Global Information Assurance Certification Paper

Protecting the Windows 2000 Schema

Securing Windows GCNT Practical Assignment
Version 2.1b

James F. Roman
August 2001

This page intentionally left blank

Table of Contents

This page intentionally left blank

Introduction

One of the most important things to secure within a Windows 2000 network is the Active Directory Schema. Without proper protection, unauthorized access or modifications to the Active Directory Schema could completely disrupt an entire network. Attacking the Schema is an effective method hackers can use for a Denial of Service attack against the whole network. Therefore, understanding what the Schema is as well as how it relates to Active Directory and the rest of the Windows 2000 network environment is essential to providing adequate security. An overview of key concepts will be discussed, including how to open all of the security locks so changes can be made to the Schema, which tools should be used to make changes, and what effects this can have on a server and network. Finally, some guidelines will be provided for protecting the Schema from unauthorized actions, logging all actions performed on the Schema, and for monitoring the Windows 2000 Schema.

This document is not intended to completely cover the Active Directory and it does not cover how to extend the Schema. A brief overview of Active Directory is given, since the Schema is a major component of Active Directory. There is also a short section about extending the Schema, but its focus is on its effects rather than how to extend the Schema. For more information on the Active Directory and how to protect it, please refer to your Windows 2000 documentation. For more information on extending the Schema, refer to the Active Directory Developer Guide.

Warning

Making changes to the Active Directory Schema should not be done without complete knowledge of the impact of the changes. Changes to the Schema have the potential of completely destroying a server and network. Experimentation with the Active Directory Schema should only be done in a test environment that is isolated from any production network or system. To recover from an error in the Active Directory Schema it may be required to either restore from a system backup or completely reinstall the Windows 2000 Server software. If any changes have previously been made to the Schema they may need to be reapplied after a system recover.

Active Directory and the Schema

The Schema is an integral part of the Windows 2000 Active Directory. In order to discuss the Schema it is important to understand what the Active Directory does and how it relates to a Windows 2000 network.

What is Active Directory?

The simplest definition of Active Directory is that it is a database of everything within the network. Active directory contains all of the user accounts, security groups, computer and printer definitions, applications, and files that have been defined for a network.

A more specific definition of Active Directory is that it is a directory service that is used by administrators to manage enterprise-wide network objects from a central location. Besides being

fully integrated at the operating system level, Active Directory is composed of following services:

- A data store that contains the all defined network objects
- Directory data
- Query and index mechanisms
- Replication service
- Links to the security subsystem

As mentioned above, Active Directory is a database of objects, but that is not its only function. Active Directory also provides the following features:

- Administrative privileges and security settings are controlled in hierarchical information structures.
- User and resource management is simplified.
- Administrators can create and assign policies over several Active Directory containers.
- Support for Kerberos V5, Secure Socket Layer v3, and Transport Layer Security authentication is provided.
- Lightweight Directory Access Protocol (LDAP) can be used to access and manage the information in the directory.
- Active Directory Service Interfaces (ADSI) is available to aid developers in writing applications that need access to Active Directory.

Since Active Directory is available throughout the entire network, users can query Active Directory to get details on any object on the network from anywhere in the network. For instance, it is possible to get details on a printer or find out a user's email address by querying the Active Directory from any workstation.

How does Active Directory Work?

Active Directory is organized into objects, containers, domains, trees, and forests. Objects represent the individual parts of a network such as a user, printer, or computer. Objects can be grouped into containers called organizational units that are used to categorize objects and simplify the administration of the individual objects. The containers themselves are also considered objects within the Active Directory.

All Active Directory objects exist within a domain. A domain consists of a collection of objects that form a network. Each domain contains a database of information about the objects that have been defined for the domain. A domain also functions as a security boundary. Access to the objects within the domain is controlled only by that domain.

Multiple domains can be grouped together to form what is called a tree. Grouping domains together allow resources to be shared from one domain to another. All domains within a tree share a common database of objects called the Global Catalog. Trees are linked together in a hierarchical fashion.

At an even higher level, multiple trees can be put together to form a forest. The separate trees within a forest function independently but communicate with one another. The trees that make up a forest share a common database of objects just like they are shared among the separate domains.

The network computers responsible for the administrative functions within a domain are called domain controllers. They responsible for many administrative functions including managing resources such as file shares and printers, providing services such as DNS and DHCP, replicating Active Directory information, and authenticating system rights. All domain controllers in Active Directory are considered to have equal authority. They also provide redundant functionality in situations where a domain controller is unavailable.

