

4417

System Administration

Jack Ramsey
Lecture 4



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Outline

Windows Lineage

Server 2012 Features

Planning for server deployment

Linux History

Windows network architecture

Active Directory Domain Services (AD DS)

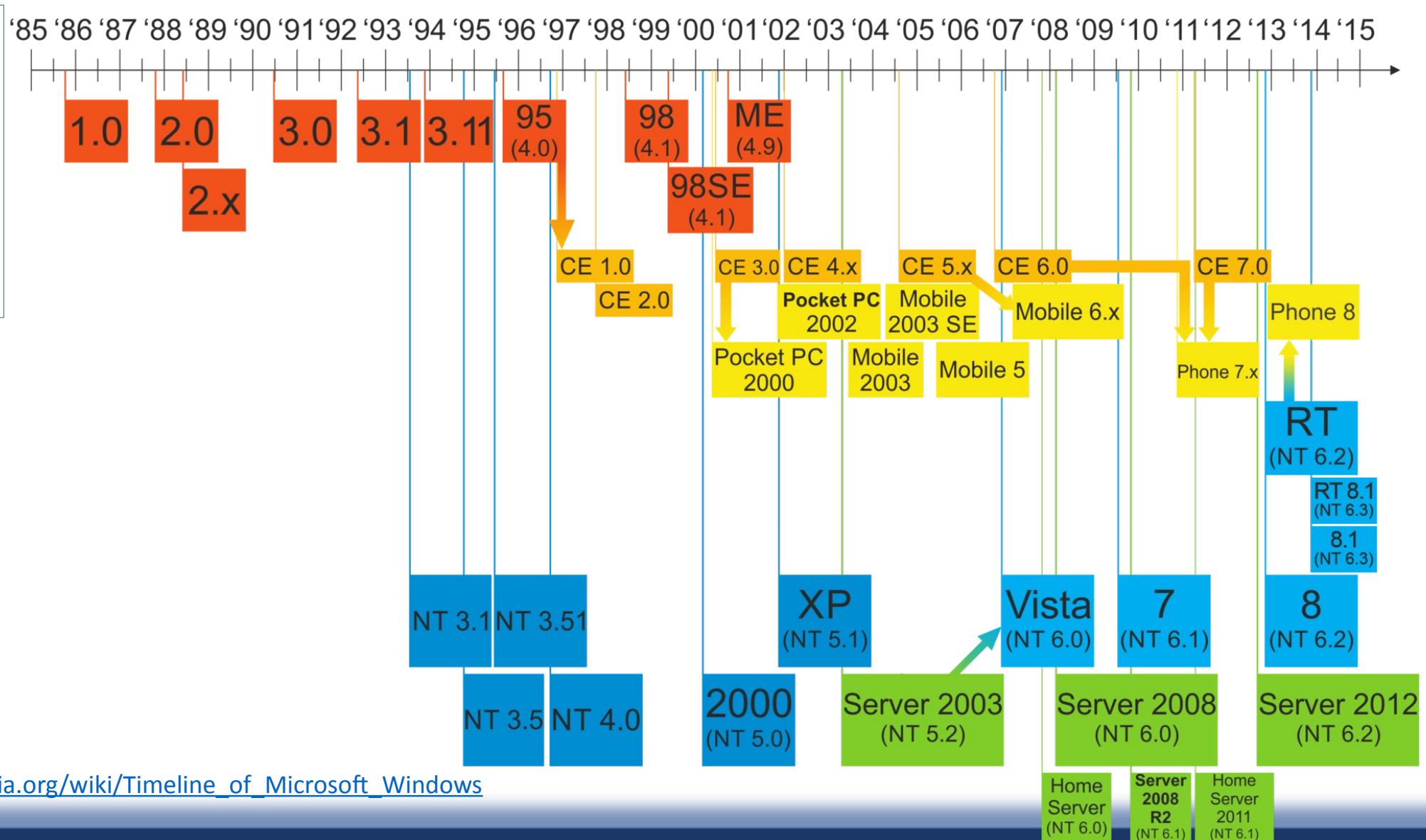


Windows - A Brief History



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Windows Clients & Servers



Server 2012 / 2012R2

Major/minor/major release schedule

Until recently (Windows 10/Server 2016), server and desktop client OSs were released in tandem

Next version due out in 2016 (deviating from past practice)

2008/Win 7 tightly integrated

2012/Win 8 tightly integrated



2012 Server App Server

File and print server

Active Directory (AD) server

- Trash recovery

- Offline join domain

Dedicated Roles

- Mail, SQL, DHCP, DNS, etc.



Server 2012 Editions

Effectively only two

Standard – Recommended for physical server that won't usually be virtualizing guest sessions

Datacenter – Provides support for unlimited number of virtual guest sessions on the server

Recommended for highly virtualized environments.



2012 Features: Self-Healing NT File System (NTFS)

OS has a worker thread that runs in the background which makes corrections to the file system when NTFS detects a corrupt file or directory

Eliminates past need to reboot server to repair



2012 Features: Server Message Block 3.0

SMB: a protocol that handles the transfer of files between systems

Compresses file communications & uses a larger communications buffer

Reduces number of round trips needed when transmitting data between systems

With large files or data sets (particularly across WAN connection), results in transfers that are 10x to 30x faster than in the past



2012 Features: Hyper-V

Virtualization service in a Windows environment

Provides a thin layer between the hardware abstract layer of the system & the operating system that provides guest sessions in a virtualized environment

Communicate directly with the hardware layer of the system

Faster performance/Elimination of host OS bottlenecks



2012 Features: Storage Spaces

Group together storage on multiple servers and having it displayed and accessible to users as a single storage share

Work in the same way as RAID striping or RAID drive mirroring, but can be done across systems.

Storage & server resilience

Eliminates single server as a bottleneck and/or single point of failure



2012 Features: De-Dupe

Data de-duplication: decreases data storage capacity demands

Many organizations store multiple copies of data files on a server

Acknowledges duplication of bits on the disk, flags the data as duplicates and opens up space for storage of other information

Can save 30% to 70%



Linux



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

A brief history ...

Late 1960's - Unix is developed and released in 1970's. It is widely adopted in business and academic circles

1983 - a programmer Richard Stallman creates the GNU Project (“**GNU's** Not Unix”). It is an attempt at creating a Unix-type operating system but composed of entirely free software

1987 - Another programmer Andrew S. Tanenbaum creates Minix, a Unix like operating system for Academic use

1991 - a Finnish student Linus Torvalds creates a non commercial version of Minix and calls it Linux

<http://www.gnu.org/gnu/thegnuproject.en.html>



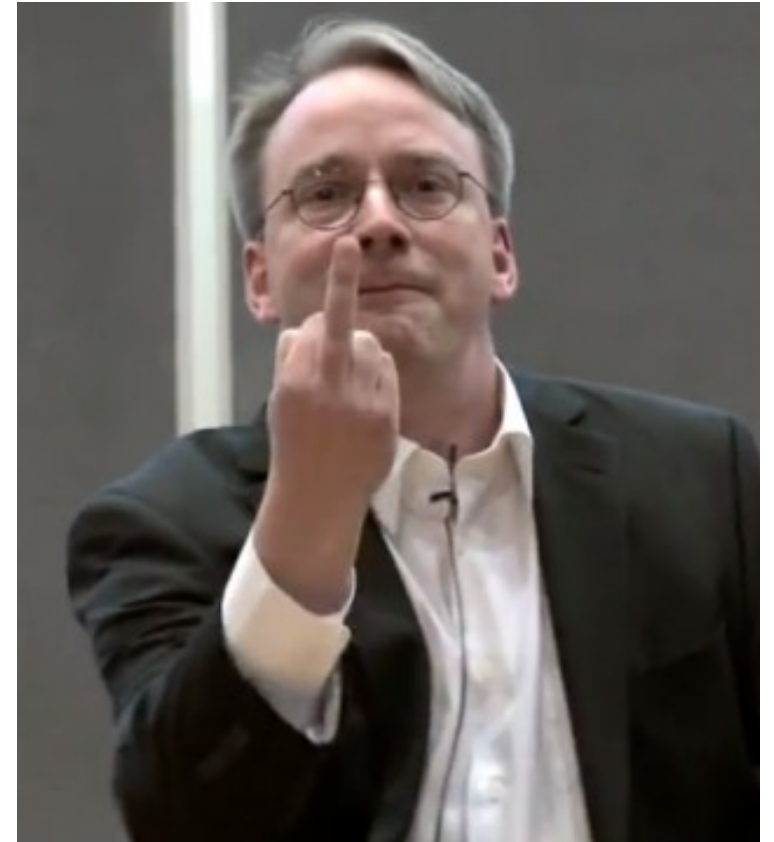
East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Linus Torvalds

Linus Torvalds is considered one of the greatest living programmers, and for good reason, having written some of the most widely used software, such as the Linux kernel and the Git revision control system. He's also known for not being shy about sharing his opinions on things that he doesn't like through colorful and sometimes NSFW language.

