FreeRadius integration with Novell eDirectory

Date: 28 December 2005 Author: Alexandre Dachine Version: 1.1

Prerequisites

Necessary hardware

- 1. Server to host Novell OES Linux
- 2. Access Point WiFi CISCO AIRONET 1100 series (AIR-AP1121G-A-K9)
- 3. Windows XP/W2K laptops with WiFi network adapter

Necessary software

- <u>Novell OES Linux</u> <u>http://download.novell.com/Download?buildid=ppIBUh_8JW0</u> The following images are necessary: oes-sp1-linux-1.iso oes-sp1-linux-2.iso oes-sp1-linux-3.iso oes-sp1-linux-5-sles9-2.iso oes-sp1-linux-6-sles9-3.iso oes-sp1-linux-7-sles9-4.iso
 <u>FreeRadius</u>
 - http://forge.novell.com/modules/xfcontent/downloads.php/edirfreeradius Use the SLES9 modules.
- 3. <u>RADIUS Plug-in for iManager</u> http://forge.novell.com/modules/xfcontent/downloads.php/edirfreeradius
- 4. <u>Certificate creation scripts for FreeRadius</u> <u>http://oriol.joor.net/article_fitxers/1574/certs.tar.gz</u>
- 5. <u>iManager v2.5</u>
- 6. Latest Novell client for Windows with NMAS/NICI option

Useful documentation

- 1. <u>http://www.novell.com/documentation/edir_radius/index.html</u> (by Novell)
- 2. <u>http://www.novell.com/coolsolutions/tip/15922.html</u> (by E.Champagne)

Novell OES Linux Server Installation

Important: Before starting, read the following Novell document: (http://www.novell.com/documentation/oes/pdfdoc/install linux/install linux.pdf)

- 1. Burn CDs from downloaded images.
- 2. Boot the server with the "OES-SP1-LINUX-1" CD.

The Installation program starts automatically:



3. Accept the license and continue.

Base In	都 To view the license agreement in English, please scroll or page down.	
InstPert	Pour afficher le contrat de licence en français, faites défiler le texte ou appuyez sur la touche Pg Suiv.	
• Roc	Führen Sie einen Bildlauf nach unten aus, um die Lizenzvereinbarungin deutscher Sprache anzuzeigen.	
Onli Ser	Para consultar el acuerdo de licencia en español, avance por el documento.	
 OES Clei Reli 	Per visualizzare il Contratto di licenza in lingua italiana. scorrere la pagina o utilizzare PgGiù.	
• Dev	Para ver o contrato de licença em português, mova a barra de rolagem para baixo ou use a tecla Page Down.	
	Schulf omlaag of gebruik Page Down om de gebruiksrechtovereenkomst in het Nederlands weer te geven.	ł
	17	

4. Start the setup.

Base Installation	Welcome to YaST2 The	
+ Language	installation and system Administration Progra	
Installation Settings		
 Perform Installation 	Select your language:	
Configuration	pourse (a)	
Root Password	Deutsch	
Network	English (UK)	
Online Update Service	English (US)	
OES Configuration	Espanol	
Clean Up	Ελληνικά	
Release Notes	Italiano	
Device Configuration	日本語	
	한글	
	Lietuvių	
	Magyar	
	Norsk	
	Polski	
Yast		00
YaST	Installation Settings	
Yessi Base Installation	s Installation Settings	
VaSt Base Installation Language	Installation Settings Click any headline to make changes or use the "Change* menu b	elow.
Vast Base Installation Language Installation Settings Derform Installation	Installation Settings Click any headline to make changes or use the "Change" menu b	elow.
Vasues Base Installation - Language - Installation Settings - Perform Installation	Installation Settings Click any headline to make changes or use the "Change" menu b System	elow
VesSt Base Installation · Language • Installation Settings • Perform Installation Configuration	Installation Settings Click any headline to make changes or use the "Change" menu b System System: VMware, inc VMware Virtual Platform (None) System: VMware, inc VMware Virtual Platform (None)	elow
VesSt Base Installation - Language - Installation Settings - Perform Installation Configuration - Root Password - Network	Installation Settings Click any headline to make changes or use the "Change" menu b System: System: VMware, inc VMware Virtual Platform (None) Processor: Intell(R) Pentium(R) 4 CPU 2, BOGHz Main Memory, 256 MB	elow
Yce.SST Base Installation 4 Language 5 Installation Settings 9 Perform Installation Configuration 1 Note Password Network 0 Online Update	Installation Settings Click any headline to make changes or use the "Change" menu b System: VMware, Inc VMware Virtual Platform (None) Processor: Intel(R) Pentum(R) 4 CPU 2.80GHz Main Memory. 256 MB	elow.
VCCSCC Base Installation Installation Settings Perform Installation Configuration Root Password Network Notwork Service	Installation Settings Click any headline to make changes or use the "Change" menu b System System: VMware, inc VMware Virtual Platform (None) System: VMware, inc VMware Virtual Platform (None) Main Memory: 256 MB Mode	elow.
Accession of the second	Installation Settings Click any headline to make changes or use the "Change" menu b System System: VMware, Inc VMware Virtual Platform (None) Processor: Intel(R) Pentum(R) 4 CPU 2.00GHz Main Memory. 256 MB Mode New installation	elow.
Action of the second se	Installation Settings Click any headline to make changes or use the "Change" menu b System System: VMware, Inc VMware Virtual Platform (None) Processor: Intel(R) Pentaum(R) 4 CPU 2.80GHz Mode New Installation New Install	elow.
VCCSCC Base Installation Installation Settings Perform Installation Configuration Root Password Network Online Update Service OES Configuration Clean Up Refease Notes Device Configuration	Installation Settings Click any headline to make changes or use the "Change" menu b System System: VMware, Inc VMware Virtual Platform (None) System: VMware, Inc VMware Virtual Platform (None) Mode New Installation Keyboard layout	elow.
VCCSCC Base Installation Installation Settings Installation Settings Perform Installation Configuration Network Onfiguration Service OBS Configuration Clean Up Release Notes Device Configuration	Installation Settings Click any headline to make changes or use the "Change" menu b System System: VMware, inc VMware Virtual Platform (None) Processor: intelling: Pentium(R) 4 CPU 2.B0GHz Main Memory: 256 M8 Mode New installation Keyboard layout French	elow.
Construction Co	Installation Settings Click any headline to make changes or use the "Change" menu b System System: VMware, inc VMware Virtual Platform (None) Processor: Intel(R) Pentum(R) 4 CPU 2.00GHz Mode New Installation Keyboard layout French Mouse	elow.
VCCSCC Base Installation Maguage Matalian Settings Perform Installation Configuration Notife Service Service OES Configuration Sclean Up Release Notes Device Configuration	Installation Settings Click any headline to make changes or use the "Change" menu b System System: VMware, Inc VMware Virtual Platform (None) System: VMware, Inc VMware Virtual Platform (None) Mode New Installation Keyboard layout French Mouse System: VMware System (Strengthere) System: VMware (Strengthere) System: System: System: System: System: Strengthere) System: Syst	elow.
VCCSCC Base Installation Maguage Installation Settings Perform Installation Configuration Network Notwork Online Update Service OES Configuration Clean Up Release Notes Device Configuration	Installation Settings Click any headline to make changes or use the "Change" menu b System System: VMware, inc VMware Virtual Platform (None) System: VMware Virtual Platform (None) Mode New installation Keyboard layout French Mouse NoteliMouse Explorer (ps2)	elow.
YCCSSC Base Installation Magnage Matalation Settings Perform Installation Configuration Network Online Update Service OES Configuration Service Release Notes Device Configuration	Installation Settings Click any headline to make changes or use the "Change" menu b System System: VMware, inc VMware Virtual Platform (None) System: VMware Virtual Platform (None) Mode New installation Keyboard layout French Mouse Newlinstallation Keyboard layout System: VMware System: (ps2) Partitioning	elow.
YCCSSC Base Installation A Language Installation Settings Perform Installation Configuration R Rot Password Network Online Update Service OES Configuration Clean Up Release Notes Device Configuration	Installation Settings Click any headline to make changes or use the "Change" menu b System System: VMware, Inc VMware Virtual Platform (None) System: VMware Virtual Platform (None) Mode New Installation Keyboard layout French Mouse NineliMouse Explorer (ps2) Partitioning	elow.
YCGSSC Base Installation A Language Installation Settings Configuration Network Configuration Service Service Service Service Service Service Service Service Desice Configuration	Installation Settings Click any headline to make changes or use the "Change * menu b System System: VMware, inc VMware Virtual Platform (None) System: VMware, inc VMware Virtual Platform (None) Mode New Installation Keyboard layout System: NetellMouse Explorer (ps2) Partitioning	elow.

5. Create partitions depending on your needs. Generally, the default configuration proposed by Setup is not sufficient.

In our case (one physical disk or one logical drive RAID5) the three partitions /, **boot**, and **swap** will be native Linux (outside of the LVM group) and the eventual other ones will be in LVM group. The advantage of LVM partitions is that they can be extended online, without stopping the running system.