The Global Catalog is a subset of all of the objects defined in the Active Directory. The Global Catalog is periodically replicated to every domain controller within the domain, tree, or forest to speed up searches within Active Directory. This also provides a mean to maintain consistency within Active Directory.

What is the Schema?

The Schema is the basis for how objects are stored in the Windows 2000 Active Directory. The Schema is the formal definition of all of the objects that can potentially be stored in Active Directory. In other words, it is the database layout or its metadata. It tells Active Directory what an object looks like and what information it should contain. The Schema itself it made up of two types of Active Directory objects called attributes and classes.

Attributes are defined separately from classes and each attribute can only be defined once. However, each attribute can be used to make up more than one class. For example: the Description attribute is part of the definition for both the User and Site classes.

Classes, also called object classes, describe all of the possible directory objects that can be created. Each class is a collection of attributes. When an object is created, the attributes store the information that describes the object. For example, the User class contains attributes such as first name, last name, phone number, e-mail address, and mailing address. Each object defined within the Active Directory is an instance of one or more object classes. An instance of the User class would be an account that has been set up for a user to access the network.

Every Windows 2000 Server comes with a set of basic classes and attributes already defined. Experienced administrators can extend the Schema by adding new classes and attributes either manually or programmatically. Active Directory does not support the deletion of Schema objects. Unwanted objects can only be marked as deactivated.

Within a domain, all domain controllers share the same Global Catalog and the underlying Schema. As domains are linked into trees and forests, the Global Catalog and Schema must also be consistent so the domain controllers can communicate with one another. Before one domain controller can tell another about a user object they both need to be talking the same language.

For example, when one domain controller is talking about a user object, it needs to be the exact same definition for a user object on all other domain controllers. Since the Global Catalog and Schema are periodically replicated to all other domain controllers, any change made is also replicated. This also means that a change made to the Schema on one domain controller can have adverse affects on all domain controllers within Active Directory.

Viewing the Schema

The primary means to viewing the Active Directory schema is with the Microsoft Management Console (MMC) Active Directory Schema snap-in. Before the Schema snap-in can be accessed through the MMC it must either be registered or the Windows 2000 Administrative tools must be installed.

Registering the Active Directory Schema Snap-in

The Active Directory Schema snap-in is located in the %systemroot%\System32 directory on the domain controller. Before the snap-in can be made available to the MMC the schmmgmy.dll file must be registered with the REGSRV32 command. This is done by:

1. Click **Start**, point to **Programs**, point to **Accessories**, and click the **Command Prompt** menu option.
2. Type **c:** to go to the C drive.
3. Type **cd %systemroot\system32** to change directories.
4. Type **regsvr32 schmmgmt.dll** to install the snap-in.
5. A message box appears and displays "DllRegisterServer in schmmgmt.dll succeeded." Click the **OK** button to close the window.
6. Type **exit** to close the Command Prompt window.

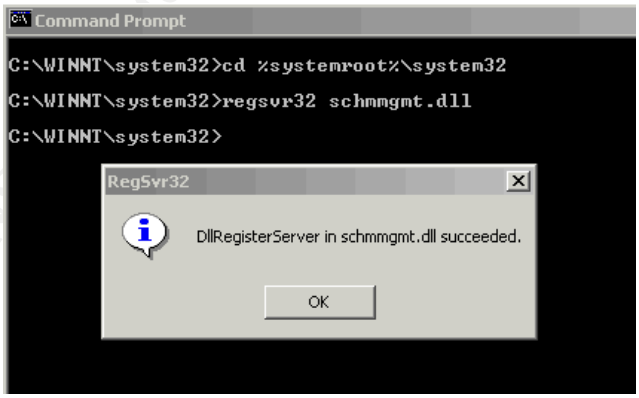

Figure 1 – Snap-in Registration Confirmation

At this point the Active Directory Schema snap-in is available to the Microsoft Management Console.

Installing the Windows 2000 Administrative Tools

Another way to make the Active Directory Schema snap-in available to the MMC is to completely install the Windows 2000 Administrative Tools. All of the tools that are part of the Administrative Tools are not installed by default during a normal installation. Install the remaining tools onto a domain controller by doing the following:

1. Click **Start**, point to **Settings** and click on the **Control Panel** menu option.
2. Double-click the **Add/Remove Programs** icon.
3. Select **Windows 2000 Administrative Tools** and click the **Change** button.
4. When the Windows 2000 Administrative Tools Setup Wizard is displayed, click the **Next** button.
5. Select the **Install all of the Administrative Tools** option and click the **Next** button to start the installation.
6. Once the new files are installed, click the **Finish** button to close the wizard.
7. Click the **Close** button to close the Add/Remove Programs windows.

