

Linux i Windows dwa bratanki



Sebastian Stybel

MCSE, MCSA, MCITP, VCP-DCV

sebastian.stybel@bono.edu.pl | www.bono.edu.pl

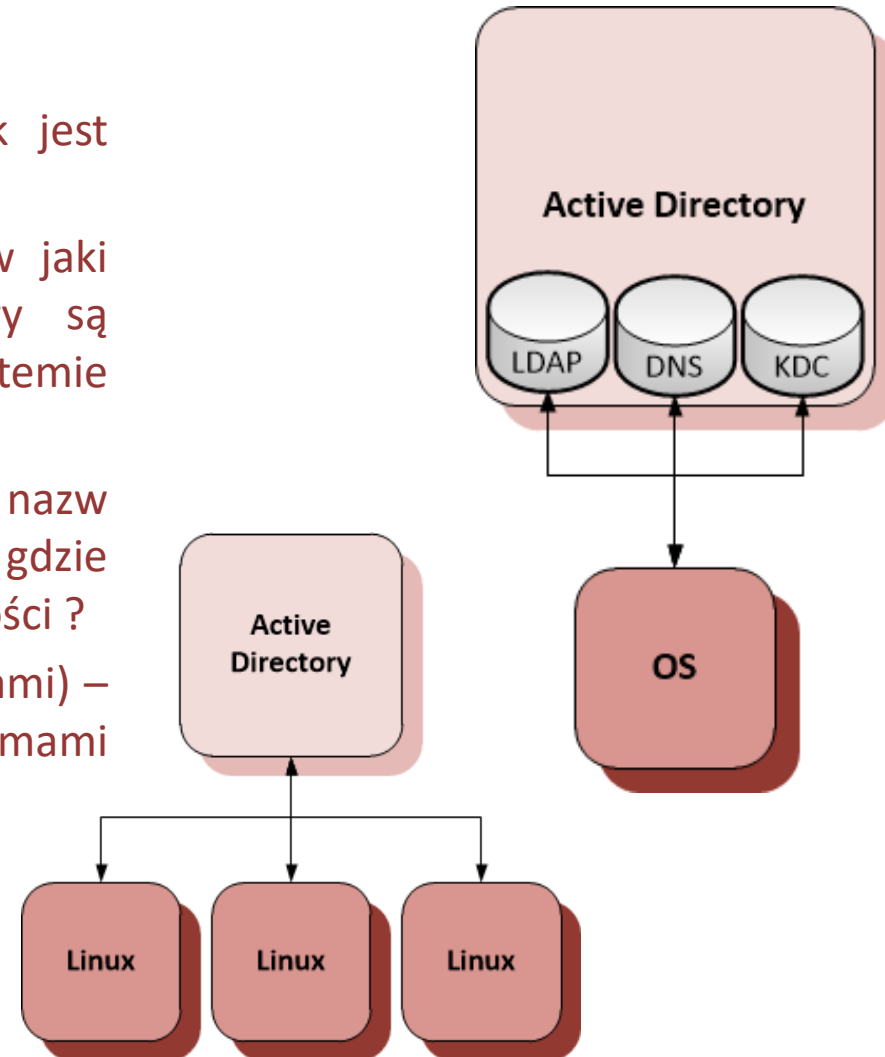
Wprowadzenie

- Integracja Linux / Windows
- Sposoby bezpośredniej integracja z AD
- Porównanie SSSD vs Winbind
- Środowisko demonstracyjne
- Demo

