GALGOTIAS UNIVERSITY

(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

SAML BASED AUTHENTICATION USING LDAP

A Project Report of Capstone Project - 2

Submitted by

PANKAJ NAGPAL

(16SCSE101396 / 1613101474)

in partial fulfillment for the award of the degree of

Bachelor of Technology

IN

Computer Science and Engineering

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING

Under the Supervision of

Mr. P.RAJAKUMAR

Assistant Professor

APRIL / MAY- 2020

GALGOTIAS
UNIVERSITY

SCHOOL OF COMPUTING AND SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

Certified that is project report "**SAML BASED AUTHENTICATION USING LDAP**"
Is the bonafide work of "**PANKAJ NAGPAL (1613101474)**" who carried out the
project work under my supervision.

SIGNATURE OF HEAD

Professor & Dean,

School of Computing Science & Engineering

SIGNATURE OF SUPERVISOR

Mr. P.RAJAKUMAR

Assistant Professor

School of Computing Science & Engineering

TABLE OF CONTENTS

ABSTRACT

This project provides the facility of Single Sign On (SSO) with LDAP Authentication. LDAP is a protocol that works on Directory Servers it can be Enterprise Directory or Active Directory.

For this we need to add some roles to the Domain controller. For any user when login attempt for any application, it depends for which application or portal user wants to login or what policies and processes defined for the same. As per the process Authentication will be via LDAP only but the processes of Journey may be vary accordingly.

To access a network's **LDAP** services, your computer must first log in to a server that supports the protocol, a **process** called **authentication**. **LDAP** lets a network administrator assign different levels of access to its many users, keeping the information secure.

LDAP is a protocol that supports directory servers like servers used for Active directory or enterprise directory. Authentication validation of user credential also be done by IDP via LDAP only. Required claims also provided by IDP from LDAP as per the request.

We have taken different bindings also to done this authentication process successfully. Binding are the mechanisms to transfer the messages. There are three types of bindings used :Redirect binding, Post binding, Artifact binding.

LIST OF FIGURES

LIST OF ABBREVIATIONS

ACRONYM	EXPANSION
LDAP	Lightweight Directory Access Protocol
IT	Information Technology
ADFS	Active Directory Federation Services
SP	Service Provider
IDP	Identity Provider
ACP	Access control policy
SSO	Single Sign on
ED	Enterprise Directory
IWA	Internal window authentication

INTRODUCTION

I. Overall Description:

The goal of this project is to provide the Authentication to different applications via two Methods :

1. Internal Window Authentication (IWA)
2. Single Sign on (SSO)

Internal Window Authentication (IWA) : Authentication Server in an environment based on Windows users is straightforward.

- The user credentials are validated when the user logs in to the Windows operating system on the client machine.
- Later when the user wants to establish a session with Server (for example, via a browser on the desktop), then can use the built-in Integrated Windows Authentication (IWA).
- The identity of the logged-in user is communicated to Server using SAML token. This solution provides single sign-on capabilities right out of the box. In case the authentication exchange fails to identify the user, the browser prompts the user for a Windows user account name and password.

Single Sign on (SSO) : Single sign-on (SSO) is a session and user authentication service that permits an end user to enter one set of login credentials (such as a name and password) and be able to access multiple applications.

II.Objective:

This is use to design the following tasks :

1. User experience: The most apparent benefit is that users can move between services securely and uninterrupted without specifying their credentials each time.

2. Ability for employees to log in just one time with one set of credentials to get access to all corporate apps, websites, and data for which they have permission.

3. Security: The users credentials are provided directly to the central SSO server, not the actual service that the user is trying to access, and therefore the credentials cannot be cached by the service. The central authentication point – the SSO service – limits the possibility of phishing.

4. Resource savings: IT administrators can save their time and resources by utilizing the central web access management service Application and web developers receive a complete authentication and authorization framework that they can use to build secure, user customized services.

5. SSO saves money: Around half of all IT helpdesk calls are for password resets. With only one password to remember, SSO can significantly reduce IT helpdesk costs.

6. Building a centralized database, SSO supports compliance, promotes secure file sharing, and ensures effective access reporting.

III.Background:

The pool for outlining SAML standards and security is OASIS (Organization for the Advancement of structured data standards) they're a non-profit international organization that promotes the event and adoption of open standards for security and internet services. OASIS was supported in 1993 beneath standard generalized markup language (Standard Generalized Markup Language) Open till its name amendment in 1998. Headquarters for OASIS area unit located in North America however there's active member participation internationally in one hundred countries on 5 continents SAML 1.0 became associate OASIS

customary toward the top of 2002, with its early formations starting in 2001. The goal behind SAML one.0 was to create a XML framework to allow for the authentication and authorization from a single sign-on perspective. At the time of this milestone, other firms and consortiums started extending SAML 1.0. whereas these extensions were being shaped, the SAML 1.1 specification was sanctioned as associate OASIS standard within the fall of 2003. The next major revision of SAML is a pair of.0, and it became an official OASIS customary in 2005. SAML 2.0 involves major changes to the SAML specifications. this can be the first revision of the quality that's not backwards compatible, and it provides vital further functionality. SAML 2.0 currently supports W3C XML encryption to satisfy privacy needs [3]. Another advantage that SAML a pair of.0 includes is that the support for

service supplier initiated net single sign-on exchanges. This allows for the service supplier to question the identity provider for authentication in addition, SAML 2.0 adds “Single Logout” practicality. the rest of this text

are going to be discussing implementation of a SAML 2.0 atmosphere. There area unit 3 roles concerned in a very SAML group action –

an declarative party, a relying party, and a topic. The asserting party (identity provider) is that the system in authority that gives the user info. The relying party (service provider) is that the system that trusts the asserting party’s info, and uses the info to provide associate application to the user. The user and their identity that’s concerned within the group action area unit called the subject. The elements that structure the SAML customary area unit assertions, protocols, bindings and profiles. Each layer

of the quality areoften custom, permitting specific business cases to be self-addressed per company. Since each company’s situations might be distinctive, the implementation of those business cases ought to be ready to be

customized per service and per identity suppliers.

The group action from the declarative party to the relying party is termed a SAML assertion. The relying party assumes that each one knowledge contained within the assertion from the asserting party is valid. The structure of the SAML assertion is outlined by the XML schema and contains header info, the topic and statements regarding the subject within the type of attributes and conditions. The assertion can even contain authorization statements defining what the user is allowable to try and do within the net application.

The SAML customary defines request and response protocols accustomed communicate the assertions between the service supplier (relying party) and also the identity provider (asserting party).

SOFTWARE REQUIREMENT SPECIFICATION

HARD WARE SPECIFICATION:

GCP Plateform

Created instance Window Server 2016

HARD DISK DRIVE : 500 GB

RAM : 8 Gb

SOFTWARE SPECIFICATION:

OPERATING SYSTEM : Windows server 2016

ROLES : ADFS, ADDS, IIS, DNS

LITERATURE SURVEY

Active Directory Federation Services provides access control and single sign on across a wide variety of applications including Office 365, cloud based SaaS applications, and applications on the corporate network. Introducing AD FS 2.0". Microsoft TechNet. May 2, 2010. Retrieved March 2, 2017

- For the IT organization, it enables you to provide sign on and access control to both modern and legacy applications, on premises and in the cloud, based on the same set of credentials and policies.
- For the user, it provides seamless sign on using the same, familiar account credentials.
- For the developer, it provides an easy way to authenticate users whose identities live in the organizational directory so that you can focus your efforts on your application, not authentication or identity.

Active Directory Federation Services (AD FS), a software component developed by Microsoft, can run on Windows Server operating systems to provide users with single sign-on access to systems.

In AD FS, identity federation is established between two organizations by establishing trust between two security realms. A federation server on one side (the Accounts side) authenticates the user through the standard means in Active Directory Domain Services and then issues a token containing a series of claims about the user, including its identity. On the other side, the Resources side, another federation server validates the token and issues another token for the local servers to accept the claimed identity. This allows a system to provide controlled access to its resources or services to a user that belongs to another security realm without requiring the user to authenticate directly to the system and without the two systems sharing a database of user identities or passwords.

EXISTING SYSTEM

Many business owners and IT managers of growing businesses prefer Linux over competitive operating systems. The major factors leading businesses to move to Linux are its low cost, security, reliability, openness, and freedom to avoid single-vendor environments.

In fact, businesses such as Amazon.com and Google rave about operational costs saved and efficiencies found from implementing Linux on their servers. These commercial examples, combined with the experiences of developers and IT managers, have led to widespread installations of Linux servers within small and medium-sized businesses. An IDC 2007 report says that Linux holds 12.7 percent of the overall server market.

Oracle Directory Server provides enterprise-wide directory services, meaning it provides information to a wide variety of applications. Until recently, many applications came bundled with their own proprietary user databases, with information about the users specific to that application. While a proprietary database can be convenient if you use only one application, multiple databases become an administrative burden if the databases manage the same information.Directory Server serves directory data to standards compliant LDAP and DSML applications. Directory Server stores the data in customized, binary tree databases, allowing quick searches even for large data sets only.

Each directory entry has attributes. For entries that concern people, these attributes may reflect names, phone numbers, and email addresses. No need to use any algorithms or applications, It will be like database only from where you can take the data of users that needed. This is only like a database where all the user entries saved at one place, Neither SSO nor real-time authentication was provided.Only one team/person has rights to change password and many different team to handle on task.

Here password is different for all the different applications.

PROPOSED SYSTEM

In this project Single Sign-On services protects thousands of applications from risks associated with password management and enables users to access mobile, cloud, and on-premises programs on any device. By implementing SSO, users need to enter a single username and password for once and then, acquire access to the devices and apps that are based upon policy from enterprise. It gives support to internal (contractors, employees) as well as external (customers, partners) users.

Our Single Sign-On solution strengthens the existing cloud security protocols along with single access to several users for IT monitoring ease. The challenges get significantly reduced in terms of clicks and hence, eliminating time in remembering the account usernames and passwords. An administrator will be able to track real-time activities with the provisioning and de-provisioning of sanctioned applications. We are also providing capability of restricting access to unsanctioned programs for organization users. Our SSO security is compatible with all mobile platforms and it does not need re-configuration in case of operating system updates.

LDAP, Lightweight Directory Access Protocol, is an Internet protocol that email and other programs use to look up information from a server.

LDAP is not limited to contact information, or even information about people. LDAP is used to look up encryption certificates, pointers to printers and other services on a network, and provide "single sign-on" where one password for a user is shared between many services. LDAP is appropriate for any kind of directory-like information, where fast lookups and less-frequent updates are the norm.

- Here Server version which is used is 4.0.
- It is not just the stored database but providing, SSO supports compliance, promotes secure file sharing, and ensures effective access reporting.
- AD FS is a native Windows Server Role that allows users to access third-party systems

and applications insid90e or outside the corporate firewall with a single login.

- Service provider (SP) and Identity Provider (IDP) plays important role to provide authentication. A trust should be maintained in between SP and IDP and that happened via Certificate.
- Certificates are used to authenticate an individual’s identity.
- Data transferred in the form of Metadata. Metadata is a xml file which contains the information required by the resource parties (IDP and SP).
- Enables end users to achieve one-point access to all business programs
- All cloud applications will be accessed through desktops, smartphones, etc.
- Consolidate with custom on-premises applications through custom protocol / development
- Easy provisioning and deprovisioning of cloud applications
- Add or remove existing cloud programs without hard efforts
- Manage several users with an individual account from 1 console

Helps in increasing productivity by keeping the data safe and secure

IMPLIMENTATION AND ARCHITECTURE

This architecture shows the single sign on (SSO) mechanism for all applications. There will a centralized access directory where all the data will be saved. That directory will be enterprise directory or Active directory. The users of Application (Salesforce) will be integrated with the directory and then whenever user login in any application just one time need to enter password and that too is correct or not will be validated via LDAP, and session created. For the next time when user login in that application automatically get logged-in, no need to enter ID and password again.

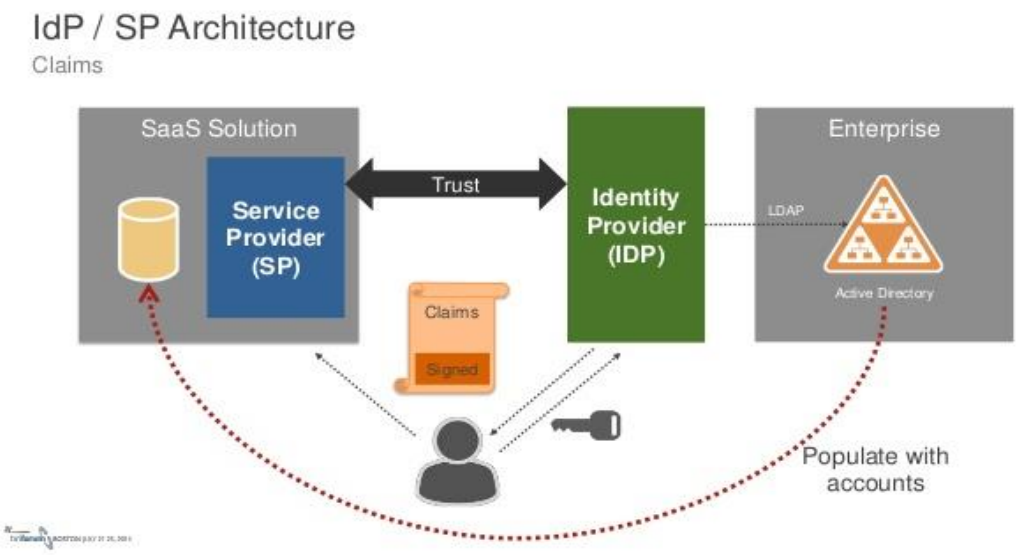


Figure1.1

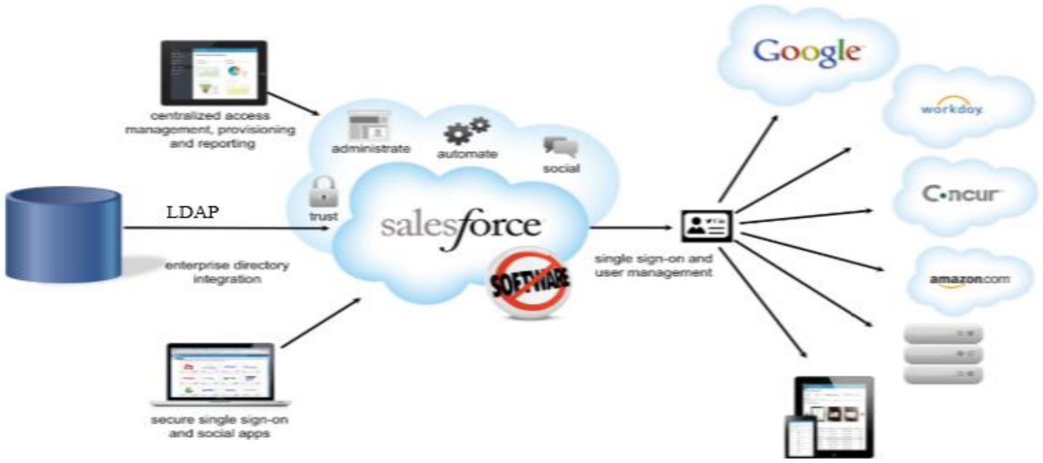

centralized access management, provisioning and reporting
administrate
automate
social
trust
LDAP
salesforce
enterprise directory integration
SOFTWARE
single sign-on and user management
secure single sign-on and social apps
Google
workday
Concur
amazon.com

Figure 2.2

When the session is SP-initiated then process will be as follows:

1. User will attempt to login in any application on a browser.
2. Then service provider will check if previous login session is saved if yes then user will be directly accessible else send authentication request to identity provider.
3. Here also any Identity provider checked for the saved previous session else redirect to login page of that organization.
4. There user put credentials to login and those credentials will be authenticating via LDAP.
5. Then a SAML token will be generated that token IDP will be send to SP.
6. Then whatever the claims required send to application for authentication and finally permission granted or we can say user successfully logged in.

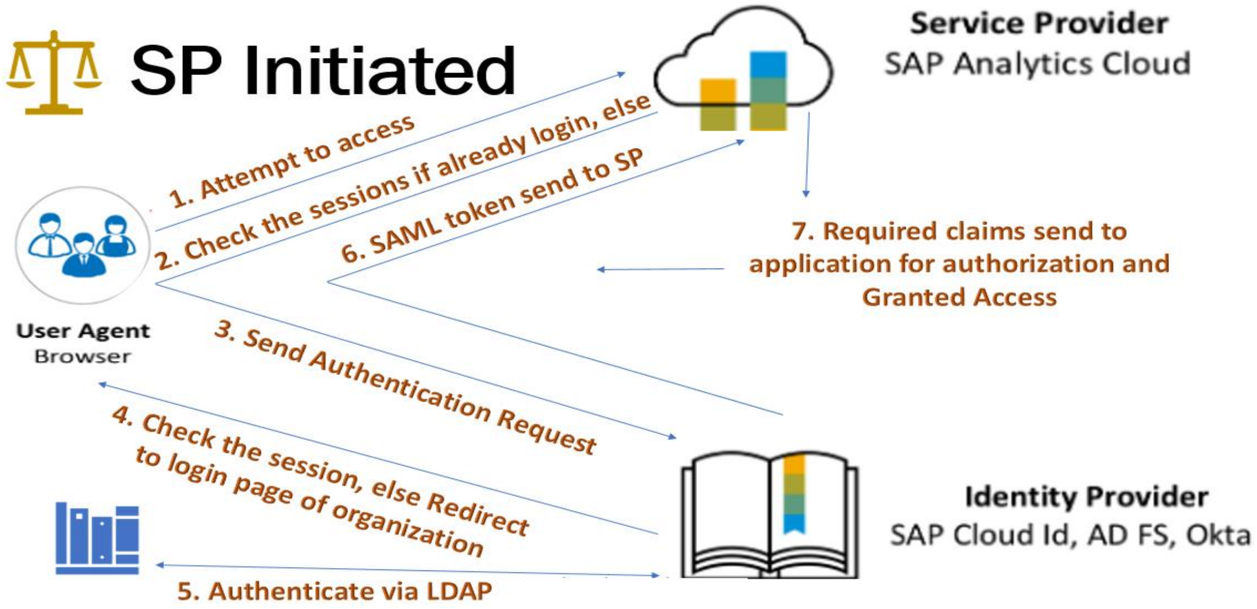

SP Initiated
Service Provider
SAP Analytics Cloud
1. Attempt to access
2. Check the sessions if already login, else
6. SAML token send to SP
7. Required claims send to application for authorization and Granted Access
User Agent
Browser
3. Send Authentication Request
4. Check the session, else Redirect to login page of organization
Identity Provider
SAP Cloud Id, AD FS, Okta
5. Authenticate via LDAP

Figure 3.3

When the session is IDP-initiated then process will be as follows:

1. Here user attempt to login to any portal or an application.
2. Then Identity provider will check for the session already login by another application if yes then user will be directly accessible else redirect to login page of that organization.
3. Here when user put credentials for login authenticated via Active directory (AD).
4. Then a SAML token will be generated that Identity provider sends to the Service provider.
5. Then service provider sends required claims to application for authorization and user will be successfully logged in.