At this point, the Active Directory Schema snap-in is available to the Microsoft Management Console.

It is also possible to install the Administrative Tools on any computer running Windows 2000 by running the Adminpak.msi file from the I386 directory on any Windows 2000 server installation compact disc.

Creating an Active Directory Schema Console

To start the Active Directory Schema snap-in using the Microsoft Management Console (MMC) do the following:

1. Select **Run** from the **Start** menu.
2. Enter **MMC** in the **Open** field and click the **Ok** button.
3. From within the console, select **Add/Remove Snap-in** from the **Console** menu.
4. In the Add/Remove Snap-in window click the **Add** button.
5. Select **Active Directory Schema** from the Available Standalone Snap-ins list box and click the **Add** button.
6. Click the **Close** button to return to the previous window.
7. Click the **OK** button to close this window.

Active Directory Schema console can now be used to browse the Schema.

Note: The Active Directory Schema snap-in is only available on domain controllers within the network.

To save the MMC console containing the Active Directory Schema snap-in:

1. From within the console select **Save As** from the **Console** menu.

2. Select the location for the console to be saved.
3. Type the name for the saved console (Example: schema.msc) in the **File name** field.
4. Click the **Save** button.

At this point, the Active Directory Schema console can be used to browse through all the class and attribute definitions. Selecting a class from the Classes sub-tree will display a complete listing of all the attributes that make up the definition of the class. Selecting the Attributes sub-tree will display a list of all the attributes defined in the Active Directory and their details.

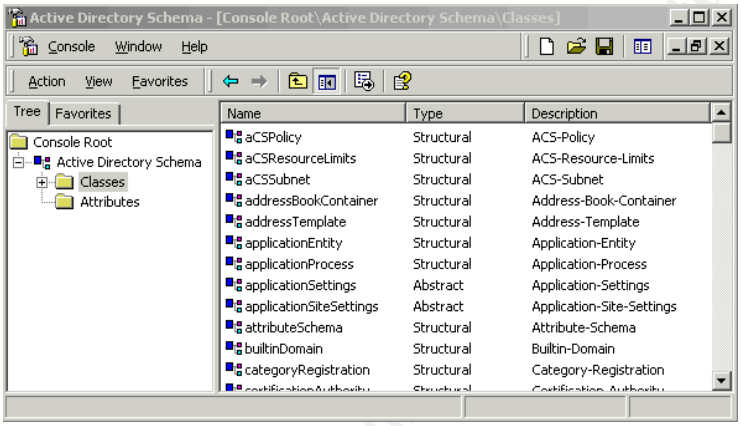

Figure 2 – Active Directory Schema Console

Class Properties

All classes within the Active Directory are instances of other classes in Active Directory. Primarily they are all subclasses of the Class-Schema object, which itself is a subclass of the Top class. Every class within the Active Directory Schema is defined by its description, common name, X.500 OID, class type, relationships, attributes and security permissions.

To view the properties of a class:

1. From within the Active Directory Schema snap-in select the **Classes** sub-tree. A list of classes should be displayed in the right hand side of the console.
2. Select a class from the list and right-click it.
3. Select **Properties** from the pop-up menu.

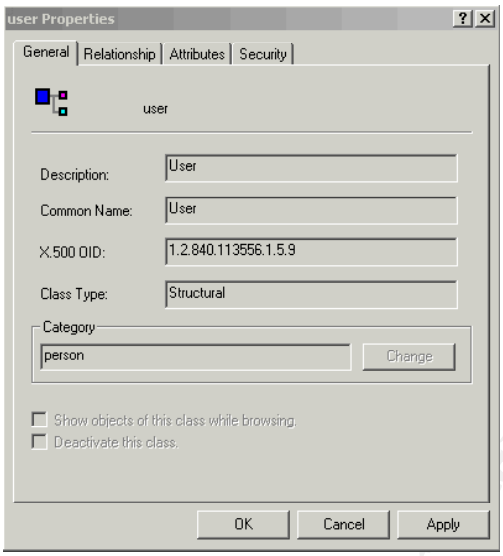

Figure 3 – Class Properties

The Properties window for the class is also where changes can be made to the class. For example: the Security tab is used for granting access to the Schema class and the Attributes tab can be used to add new attributes to the class.

Note: Changing the Schema should not be done without fully testing the impact of the changes on a test system isolated from any production network or system.

Attribute Properties

Attributes are also instances of other objects in the Active Directory. Specifically they are instances of the Attribute-Schema class. In turn the Attribute-Schema class is an instance of the Top class.

