

WPC-LDAP Integration Setup Guide

Tab	le of	Conter	its

WPC-LDAP Integration Setup Guide	4
1. Introduction	4
Configuring WPC	5
2. Configuration in Login.wpcs	5
3. Configuration through lookup table	5
Configuring Novell eDirectory Server	9
 4. Configure LDAP schema for users and roles	9 9 10 11
5.1 Password Encryption Support	12 12
 6. SSL Setup 6.1 Steps to extract self signed certificate for client: 6.2 SSL Setup - Client Side (WPC end) 	14 14 18
7. Changes required in the Login Script for Novell (DIGEST-MD5)	19
Configuration requirement for SUNONE Directory Server	20
8. Creating a Directory Tree 8.1 For Simple Bind 8.2 For SASL Bind 8.3 For SSL	20 20 20
Configuring Microsoft Active Directory Server	26
 9. Configure LDAP schema for users and roles 9.1 Create a new Domain 9.2 Create a new Organization 9.3 Create a new user 9.4 Create a new group 	26 26 26 27 27 29
10. Configuration Notes: 10.1 Configuring Microsoft Active Directory for SSL access and Extract Self Signed Ce for client	rtificate
Configuring Lotus Domino Server 6.5	33
11. Configure LDAP schema for users and roles 11.1 Create a new Person 11.2 Create a new group 11.3 Configuration Notes	33 33 34 36 36
Configuring Tivoli Directory Server	37
12. Configure LDAP schema for users and roles	37 37 38

12.3 Create a new user	39
13. SASL - CONFIGURING DIGEST-MD5 on TDS	42
13.1 Configuration Notes	43
13.2 SSL Setup	44
13.3 SSL Setup – Client Side (WPC end)	47
Configuring Z/OS	48
14. Creating Users and Groups:	48
14.1 Create a new user:	48
14.2 Create a new Group:	51

WPC-LDAP Integration Setup Guide

1.Introduction

The Lightweight Directory Access Protocol (LDAP) is an open industry standard. LDAP defines a standard method for accessing and updating information in a directory. LDAP is gaining a wide acceptance as the directory access method of the Internet and is therefore also becoming strategic within corporate intranets.

WPC has traditionally managed its own authentication strategy. However as WPC evolves into a middleware solution that is a component of a larger customer strategic enterprise integration with the other components is core requirement. One such component is the directory server which maintains the enterprise wide business critical User information.

The WPC 5.3 provides integration with the LDAP server using customizable Login & Logout script, it satisfies the IBM directory integration compliance requirements, and it can become interoperable with another directory server.

The WPC-LDAP integration is a two setup process involving changes in the WPC end and at LDAP server end. This document will detail out the setup and configuration steps that are required for various LDAP servers and also the changes need to be made on WPC end for successful WPC-LDAP integration.

Configuring WPC

2. Configuration in Login.wpcs

We need to modify the following configurations in Login.wpcs

- wpcOnlyAuthentication Flag that identifies the authentication mechanism. Set to false in case ldapAuthentication is required **Default value** is true.
- 2) logger_name The logger variable configure in log.xml **Default value** is ldap.

3. Configuration through lookup table

The other configurations to be done for LDAP server is moved from Login.wpcs to a lookup Table (LDAP Properties for English locale). Also the user attributes required to be fetched using LDAPUserDataFetch.wpcs have been moved to this lookup table.

If we are using multiple LDAP URLs, Each ldap url should contain row with the relevant values filled in.

The description of each attributes for LDAP server is given below.

Attribute Names	Description Of Attributes
LDAP URL	Ldap Server url. PK of the lookup table entry. The values are for the ldap server given.
LDAP User Naming Attr	The naming attribute for the users in this LDAP Server
LDAP Group Naming Attr	The naming attribute for the groups in this LDAP Server
User Parent DNs	The Pipe (I) delimited Parent DNs where the users are likely to be found (Can be set to "") if you do not know the Parent DN
Group Parent DNs	The Pipe () delimited Parent DN where the groups are

	likely to be found (Can be set to "") if you do not know the Parent DN
Root Entry DN	The root user's entrydn in the ldap
Root Password	The password of the root user
Bind Type	The bind type could be one of simple/sasl/ssl. This is provided as an enum.
SSL Bind Type	The subtypes allowed in ssl bind. One of simple/DIGEST-MD5.This is provided as an enum.
personClassNames	The person class name in the LDAP server
groupClassNames	The groups class name in the LDAP server
keystore	The location of the cacerts file that has been imported in to the JVM
supportedSaslMechanis ms	Subset of server Supported sasl mechanisms using which the customer wants to authenticate LDAP users if the Bind Type is sasl. The list of mechanisms should be delimited by space character.
First Name Attribute	The user attribute which represents first name in ldap. E.g givenname in Tivoli.
Last Name Attribute	The user attribute which represents last name in ldap. E.g sn in Tivoli.
Full Name Attribute	The user attribute which represents full name in ldap. E.g cn in Tivoli.
Mail ID Attribute	The user attribute which represents mail ID in ldap. E.g mail in Tivoli.
Telephone Number Attribute	The user attribute which represents telephone number in Idap. E.g telephonenumber in Tivoli.
FAX Number Attribute	The user attribute which represents fax number in ldap. E.g facsimiletelephonenumber in Tivoli.
Postal Address Attribute	The user attribute which represents postal address in Idap. E.g postaladdress in Tivoli.
Title Attribute	The user attribute which represents title in ldap. E.g title in Tivoli.

	Sun-One	Novell	Notes Domino	
LDAP URL	ldap://9.184.114.57:3537	ldap://9.184.112.116: 389	ldap://9.182.149.115: 389	
LDAP User Naming Attr	Uid	Cn	Cn	
LDAP Group Naming Attr	Cn	Cn	Cn	
User Parent DNs	dc=in,dc=ibm,dc=com (Mandatory)			
Group Parent DNs	dc=in,dc=ibm,dc=com (Mandatory)			
Root Entry DN	uid=admin, ou=administrators, ou=topologymanagem ent, o=netscaperoot	Cn=admin,o=compa ny	cn=SanjayIBM_User	
Root Password	trinitron	root1234	wpcldap	
Bind Type	simple	Simple	simple	
personClassNam es	inetOrgPerson	Inetorgperson	inetorgPerson	
groupClassName s	groupOfUniqueNames	groupofUniqueNam es	groupOfUniqueNa mes	
keystore				
supportedSaslMe chanisms				

Sample Configuration Values for Various Directory Servers

	Tivoli	Z/OS	Microsoft
LDAP URL	ldap://9.184.114.80:389	ldap://tvt1003.tivlab. raleigh.ibm.com:338 9	ldap://9.182.149.46:3 89
LDAP User Naming Attr	Cn	Cn	cn
LDAP Group Naming Attr	Cn	Cn	cn
User Parent DNs	Cn=localhost (Mandatory)	cn=admin,cn=wpctr eeroot,dc=tvt1003	dc=wpc,dc=com (Mandatory)
Group Parent DNs	Cn=localhost (Mandatory)	cn=admin,cn=wpctr eeroot,dc=tvt1003	dc=wpc,dc=com(Ma ndatory)
Root Entry DN	Cn=root	Bryan	CN=wpcuser,OU=isl ,OU=ibm,dc=wpc,dc =com
Root Password	root	secret	root1234
Bind Type	simple	Simple	Simple

personClassNam es	inetOrgPerson	Inetorgperson	person
groupClassName s	groupOfUniqueNames	groupofUniqueNam es	group
keystore			
supportedSaslMe chanisms			

Ð	LDAP Properties		
-	Common Attributes		
	Primary Key, Display		
	LDAP URL 🛞 🛅	>>	ldap://ldapsrv3:389
•	LDAP Properties Spec 🗭		
	LDAP User Naming Attr	>	cn
	LDAP Group Naming Attr	>>	cn
	User Parent DNs	>>	cn=localhost
	Group Parent DNs	>>	cn=localhost
	Root Entry DN	>>	cn=root
	Root Password	>>	•••••
	Bind Type	>>	simple 💌
	SSL Bind Type	>>	simple 💌
	personClassNames	>>	inetOrgPerson
	groupClassNames	»	groupOfUniqueNames
	Keystore	»	
	supportedSasIMechanisms	>>	DIGEST-MD5
	First Name Attribute	>>	givenname
	Last Name Attribute	>>	sn
	Full Name Attribute	>>	cn
	Mail ID Attribute	>>	mail
	Telephone Number Attribute	>>	telephonenumber
	FAX Number Attribute	>>	facsimilenumber
	Postal Address Attribute	>>	address
	Title Attribute	>>	title

Configuring Novell eDirectory Server

4. Configure LDAP schema for users and roles

- 4.1 Create a new Organization
 - **1.** Create a new Organization from Novell iManager web console using eDirectory Administration > Create Object option.
 - **2.** Give organization name and context in which Organization should reside.

