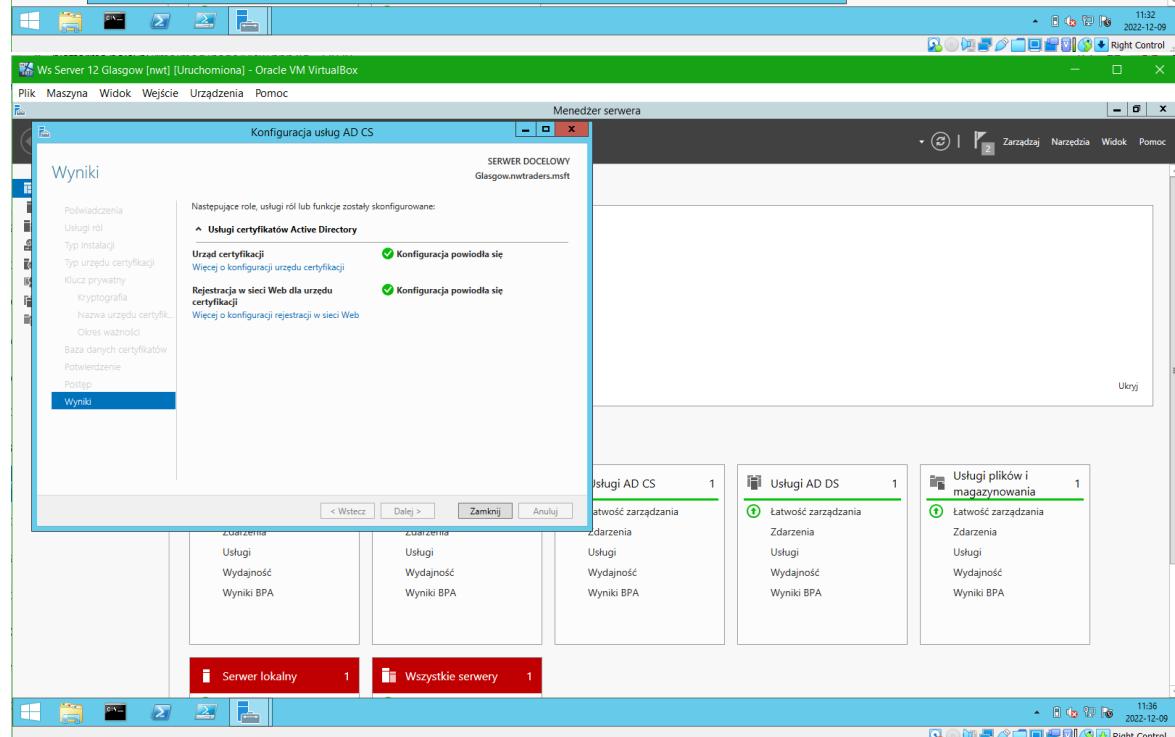
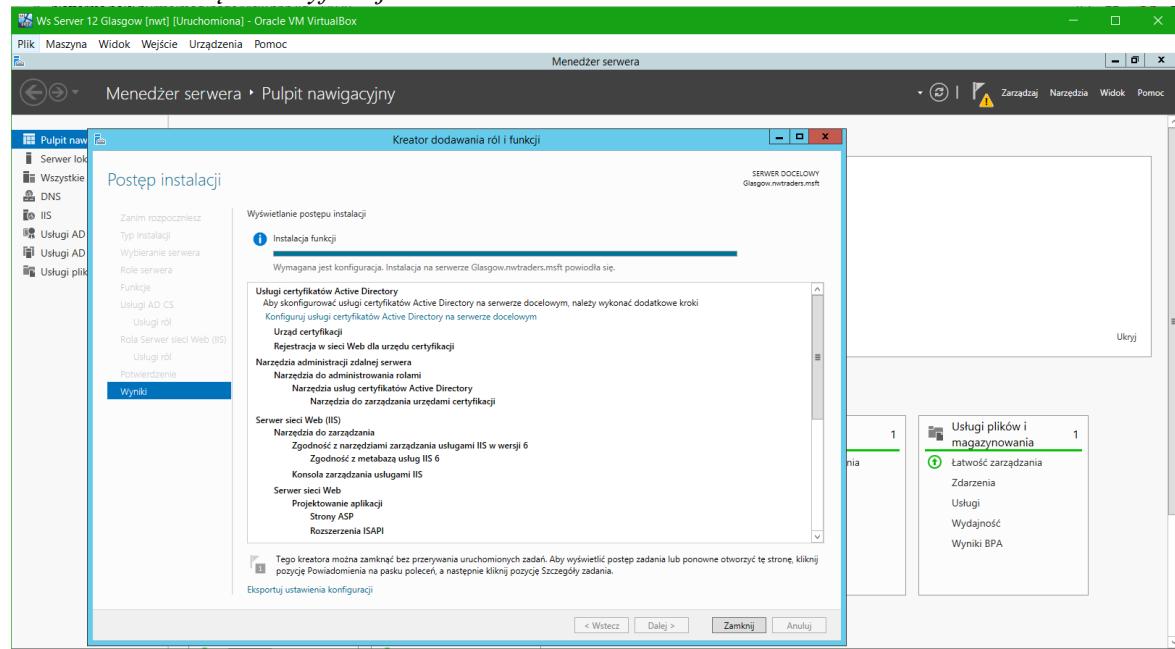


Laboratorium realizowane na zajęciach (Moduł 3) – Kryptograficzne metody ochrony informacji

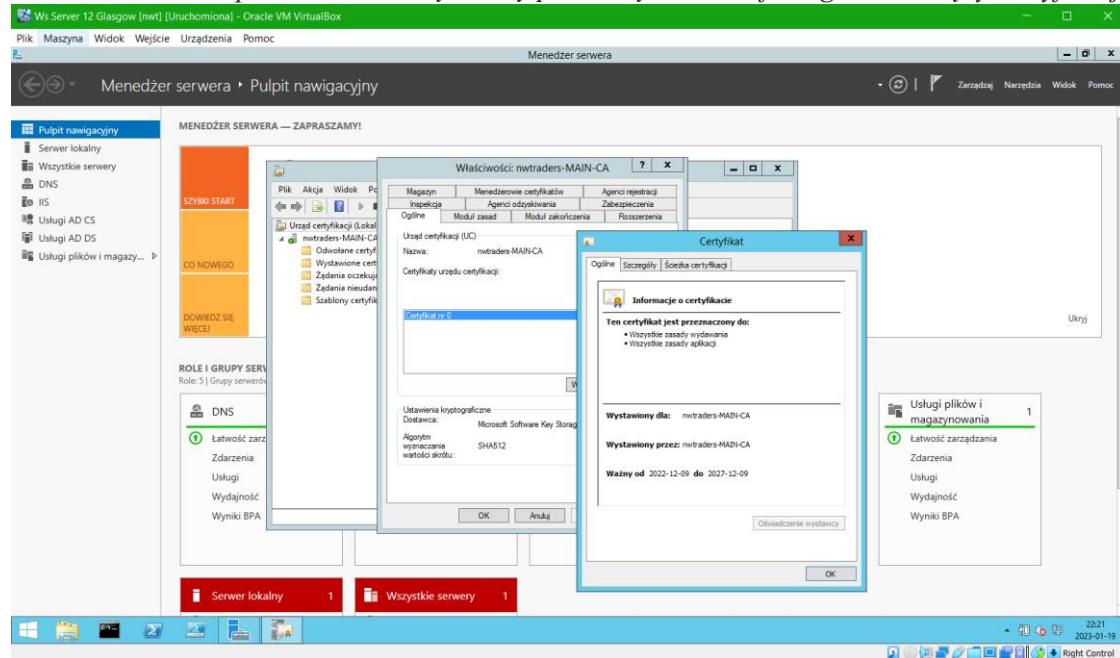
Zadanie 1

Zainstalowanie głównego serwera certyfikującego zintegrowanego z usługą Active Directory w systemie Windows Server, dla którego należy określić nazwę "*Nwtraders MAIN CA*", instalując rolę "*Usługi certyfikatów Active Directory*" wraz z usługami roli: "*Urząd certyfikacji*" oraz "*Rejestracja w sieci Web dla urzędu certyfikacji*".

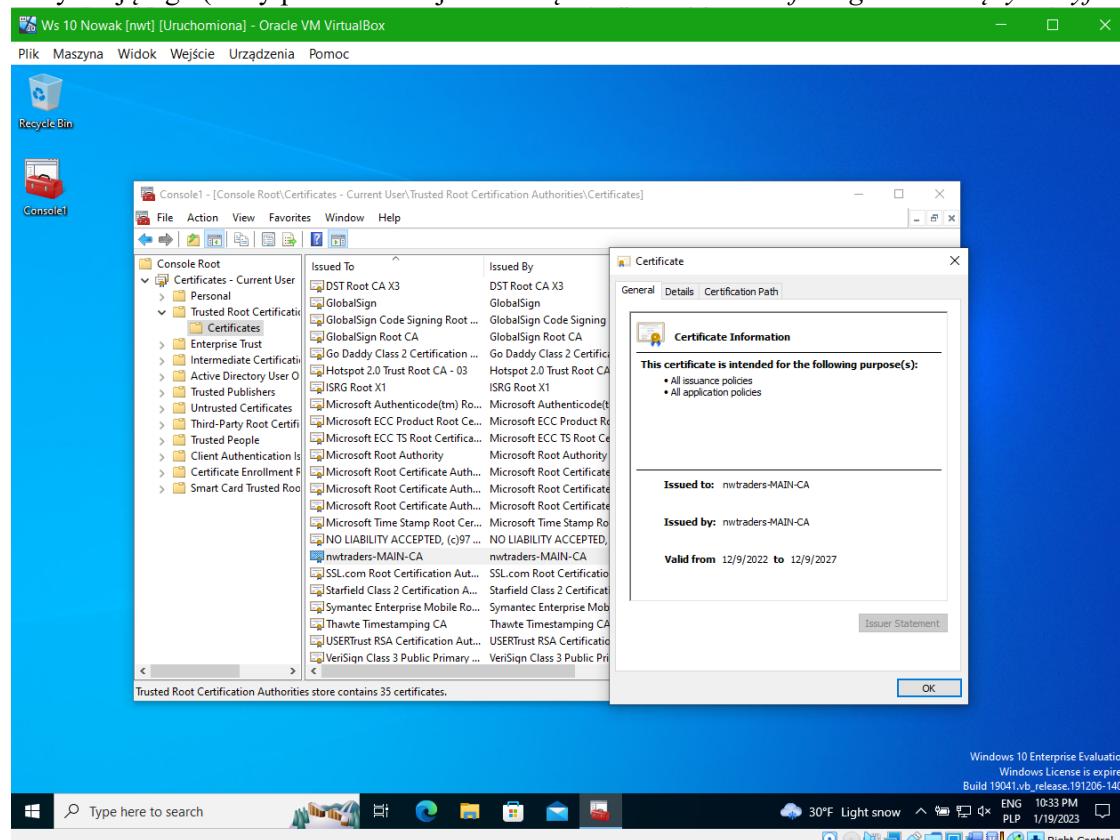


Zadanie 2

Wykorzystanie zasady grupy "Default Domain Policy" do zainportowania z pliku głównego urzędu certyfikującego (w kontenerze: Konfiguracja komputera-->Ustawienia systemu Windows-->Ustawienia zabezpieczeń-->Zasady kluczy publicznych-->Zaufane główne urzędy certyfikacji).

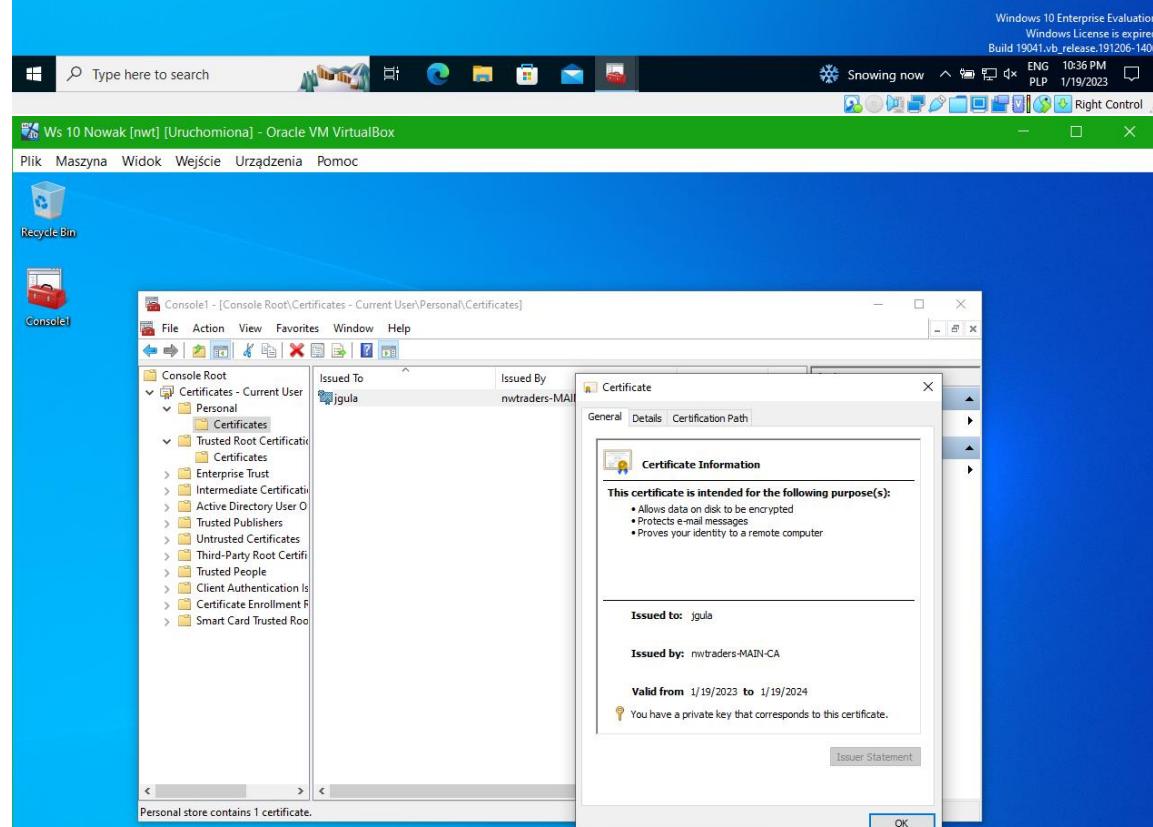
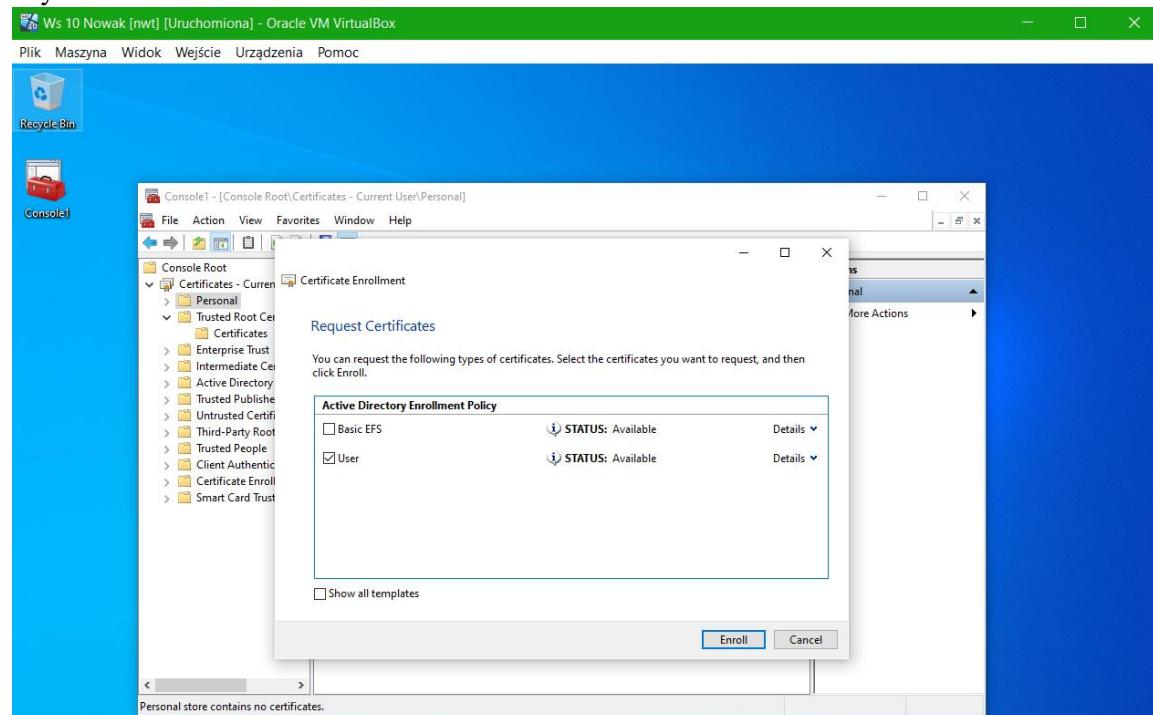


Zweryfikowanie w systemie Windows "Nowak" prawidłowego pobrania w/w certyfikatu poprzez wydanie polecenia "gpupdate /force" i uruchomienie konsoli MMC, a następnie dodanie do niej przystawki "Certyfikaty" (dla użytkownika), i zweryfikowania istnienia certyfikatu głównego urzędu certyfikującego (który powinien znajdować się w kontenerze "Zaufane główne urzędy certyfikujące").



