INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 6.078
(Volume 6, Issue 3)
Available online at: www.ijariit.com

Achieving Single Sign-On (SSO) using federated repositories

Mallikarjuna Akkinapalli
mallik4ureddy@yahoo.com

ABSTRACT

Application Server Agent (ASA) & Trust Association Interceptors (TAI) setup for Single Sign-On. ASA and TAI are critical parts when implementing Single Sign On in a multiple federated Light Weight Directory Protocol's environment. There needs to be a presence of web agents on the web servers to intercept the web requests and an ASA agent on the Application Servers to intercept the Application Server's requests. Then you enable TAI on your Application Servers to intercept the requests and perform Single Sign On. We need to understand the request flow to achieve a successful Single Sign On authentication. The key to achieve SSO is to intercept the user requests and update the HTTP headers with LTPA or other authentication tokens from Application1 to successfully authenticate onto Application2. Single Sign On between any two or multiple systems can be achieved in a Federated repository configuration.

Keywords— *Single Sign-On, Federated Repositories, LDAP*

1. INTRODUCTION

This paper talks about how to setup Single Sign On be-tween multiple applications using federated repository configuration. Imagine the users in Application1 are in LDAP1 and the user base for Application2 are in LDAP2. The key to a successful single sign on authentication is to federate the LDAP servers onto a single platform. Many types of LDAP servers exist in the market offered by multiple companies like MS Active Directory [2] or any Custom Directory servers. For Application Server exam-ple we will consider WebSphere Application Server [1] for federation and authentication.

2. PREREQUISITES

2.1 Web Agent setup

Download the WebAgent binaries from the vendor provided and unzip onto target web servers. And follow through the installation steps in GUI or silent mode and finish the setup. Once the Web Agent installation is per-formed on target Apache servers make sure you source the environment variables before proceeding. Perform the post configuration steps if any listed by the vendors. Most post configuration steps involve in directory or file permissions and updating the configuration files.

2.2 Application Server Agent Setup

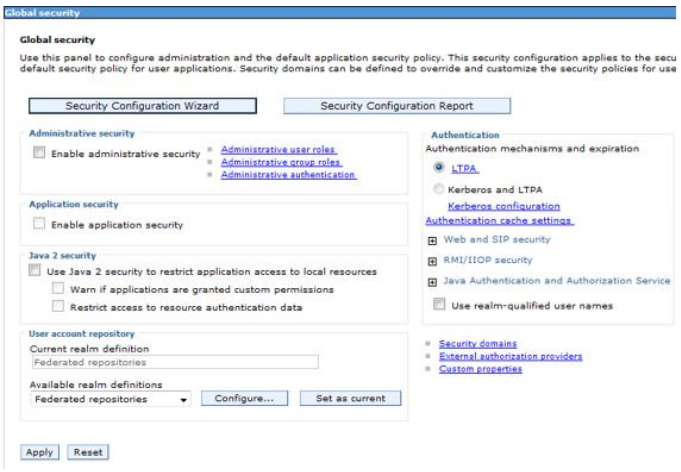
Similar to Webagent the ASA agent binaries which are provided by the vendor needs to be installed on the tar-get Application Servers. This installation needs to be performed on every application server which are part of the cluster. Perform any post installation steps defined in the vendor documentation. Source the environment variables before proceeding further.

3. LDAP CONFIGURATION

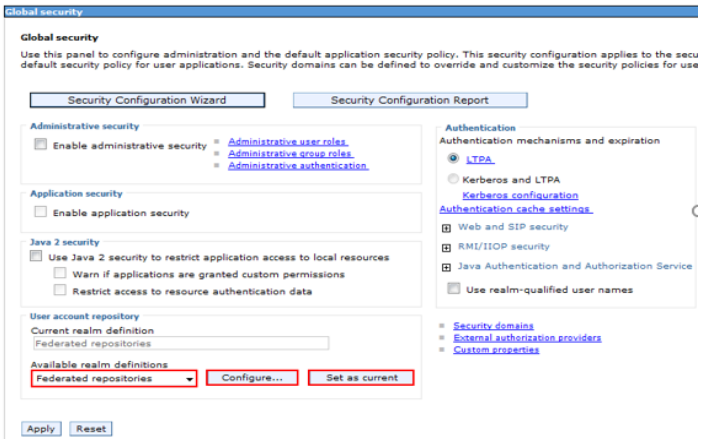
Considering WebSphere Application Server [1] Deployment Manager as an example in the screenshots lets proceed in setting up federated repositories and binding the LDAP servers which is the critical step in achieving Single Sign On.