🙆 Novell iManager - Microsoft	Internet Explorer	
File Edit View Favorites Tools	s Help	At
🔇 Back 🝷 🐑 - 💌 🛃 (🏠 🔎 Search 👷 Favorites 🜒 Media 🚱 🍙 🍓 🚍 🛄 🗐 • 🆓	
Address Address //9. 184. 112. 111/nps	s/servlet/webacc	🗸 🄁 Go
Novell® iManager		
ADMIN		
Unrestricted Access		N
Roles and Tasks	Carrete Object	
All Categories	v Create Object	
eDirectory Administration	Select the object class to create.	
Copy Object		
Create Object	Available object dasses:	
Delete Object	Dynamic Group	
Modify Object	Group	
Move Object	Locality	
Kename Object	Organization	
eDirectory Maintenance	Organizational Person	
Groups	Organizational Unit	
Help Desk	Person	
TI I DID	Profile	
Novell Certificate Access		
Rovett Certificate Server	OK Cancel	
E Scheme		
I SHMP		
1 Users	×	0
		🖃 🐨 Internet
🔧 start 🚽 🕴 🖬 🗮 🍮	🦻 🔴 🍪 🛸 📿 👔 💼 > Fw: LDAP looku 🛛 🖉 Tivoli Directory Se 🦉 Contents - Micros	2 12:16 PM
🛃 🚱 👬 🔽	😰 😂 😰 🖉 Novell iManager 🐨 2 Microsoft Word 🕞	

Anter State Sta	nteri	net Explorer	. [🗗] 🗙
File Edit View Favorites Tools	Hel	p	
Sack • 🕑 - 💌 😰 🄇		🔎 Search 🤺 Favorites 🜒 Media 🔗 🖉 🧫 🌄 🛄 😏 🖏	
Address 👹 https://9.184.112.111/nps/	servle	et/webacc	🔁 Go
Novell® iManager			
ADMIN Unrestricted Access			Ν
Roles and Tasks			
All Categories	~	💩 Create Organization	
eDirectory Administration <u>Copy Object</u> <u>Create Object</u> <u>Delete Object</u> <u>Modify Object</u> <u>Modify Object</u> <u>Bename Object</u> eDirectory Maintenance Groups Help Desk LDAP NMAS Novell Certificate Access Novell Certificate Server Partition and Replicas Rights Schema Counte		Specify the object name to be created. Organization name: WPC Test Data Context: WPCLDAP_TREE4. OK Cancel	
+ Users	~		
@]		A District	
	() ()	2 ● > Fw: LDAP lookup ta ● Internet Explorer ● 2	4:37 PM hursday /23/2006

- 4.2 Create a new user
 - 1. Create a new User from the Novell iManager web console using the menu path **Users > Create User**.
 - 2. Select the above-created Organization for this user.
 - 3. Set NDS Password and Simple Password.

🔄 Novell iManager - Microsoft Int	ternet Explorer			_ 2 🛛			
File Edit View Favorites Tools Help							
🌀 Back 👻 🐑 🔺 😰 🎸	😋 Back 🔻 📀 - 🖹 🗟 🟠 🔎 Search 🤺 Favorites 🜒 Media 🤣 🎅 - 🌺 🚍 🛄 😒 - 🏂						
Address 🕘 https://9.184.112.111/nps/se	ervlet/webacc			💌 🄁 Go			
Novell _® iManager							
ADMIN		- 6					
Unrestricted Access				N			
Roles and Tasks	🚽 🗳 Create User			2			
All Categories				*=required			
eDirectory Administration	<u>~</u>						
eDirectory Maintenance	Username: *	Test User 1		<u>^</u>			
Groups	First name:	Test					
Help Desk	Last name: *	User 1		=			
LDAP	Full name:	Test Liser 1	7				
NMAS	rua name.	Test Oser T					
Novell Certificate Access	Context: *	WPC Test Data					
Novell Certificate Server							
Partition and Replicas	Password:	••••					
Rights	Retype password:	••••					
🗉 Schema	Note: Failure to enter a passw	ord will allow the user to login without a password.					
SNMP							
Users	Set simple password						
Create User Delete User	Simple password:			~			
Disable Account							
Enable Account	OK Cancel						
Modify User							
Done				Internet			
				(2) 200 L 4-40 PM			
	👐 🌌 🗩 🤜 🔤	okup ta	P 💀 🔥 🕁	Thursday			
) 🛃 🚾 🤅	🔄 😅 🗾 🕴 🔢 🖾	ord 👻		3/23/2006			

4.3 Create a new group

- 1. Create a new Group from the Novell iManager web console using the menu path **Groups > Create Group**.
- 2. Select the above-created Organization for this group.
- 3. Modify the Group and associate the Users to Groups.

🕙 Novell iManager - Microsoft Intern	et Explorer	_ 7 🗙
File Edit View Favorites Tools Help		
🌀 Back 👻 🐑 🖉 🏑	🔎 Search 🧙 Favorites 🜒 Media 🕢 🎓 چ 🧫 🔜 🚱 🕉	
Address 💰 https://9.184.112.111/nps/servlet	/webacc	💌 🄁 Go
Novell _® iManager		
ADMIN Unrestricted Access		Ν
Roles and Tasks	۵	
All Categories	🍪 Create Group	
eDirectory Administration	Specify the group name to be created.	
eDirectory Maintenance	Group name:	
Groups	Test Group 1	
Create Group	Context:	
Modify Group	WPC Test Data	
Modify Members of Group		
View My Groups	(To create a dynamic group, check this box)	
⊞ Help Desk		
E LDAP I	OK Cancel	
• NMAS		
Novell Certificate Access		
Novell Certificate Server		
Partition and Replicas		
Rights		
⊕ Schema		
SNMP		
Users		
H WAN Traffic		
	📄 🔮 Internet	
🦺 start 🚽 🚺 🖬 🗮 🥭 🔴 a	🥹 🕒 📿 🛛 🥮 > Fw: LDAP lookup ta 🥥 🖬 Internet Explorer 🔹 🖉 🖓 🖓 🖓 🖓 🖓 🖓 🖓 🖓	4:41 PM
j 🖉 🔛 🚾 👔	😜 🗾 🛛 🕅 🛛 Microsoft Word 🕞	3/23/2006

🕘 Novell iManager - Microsoft Inte	rnet Explorer	_ 0 🗙
File Edit View Favorites Tools H	lp	
🚱 Back 🔹 🐑 🔺 🛃 🏠	🔎 Search 🤺 Favorites 🜒 Media 🚱 🍙 - 🌺 🚍 🔜 😏	
Address Address //9.184.112.111/nps/serv	let/webacc	🛩 芛 Go
Novell _® iManager		
ADMIN Unrestricted Access		Ν
Roles and Tasks	Modify Group: 🚳 Test Group 1.WPC Test Data	8
All Categories	Capacel Security Duramic Members	
eDirectory Administration	Members	
eDirectory Maintenance		
 Groups Create Group Delete Group Modify Group Modify Members of Group View My Groups Help Desk LDAP NMAS Novell Certificate Access Novell Certificate Server Partition and Replicas Rights Schema 	Members: Test User 1.WPC Test Data	
± SNMP	Count: 0	~
± Users	OK Cancel Apply	
H WAN Traffic		
é l		Internet
<mark>- ≹; start</mark>) 🚦 🔤 💭 💭 & Ø 👭 <u>V</u> 2 ⊆	 W DAP lookup ta Internet Explorer W 2 Microsoft Word 	Image: Second system 4:42 PM Image: Second system Thursday Image: Second system 3/23/2006

5. Configuration Notes

5.1 Password Encryption Support

SHA-1 and Crypt Password encryptions are tested by importing the LDIF which has user objects with SHA/Crypt encrypted password through iManager web console.

- Go to eDirectory Maintenance -> Import Convert Export Wizard.
- Select Import data from file on disk and click next.
- Browse the file from disk to be imported and click next.
- Give the destination IP address and the login details. In the advanced settings select Allow forward references.



🕙 Novell iManager - Microsoft I	Interi	net Explorer	_ D 🗙
File Edit View Favorites Tools	Help		
🕒 Back 🔹 🐑 - 💌 🙋 🤇	6	🔎 Search 🤺 Favorites 🜒 Media 🕢 🎓 چ 🧫 🔜 🚱 😵	
Address 🙆 https://9.184.112.111/nps	/servle	t/webacc	🕶 🔁 Go
Novell® iManager	X		
ADMIN			_
Unrestricted Access			N
Roles and Tasks			
All Categories	~	ICE Wizard	8
Backup Configuration	~	C:\Documents and Settings\Administrator\My Documents\sandhya\LDAP\WPC Test Data.ldif	
Graft Tree		<u>A</u>	
Import Convert Export Wizard			
Indexes			
Log File		Salast the impact destination	^
Merge Tree		Select the import destination.	
Renaine Tree Repair eDirectory		Server DNS name/IP address:	
Repair Server		9.184.112.111	
Repair Sync	=	Durte Data	=
Repair via iMonitor		Port: 389	
Replica Repair		DEP file: Browse	
Replica Ring Repair		(Needed if a secure port is used.)	
Restore			
Service Manager		Anonymous login	
Groups		Authenticated login	
Help Desk		cn=admin o=company	
		User DN: User Sentenino-encovell)	
Create DAP Object			~
Delete LDAP Object			
LDAP Options		<< Back Next >> Cancel	
	~		
é		🔒 🧶 Internet	
🤧 start 🌒 🗄 📓 📼 🗮 🥔		😜 🐻 📿 🕴 🛑 > Fw: LDAP lookup ta 🧉 🛛 Internet Explorer 🕞 👘 👔	4:56 PM
	-		Thursday
) 🔗 🕑 🗰 <u>Va</u>	<i></i>	🐷 🔟 2 Microsoft Word 👻 👘 🖉 📜 🔤	3/23/2006

- 6. SSL Setup
- 6.1 Steps to extract self signed certificate for client:
 - 1. Go to eDirectory Administrator -> Modify Object.
 - i. Object name is selected from the Object Selector window. Click Object Selector.
 - ii. Select the <Tree>CA object, for example: WPCLDAP_TREE4 CA object.

