also have a Managed By tab.

One problem with large AD deployments is keeping track of which access levels and resources a given group extends to its members. You can document this information in English in the Notes field of the General tab on the group's Properties dialog box. Or, you can use the two-level group method for access control that I wrote about in "Effective Access Control for Win2K and NT," October 2000, <http://www.winnetmag.com>, InstantDoc ID 15482.

Deletion of users, groups, or computers rarely presents a security risk, so you typically don't need to perform ongoing monitoring for deletion events. However, these events can be useful when you need to track down who accidentally deleted an important account or group or if you're worried about someone performing mass deletions of users or groups in a Denial of Service (DoS) attack.

Change events, on the other hand, can have important security implications, depending on which information about a user, group, or computer was changed. With a few exceptions, account management auditing provides only one change event ID for each object type; therefore, you can't tell what changed simply by the event ID—but, in some cases, the event details tell you more.

In general, for user accounts, account management auditing produces event ID 642 for any change made on the Account tab of a user object's Properties dialog box and provides specific text only for important security status changes such as disable or enable events. For example, if you change a user's description, you'll simply get an event ID 642 with the text User Account Changed but no further information. If you enable or disable an account, you get the same event ID 642 but with the additional information User Account Changed: Account Disabled. Having to look for more information in the event's details makes implementing automated monitoring or selective reporting more difficult; however, tools such as GFI Software's GFI LANguard Security Event Log Monitor (S.E.L.M.), NetIQ's AppManager Suite, and Microsoft Operations Manager (MOM) let you define rules and create reports based on event details.

Account management auditing does provide specific event IDs for a few user account changes. When someone with reset-password authority resets a user's password, you'll see event ID 628 (user account password set). When someone tries to change his or her own password, you'll encounter event ID 627 (change password attempt). After someone repeatedly attempts to log on with an invalid password, Windows 2000 Server locks out the account (assuming the domain has an account-lockout policy enabled) and produces event ID 644 (user account locked out).

You'll find frequent occurrences of event ID 643 (Domain Policy Changed: Password Policy modified), even if you haven't changed your password policy. This behavior is a bug in Win2K. Each time Win2K applies Group Policy, it doesn't check to see whether the new and old policies are actually different. It

# Monitoring AD Changes

Randy Franklin Smith

(Reprinted from WindowsItPro Magazine)

configures the password policy from the Default Domain Policy Group Policy Object (GPO), which triggers Win2K to report event ID 643. The bottom line is that you can ignore event ID 643.

Table 2 lists the specific event IDs that account management provides for adding members to and deleting them from each type of group list. Provided your organization grants users access to folders and other resources exclusively through groups, event IDs 632, 636, and 660 are extremely valuable because they let you track each instance of a user or group being granted new access. Figure 1 shows the details for an event that added a member to a universal group. The details report which group was affected (Target Account Name), who was added to the group (Member Name), and who performed the operation (Caller User Name). Given that information, you can follow up with the group's owner or through your support call tracking system to verify that the change is legitimate.

**Table 2: Event IDs for Adding Members to and Deleting Them from Groups**

Group Type	Member Added Event ID	Member Removed Event ID
Local group	Event ID 636	Event ID 637
Global group	Event ID 632	Event ID 633
Universal group	Event ID 660	Event ID 661

**Figure 1: Event ID 660 details**

```
Event Type:      Success Audit
Event Source:    Security
Event Category: Account Management
Event ID:        660
Date:            4/21/2003
Time:            2:39:43 PM
User:            AD\administrator
Computer:        AD1
Description:
Security Enabled Universal Group Member Added:
Member Name:     cn=al,OU=Monterey,DC=ad,DC=local
Member ID:       AD\al
Target Account Name: Enterprise Admins
Target Domain:   AD
Target Account ID: AD\Enterprise Admins
Caller User Name: Administrator
Caller Domain:   AD
Caller Logon ID: (0x0,0x4AC35)
Privileges:      -
```

## Directory Service Access Auditing

As you can see, account management auditing provides good information for tracking user, computer, and group maintenance, but what about monitoring other areas of AD such as changes to GPOs and organizational units (OUs)? This area is where directory service access auditing shows its value. Although a bit more obscure and cryptic, directory service access audit events give you extremely detailed information about every change that takes place in AD. Directory service access auditing reports just one event ID—event ID 565 (Object open). All the useful information is in this event's details. To turn on directory service access auditing, select Domain Controller Security Policy under Administrative Tools; maneuver to Security Settings, Local Policies, Audit Policy; double-click Audit directory service access; and select both Success and Failure.

