



POLITECHNIKA ŚLĄSKA
WYDZIAŁ AUTOMATYKI, ELEKTRONIKI I INFORMATYKI
KIERUNEK INFORMATYKA

Projekt inżynierski

Wdrożenie systemu pojedynczego logowania w sieci komputerowej
opartej o Active Directory

Single sign-on deployment in a computer network based on Active Directory

Autor: Radosław Serba

Kierujący pracą: dr Adam Józefiok

Gliwice, marzec 2021

Oświadczenie

Wyrażam zgodę/nie wyrażam* zgody na udostępnienie mojej pracy dyplomowej/rozprawy doktorskiej*

....., dnia

.....
(podpis)

.....
(poświadczenie wiarygodności podpisu przez Dziekanat)

* właściwe podkreślić

Oświadczenie promotora

Oświadczam, że praca „ ” spełnia wymagania formalne pracy dyplomowej inżynierskiej.

Gliwice, dnia

.....
(podpis)

Spis treści

WSTĘP	7
1. ANALIZA TEMATU	8
2. WYMAGANIA I NARZĘDZIA	10
3. SPECYFIKACJA ZEWNĘTRZNA.....	13
3.1. KONFIGURACJA POCZĄTKOWA.....	13
3.2. POCZĄTKOWA KONFIGURACJA SIECIOWA.....	15
3.3. DOCELOWA KONFIGURACJA	15
3.4. DOCELOWA KONFIGURACJA SIECIOWA	19
3.5. INSTALACJA SYSTEMU - WSTĘPNE PRZYGOTOWANIE.....	20
3.6. WDROŻENIE VMWARE ESXI.....	21
3.7. KONFIGURACJA VMWARE ESXI	22
3.8. INSTALACJA WINDOWS SERVER 2019	24
3.9. KONFIGURACJA KONTROLERÓW DOMENY	25
3.10. KONFIGURACJA FORTIGATE WRAZ Z INTEGRACJĄ Z DOMENĄ ACTIVE DIRECTORY	29
3.11. INSTALACJA EXCHANGE 2019.....	31
3.12. KONFIGURACJA EXCHANGE 2019.....	33
3.13. KONFIGURACJA RADIUS	39
3.14. KONFIGURACJA UDZIAŁU DO KOLABORACJI Z SERWEREM PLIKÓW QNAP	44
3.15. KONFIGURACJA STACJI KLIENCKICH	47
4. SPECYFIKACJA WEWNĘTRZNA.....	49
4.1. POCZĄTKOWA KONFIGURACJA	49
4.2. DOCELOWA KONFIGURACJA	49

4.3. DZIAŁANIE MECHANIZMU POJEDYNCZEGO LOGOWANIA W OPARCIU O KERBEROS	52
4.4. DZIAŁANIE SERWERÓW RADIUS	57
5. WERYFIKACJA I WALIDACJA	59
5.1. TEST MIGRACJI KONTA LOKALNEGO DO DOMENOWEGO ORAZ TEST PODŁĄCZENIA DO DOMENY ACTIVE DIRECTORY	59
5.2. TEST KONFIGURACJI SERWERA POCZTOWEGO	60
5.2.1. Test działania serwera Exchange	61
5.2.2. Test konfiguracji wirtualnych katalogów w Exchange	62
5.2.3. OWA	62
5.2.4. ECP	62
5.2.5. Outlook Anywhere	63
5.2.6. ActiveSync	63
5.2.7. Exchange Web Services	64
5.2.8. Online Address Book	64
5.2.9. Client Access	65
5.2.10. MAPI	65
5.2.11. Test logowania konta użytkownika poprzez OWA	66
5.2.12. Test logowania konta administratora poprzez ECP	67
5.2.13. Test logowania poprzez klienta pocztowego Microsoft Outlook	68
5.3. TEST LOGOWANIA DO VMWARE ESXI	69
5.4. TEST LOGOWANIA DO ZASOBU SIECIOWEGO NA SERWERZE PLIKÓW QNAP	70
5.5. TEST AUTORYZACJI W SIECI PRZEWODOWEJ KOMPUTERA KLIENCKIEGO	72
5.6. TEST POJEDYNCZEGO LOGOWANIA KONTA ACTIVE DIRECTORY W FORTIGATE	74
6. PODSUMOWANIE I WNIOSKI	76
A. BIBLIOGRAFIA	77
B. SŁOWNIK SKRÓTÓW I SYMBOLI	79
C. SPIS RYSUNKÓW	82

D.	SPIS ZAŁĄCZNIKÓW.....	85
D.1.	ZAŁĄCZNIK 1 – SKRYPT TWORZĄCY SCHEMAT JEDNOSTEK ORGANIZACYJNYCH ORAZ UŻYTKOWNIKÓW W DOMENIE ACTIVE DIRECTORY	85
D.2.	ZAŁĄCZNIK 2 – FRAGMENT PLIKU CSV WYKORZYSTYWANEGO PRZEZ SKRYPT TWORZĄCY UŻYTKOWNIKÓW W DOMENIE ACTIVE DIRECTORY	87
D.3.	ZAŁĄCZNIK 3 – FRAGMENT WYNIKU SKRYPTU TWORZĄCEGO SKRZYNKI W EXCHANGE 2019 NA PODSTAWIE KONT W DOMENIE ACTIVE DIRECTORY	88

Wstęp

W niniejszej pracy przedstawiono projekt systemu pojedynczego logowania oparty o bazę użytkowników w domenie Active Directory. Ma on ułatwić obsługę wewnętrznych systemów organizacji użytkownikom, ze względu na ograniczenie potrzebnej ilości poświadczeń (loginów i haseł) do pracy. Celem pracy jest ukazanie korzyści korzystania z systemów pojedynczego logowania wraz z przykładowym rozwiązaniem. W ramach pracy przedstawiono:

- Porównanie środowiska funkcjonującego bez systemu pojedynczego z systemem, który ma wspomniany system wdrożony do infrastruktury.
- Przykładowy sposób wdrożenia systemu pojedynczego logowania.
- Sposób działania systemu w podstawie przykładów.

Projekt został przedstawiony w postaci rozdziałów:

- **Analiza tematu** – ma na celu zapoznanie się z problemem wykorzystywania wielu loginów i haseł w ramach pracy na komputerze ogólnie i w organizacji.
- **Wymagania i narzędzia** – przedstawia uproszczone wymagania fizyczne i programowe, które muszą być spełnione w celu wdrożenia projektu.
- **Specyfikacja zewnętrzna** – określa metodykę przyjętą pod kątem początkowej konfiguracji sprzętowej/programowej, sposób instalacji i konfiguracji oprogramowania w celu wdrożenia projektu.
- **Specyfikacja wewnętrzna** – omawia teorię określającą sposób działania istotnych komponentów projektu.
- **Weryfikacja i walidacja** – przedstawia metodykę wykonywania testów wdrożenia systemu pojedynczego logowania pod kątem konfiguracji oraz działania systemu.

1. Analiza tematu

Codziennie każdy człowiek korzystający z usług dostępnych w Internecie, jak i człowiek pracujący w biurze używa systemów komputerowych. W wielu przypadkach dostęp do nich można otrzymać po uwierzytelnieniu się za pomocą loginu i hasła, czyli przedstawieniu unikalnych danych, którymi można zidentyfikować tożsamość użytkownika. Z faktu, że ludzie korzystają z różnych aplikacji zarówno prywatnie jak i służbowo powstaje problem, w którym jeden użytkownik może mieć nawet kilkadziesiąt różnych loginów i haseł w sieci. Ze względu na to, że większość osób nie jest w stanie zapamiętać kilkudziesięciu haseł do różnych kont, stosują oni uproszczenia w postaci jednego, dwóch lub trzech haseł do wszystkich usług. Ma to swoje konsekwencje – atakujący w momencie uzyskania jednego hasła uzyskuje dostęp do wielu usług, z których korzysta użytkownik.

Drugim problemem, który sprawia taki sposób zarządzania loginami i hasłami jest to, że serwisy posiadają różne polityki haseł, przez co wymuszają na użytkowniku zmianę hasła co jakiś czas (na przykład raz co pół roku) ze względów bezpieczeństwa. Takie hasła muszą mieć konkretną ilość znaków i ich typ (na przykład minimum 11 znaków, w tym duża litera, mała litera, cyfra i znak specjalny), na dodatek czasami nie można korzystać z poprzednich haseł. Jest to dobre podejście, ponieważ w ten sposób potencjalny atakujący będzie miał utrudnione zadanie, jeśli podejmie próby odgadnięcia hasła ofiary. Zakładając, że typowy użytkownik posiada konto w 60 różnych serwisach i każde ma wspomnianą politykę, świadomy zagrożenia użytkownik dla każdego serwisu z osobna musi zmieniać hasło.

Ponadto problemem mogą być wycieki haseł z różnych serwisów publicznych – jest to bardziej kłopotliwe niż utrata hasła przez roztargnienie, ponieważ często w takich wyciekach są udostępniane loginy i przypisane do nich hasła. Dzieje się to, ponieważ wiele serwisów przechowuje hasła jako zwykły, niezaszyfrowany tekst. Znając adres mailowy potencjalnej ofiary często można posiadać już login w serwisie/serwisach internetowych. Następnie wystarczy w jednym z wycieku znaleźć taki adres mailowy oraz przypisane do niego hasło – w ten sposób można próbować tymi samymi danymi logowania dostawać się do kolejnych zasobów prywatnych bądź służbowych ofiary.

Rozwiązaniem tych problemów jest mechanizm pojedynczego logowania (ang. single sign-on, SSO). W przypadku, gdy się z niego nie korzysta – każde poświadczenia (na przykład login i hasło) są przechowywane w różnych bazach. SSO zakłada korzystanie z jednej bazy do wszystkich usług na podstawie konta użytkownika. Dzięki temu w przypadku, gdy hasło użytkownika wygaśnie i będzie wymagało zmiany lub też zostanie skompromitowane w wycieku danych – wystarczy zmienić jedno hasło do konta i problem zmiany haseł jest rozwiązany. Za pomocą nowego hasła przypisanego do loginu można się zalogować do wszystkich serwisów wykorzystujących SSO. Do realizacji SSO można wykorzystywać różne mechanizmy, na przykład OAuth. Spotykamy je, korzystając z serwisów, gdzie można zalogować się za pomocą istniejących kont w Google czy Facebook.

W tej pracy podjęto się wdrożenia systemu pojedynczego logowania na bazie serwisów, które są dostępne w większości firm. Wdrożenie to ma udowodnić przewagę korzystania z jednej bazy do przechowywania haseł, zamiast rozproszonego systemu logowania, gdzie każdy serwis ma własną bazę loginów i haseł. W pierwszym rozdziale zawarto założenia systemu komputerowego, w którym ma być wdrożone SSO. Przedstawiono elementy, które tworzą system komputerowy oraz założenia, które muszą być spełnione, aby system umożliwiał na najszersze wykorzystanie mechanizmu pojedynczego logowania w sieci. Przedstawione elementy opisano pod kątem sprzętowym oraz programowym. W drugim rozdziale ukazano pojęcia, które należy zrozumieć, aby wiedzieć jak z praktycznego punktu działania wygląda wykorzystany mechanizm integracji. W trzecim rozdziale opisano praktyczne wdrożenie wspomnianych systemów. Ze względu na zakres, instalacja ta została podzielona na poszczególne elementy w celu łatwiejszego zrozumienia wykonanej pracy.

Ponadto rozdziały są ustawione w takiej kolejności, w jakiej instalacja była by realizowana w praktyce. W ostatnim rozdziale przedstawiono testy skonfigurowanego rozwiązania. Celem projektu jest wdrożenie mechanizmu pojedynczego logowania w celu umożliwienia na uwierzytelnienie się w różnych systemach wykorzystywanych w sieciach produkcyjnych w firmach w oparciu o usługę domenową Active Directory.

2. Wymagania i narzędzia

Aby projekt był możliwy do zrealizowania, potrzebna jest grupa komputerów połączonych siecią komputerową. Wymagane jest, aby na komputerach był zainstalowany system Windows 7 Pro/Enterprise lub nowszy (zalecany system to Windows 10) oraz by każda stacja kliencka była wyposażona w kartę sieciową przewodową obsługującą standard Fast Ethernet lub/i kartę bezprzewodową obsługującą standard 802.11 b/g/n/ac. Zaleca się, aby komputery miały dostęp do Internetu, dzięki czemu pobranie aktualizacji byłoby możliwe.

Część serwerowa infrastruktury wymaga komputera lub stacji roboczej, na której jest zainstalowany system operacyjny pozwalający na wirtualizację bądź osobne serwery fizyczne, które pełniłyby rolę kontrolera domeny Active Directory oraz serwera pocztowego Microsoft Exchange 2019, oba z zainstalowanym systemem Windows Server 2019. W przypadku wybrania opcji wirtualizacji serwerów zaleca się wykorzystanie oprogramowania VMware ESXi 7.0, Windows Hyper-V Server 2019 lub Windows Server 2019 z zainstalowaną rolą Hyper-V.

Do instalacji oprogramowania są potrzebne następujące nośniki:

- Nośnik instalacyjny Windows Server 2019 (dostępny w postaci płyty dołączonej serwera oraz w postaci brazy ISO pobranego z Internetu ze strony Microsoft.com).
- Instalator .NET Framework 4.8¹ (dostępny w postaci pakietu MSI pobranego z Internetu ze strony Microsoft.com).
- Instalator Visual C++ Redistributable Package for Visual Studio 2012² (dostępny w postaci pakietu MSI pobranego z Internetu ze strony Microsoft.com).
- Instalator Visual C++ Redistributable Package for Visual Studio 2013³ (dostępny w postaci pakietu MSI pobranego z Internetu ze strony Microsoft.com).

¹ Exchange Server system requirements <https://docs.microsoft.com/en-us/exchange/plan-and-deploy/system-requirements?view=exchserver-2019>

² Exchange Server system requirements <https://docs.microsoft.com/en-us/exchange/plan-and-deploy/system-requirements?view=exchserver-2019>

³ Exchange Server system requirements <https://docs.microsoft.com/en-us/exchange/plan-and-deploy/system-requirements?view=exchserver-2019>

- Instalator Microsoft Unified Communications Managed API 4.0⁴ (dostępny w postaci pakietu MSI pobranego z Internetu ze strony Microsoft.com).
- Instalator zestawu narzędzi Remote Server Administration Tools⁵ (dostępny w postaci pakietu MSI pobranego z Internetu ze strony Microsoft.com lub dostępny do zainstalowania w postaci odpowiednich funkcji w systemie Windows Server 2019).
- Nośnik instalacyjny Microsoft Exchange 2019 (dostępny w postaci płyty dołączonej serwera oraz w postaci pliku ISO pobranego z Internetu ze strony Microsoft.com).
- W przypadku wirtualizacji za pomocą VMware ESXi 7.0 nośnik instalacyjny VMware ESXi 7.0 (dostępne w postaci obrazu ISO pobranych z Internetu ze strony my.vmware.com).
- W przypadku wirtualizacji za pomocą Windows Hyper-V Server nośnik instalacyjny Windows Hyper-V Server (dostępny w postaci pakietu MSI pobranego z Internetu ze strony Microsoft.com).

Ponadto, wymagany jest program umożliwiający migrację profili użytkowników kont lokalnych do kont domenowych, na przykład program ForensiT User Profile Wizard 21 (dostępny w postaci płyty dołączonej serwera oraz w postaci pliku ISO pobranego z Internetu ze strony forensit.com).

Serwer musi posiadać co najmniej jeden procesor wielordzeniowy, przy czym zaleca się, aby procesor pochodził z serii przeznaczonej do rozwiązań serwerowych (na przykład procesory Intel Xeon Bronze lub lepsze, AMD EPYC 72xx lub lepsze) oraz aby serwer obsługiwał wirtualizację sprzętową (funkcja Intel VT-x lub AMD-V). Ponadto serwer powinien posiadać co najmniej 2 dyski połączone w grupę RAID1 w celu zapewnienia bezpieczeństwa danych przed awarią 1 dysku), najlepiej dyski SAS HDD z prędkością 15 tysięcy RPM o pojemności co najmniej 900 GB lub dyski SATA SSD o pojemności 980 GB

Oprogramowanie wdrażane na serwery ma następujące zalecane wymagania pod kątem pamięci RAM:

- Windows Server 2019 – 2 GB RAM w przypadku posiadania zainstalowanego środowiska graficznego⁶, lecz w przypadku kontrolera domeny zostanie użyte 8 GB RAM, aby umożliwić większą stabilność rozwiązania,

⁴ Exchange Server system requirements <https://docs.microsoft.com/en-us/exchange/plan-and-deploy/system-requirements?view=exchserver-2019>

⁵ Exchange Server system requirements <https://docs.microsoft.com/en-us/exchange/plan-and-deploy/system-requirements?view=exchserver-2019>

⁶ Windows Server 2019 System Requirements <https://docs.microsoft.com/en-us/windows-server/get-started-19/sys-reqs-19>

- Exchange 2019 – zalecana ilość to 128 GB RAM⁷, lecz w praktyce potrzebna ilość pamięci RAM zależy od średniej ilości wiadomości mailowych wysyłanych na godzinę oraz liczby użytkowników, dozwolonego maksymalnego rozmiaru wiadomości oraz jednoczesnej liczby użytkowników serwera w jednym czasie i w ramach tego projektu zostanie użyte 16 GB RAM, ponadto Exchange musi być zainstalowany w systemie Windows Server 2019, więc dodatkowo do maszyny z pamięcią RAM doliczone jest 8 GB RAM, co daje 24 GB RAM,
- W przypadku stosowania VMware ESXi do wirtualizacji te wymaga minimum 8 GB pamięci RAM do użytku produkcyjnego⁸,
- W przypadku stosowania Windows Hyper-V Server do wirtualizacji te wymaga minimum 4 GB pamięci RAM do użytku produkcyjnego⁹,

Sumarycznie otrzymano 40 GB RAM w przypadku wykorzystania środowiska fizycznego, 44 GB w przypadku środowiska wirtualnego bazowanego na Windows Hyper-V Server i 48 GB w przypadku środowiska wirtualnego bazowanego na VMware ESXi. W projekcie zostało zastosowane środowisko VMware ESXi ze względu na ogólną wydajność wirtualizacji w stosunku do Microsoft Hyper-V.

Do szybkiej instalacji oprogramowania zaleca się korzystanie z nośnika flash w postaci pendrive lub dysku zewnętrznego podłączanego złączem USB o standardzie co najmniej 3.0. Alternatywnie możliwe jest wykorzystanie nośników DVD wraz z odpowiednim odtwarzaczem (wbudowany w serwer lub zewnętrzny, podłączany przez port USB).

⁷ Exchange Server system requirements <https://docs.microsoft.com/en-us/exchange/plan-and-deploy/system-requirements?view=exchserver-2019>

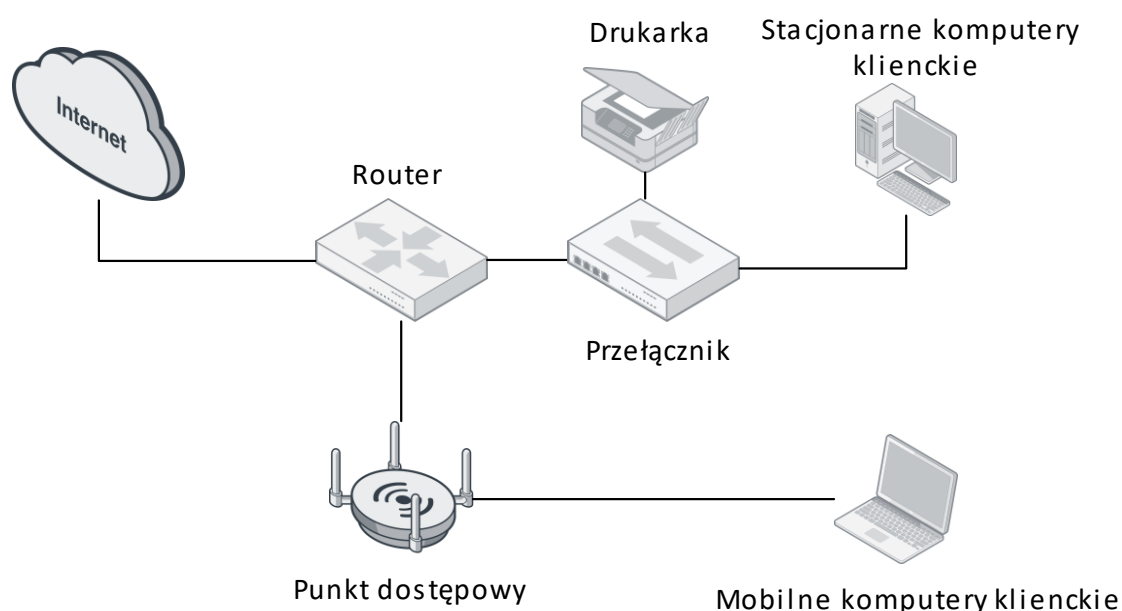
⁸ ESXi Hardware Requirements <https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.esxi.install.doc/GUID-DEB8086A-306B-4239-BF76-E354679202FC.html>

⁹ System requirements for Hyper-V on Windows Server <https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/system-requirements-for-hyper-v-on-windows>

3. Specyfikacja zewnętrzna

3.1. Konfiguracja początkowa

Konfiguracja początkowa opisuje działanie sieci komputerowej umożliwiającej użytkownikom pracę w sieci lokalnej z szerokopasmowym dostępem do Internetu. Najpopularniejsza konfiguracja w małych organizacjach składa się z routera, który jest podłączony do Internetu oraz przełącznika, do którego są bezpośrednio podłączone komputery. Aby umożliwić połączenie komputerom mobilnym, w sieci jest podłączony punkt dostępowy do routera. Schemat poglądowy sieci przedstawiono na rys. 3.1.



Rys. 3.1. Początkowa konfiguracja sieci komputerowej, bez wdrożonego mechanizmu pojedynczego logowania

Opisując powyższy schemat, należy podkreślić, że jest to konfiguracja zabezpieczona w podstawowym stopniu, pozbawiona mechanizmu pojedynczego logowania. W tej sieci łącząc się z siecią bezprzewodową, nie jest realizowana żadna autoryzacja – użytkownik po podłączeniu się do przełącznika po prostu ma dostęp do sieci. Najczęściej przełącznik jest typu niezarządzanego, co oznacza, że nie ma możliwości ustawienia go w jakikolwiek sposób. Oznacza to też, że nie można logować się do urządzenia w celu zmiany konfiguracji, ponieważ realizuje ono proces przełączania w ramach wszystkich urządzeń podłączonych fizycznie do niego. W przypadku sieci bezprzewodowej jest wykorzystywany typ zabezpieczeń WPA2-PSK – co oznacza, że każdy użytkownik łączący się do sieci bezprzewodowej wykorzystuje to same hasło do podłączenia się do sieci. Jest to problematyczne z tego względu, że w przypadku wycieku hasła nie jesteśmy w stanie sprawdzić z jakiego źródła ono pochodzi. Po wycieku należy zmienić hasło współdzielone wszystkim użytkownikom i ponownie występuje takie same zagrożenie wycieku hasła. Ponadto, ze względu na brak integracji z domeną routera oraz brakiem funkcjonalności NGFW nie ma możliwości identyfikacji użytkowników w sieci lokalnej poza analizą ruchu na podstawie adresów MAC urządzeń i statycznej adresacji IP w sieci lokalnej. Aby administrator miał jakąkolwiek kontrolę nad tym jakie urządzenie ma dostęp do konkretnego elementu w sieci komputerowej, należałoby analizować ruch względem konkretnych adresów IP. Na przykład, jeśli konkretny użytkownik miałby rozwiązywać nazwy poprzez serwer DNS o konkretnym adresie IP, należałoby stworzyć regułę zapory ogniowej pozwalającej na ruch wychodzący na port docelowy TCP 53 z adresu IP wspomnianego komputera. Taka reguła działałaby na użytkownika tylko i wyłącznie wtedy, gdy pracuje przy stanowisku, który ma wspomniany wcześniej adres IP. Gdy go nie ma, reguła nie ma zastosowania – na przykład w sytuacji, gdy ten postanowi używać innego stanowiska komputerowego w organizacji. Bez dodatkowej zmiany konfiguracji karty sieciowej (i zmiany adresu IP na poprzedni używany przez użytkownika) reguła nie miałaby dalszego zastosowania.

Przykładowe graficzne przedstawienie sieci można zobaczyć na *Rys. 3.1*.