Integracja Linux / Windows

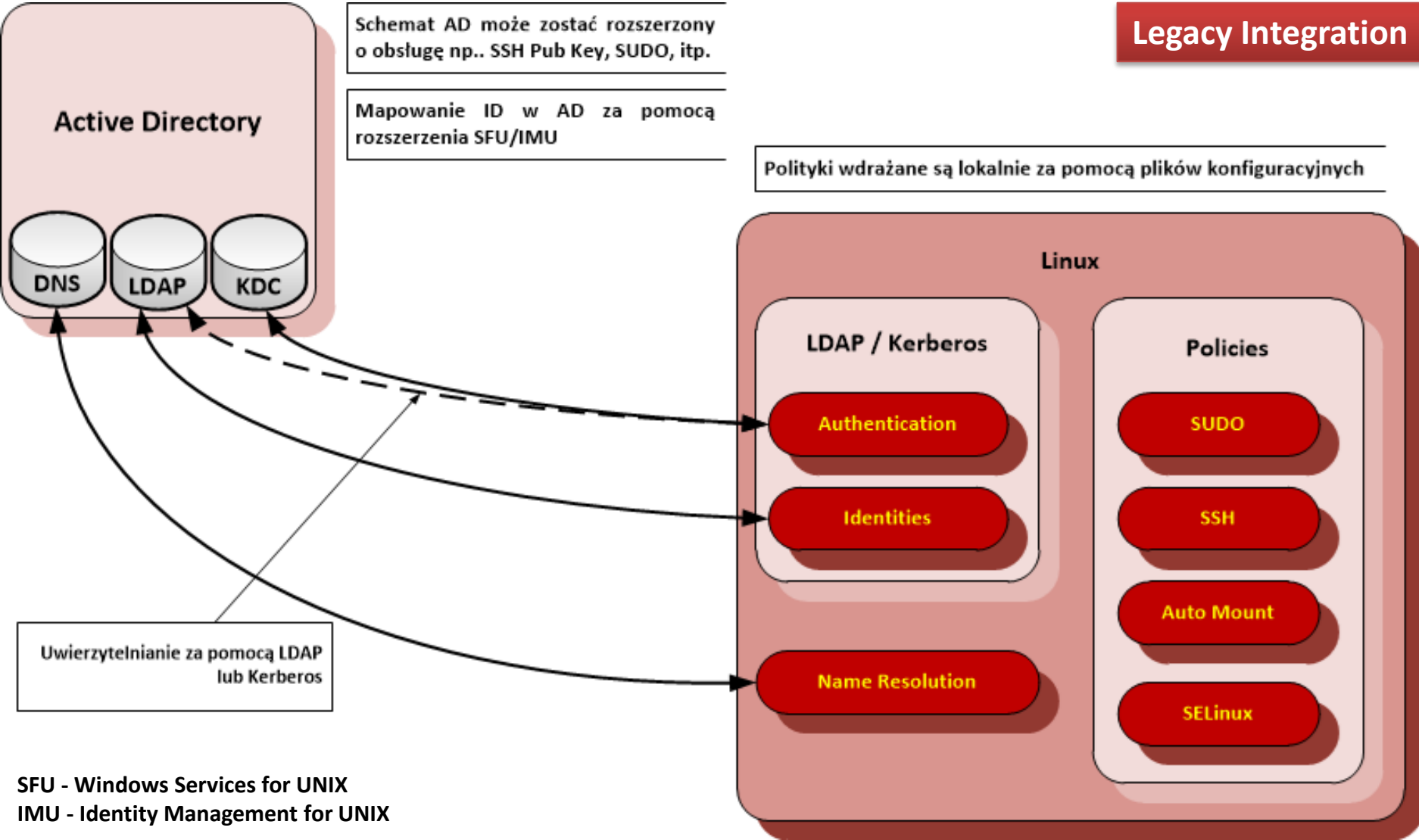
Aspekty integracji to:

- **Authentication** (uwierzelnianie) – jak jest uwierzelniony użytkownik ?
- **Identity** (wyszukiwanie tożsamości) – w jaki sposób konta usługi Active Directory są mapowane na konta używane w systemie Linux ?
- **Name Resolution** (rozwiązywanie nazw i wykrywanie usług) – skąd system wie, gdzie znaleźć serwer uwierzelniania i tożsamości ?
- **Policy Management** (zarządzanie politykami) – w jaki sposób zarządza się systemami związanymi z tożsamością ?