To view the properties of an attribute:

1. From within the Active Directory Schema snap-in select the **Attributes** sub-tree. A list of attributes should be displayed in the right hand side of the console.
2. Select an attribute from the list and right-click it.
3. Select **Properties** from the pop-up menu.

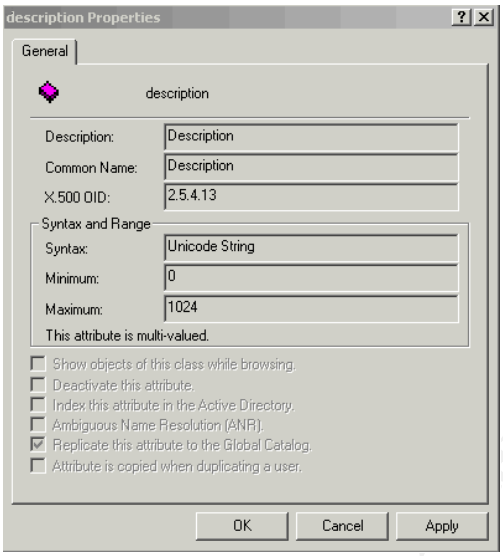

Figure 4 – Attribute Properties

The Properties window for the attribute displays the attribute's description, common name, X.500 OID, the type of data the attribute can contain, and its range of values. The attribute can also be deactivated from the Properties window or added to the Global Catalog to be replicated to all domain controllers in the network.

Note: Changing the Schema should not be done without fully testing the impact of the changes on a test system isolated from any production network or system.

Managing the Active Directory Schema

Managing the Schema can be done from any domain controller within the Active Directory network. Since changes to the Schema can severely affect the network, several safety mechanisms have been put into place to protect the Schema. The mechanisms that control and limit Schema modification are:

- Schema objects are protected by the Windows 2000 Security model; therefore, administrators must be given explicit permission or be members of the Schema Administrators group to make changes to the Schema.
- A registry entry must be set on a domain controller to permit Write access to the Schema on that domain controller. By default all domain controllers are installed to have only read-only access to the Schema.
- Only one domain controller can write to the Schema at any given time. This role is known as Schema Floating Single Master Operations (FSMO). The Schema can only be managed while connected to the Schema FSMO.

Schema Floating Single Master Operations

Active Directory supports multi-master replication of the directory data store among all domain controllers in the domain. Some changes must be made from only one domain controller at a

time. The domain controller where the changes are made is called the operations master. In Active Directory there are five different types of operations master roles that are called Flexible Single Master Operations (FSMO). Each FSMO role is assigned to one or more domain controllers within the network.

- **Schema Master** – Controls all updates and modifications to the Schema. There can only be one Schema Master per Active Directory forest.
- **Domain Naming Master** – Controls the addition or removal of domains in the Active Directory forest. There can only be one Domain Naming Master per Active Directory forest.
- **Relative-ID Master** – Allocates sequences of relative IDs to each of the various domain controllers in its domain. There can only be one domain controller acting as the relative ID master in each domain in the Active Directory forest.
- **PDC Emulator** – Acts as a Windows NT primary domain controller. There can be only one domain controller acting as the PDC emulator in each domain in the Active Directory forest.
- **Infrastructure Master** – Responsible for updating the group-to-user references whenever the members of groups are renamed or changed. There can be only one domain controller acting as the Infrastructure Master in each domain in the Active Directory forest.

By default the first domain controller installed is nominated to be the Schema Floating Single Master Operator. To find out where the current Schema Master is located do the following:

1. Start the Active Directory Schema console.
2. Select the **Active Directory Schema** sub-tree item.
3. Select **Operations Master** from the **Action** menu.
4. The name of the current Schema master appears in the Current Operations Master.

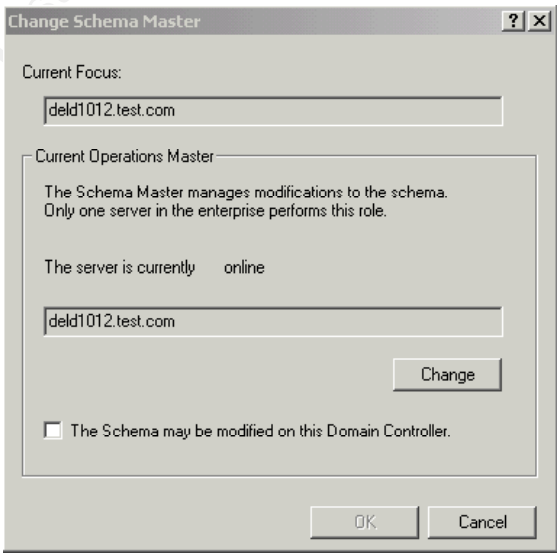

Figure 5 – Operations Master

Moving the Schema FSMO

At times it might be required to move the Schema FSMO. One reason would be if the domain controller that is the currently holding Schema FSMO is being shut down for an extended period of time. It can also be beneficial to move the Schema FSMO to another domain controller for performance reasons.

