	The second secon

IBM Connections 4.5 Deployment Scenarios

Deployment Scenarios ERC 1.0



Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide.

The following are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide:

Cognos®	DB2 Universal Database™	DB2®
Domino®	FileNet®	Lotus Notes®
Lotus®	Notes®	Rational®
Tivoli®	WebSphere®	

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows 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 Oracle and/or its affiliates.

Other product and service names might be trademarks of IBM or other companies.

June 2013 edition

The information contained in this document has not been submitted to any formal IBM test and is distributed on an "as is" basis without any warranty either express or implied. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will result elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

© Copyright International Business Machines Corporation 2013.

This document may not be reproduced in whole or in part without the prior written permission of IBM.

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

Enabling single sign-on for Tivoli Access Manager with SPNEGO

About the author



Tracy Green has worked for IBM, initially with Lotus for 17 years. She has been an Advisory Software Engineer with the Dublin System Verification Test team for the last eight years, and has worked on a range of IBM products, most recently IBM Connections. Tracy can be reached at tracy_green@ie.ibm.com.

Contents

- 1. Environment description
- 2. Enabling single sign-on for Tivoli Access Manager with SPNEGO
- 3. WebSphere security changes

Environment description

- The test environment that is described in this article is a 2-Node Medium Cluster running on Windows Server 2008 R2 Enterprise 64-bit edition that uses Microsoft SQL Server 2008 R2 database back end and Microsoft Active Directory 2008 LDAP repository.
- This article describes how to enable single sign-on for Tivoli Access Manager with SPNEGO after the IBM Connections 4.5 cluster is successfully deployed and configured.
- The Windows Domain is .LITBG02.SWG.USMA.IBM.COM.

Host name	Function	RAM	Disk space
dmgrHTTPsrv	WebSphere DMGR+HTTP	8 GB 2 CPU	60 GB
wasNode1srv	WebSphere Application Server Node1	8 GB 2 CPU	60 GB
wasNode2srv	WebSphere Application Server Node2	8 GB 2 CPU	60 GB
sqlTDIsrv	SQLServer + Tivoli Directory Integrator	8 GB 2 CPU	60 GB

Host name	Function	Branch	# Users
LDAPsrv	LDAP repository	OU=SharedLDAP,OU=Lotus,OU=Software	300k
		Group,DC=IItbg02,DC=swg,DC=usma,DC=lbm,DC=com	

Host name	Function	Version
webSealsrv	WebSEAL Server	06/01/01

Connections 4.5 is fully deployed and users can log on from the remote HTTP Server host name, for example, https://dmgrHTTPsrv.mycompany.com/homepage.

	<u><u><u>n</u> + e</u></u>
	IBM.
Cross Manager WebSEAL Junite 6.1	Af Segim Transmitti Jaan ant af Jaan Sant
	S.
I og File nune	inva Log File Link
Eng File name 1721-wo4 Web/SEAL Server mag_web/codd ing file	Ing File Link mag_ weberald-iefenblug
Ing File name Til word WebSEAL Server mag, serberad ing file Til word WebSEAL Server codig ing file	Eng File Link mag. Archaeold-definit lag confat. data.log.
Ing File name Til-work Web/SEAL Server mag, webworkd ing file Til-work Web/SEAL Server codig ing file Til-work Web/SEAL Server Enquent ing file	Ing File Link nuz, webscald-defeat has route, data has Respective Respective
Eng File name TTT-work WebSSAL Server mag, webceadd Ing file TTT-work WebSSAL Server config log file TTT-work WebSSAL Server Require log file TTT-work WebSSAL Server Referen log file	Eng File Link nuz. wrbanid-isfiekluz nosiz, dealog Referentiog Referentiog
Eng File name TiT-work Web/SEAL Server nang, web/could ing the TiT-work Web/SEAL Server couldg ing the TiT-work Web/SEAL Server Request ing the TiT-work Web/SEAL Server Agent ing the TiT-work Web/SEAL Server Agent ing the	Eng File Link max. websendd-idfeithlur roefic.detalog Respecting References Agenting

The WebSEAL server can be accessed from https://webSealsrv.mycompany.com.