Zadanie 3

Zalogowanie się w systemie Windows jako użytkownik *jgula* i wygenerowanie certyfikatu dla użytkownika.



Zadanie 4

Nadanie uprawnień dla J. Guli umożliwiających mu wygenerowania żądania o certyfikat "EFS Recovery Agent".

The screenshot shows the Windows Server 2012 R2 Control Panel with the 'Menedżer serwera' (Server Manager) open. A context menu is displayed over the 'Szablony certyfikatów (Glasgow)' item, with the 'Właściwości: Agent odzyskiwania EFS' (Properties: EFS Recovery Agent) option selected. The 'Ogólne' (General) tab is active, showing the 'Nazwa grupy lub użytkownika:' field populated with 'Jacek Gula (NWTRADERS\gula)'. Under 'Uprawnienia dla: jgula', the 'Odczyt' (Read) and 'Zapis' (Write) checkboxes are checked. A note at the bottom states: 'Kliknij przycisk Zaawansowane, aby przejść do szczegółowych uprawnień lub ustawień zaawansowanych.' (Click the Advanced button to view detailed permissions or advanced settings.)

Windows Server 2012 R2 - Menedżer serwera

Pulpit nawigacyjny

Szablony certyfikatów (Glasgow)

Właściwości: Agent odzyskiwania EFS

Ogólne

Nazwa grupy lub użytkownika: Jacek Gula (NWTRADERS\gula)

Uprawnienia dla: jgula

OK Anuluj Zastosuj Pomoc

Windows 10 Enterprise Evaluation - Konsola

Console1 - [Console Root\Certificates - Current User\Personal]

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

Active Directory Enrollment Policy

Certyfikat	Status	Akcje
Basic EFS	Available	Details
EFS Recovery Agent	Available	Details
User	Available	Details

Show all templates

Enroll Cancel

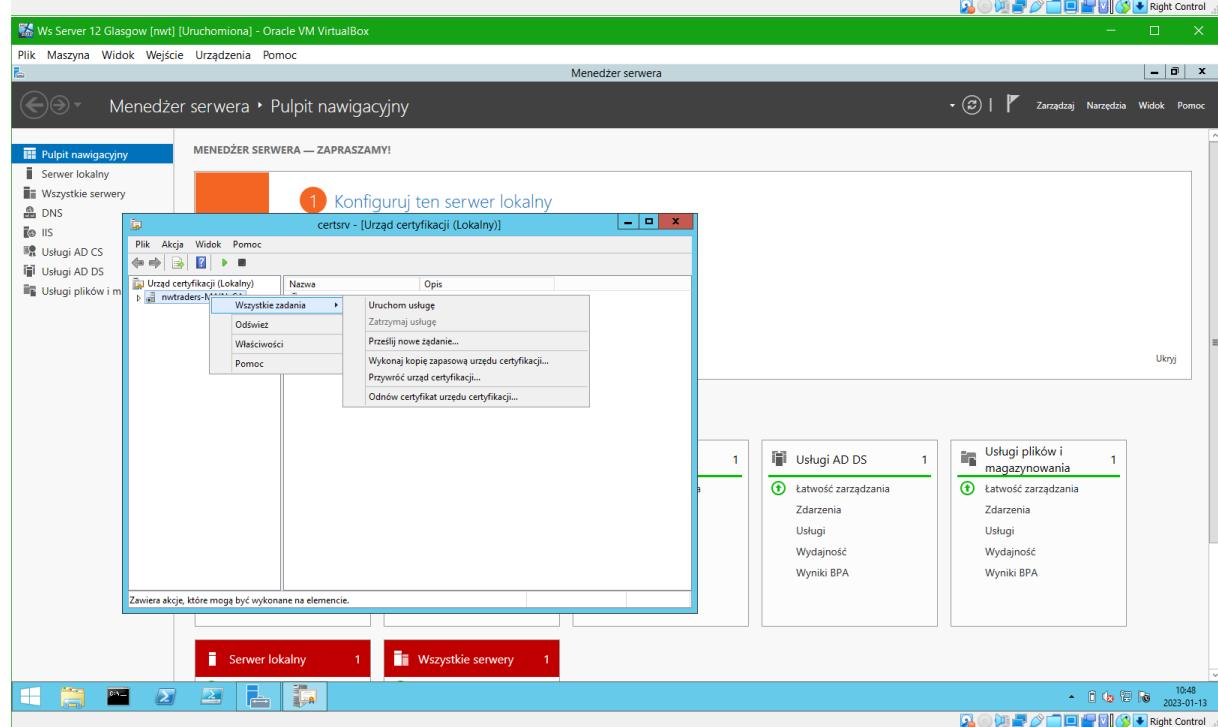
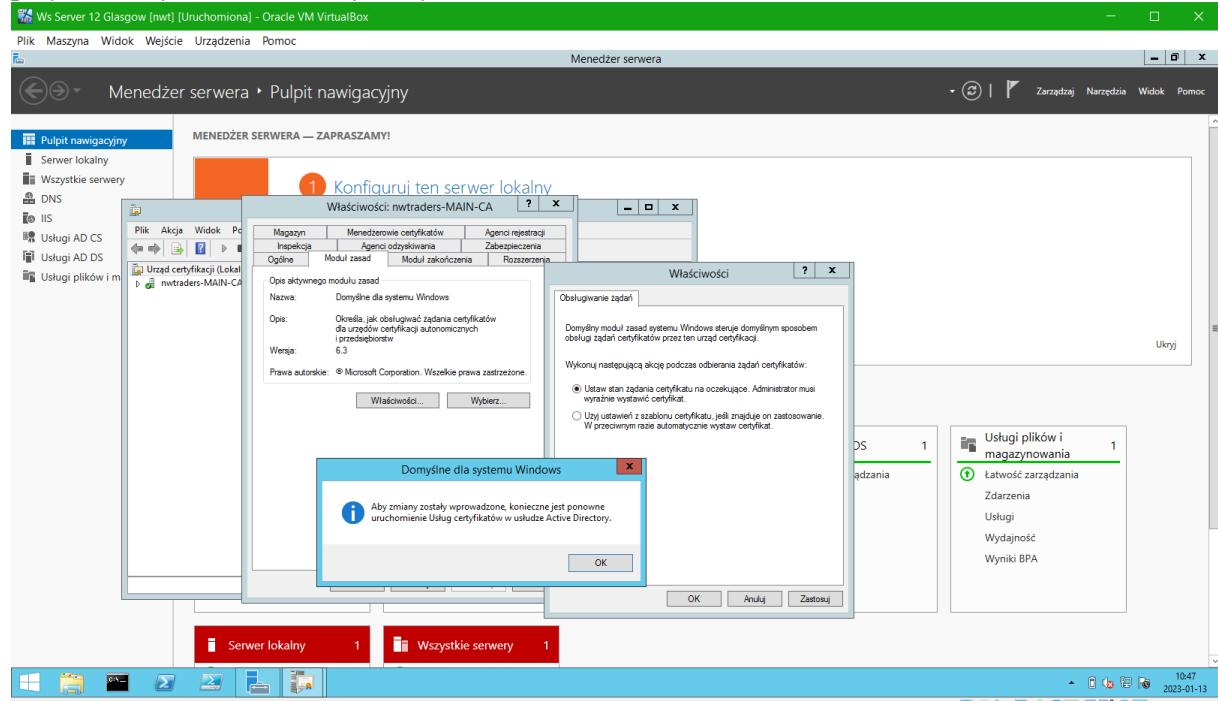
Windows License is expired
Build 19041.vb_release.191206-1406

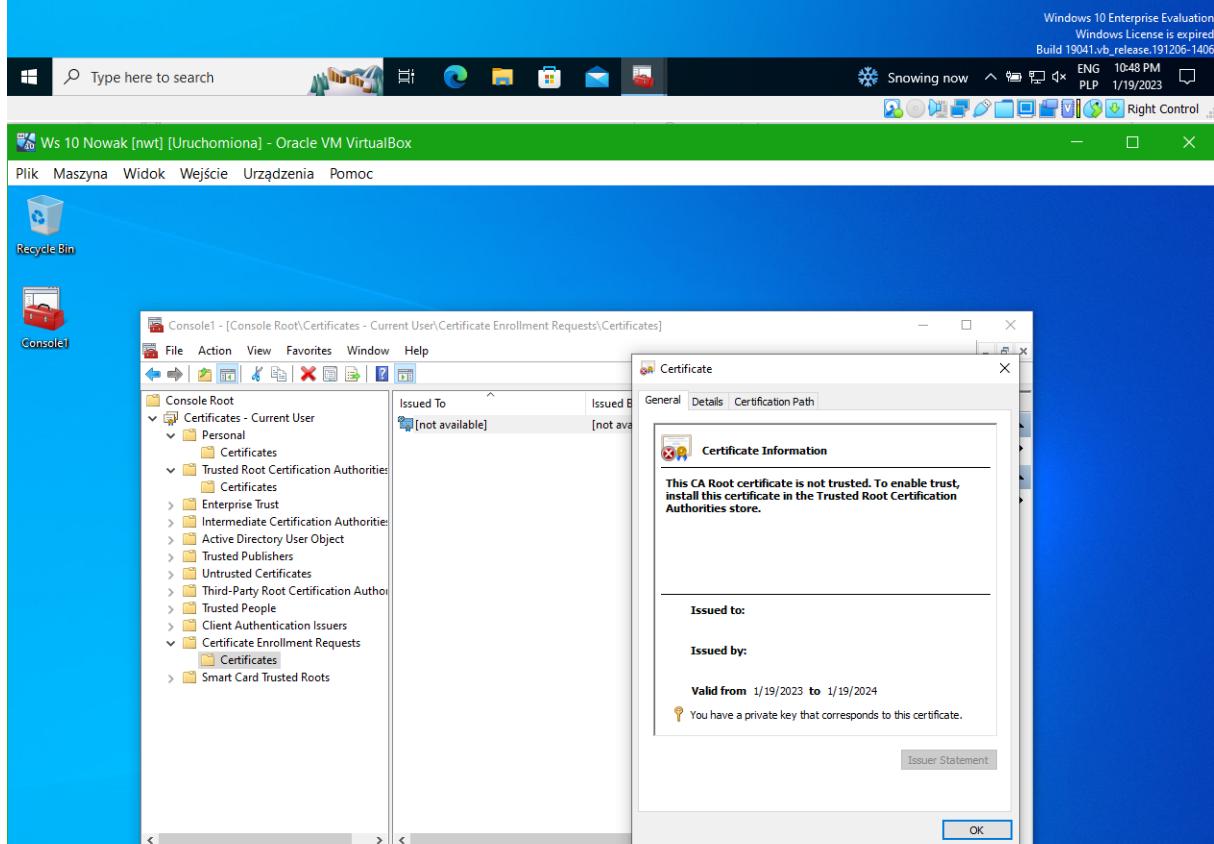
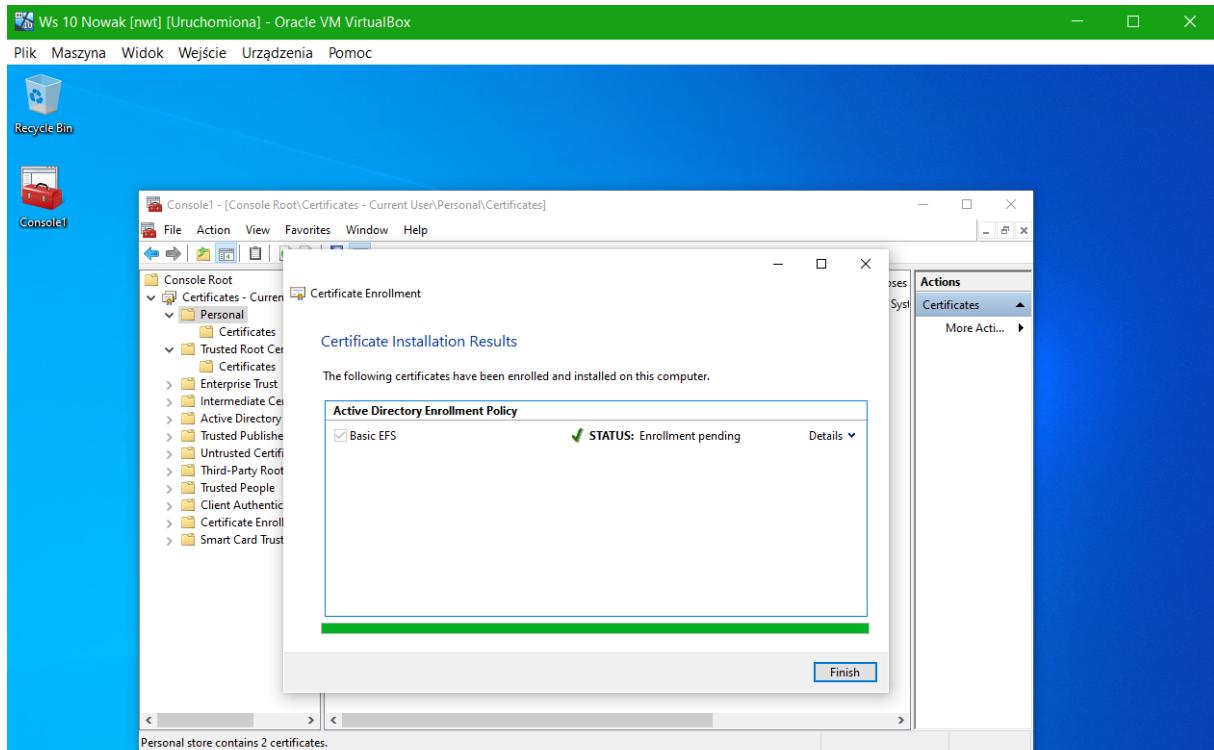
Type here to search

ENG 10:43 PM PLP 1/19/2023

Zadanie 5

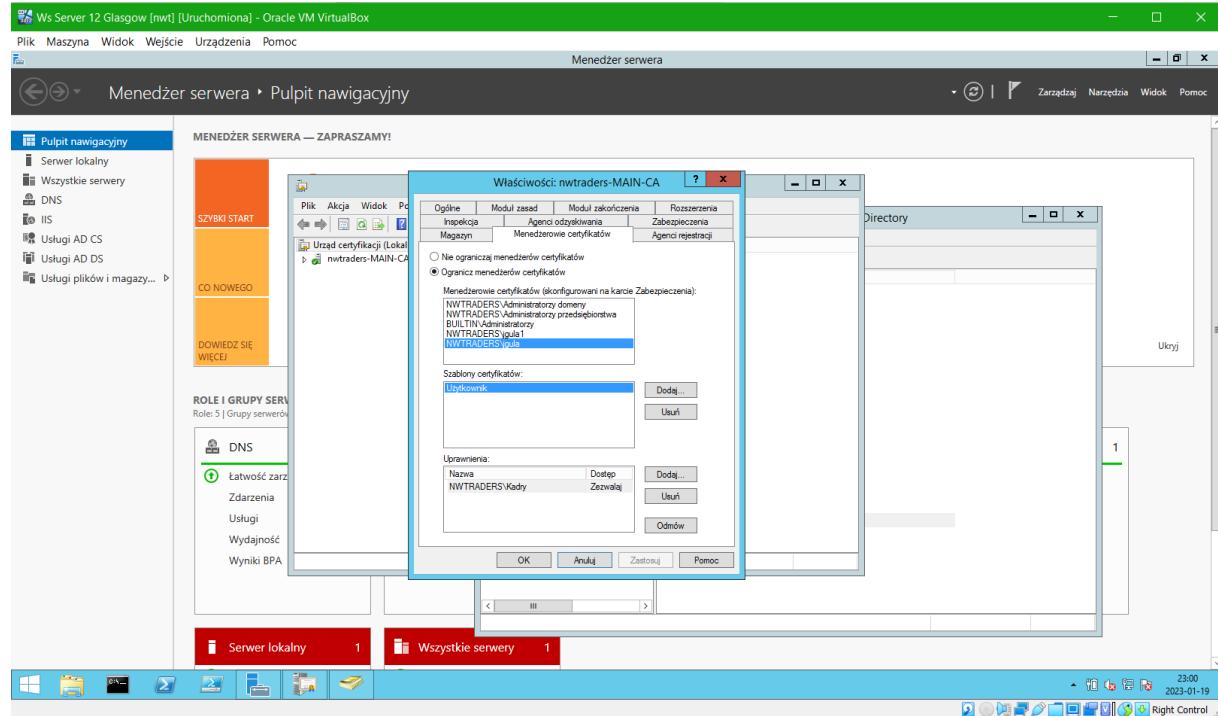
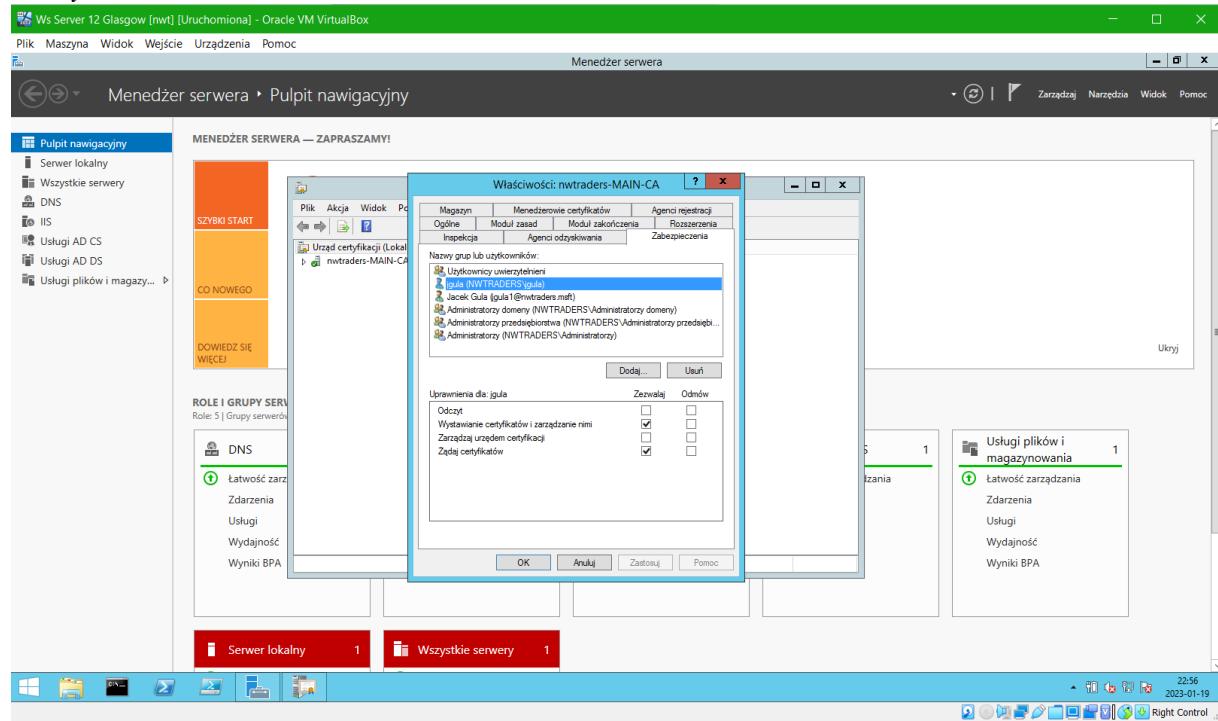
Włączenie wymuszenia ręcznego wyrażania zgody przez administratora Urzędu Certyfikacyjnego, dla przychodzących żądań o certyfikaty.





