IW3 - Active Directory: LDS, Kerberos, WDS

Ing. Jan Pluskal
UIFS
Brno University of Technology, Czech Republic
ipluskal@fit.vutbr.cz

BRNO UNIVERSITY OF TECHNOLOGY

FACULTY OF INFORMATION TECHNOLOGY

Lab 0: Prerequisites

- Použijte w2012-dc, w2012-repl, w2012-dc2, w2012-base, w2012-child
- Konfigurace:
  - Startup RAM 768MB
  - Dynamic RAM
    - Minimal 768MB
    - Maximal 2048MB
  - Síťové adaptéry: not connected, private 1

Active Directory Lightweight Directory Services

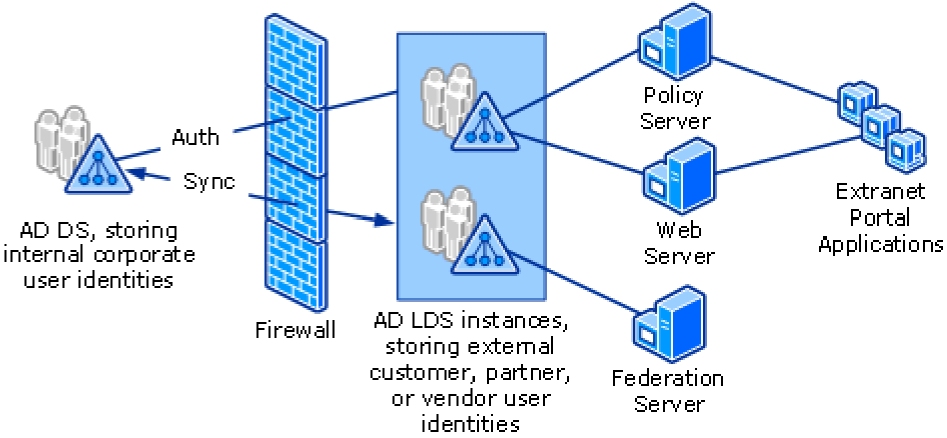
- **Lightweight Directory Access Protocol** (LDAP)
  - directory service that provides flexible support for directory-enabled applications
  - without the restrictions of Active Directory Domain Services (AD DS)
  - formerly known as Active Directory Application Mode (ADAM)
  - provide directory services for directory-enabled applications without incurring the overhead of domains and forests and the requirements of a single schema throughout a forest

Providing an enterprise directory store

- full-fledged LDAP directory solution for enterprises.
- can store “private” directory data, which is relevant only to the application, in a local directory service
- *“private” directory data, which is relevant only to the application, in a local directory service—possibly on the same server as the application—without requiring any additional configuration to the server operating system directory*
- Data relevant only to the application and which does not have to be widely replicated, is stored solely in the AD LDS directory that is associated with the application
- **reduces replication traffic** on the network between domain controllers

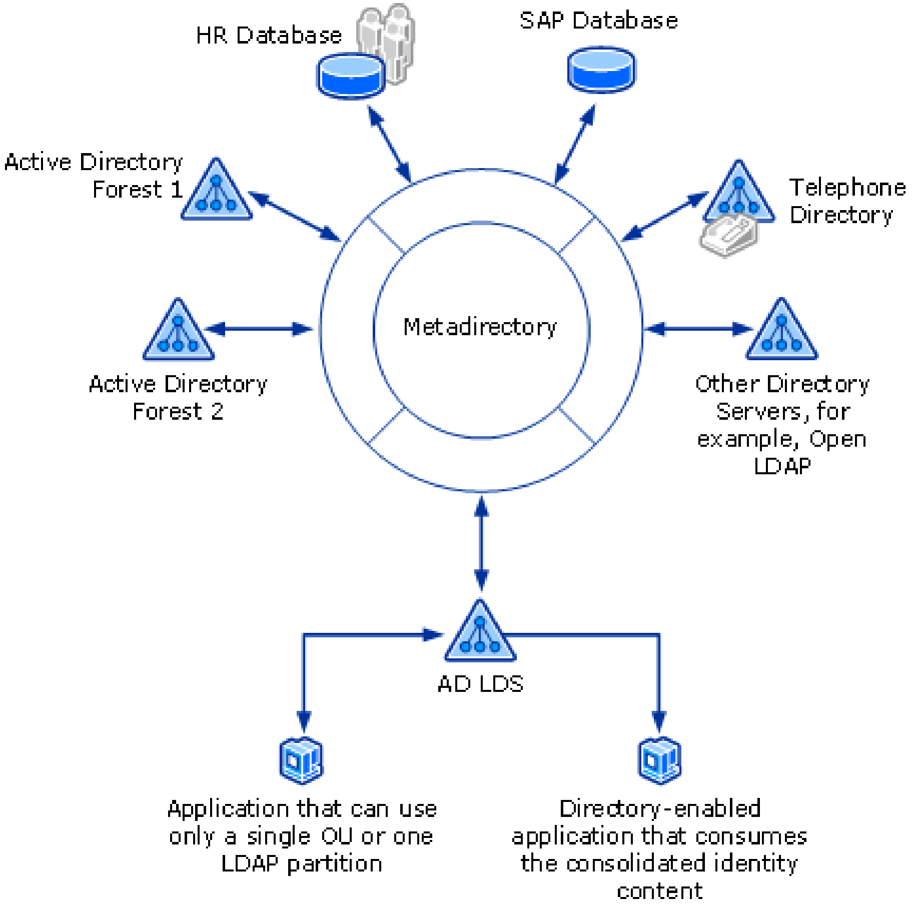
Providing an extranet authentication store

