NETWORK ADMINISTRATION

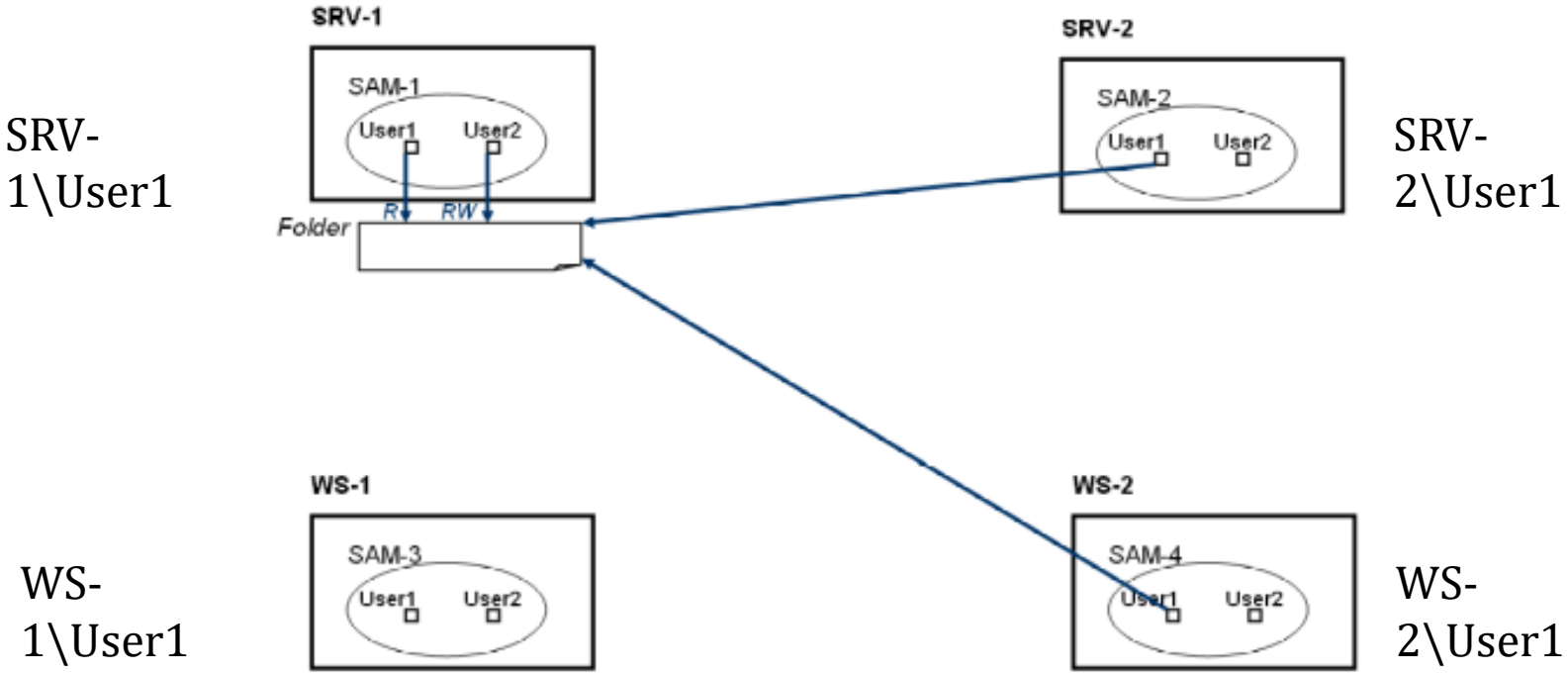
Lecture 3

Logical organization of the computer network. Active directory - concept and architecture.

