Active Directory - Omówienie

Oprac. Dawid Polowczyk

Spis treści

1.Wstęp

Active Directory to microsoftowa implementacja protokołu sieciowego warstwy aplikacji **LDAP** (ang. Lightweight Directory Access Protocol). Pozwala administratorom sieci, centralnie, z poziomu jednego komputera (odpowiednio skonfigurowanego serwera) zarządzać całym zbiorem użytkowników w sieci. Możliwe jest określanie ich uprawnień do zasobów sieciowych, a także konfiguracja komputerów, na których pracują. To potężne narzędzie zdecydowanie ułatwia pracę administratora w sieciach, gdzie pracują dziesiątki użytkowników i komputerów.

2.LDAP

Z angielskiego: **Lightweight Directory Access Protocol**. **LDAP** jest wykorzystywany praktycznie w adresacji sieci Internet/Intranet w celu zapewnienia niezawodności, skalowalności i bezpieczeństwa danych. Protokół **LDAP** stosowany jest w usługach katalogowych. **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), daje niezwykle szybkie odpowiedzi na żądania zgłaszane przez klienta.

3.Usługi katalogowe

Usługa katalogowa to obszerna, hierarchiczna baza danych, zawierająca informacje o użytkownikach, grupach użytkowników, komputerach, a także zasobach sieciowych, działających w sieciach firmowych. To zbiór informacji o użytkownikach sieci, ich uprawnieniach do różnego rodzaju zasobów, komputerach, na jakich pracują, konfiguracji tych komputerów itp.

4.Składniki podstawowe Active Directory

Na całość usług związanych z Active Directory składa się aż pięć elementów:

- AD Domain Service. - *jest usługą służącą do zarządzania tożsamością, nadawania dostępu do zasobów sieciowych lub usług w sieci. Pozwala zabezpieczyć i zarządzać infrastrukturą, użytkownikami i zasobami.*

- AD 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 Lightweight Directory Services - *jest magazynem katalogu hierarchicznego opartego na pliku. Usługi AD LDS znajdujące się w katalogu, są źródłem informacji i usług dla aplikacji Lightweight Directory Access Protocol (LDAP).*

- AD Rights Management Services - *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.*

- AD Federation Services - ***u****możliwia użytkownikom logowanie się do zewnętrznej usługi WEB przy użyciu loginu i hasła, w wewnętrznym Active Directory. Rola AD FS zapewnia stworzenie federacji pomiędzy organizacjami, zarządzanie tożsamością oraz daje możliwość logowania pojedynczego (SSO).*

5.Pojęcia związane z korzystaniem z AD

a) Czym jest magazyn danych?

Magazyn danych przechowuje informacje o obiektach takich jak konta użytkowników, udostęp-nione zasoby, jednostki organizacyjne czy zasady grupy. Innym określeniem magazynu danych jest katalog, używany też jako zamienna nazwa samego systemu Active Directory.

b) W jakim celu wykorzystywany jest kontroler domeny?

Kontroler domeny przechowuje katalog w pliku o nazwie Ntds. dit. Lokalizacja tego pliku defi-niowana jest w trakcie instalacji Active Directory i musi znajdować się na dysku używającym systemu plików NTFS. Wybrane informacje katalogowe mogą zostać też zapisane oddzielnie, poza głównym magazynem danych. Dotyczy to zasad grupy, skryptów i innych informacji publicznych przechowywanych w udostępnianym woluminie systemowym (sysvol).

c) Domena i jej znaczenie?

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.

d) Zbiór jednej lub wielu domen?

*Jest to tzw. **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.*

e) Praca pod tą samą nazwą domeny?

Jest to tzw. Drzewo - jedna domena, albo kilka domen pracujących pod tą samą przestrzenią nazw DNS.

f) Podstawowa jednostka organizacyjna?

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

6.Wymagania na potrzeby stosowania systemów klienckich

Licencja Dostępowa (CAL) *oznacza licencję dostępową, którą można przypisać odpowiednio do użytkownika lub urządzenia. Licencja CAL użytkownika umożliwia jednemu użytkownikowi dostęp z dowolnego urządzenia do odpowiedniej wersji oprogramowania serwerowego lub jego wersji wcześniejszych. Licencja CAL urządzenia umożliwia dowolnemu użytkownikowi dostęp z jednego urządzenia do odpowiednich wersji oprogramowania serwerowego lub jego wersji wcześniejszych. Licencje CAL umożliwiają dostęp do oprogramowania serwerowego działającego wyłącznie na Licencjonowanych Serwerach klienta.*

CAL dostępowy na użytkownika *pozwala nam wykorzystać wiele urządzeń do dostępu do licencjonowanego serwera przez jednego użytkownika*

CAL dostępowy na urządzenie *pozwala nam na dostęp wielu użytkowników z jednego, licencjonowanego urządzenia do zasobów serwera*

Pytanie: *Czy inne serwery muszą posiadać licencję dostępową CAL żeby „rozmawiać" z innymi serwerami?*

Odpowiedź: *Nie, nie ma takiego wymogu, jeżeli są w tym samym środowisku Active Directory.*

7.Implementacja – proces instalacyjny na potrzeby serwera

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. Po instalacji i wstępnej konfiguracji usługi należy przyłączyć komputery klienckie do domeny.