IBM Software Group

Ask the Experts

WebSphere Application Server V8 Security Concepts

31 July 2014

WebSphere® Support Technical Exchange

ON DEMAND BUSINESS™

Agenda

- Introduce the panel of experts
- Introduce WebSphere Application Server Security Concepts Topics
- Answer 5 questions submitted by the panel
- Open telephone lines for questions
- Summarize highlights

Panel of Experts

Panelist	Role at IBM
Varun Tallapragada varunt@us.ibm.com	Varun has been in WebSphere Application Server support since Feb 2006. He is responsible for solving customer problems related to WebSphere Application Server, with specialization in various components including Dynamic caching, Session management, Webcontainer, JSP™, JSF™, ClassLoader, SIP and Security.
Bill Holtzhauser wrh@us.ibm.com	Bill Holtzhauser has been involved with support in IBM for over 20 years and in WebSphere Application Server Level 2 support since 2003 working on multiple teams, currently he is on the security team.
Ajit Jariwala jariwala@us.ibm.com	Ajit has been in WebSphere Application Server support since 2000. He is responsible for solving customer problems related to WebSphere Application Server, with specialization in various components including Securiy, Dynamic caching, Session management, Webcontainer, JSP, JSF and ClassLoader, System Management.

Introduction

- We will be covering a number of questions that cover various WebSphere Application Server V8 Security Topics :

  - Dynamic Outbound SSL configuration
  - Java™ 2 security
  - Cross cell communication
  - LTPA

