ibm.com

Powerful and secure infrastructures with WebSphere Application Server for z/OS

The security side of Application Migration

Redbooks

International Technical
Support Organization

Holger Wunderlich / wunderl@us.ibm.com

Notices

This information was developed for products and services offered in the U.S.A.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

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 and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Trademarks

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

Affinity™
AIX®
CICS®
DB2®
@server™
eServer™
Everyplace™
IBM®
IMS™

IMS/ESA®
MQSeries®
MVS™
MVS/ESA™
Notes®
OS/2®
OS/390®
Parallel Sysplex®
Redbooks™

Redbooks(logo)™
RACF®
S/390®
SecureWay®
SOM®
Tivoli®
WebSphere®
z/OS™
zSeries™

The following terms are trademarks of other companies:

Intel, Intel Inside (logos), MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

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

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

SET, SET Secure Electronic Transaction, and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

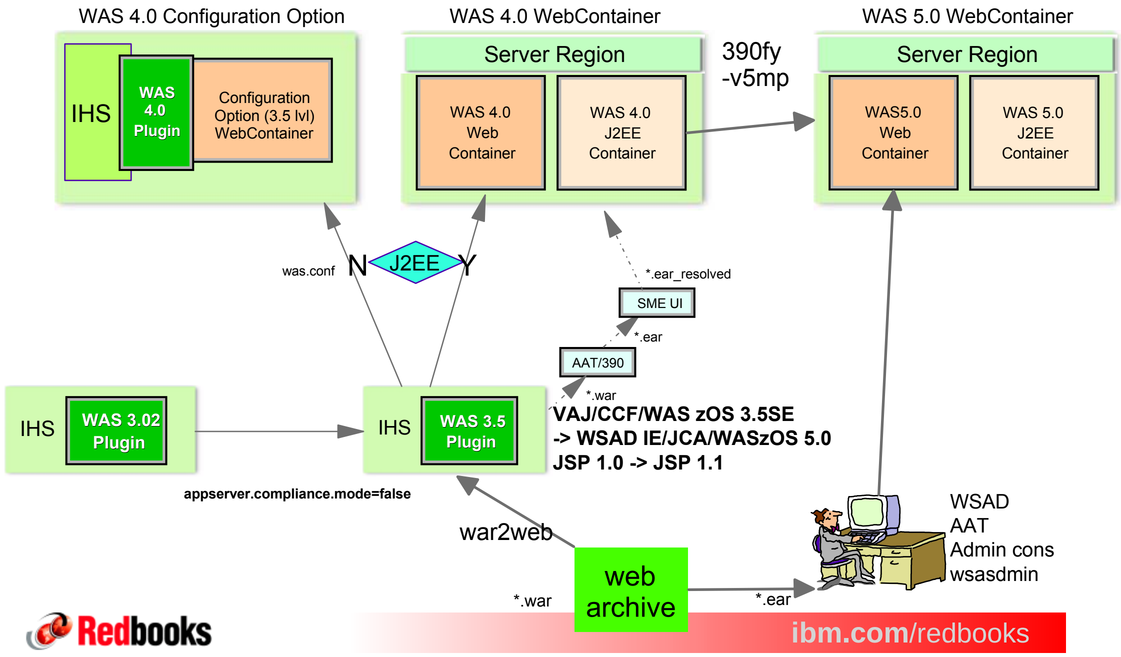
Other company, product, and service names may be trademarks or service marks of others.