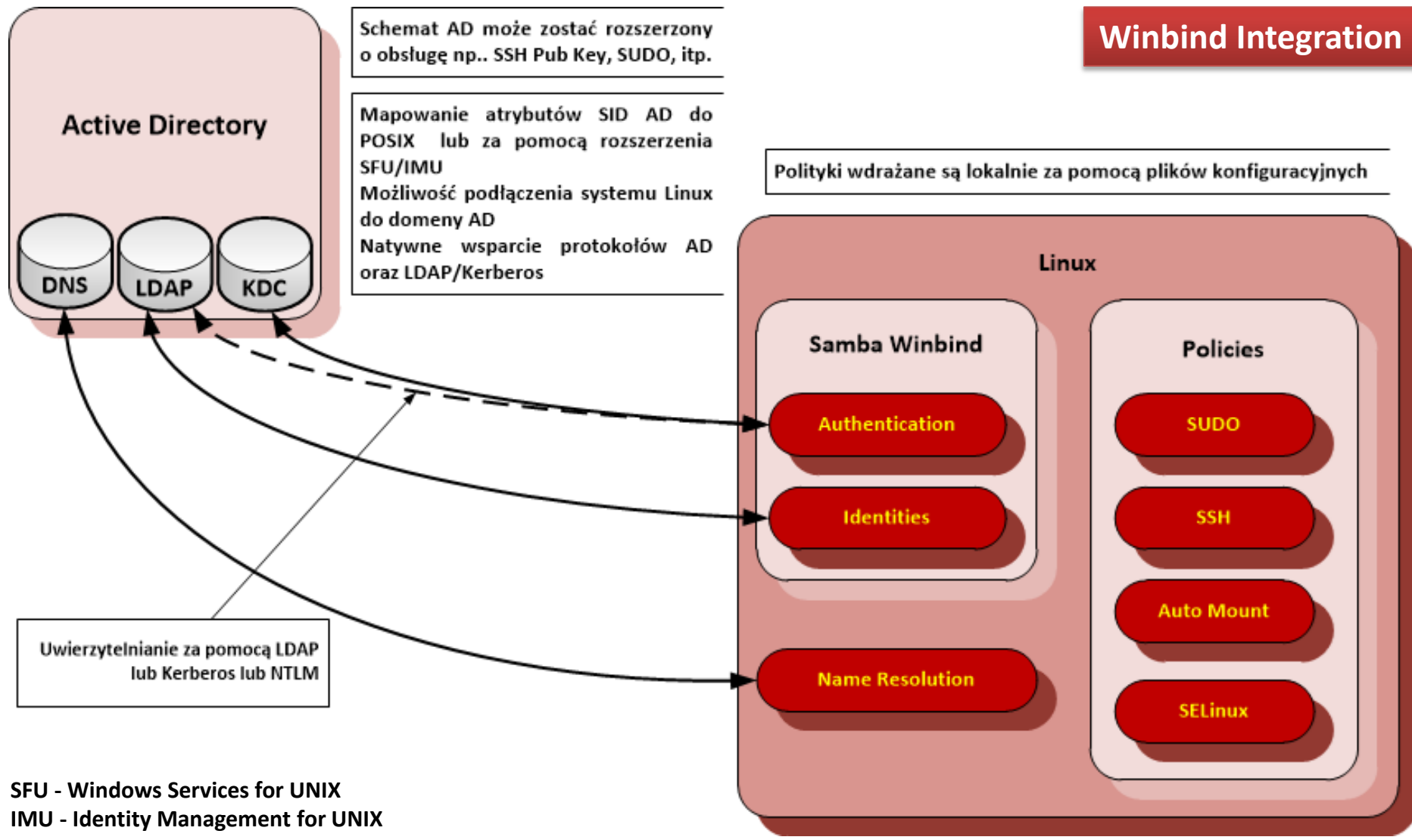
Sposoby bezpośredniej integracja z AD 1/3

Legacy Integration



SFU - Windows Services for UNIX
IMU - Identity Management for UNIX

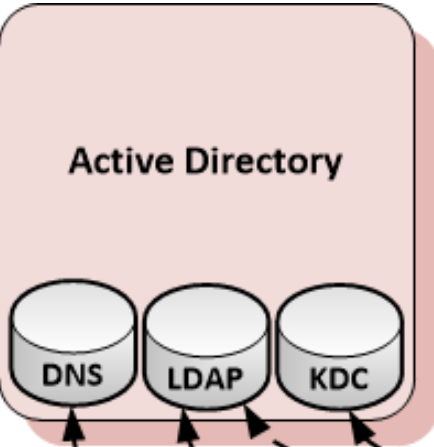
Sposoby bezpośredniej integracja z AD 2/3