- Example: a Web portal application that manages extranet access to corporate business applications and services identities that are external to the corporate AD DS.
- If a portal application that you deploy in an extranet must service internal AD DS-authenticated identities that are currently located outside the corporate firewall, you can still deploy AD LDS as the authentication store with the corporate account credentials of these identities provisioned on the extranet instances of AD LDS, as shown in the following illustration.


Auth
Sync
AD DS, storing internal corporate user identities
Firewall
AD LDS instances, storing external customer, partner, or vendor user identities
Policy Server
Web Server
Federation Server
Extranet Portal Applications

Consolidating identity systems

You may have a scenario in which a **data model restriction**, such as a single LDAP partition view or a single organizational unit (OU) view, is imposed on an enterprise directory-enabled application that must access data that is associated with **AD DS-authenticated users, applications, or network resources** that are located in **multiple forests, domains, or OUs in the enterprise**. Identity information for this directory-enabled application **must be consolidated** from multiple Active Directory forests, domains, and OUs or from multiple identity systems and other directories, such as human resource databases, SAP databases, telephone directories, and so on.


HR Database
SAP Database
Active Directory Forest 1
Telephone Directory
Metadirectory
Active Directory Forest 2
Other Directory Servers, for example, Open LDAP
AD LDS
Application that can use only a single OU or one LDAP partition
Directory-enabled application that consumes the consolidated identity content

Features in the AD LDS server role

- Multiple instances on a single computer.
  - Each instance runs as a separate service in its own execution context.
- AD LDS server role includes the following features to make it easy to create, configure, and manage AD LDS instances:
  - A **wizard** that guides you through the process of creating an AD LDS instance
  - **Command-line tools** for performing *unattended installation* and *removal* of AD LDS instances
  - **Microsoft Management Console** (MMC) snap-ins for configuring and managing AD LDS instances, including the schema for each instance
  - **AD LDS-specific command-line tools** for *managing, populating, and synchronizing* AD LDS instances

LAB 1: Installing AD LDS

- **To install AD LDS on Windows Server 2012**

1. Open **Server Manager Dashboard**, click **Add roles and features**.
2. On the **Before you begin** page, select **Role-based or Feature-based installation** and then select the option **Select a server from the server pool**.
3. Select the server name, and follow the rest of the instructions on the AD LDS installation wizard.

- **To install AD LDS on Windows 8**

1. In Windows 8, AD LDS is listed within **Windows Features**. To install AD LDS, open control panel, click **Programs**, click **Turn Windows features on or off**, select **Active Directory Light Weight Directory Services**
2. Follow the rest of the instructions on the installation wizard.

Understanding AD LDS Instances

- AD LDS **uses** the *same architecture*—and even the same code base—as AD DS
- AD LDS **provides** a *hierarchical data store*, a *directory service component*, and *interfaces* that clients can use to communicate with the directory service.
- AD LDS **does not require** a *domain controller* or a *Domain Name System* (DNS) server.
- In AD LDS, a "*service instance*" (or, simply, "instance") refers to a **single running copy** of the AD LDS directory service.
- *Multiple copies of the AD LDS directory service can run simultaneously on the same computer.*
  - Each instance of the AD LDS directory service has a separate directory data store, a unique service name, and a unique service description that is assigned during installation.