 Object Selector (Browser) - Micro 	soft Internet Explorer	_ @ 🔀
Browse Search		
Look in:	Contents: (click object to select)	
Security	1. ··· (up one level)	
(Example: novell)		
Look for objects named:	KAP Select this object	
(Example: A*, Lar*, Bob)		
Look for these types:		
[All] [Rect] Apply	< Previous Next >> 22	
<u></u>	W → Pw: LDAP lookup ta Internet Explorer W → P W → P W → P W → P	C 3/23/2005

🕘 Novell iManager - Microsoft	Interr	net Explorer	_ 0 🔀
File Edit View Favorites Tools	s Help		
😋 Back 🝷 🕥 🕤 💌 🛃		🔎 Search 🤺 Favorites 🜒 Media 🤣 🍙 - 🌺 🥽 🛄 😒 - 🆓	
Address 🛃 https://9.184.112.111/np	s/servle	t/webacc	🛩 🔁 Go
Novell® iManager 🛛 🔜	SP		
ADMIN Unrestricted Access			N
Roles and Tasks		· · · · ·	
All Categories	~	Modify Object	
eDirectory Administration Copy Object Create Object Delete Object Move Object Rename Object e oDirectory Maintenance Groups Help Desk Dupp		Specify the object(s) to modify. Select a single object Selection Advanced Selection Object name: WPCLDAP_TREE4 CA. Security Object Selector OK Cancel	
NMAS Novell Certificate Access			
Novell Certificate Server			
Partition and Replicas			
Rights			
Schema			
III SNMP			
Users	~		
https://9.184.112.111/nps/servlet/f	rameser	vice?NPService=fw.LaunchService&NPAction=Delegate&delegate=base%2eModifyObject&launch 🔒 😁 Internet	
	9 😶 2 😋	 Fw: LDAP lookup ta Internet Explorer Image: A start of the start of	5:08 PM Thursday 3/23/2006

- 2. Go to Certificates -> Self Signed certificate -> Export.
 - Do you want to export the private key with the certificate? Select an output format. File in Base64 format. i. No
 - ii.
 - Click "Save the exported certificate to a file" -> Save the file. iii.

🕙 Novell iManager - Microsoft Inte	rnet Explorer		_ 8 🗙
File Edit View Favorites Tools H	elp		A.
🚱 Back 🝷 🕥 🕤 🖹 🛃 🏠	🔎 Search 🤺 Favorites 🜒 Media 🤣 🎯 🍚 🧾	⊗! - 2 <u>3</u>	
Address 💰 https://9.184.112.111/nps/serv	/let/webacc		🛩 ラ Go
Novell® iManager			
ADMIN			
Unrestricted Access			N
Roles and Tasks	Modify Object: 🙀 WPCLDAP_TREE4 CA.Security		2
All Categories	Conserve Certificates CPL Configuration		
eDirectory Administration	Public Key Certificate Self Signed Certificate		
Copy Object			
Create Object	Subject name:	OU=Organizational CA.O=WPCI DAP_TRFF4	
Modify Object	Issuer name:	OU=Organizational CA.O=WPCLDAP TREE4	
Move Object	Effective date:	Wednesday, February 22, 2006 12:47:28 AM	
Rename Object	Expiration date:	Monday, February 22, 2016 12:47:28 AM	
eDirectory Maintenance	Certificate status:	Click validate	
± Groups	Details Export Validate Replace	1	
Help Desk	Export		
+ LDAP			
NMAS			
Novell Certificate Access			
Novell Certificate Server			
Partition and Replicas			
± Rights			
± Schema			
± SNMP			
± Users	OK Cancel Apply		
javascript: doExport()		≙ (Internet
🤳 start 📄 📓 🔤 🥔 🗐	Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system Image: Second system	2 2 4 2	> ⇒ = 10 ≤ 5:15 PM ⇒ 1 (0) → 10 <

3. Go to Novell Directory Server -> Create Trusted Root Container -> Give a Trusted Root Container name and Context.

Novell iManager - Microsoft In	Internet Explorer	
File Edit View Favorites Tools	Help	
🔇 Back 🔹 🜍 - 💌 😰 🦿	🏠 🔎 Search 🤺 Favorites 🜒 Media 🤣 🍰 - 🌺 🔜 🛄 😏 - 🎎	
Address 🚳 https://9.184.112.111/nps/s	s/servlet/webacc	🛩 🛃 Go
Novell® iManager		N
Roles and Tasks	R country Transferd Based Controller	
All Categories	Create Trusted Root Container	
eDirectory Administration eDirectory Maintenance Groups Help Desk DAP NMAS Novell Certificate Access Novell Certificate Access Novell Certificate Access Create CRL Object Create Safe Service Object Create Trusted Root Container Create User Certificate	Specify the object name to be created. Trusted Root Container WVPC Test Data Root Container Context: WPC Test Data OK Cancel	
Partition and Replicas		
I Rights		
🗉 Schema		
e	A Sector A S	
🤳 start 🚽 📃 🔤 🥔	● ● ≫ > Fw: LDAP lookup ta ● 2 Internet Explorer ●	6:10 PM Thursday

4. Create a Trusted Root with the above container and certificate file created in step2.

Novell iManager - Microsoft Intern File Edit View Eavorites Tools Help	et Explorer	
🔇 Back - 🕥 - 💌 😰 🏠	🔎 Search 🤺 Favorites 🜒 Media 🤣 🎯 - چ 🚍 🛄 🞯! - 🆓	~
Address Address https://9.184.112.111/nps/servle	t/webacc	🕶 🔁 Go
Novell® iManager		
ADMIN Unrestricted Access		N
Roles and Tasks	Create Trusted Poet Cartificate	হি
All Categories		
	To create a Trusted Root Certificate, enter a name, specify the container where the Trusted Root will be created, and specify the file containing the Trusted Root Certificate data. Name: WPC Test Data Root Container: WPC Test Data Root Container.WPC Test Dat P To Certificate file: C:\Documents and Settings\Administrator\My Documents Browse OK Cancet	
Partition and Replicas		
1 Rights		
🖲 Schema		
javascript: okBtnPressed()	🔒 🧶 Interne	t
🤧 start 📄 📰 🔤 🔊 🕮	2 0 > Fw: LDAP lookup ta 2 Internet Explorer 2 2 Microsoft Word	6:22 PM Thursday 3/23/2006

- 5. Go to eDirectory Administration -> Modify Object -> Modify the Trusted Root object (which will be under Trusted root container).
 - Export the certificate in Base 64 format and save the certificate.



6. You have now created a file that holds your own root certificate. This must be imported to all communication partners that will connect to the server through SSL.

6.2 SSL Setup – Client Side (WPC end)

- 1. Get the .b64 file generated in the above steps in to the WPC environment.
- 2. Use the keytool command to import this in to the JVM. keytool -import -trustcacerts -keystore cacerts -storepass changeit noprompt -alias mycert -file <cert_file_generated>
- 3. Change the location of the cacerts file in the keystore variable in the login script. If the file that was generated in the step2 was in /home/sgopan/cert/cacerts, make the value for the keyStore variable to this location.

Note: Set the bindType variable to ssl and sslBindType to either simple or DIGEST-MD5.

7. Changes required in the Login Script for Novell (DIGEST-MD5)

The login script has appropriate sections that describe the steps to be followed to enable SASL Bind for Novell.

Novell expects the principal to be prefixed with dn:, followed by the entryDn unlike Tivoli where the just the naming attributes value would be sufficient for the SASL Bind.

Configuration requirement for SUNONE Directory Server

8. Creating a Directory Tree

Follow the instructions given in the link <u>http://docs.sun.com/source/816-6698-10/suffixes.html</u> to create a directory tree structure.

8.1 For Simple Bind

1. In the login script the parentDN for the users and for the groups should be set atleast to the top level DN e.g "o=IBM".

8.2 For SASL Bind

- 1. The changes done in the login script for SASL Bind are similar to the changes done for Novell eDirecotry. The Context.SECURITY_PRINCIPAL should have the full entry DN with prefix as "dn:".
- 2. In the login script the parent DN value should have atleast the top level dn. For e.g. "o=IBM".
- 3. The fully qualified host name of the server should be entered in the etc/hosts file of the client machine. The provider url should be the fully qualified host name of the server. Using IP address for provider url will throw protocol error.

Following are the changes required to be done in the login script for SUN ONE Directory Server :

The login script has appropriate sections that describe the steps to be followed to enable SASL Bind for Sun-One.

Sun-One like Novell expects the principal to be prefixed with dn: , followed by the entryDn unlike Tivoli where the just the naming attributes value would be sufficient for the SASL Bind.

8.3 For SSL

Refer the following url : <u>http://docs.sun.com/source/816-6704-10/ssl.html</u>.

Follow the steps given below for server side setup :

- 1. Request for a certificate for the certifying authority. E.g <u>https://www.verisign.com/products-services/security-services/ssl/index.html</u>.
- 2. To request for a certificate you need to generate a CSR(Cerficate Signing Request).
- Go to Tasks -> Manage Certificates -> Server Certs (Tab) Enter the details required for generating the certificate like the hostname of the server, company name, organization name, city, country etc.

Certificate Re	juest Wizard	
Requestor Infor	nation	2 of 4
Server name:	2fdibm412.in.ibm.com	
Organization:	IBM	
Organizational unit:	WPC-GDS	
City/locality:	Bangalore	
State/province:	Karanataka	
Country/region:	N India	
		Show DN
	< Back Next > Car	ncel <u>H</u> elp

- 4. After going through these steps a CSR will be generated. This CSR can be used to request a certificate from Verisign.
- 5. A mail will be sent to you with a certificate of 15 day validity period. The certificate would be as below. It includes the header and the footer.