Assoc. Prof. Rosen Radkov PhD

NETWORK ADMINISTRATION

Workgroup security model

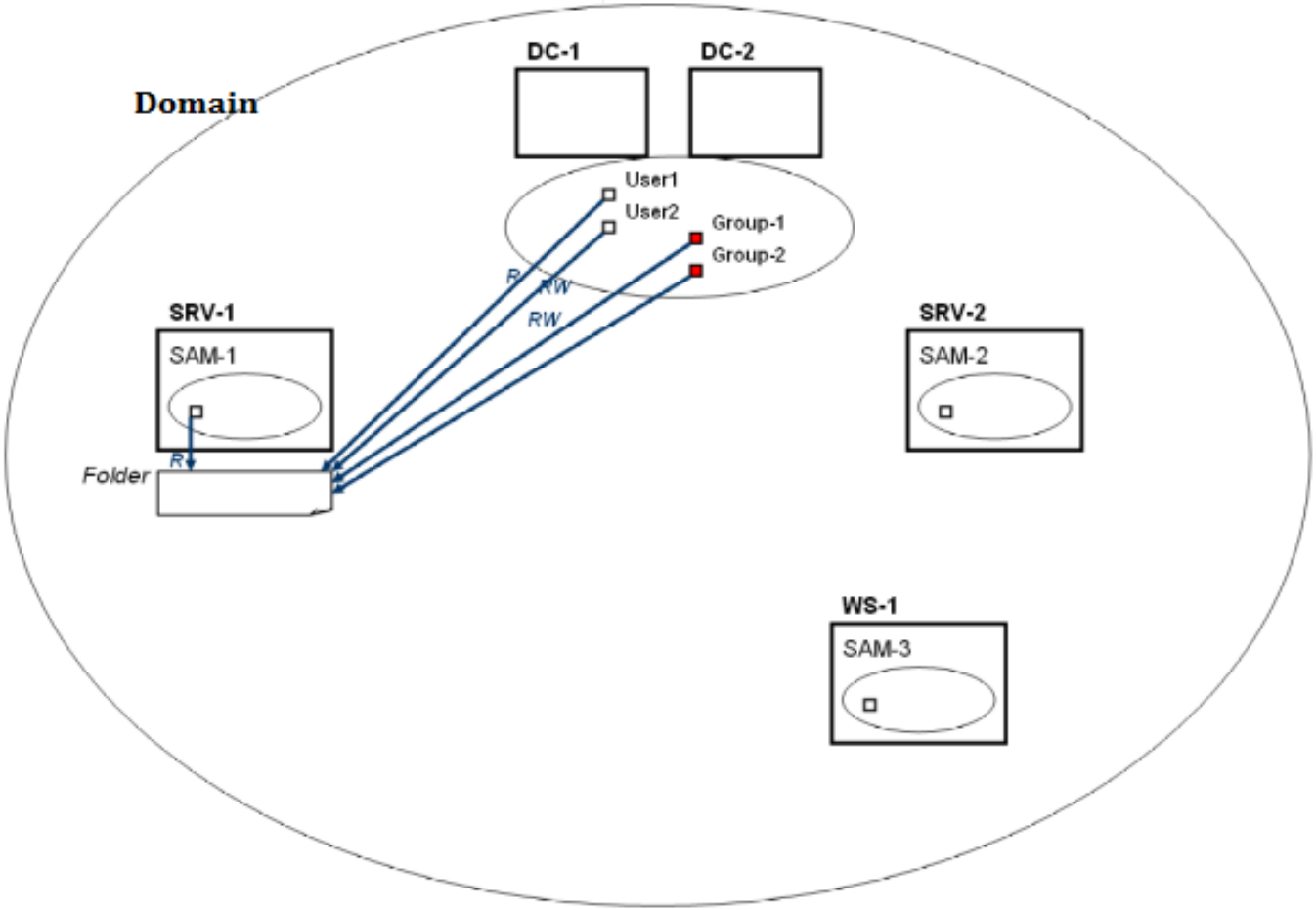


SAM – Security Account Manager

Assoc. Prof. Rosen Radkov PhD

NETWORK ADMINISTRATION

Domain security model



Assoc. Prof. Rosen Radkov PhD

NETWORK ADMINISTRATION

What is the „Active Directory“?

The Active Directory (AD) is a specialized and centralized hierarchical database developed by Microsoft based on X.500 and LDAP, which contains information about objects (users, user groups, computers, etc.) in a corporate network. It describes the logical structure of this network, which is a reflection of the structure of the organization. It is a key component in shaping the boundaries of security in the organization.

Assoc. Prof. Rosen Radkov PhD

Characteristics of the „Active Directory“

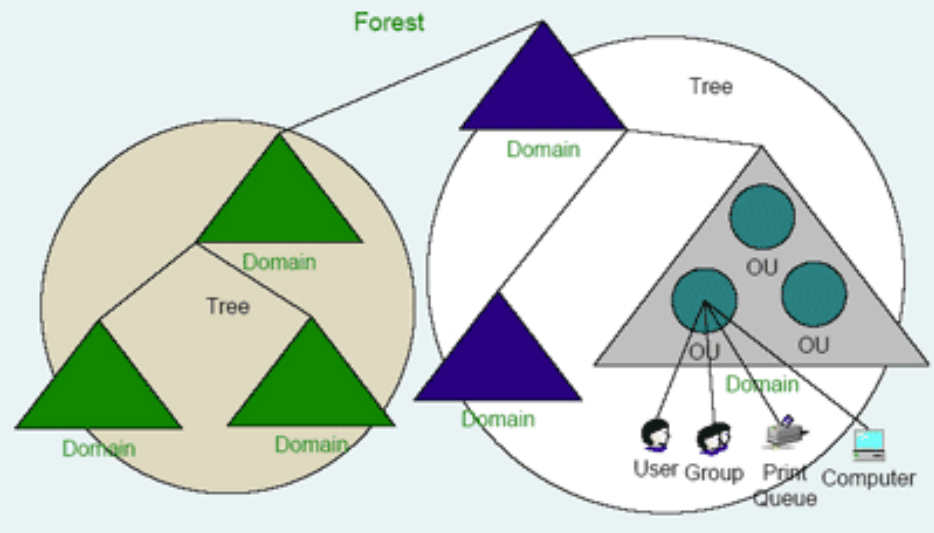
- Single registration - through one name the user gets access to all the resources he needs
- Information security - secure authentication mechanisms (Kerberos) and resource access management are used
- Centralized management - administrators can manage all resources
- Administration using group policies

Characteristics of the „Active Directory“

- Integration with DNS – AD is dependent on the system supporting the names of the domains
- Replication of the information in the database - it is mandatory to maintain the database in more than one place. This ensures fault tolerance and load distribution
- Flexibility of queries to the directory - the search can be done on any attribute of the object
- Standard programming interfaces - API

NETWORK ADMINISTRATION

Structure of the "Active Directory"



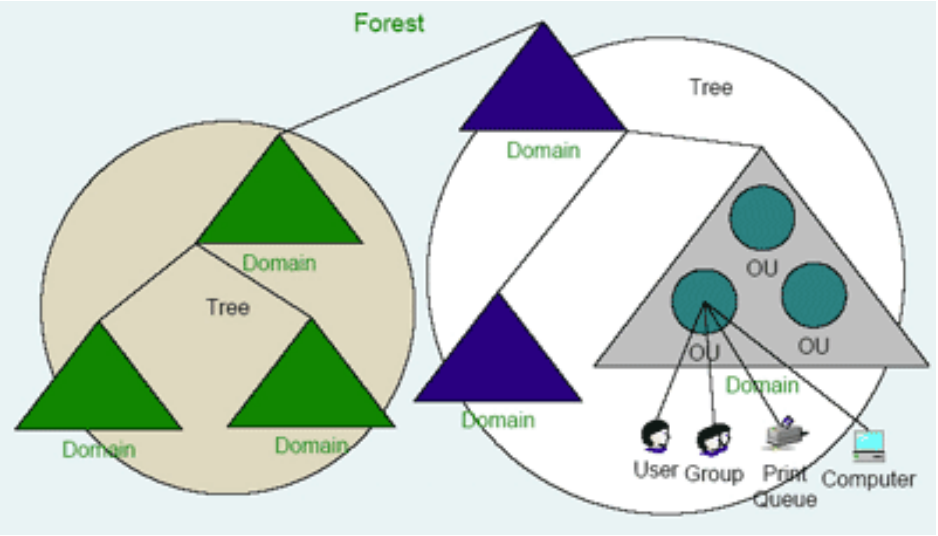
- **Domain** – basic unit that maintains a DB with object names and provides management of: authentication, access control, services, security policies and replication