3.2. Początkowa konfiguracja sieciowa

Adresacja sieciowa wykorzystana w projekcie jest przykładowa, co oznacza, że w praktyce w celu wdrożenia projektu może być wykorzystana inna adresacja z zachowaniem odpowiedniego schematu:

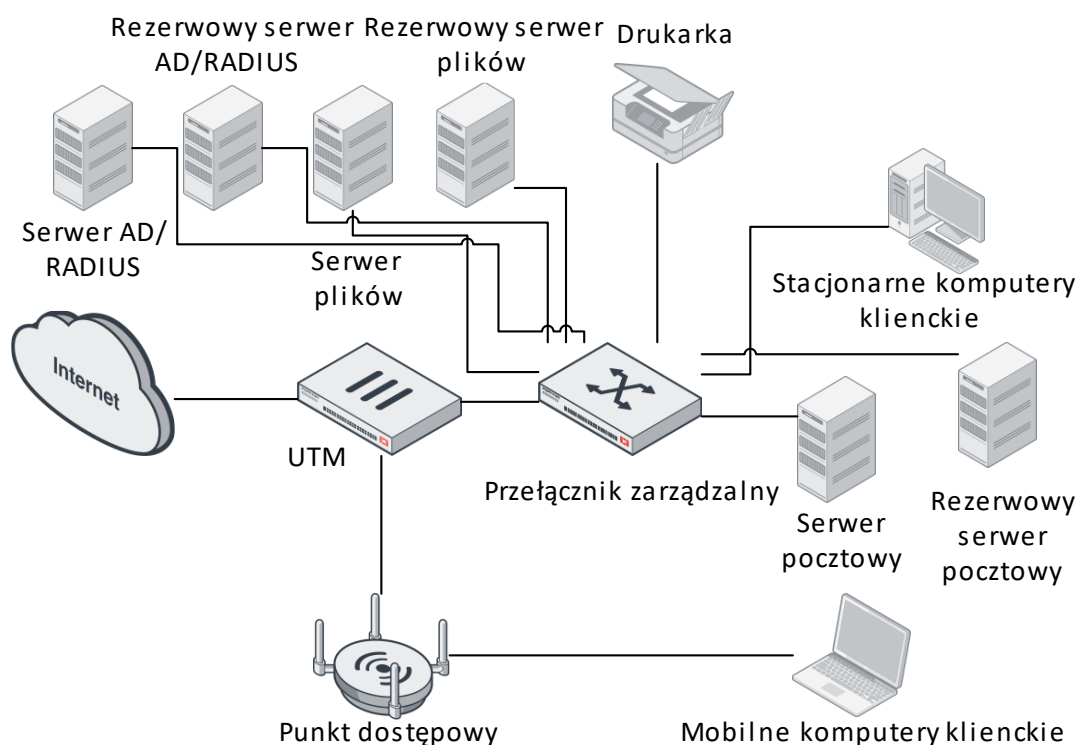
- Publiczny adres IP routera/UTM: przydzielony przez dostawcę, na przykład **89.71.117.58/22**.
- Prywatny adres IP routera/UTM: **192.168.30.1/24**
- Adres drukarki: **192.168.30.20/24**
- Adres punktu dostępowego: **192.168.30.19/24**
- Zakres adresów przypisywanych urządzeniom przez serwer DHCP: **192.168.30.100-192.168.30.200**
- Suffix DNS sieci: **serba.local**
- Adres serwera DNS: **9.9.9.9**
- Rezerwowany adres serwera DNS: **1.1.1.1**

3.3. Docelowa konfiguracja

Docelowe rozwiązanie ma zapewnić uwierzytelnienie na poziomie połączenia przewodowego/bezprzewodowego – przełącznik ma umożliwiać sprawdzenie czy wskazany komputer jest częścią domeny Active Directory oraz czy ma uprawnienia do łączenia się do wybranego segmentu sieci na podstawie komunikacji z serwerem RADIUS. Podobnie jest w przypadku sieci bezprzewodowej – zamiast wykorzystania mechanizmu WPA2-PSK w sieci docelowo zostałyby wykorzystany WPA2-Enterprise, co pozwala na jednoznaczną identyfikację oraz uwierzytelnienie łączącego się użytkownika, także przy użyciu serwera RADIUS. W tym scenariuszu nie ma możliwości na anonimową kompromitację dostępu do sieci przez sieć bezprzewodową ze względu na to, że w przypadku niepożądanego ruchu sieciowego będzie możliwe sprawdzenie kto w konkretnym czasie się autoryzował w sieci i kto wykonywał taki ruch.

Ponadto serwery fizyczne są wyposażone w interfejsy IPMI, które pozwalają na zdalne zarządzanie (włączanie/wyłączanie serwera, zdalna instalacja systemu operacyjnego, zdalna kontrola i podgląd ekranu serwera, informacje o stanie i kondycji urządzenia (status sprawności wiatraków, dysków, procesora, zasilaczy itd.)). Całe środowisko serwerowe jest zwirtualizowane, co oznacza, że systemy serwerowe pracują w maszynach wirtualnych. To pozwala na lepsze wykorzystanie dostępnego sprzętu do realizacji projektu oraz minimalizację kosztów związanych z kolejnymi maszynami fizycznymi. Ponadto, w końcowym scenariuszu możliwa jest analiza ruchu sieciowego na podstawie obiektów w domenie Active Directory, co oznacza, że urządzenie pełniące rolę routera (UTM) jest w stanie sprawdzić jaki użytkownik próbuje wykonać połączenie z wybranym segmentem sieci bez względu na adres IP komputera w sieci lokalnej, z której się łączy.

Przykładowe graficzne przedstawienie sieci można zobaczyć na Rys. 3.2.



Rys. 3.2. Docelowa konfiguracja sieci komputerowej z wdrożonym mechanizmem pojedynczego logowania

Ze względu na potrzebę utrzymywania pracy systemów i aplikacji serwerowych bez przerwy należy zapewnić sprzęt, który umożliwi łatwą naprawę oraz w odporność na awarię niektórych części, dlatego w projekcie został zastosowany serwer FUJITSU RX2540 M4 z dwoma procesorami Intel Xeon Silver 4114, gdzie każdy z nich posiada 10 rdzeni, częstotliwość taktowania procesora 2,2 GHz oraz Hyper-threading, pamięcią RAM 64 GB RDIMM ECC z częstotliwością taktowania 2666 MHz oraz 4 dyskami SSD SATA INTEL SSDSC2BB480G7C o rozmiarze 512 GB na dysk dla zapewnienia szybkiego dostępu do danych systemu oraz karta PLAN EM 10 Gb SFP+ OCP, która pozwala na komunikację w sieci 10 Gigabit Ethernet. Ma on dwa interfejsy, dzięki można pracować na większej przepustowości lub wykorzystywać dwa złącza w celu redundancji łącza. Dodatkowo serwer był wyposażony we wbudowane 3 interfejsy sieciowe obsługujące standard 1 Gigabit Ethernet, z czego domyślnie jeden interfejs był wykorzystywany do zdalnego zarządzania serwerem (poprzez mechanizm iRMC (integrated Remote Management Controller)/IPMI), a dwa pozostałe były dostępne dla systemu operacyjnego hosta. Serwer wyposażono w kartę Fibre Channel PFC EP QLE2692 16 Gbit/s, która umożliwiałaby podłączenie macierzy dyskowej i utworzenie klastra wysokodostępnego, lecz nie zostało to zrealizowane w ramach tego projektu, mimo to dzięki temu interfejsowi cały projekt mógłby być rozbudowany o dodatkowe elementy w przyszłości. Ponadto serwer był wyposażony w podwójny zasilacz 450W, dzięki czemu w przypadku spalenia się jednego z nich drugi mógł podtrzymać pracę serwera bez restartu systemu operacyjnego. Powyższy host można zastąpić innym – wskazana maszyna została wybrana ze względu na najlepsze dostępne predyspozycje szybkiej i bezawaryjnej pracy przez długi czas.

W tym przypadku został wykorzystany przełącznik NETGEAR GS716Tv3-300EUS. Ten przełącznik został wybrany ze względu na możliwość komunikacji z serwerami RADIUS¹⁰, obsługę protokołu 802.1X, obsługę portów w standardzie Gigabit Ethernet i budowę przystosowaną do montażu w szafie serwerowej typu rack. Dzięki takiemu przełącznikowi można podłączyć komputery klienckie poprzez sieć przewodową.

Następnym elementem jest umożliwienie bezpiecznego połączenia z Internetem oraz możliwość łączenia się komputerów klienckich przez sieć bezprzewodową. Do tego zadania został wykorzystany sprzęt typu UTM FortiWiFi 60E posiadający wbudowaną kartę

¹⁰ NETGEAR GS716Tv3, GS624Tv4, GS748Tv5 Data Sheet
<https://www.downloads.netgear.com/files/GDC/datasheet/en/GS716Tv3-GS724Tv4-GS748Tv5.pdf>

beprzewodową obsługującą sieci w standardzie 802.11 a/b/g/n/ac<sup>Błąd! Nie można odnaleźć źródła o
dwołania.</sup>¹¹, 7 interfejsów przeznaczonych dla sieci LAN, 1 interfejs przeznaczony dla sieci DMZ oraz 2 interfejsy sieciowe przeznaczone do połączenia z siecią WAN. Wszystkie wymienione interfejsy sieciowe obsługują standard Gigabit Ethernet poprzez złącze RJ-45. Urządzenie to można wykorzystać jako klienta RADIUS do autoryzacji użytkowników w sieci bezprzewodowej oraz pozwala na realizowanie polityk firewalla na podstawie kont i grup w bazie Active Directory. Dzięki temu konkretny użytkownik ma dostęp do konkretnych zasobów bez względu na to, z jakiego komputera będącego członkiem domeny Active Directory się zaloguje. Ponadto urządzenie może pełnić rolę serwera VPN, gdzie użytkownicy za pomocą dedykowanego klienta VPN może uzyskać dostęp do sieci produkcyjnej z użyciem poświadczeń konta w domenie Active Directory.

Chcąc umożliwić łatwą wymianę danymi pomiędzy użytkownikami zastosowano macierz dyskową QNAP TS-453A-8G z wbudowanym procesorem Intel Celeron N3150, pamięcią RAM 8 GB SODIMM DDR3L-1600, 4 portami RJ-45 obsługującymi standard Gigabit Ethernet¹² oraz zamontowanymi 4 dyskami HDD SATA WD RED WD20EFRX o rozmiarze 2 TB na dysk. Macierz ta pracuje pod kontrolą systemu QTS (QNAP Turbo System), który bazuje na Linuksie. Jedną z funkcjonalności, która zostanie wykorzystana w tym systemie jest integracja z domeną Active Directory, dzięki czemu użytkownicy będą mogli otrzymywać dostęp do zasobów na bazie ich kont użytkowników lub grup, do których należą.

¹¹ FortiGate/FortiWiFi 60E Series Data Sheet https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_FortiWiFi_60E_Series.pdf

¹² QNAP TS-453A – Specyfikacja sprzętowa <https://www.qnap.com/pl-pl/product/ts-453a/specs/hardware>

3.4. Docelowa konfiguracja sieciowa

Adresacja sieciowa wykorzystana w projekcie jest przykładowa, co oznacza, że w praktyce w celu wdrożenia projektu może być wykorzystana inna adresacja z zachowaniem odpowiedniego schematu:

- Publiczny adres IP routera/UTM: przydzielony przez dostawcę, na przykład **89.71.117.58/22**.
- Prywatny adres IP routera/UTM: **192.168.30.1/24**
- Adres drukarki: **192.168.30.20/24**
- Adres punktu dostępowego: **192.168.30.19/24**
- Zakres adresów przypisywanych urządzeniom przez serwer DHCP:
192.168.30.100-192.168.30.200
- Suffix DNS sieci: **serba.local**
- Adres serwera DNS: **192.168.30.2**
- Rezerwowany adres serwera DNS: **192.168.30.3**
- Nazwa domeny Active Directory: **serba.local**
- Adres FQDN pierwszego kontrolera domeny oraz pierwszego serwera RADIUS:
dc1.serba.local
- Adres IP pierwszego kontrolera domeny oraz pierwszego serwera RADIUS:
192.168.30.2
- Adres FQDN drugiego kontrolera domeny oraz drugiego serwera RADIUS:
dc2.serba.local
- Adres IP drugiego kontrolera domeny oraz drugiego serwera RADIUS:
192.168.30.3
- Adres FQDN serwera Exchange w sieci prywatnej: **exchange.serba.local**
- Adres FQDN serwera Exchange w sieci publicznej: **mail.serba.website**
- Adres IP serwera Exchange: **192.168.30.7**
- Adres FQDN hipernadzorcy: **vhost1.serba.local**
- Adres IP hipernadzorcy: **192.168.30.18**
- Adres FQDN serwera plików: **qnap.serba.local**
- Adres IP serwera plików: **192.168.30.8**
- Adres FQDN przełącznika zarządzalnego: **netgear.serba.local**
- Adres IP przełącznika zarządzalnego: **192.168.30.254**

- Domena dla adresów mailowych użytkowników domeny: **serba.website**

Rezerwowany serwer pocztowy został przedstawiony w projekcie jako przykład możliwego potencjalnej rozbudowy infrastruktury i nie został wzięty pod uwagę w realizacji projektu. Kontrolery domeny pełnią rolę serwerów DNS. W przypadku zapytań DNS o domeny spoza stref DNS domeny serba.local zapytania są przekierowywane dalej do serwerów w kolejności: **9.9.9.9, 1.1.1.1**.

3.5. Instalacja systemu - wstępne przygotowanie

Początkowym etapem jest skonfigurowanie serwera w sposób pozwalający na instalację systemu operacyjnego i późniejsze jego uruchamianie. Niezbędne rzeczy, o które należy zadbać to konfiguracja przestrzeni dyskowej (najlepiej takiej, która posiada redundancję dysków w postaci RAID). Konfiguracja ma zakładać stworzenie przestrzeni w postaci partycji dla systemu operacyjnego oraz przestrzeni dla danych maszyn wirtualnych. W kwestii serwera należy rozpatrzyć kwestię czy serwer posiada oprogramowanie układowe BIOS czy UEFI. W przypadku posiadania BIOS serwer nie będzie w stanie rozpocząć procesu uruchamiania systemu operacyjnego ze względu na ograniczenia schematu partycjonowania MBR. W BIOS system operacyjny jest uruchamiany tylko z pierwszego sektora (tzw. sektora startowego), a poważną wadą tego schematu partycjonowania jest limit wielkości tabeli partycji, który ogranicza rozmiar używanych dysków do 2 TB. W takich sytuacjach należy korzystać z mniejszych dysków w celu przechowywania systemu operacyjnego i z osobnej przestrzeni dyskowej na dane maszyn wirtualnych. W przypadku korzystania z oprogramowania układowego UEFI nie należy przejmować się tym problemem, ponieważ UEFI obsługuje dyski o teoretycznym rozmiarze to 9,4 ZB (zetabajtów). UEFI posiada funkcjonalność CSM (compatibility support mode) pozwalającą uruchamiać nośniki z systemem operacyjnym ze schematem MBR. W trybie natywnym UEFI obsługuje dyski ze schematem partycjonowania GPT. Świadomość tych różnic jest istotna, ponieważ w przypadku przygotowania nośnika instalacyjnego ze schematem partycjonowania MBR dla oprogramowania układowego

UEFI w trybie natywnym lub w przypadku korzystania ze schematu partycjonowania GPT dla oprogramowania układowego BIOS nośnik instalacyjny nie uruchomi się.

Przygotowany nośnik startowy powinien być wskazany w kolejce startowej nośników wskazany jako pierwszy, by mieć pewność, że instalator systemu operacyjnego się uruchomi. W przypadku posiadania UEFI najlepszym rozwiązaniem jest korzystanie z natywnej metody uruchamiania systemów (z użyciem dysków posiadających schemat GPT).

Ponadto, ze względu na wirtualizację serwer powinien mieć włączoną funkcję Intel VT-x (Intel Virtualization Technology) dla procesorów marki Intel lub funkcję AMD-V (AMD Virtualization) dla procesorów marki AMD.

3.6. Wdrożenie VMware ESXi

Wdrożenie te ma na celu instalację systemu hipernadzorcy (hypervisor) w celu późniejszej możliwości utworzenia maszyn wirtualnych dla serwerów pełniących rolę kontrolerów domeny, serwera RADIUS oraz serwera Exchange. Początkowym elementem wdrożenia jest pobranie obrazów ISO ze strony vmware.com. Następnie należy przygotować nośnik typu płyta CD/DVD lub pendrive oraz wgrać obraz instalacyjny z użyciem narzędzi typu Rufus¹³ w zależności od konfiguracji serwera (biorąc pod uwagę sugestie z punktu 3.6). Po uruchomieniu instalatora należy zaakceptować warunki licencyjne, wskazać nośnik przeznaczony na system operacyjny, wybrać polski układ klawiatury, dwukrotnie podać hasło do konta *root* (konto do zarządzania systemem operacyjnym ESXi) oraz zatwierdzić wybór. Po wykonaniu wyżej wymienionych czynności system operacyjny zostanie zainstalowany. Po instalacji należy uruchomić serwer ponownie. Po wyłączeniu się systemu instalacyjnego należy odpiąć nośnik instalacyjny z serwera.

¹³ Rufus <https://rufus.ie/>

3.7. Konfiguracja VMware ESXi

Po uruchomieniu systemu należy skonfigurować jego kartę/karty sieciowe w celu pracy z siecią lokalną. Najistotniejszą kartą, którą należy skonfigurować jest karta do zarządzania hostem. Dzięki niej można zarządzać systemem za pomocą interfejsu vSphere Web Client. W celu zmiany konfiguracji początkowej ESXi należy zalogować się za pomocą konta root do serwera przez konsolę wyświetlającą się po podłączeniu monitora do serwera, z wykorzystaniem klawiatury. Po zalogowaniu należy zmienić następujące elementy:

- Nazwa hosta,
- Suffix DNS,
- Adres IP, maska podsieci oraz adres bramy domyślnej dla karty do zarządzania serwerem,
- Adresy serwerów DNS (adresy IP kontrolerów domeny, które jeszcze nie są utworzone),
- Wyłączyć obsługę IPv6.

Po wykonaniu zmian dalsza konfiguracja jest wykonywana przez vSphere Web Client z użyciem dowolnej przeglądarki internetowej. Wyłączenie obsługi IPv6 spowoduje także restart systemu operacyjnego. Następnie należy stworzyć tzw. *datastore*, czyli przestrzeń na przechowywanie maszyn wirtualnych.

Po stworzeniu datastore i sieci dla danych należy utworzyć maszyny wirtualne dla poszczególnych maszyn z następującą specyfikacją:

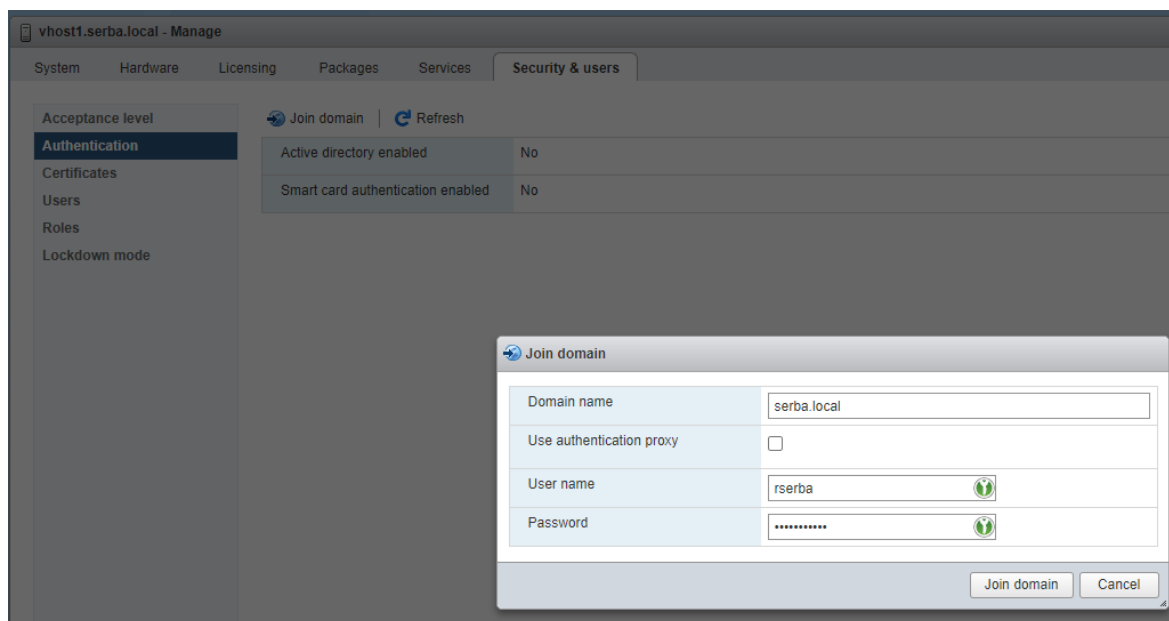
- dc1, system Microsoft Windows Server 2019, 8 GB RAM, kontroler dyskowy NVM Express (NVMe), 4 vCPU w ramach 1 procesora, dysk o rozmiarze 200 GB z włączoną opcją Thick Provision Eagerly Zeroed, karta sieciowa ze sterownikiem VMXNET3 w VM Network (domyślna nazwa sieci), oprogramowanie układowe UEFI.
- dc2, system Microsoft Windows Server 2019, 8 GB RAM, kontroler dyskowy NVM Express (NVMe), 4 vCPU w ramach 1 procesora, dysk o rozmiarze 200 GB z włączoną opcją Thick Provision Eagerly Zeroed, karta sieciowa ze sterownikiem VMXNET3 w VM Network (domyślna nazwa sieci), oprogramowanie układowe UEFI.

- exchange, system Microsoft Windows Server 2019, 24 GB RAM, kontroler dyskowy NVM Express (NVMe), 8 vCPU w ramach 1 procesora, dysk o rozmiarze 500 GB z włączoną opcją Thick Provision Eagerly Zeroed, karta sieciowa ze sterownikiem VMXNET3 w VM Network (domyślna nazwa sieci), oprogramowanie układowe UEFI.

Po skonfigurowaniu maszyn wirtualnych należy otworzyć opcje datastore i wysłać plik obrazu ISO systemu Windows Server 2019 w celu dalszej instalacji.

Gdy domena Active Directory funkcjonuje, możliwe jest zintegrowanie logowania w celu umożliwienia logowania kontem w domenę AD. W tym celu należy zmienić ustawienie **Host > Manage > System > Advanced settings** oraz zmienić zmienną **Config.HostAgent.plugins.hostsvc.esxAdminsGroup**. Ustawienie to definiuje grupę w domenie Active Directory, która ma uprawnienia do logowania i zarządzania hostem ESXi, a jego domyślna wartość to **ESX Admins**. Kwestię ustawienia odpowiedniej grupy można rozwiązać na dwa sposoby: poprzez utworzenie grupy ESX Admins w domenie Active Directory i dodanie wszystkich administratorów (lub grupy **Administratorzy domeny**, jest to możliwe poprzez dziedziczenie grup) lub poprzez zmianę wartości na nazwę grupy, która aktualnie zawiera administratorów, tak jak wbudowana grupa w domenie AD o nazwie **Administratorzy domeny**.

Po zdefiniowaniu opcji należy otworzyć zakładkę Security & Users, przejść do opcji Authentication i wybrać **Join domain**, następnie podać nazwę domeny **serba.local** oraz poświadczenia konta umożliwiającego dodanie komputera (hosta ESXi) do domeny. Przykład przedstawiono na rys. 3.3.



Rys. 3.3. Dołączanie hosta ESXi do domeny Active Directory

3.8. Instalacja Windows Server 2019

Poniższe czynności dotyczą wszystkich trzech maszyn wykorzystywanych w projekcie, przedstawionych powyżej.

Po przesłaniu obrazu ISO, należy w maszynie wirtualnej wskazać plik ISO w napędzie oraz uruchomić maszynę wirtualną. Instalator uruchomi się automatycznie. W instalatorze należy wskazać język, układ klawiatury oraz kraj pochodzenia systemu jednostek wykorzystywany w systemie po instalacji, następnie należy akceptować warunki użytkowania systemu, utworzyć partycję i wskazać ją do instalacji. Po tym system zainstaluje się automatycznie. Gdy proces instalacji się zakończy, instalator poinformuje administratora o potrzebie restartu maszyny. Po wykonaniu restartu pierwsze uruchomienie systemu operacyjnego zainstalowanego na maszynie wirtualnej trwa do kilku minut. Kiedy system dokona początkowej konfiguracji, należy dwukrotnie podać hasło dla konta lokalnego Administrator. Po tym należy się zalogować na konto administratora, zainstalować narzędzia do maszyn wirtualnych VMware Tools, zmienić nazwę hosta na odpowiednią dla maszyny nawiązując do wcześniejszej rozpiski. Po wszystkim należy aktywować licencję Windows na każdej maszynie wirtualnej oraz zdefiniować nazwy hosta

na każdej maszynie wirtualnej. Po wykonaniu wszystkich czynności należy ponownie uruchomić system.

3.9. Konfiguracja kontrolerów domeny

Zanim zostaną skonfigurowane kontrolery domeny, należy skonfigurować odpowiednie adresy na kartach sieciowych maszyn wirtualnych, zgodnie z rozpiską w punkcie 3.2.1. Następnie na kontrolerach należy zainstalować funkcję Usługi domenowe Active Directory. To spowoduje instalację funkcji Serwer DNS ze względu na to, że jest to funkcja wymagana do działania domeny Active Directory.

Po instalacji funkcji na maszynie o nazwie hosta **dc1** należy uruchomić **Kreator konfiguracji usług domenowych Active Directory**. W sekcji Konfiguracja wdrażania należy wybrać opcję utworzenia nowego lasu, a następnie wskazać nazwę domeny głównej **serba.local**. Następnie należy określić nazwę NetBIOS domeny – w tym przypadku jest to **SERBA**. Następnie należy zdefiniować hasło DSRM (Directory Services Restore Mode), które może być potrzebne w przypadku przywracania domeny z kopii zapasowej w przypadku awarii. Następnie należy zatwierdzić ustawienia – rozpocznie to proces weryfikacji konfiguracji serwera, po czym w przypadku powodzenia rozpocznie proces konfiguracji domeny. Po zakończeniu system uruchomi się ponownie. Po uruchomieniu domena będzie funkcjonowała, a host **dc1** od tego momentu stał się kontrolerem domeny **serba.local**.