G Preparing Hard Disk Step 1	🕟 Suggested Partitioning
	 Create swap partition 502.0 MB on /dev/sda1 Create root partition 9.5 GB (/dev/sda2 with reiser)
Choose a hard disk- 1: 1. SCSI, 10.00 GB, /dev/sda, VMware, VMware Virtual S <u>c</u> ustom partitioning for experts	ß
<u> </u>	Choose Choose Baccept proposal as-is Bage partition setup on this proposal Cereate custom partition setup
Back	Back Abort

Select 'Expert', then 'Delete partition table and disk label'.

CAUTION!	
If you delete the part	tition table and disk label of
device /dev/sda, dat	a on this device will be lost. 💦
The executed comm	and will be: (/bin/dd if=/dev/zero of=/dev/sda bs=2k count=1
Do you really want to	o do this now?

Create partitions /boot, swap, etc.

	Jartition on /dev/sua	Create a primary	partition on /dev/sda
iormat Do not format File system (D) (0x83 Linux File system	-Size Cylinder size: 7.84 M St <u>a</u> rt cylinder: 0 En <u>d:</u> (9 or +9M or +3.2GB)	Format Do not format File system (D): (0x82 Linux swap)) Eormat File system	Size Cylinder size: 7.84 M Start cylinder: 20 End: (9 or +9M or +3.2G +512M
Reiser F	Fstab Options	Swap 두	Fstab Options
<u>Encrypt file system</u>	Mount Point	Encrypt file system	Mount Point
Create a primary p	partition on /dev/sda		
Create a primary p	Size Cylinder size: 7.84 M		
Create a primary p ormat Do not format File system (D):	Size Cylinder size: 7.84 M St <u>a</u> rt cylinder: 86		
Create a primary p format Do got format File system (D): (0x83 Linux Epormat File system	-Size Cylinder size: 7.84 M St <u>art cylinder:</u> 86 En <u>d</u> : (9 or +9M or +3.2GB) +8GB		
Create a primary p format Do not format File system ID: 0x83 Linux File system Reiser Options	Size Cylinder size: 7.84 M St <u>art cylinder:</u> 86 Eng: (9 or +9M or +3.2GB) +8GB Fstab Options		

LVM configuration:

		Create a Volume Group
Format Do <u>n</u> ot format File system <u>I</u> D:	Size Cylinder size: 7.84 M St <u>a</u> rt cylinder:	Now we have to create a volume group. Typically you don't have to change anything, but if you are an expert, feel free to change
0x8E Linux LVM	1131	our defaults:
	En <u>d</u> : (9 or +9M or +3.2GB)	Volume Group <u>N</u> ame:
D Eormat	1304	(system)
Reiser	Setab Ontions	Physical Extent Size
Cathorn		4M
Encrypt file system	Mount Point	🔲 Use Old LVM1 Compatible Metadata Forma
[or		OK Cancel



This final table shows partitions before continuing:

Device	Size	F	Туре	Mount	Start	End	1
/dev/sda	9.9 GB		VMware Virtual S		0	1304	Ċ
/dev/sda1	156.8 MB	F	Linux native (Reiser)	/boot	0	19	
/dev/sda2	517.6 MB	F	Linux swap	swap	20	85	
/dev/sda3	8.0 GB	F	Linux native (Reiser)	1	86	1130	
/dev/sda4	1.3 GB		Linux LVM		1131	1304	L
/dev/system	1.3 GB		LVM2 system		100	1.00	
/dev/system/VOL1	1.3 GB	F	LV	/vol1-iprint			
	Þ						
•						(*
- C	eate	Ed	it <u>D</u> elete	Resize			

6. Select the installation type 'Novell Open Enterprise Server' and the necessary packages.

Software Selection			
Software Selection Software Minimu Eul Inst Default Novell	n system n graphical system (without KDE) iallation system QuickFinder Server Folder2 Server Virtual Office Server Print Server Open Enterprise Server Detailed selection		
Filter: Selections	Package Summar Image: Summar Novel P Image: Summar Novel P Image: Summar Novel P Image: Summar Novel P	nt Client Int command lin Int Server:	es manual selections, the following packages have been changed to ies:
Novell Linux User Management		Package	Summary
Novell eGuide		apache2	The Apache web server (version 2.0)
Novell iFolder 2.x		apache2-jakarta-tomca	at-connectors Connectors between Apache 2.0 and Tomcat Seviet (
Novell NetStorage		per db1	Berkeley DB database library Version 1.85
Novell QuickFinder		jk∰ gdk-pixbuf	A Library for Fast Pixel Manipulation
Novell Virtual Office		k glibc-devel	Include Files and Libraries mandatory for Developmen
Novell NSS		s gnome-libs	The GNOME Base Libraries
Novell Cluster Services		jakarta-tomcat	A servlet container
Novell IP Management		Java2	Java(TM) 2 SDK, Standard Edition
Novell Samba Configuration	Description Technical Data Dependencies Version	i java2-jre	java(TM) 2 Runtime Environment
Novell Backup Services (SMS)	and the start struct the start	• Ibapro	Apache Portable Runtime (APR) Library
Novell Health Monitoring	noven-iprint-client - Novell iPrint Client	in in bgcj	Java Runtime Library for gcc
Novell iFolder 3 x Web Access	Contains the iPrint clients for Linux, Macintosh. and Window	This rpm	Glade Library Compatible with the GNOVE 1 - Decites
Hoven Polder 3.x	should be installed on an iPrint server so users can install t	e iPrint	Shade Library compatible with the GNOME 1 x Desktor
	client from an iPrint Linux server.	libstdc++.devel	Include Files and Libraries mandatory for Developmen
Name Disk Usage Used Free	Novell iPrint is a print solution that lets you have global acc	iss to	include thes and chorares mandatory for Development
/ 24% 1.96 GB 6.04 (nrintare and ructomitable views of your print environment	•	•I•
10001 2% 4.2 MR 147.6 F		trunt [and the second se



7. Validate other parameters, such as boot type, OS language, time zone and default run-level.



8. Now Setup is ready to copy files.



The copy starts and takes between 20 and 60 min., depending on server performances and amount of selected packages. After that the server restarts automatically.

Current Ruckana	Installation	
noveli-lum-2.2.0		Time remaining (estimated)
100%	Open Enterprise	Server
	CD 1:	08.14
Current Package	CD 2	14:13
novell-lum-2.2.0	1	8%
Description	CD 3	03:48
Linux User Management	CD 4	
	Open Enterprise	Server
Size	CD 1	
• 2.31 MB	CD 2	
	CD 3	
	CD 4:	
	SUSE CORE	
stallation I on (Extract)	CD 1	06:10
esmgr-0.9.8 A program to allow arbitrary access to device files	CD 2	00:10
ibxml2-2.6.7 A library to manipulate XML files 🔊	CD 3	00:11
ubmount-0.9 Auto Mounting of Removable Me	CD 4	
Isa-1.0.9 Advanced Linux Sound Architecture	CD S	-
Icc-Info-3 3 3 GNU Info-Pages for GCC Iovell-lum-2 2.0 Linux User Management.	Total	32:46

9. After reboot the setup goes on. You are asked to give the root password. If the password is longer than 8 characters, click 'Expert', then 'Blowfish'; if not, the password will be truncated.

1	assword for "root", the system administ	rator
Base installation	Do not forget what you enter her Briter a password for the root use Resetter the password for servical Eggert Options	re F: blos
1	Abors	Next

10. Select and configure the NIC(s).

Base Installation	Wetwork Configuration	Base Installation	Vetwork Configuration
Language Installation Settings Perform Installation Configuration	Skip Configuration (a) Lise Following Configuration	Language Installation Settings Perform Installation Configuration	Skip Configuration
Rotzwork Notetwork Ordine Update Service Olds Configuration Clean Up Release Notes Device Configuration	Network Interfaces • AND PCnet - Fast 79/C9/1 DSL Connections • Not detected. ISDN Adapters • Not detected. Chapters on Owner with the inductions • Not detected.	Roof Passenrif Netrool Online Update Service Otd Configuration Otd Configuration Class Up Release Notes Device Configuration	Hetwork Interfaces AND Proof: Fx87 75071 Configured with Address 10 ds 10 191 DSL Connections Not detected. ISDN Adapters Not detected. Modems Not detected.
	Charge • Back Aboyt	Next	Change • Back Abopt Best

