TOPIC: IMPLEMENTING AND ADMINISTERING AD FS

Objective:

Implement and configure Active Directory Federation Services (AD FS) to enable federated authentication and secure access to applications across organizations.

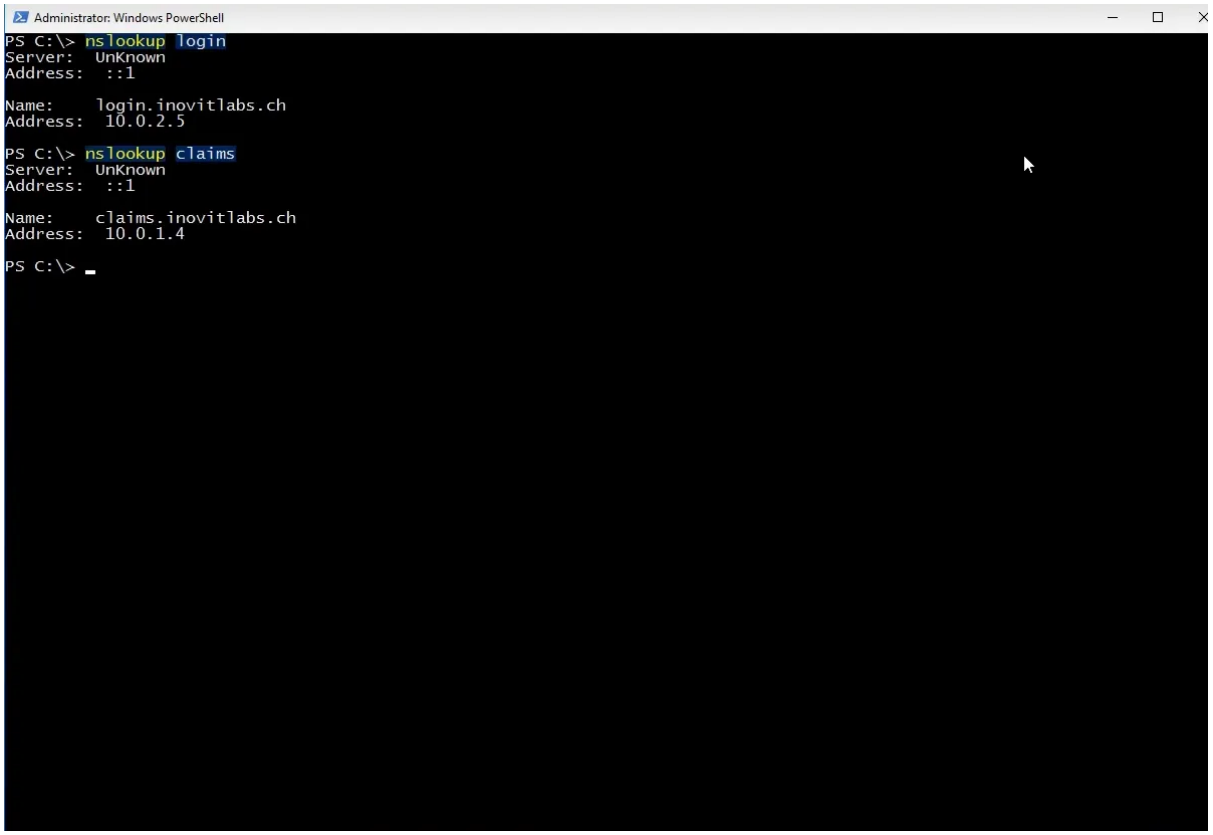
Prerequisites:

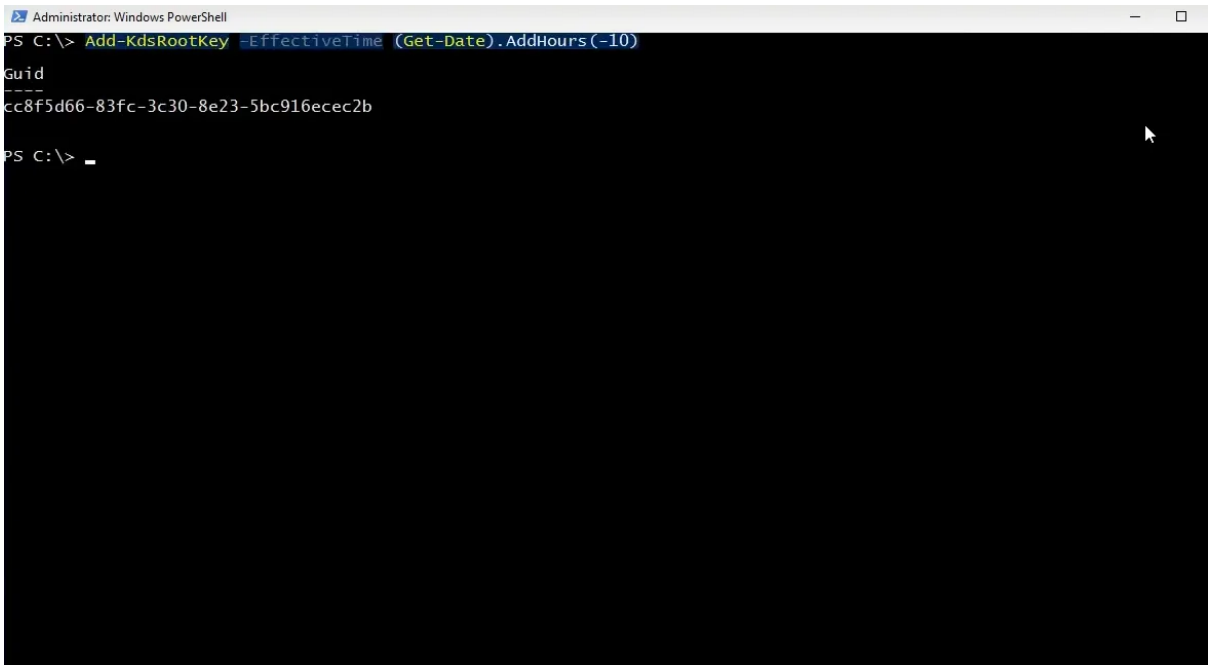
- A functioning Active Directory environment with domain controllers (e.g., LON-DC1)
- DNS infrastructure properly configured
- SSL certificates available for AD FS servers
- Administrative credentials for domain and servers
- Network connectivity between partner systems (for federated business partners)

Procedure:

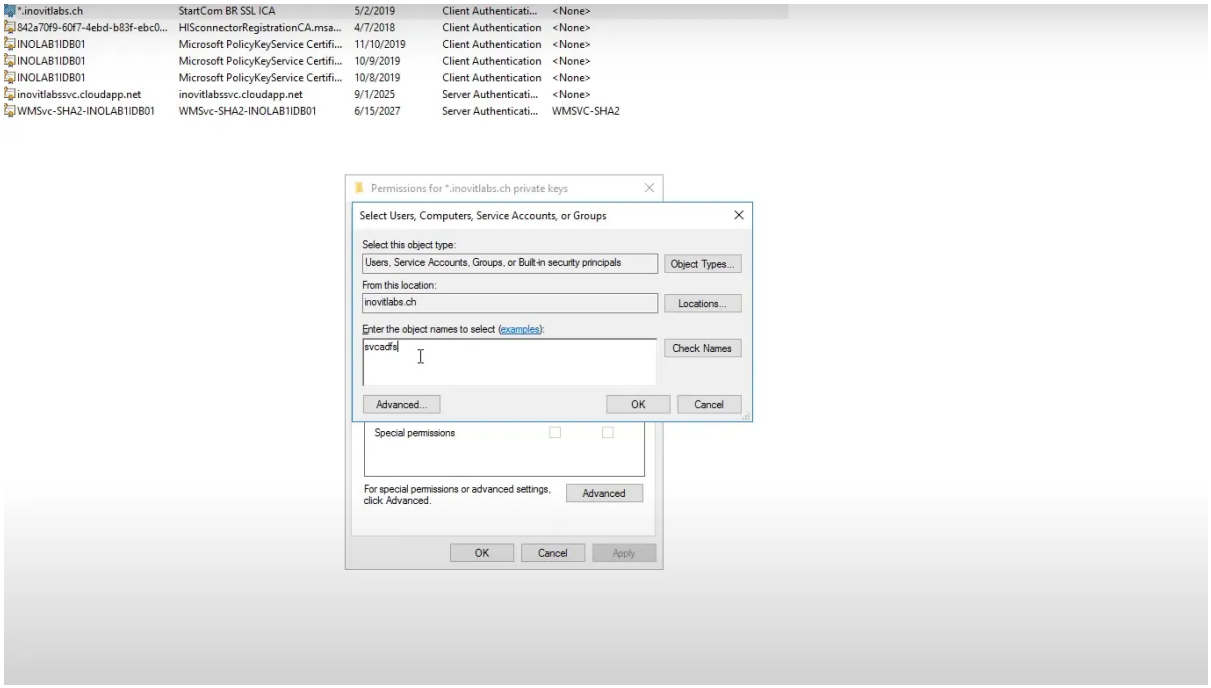
Exercise 1: Configuring the AD FS prerequisites

1. **Configure DNS Forwarders**
    - On LON-DC1, open DNS Manager.
    - Add a new Conditional Forwarder for the domain TreyResearch.net with IP 172.16.10.10, replicate to all DNS servers.
    - On TREY-DC1, add Conditional Forwarder for Adatum.com with IP 172.16.0.10 and replicate.
    - Close DNS Manager.
2. **Configure Certificate Trusts**
    - On LON-DC1, copy TREY-DC1's CA certificate from \TREY-DC1\CertEnroll to C:.
    - In Group Policy Management, edit the Default Domain Policy.
    - Import the TREY-DC1 CA certificate into Trusted Root Certification Authorities.
    - On TREY-DC1, import the AdatumCA certificate similarly.
    - Run gpupdate on LON-SVR1.



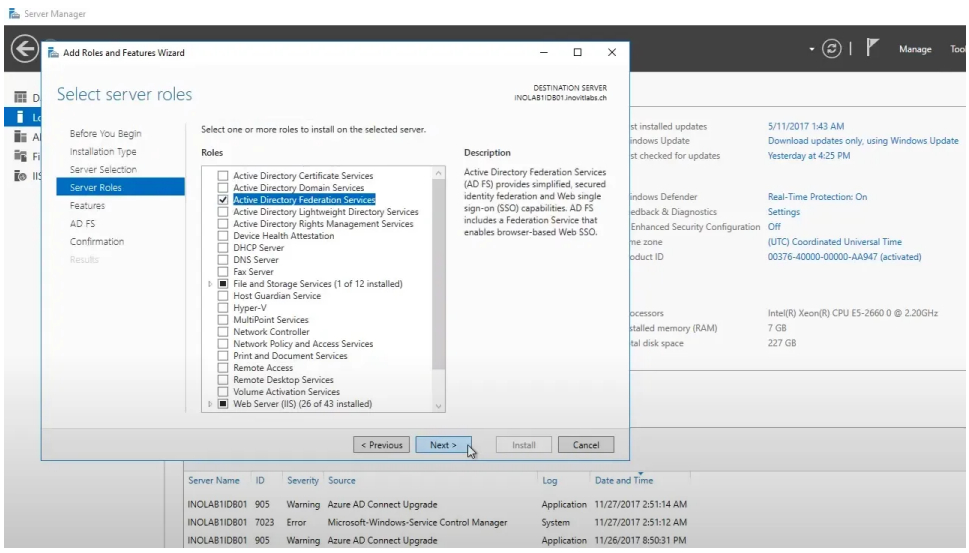


3. **Request and Install Web Server Certificate**
    - On LON-SVR1, open IIS Manager and create a new domain certificate with appropriate distinguished name fields.
    - Assign the SSL certificate to Default Web Site with https binding.
    - Close IIS Manager.



