Hudson Role-based Authorization Strategy

This plugin enables authorization using a role-based strategy. There was an issue with the plugin accessing roles that were created in WebLogic LDAP.

WebLogic Group and User

The group, mygroup, and the user, myuser, were created using the WebLogic console using the DefaultAuthenticator based on the Embedded LDAP server.

dminist	tration Con	sole								Q
🔒 Ho	ome Log Out	Preferences 🔤 R	ecord Help	٩				Welcome, weblogic	Connected to: bas	e_domair
Home	e ≻Summary o	f Security Realms >my	realm >Users and Gro	oups						
Settin	gs for myre	alm								
Confi	guration U	sers and Groups	Roles and Policies	Credential Mappings	Providers	Migration				
Users	s Groups				11		1			
	tomize this		sach group that has b	een configured in this se	ecuricy realm.			Showing 1 b	o 10 of 10 Previous	Nevt
								Showing I t		TNEXC
	Name 💛	D	escription						Provider	
	TESTGRP								DefaultAuthentical	tor
	OracleSyste	mGroup O	racle application softv	vare system group.					DefaultAuthentical	tor
	Operators	0	perators can view and	d modify all resource att	ributes and p	rform serve	r lifecycle operation	s.	DefaultAuthentical	tor
	mygroup								DefaultAuthentical	tor

Checking the LDAP group query

The following LDAP query was being sent to try to locate the roles a user was in when they logged in:

[31/Mar/2012 11:07:07 EDT] conn=35 op=35 SRCH

base="ou=groups,ou=myrealm,dc=base_domain" scope=2

filter="(|(member=uid=myuser,ou=people,ou=myrealm,dc=base_domain)(uniqueMembe r=uid=myuser,ou=people,ou=myrealm,dc=base_domain)(memberUid=myuser))"

The search was looking for the ID myuser, and it was using three different versions of the filter (member, uniqueMember, and memberUid) to try to find the groups the user was in. The WebLogic LDAP stores the group relationship using the more modern LDAP attribute memberURL. This meant the plugin could never find the user in the group. WebLogic supports the older method of specifying individual entries for each user within the group using the uniqueMember attribute, which is one of the ways the searching was being done.

Using JXplorer you can see that when the group is initially created in the WebLogic console the group entry is created with the memberURL attribute, which uses a dynamic search to find members of the group.



The group entry was modified to add the uniqueMember attribute containing the DN for the myuser entry.

🚸 JXplorer		
File Edit View Bookmark Search LDIF	Options Tools Security Help	
N N 🖨 🕺 🖻 🛍 🖻	X D 🗃 🚸 🔍 🗖	Quick Search
📭 Explore 🛛 🙀 Results 🛛 🖓 Schema	HTML View Table Editor	
Sworld	attribute type	value
🖶 💿 base_domain	cn	mygroup
e- الله myrealm الله الله groups	objectclass	top
🖃 🧱 groups	objectclass	groupOfURLs
🕀 🖳 AdminChannelUsers	objectclass	groupOfUniqueNames
⊕ ⊕ Administrators	memberURL	ldap:///ou=people.ou=myrealm.dc=base_domain??sub?(&(objectclass=person
⊕	orclguid	76C99F40856D11E1BF8FD155A3B8640C
E CrossDomainConnectors	businessCategory	
E Deployers	createTimestamp	
Ben Monitors	creatorsName	
B mygroup	description	
⊕ Operators	modifiersName	
⊕ © OracleSystemGroup	modifyTimestamp	
E C TESTGRP	0	
E Beople	ou	
i a123456	owner	
	seeAlso	
⊕ [©] d123456	uniqueMember	uid=myuser,ou=people,ou=myrealm,dc=base_domain
± € d223456		
myuser		
ter		
ACMLAuthorization XACMLRole		
🗎 🚊 XACMLRole	Submit Reset	Change Class Properties
庄 🖲 changelog 📃		
Opening Connection To Idap://192.168.1.10:738	9	

Role Plugin Configuration

To setup the role plugin you go to Manage roles. In the setup below a global role was setup with the privilege to create jobs. A project role was setup for the role developer to provide full privileges to configure and run jobs that begin with the prefix DEVJOB. The screenshot below shows the role configuration.

Role	Over	all	Slav	e			Jo	Ь			R	un		View	L. C.	SCM
Rule	Administer	Read	Configure	Delete	Create	Delete	Configure	Read	Build	Workspace	Delete	Update	Create	Delete	Configure	Tag
admin 🛛	~	~	~	•		~	~	~	•	V	•		~	~	~	~
anonymou	s 🗖	~														
create-job					~											
Role to ac	ld															
oject roles					Add											

Once the attribute entry uniqueMember was added to LDAP the Role plugin was able to find the groups. You need to prefix the group name with the word ROLE_, and you must put the group in all caps. LDAP does not care about the caps, but the plugin does. Now the plugin shows the entries for global groups and project groups with the correct group icon on the assign roles screen. In this setup mygroup, which is a group of developers, was assigned the global role to create jobs and the project role to configure and run jobs based on the pattern set in manage roles.



User/group	admin	anonymous	create-job
ROLE_MYGROUP			
📓 ቆ a123456	•		
Anonymous		~	
User/group to add			
User/group to add roject roles		dd	
	develo		
roject roles			

Hudson Login

When the user logs in as myuser, using LDAP credentials and the LDAP group setup, the user will have the New Job privilege and will only see the jobs that match the pattern DEVJOB.*:

Hudson					🔍 search		🕐 myu	ser log out
Hudson	All P	ipeline	iah				ENABLE	AUTO REFRESH
🍇 <u>People</u> 萨 <u>Build History</u>	S	W	Jop †	Last Success	Last Failure	Last Duration	Console N/A	
A My Views			DEVJOB-Compile	N/A	N/A	N/A	N/A	N

WebLogic LDAP connections

Channel-2-Idaps

Idaps

true

The network channel feature can be used to separate the traffic for the LDAP or LDAPS queries from the normal admin traffic. This will allow the admin traffic to use HTTPS on the standard port, which will be accessed via the public network. The LDAP or LDAPS traffic can be setup to listen on the internal network. Below is a sample setup of the WebLogic channel configuration:

•	ation Con				1							
D Hom	ne Log Out	Preferenc	es 🔤 F	Record Help			Q				Welcome, weblogic	Connected to: base_0
Home >	•base_doma	n >Summar	y of Secu	urity Realms >ł	oase_domain ≻S	Summary of	Servers >AdminS	erver > Prot	ocols			
ettings	s for Admi	nServer										
Configu	ration P	rotocols	Loggin	ig Debug	Monitoring	Control	Deployments	Services	Security	Notes		
Genera	al HTTP	jCOM	IIOP	Channels								
							nnection requirem				our systems and network	resources.
This N Custo		nnels page table									ur systems and network	resources.
This N Custo	letwork Cha omize this ork Chann	nnels page table										resources. I to 3 of 3 Previous ∣N
This N Custo Netwo	letwork Cha omize this ork Chann	nnels page table els	displays			n network c		been configu		server.		
This N Custo Netwo	letwork Cha omize this ork Chann Clone	table els	displays	s key informat	ion about each	n network c	en Address	been configu	ured for this	server.	Showing 1	L to 3 of 3 Previous N

192.168.1.10

7636

192.168.1.10

7636