11. Test the Internet connection during the setup.

	Rear Installation	Section Test Internet Connection		
Perform installation Configuration Root Password Net Work Configuration Online Updates Available Download latest release notes Online Updates Available Download latest release notes Check for latest updates Select: <td>✓ Language ✓ Installation Settings</td> <td></td> <td>Dis.</td> <td></td>	✓ Language ✓ Installation Settings		Dis.	
Configuration activate the test procedure. • Not Passand Activate the test procedure. • Notione Update Service • Service • Download latest release notes • Clean Up • Check for latest update • Service • Check for latest update • Select: • Yes, Test Connection to the Internet • No, Skip This Test • Motor • Matcome to YaST Online Update • Metcome to YaST Online Update	 Perform Installation 	To validate your internet access		
• Root Password • Root Password • Network • Network • Online Update • Oor Figuration • Oor Gonfiguration • Clear Up • Release Notes • Device Configuration • Select: • Yes, Run Online Update Now • Yes, Skip Update • Welcome to YaST Online Update	Configuration	activate the test procedure.		
• Network: • Online Update • Service • Dots Configuration • Clear up • Clear up • Release Notes • Device Configuration • Check for latest updates • Select: • Select: • Yes, Run Online Update Now • No, Skip Update • Mex • Aboyt • Welcome to YaST Online Update	✓ Root Password			
Service Download latest release notes Check for latest updates Device Configuration Clear Up Release Notes Device Configuration Select: Select: Na, Skip This Test Device Configuration Reck Aboyt Reck Aboyt Reck Mexet Mexet	Network Online Update	The following steps will be perform	ed:	
• Clean Up • Clean Up • Cleak for latest updates • Leck for latest updates • Select: • Yes, Run Online Update Now • Yes, Run Online Update Now • Mo, Skip Update • Welcome to YaST Online Update	Service OFS Configuration	- Download latest release notes		Online Updates Available
	Clean Up Release Notes	- Check for latest updates	st conseillé de faire le test de connexion ernet lors de l'installation	
Select: Ves, Run Online Update Now No, Skip Update Reck Abogt Next Welcome to YaST Online Update	Device Configuration			Download and install them via the YaST Online Update?
Image: Welcome to YaST Online Update Image: Welcome to YaST Online Update Image: Welcome to YaST Online Update		Select:		
Image: Welcome to YaST Online Update				
Welcome to YaST Online Update		 Yes. Test Connection to the Internet 		Yes, Run Online Update Now
Wekcome to YaST Online Update		No. Skip This Test		
Beck Abogt Bext				🔘 <u>N</u> o, Skip Update
Welcome to YaST Online Update				
Welcome to YaST Online Update				
Welcome to YaST Online Update		Back	Next	
🚱 Welcome to YaST Online Update				1
🚱 Welcome to YaST Online Update				
🛐 Welcome to YaST Online Update				
welcome to YaST Online Update	_		_	
	Welcome to YaST C	Online Update		
~ System Information	-System Information-			



12. Customize the properties of the CA and the common certificate. Personally, I would name the common certificate the same as the server, such as *srv1.domain.org*

Skip	Configuration
Use	Following Configuration
C	A Management
C	eating default CA and certificate.
W	th higher security requirements, you should change the password.
	+ CA Name: YaST Default CA
	Common Name: YaST Default CA (skyvan-v)
	Server Name: skyvan-v.lesieurfr.com
	Country: US
	Password: [root password] Clover sur "Change' afin de
	E-Mail: postmasterigiesieum: com personnaiser les propriétés du Ci de cartificat
0	penLDAP Server
St	art LDAP Server: NO
-	

The next step is eDirectory configuration. You have two options:

- (A) Join an existing tree
- (B) Create a new tree
- 13. In case (A) you must make sure that the tree is healthy and ready to accept a new Linux server, and the schema has been extended. See <u>http://www.novell.com/documentation/oes/pdfdoc/coexist-mig/coexist-mig.pdf</u> and <u>http://www.novell.com/documentation/oes/pdfdoc/install_linux.pdf</u>. The following screenshots show how to create new tree.

📸 eDirectory Configuration - New or Existing Tree	👸 eDirectory Configuration - New Tree Information
New or Existing Tree ⓒ Ngw Tree ⓒ Egisting Tree]ree Name SKKM	EDN admin name with context (i.e. cn=admin.o=novell cn=admin.o=asn Admin Password ********* Yenfy Admin Password *********
Back Abogt Next	Back Abogt Next
Birectory Configuration - New Server Configuration	eDirectory Configuration - NTP & SLP
Enter Server <u>C</u> ontext Casin Directory Information Base (DIB) Location (var/nds/dib	Network Time Protocol (NTP) Server Un des serveurs locaux 10 68 10 166
Enter LDAP Port 389 ¢ Enter Secure LDAP Port 636 ¢ Enter [Monitor Port 8028 ¢	Service Location Protocol Scopes
Enter Secure (Monitor Port. 8030 ¢ Back Aboyt Next	Back Abogt Next
Verform eDirectory Configuration	
Save configuration information for YaST2 Perform time synchronization Configure and start the Service Location Protocol Copy the NICI Foundation Key file Establish eDirectory on all static IP addresses Configuring and starting eDirectory This will take a while	
Image: Second to LDAP requests - Wait for eDirectory to respond to LDAP requests - Fetch the eDirectory tree root certificate - Perform DES schema extension - Configure the default NMAS login method Configure and start eDirectory using "ndsconfig"	
gack Abogt	

14. After eDirectory configuration has finished, the setup shows a summary table indicating the configuration of Novell products selected during previous steps (for example, iManager, SMS, LDAP, etc.).



15. The configuration of selected products is now finalized.

🧯 Completing i	Manager Configuration	
✔ Configure iMan	ager	
➔ Install iManage	r Plug-ins	
Please Wait		
nstalling iManager Pl	ug-ins. This may take a while	
	un inc	
nstalling iManager Pl	ag man	
installing iManager Pl	50 <mark>%</mark>	

16. Release notes are displayed.



Check the video configuration (monitor, resolution, graphical adapter, etc.) and modify if necessary.
 Finally, the last screen says the setup is finished. Click OK and reboot.

Applying Patches on Novell OES Linux server

There are two possibilities: **rug** or **RedCarpet**. Officially Novell doesn't support Red Carpet in this version of OES (see http://www.novell.com/documentation/oes/pdfdoc/install_linux/install_linux.pdf).

1. Open a Terminal session with root account and type the following commands:

rug set-prefs cache-directory /patches/oes/10-nov-2005 #optional *rpm –qa |grep pubkey*

skyvan-v:/media/cdrom # rpm -qa	grep	pubkey
gpg-pubkey-0dfb3188-41ed929b	1.0000000000	a land the second state
gpg-pubkey-9c800aca-40d8063e		
gpg-pubkey-15c17deb-3f9e80c9		
gpg-pubkey-3d25d3d9-36e12d04		
skyvan-v:/media/cdrom #		

rug sl

skyvan-v:/media/cdrom #'rug sl	
# Service URI	l Name
1 https://update.novell.com/data	Novell_Update_Server
skyvan-v:/media/cdrom #	

rug act -s 1 activation-code-received-from-Novell email-address #activation OES

rug sub oes



rug pl #lists all available patches
rug pin oes:* #installation of patches, time-consuming!

The download and successful installation are confirmed by following messages:

Download complete Transaction finished

If patches were applied with Red Carpet, you will see following messages:

a R I	(C)						
Channels	trest						
Ding Actions	Depende	incy Resolution				-	
in Taxtage	Channel	Package		Current Version	New Version	Size	
	Reque	sted Install	ations		1000		
	52	S Updating	System 🌏		X 27.34	750 kB	
	2	A. U	pdating Sys	tem	27.34	300 k8	
	8	Mr. P	ownloading pac	kages	- 3.3	620 kB	
	82				0.3	171 18	
	2	2.8	% - 3.1 MB / 112	5 MB (69 kB/s)	19.9	305 kB	
	1 8	a dia				40 18	
	82	1	1.8% comp	sleted	52.13	175 kB	
	62			X 9	ancel 15.10	2.3 MB	
	8				19.15	39.4 MB	
	2	java2-jre		1.4.2-129.14	1.4.2-129.15	10.6 MD	
						70.7.1.10	
onnected to localhos opendency Ectober Edit View Actio	it Hone leed Can as <u>H</u> elp	kemei-default		2.6.5-7.195	2657201	X Cancel	🗣 Continu
Connected to localitos opentifensyscotoliti Lott View Actio Channets	t Hone Red Chr ns <u>H</u> elp	kemel-default		2.6.5-7.195	2657201	Z S A HO	🗣 Continu
Connected to localhos Connected to localhos Connecting & coold Edit View Action Channels Channels	t Hond Red Car ns Help R Depends	kemel-default pet-2.4.4 ency Resolution		2.6.5-7.195	2657201	Z Sancel	Continu
Connected to localhos	t tion o Red Cas ns Help Depende	pet 2.4.4		Current Version	265-7201 New Version	233 HO	Continu
connected to localhos oppandency Actool Lat View Actool Oppannets Oppannets Channets Channets Channets	t tion - Red Car ms _ielp Depende Channe Reque	pet 2.4.4 pet 2.4.4 Package sted Install	ations	Current Version	2657201 New Version	Size	Continu
Connected to locations opensionary according Lat yiew Action Opension Opension Opension Connected Connecte	it Hone Red Car ns Help © Depends Channe Requir Qu	kernel-default pet 2.4.4 ency Resolution Package ested Install	ations ion Finished	Current Version	New Version	Size	Continu
Connected to localinos opendency Recolu Lat yea Actor Otannets Channets Channets Channets Channets Channets Channets	t Hone Red Chr ns Help Channe Requir Q	kernel-default pet 2.4.4 incy Resolution Package ested Install	ations ion Finished ransaction I	Current Version	New Version 77.34 77.36	233 M0 X Cancel Size 750 kB 300 kB	Continu
Connected to localinos ependency Accolu Lat View Actoo Channels Channels In Actons	t thon at cel Car nt Lielp Pepende Channe Reque Q Q Q Q Q Q	kernel-default pet 2.4.4 mcy Resolution Package sted Install Transett Transett	ations ion Finished rensection I	Current Version	New Version 77.34 73.34	233 MB X Cancel Size 750 KB 300 KB 620 kB	Continu
innerette to localhase connected to localhase pandency 2 2 2010 Lat yew Actoo Quancets One Actions The Actions	t tiones Iccl Can ns Leip Regue Regue Q Q Q Q Q Q Q Q Q Q	kernel-default pet 2.4.4 Pet 2.4.4 Package sted Install Transact Transact Transact	ations ion Finished ransaction I he transaction he transaction he	Current Version	New Version 77 34 72 34 33	23 3 MB 2 Cancel 5ize 5ize 750 kB 300 kB 620 kB 171 kB	Continu
Connected to localhose openationcy actors Det User Actor Channets	t tion = see Cas ns _see Cas Channe Requi	kernel-default pet 2.4.4 Incy Resolution Package sted Install Transact Transact	ations Iron Finished rensections uccessfully	Current Version	New Version 7 34 7 34 3 99	233 MB 2 Cancel 5ize 5ize 750 kB 300 kB 620 kB 171 kB 305 kB	Continu
Connected to localitose annected to localitose pandency actool (bet yow actool Counces)	t tition = Eccl Car ns _Eccl Car @ Channe Requir Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q	remei-default pet 2-2-4 mcy Resolution Package sted Install Transact Transact	ations ion Pinished renascion Pinished uccessfully	Current Version	New Version	23 3 M9 24 Cancel [5ize 750 kB 300 kB 620 kB 171 kB 300 kB 40 kB	Continue
Connected to localitos	t tion C Ced Car to Long Channe Regut Q Q Q Q Q Q Q Q Q Q Q Q Q	kernel-default pet 2.4.4 Package seted Install	ations for Pinished ransaction I accessfully 100.0% com	Current Versian Current Versian Prinished as completed upleted	Rew Version	23 3 Mo 2 Cancel 5ize	Continu
Connected to locathow expendency a cool (bit yew Artso Channels In Action Channels	t titiones ce cera ns york Channe Requir Q Q Q Q Q Q Q Q Q Q Q Q Q	kernel-default pet 2.4.4 Package sted Install Trensect T	ations ion Finished ransaction I he transaction I he transaction of 100.0% corr	Current Version Current Versio	New Version 7 34 7 34 13 33 33 35 95 52 13 15 20	233 H9 242 Cancel 5ize 750 kB 300 kB 620 kB 171 kB 305 kB 171 kB 305 kB 171 kB 305 kB 2,3 MB	Continu
Connected to localitose openationary action (set your Antion Channels	tt Dependent Corporation Require Q Q Q Q Q Q Q Q Q Q Q Q Q	kernel-default pet 2.4.4 Incy Resolution Package Install Tremsect Tremsect	ations ion Finished rensections uccessfully 100.0% com	Current Version Current Versio	New Version 7 34 7 34 7 34 9 5 9 5 3 2 33 9 5 9 5 9 5 9 5 9 5 9 5 9 5 9 5	233 M9 24 Cancel 5ize 750 kB 300 kB 620 kB 173 kB 305 kB 40 kB 175 kB 2.3 M9 19 4 M8	Continu
Connected to localitose annected to localitose Los yew Action Orannets Connected Connected	t thouse lead Case Are Lipsip Channe Reque Q Q Q Q Q Q Q Q Q Q Q Q Q	ner 7:4.4	ations ion Finished rensaction he transaction he uccessfully 100.0% corr	Current Version	New Version 72 35 57 201 72 34 72 34 73 34 74 74 74	53 3 M9 2 Cancel 5ize 750 kB 300 kB 620 kB 173 kB 40 kB 175 kB 194 MB 194 MB 194 MB	Continu

2. Reboot the server.

FreeRadius Server Installation

- 1. Copy the packages *freeradius-1.0.2-0.i586.rpm*, *freeradius-devel-1.0.2-0.i586.rpm*, *certs.tar.gz* and *radius_npm.tar.gz* into a temporary folder (for example, /tmp/freeradius/sources).
- 2. Launch YAST and install the following packages:

cyrus-sasl-devel	openssl	postgresql-libs
heimdal-devel	openssl-devel	python
heimdal-lib	postgresql-devel	python-devel
mysql-devel	openIdap2-client	db-devel
mysql-shared	openIdap-devel	

- 3. Install FreeRadius, from the Terminal console:
- 4.rpm –Uhv freeradius-1.0.2-0.i586.rpm rpm –Uhv freeradius-devel-1.0.2-0.i586.rpm

SRVASNO2:/tmp/freeradius,	/sources #	
SRVASNO2:/tmp/freeradius,	<pre>/sources # rpm -Uhv freeradius-1.0.2-0.i586.rpm</pre>	
Preparing	***************************************	[100%]
1:freeradius	***************************************	[100%]
SRVASNO2:/tmp/freeradius,	/sources	6.rpm
Preparing	***************************************	[100%]
1:freeradius-devel	***************************************	[100%]
SRVASNO2:/tmp/freeradius,	/sources # 🗧	

FreeRadius Server Configuration+

1. Uncompress the package *radius_npm.tar.gz tar -zxf radius_npm.tar.gz*

Copy *radius.npm* to /var/opt/novell/iManager/nps/packages/ so iManager can find it. *cp /tmp/freeradius/sources/radius.npm /var/opt/novell/iManager/nps/packages/*

- 2. Install the FreeRadius and NMAS plug-ins in iManager.
 - Launch iManager.
 - Go to Configure iManager, then Module Installation, then Available Novell Plug-in Modules.
 - Select Novell Radius Plugin (2.5.20050406) and NMAS plugin for eDirectory (2.5.0.20050224).
 - Click Install.
 - Re-launch Tomcat and Apache.

rcnovell-tomcat4 restart rcapache2 restart

- If needed, reboot the server

3. Extend the eDirectory schema.

The Novell documentation describes three possible scenarios. In our case it's number 3 (rather simple):

- Launch iManager.

- Choose RADIUS, 'Extend Schema for Radius'.

Extend Schema for RADIUS		
The schema extensions for RADIUS have not been installed. Wo	ould you like to extend schema now?	
OK Cancel		
Complete: Schema extension is done.		
Successfully extended the schema for RADIUS.		
OK Repeat Task		

If the schema is already extended, a message will confirm that.

Extend Schema for RADIUS]
The schema extensions for RADIUS have previously been installed and are up to date	1000
Close	I

4. Generate and customize the FreeRadius client & server certificates.

mv /etc/raddb/certs /etc/raddb/certs.org tar -zxf /tmp/freeradius/sources/certs.tar.gz

One of files generated is root.der. You will need to install it on your laptops.

- Open CA.certs and modify it as follows:

Edit the following variables for your organization. # COUNTRY="FR" PROVINCE="IdF" CITY="PARIS" ORGANIZATION="Your-Company" ORG_UNIT="HeadOffice" PASSWORD="XXXXX" COMMON_NAME_CLIENT="LESIEUR FreeRadius" EMAIL_CLIENT="v-info@rin2.fr" PASSWORD_CLIENT=\$PASSWORD COMMON_NAME_SERVER="LESIEUR Server FreeRadius" EMAIL SERVER="v-info@rin2.fr" PASSWORD_SERVER=\$PASSWORD COMMON_NAME_ROOT="LESIEUR SRVASN02" EMAIL_ROOT="v-info@rin2.fr" PASSWORD_ROOT=\$PASSWORD # lifetime, in days, of the certs # #LIFETIME=760 # modified by A.Dachine, Dec 7, 2005 LIFETIME=3650

- Modify also the line number 85, as follows echo "newreq.pem" | ./CA.pl -newca || exit 2

5. (optional) Modify also the line number 68 of the file /etc/ssl/openssl.cnf, as follows default_days = 3650 #10 years

- Go to the folder where the script **certs.sh** is stored (/tmp/freeradius/sources) and run it, as follows: ./certs.sh

- Copy the entire folder /tmp/freeradius/sources/certs to /etc/raddb/certs. *cp –r /tmp/freeradius/sources/certs /etc/raddb/*

6. Extract the eDirectory auto-signed certificate.

- Launch iManager and login to eDirectory.

- Go to 'eDirectory administration', then 'Modify Object'

- Select the CA object and go to its properties. This object is unique in eDirectory and is found in the SECURITY container. In our production eDirectory, the server holding CA role is NOT the FreeRadius server - this is *not* a problem.

- Click the Certificates tab, then choose Self-Signed.