The Change Schema Master permission is needed to move the Schema FSMO. By default, this permission is only granted to the Schema Admins group. To move the Schema FSMO, an account must be used that is a member of the Schema Admins group. For more information on the Schema Admins group, refer to the section title "Schema Administrators Group".

The Active Directory Schema console can be used to move the Schema Master to another domain controller. To move the Schema FSMO:

1. Start the Active Directory Schema console.
2. Select the **Active Directory Schema** sub-tree item.
3. Select **Change Domain Controller** from the **Action** menu.
4. Select the **Specify Name** radio button and enter the name of the domain controller where the Schema Master will be moved.
5. Select **Operations Master** from the **Action** menu.
6. Click the **Change** button to switch the Schema FSMO to the domain controller listed in the **Current Focus** field.
7. Click the **OK** button when the **Are you sure you want to change the Operations Master?** prompt is displayed.
8. Click the **OK** button.

Another way to transfer the Schema FSMO is with the NTDSUTIL tool. One way to do this with the NTDSUTIL is to:

1. Click **Start**, point to **Programs**, point to **Accessories**, and click the **Command Prompt** menu option.
2. Type **NTDSUTIL** to start the tool.
3. Type **roles** to access the fsmo maintenance menu.
4. Type **connection** to access the server connections menu.
5. Type **connect to server {server name}** to connect to the domain controller that will assigned control of the Schema FSMO. Replace {server name} with the name of a valid domain controller.
6. Type **quit** to return to the fsmo maintenance menu.
7. Type **transfer schema master** to transfer the Schema FSMO to connected domain controller.
8. Click the **Yes** button when the "**Are you sure you want server "server" to transfer**

the schema master for the enterprise?" prompt is displayed.
9. Type **quit** to return to the ntdsutil menu.
10. Type **quit** to exit the tool
11. Type **exit** to close the Command Prompt.

All of this can also be scripted by stacking the commands on a single command line. The command that contain spaces must be enclosed in quotes. For example, the above operation could also be accomplished with the following command:

> C:\ntdsutil roles "connections" "connect to server {server name}" quit "transfer schema master" quit quit

The above command will still prompt the user to make sure the Schema FSMO should be transferred.

Permitting a Domain Controller Write Access

To permit a domain controller write access to the Schema, a registry setting must be added to the domain controller where the Schema maintenance will be performed. This can either be done manually by setting the registry key with the REGEDIT utility or it can be done through the Active Directory Schema console.

To allow writes through the console:

1. Start the Active Directory Schema console.
2. Select the **Active Directory Schema** sub-tree item.
3. Select **Operations Master** from the **Action** menu.
4. Click **The Schema may be modified on this Domain Controller** check box.
5. Click the **OK** button.

Microsoft recommends that you use the Active Directory Schema console whenever possible. If for some reason the console method can not be used, manually add the registry setting by:

1. Select **Run** from the **Start** menu.
2. Enter **REGEDIT** on the **Open** field and click the **OK** button.
3. Find the **KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ NTDS\Parameters** registry key and click on it.
4. From the **Edit** menu select **New** and then **DWORD value**.
5. Enter **Schema Update Allowed** for the name of the new key.
6. Double-click the new key to access it properties.
7. Enter **1** on the **Value data** field and click the **OK** button.
8. Close REGEDIT.

This operation can be scripted by creating a text file with the REG file extension. Include the