3.1 AD-LDAP Configuration

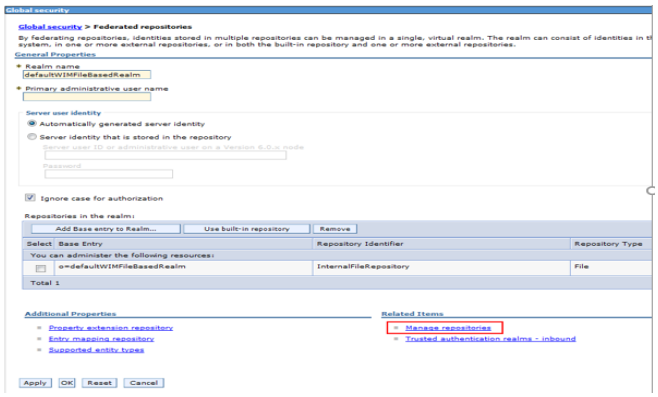
Select 'global security'



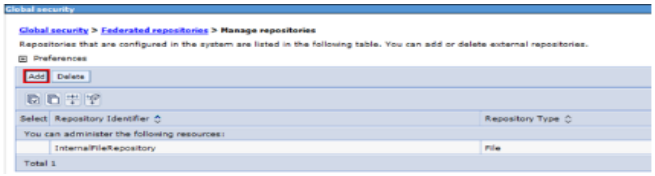
Select the "Federated repositories" from the Available realm definitions. Click on "Set as current" and click on "Configure" to start the configuration.



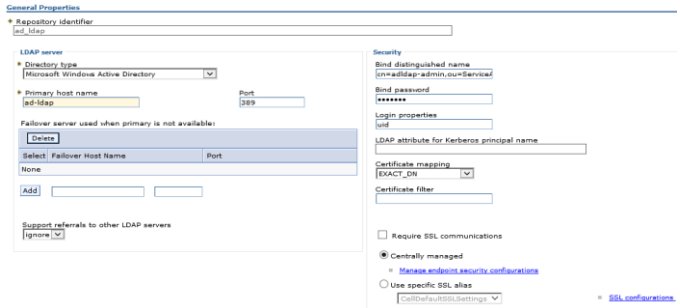
Click on “Manage repositories”



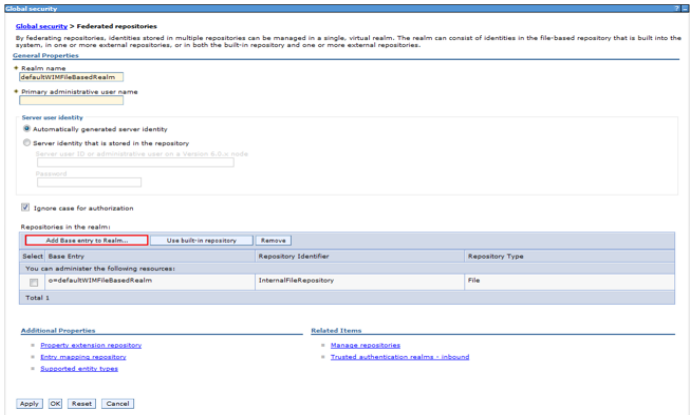
Select ‘Add’



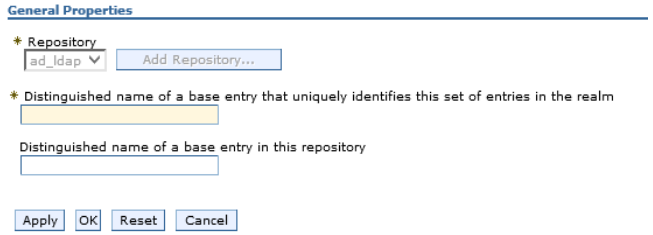
Supply the below values and click “Apply”



Select “Add Base entry to Realm”. We are adding the ad_ldap repository to the Realm which we setup in the previous screen.