-- ITWorld Magazine (1/21/2015)

11 technologies that tick off Linus Torvalds, <http://www.itworld.com/article/2873200/11-technologies-that-tick-off-linus-torvalds.html>



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Linux Distros

Wikipedia provides a pretty comprehensive list <http://distrowatch.com/>

Here are some of the better known, in addition to Ubuntu:



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Linux Distros (...an abbreviated list)

Linux Mint	Mageia	LXLE	Tails
Arch Linux	PCLinuxOS	Zorin	Simplicity
Gentoo	Puppy	Lubuntu	Ultimate
Red Hat Linux	Mandriva	Kubuntu	SparkyLinux
Fedora	Slackware	Deepin	KaOS
CentOS	Xandros	Manjaro	Lite
Debian	Robolinux	SteamOS	KNOPPIX
OpenSuse	FreeBSD	Crunchbang	And many, many more...



A GUI?

The Linux kernel is command line

The X Window System (X11) developed by MIT is foundation for GUIs

Desktop manager and Window manager

Allow windows-like GUIs

This allows Linux to have a low degree of coupling

You can run different desktop managers on the same kernel

Gnome Vs. KDE (I like Gnome 3)



Installing Linux

Similar considerations should be taken as with Windows deployments

Both 32 and 64 bit versions

Depending upon what you install, HW can be very modest



4417/5417

System Administration

Active Directory



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Outline

AD basics

Plan AD Containers

Configure Security Groups

Object Management

New features to AD



Active Directory Basics

Directory service

Houses information about all network resources:

Servers, printers, user accounts, groups of user accounts, security policies, and other information

Domain controllers (DCs)

Servers that have the AD DS server role installed

Member servers

Do not have AD installed



Active Directory Basics

Domain

Fundamental component or container

Holds information about all network resources that are grouped within it

Each DC is equal to every other DC

Multimaster replication

Advantage

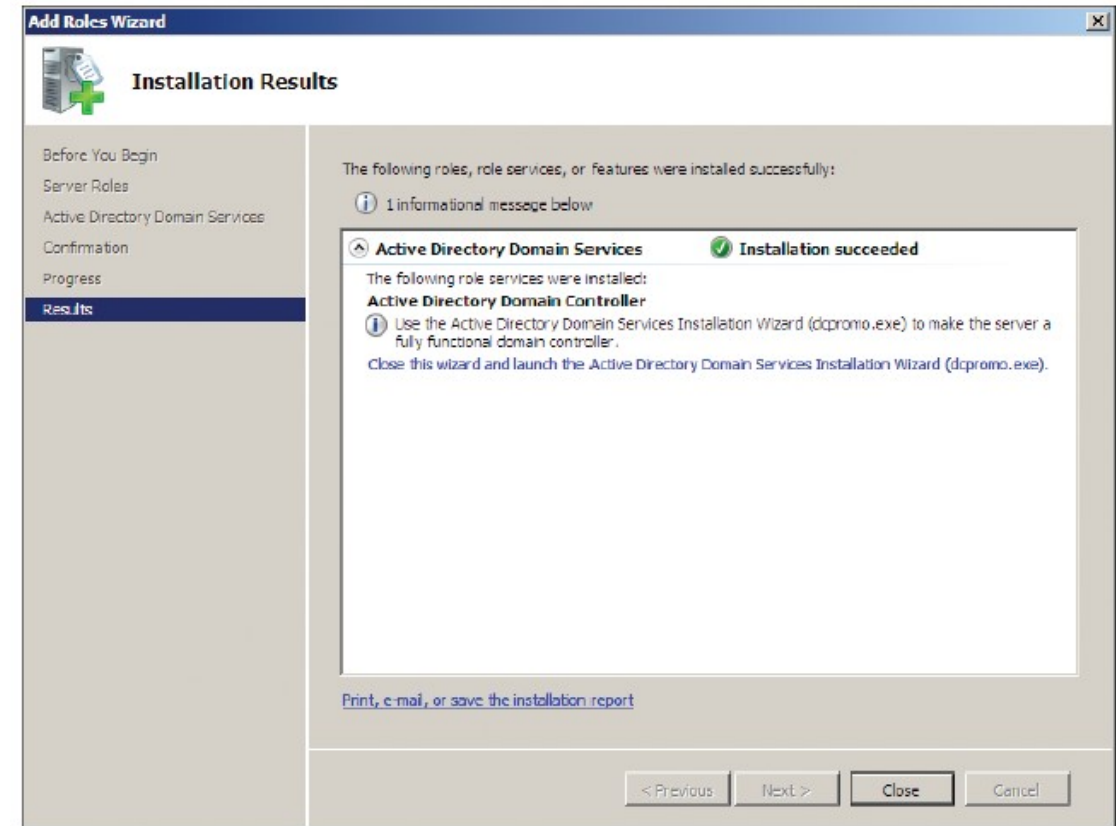
If one DC goes down, no network interruption



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Active Directory Basics

Installing Active Directory



Installation Results window

Schema

Defines objects and the information pertaining to those objects that can be stored in Active Directory

Characteristics of objects

Each attribute automatically given a version number and date

When created or changed



Schema

Sample schema for user account

Includes **globally unique identifier (GUID)**

Unique number associated with the object name

Examples:

{25892e17-80f6-415f-9c65-7395632f0223}

{a53e98e4-0197-4513-be6d-49836e406aaa}

{e33898de-6302-4756-8f0c-5f6c5218e02e}

{3a768eea-cbda-4926-a82d-831cb89092aa}



Global Catalog

Stores information about every object within forest

First DC configured in a forest becomes **global catalog**

Can change to another DC

Purposes:

- Authentication

- Forest-wide searches of data

- Replication of key AD elements

- Keeps copy of most used attributes for quick access



Containers in Active Directory

Treelike structure

Containers:

