



IBM Software Group

IBM WebSphere Partner Gateway V6.1

Security enhancements



@business on demand.

© 2007 IBM Corporation
Converted to video August 5, 2014

This presentation provides details of the security enhancements made in WebSphere Partner Gateway V6.1

Goals

- Provide a high level overview of the security enhancements made in WebSphere Partner Gateway V6.1

The goal of the presentation is to provide a high level overview of the enhancements related to security in WebSphere Partner Gateway V6.1.

Agenda

- What's new in WebSphere Partner Gateway V6.1
- What is Light Weight Directory Access Protocol (LDAP) ?
- Support for LDAP based authentication
- Multiple Hubadmin users
- Unique user names among partners
- Summary and references

This slide shows the agenda for the presentation

Authentication

Existing 6.0	<ul style="list-style-type: none"> ▪ Supports database based authentication <ul style="list-style-type: none"> ▶ Need to use unique username and password specific to WebSphere Partner Gateway application ▪ Single hubadmin user
New 6.1	<ul style="list-style-type: none"> ▪ LDAP container-based authentication <ul style="list-style-type: none"> ▶ Authentication delegated to directory storage system ▪ Support for multiple hubadmin users
Benefits	<ul style="list-style-type: none"> ▪ Flexibility to the users and as well management to maintain login credentials uniquely irrespective of the applications <ul style="list-style-type: none"> ▶ User is allowed to login to WebSphere Partner Gateway console through his/her single credential ▶ LDAP authentication is delegated to WebSphere Application Server infrastructure ▪ Support for multiple hubadmin users



WebSphere Partner Gateway 6.0 supports only database based authentication, which forces you to remember unique username and password for logging into WebSphere Partner Gateway console application. With V6.1 Light Weight Directory Access Protocol (LDAP) based authentication is supported. Authentication is delegated to the directory storage system which allows you to log in to WebSphere Partner Gateway console using your single sign on credentials. This gives more flexibility to you and for the management to maintain login credentials uniquely irrespective of the applications. LDAP authentication is delegated to WebSphere Application Server infrastructure.

Also in V6.0 there is only one hubadmin user who is the super user with capabilities of configuring the partners and administering the WebSphere Partner Gateway system. With V6.1, you have the ability to create multiple hubadmin users by creating a user and assigning the user to the Hubadmin group. This resolves the issue of having to share the hubadmin user password among multiple users who need to access the WebSphere Partner Gateway Community console as the hubadmin super user.

LDAP

- What is LDAP?
 - ▶ Networking protocol for querying and modifying directory services running over TCP/IP
 - ▶ Based on X.500 standard
 - ▶ Can be used for authenticating users

Lightweight Directory Access Protocol, or **LDAP** is a networking protocol for querying and modifying directory services running over [TCP/IP](#). A directory is a set of information with similar attributes organized in a logical and hierarchical manner. So LDAP repositories can store static information related to users and can be used across the enterprise by all applications.

The main difference between a database and directory is that in a database you not only retrieve data but also make frequent updates to the data. Whereas in the case of the directory most of the actions relate to retrieve rather than updates.

Today people and businesses rely on networked computer systems to support distributed applications. These distributed applications might interact with computers on the same local area network, within a corporate intranet, within extranets linking up partners and suppliers, or anywhere on the worldwide Internet. To improve functionality and ease-of-use, information about the services, resources, users, and other objects accessible from the applications needs to be organized in a clear and consistent manner. Much of this information can be shared among many applications, but it must also be protected in order to prevent unauthorized modification or the disclosure of private information. Information describing the various users, applications, files, printers, and other resources accessible from a network is often collected into a special database that is sometimes called a directory. As the number of different networks and applications has grown, the number of specialized directories of information has also grown, resulting in islands of information that are difficult to share and manage. If all of this information could be maintained and accessed in a consistent and controlled manner, it would provide a focal point for integrating a distributed environment into a consistent and seamless system. The Lightweight Directory Access Protocol (LDAP) is an open industry standard that has evolved to meet these needs.

LDAP defines a standard method for accessing and updating information in a directory. LDAP has gained wide acceptance as the directory access method of the Internet and is therefore also becoming strategic within corporate intranets. It is being supported by a growing number of software vendors and is being incorporated into a number of applications. For example IBM WebSphere Application Server and the IBM HTTP server, support LDAP functionality as a base feature.