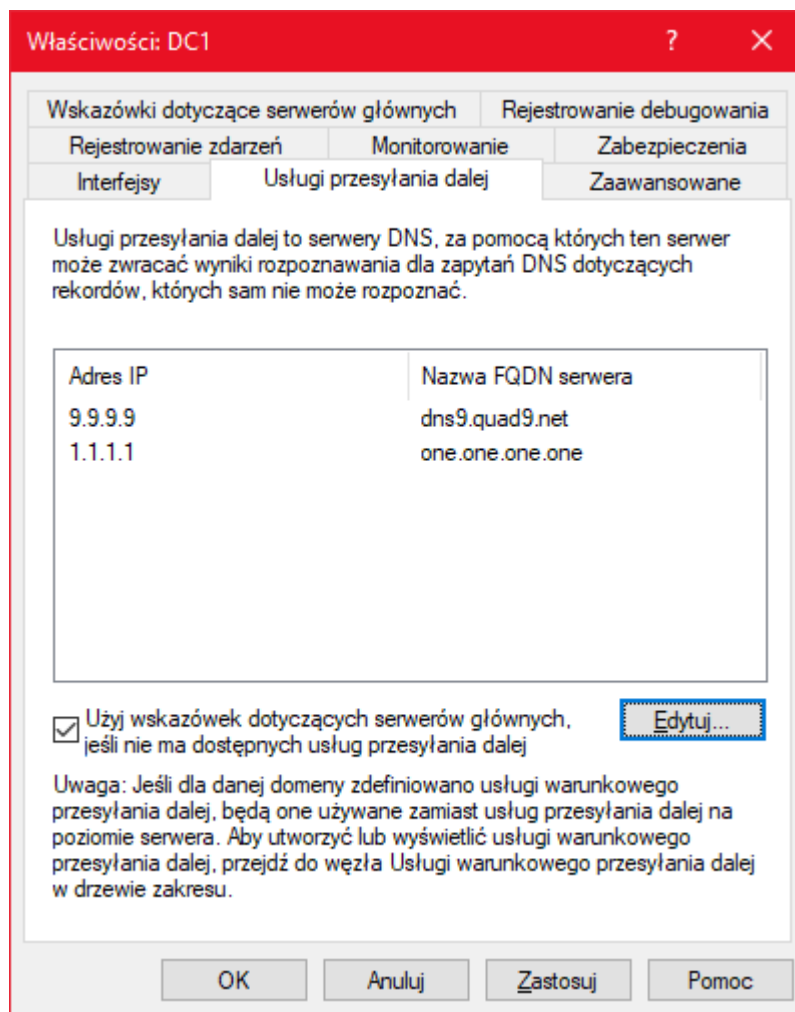
Host **dc2** musi być członkiem domeny, by promocja serwera do kontrolera domeny była możliwa, dlatego najpierw należy upewnić się, że serwer DNS skonfigurowany na karcie sieciowej to adres IP hosta **dc1**. Dzięki temu host **dc2** będzie w stanie rozwiązać nazwy z domeny **serba.local**, dzięki czemu podłączenie do domeny będzie możliwe. Po skonfigurowaniu serwera DNS należy w ustawieniach komputera zmienić ustawienie dotyczące pracy w grupie roboczej na pracę w domenie oraz wskazać domenę **serba.local**. Po zatwierdzeniu należy podać uprawnienia konta użytkownika posiadającego uprawnienia do dodawania komputerów do domeny Active Directory (zaleca się użycie konta **Administrator@serba.local** ze względu na pełne uprawnienia w tym zakresie).

Następnie należy uruchomić **Kreator konfiguracji usług domenowych Active Directory** na maszynie hosta dc2. W przypadku hosta dc2 należy w sekcji Konfiguracja wdrażania wybrać opcję Dodaj kontroler domeny do istniejącej domeny, a następnie podać nazwę użytkownika, która ma prawa do administracji domeną Active Directory. Zaleca się do tego wykorzystanie konta **Administrator@serba.local** ze względu na to, że to wbudowane konto administracyjne w domenie Active Directory posiadające pełne uprawnienia do wszystkich segmentów domeny. Następnie, podobnie jak w przypadku hosta dc1 należy określić hasło DSRM, potem określić sposób replikacji wszystkich obiektów z pierwszego kontrolera domeny (opcje można pozostawić bez zmian, ponieważ domyślnie kreator wskaże dowolny kontroler domeny funkcjonujący w domenie w momencie, kiedy funkcjonuje tylko jeden) i zatwierdzić ustawienia. Kreator zweryfikuje ustawienia hosta i po weryfikacji rozpocznie proces wdrażania drugiego kontrolera domeny. Po wykonaniu prac instalacyjnych kreator uruchomi system ponownie i po uruchomieniu proces wdrażania nowego kontrolera się zakończy.

Po wykonaniu czynności należy zmienić ustawienia serwerów DNS w kartach sieciowych kontrolerów domeny tak, aby kontroler domeny w pierwszej kolejności kierował zapytania do samego siebie, a w przypadku nieudanego rozwiązania nazwy kierował zapytania do innego kontrolera domeny. Odnosząc się do adresacji sieciowej podanej w punkcie 3.2.1. Konfiguracja powinna wyglądać następująco:

- Host dc1:
 - Preferowany serwer DNS: **127.0.0.1**
 - Alternatywny serwer DNS: **192.168.30.3**
- Host dc2:
 - Preferowany serwer DNS: **127.0.0.1**
 - Alternatywny serwer DNS: **192.168.30.2**

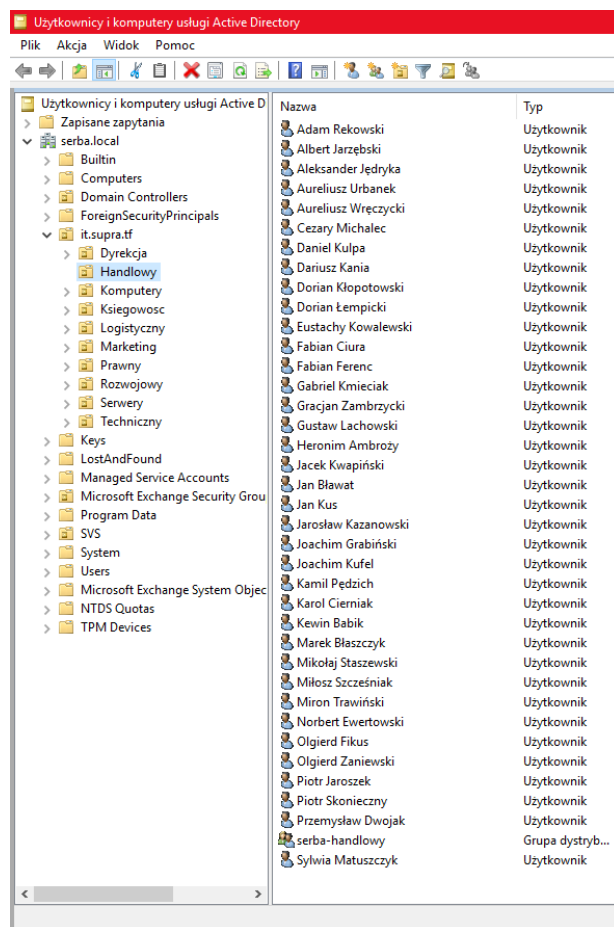
Ponadto serwery powinny mieć skonfigurowaną usługę przekazywania dalej w taki sposób, by przekazywać zapytania, których nie można rozwiązać na adresy 9.9.9.9 oraz 1.1.1.1. Rys. 3.4. przedstawia docelową konfigurację.



Rys. 3.4. Docelowa konfiguracja usług przekazywania dalej serwera DNS dla kontrolerów domeny

Następnie należy utworzyć konta użytkowników oraz schemat jednostki organizacyjnej. Konta użytkowników jak i jednostki organizacyjne można tworzyć ręcznie w przystawce **Użytkownicy i komputery usługi Active Directory** ręcznie lub tworząc je za pomocą skryptu PowerShell z plikiem CSV (comma separated values, pol. wartości oddzielone przecinkiem). Skrypt wykorzystywany do utworzenia schematu i kont został przedstawiony w załączniku 1. Potrzebny dla skryptu CSV zamieszczono w załączniku 2 (plik został skrócony ze względu na jego długość, fragment ma na celu przedstawienie schematu pliku).

Na rys. 3.5 przedstawiono przykład wdrożonej domeny z utworzonymi jednostkami organizacyjnymi oraz użytkownikami:



Rys. 3.5. Docelowa konfiguracja schematu organizacji w domenę Active Directory

Ze względu na bezpieczeństwo komunikacji pomiędzy kontrolerami domen a klientami na serwerze dc1 został zainstalowany główny urząd certyfikacji poprzez instalację oraz konfigurację roli **Usługi certyfikatów Active Directory** z komponentami: **Urząd certyfikacji, Rejestracja w sieci Web dla urzędu certyfikacji**. Urząd certyfikacji został nazwany „serba-DC1-CA”. Utworzenie urzędu certyfikacji automatycznie wygenerowało certyfikaty dla kontrolerów domeny, umożliwiając komunikację z kontrolerami domeny za pomocą LDAPS (LDAP over SSL) lub LDAP over STARTTLS jednocześnie pozwalając uniknąć nieszyfrowanej komunikacji.

3.10. Konfiguracja FortiGate wraz z integracją z domeną Active Directory

Integracja FortiGate z domeną Active Directory wymaga utworzenia konta pozwalającego dla FortiGate na wykonywanie zapytań do bazy LDAP pozwalających na wyświetlanie użytkowników i przypisywanie do nich uprawnień, dzięki czemu możliwe jest:

- logowanie do interfejsu konfiguracyjnego urządzenia,
- logowanie do usługi VPN za pomocą klienta FortiClient VPN,
- realizowanie polityk zapory sieciowej oparte o obiekty w domenie Active Directory (bazowane na grupach użytkowników oraz na użytkownikach).

Na urządzeniu został zainstalowany certyfikat głównego urzędu certyfikacji **serba-DC1-CA**, nazywający się w konfiguracji jako **SERBA-CA**.

W ramach projektu zostało utworzone konto o nazwie **fsso**. Następnie w FortiGate zdefiniowano następujący profil LDAP w ustawieniach **User & Authentication > LDAP Servers**:

- Name (nazwa): **serba.local**
- Server IP/Name (adres FQDN (Fully Qualified Domain Name) serwera LDAP):
dc1.serba.local
- Server Port (port serwera LDAP): **389**
- Common Name Identifier (identyfikator nazwy użytkownika): **sAMAccountName**
- Distinguished Name (notacja X.500): **DC=serba,DC=local**
- Bind Type (sposób łączenia): **Regular**
- Username (nazwa użytkownika): **SERBA\fsso**
- Password (hasło): podano zdefiniowane hasło dla użytkownika
- Protocol (protokół): **STARTTLS** (LDAP over STARTTLS)
- Certificate (certyfikat): **SERBA-CA**.

Konfiguracja została przedstawiona na rys. 3.6.

Ponadto w wierszu poleceń urządzenia FortiGate dodano wskazanie na drugi kontroler domeny za pomocą poleceń:

- `config user ldap,`

- edit serba.local,
- set secondary-server dc2.serba.local,
- end.

FortiWiFi 60E anzena-forti

Dashboard > Edit LDAP Server

Security Fabric >

Network >

System >

Policy & Objects >

Security Profiles >

VPN >

User & Authentication >

User Definition

User Groups

Guest Management

LDAP Servers ☆

RADIUS Servers

Authentication Settings

FortiTokens

PKI

WiFi & Switch Controller >

Log & Report >

Name: serba.local

Server IP/Name: dc1.serba.local

Server Port: 389

Common Name Identifier: sAMAccountName

Distinguished Name: DC=serba,DC=local Browse

Exchange server: ☐

Bind Type: Simple Anonymous Regular

Username: SERBA\fsso

Password: Change

Secure Connection: ☒

Protocol: STARTTLS LDAPS

Certificate: SERBA-CA

Connection status: ✔ Successful

Test Connectivity

Test User Credentials

Rys. 3.6. Docelowa konfiguracja profilu LDAP w FortiGate

Kolejnym krokiem było zdefiniowanie w ustawieniach serwera DNS FortiGate - **Network > DNS** następujących adresów serwerów:

- Primary DNS Server: **192.168.30.2**
- Secondary DNS Server: **192.168.30.3**
- Local Domain Name: **serba.local**

Następnie dodano obiekt grupy **domain_admins_ldap** wskazujący na grupę **Domain Admins** (*Administratorzy domeny*) w domenie Active Directory, a potem ustawiono dostęp administracyjny dla kont w grupie **Domain Admins** w domenie Active Directory. W ten sposób umożliwiono logowanie się na urządzenie w celu zmiany konfiguracji z użyciem kont domenowych i kont lokalnych urządzenia.

W celu umożliwienia logowania do sieci firmowej poprzez serwer VPN utworzono grupę **domain_users_ldap** bazującą na grupie **Pracownicy serba.local** zawierającą wszystkich użytkowników organizacji, a następnie przypisano tę grupę w profilu SSL-VPN

o nazwie **user-access**. Profil ten ma włączony dostęp do sieci w trybie tunelowym z włączoną opcją split-tunneling ze wskazaniem na sieć 192.168.30.0/24, DNS split tunneling z wskazaniem dla domeny **serba.local** na adresy serwerów DNS **192.168.30.2** oraz **192.168.30.3**. Ponadto w ramach ustawień tunelu VPN wskazano te same adresy DNS, co w ustawieniach DNS split-tunneling.

3.11. Instalacja Exchange 2019

Instalacja serwera pocztowego Exchange 2019 jest wykonywana na maszynie wirtualnej o nazwie **exchange**. Zanim instalacja zostanie rozpoczęta, należy upewnić się, że system posiada zainstalowane wszystkie aktualizacje, następnie należy podłączyć system do domeny, podobnie jak w przypadku kontrolerów domeny i stacji klienckich. Następnie należy zainstalować pakiety instalacyjne dla *.NET Framework 4.8*, *Visual C++ Redistributable Package for Visual Studio 2012* i *Microsoft Unified Communications Managed API 4.0*¹⁴. Następnie należy zainstalować narzędzia administracyjne RSAT (Remote Server Administration Tools) oraz wszystkie potrzebne zależności z użyciem polecenia znajdującego się na rys. 3.7. w PowerShell z uprawnieniami administratora. Po zainstalowaniu należy ponownie upewnić się, że wszystkie aktualizacje systemu są zainstalowane.

```
Install-WindowsFeature Server-Media-Foundation, NET-Framework-45-Features, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-Clustering-CmdInterface, RSAT-Clustering-Mgmt, RSAT-Clustering-PowerShell, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-Auth, Web-Digest-Auth, Web-DirBrowsing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-HttpTracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console, Web-Metabase, Web-MgmtConsole, Web-Mgmt-Service, Web-Net-Ext45, Web-Request-Monitor, Web-Server, Web-StaticCompression, Web-Static-Content, Web-Windows-Auth, Web-WMI, Windows-Identity-Foundation, RSAT-ADDS
```

Rys. 3.7. Polecenie instalujące zależności systemowe dla Exchange 2019

¹⁴ Exchange Server prerequisites <https://docs.microsoft.com/en-us/exchange/plan-and-deploy/prerequisites?view=exchserver-2019>

Następnie należy zaaktualizować schemat Active Directory o pola, które są potrzebne do funkcjonowania Exchange 2019 podłączając nośnik instalacyjny oraz w PowerShell z uprawnieniami administratora, znajdując się w lokalizacji nośnika instalacyjnego wykonać polecenia znajdujące się na rys. 3.8.

```
.\Setup.exe /IAcceptExchangeServerLicenseTerms /PrepareSchema  
.\Setup.exe /IAcceptExchangeServerLicenseTerms /PrepareAD  
/OrganizationName "serba"  
.\Setup.exe /IAcceptExchangeServerLicenseTerms /PrepareAllDomains
```

Rys. 3.8. Polecenia przygotowujące schemat, domenę i organizację do instalacji Exchange 2019

Po wykonaniu poleceń należy uruchomić instalator, sprawdzić w instalatorze, czy są dostępne aktualizacje Exchange 2019 i przejść do dalszego etapu. W instalatorze powinno się w dalszych krokach zaakceptować warunki użytkowania Exchange 2019, wybrać opcję rekomendowanych ustawień Exchange. W opcjach Server Role Selection trzeba zaznaczyć rolę **Mailbox role**, która zaznaczy automatycznie Management tools. Ponadto, należy zaznaczyć opcję **Automatically install Windows Server roles and features that are required to install Exchange Server** po to, by w razie potrzeby instalator mógł doinstalować dodatkowe role serwera. Potem istnieje możliwość zmiany lokalizacji katalogu instalacyjnego serwera, aczkolwiek zaleca się zostawienie go w domyślnym ustawieniu. Jest też możliwe włączenie ochrony przed malware, co jest wbudowaną opcją Exchange (domyślnie zaznaczona opcja to **No**, która nie uruchamia skanowania) – wybór zaleca się bazować na tym, czy serwer ma mieć w przyszłości oprogramowanie antywirusowe. Jeśli nie – zaleca się zaznaczyć opcję **Yes**, w innym wypadku zaleca się zostawić opcję **No**.

Po zatwierdzeniu opcji Instalator rozpocznie sprawdzanie zgodności systemu oraz domeny z wymaganiami instalacyjnymi i w przypadku problemów poinformuje o potencjalnych nieprawidłowościach. W przypadku braku przeciwwskazań instalator rozpocznie proces instalacji serwera. Po zainstalowaniu serwera należy zamknąć kreator. W wyniku wykonania powyższych czynności serwer Exchange 2019 został zainstalowany.

3.12. Konfiguracja Exchange 2019

Przed rozpoczęciem konfiguracji Exchange należy zapewnić odpowiednio sposób rozwiązywania nazw dla serwera w celu prawidłowego działania:

- **exchange.serba.local** powinna być rozwiązywana przez serwery DNS w sieci lokalnej tak, aby wskazywała na adres **192.168.30.7**,
- domena **serba.website** powinna posiadać następujące wpisy:
 - wpis **A** o nazwie **serba.website** i zawartości **89.71.117.58**,
 - wpis **CNAME** o nazwie **mail.serba.website** i zawartości **serba.website**,
 - wpis **CNAME** o nazwie **autoconfig.serba.website** i zawartości **mail.serba.website**,
 - wpis **CNAME** o nazwie **webmail.serba.website** i zawartości **mail.serba.website**,
 - wpis **CNAME** o nazwie **autodiscover.serba.website** i zawartości **mail.serba.website**,
 - wpis **MX** o nazwie **serba.website** i zawartości **mail.serba.website**,
 - wpis **SRV** o nazwie **_autodiscover._tcp** i zawartości **0 0 443 serba.website**,
 - wpis **SRV** o nazwie **_imaps._tcp** i zawartości **0 0 993 serba.website**,
 - wpis **SRV** o nazwie **_submission._tcp** i zawartości **0 0 465 serba.website¹⁵**,
 - wpis **TXT** o nazwie **serba.website** i zawartości **v=spf1 include:_spf.google.com ~all**.

Przykład konfiguracji wpisów DNS w domenie **serba.website** został przedstawiony na rys. 3.9.

Pierwszym etapem konfiguracji jest zmiana nazwy bazy danych Exchange. Serwer Exchange może być zarządzany przez interfejs ECP (Exchange Control Panel). Używa się ten interfejs poprzez przeglądarkę internetową, otwierając stronę **<nazwa-hosta>/ecp**, na przykład <https://exchange.serba.local/ecp> lub <https://mail.serba.website/ecp>. Domyślnie wyłącznym użytkownikiem, który ma prawa administracyjne jest konto **serba/administrator** i takim należy się zalogować.

Nazwę bazy danych trzeba zmienić w ustawieniach serwera, w zakładce **bazy danych**. Po zmianie w zakładce serwery należy aktywować licencję dla serwera Exchange 2019. Po podaniu klucza należy zrestartować usługę **Microsoft Exchange Information Store** z przystawki **Usługi**.

¹⁵ Use of SRV Records for Locating Email Submission/Access Services <https://tools.ietf.org/html/rfc6186>

DNS management for **serba.website**

[+ Add record](#) [Advanced](#)

Type	Name	Content	TTL	Proxy status	
A	serba.website	89.71.117.58	Auto	DNS only	Edit ▶
A	www	89.71.117.58	Auto	DNS only	Edit ▶
CNAME	autoconfig	mailconfig.ovh.net	Auto	DNS only	Edit ▶
CNAME	autodiscover	mailconfig.ovh.net	Auto	DNS only	Edit ▶
CNAME	ftp	serba.website	Auto	DNS only	Edit ▶
CNAME	imap	serba.website	Auto	DNS only	Edit ▶
CNAME	mail	serba.website	Auto	DNS only	Edit ▶
CNAME	pop3	serba.website	Auto	DNS only	Edit ▶
CNAME	smtp	serba.website	Auto	DNS only	Edit ▶
CNAME	webmail	serba.website	Auto	DNS only	Edit ▶
MX	serba.website	mail.serba.website	Auto	DNS only	Edit ▶
SRV	_autodiscover._tcp	0 0 443 serba.website	Auto	DNS only	Edit ▶
SRV	_imaps._tcp	0 0 993 serba.website	Auto	DNS only	Edit ▶
SRV	_submission._tcp	0 0 465 serba.website	Auto	DNS only	Edit ▶
TXT	serba.website	MS=ms15735587	1 hr	DNS only	Edit ▶
TXT	serba.website	v=spf1 include:_spf.google.com ~...	Auto	DNS only	Edit ▶

Rys. 3.9. Konfiguracja strefy DNS dla nazwy *serba.website*

Kolejnym etapem konfiguracji jest utworzenie tzw. *łącznik Send*. Umożliwia on wysyłanie wiadomości przez serwer Exchange do adresatów. W tym celu należy przejść do sekcji **przepływ poczty e-mail**, zakładki **łączniki Send**. Zaleca się zdefiniować connector o następujących danych:

- Nazwa: **outbound to internet**
- Typ: **Internet (na przykład do wysyłania poczty internetowej)**
- Ustawienia sieci: Rekord MX skojarzony z domeną adresata
- Przestrzeń adresowa:
 - Typ: **SMTP**
 - Domena: *****
 - Koszt: **1**
- Serwer źródłowy:
 - Serwer: **EXCHANGE**
 - Witryna: **serba.local/Configuration/Sites/SERBA-Headquarters**
 - Rola: **Mailbox**

Kolejnym istotnym etapem jest konfiguracja wirtualnych katalogów.

Domyślnie one prowadzą do localhost lub lokalnego FQDN serwera (w tym projekcie **exchange.serba.local**) i ze względu na dostępność hosta w sieci oraz wystawienie certyfikatów w celu wygodnego dostępu dla użytkowników (bez ostrzeżeń o niezaufanych certyfikatach) należy zmienić poniższe adresy. Adresem docelowym jest **webmail.serba.website**. Poniżej przedstawiono krótki skrypt na rys. 3.10., który zmienia ścieżki dla:

- OWA (Outlook Web Access),
- ECP Virtual Directory,
- Outlook Anywhere,
- ActiveSync,
- Exchange Web Services,
- OAB (Offline Address Book),
- Client Access Service,
- MAPI (Messaging Application Program Interface).

```
$namespace = "webmail.serba.website"
Set-OwaVirtualDirectory -Identity "EXCHANGE\OWA (Default Web Site)" -
ExternalUrl https://$namespace/owa -InternalUrl https://$namespace/owa
Set-EcpVirtualDirectory -Identity "HOSTNAME\ECP (Default Web Site)" -
ExternalUrl
Set-EcpVirtualDirectory -Identity "EXCHANGE\ECP (Default Web Site)" -
ExternalUrl https://$namespace/ecp -InternalUrl https://$namespace/ecp
Set-OutlookAnywhere -Identity "EXCHANGE\RPC (Default Web Site)" -
ExternalHostname $namespace -InternalHostname $namespace -
ExternalClientsRequireSsl $true -InternalClientsRequireSsl $true -
DefaultAuthenticationMethod NTLM
Set-ActiveSyncVirtualDirectory -Identity "HOSTNAME\Microsoft-Server-
ActiveSync (Default Web Site)" -ExternalUrl https://$namespace/Microsoft-
Server-ActiveSync -InternalUrl https://$namespace/Microsoft-Server-
ActiveSync
Set-WebServicesVirtualDirectory -Identity "EXCHANGE\EWS (Default Web
Site)" -ExternalUrl https://$namespace/EWS/Exchange.asmx -InternalUrl
https://$namespace/EWS/Exchange.asmx
Set-OabVirtualDirectory -Identity "EXCHANGE\OAB (Default Web Site)" -
ExternalUrl https://$namespace/OAB -InternalUrl https://$namespace/OAB
Set-ClientAccessService -Identity "EXCHANGE" -
AutoDiscoverServiceInternalUri
"https://autodiscover.serba.website/Autodiscover/Autodiscover.xml"
Set-MapiVirtualDirectory -Identity "EXCHANGE\mapi (Default Web Site)" -
ExternalUrl https://$namespace/mapi -InternalUrl https://$namespace/mapi
IISReset
```

Rys. 3.10. Skrypt zmieniający adresy wirtualnych katalogów Exchange 2019

Po zmianie wszystkich adresów należy zrestartować serwer IIS (Internet Information Services). Wspomniany skrypt wykonuje to na samym końcu. Po wykonaniu wszystkich czynności przez skrypt należy utworzyć domyślną zasadę adresów e-mail. Istnieje ona po to, by określić jakie adresy mają być wykorzystywane w wysyłce wiadomości. Politykę docelowo powinno określać się tak, by wykorzystywać adres w schemacie **alias@serba.website**. Wynika to z tego, że użytkownicy, którzy są dodawani z domeny Active Directory posiadają konta w domenie **serba.local**, dlatego prawidłowym UPN (User Principal Name) jest dla użytkownika Radosław Serba o nazwie **rserba** UPN **rserba@serba.local** zamiast **rserba@serba.website**. Polityka jest zdefiniowana tak, by wspomniany schemat był używany w wysyłkach wiadomości do wszystkich typów odbiorców (bez względu na to, czy są to użytkownicy lokalni czy zewnętrzni).