Objectives

Security Aspects when migrating WebSphere Applications

- Overview
- Affected Environments
- Most likely problems
- Strategies
- Summary

Migrating WebApps to WebSphere 5



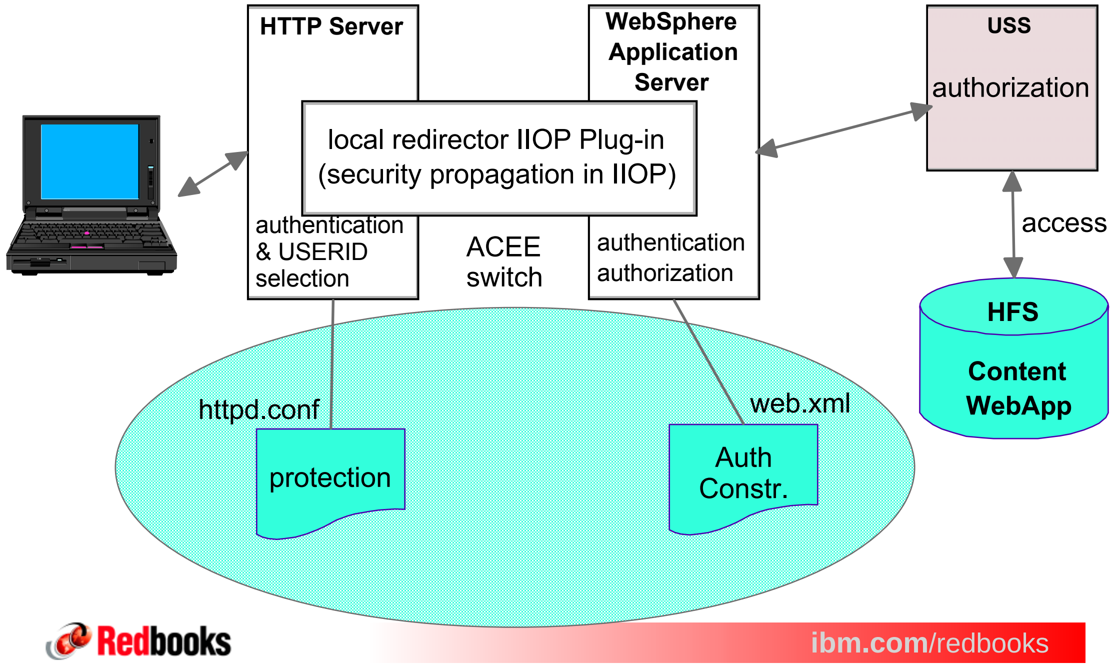
Generic migration tips

- get WebSphere migration handbook
  - generic: http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg246910.pdf
  - z/OS: Redpiece will be available soon, contact Tamas Vilaghy, Poughkeepsie
  - use 390fy tool -v5mp option for quick migration from 4.01 to 5.. (Note that only the "new" version of the 390fy tool provides the -v5mp option. The "new" 390fy tool is included in level W401502 for WebSphere Application Server 4.0.1 for z/OS
- **The Class API Checker Tool (CACT)** can be used to analyze servlets and EJBs to determine if they contain any unsupported or deprecated APIs.
  - http://www7b.software.ibm.com/wsdd/library/techarticles/0208_cocasse/0208_cocasse.html
- Migrate servlets to API 2.2 and JSP 1.1, with the MigrateWC tool
  - http://www-1.ibm.com/support/docview.wss?uid=swg24001150
- **Changes SERVER class profiles from**
  - <subsys_type>.<subsys_name>.<appl_envir_name> to ..
  - <subsys_type>.<subsys_name>.<appl_envir_name>.<cell_name>

Affected Environments

- ➤Applications using the local redirector together with IHS protection
- ➤Applications using the simple config option
- ➤Applications running in IBM HTTP Server address space
- ➤Applications who's security is based on IHS protection setups
- ➤Applications based on IHS password file capability
- ➤Applications that use SOMDOBJS
- ➤Applications that use sync2thread
- ➤Applications that use CCF connectors
- ➤Applications that use unmanaged threads

Security Migration Problem: protection setups and redirector plug-in


HTTP Server
WebSphere Application Server
USS
authorization
local redirector IIOP Plug-in (security propagation in IIOP)
authentication & USERID selection
ACEE switch
authentication authorization
access
HFS
Content WebApp
httpd.conf
protection
web.xml
Auth Constr.

What are the reasons?

