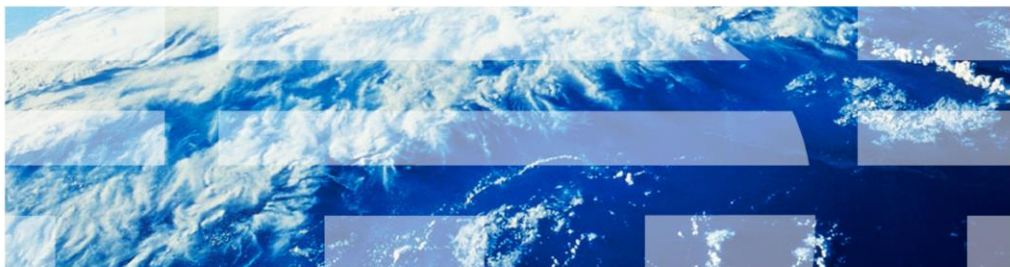


InfoSphere Information Server

Troubleshooting Information Server version 8 LDAP authentication issues



© 2013 IBM Corporation

This presentation will discuss common authentication issues found when configuring Information Server version 8 with a Lightweight Directory Access Protocol user registry. Lightweight Directory Access Protocol is referred to as LDAP throughout this presentation.

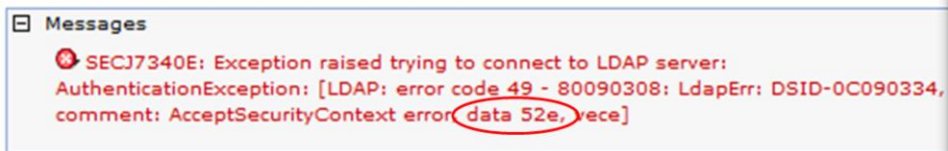
Objectives

- What does error 49 mean
- Common causes of error 49

The objectives of this presentation are to discuss what an LDAP error 49 means and how to determine why the user authentication failed. It will also discuss common issues that will cause an LDAP error 49.

LDAP error code 49 – Active Directory

- LDAP error 49 – authentication error
 - Check “data” value
 - Data Value definition
 - 525 user not found
 - 52e invalid credentials
 - 530 not permitted to logon at this time
 - 531 not permitted to logon at this workstation
 - 532 password expired
 - 533 account disabled
 - 701 account expired
 - 773 user must reset password
 - 775 user account locked
- Correct user account and try login again



The screenshot shows a Windows Messages window with the following text:

```
Messages
SECJ7340E: Exception raised trying to connect to LDAP server:
AuthenticationException: [LDAP: error code 49 - 80090308: LdapErr: DSID-0C090334,
comment: AcceptSecurityContext error: data 52e, vce]
```

The first error that this presentation will discuss is the LDAP error code 49. An error 49 is an authentication error. When the authentication of a user fails, there are many different reasons for the failure such as in invalid user name or password, the user account is locked, the account is disabled, and more. When an error 49 is received when connecting to an Active Directory Server, it is important to look at the data value in the error to determine why the login is failing. In the example displayed on this slide, the data value is 52e which means the user credentials are incorrect. Once it is determined why the login is failing, it is easier to determine what actions need to be taken to resolve the issue.

LDAP error code 49 – non-Active Directory

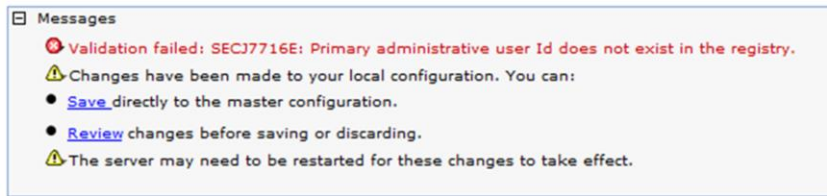
- Tivoli®, Open LDAP, and so on
 - Data value description shown instead of number

Messages

SECJ7340E: Exception raised trying to connect to LDAP server:
AuthenticationException: [LDAP: error code 49 - Invalid Credentials]

On other types of LDAP servers, Tivoli and Open LDAP for example, the actual text of the reason for the failure is printed. In this example, the user's password was wrong and the error displays the text "Invalid Credentials". Again, it is important to look at the text following the error 49 to determine why the login is failing.

