Active Directory Best practices

Updated: January 21, 2005

Applies To: Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with SP2

Best practices

- **As a security best practice, it is recommended that you do not log on to your computer with administrative credentials.**

  When you are logged on to your computer without administrative credentials, you can use Run as to accomplish administrative tasks.

  For more information, see Why you should not run your computer as an administrator and Using Run as.

- **To further secure Active Directory, it is recommended that you implement the following security guidelines:**

  - Rename or disable the Administrator account (and guest account) in each domain to prevent attacks on your domains. For more information, see User and computer accounts.

  - Physically secure all domain controllers in a locked room. For more information, see Domain controllers and Securing Active Directory.

  - Manage the security relationship between two forests and simplify security administration and authentication across forests. For more information, see Forest trusts.

  - To provide additional protection for the Active Directory schema, remove all users from the Schema Admins group, and add a user to the group only when schema changes need to be made. Once the change has been made remove the user from the group.

  - Restrict user, group, and computer access to shared resources and to filter Group Policy settings. For more information, see Group types.

  - Avoid disabling the use of signed or encrypted LDAP traffic for Active Directory administrative tools. For more information, see Connecting to domain controllers running Windows 2000.

  - Some default user rights assigned to specific default groups may allow members of those groups to gain additional rights in the domain, including administrative rights. Therefore, your organization must equally trust all personnel that are members of the Enterprise Admins, Domain Admins, Account Operators, Server Operators, Print Operators and Backup Operators groups. For more information about these groups, see Default groups.

  - Use global groups or universal groups instead of domain local groups when specifying permissions on domain directory objects replicated to the global catalog. For more information, see Global catalog replication.

    For general security information about Active Directory, see Security information for Active Directory and Securing Active Directory.

- **Establish as a site every geographic area that requires fast access to the latest directory information.**

  Establishing areas that require immediate access to up-to-date Active Directory information as separate sites will provide the resources required to meet your needs.

  For more information, see Create a site.

- **Place at least one domain controller in every site, and make at least one domain controller in each site a global catalog.**

  Sites that do not have their own domain controllers and at least one global catalog are dependent on other sites for directory information and are less efficient.

  For more information, see Enable or disable a global catalog.

- **Perform regular backups of domain controllers in order to preserve all trust relationships within that domain.**

  For more information, see Domain controllers.

Community Additions