Department of Information Technology
Active Directory Audit
Final Report

August 2008

"promoting efficient & effective local government"
Executive Summary

Active Directory (AD) is a directory service by Microsoft for use in Windows environments. Its main purpose is to provide central authentication and authorization services for Windows based computers. AD is a way to manage all elements of organization’s network, including computers, groups, users, domains, security policies, and any type of user-defined objects. AD allows administrators to assign policies, deploy software, and apply critical updates to an organization’s network of computers. AD stores information and settings in a central database.

Windows 2003 is the operating system for the county’s local area network servers. The Department of Information Technology (DIT) Technical Support Services (TSS) division is responsible for the configuration, administration, maintenance, and security of the Windows 2003. DIT uses AD to provide centralized security configuration including file permissions, audit policy for user activities, assignments of user rights, etc.

Our audit found that database files in which Active Directory was stored were secured and protected from unauthorized access. However, we also found that users were not removed from the group accounts after their roles had been changed within the county or were separated from the county. DIT had not developed policies and procedures for Group Policy Objects (GPOs) management and AD configuration audit alerts reviews. Moreover, high risk AD configuration changes were not documented in change request forms. AD configuration changes include the changes of GPO, users, group accounts and etc. GPOs are a set of rules used to control almost every aspect of the computer and user environment, including security settings, user rights, software installation, and etc. The primary issues noted were:

- Only the Domain Administrator Group was monitored by the DIT Information Security Group on a weekly basis. DIT had not set up procedures to review the security sensitive groups periodically and remove users promptly after employees were transferred to another department or left the job with the county. Security can be compromised if the users belong to groups that provide administrative access which is not a part of their job.

- Audit configuration settings for each domain did not meet the DIT Windows 2000 Server Configuration Standards. If an attack is attempted, it will be difficult to determine the origin of the attack.

- DIT had not established formal policy and procedures for GPO management, including reviewing and approving new GPOs. Untested, unapproved and undocumented changes in GPOs can affect the overall security of the Windows environment.

- Security logs were not being reviewed on a regular basis. Reviewing the security logs regularly can help DIT to identify trends of the security incidents; measures can be taken to prevent and defend against future attacks.
• DIT had not established formal procedures to ensure that all the Change Audit for Active Directory (CAAD) audit alerts were reviewed and investigated by the assigned IT staff. High risk configuration changes were not accompanied by written change request forms to ensure the change was authorized and approved by the management prior to implementation in the production environment. Unauthorized configuration changes may be implemented if there are no change control procedures in place.

Scope and Objectives

This audit was performed as part of our fiscal year 2007 Annual Audit Plan and was conducted in accordance with generally accepted government auditing standards. The audit covered the period of July 2005 through September 2006, and our audit objectives were to determine:

• Active Directory policies and option settings are set to provide appropriate information security
• All policies and option settings have been authorized, evaluated and validated
• Database files in which Active Directory is stored are secured and protected from unauthorized access
• Audit policies (per-computer settings that track the security and control points of the computer) are set to ensure the correct tracking within Active Directory
• Management controls are in place to provide program oversight, monitor progress and achieve security objectives

Methodology

Our audit methodology included a review and analysis of the county’s Active Directory Design Diagram. Our audit approach included interviewing appropriate employees to understand county Active Directory design and the trust relationship among the forests and domains (In Windows environment, a trust is designed to allow users from one domain to access resources in another domain), reviewing the group policy settings to ensure appropriate authentication controls, and examining some key Global Group Membership to determine whether the numbers of users are kept to a minimum. We also assessed the audit policy settings and the procedures of monitoring the Active Directory activities to determine whether the security activity is logged and the security violation is monitored by the IT management.

The Fairfax County Internal Audit Office is free from organizational impairments to independence in our reporting as defined by Government Auditing Standards. We report directly and are accountable to the county executive. Organizationally, we are outside the staff or line management function of the units that we audit. We report the results of our audits the county executive and the Board of Supervisors, and reports are available to the public.
Findings, Recommendations, and Management Response

1. Security Sensitive Groups

We noted that there were seven unused guest accounts; DIT staff disabled these accounts during the fieldwork phase of this audit. We also noted that six users should be removed from the Account Operator group because they had resigned from DIT. There are many default groups in an Active Directory domain, some of them are security sensitive groups that exist on a default Active Directory installation. These groups are used to control security on the resources. We obtained the lists of users in the security sensitive groups, which are Domain Administrator Group, Schema Administrator Group, Domain Guests Group, Server Operator Group, and Account Operator Group, and checked each user in these groups to determine whether the users in the groups were up-to-date.