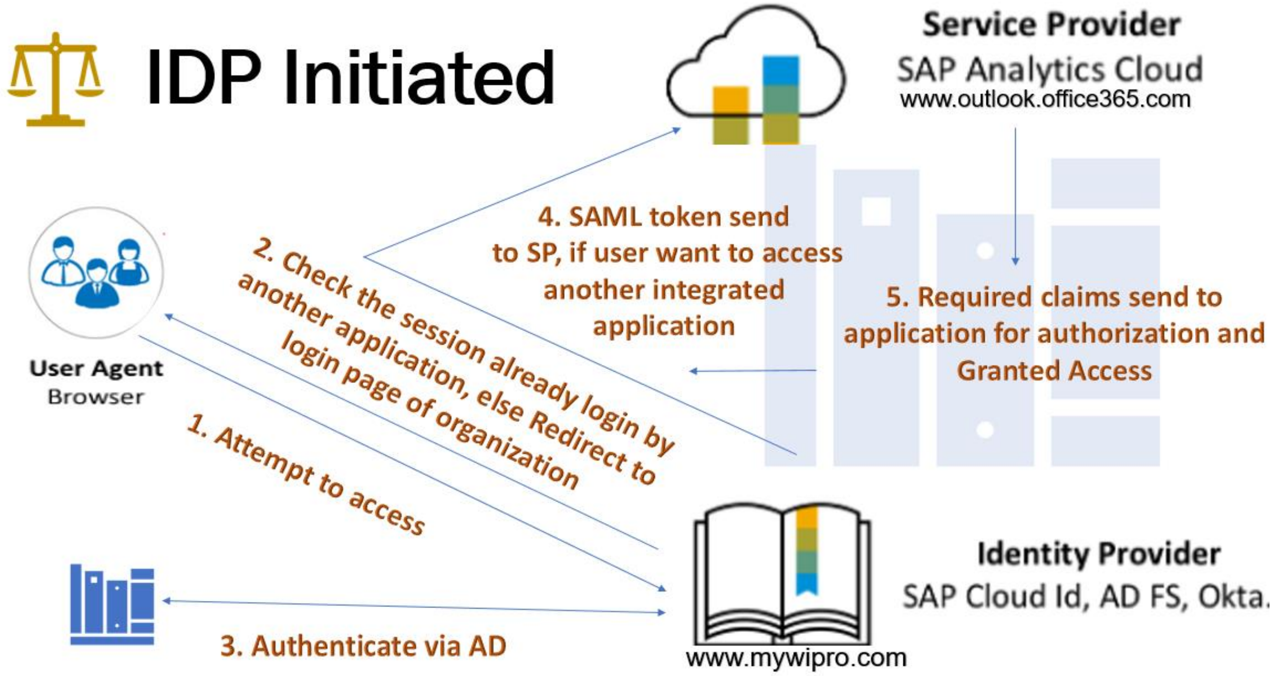

IDP Initiated
Service Provider
SAP Analytics Cloud
www.outlook.office365.com
User Agent
Browser
2. Check the session already login by another application, else Redirect to login page of organization
4. SAML token send to SP, if user want to access another integrated application
5. Required claims send to application for authorization and Granted Access
1. Attempt to access
3. Authenticate via AD
Identity Provider
SAP Cloud Id, AD FS, Okta.
www.mywipro.com

Figure 4.4

Sequential Diagram :

This structure is showing the authentication process. Service Provider and Identity provider plays very important role for communication. User will be request first then Service provider redirect to Identity provider, then from Identity provider SSO service requested. User identified and Identity provider redirect back to Service provider with SAML assertion. User request a=Assertion Consumer Service (ACS). And finally service provider respond to the requested user. Authentication request contains some of the attributes, which are send by the SP to IDP.

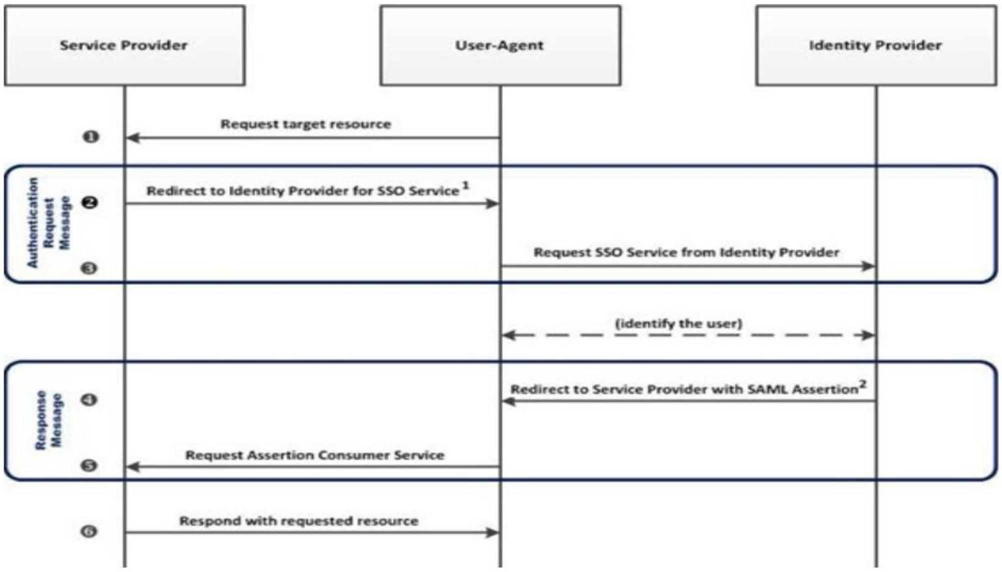
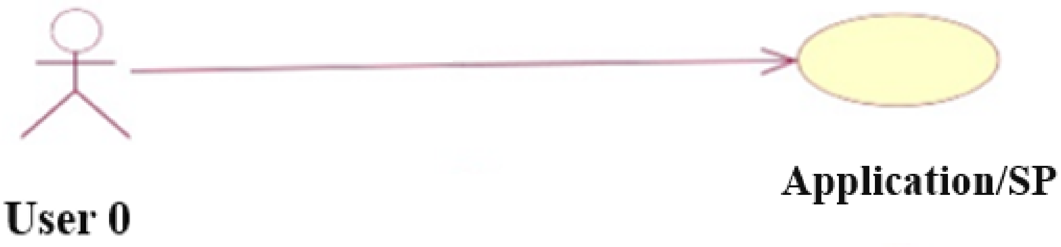
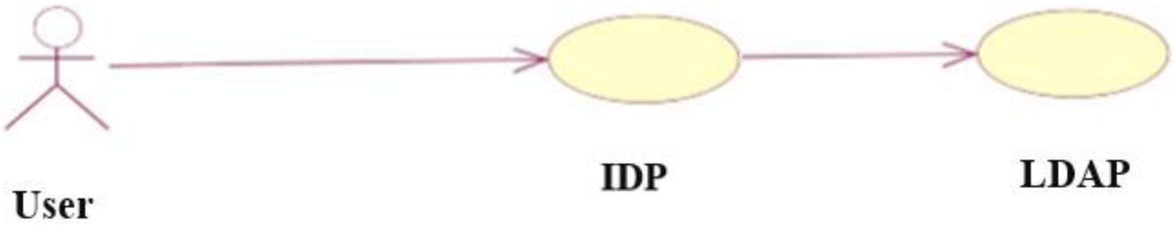

Service Provider
User-Agent
Identity Provider
❶
Request target resource
Authentication Request Message
❷
Redirect to Identity Provider for SSO Service[1]
❸
Request SSO Service from Identity Provider
(identify the user)
Response Message
❹
Redirect to Service Provider with SAML Assertion[2]
❺
Request Assertion Consumer Service
❻
Respond with requested resource

Figure 5.5

Usecase Diagram :



User Authentication Request



Authentication via LDAP

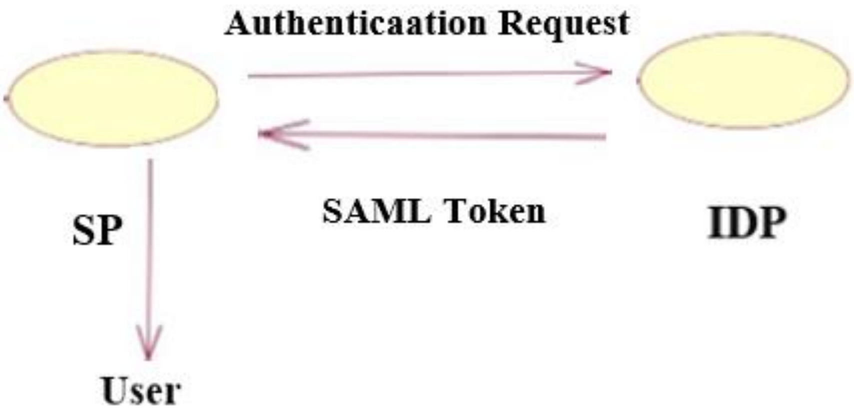
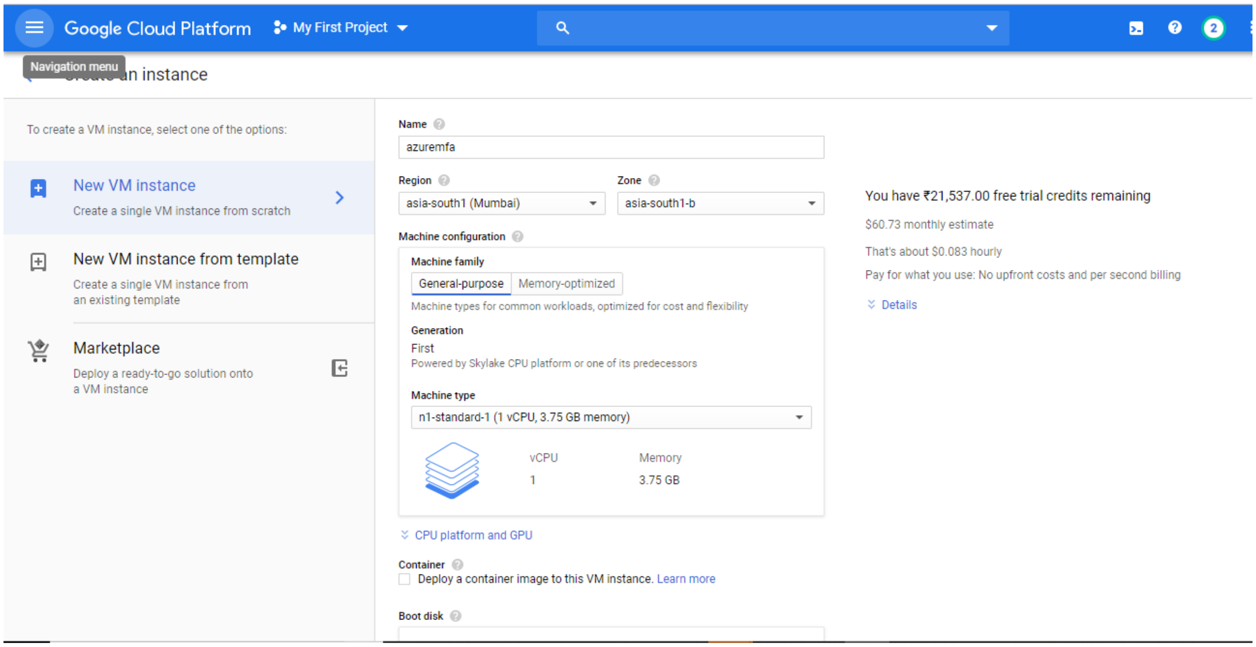


Figure 6.6

INSTALLATION AND CONFIGURATION

INSTALLATION:

1. Deployment using GCP platform



To create a VM instance, select one of the options:

New VM instance
Create a single VM instance from scratch

New VM instance from template
Create a single VM instance from an existing template

Marketplace
Deploy a ready-to-go solution onto a VM instance

Name: azuremfa

Region: asia-south1 (Mumbai)

Zone: asia-south1-b

Machine configuration

Machine family: General-purpose | Memory-optimized

Machine types for common workloads, optimized for cost and flexibility

Generation: First
Powered by Skylake CPU platform or one of its predecessors

Machine type: n1-standard-1 (1 vCPU, 3.75 GB memory)

vCPU: 1 Memory: 3.75 GB

CPU platform and GPU

Container
□ Deploy a container image to this VM instance. Learn more

Boot disk

You have ₹21,537.00 free trial credits remaining

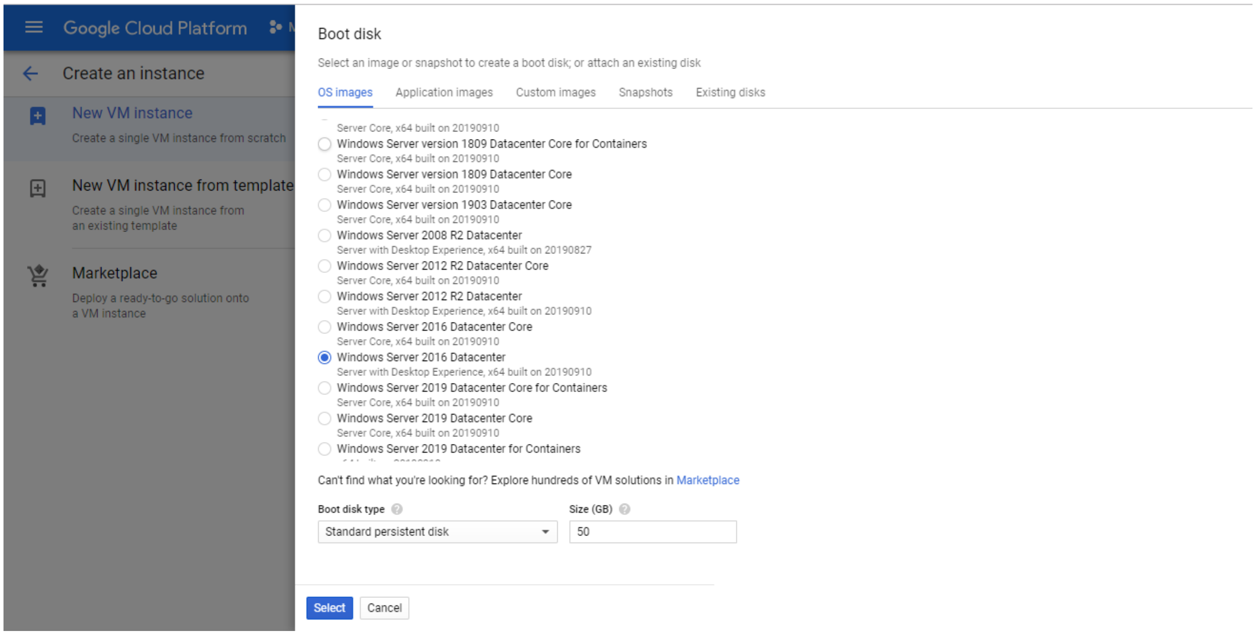
$60.73 monthly estimate

That's about $0.083 hourly

Pay for what you use: No upfront costs and per second billing

Details

2. Selecting Windows Server 2016 with Desktop server experience as Boot Disk



Google Cloud Platform
Create an instance
New VM instance
Create a single VM instance from scratch
New VM instance from template
Create a single VM instance from an existing template
Marketplace
Deploy a ready-to-go solution onto a VM instance

Boot disk

Select an image or snapshot to create a boot disk; or attach an existing disk

OS images | Application images | Custom images | Snapshots | Existing disks

Server Core, x64 built on 20190910
○ Windows Server version 1809 Datacenter Core for Containers
Server Core, x64 built on 20190910
○ Windows Server version 1809 Datacenter Core
Server Core, x64 built on 20190910
○ Windows Server version 1903 Datacenter Core
Server Core, x64 built on 20190910
○ Windows Server 2008 R2 Datacenter
Server with Desktop Experience, x64 built on 20190827
○ Windows Server 2012 R2 Datacenter Core
Server Core, x64 built on 20190910
○ Windows Server 2012 R2 Datacenter
Server with Desktop Experience, x64 built on 20190910
○ Windows Server 2016 Datacenter Core
Server Core, x64 built on 20190910
● Windows Server 2016 Datacenter
Server with Desktop Experience, x64 built on 20190910
○ Windows Server 2019 Datacenter Core for Containers
Server Core, x64 built on 20190910
○ Windows Server 2019 Datacenter Core
Server Core, x64 built on 20190910
○ Windows Server 2019 Datacenter for Containers

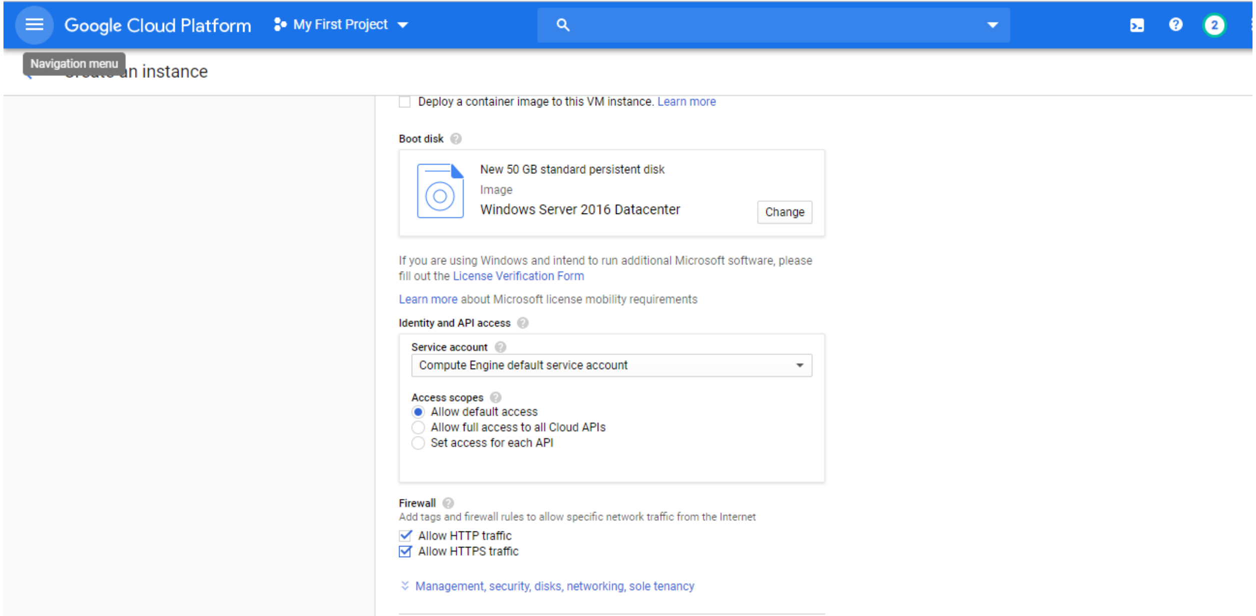
Can't find what you're looking for? Explore hundreds of VM solutions in Marketplace

Boot disk type: Standard persistent disk

Size (GB): 50

Select | Cancel

3. Allowing HTTP and HTTPS traffic in the VM Instance.



□ Deploy a container image to this VM instance. Learn more

Boot disk

New 50 GB standard persistent disk
Image
Windows Server 2016 Datacenter
Change

If you are using Windows and intend to run additional Microsoft software, please fill out the License Verification Form

Learn more about Microsoft license mobility requirements

Identity and API access

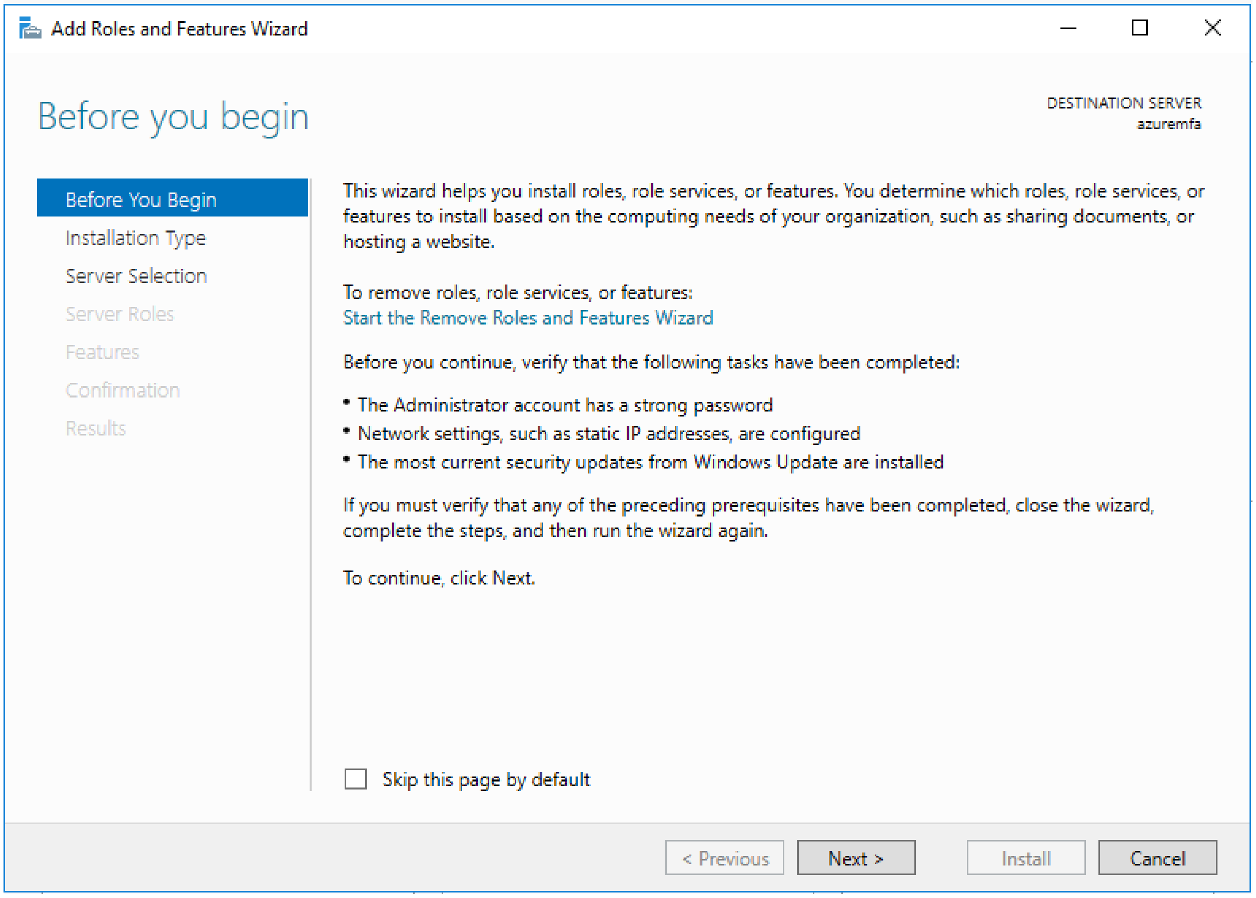
Service account: Compute Engine default service account