SFU - Windows Services for UNIX
IMU - Identity Management for UNIX

Sposoby bezpośredniej integracja z AD 3/3

SSSD Integration

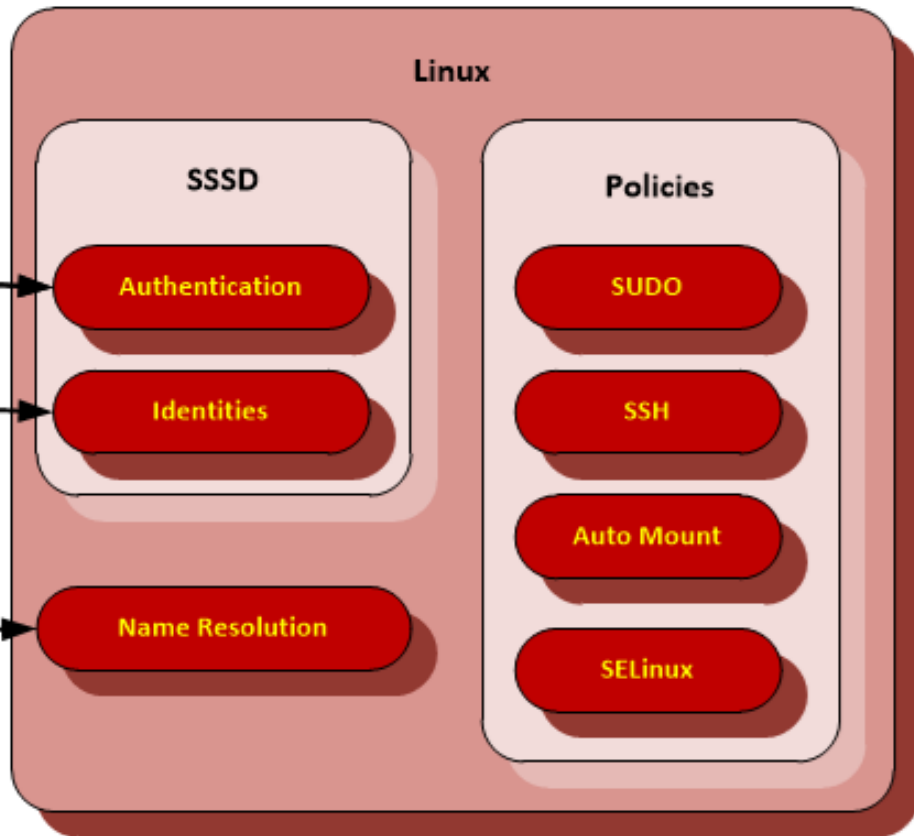


Schemat AD może zostać rozszerzony o obsługę np.. SSH Pub Key, SUDO, itp.

Mapowanie atrybutów SID AD do POSIX lub za pomocą rozszerzenia SFU/IMU
Możliwość podłączenia systemu Linux do domeny AD
Natywne wsparcie protokołów AD oraz LDAP/Kerberos

Polityki wdrażane są lokalnie za pomocą plików konfiguracyjnych
Wsparcie GPO dla HBAC jest obecnie rozwijane