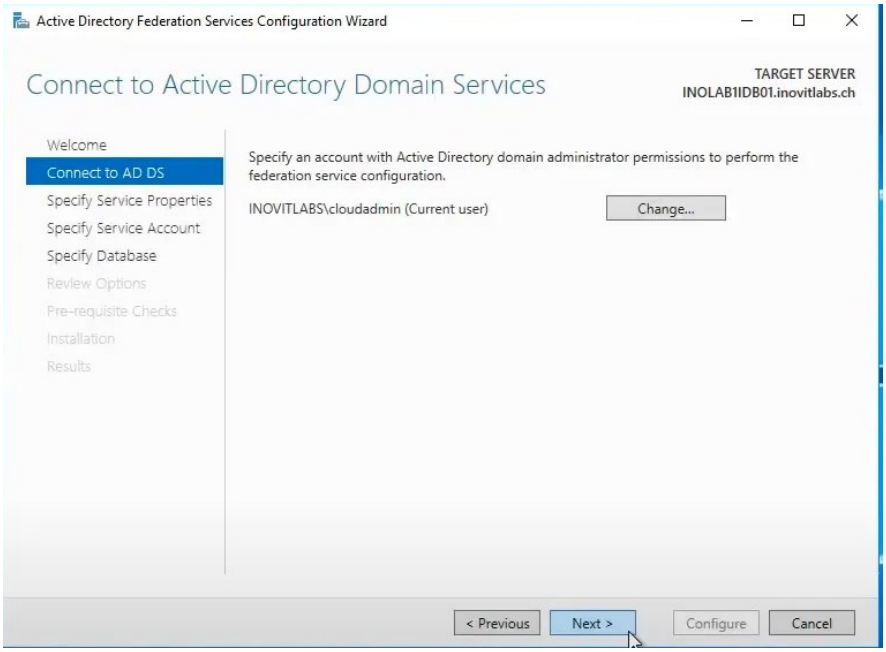
Exercise 2: Installing and configuring AD FS