Understanding AD LDS Instances

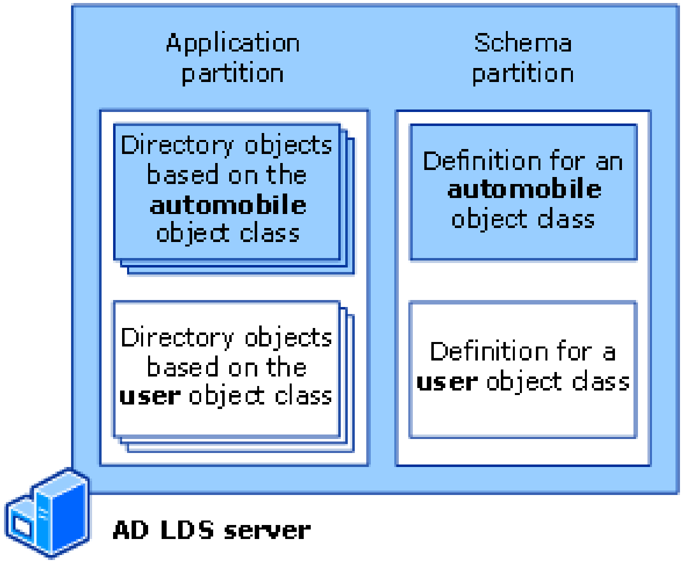
- **Manages** the directory data store, responding to directory requests from directory clients and from other directory services.
- Directory service **runs** in the *security context of the account* that is specified as the AD LDS *service account*.
- Directory service **provides** all the following functions:
  - Authentication of directory users
  - Fulfillment of data requests
  - Data synchronization between directory servers (through multimaster replication)
  - Data management

Understanding the AD LDS Schema

- Schema defines, **using** *object classes* and *attributes*, the types of objects and data that can be created and stored in an AD LDS directory.
- Each AD LDS *configuration set has its own independently manageable schema*, which is stored in the schema directory partition.
- The base (or default) AD LDS schema **contains** only the *classes and attributes that are needed to start* an AD LDS instance.
- The schema **can be extended** with *new classes* and *attributes*, either by *administrators* or by the *applications themselves*.

Understanding the AD LDS Schema

- Unneeded *schema classes* and *attributes* can be **deactivated**
- As with all objects in the directory, *access control lists* (ACLs) **protect** schema objects.
  - Only authorized users can alter the schema.
- Every object in an AD LDS directory is an instance of an object class that is defined in a schema.


Application partition
Schema partition
Directory objects based on the **automobile** object class
Definition for an **automobile** object class
Directory objects based on the **user** object class
Definition for a **user** object class
AD LDS server

Understanding the AD LDS Schema

- **Object classes**
  - Represents a category of objects, such as users, printers, or application programs, that share a set of common characteristics.
  - The definition for each object class contains a list of the attributes that can be used to describe instances of the class.

Attribute	Value
distinguishedName	CN=User,CN=Schema,CN=Configuration
objectClass	top; classSchema;
objectGUID	dac9093a-d2aa-408a-81bb-0fe8179165da;
objectCategory	CN=Class-Schema,CN=Schema,CN=Configuration;

Understanding the AD LDS Schema

- **Attributes**
  - The definition for each attribute includes unique identifiers for the attribute, the syntax for the attribute, optional range limits for the attribute values, whether the attribute can have only one value or multiple values, and whether the attribute is indexed.

Attribute	Value
distinguishedName	CN=Telephone-Number,CN=Schema,CN=Configuration;
objectClass	top; attributeSchema;
objectGUID	dac9093a-d2aa-408a-81bb-0fe8179165da;
objectCategory	CN=Attribute-Schema,CN=Schema,CN=Configuration;

LAB 2: **Create a New AD LDS Instance**

- **To use the Active Directory Lightweight Directory Services Setup Wizard to create a new AD LDS instance**

1. Click **Start** , point to **Administrative Tools** , and then click **Active Directory Lightweight Directory Services Setup Wizard.**
2. On the **Welcome to the Active Directory Lightweight Directory Services Setup Wizard** page, click **Next**.
3. On the **Setup Options** page, click **A unique instance** , and then click **Next**.
4. Finish creating the new instance by following the wizard instructions.