⁻⁻⁻⁻BEGIN CERTIFICATE----

MIIEOjCCA6OgAwIBAgIQN77E+RcOX6hx5pJXsfNQIjANBgkqhkiG9w0BAQUFADCB jDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAwLgYDVQQL EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xMjAwBgNV BAMTKVZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBSb290IENBMB4X DTA1MTIyNzAwMDAwMFoXDTA2MDExMDIzNTk1OVowgbAxCzAJBgNVBAYTAklOMRIw EAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcUCUJhbmdhbG9yZTEMMAoGA1UEChQD SUJNMRAwDgYDVQQLFAdXUEMtR0RTMTowOAYDVQQLFDFUZXJtcyBvZiBlc2UgYXQg d3d3LnZlcmlzaWduLmNvbS9jcHMvdGVzdGNhIChjKTA1MR0wGwYDVQQDFBQyZmRp Ym00MTIuaW4uaWJtLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAs1YP QtIIQu44aU55YmAkbld96SUIolK3wYfmQ1gW21c2Lihc8IfqGOH7r9HMjpq78TOZ 2c/FB3awI1U8uBl239wMTbneiKbP2jWnO/YCAk0z53Bt2UZHdCxaGMyjNnoxVD9C

HxRZJ34d9EqolFcuyNLFvLTfgvc/fYAMwrlXM78CAwEAAaOCAXUwggFxMAkGA1Ud EwQCMAAwCwYDVR0PBAQDAgWgMEcGA1UdHwRAMD4wPKA6oDiGNmh0dHA6Ly9TVlJT ZWN1cmUtY3JsLnZ1cmlzaWduLmNvbS9TVlJUcmlhbFJvb3QyMDA1LmNybDBKBgNV HSAEQzBBMD8GCmCGSAGG+EUBBxUwMTAvBggrBgEFBQcCARYjaHR0cHM6Ly93d3cu dmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EwHQYDVR01BBYwFAYIKwYBBQUHAwEGCCsG AQUFBwMCMDQGCCsGAQUFBwEBBCgwJjAkBggrBgEFBQcwAYYYaHR0cDovL29jc3Au dmVyaXNpZ24uY29tMG0GCCsGAQUFBwEMBGEwX6FdoFswWTBXMFUWCWltYWdlL2dp ZjAhMB8wBwYFKw4DAhoEFI/10xqGrI2Oa8PPgGrUSBgsexkuMCUWI2h0dHA6Ly9s b2dvLnZ1cmlzaWduLmNvbS92c2xvZ28uZ21mMA0GCSqGSIb3DQEBBQUAA4GBAJkH 7bLGW4CDUyc1bG0dIg/c15Ab/5fd+MhVss1RsGZEevevjkbqbhwktKtGTQGR4ti1 sffCc0Xh6ksRB0Td0bf7jch0z3tTe92EHY++YcgPXYOVdKNi4MPKZ+bRMJr7r5Ry mINY3LXU2JLGasf3ZInInu44y9jqbTEXC7oqG07M _----END CERTIFICATE-----

6. Install this certificate in your server. To do this you need to go to Tasks -> Manage Certificates -> Server Certs (Tab) -> Install (button).

Wanage Certificates: slapd-2fdibm412						
Security Device: internal (software) Change Password						
Server Certs CA Certs Revoked Certs						
Server certificate are us	ed for server authentica	tion to clients.				
Certificate Name	Issued To	Issued By	Expiration Date			
server-cert	2fdibm412.in.ibm.com	VeriSign Trial Secure	. Wed Jan 11 05:29:59			
Detail	Request Ren	ew	Delete			
			stall a new certificate			
			Close <u>H</u> elp			

 After installing the certificate you need to enable SSL in the server. To do this go to Configuration (Tab) -> Encryption (Tab).

2fdibm412.in.ibm.com - iPlan	net Directory Server - 2fdibm412	_ 7 ×
Console Edit View Object Help		
iPlanet Directory Server		
Tasks Configuration Direc	tory Status	
Base Computer Sec Instantial Longon Data Instantial Longon Data Instantial Logs Instantial Logs Instantial Logs Instantial Logs	Setting: Performance Encryption SIMP Manager Finable SSL for this server Certificate: generic-ent Copher: Settings Certificate: generic-ent Copher: Settings Cert Authentication C Do not allow clert authentication C Require clert authentication Use SSL in Planet Console	
	<u>Save</u> Reed	Help

The "Enable SSL" checkbox should be checked. Check the "Use this cipher family" checkbox and select the cerficate which you have installed. Under "Client Authentication" section, select "Do not allow client authentication".

Follow are the steps below for client side setup :

- 1. Save the certificate which you had obtained from verisign in a file. Save it in a folder where you want to generate your keystore.
- 2. Use certutil for creating a certificate database.

certutil -N -d *certdir* (Where certdir is the directory where certificate db is to be generated. For eg the current directory).

This will gererate cert7.db and key3.db in the directory specified with -d option.

3. Import the certificate which you have saved as part of step 2 in the certificate database using the following command.

certutil -A -n nameoftheserver -t trustargs -i cerfile -d certdir

Eg certutil -A -n "2fdibm412.in.ibm.com" -t "C,C,C" -i iplanetcert.cert -d.

4. To check if the certificate has been imported properly. Use the following command.

certutil -L -n "2fdibm412.in.ibm.com" -d.

5. Get the binary format for the certificate using the following command.

certutil -L -n "2fdibm412.in.ibm.com" -d . -r > checkcert

This will generate the file checkcert which is the binary format of the certificate.

6. Using keytool import the certificate in keystore.

keytool -import -trustcacerts -keystore cacerts -storepass changeit -noprompt - alias ipcert -file checkcert

Configuring Microsoft Active Directory Server

9. Configure LDAP schema for users and roles

9.1 Create a new Domain

A new domain is created by creating the first domain controller. To do this, install Active Directory on a member server running Windows Server 2003 by using the Active Directory Installation Wizard. The wizard uses the information that you provide to create the domain controller and create the domain within the existing domain structure of your organization. Depending on the existing domain structure, the new domain could be the first domain in a new forest, the first domain in a new domain tree, or a child domain of an existing domain tree.

A domain controller provides the Active Directory Server's directory services to network users and computers, stores directory data, and manages user and domain interactions, including user logon processes, authentication, and directory searches.

9.2 Create a new Organization

1. Create a new Organization from Microsoft Management Console (MMC) by selecting the domain and right clicking and choosing new OrganisationalUnit.

2. Fill in the name of the organization.



9.3 Create a new user

1. Create a new User from MMC by selecting the OrganizationalUnit created above and right clicking and choosing new InetOrgPerson

2. Complete the process by filling in the details.

line computers and Computers				
				_8×
Active Directory Users and Computer: Test Data 4 ob	iects			
Saved Queries Name	Туре	Description		
E 🗊 wpc.com	User			
Builtin 🕵 test user2	User			
Computers Stestgroup1	Security	Group		
EpreignSecurityPrincipals	InetOrg	Person		
Tech Data				
Delegate Control				
Mo <u>v</u> e				
Find				
New Computer				
All Tasks Contact				
Group				
View InetOrgPet	son			
New Window from Here MSMO Que	ue Alias			
Cut Organizatio	onal Unit			
Delete Printer				
Rename User				
Refresh Shared Fol	der			
Export List				
Properties				
Help				
Create a new object				
🎢 Start 🔞 进 😪 📑 Manage Your Server	3.182.149.159 - Remote	Active Directory User		🍓 🛃 🄗 10:09 AM

Active Directory Users and Comp	uters				
Eile Action View Window He					
		(🖄 Y 🍕 🗹			
Active Directory Users and Computers	Test Data 4 objects				
□-∰ wpc.com	Name	Туре	Description		
Builtin Computers Gong Domain Controllers ForeignSecurityPrincipals Gong Data Users	New Object - InetOrg	erson wpc.com/Test Data			
	<u>F</u> irst name:	Test	Initials:		
	Last name:	User1			
	Full name:	Test User1			
		,			
	User logon name:	@₩₽9.997	_		
		Tempercom			
	User logon name (pr	E-Windows 2000):			
	Imrei	Less Oser			
		< <u>B</u> ack	<u>N</u> ext > Cano	cel	
	1 cm	(-		
💋 Start 🔯 🥭 🍓 🔄 Manage 1	Your Server 🛛 😔 9	.182.149.159 - Remote	🖇 Active Directory Use	f	🌯 🛃 🏈 10:12 AM

9.4 Create a new group

- 1. Create a new Group from MMC by selecting the OrganizationalUnit created and right clicking and choosing new Group
- 2. Complete the process by filling in the details.