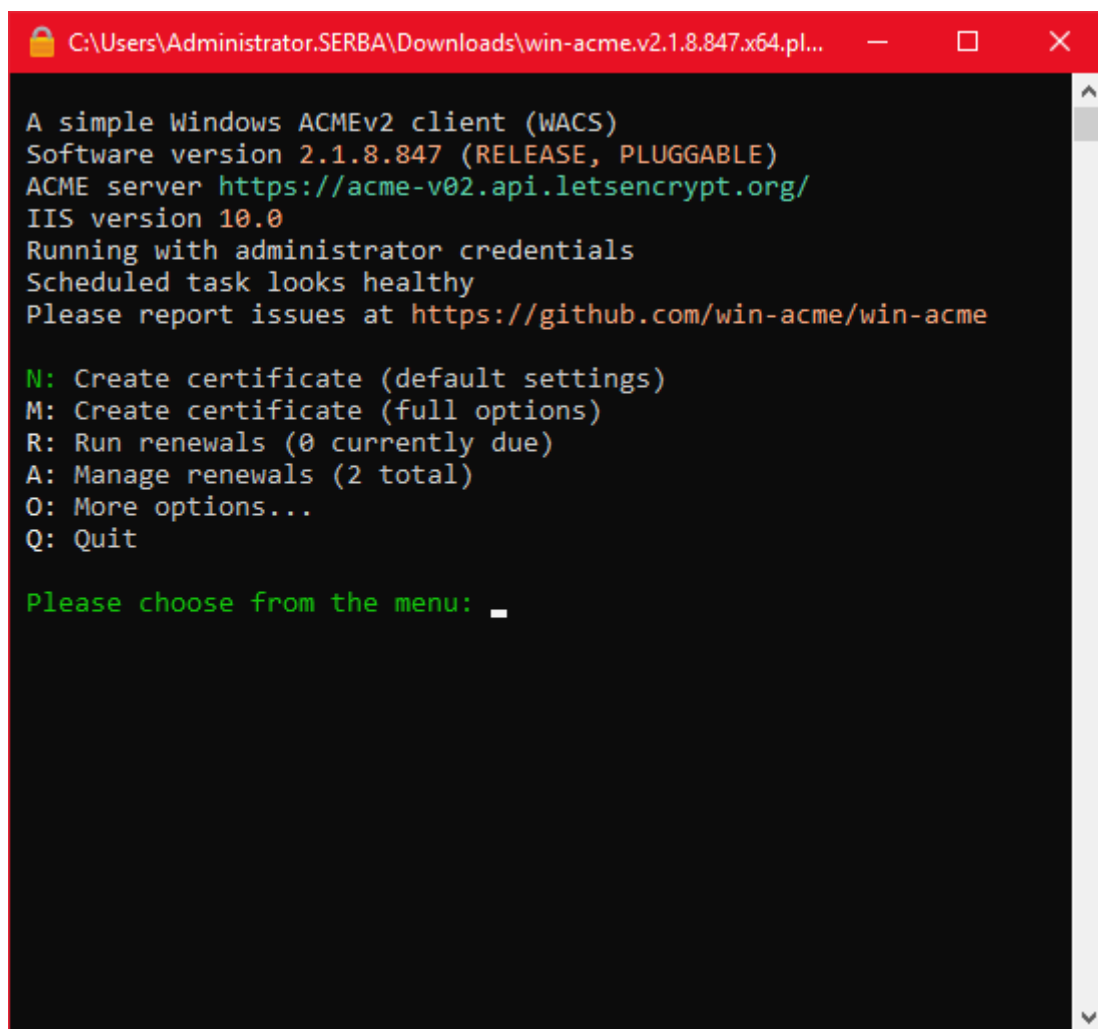
Przedostatnim etapem konfiguracji serwera Exchange jest konfiguracja certyfikatów Exchange 2019. Certyfikaty mogą być generowane przez wewnętrzny urząd certyfikacji – zaletą tego rozwiązania jest brak kosztów oraz możliwość wykorzystywania domen lokalnych, na przykład **exchange.serba.local**. W przypadku, gdy polityka bezpieczeństwa firmy nie pozwala na połączenie z serwerem pocztowym poprzez IMAP (Internet Message Access Protocol)/SMTP (Simple Mail Transfer Protocol), OWA, ActiveSync, Outlook Anywhere i podobne rozwiązania, to jest jedyne rozwiązanie. W przypadku domen publicznych problematyczne może być to, że aby komputer uznał domenę za zaufaną, ten musi mieć zaimportowany certyfikat głównego urzędu certyfikacji do odpowiedniego magazynu w magazynie certyfikatów komputera.

Gdy dostęp do wspomnianych zasobów jest dozwolony, istnieje drugie źródło certyfikatów – są to publiczne certyfikaty. Mogą one być zarówno płatne jak i bezpłatne. Jednym z bezpłatnych dostawców certyfikatów SSL (Secure Sockets Layer) jest **Let's Encrypt**. Proces otrzymywania certyfikatów upraszcza aplikacja **win-acme**¹⁶ poprzez użycie jednej z dwóch metod: HTTP-01 (Hypertext Transfer Protocol) lub DNS-01¹⁷. W ramach projektu skorzystano z metody DNS-01 ze względu na możliwość wygenerowania certyfikatu wildcard (certyfikatu odpowiadającego nazwie dowolnej subdomeny) oraz znacznie łatwiejszą obsługę (wymaga ona dostępu do interfejsu API (Application Programming Interface) podmiotu zarządzającego strefą DNS, w projekcie wykorzystano serwis **cloudflare.com**). Aplikacja automatycznie wykrywa wszystkie domeny wykorzystywane przez serwer Exchange i generuje dla nich certyfikat, instaluje go w

¹⁶ win-acme – Getting started <https://www.win-acme.com/manual/getting-started>

¹⁷ Challenge Types – Let's Encrypt <https://letsencrypt.org/docs/challenge-types/>

odpowiednich magazynach oraz restartuje usługi serwera Exchange w celu odświeżenia certyfikatów. Interfejs zarządzania aplikacją został przedstawiony na rys. 3.11.

The image shows a Windows command prompt window titled "C:\Users\Administrator.SERBA\Downloads\win-acme.v2.1.8.847.x64.pl...". The text inside the window is as follows:

```
A simple Windows ACMEv2 client (WACS)
Software version 2.1.8.847 (RELEASE, PLUGGABLE)
ACME server https://acme-v02.api.letsencrypt.org/
IIS version 10.0
Running with administrator credentials
Scheduled task looks healthy
Please report issues at https://github.com/win-acme/win-acme

N: Create certificate (default settings)
M: Create certificate (full options)
R: Run renewals (0 currently due)
A: Manage renewals (2 total)
O: More options...
Q: Quit

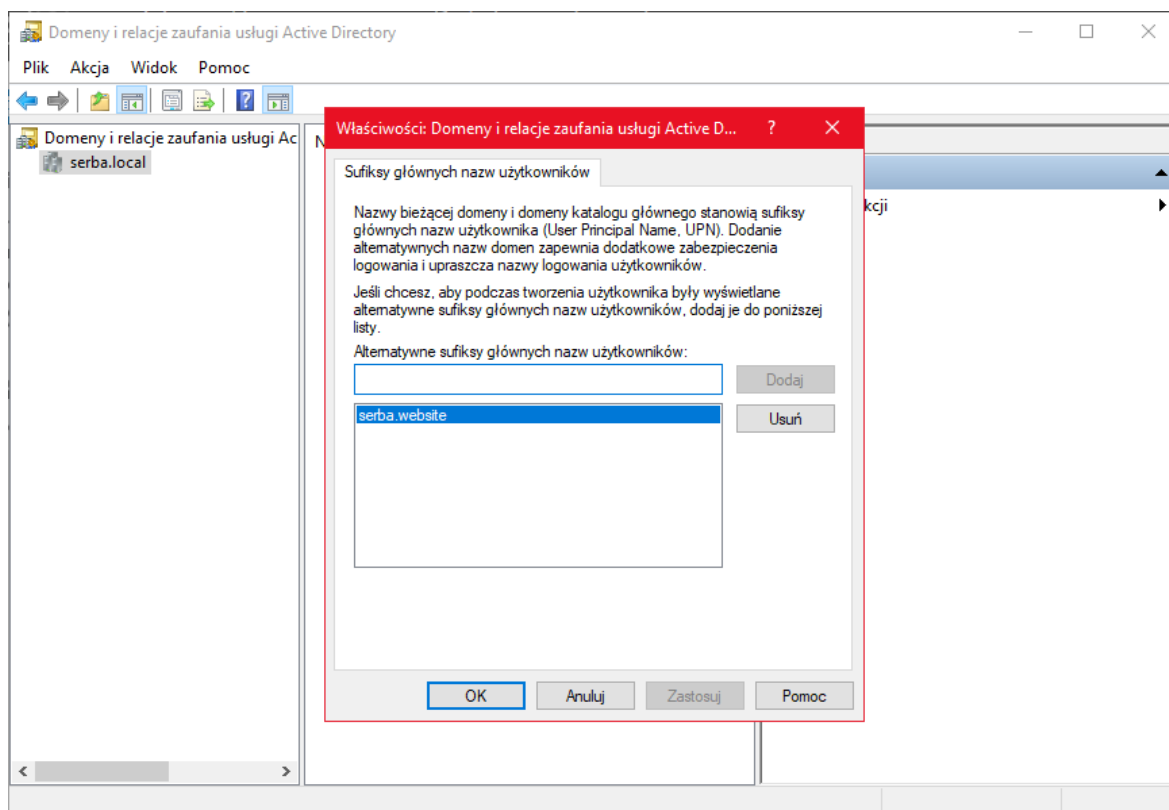
Please choose from the menu: _
```

Rys. 3.11. Interfejs konfiguracyjny win-acme

Ostatnim etapem konfiguracji jest import użytkowników z domeny Active Directory do Exchange oraz umożliwienie użytkownikom logowania się za pomocą sufiksu lokalnego jak i domenowego.

Domyślnie każdy użytkownik może się logować w ramach lokalnej domeny, lecz takie logowanie będzie możliwe tylko w środowisku lokalnym. W przypadku logowania z zewnątrz istnieje szansa, że logowanie się nie powiedzie. Z tego względu należy w opcjach **Domeny i relacje zaufania usługi Active Directory**, otwierając właściwości domeny dodać

alternatywny sufiks główny nazw użytkowników i dodać domenę **serba.website**. Przedstawiono to na rys. 3.12.



Rys. 3.12. Konfiguracja alternatywnego sufiksu głównych nazw użytkowników

W celu ułatwienia procesu tworzenia skrzynek dla użytkowników, wykorzystano skrypt, którego fragment działania znajduje się w załączniku 3. Skrypt przeszukuje całe drzewo w domenie AD **serba.local** w poszukiwaniu użytkowników, którzy pracują w firmie **it.supra.tf** (jest to jeden z parametrów konta użytkownika). Następnie dla każdego znalezionej użytkownika jest tworzona skrzynka użytkownika w Exchange 2019. Zawartość skryptu znajduje się na rys. 3.13.

```
Import-Module activedirectory
Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn

$users = Get-ADUser -Filter {company -eq "it.supra.tf"}
foreach($user in $users)
{
    Enable-Mailbox -Identity $user.SamAccountName
}
```

Rys. 3.13. Skrypt PowerShell tworzący skrzynki w Exchange 2019 na bazie kont użytkowników

W przypadku korzystania z oprogramowania antywirusowego z zaporą sieciową może być wymagane odblokowanie portów: TCP 25, 443, 465, 587 i 993. W innym wypadku instalator Exchange 2019 tworzy reguły odblokowujące ruch dla wspomnianych portów. Ponadto, w celu prawidłowego działania router powinien przekierowywać ruch z adresu WAN na wskazanych portach na adres **192.168.30.7**.

3.13. Konfiguracja RADIUS

W Windows Server rola serwera odpowiadająca serwerowi RADIUS nazywa się **Usługi zasad sieciowych i dostępu sieciowego**. Należy taką rolę zainstalować na hostach dc1 oraz dc2 wraz z narzędziami. Po instalacji należy otworzyć okno **Serwer zasad sieciowych**, a następnie w głównym elemencie drzewa (nazwa **Serwer zasad sieciowych (Lokalny)**). W ekranie głównym należy wybrać opcję konfiguracji standardowej **Serwer usługi RADIUS na potrzeby bezprzewodowych i przewodowych połączeń 802.1X**. Następnie należy wybrać typ połączeń 802.1X: **Bezpieczne połączenia przewodowe (Ethernet)** oraz określić nazwę **switch netgear**. Następnie należy dodać nowego klienta usługi RADIUS, którego przyjazną nazwę należy określić jako **netgear.serba.local**. Jeśli ten adres FQDN jest przypisany do adresu IP 192.168.30.254, możliwe jest uzupełnienie w polu Adres (IP lub DNS) wspomnianego adresu FQDN lub IP. Każdy klient RADIUS musi mieć zdefiniowany wspólny klucz tajny. W ramach testowej konfiguracji podano hasło: **1234567890**. Zaleca się używanie skomplikowanego hasła o długości 32 znaków lub więcej, lecz zanim takie hasło zostanie ustawione, zaleca się skonfigurowanie w pełni połączenia z przełącznikiem i potwierdzenia właściwej komunikacji pomiędzy przełącznikiem a serwerem RADIUS.

Następnie należy wybrać typ protokołu EAP dla ustawianej zasady: **Microsoft: Chroniony protokół EAP**. Klikając przycisk **Konfiguruj...** można potwierdzić istnienie certyfikatu, który jest wykorzystywany w komunikacji serwera RADIUS (przedstawiono to rys. 3.14). Kolejnym etapem kreatora jest zdefiniowanie grup, które powinny mieć autoryzowane w ramach komunikacji. Należy wybrać grupy **Komputery domeny** (*Domain Computers*) i **Użytkownicy domeny** (*Domain Users*). Są to wbudowane w domenę grupy zawierające wszystkie konta komputerów oraz użytkowników w całej domenie Active Directory.

Następnie należy kontynuować. Utworzy to zasadę żądań sieciowych i zasadę sieciową. Ich prawidłowa konfiguracja powoduje udaną komunikację z przełącznikiem.

Zasada żądań sieciowych powinna mieć zdefiniowane następujące parametry:

- Ogólne:
 - Typ serwera dostępu do sieci: **Nieokreślone**
- Warunki:
 - Adres IPv4 klienta dostępu: **192.168.30.254**
- Ustawienia:
 - Wszystkie ustawienia domyślne.

Zasada sieciowa powinna mieć skonfigurowane następujące parametry:

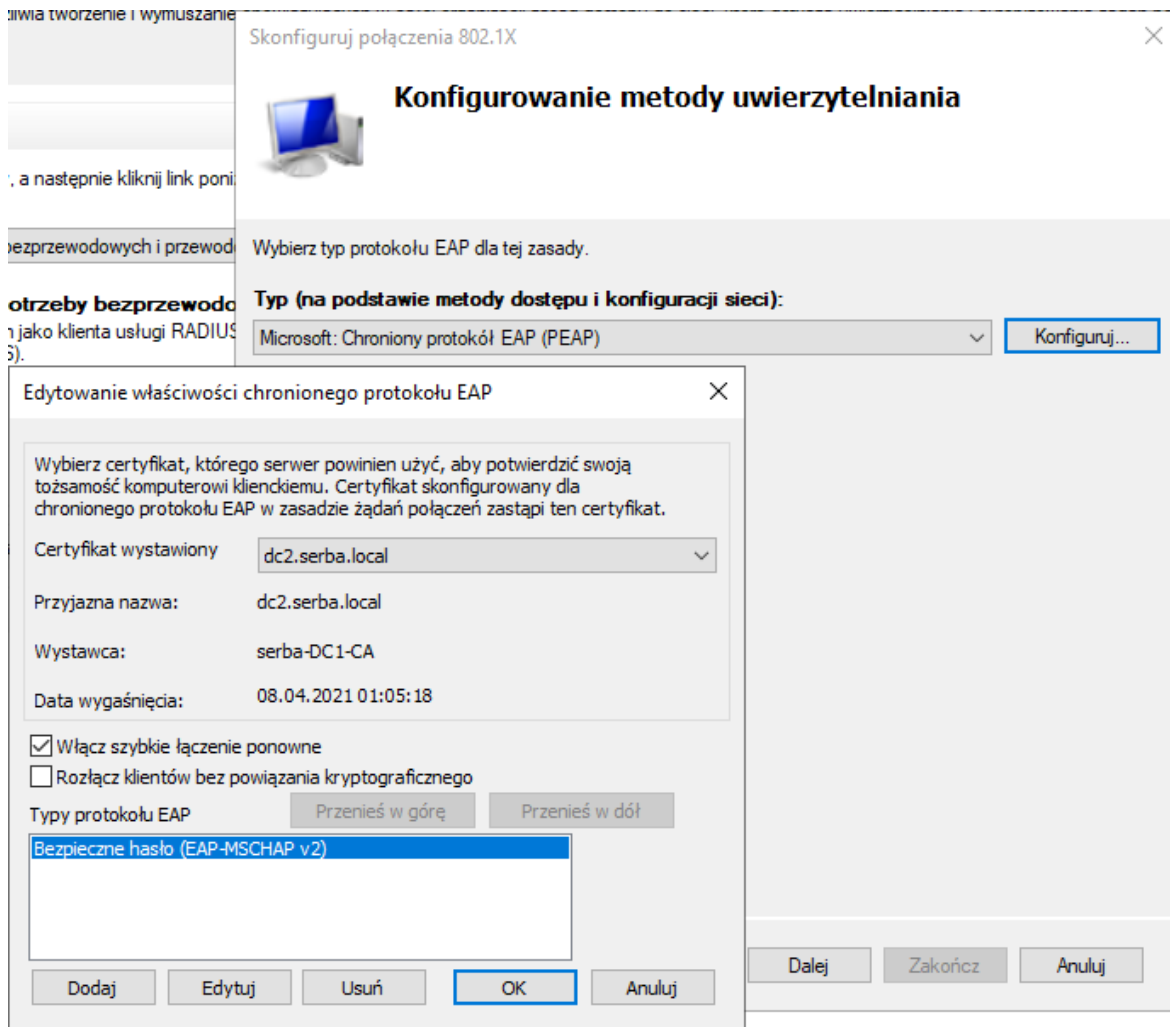
- Ogólne:
 - Typ serwera dostępu do sieci: **Nieokreślone**
 - Uprawnienie dostępu: Udziel dostępu; **udziel dostępu, jeśli żądanie połączenia jest**

zgodne z tą zasadą

- Warunki:
 - Grupy systemu Windows: **SERBA\Komputery domeny** LUB

SERBA\Użytkownicy domeny

- Ograniczenia:
 - Metody uwierzytelnienia: **Microsoft: Chroniony protokół EAP (PEAP)**
 - Ustawienia:
 - Atrybuty usługi RADIUS
- Standardowe
 - Framed-Protocol: **PPP**
 - Service-Type: **Framed**



Rys. 3.14. Konfigurowanie metody uwierzytelnienia w serwerze zasad sieciowych

Następnie należy całą konfigurację zapisać i skopiować na drugi serwer RADIUS. W tym celu należy kliknąć prawym przyciskiem myszy na główny element drzewa serwera zasad sieciowych oraz wybrać **Eksportuj konfigurację**, zapisać ją do pliku i następnie zrobić to samo na drugim serwerze RADIUS, lecz należy tam wybrać opcję **Importuj konfigurację**. Ponadto, należy odblokować komunikację w zaporze sieciowej w obu kierunkach na portach UDP 1812 i 1813. Po wykonanym imporcie konfiguracji należy zarejestrować usługi serwera w usłudze Active Directory¹⁸.

Drugim etapem konfiguracja przełącznika. Przełącznik powinien mieć skonfigurowane elementy:

¹⁸ A.Józefiok, *Security CCNA 210-260. Zostań administratorem sieci komputerowych Cisco*, Helion 2016, str. 76-89

- Adres IP do zarządzania przełącznikiem: **192.168.30.254/24**
- Adres bramy domyślnej: **192.168.30.1**
- Serwery DNS: **192.168.30.2, 192.168.30.3**
- Serwery RADIUS:
 - Adres: **dc1.serba.local**
- Port: **1812**
- Wykorzystywanie hasła: **włączone**
- Hasło: **1234567890**
 - Message Authenticator: **wyłączony**
 - Adres: **dc2.serba.local**
- Port: **1812**
- Wykorzystywanie hasła: **włączone**
- Hasło: **1234567890**
- Message Authenticator: **wyłączony**
- Dot1x Authentication List: **Radius**

Ostatnie ustawienie w przełączniku do skonfigurowania to wymuszenie autoryzacji ze wskazaniem na porty. Proces ten realizowany jest w **Security > Port Authentication > Advanced > Port Authentication**. Ustawienie definiujące autoryzację użytkownika to **Port Control**. Domyślnie ustawiona wartość to **Authorized** oznaczająca pominięcie autoryzacji urządzenia. Inne opcje to **Unauthorized**, czyli automatyczne odrzucenie autoryzacji użytkownika oraz **Auto** – ustawienie, które powoduje autoryzację urządzenia w momencie, gdy autoryzacja w przełączniku jest włączona¹⁹. Ta opcja powinna być włączona w portach, do których są podłączane komputery użytkowników końcowych. Opcja Authorized powinna być pozostawiona dla wszystkich portów, do których są podłączone urządzenia niewymagające autoryzacji (na przykład same serwery RADIUS). Dla przykładu skonfigurowano dwa pierwsze porty przełącznika w trybie automatycznym, co przedstawiono na rys. 3.15.

Po skonfigurowaniu portów należy w **Security > Port Authentication > Advanced > 802.1X Configuration** włączyć opcję **Port Based Authentication State**.

¹⁹ GS716 and GS724T Gigabit Smart Switches Software Administration Manual
https://www.downloads.netgear.com/files/GDC/GS716TV2/GS716T_GS724T-SWA-October2012.pdf, str. 194-197

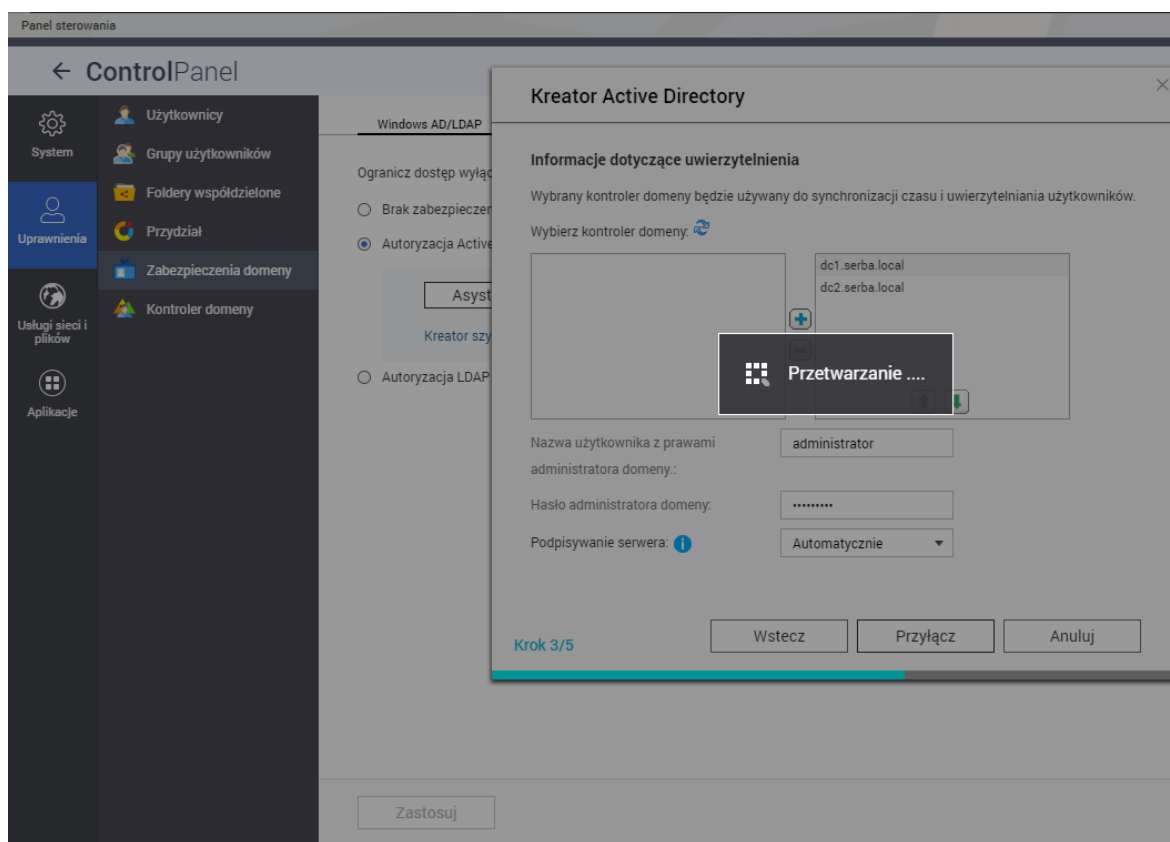
Komputery klienckie z systemem Windows posiadają usługę **Automatyczna konfiguracja sieci przewodowej** (dot3svc) wyłączoną. Należy taką usługę włączyć na wszystkich stanowiskach. Najlepszym rozwiązaniem jest skonfigurowanie polityki GPO (Group Policy Object) w oknie **Edytor zarządzania zasadami grupy**, włączając usługę **dot3svc** w trybie **Automatycznym** z zaznaczoną akcją **Uruchom usługę** w ustawieniu **Konfiguracja komputera > Preferencje > Ustawienia Panelu sterowania > Usługi**. Sposób konfiguracji został przedstawiony na rys. 3.16..