Primary administrative user ID does not exist (1 of 2)



- Error: Primary administrative user Id does not exist in registry
 - Standalone LDAP
 - Administrative user must be an LDAP user



5

Troubleshooting Information Server version 8 LDAP authentication issues

© 2013 IBM Corporation

Another common error that can occur when configuring LDAP in WebSphere® is Validation Failed, Primary user Id does not exist in the registry. When stand-alone LDAP is configured, the user ID that is entered as the Primary administrative user name must be a valid LDAP user. If the user entered is not a valid user, change the user name to a user that is a valid LDAP user. If the user is a valid LDAP user, then the issue may be a problem with the configured base distinguished name.

Primary administrative user ID does not exist (2 of 2)

- Distinguished name of administrative user must fall within configured Base DN
- Base DN
OU=ServAccts,DC=NewCo,DC=com
- DN for the WebSphere Application Server administrative user
CN=wasadmin,CN=Users,DC=NewCo,DC=com
- Primary administrative user not within Base DN
- Change to Base DN to include administrative user
 - Example
Base DN = DC=NewCo,DC=com

General Properties

* Primary administrative user name
wasadmin

Server user identity

Automatically generated server identity

Server identity that is stored in the repository

Server user ID or administrative user on a Version 6.0.x node
tdwasadmin

Password

Type of LDAP server
Microsoft Active Directory

* Host
MyADServer.newco.com

Port
389

Base distinguished name (DN)
OU=ServAccts,DC=NewCo,DC=com

Bind distinguished name (DN)
CN=BindUser,OU=ServAccts,dc=NewCo,DC

Bind password

Search timeout
120 seconds

Reuse connection

Ignore case for authorization

6

Troubleshooting Information Server version 8 LDAP authentication issues

© 2013 IBM Corporation

When stand-alone LDAP authenticates a user, it uses the base distinguished name as the starting location for the search. If the user it is searching for is not within that branch of the LDAP search, it is not able to find the user. In this example, the WebSphere Administrative Server administrative user is in the CN=Users,DC=NewCo,DC=com branch but the search is only searching down the OU=ServAccts,DC=NewCo,DC=com branch so it is not able to find the WebSphere Administrative Server administrative user. To fix this, change the base DN in the LDAP configuration to include the WebSphere Administrative Server administrative user's branch. For example, DC=NewCo,DC=com. This holds true for any other user that is going to use Information Server. You must ensure the users all fall within the search path defined by the base DN.

WebSphere will not start due to LDAP errors (1 of 2)

- WebSphere fails to start
- Check SystemOut.log for errors
 - <WAS_InstallDir>/profiles/<profileName>/logs/server1
 - Example

```
[<date> <time>] 0000000a distSecurityCE SECJ0007E: Error during security initialization. The exception is javax.naming.AuthenticationException: [LDAP: error code 49 - 80090308: LdapErr: DSID-0C090334, comment: AcceptSecurityContext error, data 52e, vece]
```

 - Error code is 49 – Shows Authentication issue
 - Data code 52e – Shows invalid credentials
- UNIX/Linux
 - As root run AppServerAdmin.sh command to reset WebSphere Application Server administrative user password

```
<IS_InstallDir>/ASBServer/bin/AppServerAdmin.sh -was -user <userId> -password <password>
```
- Windows
 - As Windows administrative user run AppServerAdmin.bat command to reset WebSphere Application Server administrative user password

```
<IS_InstallDir>/ASBServer/bin/AppServerAdmin.bat -was -user <userId> -password <password>
```

The next issue that may occur is WebSphere Application Server failing to start with authentication errors. If WebSphere Application Server fails to start, it is important to check the SystemOut.log file to determine the nature of the failure. For authentication issues, the same LDAP error code 49 can be seen in the SystemOut.log file. Look at the full error as seen earlier in this presentation to determine why the authentication is failing. In most cases, it is because the WebSphere Application Server administrative user's password has been changed and WebSphere Application Server was not updated before it was restarted. To correct this problem, login to the services tier as root or a windows administrator and run the AppServerAdmin command as displayed on this slide to reset the WebSphere Application Server administrative user's password. Once it completes successfully, restart WebSphere Application Server.