Active Directory Users and Co	nputers		
Eile Action View Window	Help		_8×
• 🔿 🗈 🖬 👗 🛍 🗙	7 🗗 🖧 🕄 🐮 🖉 🖄 🖓 🍕 📁		
Active Directory Users and Compu	rs Test Data 4 objects		
- Saved Queries	Name Type	Description	
- 📋 Builtin	S test user User User User		
Computers Domain Controllers	Security Gro	ир	
ForeignSecurityPrincipals	g user1 InetOrgPers	on	
Delegate Contro			
Move			
- index			
All Tasks	Contact		
View	Group		
New Window fro	Here MSMO Queue Alias		
Cu <u>t</u>	Organizational Unit		
<u>D</u> elete	Printer		
Rena <u>m</u> e Refresh	User Shared Folder		
Export List			
Properties			
Help			
-2-4			
	u		
ate a new object	<u>a</u>]		
ate a new object Start 🕜 🥭 સ 💽 Man	e Your Server	Active Directory User	 10:09 AM
ate a new object Start 🕝 🏈 🖓 🔟 Man	ge Your Server 39.182.149.159 - Remote	Active Directory User	🗞 🔊 🖉 🔊 10:09 AM
ate a new object Start 🕝 🔗 🕄 🧾 Man Active Directory Users and F	pe Your Server 9.182.149.159 - Remote 🧭	Active Directory User	الم 10:09 AM
ate a new object Start @ @ ?	pe Your Server 😥 9.182.149.159 - Remote 🧭 noutcers Help To TEAL 169 140 140 75 460 77	Active Directory User	اھ 10:09 AM اھ ا
te a new object Start @ @ @ @	pe Your Server 😥 9.182.149.159 - Remote 🧭 mputers Help T D G C2 20 20 7 40 20 er Test Data 4 objects	Active Directory User	() () () () () () () () () () () () () (
te a new object Start @ @ @ @	pe Your Server 20,182.149.159 - Remote 20 mputers Help Total 1 CP 20 20 20 20 20 20 Total 2 CP 20 Total 2 CP 20 Type Type	Active Directory User	() () () () () () () () () () () () () (
te a new object Start () () () () () () () () () () () () ()	pe Your Server 국 9,182,149,159 - Remote mputers Help CT 문 문 전 한 전 종 전 err Test Data 4 objects Name Type New Object - Group	Active Directory User	() () () () () () () () () () () () () (
te a new object Start @ @ @ @	pe Your Server 9,182.149.159 - Remote mputers Help Test Data 4 objects Name Type Name Type	Active Directory User	() () () () () () () () () () () () () (
te a new object start @ @ @ @	e Your Server 9,182,149,159 - Remote hputcers Help T Es Data 4 objects Name Name Type Name Create in: wpc.com/Test Data	Active Directory User	ຈິງ 🖗 🔊 10:09 AM [ສ] [ສ]
te a new object Start ② ③ ③ ③ ③ Man Active Directory Users and C Ele Action View Window → C I III Window → C IIII Window → Window → Swed Queries → wrpc.com → Bulkin ← Computers → Dorain Controllers ← ForeignSecurityPrincipals ← Test Data ← Users	e Your Server 9,182,149,159 - Remote hputers Help Tost Data 4 objects Name Test Data 4 objects Name Type Create in: wpc.com/Test Data Group name:	Active Directory User	ම ම ව 10:09 AM
te a new object start @ @ @ @	pe Your Server 2 9,182,149,159 - Remote 2 mputers Help Eff D:	Active Directory User	ම ම ව 10:09 AM
te a new object start @ @ @ @ @ Man Active Directory Users and C Ele Action View Window P C Com View Window Saved Queries Saved Queries Window Builtin Computers Computers PoreignSecurityPrincipals Computers Data Users	pe Your Server 9,182,149,159 - Remote puters Help Test Data 4 objects Name Test Data 4 objects Create in: wpc.com/Test Data Group name: TestGroup1 Group name (pre-Windows 2000);	Active Directory User	🗞 🔮 🏈 10:09 AM
te a new object Start 🕜 🏈 🕄 Man Active Directory Users and Comp Saved Queries Saved	ge Your Server 9.182.149.159 - Remote puters Help To Ep 12 2 2 2 2 2 rest Data 4 objects Name Type Name Type Create in: wpc.com/Test Data Group name: TestGroup1 Group name (pre-Windows 2000): TestGroup1	Active Directory User	🗞 🔮 🔗 10:09 AM
te a new object Start ② ② ③ ③ ③ Man Active Directory Users and Comp Saved Queries Saved	pe Your Server 29.182.149.159 - Remote 20 hputers Help Test Data 4 objects Name Type Frew Object - Group Create in: wpc.com/Test Data Group name: TestGroup1 Group name (pre-Windows 2000): TestGroup1 Group scope Group Group to the first of	Active Directory User	کی اوری کی کی کی کی کی کی کی ک اوری کی
te a new object Start 🚱 🏚 🖓 🔰 Man Active Directory Users and C Ele Action View Window Active Directory Users and Comp Saved Queries Vanctory Users and Comp Saved Queries Vanctory Users and Comp Saved Queries Saved	pe Your Server 2 9.182.149.159 - Remote 2	Active Directory User	े जिल्लाम विविध
te a new object Start @ @ @ @ Man Active Directory Users and C Ele Action View Window → C Mon Active Directory Users and Comp Saved Queries Vape.com Builtin Computers Domain Controllers — PoreignSecurityPrincipals @ Test Data Users	pe Your Server 2 9.182.149.159 - Remote 2 poutcers Help erf Test Data 4 objects Type remove Total 4 objects Name TestGroup1 Group name: TestGroup1 Group name: TestGroup1 Group name (pre-Windows 2000): TestGroup1 Group name (pre-Windows 2000): Group name (pre-Windo	Active Directory User	کی ا0:09 AM اوریا اوریا
te a new object Start ② ③ ③ ③ ③ Man Active Directory Users and C Ele Action View Window → ① ① ③ ④ ② ◎ Man Active Directory Users and Comp ⑤ Saved Queries ⑤ Vape.com ⑤ Builtin C Computers ⑧ Domain Controllers ⑥ Test Data ⑥ Users	pe Your Server 2 9.182.149.159 - Remote 2	Active Directory User	کی ان 0:09 AM ۱۵:09 AM
Active Directory Users and C Ele Action View Window C IN View Wi	pe Your Server 2 9.182.149.159 - Remote 2 pouters Help Test Data 4 objects Name Type Petw Object - Group Petw Object - Group Create in: wpc.com/Test Data Group name: TestGroup1 Group name (pre-Windows 2000): TestGroup1 Group name (pre-Windows 2000): Group name (pre-Windows 2000	Active Directory User	کی ان 0:09 AM ا ان کی ان ان 9 AM
Active Directory Users and C Ele Action View Window Computers Saved Queries Wec.com Builtin Computers Domain Controllers ForeignSecurityPrincipals Test Data Users	ge Your Server 9.182.149.159 - Remote pouters Help Test Data 4 objects Name Frew Object - Group Create in: wpc.com/Test Data Group name (pre-Windows 2000): TestGroup1 Group name (pre-Windows 2000): TestGroup1 Group sope Data Group to the formation of the formati	Active Directory User	MA 90:01 <table-cell> کی کی ا</table-cell>
Active Directory Users and C Ele Action Yew Window C III X Computers Active Directory Users and Comp Saved Queries Wpc.com Doman Controllers PoreinSecurityPrincipals Test Data Users	ge Your Server 9,182,149,159 - Remote mputers Help Test Data 4 objects Name Test Carup 1 Group name (pre-Windows 2000): TestGroup 1 Group name (pre-Windows 2000): Group name (pre-Win	Active Directory User	L COLUMN
ate a new object Start	ge Your Server 9,182,149,159 - Remote mputers Help Test Data 4 objects Name Type New Object - Group Vew Object - Group Create in: wpc.com/Test Data Group name: TestGroup1 Group name (pre-Windows 2000): TestGroup1 Group name (pre-Windows 2000): Group name (pre-Windows 2000): TestGroup name (pre-Windows 2000): Group name (pre-Windows 2000): Grou	Active Directory User	L 0109 AM
Active Directory Users and Comp Start @ @ @ @ @ Man Active Directory Users and Comp Saved Queries 9 wpc.com ■ Builtin Computers Domain Controllers ■ Domain Controllers	ge Your Server	Active Directory User	10:09 AM
te a new object Start ② ③ ③ ③ ③ Man Active Directory Users and C Ele Action View Window ⇒ C © ③ & C © Saved Queries ⇒ wpc.com Domain Controllers Domain Controllers © Test Data © Users	ge Your Server	Active Directory User	کی ا0:09 AM (۱۳۵۵)
ate a new object Start Start Computers and Comp Saved Queries Saved Que	ge Your Server	Active Directory User	الله الله 10:09 AM الله الله الله الله الله الله الله الله
te a new object Start Start Computers Computers Domain Controllers PoreignecurityPrincipals Test Data Users	pe Your Server 2 9.182.149.159 - Remote 2 Topulters Help Tost Data 4 objects Name Tost Data 4 objects Name Tost Data 4 objects Name Tost Data 4 objects Name Tost Data 4 objects Create in: wpc.com/Test Data Group name: TestGroup1] Group name (pre-Windows 2000): TestGroup1 Group name (pre-Windows 2000): TestGroup (pre-Windows 2000): Group (pre-Windows 2000): TestGroup (pre-Windows 2000): TestGr	Active Directory User	الا ال ال ال ا
te a new object Start 🚱 🏚 🖓 Man Starte Directory Users and Comp Saved Queries Saved	pe Your Server 2 9.182.149.159 - Remote 2	Active Directory User	الله الله الله الله الله الله الله الله
te a new object Start ② ③ ③ ③ ③ ③ Man Active Directory Users and C Ele Action View Window → ① ① ③ ④ ④ ④ ○ Saved Queries ¥ vpc.com ⊕ Domain Controllers ⊕ PoreignSecurityPrincipals @ Test Data ⊕ Users	pe Your Server 2 9.182.149.159 - Remote 2	Active Directory User	▲ ● ● ● 10:09 AM
Active Directory Users and C Ele Action View Window Computers Builtin Computers Domain Controllers PoreignecurityPrincipals Test Data Users	pe Your Server 9.182.149.159 - Remote pe Your Server 9.182.149.159 - Remote providers Help For Test Data 4 objects Name TestGroup1 Group name: TestGroup1 Group name: TestGroup name: TestGroup name: TestGroup1 TestGroup name: TestGroup name: TestGroup name	Active Directory User	

10. Configuration Notes:

10.1 Configuring Microsoft Active Directory for SSL access and Extract Self Signed Certificate for client

Ensure that the Active Directory domain is set up and Certificate Authority (CA) is installed on the system.

If the Certificate Authority (CA) is not installed, you can install it on your Active Directory server as follows:

- 1. Click Start -> Control Panel -> Add or Remove Programs.
- 2. Click Add/Remove Windows Components and select Certificate Services.
- 3. Follow the procedure provided to install the Certificate Services CA.

10.1.1 Verifying that SSL is enabled on the Active Directory server

To verify that SSL has been enabled on the Active Directory server, do the following:

- 1. Ensure that Windows Support Tools is installed on the Active Directory machine. The **suptools.msi** setup program is located in the \Support\Tools directory on your Windows installation CD.
- Select Start -> All Programs -> Windows Support Tools -> Command Prompt. Start the ldp tool by typing ldp at the command prompt.
- 3. From the ldp window, select **Connection -> Connect** and supply the host name and port number (**636**). Also select the SSL check box.