following text in the file:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters]
“Schema Update Allowed”=dword:00000001
```

When giving a domain controller write access to the Active Directory Schema, the Schema FSMO must also be transferred to the domain controller before changes are made. If the Schema FSMO is not transferred before changes are made, the changes will only be made to the local domain controller and they will not be replicated to the other domain controllers in the Active Directory forest. Eventually these changes will be overwritten when the Schema is replicated from the Schema FSMO, either when the domain controller is rebooted, or when the Schema is changed on the Schema FSMO.

Schema Administrators Group

The Schema Admins group is defined at the root of the forest and it has permissions to modify the Active Directory Schema. By default, only the Administrator account is a member of the Schema Administrators group. Only members of the Schema Admins group have the permission to make changes to the Schema. Therefore, membership within the Schema Admins group should be carefully restricted to prevent any unauthorized access.

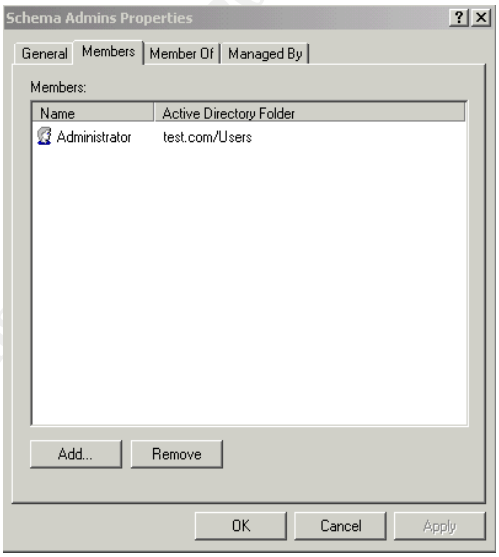

Figure 6 – Schema Admins Members

To give a user access to change the Schema or transfer the Schema FSMO to another domain controller, they will need to be added to the Schema Admins group. Once the Schema changes have been made, the user should immediately be removed from the Schema Admins group. This insures that the Schema will be protected from being accidentally or purposefully changed without taking the proper precautions.

By default, all authenticated users have read access to the Schema. They may use the Active Directory Schema console to view the classes and attributes within the Schema.

Seizing Control of the Schema FSMO

At times it may be required to forcibly take control of the Schema FSMO, such as if the current FSMO is offline or unrecoverable. To seize control of the Schema FSMO the NTDSUTIL must be used as follows:

1. Click **Start**, point to **Programs**, point to **Accessories**, and click the **Command Prompt** menu option.
2. Type **NTDSUTIL** to start the tool.
3. Type **roles** to access the fsmo maintenance menu.
4. Type **connection** to access the server connections menu.
5. Type **connect to server {server name}** to connect to the domain controller that will be assigned control of the Schema FSMO. Replace {server name} with the name of a valid domain controller.
6. Type **quit** to return to the fsmo maintenance menu.
7. Type **seize schema master** to take control of the Schema FSMO and give it to the connected domain controller.
8. Click the **Yes** button when the "**Are you sure you want server "server" to transfer the schema master for the enterprise?"** prompt is displayed.
9. Type **quit** to return to the ntdsutil menu.
10. Type **quit** to exit the tool
11. Type **exit** to close the Command Prompt.

To script this procedure use the following command:

> C:\ntdsutil roles "connections" "connect to server {server name}" quit "seize schema master" quit quit

NOTE: Seizing control of the Schema FSMO should only be considered when there is no way to recover the current master. If the original Schema FSMO is brought back online after control has been seized, then the Schema may be corrupted from changes that have not been replicated.

Logging Schema Events

Changes to the Active Directory Schema may be logged to the Security Logs on the domain controllers. To enable the logging:

1. Start the **Active Directory Users and Computers** snap-in by clicking **Start**, pointing to **Programs**, and then pointing to **Administrative Tools**.
2. On the **View** menu, click **Advanced Features**.
3. Right-click the **Domain Controllers** container, and then click **Properties**.

4. Click the **Group Policy** tab.
5. Click **Default Domain Controller Policy**, and then click **Edit**.
6. Double-click the following items to open them: **Computer Configuration**, **Windows Settings**, **Security Settings**, **Local Policies**, **Audit Policy**.
7. In the right pane, open **Audit Directory Services Access**.
8. Click the appropriate option(s): **Audit Successful Attempts** and/or **Audit Failed Attempts**.
9. Close the console.

Auditing Schema Changes

By using the Event Viewer it is possible to see when changes have been made to the Schema. To view the Schema events:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click the **Event Viewer** menu option.
2. Select the **Security Log** from the list of Event Viewers. The list of event will be displayed on the right hand side of the window.

Changes to the Schema will be logged with a Category of Directory Service Access. To view the details for a particular event, double-click the event. The details of the event will include a list the user who made the change, the name of the object that was changed, and a brief description of what was changed.

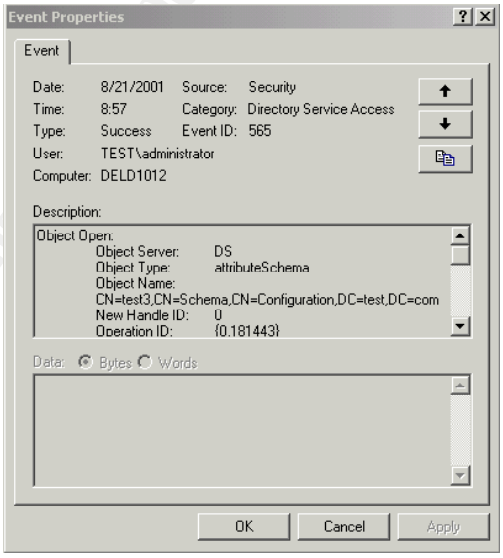

Figure 7 – Event Properties

Schema Replication

Every domain controller has two copies of the Active Directory Schema. One copy is kept on the hard drive in the NTDS.DIT (Active Directory database) on the domain controller. The other