## Monitoring AD Changes

Randy Franklin Smith

(Reprinted from WindowsItPro Magazine)

You can use directory service access auditing to track Group Policy—related changes. The most basic Group Policy change you want to be aware of is when someone edits one or more of the policies that a GPO defines. Although no specific event ID exists for this situation, you can recognize it if you know what to look for. In AD's schema, GPOs have the object type `groupPolicyContainer` and a version property called `versionNumber`. Whenever someone edits a GPO, Win2K increments the version number. When computers throughout the domain reapply Group Policy, they compare the current version number of each GPO with the version number that was current the last time the computer applied the GPO. If the version numbers haven't changed, the computer doesn't reapply the GPOs and thus saves resources on the local computers as well as the domain controller (DC). You can detect changes to GPOs by finding event ID 565s that have the Object Type value `groupPolicyContainer`, the Accesses value `Write Property`, and a `Write Property` that includes `versionNumber`, as Figure 2 shows.

**Figure 2:** Details from a GPO-changing event

```
Event Type:          Success Audit
Event Source:        Security
Event Category:      Directory Service Access
Event ID:            565
Date:                4/18/2003
Time:                5:47:12 PM
User:                AD\administrator
Computer:            AD1
Description:
Object Open:
  Object Server:     DS
  Object Type:       groupPolicyContainer
  Object Name:       CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=ad,DC=local
  New Handle ID:     0
  Operation ID:      (0,157656)
  Process ID:        260
  Primary User Name: AD1$
  Primary Domain:    AD
  Primary Logon ID:  (0x0,0x3E7)
  Client User Name:  Administrator
  Client Domain:     AD
  Client Logon ID:   (0x0,0x20318)
  Accesses           Write Property

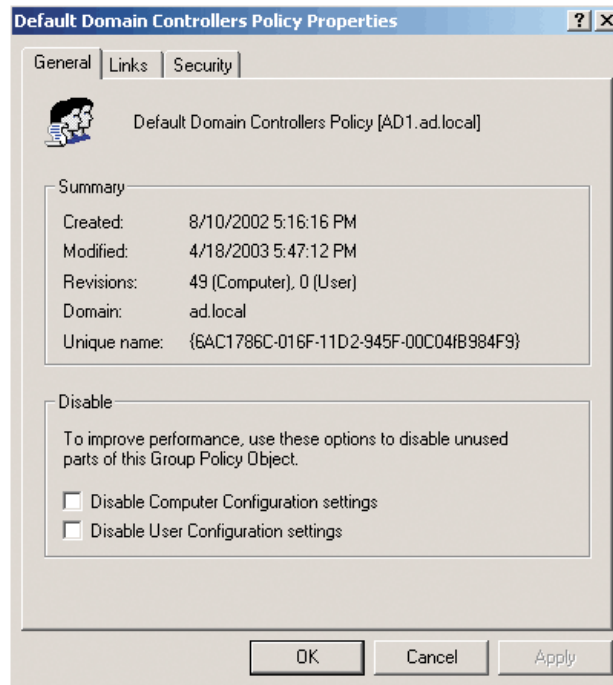
Privileges           -

Properties:
Write Property
  %(00000000-0000-0000-0000-000000000000)
  versionNumber
```

Notice that Win2K doesn't report the GPO display name that you're used to seeing in the Microsoft Management Console (MMC) Active Directory Users and Computers console. Instead, the event provides the object's X.500 distinguished name (DN). For example, in Figure 2, the Object Name is `CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=ad,DC=local`. The relevant information in a GPO's DN is the long string of characters at the beginning, which is the GPO's globally unique identifier (GUID). You can use the Active Directory Users and Computers snap-in to track a GPO from its display name to its GUID. For example, to obtain the GUID of the Default Domain Controllers Policy GPO, open the Properties dialog box for the Domain Controllers OU and select the Group Policy tab. In the list of GPOs, select Default Domain Controllers Policy, then click Properties. The GPO's GUID is displayed on the General tab in the Unique name field, as Figure 3 shows.

# Monitoring AD Changes

Randy Franklin Smith  
(Reprinted from WindowsItPro Magazine)



While you're looking at Figure 3, notice the Disable section, which lets you disable the GPO's Computer Configuration policy, User Configuration policy, or both. If someone selects one or both of the check boxes, Win2K stops applying all the associated policies, which could have a wide-reaching effect on computers and users in your domain. To detect when someone changes the status of either or both of these boxes on any GPO, you need to look for event ID 565 where Object Type is groupPolicyContainer and Properties is flags.