Port Authentication

:: Port Authentication						
1 All						
	Port	Port Control	Guest VLAN ID	Guest VLAN Period	Unauthenticated VLAN ID	Periodic Reauthentication
<input type="checkbox"/>		<input type="text" value="v"/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value="v"/>
<input type="checkbox"/>	g1	Auto	0	90	0	Disable
<input type="checkbox"/>	g2	Auto	0	90	0	Disable
<input type="checkbox"/>	g3	Authorized	0	90	0	Disable
<input type="checkbox"/>	g4	Authorized	0	90	0	Disable
<input type="checkbox"/>	g5	Authorized	0	90	0	Disable
<input type="checkbox"/>	g6	Authorized	0	90	0	Disable
<input type="checkbox"/>	g7	Authorized	0	90	0	Disable
<input type="checkbox"/>	g8	Authorized	0	90	0	Disable
<input type="checkbox"/>	g9	Authorized	0	90	0	Disable
<input type="checkbox"/>	g10	Authorized	0	90	0	Disable
<input type="checkbox"/>	g11	Authorized	0	90	0	Disable
<input type="checkbox"/>	g12	Authorized	0	90	0	Disable
<input type="checkbox"/>	g13	Authorized	0	90	0	Disable
<input type="checkbox"/>	g14	Authorized	0	90	0	Disable
<input type="checkbox"/>	g15	Authorized	0	90	0	Disable
<input type="checkbox"/>	g16	Authorized	0	90	0	Disable
<input type="checkbox"/>	g17	Authorized	0	90	0	Disable
<input type="checkbox"/>	g18	Authorized	0	90	0	Disable
1 All						

Rys. 3.15. Konfiguracja autoryzacji urządzeń w portach przełącznika Netgear GS716T

przestrzeń nazw domeny, następnie należy wskazać kontrolery domeny używane do synchronizacji czasu oraz uwierzytelniania użytkowników wraz z priorytetem. Ponadto, należy podać poświadczenia do konta z uprawnieniami administracyjnymi w domenie. Przykład przedstawiono na rys. 3.17. Po podłączeniu serwera plików do domeny możliwe jest określenie konkretnych jednostek organizacyjnych, które mają mieć uprawnienia do logowania w serwerze plików. Jest to opcjonalne i opcja ta nie została wykorzystana w projekcie.



Rys. 3.17. Dołączanie serwera plików QNAP do domeny Active Directory

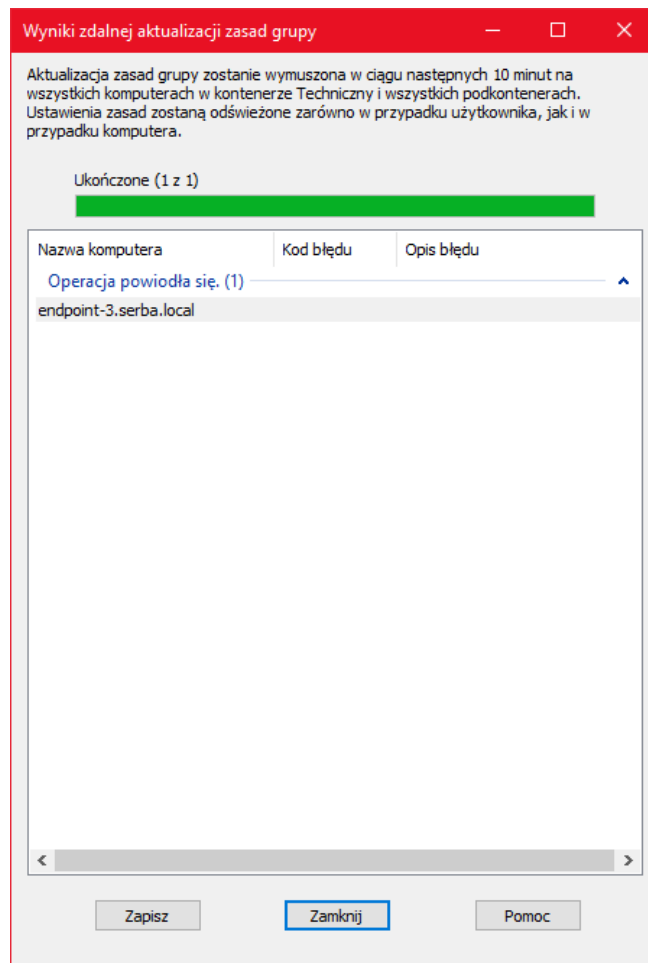
Następnie należy utworzyć folder współdzielony oraz przypisać do niego uprawnienia do odczytu i zapisu dla użytkowników będących członkami grupy **Użytkownicy domeny**. Pozwala to każdemu użytkownikowi w domenie Active Directory na dostęp do zasobu sieciowego. Utworzenie folderu jest możliwe w oknie **Panel sterowania > Uprawnienia > Foldery współdzielone > Utwórz > Folder współdzielony**. Utworzony folder nazwano **serba-public**, zatem ze względu na to, że adresem FQDN serwera plików jest **nas.serba.local**, adres udziału sieciowego to **//nas.serba.local/serba-public**.

Ostatnim etapem konfiguracji jest podłączenie zasobu sieciowego użytkownikom. Ze względu na to, że każdy użytkownik ma uprawnienia do przeglądania i modyfikowania zawartości udziału, ma też możliwość mapowania go samodzielnie. Jednakże, bardziej profesjonalne podejście zakłada automatyczne mapowanie zasobu z góry określonym użytkownikom.

W tym celu należy utworzyć obiekt GPO zawierający następujące ustawienie w sekcji Konfiguracja użytkownika > Preferencje > Ustawienia systemu Windows > Mapowania dysków. W sekcji Mapowania dysków należy utworzyć mapowanie z następującymi parametrami:

- Ogólne:
 - Akcja: **Aktualizuj**
 - Lokalizacja: **\\nas.serba.local\serba-public**
 - Połącz ponownie: **Tak**
 - Oznacz jako: **serba-public**
 - Użyj: **Q** (litera dysku przypisywana do zasobu sieciowego na komputerze docelowym)
 - Ukryj/Pokaż ten dysk: **Pokaż ten dysk**
 - Wspólne:
- Uruchom w kontekście zabezpieczeń zalogowanego użytkownika (opcja zasad użytkownika): **Tak**
- Określ wartość docelową na poziomie elementu: Jednostka organizacyjna: **OU=it.supra.tf,DC=serba,DC=local**

Po zapisaniu ustawień zmiany zaczną być stosowane do 90 minut przy założeniu, że komputery będą w stanie nawiązać połączenie z kontrolerem domeny. Wynika to ze względu na fakt pobierania zestawu polityk grup przez stacje robocze raz na 90 minut z losowym przedziałem czasowym od 0 do 30 minut. Istnieje możliwość wymuszenia aktualizacji polityk poprzez wykonanie operacji aktualizacji zasad grupy z poziomu przystawki **Zarządzanie zasadami grupy** będąc podłączonym do jednego z kontrolerów domeny lub wykonując polecenie **gpupdate /force** na stacji roboczej. Wynik aktualizacji z poziomu kontrolera domeny przedstawiono na rys. 3.18.

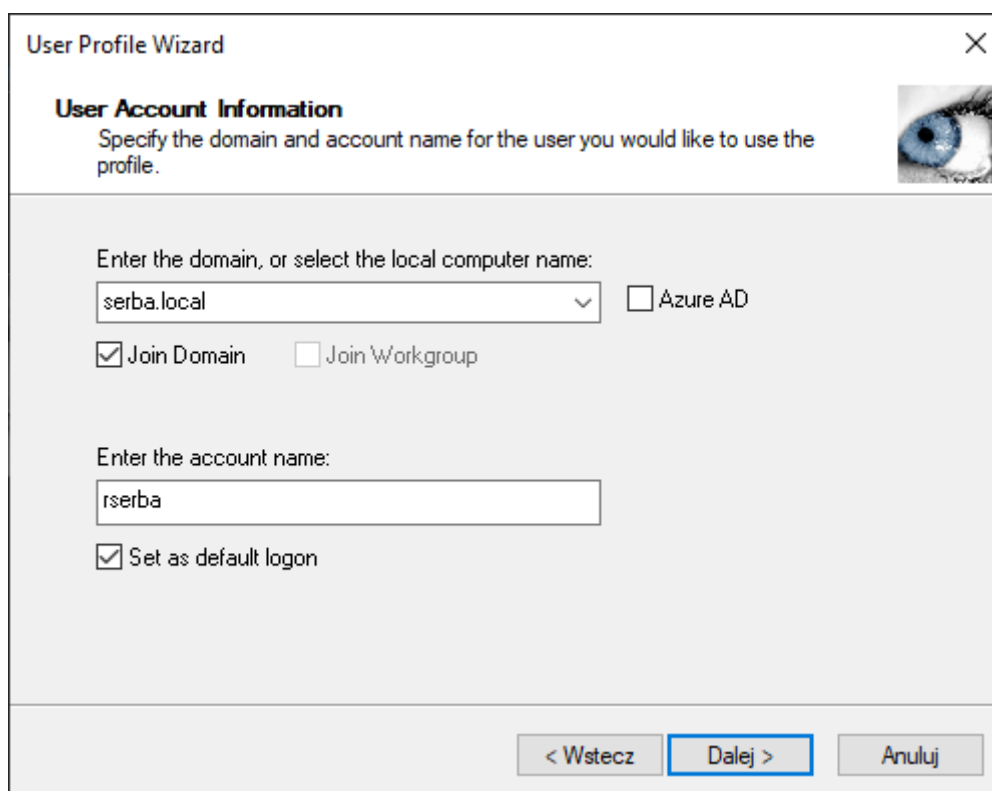


Rys. 3.18. Aktualizacja zasad grupy z poziomu kontrolera domeny

3.15. Konfiguracja stacji klienckich

Każdy komputer kliencki z zainstalowanym systemem Windows domyślnie znajduje się w grupie roboczej **WORKGROUP**. Po wykonaniu czynności konfiguracyjnych związanych z usługami serwerowymi należy podłączyć komputery do domeny. Należy wziąć pod uwagę fakt, iż w przypadku, gdy użytkownik posługiwał się komputerem, posiada on utworzony profil lokalny użytkownika. Po podłączeniu komputera do domeny nowe konto użytkownika w żaden sposób nie zostanie automatycznie zintegrowane z dotychczasowym profilem użytkownika. W dodatku, w przypadku zalogowania się użytkownika poprzez konto domenowe po raz pierwszy, zostanie utworzony nowy profil

użytkownika. Aby temu zapobiec, trzeba skorzystać z narzędzi umożliwiających transfer profili użytkowników kont lokalnych do kont domenowych. Jednym z narzędzi umożliwiających operację jest oprogramowanie **ForensiT User Profile Wizard 21**²⁰. Po zainstalowaniu i uruchomieniu programu na stacji klienckiej należy wskazać profil do migracji, podać nazwę domeny, do której ma dołączyć komputer oraz podać nazwę użytkownika, do którego ma być przypisany profil. Przykład przedstawiono na rys. 3.19.



Rys. 3.19. Dołączanie komputera do domeny wraz z migracją profilu użytkownika konta lokalnego do konta domenowego z użyciem User Profile Wizard

Po podaniu danych należy przejść do dalszego etapu kreatora, a w nim należy podać poświadczenia konta użytkownika posiadającego uprawnienia do dodawania komputerów do domeny. Następnie kreator doda komputer do domeny, przeniesie uprawnienia na wskazane konto użytkownika (jeśli istnieje) i uruchomi komputer ponownie.

²⁰ ForensiT User Profile Wizard Corporate Guide
<https://www.forensit.com/Downloads/User%20Profile%20Wizard%20Corporate%20User%20Guide.pdf>

4. Specyfikacja wewnętrzna

4.1. Początkowa konfiguracja

W sieci wewnątrz organizacji każdy użytkownik pracuje na swoim komputerze będąc członkiem grupy roboczej. W razie awarii swojego komputera pracownik kontynuuje pracę na komputerze zastępczym. Ze względu na to, że każde ze stanowisk komputerowych z osobna przechowuje bazę loginów i haseł osobno, na każdym stanowisku należy utworzyć login i hasło dla każdego pracownika. Każdy komputer ma osobną politykę haseł (pomimo tego, że w większości wypadków ustawienia polityki haseł są takie same, wymuszanie polityki jest realizowane przez każdy pecet osobno) i w przypadku wygaśnięcia hasła należy takie zmienić na każdym z komputerów z osobna. W celu konfiguracji routera należy się zalogować na lokalne konto administracyjne, gdzie także występuje osobna baza haseł i osobna polityka haseł, więc w ostatecznym rozrachunku administrator sieci jak i wszyscy użytkownicy powinni co jakiś czas zmieniać na wszystkich urządzeniach hasło tak, aby przestrzegać polityki haseł. Ze względu na to, że administrator poza standardowymi dostępnymi ma dostęp do konfiguracji sprzętu sieciowego – od niego wymaga się dodatkowych zmian haseł do kont administracyjnych. W dodatku każdy użytkownik korzysta z poczty skonfigurowanej na serwerze pocztowym będącym w Internecie lub w sieci lokalnej. Serwer pocztowy także realizuje własną politykę haseł oraz przechowuje loginy i hasła osobno. Jak można zauważyć, to powoduje jeszcze większą komplikację dla potencjalnego użytkownika systemu komputerowego.

4.2. Docelowa konfiguracja

Głównym celem zadania postawionego inżynierowi jest utworzenie pojedynczej bazy loginów i haseł dla kont użytkowników oraz urządzeń, dzięki czemu możliwe jest uwierzytelnienie i autoryzacja w wielu rozwiązaniach programowych i sprzętowych, takich

jak przełączniki, punkty dostępowe, serwery pocztowe czy komputery klienckie. W ramach omawianego projektu wspólną bazą użytkowników i urządzeń będzie usługa domenowa Active Directory w ramach instalacji systemu Windows Server 2019 Standard. Częścią usług domenowych Active Directory jest baza LDAP, w której są przechowywani użytkownicy. Domena Active Directory sama w sobie jest logiczną jednostką administracyjną, która zawiera w sobie wspomnianych użytkowników i komputery²¹, ale też grupy, dzięki czemu w trakcie operacji na obiektach AD można bardzo konkretnie określić miejsce działania.

Na przykład mając grupę użytkowników będących jednocześnie w organizacji grupą wszystkich pracowników handlowych możemy definiować konfigurację, która jest potrzebna do wdrożenia tylko dla tej grupy, przykładowo instalacja oprogramowania handlowego.

Podłączenie i skonfigurowanie komputerów klienckich lub usług do wykorzystania bazy użytkowników z domeny Active Directory nazywa się integracją z domeną Active Directory. Wykorzystując domenę Active Directory na komputerach po wdrożeniu ich do domeny można wykorzystywać loginy i hasła dla kont należących do domeny jak i tych należących poprzednio do grupy roboczej. Jest to dosyć istotne ze względu na działania profili kont użytkowników w systemie Windows. Każde konto użytkownika (zarówno domenowe jak i lokalne) posiada swój własny profil użytkownika, w którym są zapisane podstawowe informacje o użytkowniku oraz jego dane w postaci plików i konfiguracji, którą posiada (ustawienia pulpitu, ikony programów, z których użytkownik korzysta na pulpicie w odpowiednim ułożeniu, ustawienia programów, z których korzysta użytkownik, pliki personalne (na przykład w folderze Pulpit, Dokumenty, Pobrane) i wiele innych). W standardowym scenariuszu po integracji komputera z Active Directory użytkownik po zalogowaniu się na nowopowstałe konto w domenie może zobaczyć pusty pulpit z domyślną tapetą ze względu na to, że dla takiego konta jest tworzony nowy profil użytkownika. Dobre wdrożenie domeny Active Directory do organizacji zakłada rozwiązanie takiego problemu polegające na tym, że profil(e) lokalnego konta/kont użytkowników są przypisywane do wcześniej utworzonych kont w domenie. Dzięki temu przejście użytkownika do konto domenowe nie sprawia użytkownikowi żadnej trudności. Biorąc pod uwagę fakt, że wspomnianych profili użytkowników w grupie roboczej jest co najmniej tyle ilu użytkowników zakładając, że każdy użytkownik ma co najmniej jeden profil użytkownika na jednym komputerze, proces przenoszenia dla administratora może być czasochłonny. Na

²¹ B.Desmond, J.Richards, R.Allen, A.G.Lowe-Norris, Active Directory, 5th Edition Designing, Deploying, and Running Active Directory, O'Reilly Media Inc. 2013, str. 261-275

czas przeniesienia użytkownika wpływa ilość profili do przeniesienia oraz rozmiar profili (w postaci zajmowanego miejsca na dyskach komputerów). Należy pamiętać o tym, że nawet po przypisaniu profilu użytkownika konta lokalnego do konta domenowego wspomniany profil jest przechowywany na dysku lokalnym komputera, co oznacza, że jeśli profil został utworzony na wielu różnych komputerach, w praktyce będą różniły się zawartością (pomimo tego, że należą nadal do jednego użytkownika). Rozwiązaniem takiego problemu jest przeniesienie profilu użytkownika na serwer i zmiana typu profilu na mobilny. Dzięki temu bez względu na to, z jakiego komputera użytkownik się zaloguje, zawsze będzie miał dostęp do tych samych danych w obrębie swojego profilu użytkownika na każdym stanowisku podłączonym do domeny Active Directory. Korzystając z profili mobilnych w momencie zalogowania użytkownika na stację roboczą profil użytkownika jest zawsze pobierany z serwera, co jest jednocześnie zaletą jak i wadą. O zalecie mobilności wspomniano już powyżej, lecz wadą jest fakt pobrania takiego profilu.

Bardzo często doświadczenie udowadnia, że użytkownicy często w swoich folderach przechowują pliki o bardzo dużych rozmiarach i często te pliki są prywatne, na przykład mała biblioteka filmów. Wystarczy kilka takich filmów w profilu, by sprawić, że profil użytkownika będzie się pobierał długo, co może sprawić, że użytkownik zanim się zaloguje będzie musiał poczekać czasami nawet kilkanaście minut. Rozwiązanie profili mobilnych wymaga ciągłego połączenia z siecią produkcyjną, stąd jest to dobre rozwiązanie szczególnie dla stacjonarnych stacji roboczych, które stale się nie odłączają/podłączają do sieci. Takie rozwiązanie wymaga też od strony serwerowej szybkiego dostępu do profili użytkowników, które są przechowywane w postaci zwykłych folderów i najlepszym rozwiązaniem jest umieszczenie ich na serwerze plików, z którego jest możliwy dostęp do tych danych tylko dla użytkownika do którego konkretny profil należy. Ponadto serwer plików powinien pracować w wysokiej dostępności, dzięki czemu nawet w przypadku awarii jednego serwera drugi jest w stanie kontynuować udostępnianie plików poprzez udział sieciowy.

4.3. Działanie mechanizmu pojedynczego logowania w oparciu o Kerberos

Wykorzystywanie jednego konta użytkownika w obrębie różnych usług jest oparte o protokół Kerberos. Kerberos zapewnia mechanizm uwierzytelnienia, który umożliwia na logowanie się użytkowników do systemu operacyjnego, logowania do aplikacji jak i umożliwia bezpieczną komunikację pomiędzy kontrolerami domeny.

W przypadku logowania użytkownika proces uzyskiwania dostępu jest następujący:

1. Klient wysyła żądanie autoryzacji usługi (**AS_REQ**) do KDC (Key Distribution Center), które jest składnikiem każdego kontrolera domeny.
2. KDC odsyła odpowiedź klientowi (**AS_REP**), która zawiera TGT (Ticket Granting Service).
3. Klient wysyła żądanie przydzielenia TGS (Ticket Granting Service) (**TGS_REQ**) dla określonej usługi na określonym hoście do KDC poprzez podanie SPN (Service Principal Name) oraz TGT.
4. KDC odsyła TGS klientowi (**TGS_REP**).
5. Klient wysyła żądanie uzyskania dostępu do usługi do serwera, dla którego posiada odpowiedni TGS (**AP_REQ**). TGS jest częścią żądania.
6. (opcjonalne) Usługa odpowiada na żądanie w celu wzajemnej autoryzacji.

Żądanie **AS_REQ** składa się z następujących elementów:

- **Nazwa klienta** – dotyczy nazwy użytkownika.
- **Nazwa usługi** - dotyczy SPN (service principal name). Konkretniej, dotyczy ona usługi krbtgt na kontrolerze domeny.
- **Czas klienta** – zawiera zapisany punkt w czasie, gdy jest wykonywane żądanie. Jest on istotny ze względu na ograniczenia czasowe narzucone przez Kerberos w procesie autoryzacji. Aby uniknąć ataków typu replay attack, żądanie jest ważne domyślnie przez 5 minut od jego utworzenia. Wymusza to na klientach oraz kontrolerach domeny synchronizację czasu tak, aby uniknąć przesunięcia czasu na maszynach. Przesunięcie większe niż 5 minut z domyślną konfiguracją mogłoby uniemożliwić uwierzytelnianie.

- **Hash hasła użytkownika** – hasła użytkowników nie są wysyłane poprzez sieć, lecz jedynie wygenerowany hash, który jest później porównywany przez kontroler domeny w celu sprawdzenia, czy użytkownik w procesie uwierzytelniania podał prawidłowe hasło.

Ticket Granting Ticket jest plikiem, którego celem jest umożliwienie użytkownikowi na otrzymywanie plików, które pozwalają na dostęp do usług, konkretniej **Ticket Granting Service**.

Żądanie **AS_REP** składa się z następujących elementów:

- **Nazwa klienta** – dotyczy nazwy użytkownika,
- **Klucz sesji** – jest to losowy klucz kryptograficzny, który jest wykorzystywany w komunikacji pomiędzy kontrolerem domeny (właściwie KDC) a klientem. Klucz sesji jest hash hasła użytkownika,
- **Czas wygaśnięcia** – każdy TGT jest ważny czasowo (domyślnie przez 10 godzin). Po wygaśnięciu TGT klient musi wykonać żądanie kolejnego TGT.
- **TGT** – jest on przechowywany w pamięci cache, w postaci zaszyfrowanej, dzięki czemu użytkownik nie może odczytywać zawartości pliku, zawiera on:
 - **Klucz sesji** – jest to kopia klucza sesji, lecz zaszyfrowana za pomocą hash konta **krbtgt** w domenie AD,
 - **Informacje tokena** – zawiera dane użytkownika takie jak przynależność do grup w domenie, prawa użytkownika oraz informacje o dostęпах DAC (Dynamic Access Control),
 - **Czas wygaśnięcia** – ten czas jest kopią czasu opisanego powyżej.

W systemie Windows istnieje możliwość podejrzenia szczegółów jakie bilety TGT i TGS posiada komputer/użytkownik za pomocą polecenia **klist**. Przykład przedstawiający TGT w wyniku polecenia pokazano na rys 4.1.

```
C:\Users\rserba.SERBA>klist

Current LogonId is 0:0x7a1490

Cached Tickets: (7)

#0>      Client: rserba @ SERBA.LOCAL
        Server: krbtgt/SERBA.LOCAL @ SERBA.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x60210000 -> forwardable forwarded pre_authent
name_canonicalize
```

```
Start Time: 2/27/2021 19:08:37 (local)
End Time: 2/28/2021 5:08:37 (local)
Renew Time: 0
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0x2 -> DELEGATION
Kdc Called: dcl.serba.local

#1> Client: rserba @ SERBA.LOCAL
Server: krbtgt/SERBA.LOCAL @ SERBA.LOCAL
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e10000 -> forwardable renewable initial
pre_authent name_canonicalize
Start Time: 2/27/2021 19:08:37 (local)
End Time: 2/28/2021 5:08:37 (local)
Renew Time: 3/6/2021 19:08:37 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0x1 -> PRIMARY
Kdc Called: dcl.serba.local
```

Rys. 4.1. Fragment wyniku polecenia *klist* na komputerze klienckim zawierającym dane o TGT użytkownika

Kolejnym etapem w przypadku komunikacji z usługą jest uzyskanie TGS (Ticket Granting Service). Pozwala ona na uzyskiwanie dostępu do usługi. W TGS używane są tzw. SPN (service principal name) – służą one do określenia usługi oraz nazwy hosta/FQDN serwera, który dostarcza usługę. Przykładem jest SPN: **ldap/dc1.serba.local**, który wskazuje na usługę serwera LDAP będącego częścią kontrolera domeny. Inny przykład to **cifs/nas.serba.local**, który jest SPN dla usługi umożliwiającej dostęp do zasobu sieciowego na serwerze plików QNAP.

Żądanie **TGS_REQ** wykorzystywane w pozyskiwaniu TGS zawiera:

- **SPN** – podawany jest w celu określenia usługi, do której klient ma otrzymać dostęp,
- **Czas klienta** – podobnie, jak w przypadku żądań TGT, żądania TGS są ograniczone czasowo w celu uniknięcia ataków czasowych,
- **TGT** – cała zawartość TGT posiadanego przez klienta jest zawierana w żądaniu, jest ona zaszyfrowana kluczem KDC.

Odpowiedź KDC do klienta (**TGS_REP**) zawiera:

- **SPN** – jest on taki sam, jak w żądaniu TGS_REQ,
- **Czas klienta** – jest on wykorzystywany w takim samym celu, jak w przypadku poprzedniej komunikacji,

- **Klucz sesji usługi** – klucz zapisany w pamięci cache zapisany w celu szyfrowania komunikacji z określoną usługą.
- **TGS** – jest plikiem umożliwiającym klientowi komunikację z usługą na serwerze, zawiera on:
 - **Nazwę klienta**, dla którego bilet jest utworzony,
 - **SPN** – kopię z **TGS_REQ**,
 - **Klucz sesji usługi** – kopia klucza w odpowiedzi **TGS_REP**,
 - **Czas klienta** – działa on w identyczny sposób, jak w poprzedniej komunikacji.

