PCM - How To configure multi domain SSO authentication using AD or LDAP

Purpose

There are some additional questions, not covered in the documentation, which are usually raised when configuring SSO (Single Sign On) to use AD (Windows Active Directory) or LDAP (Lightweight Directory Access Protocol).

This Wiki will use working examples to cover topics that give rise to the most common questions/topics not covered in the documentation:

1. Configure AD (Active Directory) SSO for a single domain.
2. Radio buttons “Use security inherited…” / “Specify a fixed…”
3. Add a second domain for AD (Active Directory) to enable multi-domain SSO.
4. What is the Check-box “Enable Secondary Logon” used for?
5. Configure LDAP (Lightweight Directory Access Protocol) SSO for a single domain

Configure AD (Active Directory) SSO for a single domain

For this example let’s assume that we have the following environment:

- A Microsoft Windows domain:
  NetBIOS="DOMAIN", FQDN="domain.local".
- Windows AD (Active Directory) DC (Domain Controller):
  NetBIOS="LMW08R2X64-AIO1", FQDN="lmw08r2x64-aio1.domain.local".
- PCM primary applications server:
  NetBIOS="LMW08R2X64-APP1", FQDN="lmw08r2x64-app1.domain.local".

1. Using the PCM Configuration Wizard, in the “Login options” dialogue-box, select “Windows Active Directory” under “Single Sign on type” then press the “Configure” button:
2. The “Active Directory Parameters” will, by default, contain a single entry which is used to define the command and parameters that the PCMServer.exe service will use to verify the logged in user’s account with the correct AD Domain Controller.

Press the “Edit…” button to configure and test the parameters for the highlighted default entry.

3. The “Parameters” dialogue-box is displayed as follows:

Where:
1. **Domain** – This is a reference name that represents the configuration entry for the domain being configured. When there is just a single domain then this reference name is set to the NetBIOS name of the PCM Primary Applications Server.

2. **Active Directory Parameters** – This is the definition of the command and parameters that will be used by the PCMServer.exe service to verify the SSO users to the AD Domain Controller.
   
   1. **WinNT** – This parameter defines this entry as an AD (Active Directory) verification.
   
   2. **%DOMAIN%** - This is a variable which is replaced, during the verification process, by the NetBIOS name of the domain that the SSO user logged into.
   
   3. **%USER%** - This is a variable which is replaced, during the verification process, by the username that the SSO user used to login to the domain.
   
   4. **user** – This parameter tells the verifying AD Domain Controller that we are verifying a user account rather than some other AD object like a group, printer or computer. Only use the “user” parameter here... any other object like “group” is not valid.

4. In the lower half of the dialogue-box in the “Test Settings” group-box, notice that the edit-boxes:

   - **Test Domain** – Has defaulted to the NetBIOS domain name that the PCM Primary Applications Server it attached to.
   
   - **Test User** – Has defaulted to the currently logged in user.

   Also notice how the “Active Directory Preview” displays a command which has been constructed from the entry in “Active Directory Parameters” using the “Test Domain” and “Test User” to replace the variables %DOMAIN% and %USER%.

5. Press the “Test” button to send the command in “Active Directory Preview” to the verifying AD Domain Controller. The test should be confirmed successful as follows:

   ![Successful validation message]

6. Now place an “X” at the end of the “Test Domain” and notice how this is reflected in the “Active Directory Preview” command that is constructed. Now press the “Test” button again:
7. This time there is a pop-up error message “80070035” because the domain “DOMAINX” does not exist.

8. Now correct the “Test Domain” by removing the “X” and place an “X” at the end of the “Test User”. Notice how this is reflected in the “Active Directory Preview” command that is constructed. Now press the “Test” button again:

9. This time there is a pop-up error message “800708ad” because the user “AdministratorX” does not exist.

10. Correct the “Test Domain” and “Test User” entries and press the “Test” button one last time to check that user verification is working properly again. Then press the “OK” button to save the new entry.

