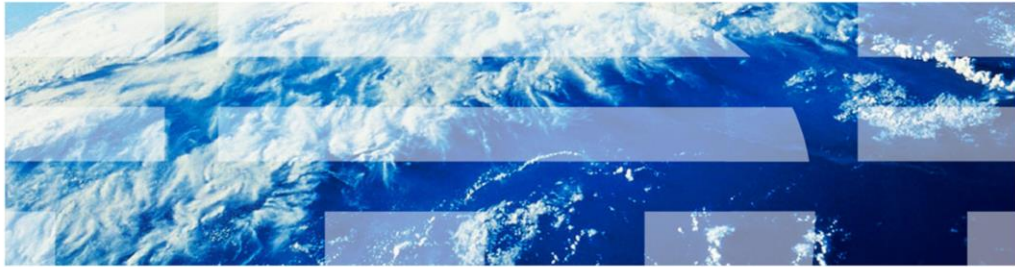


IBM WebSphere Application Server V7.0.0.23

Certificate login in VMM file repository



© 2012 IBM Corporation

This presentation describes support for certificate login in the virtual member manager file repository that is included in IBM WebSphere® Application Server V7.0.0.23

Certificate login in the VMM file repository

- Before 7.0.0.23, VMM supports certificate login but support is limited to LDAP and UR Bridge
- As part of this feature you can enable the certificate login support for a file repository.
- This feature is not enabled by default, but can be configured
- certificateMapMode values:
 - exactDN
 - filterDescriptorMode
 - notSupported

Before 7.0.0.23, the virtual member manager supports certificate login only for LDAP and UR Bridge. Additionally, in the case of UR Bridge, the support is only available if the underlying repository supports certificate login. This feature extends the support of certificate login to include the file repository.

For compatibility with earlier versions, the default behavior is for the file repository to ignore certificate login requests. You can configure the VMM to enable this new support. As shown here, two new custom properties are added: `certificateMapMode` and `certificateFilter`.

With changes introduced in 7.0.0.23, the file adapter component's login behavior is now dependent on a custom property: `certificateMapMode`.

If the custom property `certificateMapMode` is not defined, the file adapter returns an empty result for certificate login. This is also the default behavior of the file adapter before 7.0.0.23.

If `certificateMapMode` is set to `exactDN`, the certificate login is mapped to the distinguished name.

If `certificateMapMode` is set to `filterDescriptorMode`, mapping occurs using the `certificateFilter` custom property.

If `certificateMapMode` is set to `notSupported`, the feature creates `CertificateMapNotSupportedException`. This is a new property value to support behavior before 7.0.0.19.

If `certificateMapMode` is set to an not valid value, an error is logged during adapter initialization and an empty result is returned at runtime.

Usage scenarios

This feature is used in the scenarios shown in the next few slides.

Default behavior

- Ignore certificate login requests.
- Requests are either processed by other configured repositories or the if no repositories are configured that support certificate login, the login attempt fails.

If custom property “certificateMapMode” is not defined, then all certificate log in requests are ignored by the file repository adapter.

In a multiple repository configuration, the VMM tries to log in the user against all configured repositories. After the file repository ignores the request, the VMM proceeds to attempt to log in the user to the next configured repository, for example an LDAP repository. If the log in attempt to the repository is successful, the log in attempt is successful. If the log in attempt to the other repository fails, the log in attempt fails. Details of exceptions encountered in a multiple repository scenario are listed on following slides.

In the case of a single repository the login attempt fails, as the file repository ignores the login request.

Disabled certificate login support

- Certificate login requests fail with a `CertificateMapNotSupportedException`.
- **`$AdminTask setIdMgrCustomProperty { -id InternalFileRepository -name certificateMapMode -value notSupported }`**

If you add the custom property, `certificateMapMode`, and set the value to “notSupported”, the File repository adapter is configured to fail all certificate login attempts.

Any attempt to perform a certificate login will result in a `CertificateMapNotSupportedException` thrown by the file repository adapter.

If the VMM is configured with only one file repository, a `CertificateMapNotSupportedException` is created.

If the VMM is configured with more than one repository, a `CertificateMapFailedException` is created.