WebSphere will not start due to LDAP errors (2 of 2)

- Ran AppServerAdmin but WebSphere still will not start
 - AppServerAdmin only changes WebSphere Application Server administrative user and password
 - Bind distinguished name may be WebSphere Application Server administrative user
 - Need to turn security off to update bind password

If the attempt to restart WebSphere Application Server fails with another LDAP error code 49 after running AppServerAdmin, the issue is that the user that was used for the bind DN in the LDAP configuration is the same user as the WebSphere Application Server administrative user. When the AppServerAdmin command is run, it only updates the username and password for the WebSphere Application Server administrative user. It does not update the bind password. In this case, WebSphere Application Server security will need to be manually turned off to update the bind password.

Manually turn security off

- Make backup of security.xml file
 <WAS_home>/AppServer/profiles/<profileName>/config/cells/<cellname>/security.xml
- Edit security.xml file
- Search for first instance of “enabled”

```
<?xml version="1.0" encoding="UTF-8"?>  
<security:Security xmi:version="2.0" xmlns:xmi="http://www.omg.org/XMI" xmlns:orb.secur  
b.securityprotocol="http://www.ibm.com/websphere/appserver/schemas/5.0/orb.secur  
ityprotocol.xmi" xmlns:security="http://www.ibm.com/websphere/appserver/schemas/  
5.0/security.xmi" xmi:id="Security_1" useLocalSecurityServer="true" useDomainQua  
lifiedUserNames="false" enabled="true" cacheTimeout="600" issuePermissionWarning  
="false" activeProtocol="BOTH" enforceJava2Security="false" enforceFineGrainedJC  
ASecurity="false" appEnabled="true" dynamicallyUpdateSSLConfig="true" allowBasic  
Auth="true" activeAuthMechanism="LTPA_1" activeUserRegistry="LDAPUserRegistry_1"  
defaultSSLSettings="SSLConfig_orrNode01_1" adminPreferredAuthMech="RSAToken_1">
```

- Change enabled="true" to enabled="false"
- Save file
- Restart WebSphere

The first step to manually turning off security in WebSphere is to edit the security.xml file. It is important to make a backup copy of this file before editing it. Once a copy is made, edit the security.xml file located in the directory displayed on this slide. Search the file for the first occurrence of the word “enabled”. It will read, enabled=“true”. Change the word true to false and save the file. Next, start WebSphere.

Reconfigure LDAP settings – 8.0/8.1

- Open WebSphere Application Server administrative console
- Security => Global Security
- Open LDAP configuration Settings

The screenshot displays the WebSphere Administrative Console interface. On the left, a navigation pane shows a tree structure with 'Global security' selected and highlighted by a red arrow. The main content area is titled 'Global security' and contains several sections:

- General Properties:** Includes checkboxes for 'Enable global security', 'Enforce Java 2 security', 'Enforce fine-grained JCA security' (checked), and 'Use domain-qualified user IDs'. There is also a 'Cache timeout' field set to 600 seconds and an 'Issue permission warning' checkbox (checked).
- Active protocol:** A dropdown menu set to 'CSI and SAS'.
- Active authentication mechanism:** A dropdown menu set to 'Lightweight Third Party Authentication (LTPA)'.
- Active user registry:** A dropdown menu set to 'Lightweight Directory Access Protocol (LDAP) user registry'.
- User registries:** A section with a tree view where 'LDAP' is selected and circled in red. Other options include 'Custom' and 'Local OS'.
- Authentication:** Includes checkboxes for 'Authentication mechanism', 'Authentication protocol', and 'JAAS Configuration'.
- Authorization:** Includes a tree view for 'Authorization providers'.
- Additional Properties:** Includes a tree view for 'Custom properties'.

At the bottom left, the page number '10' is visible. At the bottom center, the text 'Troubleshooting Information Server version 8 LDAP authentication issues' is present. At the bottom right, the copyright notice '© 2013 IBM Corporation' is displayed.

Once WebSphere is started, open the WebSphere administrative console. Click Security and then click Global security. For Information Server versions 8.0 and 8.1 with WebSphere Application Server version 6.0, click LDAP under User registries.