- Click Export and choose NO for private key.
- Save the file in B64 format, named as /etc/raddb/certs/rootder.b64

I Roles and Tasks	Modify Object: 🜠 ca.security	
Directory	General Certificates CRI Configuration Di	IF XAAI
🗉 Droits basés sur le rôle	Public Key Certificate Self Signed Certificate	a same
eDirectory Administration		
Copy Object	Subject name:	O=LESIEUR.OU=Organizational CA
Delete Object	Issuer name:	O=LESIEUR. OU=Organizational CA
Modify Object	Effective date:	samedi 5 novembre 2005 13:12:00
Move Object	Expiration date:	jeudi 5 novembre 2015 15:12:00
Rename Object	Certificate status:	Click validate
± eDirectory Maintenance	Details Export Validate	Replace

Select an output format.
C File in binary DER format



7. Modify the file /etc/raddb/radiusd.conf as follows:

```
max_requests = 7680
#server's IP
bind address = 100.68.100.152
port = 1812
hostname_lookups = no
log_stripped_names = yes
log_auth = yes
# MODULE CONFIGURATION
modules {
        pap {
                 encryption_scheme = crypt
        }
        chap {
                 authtype = CHAP
        }
        pam {
                 pam_auth = radiusd
        }
        # Extensible Authentication Protocol
$INCLUDE ${confdir}/eap.conf
        # Microsoft CHAP authentication
        mschap {
                authtype = MS-CHAP
                use_mppe = yes
                require encryption = yes
           require_strong = yes
                }
        # Lightweight Directory Access Protocol (LDAP)
        Idap {
                 server = "srv02.zoo.com"
                 identity = "cn=adm-radius,ou=site2,o=zoo"
                 password = YYYYY
                 basedn = "o=zoo"
                filter = "(uid=%{Stripped-User-Name:-%{User-Name}})"
                 base_filter = "(objectclass=radiusprofile)"
           start tls = yes
                                         = /etc/raddb/certs/rootder.b64
                tls cacertfile
                 tls cacertdir
                                         = /etc/raddb/certs/
                 tls_require_cert = "demand"
                 access attr = "dialupAccess"
                 dictionary_mapping = ${raddbdir}/ldap.attrmap
                 Idap_connections_number = 10
                 password_attribute = nspmPassword
                 edir_account_policy_check=yes
```

```
timeout = 4
                 timelimit = 3
                 net_timeout = 1
        }
authorize {
        #
        preprocess
        auth_log
        chap
        mschap
        suffix
        eap
        # Read the 'users' file
   files
        ldap
}
# Authentication.
authenticate {
        Auth-Type PAP {
                 pap
        Auth-Type CHAP {
                 chap
        }
        Auth-Type MS-CHAP {
                 mschap
        }
        unix
        Auth-Type LDAP {
                 ldap
        }
        eap
}
# Post-Authentication
post-auth {
        reply_log
        ldap
        Post-Auth-Type REJECT {
Idap
        }
```

8. Modify the file /etc/raddb/clients.conf as follows:

```
client 100.68.100.0/23 {
    secret = XXXXX
    shortname = Site-ASN-Servers
}
#
client 100.68.160.0/24 {
    secret = XXXXX
    shortname = Access-Points-WiFi_DATA
    nastype = other
    ### nastype = cisco
}
```

9. Modify the file /etc/raddb/eap.conf as follows :

```
eap {
default_eap_type = peap
timer_expire = 60
ignore_unknown_eap_types = no
cisco_accounting_username_bug = no
        md5 {
        leap {
        }
        gtc {
                 challenge = "XXXXX"
                 auth_type = PAP
        }
        tls {
        #
                 private_key_password = whatever
                 private_key_password = XXXXX
                 private_key_file = /etc/raddb/certs/cert-srv.pem
                 certificate_file = /etc/raddb/certs/cert-srv.pem
                 # Trusted Root CA list
                 CA file = /etc/raddb/certs/demoCA/cacert.pem
                 dh_file = ${raddbdir}/certs/dh
                 random_file = ${raddbdir}/certs/random
                 fragment size = 1024
                 include_length = yes
        #
                 check_crl = yes
#
     check_cert_cn = %{User-Name}
        ttls {
                 default_eap_type = md5
                 copy request to tunnel = yes
                 use tunneled reply = yes
        }
         peap {
                 default_eap_type = mschapv2
        }
        mschapv2 {
        }
}
```

10. Modify the file /etc/raddb/users.

The goal of modification is to just empty the file, because LDAP directory will be used instead. If you do not want to empty it, find the following line

```
DEFAULT Auth-Type = System
```

and replace it with DEFAULT Auth-Type = LDAP

- 11. Activate the UP (Universal Password) for eDirectory users who are going to use FreeRadius.
 - Launch iManager
 - Go to 'Passwords', Password policies, New
 - Give a name to the policy and configure it.
 - ** ' Remove the NDS Password when setting Universal Password ' : No
 - ** ' Synchronize NDS Password when setting Universal Password ' : Yes
 - ** ' Synchronize Simple Password when setting Universal Password ' : Yes

** 'Allow user agent to retrieve password': Yes
** 'Allow admin agent to retrieve passwords': Yes
** 'Synchronize distribution password when setting Universal Password': Yes
** 'Verify whether existing passwords comply with the password policy (verification occurs on login)'

: Yes

Password Policy Wizard	
Step 1 of 8: Name and describe the Password	Policy
Create a policy name and description of the policy that y	ou are creating.
Policy Name:	
WiFi LESIEUR SIEGE	(ex. Engineer
Description:	
Cet ensemble des règles a été créé le 8 Déc 2005 par A.Dachine dans le cadre de déploiement de WiFi-DATA dans la eDirectory LESIEUR	X
Password Change Message:	
Serveur RADIUS (WiFi) vous demande de changer votre mot de passe	
	Y
Create a new Password Policy based on the defa (Click Next to see summary)	ult settings

Pas	sword Policy Wizard
	Step 2 of 8: Select the Universal Password options
Univ Polic	ersal Password lets you simplify the integration and management of different password and authentication y, you can increase security by setting rules for how users create their passwords.
Wou	ıld you like to enable Universal Password?
С	No (skip to Step 4)
0	Yes (skin to Step 4)
0	Enable the Advanced Password Rules (go to Step 3)
Y	Hide Options
Un	iversal Password Synchronization
	Remove the NDS password when setting Universal Password
•	Synchronize NDS password when setting Universal Password
¥	Synchronize Simple Password when setting Universal Password
Un	iversal Password Retrieval
2	Allow user agent to retrieve password
•	Allow admin to retrieve passwords
•	Synchronize Distribution Password when setting Universal Password
Aut	hentication
¥	Verify whether existing passwords comply with the password policy (verification occurs on login)
P	assword Policy Wizard
	Step 4 of 8: Enable the Forgotten Password feature
Th rei	is feature lets you set up self-service options for users who i nember a password.
W	ould you like to enable the Forgotten Password feature?
12	Yes
C	

- Associate the policy with FreeRadius users (user by user, or with OU).

Password Policy Wizard	
Step 7 of 8: Assign the Password F	olicy
You can assign this policy to multiple indivic object in the tree. To remove an assignmer	Juals, org 1t, select
Assign to:	
user_radius.Lsieur	

Password Policy Wizard		
📑 Step 8 of 8: Summary	r of the Password Policy	
our policy has the following :	settings:	Last Modified
Password Policy Summ	ary	
Name	WIFI LESIEUR SIEGE	
Description	Cet ensemble des règles a été créé le 8 Déc 2005 par A.Dachine dans le cadre de déploiement de \ eDirectory LESIEUR	ViFi-DATA dans la
Universal Password		
Options	Enable Universal Password	true
	Enable the Advanced Password Rules	false
	Remove the NDS password when setting Universal Password	false
	Synchronize NDS password when setting Universal Password	true
	Synchronize Simple Password when setting Universal Password	true
	Synchronize Distribution Password when setting Universal Password	true
	Allow user agent to retrieve password	true
	Verify whether existing passwords comply with the password policy (verification occurs on login)	true
Forgotten Password	Enabled:	false
Policy Assignments	user radius.Lsieur	

	Success
	Complete: Your Password Policy was successfully created.
Click (Close to return to the Password Policy List.

- 12. Create a user like *adm_radius*, with a password. This account will be used to do LDAP searches. Do not deactivate it!
- 13. Make sure the user *adm_radius* has the following rights for each FreeRadius user:
 - ** Compare/Read/Write for ACL attribute
 - ** Compare/Read for all attributes rights
 - ** Browse for Entry rights



14. Give the user *adm_radius* retrieval rights for Universal Password (if this wasn't done yet).

- Launch iManager

- Go to Passwords, Password Policies
- Select or create a policy, then edit it
- Go to Universal Password, Configuration Options
- Select 'Allow admin to retrieve passwords' in 'Universal Password Retrieval'
- 15. Declare an eDirectory user as a FreeRadius user.
 - Create a new eDirectory user (or choose an existing one) with a password.
 - Launch iManager and go to the RADIUS category.
 - Click Create Radius User and select the user just created, then click OK.
 - Click Modify Radius User, select the user just created, and click the 'Other Items' tab.
 - Find the 'Dial Up Access' attribute and set it to ON, then click OK.
 - Make sure the user is associated with the policy created in step 11 (Passwords, Passwords Policies).
 - If necessary, manually type the UP.
 - In iManager, go to Set Universal Password and check to see that the NDS has not expired.
- 16. Make absolutely sure that eDirectory object of each FreeRadius user contains the 'UniqueID' attribute. It must contain the login name of the user. If the attribute doesn't exist, add it. Otherwise, LDAP searches, which are the part of authorization / authentication FreeRadius process, will fail.