- **Organizational unit (OU) -** a pseudo-container in the domain that combines objects in order to delegate administrative rights and group policies

Assoc. Prof. Rosen Radkov PhD

NETWORK ADMINISTRATION

Structure of the "Active Directory"

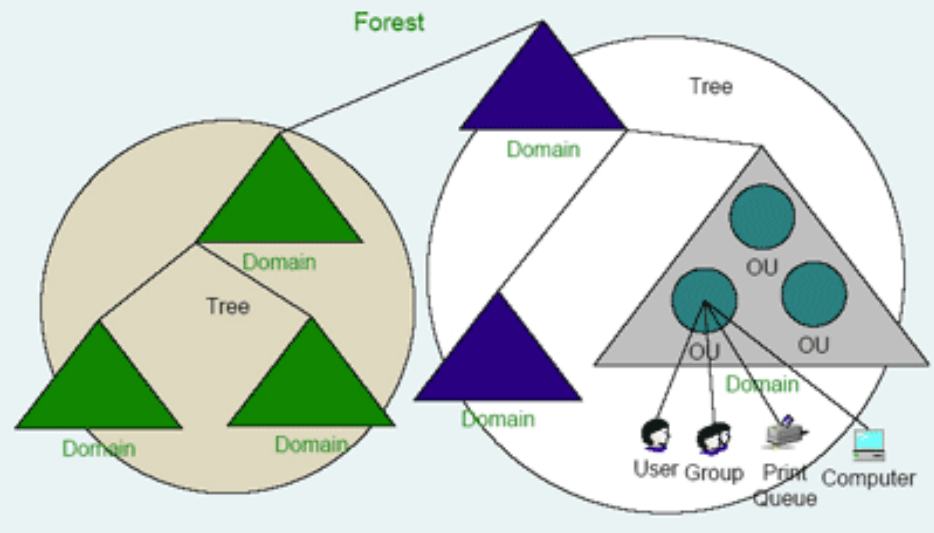


The OU does not allow the assignment of rights and privileges to the objects that are in the given OU. For this purpose it is necessary for these objects to be members of a group.

For convenience, by the use of a suitable script, groups, with the name of the OU, can be created - called *Shadow groups*

- **Object –** user, group, computer

Structure of the "Active Directory"

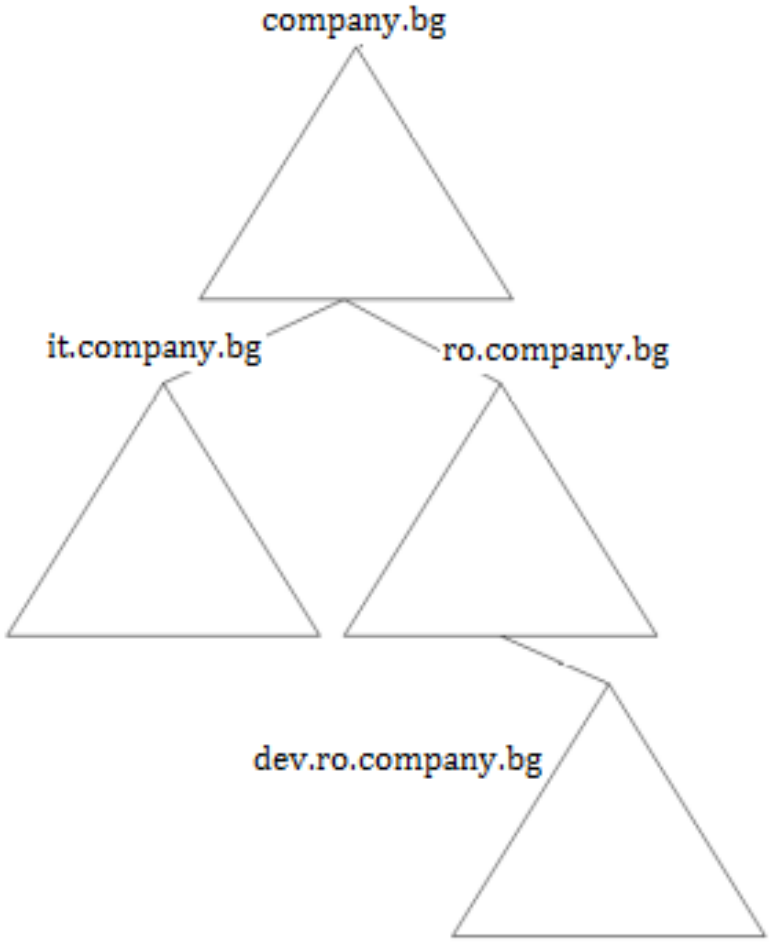


- **Tree** – a set of domains that use a single namespace. Child domains inherit the domain name from the parent.

Child domains establish a trust relationship with the parent, which means that the resources of one domain can be available to users of the other domain.

NETWORK ADMINISTRATION

Structure of the “Active Directory”



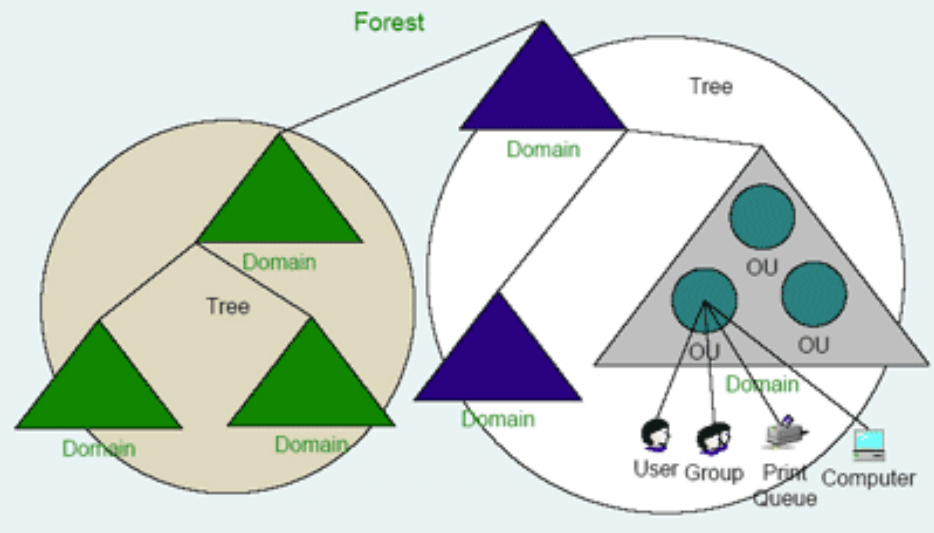
Assoc. Prof. Rosen Radkov PhD

Structure of the "Active Directory"