copy, called the Schema cache, is loaded into memory when the domain controller is booted. The Schema cache is updated when the domain controller is booted or when the Schema changes are replicated.

The domain controller that holds the Schema FSMO also controls the structure and content of the Schema. When changes are made to the Schema, they are immediately written to the hard drive of the Schema FSMO. About five minutes after the changes have been made, a copy of the Schema is replicated to all of the other domain controllers in the domain, tree, and forest. The delay before the changes are replicated is used to maintain system performance. If after five minutes the Schema changes have not been fully implemented in Active Directory, then another delay may occur. This cycle will continue until all of the changes to the classes and attributes can be implemented within Active Directory. Any attempt to use any of the changed objects before they have been replicated will result in an error.

When the Schema needs to be updated immediately there is a mechanism available in the Active Directory Schema console that will allow a forced reload of the Schema. To reload the Schema do the following:

1. Start the Active Directory Schema console.
2. Select the **Active Directory Schema** sub-tree item.
3. Select **Reload the Schema** from the **Action** menu.

This will force an immediate reload of the Schema. The changes may still take time to be processed. The amount of time needed all depends on the scope of the changes and the number of objects within Active Directory.

Extending the Schema

Extending the Schema is an advanced and complex operation that can have implications that potentially affect the entire network and should only be done when absolutely needed. If changes are made incorrectly, they could impair or disable the server, network, tree, and forest. When extending the Schema consider the following points:

- Only add new classes and attributes to the Active Directory Schema when no other object exists to handle the need.
- Avoid modifying existing classes and attributes. Instead derive a new class subclass.
- Only extend an existing class when data must be directly linked to the object.
- Schema objects can never be deleted. If a class or attribute is no longer needed then it can be disabled.
- Modifying the Schema is best done programmatically.
- When new classes and attributes are added to the Schema, the administrative tools must also be extended. The default tools provided by Microsoft can handle only the default Schema.
- Test all changes to the Schema to determine their impact on the network.

- Before developing and testing a Schema modification, remove the Schema FSMO from the network or set up an isolated test network.
- Schema changes are replicated to every domain controller in the forest.

The best source for information about extending the Schema and updating the administrative tools can be found within the Active Directory Programmer's Guide at the Microsoft Web Site.

Schema Permissions

Like every object in the Active Directory, rights can be set for every object within the Schema. By default only the local System account on the domain controller has the Full Control permission for the Schema. The other root permissions for the Schema are:

Permission	Accounts Allowed
Full Control	System
Read	System Authenticated Users Schema Admins
Write	System Schema Admins
Create All Child Objects	System Schema Admins
Delete All Child Objects	System
Change Schema Master	System Schema Admins
Manage Replication Topology	System Administrators Enterprise Domain Controllers Schema Admins
Replicating Directory Changes	System Administrators Enterprise Domain Controllers Schema Admins
Replication Synchronization	System Administrators Enterprise Domain Controllers Schema Admins
Update Schema Cache	System Schema Admins

Changes to the Schema permissions must be made on the domain controller with the Schema FSMO that has permission to modify the Schema. If the write privilege is not set on the domain controller, the Schema permissions can only be viewed. The Active Directory Schema console is used for viewing and changing Schema permissions. To view the root permissions for the

Schema:

1. Start the Active Directory Schema console.
2. Select the **Active Directory Schema** sub-tree item.
3. Select **Permissions** from the **Action** menu.

The permissions for the individual classes within the Schema can be found on the Security tab in the class's properties window. Each class may have a different set of permissions. For instance, the Site class has the standard permissions such as Full Control, Read, and Write. The Site class also has a specialized permission called Open Connector Queue. The User Class has specialized permissions such as Reset Password and Change Password. There are not any rights in the Domain class that can be viewed.

Just like extending the Schema, changing the Schema permissions can cause many unwanted side effects. Therefore, the changes should only be made after they have been fully tested to determine how they will impact the network.

Schema Backup and Restore