- Platforms covered will include 7.0, 8.0, 8.5 and 8.5.5

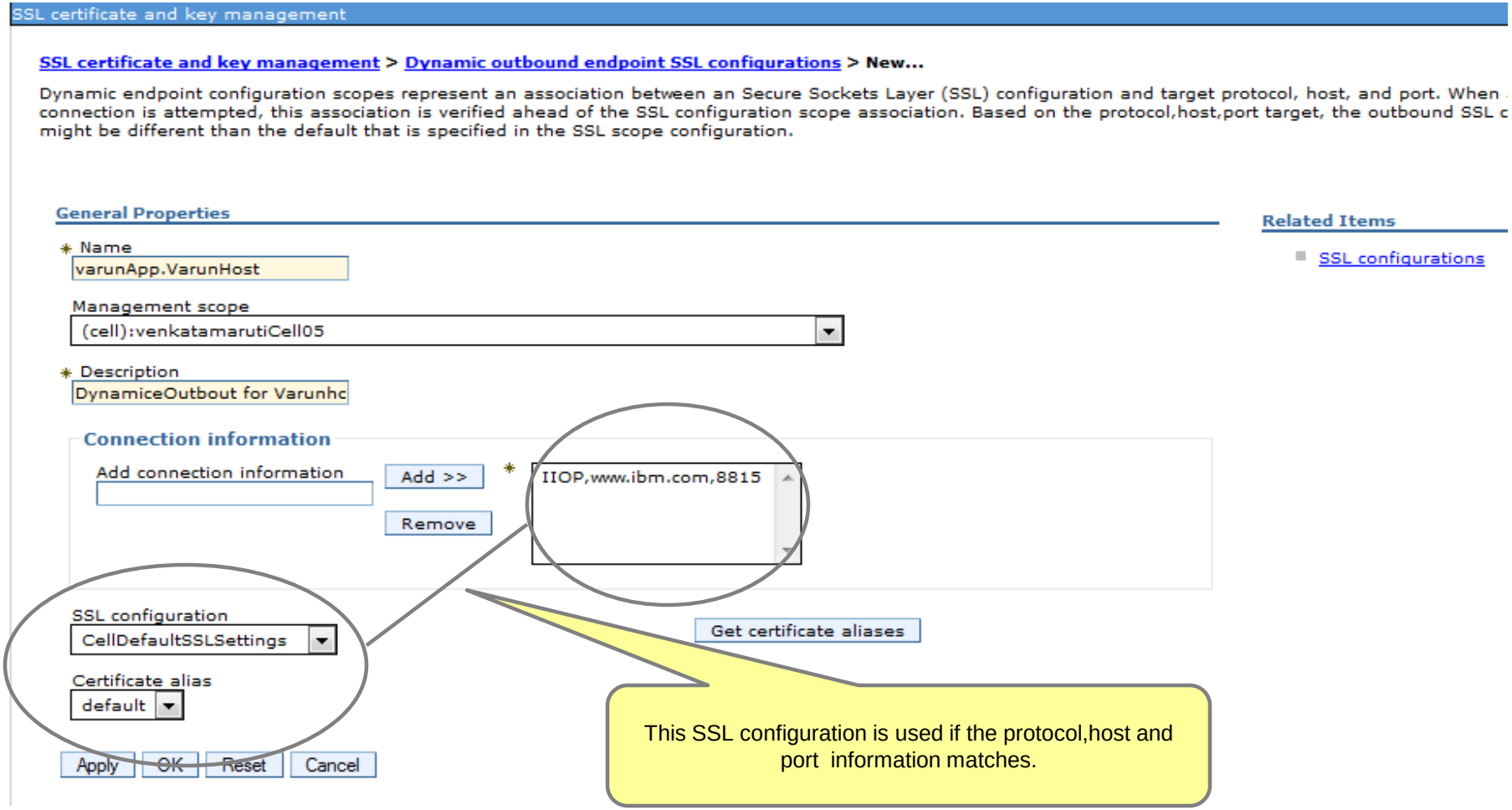
Question 1

- What is Dynamic Out bound SSL and How to configure Dynamic Out bound SSL?

Dynamic Outbound SSL

- Used in certain scenarios where the static SSL configuration for a given end point is not sufficient to meet the requirements for a particular connection
- If one wants different SSL configurations for different hosts eg: www.ibm.com and www.bankofamerica.com then Dynamic Outbound SSL configuration is the good option.
- Ability to associate an SSL configuration dynamically by predefined selection of a specific target host, port, or outbound protocol
- WebSphere checks to see if the target host and port match a predefined criteria that includes the domain portion of the host
- Ability to predefine the protocol for a specific outbound SSL configuration and certificate alias selection
- When the selection of an SSL configuration occurs for a particular outbound connection using the JSSEHelper API, the connection information passed into the API is used to check the selection criteria to determine if a match is made

Dynamic Outbound SSL Configuration



Question 2

- What policy files are used by Java 2 security in WebSphere Application Server?

What policy files are used by Java 2 security in WSAS?

- java.policy
- server.policy
- spi.policy
- app.policy*
- library.policy
- was.policy* (in EAR META-INF)
- ra.xml

* Most commonly edited policy files

When Java 2 security is enabled in WSAS, by default what is restricted?

- WSAS gives itself any permission it needs to function.
- EJBs have no filesystem access
- Servlets have access to files in the WAR
- API calls like getUserPrincipal() are blocked
- Java 2 security protects WSAS from apps and apps from each other

Question 3

- What variables can be used in was.policy and app.policy?

What variables can be used in was.policy and app.policy?

- ${app.installed.path} - application install location
- ${was.module.path} - module install location
- ${current.cell.name} - Current cell
- ${current.node.name} - Current node
- ${current.server.name} - Current server name
- Policy files can also use JVM system variables

Example: WSAS etc directory

${user.install.root}/etc/

Question 4

- Cross Cell Single Sign-On (SSO) common scenarios and what is best practice for cross cell SSO settings?

