Access Manager: Deep Dive with the SAML Federation Protocol Lab

NIQ17

Novell Training Services

www.novell.com

ATT LIVE 2012 LAS VEGAS

Novell®

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.

404 Wyman Street, Suite 500

Waltham, MA 02451

U.S.A.

www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Exercise 1.0 SAML 2.0 SaaS Application

The objective of this lab is to setup the Novell Access Manager as a SAML2 Identity server providing authentication information to a Salesforce SaaS connector with the goal of SSO. As with all Federations, it's imperative that one understands both the SP and IDP requirements before starting.

Salesforce configuration:

A sample user (attliveuser1 to attliveuser24@gmail.com) will be created for everyone (Novell1234 is the password).

1. Login to https://login.salesforce.com/ as this user
2. Note the hostname that you have been redirected to on the Salesforce side e.g. https://na14.salesforce.com. This will be needed for use later on.
3. Go to Administration Setup -> Security Controls -> Single-Sign-On settings
4. Click Edit link under 'Single Sign-On settings'
5. Enable the 'SAML enabled' flag. Once done, a list of new configuration options will appear for the SAML setup
    a. Set the 'SAML version' to be 2.0
    b. Set the 'Issuer' field to be https://idpedir.am3.com:8443/nidp/saml2/metadata
    c. In order to import the 'Identity Provider Certificate', go to the iManager setup for Access Manager and export the IDP signing certificate
        c.i. Go to Security -> Certificates and click on 'test-signing' certificate
        c.ii. Export the Public Certificate (will be in c:\users\novell\downloads\ directory) as a DER file
    d. Set the 'Identity Provider Login URL' to be https://idpedir.am3.com:8443/nidp/saml2/sso
    e. Set the 'Custom Error URL' to be http://www.novell.com – any issues consuming the assertion will cause a redirect to this location
    f. Set the 'SAML User ID Type' to be "Assertion contains salesforce.com username"
    g. Set the 'SAML User ID Location' to be "UserID is in the NameIdentifier element of the Subject statement"
    h. Set the 'Identity Provider logout URL' to be https://idpedir.am3.com.com:8443/nidp/app/logout
    i. Leave the 'User Provisioning enabled' flag to be off
    j. Set the 'Entity ID' to https://attliveuserXX-dev-ed.my.salesforce.com and not the https://saml.salesforce.com URL.
6. Click the 'Save' option at the bottom to save the Salesforce SAML setup.
7. From the main Single Sign-On page, Export the metadata by clicking on the 'Download Metadata' tab. Note the location of this metadata file.

Access Manager Identity Server configuration:

1. Select the Identity Server cluster configuration (Devices -> Identity Server -> IDPeDir)
2. Select the SAML2 Tab and Add a new Service Provider (New -> Service Provider)
3. Under the Service Provider source, change the default 'Metadata URL' to 'Metadata Text'
    a. Under 'Name', assign it any logical name e.g. Salesforce connector.
    b. Under 'Text', insert the Salesforce SP metadata exported above.

b.i. Need to add signing cert from Salesforce here! This has been done already to save time.
b.ii. Need to add inter/root certs into the IDP/OCSP trusted root stores. This has been done already to save time.

4. Click 'next' to save all the options and the 'Finish' tab in the next Window presented (Create Trusted Service Provider)

   Now that the SAML2 Service Provider entry has been created, the next step is to configure it so that the Access Manager SAML2 Identity Server sends the parameters required by the Salesforce SAML2 Service Provider. Typically, the Service Provider documentation outlines what information is expected in the assertion

5. After clicking on the Salesforce Connector Service Provider, go to the 'Attributes' TAB. Under Attribute Set drop down menu, click on 'New Attribute' set
6. Add 'Salesforce Attribute Set' to 'Set Name' field and click 'Next'
   a. Click 'New' in the 'Create Attribute Set' Window and set the 'Local Attribute' field to be 'LDAP Attribute: mail'
   b. Click OK to continue
   c. Click 'New' again and enable the 'Constant' radio button this time. In the 'Constant' value field, add http://www.novell.com
   d. In the 'Remote Attribute' field, add the 'logouturl' string without the quotes
   e. Click OK to continue
7. Click 'Finish' and then 'Apply' to save the attribute set. Do not move the 'Available' LDAP mail attribute to the 'Send with Authentication field'. What happens when this is done?