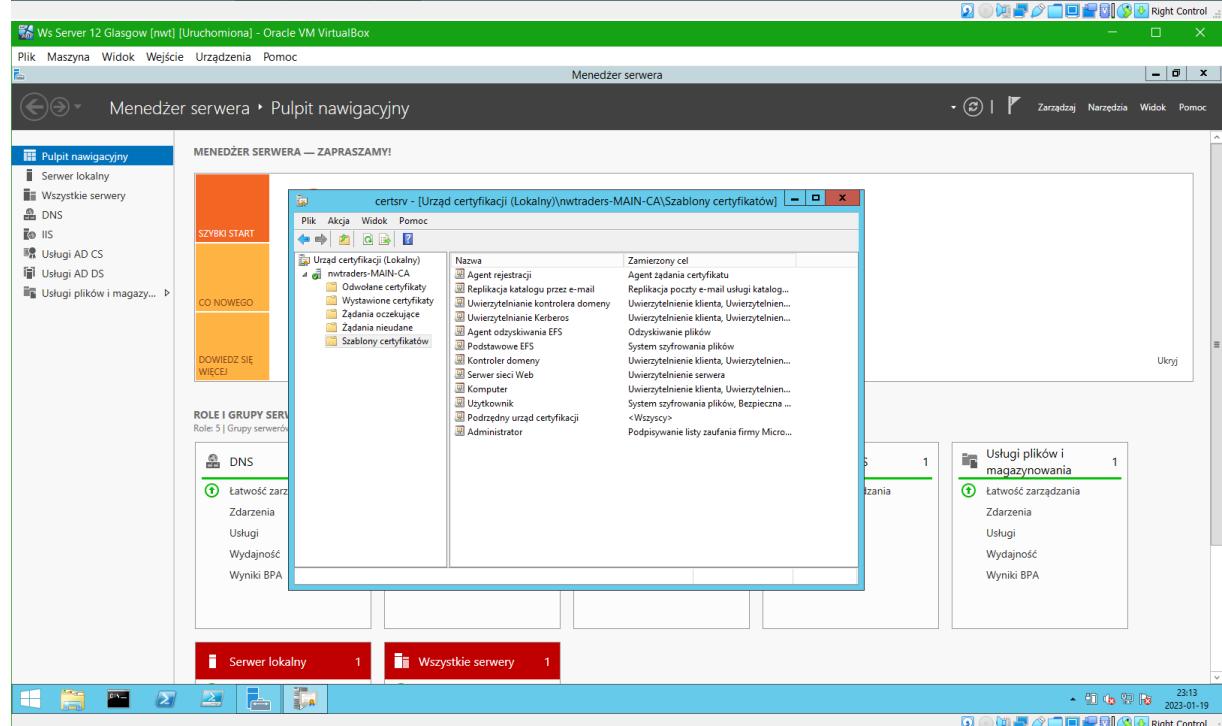
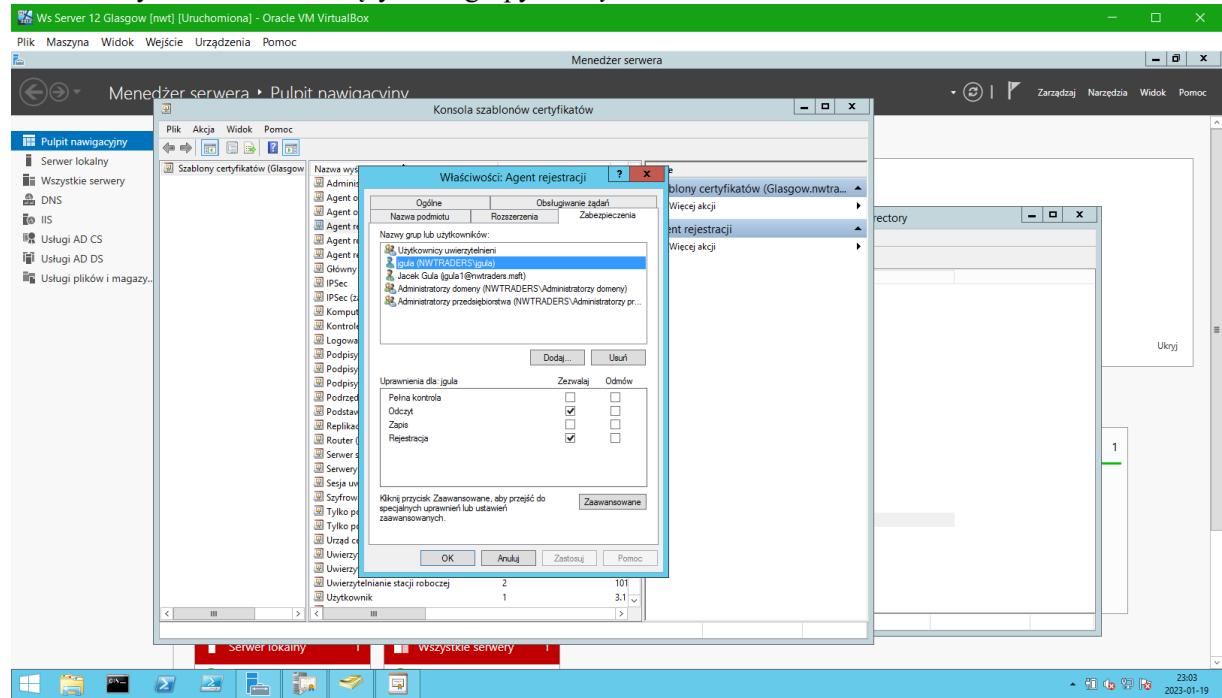
Zadanie 6

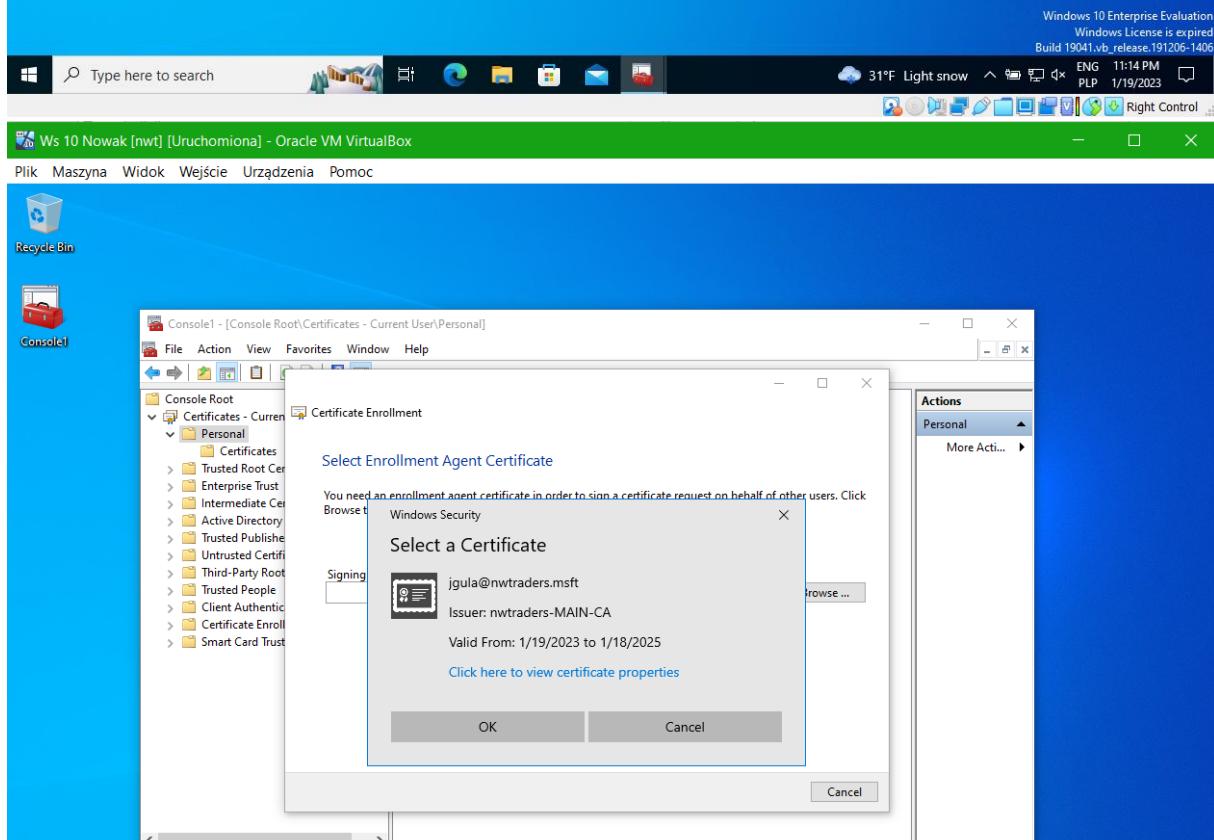
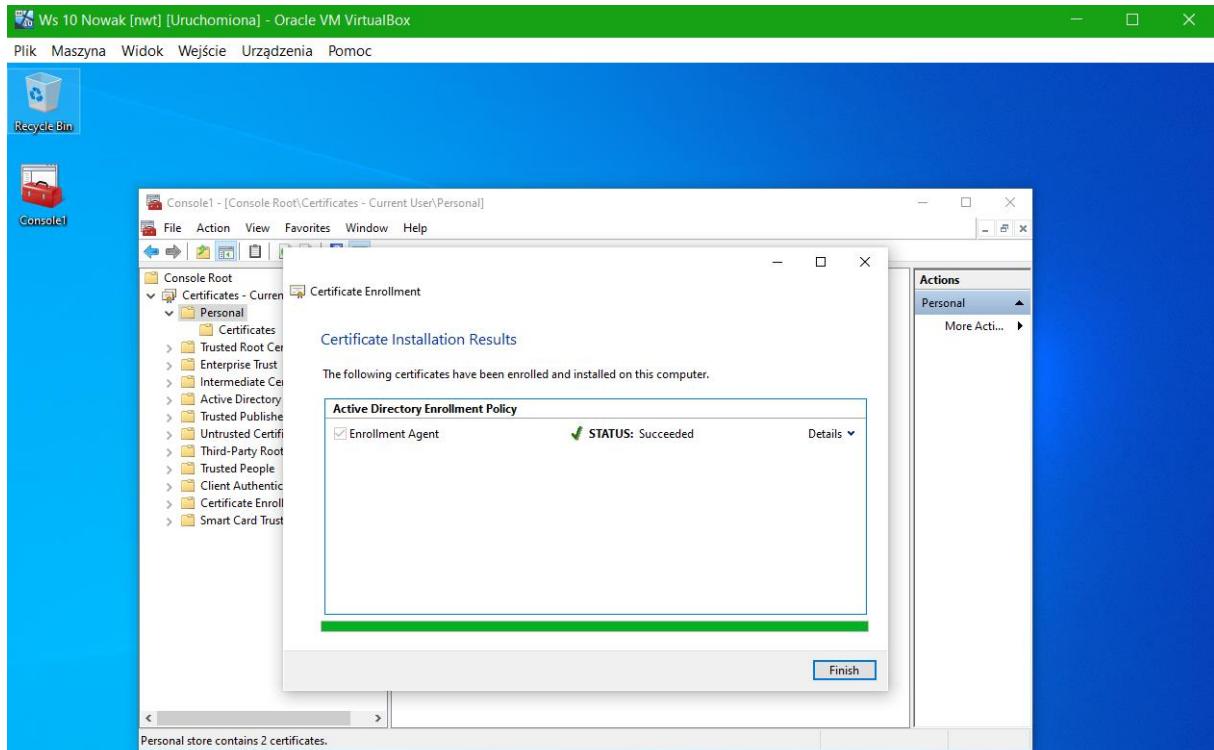
Nadanie uprawnień dla użytkownika *jgula* do zatwierdzania żądań o certyfikaty osobiste użytkowników oraz certyfikaty na potrzeby usługi EFS dla użytkowników należących do grupy *Kadry*.

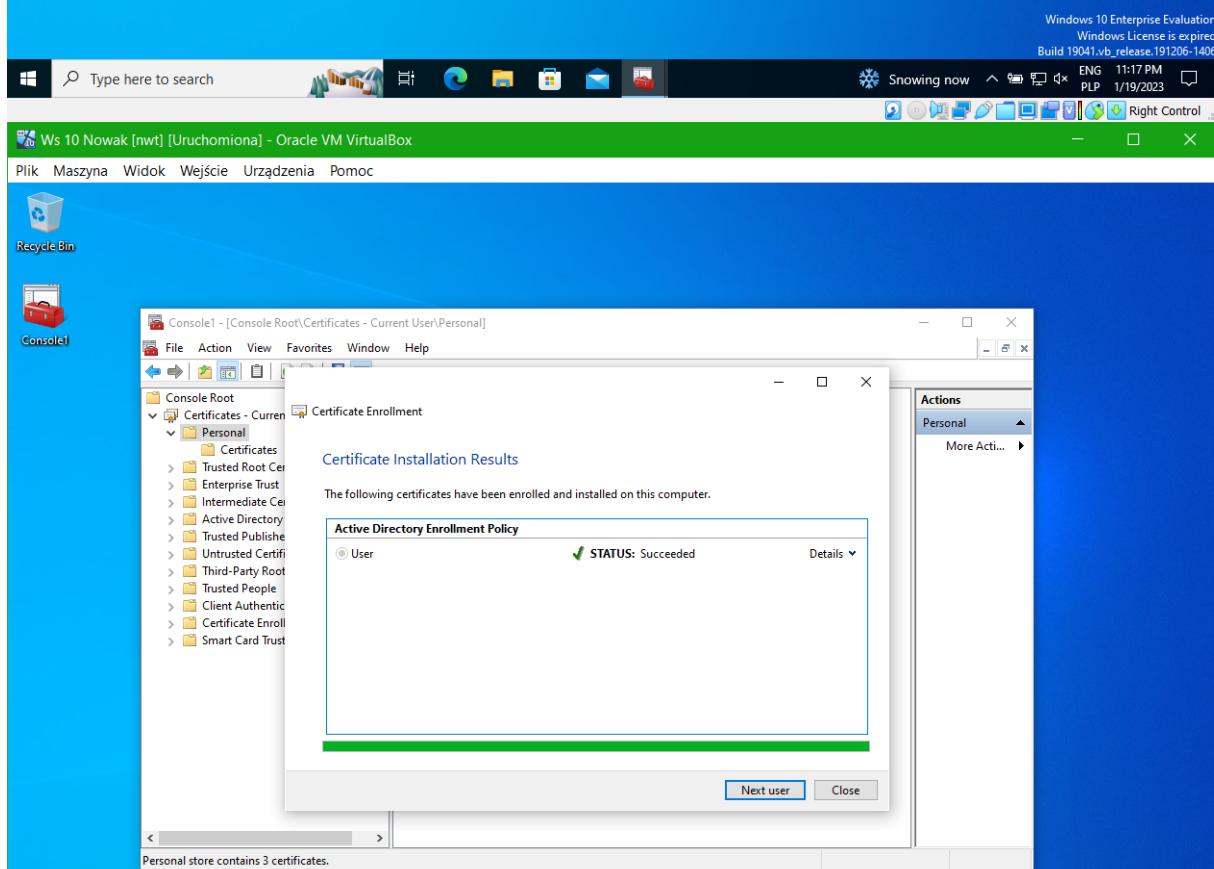
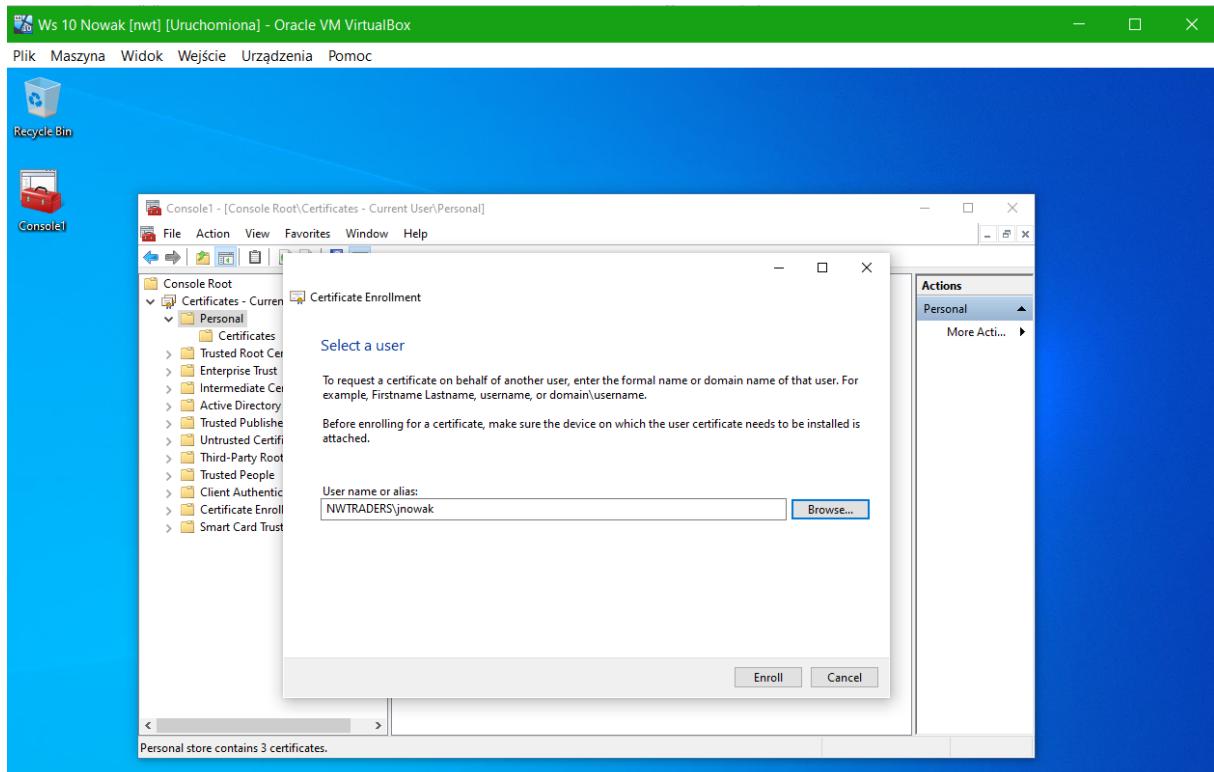