Enabled certificate login support

- Certificate login requests can be configured in two modes.
- **\$AdminTask setIdMgrCustomProperty { -id InternalFileRepository -name certificateMapMode -value <<mode>> }**
- If certificateMapMode = exactDN
 - File adapter extracts the PrincipalName from the certificate
 - The adapter tries to find the principal name in the file repository as the exact DN
 - Matching entity found - login is successful
 - No matching entity found - EntityNotFoundException
 - Handled by the Profile Manager
 - Error message displayed
- If certificateMapMode = filterDescriptorMode
 - The file adapter extract the filter specified in the “certificateFilter” custom property
 - The adapter tries to find an entity matching the filter specified.
 - Single matching entity found - login is successful
 - More than one matching entities are found – multiple principles found exception

The certificate login enabled mode for the file repository is similar to the certificate login in an LDAP repository.

Certificate login can be used in two modes.

When the certificateMapMode is set to “exactDN”, the file adapter extracts the PrincipalName from the certificate. The adapter tries to find the principal name in the file repository as the exact distinguished name. If a matching entity is found, the login is successful. If a matching entity is not found, the adapter throws an EntityNotFoundException exception. This is handled by the Profile Manager and an appropriate error message is displayed.

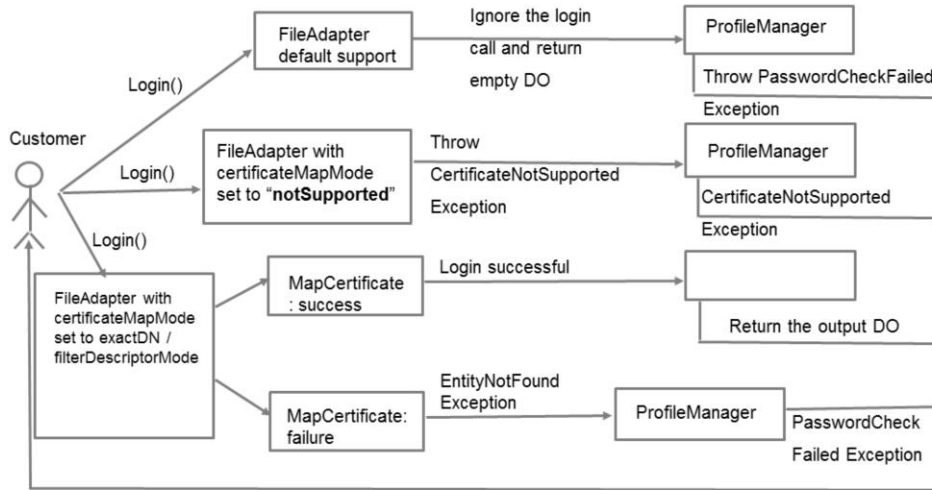
When the certificateMapMode is set to “filterDescriptorMode”, the file adapter extracts the filter specified in the “certificateFilter” custom property. The adapter tries to find an entity matching the filter specified. If a single matching entity is found, the login is successful. If more than one matching entities are found, the adapter throws a multiple principals found exception.

Examples

- `cn='${IssuerCN}'`
 - searches for a user whose CN has the value specified by the IssuerCN property of the certificate.
- `cn='${IssuerCN}' and mobile=${SerialNumber}`
 - searches for a user whose CN has the value specified by the IssuerCN property of the certificate and whose mobile equals the SerialNumber property of the certificate.
- The expression requires quotation marks around string properties.

This slide shows sample expressions. Note that these expressions require quotation marks around any string properties.

Single repository scenario



This diagram shows the various modes of usage and their possible outputs.

Multiple repository scenario

- Multiple repository setup exceptions

Repository 1 behavior	Repository 2 behavior	Behavior seen by the User
Certificate Login successful / Certificate Login not successful	CertificateMapNotSupportedException	CertificateMapFailedException
CertificateMapNotSupportedException	CertificateMapNotSupportedException	CertificateMapNotSupportedException
Certificate Login successful	EntityNotFoundException	Certificate Login successful
Certificate Login successful	Certificate Login request ignored	Certificate Login successful
EntityNotFoundException	Certificate Login request ignored	PasswordCheckFailedException
EntityNotFoundException	EntityNotFoundException	PasswordCheckFailedException
Certificate Login successful	Certificate Login successful	DuplicateLogonIdException

This table lists the different exceptions encountered in multiple repository configuration.

Summary

In summary.

Summary

- Addition of certificate login support for file repository.
- Various modes of operations
 - Ignore
 - notSupported
 - exactDN
 - filterDescriptorMode

This feature extends certificate login support to include the file repository.

Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, 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>

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 2012. All rights reserved.