

Re: ADAM account store in ADFS

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-07/msg00030

- *From:* Anindya_TCS <AnindyaTCS@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sun, 1 Jul 2007 17:28:00 -0700
-

do you have any step by step guide to configure shadow accounts and groups.

"Joe Kaplan" wrote:

I'm not really sure what a good link would be here. It would help me more if you asked a specific question about configuring a token app.

The most important consideration with a token-based app is how you will generate and manage your resource accounts. ADFS has two options, "shadow accounts" and "shadow groups". Shadow accounts map your federated users to actual user objects in your resource forest. You can map 1:1 or many:1. They are usually the easiest to get working but often times are the most difficult to operate and maintain, especially when you are mapping 1:1 as you need a shadow account for each external user but you don't have a natural way to find out who the external users are in advance, so you must create that.

Shadow groups are more interesting and powerful, but harder to get working initially. With shadow groups, you don't map the external users to specific resource users but instead have a token created for the user that contains group SIDs that map to group claims provided by the external partner.

Joe K.

—
Joe Kaplan—MS MVP Directory Services Programming
Co-author of "The .NET Developer's Guide to Directory Services Programming"
<http://www.directoryprogramming.net>
—

"Anindya_TCS" <AnindyaTCS@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:49C741BC-361E-4D34-A08A-1691EC6D9DB3@xxxxxxxxxxxxxxxxxxxxx

Hello Joe,

Can u please provide some link for configuration of web sso in firewalled environment for windows NT token Based application?

Re: ADAM account store in ADFS

We have followed the ADFS step by step guide for federated web sso but in production we need to configure web sso with winnt token based app.

Could you please provide us a good link ?

"Joe Kaplan" wrote:

FSP = Federation Service Proxy. It is able to authenticate ADAM users because it presents the forms-based login.

If you want the forms-based login page on the FS itself, you can replace the clientlogon.aspx in the /adfs/ls/ directory on the FS with the one from the FSP in the same location. Note that this is not a recommended or supported change. I just know that this works. :)

To add the app pool identity to the readers role in ADAM, you need the federation server's machine account's SID. Or, you could just add the "authenticated users" SID to the readers role. That's what I usually do. With ADAM ADSI Edit, add a Windows group to the readers role in the partition you have created and select "authenticated users".

If that doesn't work, then post some of your federation server log file with the logging set with everything "on" and we'll see if we can fix it.

Joe K.

Joe Kaplan-MS MVP Directory Services Programming
Co-author of "The .NET Developer's Guide to Directory Services Programming"
<http://www.directoryprogramming.net>

"Anindya_TCS"
<AnindyaTCS@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message

Re: ADAM account store in ADFS

news:D59B919C-B735-479D-A586-C10A15B74EAA@xxxxxxxxxxxxxxxxxxxx

Hi Joe,

Thanks for the great help.

But still , i have some confusion.

- 1)How to customize the FS with the clientlogon.aspx page from the FSP?
- 2)Or how to configure FSP?

If FSP is Federation Proxy , i have already configure it to my perimeter DNS to resolve the Federation server name and the Web server name.

- 3)How to add ADFS app pool account to readers role in ADAM?

I have follow the article from Microsoft Technet:

<http://technet2.microsoft.com/windowsserver/en/library/8463deb5-f96e-43d5-ad85->

After that i have checked with the article if ADAM is working or not with below article:

<http://technet2.microsoft.com/windowsserver/en/library/8463deb5-f96e-43d5-ad85->

it can make LDAP query.

"Joe Kaplan" wrote:

It is a bit tricky to get working, but it can be made to happen. Here are some high level things to keep in mind:

The FS does not have a forms-based login page out of the box, only the

Re: ADAM account store in ADFS

FSP

does. The FS uses Windows auth (integrated auth in IIS) by default, so that won't work with ADAM. As such, you need to either customize the FS with the clientlogon.aspx page from the FSP or just configure the FSP as well.

You need to make sure the ADFS app pool identity (usually network service) has read access to the entire ADAM store. This can be done by adding the ADFS app pool account to the readers role in ADAM.

You need to make sure you ADAM users are "bindable". This means that they have valid unique user names, passwords set and have msds-useraccountdisabled set to FALSE. You may also wish to be careful about the use of msds-userDontExpirePassword.

You need a good user name strategy for ADAM. I generally like to use userPrincipalName as the logon name since it can be used for an LDAP bind. This would then be the user name that users type in the logon form. You

Re: ADAM account store in ADFS

would configure the ADAM account store to use that name as the user name for query purposes. Be warned though that ADFS likes the UPN to use the AD format, meaning that it should have an @ symbol in it like an email address. ADFS also wants you to use a specific narrow range of UPN suffixes if you will use that as the identity claim.

It is also a good idea to configure ADAM to use SSL so the bind authentication will be secure. ADFS accepts that.

It isn't nearly as easy to get ADAM running as an account store as it is to get AD, but it is definitely doable. I've done it several times already.
Best of luck!

Joe K.

--

Joe Kaplan—MS MVP
Directory Services
Programming
Co—author of "The .NET
Developer's Guide to
Directory Services
Programming"
<http://www.directoryprogramming.net>

--

"Anindya_TCS"
<Anindya_TCS@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
wrote in message

Re: ADAM account store in ADFS

news:B162D5CD-2496-4D32-A213-F51219BEE772@xxxxxxxxxxxxxxxxxxxx

Hi ,

I am new in ADFS.I have configured ADFS for single sign on for sharepoint portal claim aware application with 2 active directory forest.One active directory forest is for external users and other for internal user.I have configured federation trust and active directory account store to configure the same. Up to this point the configuration is working fine and single sign on is happening.

But while i am trying to configure

Re: ADAM account store in ADFS

the same by
removing
the external
active
directory
and place a
ADAM in
stead of that
i am facing
problem.

My believe
is that i am
not
configuring
ADAM
account
store
properly
to
work
with ADFS.

Please
guide how
to configure
ADAM
account
store in
ADFS.