A final type of GPO change that you might monitor is a change to a GPO's ACL, which controls who can edit the GPO and which you can use to limit the users and computers the GPO applies to within the OU or domain to which the GPO is linked. (For more information about changing a GPO's ACL, see "Controlling Group Policy, Part 2," Winter 2000, <http://www.winnetmag.com>, InstantDoc ID 15886.) In this case, look for event ID 565 and Object Type groupPolicyContainer as usual, but the Accesses field should have the value WRITE\_DAC (write access to discretionary ACL).

If someone deletes a GPO, you'll see event ID 565 with the Object Type groupPolicyContainer, an Object Name that begins with CN=Policies,CN=System, and an Accesses value of Delete Child. The same event ID with the same Object Type and the same opening phrase for the Object Name but whose Accesses value is Create Child instead of Delete Child tells you that someone created a new GPO. Unfortunately, neither event specifies the GUID or display name of the GPO.

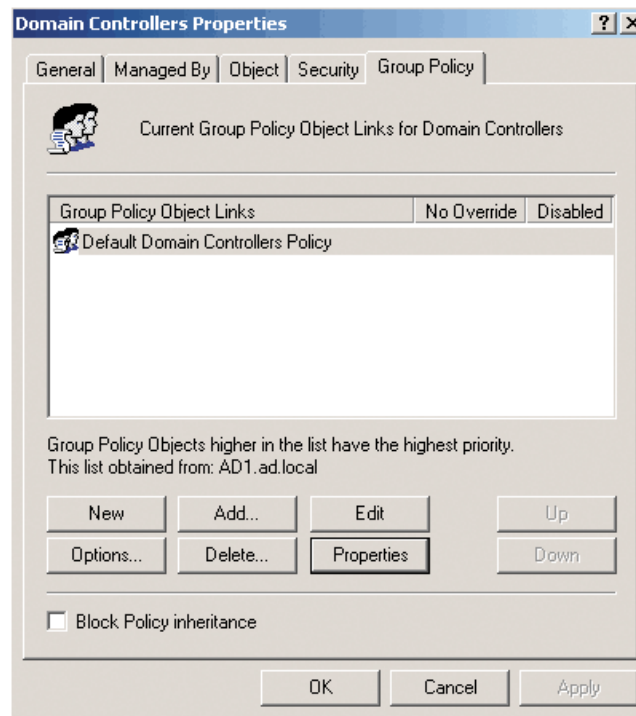
The other area of Group Policy—related changes that warrants monitoring is changes to Group Policy—related properties on an OU. As Figure 4 shows, each OU has a list of GPOs that are linked to it; each linked GPO has two options, No Override and Disabled; and the OU has a Group Policy—related Block Policy inheritance check box. If someone links or unlinks a GPO or selects or clears any of the other options, the change can have wide-reaching effects on the computers and users contained in that OU. To detect changes to an OU's list of linked GPOs, changes in the No Override or Disabled options for a GPO link, or changes to the Block Policy inheritance value, look for event ID

# Monitoring AD Changes

Randy Franklin Smith

(Reprinted from WindowsItPro Magazine)

565 with an Object Type value of organizationalUnit and the Write Property values gPOptions and gPLink, as Figure 5 shows.



**Figure 5:** Event ID details for a changed OU GPO

```
Event Type:      Success Audit
Event Source:    Security
Event Category:  Directory Service Access
Event ID:        565
Date:           4/21/2003
Time:           1:50:35 PM
User:           AD\administrator
Computer:       AD1
Description:
Object Open:
  Object Server: DS
  Object Type:   organizationalUnit
  Object Name:   OU=Accounting,OU=Monterey,DC=ad,DC=local
  New Handle ID: 0
  Operation ID:  {0,282784}
  Process ID:    260
  Primary User Name: AD1$
  Primary Domain: AD
  Primary Logon ID: {0x0,0x3E7}
  Client User Name: Administrator
  Client Domain:  AD
  Client Logon ID: {0x0,0x44F3D}
  Accesses:      Write Property

Privileges:      -

Properties:
Write Property
  %00000000-0000-0000-0000-000000000000}
  gPLink
  gPOptions
```

# Monitoring AD Changes

Randy Franklin Smith

(Reprinted from WindowsItPro Magazine)

GPOs can also be linked to domains or to sites. To detect Group Policy—related changes to a domain or site, look for event ID 565 where the Object Type is domainDNS or site and the Write Property values are gPLink and gPOptions.