WAS3 SOMDOBJS is no longer supported in WAS4 and higher

WAS4 local redirector is no longer available

WAS4 simple config option is no longer available

WAS5 never switches is ACEE

WAS5 TH does not support password files

WAS4 and higher don't support CCF connectors

WAS5 does no longer support sync2

Strategies

Migrate to J2EE 1.3

Migrate password files to RACF or CUR

Migrate cleanly from local redirector to HTTP plug-in

If using surrogate users RunAS Role might be the solution

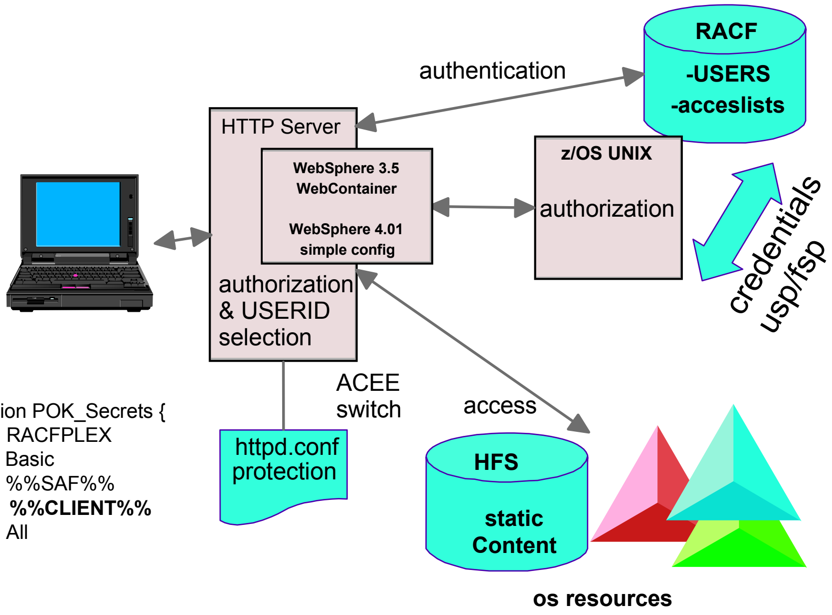
Migrate SOMDOBJS to EJBROLES

Migrate CCF connectors to JCA

Thread level based problems:

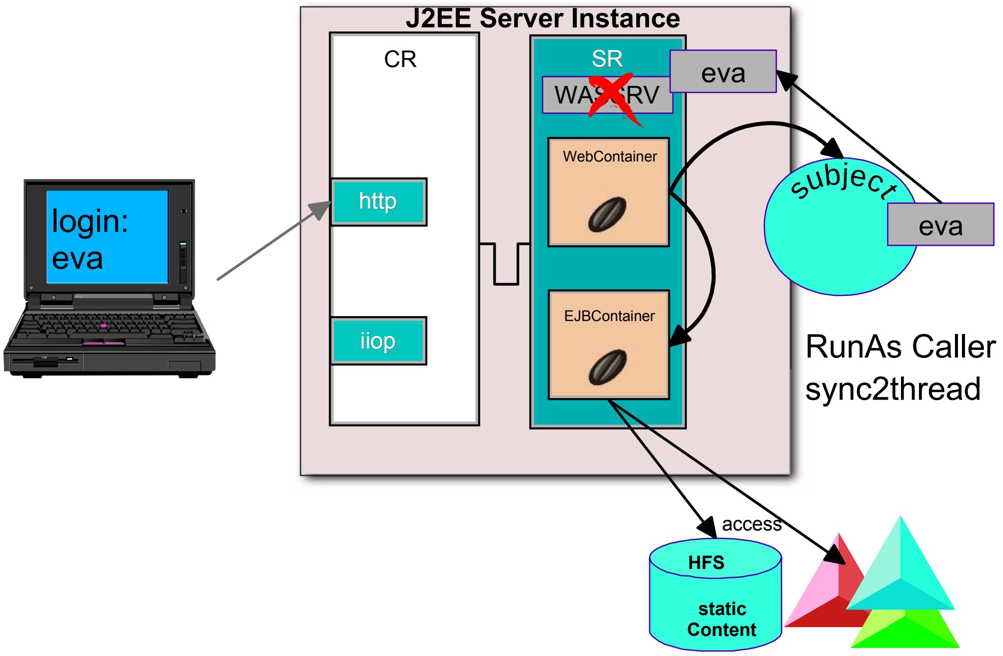
- Avoid sync2thread options
- Avoid thread level based security
- If not possible a solution needs to be architected

TLS Problem No1:
Protection setup based os resource access



```
Example: Protection POK_Secrets {
        ServerId      RACFPLEX
        AuthType      Basic
        PasswdFile  %%SAF%%
        Userid          %%CLIENT%%
        Mask            All
}
```