Access scopes
● Allow default access
○ Allow full access to all Cloud APIs
○ Set access for each API

Firewall
Add tags and firewall rules to allow specific network traffic from the Internet
☑ Allow HTTP traffic
☑ Allow HTTPS traffic

Management, security, disks, networking, sole tenancy

4. Adding Roles in the server



Before you begin

DESTINATION SERVER
azuremfa

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

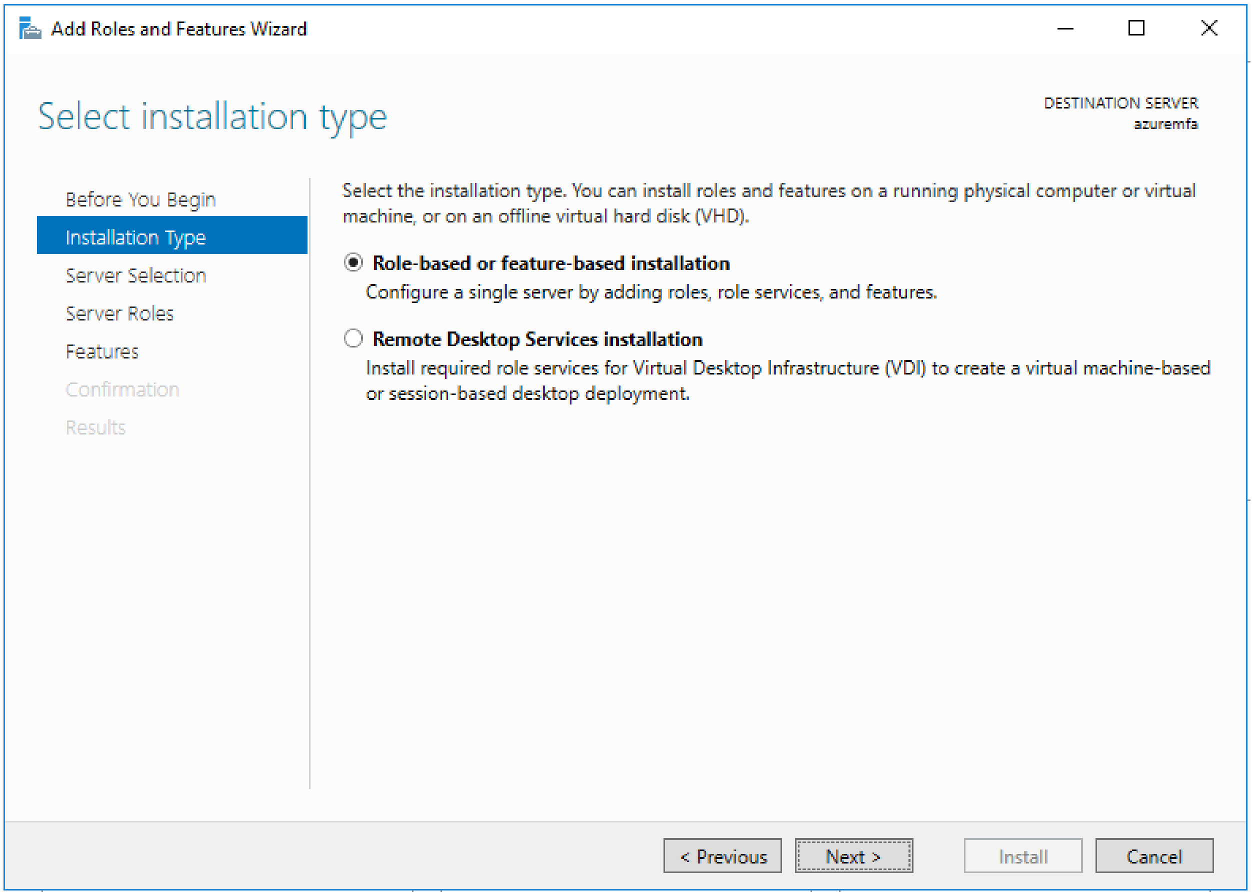
Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default



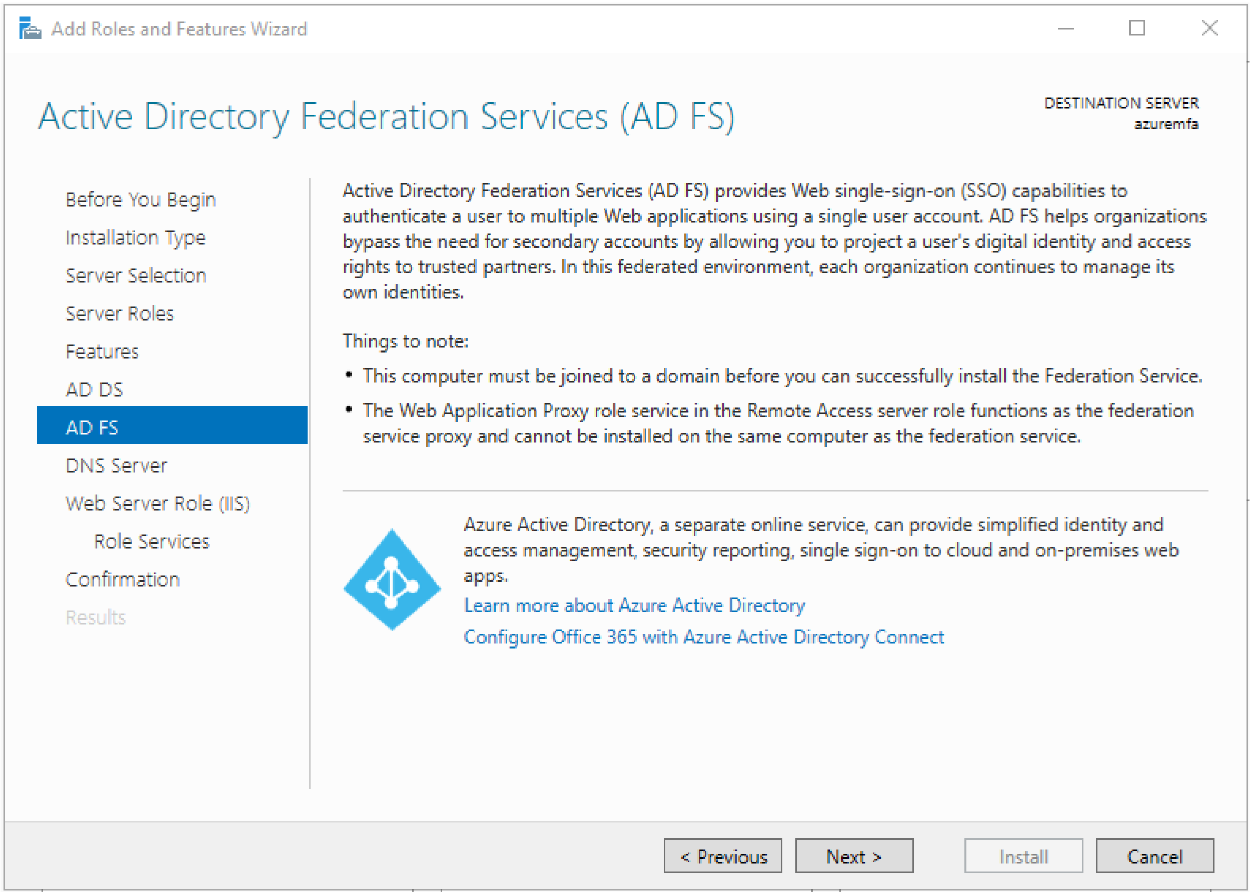
Select installation type

DESTINATION SERVER
azuremfa

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.



Active Directory Federation Services (AD FS)

DESTINATION SERVER
azuremfa

Active Directory Federation Services (AD FS) provides Web single-sign-on (SSO) capabilities to authenticate a user to multiple Web applications using a single user account. AD FS helps organizations bypass the need for secondary accounts by allowing you to project a user's digital identity and access rights to trusted partners. In this federated environment, each organization continues to manage its own identities.

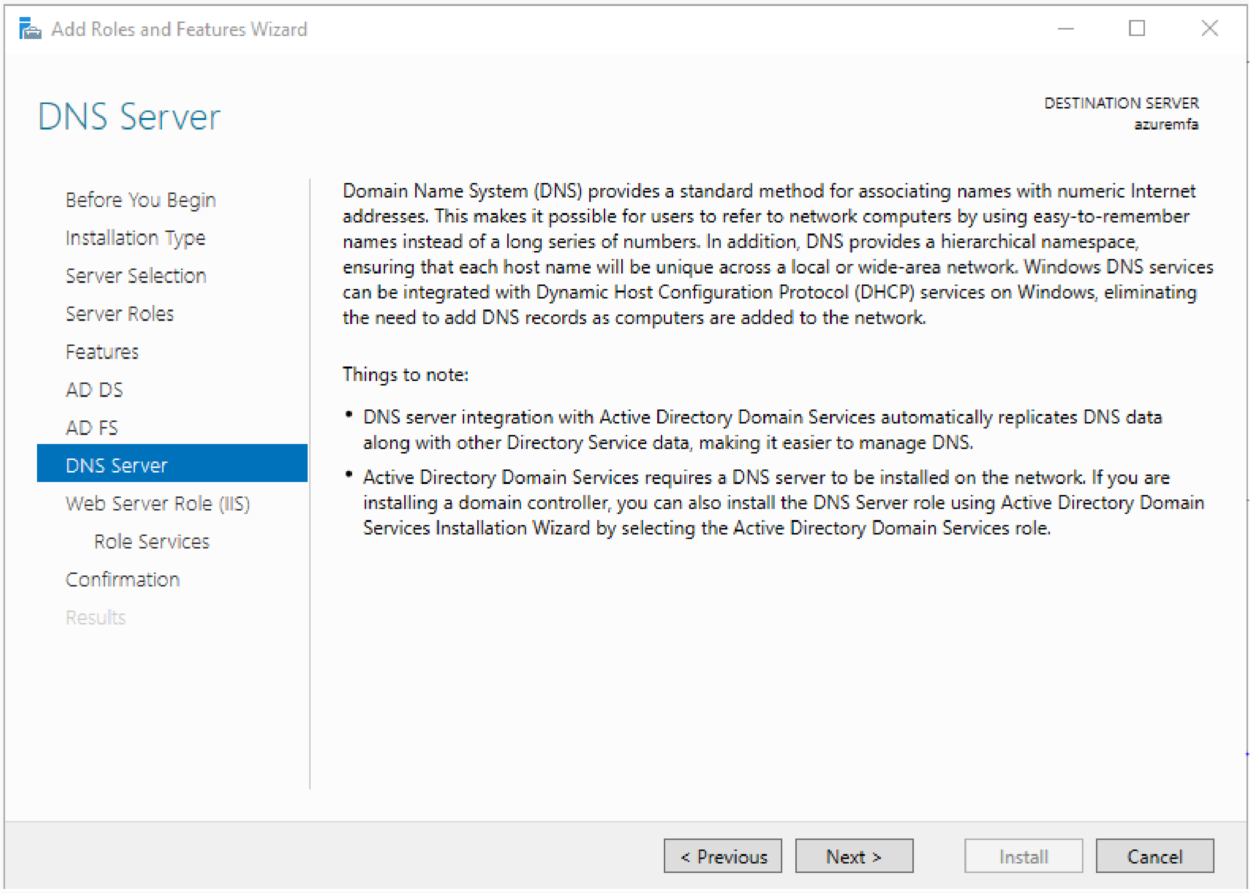
Things to note:

- This computer must be joined to a domain before you can successfully install the Federation Service.
- The Web Application Proxy role service in the Remote Access server role functions as the federation service proxy and cannot be installed on the same computer as the federation service.

Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.

Learn more about Azure Active Directory

Configure Office 365 with Azure Active Directory Connect



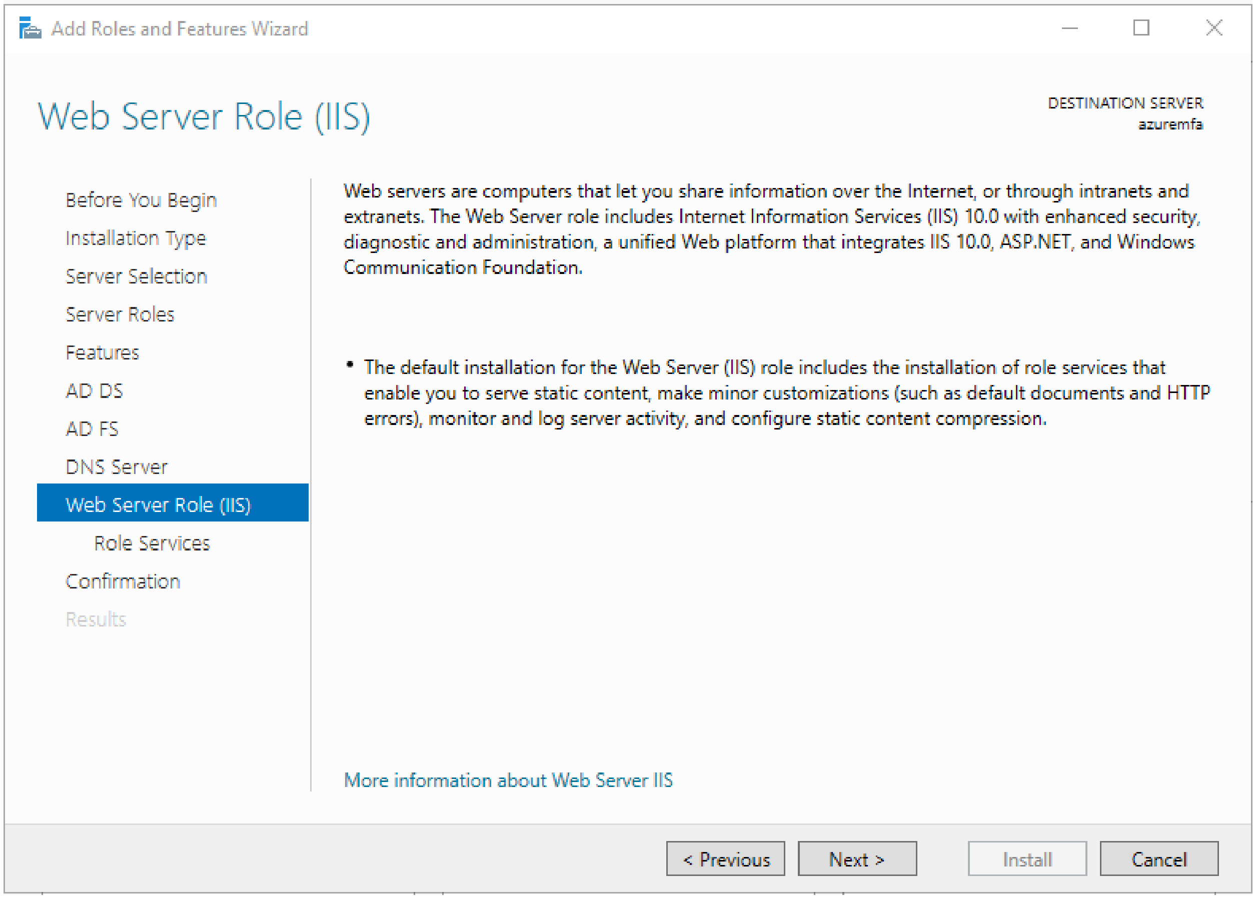
DNS Server

DESTINATION SERVER
azuremfa

Domain Name System (DNS) provides a standard method for associating names with numeric Internet addresses. This makes it possible for users to refer to network computers by using easy-to-remember names instead of a long series of numbers. In addition, DNS provides a hierarchical namespace, ensuring that each host name will be unique across a local or wide-area network. Windows DNS services can be integrated with Dynamic Host Configuration Protocol (DHCP) services on Windows, eliminating the need to add DNS records as computers are added to the network.

Things to note:

- DNS server integration with Active Directory Domain Services automatically replicates DNS data along with other Directory Service data, making it easier to manage DNS.
- Active Directory Domain Services requires a DNS server to be installed on the network. If you are installing a domain controller, you can also install the DNS Server role using Active Directory Domain Services Installation Wizard by selecting the Active Directory Domain Services role.



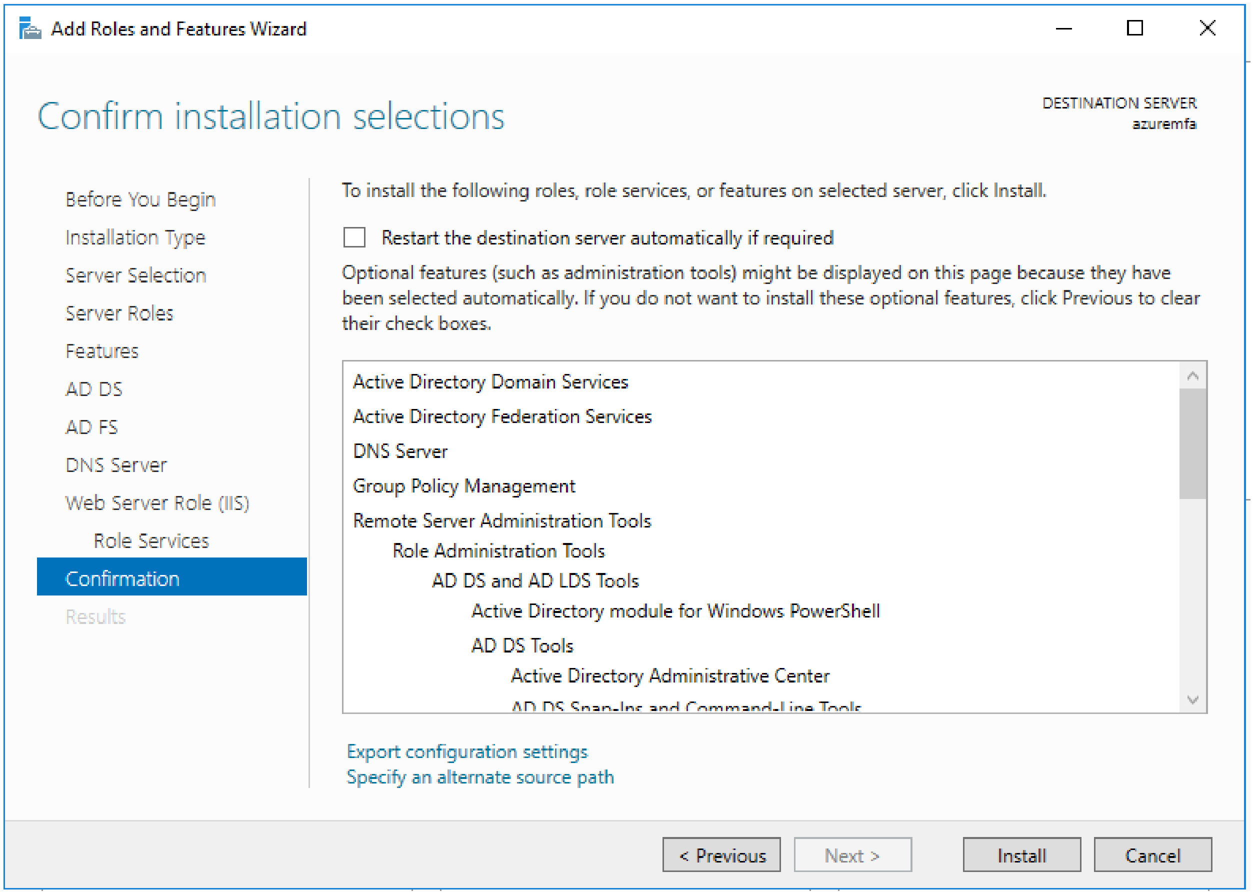
Web Server Role (IIS)

DESTINATION SERVER
azuremfa

Web servers are computers that let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 10.0 with enhanced security, diagnostic and administration, a unified Web platform that integrates IIS 10.0, ASP.NET, and Windows Communication Foundation.

