Active Directory and Group Policy

Blackhat Amsterdam
Raymond Forbes

Overview

- Active Directory Basics
  - Structure
  - Components
  - Objects
  - Roles
  - Schema
  - Sites
  - Interop

Overview

- Group Policy

Active Directory

- What is Active Directory?
  - LDAP Directory Service
  - Works with and requires DNS
  - Incorporated into Windows 2000 and XP
  - Centrally Managed
  - Extensible
  - Interoperable

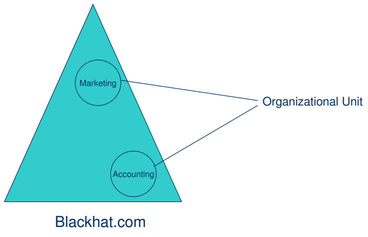
Active Directory

- Building blocks of Active Directory
  - Objects
    - Users
    - Machines
  - Sites
  - Domains
  - Trees
  - Forests
  - Trusts
    - Transitive
    - Non-Transitive
    - Cross Link

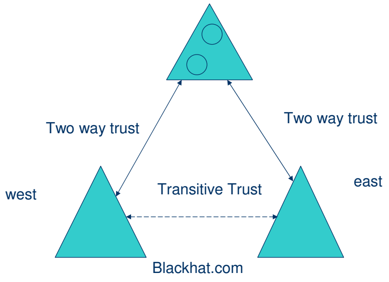
Active Directory

- Building blocks cont'd
  - Domain Controllers
  - Groups
    - Global Groups
    - Universal Groups
    - Domain Local Groups

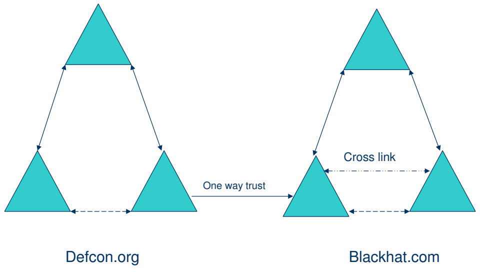
Active Directory



Active Directory



Active Directory



Active Directory

- Sites
  - Collection of IP addresses
  - Information is stored by all domain controllers in the forest
  - Intra-site replication is instant
  - Inter-site replication can be scheduled
  - Used at logon to find closest Domain Controller
  - Bridgehead Server
    - Maintains link between sites.

Active Directory

- Sites cont'd
  - Subnets
    - Does not necessarily translate from actual subnets
  - Knowledge Consistency Checker
    - Automatically defines the replication topology and bridgehead servers.
    - These can be set manually

Active Directory

- FSMO Rules (Flexible Single-Master Operation)
  - Domain Naming Master
    - Domain specific tasks (addition, removal of domains)
  - Infrastructure Master
    - Maintains cross directory links
  - PDC Emulator
    - Support for NT4 domains. First server that takes password changes
  - Relative ID (RID) Master
    - Makes sure all SIDs are unique. All object moves happen through here.
  - Schema Master

Active Directory

- Global Catalog
  - Read Only
  - Partial database. Subset of information in the schema
  - Used for fast searching and logons
    - All universal group information is stored in the Global Catalog.

Active Directory

- Schema
  - Holds what type of information can be stored in the Active Directory
  - Each object is an instance of a class
  - Attributes are defined for classes
    - Optional or mandatory
  - Tree like structure
  - Classes are inherited

Active Directory

- Schema cont'd
  - Schema Classes
    - Abstract Classes
      - Not actually used to make objects.
      - Used to provide structure to the schema
    - Structural Classes
      - This is used to make directory objects
    - Auxiliary Classes
      - Provides add on information that can be applied to other classes

Active Directory

- Schema Cont'd
  - Schema is cached in memory
  - Only one Schema for the entire forest
  - Cannot actually delete anything from the Schema after it has been extended.
    - The only option you have is to deactivate any non used classes

Active Directory

- DNS
  - AD puts in a number of SRV records into your DNS.
    - _ldap._tcp. 600 IN SRV 0 100 389 server1
    - _ldap._tcp.pdc IN SRV 0 100 389 server 1
    - _kerberos._tcp.dc._msdcs IN SRV 0 100 88 server1

Active Directory

- Replication
  - Multi Mastered
  - Tracks meta-data
  - Different based on whether intra-site or inter-site
    - Intra-site is simple, and not very configurable
    - Inter-site can use RPC or SMTP
  - Not all data is replicated
    - For instance, user last logon time
  - Replicates attributes, not entire objects

Active Directory

- Replication cont'd
  - Meta-Data
    - Update Sequence Number (USN)
      - Defines latest update on a paticular Domain Controller
    - Property Version Number
      - Version of attribute
    - Attribute Timestamp
    - IP address of Domain Controller
  - Server stores the USN of each DC seperately
    - Each USN is stored by the server's GUID

Active Directory

- Replication Cont'd
  - When a change is made on the Domain controller the USN is changed. The other DCs are notified.
  - The DC asks for all the changes post the USN it has recorded.
  - DC applies changes and stores new USN for that DC.

Active Directory

- Replication cont'd
  - Conflict Resolution
    - A conflict is detected by the DC comparing the PVN on the local store with the one in the change.
    - If a conflict is detected it is resolved with these values
      - Highest PVN
      - Timestamp
      - IP address

Active Directory

- Inter-site replication
  - By default, this is done by a schedule
  - Very configurable. Can define what servers replicate to what servers.
  - Can use RPC or SMTP
    - SMTP doesn't support file replication (e.g. logon scripts)
  - Compressed by up to 15%
  - You CAN turn on inter-site notification
    - This has the effect of making inter-site communication just like intra-site.

Active Directory

- Password Replication
  - Password changes can happen on any DC
  - When a password is changed on a DC it pushes that change immediately to the PDC Emulator
  - Before a server actually rejects a bad password, it contacts the PDC Emulator and verifies it there
  - This makes sure that a password change does not deny access

Active Directory

- Other replication issues
  - Multiple Values
    - Some attributes have multiple values (i.e. Groups)
      - This can be a problem as it could lead to two valid changes but both with the same PVN
      - Only the latest change will be kept. The previous ones will be dropped
    - Inherited permissions
      - Inherited permissions are actually stored on each object
      - However, the DC only replicates the inheritable permission and let's the receiving server actually do the work.

Active Directory

- Other Replication Issues cont'd
  - Tombstone
    - When an object is deleted it isn't removed at first
    - This would cause the other DCs to not know the object should be deleted.
    - Instead, when an object is deleted it has a "tombstone" placed on it.
    - This object is moved to a hidden Deleted Objects container. This is hidden even from ADSI
    - The tombstone is replicated to all controllers
    - Garbage collection goes through and removes tombstoned objects that have expired

Active Directory

- Other Replication Issues cont'd
  - LostAndFound
    - The LostAndFound container holds objects that tried to replicate but could not for some reason
    - Suppose somebody adds a user to an OU on one server but then deletes the OU on another server

Active Directory

- Other Replication Issues cont'd
  - Urgent Replication
    - Standard replication happens every 5 minutes intra-site and upon schedule for inter-site
    - Certain circumstances demand immediate replication
    - RID Master change
      - If another server has been given the role as RID Master
    - LSA Secret Change
    - Account lock-outs
    - Urgent Replication doesn't happen inter-site unless notification is turned on.