Zadanie 7

Nadanie uprawnień dla użytkownika *jgula* do występowania o certyfikaty osobiste użytkowników w imieniu użytkowników należących do grupy *Kadry*.

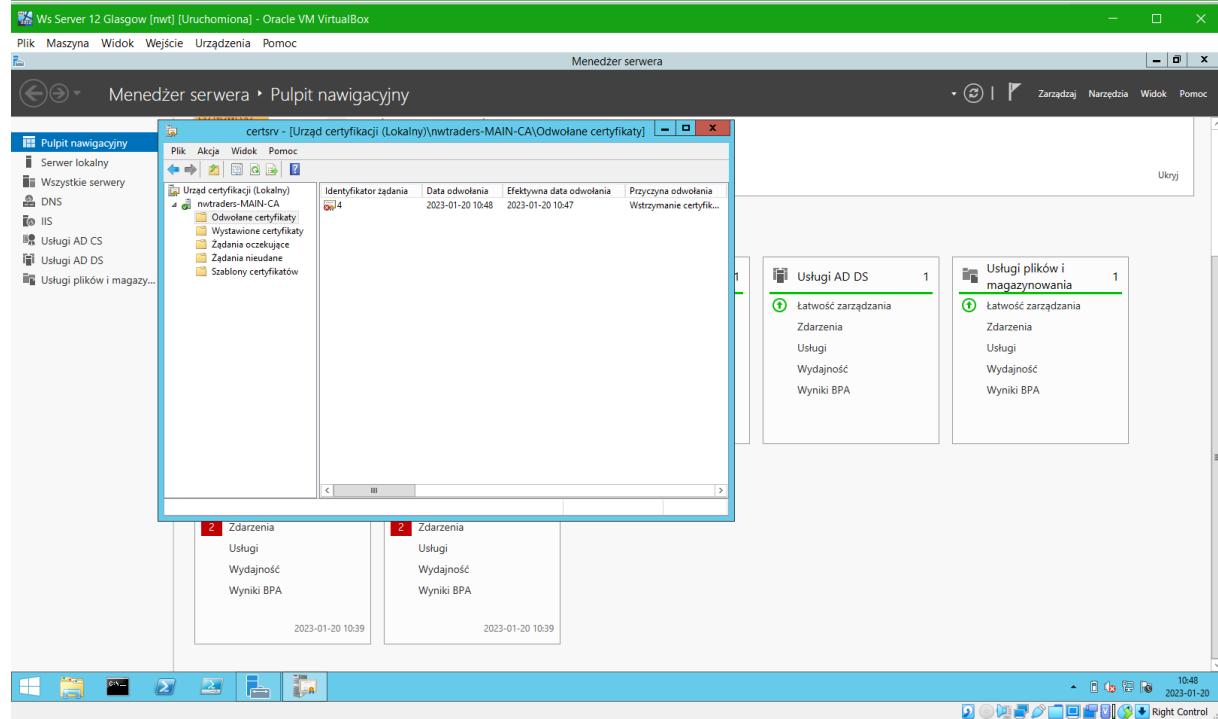
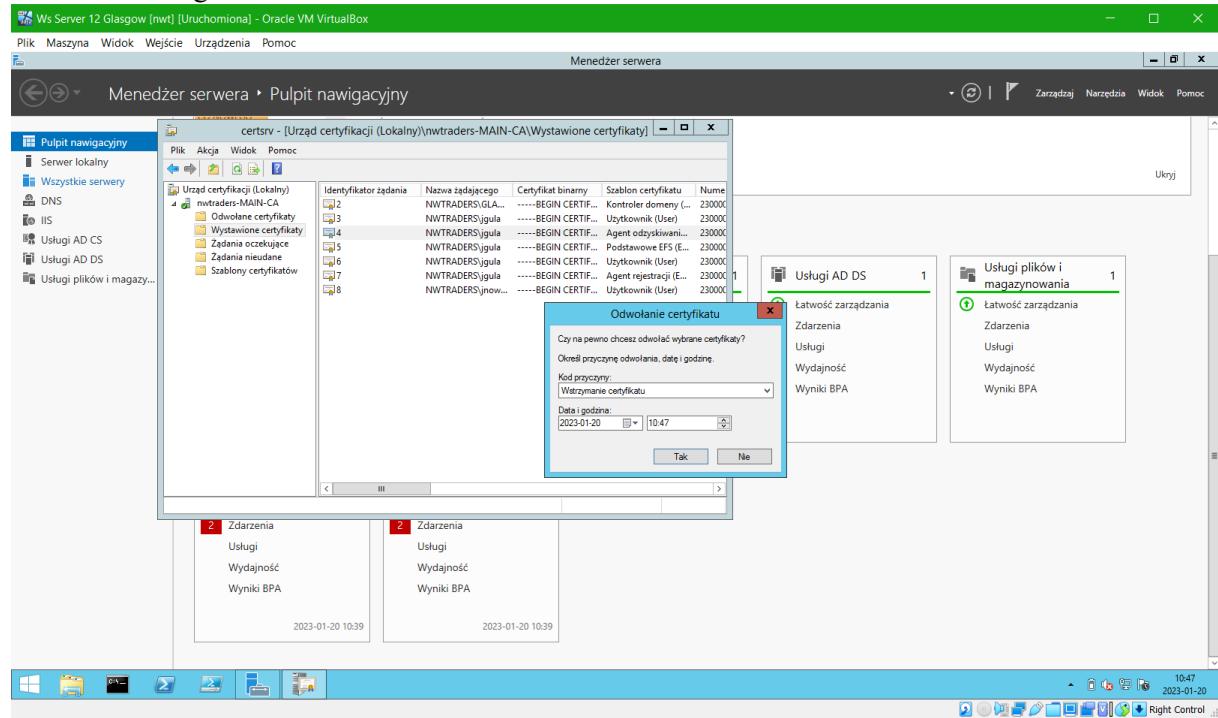






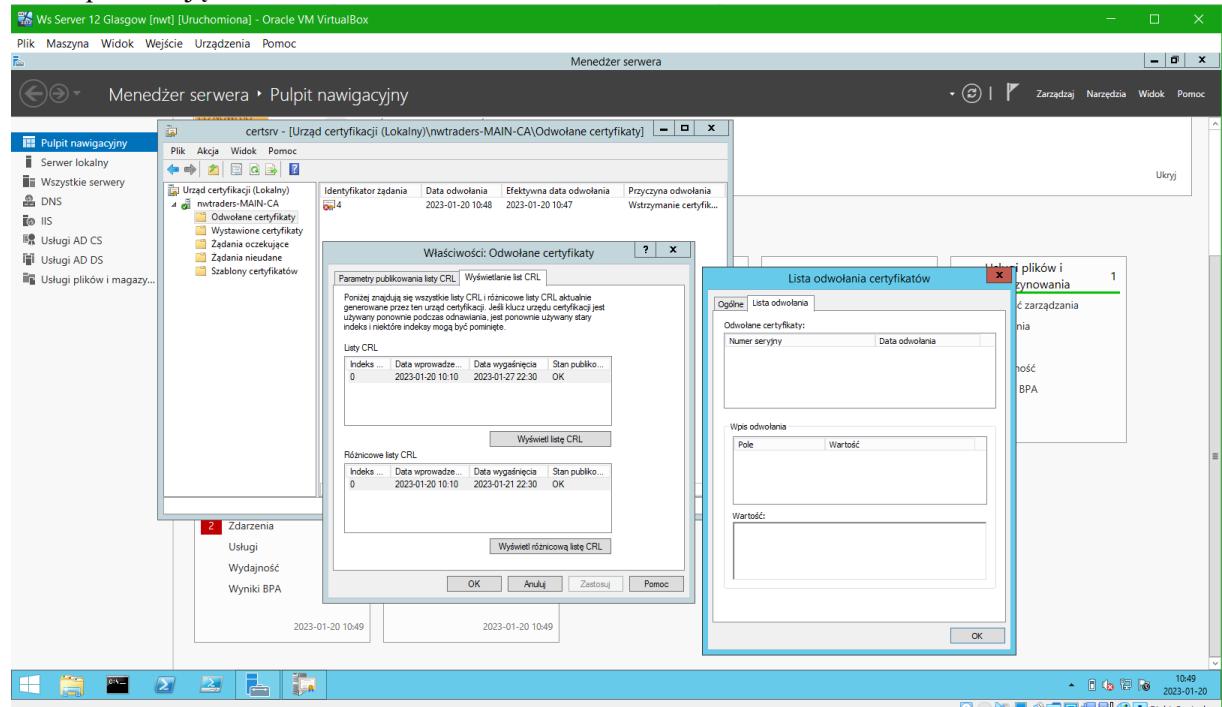
Zadanie 8

W systemie Windows Server uruchomić przystawkę do zarządzania urzędem certyfikacji, przejść do pozycji Nwtraders Main CA>Wystawione certyfikaty, znaleźć certyfikat "EFS Recovery Agent" J. Guli i odwołać go.

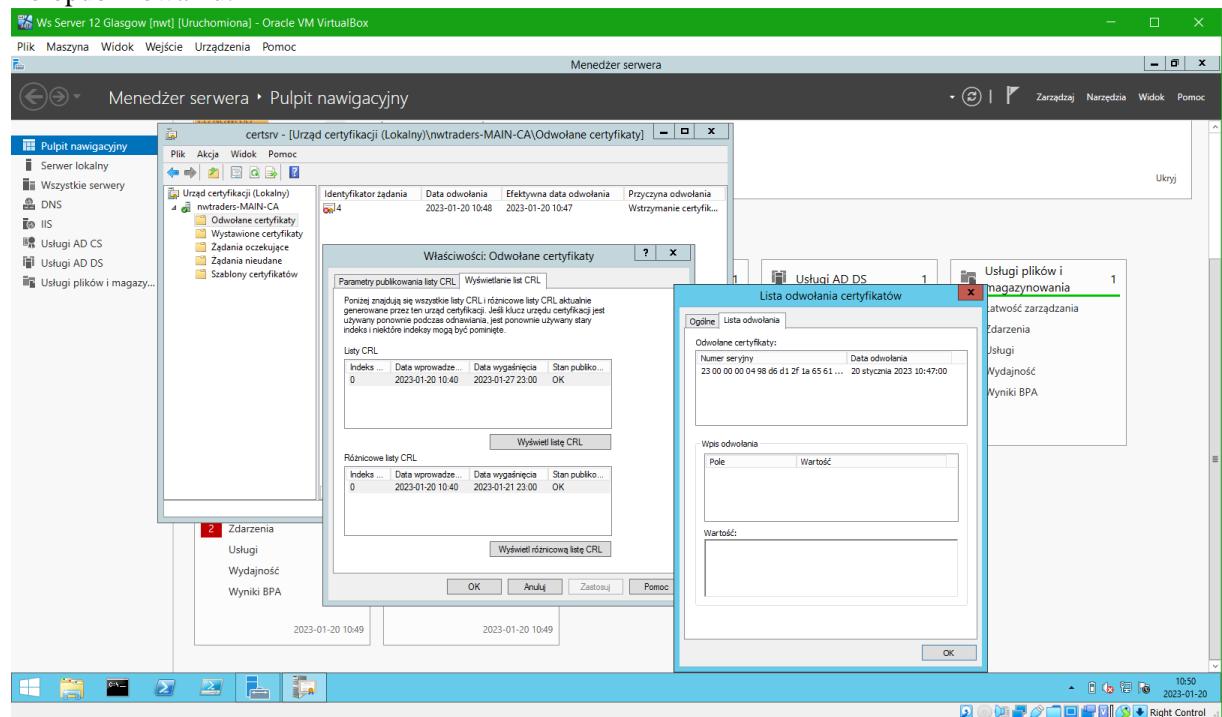


W przystawce do zarządzania urzędem certyfikacji nacisnąć prawym przyciskiem myszy na pozycję **Nwtraders Main CA>Odwołane certyfikaty**, z menu wybrać "Właściwości" i w zakładce "Wyświetlanie list CRL" znaleźć odwołany certyfikat "EFS Recovery Agent" J. Guli.

Przed publikacją:

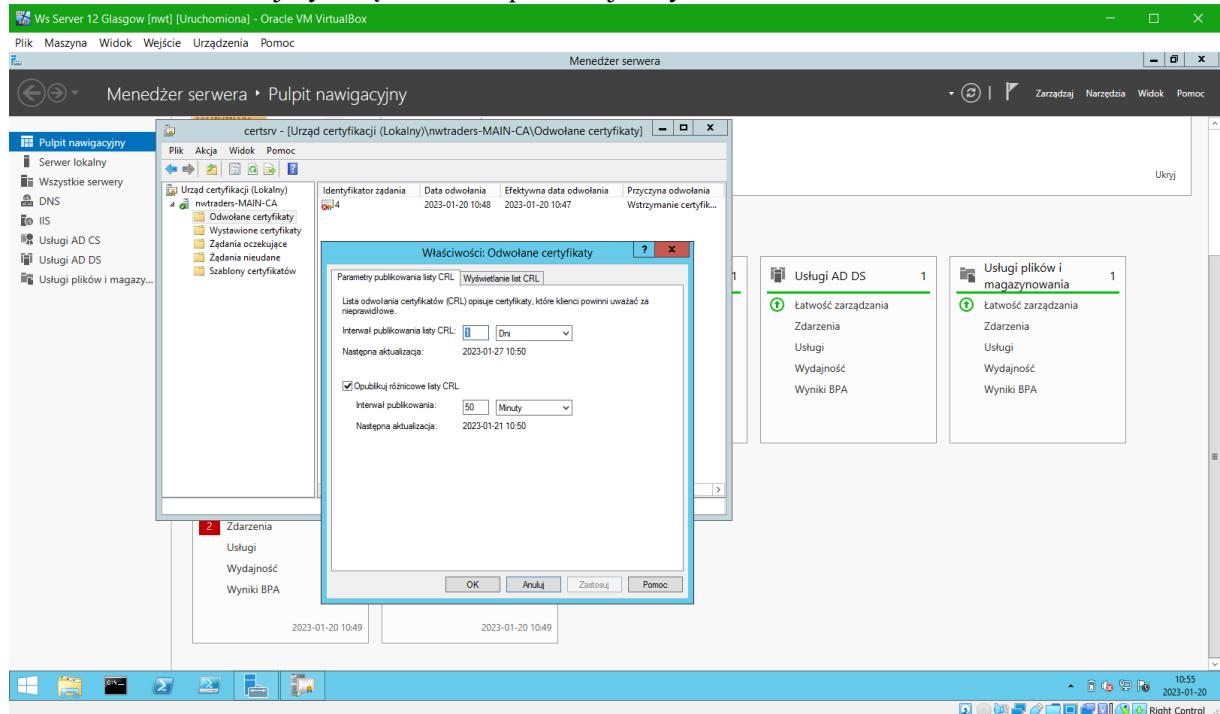


Po opublikowaniu:

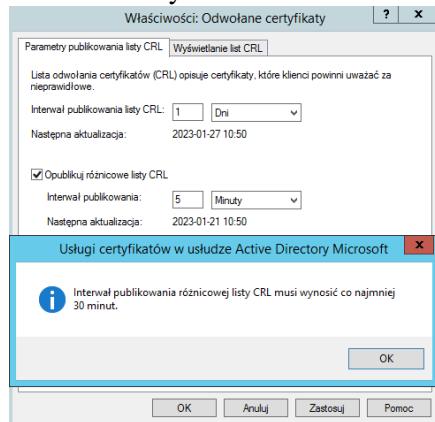


Zadanie 9

W systemie Windows Server uruchomić przystawkę do zarządzania urzędem certyfikacji, nacisnąć prawym przyciskiem myszy na pozycję *Nwtraders Main CA>Odwołane certyfikaty*, z menu wybrać "Właściwości" i zmniejszyć częstotliwość publikacji listy CRL do 1 dnia oraz Delta CRL do 5 minut.