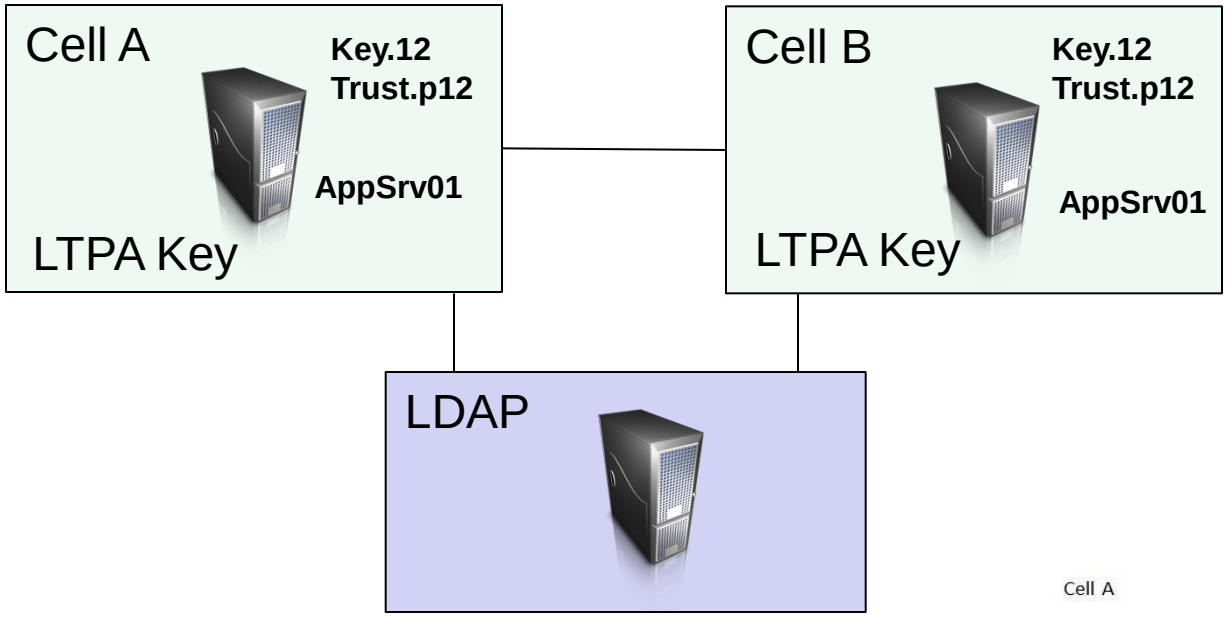
Common Secure Interoperability Version 2 (CSIv2) inbound and outbound configuration settings.

- Identify how to configure inbound and outbound in your topology
- Specify the type of authentication
  - By default, authentication by a user id and password is performed – basic
  - By default, Java client certificate authentication and Identity assertion are disabled
- Configure clients and servers
  - Two options
    - Define at CSIv2 inbound or outbound configuration at Global Level
    - Define at CSIv2 inbound or outbound configuration at Security Domain level – security attribute with specific JVM scope

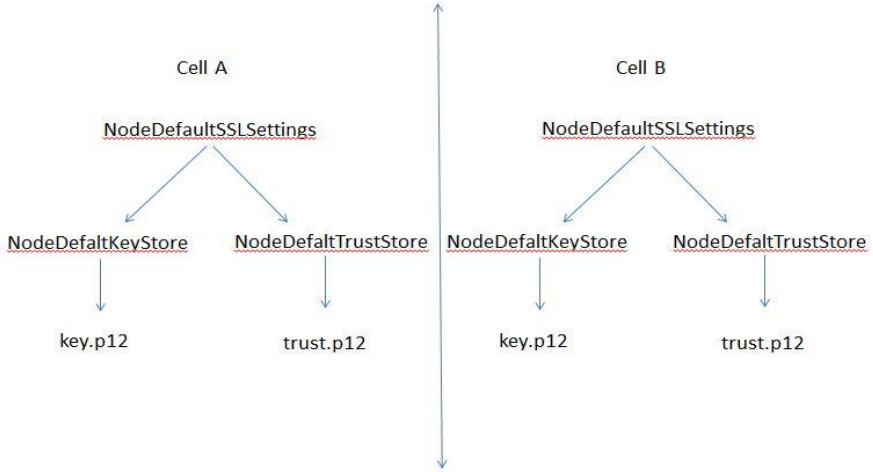
IBM Knowledge Center

http://www.ibm.com/support/knowledgecenter/SSAW57_7.0.0/com.ibm.websphere.nd.doc/info/ae/ae/tsec_configiiopauth.html?cp=SSAW57_7.0.0%2F1-8-30-2-14&lang=en