17. Start the RADIUS service:

rcradiusd start

- 18. Before configuring the laptops, test FreeRadius with:
 - *** NTRadPing, from a workstation

	🕷 NTRadPing Test	Utility		
	RADIUS Server/port	iprint2	1812	NTRadPing 1.5 - RADIUS Server Testing Tool
	Reply timeout (sec.):	3	Retries: 6	http://www.dialways.com/
	RADIUS Secret key:	your-secret-key		
	User-Name:	user2-radius		
	Password:	******	CHAP	MASTERSOFT DIALWAYS
	Request type:	Authentication Request	• 0	RADIUS Server reply:
	Additional RADIUS A	ttri <u>b</u> utes:		Sending authentication request to server iprint2.1812 Transmiting packet, code-1 ide-] length-52 received response from the server in 172 milliseconds reply packet code-2 ide-] length=20 response: <u>Access: Accept</u>
Good result>	Add <u>R</u> emove	Clear list Loa	▼ d Sa <u>v</u> e	Send Help Close
	💐 NTRadPing Test	Utility		
	RADIUS Server/port	iprint2	1812	NTRadPing 1.5 - RADIUS Server Testing Tool © 1999-2003 Master Soft SpA - Italy - All rights reserved
	Reply timeout (sec.):	3	Retries: 6	http://www.dialways.com/
	RADIUS Secret key:	your-secret-key		ms lo
	<u>U</u> ser-Name:	user2-radius		
	Password:	RNENNENER	CHAP	WASTERSUFT DIALWAYS
	Request type:	Authentication Request	• 0	RADIUS Server reply:
	Additional RADIUS A	ttri <u>b</u> utes:		Sending authentication request to server ipinit2.1812 Transmitting packet, code=1 id=4 length=52 no response from server (limed out), new attempt (#1) received response from the server in 3546 milliseconds reply packet code=3 id=4 length=61 response. Access-Reject
				Reply-Message=NDS error: failed authentication (-669)
			7000	Reply-Message=NDS error: failed authentication (-669)

Bad result --->

*** radtest command, locally on server

Good result:

```
radtest user2-radius password iprint2:1812 1812 secret-passphrase
Sending Access-Request of id 218 to 10.68.10.152:1812
User-Name = "user2-radius"
User-Password = "password"
NAS-IP-Address = iprint2
NAS-Port = 1812
rad_recv: Access-Accept packet from host 10.68.10.152:1812, id=218, length=20
```

Bad result:

```
radtest user2-radius password iprint2:1812 1812 secret-passphrase
Sending Access-Request of id 218 to 10.68.10.152:1812
User-Name = "user2-radius"
User-Password = "password"
NAS-IP-Address = iprint2
NAS-Port = 1812
rad_recv: Access-Reject packet from host 10.68.10.152:1812, id=218, length=20
```

*** Testing the UP and NDS passwords synchronization with UP Diag Tool could be useful, too. We did not need it. (<u>http://support.novell.com/cgi-bin/search/searchtid.cgi?/2970885.htm</u>)

Access Points Configuration

Model: CISCO AIRONET 1100 series (AIR-AP1121G-A-K9) Note: Your configuration may be different.

- 1. Log in to the HTTP interface of the AP (Access point). We have two.
- 2. Go to Security/Server Manager/ and add the following information to the 'Current Server List RADIUS' list:
 - IP address of FreeRadius server
 - Secret phrase
 - Port numbers (1812 and 1813, by default)
 - Click Apply.

EXPRESS SET-UP	Hostname APASN02		
EXPRESS SECURITY			
NETWORK MAP +	Security: Server Manager		
ASSOCIATION +	Backup RADIUS Server		
NETWORK INTERFACES	Backup RADIUS Server:	0fothame or IP A	66r4at)
SECURITY	E C		
Admin Access	shared secret:		
Encryption Manager			
SSID Manager			
Server Manager	Corporate Servers		
Local RADIUS Server			
Advanced Security	Current Server List		
SERVICES +	RADIUS .		
WIRELESS SERVICES +			
SYSTEM SOFTWARE +	(NEW)	Server	10.68.10.152
EVENT LÓG +	10.68.16.15 10.68.16.15 10.68.10.150 10.68.10.150	Shared Secret	
	Delote	Authentication Port (optional);	1812 (0-65536)
		Accounting Port (optional):	1813 (0-65536)

- 3. Go to Wireless Services/WDS, 'Server Groups' tab, select the server group list 'Data' and:
 - Put the IP address of FreeRadius server in the 'Priority 1' field
 - make sure that 'Client Authentication' = 'EAP Authentication'
 - make sure that 'Restrict SSID' = 'ASN_DATA'
- 4. Click Apply.

	- 1 (i	WDS STATUS	Ye	SERVER GROUPS	TE GENE	IRAL SET-UP
IME		Hardmanna ADACNO3				
PRESS SET-UP		Hostname APASNU2				
PRESS SECURITY						
TWORK MAP	+	Wreless Services: WDS - Server Grou	et.			
SOCIATION	+	Conversion Conversion				
TWORK		and a cop and				
TERFACES				Server Group Name: Data		
CURITY	+	<new></new>				
RVICES	+	Telephonie				
RELESS SERVICES		Data		Group Server Priorities: De	afine Servers	
P		-	Dalata	Barrier 1 10 00 10 1	62	
IDS	_		P, ciero	Phone I To be To I		
STEM SOFTWARE				Priority 2: < NONE >		
ENT LOO	+			LANDAR -		
				Priority 2: < NUNE >		
		Use Group For:				
		C Infrastructure Authentication				
		·				
		Courte Authentication				
		Authentication Settin	04		SSID Settings	
		EAP AND	ventination		C Apply to all SSIDs	
		LEAP Au	thentication		Restrict SSIDs (Apply or	vly to listed SSIDa)
		I MAC AVE	hentication		SSID:	
		F				_
		Default (A	Any) Authentication		ASN_DAT	A 4

The WiFi APs now redirect the authentication requests of laptops to the FreeRadius server.

Laptop Configuration

Context:

We want to have as few authentications as possible (our laptops open two sessions: local and Novell). The goal here is to catch the login/password pair of the local Windows session and forward it to FreeRadius, which, in turn, will check it against eDirectory. If the login/password is validated by eDirectory, the user is assigned an IP address and allowed to use network services. Otherwise, IP address is not assigned and the user can access nothing on the LAN.

So, if FreeRadius is configured correctly, a user opens local Windows session, is validated by LDAP (eDirectory), and then opens a second session to the Novell network.

Models used:

Dell Latitude D610 (Intel PRO 2200BG), Dell Latitude D600 (TrueMobile 1300 MiniPCI) and Dell Latitude D600 (Intel PRO 2100 3A)

Common steps for all models:

*** Do not use the Windows WiFi client, because it functions poorly. Use the proprietary WiFi client/tool instead.

*** Update the WiFi driver and configuration tool.

*** Install the *root.der* certificate in the 'Trusted root certification authorities' category. During WiFi connection profile configuration do not forget to select this security certificate.



Dell Latitude D610 (Intel PRO 2200BG)

For a driver update go to http://support.euro.dell.com/support/downloads/ and find the R107434.exe file.

ntel PROSet/	Wireless			- 8 🛛		
ier <u>O</u> utils <u>P</u> rol	ils <u>A</u> ide					
	Vous êtes connecté	(e) à SIEGE.			étails de connexion	
Profils Se connecter	Nom du réseau : Vîtesse : Qualité du signal : automatiquement aux prol	ASN_DATA 54.0 Mbit/s Très bonne ils sans fil dans l'ord	<u>D</u> étails Ire spécifié		Nom du profil : Nom du réseau : Adresse IP : Qualité du signal :	SIEGE ASN_DATA 10.68.40.13 Très borne ==0
- N	am du profil EGE	Nom du réseau ASN_DATA	Propřátás	 ▲ ↓ 	Adresse MAC de la carte Bande Débits de données pris el Fréquence de l'émetteur- Numéro du canal Authentification réceau	00:12:F0:03:40:08 802.11g n ch 1, 2, 55, 6, 9, 11, 12, 18, réce 2.412 GHz 1 WPA-Entransise
Réseaux dispor	ibles (2) G <ssid du="" non="" rése<br="">ASN_DATA</ssid>	au (flusé>			Chiffrement des données Type d'authentification 80 Protocole d'authentification Version CCX TPC CCX Niveaux d'alimentation CC Adresse MAC du point d'a Point d'accès obligatoire	TKIP TKIP 22.1x PEAP 30.0 10.0 mW X 1.0, 5.0, 20.0, 31.6, 50.1 r accès 00:13:7F:52:EF:60 Aucun
Configurer	<u>D</u> étails		Actualise	ei -	Aide ?	Eerme