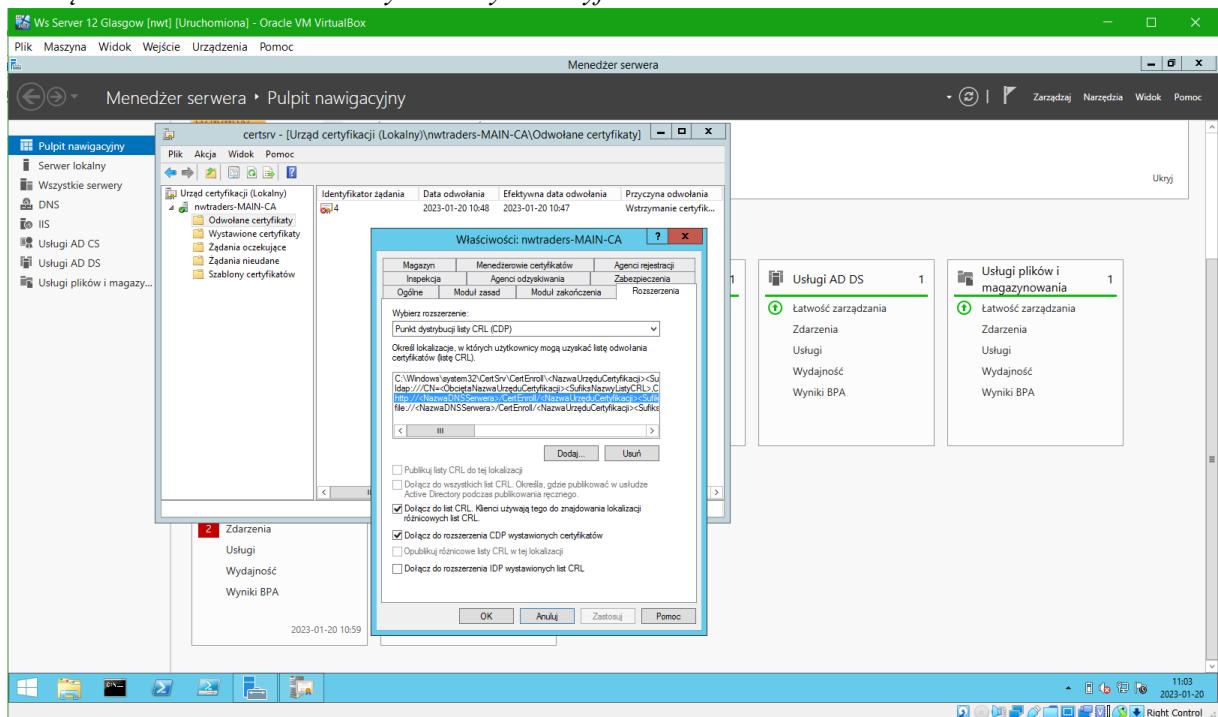
*Zmniejszyłem częstotliwość publikacji listy Delta CRL do 50min, ponieważ najmniejszy interwał tworzenia listy to 30min.



Zadanie 10

W systemie Windows Server uruchomić przystawkę do zarządzania urzędem certyfikacji, nacisnąć prawym przyciskiem myszy na pozycję *Nwtraders Main CA*, z menu wybrać "Właściwości" w zakładce "Rozszerzenia" zaznaczyć pozycję rozpoczęającą się od *http* oraz aktywować opcje "Dolacz do list CRL. Klienci używają tego do znajdowania lokalizacji różnicowych list CRL" jak również

"Dołącz do rozszerzenia CDP wystawionych certyfikatów".



W systemie Windows zalogować się na wybranego użytkownika, wygenerować dla niego nowy certyfikat i sprawdzić w tym certyfikacie czy został umieszczony w nim dodany wcześniej punkt CRL.

Ws 10 Nowak [nwt] [Uruchomiona] - Oracle VM VirtualBox

Plik Maszyna Widok Wejście Urządzenia Pomoc

Recycle Bin

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

File Action View Favorites Window Help

Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Certificate Enrollment Requests
Smart Card Trusted Roots

Issued To: Jan Nowak
Issued By: nwtraders-MAIN-CA
Expiration Date: 1/19/2024
Intended Purposes: Encrypting File System, Encrypting File System, File Recovery, Certificate Request, Encrypting File System

Certificate
General Details Certification Path

Show: <All>

Field Value
Subject Key Identifier ce098c8c3fa8ebc32e486a2a9...
Authority Key Identifier KeyID=00dbc7e974b08a0c27...
CRL Distribution Points [1]CRL Distribution Point: Distr...
Authority Information Access [1]Authority Info Access: Acc...
Subject Alternative Name Other Name:Principal Name=j...
Key Usage Digital Signature, Key Encipherment
Thumbprint 9db5d4b02028afb76f1640579...

URL=dap://CN=nwtraders-MAIN-CA,CN=Glasgow,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=nwtraders,DC=msft?certificateRevocationList?base?objectClass=rLDistributionPoint
(dap://CN=nwtraders-MAIN-CA,CN=Glasgow,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=nwtraders,DC=msft?certificateRevocationList?base?objectClass=rLDistributionPoint)

Edit Properties... Copy to File... OK

Personal store contains 5 certificates.

Windows 10 Enterprise Evaluation
Windows License is expired
Build 19041.vb_release.191206-1406

Type here to search Afternoon snow ENG 11:10 AM PLP 1/20/2023 Right Control

Ws 10 Nowak [nwt] [Uruchomiona] - Oracle VM VirtualBox

Plik Maszyna Widok Wejście Urządzenia Pomoc

Recycle Bin

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

File Action View Favorites Window Help

Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Certificate Enrollment Requests
Smart Card Trusted Roots

Issued To: Jan Nowak
Issued By: nwtraders-MAIN-CA
Expiration Date: 1/19/2024
Intended Purposes: Encrypting File System, Encrypting File System, File Recovery, Certificate Request, Encrypting File System

Certificate
General Details Certification Path

Show: <All>

Field Value
Subject Key Identifier 780f8da65f135adaa100edad...
Authority Key Identifier KeyID=00dbc7e974b08a0c27...
CRL Distribution Points [1]CRL Distribution Point: Distr...
Authority Information Access [1]Authority Info Access: Acc...
Subject Alternative Name Other Name:Principal Name=j...
Key Usage Digital Signature, Key Encipherment
Thumbprint bdf2262a6458e892b43f933...

URL=dap://CN=nwtraders-MAIN-CA,CN=Glasgow,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=nwtraders,DC=msft?certificateRevocationList?base?objectClass=rLDistributionPoint
(dap://CN=nwtraders-MAIN-CA,CN=Glasgow,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=nwtraders,DC=msft?certificateRevocationList?base?objectClass=rLDistributionPoint)
URL=http://Glasgow.nwtraders.msft/CerEnroll/nwtraders...

Edit Properties... Copy to File... OK

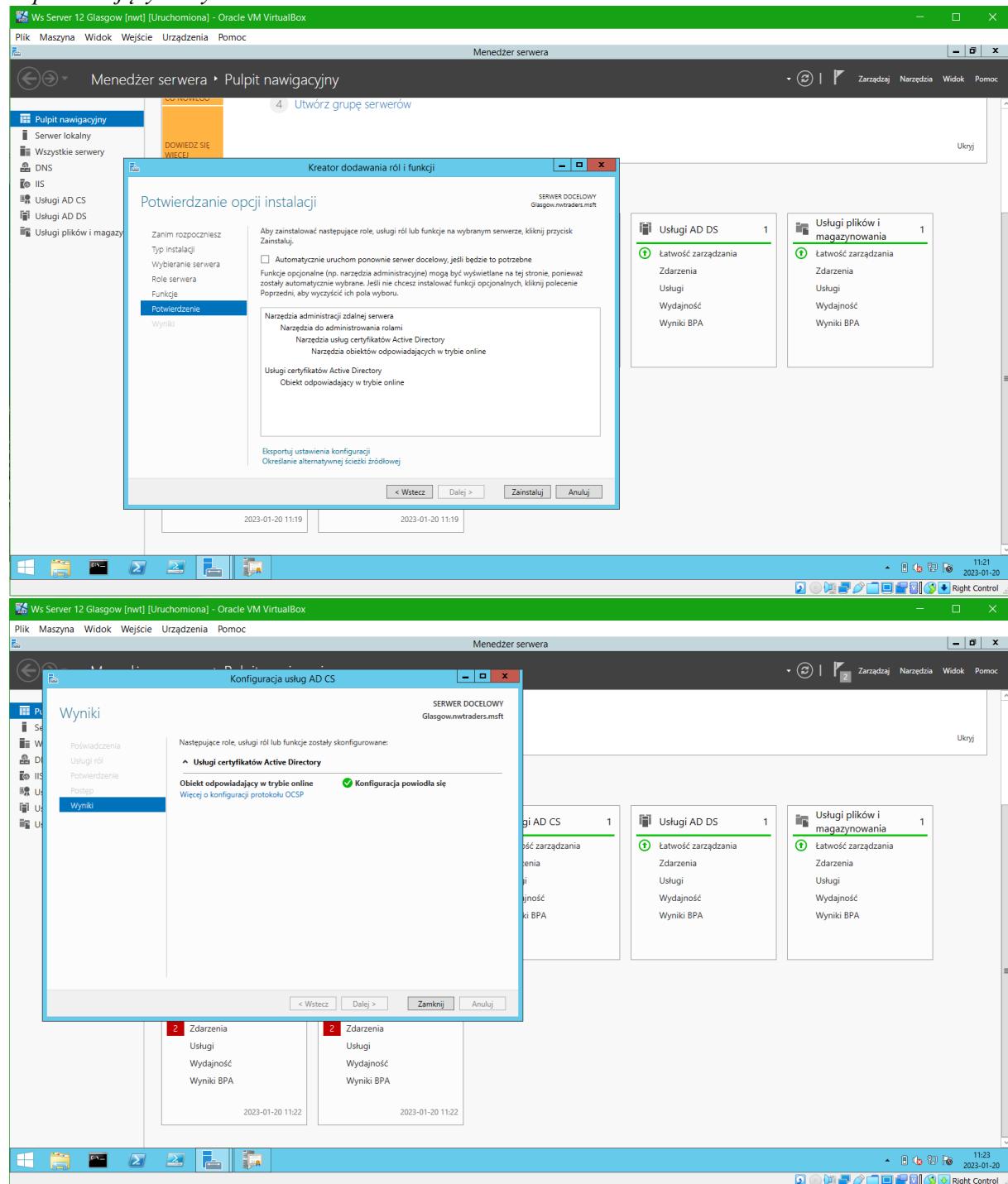
Personal store contains 5 certificates.

Windows 10 Enterprise Evaluation
Windows License is expired
Build 19041.vb_release.191206-1406

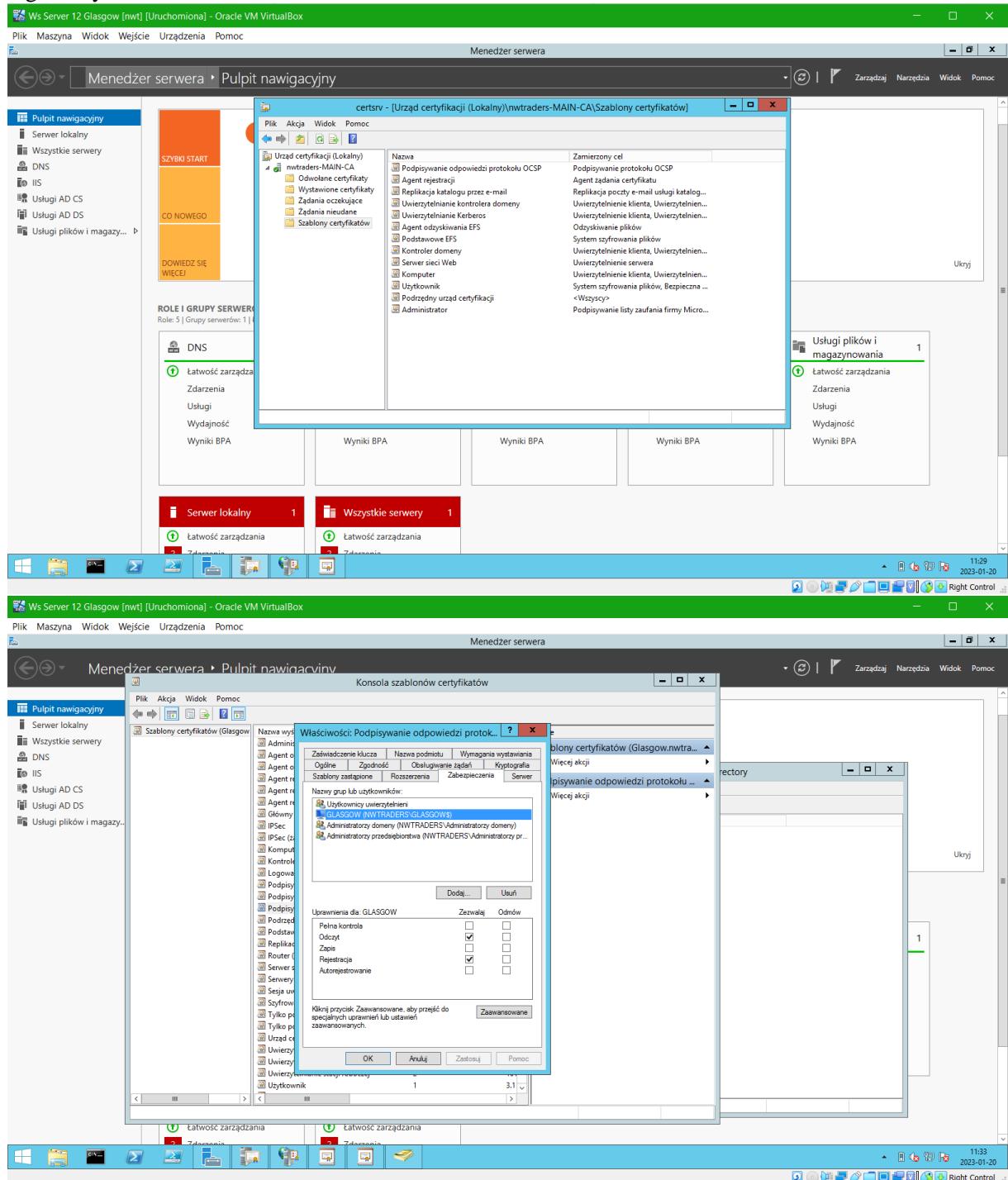
Type here to search Afternoon snow ENG 11:09 AM PLP 1/20/2023 Right Control

Zadanie 11

W systemie Windows Server doinstalować do roli urzędu certyfikacji usługę roli "Obiekt odpowiadający w trybie online".