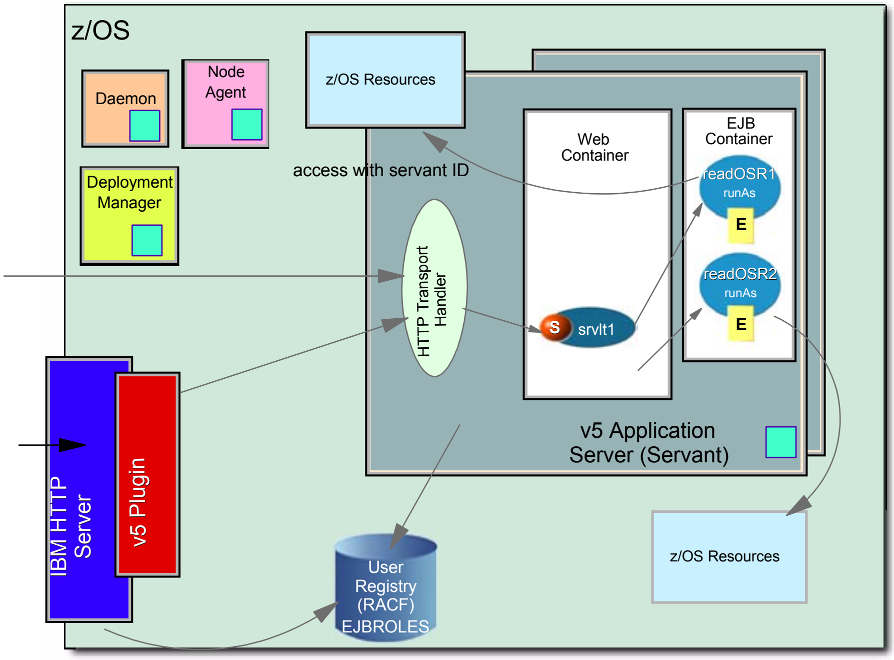
TLS Problem No2:
Protection setup based os resource access



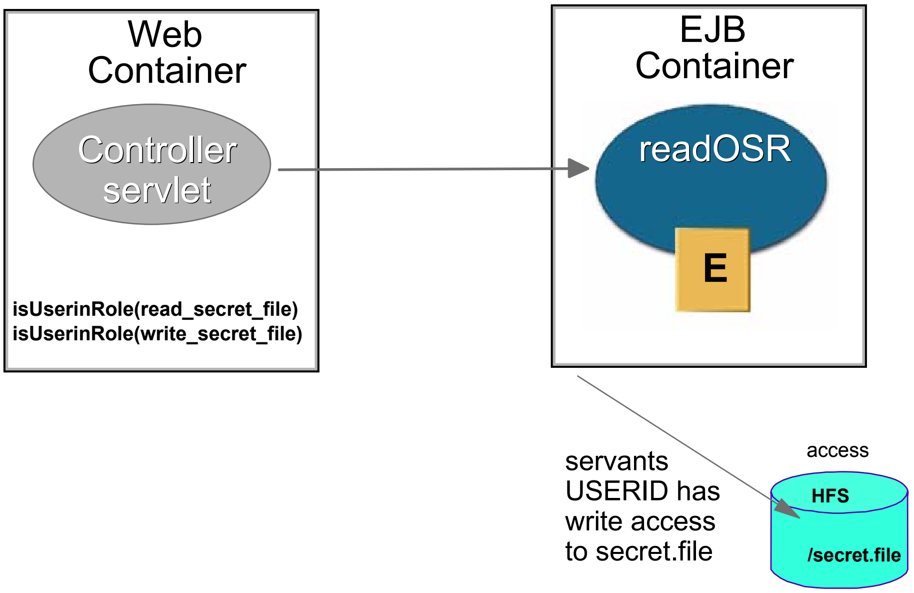
Strategies if ACEE based security is a problem

- Wait for sync2thread (not recommended)
- Wait for simple config (not recommended)
- Map OS resources to J2EE methods and protect the method
- Use JAVA2 security
- Use a authorization engine (J2EE server that does RACHECKS)
- Use a access engine (URL called from WebApp)