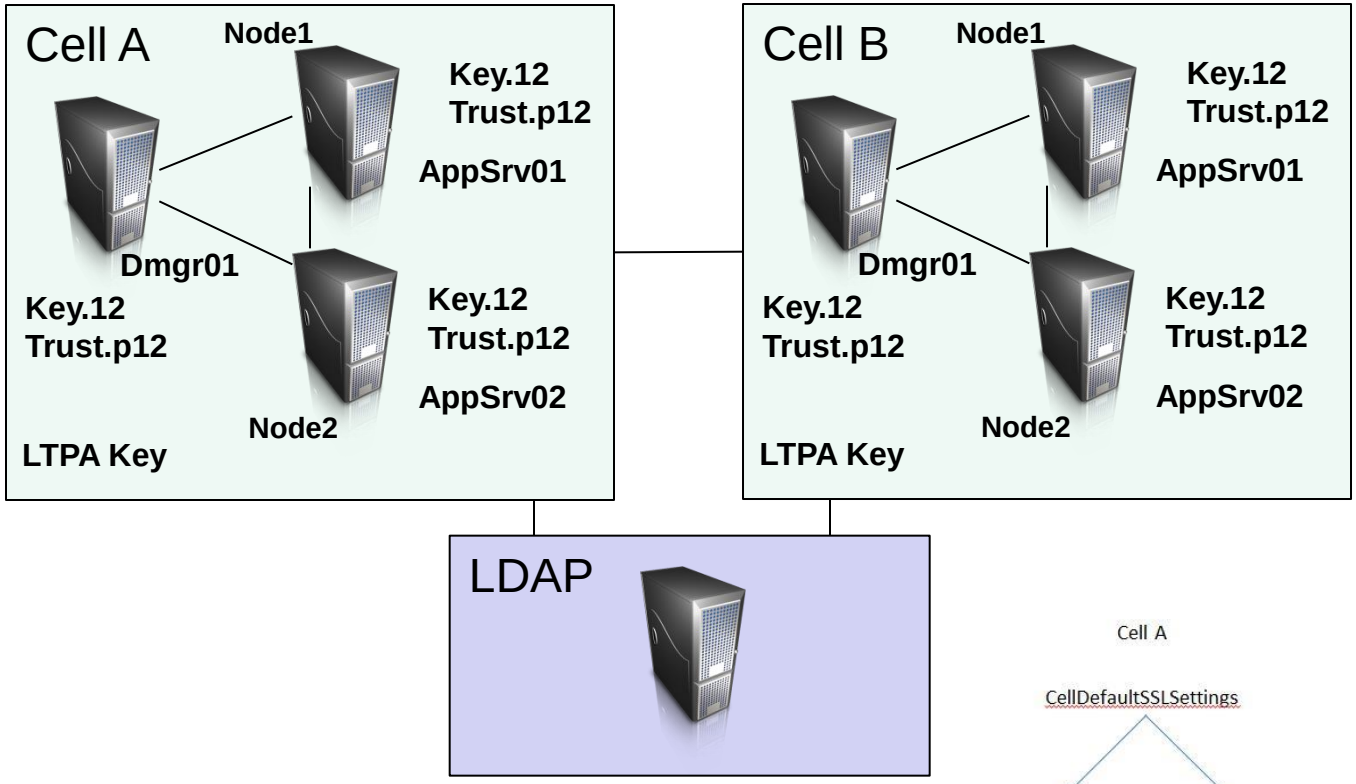
Cross Cell SSO common scenarios: Single profile