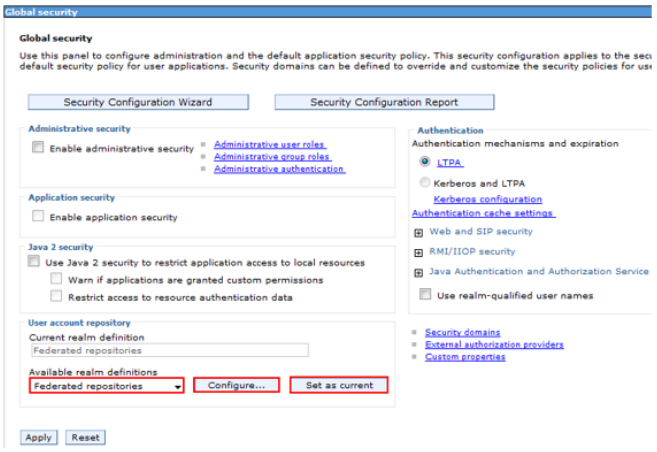
Select the “ad_ldap” from the Repository list and pro-vide the below two Distinguished names and click “Ap-ply” and save.



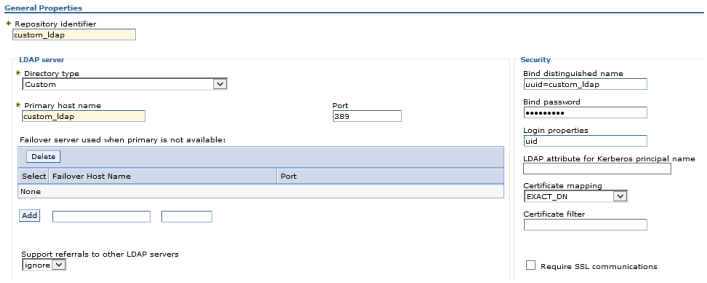
The ad-ldap has been added as shows in the above screenshot. Click “OK” and save

3.2 Custom LDAP Configuration

Perform the steps to configure custom LDAP as second LDAP federated repository. Under “Global security” select the “Federated reposito-ries” and click “Set as current” and click on “Configure” to start configuration.



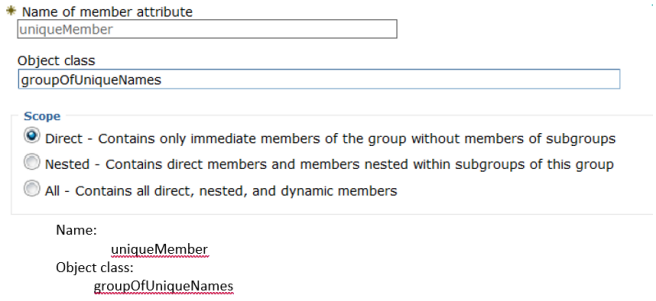
Select “Manage repositories” and New



Provide the corresponding and add base entry to the realm. Configure the entity types as custom.

Group Attributes Setup: Select Global security > Federated repositories > cus-tom_ldap->Group attribute definition

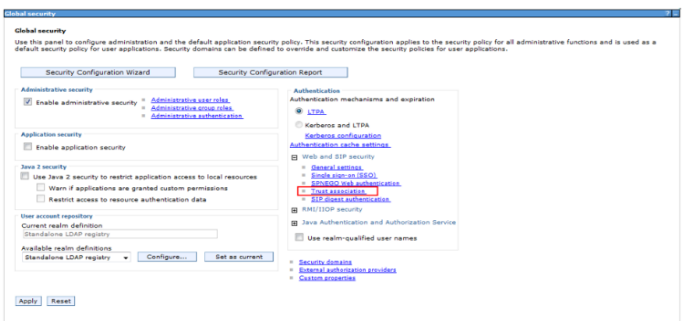
Select Member attributes under Additional Properties, Select New



