Active Directory Overview and Security Basics

Overview

Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks and is included in most Windows Server operating systems as a set of processes and services. Below is a list of terms you may encounter when using AD.

(http://msdn.microsoft.com/en-us/library/hh871788.aspx)

- **Domain controller**: A domain controller is a server that takes care of managing Active Directory, including hosting its database and handling the authorization, authentication and accounting mechanisms.
    - Can run on Windows 2000 Server edition, Windows Server 2003. Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2, Windows Server 2012 and Windows Server 2012 R2.
    - Active Directory is fully integrated with DNS and requires TCP/IP—DNS. To be fully functional, the DNS server must support SRV resource records, also known as service records.
    - Microsoft recommends more than one domain controller to provide automatic failover protection of the directory.
    - Domain controllers are also ideally single-purpose for directory operations only, and should not run any other software or role. Certain Microsoft products such as SQL Server and Exchange can interfere with the operation of a domain controller.
    - Microsoft recommends not running multiple virtualized domain controllers on the same physical hardware.
    - You not only have to have robust hardware to support higher auditing levels (specifically fast disks to support the increased I/O), but also more disk space so that events don't get overwritten quickly. For servers, ideally you will forward the events to a centralized log server, so disk space should not be an issue in this case. For workstations and laptops on the other hand, log forwarding becomes logistically harder and more expensive to implement, so you may need to find a sweet spot between verbose logging and local storage limitations.
- **Domain:** A domain is defined as a logical group of network objects (computers, users, devices) that share the same active directory database. Domains are identified by their DNS name structure, the namespace.
- **Tree:** A tree is a collection of one or more domains and/or domain trees in a contiguous namespace, linked in a transitive trust hierarchy.
- **Forest:** A forest is a collection of trees that share a common global catalog, directory schema, logical structure, and directory configuration. The forest represents the security boundary within which users, computers, groups, and other objects are accessible.

- **Organizational Unit (OU):** OUs are nested inside domains. (ex. ABC company has multiple offices in multiple cities. Create an OU for each city then an OU under each city for things like “computers”, “users”, “servers”, and “groups”. Can even go further to add OUs under “Users” for “HR” and “R&D”) The OU is the recommended level at which to apply group policies.
- **Shadow groups:** OUs do not confer access permissions, and objects placed within OUs are not automatically assigned access privileges based on their containing OU. A common workaround for an Active Directory administrator is to write a custom PowerShell or Visual Basic script to automatically create and maintain a user group for each OU in their directory. Such groups are known as Shadow Groups. Microsoft refers to shadow groups in the Server 2008 Reference documentation
- **Partitions:** The Active Directory database is organized in partitions. Microsoft often refers to these partitions as 'naming contexts'. The 'Schema' partition contains the definition of object classes and attributes within the Forest. The 'Configuration' partition contains information on the physical structure and configuration of the forest (such as the site topology). Both replicate to all domains in the Forest. The 'Domain' partition holds all objects created in that domain and replicates only within its domain.
- **Protocols**:
    - Lightweight Directory Access Protocol (LDAP) versions 2 and 3,
    - Microsoft's version of Kerberos
    - Objects in Active Directory databases can be accessed via LDAP protocol, ADSI, messaging API and Security Accounts Manager services.
- **Replication:** Active Directory synchronizes changes using multi-master replication. Replication of Active Directory uses Remote Procedure Calls (RPC) over IP (RPC/IP). Between Sites SMTP can be used for replication, but only for changes in the Schema, Configuration, or Partial Attribute Set (Global Catalog) GCs. SMTP cannot be used for replicating the default Domain partition.
- **Trust**
    - Terminology
        - **One-way trust:** One domain allows access to users on another domain, but the other domain does not allow access to users on the first domain.
        - **Two-way trust:** Two domains allow access to users on both domains.
        - **Trusted domain:** The domain that is trusted; whose users have access to the trusting domain.
        - **Transitive trust:** A trust that can extend beyond two domains to other trusted domains in the forest.
        - **Intransitive trust:** A one way trust that does not extend beyond two domains.
        - **Explicit trust:** A trust that an admin creates. It is not transitive and is one way only.
        - **Cross-link trust:** An explicit trust between domains in different trees or in the same tree when a descendant/ancestor (child/parent) relationship does not exist between the two domains.
        - **Shortcut:** Joins two domains in different trees, transitive, one- or two-way.
        - **Forest trust:** Applies to the entire forest. Transitive, one- or two-way.
        - **Realm:** Can be transitive or nontransitive (intransitive), one- or two-way.