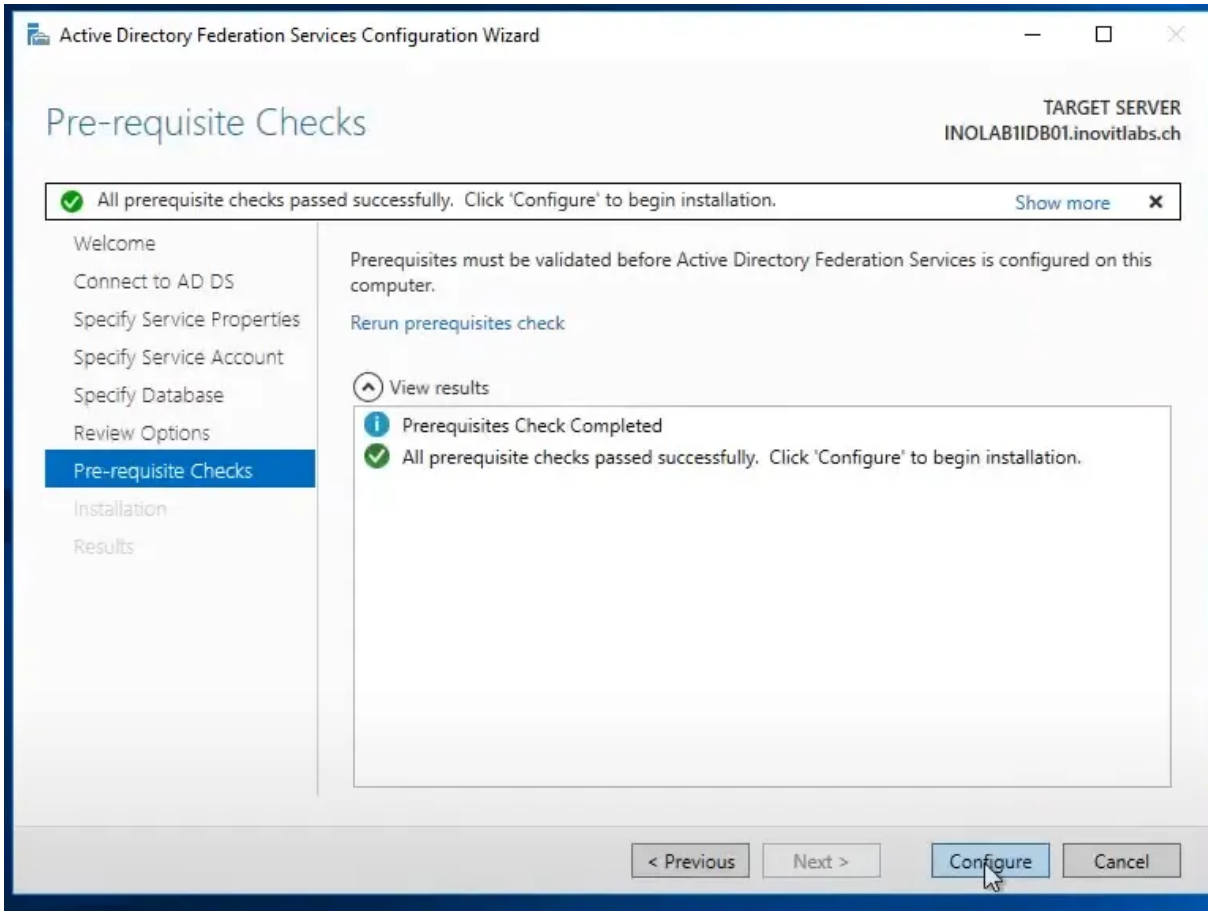
1. On LON-DC1, install the AD FS role via Server Manager.
2. Launch the AD FS Configuration Wizard.
3. Select to create the first federation server in a federation server farm.
4. Use administrator credentials to connect to AD DS.
5. Select the preconfigured SSL certificate for adfs.adatum.com.
6. Specify the federation service display name.
7. Create and specify a group Managed Service Account (gMSA) for AD FS service.
8. Create the AD FS configuration database using Windows Internal Database.
9. Complete the configuration and close the wizard.
10. Verify AD FS functionality by accessing https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml on LON-CL1 via Internet Explorer.



Exercise 3: Configuring an internal application for AD FS

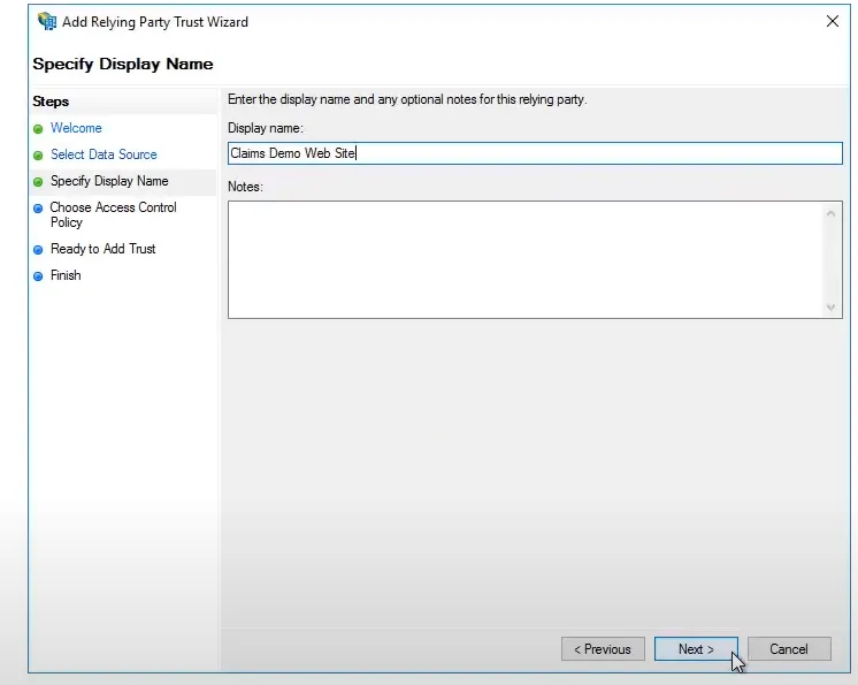
1. Configure claims provider trust for Active Directory in AD FS Management.
2. Set up LDAP attributes to outgoing claims mapping (email, UPN, display name).
3. On LON-SVR1, use the Federation Utility Wizard to configure the sample web application with AD FS.
4. Configure a relying party trust for the application with appropriate claim issuance rules.
5. Test access to the claims-aware application in Internet Explorer by signing in as a domain user.
6. Configure Internet Explorer to automatically pass local credentials to the application.