LAB 3: **Start, Stop, or Restart an AD LDS Instance**

- **To start, stop, or restart an AD LDS instance using the graphical user interface**

1. Open Server Manager.
2. In the console tree, double-click **Roles** , and then click **Active Directory Lightweight Directory Services.**
3. In the details pane, in the **System Services** list, click the AD LDS instance that you want to manage.
4. Click **Start** , **Stop** , or **Restart.**

- **To start or stop an AD LDS instance using a command prompt**

1. **net start** *instance_name*
2. **net stop** *instance_name*

LAB 4: **Use ADSI Edit to Manage an AD LDS Instance**

- **To connect and bind to an AD LDS instance using ADSI Edit**

1. Open ADSI Edit. *Administrative Tools/ADSI Edit*
2. In the console tree, click **ADSI Edit** .
3. In **Select or type a domain or server:** (Server | Domain[:port])
4. Under **Connection point** , do one of the following
    1. Click **Select or type a distinguished name (DN) or naming context** , and then specify the distinguished name to which you want to connect.
    2. Click **Select a well-known naming context** , and then click **Configuration** , **RootDSE** , or **Schema.**
5. To connect with an alternative account, click **Advanced** ; click **Specify Credentials** ; and then, under **Connect using these credentials**, type the domain, user name, and password of the account

LAB 5: **Import Data into an AD LDS Instance**

- **To import or export directory objects using ldifde**

1. Open a command prompt as Administrator.
2. Do one of the following:
   - To import directory objects, at the command prompt, type the following command, and then press ENTER:
     - **Ldifde –I –f** *filename* **–s** *servername:port* **–m -a***username domain password*
   - To export directory objects, at the command prompt, type the following command, and then press ENTER:
     - **Ldifde –e –f** *filename* **–s** *servername:port* **–m –a** *username domain password*

- **Ldifde /?**

LAB 6: **Back Up AD LDS Instance Data**

- **To back up an AD LDS instance using Windows Server Backup**

1. Click **Start** , point to **Administrative Tools** , and then click **Backup**
2. On the **Action** menu, click **Backup once**
3. In the Backup Once Wizard, click **Different options** , and then click **Next**
4. Click **Custom** , and then click **Next**
5. Select the volume that contains the AD LDS database and log files
6. Complete the wizard to begin the backup operation

LAB 7: **Use Ldp.exe to Manage an AD LDS Instance**

- **To view the contents of an AD LDS instance using Ldp.exe**

1. Open Ldp - click **Start** , point to **Run** , type **ldp** , and then click **OK**
2. On the **Connection** menu, click **Connect**.
3. In **Server** , type the Domain Name System (DNS) name, NetBIOS name, or IP address of the computer on which the AD LDS instance is running.
4. In **Port** , type the LDAP or Secure Sockets Layer (SSL) communication port number that the AD LDS instance to which you want to connect is using, and then click **OK.**
5. On the **Connection** menu, click **Bind.**
6. When you are finished specifying the bind options, click **OK.**
7. On the **View** menu, click **Tree.**
8. In the **BaseDN** list, click the distinguished name of the object to use as the base object in the navigation pane.
9. **Make some noticeable changes.**

LAB 8: **Restore AD LDS Instance Data**

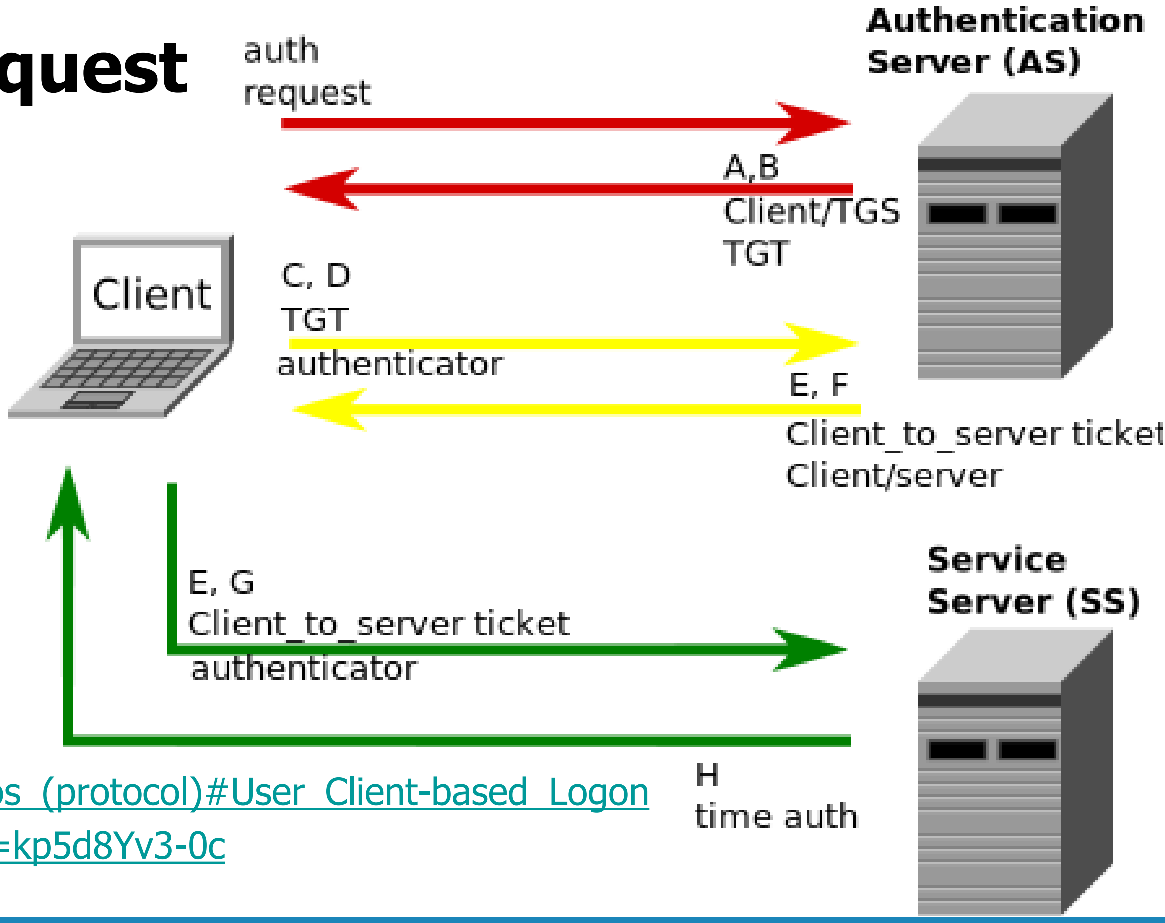
- **Restoring AD LDS data on an existing AD LDS instance that belongs to a configuration set**