Note:

Ensure that you type the Active Directory domain server name correctly.

If successful, a window is displayed listing information related to the Active Directory SSL connection. If the connection is unsuccessful, restart your system, and repeat this procedure.

10.1.2 Exporting the certificate from the Active Directory server

To export the CA certificate from the Active Directory server, follow these steps:

- 1. Log on as a Domain Administrator to the Active Directory domain server
- 2. Export the certificate from the Active Directory server to a file. To do so, follow these steps:

- a. Click **Start** -> **Control Panel** -> **Administrative Tools** -> **Certificate Authority** to open the CA Microsoft Management Console (MMC) GUI.
- b. Highlight the CA machine and right-click to select **Properties** for the CA.
- c. From General menu, click View Certificate.
- d. Select the **Details** view, and click the **Copy to File** button on the lowerright corner of the window.
- e. Use the Certificate Export Wizard to save the CA certificate in a file.

Note: You can save the CA certificate in either DER Encoded Binary X-509 format or Based-64 Encoded X-509 format.

10.1.3 Importing the certificate in WPC environment

- a) Get the file generated in the above steps in to the WPC environment
- b) Use the keytool command to import this in to the JVM keytool -import -trustcacerts -keystore cacerts -storepass changeit noprompt -alias mycert -file <cert_file_generated>
- c) Change the location of the cacerts file in the keystore variable in the login script. If the file that was generated in the step b was in /home/sgopan/cert/cacerts, make the value for the keyStore variable to this location.

Set the bindType variable to ssl and sslBindType to either simple or DIGEST-MD5

Note:

1. For DIGEST-MD5 to work, the user's password has to be stored in reversible encryption format.

2. User and Group parent DN fields are mandatory, and has to be filled up with domain names E.g. dc=wpc,dc=com is a valid DN for wpc.com domain.

Configuring Lotus Domino Server 6.5

11. Configure LDAP schema for users and roles

11.1 Create a new Person

- 1. Create a new Person (User) using the menu path People > Add Person.
- 2. Enter details like user id first name, last name and Password.



	WPCLDAP.COM Domain	1 Welcome 🗙 🕼 New Person	×		
M	Save & Close	kamine Internet Certificate(s)	Examin	e Notes Certificate(s) (Ӿ Cancel
	Person				Angla
	Basics Work/Home Ot	her Miscellaneous Certific	ates Roami	ng Administration	
	Basics			Mail	
	First name:	^r Test_		Mail system:	r Notes 💵
	Middle name:	Г 		Domain:	Г
	Last name:	[©] User1 ⊒		Mail server:	r j
	User name:	[╔] TestUser1 _		Mail file:	۲
	Alternate name:		2	Forwarding address:	Г
			č	Internet address:	Г
	Short name/UserID:	ି TestUser1 ୍ର		Format preference for	″ ″Keep in senders' format⊿ ∵
	Personal title:			Mana mana ini ang mana mana mana mana mana mana mana	
	Generational qualifier:	r J		When receiving unencrypted mail	P
	Internet password:	^r test_		encrypt before storing	in ^{"No} I
	Preferred language:	r J		your mailfile:	
		* soot			

11.2 Create a new group

- 4. Create a new Group from Lotus client using the menu path Groups > Add Group.
- 5. Modify the Group and associate the Users to Groups.

WPCLDAP.COM Domain A Welcome X				
People & Groups Files Server Messaging Replication Configuration				
Server: Idapsrv5/wpc_domino Release 6.5.4 on Windows NT 5.0	∽Tools			
▼ U Domino Directories ▼ U wpcldap.com's Directory ▼ M People ↓ by Organization ▼ M Groups ↓ by Organization ↓ M ail-In Databases_Reso M Policies ➡ Settings ➡ Certificates	p			
Alt Language Info Alt Canguage Info	roup1 roup2 roup_1 p1 p1 pcalDomainAdmins pcalDomainServers therDomainServers			
WPCLDAP.COM Domain 🏼 Welcome 🗙 🛄 New Group 🗙				
🗑 Save & Close 🗿 Refresh 🔊 Sort Member List 🛞	Cancel			
Multi-purpose group Basics Comments Administration	dista.			
Basics	Group type description			
Group name: TestGroup1				
Group type: Category: Description: Mail Domain: Internet Address: Members: TestUser1	'Multi-purpose' groups are the default group type and used in most situations. They can be used for access control and email purposes.			
Comments about t	e connection description			

11.3 Configuration Notes

Password Encryption Support

Lotus notes do not support password encryption.

11.4 SSL Setup

11.4.1 Steps to set up the SSL at the server side:

- 1) Create a key ring
- 2) Create a certificate request.
- 3) Get a trial certificate or full fledge certificate from the verisign or any other CA.

4) Install the certificate which has been obtained from the CA. If the CA is not trusted then the certificate of CA needs to be installed prior to installation of server certificate.

5) Go to Admin- \rightarrow port---internet port input the key ring file which contains the server certificate and key pair of server.

6) Go to Admin- \rightarrow port---internet port---Directory- Enable the SSL.

11.4.2 SSL Setup – Client Side (WPC end)

- d) Use the server side trial certificate for importing to the client side jvm
- e) Use the ikey man/keytool command to import this in to the JVM keytool -import -trustcacerts -keystore cacerts -storepass changeit noprompt -alias mycert -file <cert_file_generated>
- f) Change the location of the cacerts file in the keystore variable in the login script. If the file that was generated in the step **b** was in /home/ksanjay/cert/cacerts, make the value for the keyStore variable to this location.

Use the standard script for testing the SSL and simple binding.

Lotus does not support SASL.

Configuring Tivoli Directory Server

12. Configure LDAP schema for users and roles

- 12.1 Create a new realm
 - i. Create a new Realm from the IBM Tivoli Directory Server Web Administration Tool using the menu path **Realms and Templates > Add Realm**.
 - ii. Complete all the required fields.
- iii. Select the Object Class *domain* as the Parent DN.

Tivoli Directory Server Web A	dministration Tool - Microsoft Internet Explorer	
File Edit View Favorites Tools	Help	🥂 🕹 💦 🕹 🖓
🕒 Back 🝷 🐑 💌 🛃 🄇	🏠 🔎 Search 🧙 Favorites 🜒 Media 🚱 🔗 🍓 🚍 🛄 😒 🖓	
Address 🛃 http://9.184.114.80:9080/I	DSWebApp/IDSjsp/IDSConsoleFrameWork.jsp	🛩 🄁 Go
Tivoli. Directory Server Web	Administration Tool	
Introduction	OO Iocalhost	00
<u>Iser properties</u>	Add realm	Logfiles Help
Server administration		
Schema management	Copy settings from realm	
Directory management	×	
The second	Realm name	
	* myrealm	
Add user template	Parent DN	
Manage user templates	* dc=wps,dc=com	Browse
Add realm		
Users and groups		
Cone Done		Internet
🛃 start 🚽 🕴 🖬 🗮 🥥	🌐 🥹 🛸 🔍 🕴 🛑 Sandhya - Inbox - Lo 🏾 🏠 My Documents	C
	🔄 😄 🔽 👘 Configuration TDS.do 🖉 Tivoli Directory Serve	

12.2 Create a new user template

- i. Create a new User Template from the IBM Tivoli Directory Server Web Administration Tool by clicking **Realms and Templates > Add User Template**.
- ii. Key in above created realm entry as the Parent DN. Select the Structural object class as *inetOrgPerson*.
- iii. Edit the Required attribute tab to include all the following list of required attributes:
 - Cn
 - Sn
 - Uid (This is the Naming Attribute)
 - Mail
 - TelephoneNumber
 - TelexNumber
 - postalAddress
- iv. Associate this User Template with the above created Realm using the menu path Realms and Templates > Manage Realms > Edit.

🕙 Tivoli Directory Server Web A	Administration Tool - Microsoft Internet Explorer		_ 7 🗙
File Edit View Favorites Tools	Help		1
🚱 Back 🝷 🐑 💌 🗾 🤇	🏠 🔎 Search 🤺 Favorites 🜒 Media 🤣 🔗 - 嫨 🖂 🛄 😒 - 🖓		
Address 🛃 http://9.184.114.80:9080/I	DSWebApp/IDSjsp/IDSConsoleFrameWork.jsp		💌 🄁 Go
Tivoli. Directory Server Web	Administration Tool		ibn.
Introduction	O O D localhost		0 0
User properties	Add user template		Logfiles Help
Server administration			
• 📄 Schema management	Copy settings from template		
Directory management		~	
Replication management	User template name		
 Realms and templates 	* mytemplate		
Add user template	Parent DN		
Manage user templates	* dc=wps,dc=com Brows	ie	
Manage realms			≡
Users and groups			
Logout			
			~
			^
	2		×
Uone			Internet
🥑 start 🚽 📳 🖬 🗮 🥔	🔲 ờ 」 📿 👔 🌐 Sandhya - Inbox - Lo 🛛 🏠 My Documents) 🚟 🕰 🆕 11:17 AM
/ 🖓 💾 🔽	😂 🔁 🕴 🗐 Configuration TDS.do 🖉 Tivoli Directory Serve	6 6 6 6	3/27/2006

12.3 Create a new user

- i. Create a new User from the IBM Tivoli Directory Server Web Administration Tool using the menu path Users and Groups > Add User.
- ii. Select the above-created realm as Realm for this user.
- iii. Key in the "Required" attribute tab to include all the above-mentioned attributes.