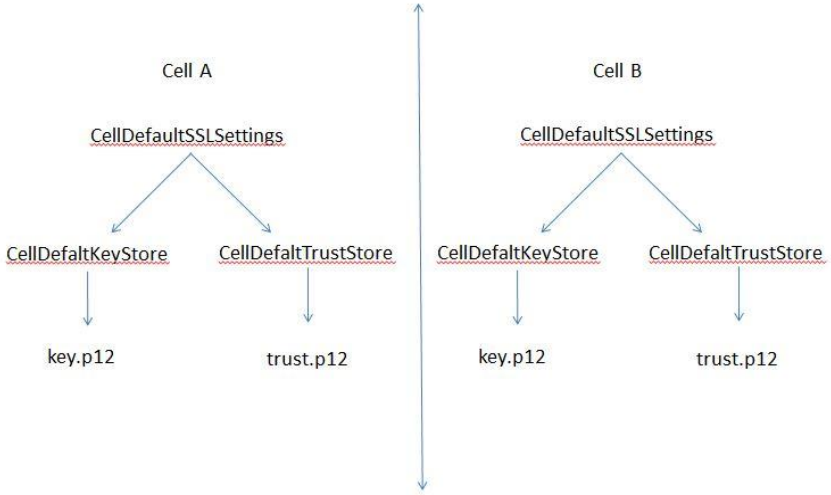


Example – Cell A is outbound, Cell B is inbound



Cross Cell SSO common scenarios: Network Deployment





Example – Cell A is outbound, Cell B is inbound

WebSphere® Support Technical Exchange

Question 5

- What is the LTPA key and how to prevent LTPA keys from becoming out of sync or corrupted?

- LTPA - Lightweight Third Party Authentication
  - It's an authentication protocol
  - It's supports Single Sign-on (SSO) in same DNS domain
  - It's supports forward able credentials
  - This support permits LTPA to encrypt, digitally sign, and securely transmit authentication-related data, and later decrypt and verify the signature.

IBM Knowledge Center

http://www.ibm.com/support/knowledgecenter/SSAW57_7.0.0/com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/csec_ltpa.html?cp=SSAW57_7.0.0%2F3-8-30-2-2-0&lang=en

Automatically generate keys

- In WebSphere Application Server V7, and up this feature is off by default, and in for any new profiles that are created V6.1.0.23 this feature is turned off by default.

IBM Knowledge Center

http://www.ibm.com/support/knowledgecenter/SSAW57_7.0.0/com.ibm.websphere.soafep.multiplatform.doc/info/ae/ae/tsec_ltpa_and_keys.html?cp=SSAW57_7.0.0%2F8-4-0-0&lang=en

Open Lines for Questions

Connect with us!

1. **Get notified on upcoming webcasts**
   Send an e-mail to wsehelp@us.ibm.com with subject line “wste subscribe” to get a list of mailing lists and to subscribe
2. **Tell us what you want to learn**
   Send us suggestions for future topics or improvements about our webcasts to wsehelp@us.ibm.com

Summary

Additional WebSphere Product Resources

- Learn about upcoming WebSphere Support Technical Exchange webcasts, and access previously recorded presentations at: http://www.ibm.com/software/websphere/support/supp_tech.html
- Discover the latest trends in WebSphere Technology and implementation, participate in technically-focused briefings, webcasts and podcasts at: http://www.ibm.com/developerworks/websphere/community/
- Join the Global WebSphere Community: http://www.websphereusergroup.org
- Access key product show-me demos and tutorials by visiting IBM® Education Assistant: http://www.ibm.com/software/info/education/assistant
- View a webcast replay with step-by-step instructions for using the Service Request (SR) tool for submitting problems electronically: http://www.ibm.com/software/websphere/support/d2w.html
- Sign up to receive weekly technical My Notifications emails: http://www.ibm.com/software/support/einfo.html