1. If it is running, stop the AD LDS instance for which data will be restored
2. Open Backup
3. On the **Action** menu, click **Recover**
4. Follow the steps in the Recovery Wizard to specify the location of the source backup data and to identify the specific backup from which you want to recover instance data
5. In Click **Select recovery type** , click **Files and folders** , and then click **Next**
6. In **Select items to recover** , browse to and select the folder that contains the instance data files. By default, AD LDS database and log files are located in %ProgramFiles%\Microsoft ADAM\ *instancename,* where *instancename* is the AD LDS instance name
7. In **Specify recovery options** , click **Original locations** and **Overwrite existing files with recovered files** , and then click **Next.**
8. To complete the restore, click **Finish.**
9. Open a command prompt
10. At the command prompt, type the following command, and then press ENTER: **dsdbutil**
11. At the **dsdbutil: activate instance** *instancename*
12. At the **dsdbutil: authoritative restore**
13. At the **authoritative restore: [restore database]**

Kerberos: The Network Authentication Protocol

How Does Kerberos Work?

- **User Client-based Logon**
- **Client Authentication**
- **Client Service Authorization**
- **Client Service Request**



- http://en.wikipedia.org/wiki/Kerberos_(protocol)#User_Client-based_Logon
- https://www.youtube.com/watch?v=kp5d8Yv3-0c