WebSphere Partner Gateway V6.1 and LDAP

- How does LDAP fit into WebSphere Partner Gateway security?
 - ▶ Users can login to WebSphere Partner Gateway console through his or her single sign on credentials
 - ▶ Used for Authentication but not for authorization
 - ▶ Administration of user name and password on user registry will not be done by WebSphere Partner Gateway
 - ▶ User needs to configure underlying WebSphere Application Server container to make use of LDAP.
 - ▶ Supports all LDAP Servers supported by WebSphere Application Server V6.1

8

Security enhancements

© 2007 IBM Corporation

WebSphere Partner Gateway V6.0 supports only database-based authentication, which forces you to remember unique password for logging into WebSphere Partner Gateway console application. Delegating the authentication to directory access system allows you to login to WebSphere Partner Gateway console using your single sign on credentials. This gives the flexibility to you and for management to maintain login credentials uniquely irrespective of the applications.

In order for you to be able to logon to WebSphere Partner Gateway console, you would need to have your user id (username) defined in WebSphere Partner Gateway and in LDAP user registry.

You should enable security on the WebSphere Application Server and configure the container to make use of the LDAP user registry. Container configured user registries will be used for authentication but not for authorization. Administration of user name and password on user registry will not be done by WebSphere Partner Gateway. WebSphere Partner Gateway document manager component also makes use of container based authentication during its Web Service inbound processing.

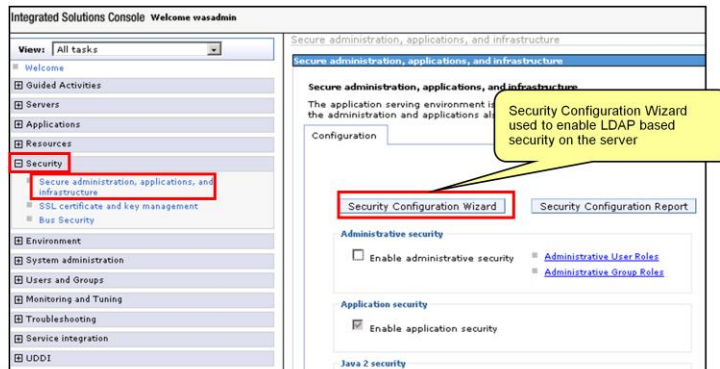
Steps to configure LDAP based authentication

- Install and configure LDAP server
 - ▶ Populate the user registry
- Configure security on the underlying WebSphere Application Server
 - ▶ Used LDAP based authentication
- Map users or groups to the Hub user role
- Configure WebSphere Partner Gateway to use container based authentication

This slide shows the steps involved in enabling LDAP based authentication for WebSphere Partner Gateway. The first step is to install and configure LDAP server and populate the user registry with the organizational information like groups and users. The next step is to enable security on the WebSphere Application server hosting the WebSphere Partner Gateway applications. The application server should be configured to use the LDAP user registry for authenticating users. The third step involves mapping the users in the user registry to the Hubuser role of the WebSphere Partner Gateway console application. This allows the users and groups mapped to the Hubuser role to log into the community console provided the user is also configured in the WebSphere Partner Gateway. The last step is to configure WebSphere Partner Gateway to use LDAP based authentication. The following slides in the presentations provide more details on the last three steps.

Configure WebSphere Application Server to use LDAP

- How to configure WebSphere Application Server to use of LDAP?
 - Can be configured using the administrative console
 - Security Secure administration, applications, and infrastructure Security Configuration Wizard
 - Enable application security
 - Select Stand-alone LDAP registry as user repository
 - Server restart needed for changes to take effect



10

Security enhancements

© 2007 IBM Corporation

This slide provides details on how you can configure security for the WebSphere Application Server. WebSphere application server administrative console provides a security wizard which can be used to configure security on the application server hosting the WebSphere Partner Gateway component applications. Any changes made using the wizard will require a server restart for the changes to take effect.

Configure WebSphere Application Server to use LDAP

The screenshot displays two steps of the Security Configuration wizard. Step 1, 'Specify extent of protection', shows the 'Enable application security' checkbox selected. Step 2, 'Select user repository', shows the 'Standalone LDAP registry' radio button selected. A yellow callout box points to the 'Standalone LDAP registry' option with the text: 'WebSphere Partner Gateway supports LDAP based authentication.' The wizard interface includes a progress indicator on the left, descriptive text on the right, and navigation buttons at the bottom.