Figure 1. Tivoli Access Manager WebSEAL

After you complete the steps to enable single sign-on, you then access the Connections cluster from the WebSEAL host name, for example:

https://webSealsrv.mycompany.com/homepage.

Enabling single sign-on for Tivoli Access Manager with SPNEGO



Refer to the IBM Connections information center for full instructions on how to apply any required changes to Tivoli Access Manager for Connections 4.5:

Enabling single sign-on for Tivoli Access Manager,

http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connectio ns+4.5+Documentation#action=openDocument&res_title=Enabling_single_signon_for_T ivoli_Access_Manager_ic45&content=pdcontent

Most of the previous configuration is also required when enabling single sign-on for Tivoli Access Manager with SPNEGO, except where otherwise noted. The steps for updating interService URLs, adding a Tivoli Allow Access to the Embedded Experience gadget and adding a Tivoli Access Manager authenticator property can be omitted in an SPNEGO environment.

Refer to the following information center topic for instructions on how to enable SPNEGO for WebSEAL:

• Enabling single sign-on for Tivoli Access Manager with SPNEGO, http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connectio ns+4.5+Documentation#action=openDocument&res_title=Enabling_single_signon_for_T ivoli_Access_Manager_with_SPNEGO_ic45&content=pdcontent

This article outlines the configuration changes required to the Connections Cluster.

WebSphere security changes

Verifying ConnectionsAdmin

- ____1. Log in to WebSphere Admin Console and go to Security > Bus Security.
- ____2. Click ConnectionsBus and select Security > Users and groups in the bus connector role. Ensure that your ConnectionsAdmin is listed.

Igenerations	 GelinisetitThoGelitti, hufferOneriti. 	
Tree Application	Exercised and the second se	
Application Types with the investment of applications Applications Applications Applications Machine matrix amount	Bases > Contentionalities > Becarity for has Connection Usaws in the bas connector role are able to connect to or believes they are in a group with that role. In Performance	ntiles > Users and groups in the box consector rule the bus to perform messaging operations. Lizers can have the role either by specifically having that rol
	Den. Delate	
lervites	DDTY	
Weburgen .		7.452.4
lariurity.	Revell Name D.	7104 0
Blabal meaning	AlAuthenticated	0rova
Desuring domains	📇 connAdmin	Uner

Figure 2. WebSphere Admin Console

This is the user that is specified during the Connections installation and must exist in your LDAP repository.

Changing default realm

- ____1. Change the default realm name in the Federated Repositories section of the Deployment Manager to match the value of the LDAP name, including the port number (for example, ldap.mycompany.com:389).
- ____2. From WebSphere administration console, go to Security > Global Security.
- ___3. Click Configure beside Federated Repositories. Change the realm name to be the host name of your LDAP repository.

Without allows			Welcome sunnikdnia
2 Applications	· Second and the Second St. States Second		
Ton Application Windowsky System Statistics endployed one Substatistics from Applications Automatic from Applications Automatic Substatistics	Exclusion and the second secon	is repositores can be managed in a single, o or more external repositories, or in both the	rhal main. The rasin can consist of identities in the fit buffer regestroy and one or more external repositories
Carlas	LDAPaty mycompany com		
f Services	· Bronzey administrative user name		
A Bassuryas	condition		
- Security	Received and the set		
Expander (Instance definition/configurations Groupy EDC, partificate and law, instaglandam Expanders Society and thing For instance Society Society and SAX-RNC Concerns installers	C Server identity that is strend in the representative	<u>an da a</u> rte	
: Environment			
 Comparison Update postal reductive plag-to configuration Underglobal reductive Underglobal resultance Usdate plags resultance Usdate plags resultance Reglobal resultance Reglobal resultance Mit Devea 	Ignore can for authorization Alion operations if annex of the repeatement are Apportances of the realm, Add Bare entry to Tealm	daar 6 built in repeatiny 6 Annyse	
Wittening	Salact Bass Srivy	Reportary Identifier	Reportiny Type
# 090 kunde reportortes	The can administer the following resources:		
Bystee administration	CU-Sofware, DC-mycompany, DC-com	LDAParx	LOAP-AD
e Call e Suk nunapar	andelevititieEasedfaaim	InternalPlathepository	File
 Tario Charges to Instato Insporting Desiriyuman Manager Nordes Nordes Nordes Nordes Nordes 	Tutal 2 Additional Properties	Related Name	
B Controlland Installation Wanager Controls Professory Zyth acted/dat Controls United	Provide entertaint resources Endourneauma resources Europated entry topes	 Manage results Southed extreme 	tan adam metros - interent