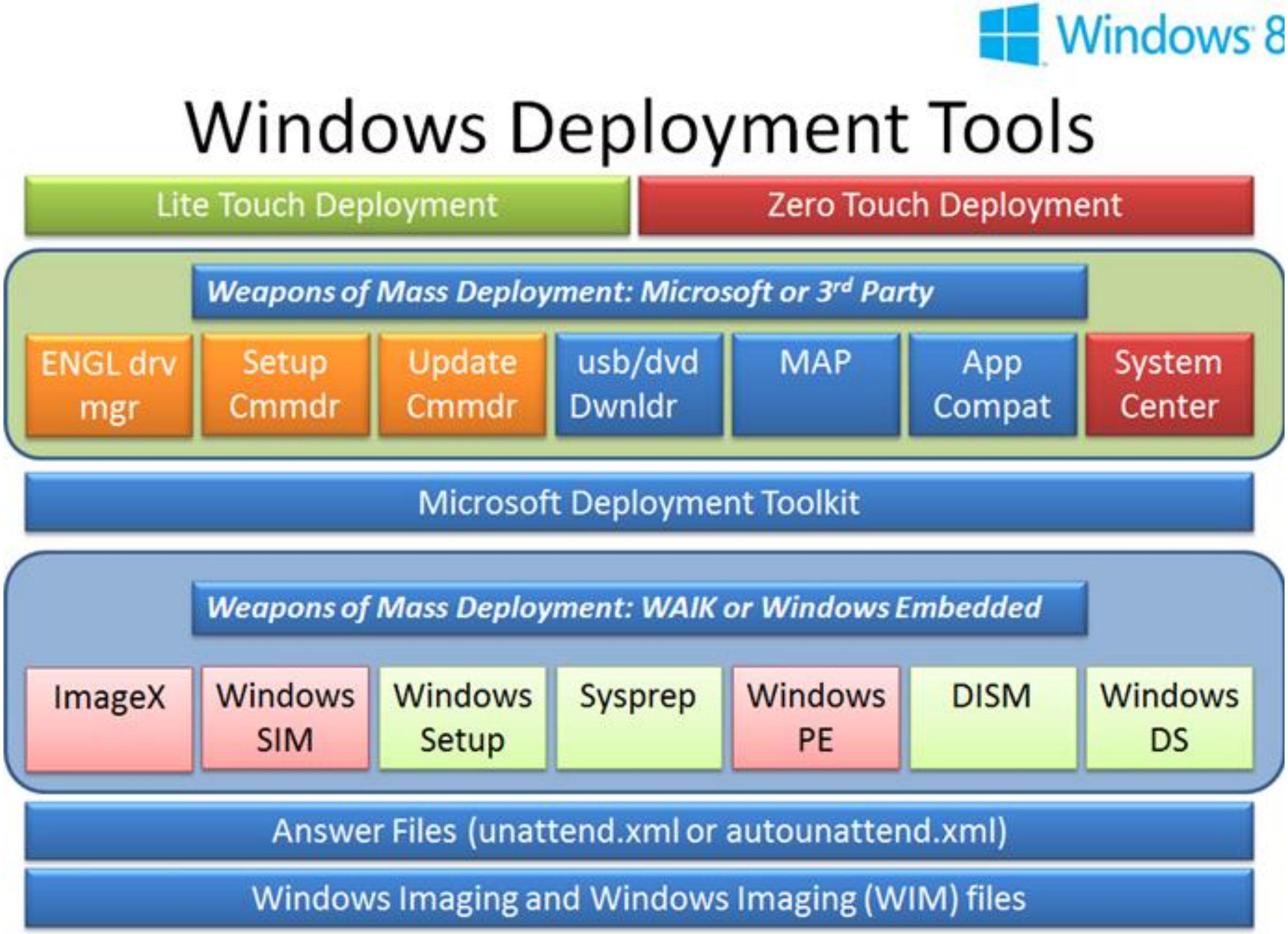
LAB 9: **Kerberos event logging**

- Use W2008R2-DC and W7-Domain:
- **Download and install Wireshark**
- **Enabling Kerberos Event Logging on a Specific Computer**

1. Start Registry Editor – cmd: regedit.exe
2. Add the following registry value: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters
   - Registry Value: LogLevel
   - Value Type: REG_DWORD
   - Value Data: 0x1
   - *If the Parameters subkey does not exist, create it.*
3. Quit Registry Editor. The setting will become effective immediately on Windows Server 2008, on Windows Vista, on Windows Server 2003, and on Windows XP. For Windows 2000, you must restart the computer.