Step 1: Specify extent of protection

This wizard assists you in securing your application serving environment. The application serving infrastructure can store administrative users and passwords or can use an existing registry with stored administrative users, application users, or both.

If you are using an existing registry such as the local operating system, LDAP, or a custom registry, you need the following information:

- Configuration information to connect to the existing registry
- An existing user name in the registry to act as the primary administrative user

At a minimum, this task provides for secure administration. However, administrative security alone does not provide full security. In most environments, it is recommended that you also enable application and resource security.

Enable application security

Use Java 2 security to restrict application access to local resources

Next Cancel

Step 2: Select user repository

The user account repository stores users and group names that are used for authentication and authorization. The default repository is built into the application serving system and can be federated with one or more external Lightweight Directory Access Protocol (LDAP) repositories. You can also select a standalone external repository.

Federated repositories

Standalone LDAP registry

Local operating system

Standalone custom registry

WebSphere Partner Gateway supports LDAP based authentication.

Previous Next Cancel

This slide shows the screen capture of the first two steps of the Security Configuration wizard. In the first step, select the option **Enable application security**. WebSphere Application server supports several user registries and repositories that you can use for authentication. WebSphere partner Gateway supports just the LDAP registry. You need to select the **Stand-alone LDAP** registry option in step two of the wizard.

Configure WebSphere Application Server to use LDAP

Configure user repository

The repository stores users and group names that are used for authentication. The application server infrastructure can register users and groups in the repository. To use the repository for authentication, provide the details of the repository that is in the repository.

Primary administrative user name: wasadmin

Type of LDAP server: IBM Tivoli Directory Server

Host: aimcp097.austin.ibm.com

Port: 389

Base distinguished name (DN): o=ibm,c=us

Bind distinguished name (DN): cn=root

Bind password: *****




Summary

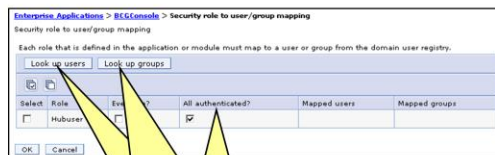
Displays the list of values that are selected during the wizard and are used to enable security.

Options	Values
Enable administrative security	true
Enable application security	true
Use Java 2 security to restrict application access to local resources	false
User repository	Standalone LDAP registry
Primary administrative user name	wasadmin
Type of LDAP server	IBM Tivoli Directory Server
Host	aimcp097.austin.ibm.com
Port	389
Base distinguished name (DN)	o=ibm,c=us
Bind distinguished name (DN)	cn=root
Bind password	*****

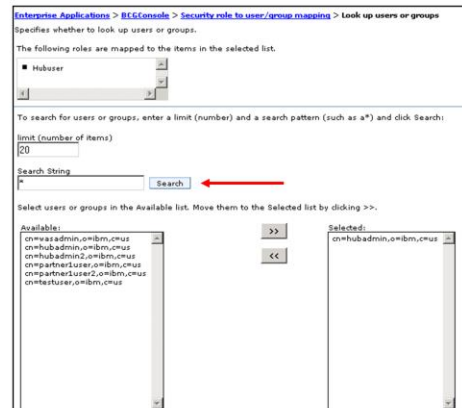
Once you choose to use LDAP registry for authentication, in step three, you would be prompted to provide details of the LDAP server instance and user information. For the Primary administrative username you would need to provide the name of the user you want to use as the administrator for WebSphere Application Server. The user you specify here should already be part of the LDAP registry. Select the Type of Directory Server from the list of options available in the dropdown menu. Port corresponds to the port on which the LDAP server instance is listening. For Base distinguished name, provide the base distinguished name (DN) of the directory service, which indicates the starting point for LDAP searches of the directory service. For Bind distinguished name (DN) and Bind password, provide the username and password of the user who has the privileges to lookup the user registry configured in the LDAP server.