Figure 3. WebSphere Administration Console - Global Security

Setting the single sign-on domain name to match the Tivoli Access Manager server domain name

- 1. From the WebSphere Administration Console, go to Security > Global Security > Web and SIP security > Single sign-on (SSO).
- ____2. Ensure that the following check boxes are selected:
 - Enabled
 - · Interoperability mode
 - · Web inbound security attribute propagation
 - · Set security cookies to HTTPOnly to help prevent cross-site scripting attacks
 - _3. Set the domain name, for example, mycompany.com, and click Apply, OK, and Save.

WebSphere, acitware	Welcome connAdmin
T Applications	CallsdmarteTTParvCe101.Frofile=Onwr01. CallsdmarteTTParvCe101.Frofile=Onwr01.
Application Types WebGelwere enterprise applications Bushinger-level applications Appen Global deployment settings	Cisited security > Single sign-on (SSO) Specifies the configuration values for single sign-on. General Properties
t John	and an and a second sec
5 Services	I Requires SSL
t Resources	Domain name
5 Security	invcompany.com
Obial security Security domains Administrative Authorization Orsups Security and key management Security and key management Security and iting Bus security AVV-WS and 2AV-RIPC security retitime	Interoperabliky mode LTEA VI cockie name Ltpatoken Ltpatoken Ltpatoken Ltpatoken Mode assurb attribute emphasion
- Environment	and many moonle sectual structure biobadance
Virtual heets Update global Web server plag in configuration WebGetwe variables Shared Ubranes SIP application mothers Replication mothers Replication mothers URE Groups	Set security cookies to HTTPOnly to help prevent coss-site scripting attacks Apply OK Reset Cancel

Figure 4. WebSphere Admin Console - Global Security - Web and SIP security - Single sign-on (SSO)

- ____4. You must now go to Security > Global Security > Web Security General Settings.
- 5. Click Authenticate only when the URI is protected and select Use available authentication data when an unprotected URI is accessed.

___6. Click **OK** and save the changes.

WebSphere, sometry	_		Welcome connAdmin
R Applications	* <u>cel</u>	edmanistTPaceGeR01. ProfilesOmar01.	
Heav Application Heaview Application Application Types WebSphere extraptions applications Business - Invel applications Assert Other displayment settings	9 1 1	interventy indust security > Web security - General settings (pecifies the settings for web authentication, eneral frequenties	
N Joba		Web authentication trenavior	
N Services		Vise available authentication data when an unprotected URI is accessed	
m Resources		C Authenticate when any URI is accessed	
d Security			
Othelia excently Security domains Administration Authorityation Oroupe Administration Authorityation Oroupe Solution and they management Security and they No a security Solution and MAX-REC security continue	0	Default to basic authentication when certificate authentication for the HTTPS client fails Apply OK Reset Cancel	

Figure 5. WebSphere Admin Console - Global Security - Web Security - General Settings

Extracting the LTPA token

- ___1. From the WebSphere administration console, go to **Security > Global Security** and click the **LTPA** link.
- 2. Go to the **Cross-cell single sign-on** section and enter a password for your LTPA key and set the path and key file name.
- ____3. Then, click **Export**, followed by **Apply**, **OK**, and **Save**.