11. Back in the “Configure Active Directory Options” dialogue-box, select the default domain entry that we just tested and notice how the “Active Directory Preview” reflects the command that has been constructed according to this entry:
Now press the "Test" button to test this command... the following pop-up message should be displayed to confirm the command in "Active Directory Preview" successfully verified the user in the domain.

Radio buttons “Use security inherited...” / “Specify a fixed...”

It is the "PCMServer.exe" service that constructs and submits the command to the appropriate AD Domain Controller in order to verify the SSO user. The PCMServer.exe service must have the appropriate rights for this verification request to be successful. The verification request can be submitted using the account that the PCMServer.exe service is "Logged on as", or we can configure a specific account that has been setup for this purpose.

From the "Configure Active Directory Options" dialogue-box, select the required entry and then press the "Edit..." button to launch the

"Parameters" dialogue-box:

1. **Use security inherited from PCM security service to validate users** - By default this option is selected causing the request for verification to be submitted using the account that the "PCMServer.exe" service has configured for "Logged on as".
   1. This is usually fine where the SSO users are in the same domain as the PCM Primary Applications Server and so the following default setting works:
1. In our example we can see from the “Services” utility that the account being used to run the “PCMServer.exe” service is the “Local System” account. This account must have the required rights in order to successfully perform the verification request to the authenticating AD Domain Controller.

![Services Utility](image1)

2. Specify a fixed specific user to validate a user’s logon credentials -- When SSO users are spread across multiple domains which are different to the domain that the PCM Primary Application Server is connected to then the “Logged on as” account configured for the “PCMServer.exe” service probably won’t have the required rights in order to perform cross domain verification. So you will need to configure a special account that has been setup with the required permissions specifically for the purposes of cross-domain account verification.

   1. Here you define the “User name” and “Password” of a “Domain Global Security” account that has rights to perform account verification requests across multiple domains.

   ![Parameter Settings](image2)

   2. Press the “Test” button to send the command in “Active Directory Preview” to the verifying AD Domain Controller using the credentials specified above. The test should be confirmed successful as follows:
3. Now place an “X” at the end of the “User Name” and press the “Test” button again:

   ![Image of SAP BusinessObjects Profitability and Cost Management Co...]

   Successfully validated user 'Administrator' on specified Server.

   OK

4. This time there is a popup error message “800704c3” because the account being used to perform the verification request does not exist:

   ![Image of SAP BusinessObjects Profitability and Cost Management Configuration Wizard]

   Failed to validate user 'Administrator' on specified Server - (800704c3). Multiple connections to a server or shared resource by the same user, using more than one user name, are not allowed. Disconnect all previous connections to the server or shared resource and try again.

   OK

5. Now correct the “User Name” by removing the “X” and place an “X” at the end of the “Password”. Now press the “Test” button again:

   ![Image of SAP BusinessObjects Profitability and Cost Management Configuration Wizard]

   Use security inherited from PCM security service to validate user

   Specify a fixed specific user to validate a user’s logon credentials

   User Name: Administrator

   Password: ********

6. This time there is a popup error message “800704c3” because the account being used to perform the verification request has an invalid password:

   ![Image of SAP BusinessObjects Profitability and Cost Management Configuration Wizard]

   Failed to validate user 'Administrator' on specified Server - (800704c3). Multiple connections to a server or shared resource by the same user, using more than one user name, are not allowed. Disconnect all previous connections to the server or shared resource and try again.

   OK

7. Correct the “User Name” and “Password” entries and press the “Test” button one last time to check that user verification is working properly again. Then press the “OK” button to save the entry.

Add a second domain for AD (Active Directory) to enable multi-domain SSO.
If your PCM environment has two separate domains then you will need to reflect this in the PCM Configuration Wizard so that PCM knows where to send the SSO verification requests. In this example we will configure SSO to use AD where our user community is spread across two domains “domain.company.com” and “domain2.company.com”. Let’s assume that we have the following environment:

**First Domain**

- A Microsoft Windows domain:
  NetBIOS="DOMAIN", FQDN="domain.local".
- Windows AD (Active Directory) DC (Domain Controller):
  NetBIOS="LMW08R2X64-AIO1", FQDN="lmw08r2x64-aio1.domain.local".
- PCM primary applications server:
  NetBIOS="LMW08R2X64-APP1", FQDN="lmw08r2x64-app1.domain.local".