Tivoli Directory Server Web A	dministration Tool - Microsoft Internet Explorer	_ 2 🛛
File Edit View Favorites Tools	Help	AT 10
🌀 Back 🝷 🕥 🕤 🗾 🛃 🄮	🏠 🔎 Search 🤺 Favorites 🜒 Media 🤣 🍰 - 🌺 🔜 🛄 🗐 - 🖓	
Address 🛃 http://9.184.114.80:9080/II	SWebApp/IDSjsp/IDSConsoleFrameWork.jsp	🛩 ラ Go
Tivoli. Directory Server Web A	Administration Tool	K 🛃 IEM.
Introduction	OO Iccalhost	00
Diser properties	Add user	Logfiles Help
Server administration		
Schema management	Realm	
<u>Directory management</u>	myrealm	
The second	Naming attribute	
Realms and templates	sn	=
 Users and groups 	*testuser1	=
Add user		
Manage users Find uppers	Degrating to *CD	
Add group	testuser1 Multiple values	
Manage groups	User groups	
Find groups	testuser1 Multiple values	
Logout		
		*
é		Internet
🦺 start 💧 🕴 🖬 🗮 🥥	🜐 ờ 📡 📿 🕴 🛞 > Fw: LDAP looku 🏾 🏠 My Documents 🛛 🐻 Configuration TDS 🕴 🚬 👘	😑 🧱 🍋 11:27 AM
🖉 🔐 🔽	😂 😄 🗾 👔 Tivoli Directory Se 🗿 Hutchison Essar 🗿 http://selfservices	Image: Second system Monday Image: Second system 3/27/2006

- 12.4 Create a new group
 - i. Create a new Group from the IBM Tivoli Directory Server Web Administration Tool using the menu path Users and Groups > Add Group.
 - ii. Select the previously created realm as Realm for this group. The Object class for the group is groupOfNames.
- iii. Associate the Users to Groups.

Tivoli Directory Server Web Administration Tool - Microsoft Internet	et Explorer 📃 🗗 🔀
File Edit View Favorites Tools Help	🥂 🕹 🕹 🕹 🖓
🚱 Back 🔹 🐑 🔹 😰 🏠 🔎 Search 🤺 Favorites 🔇 Med	ia 🔗 🍃 📄 🛄 🛛 🖓
Address 🛃 http://9.184.114.80:9080/IDSWebApp/IDSjsp/IDSConsoleFrameWork.jsp	🗸 🄁 Go
Tivoli Directory Server Web Administration Tool	
Introduction	0 0
Add group	Logfiles Help
Carter administration	
Enter the group name and results	ealm
Directory management	
Enter the Name and the Rea Then click Next to continue	Im of the new group below.
Realms and templates	
Group Name Group Name Iteratoroup 1	
Add user	
Manage users Realm	
Find users ★ myrealm ★	
Add group	
Find groups	
ê	Internet
🛃 start 🌒 🗄 📓 📼 🧱 🥔 🛞 ờ 🥥 🔍 🕴 🛑 > Fw: LDAP looku	o ta 🏠 My Documents 🕴 🔅 📰 🎎 🆕 11:28 AM
	do 🖉 Tuyali Directory Serve 🖉 🖓 🖓 🗘 🗮 🏉 🖓 🛄 Monday

Tivoli Directory Server Web A	dministration Tool - Microsoft Internet Explorer		_ 2 ×
File Edit View Favorites Tools	Help		<u></u>
Address Addres	DSWebApp/IDSIsp/IDSConsoleFrameWork.isp		🗸 🄁 Co
Tivoli. Directory Server Web	Administration Tool		
Introduction	O O > localhost		0 0
User properties	Add group		Logfiles Help
Server administration			
Schema management	Realm		
Directory management	myrealm		
Englication management	Group name		
Realms and templates	testgroup1		
	Members		
Add user	Available users Selected users		
Manage users			=
Add group	ashish Add >> test user 1		
Manage groups	test2 << Remove		
Find groups	test3 Filter		
Logout			
			~
			<u>^</u>
A Dana			M Internet
			() Internet
📑 start 🚽 👔 🖬 🗮 🥥	19 29 Several Contraction of the several sever	1 2 6 2	Monday
) 🛃 🕑 🛗 🔽	😂 📴 🚺 Configuration TDS.do 🦉 Tivoli Directory Serve		⊘⊇⊒ 3/27/2006

13. SASL - CONFIGURING DIGEST-MD5 on TDS

Under Server administration in the Web Administration console, expand the Manage security properties category in the navigation area of the Web Administration Tool, select the DIGEST-MD5 tab.

a) Under Server realm, you can use the pre selected Default setting, which is the fully qualified host name of the server, or you can click Realm and type the name of the realm that you want to configure the server as. Note:

If the ibm-slapd Digest Realm attribute in the configuration entry is set, the server uses that value instead of the default for the realm. In this case, the Realm button is pre selected and the realm value is displayed in the field. This realm name is used by the client to determine which user name and password to use.

- b) Under Username attribute, you can use the pre selected Default setting, which is uid, or you can click Attribute and type the name of the attribute that you want the server to use to uniquely identify the user entry during DIGEST-MD5 SASL binds.
- c) IF you are logged in as the directory administrator, under Administrator username, type the administrator username. This field cannot be edited by members of the administrative group. If the username specified on a DIGEST-MD5 SASL bind matches this string, the user is has the administrator.
- d) When you are finished, click Apply to save your changes without exiting, or click OK to apply your changes and exit, or click Cancel to exit this panel without making any changes.

Tivoli Directory Server Web A	Administration Tool - Microsoft Internet Explorer	- 8 🛛
File Edit View Favorites Tools	Help	A.
🕒 Back 🔹 🐑 👻 🛃 🍕	🏠 🔎 Search 🤺 Favorites 🜒 Media 🤣 🍃 🎍 🔜 🧾 😏 🦓	
Address 🙆 http://9.184.114.80:9080/I	DSWebApp/IDSjsp/IDSConsoleFrameWork.jsp	💌 🏓 Go
Tivoli. Directory Server Web	Administration Tool	
Introduction	O O O Iocalhost	00
<u>Iser properties</u>	Manage security properties	Logfiles Help
	Settings Digest-MD5	
Start/stop/restart server	Key database Server realm	
Manage server connections	Password policy	
Manage server properties	Password lockout Default 	
Manage security properties	Password validation Username attribute	
Manage administrative group	Kerberos	_
	Certificate revocation Attribute uid	
Schema management	Digest-MD5 O Default	
Directory management	Administrator username	
Replication management	root	
Realms and templates		
Users and groups		
Logout		
		•
<pre>(</pre>	J	v
E		 Internet
🤧 start 📄 📓 🔤 🥔	 interference in the second seco	

13.1 Configuration Notes

1. Password Encryption Support

The DIGEST-MD5 mechanism authenticates clients by comparing a hashed value sent by the client with a hash of the user's password. However, because the mechanism must read user passwords, all users wishing to be authenticated through DIGEST-MD5 must have {CLEAR} passwords in the directory. When

storing {CLEAR} passwords in the directory, you must ensure that access to password values is properly restricted through ACIs. You may wish to further protect {CLEAR} passwords by configuring attribute encryption in that suffix, as described in Encrypting Attribute Values.

Refer - http://docs.sun.com/source/817-7613/ssl.html#wp14354

2. Client Side Configuration

The hostname of the Tivoli Server should be entered in the hosts file of the Server.

13.2 SSL Setup

To enable security with server authentication, you can follow one of the given steps:

i. SSL Setup – Certificate from a Certifying Authority (CA)Self Signed Certificate

Create a public/private key pair and obtain and store a certificate from one of the predefined (well-known) Certificate Authorities. This procedure requires less setup because the key ring file is preconfigured with the CA root certificates required to identify the CAs from whom the certificate is issued.

ii. SSL Setup – Self Signed Certificate

To enable SSL security we can create a self-signed root certificate and store the certificate in the database and class files. To ensure maximum security for your site, you should only use a self-signed certificate for server authentication until you receive a CA-issued certificate.

You can use the ikmgui (IBM Key Management GUI) utility to create a selfsigned certificate to enable SSL sessions between clients and servers. The steps are essentially the same except that, in this case, you are the CA for the keys you will be creating, and you will be creating your own root certificate. The advantage of using this type of certificate is a quick start, it is free, and you have no dependencies on other organizations. The drawback, on the other hand, is that each client or server using this kind of certificate needs to have the new root certificate imported, which may impose some administrative burden.

1. Create server key database (.kdb file).

	Kov databases inf	ormation
Type:	Ney tanabase in	or mackin
e Name:		
oken Label:		
	Key database o	ontent
Signer Certific		▼ Add_
		Delete
		View Eslit
		Extract_

b. Click New, from that dropdown that appears in point a. above.

c. On the dialog window that pops up, select **CMS key database** file in the Key database type selection list and then type in the name and location of the key database file to be created. This file has an extension of .kdb, as, for example, in ldap_key.kdb. Then, click **OK** to close the dialog panel.

d. A new dialog pops up that requests your input for a password for the key database file, an optional expiration time, and whether or not the password is to be stashed to a file. Enter a password, an optional expiration time, and make sure that you check the check box next to Stash the password to a file? otherwise, you have to enter the password manually in the configuration file of the directory server. Click **OK** to close

this dialog. The password is then encrypted and stored in a file with the same name as the key database file but with an extension of .sth.