Fairfax County Information Technology Security Policy 70-05.01 states that System Administrators or other designated staff:

- are responsible for removing the accounts of individuals that change roles within Fairfax County or are separated from their relationship with Fairfax County
- must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes
- must have a documented process for periodically reviewing existing accounts for
- are subject to independent audit review
- must provide a list of accounts for the systems they administer when requested by authorized Fairfax County management
- must cooperate with authorized Fairfax County management investigating security incidents

DIT had not set up procedures to review the security sensitive groups periodically and remove the user promptly after the employee had transferred to another department or terminated the job from the county. In addition, the county did not have an integrated HR system to automate the timely tracking of the county employees' employment status. The foundation of resource access security in a domain is the protection of the user and group accounts that are created in Active Directory. If the user and group accounts have excessive privileges, or belong to groups that provide administrative access inappropriately, security can be compromised. For example, Account Operator could create user accounts and groups, modify membership of non-admin groups and reset passwords. If a user had the Account Operator privileges, he/she could create an account and obtain direct access to application programs used to process transactions, such as accounts payable system. By obtaining the access, a person could alter an accounts payable program to inappropriately generate a check for him or herself.

Recommendation: We recommend that DIT develop procedures to review the security sensitive groups periodically and remove the users promptly after the employees have transferred to another department or left county employment.
Management Response: DIT will develop a written procedure that will require at least a quarterly review and report of AD security sensitive groups. DIT will include a group review action in the existing account transfer process. DIT will utilize the Active Roles Server (ARS) to track and update the county employees’ employment status. As part of the planned automated deprovisioning solution; DIT is including the process to remove users from sensitive groups once they leave the county. These steps are expected to be completed by December 2008.

2. Audit Policy Configuration Settings

We obtained the audit policy configuration settings for each domain, compared them with the Windows 2000 Server Secure Configuration Standards Checklist, and found that the audit policies configuration settings for each domain did not meet the recommended minimum standards. Audit policies are per-computer settings that can track the security and control points of the computer. These policies are configured through Group Policy and can target different aspects of the operating system and computer security. There are nine different audit policies for a Windows computer. Each audit policy tracks something unique that is related to security on the computer. DIT has published the Windows 2000 Server Secure Configuration Standards Checklist on the County Infoweb. DIT and all county agencies Organizational Unit (OU) administrators should follow these standards to install and configure Windows 2000 server.

The Department of Information Technology has developed the Windows 2000 Configuration Standards, which state that audit policies should be enabled to meet the minimum standards (See Appendix A). For example, the Logon Events policy tracks when a user attempts to logon to the domain controller. If this audit policy is enabled, the information will be documented on the computer where the logon was performed.

Recommended configuration standards for the audit policies settings were not consistently followed by DIT. The audit policies should be configured properly to ensure that the correct tracking is enabled on the specified domain controllers. If a security breach occurs or an attack is attempted, it will be almost impossible to determine the origin of the attack without some form of auditing enabled.

Recommendation: We recommend that DIT enable the audit policies in all domain controllers’ group policy objects to meet the DIT recommended standards.

During the course of this audit, DIT corrected audit policies configuration settings for each domain. No management response is required for this recommendation.

Management Response: No management response is required for this recommendation.

3. Group Policy Object (GPO) Management
DIT had not established formal written policy or procedure for GPO management, including reviewing and approving new GPOs. All the domain administrators and Enterprise Administrators have the rights to create, edit, delete and link GPOs. The Organizational Unit (OU) administrator can link the OU-level GPO. In addition, DIT could not provide any documentation showing that current GPOs had been reviewed and authorized by management. Group Policy allows IT administrators to implement specific configurations for users and computers. Group Policy settings are contained in Group Policy objects, which are linked to selected Active Directory containers: sites, domains, and organizational units (OUs). Group Policy Objects are an essential part of every Windows computer and Active Directory domain. GPOs control almost every aspect of the computer and user environment, including security settings, user rights, software installation, and etc. It is not possible to secure Windows computers without using GPOs.