**Second Domain**

- A Microsoft Windows domain:
  NetBIOS="DOMAIN2", FQDN="domain2.local".
- Windows AD (Active Directory) DC (Domain Controller):
  NetBIOS="LMW08R2X64-AIO2", FQDN="lmw08r2x64-aio2.domain2.local".

1. In the “Configure Active Directory Options” dialogue-box press the “Add…” button to create a new entry for the second domain:

   ![Configure Active Directory Options](image)

   1. In the “Parameters” dialogue-box complete the configuration as follows:

   ![Parameters](image)
Settings:

- **Domain** – This is the NetBIOS name of the domain that the users belong to.
- **Active Directory Parameters** – This is edit-box is used to define the string which is constructed and then sent to the AD Domain Controller to verify the logged in user. The default format for the string is “WinNT://%DOMAIN%/%USER%,user”.
- **Specify a fixed specific user to validate a user’s logon credentials** – Select this option then complete the account details below:
  - **User Name** – Specify the “User name” of a “Domain Global Security” account in the domain “DOMAIN” that has rights to perform account verification requests to the DC in “DOMAIN2”.
  - **Password** – Specify the password for the above account.

Test Settings:

1. **Test Domain** – Has defaulted to the name of this entry which was the name entered into the “Domain” edit-box at the top of this dialogue-box.
2. **Test User** – This will default to the currently logged on user. However, this should be changed to a suitable SSO user’s account that you know exists within the “DOMAIN2” AD.

3. Press the “Test” button to send the command in “Active Directory Preview” to the verifying AD Domain Controller using the credentials specified above. The test should be confirmed successful as follows:
4. On the “Parameters” dialogue-box press the “OK” button to save the new “DOMAIN2” entry.

5. We now need to rename the default entry from “LMW08R2X64-APP1” to “DOMAIN” so that each of the two entries has a “Domain Name” that matches the NetBIOS name of the domain that it serves.

6. However, if you select the default domain “LMW08R2X64-APP1” and then press the “Edit…” button you will see that the “Domain” edit-box is disabled and you can’t change the name.

7. Create the new entry for domain “DOMAIN” as follows then press the “OK” button to save the entry:
8. On the “Configure Active Directory options” dialogue-box, select the default entry “LMW08R2X64-APP1” then press the “Delete” button and confirm.

9. The final result of the above configuration steps will look something like this:
9. Press the “OK” button to save the configuration.

10. How this will work:
   1. A user logs on to Windows in the domain “DOMAIN2” using their username “FBLOGGS”.
   2. The user launches PCM Model Builder.
   3. PCM Model Builder interrogates Windows and determines that the user is “FBLOGGS” in domain “DOMAIN2”. This information is passed back to the PCMServer.exe service running on the PCM Primary Applications Server.
   4. The PCMServer.exe process takes the domain “DOMAIN2” passed to it by Model Builder and then scans the entries configured in step (9) above searching for a match under the “Domain Name” column.
   5. When a match is found the PCMServer.exe process will use the entry to construct a command substituting any parameters like “%DOMAIN%” and “%USERNAME%” with the information “DOMAIN2” and “FBLOGGS” passed to it by Model Builder.
   6. The constructed command is then submitted to the appropriate AD Domain Controller to verify that the user does exist in that domain using the account provided in the entry.
   7. If the verification process is successful then access is granted and the PCMServer.exe service will search for an account in PCM with the exact same username to use to logon the user to PCM.

What is the Check-box “Enable Secondary Logon” used for?

Using the PCM Configuration Wizard, on the “Login options” page, there is a check-box called “Enable Secondary Logon”:

Unchecked - With “Enable Secondary Logon” un-checked, if the selected SSO authentication type fails then the user will be denied access to
PCM.