Map users to security role

- Configure WebSphere Partner Gateway Console application user roles
 - ▶ Configured using WebSphere Administrative console
 - ▶ Applications  Enterprise Applications  BCGConsole 
Security role to user/group mapping



You can set all authenticated users to log into WebSphere Partner Gateway console or select specific users or groups



13

Security enhancements

© 2007 IBM Corporation

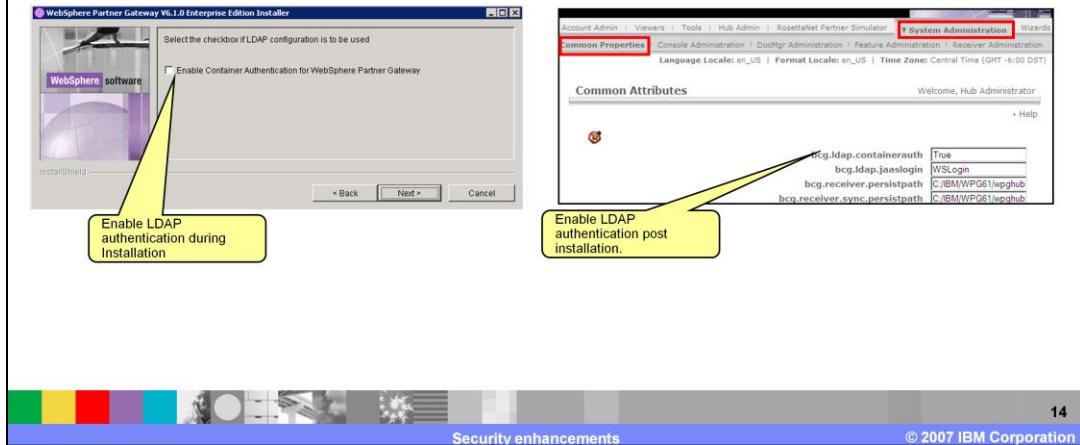
After authentication using LDAP server is setup for the WebSphere Application Server, you must associate the LDAP users with the Hubuser role of the WebSphere Partner Gateway BCGConsole application. Only users who are members of this role can enter the application after authentication. You can use the administrative console to specify the users and groups that are mapped to the security roles that are used with the enterprise application. This slide shows the screen captures from the WebSphere Application Server administrative console that show how to map the users.

When you map all authenticated users to a specified role, all of the valid users in the current registry who have been authenticated can access resources that are protected by this role. Look up users and Look up groups options enable the server to locate the users or groups that you can define for Hubuser role. Select the check box beside the role and click Look up users or Look up groups . Complete the Limit and the Search string fields. The Limit field contains the number of entries that the search function returns. The Search string field contains the search pattern used for searching entries. Move the users or groups that you want to assign the Hubuser role from the Available list to Selected list. Only users who are in the selected list will be members of this role can enter the application after authentication provided that they are also defined in the WebSphere Partner Gateway Community console.

Configure WebSphere Partner Gateway to use LDAP

How to configure WebSphere Partner Gateway to make use of LDAP?

- ▶ During installation
- ▶ Using the WebSphere Partner Gateway console

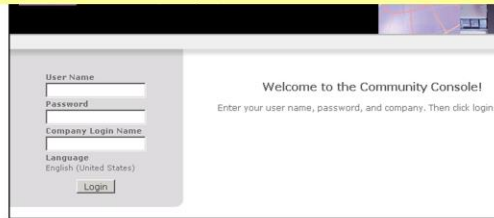


This slide provides details on enabling LDAP based authentication for WebSphere Partner Gateway. You have the option to configure WebSphere Partner Gateway to use LDAP based authentication during the installation. The screen capture is shown above. You can also configure LDAP based authentication by setting the `bcg.Idap.containerauth` flag to True . This flag can be set by navigating to System Administration ->Common Properties and clicking on the edit icon.

After you have enabled the authentication, users are authenticated against the LDAP server when logging into WebSphere Partner Gateway. When LDAP is enabled during the installation process, the administrator must ensure that the configured LDAP server is configured to include a user named hubadmin in its user registry (or repository).

LDAP authentication

WebSphere Partner Gateway Console with database authentication



The screenshot shows a login form for the WebSphere Partner Gateway Console using database authentication. The form is titled "Welcome to the Community Console!" and includes the following fields: "User Name", "Password", "Company Login Name", and "Language" (set to "English (United States)"). A "Login" button is located at the bottom of the form. The instructions below the fields read: "Enter your user name, password, and company. Then click login."