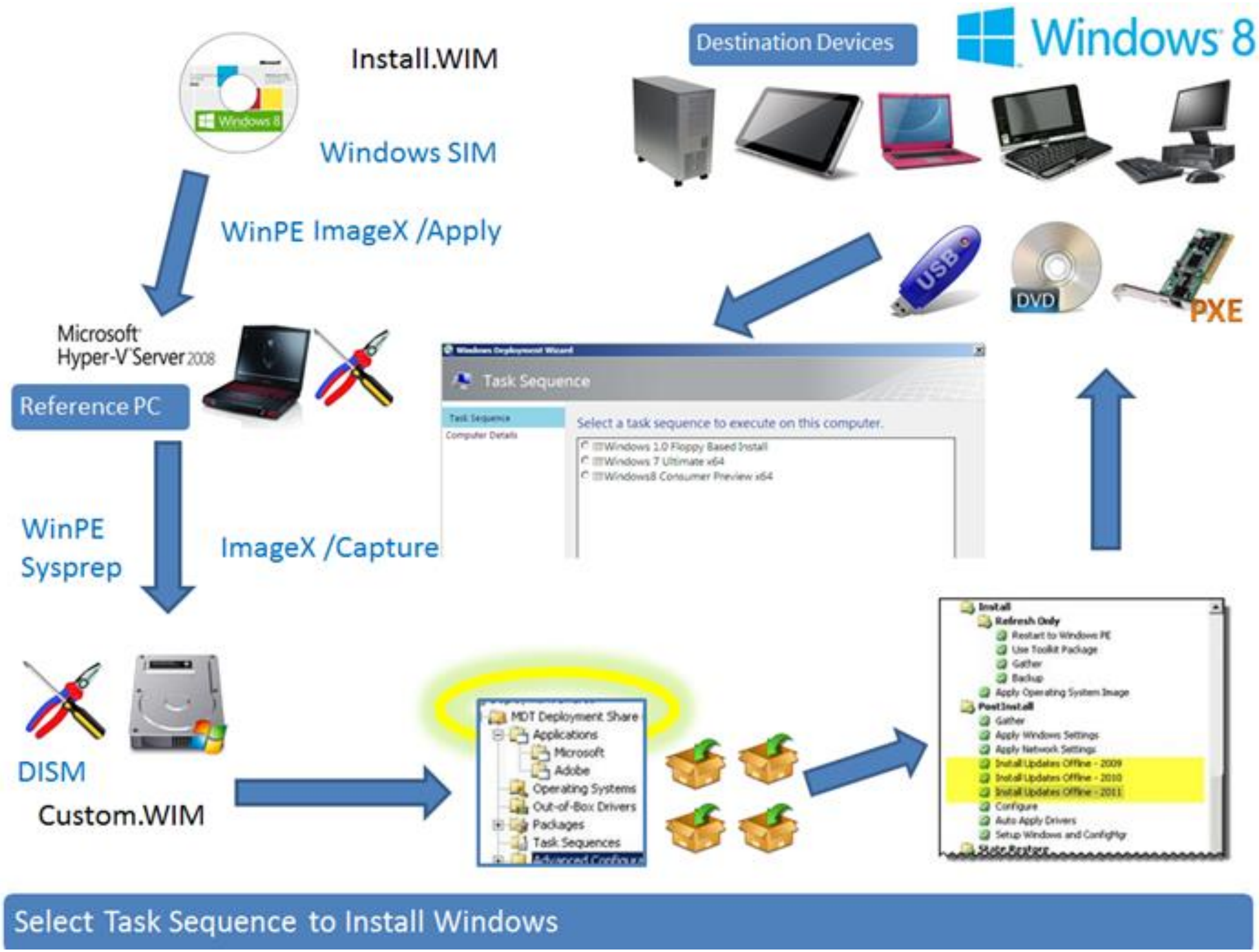
- **Start wireshark, sniff network traffic and try to access some resource on server, or switch user, etc...**
- **Examine logs and sniffed traffic by wireshark**

Windows 8 Deployment tools


Windows 8
Windows Deployment Tools
Lite Touch Deployment
Zero Touch Deployment
Weapons of Mass Deployment: Microsoft or 3rd Party
ENGL drv mgr
Setup Cmmdr
Update Cmmdr
usb/dvd Dwnldr
MAP
App Compat
System Center
Microsoft Deployment Toolkit
Weapons of Mass Deployment: WAIK or Windows Embedded
ImageX
Windows SIM
Windows Setup
Sysprep
Windows PE
DISM
Windows DS
Answer Files (unattend.xml or autounattend.xml)
Windows Imaging and Windows Imaging (WIM) files