Webgers, selfant,	Welcome considerer
C Applications	Geliningentities Gelitz, BurlierGrandz.
 New Application Application Types Well-being entropy to a spatial and Restance Total conferences 	Child is assuming it. Child assuming a constraint of the second s
Assets Midal Asphonent settings	address and the second part of a subarged between servers motives the LTDR methanism.
k John	Adhentication data is encrypted and decrypted by using keys that are heart in one or more key stareat
E Servicer	Key set group
Autourcan	Carls, TRACeyter/Innod Optimize Service
Decarts.	* Sec.int.union
Concern Internet Concern Internet Concern Internet Concern Internet Concern Internet Concern Internet Concernit Andrea Concernit Andrea Concernit Andrea Concernit Andrea Concernit Andrea Concernit	LTPA lineauf LTPA lineauf value for formanded credentials between services [120] minutes Cross-cell single sign on
devisioner	Bingle age on acress cells can be precided by sharing keys and passion to share the keys and passion. Sing to to see call, apacity a key the, and do Rabot have. Then, by or to the other cell, scorely the key the, and cick import have.
Virtual function Virtual function Virtual function Virtual function Virtual function Virtual Virt	2 * Seasonid Conference parameter Pully sublified kay file marres processmentsmail.tag (monorlarge) (Sport large)
System administration	
 Gall Jub manager Same changer to manage regulatory 	[Apply] (X) [Result] [Carrow]

Figure 6. WebSphere Admin Console - Security - Global Security - LTPA

The LTPA key is used for configuring the transparent path junctions in Tivoli Access Manager as described in the information center.

Extracting the IBM HTTP Server SSL certificate

- ____1. From the HTTP server, choose **IBM HTTP Server v8.0 > Start Key Management Utility** from the Start menu.
- ___2. Select Key Database File > Open.
- ___3. Open the plugin-key.kdb, which contains the IBM HTTP Server WebSphere Application Server keys and extracts the Personal Certificate.



The default password, if not changed, is WebAS.

L 🎽			
	Key database information	_	
OB-Type:	CMS		
File Name:	C:\IBMWVebSpherelPlugins\configidubxpcvm956-webserveriplugin-key.kdb		
Token Label:			
	Key database content		
Personal Certi	ficates	-	Receive
default			Delete
			View/Edit
			Export/Import
			Export/Import Recre <u>a</u> te Request
			Export/Import Recregte Request Rename
			Export/Import Recreate Request Rename New Self-Signed

Figure 7. IBM Key Management

_4. Click **Extract Certificate** and provide a path and name for the extracted file, leaving the .arm extension, and click **OK**.

🙀 III M Key Man	ogement - [C.\1894 WebSphere Plu	gina) condig), drogrif IT TParv webserver(plugin Key kob)	-	P
Key Database E	Ae Greate Yew Help			
		Key database information		
DB-Type:	CMS			
File Name:	C \IBMWebSphere\Plugins\config	ldubxpcvm956-webserverlplugin-key.kdb		
Token Labet				
		Key database content		
Personal Cert	ficates New		E	Receive
default	Data type	Base64-encoded ASCII data		Delete
1000	Certificate file name:	cert.arm	Browse	Economic Contraction
	Location	C trantal		ViewEdit_
				ExportAmport
		QK Cancel		Recreate Reques
			[Rename
			0	New Self-Signed
			7	

Figure 8. Start Key Management Utility

The SSL certificate is copied to the WebSEAL server when applying the Connections changes to Tivoli Access Manager as described in the information center.



Information

Review the information center to complete the Tivoli Access Manager configuration:

- Enabling single sign-on for Tivoli Access Manager, http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connectio ns+4.5+Documentation#action=openDocument&res_title=Enabling_single_signon_for_T ivoli_Access_Manager_ic45&content=pdcontent
- Enabling single sign-on for Tivoli Access Manager with SPNEGO, https://idoc2.swg.usma.ibm.com/connections/topic/com.ibm.lotus.connections.doc/ secure/t secure with tam-spnego.html

11

Configuring the LotusConnections-config.xml

___1. On your Deployment Manager computer where Connections is installed, go to:

```
C:\WebSphere\AppServer\profiles\Dmgr01\config\cells\dmgrHTTPsrvCell01\LotusC onnections-config
```

- ____2. Back up the LotusConnections-config.xml file and move the backup to another location, because leaving multiple versions of the .xml files in the LotusConnections-config folder causes functional problems.
- ____3. Now, edit LotusConnections-config.xml with a text editor and scroll to the bottom of the file. Locate dynamicHosts and set it to "Enabled" and set the href and ssl-href values to the host name of your WebSEAL server, for example, webSealsrv.mycompany.com.