Przykład TGS przedstawiono na rys 4.2. na podstawie wyniku polecenia **klist** w systemie Windows.

```
#3> Client: rserba @ SERBA.LOCAL
Server: cifs/dcl.serba.local/serba.local @ SERBA.LOCAL
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40250000 -> forwardable pre_authent ok_as_delegate
name_canonicalize
Start Time: 2/27/2021 19:08:38 (local)
End Time: 2/28/2021 5:08:37 (local)
Renew Time: 0
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called: dcl.serba.local

#4> Client: rserba @ SERBA.LOCAL
Server: ldap/dc2.serba.local/serba.local @ SERBA.LOCAL
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40250000 -> forwardable pre_authent ok_as_delegate
name_canonicalize
Start Time: 2/27/2021 19:08:38 (local)
End Time: 2/28/2021 5:08:37 (local)
Renew Time: 0
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called: dcl.serba.local

#5> Client: rserba @ SERBA.LOCAL
Server: cifs/nas.serba.local @ SERBA.LOCAL
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40210000 -> forwardable pre_authent
name_canonicalize
Start Time: 2/27/2021 19:08:37 (local)
End Time: 2/28/2021 5:08:37 (local)
Renew Time: 0
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called: dcl.serba.local

#6> Client: rserba @ SERBA.LOCAL
Server: cifs/dcl.serba.local @ SERBA.LOCAL
```

```
Kerberos Ticket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40250000 -> forwardable pre_authent ok_as_delegate
name_canonicalize
Start Time: 2/27/2021 19:08:37 (local)
End Time: 2/28/2021 5:08:37 (local)
Renew Time: 0
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called: dcl.serba.local
```

Rys. 4.2. Fragment wyniku polecenia *klist* na komputerze klienckim zawierającym dane o TGS użytkownika

Po otrzymaniu TGS klient może wykonać żądanie dostępu do usługi jej serwerze przesyłając w żądaniu TGS dla odpowiedniego serwera w celu otrzymania dostępu do zasobów usługi²².

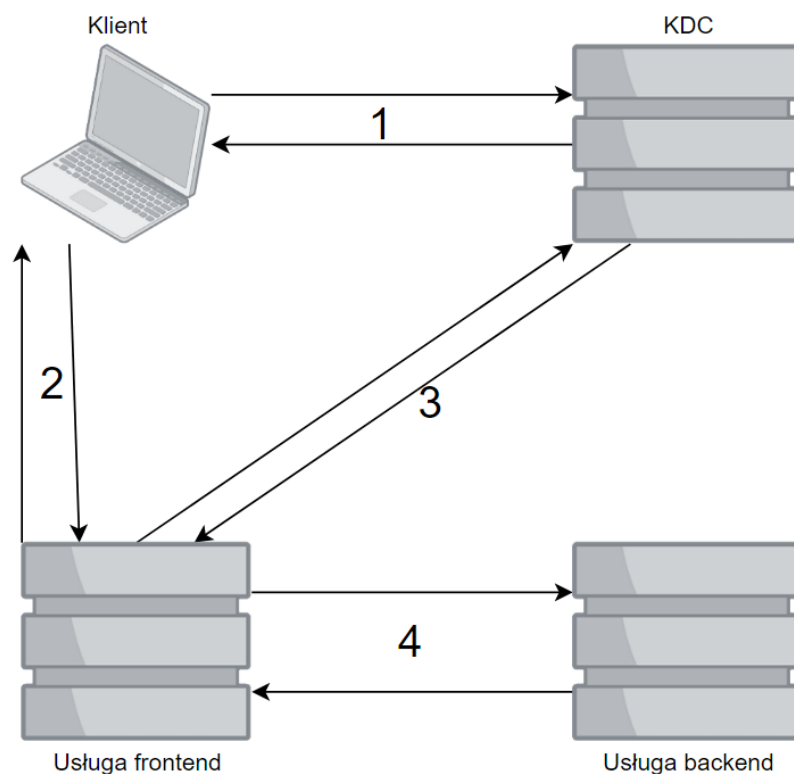
Na podstawie tego typu komunikacji użytkownik w ramach projektu jest w stanie zalogować się na swoje konto użytkownika na komputerze oraz otrzymać dostęp do zasobu na serwerze plików QNAP.

W przypadku logowania się pozostałych usług takich jak na przykład logowanie kontem administracyjnym do FortiGate wykorzystywany jest mechanizm delegacji w modelu zaufanego podsystemu. W modelu tym dostęp do usługi jest uzyskiwany w następujący sposób:

1. Klient wykonuje żądanie TGS do usługi frontend.
2. Klient przedstawia TGS jako część żądania do serwera frontend.
3. Serwer frontend wysyła TGS do kontrolera domeny i żąda TGS dla usługi backend.
4. Serwer frontend wysyła TGS do usługi backend i odpowiada usłudze na podstawie kontekstu użytkownika.

Schemat działania delegacji w ramach której użytkownik loguje się do usługi przedstawiono na rys. 4.3.

²² B.Desmond, J.Richards, R.Allen, A.G.Lowe-Norris, Active Directory, 5th Edition Designing, Deploying, and Running Active Directory, O'Reilly Media Inc. 2013, str. 261-275



Rys. 4.3. Schemat działania delegacji

4.4. Działanie serwerów RADIUS

RADIUS (Remote Authentication Dial-In User) jest protokołem, który umożliwia uwierzytelnianie użytkowników w strukturze klient-serwer. W ramach projektu klientem jest przełącznik, ponieważ to on komunikuje się z serwerem RADIUS w celu uwierzytelnienia użytkownika. RADIUS jest zgodny z modelem AAA²³ wywodzącym się ze słów authentication (uwierzytelnienie), authorization (autoryzacja) i accounting (raportowanie).

²³ A.Józefiok, *Security CCNA 210-260. Zostań administratorem sieci komputerowych Cisco*, Helion 2016, str. 76-89

Uwierzytelnienie polega na zidentyfikowaniu podmiotu próbującego otrzymać dostęp do systemu. Uwierzytelnienie samo w sobie może odbywać się na wiele różnych sposobów:

- **coś co wiesz** – informacja, którą zna tylko i wyłącznie konkretna osoba lub grupa osób, na przykład login i hasło,
- **coś co masz** – materiał fizyczny lub wirtualny pozwalający, który jest posiadany przez osobę lub grupę osób, na przykład klucz prywatny RSA (Rivest-Shamir-Adleman) czy klucz do zamka w drzwiach,
- **coś czym jesteś** – informacja zawierająca nieodłączną część osoby, najczęściej dane biometryczne takie jak skan tęczówki oczu czy odciski palców.

Autoryzacja następuje po uwierzytelnieniu użytkownika systemu. W momencie, gdy użytkownik jest znany systemowi, system sprawdza czy i jakie uprawnienia ma w systemie. Dzięki wykorzystaniu RADIUS możliwe jest podjęcie decyzji, czy konkretny użytkownik ma mieć dostęp do sieci wewnętrznej firmy.

Raportowanie w ramach RADIUS polega na zapisywaniu prób logowania (udanych i nieudanych), dzięki czemu jest możliwe śledzenie prób uwierzytelniania. Jest to przydatne w celu wykrywania potencjalnych intruzów w sieci.

RADIUS korzysta z protokołu UDP na portach 1812 i 1813. Jest on protokołem ogólnodostępnym, co umożliwia jego implementację bez dodatkowych kosztów licencyjnych. Dzięki temu protokół jest obsługiwany przez zdecydowaną większość przełączników zarządzalnych. Uwierzytelnienie w RADIUS polega na przesłaniu loginu i hasła (supplicant) do klienta (authenticator) za pomocą protokołu EAP (EAPOL (Extensible Authentication Protocol over LAN)). Klient, którym w ramach projektu jest przełącznik wysyła poświadczenia do serwera uwierzytelniającego. Na podstawie zdefiniowanych polityk autoryzacji serwer akceptuje, odrzuca wysłane dane lub stwierdza, że dane są niepełne. Transakcja jest wykorzystywana po podaniu hasła dla serwera (hasło te może być definiowane per klient, na przykład per przełącznik).

Odpowiedzi serwera to:

- **ACCEPT** (Access-Accept) w przypadku pomyślnego uwierzytelnienia,
- **REJECT** (Access-Reject) w przypadku nieudanego uwierzytelnienia,
- **CHALLENGE** (Access-Challenge) w przypadku przesłania niepełnych danych użytkownika. Może być to dodatkowe hasło, na przykład kod PIN, token lub karta.

Odpowiedzi są poprzedzone komendą REQUEST (Access-Request).

5. Weryfikacja i walidacja

W ramach przedstawienia wyników testu w sposób wiarygodny, logowanie do usług jest przedstawiane na bazie 1 konta użytkownika:

- Nazwa wyświetlana: **Radosław Serba**
- Nazwa użytkownika: **rserba**
- UPN (User Principal Name): **rserba@serba.local**
- Nazwa użytkownika z nazwą domeny w notacji Down-Level Logon Name: **SERBA\rserba**
- Adres skrzynki pocztowej: **rserba@serba.website**

5.1. Test migracji konta lokalnego do domenowego oraz test podłączenia do domeny Active Directory

Test ma na celu zweryfikowanie możliwości podłączenia komputera do domeny Active Directory oraz migracji profilu lokalnego do konta w domenie. Po przeniesieniu profilu użytkownika ten musi posiadać te same dane pliki w odpowiednich katalogach (na przykład **Pulpit**), jak w przypadku starego konta lokalnego. Proces migracji został przedstawiony na rys. 5.1.

```
ForensiT User Profile Wizard 21.1
Personal Edition (Freeware License)
Copyright (c) 2002-2020 ForensiT Ltd
www.ForensiT.com

Target device: ENDPOINT-5
OS build 10.0.18363.1379. Version 1909.
Local account name is a SID.
Finding Domain Controller for domain serba.local... Done.
Using Domain Controller: \\dc1.serba.local
Binding to Active Directory... Done.
Getting FQDN for user "rserba"... Done.
```

```
Getting Domain SID... Done.  
SID is S-1-5-21-723521058-2419329218-2805022534-1107  
Checking for roaming profile... Done.  
No roaming profile path set.  
Processing UWP Apps... Done.  
Setting Registry ACLs... Done.  
Set Registry ACLs in 2.703 seconds.  
Closing Apps... Done.  
Setting Profile ACL... Done.  
Set Profile ACL in 61.87 seconds.  
Creating Profile registry keys... Done.  
Joining to domain "serba.local"... Done.  
Adding new account to local groups... Done.  
Setting rserba as default logon... Done.  
Migration Complete!
```

Rys. 5.1. Test migracji konta lokalnego do domenowego oraz test podłączenia do domeny Active Directory

Test został zakończony w pełni powodzeniem, ponieważ po ponownym uruchomieniu systemu i zalogowaniu się na konto domenowe użytkownika wszystkie dane użytkownika były możliwe do wykorzystania w taki sam sposób, jak dotychczas na koncie lokalnym.

5.2. Test konfiguracji serwera pocztowego

Testy mają na celu sprawdzenie poprawności konfiguracji zgodnie z czynnościami wykonywanymi w trakcie instalacji oraz możliwości zalogowania się na skrzynkę z użyciem konta testowego.

5.2.1. Test działania serwera Exchange

Test ma na celu sprawdzenie, czy na serwerze istnieje instancja serwera Exchange. Test został przedstawiony na rys. 5.2.

```
[PS] C:\Windows\system32>Get-ExchangeServer | Select
Name,FQDN,Site,ServerRole | fl

Name           : EXCHANGE
Fqdn           : exchange.serba.local
Site           : serba.local/Configuration/Sites/SERBA-Headquarters
ServerRole    : Mailbox
```

Rys. 5.2. *Test działania serwera Exchange*

Test zakończono powodzeniem. Instancja serwera istnieje.

5.2.2. Test konfiguracji wirtualnych katalogów w Exchange

Poniższe testy mają na celu sprawdzenie zmian adresów katalogów wirtualnych różnych usług Exchange 2019 po konfiguracji.

5.2.3. OWA

Test przedstawiono na rys. 5.3.

```
[PS] C:\Windows\system32>Get-OwaVirtualDirectory | Select
Server,ExternalURL,InternalURL | fl

Server      : EXCHANGE
ExternalUrl : https://webmail.serba.website/owa
InternalUrl : https://webmail.serba.website/owa
```

Rys. 5.3. Test konfiguracji katalogu wirtualnego OWA

Test zakończono powodzeniem.

5.2.4. ECP

Test przedstawiono na rys. 5.4.

```
[PS] C:\Windows\system32>Get-EcpVirtualDirectory | Select
Server,ExternalURL,InternalURL | fl

Server          : EXCHANGE
ExternalUrl     : https://webmail.serba.website/ecp
InternalUrl     : https://webmail.serba.website/ecp
```

Rys. 5.4. Test konfiguracji katalogu wirtualnego ECP

Test zakończono powodzeniem.

5.2.5. Outlook Anywhere

Test przedstawiono na rys. 5.5.

```
[PS] C:\Windows\system32>Get-OutlookAnywhere | Select
Server,ExternalHostname,Internalhostname | fl

Server          : EXCHANGE
ExternalHostname : webmail.serba.website
InternalHostname : webmail.serba.website
```

Rys. 5.5. Test konfiguracji katalogu wirtualnego Outlook Anywhere

Test zakończono powodzeniem.

5.2.6. ActiveSync

Test przedstawiono na rys. 5.6.

```
[PS] C:\Windows\system32>Get-ActiveSyncVirtualDirectory | select
server,externalurl,internalurl | fl
```

```
Server      : EXCHANGE
ExternalUrl : https://webmail.serba.website/Microsoft-Server-ActiveSync
InternalUrl : https://webmail.serba.website/Microsoft-Server-ActiveSync
```

Rys. 5.6. Test konfiguracji katalogu wirtualnego ActiveSync

Test zakończono powodzeniem.

5.2.7. Exchange Web Services

Test przedstawiono na rys. 5.7.

```
[PS] C:\Windows\system32>Get-WebServicesVirtualDirectory | Select
Server,ExternalURL,InternalURL | fl

Server      : EXCHANGE
ExternalUrl : https://webmail.serba.website/EWS/Exchange.asmx
InternalUrl : https://webmail.serba.website/EWS/Exchange.asmx
```

Rys. 5.7. Test konfiguracji katalogu wirtualnego Exchange Web Services

Test zakończono powodzeniem.

5.2.8. Online Address Book

Test przedstawiono na rys. 5.8.

```
[PS] C:\Windows\system32>Get-OabVirtualDirectory | Select
Server,ExternalURL,InternalURL | fl

Server      : EXCHANGE
```



```
ExternalUrl : https://webmail.serba.website/OAB  
InternalUrl : https://webmail.serba.website/OAB
```

Rys. 5.8. Test konfiguracji katalogu wirtualnego Online Address Book

Test zakończono powodzeniem.

5.2.9. Client Access

Test przedstawiono na rys. 5.9.

```
[PS] C:\Windows\system32>Get-ClientAccessService | fl  
identity, autodiscoverserviceinternaluri  
  
Identity : EXCHANGE  
AutoDiscoverServiceInternalUri :  
https://autodiscover.serba.website/Autodiscover/Autodiscover.xml
```

Rys. 5.9. Test konfiguracji katalogu wirtualnego Client Access

Test zakończono powodzeniem.

5.2.10. MAPI

Test przedstawiono na rys. 5.10.

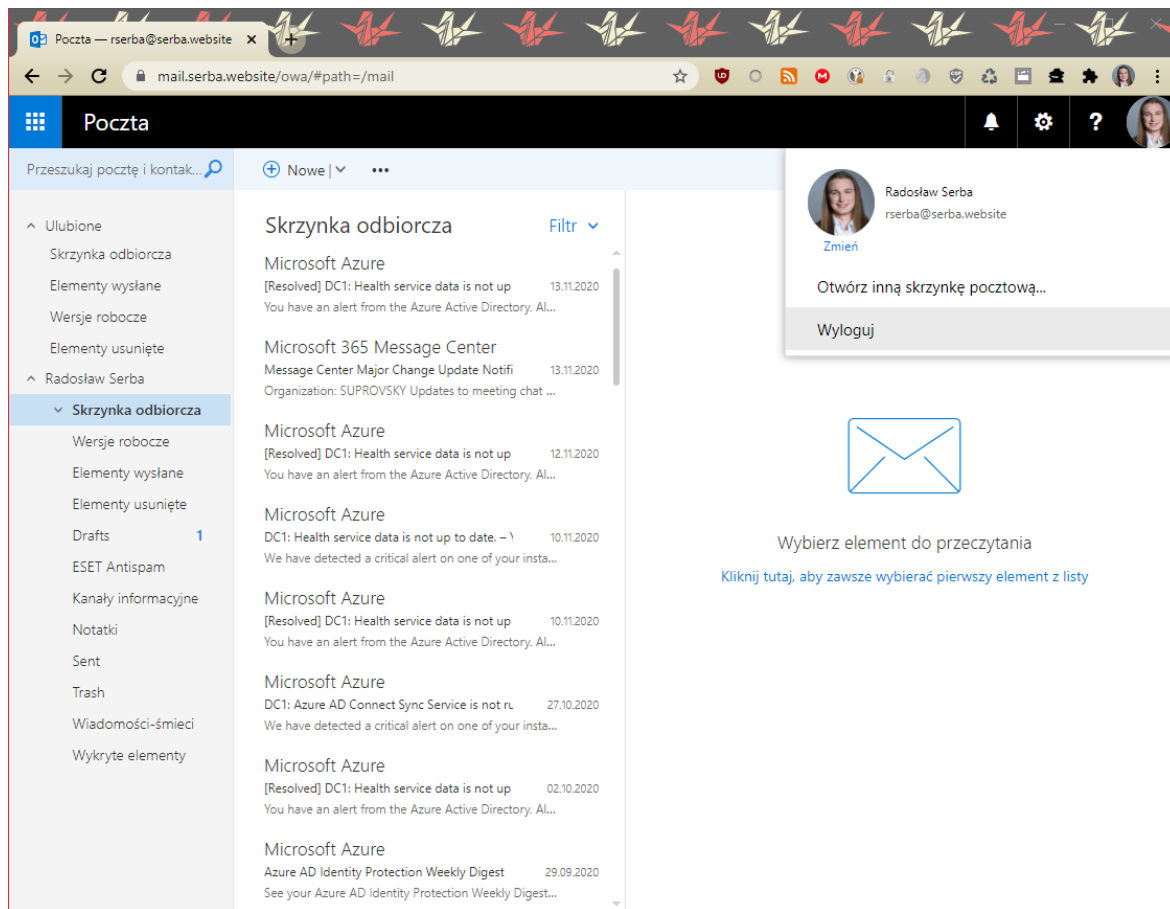
```
[PS] C:\Windows\system32>Get-MapiVirtualDirectory | Select  
Server, ExternalURL, InternalURL | fl  
  
Server : EXCHANGE  
ExternalUrl : https://webmail.serba.website/mapi  
InternalUrl : https://webmail.serba.website/mapi
```

Rys. 5.10. Test konfiguracji katalogu wirtualnego MAPI

Test zakończono powodzeniem.

5.2.11. Test logowania konta użytkownika poprzez OWA

Test ma na celu sprawdzenie, czy jest możliwe zalogowanie się poprzez interfejs Outlook Web Access, który umożliwia użytkownikowi korzystanie ze skrzynki pocztowej bez potrzeby instalowania klienta pocztowego, z użyciem przeglądarki internetowej. Podobnie jak w przypadku innych testów, zostało wykorzystane konto **SERBA\rserba**. Wynik przedstawiono na rys. 5.11, który zakończył się powodzeniem.

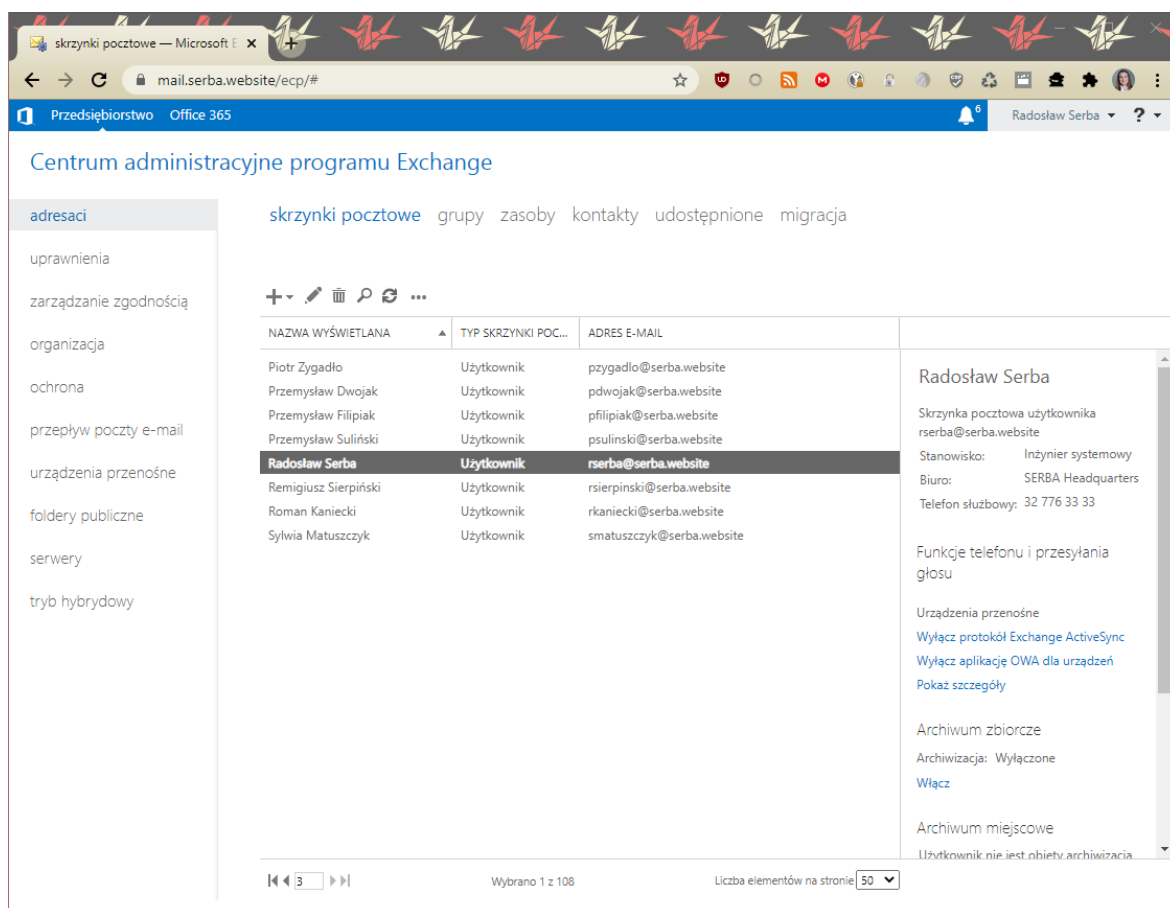


Rys. 5.11. Test logowania konta użytkownika przez OWA

5.2.12. Test logowania konta administratora poprzez ECP

Test ma na celu sprawdzenie, czy jest możliwe zalogowanie się poprzez interfejs Exchange Control Panel, który umożliwia administratorowi zarządzanie serwerem Exchange bez potrzeby korzystania z komputera posiadającego zainstalowany program Exchange Management Shell. Podobnie jak w przypadku innych testów, zostało

wykorzystane konto **SERBA\rserba**. Wynik przedstawiono na rys. 5.12, który zakończył się powodzeniem.

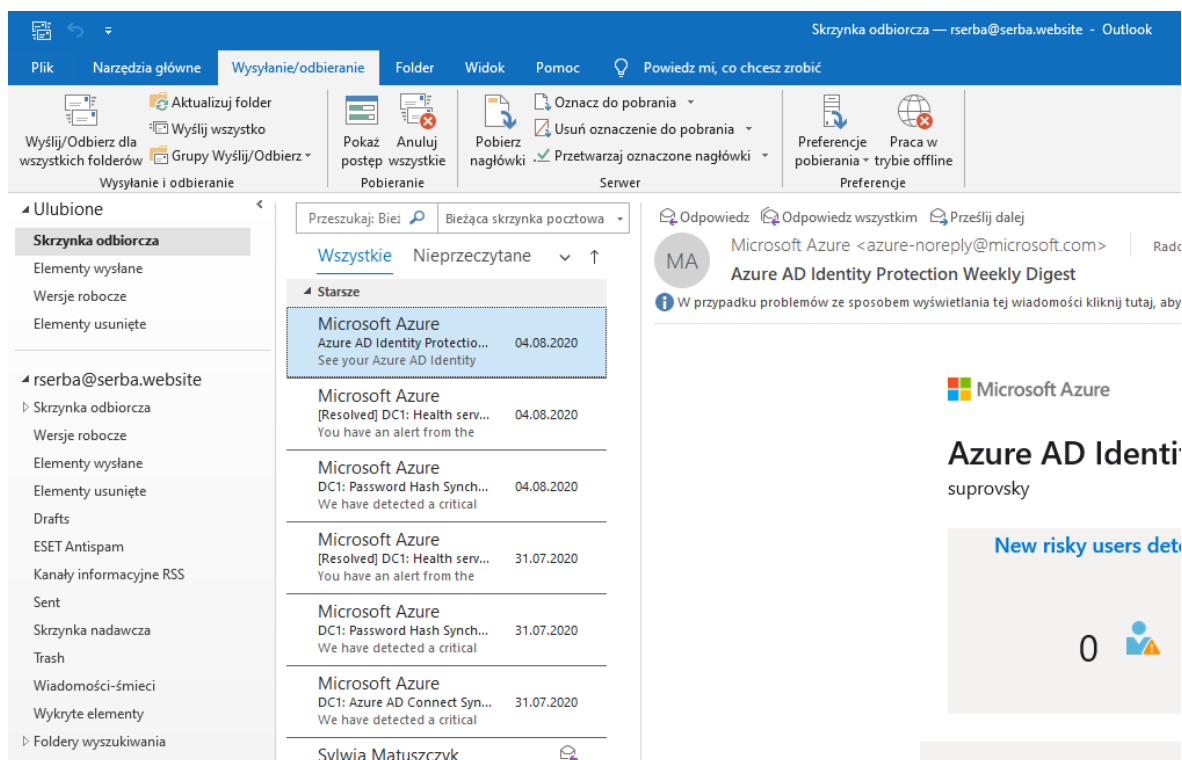


Rys. 5.12. Test logowania konta administratora przez ECP

5.2.13. Test logowania poprzez klienta pocztowego Microsoft Outlook

Test ma na celu sprawdzenie możliwości logowania się do skrzynki poprzez klienta pocztowego Microsoft Outlook za pomocą testowego konta użytkownika. Jako adres email w teście wykorzystano adres **rserba@serba.website**. Wynik został przedstawiony na rys.