How to check if you are connected:

In case of authentication failure you will see following messages and information:

🛞 Intel PROSet/Wireless		×
Eichier Qutils Profils Aide		
L'authentification a échou	é.	
Nom du réseau : A: Vîtesse : 5- Qualité du signal : Br	SN_DATA 4.0 Mbit/s onne <u>D</u> étails	
Profils		
Se connecter automatiquement aux profils sar ci-dessous.	is fil dans l'ordre spécifié	
Nom du profil Nor	m du réseau	
SIEGE ASM	LDATA	
	(+)	
		S Erreur dans le processus de connexion
Lonnexion Ajouter	upprimer Proprietes	Cliquez pour lancer les Diagnostics de l'utilitaire de dépannage
Réseaux disponibles (3)		d'Intel Wireless.
Nom du réseau		
•••••• 9 (SSID non diffusé)		
SSID non diffusé>		van En comparative State 2 a
Configurer <u>D</u> étails	Actualiser	
Désactiver l'émetteur-récepteur		
Interrupteur matériel de l'émetteur-récepteur : Act	tivé Aide ? Fermer	En cas diechec diauthentification

(In case of authentication failure)



(The WiFi card seeking the network ...)

Configuring the Intel PROset/Wireless tool

1. Go to Tools / System Administration and provide a password.

🞯 Int	el PROSet/Wireless	Création du mot de passe	
Fichier	Outils Profils Aide	Pour protéger les profils d'administration et les paramètres	
	Paramètres de l'application	Ctrl+P	en empêchant les utilisateurs ne disposant pas de
	Paramètres de la carte	Ctrl+A	privileges administratifs d'y acceder, vous devez creer un mot de passe.
	Utiliser le Client Microsoft	F10	Mot de passe :
	Statistiques avancées	Ctrl+S	Confirmer le mot de passe :
	Utilitaire de dépannage d'Intel Wireless	Ctrl+W	
⊢P	Administration système	Ctrl+T	

2. Click Options and select "Connection before session opening").



3. Click Parameters and select the options shown below.



4. Go to Tools / Application Parameters.





Connection profile "SIEGE" configuration

1. Go to Tools / System Administration, provide the password, and click the Add tab.

Propriétés du profil sans fil -	SIEGE	×
Propriétés du profil sans fil -	SIECE Paramètres généraux Ngm du profil: Ngm du profil: Nom du réseau sans fil (SSID): ASN_DATA Mode opérationnel : Pgmanert : actif si aucu utilisateur n'est connecté. Type de profil d'administration : Pgmanert : actif si aucu utilisateur n'est connecté. Expensed avant aurequire de session/Commune : actif si un Exitisateur est connecté. Ce profil est parlagé par tous les utilisateurs.	
Aide ?	<u>Avancé</u>	

Fill in the last field ('*Identité d'itinérance*') with user's last/first names, even if it's optional. This will help very much during debugging, if any. Do not use French accents!

Propriétés du profil s	ans fil - SIEGE-pilote 🔀
 Nom du profil:SIEGE Paramètres géné Paramètres de ré Paramètres de ré Paramètres de ré Paramètres de ré Serveur PEA 	Arriver Arriv
Aide ?	< <pre><< <u>Précédent</u></pre> Suivant >> OK Annuler
Souther all	
Propriétés du profil	sans fil - SIEGE-pilote
🔗 Nom du profil :SIFG	E Dama Shara da a ƙaralta
Paramètres gén	Paramétres de sécurité
Utilisateur P	Sélectionnez les paramètres de sécurité appropriés pour votre réseau sans fil. EAP Votre administrateur réseau peur vous aider à les sélectionner.
Serveur PE	AP Authentification réseau : WPA - Entreprise 💌
	Chilfrement des données : TKIP
	Activer 802.1x
	Étape 2 sur 2 : Serveur PEAP
	Émetteur du certificat :
	Autoriser les certificats intermédiaires
	Spécifier le nom du serveur/certificat
	Nom du gerveur/certificat :
	Le nom de domaine doit se terminer per le nom snécifié
	-
Aide ?	K Précédent Suivant DK Annuler
3	Administration système
TE	Paramètres d'administration
	Vous pouvez choisir le niveau de contrôle des
	utilisateurs sur leur connexion réseau sans fil.
	2 X 0. Videntation 0
F	Profils d'administration
	Les profils d'administration sont partagés par tous les utilisateurs de cet ordinateur. Pour créer un profil, cliquez
	sur Ajouter.
	Connexion avant ouverture de session/Permanent
	Nom du profil Nom du réseau
	SIEGE ASN_DATA
	+
	Désactiver la commutation de profils Intel. Les
	premier profil de connexion avant ouverture de
	session/permanent uniquement.
	Ajouter Supprimer Propriétés
100 m	
	Modifier le mot de passe Exporter Aide? Fermer

Dell Latitude D600 (TrueMobile 1300 MiniPCI)

For a driver update go to http://support.euro.dell.com/support/downloads/ and find the R94825.exe file.