- The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

More information about Web Server IIS



Confirm installation selections

DESTINATION SERVER
azuremfa

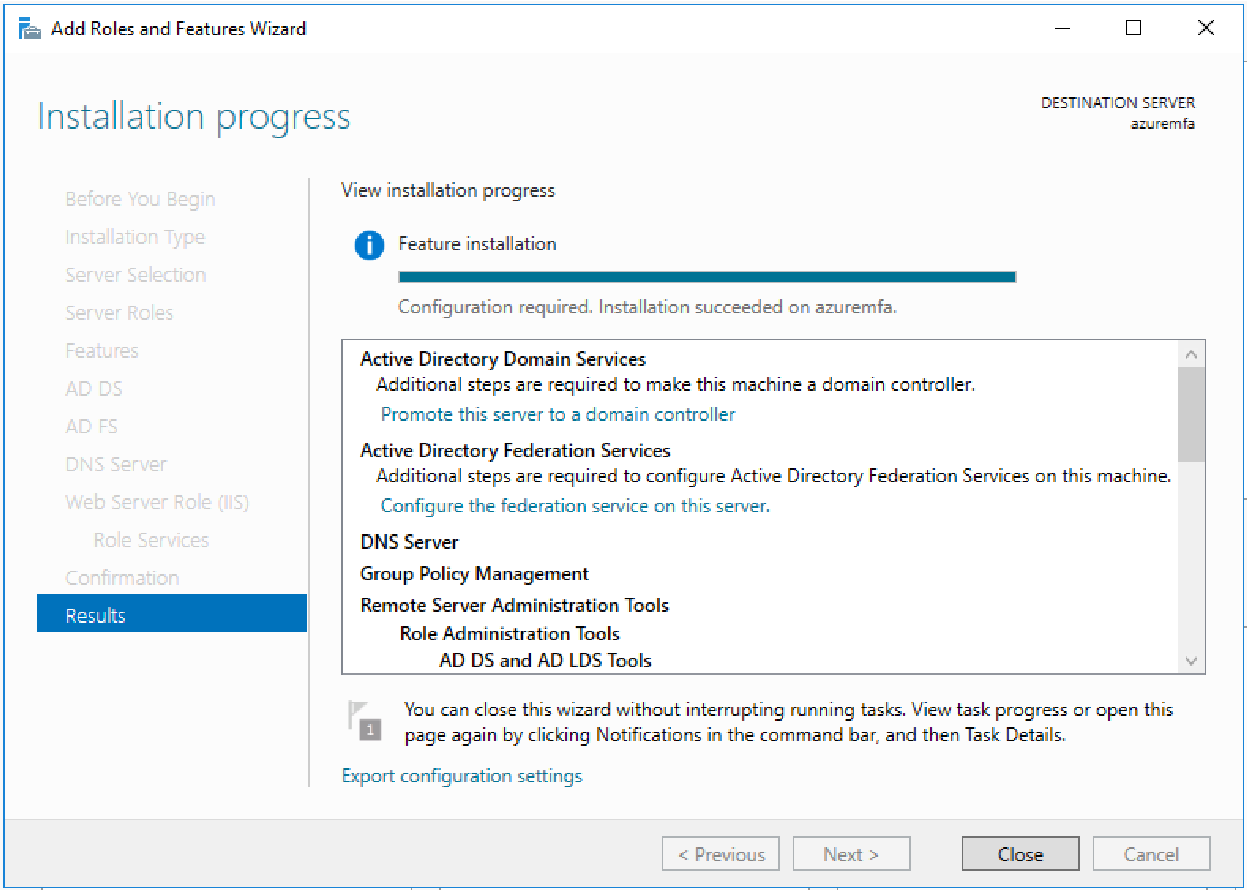
To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

- Active Directory Domain Services
- Active Directory Federation Services
- DNS Server
- Group Policy Management
- Remote Server Administration Tools
  - Role Administration Tools
    - AD DS and AD LDS Tools
      - Active Directory module for Windows PowerShell
      - AD DS Tools
        - Active Directory Administrative Center
        - AD DS Snap-Ins and Command-Line Tools

Export configuration settings
Specify an alternate source path



Installation progress

DESTINATION SERVER
azuremfa

View installation progress

Feature installation

Configuration required. Installation succeeded on azuremfa.

Active Directory Domain Services
Additional steps are required to make this machine a domain controller.
Promote this server to a domain controller

Active Directory Federation Services
Additional steps are required to configure Active Directory Federation Services on this machine.
Configure the federation service on this server.

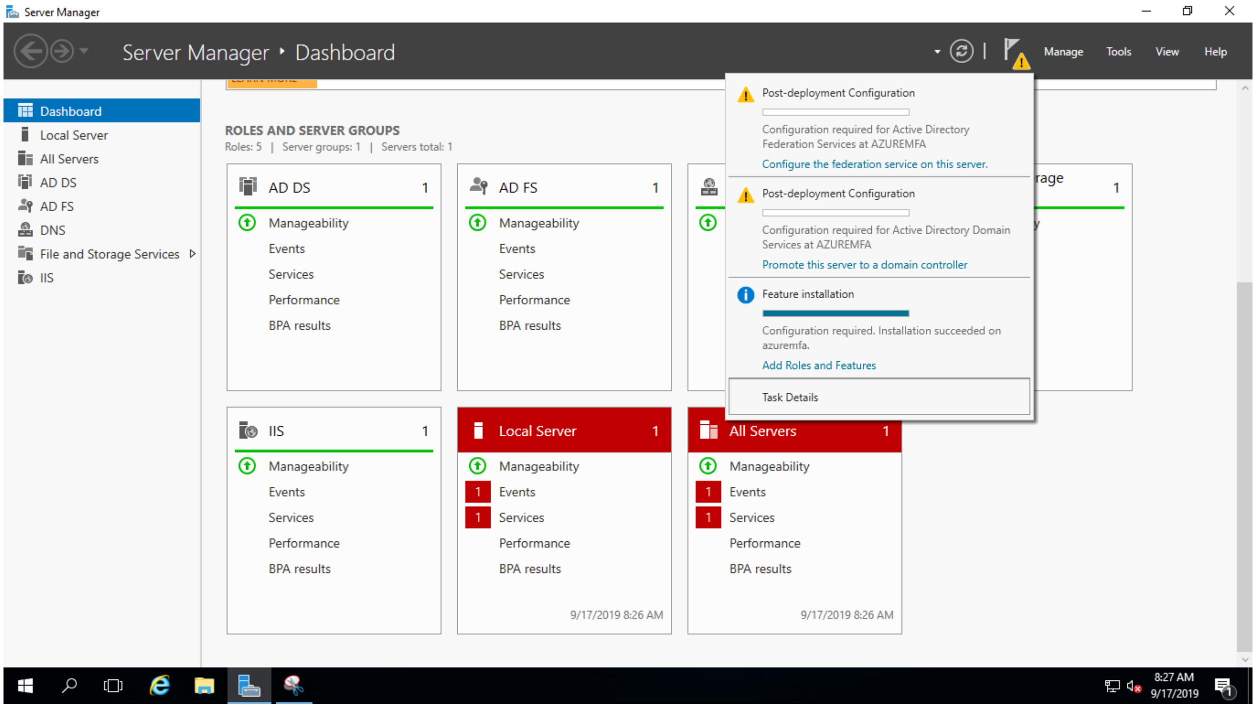
DNS Server

Group Policy Management

Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings



ROLES AND SERVER GROUPS
Roles: 5 | Server groups: 1 | Servers total: 1

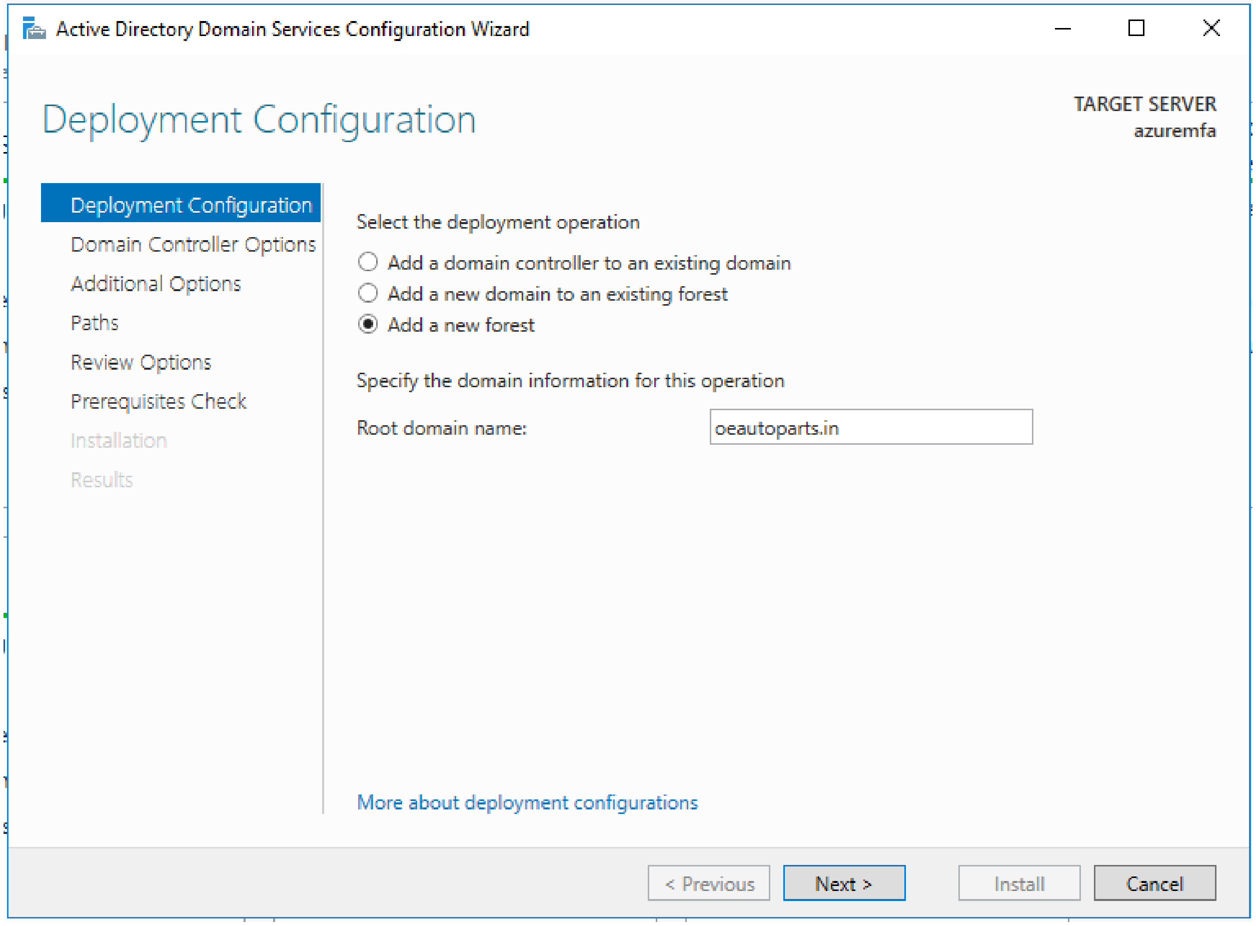
Post-deployment Configuration
Configuration required for Active Directory Federation Services at AZUREMFA
Configure the federation service on this server.

Post-deployment Configuration
Configuration required for Active Directory Domain Services at AZUREMFA
Promote this server to a domain controller

Feature installation
Configuration required. Installation succeeded on azuremfa.
Add Roles and Features

Task Details

5. LDAP Configuration



Deployment Configuration

TARGET SERVER
azuremfa

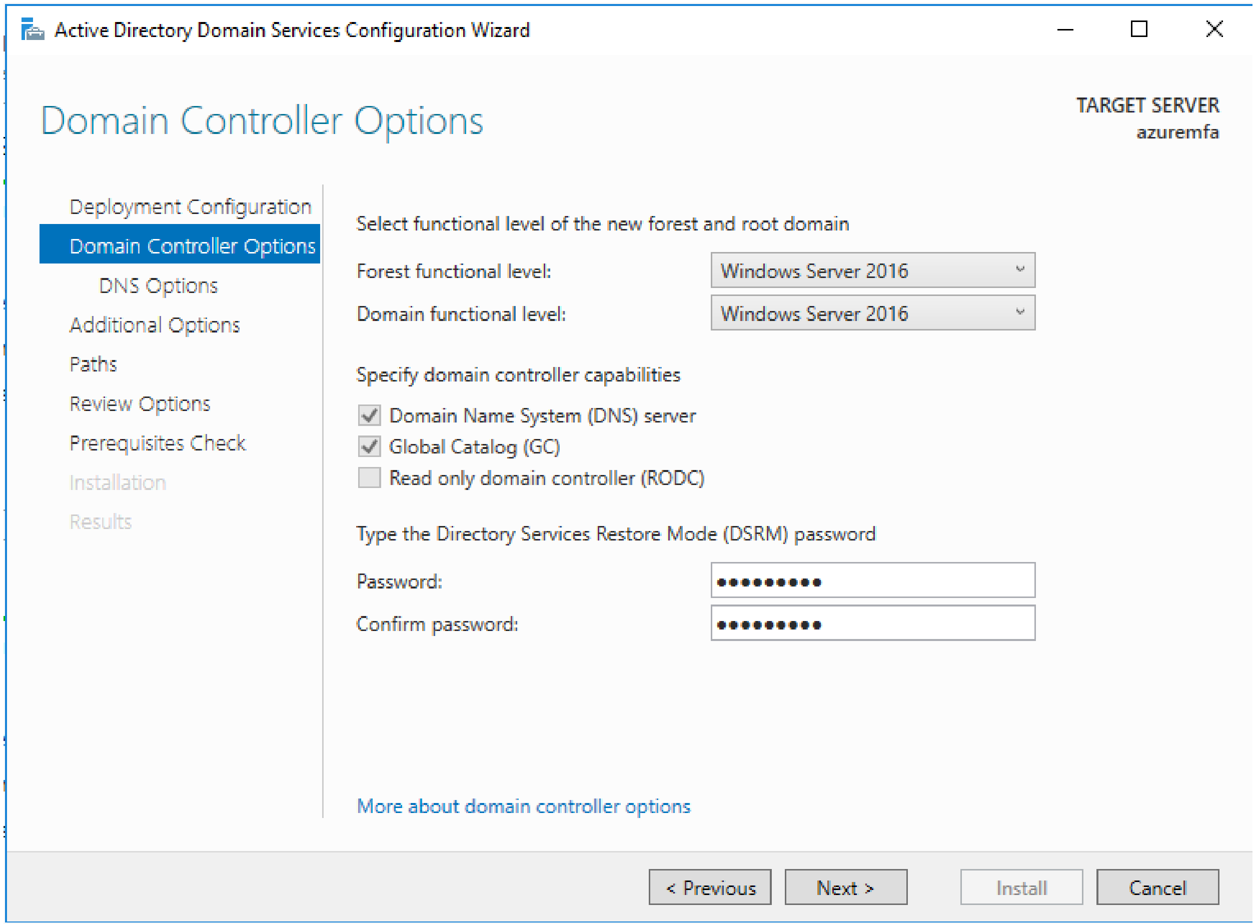
Select the deployment operation

○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

Specify the domain information for this operation

Root domain name: oeautoparts.in

More about deployment configurations



Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
azuremfa

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

☑ Domain Name System (DNS) server

☑ Global Catalog (GC)

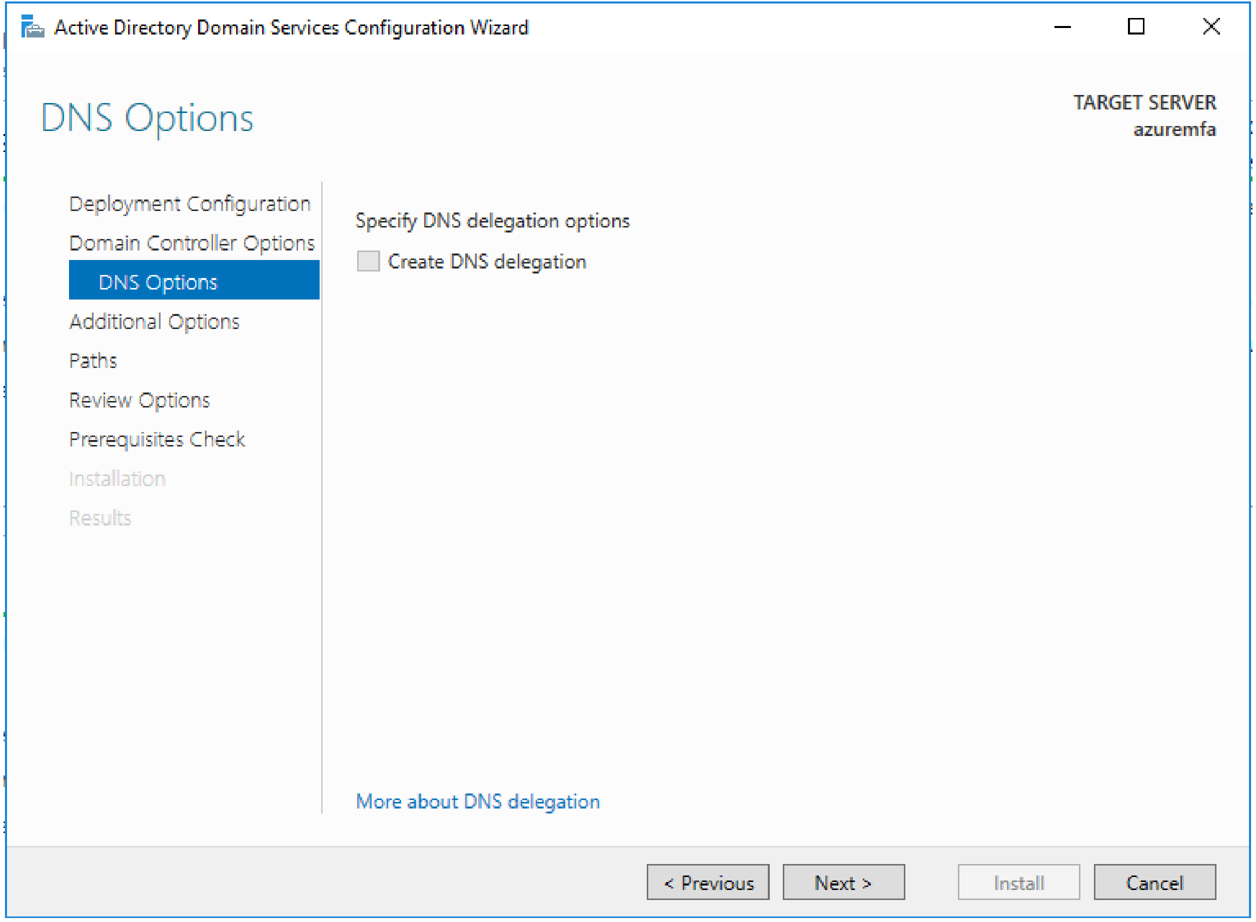
□ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

More about domain controller options



Active Directory Domain Services Configuration Wizard

DNS Options

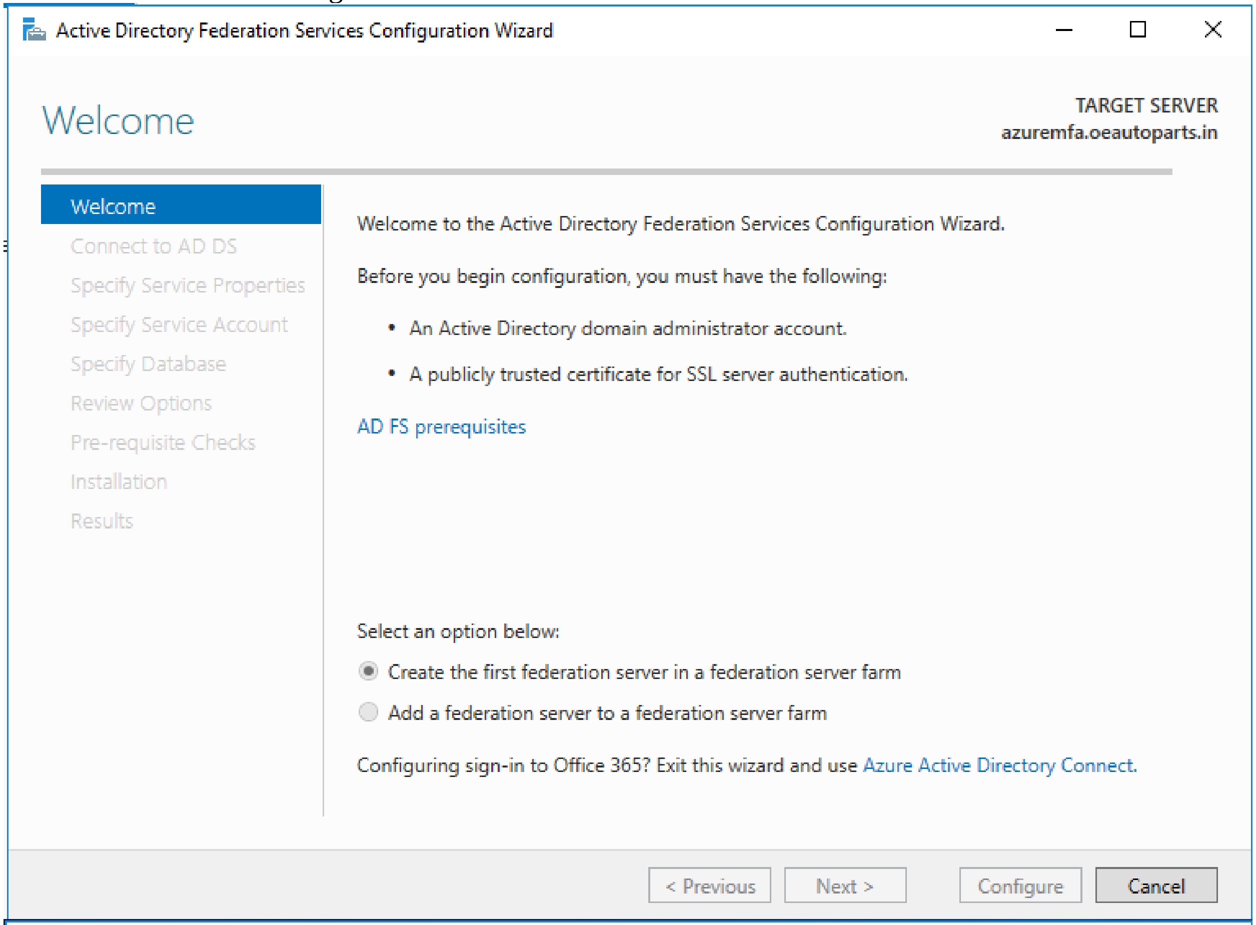
TARGET SERVER
azuremfa

Specify DNS delegation options

□ Create DNS delegation

More about DNS delegation

6. ADFS server Configuration



Active Directory Federation Services Configuration Wizard

Welcome

TARGET SERVER
azuremfa.oeautoparts.in

Welcome to the Active Directory Federation Services Configuration Wizard.