A system backup of the domain controllers should include a copy of Active Directory and it will also include the Schema. The most up-to-date copy of the Schema will always be on the Schema FSMO. When restoring a domain controller it is entirely possible to also restore a copy of the Schema that is outdated.

Recommendations

The following recommendations should be followed to protect the Active Directory Schema.

Schema Manager

Designate a Schema Manager and make that person solely responsible for all changes to the Schema. It is best to assign a primary and secondary person to the position. The Schema Manager should be a skilled Windows 2000 administrator who fully understands the implications of making changes to the Schema.

Since Active Directory is a database and the Schema is its table structures, many of the same principles and skills for database administration should apply to the Schema Manager. Before any changes are made, the Schema Manager should review the changes and ensure they are consistent with the current Active Directory Schema design and that they will not adversely affect operations.

All user accounts and groups should be removed from the Schema Admin group. Then the Schema Manager should be given permissions to add and remove users from the Schema Admins group. It should then become the Schema Manager sole responsibility to add and remove users from this Schema Admins group. The Schema Manager should only give access to senior administrators and programmers experienced in Active Directory management.

To protect the Schema from unmanaged changes, the Schema Manager should only grant access to the Schema Admins group when changes need to be made. Once the changes are complete, the Schema Manager should immediately remove the user account from the Schema Admins group.

Documentation

Anytime the Schema is extended, the changes should be completely documented. This documentation can then be used to troubleshoot network issues, replicate changes if they should ever need to be redone, and provide assistance in developing other changes to the Schema. The documentation should be kept centrally and controlled by the Schema Manager.

Scripting Changes

Changes to the Active Directory Schema are best done programmatically. Script the changes so they may be uniformly applied within the development, testing, and production environments. Scripts become part of the permanent documentation. It also might be necessary to use the scripts in the event that the Schema changes need to be reapplied due to a corruption of the Schema.

Testing Changes

Anytime the Schema must be extended or there is need to change the security permissions for any object, it must be fully tested. Making untested changes to a production environment is never a good idea. Considering the adverse affects a Schema change could have to a network, it is best to be overly cautious. Use an isolated network for testing the Schema changes. If the production network is the only environment available for testing, make sure the Schema FSMO is offline to prevent replication of the changes to the other domain controllers on the network. This way the changes will not be permanent since all domain controllers refresh their copy of the Schema from the Schema FSMO.

Backup Schema after any Change

After any change has been made to the Schema it is a good practice to make a system backup of the domain controller with the Schema FSMO. This way there is a copy of the most current Schema. Be sure to test the backup to make sure it can be used to properly restore the server.

System Account

By looking at the permissions at the root of the Active Directory Schema it is obvious that the local System account, also know as LocalSystem, has more access to the Schema than any other account. The System account is not a user account. It is an account that the operating system uses to run programs, utilities, and device drivers. The System account has the Full Control permission for the Active Directory Schema. This means that any application using the System account has unrestricted access to the Schema. This includes such things as deleting all objects within the Schema. Even the Schema Admins group does not even have these permissions by default.

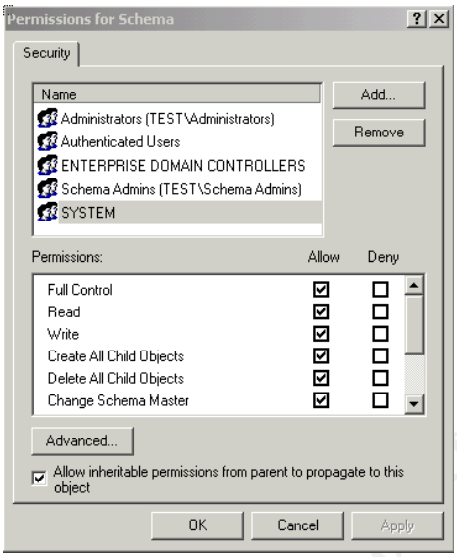

Figure 8 – System Account Permissions

This should be taken into consideration before any application is run using the System account. The safest alternative is to not run any applications on any of the domain controllers on the network. Instead, run them on an application server and use an account that has been created to give the service the lowest level of access rights.

References

Bragg, Roberta, Windows 2000 Network Security Design, New Riders Publishing, 2000

Lowe-Norris, Alistair G., Windows 2000 Active Directory, O'Reilly & Associates, Inc., 2000

Cox, Phillip, Sheldon, Tom, Windows 2000 Security Handbook, The McGraw Hill Companies, 2001

Windows 2000 Server Resource Kit, Microsoft Corporation, 2001

Step-by-Step Guide to Using Active Directory Schema and Display Specifiers, Microsoft Corporation, 2000, http://www.microsoft.com/windows2000/techinfo/planning/activedirectory/adschemasteps.asp