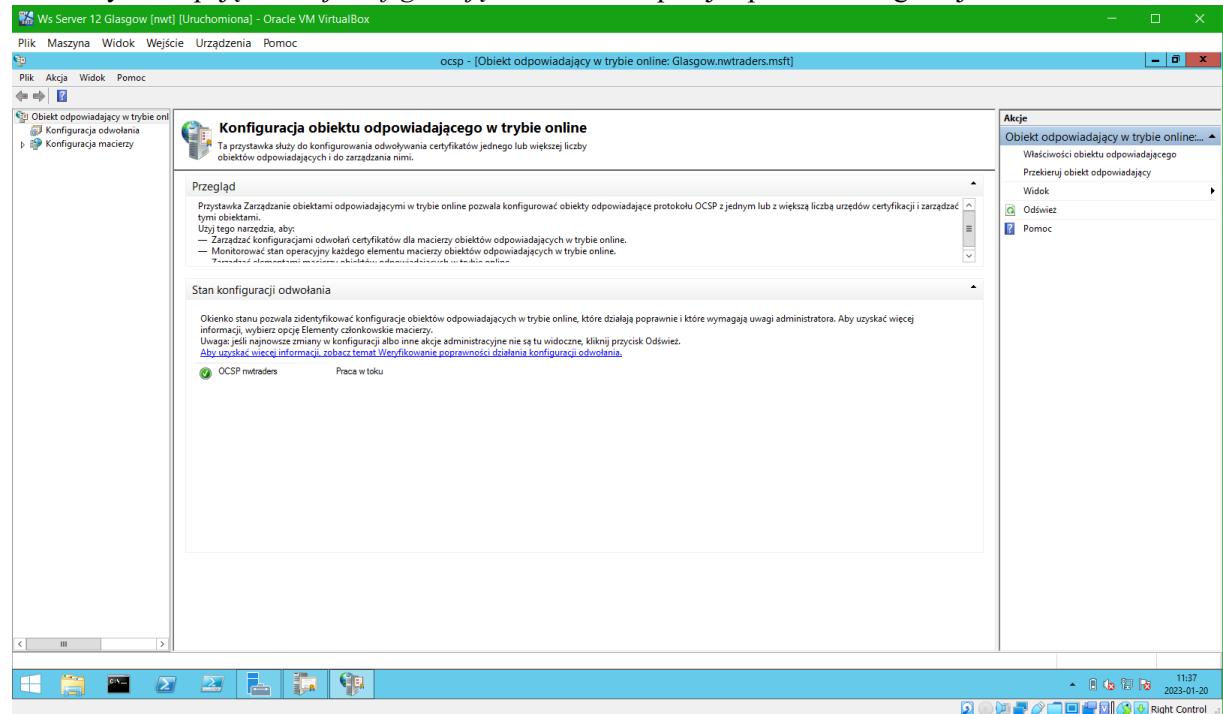


W systemie **Windows Server** uruchomić przystawkę do zarządzania urzędem certyfikacji, dodać szablon "*Podpisywanie odpowiedzi protokołu OCSP*" do obsługiwanych przez Urząd Certyfikującą i skonfigurować ten szablon tak, aby konto komputera "Glasgow" mogło występować o wystawienie tego certyfikatu.

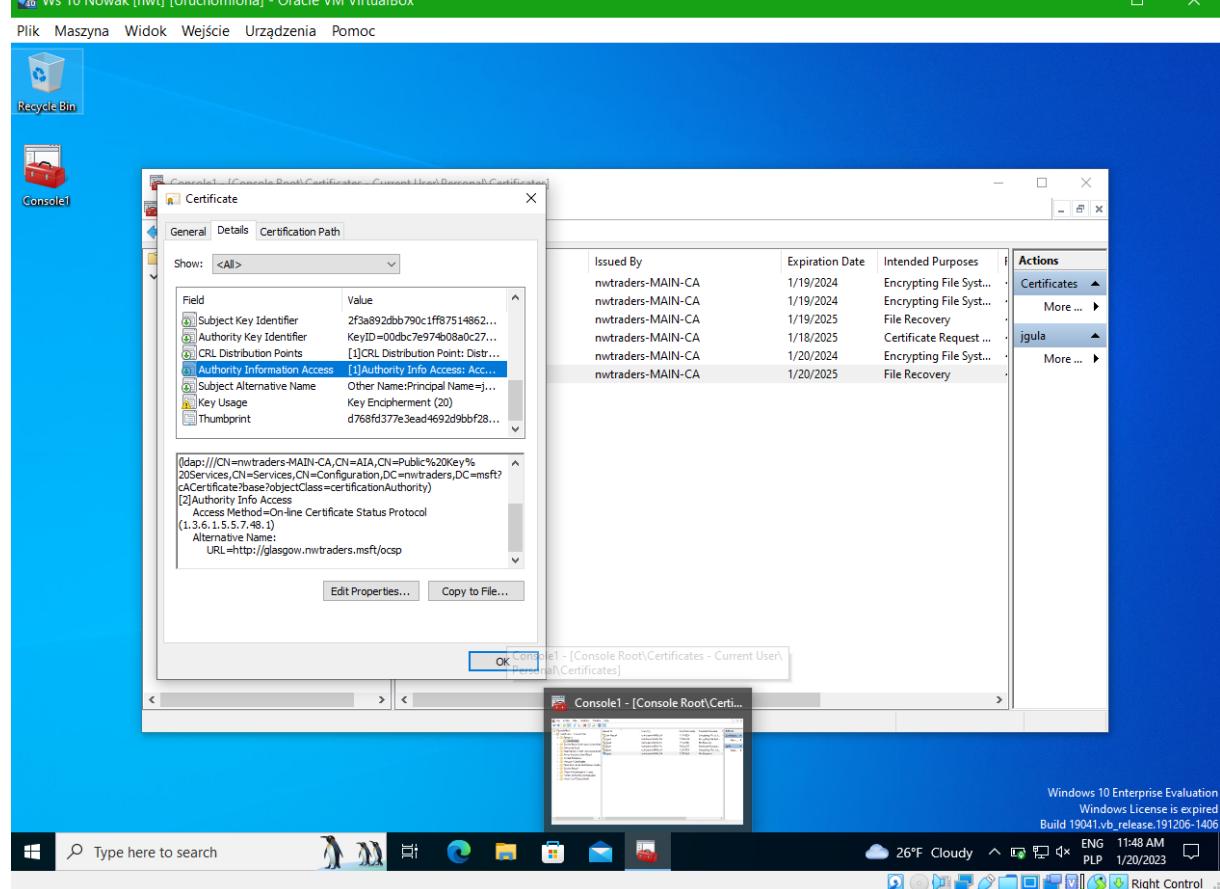
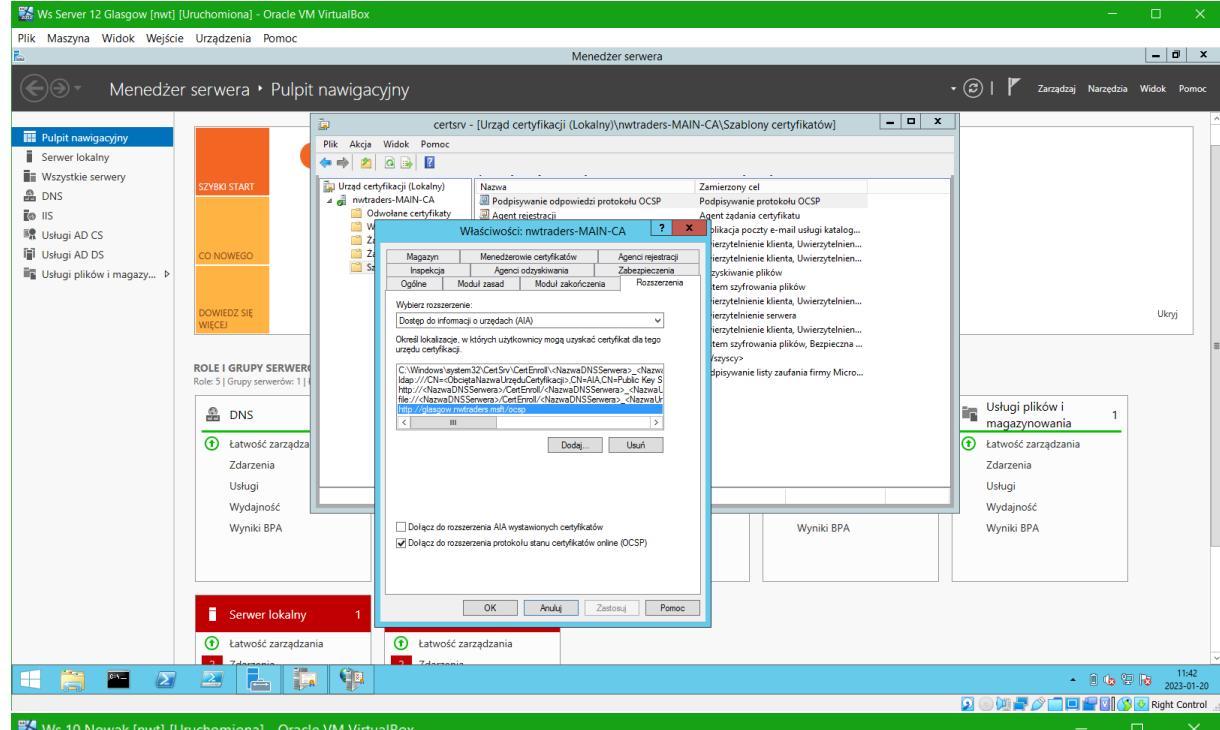


W systemie **Windows Server** uruchomić przystawkę do zarządzania usługą OCSP (*Zarządzanie obiektem odpowiadającym w trybie online*), przejść do pozycji "*Konfiguracja odwołania*", w prawym

menu wybrać opcję "Dodaj konfigurację odwołania" i przejść proces konfiguracji.

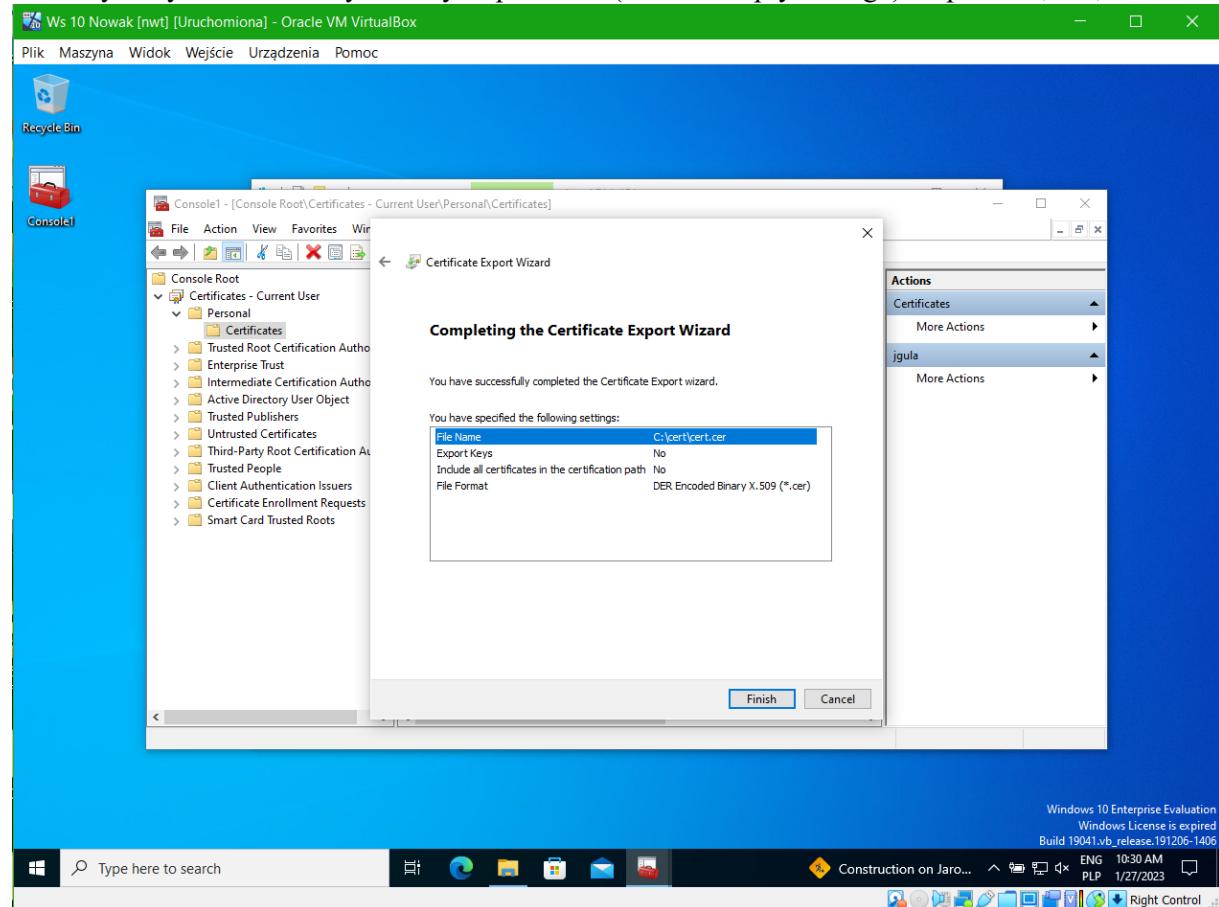


W systemie **Windows Server** uruchomić przystawkę do zarządzania urzędem certyfikacji, nacisnąć prawym przyciskiem myszy na pozycję **Nwtraders Main CA**, z menu wybrać "Właściwości", w zakładce "Rozszerzenia" wybrać z rozwijanej listy "Dostęp do informacji o urzędach (AIA)", dodać zasób **http://<nazwa komputera>.nwtraders.msft/ocsp** i zaznaczyć dla niego opcję "Dolacz do rozszerzenia protokołu stanu certyfikatów online (OCSP)".



Zadanie 12

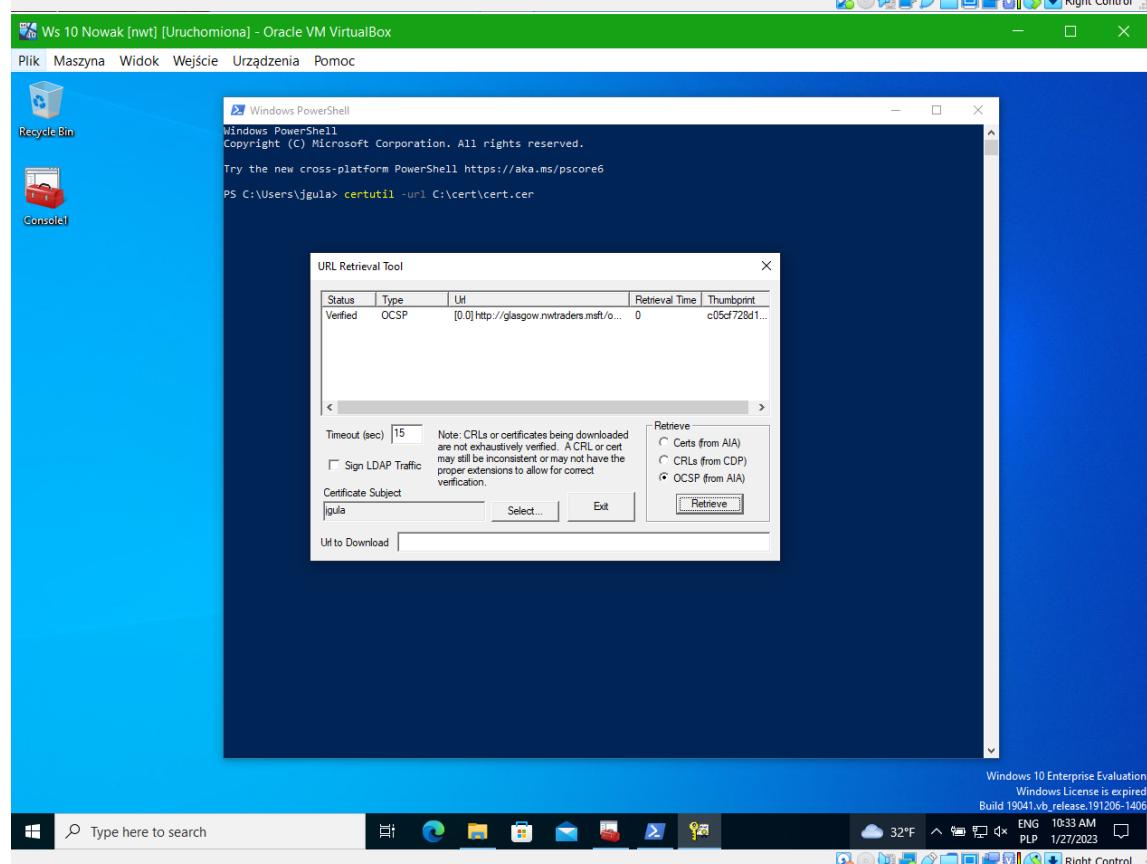
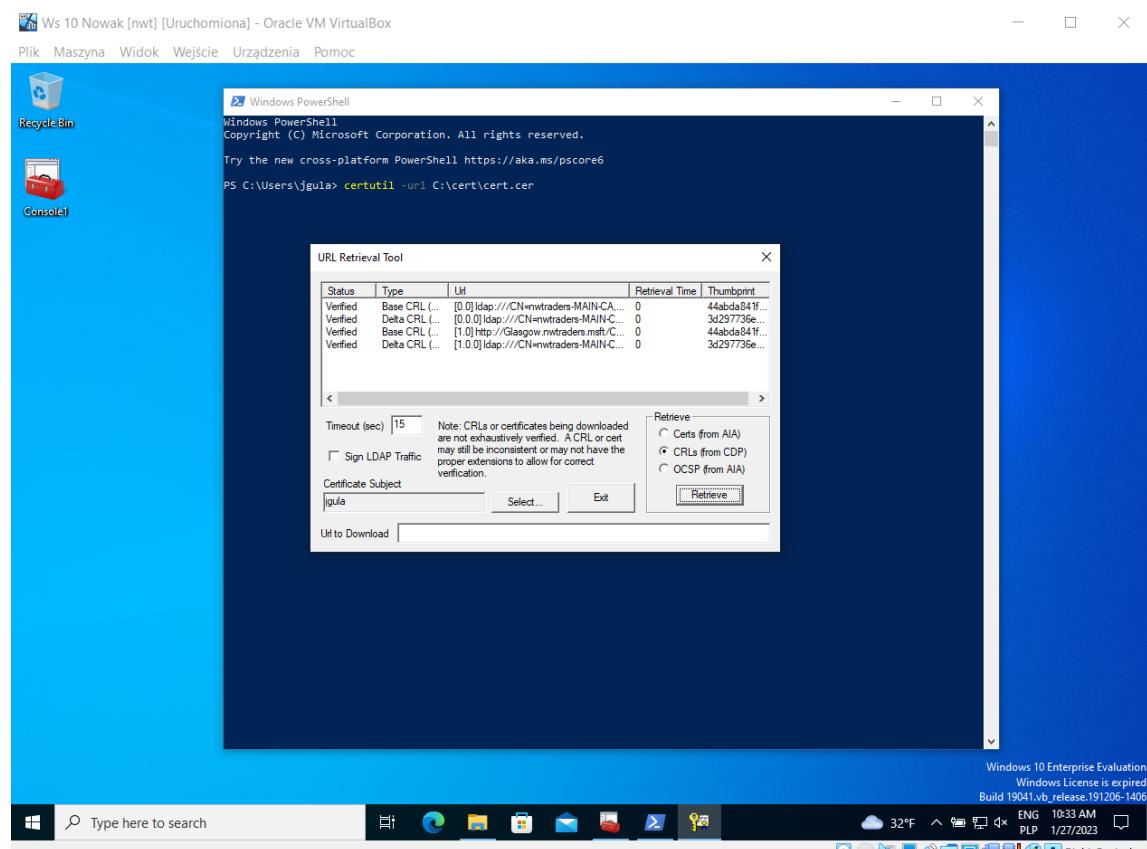
W systemie Windows zalogować się na wybranego użytkownika, wygenerować dla niego nowy dowolny certyfikat i ten certyfikat wyeksportować (bez klucza prywatnego) do pliku *c:\cert\cert.cer*.