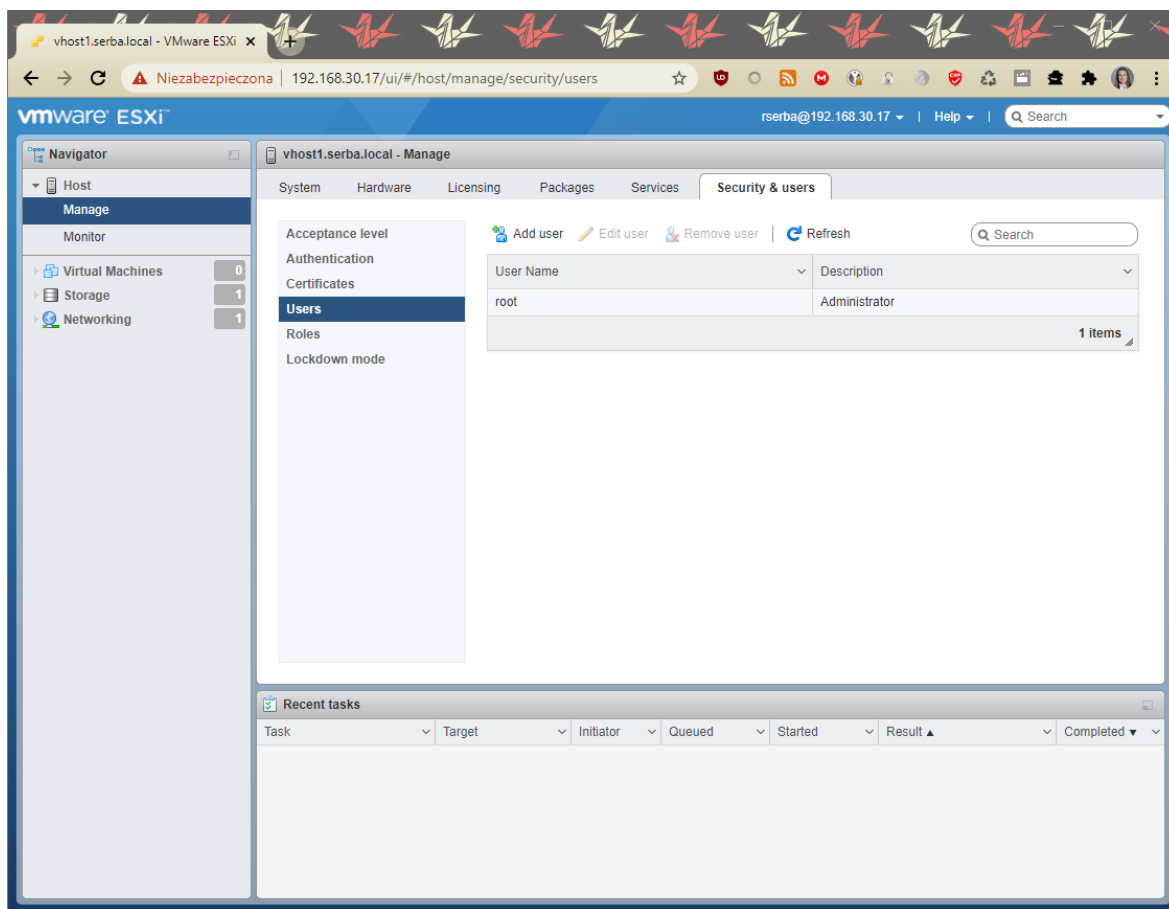
5.13. Test został zakończony powodzeniem, ponieważ ja można zauważyć na rysunku, użytkownik był w stanie pobrać wiadomości znajdujące się w jego skrzynce odbiorczej z serwera pocztowego. Na rysunku należy zwrócić uwagę na adres mailowy – zgadza się on z adresem zakładanym w teście.



Rys. 5.13. Test logowania poprzez klienta pocztowego Microsoft Outlook

5.3. Test logowania do VMware ESXi

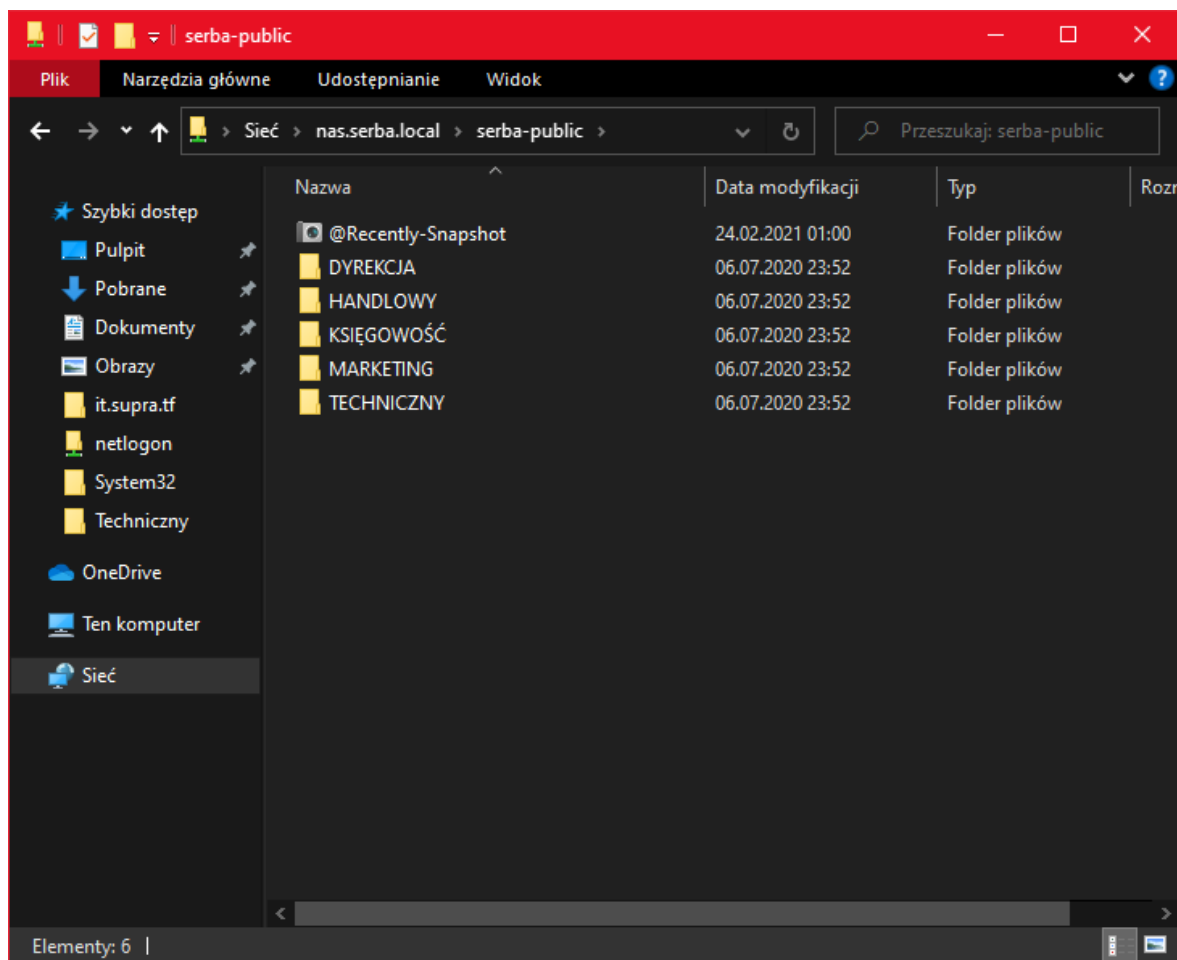
Test ma na celu sprawdzenie, czy jest możliwe zalogowanie się do strony konfiguracyjnej serwera VMware ESXi Web Client. Interfejs ten służy do zarządzania maszynami wirtualnymi obsługiwany przez hypervisor. Warunkiem zalogowania jest członkostwo w domenie Active Directory w grupie **ESX Admins**. Wynik testu przedstawia rys. 5.14. Wynik został zakończony powodzeniem. Można to ocenić poprzez widoczną zalogowaną nazwę użytkownika **rserba** oraz listę użytkowników zawierającą jedynie konto **root** będące wbudowanym kontem użytkownika.



Rys. 5.14. Test logowania do VMware ESXi

5.4. Test logowania do zasobu sieciowego na serwerze plików QNAP

Następny test polega na sprawdzeniu poprawności konfiguracji udziału sieciowego służącego do kolaboracji pomiędzy pracownikami firmy. Konfiguracja serwera plików ma pozwolić użytkownikom otworzyć zasób sieciowy `//nas.serba.local/serba-public` z poziomu komputera, na którym jest zalogowany użytkownik testowy. Użytkownik powinien także widzieć zawartość zasobu sieciowego. Wynik testu przedstawia rys. 5.15., który zakończył się powodzeniem, co można zauważyć na zrzucie ekranu.

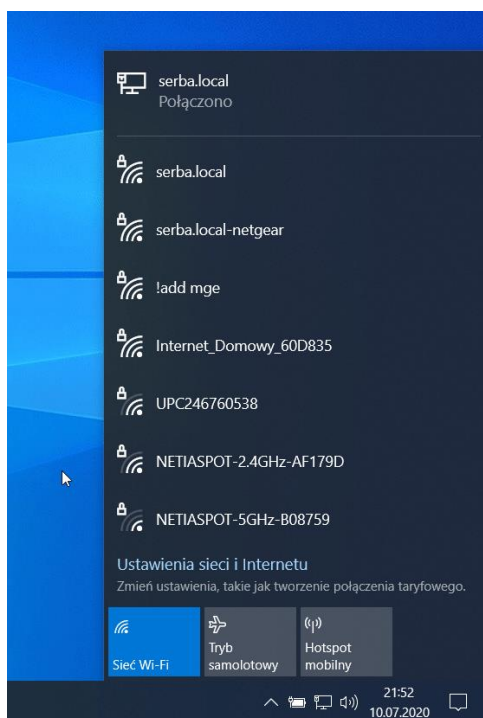


Rys. 5.15. Test logowania do zasobu sieciowego na serwerze plików QNAP

W trakcie testu jedynym napotkanym problemem była nieprzypisana nazwa `nas.serba.local` do adresu IP `192.168.30.8` – po dodaniu odpowiedniego wpisu w serwerze DNS zasób sieciowy stał się dostępny dla wszystkich użytkowników w jednostce organizacyjnej **it.supra.tf**.

5.5. Test autoryzacji w sieci przewodowej komputera klienckiego

Test ma na celu sprawdzenie autoryzacji przewodowego połączenia sieciowego. W ramach testu komputer kliencki będący członkiem domeny Active Directory ma po podłączeniu fizycznie kablem Ethernet otrzymać połączenie z siecią, dzięki czemu jest możliwe połączenie się z Internetem oraz z otoczeniem sieciowym. W przypadku podłączenia się nieautoryzowanego komputera to chronionego portu ten ma nie otrzymać połączenia z siecią lokalną jak i siecią Internet. Testowanym portem przełącznika jest port 1. Rys. 5.16. przedstawia powodzenie testu autoryzowanego komputera. Rys. 5.17. przedstawia powodzenie autoryzacji z poziomu przełącznika – port w trybie **Auto** osiągnął status **Authorized**. Inaczej jest w przypadku Rys. 5.18. – nieautoryzowany komputer otrzymał status **Unauthorized**, co spowodowało brak połączenia z otoczeniem sieciowym.



Rys. 5.16. Test autoryzacji z poziomu autoryzowanego komputera klienckiego

Port	Control Mode	Operating Control Mode	Reauthentication Enabled	Port Status
g1	Auto	Auto	FALSE	Authorized
g2	Auto	N/A	FALSE	N/A
g3	Force Authorized	N/A	FALSE	N/A
g4	Force Authorized	Force Authorized	FALSE	Authorized
g5	Force Authorized	N/A	FALSE	N/A
g6	Force Authorized	N/A	FALSE	N/A
g7	Force Authorized	N/A	FALSE	N/A
g8	Force Authorized	Force Authorized	FALSE	Authorized
g9	Force Authorized	N/A	FALSE	N/A
g10	Force Authorized	Force Authorized	FALSE	Authorized
g11	Force Authorized	N/A	FALSE	N/A
g12	Force Authorized	N/A	FALSE	N/A
g13	Force Authorized	N/A	FALSE	N/A
g14	Force Authorized	N/A	FALSE	N/A
g15	Force Authorized	Force Authorized	FALSE	Authorized
g16	Force Authorized	Force Authorized	FALSE	Authorized
g17	Force Authorized	N/A	FALSE	N/A
g18	Force Authorized	N/A	FALSE	N/A
1 All				

Rys. 5.17. Test autoryzacji z poziomu przełącznika ze wskazaniem komputera autoryzowanego

Port	Control Mode	Operating Control Mode	Reauthentication Enabled	Port Status
g1	Auto	Auto	FALSE	Unauthorized
g2	Auto	N/A	FALSE	N/A
g3	Force Authorized	N/A	FALSE	N/A
g4	Force Authorized	Force Authorized	FALSE	Authorized
g5	Force Authorized	N/A	FALSE	N/A
g6	Force Authorized	N/A	FALSE	N/A
g7	Force Authorized	N/A	FALSE	N/A
g8	Force Authorized	Force Authorized	FALSE	Authorized
g9	Force Authorized	N/A	FALSE	N/A
g10	Force Authorized	Force Authorized	FALSE	Authorized
g11	Force Authorized	N/A	FALSE	N/A
g12	Force Authorized	N/A	FALSE	N/A
g13	Force Authorized	N/A	FALSE	N/A
g14	Force Authorized	N/A	FALSE	N/A
g15	Force Authorized	Force Authorized	FALSE	Authorized
g16	Force Authorized	Force Authorized	FALSE	Authorized
g17	Force Authorized	N/A	FALSE	N/A
g18	Force Authorized	N/A	FALSE	N/A
1 All				

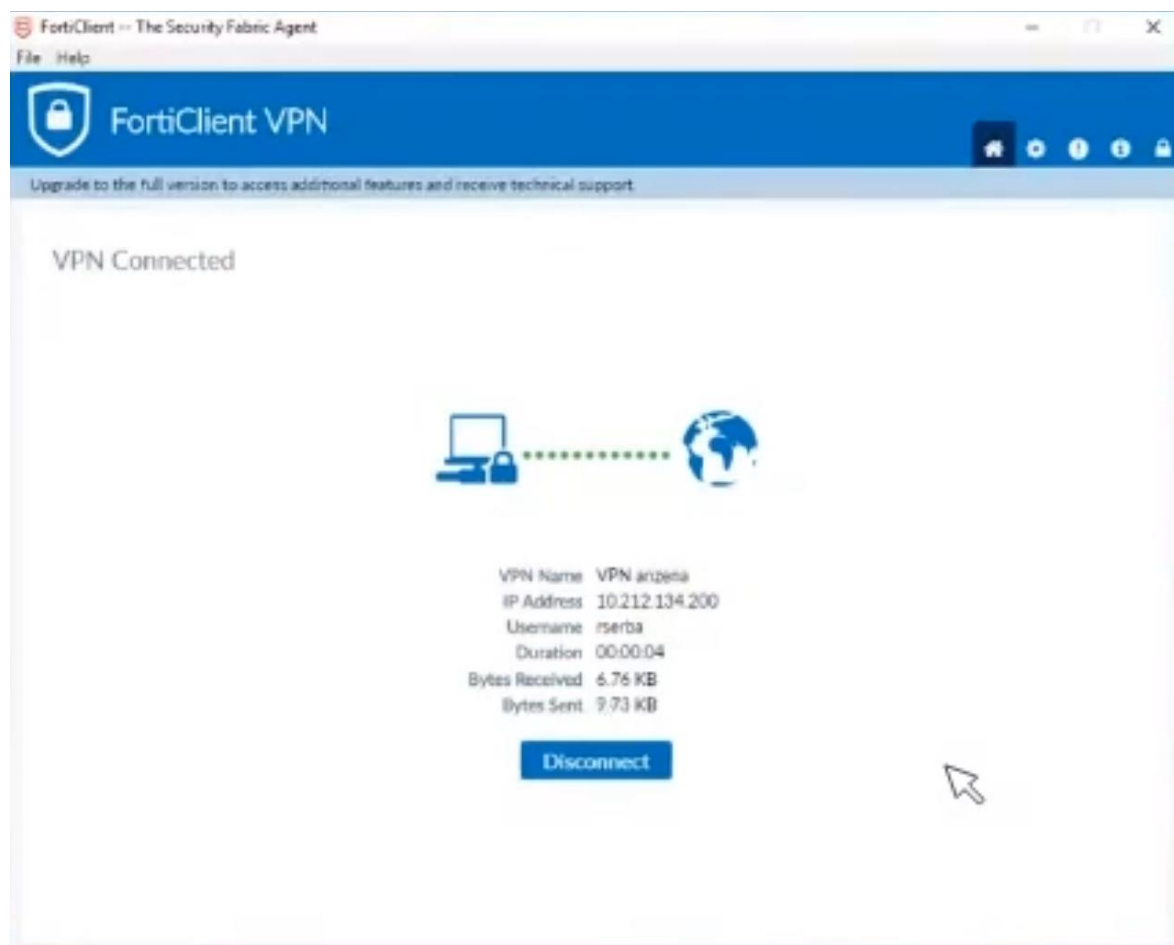
Rys. 5.18. Test autoryzacji z poziomu przełącznika ze wskazaniem komputera nieautoryzowanego

5.6. Test pojedynczego logowania konta Active Directory w FortiGate

Test ten ma sprawdzić, czy jest możliwe zalogowanie się kontem testowym do interfejsu konfiguracyjnego oraz usługi VPN urządzenia typu UTM FortiGate. Rys. 5.19. przedstawia fragment ekranu, na którym można zauważyć interfejs administracyjny z zalogowanym kontem testowym, co oznacza powodzenie testu. Rys. 5.20. przedstawia powodzenie logowania do usługi VPN FortiGate poprzez aplikację FortiClient.

<div> <div>Q</div> <div>></div> <div>?</div> <div>1</div> <div>rserba</div> </div>			
<div> <div>Q</div> <div>Group By Type</div> </div>			
IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges
10.10.10.1/255.255.255.0	PING HTTPS FMG-Access Security Fabric Connection		

Rys. 5.19. Test pojedynczego logowania konta Active Directory w FortiGate



Rys. 5.20. Test pojedynczego logowania konta Active Directory w FortiClient VPN

6. Podsumowanie i wnioski

Projekt przedstawił możliwe korzyści oraz potencjalne wyzwania postawione administratorowi systemów. Najistotniejszą korzyścią całego systemu jest możliwość szybkiego, intuicyjnego logowania się za pomocą jednego konta użytkownika, co za tym idzie – nie istnieje potrzeba pamiętania wielu loginów i haseł do kont pomimo wielu różnych usług wewnętrznych firmy.

W projekcie przedstawiono możliwość autoryzacji na bazie kont Active Directory w obrębie sieci przewodowej, w ramach interfejsów administracyjnych, udziałów sieciowych na serwerze plików i dostępu do skrzynek na serwerze pocztowym.

Projekt przedstawił część możliwości pod kątem wykorzystania systemu SSO ze względu na ogromne możliwości wykorzystania – w projekcie przedstawiono dostęp administracyjny do konsol administracyjnych do serwera plików, serwera pocztowego, infrastruktury sieciowej firmy. W rzeczywistości średnie i duże organizacje korzystają z dużej ilości systemów, co zwiększyłoby listę zintegrowanych usług o system zarządzania projektami (na przykład Jira), system księgowo-płacowy dla księgowości, system ERP, serwisy intranetowe (na przykład bazujące na Microsoft Sharepoint), sieci bezprzewodowe z wykorzystaniem WPA2-Enterprise i wiele innych.

Ponadto, projekt został przedstawiony w uproszczonej formie – istotnym problemem rozwiązania jest to, że infrastruktura serwerowa jest umieszczona na jednym serwerze fizycznym bez jakiegokolwiek redundancji, co w przypadku awarii fizycznej serwera powoduje paraliż pracy użytkowników.

Projekt mógłby być rozszerzony o system wysokiej dostępności, dzięki czemu w przypadku awarii hosta maszyny wirtualne zawierające systemy serwerowe mogłyby zostać uruchomione ponownie na innej maszynie fizycznej.

A. Bibliografia

- [1] B.Desmond, J. R.-N. (2013). *ctive Directory, 5th Edition Designing, Deploying, and Running Active Directory*. O'Reilly Media Inc.
- [2] Batard, P. (2021, Luty 14). *Rufus - The Official Website*. Pobrano z <https://rufus.ie/>
- [3] ForensiT. (2021, Luty 24). *ForensiT User Profile Wizard Corporate Guide*. Pobrano z <https://www.forensit.com/Downloads/User%20Profile%20Wizard%20Corporate%20User%20Guide.pdf>
- [4] Fortinet. (2020, Lipiec 18). *FortiGate/FortiWifi 60E Data Sheet*. Pobrano z lokalizacji https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_FortiWiFi_60E_Series.pdf
- [5] Internet Engineering Task Force. (2011, Marzec 1). *Use of SRV Records for Locating Email Submission/Access Services*. Pobrano z Luty 23, 2021, z <https://tools.ietf.org/html/rfc6186>
- [6] Internet Security Research Group. (2021, Luty 23). *Challenge Types – Let's Encrypt*. Pobrano z <https://letsencrypt.org/docs/challenge-types/>
- [7] Józefiok, A. (2016). *Security CCNA 210-260. Zostań administratorem sieci komputerowych*. Helion 2016.
- [8] Microsoft. (2020, Sierpień 22). *Exchange Server system requirements*. Pobrano z <https://docs.microsoft.com/en-us/exchange/plan-and-deploy/system-requirements?view=exchserver-2019>
- [9] Microsoft. (2020, Wrzesień 10). *System requirements for Hyper-V on Windows Server*. Pobrano z <https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/system-requirements-for-hyper-v-on-windows>
- [10] Microsoft. (2020, Lipiec 31). *Windows Server 2019 System Requirements*. Pobrano z <https://docs.microsoft.com/en-us/windows-server/get-started-19/sys-reqs-19>
- [11] Microsoft. (2021, Luty 21). *Exchange Server prerequisites*. Pobrano z <https://docs.microsoft.com/en-us/exchange/plan-and-deploy/prerequisites?view=exchserver-2019>

- [12] Netgear. (2020, Lipiec 24). *NETGEAR GS716Tv3, GS624Tv4, GS748Tv5 Data Sheet*. Pobrano z lokalizacji <https://www.downloads.netgear.com/files/GDC/datasheet/en/GS716Tv3-GS724Tv4-GS748Tv5.pdf>
- [13] Netgear. (2021, Luty 23). *GS716 and GS724T Gigabit Smart Switches Software Administration Manual*. Pobrano z https://www.downloads.netgear.com/files/GDC/GS716TV2/GS716T_GS724T-SWA-October2012.pdf
- [14] QNAP. (2020, Listopad 14). *QNAP TS-453A – Specyfikacja sprzętowa*. Pobrano z <https://www.qnap.com/pl-pl/product/ts-453a/specs/hardware>
- [15] VMware. (2020, Sierpień 22). *ESXi Hardware Requirements*. Pobrano z <https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.esxi.install.doc/GUID-DEB8086A-306B-4239-BF76-E354679202FC.html>
- win-acme. (2021, Luty 22). *win-acme – Getting started*. Pobrano z <https://www.win-acme.com/manual/getting-started>

B. Słownik skrótów i symboli

AD – Active Directory

AMD-V – AMD Virtualization

API – Application Programming Interface

BIOS – Basic Input/Output System

CD – Compact Disk

CSV – Comma Separated Values

DAC – Dynamic Access Control

DHCP – Dynamic Host Configuration Protocol

DMZ – Demilitarized Zone

DNS – Domain Name System

DSRM – Directory Service Restore Mode

DVD – Digital Versatile Disk

EAP – Extensible Authentication Protocol

EAPOL – Extensible Authentication Protocol over LAN

ECP – Exchange Control Panel

FQDN – Fully Qualified Domain Name

GPT – GUID Partition Table

HTTP – Hypertext Transfer Protocol

IIS – Internet Information Services

IMAP – Internet Message Access Protocol

IP – Internet Protocol

Intel VT-x – Intel Virtualization Technology for **IA-32** and Intel **64** Processors

IPMI – Intelligent Platform Management Interface

iRMC – integrated **R**emote **M**anagement **C**ontroller

ISO – **I**nternational **O**rganization for **S**tandardization

KDC – **K**ey **D**istribution **C**enter

LAN – **L**ocal **A**rea **N**etwork

LDAP – **L**ightweight **D**irectory **A**ccess **P**rotocol

LDAPS - **L**ightweight **D**irectory **A**ccess **P**rotocol over **SSL/TLS**

MAC – **M**edia **A**ccess **C**ontrol

MAPI – **M**essaging **A**pplication **P**rogram **I**nterface

MBR – **M**aster **B**oot **R**ecord

MSI – **M**icrosoft **I**nstaller

NGFW – **N**ext **G**eneration **F**irewall

NVMe – **N**VM **E**xpress lub **N**on-**V**olatile **M**emory **H**ost **C**ontroller **I**nterface Specification