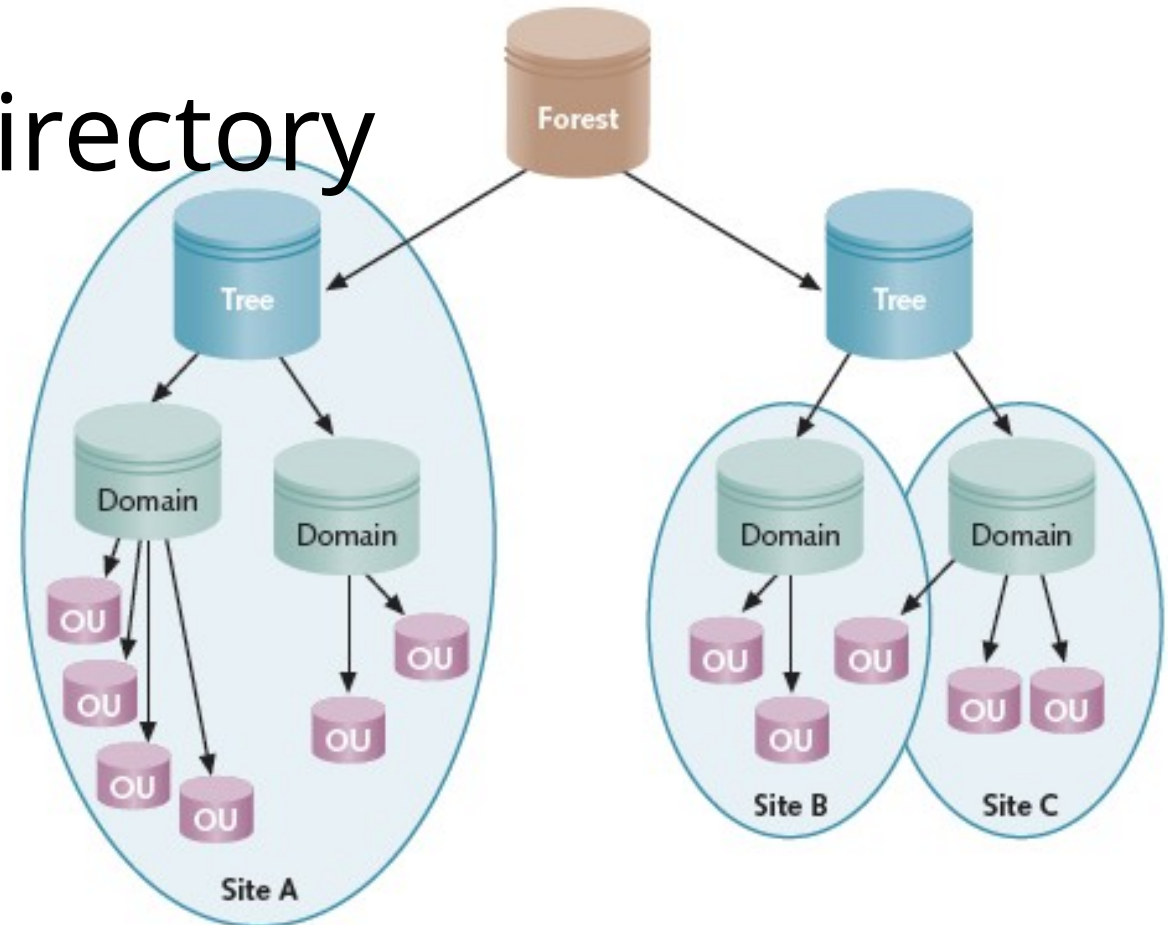
Forests

Trees

Domains

Organizational units (OUs)

Sites

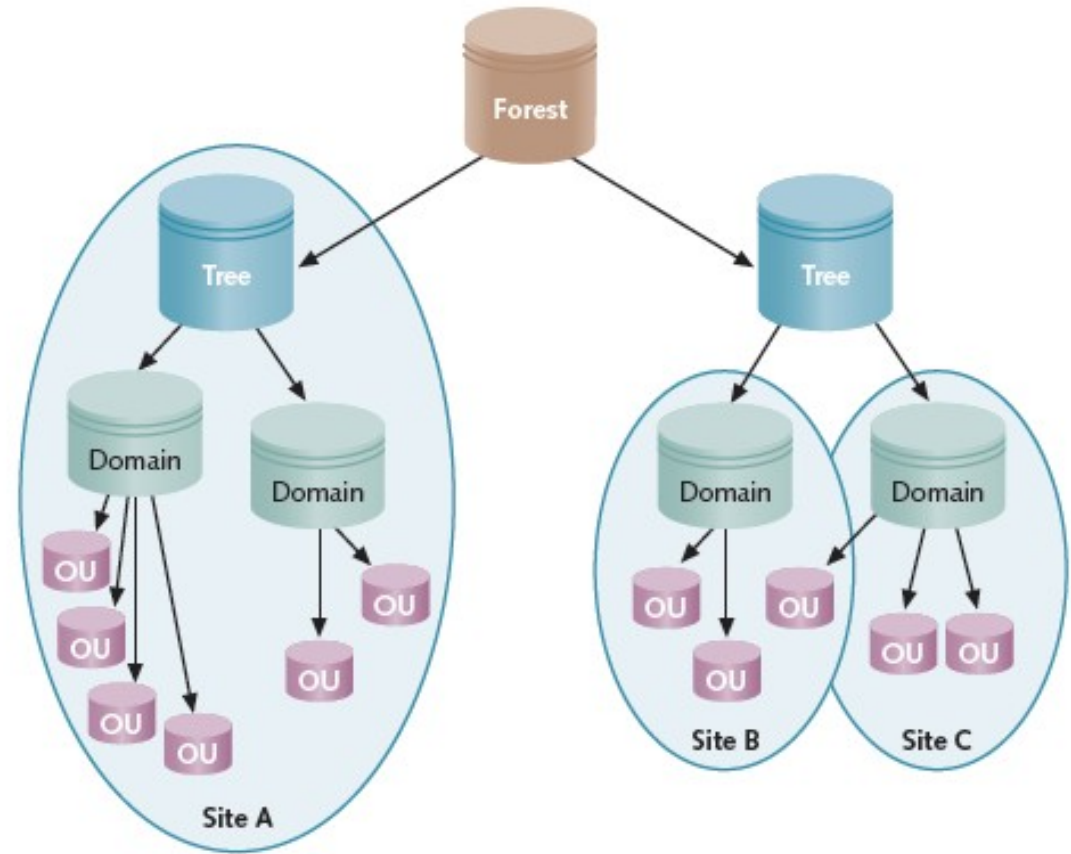


Active Directory hierarchical containers

Forest

Highest level in an Active Directory

One or more Active Directory trees that are in a common relationship



Forest

Forest functional level

Active Directory functions supported forest-wide

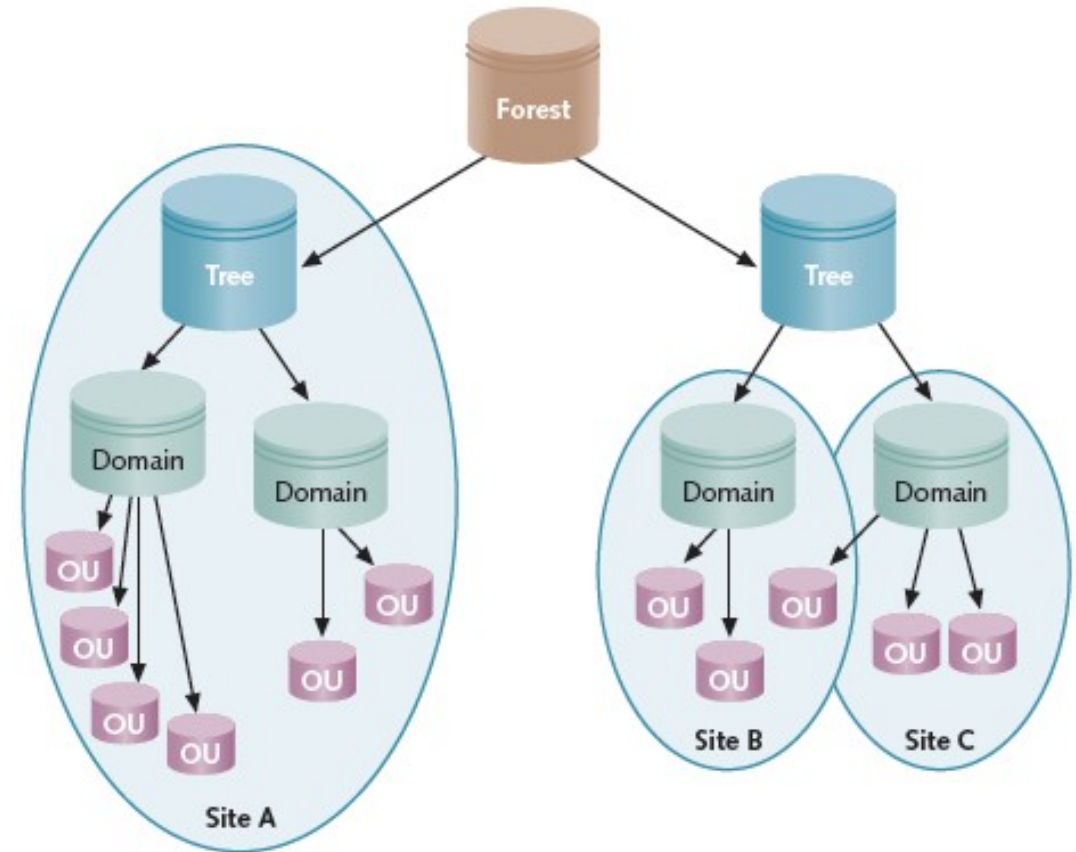
Levels:

Windows 2000 native forest functional level

Windows Server 2003 forest functional level

Windows Server 2008 forest functional level

Windows Server 2012 forest functional level



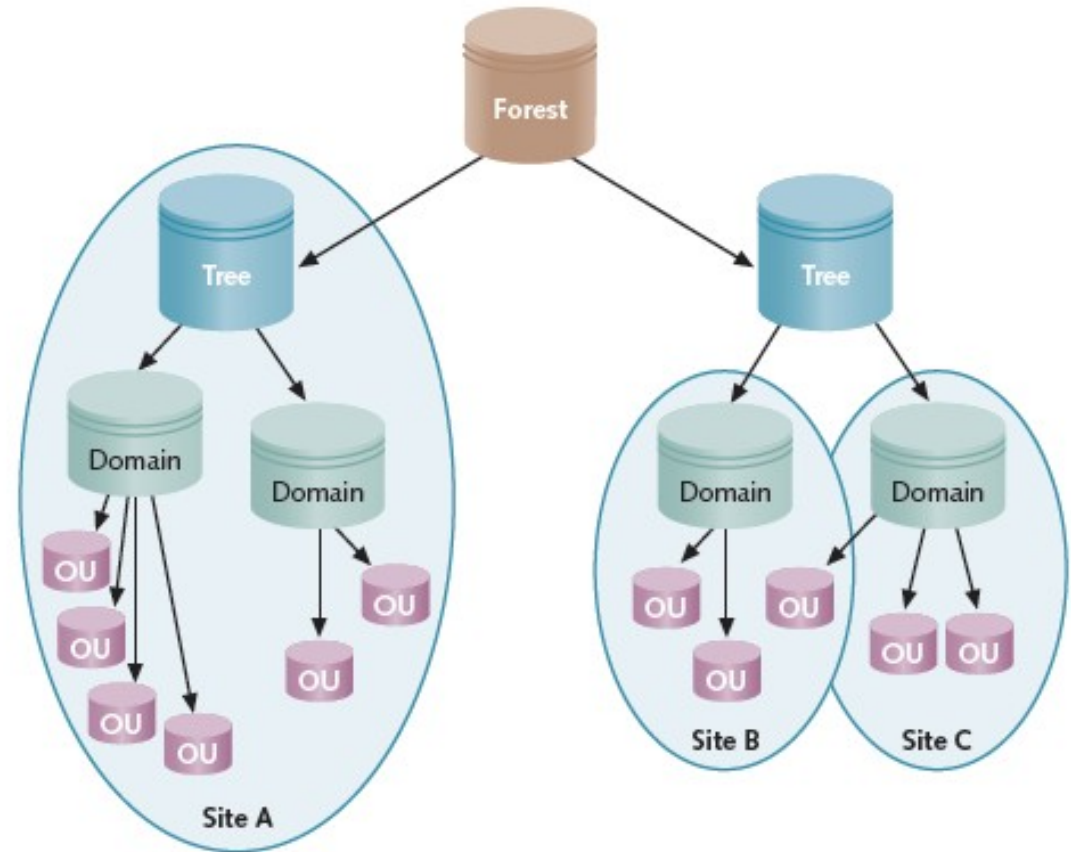
Tree

Contains one or more domains that are in a common relationship

Domains in a tree typically have a hierarchical structure

Kerberos transitive trust relationship

Two-way trusts between parent domains and child domains



Tree

Transitive trust

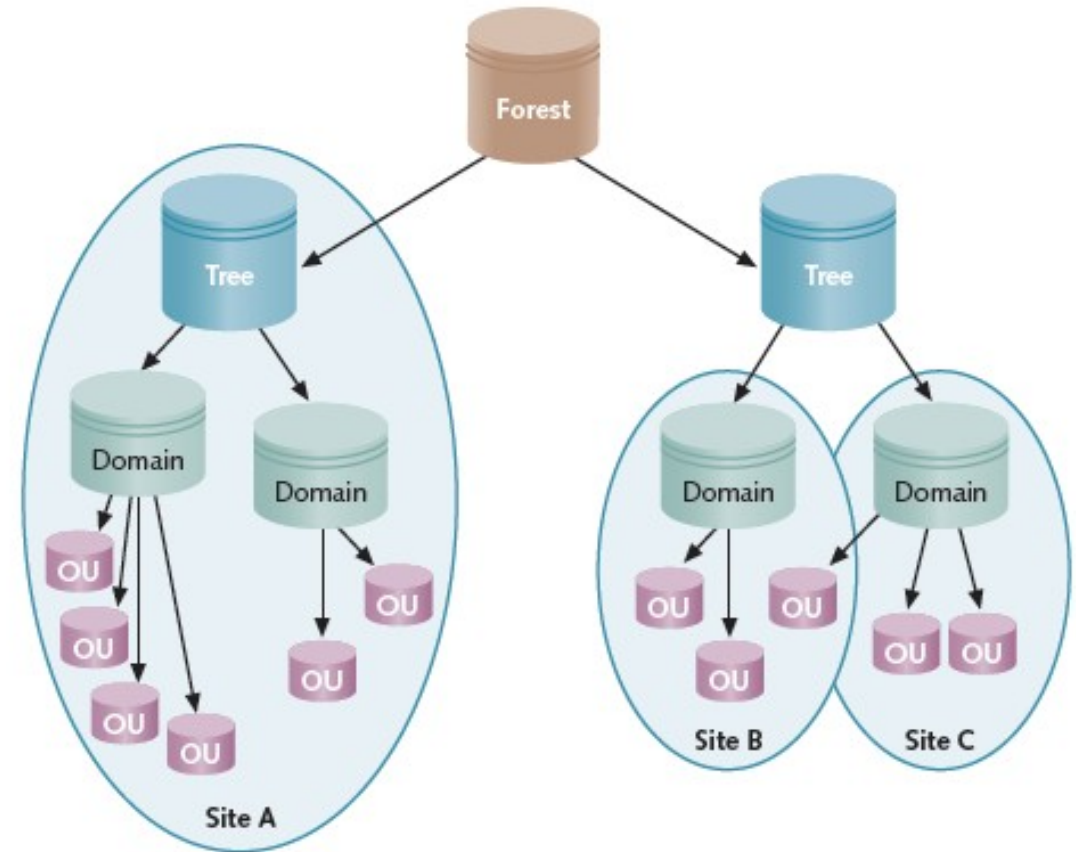
If A and B have a trust and B and C have a trust, A and C automatically have a trust as well

