https://pasja-informatyki.pl/sieci-komputerowe/active-directory-wstep/

[Sieci komputerowe](https://pasja-informatyki.pl/sieci-komputerowe) | [10. Windows Server (#2) Active Directory](https://pasja-informatyki.pl/sieci-komputerowe/windows-server-active-directory)

**Wstęp teoretyczny do Active Directory**

Damian Stelmach

**Active Directory** to microsoftowa implementacja protokołu sieciowego warstwy aplikacji **LDAP** (ang. Lightweight Directory Access Protocol). Protokół LDAP stosowany jest w tak zwanych **usługach katalogowych**. Usługa katalogowa to nic innego jak **obszerna, hierarchiczna baz danych**, zawierająca informacje o **użytkownikach, grupach użytkowników, komputerach**, a także **zasobach sieciowych**, działających w sieciach firmowych, gdzie pracują serwery microsoftowe. To nic innego jak zbiór informacji o użytkownikach sieci, ich uprawnieniach do różnego rodzaju zasobów, komputerach, na jakich pracują, konfiguracji tych komputerów i tak dalej.

Active Directory pozwala administratorom sieci, centralnie, z poziomu jednego komputera (odpowiednio skonfigurowanego serwera) zarządzać całym zbiorem użytkowników w sieci, określać ich uprawnienia do zasobów sieciowych, a także konfigurować komputery, na których pracują. To potężne narzędzie zdecydowanie ułatwia pracę administratora w sieciach, gdzie pracują dziesiątki użytkowników i komputerów. Na całość usług związanych z Active Directory składa się aż **pięć elementów**:

1. AD **Domain Services**.

Active Directory Domian Services jest usługą służącą do zarządzania tożsamością, nadawania dostępu do zasobów sieciowych lub usług w sieci. Pozwala zabezpieczyć i zarządzać infrastrukturą, użytkownikami i zasobami. AD DS. jest miejscem do przechowywania i zarządzania informacjami o zasobach sieciowych, zapewnia wsparcie dla aplikacji korzystających z katalogu , takich jak Microsoft Exchange Server oraz umożliwia scentralizowane zarządzanie.

1. AD **Certificate Services**

Active Directory Certificate Services jest implementacją Infrastruktury Klucza Publicznego (PKI) stworzoną przez Microsoft. PKI jest zbiorem użytkowników, polityk, systemów komputerowych niezbędnych do świadczenia usług uwierzytelniania, szyfrowania, integralności i niezaprzeczalności za pośrednictwem kryptografii klucza publicznego, prywatnego i certyfikatów elektronicznych   
AD CS zapewnia usługę wydawania i zarządzania certyfikatami cyfrowymi poprzez: Certification Authorities (urząd certyfikacji), CA Web Enrollment (Web wydawanie), Online Responders, Network Device Enrollment Service (NDES), Certificate Enrollment Web Service, Certificate Enrollment Policy Web Service.

1. AD **Lightweight Directory Services**.

**Lightweight Directory Access Protocol** (**LDAP**) – protokół przeznaczony do korzystania z [usług katalogowych](https://pl.wikipedia.org/wiki/Us%C5%82uga_katalogowa), bazujący na standardzie [X.500](https://pl.wikipedia.org/wiki/X.500). Jest to również nazwa usługi katalogowej pozwalającej na wymianę informacji za pośrednictwem [TCP/IP](https://pl.wikipedia.org/wiki/Model_TCP/IP).

LDAP jest wykorzystywany praktycznie w adresacji sieci [Internet](https://pl.wikipedia.org/wiki/Internet)/[Intranet](https://pl.wikipedia.org/wiki/Intranet) w celu zapewnienia niezawodności, skalowalności i bezpieczeństwa danych. W odróżnieniu od X.500 nie potrzebuje ani szerokiego pasma, ani dużej mocy obliczeniowej. Pracuje w oparciu o protokół [TCP/IP](https://pl.wikipedia.org/wiki/Model_TCP/IP) lub inne połączeniowe usługi transportu. Dane grupowane są w strukturze przypominającej drzewo katalogów. Każdy obiekt jest jednoznacznie identyfikowany poprzez swoje położenie w drzewie, tzw. *Distinguished Name* (*DN*).

LDAP w wielu sytuacjach uznawane jest za rozwiązanie lepsze od innych usług katalogowych, ponieważ korzystając z TCP/IP (które działa tylko w warstwie transportowej [modelu OSI](https://pl.wikipedia.org/wiki/Model_OSI)), daje niezwykle szybkie odpowiedzi na żądania zgłaszane przez klienta[[1]](https://pl.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol#cite_note-1).