WebSphere Partner Gateway Console with LDAP authentication



The screenshot shows a login form for the WebSphere Partner Gateway Console using LDAP authentication. The form is titled "Welcome to the Community Console!" and includes the following fields: "User Name", "Password", and "Language" (set to "English (United States)"). A "Login" button is located at the bottom of the form. The instructions below the fields read: "Enter your user name and password. Then click login."

This slide shows the screen captures of the WebSphere Partner Gateway console application log in screen when using database authentication and LDAP based authentication. When LDAP based authentication is enabled, you are automatically re routed to a log in page which is different from the one shown when using database authentication.

LDAP authentication

- Features impacted by LDAP authentication support
 - ▶ Multiple hubadmin users
 - ▶ Unique user names among partners
 - ▶ Web service inbound authentication
 - Document manager makes use of container based authentication

Some of the features supported in WebSphere Partner Gateway V6.0 are modified and enhanced to support the LDAP based authentication in V6.1. Multiple hubadmin users can now be created. Users created for partners require the usage of unique user name. Document manager makes use of the container based authentication instead of database based authentication when LDAP based authentication is enabled for the WebSphere Partner Gateway.

Multiple hubadmin users

- Multiple hubadmin users
 - ▶ WebSphere Partner Gateway V6.0 supports single hubadmin user
 - ▶ WebSphere Partner Gateway V6.1 introduces groups enabling multiple hubadmin users
 - Log in as hubadmin
 - Create new user for Hub Operator
 - Add user to Hubadmin group
 - Newly added Hubadmin users should exist in LDAP registry when LDAP based authentication enabled

Profile > Hub Operator > User List		
	User Name	Full Name
 	Admin	Administrator for Hub Operator
 	hubadmin	Hub Administrator
 	hubadmin2	hubadmin2

In WebSphere Partner Gateway V6.0, the community can have one hubadmin user and the hubadmin is created by default during installation. The hubadmin password has to be shared among users who want to log into the community console as the super user. With V6.1 you can now log into the community console using your single sign on credentials when LDAP is used and so passwords cannot be shared among users since you use the same credentials to log into several applications. WebSphere Partner Gateway V6.1 supports the creation of multiple hubadmin users. You can log in as the default hubadmin user created during installation, create a new user and make him a member of the Hubadmin group. When LDAP based authentication is enabled, make sure that the newly created user is also part of the LDAP user registry.

Unique users

- Unique user names among partners
 - ▶ WebSphere Partner Gateway V6.0 supports non unique users among partners
 - ▶ WebSphere Partner Gateway V6.1 introduces LDAP based authentication, so users for partners need to be unique
 - ▶ Non unique user names in migrated WebSphere Partner Gateway instances marked with **
 - ▶ Admin user automatically created and added to Administrators group for Partners in WebSphere Partner Gateway V6.0
 - ▶ WebSphere Partner Gateway V6.1 gives user the option to specify admin user during partner creation

18

Security enhancements

© 2007 IBM Corporation

In WebSphere Partner Gateway V6.0, a user created for one partner can use the same user name of an user created for another partner. But with V6.1 all the users created must have a unique user name. This restriction is true when using database based authentication or LDAP based authentication. If you are migrating from V6.0 to V6.1 the non unique user names are marked with a double asterisks (**). You would need to modify the user names to make them unique.

In V6.0 when you create a participant, a admin user is automatically created by default for the participant. But in V6.1 you will be asked to enter the Admin User Name . This option is useful when you have LDAP based authentication enabled. This allows you to specify a user that is part of the user registry as administrator than have the default user named Admin automatically created for you in V6.0 who may not be part of your LDAP user registry.

Section

Disable container managed authentication

The next section covers the details on how to disable container based authentication for WebSphere Partner Gateway and WebSphere Application Server.

Disable LDAP based authentication

- Disable LDAP authentication in WebSphere Partner Gateway
 - ▶ LDAP Server stops or permanently goes down
 - ▶ LDAP authentication chosen during install but LDAP server not ready
 - ▶ Use the script `bcgResetAuthentication.bat/.sh`
 - On UNIX environment run script logged in as db2instance user or Oracle user based on database used
 - Located under `<dbloader_install_path>/scripts/<database_type>`
 - Script takes database schema user name and password as input parameters
example: `bcgResetAuthentication.bat db2admin db2admin`
 - Resets `bcg.ldap.containerauth` property to false
 - Resets hubadmin user name password to installation default

Note: After these scripts are run, any passwords that were configured in LDAP must be reentered for each defined user using the WebSphere Partner Gateway Console

You might have to stop LDAP authentication under the following circumstances:

The LDAP server stops or permanently goes down or container based authentication was chosen when installing WebSphere Partner Gateway but the LDAP server is not ready.