Trusted domain

Granted access to resources

Trusting domain

One granting access to another domain

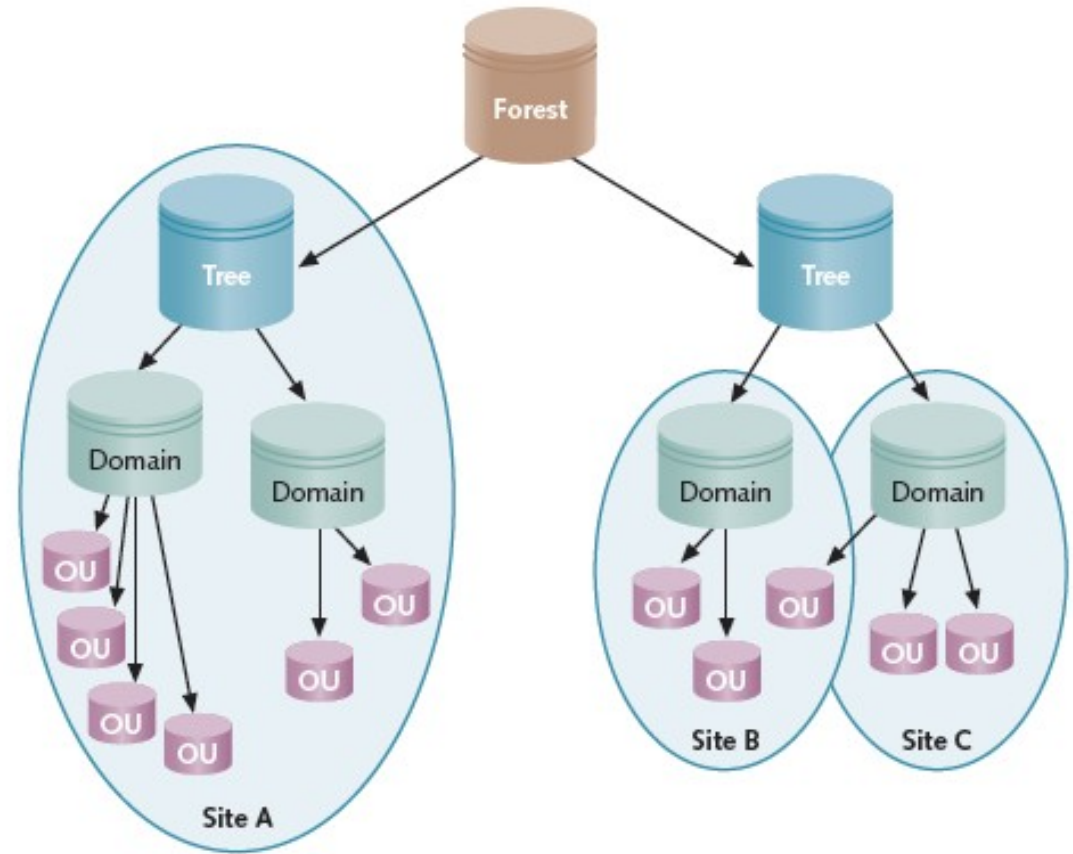


Tree

All domains within a single tree share the same schema

Defines all the object types that can be stored within Active Directory

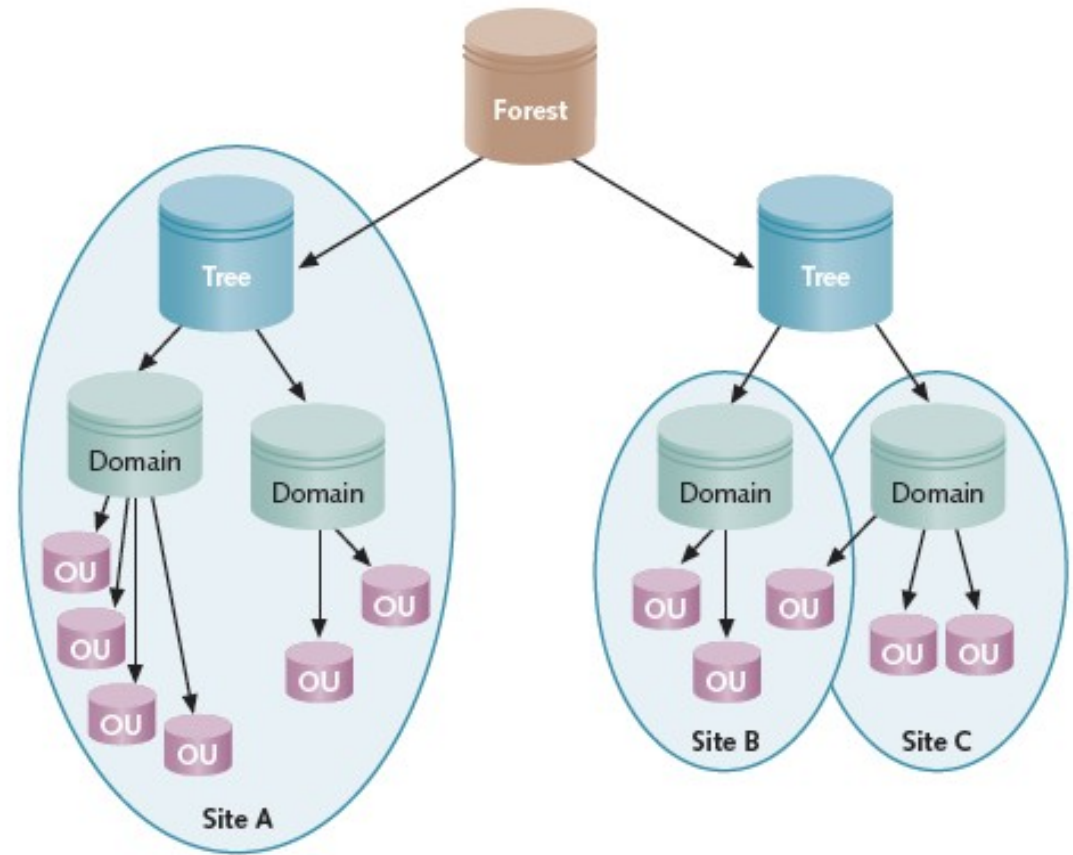
All domains in a tree share same global catalog and a portion of their namespace