W systemie Windows uruchomić wiersz poleceń, wydać komendę:

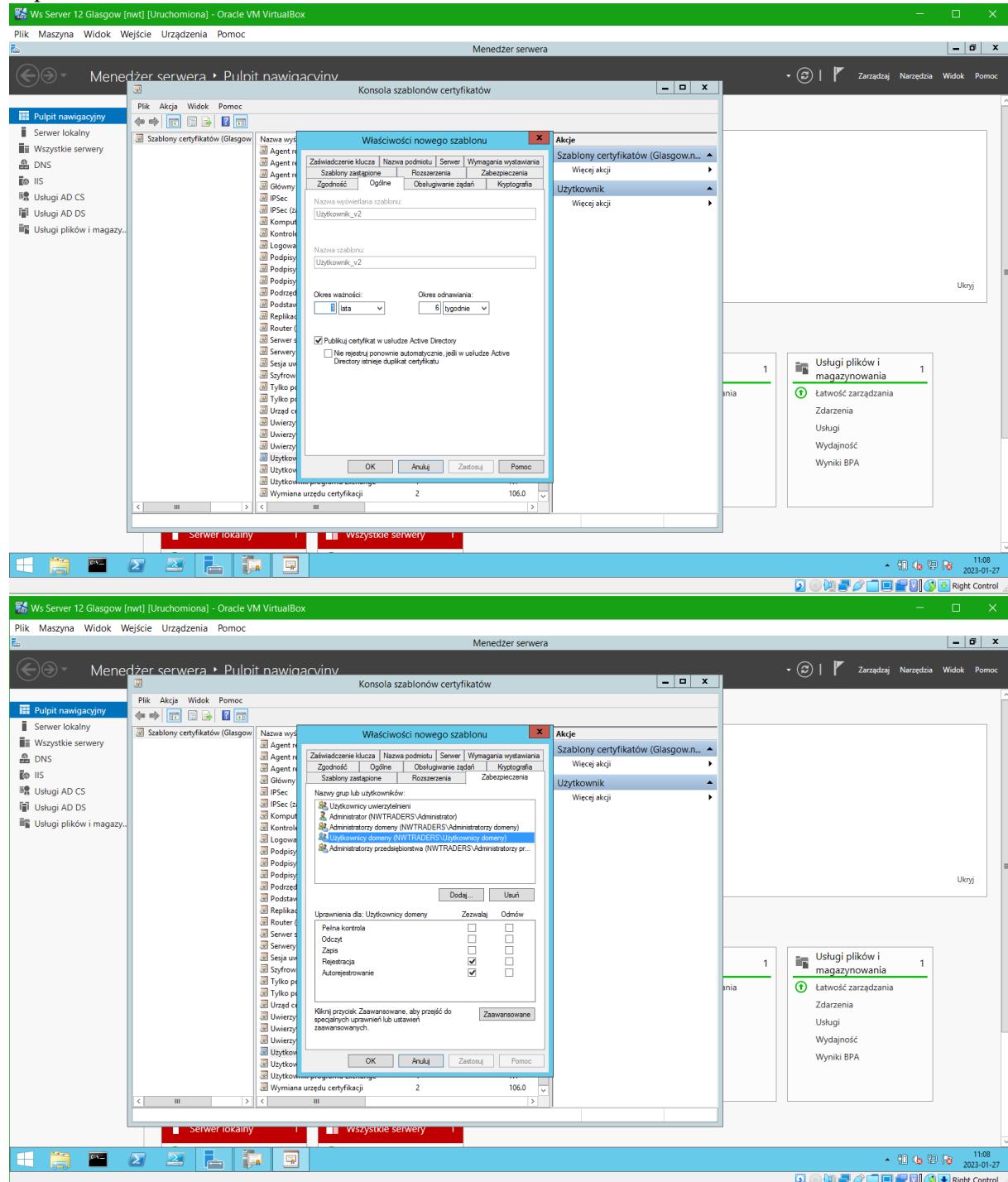
`certutil -url c:\cert\cert.cer`

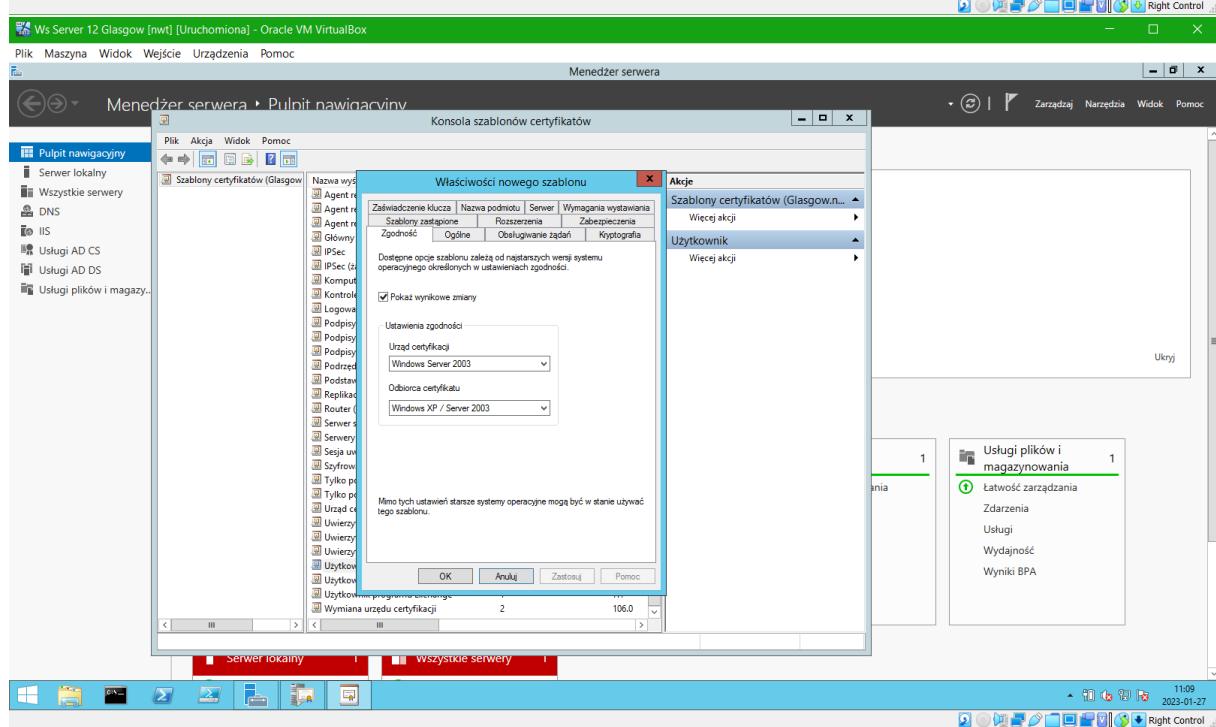
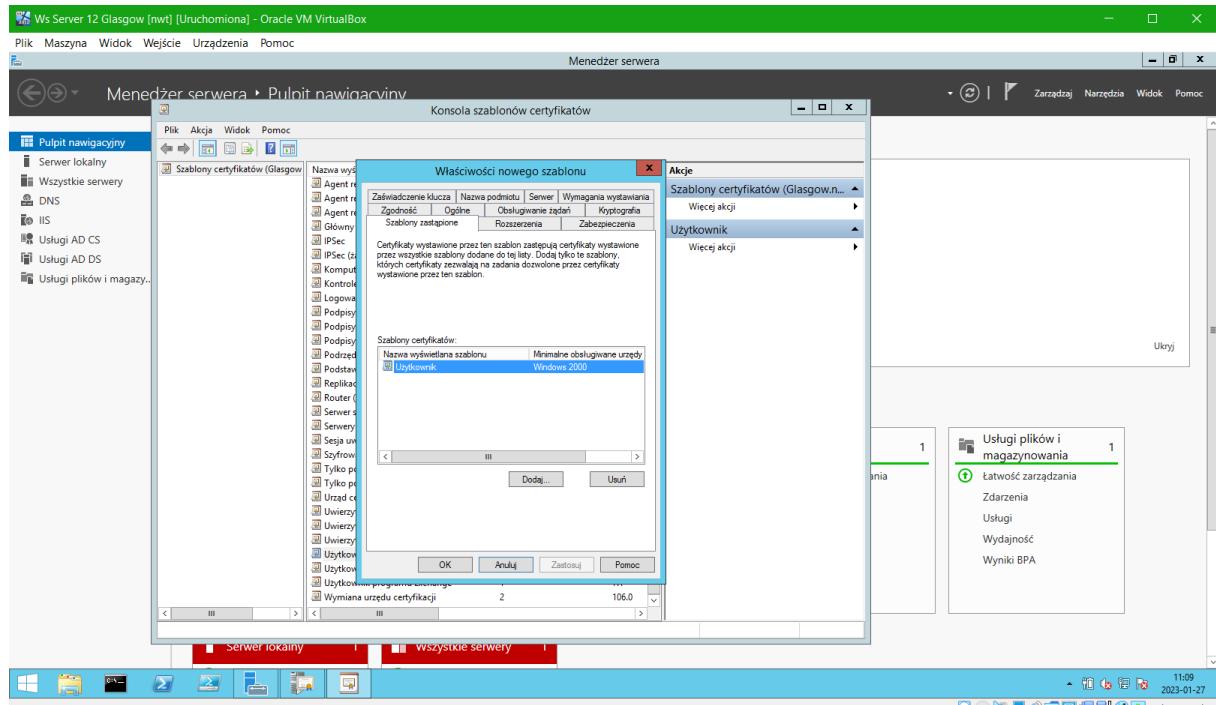
i w ramach uruchomionej aplikacji zweryfikować prawidłowe pobranie list CRL oraz działanie usługi OCSP.

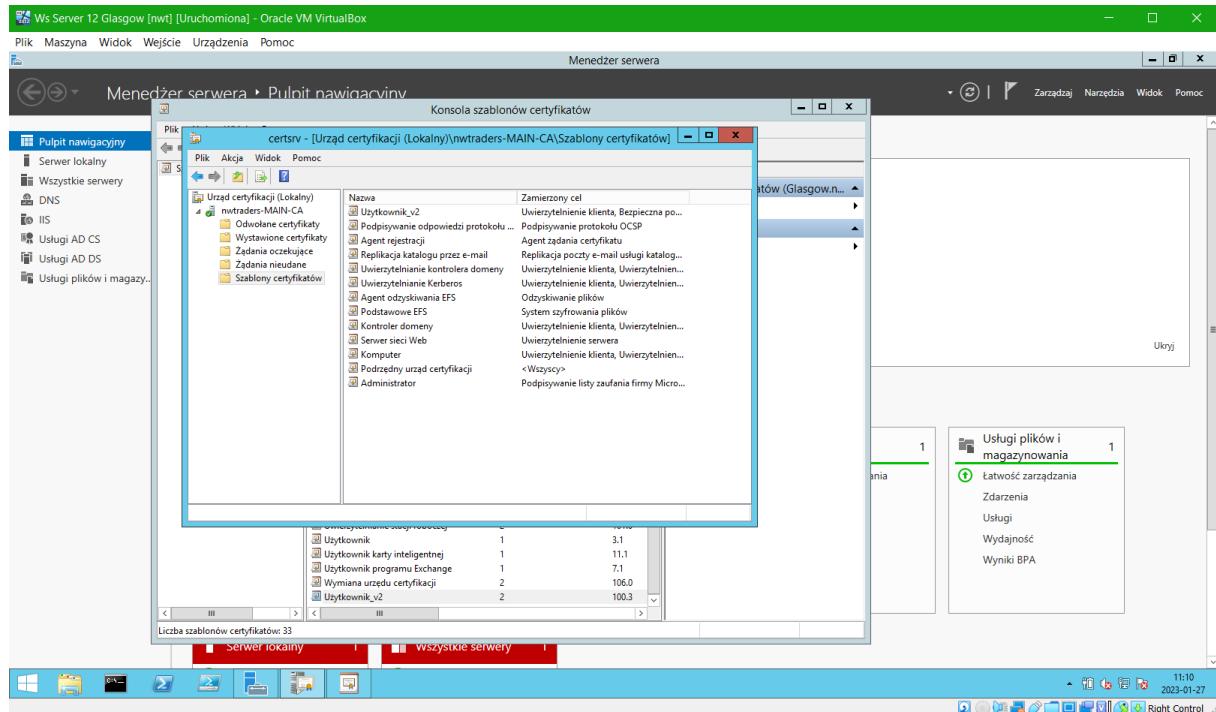


Zadanie 13

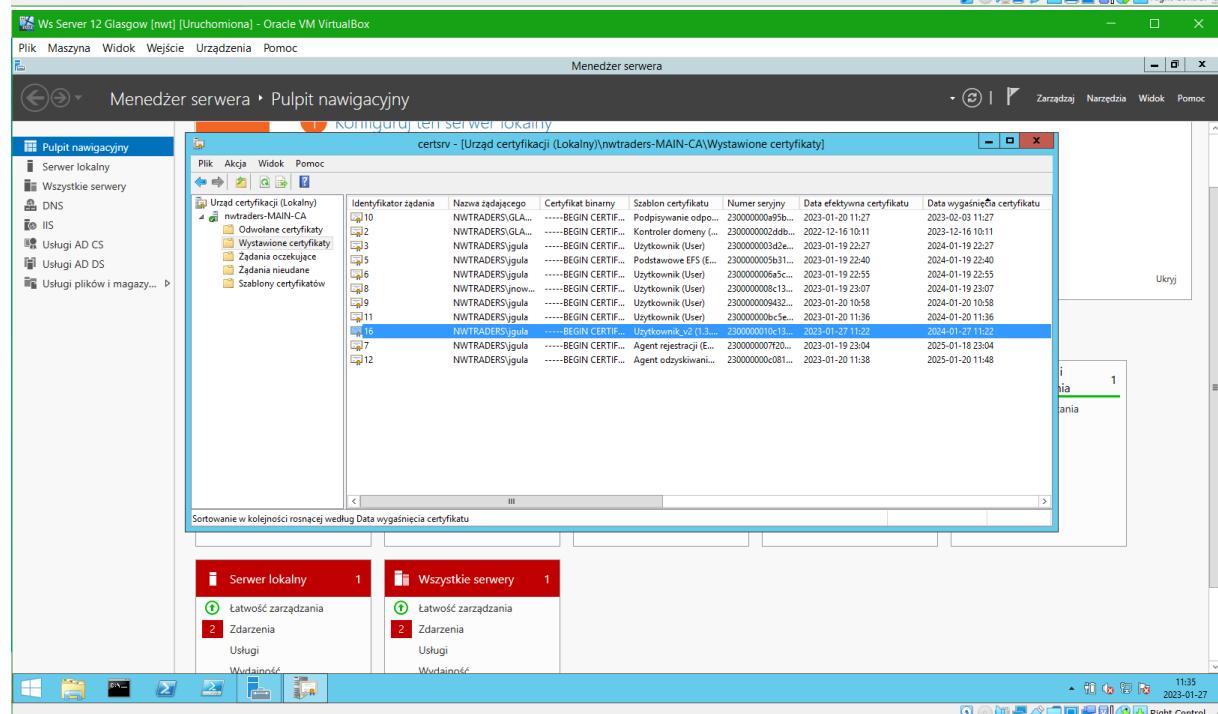
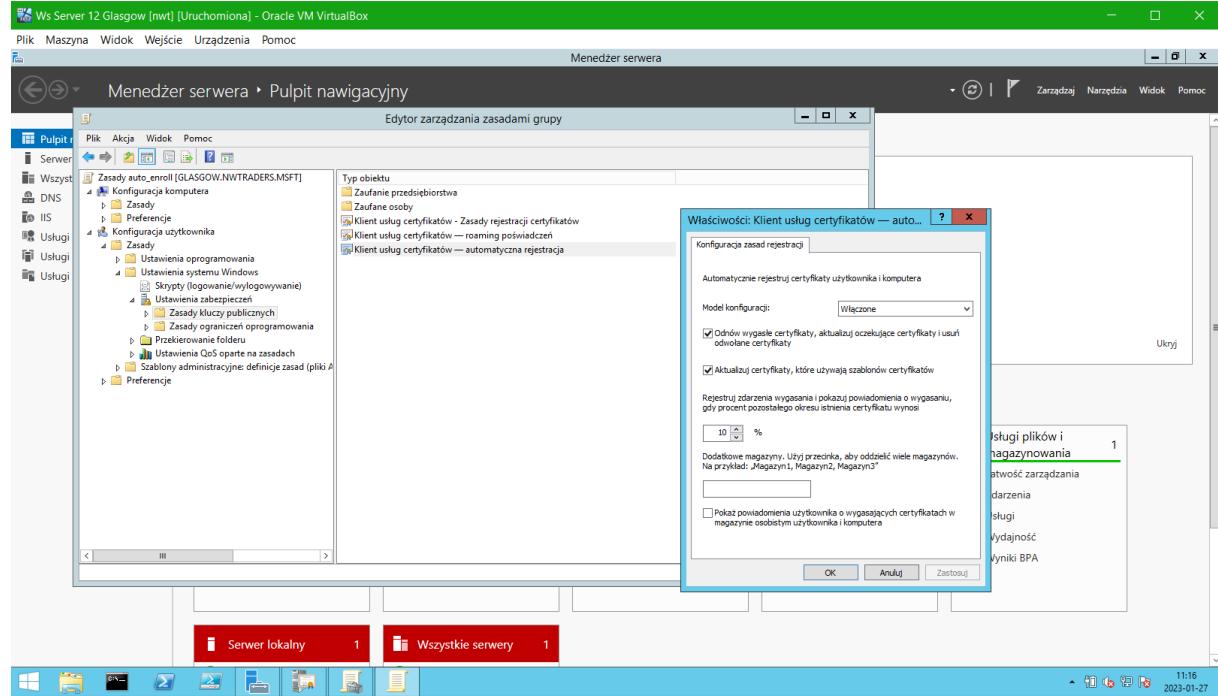
Zrealizowanie automatycznego wystawiania certyfikatów w ramach usługi AD Certificate Services.
duplikowanie szablonu