1. AD **Rights Management Services**.

Active Directory Rights Management Services (AD RMS) oferuje trwałe zasady użytkowania dotyczące poufnych informacji. Usługi AD RMS umożliwiają ochronę zawartości takiej jak witryny sieci Web, wiadomości e-mail oraz dokumenty. AD RMS Pozwala użytkownikowi określić uprawnienia dostępu do dokumentów, skoroszytów i prezentacji, uniemożliwia osobom nieupoważnionym drukowanie, przekazywanie lub kopiowanie maili oraz ogranicza dostęp bez względu na to, gdzie znajduje się informacja

1. AD **Federation Services**.

**Active Directory Federation Services** (ADFS) – część oprogramowania firmy Microsoft, instalowana na systemie operacyjnym [Windows Server](https://pl.wikipedia.org/wiki/Windows_Server). Umożliwia jednorazowe logowanie ([SSO](https://pl.wikipedia.org/wiki/Pojedyncze_logowanie)) do niezależnych aplikacji, w czasie trwania jednej sesji. ADFS oferuje bezpieczne udostępnianie tożsamości cyfrowej, jej praw, lub informacji takich jak e-mail, grupa, nazwa użytkownika (Claims).   
ADFS rozszerza Active Directory do usług internetowych. Działa podobnie jak standardowy [Active Directory](https://pl.wikipedia.org/wiki/Active_Directory). Kiedy użytkownik zostaje pomyślnie uwierzytelniony w jednym systemie, ma dostęp do innych aplikacji w całej sieci Windows (oczywiście gdy ma do tego prawo). ADFS dotyczy dokładnie takiej samej kwestii w internecie.

## Pojęcia związane z Active Directory

Magazyn danych

plik, przechowywany na dysku serwera, zawierający informacje o obiektach usługi katalogowej. Obiektem usługi katalogowej może być użytkownik, grupa, jednostka organizacyjna czy też komputer. Plik nosi nazwę NTDS.dit

Kontroler domeny

serwer, na którym zainstalowano Active Directory, przechowujący kopię magazyny danych. Wyróżnić możemy kontrolery typu Global Catalog (katalog globalny), a także kontrolery tylko do odczytu - Read-Only Domain Controler oraz odczytu i zapisu – Writeable Domain Controler.

Domena

obszar sieci, któremu przydzielono określone możliwości oraz zasoby. W niej skupione są obiekty Active Directory, takie jak użytkownicy, grupy, jednostki organizacyjne oraz komputery działające w jej obrębie. Aby można było domenę utworzyć, wymagany jest przynajmniej jeden kontroler.

Las

zbiór jednej lub też wielu domen. Pierwsza domena, która zostanie utworzona w lesie, będzie tak zwaną domeną główną lasu, a cały las przyjmie nazwę taką jak domena główna. Jeśli przykładowo tworzymy nową domenę w nowym lesie i nazwiemy ją test.local to cały las przyjmie taką nazwę.

Drzewo

jedna domena, albo kilka domen pracujących pod tą samą przestrzenią nazw DNS.

Jednostka organizacyjna

to obiekt usługi AD, pozwalający na przechowywanie użytkowników, grup użytkowników oraz komputery. Jednostkom organizacyjnym można przypisywać poszczególne zasady grupy oraz delegować uprawnienia administracyjne

**Wymagania systemów klienckich korzystających z Active Directory**

Każdy komputer kliencki, z zainstalowanym systemem Windows (7, 8.1 oraz 10) może pracować w domenie pod dwoma warunkami:

* musi być w wersji przynajmniej Professional (może być w wersji Ultimate lub Enterprise), żadnej z wersji Home do domeny nie podłączymy,
* oprócz licencji na sam system, do każdego klienta należy dokupić dodatkową licencję pozwalającą na korzystanie z zasobów serwera. Licencja to nosi nazwę CAL (ang. Client Access License). Więcej na temat licencji CAL przeczytacie na [tej stronie](https://www.microsoft.com/pl-pl/Licensing/product-licensing/client-access-license.aspx).

**Implementacja Active Directory**

Damian Stelmach

Implementacja usług katalogowych Active Directory na serwerach polega na zainstalowaniu odpowiedniej usługi. Usługa nazywa się Usługi Domenowe Active Directory (Active Directory Domain Services).

Jeśli to pierwsza nasza domena w lesie, to oprócz instalacji samej usługi, musimy jeszcze promować nasz serwer do roli kontrolera domeny. Cały proces instalacji został przedstawiony na zamieszczonych fragmentach wideo:

* Implementacja na Windows Server 2008 R2 – [https://www.youtube.com/watch?v=I1uuOiuM8v0&t=257s](https://www.youtube.com/watch?v=I1uuOiuM8v0&feature=youtu.be&t=4m17s)
* Implementacja na Windows Server 2012 R2 – https://www.youtube.com/watch?v=I1uuOiuM8v0&t=615s

Po instalacji i wstępnej konfiguracji usługi należy przyłączyć komputery klienckie do domeny, proces dla poszczególnych systemów również został przedstawiony na wideo:

* Dodawanie klienta do domeny z Windows 7 – https://www.youtube.com/watch?v=I1uuOiuM8v0&t=922s
* Dodawanie klienta do domeny z Windows 10 – https://www.youtube.com/watch?v=I1uuOiuM8v0&t=972s