Domain

Logical partition within an Active Directory forest

Primary container within Active Directory



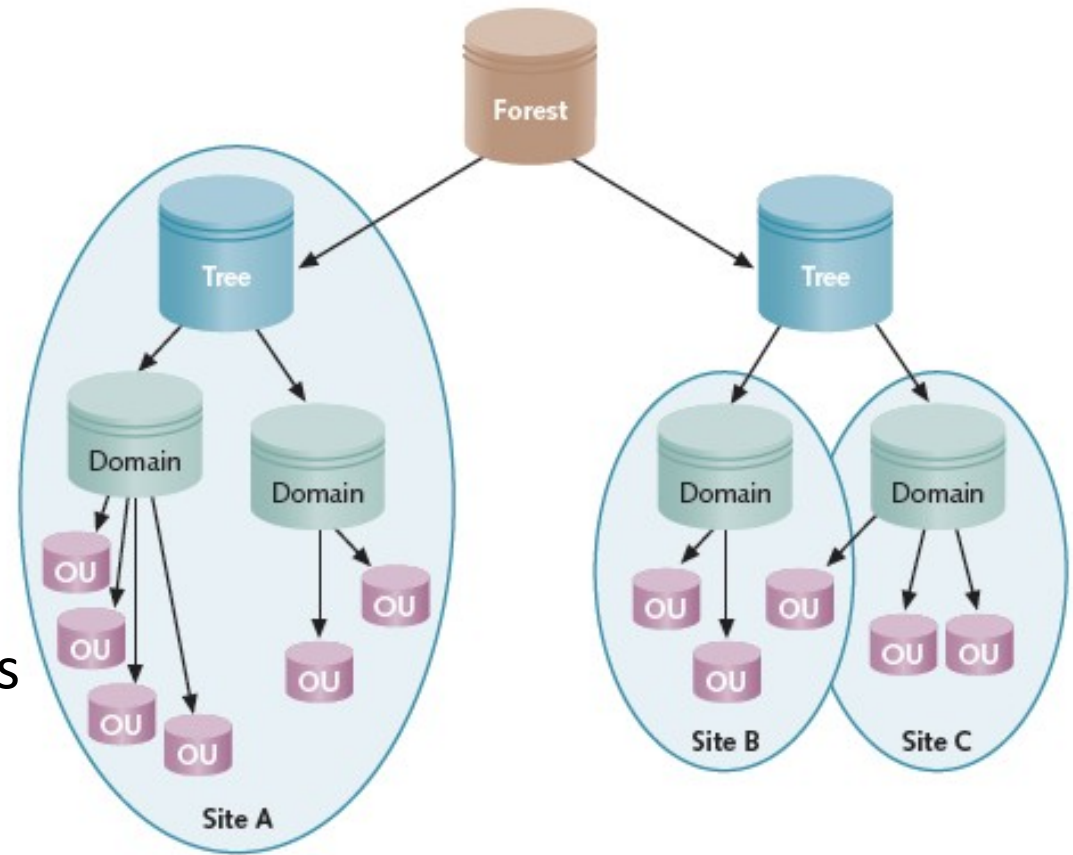
Domain

Basic functions

To provide an AD partition to house objects

To establish a set of information to be replicated

To expedite management of a set of objects



Domain

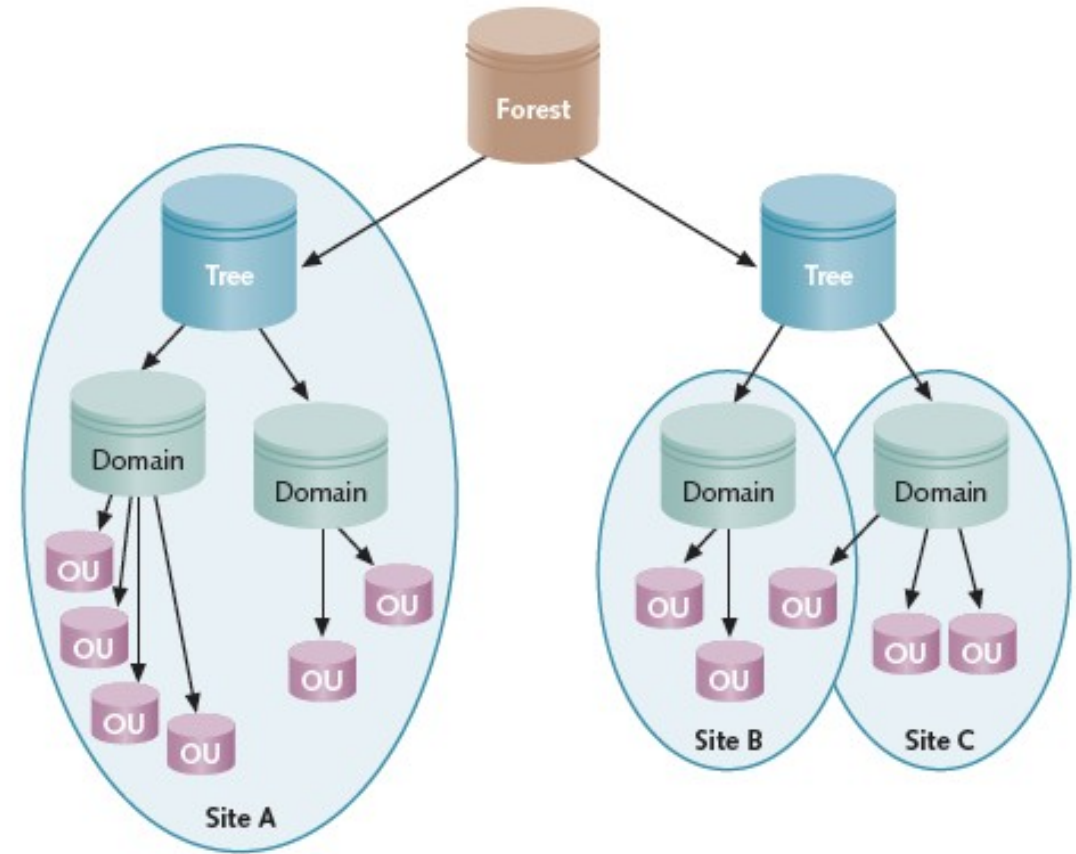
Domain functional levels:

Windows 2000 domain

Windows Server 2003 domain

Windows Server 2008 domain

Windows Server 2012 domain

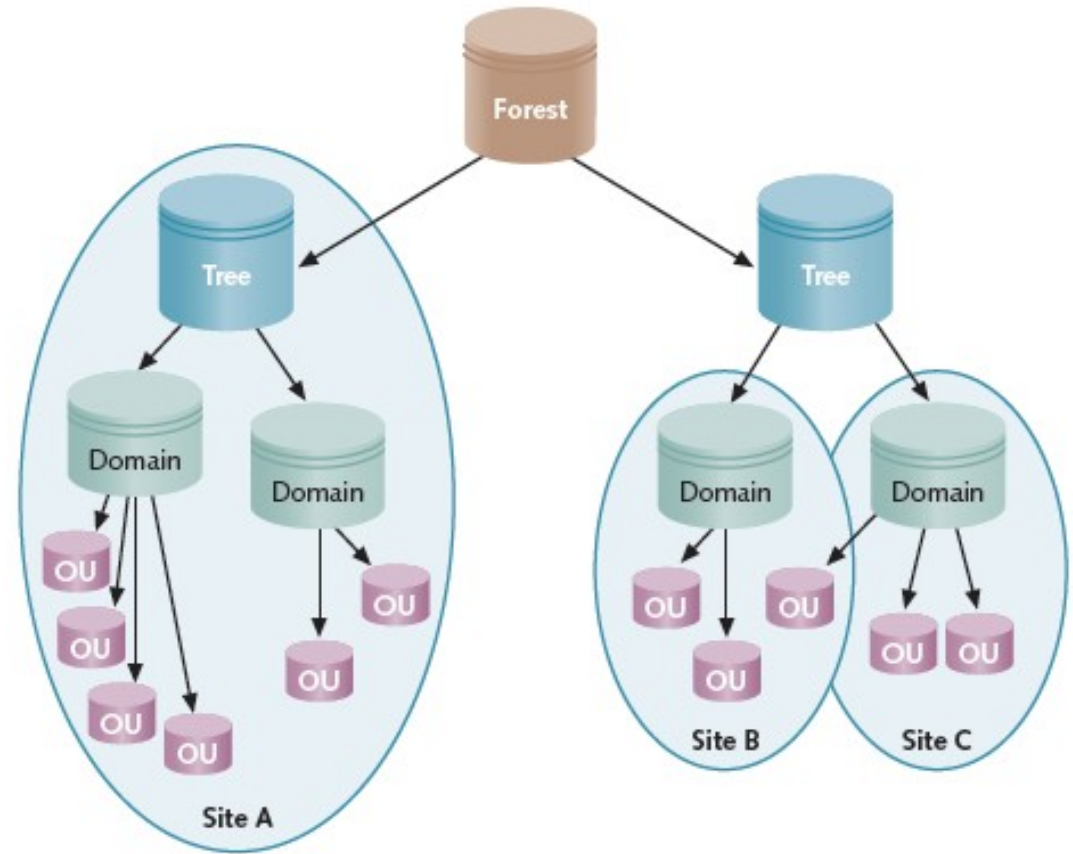


Organizational Unit

Grouping of related objects within a domain

Allow the grouping of objects so that they can be administered using the same group policies