- 2. Create a self-signed certificate.
 - a. Select **New Self-Signed Certificate**... from the Create pull-down menu in the main window. In the dialog window that shows up, you will have to fill in the following information:
 - Key label (a clear, descriptive label for the certificate)

• Key Version (normally X.509 V3, unless you have reasons for other versions)

• Key size (512 or 1024, depending upon security requirements and country version of the ikmgui utility)

• Common name

• Organization and other pertinent information to identify the owner of the certificate

•Validity period in days

3. Click **OK** to create the request. The .arm file so created contains the certificate request.

4. From the certificate just created above, you need to extract the root certificate that is necessary for other communication partners (clients and/or servers) to recognize the newly created certificate. Here are the steps for exporting the root certificate:

- a. Select the new certificate's entry in the Personal Certificate list and click **Extract Certificate** at the bottom right on the main window.
- b. Select **Base64-encoded ASCII data** from the Data type list and enter a file name (with a .arm extension) and a location (directory) for the new root certificate to be exported to. Then click **OK** to export the root certificate. (If

You have now created a file that holds your own root certificate. This must be imported to all communication partners that will connect to the server through SSL.

5. Use the following steps for importing the new root certificate into others' key database (using ikmgui):

- a. Make sure that the certificate extracted above, in the previous step, is made available to all the communication partners. You can transfer the file using ftp or a diskette or any other suitable media.
- b. Invoke the ikmgui utility on the receiving system.
- c. If not already done, create a key database file (see first step above for creating a self-signed certificate).
- d. In the Key database content portion of the window, select Signer Certificates from the selection list and click Add... on the right.
- e. Select Base64-encoded ASCII data from the Data type list and type the Certificate file name and location into the appropriate fields. Then, click OK to import the certificate.
- f. On the upcoming dialog, supply a label for this certificate and click OK.

The steps as described above need to be done on each machine that will communicate using this certificate with the machine from which the certificate was exported.

Each LDAP server should have its own certificate. Sharing certificates across multiple LDAP servers is not recommended. By using different certificates and

private keys for each server, your security exposure is minimized should a keyring file for one of the servers be compromised.

13.3 SSL Setup – Client Side (WPC end)

- a. Get the .arm file generated in the above steps in to the WPC environment
- b. Use the keytool command to import this in to the JVM
 - i. keytool -import -trustcacerts -keystore cacerts -storepass changeit noprompt -alias mycert -file <cert_file_generated>
- c. Make an entry in hosts file to point to the SSL Tivoli instance.
- d. Change the location of the cacerts file in the keystore variable in the login script. If the file that was generated in the step2 was in /home/sgopan/cert/cacerts, make the value for the keyStore variable to this location.

Set the bindType variable to ssl and sslBindType to either simple or DIGEST-MD5.

Configuring Z/OS

14. Creating Users and Groups:

Use Softerra LDAP Administrator 3.3.1 to connect to the Z/OS server.

14.1 Create a new user:

1. Create a new user through LDAP Administrator by selecting a container (say cn=wpcroot) and right clicking and choosing New -> New entry.



2. Choose the entry creation method as "Schema based", in the Entry Creation Wizard-Step 1.

ntry Creation Wizard - Step 1	? 🔀
Entry Creation Method Please choose a method for creating a new entry.	
Choose a preferred entry creation method:	
◯ <u>T</u> emplate-Based	
⊙ <u>S</u> chema-Based	
Z Back Next >	Cancel Help

3. Select inetOrgPerson in the Object class selections of Entry Creation Wizard-Step2.

vailable object classes:		Selected object classes:	
ibm-msysServiceLookup ibm-msysSharedData ibm-msysSMPEInfo ibm-msysSoftwareElement ibm-msysSoftwareFeature ibm-msysSysplex ibm-msysVSAMCluster ibm-wsnEntry ibm-wsnEntry ibm-wsnNameTreeContainer INamingService javaContainer KrbRealm-V2 LDAPServer liOrganization liPerson locality	*	inetOrgPerson	Structural

4. Enter the RDN as cn=testuser1 in the Entry Creation Wizard-step3.

	areb a	_		100
Entry RDN Please specify an RDN		Ţ		
Please specify the entry R	DN. You can sp	ecify a	a multi-valued RDN by clicking on the 'Add Value' li	ink.
Type:			Value:	
cn			testuser1	
RDN Preview: cn=testuse	r1			

5. Add values to the attributes like sn, uid, user password and more in the Entry creation Wizard-Step4 and click finish.

Please fill in attribute value	s:		
cn	testuser1	~	Add Attribute
objectclass	inetOrgPerson		
sn	testuser 1		Remove Attribut
audio		=	
businessCategory			
carLicense			Add <u>V</u> alue
departmentNumber			-
description			Remove Value
destinationIndicator			
displayName			
employeeNumber			
employeeType			
facsimileTelephoneNum			
givenName			
homePhone			
homePostalAddress		×	Save Template

14.2 Create a new Group:

1. Create a new group through LDAP Administrator by selecting a container (say cn=wpcroot) and right clicking and choosing New -> New entry.

			1.34					
cn=wpctreerc	New	•	2	New Entry	Ctrl+E			
Eile Edit Viev	Modify Value	F4	ľ۵	New <u>A</u> ttribute	Ctrl+Shift+A			
New 🔹 🔲 🖾	<u>R</u> ename	F2	ĕ	New Entry Temp	olate Ctrl+T	🗳 • 🏭 🏷 💯		objectClass=*)
	Delete	Delete	1	New Profile	Ctrl+P			
Scope Pape	Out	Ctrlax	ෂ	New Group	Ctrl+G	- 64	relation Names Descriptions	
Softerra I DAP Ar		Cultix	-			• 566	ren in: Maries, Descriptions	
🕀 📭 Internet Publ	a <u>C</u> obà	Ctri+C	Value	2			Туре	e Size 🛆
🕀 🗍 Domino	<u>P</u> aste	Ctrl+V	admi	n			Entr	y 77
🕀 🗍 Domino 1	Add to Favorites	Ctrl+D	sachi	in FromTim			Entr	y unknown
			PUDII	Criominin			Entr	y unknown
	Eilter (objectClass=*)		besh	war			Entr	y unknown
	Sort Ascending		D				Entr	y unknown
- <u>-</u>			a11				Entr	y unknown
🗄 🧰 cn=s 🗳	<u>R</u> efresh	F5	amir				Entr	y unknown
🗄 🧰 cn=p 限	Stop Operation	Ctrl+S	mous	se			Entr	y unknown 🗏
🗄 📃 cn=s	Add as Damaus Craus Mamba	an childhiftic	cat				Entr	y unknown
	Add of Remove Group Membe	rs Curtonitted	wpcG	Group			Entr	y unknown
	Change Group Membership	Ctrl+Shift+M	brya	n			Entr	y unknown
±	A Directory Search	Ctrl+E3	Grou	ip 1			Entr	y unknown
🗄 🛄 cn=n 🏅			znqf	Crewe			Entr	y unknown
🗄 💼 cn=c 👼	Export Data		WPC	Group			Entr	y unknown
🗄 🗀 cn=v 🛃	Import Data		Test	~~~~			Entr	y unknown
			allen				Entr	v unknown
	¹ <u>P</u> roperties	Alt+Enter	grou	p			Entr	y unknown
± i cn=Test	Group	id	sand	hya			Entr	y unknown
🗄 🧰 cn=WPC	-QA	_ = objectclass	contz	ainer			Attr	hute 9 🚩
🗄 🚞 cn=Test		List View	ML Vi	ew				4 Þ ×
🗄 🧰 cn=allen		Output						μ×
the charge out	p dhva+cn=sandhva	Show all items		- /	4 ** ** * *			
		Error loading Root	DSE e	entry from tvt100	3.tivlab.raleigh.ib	m.com:3389.		
		Schema for tvt100	3.tivl	lab.raleigh.ibm.co	m: 3389 loaded si	uccessfully.		
		Message	s/					
Create a new entry						🖸 🖸 cn=admin,cn=wpct	reeroot,dc=tvt1003	Schema fetched
🔒 start 💧 🕴	i 📼 🗃 🎮 🏘 😱 🔾	n 🖉 👔 💮 Ew; Testin	a on :	z/ 👔 🔯 LD/	AP Docs	Configuring ZOS.d		🖉 🧱 🍇 🖕 11:08 AM
								Tuesday
	🤌 🛃 🔽 😂 💭 😸	Configuring	g Micr	ros 🚽 en:	=wpctreeroot,d			2/28/2006

2. Choose the entry creation method as "Schema based", in the Entry Creation Wizard-Step 1.

ntry Creation Wizard - Step 1	? 🔀
Entry Creation Method Please choose a method for creating a new entry.	
Choose a preferred entry creation method:	
○ <u>T</u> emplate-Based	
⊙ <u>S</u> chema-Based	
All Novt >	
	Cancel Help

3. Select groupOfUniqueNames in the Object class selections of Entry Creation Wizard-Step2.

Available object classes:			Selected object classes:	
eProperty ePropertySet eSAP eService eSoftware eSoftwareMaintenanceUnit eSystem eTargetAdapter eTargetRecord eTargetService eTargetServiceType eUser friendlyCountry groupOfCertificates groupOfURLs	•	**	groupOfUniqueNames	Structural

1. Enter the RDN as cn=testgroup1 in the Entry Creation Wizard-step3.

try Creation Wiza	rd - Step 3					?
Entry RDN Please specify an	RDN for the e	entry.				ţ
Please specify the entr	ry RDN. You d	an specify a	multi-valued	RDN by clickin	g on the 'Add	Value' link.
cn		~ =	testgroup1			
Add Value						
RDN Preview: cn=test	tgroup 1					
		_			C	

5. Enter the Unique member of the group and click finish.

Please fill in attribute va	alues:	Add Attribute			
ohiectclass	groupOft InjqueNames	Add Attribute			
uniqueMember	testuser 1	Remove Attribut			
businessCategory					
description					
0		Add Value			
ou					
owner		Remove Value			
seeAlso					
		Save Template.			

Note:

- For SASL bind, user's password must be clear passwords.
- UId field must be populated with a unique value across the sub tree for SASL to work.
- For SASL only the principal has to be supplied in the lookup table.