        - **External:** Connect to other forests or non-AD domains. Nontransitive, one- or two-way.
    - Forest trusts: Windows Server 2003 introduced the *forest root trust*. **Example**: Suppose that a two-way transitive forest trust exists between the forest root domains in Forest A and Forest B, and another two-way transitive forest trust exists between the forest root domains in Forest B and Forest C. Such a configuration lets users in Forest B access resources in any domain in either Forest A or Forest C, and users in Forest A or C can access resources in any domain in Forest B. However, it does *not* let users in Forest A access resources in Forest C, or vice versa. To let users in Forest A and Forest C share resources, a two-way transitive trust must exist between both forests.
- **Administration**: Administration (querying, modifying, and monitoring) of Active Directory can be achieved via many scripting languages, including PowerShell, VBScript, JScript/JavaScript, Perl,Python, and Ruby. Using free AD administration tools can help to simplify AD management tasks.

Security

- http://it-audit.sans.org/blog/checklists/active-directory-security-checklist/ (AD security checklist)
- http://www.nsa.gov/ia/_files/os/win2k/w2k_active_dir.pdf (AD security checklist)
- http://web.nvd.nist.gov/view/ncp/repository/checklistDetail?id=274 (AD security checklist)
- (http://msdn.microsoft.com/en-us/library/hh871766.aspx) Other systems that interact with the Active Directory system should take the following steps to protect their own security:
    - Specify a time limit in their requests to the directory service that is not longer than the maximum amount of time clients can afford to wait for a response.
    - Enforce client-side time-outs so that even if the directory service does not respond in a timely fashion or ignores the time limit that clients specify, the clients abandon the operation and do not hang indefinitely while they wait for the directory service to respond.
    - Avoid performing inefficient operations against the directory service that take longer to complete than clients can afford to wait.
    - Use the SPNs to perform mutual authentication to ensure that it is communicating with the intended directory service and not an impostor.
- **Reducing the Active Directory Attack Surface**: (http://digital-forensics.sans.org/blog/2013/06/20/overview-of-microsofts-best-practices-for-securing-active-directory) report from 06/20/2013
    - Reduce Admin Accounts and Admin Group Memberships
        - Typical default groups include Enterprise Admins, Domain Admins, Built-in Administrators. Ideally, reduce membership to a point where there are no permanent members of these groups. A couple of the third-party tools that can help with this are privileged account management solutions from Cyber-Ark and Lieberman.
    - Establish Dedicated Administrative Hosts

    - The idea here is that users with privileged accounts should *only*use those privileged accounts on these dedicated, locked-down secure systems (i.e., no RunAs on our own machines). Suggested solutions include using dedicated physical workstations, using VMs, and/or using dedicated "jump point" servers (typically via Remote Desktop)
- Mitigate Physical Attack of DCs
    - Read-Only Domain Controllers (RODC)
- Implement Application Whitelisting
- Utilize "Authentication Mechanism Assurance" for Smart Cards
    - Two-factor authentication should be the norm, not the exception
    - new feature called "Authentication Mechanism Assurance" in Windows Server 2008 R2 allows a user's access token to be designated as having logged on with a certificate-based method.
- Utilize Templates for Secure Configurations
    - For sensitive systems, such as domain controllers and privileged-account workstations, take advantage of Microsoft Security Compliance Manager. This is a free tool that integrates security configurations that are recommended by Microsoft. Templates are available for all major OS versions and Service Packs, as well as Exchange, IE, and Office. See the available templates here: http://technet.microsoft.com/en-us/library/cc677002.aspx. Furthermore, GPOs can be used to enforce them.
- Address Poorly Coded Apps
- Make Security Easy for End Users