It is recommended to use only one domain. A tree consisting of many domains is built when it is necessary to achieve:

- Management decentralization
- An increase in productivity
- Effective replication management
- An implementation of different policies
- With a large volume of objects in AD

Structure of the "Active Directory"



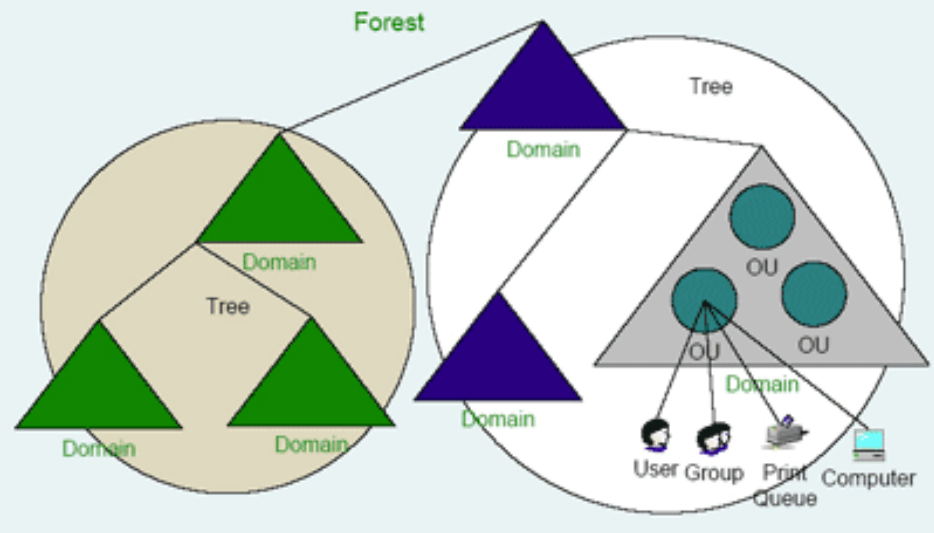
- **Forest** – combines trees that support a single schema (a schema is a set of specific types or classes of objects in AD).

In a forest, bilateral trusts is established between all domains.

Important:

- By default, the first tree created in the forest is considered its ***root (the root tree)***

Structure of the "Active Directory"