Reconfigure LDAP settings – 8.0/8.1

- Enter Server user password
- Enter Bind password
- Click Apply
- Click save in message box at top of screen

General Properties

* Server user ID
wasadmin

* Server user password

Type
Active Directory

* Host
MyADServer.newco.com

Port
389

Base distinguished name (DN)
DC=NewCo,DC=com

Bind distinguished name (DN)
CN=wasadmin,OU=ServAccts,DC=NewCo

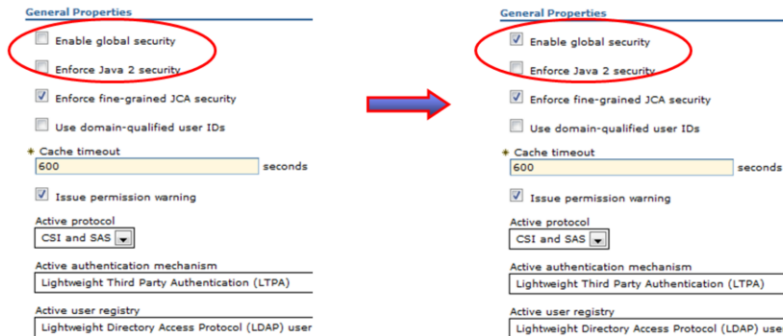
Bind password

Search timeout
120
seconds

Next, re-enter the Server user password and the Bind password. Be sure to enter the correct password for each user ID. Click Apply and Save.

Reconfigure LDAP settings – 8.0/8.1

- Go to Security => Global Security
- Check Enable Global Security
 - Will automatically check Enforce Java 2 security
- Uncheck Enforce Java 2 security
- Click OK and Save at top of screen
- Stop and restart WebSphere



12

Troubleshooting Information Server version 8 LDAP authentication issues

© 2013 IBM Corporation

Next, go back to the Global Security page and turn security back on. To do this, check Enable global security. When this is checked, it will automatically check Enforce Java 2 security. Be sure to uncheck Enforce Java 2 security. Click apply and Save. Once this is saved, the security.xml file will automatically be updated to turn security back on. Stop and restart WebSphere.

Reconfigure LDAP settings – 8.5/8.7

- Open WebSphere Application Server administrative console
- Security => Global Security
- Click Configure

The screenshot shows the WebSphere Application Server administrative console. On the left is a navigation tree with the following items: Guided Activities, Servers, Applications, Services, Resources, Security (highlighted with a red arrow), Global security (highlighted with a red arrow), Security domains, Administrative Authorization Groups, SSL certificate and key management, Security auditing, Bus security, Environment, System administration, Users and Groups, Monitoring and Tuning, Troubleshooting, Service integration, and UDDI. The main content area displays the 'Global security' configuration page. It includes a 'Global security' header, a description, and buttons for 'Security Configuration Wizard' and 'Security Configuration Report'. Below are sections for 'Administrative security' (with 'Enable administrative security' checked and links for 'Administrative user roles', 'Administrative group roles', and 'Administrative authentication'), 'Application security' (with 'Enable application security' checked), 'Java 2 security' (with 'Use Java 2 security to restrict application access to local resources' checked and options for 'Warn if applications are granted custom permissions' and 'Restrict access to resource authentication data'), and 'User account repository' (with 'Current realm definition' set to 'Standalone LDAP registry' and 'Available realm definitions' including 'Standalone LDAP registry'). The 'Configure...' button next to 'Standalone LDAP registry' is circled in red. At the bottom are 'Apply' and 'Reset' buttons.

13

Troubleshooting Information Server version 8 LDAP authentication issues

© 2013 IBM Corporation

If Information Server version 8.5 or 8.7 is installed with WebSphere Application Server version 7.0, open the WebSphere Application Server administrative console, Click Security and then Global security. On the Global security page click Configure. This example is using stand-alone LDAP.

Reconfigure LDAP settings – 8.5/8.7

- Enter Bind password
- Ensure Automatically generated server identity selected
- Click Apply
- Click Save in message box at top of screen