Any Group Policy additions, changes, or deletions should be tested in a test environment and undergo a documented approval process. DIT had not established formal policy or procedures for GPO management, including reviewing and approving new GPOs. In addition, DIT could not provide any documentation showing that GPOs had been tested in a test environment before being deployed into the production. Untested, unapproved, and undocumented changes in Group Policies can affect the overall function and security of the Active Directory.

**Recommendation:** We recommend that DIT perform the addition, modification, or deletion of the GPOs in a test environment prior to implementation in production. DIT should also formally document the approval process.

**Management Response:** DIT will implement the Infra system change management module to document and track all county’s software changes, including GPO changes. DIT will complete the validation of existing test environment and document procedures for requesting, evaluating, and approving additions, modifications, and/or removal of production GPOs. (Note: The procedures will include integration with existing change management process.) This item is expected to be completed by October 2008.

4. **Standard Procedures and Documentation**

We reviewed a list of the Group Policy Objects changes audit alerts generated from CAAD between December 2005 and September 2006, and noted that all the “Why” fields that explain the reasons for the changes were blank. In addition, we reviewed 1475 high risk configuration changes between May 2006 and December 2006; none of which was accompanied by the reason for change or any indication that the change was investigated and determined to be legitimate by the assigned IT personnel. We also used ACL data analysis software to randomly select 20 high risk configuration changes and requested the corresponding written change requests. DIT was unable to provide the support documentation. According to the informal procedures that DIT has adopted, all the configuration changes that are categorized as “high risk” shall be accompanied by written change requests. After the assigned IT staff review and investigate the high risk change events, they shall update the Change Audit for Active Directory (CAAD) “Why” field to accurately reflect the reason for the change.
DIT utilizes the CAAD to track key configuration changes of the Active Directory, including GPOs, users, groups, schema, domains, forest and etc. All the change alerts are sent to a group of IT staff via e-mail in real time. CAAD provides details about each configuration change in real time through e-mail notifications, which contain:
- *Who* made the change?
- *What* object was changed? (before and after)
- *Where* the change was made from?
- *When* the change was made?
- *Why* the change was made?

Fairfax County Information Technology Security Policy 70-05.01 states that system configurations (i.e., hardware, wiring, displays, networks) must be documented. Installations and changes to these physical configurations must be governed by a formal change management process. All Fairfax County agencies must carefully assess the risk of unauthorized alteration, unauthorized disclosure, or loss of the data for which they are responsible and ensure, through the use of monitoring systems, that the agency is protected from damage, monetary or otherwise.

DIT had not established formal written policies and procedures that govern the review of the CAAD alerts e-mail notifications. DIT had not utilized the change request form to document the configuration changes. Without polices and procedures to ensure all the CAAD alerts e-mail notifications are reviewed by the assigned personnel, security violations and unauthorized configuration changes may go undetected. Without controls over the configuration changes of the Active Directory, unauthorized changes may be implemented. In early 2008, DIT replaced the CAAD with the InTrust application to monitor all the AD configuration changes. This finding is focused on the need for establishing procedures to monitor the AD configuration changes.

**Recommendation:** We recommend that DIT develop polices and procedures that detail who can authorize a configuration modification and how these authorizations are to be documented. Authorization documentation should be maintained for at least as long as Active Directory is in operation in case questions arise regarding why or when configuration modifications are made. We also recommend DIT develop controls and procedures to ensure the assigned personnel review the InTrust alerts e-mail notifications timely and document whether the configuration change is legitimate in the InTrust system.

**Management Response:** DIT will re-educate staff on the existing change management process for requesting configuration changes in AD through in-house trainings. In addition, all the AD configuration changes will be documented and tracked in the Infra system change management module. DIT will write procedures and train staff regarding using existing investments in Quest InTrust and Microsoft System Center Operations Manager to document configuration changes. This item is expected to be completed by October 2008.

5. **Review Security Logs**

DIT did not review the significant events in the security log on a regular basis to identify trends and specific security incidents that management had established as undesirable.
events. DIT implemented the InTrust application to archive all the Active Directory event logs on May 16, 2007. The event logs were not archived prior to the implementation of the InTrust application. Security logs store security events that are triggered by enabling the audit policy on a domain controller. Security logs track when users perform certain tasks on the computer. This might include accessing files, backing up files, adding users to groups or restarting the server.