OAuth – **O**pen **A**uthorization

OAB – **O**ffline **A**ddress **B**ook

OWA – **O**utlook **W**eb **A**ccess

RADIUS – **R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice

RAID – **R**edundant **A**rray of **I**ndependent **D**isk

RJ-45 – **R**egistered **J**ack – type **45**

RPM – **R**ed **H**at **P**ackage **M**anager

RSA – **R**ivest-**S**hamir-**A**dleman

RSAT – **R**emote **S**erver **A**dministration **T**ools

SMTP – **S**imple **M**ail **T**ransfer **P**rotocol

SPN – **S**ervice **P**rincipal **N**ame

SSL – **S**ecure **S**ockets **L**ayer

SSO – **S**ingle **S**ign-**O**n

TCP – **T**ransmission **C**ontrol **P**rotocol

TGT – Ticket Granting Ticket

TGS – Ticket Granting Service

UDP – User Datagram Protocol

UEFI – Unified Extensible Firmware Interface

UEFI-CSM - Unified Extensible Firmware Interface – Compatibility Support Module

UPN – User Principal Name

UTM – Unified Threat Management

VPN – Virtual Private Network

WAN – Wide Area Network

WPA2-PSK – Wi-Fi Protected Access II – Preshared Key

C. Spis rysunków

- Rys. 3.1. Początkowa konfiguracja sieci komputerowej, bez wdrożonego mechanizmu pojedynczego logowania
- Rys. 3.2. Docelowa konfiguracja sieci komputerowej z wdrożonym mechanizmem pojedynczego logowania
- Rys. 3.3. Dołączanie hosta ESXi do domeny Active Directory
- Rys. 3.4. Docelowa konfiguracja usług przekazywania dalej serwera DNS dla kontrolerów domeny
- Rys. 3.5. Docelowa konfiguracja schematu organizacji w domenie Active Directory
- Rys. 3.6. Docelowa konfiguracja profilu LDAP w FortiGate
- Rys. 3.7. Polecenie instalujące zależności systemowe dla Exchange 2019
- Rys. 3.8. Polecenia przygotowujące schemat, domenę i organizację do instalacji Exchange 2019
- Rys. 3.9. Konfiguracja strefy DNS dla nazwy serba.website
- Rys. 3.10. Skrypt zmieniający adresy wirtualnych katalogów Exchange 2019
- Rys. 3.11. Interfejs konfiguracyjny win-acme
- Rys. 3.12. Konfiguracja alternatywnego sufiksu głównych nazw użytkowników
- Rys. 3.13. Skrypt PowerShell tworzący skrzynki w Exchange 2019 na bazie kont użytkowników
- Rys. 3.14. Konfigurowanie metody uwierzytelnienia w serwerze zasad sieciowych
- Rys. 3.15. Konfiguracja autoryzacji urządzeń w portach przełącznika Netgear GS716T
- Rys. 3.16. Konfiguracja polityki GPO wymuszającej włączanie usługi dot3svc
- Rys. 3.17. Dołączanie serwera plików QNAP do domeny Active Directory
- Rys. 3.18. Aktualizacja zasad grupy z poziomu kontrolera domeny

- Rys. 3.19. Dołączanie komputera do domeny wraz z migracją profilu użytkownika konta lokalnego do konta domenowego z użyciem User Profile Wizard
- Rys. 4.1. Fragment wyniku polecenia klist na komputerze klienckim zawierającym dane o TGT użytkownika
- Rys. 4.2. Fragment wyniku polecenia klist na komputerze klienckim zawierającym dane o TGS użytkownika
- Rys. 4.3. Schemat działania delegacji
- Rys. 5.1. Test migracji konta lokalnego do domenowego oraz test połączenia do domeny Active Directory
- Rys. 5.2. Test działania serwera Exchange
- Rys. 5.3. Test konfiguracji katalogu wirtualnego OWA
- Rys. 5.4. Test konfiguracji katalogu wirtualnego ECP
- Rys. 5.5. Test konfiguracji katalogu wirtualnego Outlook Anywhere
- Rys. 5.6. Test konfiguracji katalogu wirtualnego ActiveSync
- Rys. 5.7. Test konfiguracji katalogu wirtualnego Exchange Web Services
- Rys. 5.8. Test konfiguracji katalogu wirtualnego Online Address Book
- Rys. 5.9. Test konfiguracji katalogu wirtualnego Client Access
- Rys. 5.10. Test konfiguracji katalogu wirtualnego MAPI
- Rys. 5.11. Test logowania konta użytkownika przez OWA
- Rys. 5.12. Test logowania konta administratora przez ECP
- Rys. 5.13. Test logowania poprzez klienta pocztowego Microsoft Outlook
- Rys. 5.14. Test logowania do VMware ESXi
- Rys. 5.15. Test logowania do zasobu sieciowego na serwerze plików QNAP
- Rys. 5.16. Test autoryzacji z poziomu autoryzowanego komputera klienckiego
- Rys. 5.17. Test autoryzacji z poziomu przełącznika ze wskazaniem komputera autoryzowanego
- Rys. 5.18. Test autoryzacji z poziomu przełącznika ze wskazaniem komputera nieautoryzowanego

- Rys. 5.19. Test pojedynczego logowania konta Active Directory w FortiGate
- Rys. 5.20. Test pojedynczego logowania konta Active Directory w FortiClient VPN

D. Spis załączników

D.1. Załącznik 1 – skrypt tworzący schemat jednostek organizacyjnych oraz użytkowników w domenie Active Directory

```
1. <#Import active directory module for running AD cmdlets#>
2. Import-Module activedirectory
3.
4. <#Create main OU#>
5. $baseDN = "DC=SERBA,DC=LOCAL"
6. $baseOU = "OU=it.supra.tf"
7. $baseOUstring = $baseOU + "," + $baseDN
8. <#New-ADOrganizationalUnit -Name "SUPRA" -Path $baseOU#>
9. if (Get-ADOrganizationalUnit -Filter "distinguishedName -eq
'$baseOUstring'") {
10.     Write-Host "$baseOUstring already exists."
11. } else {
12.     New-ADOrganizationalUnit -Name $baseOU -Path $baseDN
13. }
14.
15.
16. <#Create OU's#>
17. $OUs =
    @("Dyrekcja","Handlowy","Marketing","Ksiegowosc","Rozwojowy","Prawn
y","Logistyczny","Techniczny")
18.
19. <#Loop through each name of the OU to create them#>
20. foreach ($OUcreate in $OUs) {
21.     $fullOUstring = "OU=" + $OUcreate + "," + $baseOUstring
22.     Write-Output $fullOUstring
23.     if (Get-ADOrganizationalUnit -Filter "distinguishedName -eq
'$fullOUstring'") {
24.         Write-Host "$OUcreate already exists."
25.     } else {
26.         New-ADOrganizationalUnit -Name $OUcreate -Path
$baseOUstring
27.     }
28. }
29.
30. <#Store the data from ADUsers.csv in the $ADUsers variable#>
```

```
31. $ADUsers = Import-csv -Delimiter ";" -Path .\bulk-users-  
    polska.csv  
32.  
33. <#Loop through each row containing user details in the CSV file#>  
34. foreach ($User in $ADUsers)  
35. {  
36.     <#Read user data from each field in each row and assign  
        the data to a variable as below#>  
37.  
38.         $Username      = $User.username  
39.         $Password      = $User.password  
40.         $Firstname     = $User.firstname  
41.         $Lastname      = $User.lastname  
42.         $OU            = $User.ou <#This field refers to the OU  
        the user account is to be created in#>  
43.         $email        = $User.email  
44.         $streetaddress = $User.streetaddress  
45.         $city          = $User.city  
46.         $zipcode       = $User.zipcode  
47.         $state         = $User.state  
48.         $country       = $User.country  
49.         $telephone     = $User.telephone  
50.         $jobtitle      = $User.jobtitle  
51.         $company       = $User.company  
52.         $department    = $User.department  
53.         $Password      = $User.Password  
54.  
55.  
56.         <#Check to see if the user already exists in AD#>  
57.         if (Get-ADUser -F {SamAccountName -eq $Username})  
58.         {  
59.             <#If user does exist, give a warning#>  
60.             Write-Warning "A user account with username  
        $Username already exist in Active Directory."  
61.         }  
62.         else  
63.         {  
64.             <#User does not exist then proceed to create the  
        new user account  
65.             Account will be created in the OU provided by the $OU  
        variable read from the CSV file#>  
66.             New-ADUser `   
67.                 -SamAccountName $Username `   
68.                 -UserPrincipalName "$Username@serba.local" `   
69.                 -Name "$Firstname $Lastname" `   
70.                 -GivenName "$Firstname" `   
71.                 -Surname "$Lastname" `   
72.                 -Enabled $True `   
73.                 -DisplayName "$Firstname $Lastname" `   
74.                 -Path "$OU" `   
75.                 -City "$city" `   
76.                 -Company "$company" `   
77.                 -State "$state" `   
78.                 -StreetAddress "$streetaddress" `   
79.                 -Country "$country" `   
80.                 -PostalCode "$zipcode" `   
81.                 -OfficePhone "$telephone" `
```

```

82.             -EmailAddress "$email" `
83.             -Title "$jobtitle" `
84.             -Department "$department" `
85.             -AccountPassword (convertto-securestring $Password -
AsPlainText -Force) -ChangePasswordAtLogon $False -
PasswordNeverExpires $True -CannotChangePassword $True
86.
87.         }
88.     }
89. Get-ADUser -Filter 'Name -like "*" ' -SearchBase
'OU=it.supra.tf,DC=SERBA,DC=LOCAL' -Properties DisplayName |
ForEach-Object {Set-ADUser $_ -Office 'SERBA Dntown'}
90. Get-ADUser -Filter 'Name -like "*" ' -SearchBase
'OU=Techniczny,OU=it.supra.tf,DC=SERBA,DC=LOCAL' -Properties
DisplayName | ForEach-Object {Set-ADUser $_ -Office 'SERBA
Headquarters'}
91. Get-ADUser -Filter 'Name -like "*" ' -SearchBase
'OU=Dyrekcja,OU=it.supra.tf,DC=SERBA,DC=LOCAL' -Properties
DisplayName | ForEach-Object {Set-ADUser $_ -Office 'SERBA
Headquarters'}

```

D.2. Załącznik 2 – fragment pliku CSV wykorzystywanego przez skrypt tworzący użytkowników w domenie Active Directory

```

firstname;lastname;username;email;streetaddress;city;zipcode;state;count
y;department;password;telephone;jobtitle;company;ou
Miron;Trawiński;mtrawinski;mtrawinski@serba.website;aleja Niepodległości
49;Tychy;43-100;śląskie;PL;Handlowy;Zaq12wsx!;32 776 33 33;Specjalista
ds. handlowych;it.supra.tf;OU=Handlowy,OU=it.supra.tf,DC=serba,DC=local
Mikołaj;Staszewski;mstaszewski;mstaszewski@serba.website;aleja
Niepodległości 49;Tychy;43-100;śląskie;PL;Handlowy;Zaq12wsx!;32 776 33
33;Specjalista ds.
handlowych;it.supra.tf;OU=Handlowy,OU=it.supra.tf,DC=serba,DC=local
Adam;Rekowski;arekowski;arekowski@serba.website;aleja Niepodległości
49;Tychy;43-100;śląskie;PL;Handlowy;Zaq12wsx!;32 776 33 33;Specjalista
ds. handlowych;it.supra.tf;OU=Handlowy,OU=it.supra.tf,DC=serba,DC=local

```

```
Joachim;Grabiński;jgrabinski;jgrabinski@serba.website;aleja
Niepodległości 49;Tychy;43-100;śląskie;PL;Handlowy;Zaq12wsx!;32 776 33
33;Specjalista ds.
handlowych;it.supra.tf;OU=Handlowy,OU=it.supra.tf,DC=serba,DC=local
Norbert;Ewertowski;newertowski;newertowski@serba.website;aleja
Niepodległości 49;Tychy;43-100;śląskie;PL;Handlowy;Zaq12wsx!;32 776 33
33;Specjalista ds.
handlowych;it.supra.tf;OU=Handlowy,OU=it.supra.tf,DC=serba,DC=local
Aureliusz;Wręczycki;awreczycki;awreczycki@serba.website;aleja
Niepodległości 49;Tychy;43-100;śląskie;PL;Handlowy;Zaq12wsx!;32 776 33
33;Specjalista ds.
handlowych;it.supra.tf;OU=Handlowy,OU=it.supra.tf,DC=serba,DC=local
Heronim;Ambroży;hambrozy;hambrozy@serba.website;aleja Niepodległości
49;Tychy;43-100;śląskie;PL;Handlowy;Zaq12wsx!;32 776 33 33;Specjalista
ds. handlowych;it.supra.tf;OU=Handlowy,OU=it.supra.tf,DC=serba,DC=local
Piotr;Jaroszek;pjaroszek;pjaroszek@serba.website;aleja Niepodległości
49;Tychy;43-100;śląskie;PL;Handlowy;Zaq12wsx!;32 776 33 33;Specjalista
ds. handlowych;it.supra.tf;OU=Handlowy,OU=it.supra.tf,DC=serba,DC=local
Miłosz;Szczesniak;mszesniak;mszesniak@serba.website;aleja Niepodległości
49;Tychy;43-100;śląskie;PL;Handlowy;Zaq12wsx!;32 776 33 33;Specjalista
ds. handlowych;it.supra.tf;OU=Handlowy,OU=it.supra.tf,DC=serba,DC=local
Eustachy;Kowalewski;ekowalewski;ekowalewski@serba.website;aleja
Niepodległości 49;Tychy;43-100;śląskie;PL;Handlowy;Zaq12wsx!;32 776 33
33;Specjalista ds.
handlowych;it.supra.tf;OU=Handlowy,OU=it.supra.tf,DC=serba,DC=local
Dorian;Kłopotowski;dkłopotowski;dkłopotowski@serba.website;aleja
Niepodległości 49;Tychy;43-100;śląskie;PL;Handlowy;Zaq12wsx!;32 776 33
33;Specjalista ds.
handlowych;it.supra.tf;OU=Handlowy,OU=it.supra.tf,DC=serba,DC=local
Olgierd;Zaniewski;ozaniewski;ozaniewski@serba.website;aleja
Niepodległości 49;Tychy;43-100;śląskie;PL;Handlowy;Zaq12wsx!;32 776 33
33;Specjalista ds.
handlowych;it.supra.tf;OU=Handlowy,OU=it.supra.tf,DC=serba,DC=local
Gracjan;Zambrzycki;gzambrzycki;gzambrzycki@serba.website;aleja
Niepodległości 49;Tychy;43-100;śląskie;PL;Handlowy;Zaq12wsx!;32 776 33
33;Specjalista ds.
handlowych;it.supra.tf;OU=Handlowy,OU=it.supra.tf,DC=serba,DC=local
Fabian;Ciura;fciura;fciura@serba.website;aleja Niepodległości
49;Tychy;43-100;śląskie;PL;Handlowy;Zaq12wsx!;32 776 33 33;Specjalista
ds. handlowych;it.supra.tf;OU=Handlowy,OU=it.supra.tf,DC=serba,DC=local
Piotr;Skonieczny;pskonieczny;pskonieczny@serba.website;aleja
Niepodległości 49;Tychy;43-100;śląskie;PL;Handlowy;Zaq12wsx!;32 776 33
33;Specjalista ds.
handlowych;it.supra.tf;OU=Handlowy,OU=it.supra.tf,DC=serba,DC=local
```

D.3. Załącznik 3 – Fragment wyniku skryptu tworzącego skrzynki w

Exchange 2019 na podstawie kont w domenie Active Directory

```

RunspaceId                               : 3a8a5892-cbc9-42ec-ad33-
c693fb7b379b
Database                                 : DB01
MailboxProvisioningConstraint             :
MailboxRegion                             :
MailboxRegionLastUpdateTime               :
MessageCopyForSentAsEnabled               : False
MessageCopyForSendOnBehalfEnabled         : False
MailboxProvisioningPreferences            : {}
UseDatabaseRetentionDefaults              : True
RetainDeletedItemsUntilBackup             : False
DeliverToMailboxAndForward                : False
IsExcludedFromServingHierarchy            : False
IsHierarchyReady                          : True
IsHierarchySyncEnabled                    : True
HasSnackyAppData                          : False
LitigationHoldEnabled                     : False
SingleItemRecoveryEnabled                 : False
RetentionHoldEnabled                      : False
EndDateForRetentionHold                   :
StartDateForRetentionHold                  :
RetentionComment                          :
RetentionUrl                              :
LitigationHoldDate                        :
LitigationHoldOwner                       :
ElcProcessingDisabled                     : False
ComplianceTagHoldApplied                  : False
WasInactiveMailbox                        : False
DelayHoldApplied                          : False
InactiveMailboxRetireTime                  :
OrphanSoftDeleteTrackingTime               :
LitigationHoldDuration                    : Unlimited
ManagedFolderMailboxPolicy               :
RetentionPolicy                           :
AddressBookPolicy                         :
CalendarRepairDisabled                    : False
ExchangeGuid                              : f92e33e2-1535-45e8-8ded-
8396c3894b72
MailboxContainerGuid                      :
UnifiedMailbox                            :
MailboxLocations                          : {1;f92e33e2-1535-45e8-8ded-
8396c3894b72;Primary;serba.local;5c902cf2-1e92-46d5
-8bed-d834bd1959d9}
AggregatedMailboxGuids                    : {}
ExchangeSecurityDescriptor                :
System.Security.AccessControl.RawSecurityDescriptor
ExchangeUserAccountControl                : None

```

```

AdminDisplayVersion           :
MessageTrackingReadStatusEnabled : True
ExternalOofOptions            : External
ForwardingAddress             :
ForwardingSmtppAddress        :
RetainDeletedItemsFor         : 14.00:00:00
IsMailboxEnabled              : True
Languages                     : {}
OfflineAddressBook            :
ProhibitSendQuota              : Unlimited
ProhibitReceiveQuota          : Unlimited
RecoverableItemsQuota         : 30 GB (32,212,254,720 bytes)
RecoverableItemsWarningQuota  : 20 GB (21,474,836,480 bytes)
CalendarLoggingQuota          : 6 GB (6,442,450,944 bytes)
DowngradeHighPriorityMessagesEnabled : False
ProtocolSettings              : {}
RecipientLimits               : Unlimited
ImListMigrationCompleted      : False
SiloName                      :
IsResource                    : False
IsLinked                      : False
IsShared                      : False
IsRootPublicFolderMailbox    : False
LinkedMasterAccount           :
ResetPasswordOnNextLogon      : False
ResourceCapacity              :
ResourceCustom                : {}
ResourceType                  :
RoomMailboxAccountEnabled     :
SamAccountName                : awesolowska
SCLDeleteThreshold            :
SCLDeleteEnabled              :
SCLRejectThreshold            :
SCLRejectEnabled              :
SCLQuarantineThreshold        :
SCLQuarantineEnabled          :
SCLJunkThreshold              :
SCLJunkEnabled                :
AntispamBypassEnabled         : False
ServerLegacyDN                : /o=serba/ou=Exchange
Administrative Group (FYDIBOHF23SPDLT)/cn=Configuration/cn=Servers/cn=EXCHANGE
ServerName                    : exchange
UseDatabaseQuotaDefaults      : True
IssueWarningQuota             : Unlimited
RulesQuota                    : 256 KB (262,144 bytes)
Office                        : SERBA Headquarters
UserPrincipalName             : awesolowska@serba.local
UMEnabled                     : False
MaxSafeSenders                :
MaxBlockedSenders             :
NetID                         :
ReconciliationId              :
WindowsLiveID                 :
MicrosoftOnlineServicesID     :
ThrottlingPolicy              :
RoleAssignmentPolicy           : Default Role Assignment Policy

```

```

DefaultPublicFolderMailbox      :
EffectivePublicFolderMailbox    :
SharingPolicy                   :
RemoteAccountPolicy             :
MailboxPlan                     :
ArchiveDatabase                 :
ArchiveGuid                     : 00000000-0000-0000-0000-
000000000000
ArchiveName                     : {}
JournalArchiveAddress           :
ArchiveQuota                    : 100 GB (107,374,182,400 bytes)
ArchiveWarningQuota             : 90 GB (96,636,764,160 bytes)
ArchiveDomain                   :
ArchiveStatus                   : None
ArchiveState                    : None
AutoExpandingArchiveEnabled     : False
DisabledMailboxLocations        : False
RemoteRecipientType             : None
DisabledArchiveDatabase         :
DisabledArchiveGuid             : 00000000-0000-0000-0000-
000000000000
QueryBaseDN                    :
QueryBaseDNRestrictionEnabled   : False
MailboxMoveTargetMDB            :
MailboxMoveSourceMDB            :
MailboxMoveFlags                : None
MailboxMoveRemoteHostName       :
MailboxMoveBatchName            :
MailboxMoveStatus               : None
MailboxRelease                  :
ArchiveRelease                  :
IsPersonToPersonTextMessagingEnabled : False
IsMachineToPersonTextMessagingEnabled : False
UserSMimeCertificate            : {}
UserCertificate                 : {}
CalendarVersionStoreDisabled    : False
ImmutableId                    :
PersistedCapabilities            : {}
SKUAssigned                     :
AuditEnabled                    : False
AuditLogAgeLimit                : 90.00:00:00
AuditAdmin                      : {Update, Move,
MoveToDeletedItems, SoftDelete, HardDelete, FolderBind, SendAs,
SendOnBehalf, Create,
UpdateFolderPermissions, UpdateInboxRules, UpdateCalendarDelegation}
AuditDelegate                   : {Update, SoftDelete, HardDelete,
SendAs, Create, UpdateFolderPermissions, UpdateInboxRules}
AuditOwner                      : {UpdateFolderPermissions,
UpdateInboxRules, UpdateCalendarDelegation}
WhenMailboxCreated              : 22.02.2021 22:41:18
SourceAnchor                    :
UsageLocation                   :
IsSoftDeletedByRemove           : False
IsSoftDeletedByDisable          : False
IsInactiveMailbox               : False

```

```

IncludeInGarbageCollection      : False
WhenSoftDeleted                :
InPlaceHolds                   : {}
GeneratedOfflineAddressBooks   : {}
AccountDisabled                : False
StsRefreshTokensValidFrom      :
DataEncryptionPolicy           :
DisableThrottling              : False
Extensions                     : {}
HasPicture                     : False
HasSpokenName                  : False
IsDirSynced                    : False
AcceptMessagesOnlyFrom         : {}
AcceptMessagesOnlyFromDLMembers : {}
AcceptMessagesOnlyFromSendersOrMembers : {}
AddressListMembership           : {\All Users, \Default Global
Address List, \All Recipients(VLV), \All Mailboxe
                               s(VLV), \Mailboxes(VLV)}
AdministrativeUnits             : {}
Alias                          : awesolowska
ArbitrationMailbox             :
BypassModerationFromSendersOrMembers : {}
OrganizationalUnit             :
serba.local/it.supra.tf/Rozwojowy
CustomAttribute1               :
CustomAttribute10              :
CustomAttribute11              :
CustomAttribute12              :
CustomAttribute13              :
CustomAttribute14              :
CustomAttribute15              :
CustomAttribute2               :
CustomAttribute3               :
CustomAttribute4               :
CustomAttribute5               :
CustomAttribute6               :
CustomAttribute7               :
CustomAttribute8               :
CustomAttribute9               :
ExtensionCustomAttribute1      : {}
ExtensionCustomAttribute2      : {}
ExtensionCustomAttribute3      : {}
ExtensionCustomAttribute4      : {}
ExtensionCustomAttribute5      : {}
DisplayName                    : Anna Wesołowska
EmailAddresses                 : {SMTP:awesolowska@serba.website}
GrantSendOnBehalfTo            : {}
ExternalDirectoryObjectId       :
HiddenFromAddressListsEnabled   : False
LastExchangeChangedTime        :
LegacyExchangeDN               : /o=serba/ou=Exchange
Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=u
                               ser00cfea9c
MaxSendSize                    : Unlimited
MaxReceiveSize                 : Unlimited
ModeratedBy                    : {}
ModerationEnabled              : False

```

```

PoliciesIncluded : {{26491cfc-9e50-4857-861b-0cb8df22b5d7}, 6f89af6f-8e78-458f-b3b1-e01a002b82f5}
PoliciesExcluded : {}
EmailAddressPolicyEnabled : True
PrimarySmtpAddress : awesolowska@serba.website
RecipientType : UserMailbox
RecipientTypeDetails : UserMailbox
RejectMessagesFrom : {}
RejectMessagesFromDLMembers : {}
RejectMessagesFromSendersOrMembers : {}
RequireSenderAuthenticationEnabled : False
SimpleDisplayName :
SendModerationNotifications : Always
UMDtmfMap :
{firstNameLastName:26629376569752, lastNameFirstName:93765697522662, emailAddr
ess:29376569752}
WindowsEmailAddress : awesolowska@serba.website
MailTip :
MailTipTranslations : {}
Identity :
serba.local/it.supra.tf/Rozwojowy/Anna Wesołowska
IsValid : True
ExchangeVersion : 0.20 (15.0.0.0)
Name : Anna Wesołowska
DistinguishedName : CN=Anna Wesołowska,OU=Rozwojowy,OU=it.supra.tf,DC=serba,DC=local
Guid : b6a36fe1-5653-410f-92c2-0803a1f627fa
ObjectCategory :
serba.local/Configuration/Schema/Person
ObjectClass : {top, person, organizationalPerson, user}
WhenChanged : 22.02.2021 23:41:17
WhenCreated : 22.02.2021 23:22:01
WhenChangedUTC : 22.02.2021 22:41:17
WhenCreatedUTC : 22.02.2021 22:22:01
OrganizationId :
Id :
serba.local/it.supra.tf/Rozwojowy/Anna Wesołowska
OriginatingServer : dc1.serba.local
ObjectState : Unchanged

```