Top 10 security settings after installing Active Directory

Installing Active Directory is not too difficult, but once you have installed it, there is quite a bit of work to do. The first thing in Active Directory configuration is its security settings. There are many areas you need to consider and many settings need to be changed in preparation for protecting actions in the starboard

Derek Melber

The initial settings that you need to perform with Active Directory to secure the network before you delve into setting up the entire infrastructure.

Installing Active Directory is not too difficult, but once you have installed it, there is quite a bit of work to do. The first thing in Active Directory configuration is its security settings. There are many areas you need to consider and many settings need to be changed to prepare for network actions. Let's take a look at the initial settings that you should make to Active Directory to secure the network before entering the entire infrastructure setup.

Create a separate admin account

After installing Active Directory, you need to take care of your resources immediately. Not only does it protect new Active Directory resources but also create a world through which it can be safely managed. To do that, you need to create a new user account that is used when administering anything related to Active Directory.

Note :
This means that you should not use the associated Administrator account in the habit or administration of Active Directory in the usual way!

Once you have created this new account, you need to add it to the Domain Admins group. Since there is only one domain at this time, you will get the ability to do anything within this domain if necessary.

Note :
By becoming a member in the Domain Admins group in the root domain (the first domain in forest), you will be able to add or remove users from the Schema Admins and Enterprise Admins groups. However, there is no reason to have members in these groups until you need to perform an action that requires this privilege level.

During the process of creating user accounts, you should create a long and complex password. This will help protect your account against attackers and hackers. If the password is weak, it will easily be unlocked by hackers and attack the domain as an administrator.

Set up a long and complex password for an administrator account

Now that you have an account to administer the domain, you should protect the previously designed Administrator account in the fullest sense. Initially, you need to protect the passwords of these accounts. At the very least, create a password of about 15 to 20 characters in length and complexity.

Note that all of these passwords must be very long and use at least 3 character types in each password.

Rename the Administrator account in the first Active Directory domain

This tip is not the most technical thing you can ever hear, but it should be done because it is good for you anyway. Change the name of the default Administrator account to another name. You should use the same format for other user accounts (JohnDoe, GatesBill, SLJackson, .). This will help protect the account by simple and ordinary hackers. Obviously, this does not change the SID for the account, but at least browsing through a list of users will not be easy to identify immediately.

Set password policy in default domain policy (Default Domain Policy)

There have indeed been many articles on how to properly set up a password policy for a domain to reduce the attack surface. Only when those parameters are taken away can your network be vulnerable. However, in Default Domain Policy, password policy settings must be set as shown in Figure 1.

Figure 1

Here are some guidelines for setting up these policies:

Policy setting Minimum value Safety value Minimum password life11 Maximum password life18045 Password minimum length814 + Complexity of Enabled password (Enabled) Enabled (Enabled)

Set up account lockout policy in Default Domain Policy

Account lock policy settings are a much debated topic for a long time. There are two views to this debate. The first view is that the password must be locked if there are 3 or more attempts to enter the password failed. The second view suggests that there should be an unlimited number of attempts to log in, because sometimes they don't remember the password at all.

This type of argument is quite natural because its views are reasonable. The problem with password locking after only a few attempts to block an attacker sometimes also affects the employees themselves .

With a second point of view, arguing for an unlimited number of attempts may allow an attacker to attempt multiple attempts to log into the account by guessing multiple passwords.

From my standpoint, the option to allow a certain number but not infinite for the test will be better and safer. If you follow good password restrictions on complexity and length, the ability to guess a password is nearly impossible, or even use a script to search for it. However, I suggest you set the number of tries to about 100 times before the account is locked.

Figure 2 shows the options for setting up Account Lockout Policy.

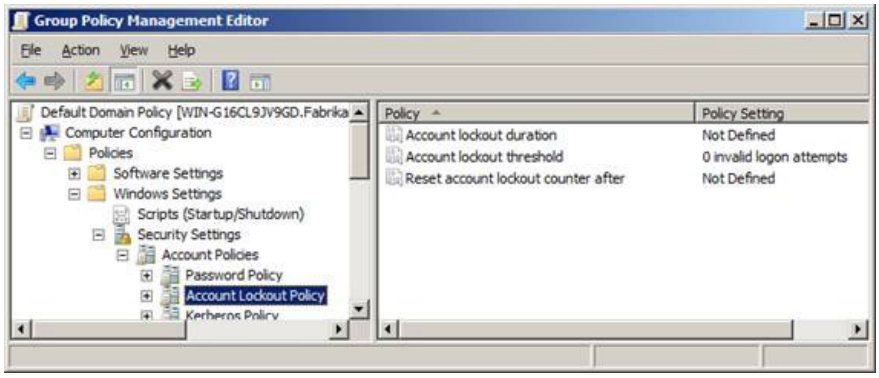

Figure 2

Create OU (Organizational Unit) for user accounts

In order for user accounts and their settings on the desktop to be controlled you need to create an OU for user accounts. User accounts (default) are placed in an item named 'Users', and there is absolutely no GPO associated with it.

You not only create an OU for user accounts, but in most cases you will create a hierarchical structure and a structured OU for user accounts. This will allow you to manage which GPO settings affect which user accounts. The ideas for the logical structure of the OU for user accounts with the OUs are given below:

1. Offices such as finance, IT, .
2. Regions such as the Northeast, Asia, Branch 1, .
3. Job Roles such as Manager, Executive, HelpDesk, .

Create OUs for computer accounts

You can also create OUs for computer accounts, for the same reason as user accounts. Here you can look at existing computer types, which can be categorized into the following categories:

1. Servers like IIS, Exchange, application, .
2. Desktops such as IT, mobile, .

Create a GPO and link to the new OU for computer accounts

To ensure your computers are safe when they are in the domain, you need to have a set of security settings when you join a domain. To do this, you only need to create a GPO and link it to the OU for computer accounts created. The idea for the settings you should have in a GPO includes:

1. Activate UAC
2. Reset internal admin password
3. Control membership of the Administrators group
4. Control anonymous connections
5. Control of login authentication protocols has been supported

Configure DSN to forward

Most companies need this installation, but not all. However, based on what you have seen in the field, most companies need to target DNS configuration immediately to allow access to the Internet, but also protect DNS that supports Active Directory. To do this, you need to configure DNS to support the Active Directory environment to forward all Internet requests to an Internet-enabled DNS server. This requires the following settings:

1. Configure all domain clients to use DNS to support Active Directory
2. Configure Active Directory DNS servers to forward requests to outgoing DNS servers.

Rename the entire Administrator account in all domains

You should reset the Administrator account name in the Security Accounts Manager (SAM) internally for each computer (server and desktop) in the domain as well as for each new domain you add to the forest. You can do this through the GPO, shown in Figure 3, which will make your configuration easier and more efficient. In addition, it does not exclude an attack that is looking for a new name, but it will reduce attacks on the system with the default name.

Figure 3

Conclude

Once you have installed Active Directory and are running, you have just started your configuration. To ensure a safe and stable Active Directory, you need to make some settings immediately to get everything configured and secure. You need to target domain administration, including the associated Administrator account and the accounts that will be used to manage Active Directory daily. With user and desktop control in the environment, you need to make settings that allow users to password protect, as well as control desktops and user accounts through Group Policy. If you do this important security after installing Active Directory, it is also good to protect your network and your company.

You finished reading the article "**Top 10 security settings after installing Active Directory**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com