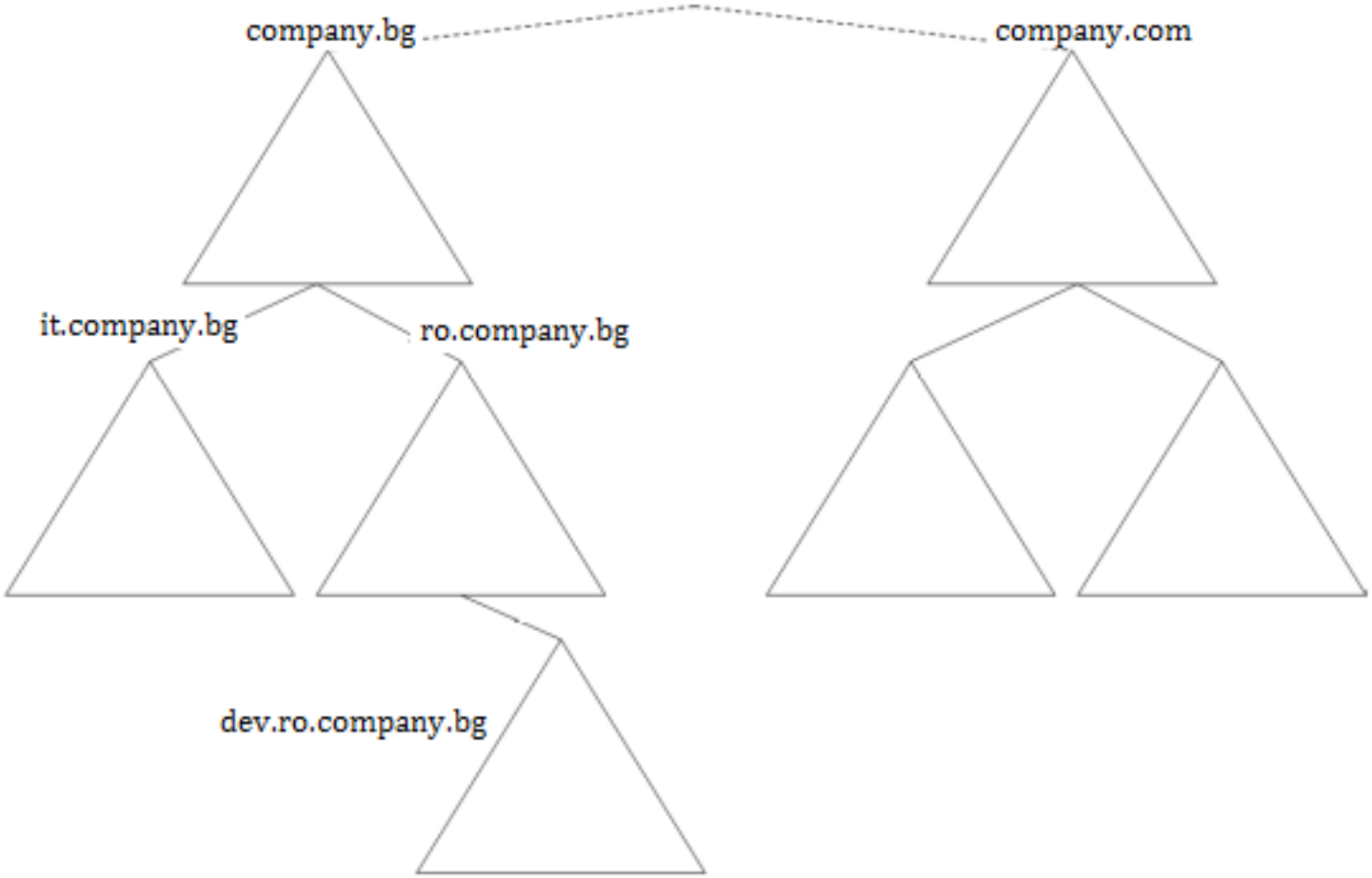


- the first domain created in the tree is considered a ***tree root domain***

- the first domain created in the forest of domains is called the ***forest root domain*** and it stores the AD schema. *This domain cannot be deleted.*

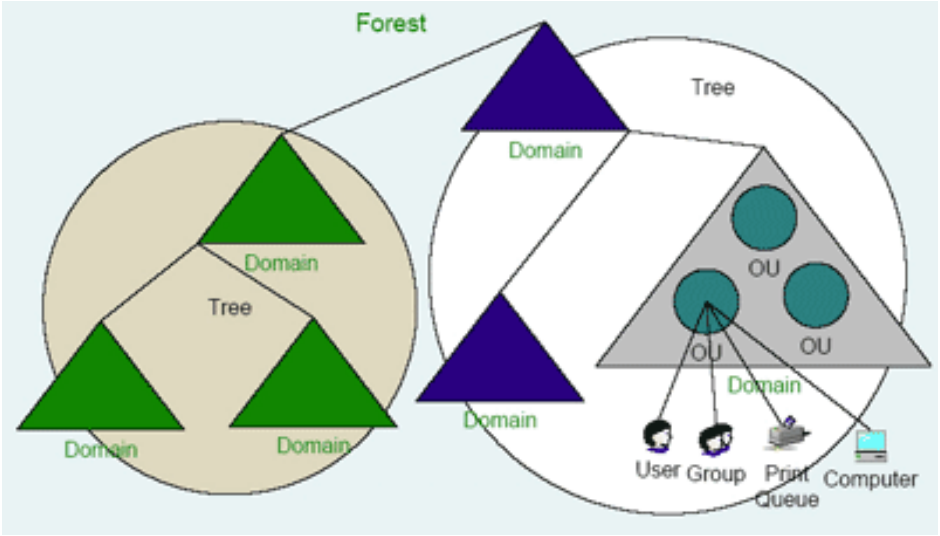
NETWORK ADMINISTRATION

Structure of the “Active Directory”



Assoc. Prof. Rosen Radkov PhD

Structure of the "Active Directory"



- **Global catalogue (GC)** - is a very important part of AD because it is used to search in the forest. GC is a catalog of all objects in a forest that contain a subset of attributes for each object.

The GC can be accessed via LDAP via port 3268 or LDAP / SSL via port 3269. The global catalog is read-only and cannot be updated directly.

Naming objects in the AD

- Each object has a unique 128-bit identifier (GUID - Globally Unique IDentifier), through which it can be uniquely identified. It is assigned to the object by the AD at the time of its creation. The ID is retained even when the object is moved to another domain.

- Distinguished name (DN) – these are the hierarchical paths in the AD, through which each object is uniquely identified

Naming objects in the AD

Example: If we have a user named *Sales*, a member of the users group *Users* in the domain company.bg, then the DN name will be written as follows:

dc=bg, dc=company, cn=Users, cn=Sales

- Relative DN (RDN) – a name by which the object is identified within its "parent" container. For the above example, the user's RDN is:

dc=Sales

Naming objects in the AD

The RDN must be unique for the container in which it is created.

- The AD uses the following types of attributes (a part of the attributes defined in RFC2253):

- CN – common name
- L – locality name
- O – organization name
- OU – organizational unit name
- C – country name
- DC – domain component

Structure of the AD scheme

The AD schema is based on LDAP, which in turn uses X.500, and consists of two types of AD objects: classes (classSchema) and attributes (attributeSchema).

To create a new object type in the AD you need:

- To create a classSchema object in the schema , that defines the class of the object and its attributes;
- To create an object in the AD that uses this class. For unique identification of objects in the schema, OIDs defined by X.500 are used:

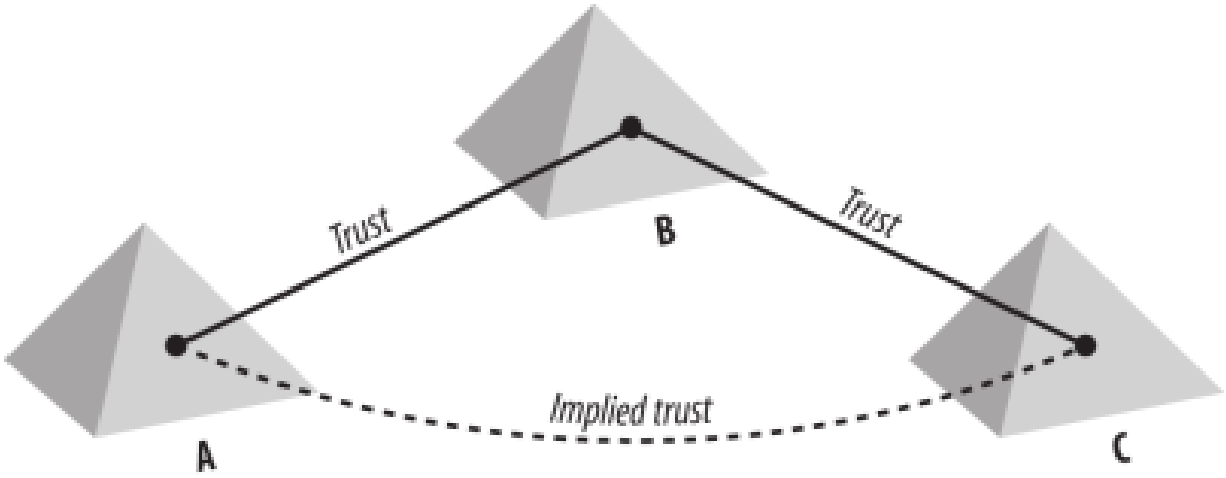
1.3.6.1.4.1.3385.12.497

Trust relationships in the AD

- One-way trust
- Two-way trust
- Trusting domain
- Trusted domain
- Transitive trust
- Intransitive trust
- Explicit trust
- Cross-link trust