   Now that the required attributes have been defined, it's time to define the contents of the response the Identity Server will send the Salesforce Service Provider i.e. The assertion details.

8. Select the 'Authentication Response' TAB of the Salesforce Connector Service provider
   a. Make sure the Binding is set to POST
   b. Enable the 'Unspecified' Name Identifier and set the value to 'LDAP attribute: mail' from the drop down menu
   c. Make the 'Unspecified' Name Identifier as the default

   The last stage of the Salesforce connector configuration on the Identity Server requires the Intersite transfer service details. These may not be needed in some cases where the Service Provider redirects the request to the Identity server. However, we will be testing both setups and therefor will populate it.

9. Select the 'Intersite transfer Service' TAB of the Salesforce Connector Service provider
   a. Under 'ID:' add a logical ID that will be used for the service e.g. salesforce
   b. Under 'Target', add the salesforce URL returned in step 2 of Salesforce configuration above) e.g. 'https://na14.salesforce.com/home/home.jsp' in my example. This is normally given by the SP but with Saleforce, one needs to locate the URL manually.
   c. Enable the option 'Allow any target'

d. Update the Identity Server with the changes

Testing whether it all works!

A) IDP Initiated SSO using the Intersite transfer URL

a. Enable the SAML Tracer tool on your Public Workstation Firefox browser by going to 'Tools -> SAML Tracer'
b. On the same browser, go to the following URL – https://idpedir.am3.com:8443/nidp/saml2/idpsend?id=salesforce
c. At the Login Page, enter the attliveuser1/Novell1234 password credential set
d. Confirm that you are signed onto the Salesforce Application as ATTLiveUser1
e. Look at the SAML tracer output to look at the Assertion details from the browser to the SAML Salesforce Service Provider

B) SP Initiated SSO

a. Shutdown and restart browser to clear out session details from the previous exercise
b. Enable the SAML Tracer tool on your Public Workstation Firefox browser by going to 'Tools -> SAML Tracer'
c. On the same browser, go to the following URL – https://attliveuser1-dev-ed.my.salesforce.com
d. Verify that you are automatically redirected to the Access Manager login page
   d.i. What is the issue (signed – need to import the signing cert)
e. Login as attliveuser1/Novell1234 and confirm that the user is redirected to the https://na14.salesforce.com/home/home.jsp Salesforce home page where the user displayed is attliveuser1
f. Look at the SAML tracer output to look at the Assertion details from the browser to the SAML Salesforce Service Provider
   f.i. Note there are two SAML entries – the AuthnRequest and the AuthnResponse!

C) Logout requests

a. After logging into Saleforce, click the User drop down list where the logout option exists. Logout the user.
b. Note that you log out of both the SP and Identity server with the Sharepoint logout.

Appendix – For reference only and not needed for the exercise

a. Google mail accounts for users attuser1@gmail.com to attuser30@gmail.com
   a.i. http://www.youtube.com/watch?v=cfO_iRv9Jro explains how to do this

b. Salesforce developer accounts for each of the above atusers
   b.i. Go to http://www.developerforce.com/events/regular/registration.php
   b.ii. Add first/last name, email address and username (attuser1@gmail.com to attuser30@gmail.com)
   b.iii. After submitting the request, an email will be sent to each account with the following details about the user