http://www.alexdejong.com/wp-content/uploads/2012/04/image_thumb.png

Windows 8 Deployment tools



Windows Deployment Wizard

Task Sequence

Task Sequence
Computer Details

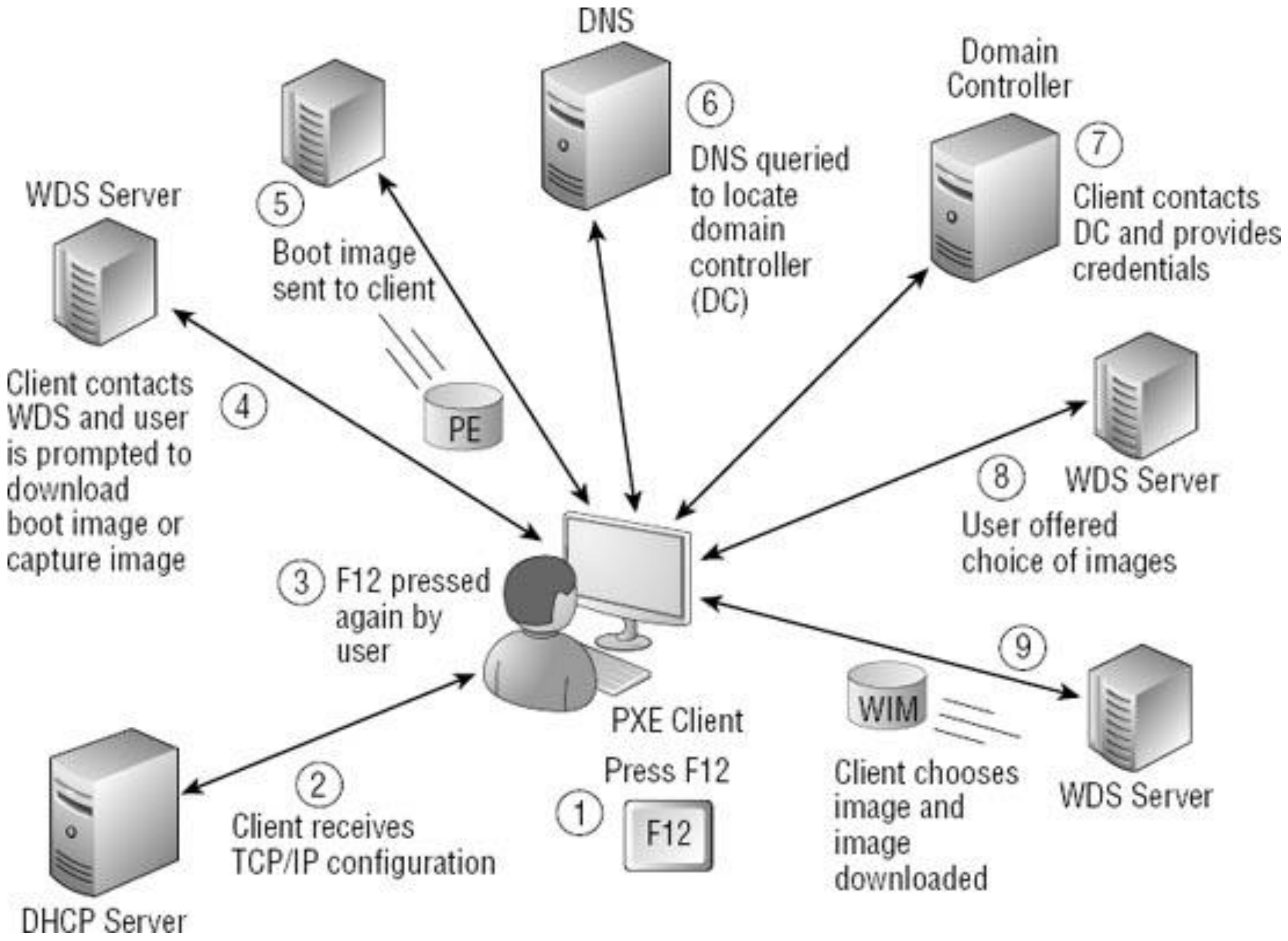
Select a task sequence to execute on this computer.

○ Windows 1.0 Floppy Based Install
○ Windows 7 Ultimate x64
○ Windows8 Consumer Preview x64

Install
Refresh Only
Restart to Windows PE
Use Toolkit Package
Gather
Backup
Apply Operating System Image
PostInstall
Gather
Apply Windows Settings
Apply Network Settings
Install Updates Offline - 2009
Install Updates Offline - 2010
Install Updates Offline - 2011
Configure
Auto Apply Drivers
Setup Windows and ConfigMgr
State Restore

http://www.alexdejong.com/wp-content/uploads/2012/04/image_thumb2.png

Windows Deployment Services


DNS
6
DNS queried to locate domain controller (DC)
Domain Controller
7
Client contacts DC and provides credentials
5
Boot image sent to client
PE
WDS Server
4
Client contacts WDS and user is prompted to download boot image or capture image
8
WDS Server
User offered choice of images
3
F12 pressed again by user
PXE Client
Press F12
1
F12
9
WIM
Client chooses image and image downloaded
WDS Server
2
Client receives TCP/IP configuration
DHCP Server

LAB 10: **Windows Deployment Services Getting Started Guide**

- W2012-DC, W8-domain
- Start here:
  - http://technet.microsoft.com/en-us/library/jj648426.aspx#WDS_InstallingWindowsDeploymentServicesintegratedwithActiveDirectory
- GL&HF

Sources

- http://technet.microsoft.com/en-us/library/hh831593.aspx
- http://technet.microsoft.com/en-us/library/cc732019.aspx
- http://www.alexdejong.com/?p=502
- http://technet.microsoft.com/en-us/library/jj648426.aspx#WDS_InstallingWindowsDeploymentServices

Thank you for attention!
Any questions?!