Trust relationships in the AD

- Transitive trusts



Implied trust – tacit trust

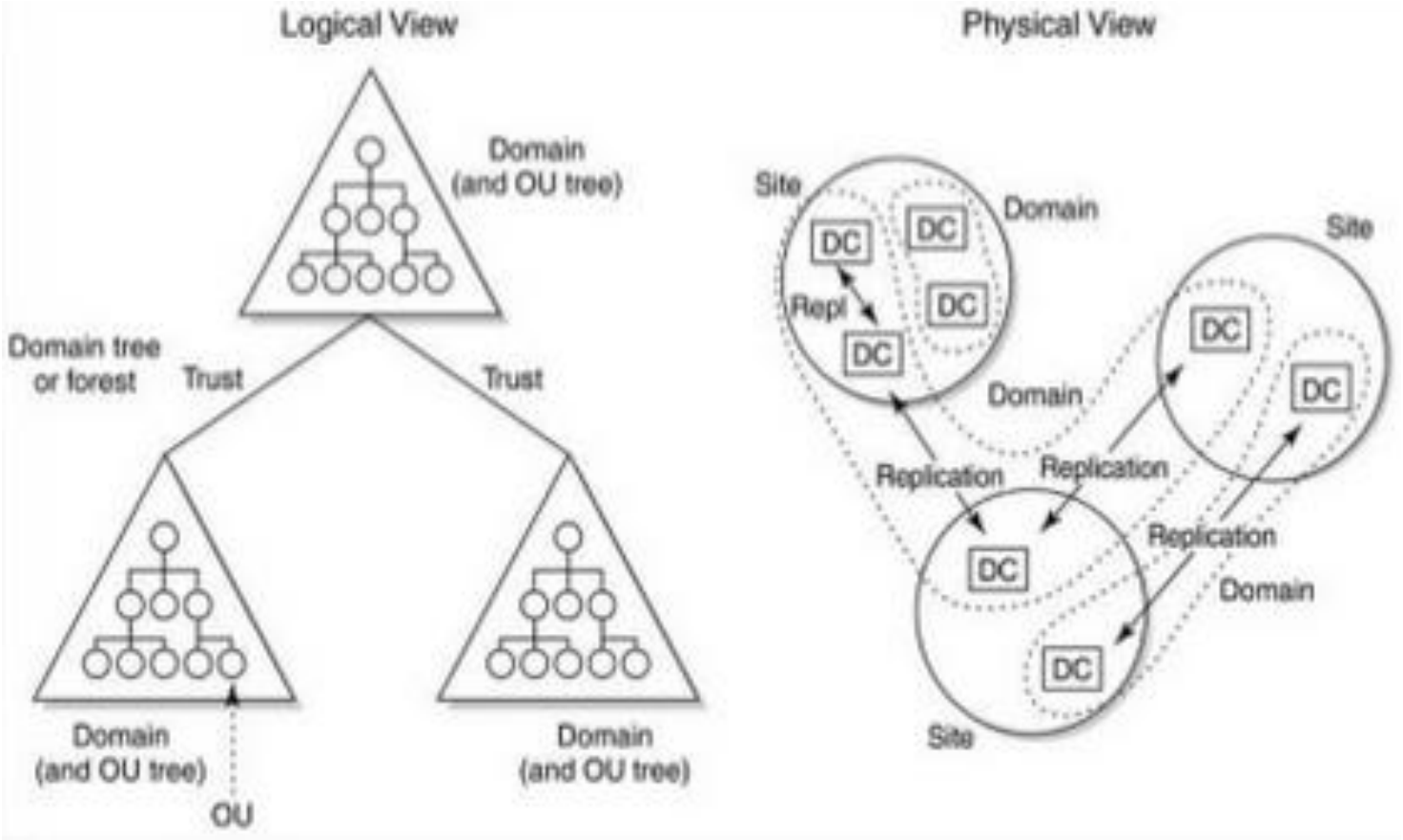
Physical structure of the "Active Directory"

- Domain controller (DC) – a server that stores the database of a specific domain from the AD, manages the synchronization of information about the objects in the domain, and provides user authentication. It is recommended for each of the domains to have at least two DCs responsible for it.

- Sites – a group of IP networks interconnected with fast (≥128kbps) and reliable communications. Their purpose is to manage the processes of data replication in DC and user authentication.