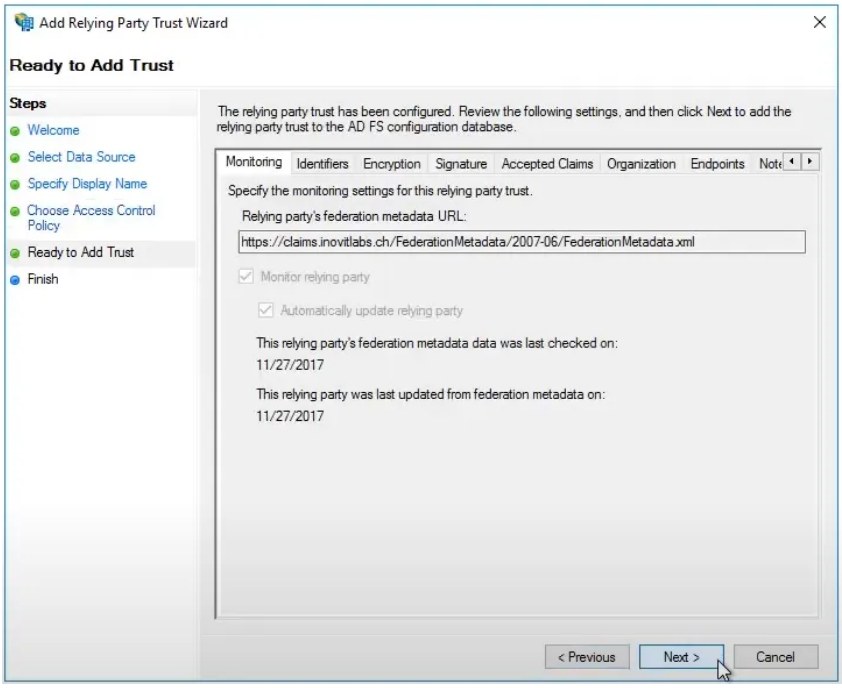




Exercise 4: Configuring AD FS for federated business partners

1. On TREY-DC1, set up DNS record for AD FS.
2. Create AD FS SSL certificate for adfs.treyresearch.net.
3. Install AD FS role and complete configuration on TREY-DC1.
4. Create a claims provider trust on LON-DC1 for Trey Research using federation metadata.
5. Configure relying party trust on TREY-DC1 for Adatum.com.
6. Test application access from Trey Research domain.
7. Configure issuance authorization claim rules to restrict access to specific groups (e.g., Production).
8. Verify group-based access restrictions.





Conclusion:

By completing this module, you have successfully implemented and configured Active Directory Federation Services (AD FS) to facilitate secure authentication and authorization across multiple organizations and internal applications. You configured DNS, certificates, AD FS servers, claims trust policies, and tested federated access, fulfilling requirements for claims-aware applications and federated business partner trust relationships.