Figure 9. Editing LotusConnections-config.xml

4. Save the file and restart your cluster. Stop all application servers and all nodes, and then restart the deployment manager, all the nodes, and all the application servers.

Configuring HTTP server for logout



This section is optional.

Determine how you want the system to behave when users log out of IBM Connections. In an SPNEGO environment when users click **Log out**, they are not logged out of IBM Connections. However, you can redirect the user by using the IBM HTTP Server HTTP configuration file, at C:\IBM\HTTPServer\conf.

- ___1. Back up and then edit httpd.conf.
- ___2. Uncomment the line that contains LoadModule rewrite_module modules/mod_rewrite.so if not already done, so that the rewrite module is enabled.
- ___3. To capture requests to /ibm_security_logout and redirect them to /pkmslogout, add the following rewrite rules to the http and https sections of the file:

```
RewriteEngine On
RewriteCond %{REQUEST_URI} /(.*)/ibm_security_logout(.*)
RewriteRule ^/(.*) /pkmslogout [noescape,L,R]
```

The following example illustrates how it would look in the httpd.conf file after the changes are implemented:

```
RewriteEngine On
RewriteCond %{REQUEST_URI} /(.*)/ibm_security_logout(.*)
RewriteRule ^/(.*) /pkmslogout [noescape,L,R]
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
<IfModule mod_ibm_ssl.c>
Listen 0.0.0.0:443
<VirtualHost *:443>
ServerName dmgr.mycompany.com
```

_4. Uncomment the line that contains LoadModule rewrite_module modules/mod_rewrite.so if not already done, so that the rewrite module is enabled:

```
SSLEnable
RewriteEngine On
RewriteCond %{REQUEST_URI} /(.*)/ibm_security_logout(.*)
RewriteRule ^/(.*) /pkmslogout [noescape,L,R]
</VirtualHost>
</IfModule>
SSLDisable
Keyfile "C:\IBM\HTTPServer\Keys\webserver-key.kdb"
SSLStashFile "C:\IBM\HTTPServer\Keys\webserver-key.sth"
```

- ____5. Save and close the httpd.conf file.
- ___6. Restart IBM HTTP Server.

Accessing IBM Connections within the SPNEGO domain

You now access IBM Connections from the WebSEAL server host name.

____1. From a client computer within the SPNEGO domain, in this case .MYCOMPANY.COM, open the following URL from your web browser: https://webSealsrv.mycompany.com/homepage

	//webSeals	rv mycompany.com/	homepage					6	• = = = 合 @
IBM Connections	Home	Profiles - Co	ommunities -	Apps +		connAdmin *	Stare	0	IB
😭 Home					🐩 All Conn	ections * Search	1		
Getting Started		Getting sta	arted with I	BM Connections					
Im Following		Do not show	w this screen at s	tart					
Status Updates My Notifications		1 WELCOM	E Welco	ome to IBM Connections					

Figure 10. IBM Connections - home page

The authenticated windows user is automatically logged in to Connections.

You must ensure that your web browser includes the WebSEAL server as a trusted host to work properly.

Example for Internet Explorer:

- a. Select Tools > Internet Options.
- b. Click the Security tab and select Local intranet.
- c. Click **Advanced** and add the WebSEAL host name to "Add this website to the zone" and click **Add**.

eneral Security p	rivacy Content Connections Programs Advanced
Internet Loc	al intranet Trusted sites Restricted sites
toc This Loca four	al intranet 23 Use the settings below to define which websites are included in the local intranet zone.
Security lev Allowed le	Automatically detect intranet network
	Local intranet
	You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.
- T	You can add and remove websites from this zone. All websites ir this zone will use the zone's security settings.
Enab	You can add and remove websites from this zone. All websites in this zone will use the zone's security settings. Add this website to the zone: http://www.google.ie Add
Enab	You can add and remove websites from this zone. All websites in this zone will use the zone's security settings. Add this website to the zone: http://www.google.ie Add Websites:
Enab W	You can add and remove websites from this zone. All websites in this zone will use the zone's security settings. Add this website to the zone: http://www.google.ie Websites: http://webSealsrv.mycompany.com



15

without the prior written permission of IBM.