Checked – With “Enable Secondary Logon” checked, if the selected SSO authentication type fails then the user will be presented with the native PCM login prompt. This means that if problem develops with the SSO process then users will still be able to logon to PCM by providing their PCM credentials in for usual way.

Configure LDAP (Lightweight Directory Access Protocol) SSO for a single domain.

1. Using the PCM Configuration Wizard, in the “Login options” dialogue-box, select “LDAP Active Directory” under “Single Sign on type” then press the “Configure” button:

![Configure LDAP Options](image)

2. The “LDAP Parameters” will, by default, contain a single entry which is used to define the LDAP command and parameters that the PCMServer.exe service will issue to verify the logged in user’s account with the correct LDAP Server. By default all Microsoft DC (Domain Controllers) also run an LDAP Server.

![Configure LDAP Options](image)

Press the “Edit…” button to configure and test the parameters for the highlighted default entry.

3. The “Parameters” dialogue-box is displayed as follows:
Where: LDAP://machinename:port/cn=%COMMONNAME%,dc=%DOMAIN%,dc=local

1. **Domain** – This is a reference name that represents this entry for the domain being configured. When there is just a single domain then this reference name is set to the NetBIOS name of the PCM Primary Applications Server.

2. **LDAP Parameters** – This is the definition of the command and parameters that will be used by the PCMServer.exe service to verify the SSO users to the AD Domain Controller.
   1. **LDAP** – This parameter defines this entry as LDAP (Lightweight Directory Access Protocol) verification.
   2. `%COMMONNAME%` - This is the name of the users.
   3. `%DOMAIN%` - This is a variable which is replaced, during the verification process, by the NetBIOS name of the domain that the SSO user logged into.
   4. `%USER%` - This is a variable which is replaced, during the verification process, by the username that the SSO user used to login to the domain.
   5. **user** – This parameter tells the verifying AD Domain Controller that we are verifying a user account rather than some other AD object like a group, printer or computer. Only use the “user” parameter here… any other object like “group” is not valid.

4. In the lower half of the dialogue-box in the “Test Settings” group-box, notice that the edit-boxes:
   1. **Test Domain** – Has defaulted to the NetBIOS domain name that the PCM Primary Applications Server it attached to.
   2. **Test User** – Has defaulted to the currently logged in user.
Also notice how the “Active Directory Preview” displays a command which has been constructed from the entry in “Active Directory Parameters” using the “Test Domain” and “Test User” to replace the variables %DOMAIN% and %USER%.

5. Press the “Test” button to send the command in “Active Directory Preview” to the verifying AD Domain Controller. The test should be confirmed successful as follows:

```
SAP BusinessObjects Profitability and Cost Management Co...
```

Successfully validated user ‘Administrator’ on specified Server.

```
OK
```

6. Now place an “X” at the end of the “Test Domain” and notice how this is reflected in the “Active Directory Preview” command that is constructed. Now press the “Test” button again:

```
[Image of test settings]
```

This time there is a pup-up error message “80070035” because the domain “DOMAINX” does not exist.

```
SAP BusinessObjects Profitability and Cost Management Configuration Wizard
```

Failed to validate user ‘Administrator’ on specified Server - (80070035) The network path was not found.

```
OK
```

8. Now correct the “Test Domain” by removing the “X” and place an “X” at the end of the “Test User”. Notice how this is reflected in the “Active Directory Preview” command that is constructed. Now press the “Test” button again:
9. This time there is a pop-up error message "800708ad" because the user "AdministratorX" does not exist. Correct the "Test Domain" and "Test User" entries and press the "Test" button one last time to check that user verification is working properly again. Then press the "OK" button to save the new entry.

10. Back in the "Configure Active Directory Options" dialogue-box, select the default domain entry that we just tested and notice how the "Active Directory Preview" reflects the command that has been constructed according to this entry:

11. Now press the "Test" button to test this command... the following pop-up message should be displayed to confirm the command in "Active Directory Preview" successfully verified the user in the domain.

Related content


http://blog.skufel.net/2011/11/how-to-windows-server-2008-r2-installing-adlds/