Such as security and desktop setup



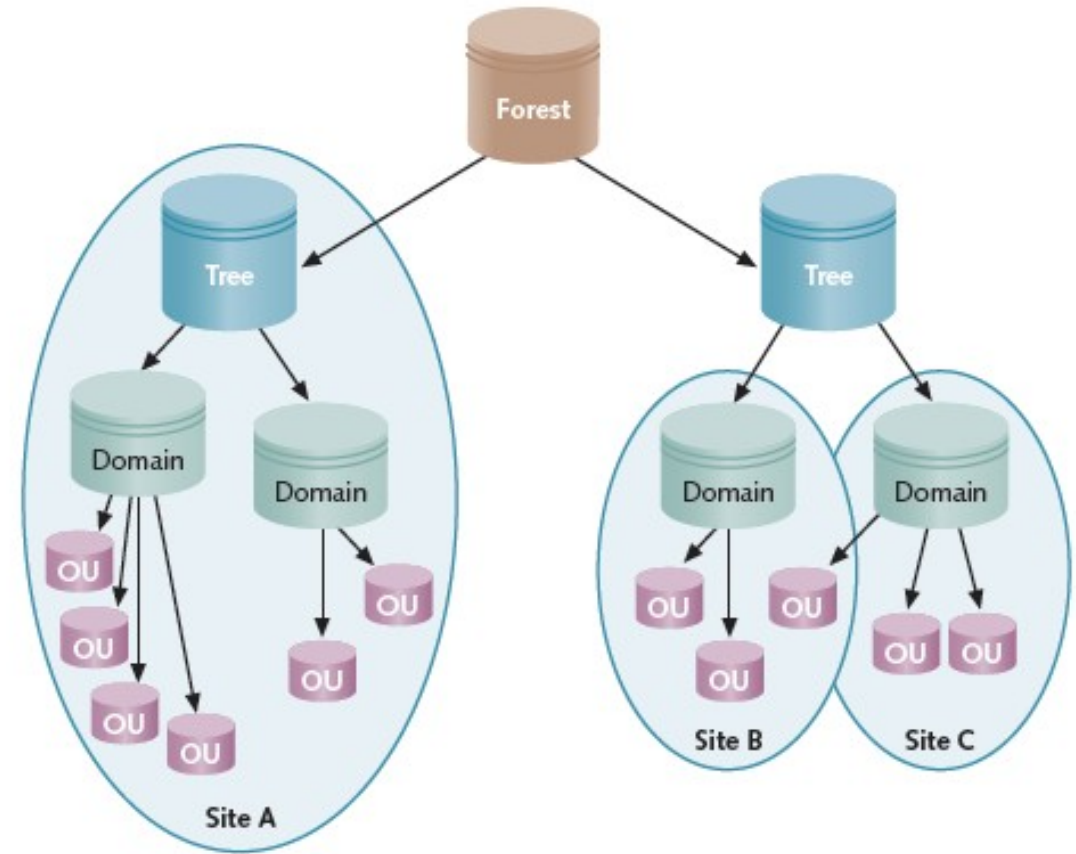
Organizational Unit

Can be nested within other OUs

Best practices when creating OUs

Keep to 10 or fewer

Set up horizontally for best efficiency

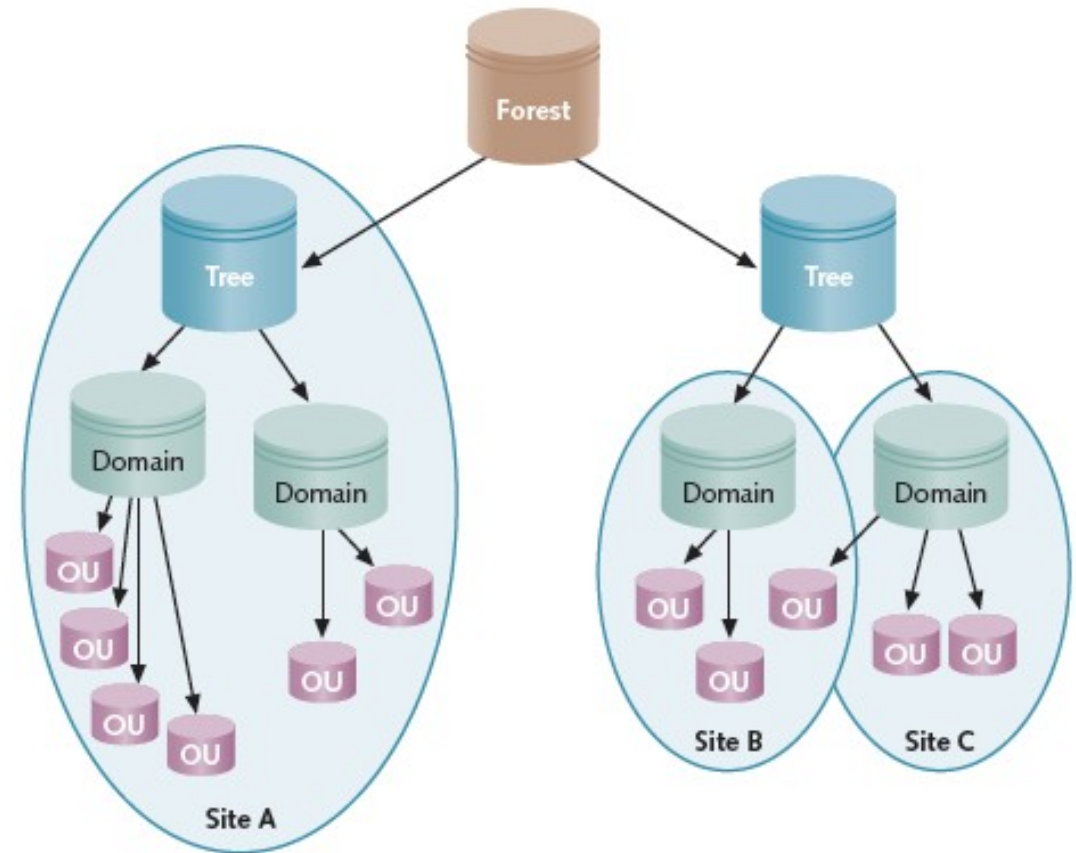


Site

TCP/IP-based concept (container)
within Active Directory

Linked to IP address

Based on connectivity and replication
functions

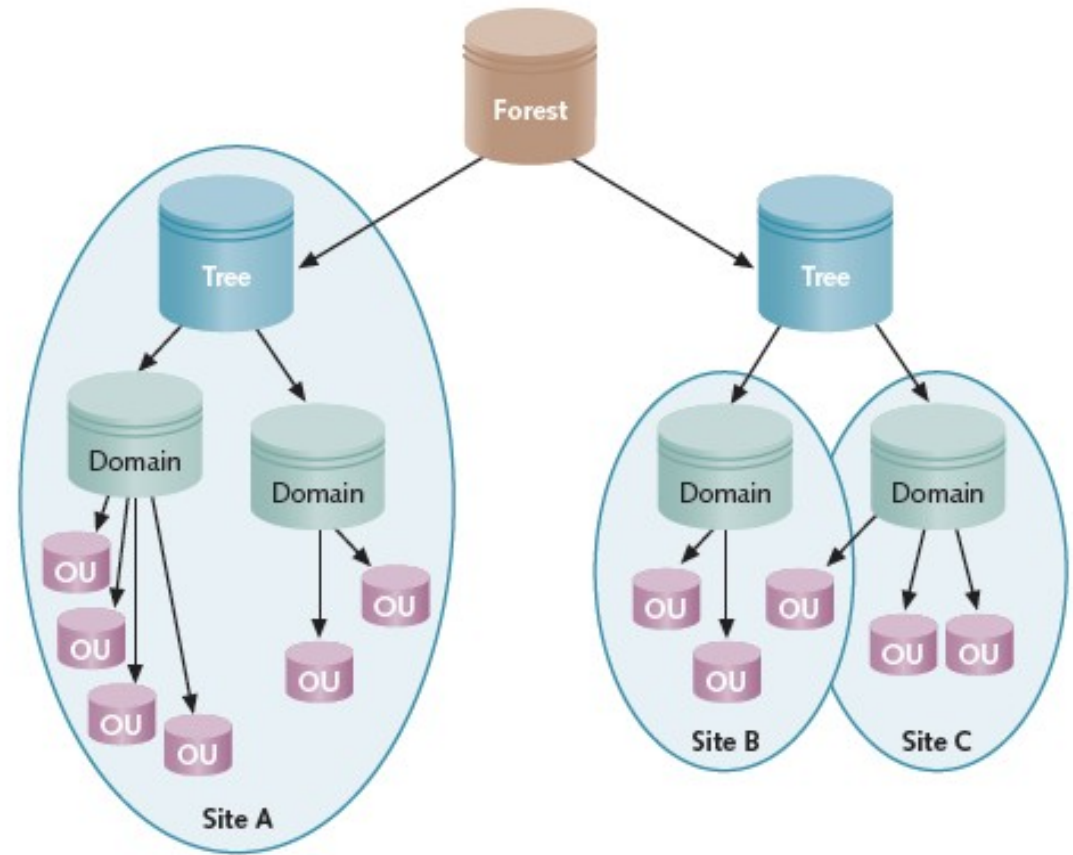


Site

Bridgehead server

DC designated to have role of exchanging replication information

One per site



Active Directory Guidelines

Keep Active Directory as simple as possible

Implement the smallest number of domains possible

Use OUs to reflect organization's structure



Active Directory Guidelines

Use domains as partitions in forests to demarcate commonly associated accounts and resources governed by group and security policies

Implement multiple trees and forests only as necessary

Use sites in situations where there are multiple IP subnets and multiple geographic locations



Planning Functional Levels and Trusts

Carefully plan trusts between forests

External trust - Creates a trust relationship with a domain that is outside of a forest

Realm trust - Enables one- or two-way access between a Windows Server domain within a forest and a realm of UNIX/Linux computers

Shortcut trust - Enable a domain in one forest to quickly access resources in a domain within a different forest



Creating Accounts with AD DS

Use Active Directory Users and Computers tool

From the Administrative Tools menu (next week, we'll use PowerShell)

Create each new account by entering account information and password controls



Creating Accounts with AD DS

Creating a user account

New Object - User

Create in: jpcomp.com/Users

First name: Jason Initials: B

Last name: RyanTest

Full name: Jason B. RyanTest

User logon name: JRTest @jpcomp.com


User logon name (pre-Windows 2000): JPCOMP\ JRTest

< Back Next > Cancel

Creating Accounts with AD DS

SMartin Properties

Member Of | Dialin | Environment | Sessions
Remote control | Terminal Services Profile | COM+
General | Address | Account | Profile | Telephones | Organization