Before you begin configuration, you must have the following:

- An Active Directory domain administrator account.
- A publicly trusted certificate for SSL server authentication.

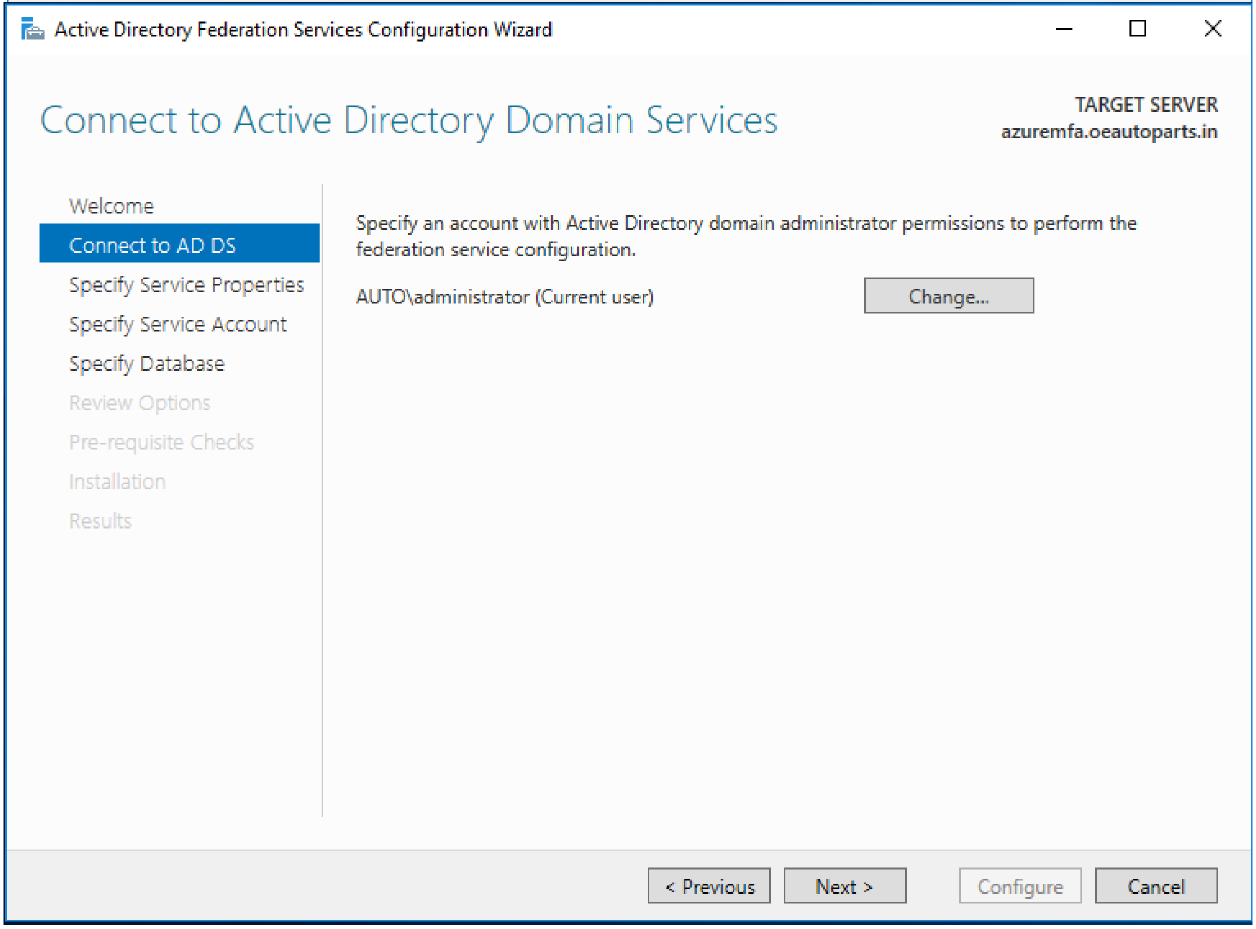
AD FS prerequisites

Select an option below:

● Create the first federation server in a federation server farm

○ Add a federation server to a federation server farm

Configuring sign-in to Office 365? Exit this wizard and use Azure Active Directory Connect.



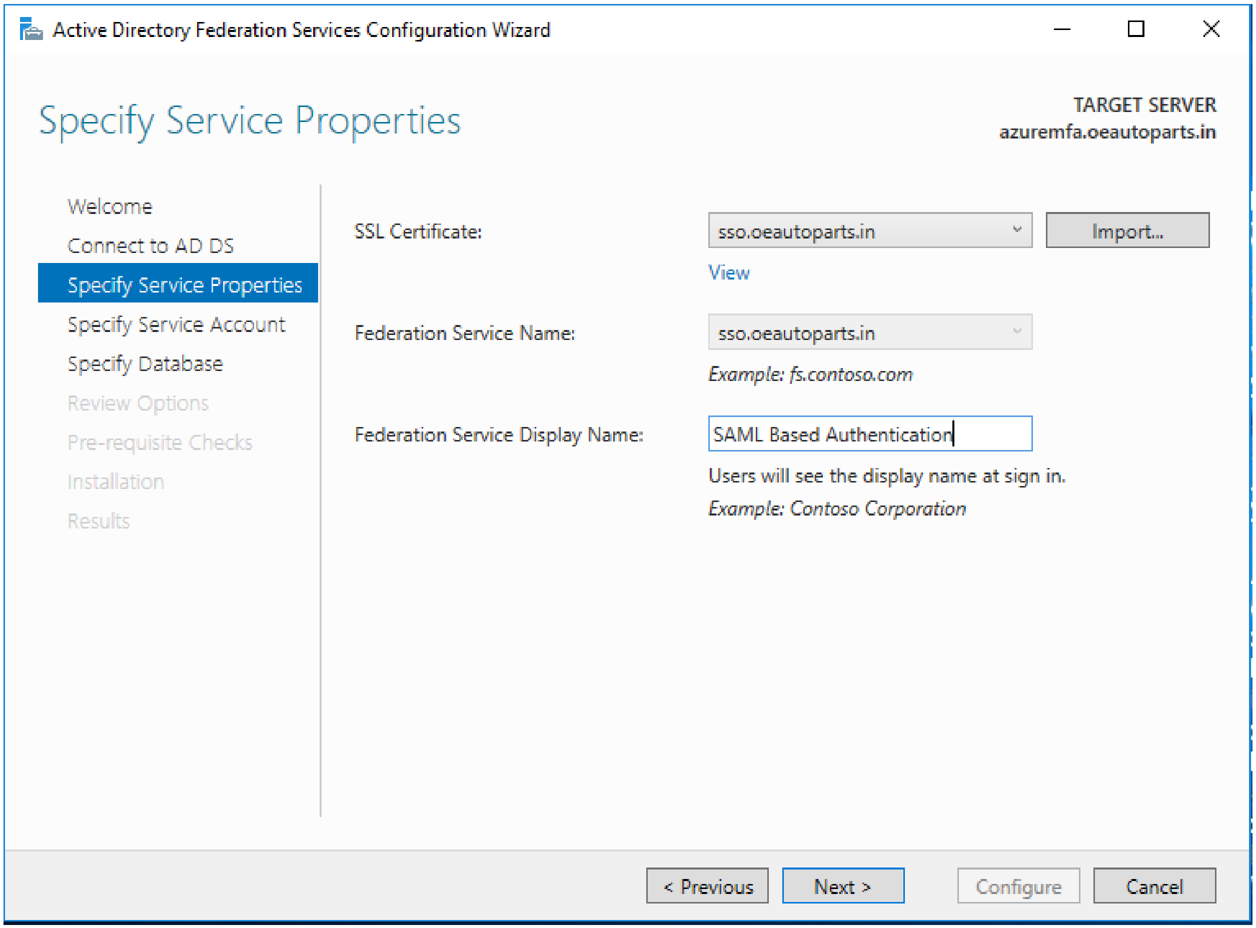
Active Directory Federation Services Configuration Wizard

Connect to Active Directory Domain Services

TARGET SERVER
azuremfa.oeautoparts.in

Specify an account with Active Directory domain administrator permissions to perform the federation service configuration.

AUTO\administrator (Current user)



Specify Service Properties

TARGET SERVER
azuremfa.oeautoparts.in

SSL Certificate: sso.oeautoparts.in

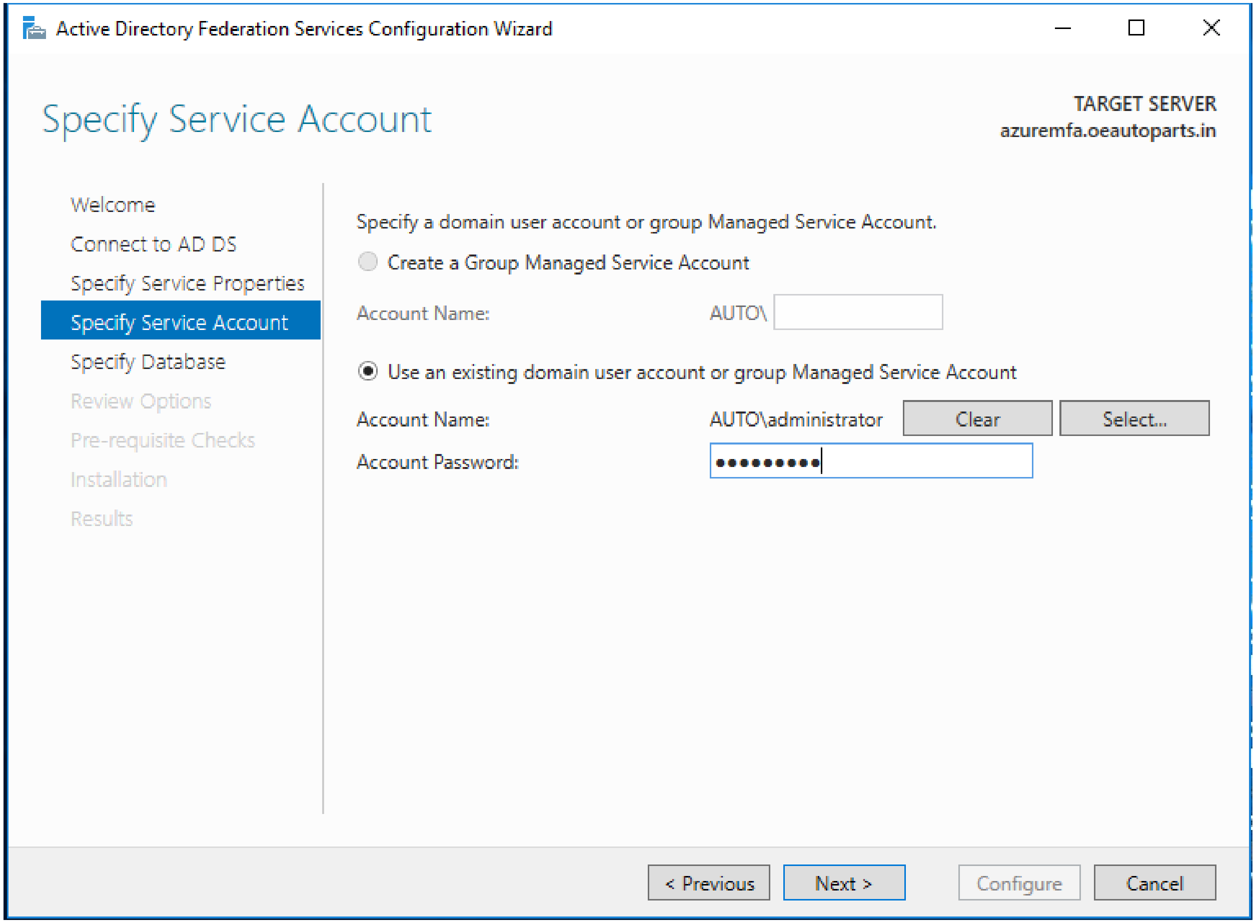
Federation Service Name: sso.oeautoparts.in

Example: fs.contoso.com

Federation Service Display Name: SAML Based Authentication

Users will see the display name at sign in.

Example: Contoso Corporation



Specify Service Account

TARGET SERVER
azuremfa.oeautoparts.in

Specify a domain user account or group Managed Service Account.

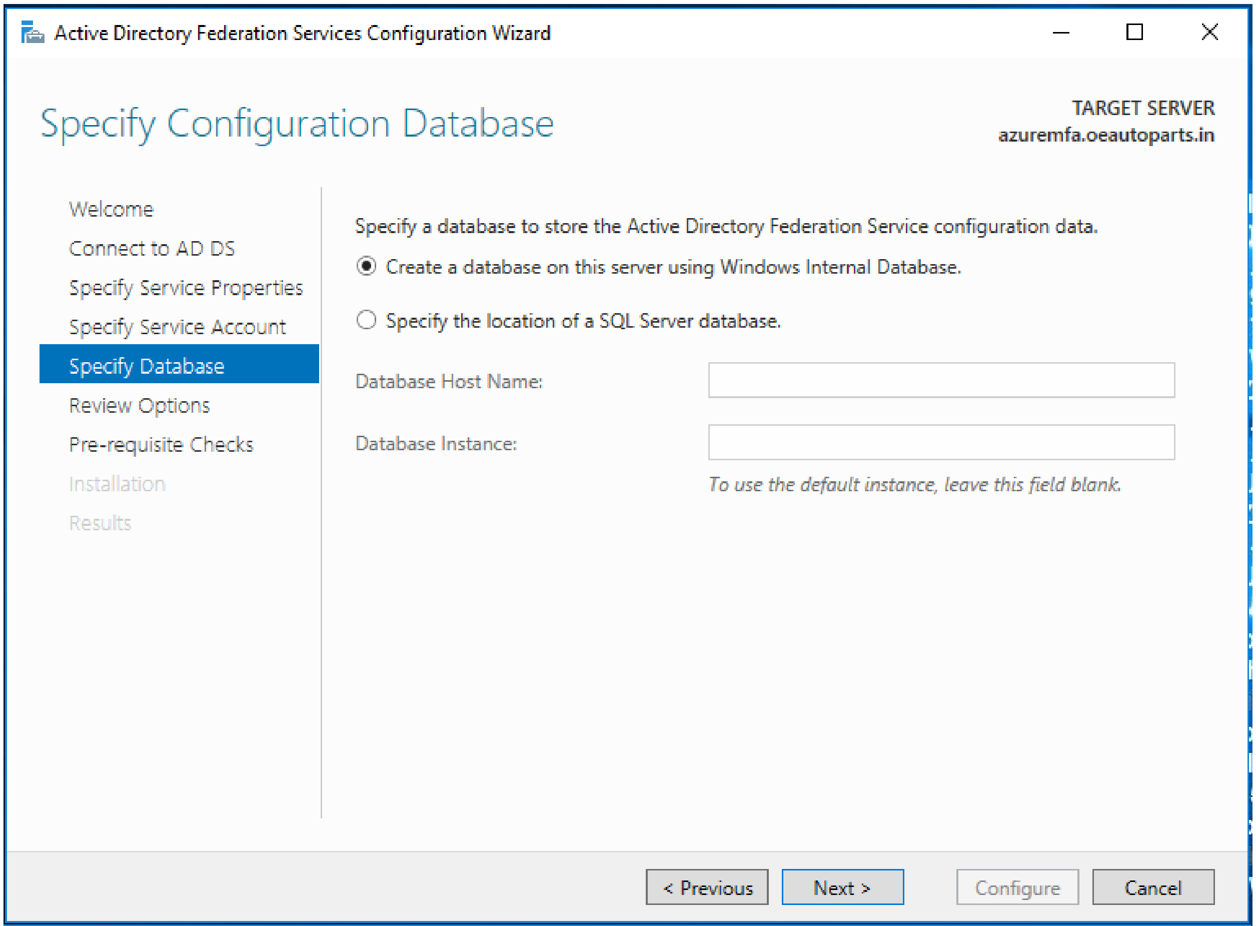
○ Create a Group Managed Service Account

Account Name: AUTO\

● Use an existing domain user account or group Managed Service Account

Account Name: AUTO\administrator

Account Password: ••••••••••



Specify Configuration Database

TARGET SERVER
azuremfa.oeautoparts.in

Specify a database to store the Active Directory Federation Service configuration data.

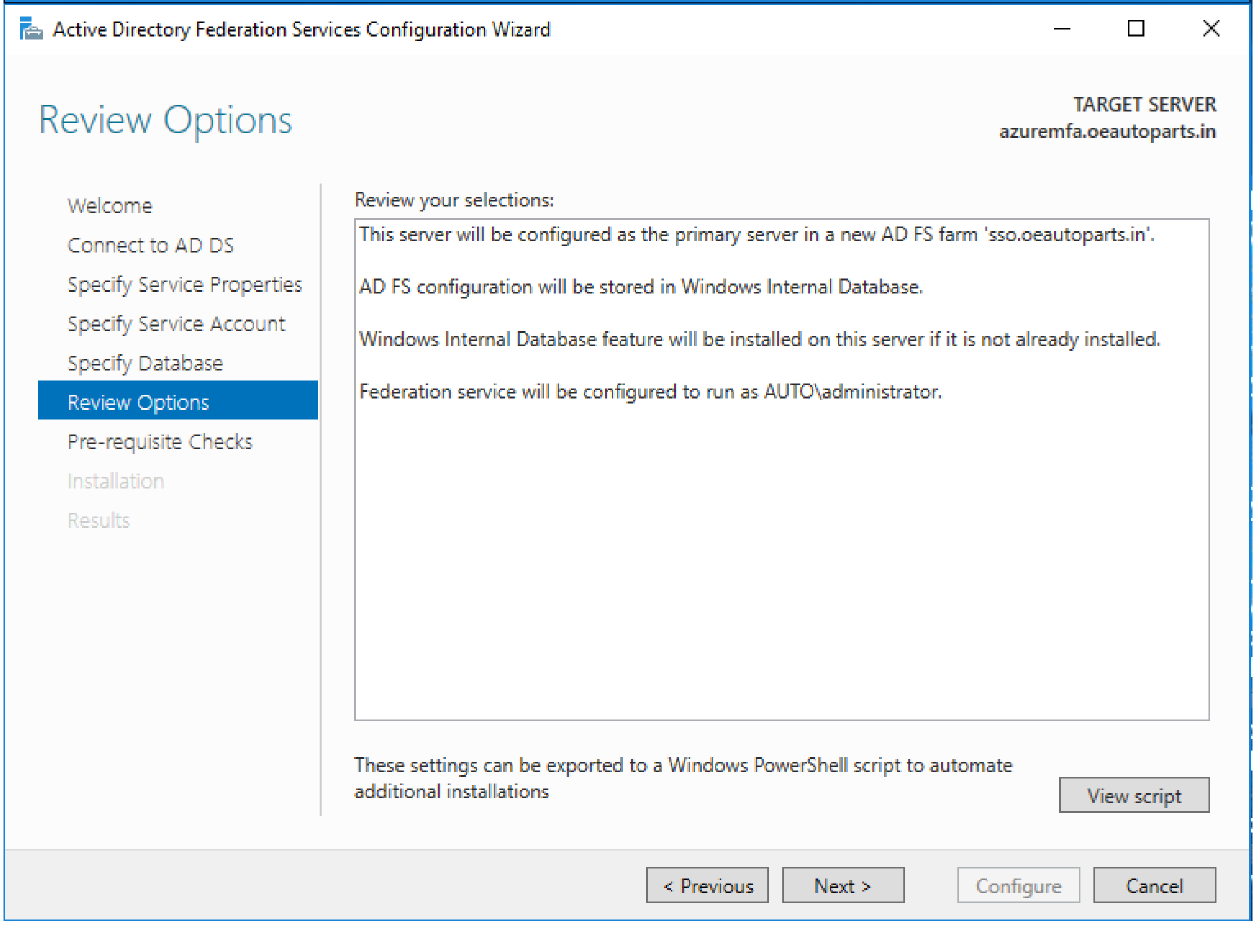
● Create a database on this server using Windows Internal Database.