General Properties

* Primary administrative user name
wasadmin

Server user identity

Automatically generated server identity

Server identity that is stored in the repository

Server user ID or administrative user on a Versio
Password

Type of LDAP server
Microsoft Active Directory

* Host
MyADServer.newco.com

Port
389

Base distinguished name (DN)
OU=ServAccts,DC=NewCo,DC=com

Bind distinguished name (DN)
CN=wasadmin,OU=ServAccts,DC=NewCo

Bind password

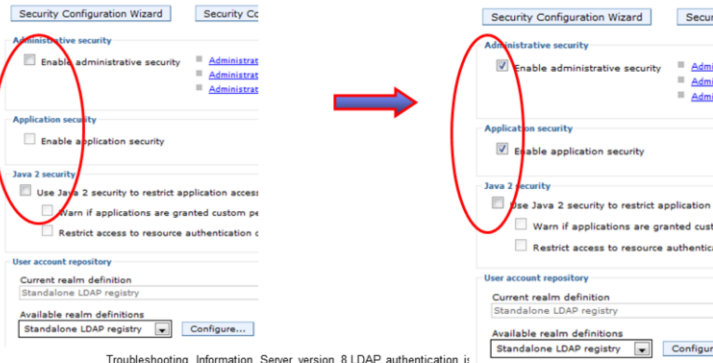
Search timeout
120 seconds

On the General Properties screen, ensure that Automatically generated server identity is checked. Next, enter the correct password for the Bind password. Notice that with Automatically generated server identity, WebSphere Application Server no longer stores the WebSphere Application Server administrative password. It is good practice to use a bind DN that will never have an expired or changed password.

Click Apply and Save at the top of the screen.

Reconfigure LDAP settings – 8.5/8.7

- Go to Security => Global Security
- Check Enable administrative Security
 - Will automatically check Use Java 2 security
- Ensure Enable application security is checked
- Uncheck Use Java 2 security
- Click OK and Save at top of screen
- Stop and restart WebSphere



15

Troubleshooting Information Server version 8 LDAP authentication i

© 2013 IBM Corporation

The last step is to turn security back on. Go back to the Global security page and check Enable administrative security. This will automatically check Use Java 2 security. Uncheck Use Java 2 security. Finally, be sure that Enable application security is checked. Click OK and save at the top of the screen. When the changes are saved, the security.xml file will automatically be updated to turn security back on. Stop and restart WebSphere Application Server.

Error 80011 connecting to DataStage

- Connecting to DataStage®
 - Two Authentications take place
 - Information Server by way of WebSphere
 - DataStage
- Shared versus Not Shared registry
 - Shared
 - Uses same user/password for both authentications
 - Not Shared
 - Uses credential mapping
- DataStage authentication
 - Local OS by default
 - May be configured for PAM
- Shared Registry
 - DataStage needs to be configured for PAM authentication
 - Review IBM education Assistant Module:

http://publib.boulder.ibm.com/infocenter/ieduasst/inv1r0/topic/com.ibm.iea.datastage/datastage/8.1/Troubleshooting/Configuring_with_PAM.pdf

- 80011 troubleshooting

<http://publib.boulder.ibm.com/infocenter/ieduasst/inv1r0/topic/com.ibm.iea.datastage/datastage/8.1/Troubleshooting/Error80011.pdf>

Another common issue when switching to LDAP is the error 80011 when attempting to connect with a DataStage client. This error indicates a login failure to the DataStage server. When connecting to DataStage, two separate authentications are performed. The first step is the authentication through WebSphere Application Server using the configured LDAP registry. The user name and password that is entered into the DataStage login screen is used for this authentication step. If the authentication against the LDAP server is successful, the user's roles are verified. Once it is determined that the user has the rights to login to DataStage, a connection needs to be made to the DataStage server. If the user registry is set to "Shared" then the system will use the same user name and password that was entered into the DataStage login screen, in this case the ID is an LDAP user and password. DataStage is configured to use local OS authentication by default. If this configuration is not changed, the login to the DataStage server will fail with an 80011 error unless the system has a local OS user and the same user name and password as the LDAP user. If PAM has been configured on the DataStage server, DataStage may be configured to use PAM authentication to allow the LDAP user's authentication to the DataStage server to succeed. This slide provides a link to an IBM Education Assistant module on how to configure DataStage to use PAM authentication. If the required result is for the user to login to DataStage with an OS user, configure the registry to be "Not shared" and use credential mapping to map the LDAP user to a valid OS user.

If everything appears to be configured correctly and the 80011 error still occurs, review the IBM Education Assistant module on Troubleshooting the 80011 error. The link to this presentation is displayed on this slide.

Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, DataStage, InfoSphere, Tivoli, and WebSphere are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)" at <http://www.ibm.com/legal/copytrade.shtml>

Windows, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.

© Copyright International Business Machines Corporation 2013. All rights reserved.