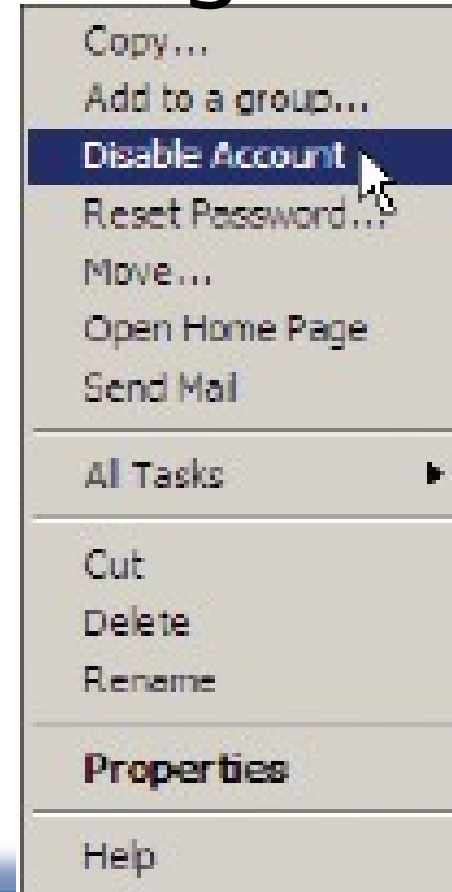
 **SMartin**

First name: Initials:
Last name:
Display name:
Description:
Office:
Telephone number:
E-mail:
Web page:

Disabling, Enabling, and Renaming Accounts

Why disable an account?

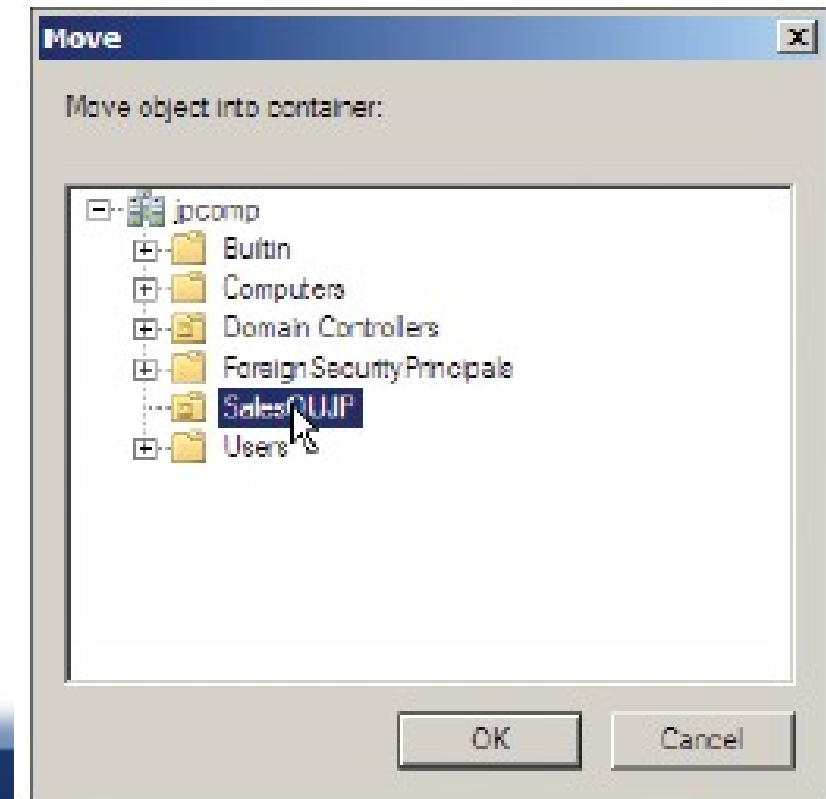
Disabling, Renaming, and Enabling an Account



Moving an Account

May need to move a person's account from one container to another

Moving an Account



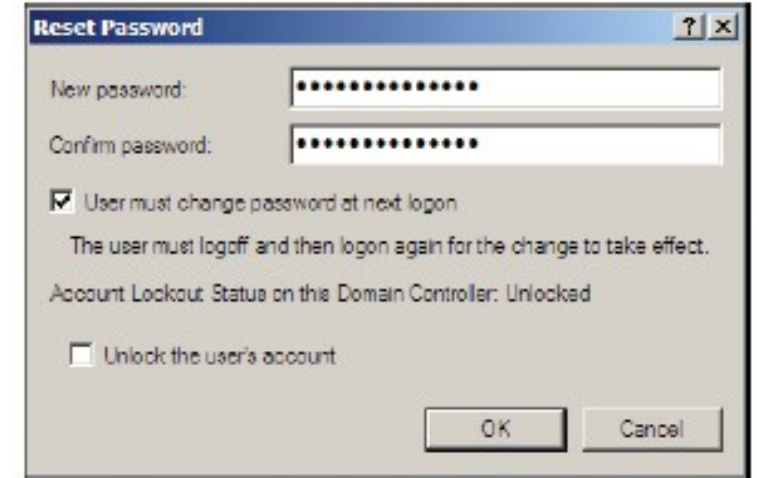
Resetting a Password

Cannot look up forgotten passwords

Reset instead

Maintain guidelines for resetting passwords

Changing an Account's Password



Deleting an Account

Delete accounts that are no longer in use

Globally unique identifier (GUID) is also deleted

Will not be reused even if you create another account using the same name



Implementing User Profiles

Local user profile

Automatically created at the local computer when you log on with an account for the first time

Roaming profile

Downloaded to client workstation each time user account is logged on

Mandatory user profile

Certain users cannot change their profiles



Server 2012 Active Directory Features

Restart capability

Read-Only Domain Controller (RODC)

Auditing

Multiple password and account lockout policies in a single domain

Active Directory Lightweight Directory Services role



Restart Capability

Stop Active Directory Domain Services without taking down the computer

Used to auto defrag database

Old way – reboot into restore mode and perform maintenance task

New Way – stop and start the Active Directory Service



Read-Only Domain Controller

Cannot use to update information in Active Directory

Does not replicate to regular DCs

Can function as a Key Distribution Center for the Kerberos authentication method

Provides better security at branch locations

Can be configured as DNS server



Multiple Password and Account Lockout Policies in a Single Domain

Set up multiple password and account lockout security requirements

Associate them with a security group, user or OU

Can now create more than one set of account policies within a domain



Multiple Password and Account Lockout Policies in a Single Domain

Password settings container (PSC)

- Contains password settings objects (PSOs)

- Represent unique set of password policies

Three policy sets:

- Ordinary users, administrators, service accounts



Taking Active Directory Snapshots

Tools for making snapshots:

ntdsutil.exe Active Directory database management tool

Active Directory Database Mounting Tool or dsamain.exe tool

Enable Active Directory snapshots to be taken for later viewing

Compare to what is in the Active Directory after it is restored

Determine which of several restores has the most complete Active Directory data



Questions?



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer

Copyrights



Presentation prepared by and copyright of John Ramsey,
East Tennessee State University, Department of
Computing . (ramseyjw@etsu.edu)



- Microsoft, Windows, Excel, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.
- IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, System z9, z10, z9, iSeries, pSeries, xSeries, zSeries, eServer, z/VM, z/OS, i5/OS, S/390, OS/390, OS/400, AS/400, S/390 Parallel Enterprise Server, PowerVM, Power Architecture, POWER6+, POWER6, POWER5+, POWER5, POWER, OpenPower, PowerPC, BatchPipes, BladeCenter, System Storage, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, Parallel Sysplex, MVS/ESA, AIX, Intelligent Miner, WebSphere, Netfinity, Tivoli and Informix are trademarks or registered trademarks of IBM Corporation.
- Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.
- Oracle is a registered trademark of Oracle Corporation.
- HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.
- Java is a registered trademark of Sun Microsystems, Inc.
- JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.
- SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.
- Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects S.A. in the United States and in other countries. Business Objects is an SAP company.
- ERPsims is a registered copyright of ERPsims Labs, HEC Montreal.
- Other products mentioned in this presentation are trademarks of their respective owners.



East Tennessee State University
Department of Computing
Jack Ramsey, Lecturer