○ Specify the location of a SQL Server database.

Database Host Name:

Database Instance:

To use the default instance, leave this field blank.



Review Options

TARGET SERVER
azuremfa.oeautoparts.in

Review your selections:

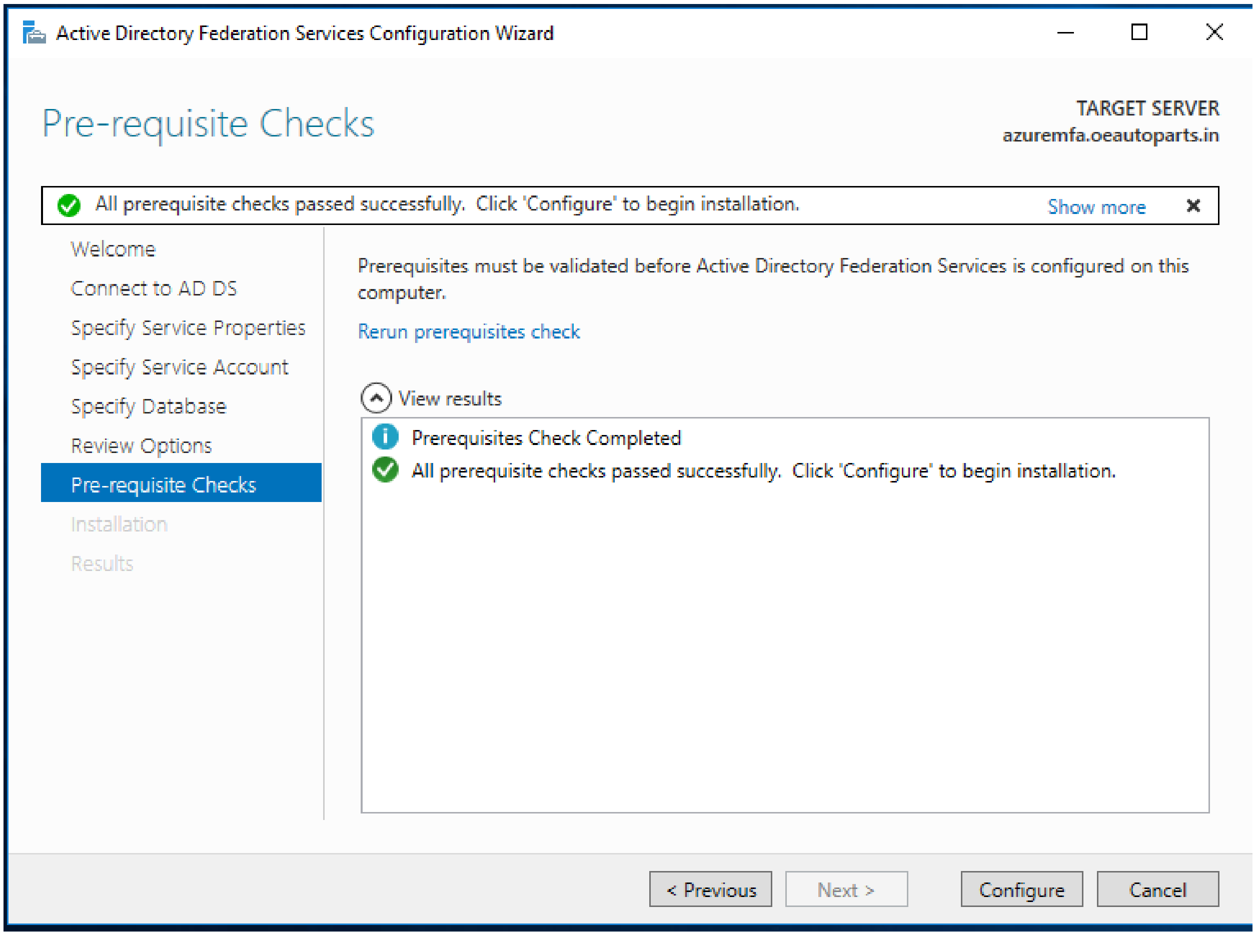
This server will be configured as the primary server in a new AD FS farm 'sso.oeautoparts.in'.

AD FS configuration will be stored in Windows Internal Database.

Windows Internal Database feature will be installed on this server if it is not already installed.

Federation service will be configured to run as AUTO\administrator.

These settings can be exported to a Windows PowerShell script to automate additional installations



Pre-requisite Checks

TARGET SERVER
azuremfa.oeautoparts.in

All prerequisite checks passed successfully. Click 'Configure' to begin installation.

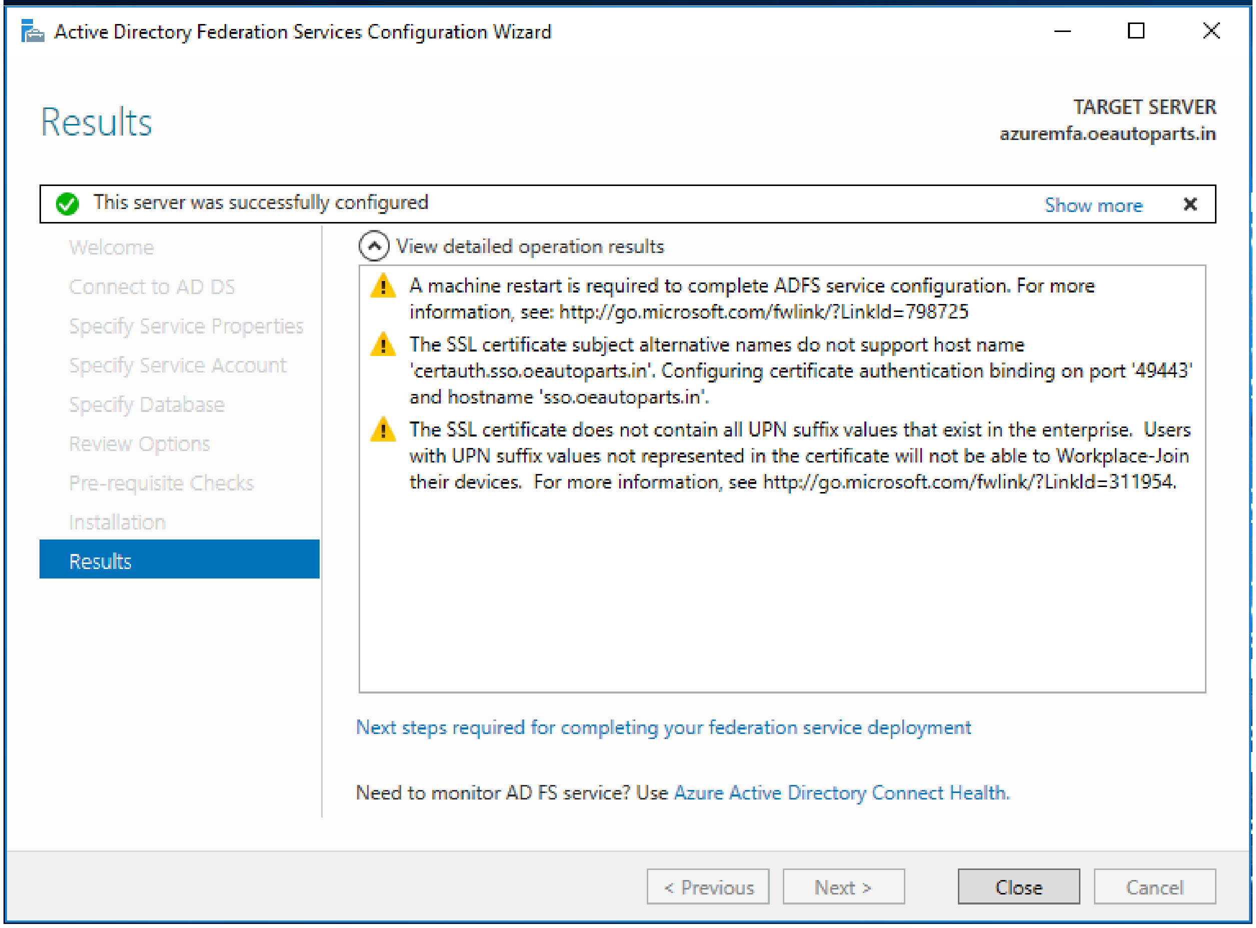
Prerequisites must be validated before Active Directory Federation Services is configured on this computer.

Rerun prerequisites check

View results

Prerequisites Check Completed

All prerequisite checks passed successfully. Click 'Configure' to begin installation.



Results

TARGET SERVER
azuremfa.oeautoparts.in

This server was successfully configured

View detailed operation results

A machine restart is required to complete ADFS service configuration. For more information, see: http://go.microsoft.com/fwlink/?LinkId=798725

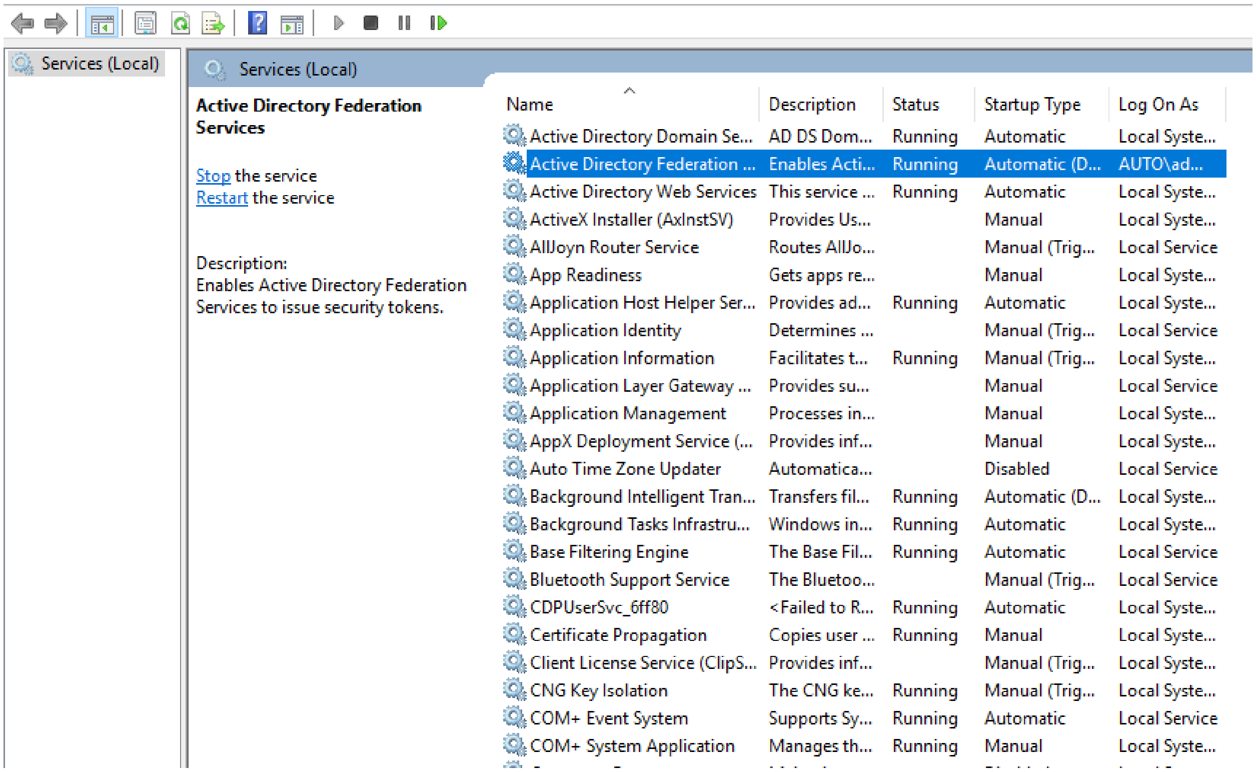
The SSL certificate subject alternative names do not support host name 'certauth.sso.oeautoparts.in'. Configuring certificate authentication binding on port '49443' and hostname 'sso.oeautoparts.in'.

The SSL certificate does not contain all UPN suffix values that exist in the enterprise. Users with UPN suffix values not represented in the certificate will not be able to Workplace-Join their devices. For more information, see http://go.microsoft.com/fwlink/?LinkId=311954.

Next steps required for completing your federation service deployment

Need to monitor AD FS service? Use Azure Active Directory Connect Health.

7. Checking ADFS and ADDS Service status



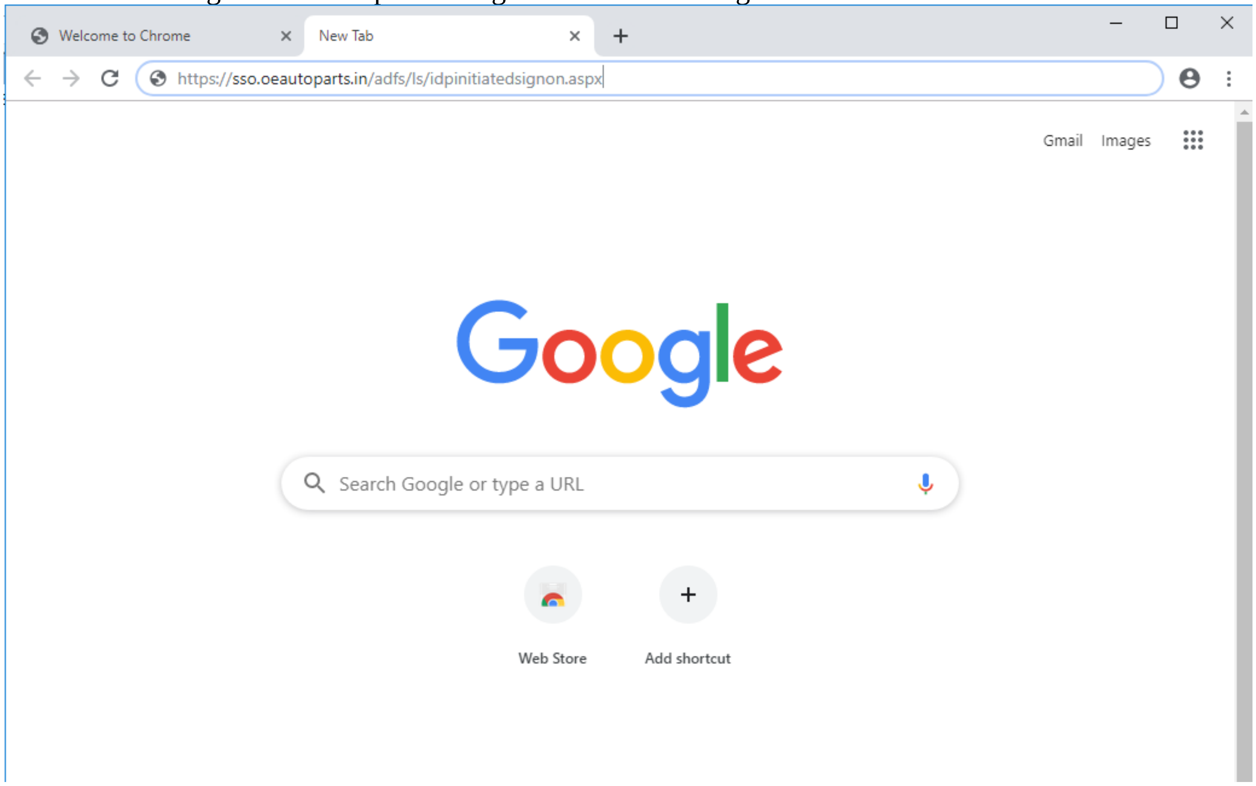
Active Directory Federation Services

Stop the service
Restart the service

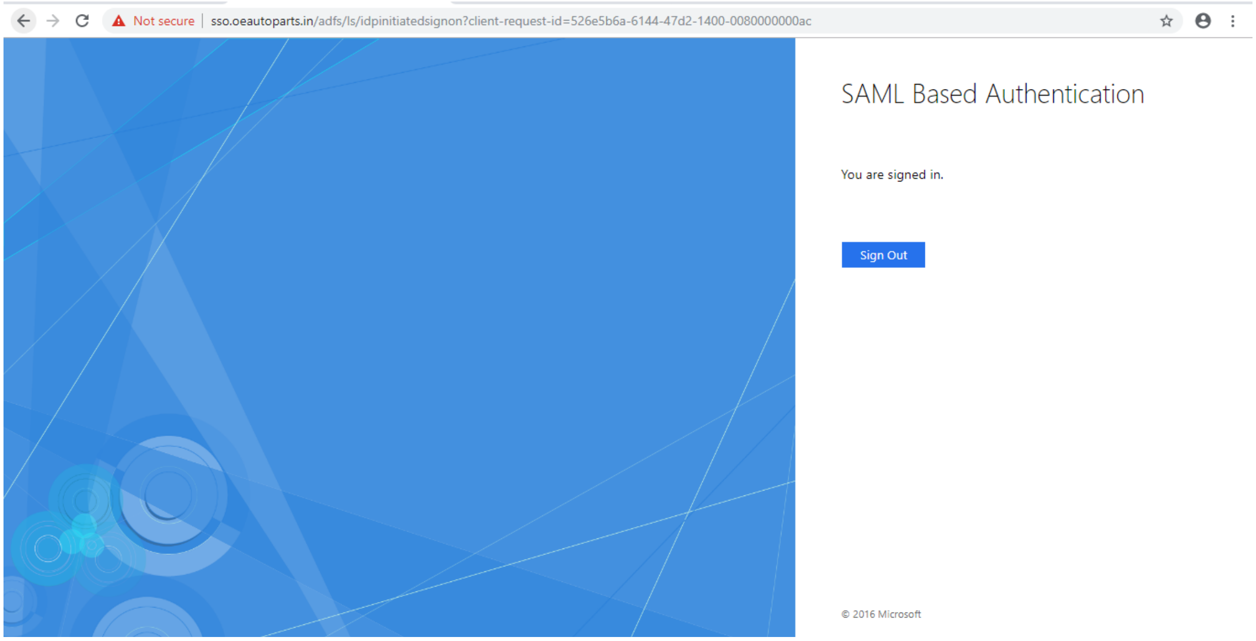
Description:
Enables Active Directory Federation Services to issue security tokens.

Name	Description	Status	Startup Type	Log On As
Active Directory Domain Se...	AD DS Dom...	Running	Automatic	Local Syste...
Active Directory Federation ...	Enables Acti...	Running	Automatic (D...	AUTO\ad...
Active Directory Web Services	This service ...	Running	Automatic	Local Syste...
ActiveX Installer (AxInstSV)	Provides Us...		Manual	Local Syste...
AllJoyn Router Service	Routes AllJo...		Manual (Trig...	Local Service
App Readiness	Gets apps re...		Manual	Local Syste...
Application Host Helper Ser...	Provides ad...	Running	Automatic	Local Syste...
Application Identity	Determines ...		Manual (Trig...	Local Service
Application Information	Facilitates t...	Running	Manual (Trig...	Local Syste...
Application Layer Gateway ...	Provides su...		Manual	Local Service
Application Management	Processes in...		Manual	Local Syste...
AppX Deployment Service (...	Provides inf...		Manual	Local Syste...
Auto Time Zone Updater	Automatica...		Disabled	Local Service
Background Intelligent Tran...	Transfers fil...	Running	Automatic (D...	Local Syste...
Background Tasks Infrastru...	Windows in...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
Bluetooth Support Service	The Bluetoo...		Manual (Trig...	Local Service
CDPUserSvc_6ff80	<Failed to R...	Running	Automatic	Local Syste...
Certificate Propagation	Copies user ...	Running	Manual	Local Syste...
Client License Service (ClipS...	Provides inf...		Manual (Trig...	Local Syste...
CNG Key Isolation	The CNG ke...	Running	Manual (Trig...	Local Syste...
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
COM+ System Application	Manages th...	Running	Manual	Local Syste...