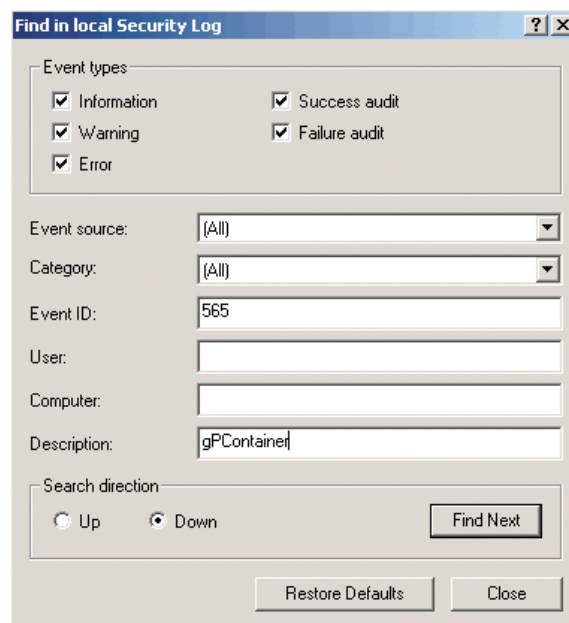
To keep tabs on how administrative authority and other AD permissions are being modified, you can monitor for changes to OU ACLs. The event details you look for are similar to those I described earlier for GPO ACLs. When you see event ID 565, Object Type organizationalUnit and Accesses WRITE\_DAC, you know that someone changed the permissions on that OU. The Object Name field plainly reports the OU's DN.

You can detect new OU creation by looking for event ID 565 where Object Type is organizationalUnit and Accesses is Create Child. On such an event, Object Name specifies the parent OU, not the name of the new OU. Deletion events have the same event details except that the Accesses value is Delete Child instead of Create Child.

You can detect site-related changes by looking for event ID 565 where Object Type is site, siteLink, siteLinkBridge, subnet, nTDSsiteSettings, or serversContainer. Changes to replication between DCs show up as event ID 565 with Object Type nTDSConnection or nTDSsiteSettings. To monitor trust relationship changes, look for event ID 565 with Object Type trustedDomain, which Win2K uses for both trusted and trusting domains. If you have one or more enterprise Certificate Authorities (CAs) set up in your domain, you can monitor changes to certificate templates, the CAs themselves, and certificate revocation lists (CRLs) by looking for Object Type pKICertificateTemplate, pKIEnrollmentService, certificationAuthority, or cRLDistributionPoint.

## Searching the Security Log

Account management and directory service access auditing truly provide the information you need to stay on top of AD changes. The details are in the Security log, but how do you find them? Manually searching through each event is obviously not an option. For ad hoc searches, you can use Event Viewer's find feature. Open Event Viewer, right-click the Security log, and select View/Find. As Figure 6 shows, you can specify the event ID and enter in the Description field text that you want Event Viewer to search for in the details of the found events.



## Monitoring AD Changes

Randy Franklin Smith

(Reprinted from WindowsItPro Magazine)

For any kind of regular monitoring, you need a more sophisticated tool. For example, you could use the Microsoft Windows 2000 Resource Kit's `dumpel.exe` utility, which you can also download from <http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/dumpel-o.asp>. You can use `Dumpel` to filter on event number—but not on event details, which `Dumpel` refers to as strings. You can use the `Findstr` command to further filter events such as event ID 565 based on the contents of their strings.

Unfortunately, though, Win2K logs schema attributes' GUID rather than their display name in the Security log, and `Dumpel` doesn't translate the GUID into the name. Therefore, when you dump event ID 565, you get something that looks like the results that Figure 7 shows. To decipher these results, you can use the Win2K AD schema documentation.

If you browse that site, you can verify that `bf967aa5-0de6-11d0-a285-00aa003049e2` is the schema GUID for `organizational-Unit` and `f30e3bbe-9ff0-11d1-b603-0000f80367c1` and `f30e3bbf-9ff0-11d1-b603-0000f80367c1` are the GUIDs for `gPLink` and `gPOptions`. With this information in hand, you could use the sample commands

```
dumpel -l security -t -format Idtus -m security -e 565 > events.txt
findstr "bf967aa5-0de6-11d0-a285-00aa003049e2" events.txt
```

to get a list of all event ID 565 events in which the object type is `organizationalUnit`.



As you can see, if you know what to look for, you can stay well informed about what's going on in AD—or at least be able to figure out what happened and who did it when a problem arises. Remember that you need to enable Audit account management and Audit directory service access in your Default Domain Controllers Policy GPO, and you must check each DC to get a complete record of activity in the domain. Happy Security log hunting!