Uwierzelnianie za pomocą LDAP lub Kerberos

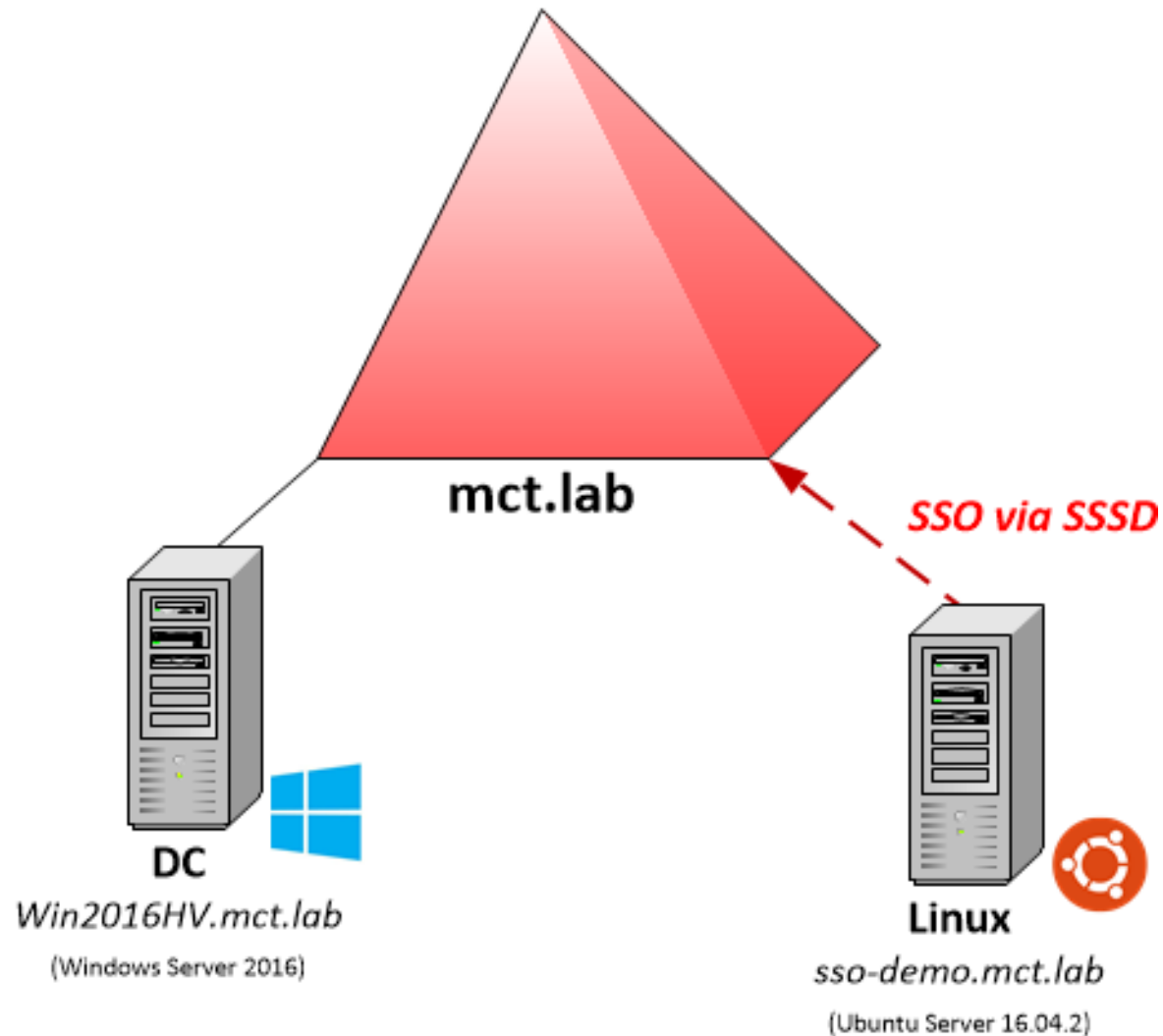


SFU - Windows Services for UNIX
IMU - Identity Management for UNIX
HBAC - Host Based Access Control