> Welcome to Force.com Developer Edition.
> Dear Neil Cashell,
>
> Your user name is below. Note that it is in the form of an email address:
> User name: ncashell@suse.de
>
> You'll be asked to set a password and password question and answer when you first log in.
> Passwords are case sensitive.
> Your password question and answer will be used if you forget your password. Make sure to choose a password question and answer that you will easily remember.
>
> Click https://login.salesforce.com/?c=l14m45XhAp1T_b1eqJIqPfec2cYFGZxYMPLXMxRVb1llZza7HIXAXJ6Abbd2lqe3reoKXxLn0TGA%3D%3D to log in now.
>
> Once again, welcome to Force.com!
>
> salesforce.com
> http://developer.salesforce.com

   b.iv. Click on the link above for each user request and enter the password for the account. Let's be consistent and use Novell1234 for all users (requires advanced password). At this stage, the user will be logged in and the account will be ready to use.

   b.v. When logged in to each user account, go to Company Profile -> My Domain and add the username to be part of the new domain. This will look like the following for each user:
   https://-dev-ed.my.salesforce.com/

   b.vi. Select the Availability button and once it displays the domain as available, agree to the terms and conditions and click the 'Register Domain' option.

c. Update SF domain before SP initiated SSO can be performed

   The setup page for this feature at Salesforce is under Setup->Company Profile->My Domain. It took just over 26 hours for the DNS record to be added. The SP initiated URL for my Salesforce account is:

   https:// nam32-dev-ed.my.salesforce.com

...where "nam32" is the name I entered for the URL (the rest is added automatically)

It takes a day or so for Saleforce to register the "nam32-dev-ed" hostname. Once completed, I received an email indicating "DNS Propagation" was now complete. SP initiated logins to Salesforce via NAM32 now work as expected.

d. Change the domains to ATT domains

Troubleshooting Exercise : We are trying to setup a SAML2 federated environment between Digair and IDPeDir

// Background:

- iDPeDir is the SAML2 SP that runs our back end service, and consume assertions generated by the SAML2 IDP server□- Digair is the SAML2 IDP server where users will authenticate and where assertions will be generated to the Digair SAML SP

// Setup details:

* DigitalAirlines IDP server is defined on IDPeDir (SAML2 SP) Administration Console□* IDPeDir defines □- how to generate the AuthnRequest attributes to the IDP server we are talking to□- how to handle the assertion returned from the IDP server we are talking to□□* IDPeDir SAML2 SP (HMOs are us) is defined on DigitalAirlines Administration Console□* Digair defines□- how to handle the incoming AuthnRequest from the IDPeDir SP□- what to include in the AuthnResponse (assertion) to the SP

// Problem scenario:□□All communication to both SAML providers will use the POST binding (SP asks to use this bidning and IDP has it enabled)□Everything appears to be setup correctly, but users are getting errors when trying to authenticate. Typically, the user will do the following:□□- browse to https://idpedir.am3.com:8443/nidp/□- select the SAML2 card to authenticate at the IDP server (https://digair.da.com:8443/nidp/) to send request to the remote SAML2 IDP server□- login at the remote Digital Airlines SAML2 IDP server□- get redirected back to the SP for SSO with valid assertion□□In our setup, the user gets the following initial error when clicking the Digital airlines IDP server auth card□□"Error:An Identity Provider response was received that failed to authenticate this session. (300101008-*)"

a) Address this initial error (hint - look at general identity provider settings). □b) Once the initial error is addressed, the user will get another 300101008 status error (Look closely at logs as this is a seperate issue to the first ....)□c) When this second issue has been addressed, the user should finally be prompted for credentials at the SAML2 IDP server (user Frankair with password as pwd). However, instead of getting prompted to federate, the user has another error

"Error:An Identity Provider response was received that failed to authenticate this session. (300101008-*)"□□ d) when this last issue is addressed, the user should now be redirected back to the SAML2 SP where a 300101041 error is displayed. Note that

- the SP tries to authenticate the authenticated Frankair locally□ - the user Frankair in The Digital Airlines user store has the same email address as a corresponding user on the IDPeDir user store.

Address all errors :-)