NETWORK ADMINISTRATION

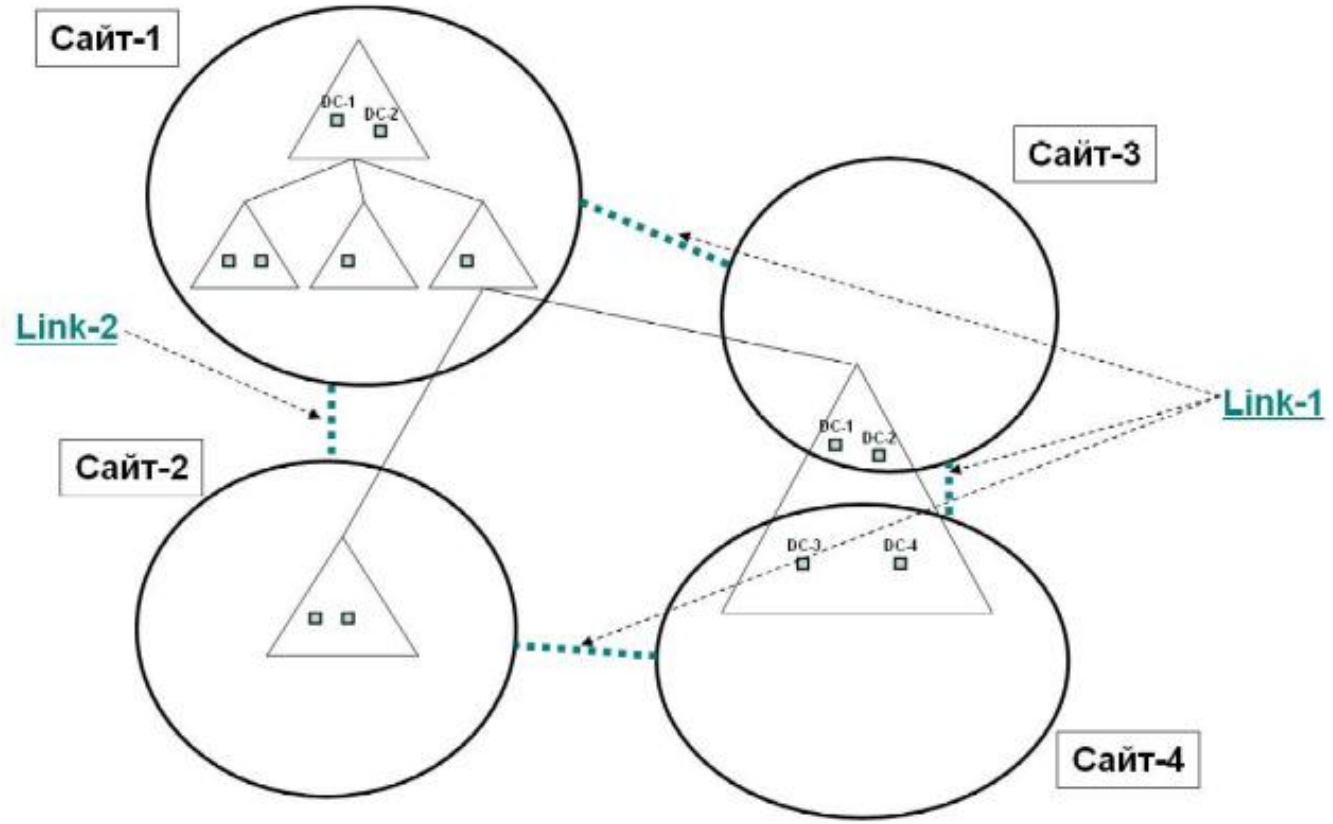
Physical structure of the “Active Directory”



Assoc. Prof. Rosen Radkov PhD

NETWORK ADMINISTRATION

Physical structure of the “Active Directory”



The structure of the sites does not depend on the structure of the domains

Assoc. Prof. Rosen Radkov PhD

Role of domain controllers

- Flexible Single Master Operator (FSMO) Roles (fizz-mo) – specialized roles that run only on specific servers to avoid conflicts

- 2 roles apply to the whole forest (forest-wide FSMOs
- 4 roles apply to the whole domain (domain-wide FSMOs)

Schema master (forest-wide) – role that entitles the AD schema to be modified (1 forest server)

Role of domain controllers

Domain naming master (forest-wide) - a role that gives the right to change the names (for example, to rename or move a domain, as well as to add or delete a domain) in the whole forest (1 server for the forest).

PDC emulator (domain-wide) – for the purposes of AD backward compatibility with a Windows NT domain. This server acts as a ***master browser*** for Windows NT and also acts as a PDC for low-level clients. The PDC emulator has other important features, such as maintaining the latest password for each user profile.

Role of domain controllers

The PDC emulator can also act as a time server, as well as a server that has a role in managing Group Policy (1 server for each domain).

Relative IDentifier master (RID master - domain-wide) – a role that ensures that all *security identifiers* (SID) in the domain are unique. It supports a large set of unique RID values that are allocated to domain controllers at the time of their creation (1 server for each domain).

Role of domain controllers

Infrastructure master (domain-wide) - used to maintain links to objects in other areas known as ***phantoms***. If three domain B users are members of a group in domain A, the Infrastructure master of domain A is used to maintain connections to B domain users, which are phantoms. These phantoms are not controllable or even visible by ordinary means. The links contain GUID, SID and DN (1 server for each domain / partition).

Partitions in the AD

Due to the distributed nature of Active Directory, it is necessary to separate the data into partitions so that not all data in the forest is replicated. It is often useful to group data based on geographic or policy requirements. Only domain controllers that are authoritative for a domain need to replicate all information within that domain. On the other hand, there is some Active Directory data that needs to be replicated to all domain controllers in the forest. There are three predefined partitions (naming context) within the Active Directory:

Partitions in the AD

- **Domain naming context** for every domain– contains all objects created in the domain - user names, user groups, computers, etc. This information is replicated only in the DCs responsible for this domain. A subset of objects are replicated in DC, which are a global catalog.

- **Configuration naming context** for the forest – contains information about the physical structure of the forest - sites and topology. This information is replicated in all DCs in the forest.

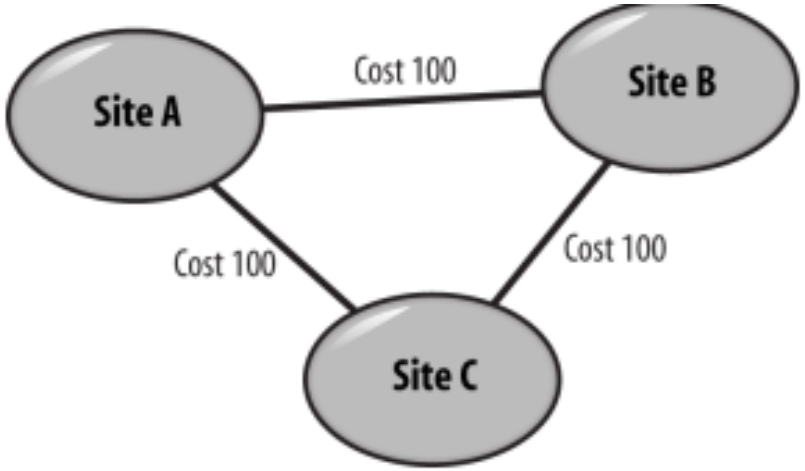
Partitions in the AD

- **Schema naming context** for the forest – contains the defined set of object classes and their attributes for the data types stored in the AD forest. This information is replicated in all DCs in the forest.