To stop WebSphere Partner Gateway from using LDAP for accessing passwords and instead use the WebSphere Partner Gateway database to store passwords, run the `bcgResetAuthentication.bat` or `bcgResetAuthentication.sh` script located under your application database scripts.

This script requires the database schema owner user name and password to connect to the WebSphere Partner Gateway database. If you are using a DB2 database, start the script from a DB2 command line. This script is located in the `{dbloader install location}/scripts/{database type}` directory. This script Sets the attribute `bcg.ldap.containerauth` to False and resets the hubadmin user name password to the installation default and the database is now used to store passwords.

After these scripts are run, any passwords that were configured in LDAP must be reentered for each defined user using the WebSphere Partner Gateway Console.

UNIX users who use DB2 must log in as the db2instance user and use the db2instance username and password to run the script. UNIX users who use Oracle must log in as the oracle user and use the username and password given at the time of installation to run the script.

Disable LDAP based authentication

- Use wsadmin to disable security
 - ▶ wsadmin conntype NONE
 - ▶ securityoff
- Restart WebSphere Application Server
 - ▶ Need to provide username and password while stopping server

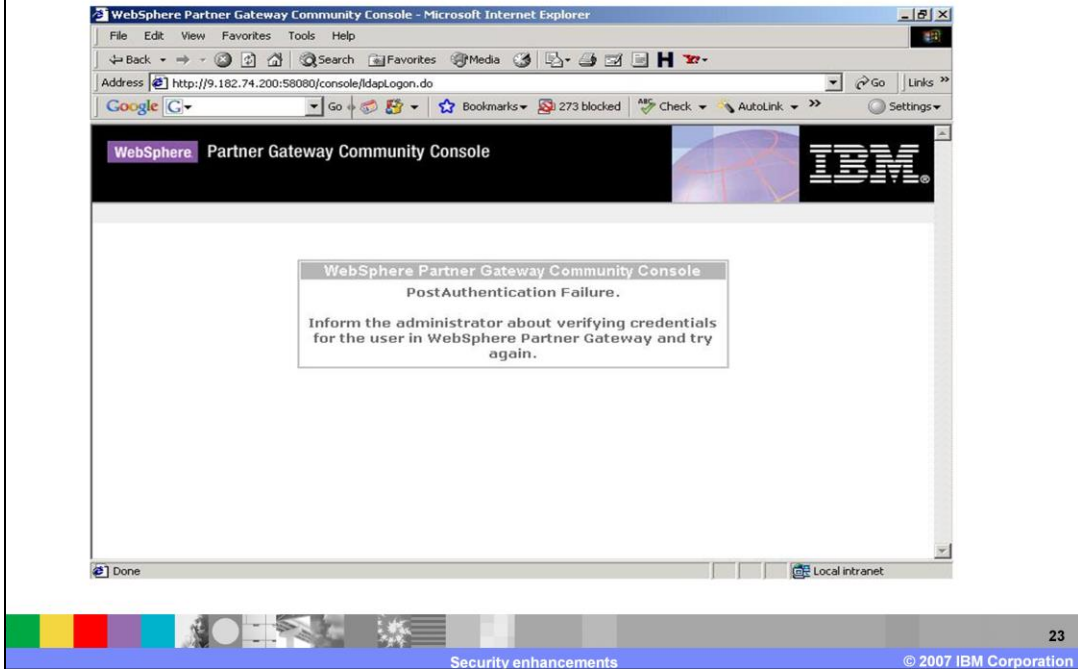
You can make use of the wsadmin scripting client to disable security for WebSphere Application Server. The server needs to be restarted in order for the changes to take effect.

Section

Best practices and problem determination

The next section covers the best practices and problem determination.