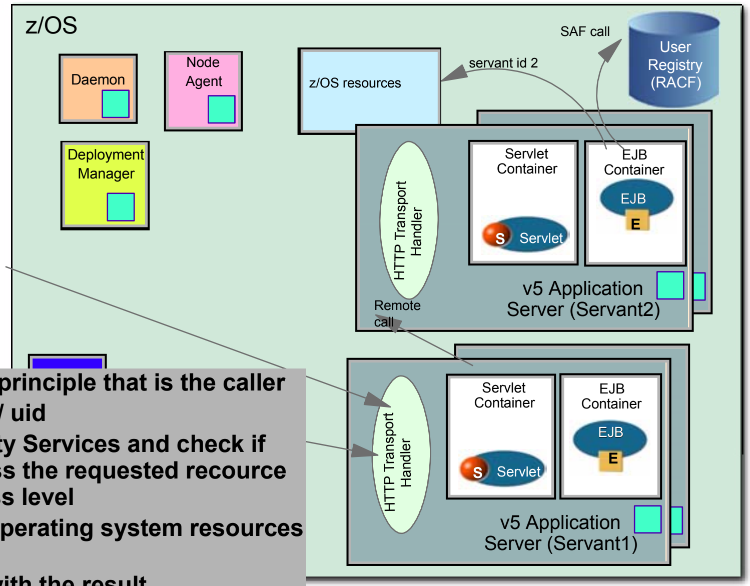
TLS Problems
Solution Strategies: declarative



TLS Problems
Solution Strategies: programmatic

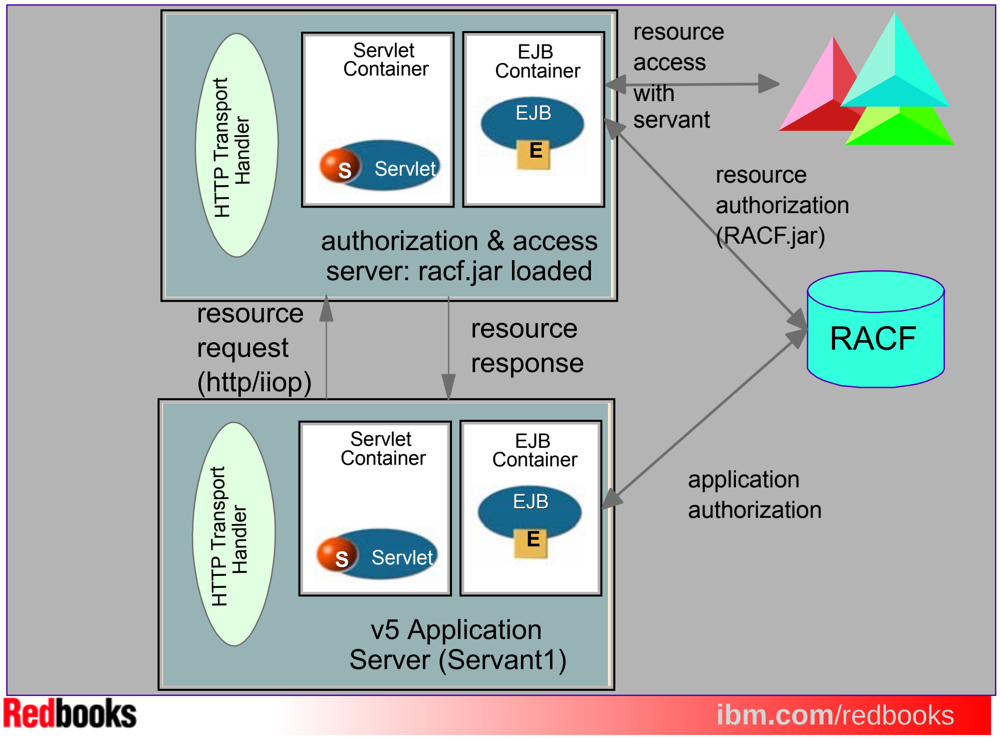

Web Container
Controller servlet
isUserinRole(read_secret_file)
isUserinRole(write_secret_file)
EJB Container
readOSR
E
servants USERID has write access to secret.file
access
HFS
/secret.file

TLS Problems
Solution Strategies: authorization engine



- **establish on server2 the principle that is the caller**
- **Get the matching userid / uid**
- **call Java for z/OS Security Services and check if caller is allowed to access the requested recource with the requested access level**
- **if allowed, access z/OS operating system resources with servants userid**
- **return from remote call with the result**