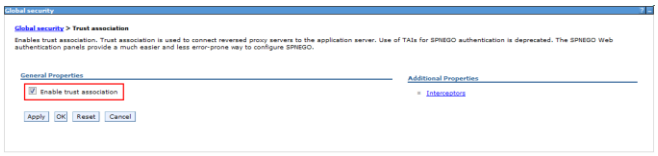
Name:
uniqueMember
Object class:
groupOfUniqueNames

3.3 Trust Associated Interceptor Setup

Follow the below steps for TAI configuration.
Select the “Trust association” under “Web and SIP security”



Select the "Enable trust association" and Apply.

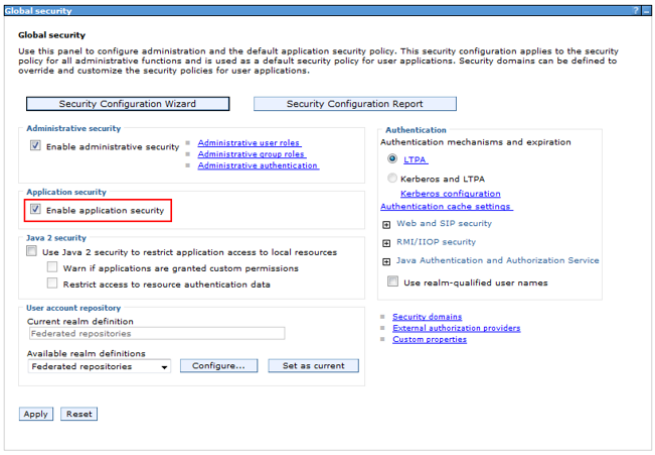


Select Interceptors and add new interceptors pertaining to the vendor product. Then setup Custom JVM properties to provide the home directory for the ASA agent.
Then enable LTPA tokens.

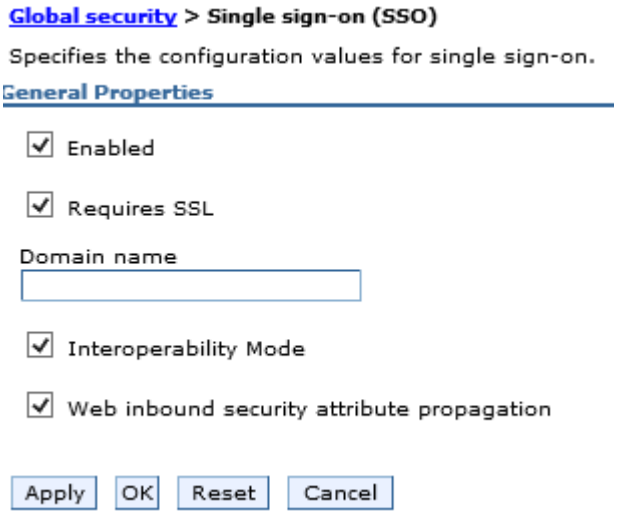
4. SNOOP TESTING

For Snoop testing you need to deploy the default ap-plication WAS provides and enable the security. Snoop test is to test the Single Sign On between your default application and your target application.

Install the Default application and configure so that we can access the snoop using webservers or VIP. Once you validate that the snoop is accessible from VIP, enable the Application Security. Follow the below screenshots to enable the application security. Enable Application Security.



Provide the "Domain name" under Single sign-on and check the "Interoperability Mode" check box.
Save the changes, synchronize the configuration and re-start the JVM's.



5. CONCLUSION

As a conclusion, once multiple LDAP servers are feder-ated, run the snoop testing and real application LDAP testing to establish the single sign on between two dif-ferent applications where the user base is present be-tween two different LDAP servers.

6. REFERENCES

[1] IBM, WebSphere Application Server - https://www.ibm.com/cloud/websphere-application-platform/
[2] MS Active Directory - https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