- Application partitions - may contain arbitrary data except security data

NETWORK ADMINISTRATION

DB replication in the AD



- AD replication is based on the links between the sites.
- RPC (IP) and SMTP protocols are used.

- SMTP is used in cases where the connection between the sites is poor and unreliable.
- Replication is done automatically every 5 minutes. The topology of the replications is built automatically and managed by the *Knowledge Consistency Checker.*

DB replication in the AD

With a large number of DCs, KCC constructs a circular topology, making several circuits for reliability.

- Replication between sites is done with the same protocols but requires careful setup.

Action	Naming context	Originating domain controller	Domain controller	USN
Initial USN value	Domain NC	N/A	DC A	1000
Initial USN value	Domain NC	N/A	DC B	2500
Create 5 new users (originating update)	Domain NC	DC A	DC A	1005
Receive 5 new users (replicated update)	Domain NC	DC A	DC B	2505
Modify user description attribute (originating update)	Domain NC	DC B	DC B	2506
Receive modified user description attribute (replicated update)	Domain NC	DC B	DC A	1006

DB replication in the AD

- High-watermark vector (HWMV) - table, supported independently of any domain controller, which aids efficient replication. The domain controller uses it to determine where the last interruption was when it replicates the naming context with a specific replication partner.

Naming context	Replication partner	High-watermark vector (USN of last update received)
Domain NC	DC B invocation ID	2506
Domain NC	DC C invocation ID	3606

DB replication in the AD

- Up-to-dateness vector (UTDV) – a table that is used to reduce unnecessary replication traffic and replication loops. Each table stores the USN number of the last update that the domain controller received from any other domain controller that ever existed in the forest, as well as the date / time at which the last DC successfully completed the replication cycle with that partner.

Naming context	Replication partner	High-watermark vector (USN of last update)	Up-to-dateness vector
Domain NC	DC B invocation ID	2506	2506
Domain NC	DC C invocation ID	3756	3756

NETWORK ADMINISTRATION

Management consoles in the AD

- Active Directory Domains and Trusts – for domain management, trust and functional levels
- Active Directory Sites and Services – for replication management
- Active Directory Users and Computers – for managing user accounts, groups, computers, etc.
- Active Directory Schema – for scheme changing
- Active Directory Administrative Center – general console

Assoc. Prof. Rosen Radkov PhD

NETWORK ADMINISTRATION

Domain functional level

Domain functional level	Important changes	Supported Domain Controller (OS)
Windows 2000 native	Universal groups Group nesting Transformation of Security Groups to Distribution Groups SIDHistory	Windows 2000 Windows Server 2003 Windows Server 2008 Windows Server 2008R2
Windows Server 2003	Domain Controller rename LastLogonTimeStamp	Windows Server 2003 Windows Server 2008 Windows Server 2008R2 Windows Server 2012 Windows Server 2012R2
Windows Server 2008	Fine-grained password and account lockout policies SYSVOL replication with Distributed File Systems Replication AD integrated DFS Trees in W2008 mode, incl. DFS ABE Last Interactive Logon Information (failed logon attempts etc...)	Windows Server 2008 Windows Server 2008R2 Windows Server 2012 Windows Server 2012R2
Windows Server 2008R2	Active Directory Web Services Windows PowerShell cmdlets for Active Directory Automated SPN update	Windows Server 2008R2 Windows Server 2012 Windows Server 2012R2
Windows Server 2012	CLAIMS support for KDC Kerberos armoring Dynamic Access Control	Windows Server 2012 Windows Server 2012R2
Windows Server 2012 R2	NTLM not supported anymore Authentication Policies	Windows Server 2012R2

Assoc. Prof. Rosen Radkov PhD

NETWORK ADMINISTRATION

Forest functional level

Forest functional level	Important changes	Supported Domain Controller (OS)
Windows 2000 native	All standard Active Directory functions	Windows 2000 Windows Server 2003 Windows Server 2008 Windows Server 2008R2
Windows Server 2003	Forest Trusts Domain rename RODC (read-only-domain-controller) Improved KDC (Knowledge Consistency Checker) Deactivation of attributed in the AD scheme Linked-value Replication – individual changes of a group membership are replicated, instead of the whole group	Windows Server 2003 Windows Server 2008 Windows Server 2008R2 Windows Server 2012 Windows Server 2012R2
Windows Server 2008	No changes compared to Windows Server 2003 Forest operating mode	Windows Server 2008 Windows Server 2008R2 Windows Server 2012 Windows Server 2012R2
Windows Server 2008 R2	Active Directory Recycle Bin	Windows Server 2008R2 Windows Server 2012 Windows Server 2012R2
Windows Server 2012	No changes compared to Windows Server 2008R2 Forest operating mode	Windows Server 2012 Windows Server 2012R2
Windows Server 2012 R2	No changes compared to Windows Server 2008R2 Forest operating mode	Windows Server 2012R2

Assoc. Prof. Rosen Radkov PhD

Integration of the AD with other directories

- Centrify DirectControl (Centrify Corporation) – Active Directory-compatible centralized authentication and access control
- Centrify Express (Centrify Corporation) – A suite of free Active Directory-compliant services for centralized authentication, monitoring, file-sharing and remote access
- Authentication Services (Quest Software)
- PowerBroker Identity Services, formerly Likewise (BeyondTrust, formerly Likewise Software) – Allows a non-Windows client to join Active Directory
- Samba – Can act as a domain controller

NETWORK ADMINISTRATION

Tools

- Adprep
- Dsadd
- Dsget
- Dsmod
- Dsmove
- Dsquery
- Dsrm
- Nsdutil

NETWORK ADMINISTRATION

THANK YOU FOR THE ATTENTION!

Assoc. Prof. Rosen Radkov PhD