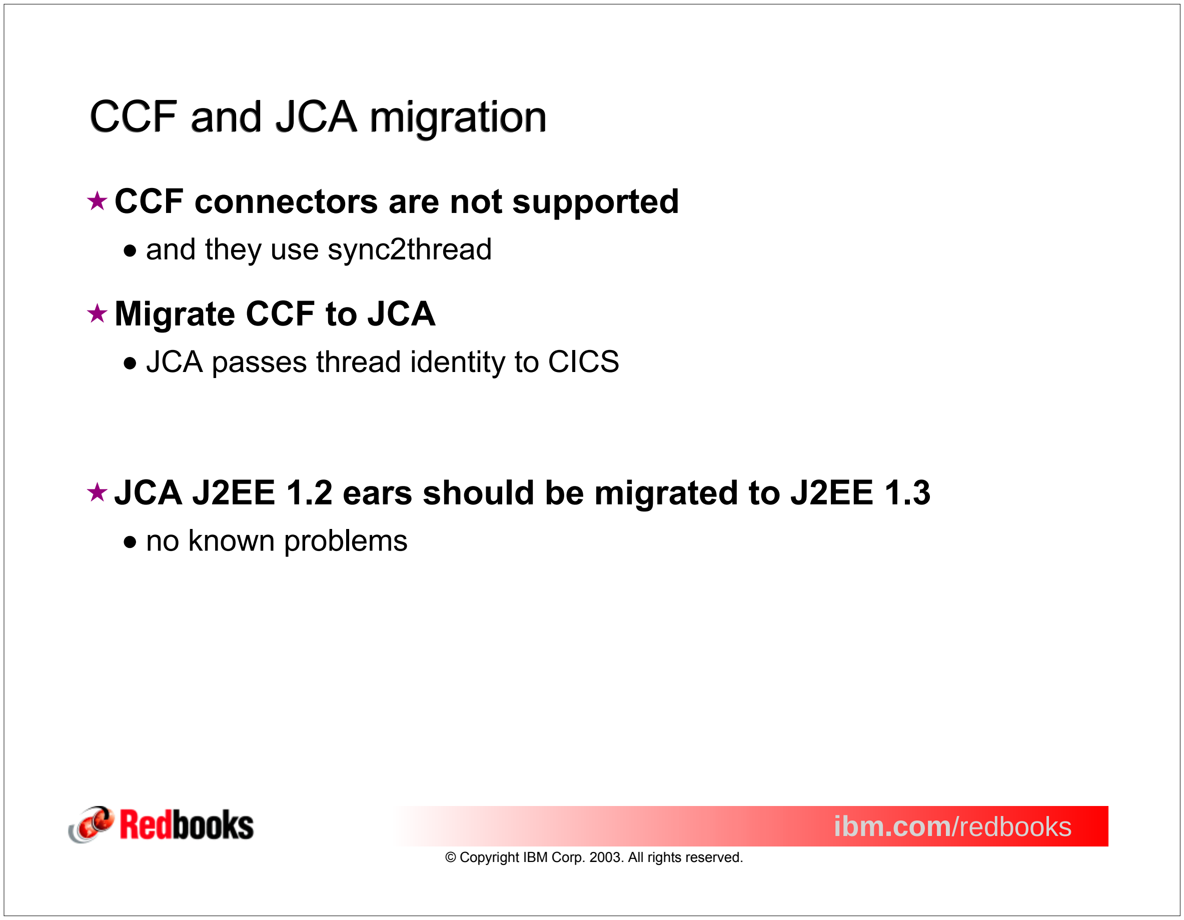
TLS Problems
Solution Strategies: authorization engine


HTTP Transport Handler
Servlet Container
S Servlet
EJB Container
EJB
E
authorization & access server: racf.jar loaded
resource access with servant
resource authorization (RACF.jar)
RACF
resource request (http/iiop)
resource response
HTTP Transport Handler
Servlet Container
S Servlet
EJB Container
EJB
E
v5 Application Server (Servant1)
application authorization

TLS Problems
Solution Strategies: Java2 and JAAS

Update was.policy (part of the .ear)

```
grant codeBase "file:readHFSWeb.war",
   Principal com.ibm.ws.security.common.auth.WS390Principal “WAS5/paul”
   {
   permission java.io.FilePermission "secret.file"."read";
   };
```



CCF and JCA migration

- ★ **CCF connectors are not supported**
  - and they use sync2thread
- ★ **Migrate CCF to JCA**
  - JCA passes thread identity to CICS
- ★ **JCA J2EE 1.2 ears should be migrated to J2EE 1.3**
  - no known problems