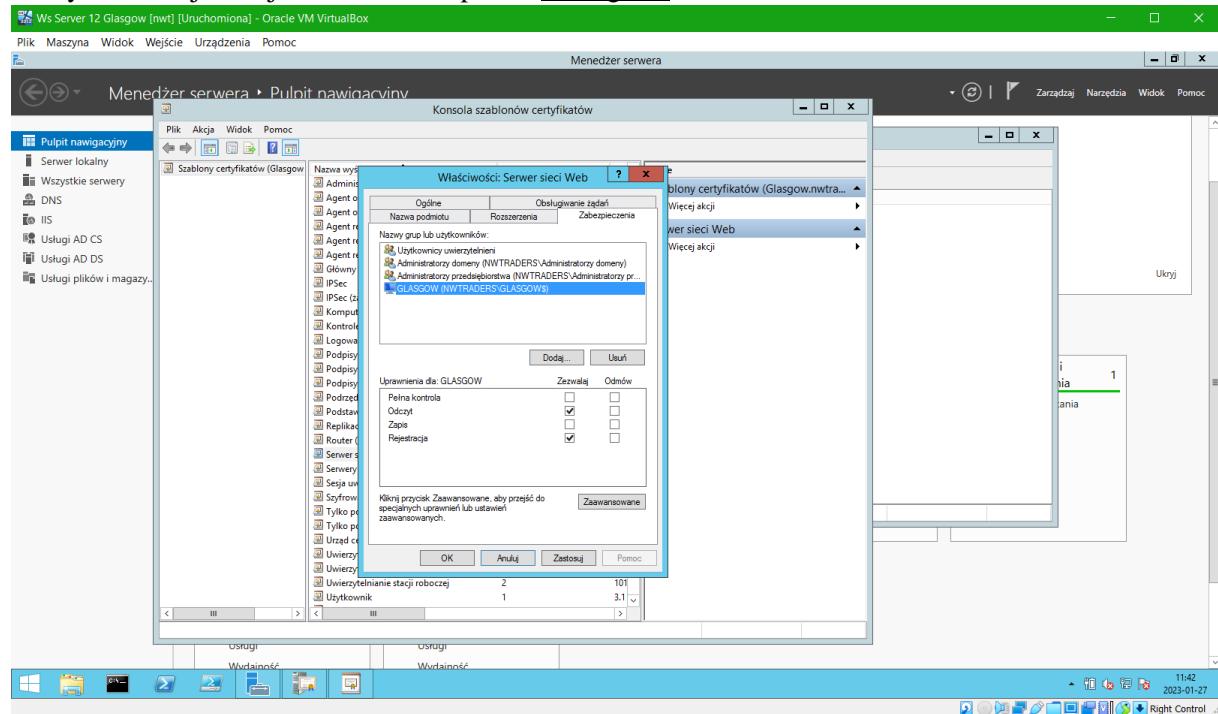
tworzenie zasady domenowej:



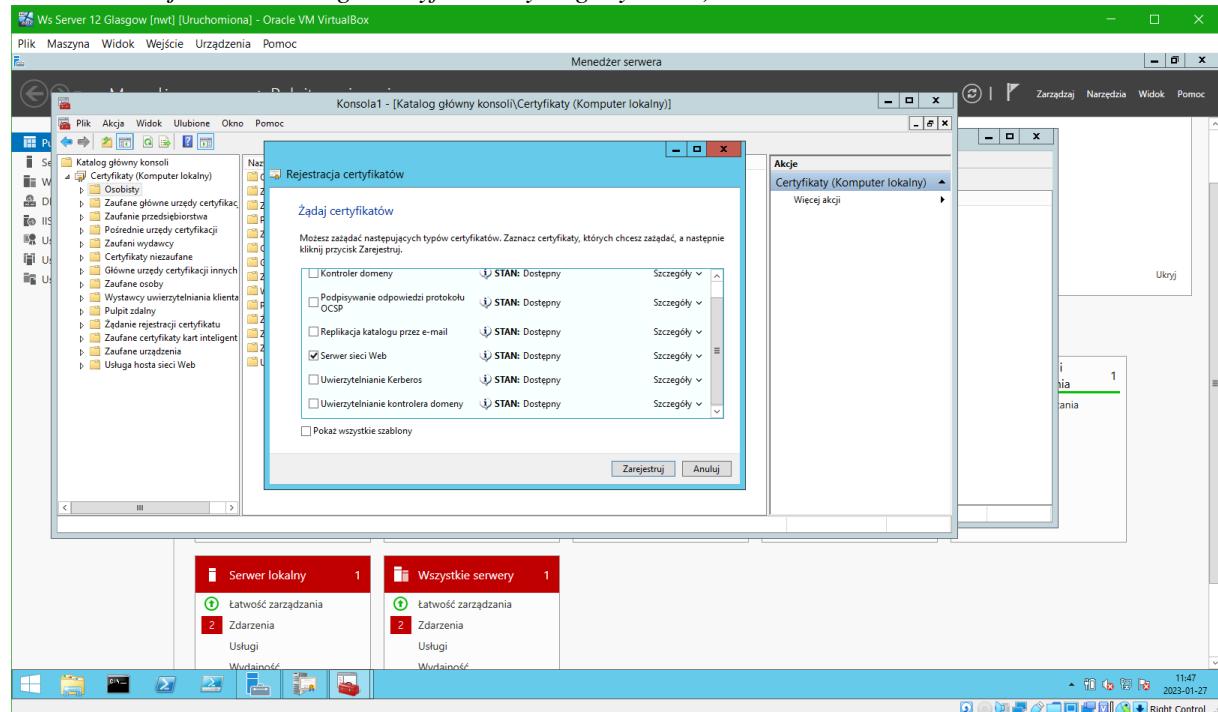
Zadanie 14

W systemie Windows Server uruchomić przystawkę do zarządzania urzędem certyfikacji i w ustawieniach szablonu certyfikatu "Serwer sieci Web" dodać możliwość występowania o certyfikat przez konto komputera "Glasgow", tj. w zabezpieczeniach szablonu certyfikatu dodać uprawnienie

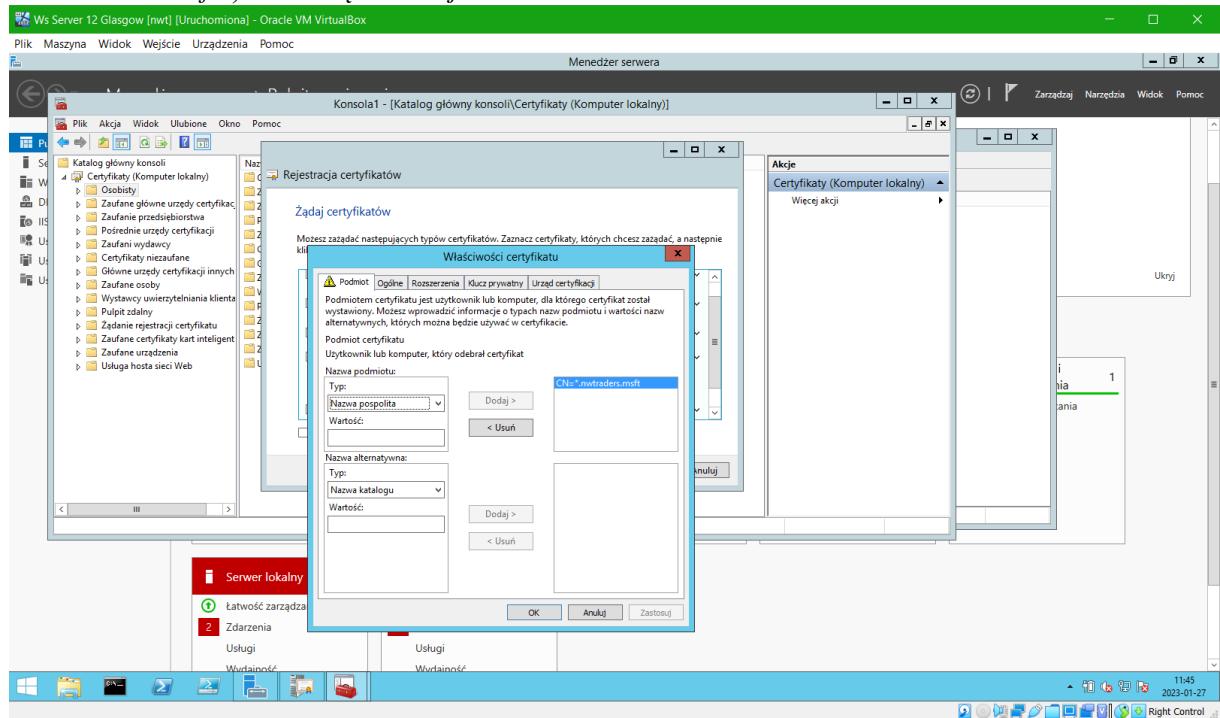
odczytu oraz rejestracji dla konta komputera "Glasgow".



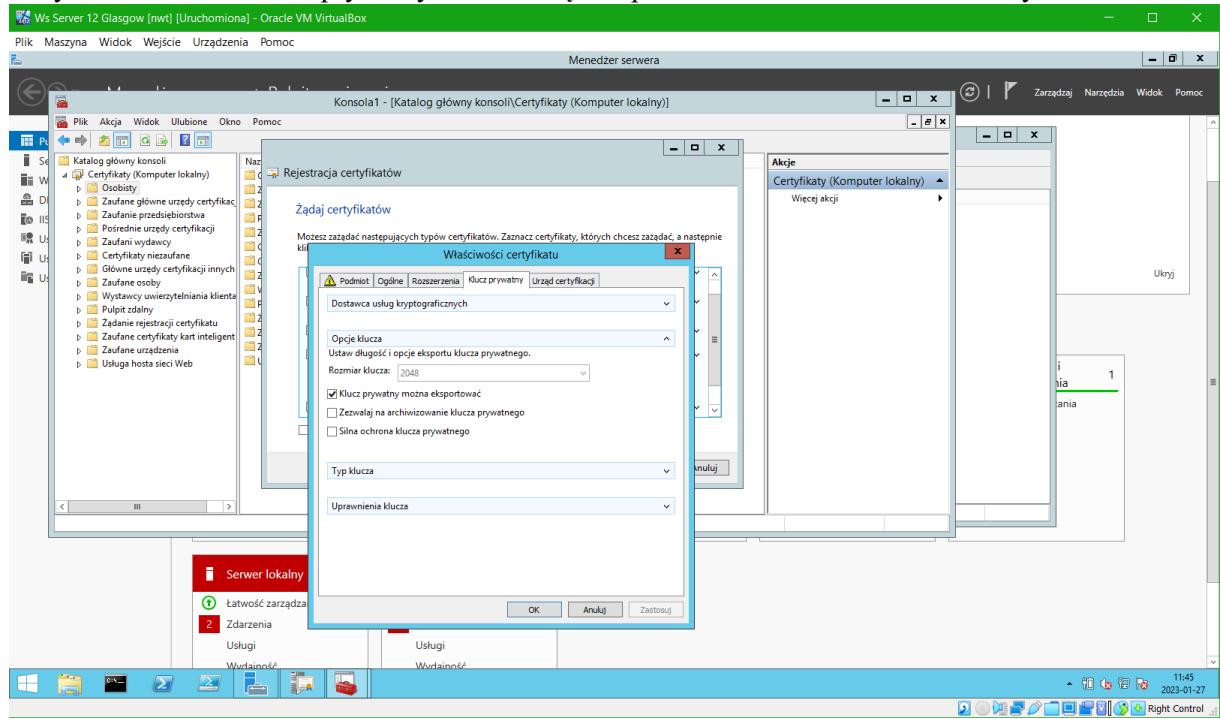
W systemie Windows Server uruchomić w konsoli MMC przystawkę "*Certyfikaty*" dla lokalnego konta komputera i w ramach kontenera "*Osobisty*" zrealizować żądanie nowego certyfikatu, wybierając jako szablon "*Serwer sieci Web*" oraz skonfigurować ustawienia tego szablonu (klikając na link "*Do zarejestrowania tego certyfikatu wymaganych ...*").



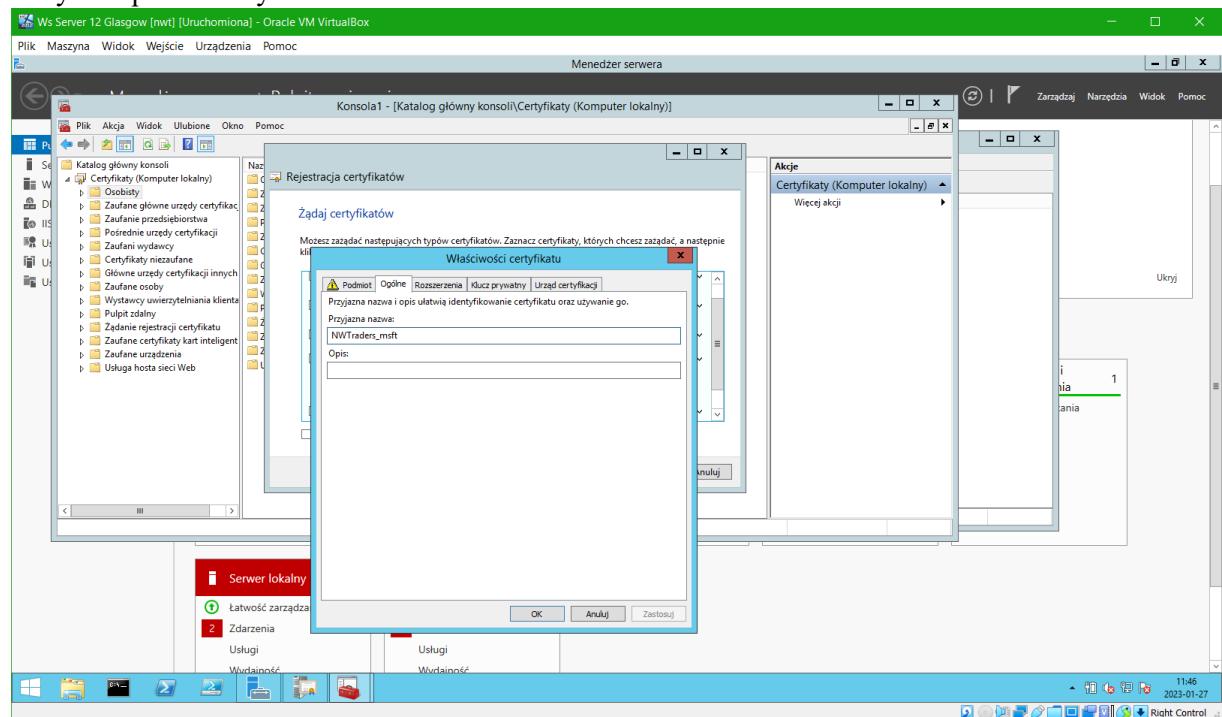
W zakładce "Podmiot" jako typ nazwy podmiotu wybrać "Nazwa pospolita" (wartość: "*.nwtraders.msft") i nacisnąć "Dodaj".



W zakładce "Klucz prywatny" aktywować opcję "Klucz prywatny można eksportować", dzięki czemu certyfikat wraz z kluczem prywatnym można będzie przenieść również na inne serwery.



W zakładce "Ogólne" wpisać przyjazną nazwę, dzięki czemu łatwiej będzie można identyfikować ten certyfikat pośród innych.



Po wygenerowaniu certyfikatu oraz klucza prywatnego wyeksportować je do pliku:
`C:\cert_ssl_wildcard_nwtraders.pfx`