8. Accessing the SSO for performing authentication using SAML token



https://sso.oeautoparts.in/adfs/ls/idpinitiatedsignon.aspx



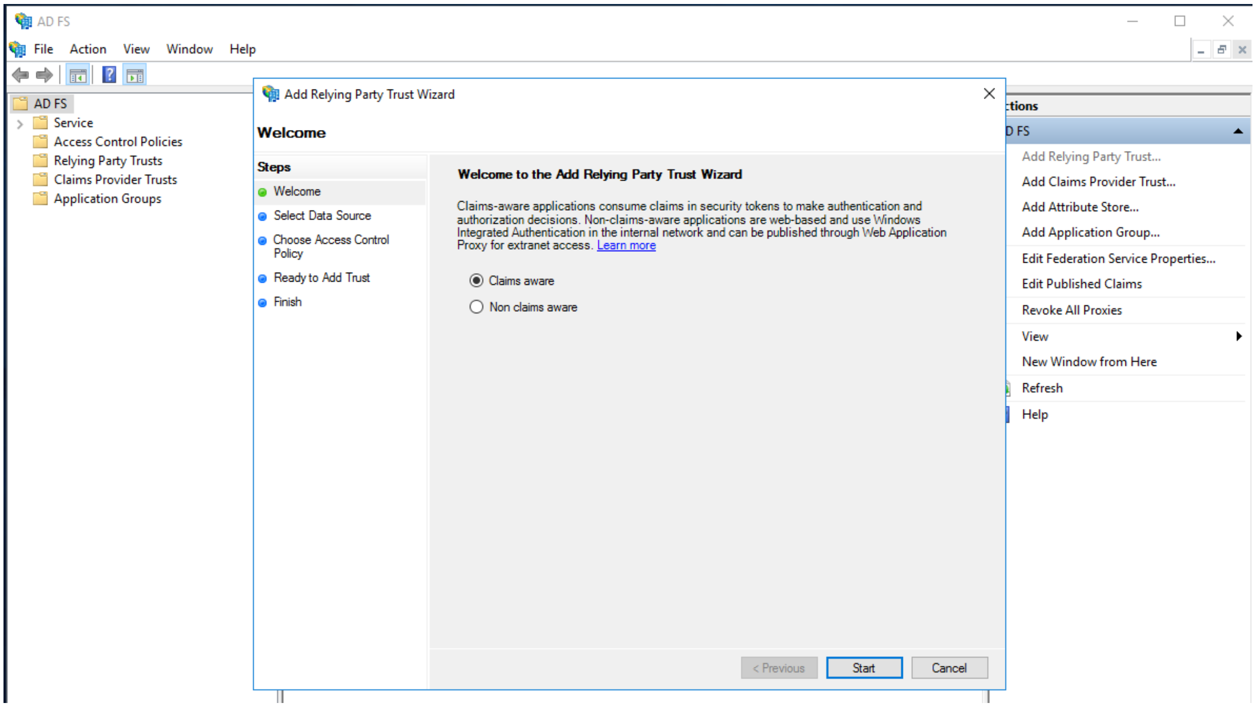
Not secure
sso.oeautoparts.in/adfs/ls/idpinitiatedsignon?client-request-id=526e5b6a-6144-47d2-1400-0080000000ac

SAML Based Authentication

You are signed in.

© 2016 Microsoft

9. Application Integration with AD FS Management console

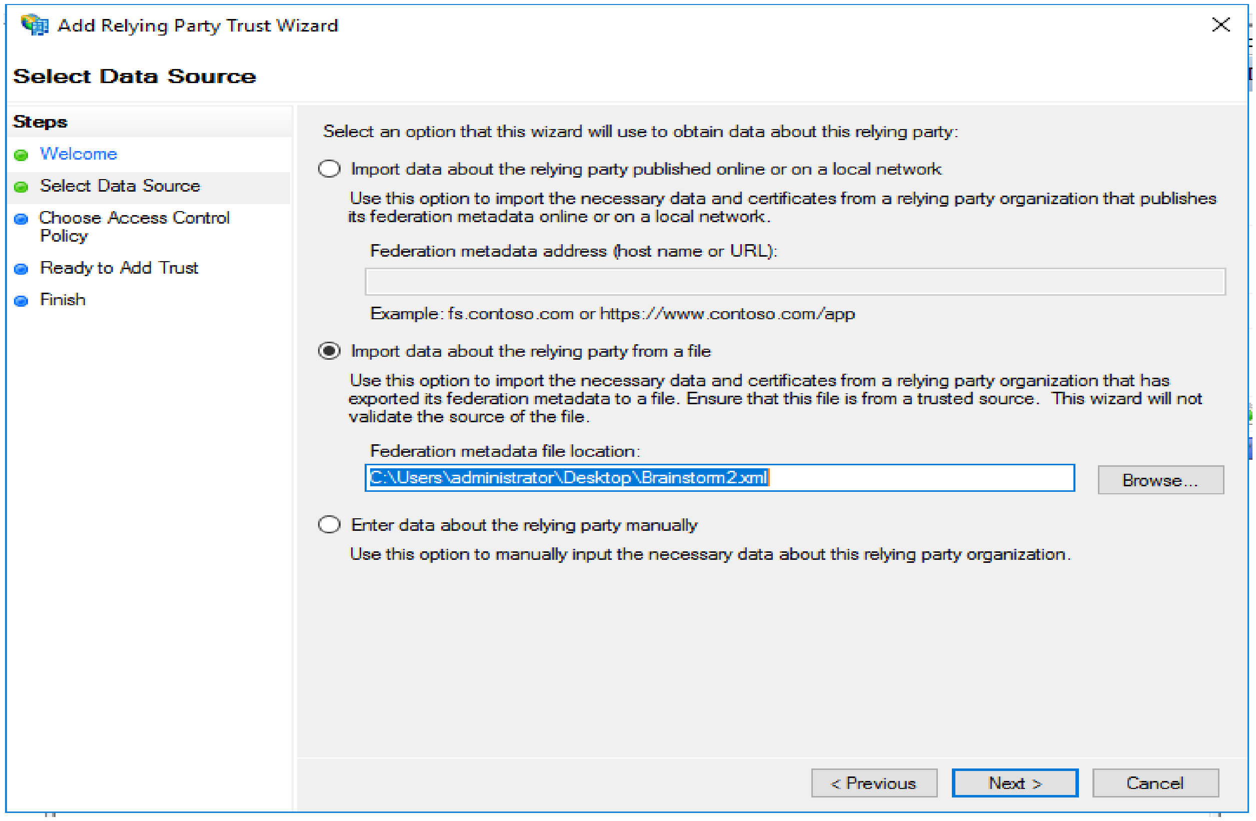


Welcome to the Add Relying Party Trust Wizard

Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. Learn more

● Claims aware

○ Non claims aware



Select Data Source

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

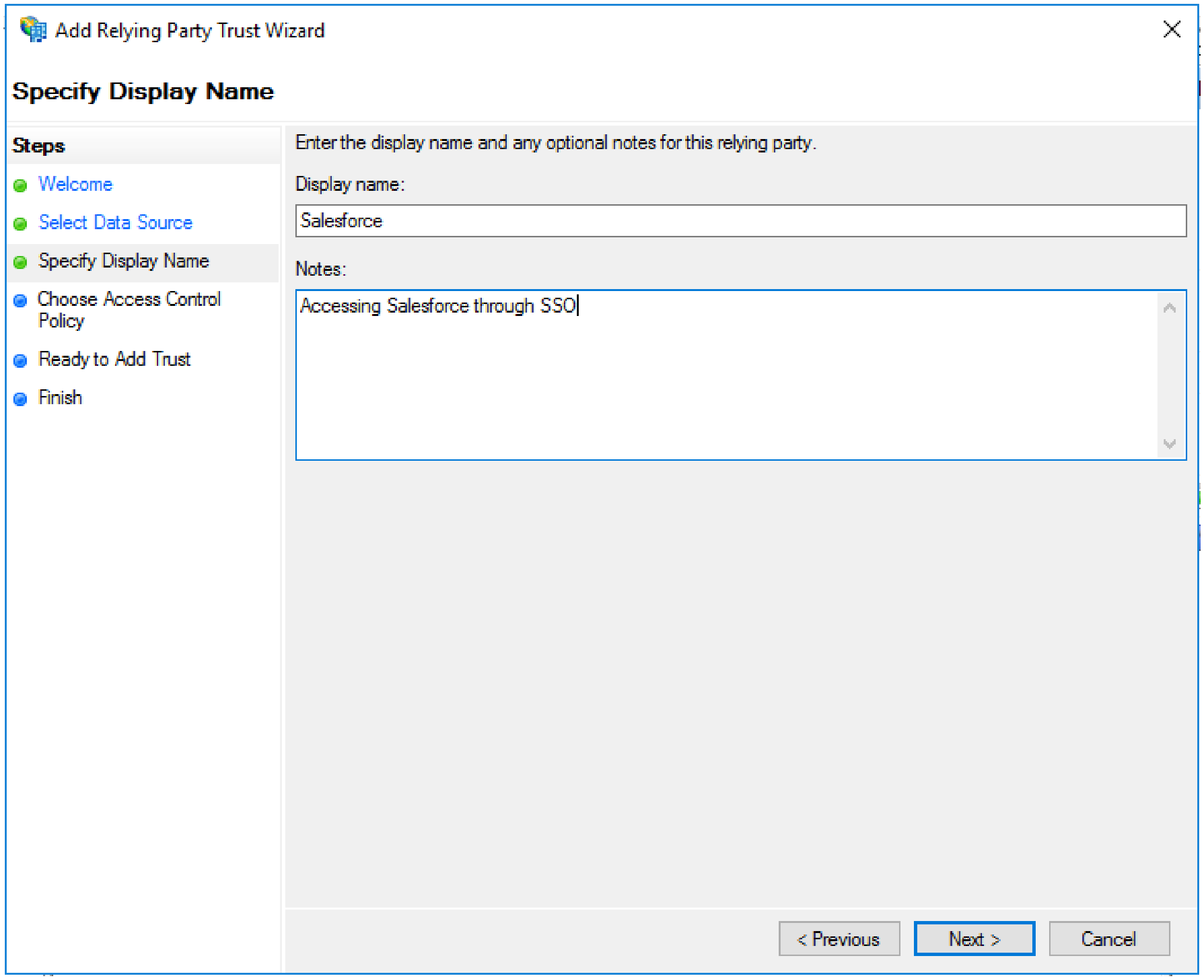
● Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location: C:\Users\administrator\Desktop\Brainstorm2.xml

○ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

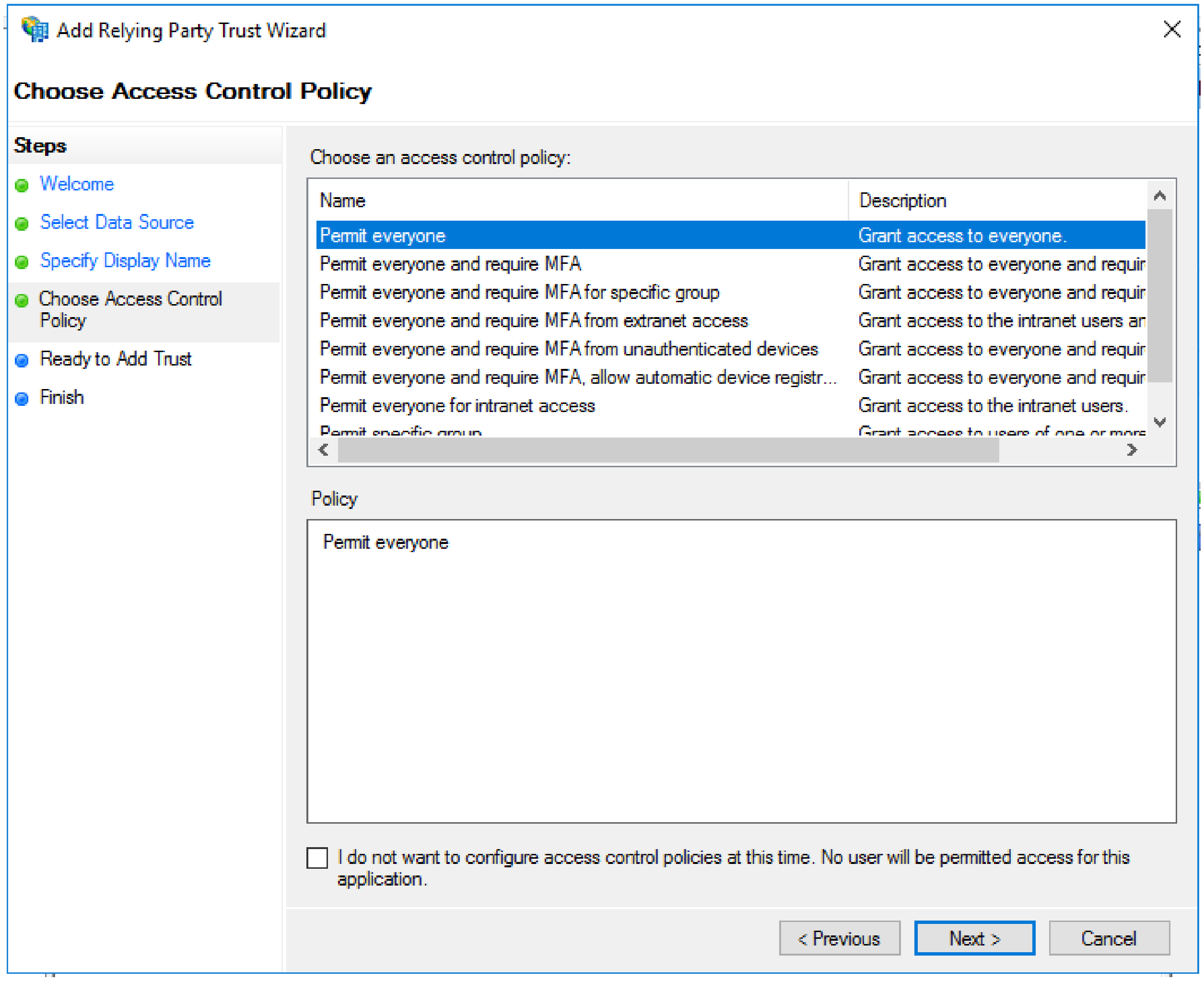


Specify Display Name

Enter the display name and any optional notes for this relying party.

Display name: Salesforce

Notes: Accessing Salesforce through SSO



Add Relying Party Trust Wizard

Choose Access Control Policy

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Access Control Policy
- Ready to Add Trust
- Finish

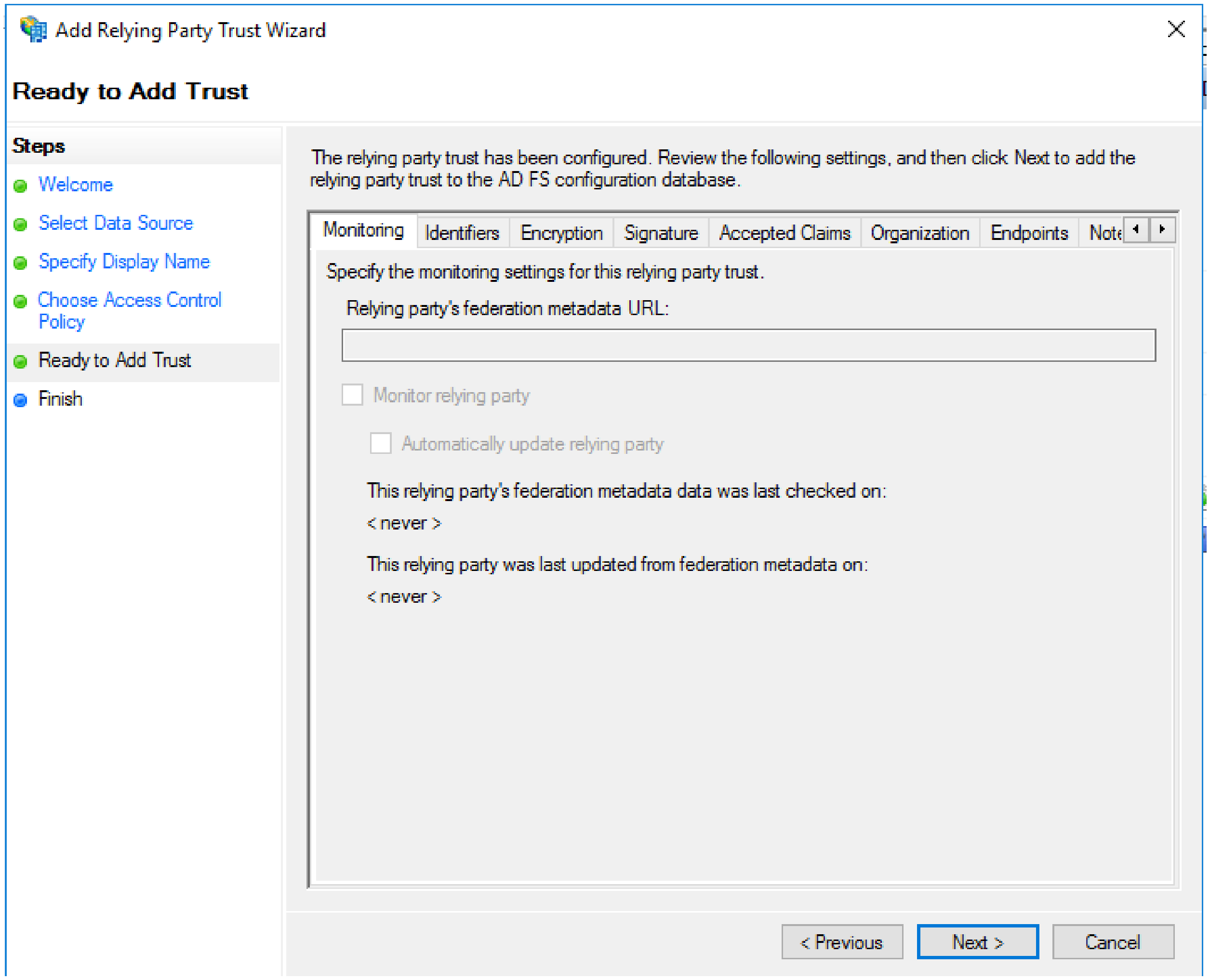
Choose an access control policy:

Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and requir
Permit everyone and require MFA for specific group	Grant access to everyone and requir
Permit everyone and require MFA from extranet access	Grant access to the intranet users ar
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and requir
Permit everyone and require MFA, allow automatic device registr...	Grant access to everyone and requir
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more

Policy

Permit everyone

□ I do not want to configure access control policies at this time. No user will be permitted access for this application.