Fairfax County Information Technology Security Policy 70-05.01 states:
The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:

- Automated intrusion detection system logs
- Firewall logs
- User account logs
- Network scanning logs
- System event logs
- Application logs
- Data backup and recovery logs
- Help desk trouble tickets
- Telephone activity – Call Detail Reports
- Network printer and fax logs

The significant events in the security logs should be reviewed to identify trends and specific security incidents. If trends are found that indicate that there has been an attack on a domain controller, measures can be taken to minimize the impact of the attack and to prevent and defend against future attacks.

**Recommendation:** We recommend that DIT review the significant events in the security logs on a regular basis to identify trends and specific security incidents that management has established as undesirable events.

**Management Response:** DIT will write procedures and create a checklist to review security logs on systems on a daily basis for security incidents that management has established as undesirable. DIT will leverage existing security log reporting tools (e.g. Quest InTrust) to run regular reports to identify any trends that will need management attention. These steps are expected to be completed by August 2008.
Appendix A

The Department of Information Technology has developed the Windows 2000 Configuration Standards, which state:

3.16 Enable Audit Policies

When Windows 2000 is first installed, no auditing is enabled. The following audit policies are recommended as minimum standards:

<table>
<thead>
<tr>
<th>Item</th>
<th>What it does</th>
<th>Recommended</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit account Logon events</td>
<td>Logs both local and remote resource logons.</td>
<td>Success, Failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit account Management</td>
<td>Audits User accounts or Groups created, changed, or deleted. User accounts renamed, disabled, or enabled. Passwords set or changed.</td>
<td>Success, Failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit Directory service Access (For DC’s)</td>
<td>Important for Domain Controllers. Audits access to the directory service.</td>
<td>Success, Failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit logon events</td>
<td>Enables auditing of logon events.</td>
<td>Success, Failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit object access</td>
<td>Enables auditing on base system objects</td>
<td>Success, Failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit policy change</td>
<td>Enables auditing of any changes to user rights or audit policies.</td>
<td>Success, Failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit privilege use</td>
<td></td>
<td>Success, Failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit process tracking</td>
<td>Tracks program activation, handle duplication, indirect object access, and process exit.</td>
<td>No Auditing Required. Good to monitor Virus behavior in a Development Environment.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit system events</td>
<td>Logs shutdowns and restarts for the local workstation.</td>
<td>Success, Failure</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Glossary

**Account Operator Group:** Account operator can create user accounts and groups, modify membership of non-admin groups and can reset passwords.

**Audit Policy:** Audit policies are per-computer settings that can track the security and control points of the computer. These policies are configured through group Policy and can target different aspects of the operating system and computer security.

**Authentication:** A security feature that determines a user’s identity and legitimacy.

**Authorization:** Authorization is the process of determining which permissions a person or system is supposed to have.

**Change Audit for Active Directory (CAAD):** CAAD is a software that can capture key configuration changes of the Active Directory, including Group Policy Objects, users, groups, schema, domains, forest and etc.

**Forest:** When multiple domains exist but do not share a contiguous Domain Naming System (DNS) name space, they can be arranged as two or more trees within the same forest. All domains within a forest trust each other.

**Domain:** A group of computers and devices on a network that are administrated as a unit with common rules and procedures.

**Domain Administrator Group:** Domain administrator has full authority to Active Directory and all computers in the domain.

**Domain Controller (DC):** On Windows Server Systems, the domain controller is the server that responds to security authentication requests (logging in, checking permissions, etc.) within the Windows Server domain.

**Domain Guests Group:** Members of this group are only allowed to access the system from across the network and have very limited privileges by default and initially only contains the Guest user account for the domain.

**Global Group:** Groups with this scope are designed to be used by any computer within the domain. Global groups are designed to be nested in Domain Local Groups, or be nested in Local groups located in the SAM of resource servers.

**Group Policy Objects (GPO):** Group Policy provides a way to manage computer and user settings using the hierarchy of Active Directory. A GPO is a collection of configuration and policy settings. GPOs are stored in Active Directory.

**Organizational Units (OUs):** Organizational units are used to subdivide objects within a domain. OUs can contain children OUs like directories and subdirectories on a disk.
drive. OUs often correspond to divisions and departments within a company.

**Schema Administrator Group:** Schema administrator has authority to modify schema for the entire forest.

**Server Operator Group:** Server operator can start and stop services, share folders and perform other powerful operations on servers.