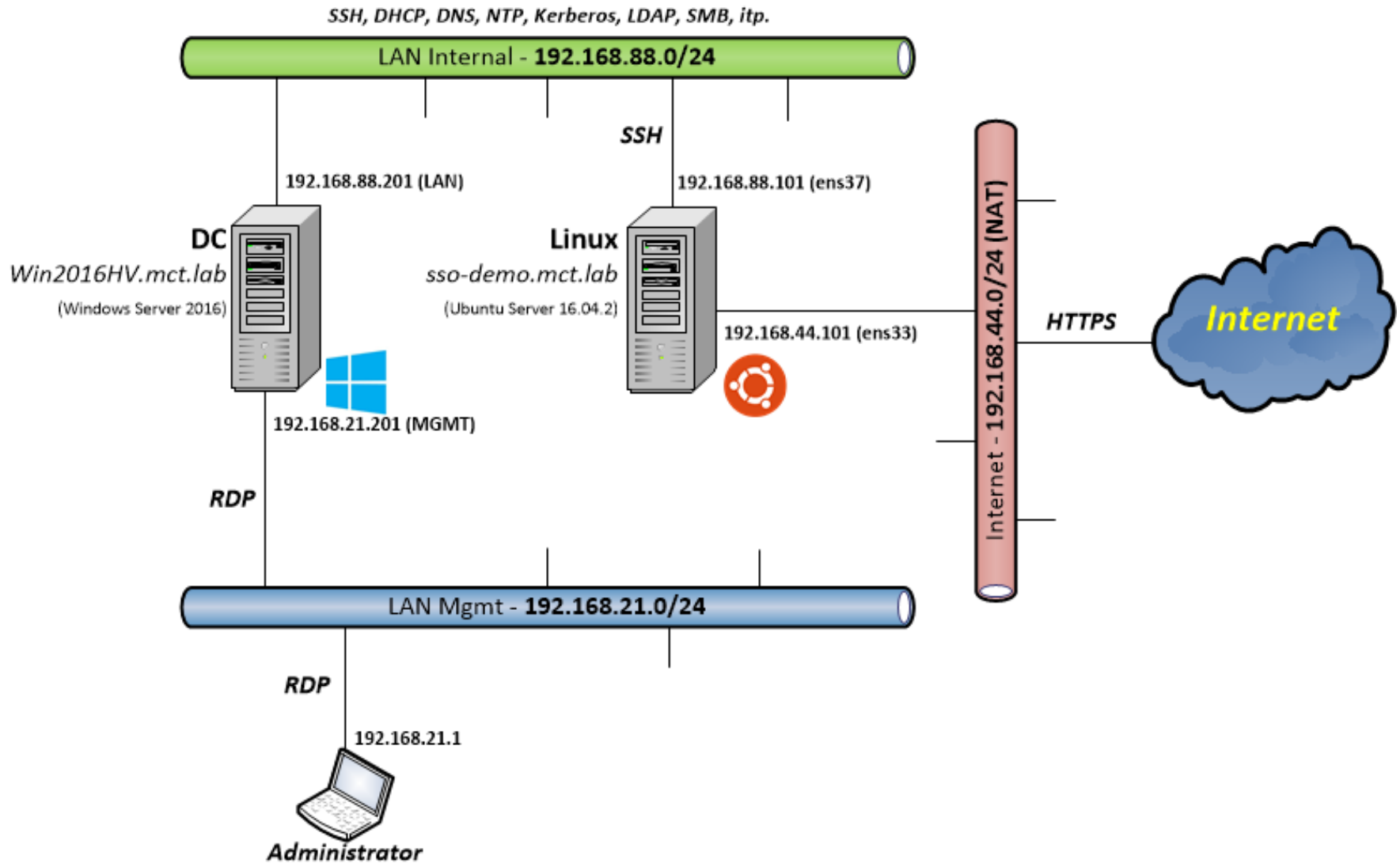
Porównanie SSSD vs Winbind

Category	Feature	Legacy (LDAP/Kerberos)	Samba Winbind	Third Party	SSSD
Authentication	Authenticate Using Kerberos	Yes	Yes	Yes	Yes
	Authenticate Using LDAP	Yes	Yes	Yes	Yes
	Support of multiple AD domains	No	Yes	Yes	Yes
	Support of AD forests	No	Yes	Yes	Yes
	Support of heterogeneous environments AD/FreeIPA (IdM)	No	No	No	Yes
Security	Easy to configure securely	No	No	Yes	Yes
	System has identity and its key is used to protect access to the central server	No	Yes	Yes	Yes
	NTLM support	No	Yes	Vendor specific	No
Identity Lookup and mapping	Requires AD POSIX extensions (SFU/IMU)	Yes	No	Vendor specific	No
	Dynamic ID mapping of AD SIDs	No	Yes	Vendor specific	Yes
	Takes advantage of the AD specific extensions and protocols.	No	Yes	Vendor specific	Yes
DNS	AD DNS Aging and Scavenging	No	No	Vendor specific	Yes
	AD DNS Sites	No	Yes	Vendor specific	Yes
File Sharing	Samba FS integration	No	Yes	Vendor specific	Yes
	CIFS client integration	No	Yes	Vendor specific	Yes
Policy	Centralized management of host based access control via GPO	No	No	Yes	Yes
Integration on the host with other services and applications	Integration with core utilities like SSH, sudo, automount	No	No	Vendor specific	Yes
	Extended identity interfaces over local message bus	No	No	No	Yes
	Special features for applications	No	No	No	Yes
User Experience	Simple installation	No	No	Yes	Yes
Cost		Free	Free	\$50-\$100 per client	Free

Środowisko demonstracyjne 1/2



Środowisko demonstracyjne 2/2



DEMO

Materiały

- Zbiór przydatnych linków

<http://www.bono.edu.pl/downloads/WGUiSW/Links.txt>

- Uaktualnienie schematów AD

<http://www.bono.edu.pl/downloads/WGUiSW/ADSchemaUpdateLDIF.txt>

<http://www.bono.edu.pl/downloads/WGUiSW/SSH.ldif>

<http://www.bono.edu.pl/downloads/WGUiSW/SUDO.ldif>

- Prezentacja

<http://www.bono.edu.pl/downloads/WGUiSW/SSO-Linux&Win.pdf>

- Porównanie SSSD vs Winbind

<http://www.bono.edu.pl/downloads/WGUiSW/SSSDvsWinbind.pdf>

- Demo

<http://www.bono.edu.pl/downloads/WGUiSW/SSO-Demo.mp4>

<http://www.bono.edu.pl/downloads/WGUiSW/SSO-Demo-CLI-Commands.txt>

Dziękuję



Sebastian Stybel

MCSE, MCSA, MCITP, VCP-DCV

sebastian.stybel@bono.edu.pl | www.bono.edu.pl