Add Relying Party Trust Wizard

Ready to Add Trust

The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

□ Monitor relying party

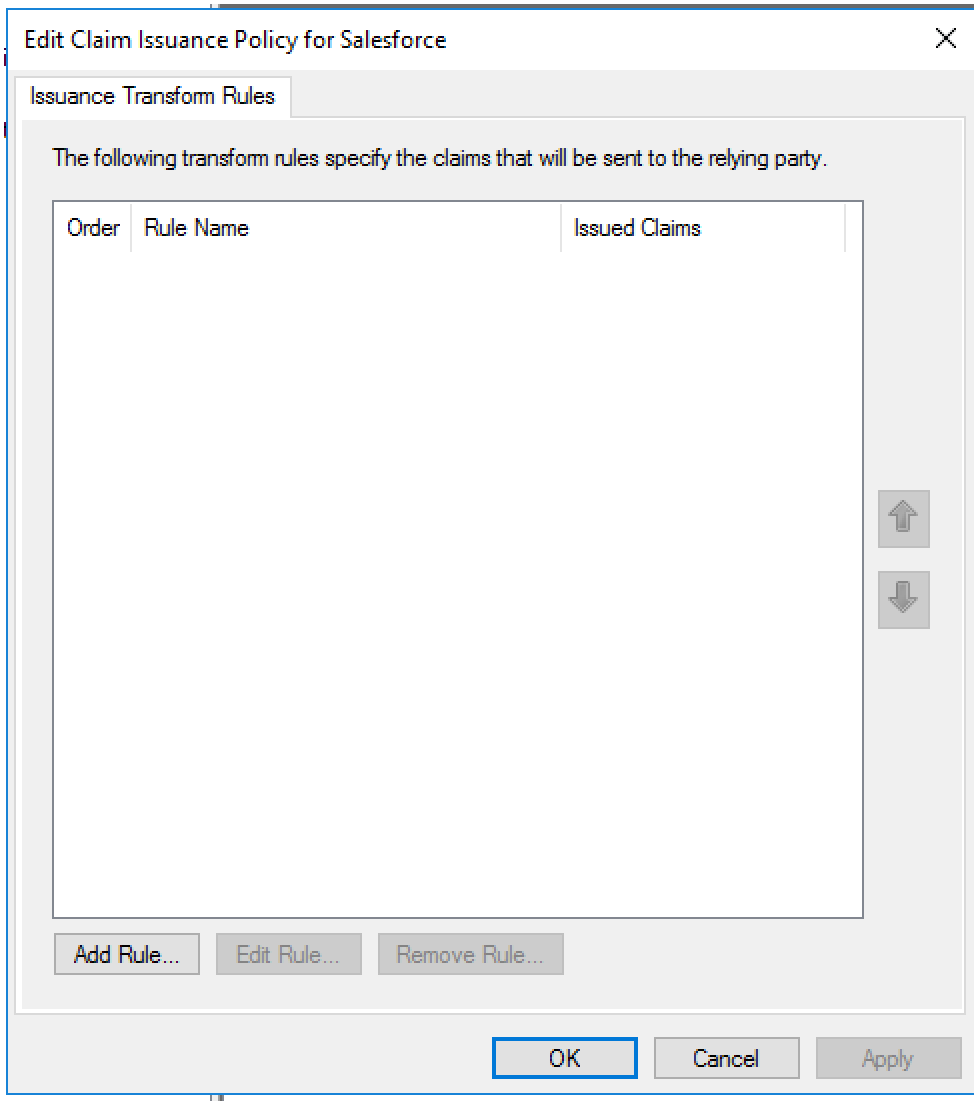
□ Automatically update relying party

This relying party's federation metadata data was last checked on:

< never >

This relying party was last updated from federation metadata on:

< never >

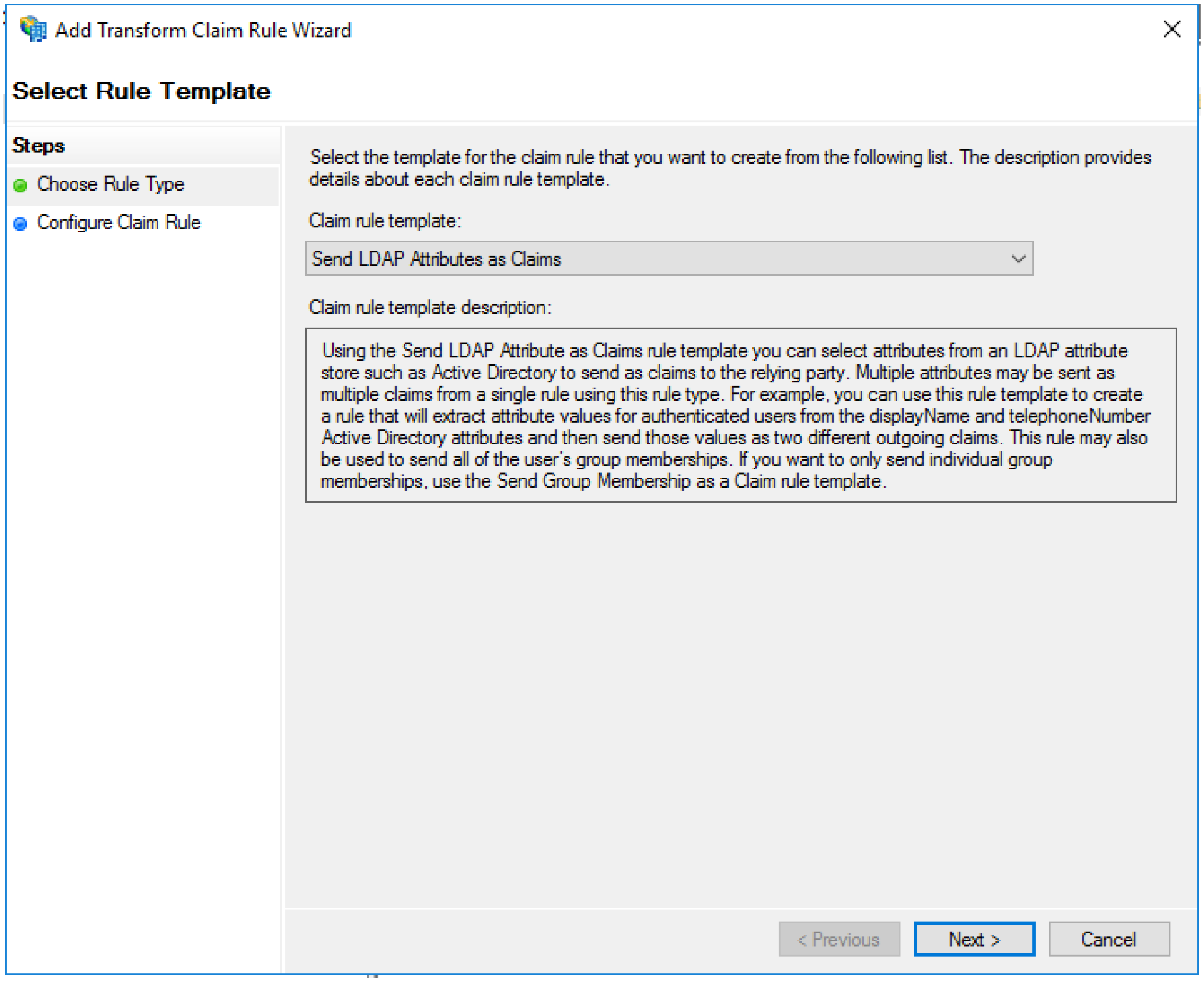


Edit Claim Issuance Policy for Salesforce

Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims



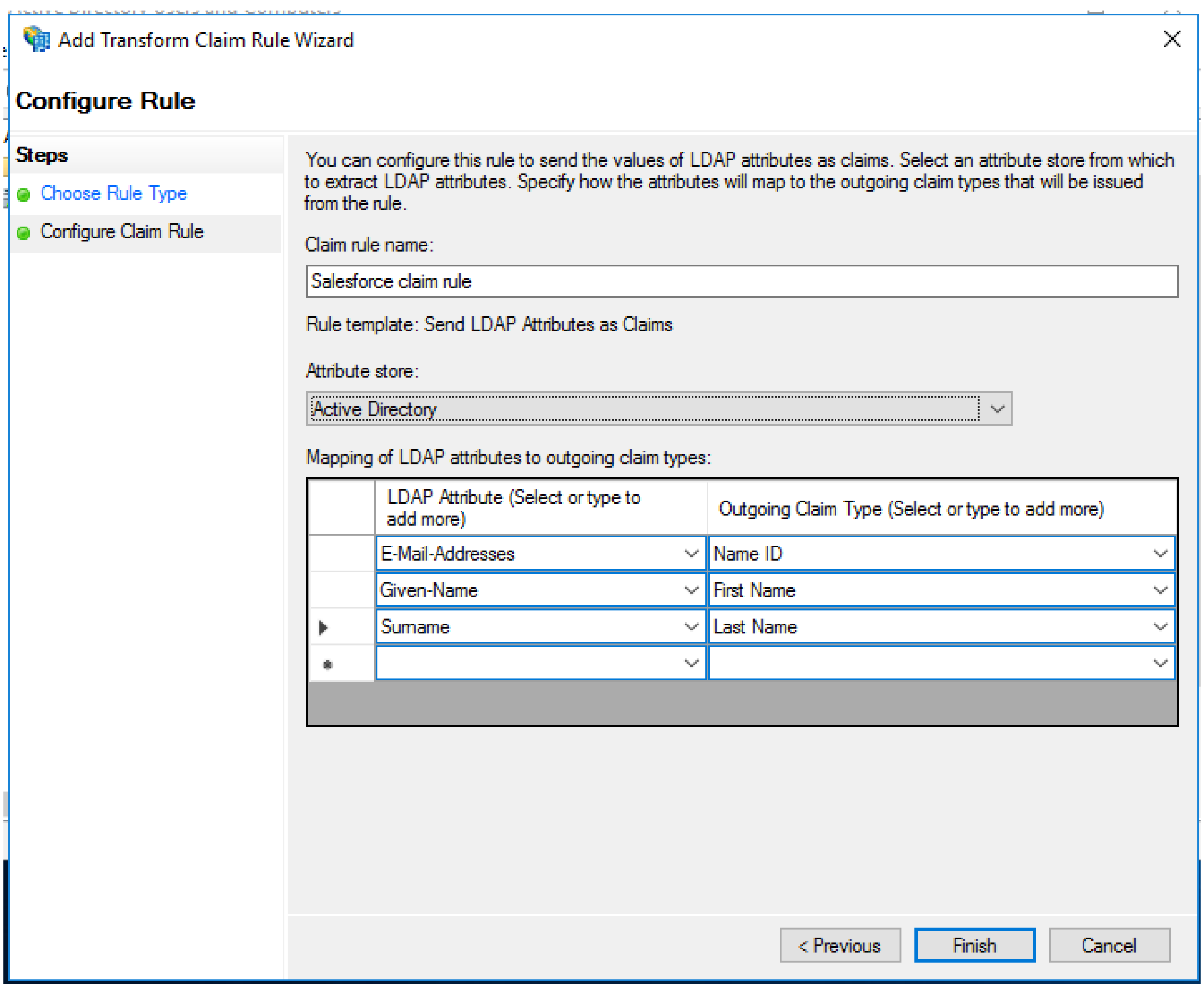
Select Rule Template

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.



Configure Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Salesforce claim rule

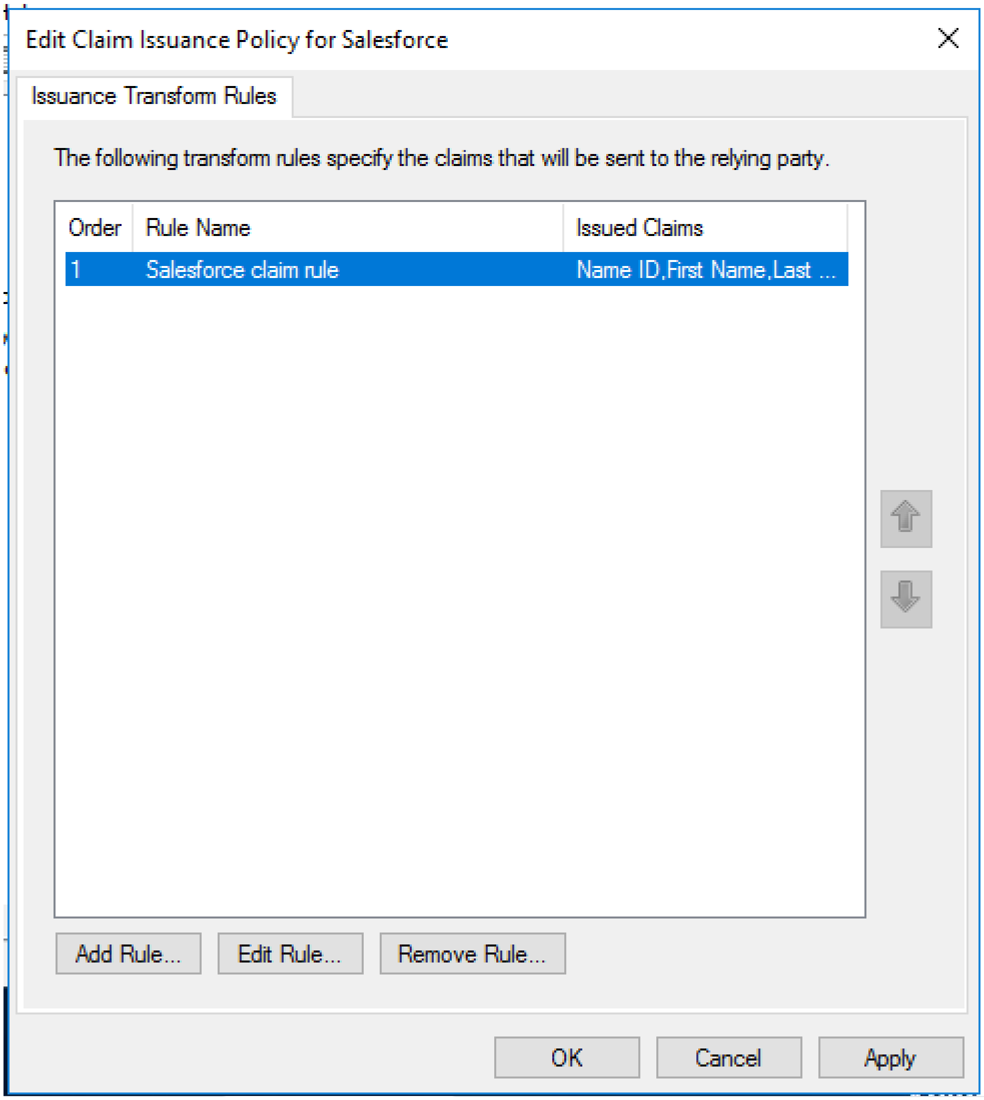
Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	E-Mail-Addresses	Name ID
	Given-Name	First Name
▶	Surname	Last Name
*		

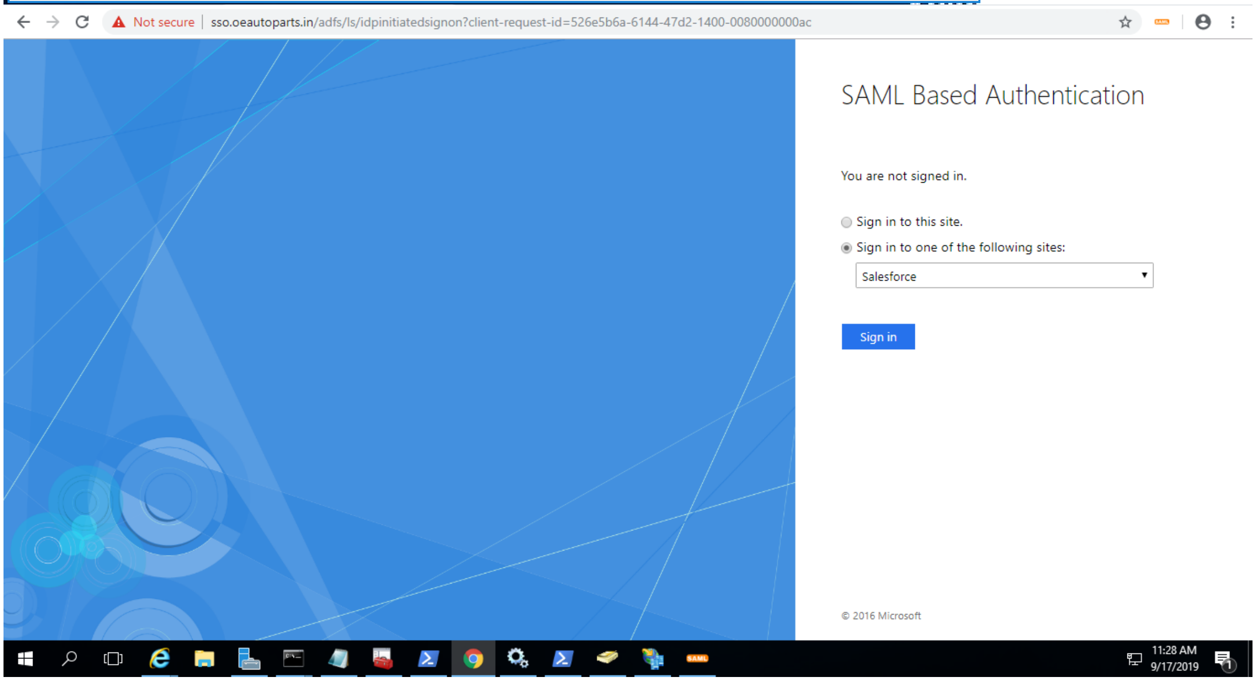


Edit Claim Issuance Policy for Salesforce

Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Salesforce claim rule	Name ID,First Name,Last ...



Not secure | sso.oeautoparts.in/adfs/ls/idpinitiatedsignon?client-request-id=526e5b6a-6144-47d2-1400-0080000000ac

SAML Based Authentication

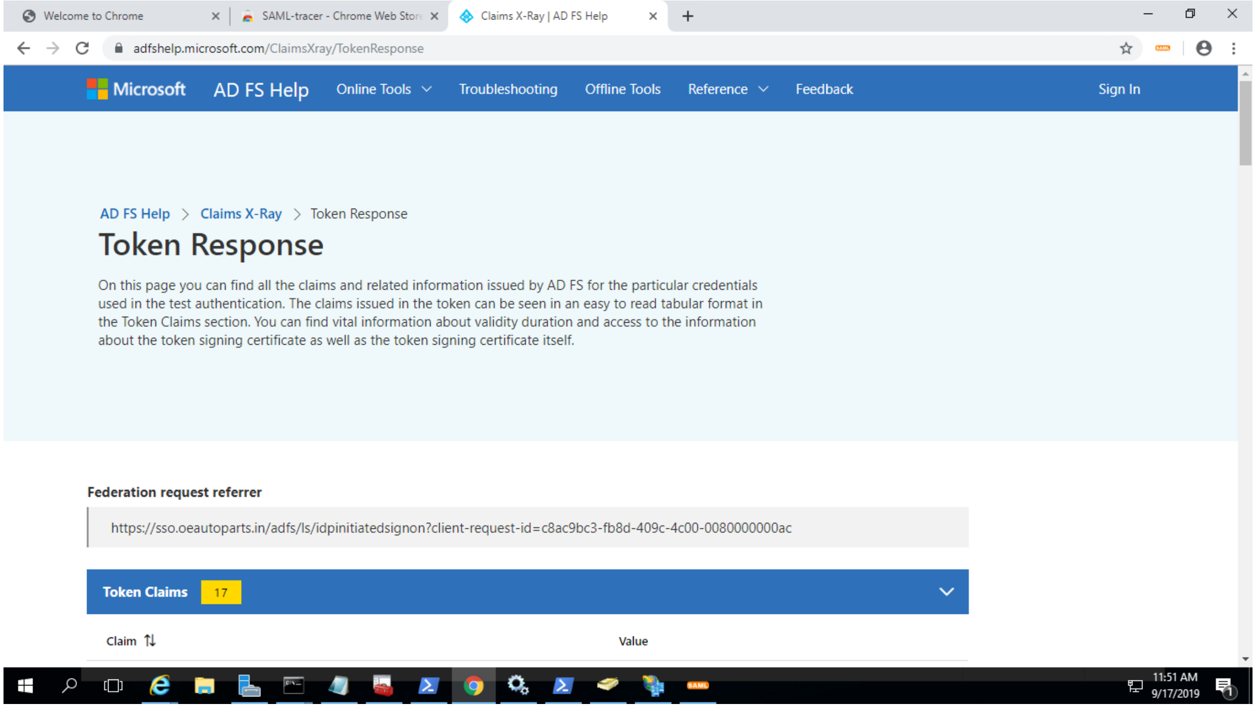
You are not signed in.

○ Sign in to this site.

● Sign in to one of the following sites:

Salesforce

10. Accessing Claim X-Ray application integrated with SSO page



AD FS Help > Claims X-Ray > Token Response

Token Response

On this page you can find all the claims and related information issued by AD FS for the particular credentials used in the test authentication. The claims issued in the token can be seen in an easy to read tabular format in the Token Claims section. You can find vital information about validity duration and access to the information about the token signing certificate as well as the token signing certificate itself.

Federation request referrer

https://sso.oeautoparts.in/adfs/ls/idpinitiatedsignon?client-request-id=c8ac9bc3-fb8d-409c-4c00-0080000000ac

Token Claims 17

Claim	Value

CONCLUSION

In this project RealTime Authentication via LDAP Servers shows. It provides the facility of Single Sign On (SSO) with LDAP Authentication. LDAP is a protocol that works on Directory Servers it can be Enterprise Directory or Active Directory.

For this we added some roles to the Domain controller. For any user when login attempt for any application, it depends for which application or portal user wants to login or what policies and processes defined for the same. As per the process Authentication will be via LDAP only but the processes of Journey may be vary accordingly.

To access a network's LDAP services, your computer must first log in to a server that supports the protocol, a process called authentication. LDAP lets a network administrator assign different levels of access to its many users, keeping the information secure.

LDAP is a protocol that supports directory servers like servers used for Active directory or enterprise directory. Authentication validation of user credential also be done by IDP via LDAP only. Required claims also provided by IDP from LDAP as per the request.

We have taken different bindings also to done this authentication process successfully. Binding are the mechanisms to transfer the messages.

Service communication certificate is a certificate which is approved by trusted third party. This is used to bind the certificate with resource login page. This certificate is required to make it secure over the internet so that trust can be established between both parties.

Token Sing in Certificate is the hash of the SAML token by sender’s private key (IDP).

The certificate which is encrypted by the receiver’s public key to achieve confidentiality.

After all Installation and Configuration, Certificate imported or exported, We will sign in via URL and user will be authenticated in that application. One time when user login then session created and for the next time user will automatically signed in.

Hence user successfully logged in in Real Time via LDAP Authentication.

REFERENCES

- https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/overview/whats-new-active-directory-federation-services-windows-server
- https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff359101(v=pandp.10)
- https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff641697(v=ws.10)
- https://www.tatvasoft.co.uk/blog/adfs-configuration-in-windows-server-2012-r2-standard-with-sharepoint-2013/
- https://blogs.technet.microsoft.com/askpfeplat/2014/11/02/adfs-deep-dive-comparing-ws-fed-saml-and-oauth/