Problem determination



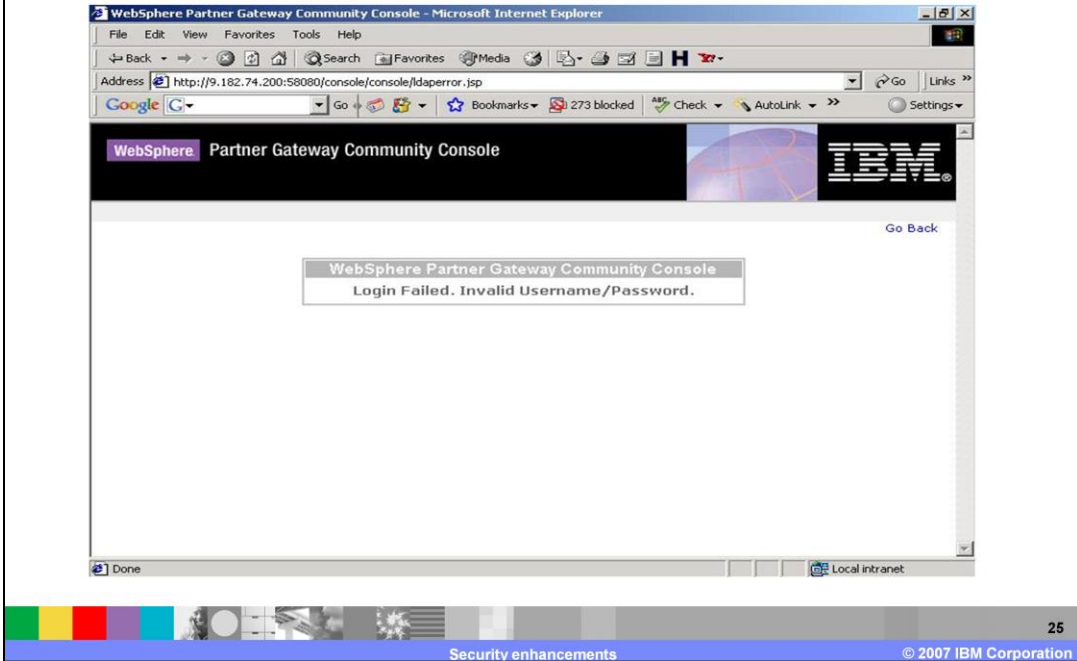
You would see the error shown in the screen capture shown in the slide if the LDAP authentication is successful, but the username is not present in WebSphere Partner Gateway. The solution is to disable LDAP authentication using the `bcgResetAuthentication` script provided with installation and then login into WebSphere Partner Gateway and create a user with the same name in the Tivoli LDAP server. Enable LDAP authentication on WebSphere Partner Gateway and login successfully.

Problem determination



You would see the error shown in the screen capture shown in the slide if the LDAP server is stopped (or not started) or if the WebSphere Application Server Network Deployment is not configured for LDAP server. The solution is to check whether the LDAP server is up and check whether there are any connectivity issues between system hosting the WebSphere Partner Gateway and the system hosting the LDAP server. If the LDAP server is not stopped and if there are no connectivity issues, then WebSphere Application Server Network Deployment may not have been configured for security using LDAP. In that scenario, disable LDAP authentication using the `bcgResetAuthentication` script provided with installation and then configure the application server security to use LDAP user registry. Enable LDAP authentication on WebSphere Partner Gateway and login successfully

Problem determination



You would see the error shown in the screen capture shown in the slide if you provided a wrong username or password.

Section

Summary and references

The next section provides the summary and references.

Summary

- This presentation covered details on
 - ▶ Container based authentication using LDAP user repository
 - ▶ Multiple hubadmin user support
 - ▶ Unique user names among partners
 - ▶ Disabling security
 - References
 - ▶ WebSphere Partner Gateway Administration Guide
 - ▶ Refer to the following link for list of LDAP servers supported
- <http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg27007642>



WebSphere Partner Gateway V6.1 supports the usage of LDAP user registry for authentication. Multiple hubadmin users can now be created and any user created for partners need to have unique user name. For a list of supported LDAP servers, refer to the link listed in the slide.

Trademarks, copyrights, and disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM WebSphere

UNIX is a registered trademark of The Open Group in the United States and other countries.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements or changes in the products or programs described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (for example, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.

IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

© Copyright International Business Machines Corporation 2007. All rights reserved.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.