Configuring the WIFI ASN_DATA Connection

1. Launch the WiFi card tool. Click Advanced, then Properties.

ques Monitorage local Diagr	nostics Informations	
afiguration réseaux sans fil	État de la liaison	
et outil gérer vos paramètres sans fil	il.	
sponibles		
connecter à un réseau sans fil, clique	ez sur Configurer.	
	Configurer	
TA.		
	Rafraichir	
voris		
er automatiquement aux réseaux dis ué ci-dessous :	sponibles dans	Avancées
TA.	Monter	Avancees
	Descendre	Accès réseau
		O Tout <u>r</u> éseau disponible (point d'accès favori)
		Béseaux avec point d'accès uniquement (infractuu
	Exporter	
r Supprimer	Propriétés	O <u>R</u> éseaux ordinateur à ordinateur (ad hoc) uniquem
licône sans fil dans la barre d'état	Avancées	Se connecter automatiquement aux réseaux non fav
OK Annuler /	Appliquer Aide	F
		Propriétés du réseau sans fil Propriétés du réseau sans fil Méthode EAP
		Propriétés du réseau sans fil Propriétés du réseau sans fil Méthode EAP TTLS/PEAP Protocole d'authentification par tunnel EAP-FAST
átés du réseau san	s fil	Propriétés du réseau sans fil Propriétés du réseau sans la Authentification Méthode EAP TTLS/PEAP Protocolo d'authentification par tunnel EAP-FAST Serveur d'authentification
tés du réseau san	s fil	Propriétés du réseau sans fil Propriétés du réseau sans fil Propriétés du réseau sans la Authentification Méthode EAP TTLS/PEAP Protocolo d'authentification per tunnel EAP-FAST Serveur d'authentification Unknown Nom d'utilisateur et mot de passe
tés du réseau san s uréseau sans fil Authentification	s fil	Propriétés du réseau sans fil Propriétés du réseau sans til Authentification Méthode EAP Protocole d'authentification per tunnel EAP-FAST Serveur d'outhentification Nom d'utilisateur et mot de passe Divide pour nom d'utilisateur et mot de passe
tés du réseau sans Il Authentification Iu (SSID) :	s fil	Propriétés du réseau sans fil Propriétés du réseau sans til Authentification Méthode EAP Protocole d'authentification par tunnel EAP-FAST Serveur d'authentification Nom d'utilisateur et mot de passe Invite pour nom d'utilisateur et mot de passe Invite
tés du réseau sans uréseau sans fi Authentification ur (SSID) : ASM <u>UDA</u> sans fi	s fil	Propriétés du réseau sans fil Propriétés du réseau sans fil Propriétés du réseau sans fil Protocole d'authentification Protocole d'authentification par tunnel Protocole d'authentification par tunnel ABP-FAST Serveur d'authentification Unknown Nom d'utilisateur et mot de passe Invite pour nom d'utilisateur et te mot de passe Invite pour nom d'utilisateur et le mot de passe
tés du réseau sans uréseau sans fil Authentification u (SSID) : ESNIDA sans fil nécessite une dé pour l'opération	s fil	Propriétés du réseau sans fil Propriétés du réseau sans fil Propriétés du réseau sans fil Authentification Méthode EAP Protocole d'authentification par tunnel EAP-FAST Serveur d'outhentification Unknown Nom d'utilisateur et mot de passe Wultisateur et mot de passe Wultisateur et mot de passe Wultisateur et is mot de passe Confirme le mot de passe :
tés du réseau sans fil uréseau sans fil Authentification u (SSID) : ASNU DAT sans fil nécessite une dé pour l'opération cation de réseau : WP2	s fil	Propriétés du réseau sans fil Propriétés du réseau sans la Authentification Méthode EAP ITLS/PEAP Protocole d'authentification per tunnel MS-CHAP v2 EAP-FAST Serveur d'authentification Unknown Nom d'utilisateur et mot de passe (m)Utilisateur et mot de passe (confirmer le mot de passe : (certificat
tés du réseau sans réseau sans fil Authentification u (SSID) : ASNUDAT sans fil nécessite une clé pour l'opération cation de réseau : WPA des données : Auto	s fîl	Propriétés du réseau sans fil Propriétés du réseau sans la Authentification Méthode EAP TTLS/PEAP Protocola d'authentification per tunnel EAP-FAST Serveur d'authentification Unixnown Nom d'utilisateur et mot de passe [m/ute pour nom d'utilisateur et le mot de passe [m/ute pour nom d'utilisateur et mot de passe [m/ute pour nom d'utilisateur et le mot de passe [m/ute pour nom d'utilisateur et le mot de passe [m/ute pour nom d'utilisateur et le mot de passe [m/ute pour nom d'utilisateur et le mot de passe [m/ute pour nom d'utilisateur et le mot de passe [m/ute pour nom d'utilisateur et le mot de passe [m/ute pour nom d'utilisateur et le mot de passe [m/ute pour nom d'utilisateur et le mot de passe [m/ute passe : [confirmer le mot de passe : Certificot [dentité/Connexion :
tés du réseau sans réseau sans fil Authentification u (SSID) : Sans fil nécessite une dé pour l'opération cation de réseau : WPA des données : Auto	s fil	Propriétés du réseau sans fil Propriétés du réseau sans la Authentification Méthode EAP TTLS/PEAP Protocola d'authentification per turnel MS.CHAP v2 EAP-FAST Serveur d'authentification Univer pour nom d'utilisateur et mot de passe Invite pour nom d'utilisateur et mot de passe Invite pour nom d'utilisateur et mot de passe Continner le mot de passe : Confirmer le mot de passe : Certificat Identité/Connexion : Queux contificest n'e été sélectionné .>
tés du réseau sans réseau sans fil Authentification u (SSID) : SSID Da sans fil nécessite une dé pour l'opération cation de réseau : WPA des données : Auto u :	s fil	Propriétés du réseau sans fil Propriétés du réseau sans la Authentification Méthode EAP TTLS/PEAP Protocole d'authentification per turnel MS.CHAP v2 EAP-FAST Serveur d'authentification Unknown Nom d'utilisateur et mot de passe Invite pour nom d'utilisateur et le mot de passe Indiquez le domaine Windows DomaineWom d'utilisateurer : Mot de passe : Confirmer le mot de passe : Certificot Identité/Connexion : Selectionnez. Afficher
tés du réseau sans réseau sans fil Authentification u (SSID) : Sans fil nécessite une dé pour l'opération cation de réseau : WP2 des données : Auto u : La cé : .	s fil	Propriétés du réseau sans fil Propriétés du réseau sans la Authentification Méthode EAP Profest Protocole d'authentification per tunnel EAP-FAST Serveur d'authentification Nom d'utilisateur et mot de passe Invide pour nom d'utilisateur et mot de passe Invide passe Invide passe: Confimer le mot de passe Confimer le mot de passe Identité/Connexion: Sélectionne2. Atticher EVValidez le certificat du serveur Emetieur: ILESIEUR FreePandua
tés du réseau sans u réseau sans fil Authentification u (SSID) : SIN DA Isans fil nécessite une clé pour l'opération cation de réseau : WP2 des données : Auto u: la clé (avancé) : 1	s fil	Propriétés du réseau sans fil Propriétés du réseau sans la Authentification Méthode EAP Protocole d'authentification per tunnel EAP-FAST Serveur d'authentification per tunnel Nom d'utilisateur et mot de passe Wite pour nom d'utilisateur et mot de passe Confirmer le mot de passe Confirmer le mot de passe Certificat Identité/Connexion : Certificat Validez le certificat du serveur Emeteur : LESIEUR FreoReadus Valides ver certificats intermédiaires
tés du réseau sans fil Authentification uréseau sans fil Authentification su (SSID) : Isans fil nécessite une clé pour l'opération ication de réseau : WP2 des données : u : la clé : la clé (avancé) : la clé (avancé) :	s fil	Propriétés du réseau sans fil Propriétés du réseau sans la Authentification Méthode EAP Protocole d'authentification per tunnel TTS.FPAP Protocole d'authentification per tunnel EAP-FAST Serveur d'authentification Value pour nom d'utilisateur et mot de passe Wate pour nom d'utilisateur et mot de passe Wate pour nom d'utilisateur et mot de passe Wate pour nom d'utilisateur et mot de passe OnmaineVion d'utilisateur et mot de passe OnmaineVion d'utilisateur et mot de passe Confirmer le mot de passe : Confirmer le mot de passe : Cartificat Identité/Connexion : Validez le certificat du serveur Emetteur : LISIEUR FreoReadus Validez le certificats intermédiaires Nom du serveur :
tés du réseau sans fil Authentification u réseau sans fil Authentification sans fil i sans fil nécessite une clé pour l'opération ication de réseau : WP2 des données : u : la clé : a clé (avancé) : 1 est spécifiée automatiquement à n	s fil suvante : A v omatique v	Propriétés du réseau sans fil Propriétés du réseau sans li Authentification Méthode EAP Protocole d'authentification per tunnel MS-CHAP-V2 Protocole d'authentification per tunnel EAP-FAST Serveur d'authentification Unknown Nam d'utilisateur et mot de passe Image: Serveur d'authentification Unknown Nam d'utilisateur et mot de passe Image: La domaine Windows DomaineWon d'utilisateur et mot de passe Confirmer le mot de passe : Confirmer le mot de passe : Confirmer le mot de passe : Certificat Identité/Connexion : Validez le certificat du serveur Emetteur : LESEUR PreoReduus Validez le certificat sintermédiaires Nom du serveur : Our on du serveur d'out correspondre exactement
Lés du réseau sans fil Authentification u (SSID) : SSID : Sans fil nécessite une clé pour l'opération sains fil nécessite une clé pour l'opération sains fil nécessite une clé pour l'opération sains fil a dé données : J; a clé : a clé (avancé) : 1 : said (avancé) : 1 : un réseau ordinateur à ordinateur sans fil ne sont pas utilisés.	s fil suivante : A v matique v r (ad hoc); les points	Propriétés du réseau sans fil Propriétés du réseau sans fil Propriétés du réseau sans fil Authentification Méthode EAP Protocole d'authentification par tunnel INS-CHAP-Q Protocole d'authentification par tunnel Indiquez le domaine Windows DomaineVNom d'utilisateur et mot de passe Confimer le mot de passe : Confimer le mot de passe : Certificat Identité/Connexion : Volidez le certificat du serveur Emetteur : LESIEUR FreoRadius Valorier certificat sintermédiaires Nom du serveur doit correspondre exactement O Le nom du serveur doit correspondre exactement O Le nom du serveur doit correspondre exactement



1. Move the mouse over the WiFi card icon. If you are connected, authentication state and IP address are displayed.



If the IP is 0.0.0, you are not connected.

Dell Latitude D600 (Intel PRO 2100 3A)

For a driver update go to http://support.dell.com/support/downloads/ and look for the R105328.exe file.

During installation do not forget to select two options: Options for unique session opening - and Connection before session opening.

Intel(R) PROSet	
Pour les cartes réseau Wired (802.3)	
□ □ □ Pour les cartes reseau sans fil (802.11)	
Options d'ouverture de session unique	Je
	Session

Configuring the WIFI ASN_DATA connection



Général	Sécurité	Avancé	Mot de passe						
Exten	sions Cisc Activer la p	o compati rise en ch	bles arge de la gestio	on r <u>a</u> dios	électi	ique			
Point	d'accès ol	oligatoire							
	Utiliser I'ad obligatoire	resse MAI	C du point d'acci	es]	1	1	*	2	1
Impor	tation auto	matique -	utemetiaue						
Gestic	on avancé	e des prot	ills						
	Ce pr <u>o</u> fil pe	ut être utili	sé par tous les ı	tilisateu	rs (Pr	ofil co	mmu	n)	



How to check if you are connected ...

Method 1

Move the mouse over the WiFi card icon. The SSID and connection state are displayed.



<u>Method 2</u> Double-click the WiFi card icon.



Click the General tab.

e ⁹ (*1	
	l rés bonne
Associé et aut	hentifié avec ASN_DATA
Nom du réseau (SSID) :	ASN_DATA
Nom du profil :	SIEGE
Mode :	Infrastructure (Point d'accès)
Sécurité :	TKIP
Vitesse :	11 Mbit/s
Bande (fréquence) :	802.11b (2,4 GHz)
Canal :	11
Protocole 802.1x :	Activé

and then click Details:

		~
Adresse IP de la carte	10.68.40.28	
Mode de sécurité	WPA	
Algorithme de chiffrement	TKIP	
Authentification 802 11	Ouvert	
Authentification 802.1x	PEAP (MS-CHAP-V2)	
Adresse MAC de la carte	00:0C:F1:17:A3:2F	
Adresse MAC du point d'accès	00:13:7F:43:B4:A0	
Type de carte	Mini PCI	
Débits de données supportés	1; 2; 5,5; 11 Mbit/s	
Fréquence du récepteur	2.462 GHz	
Version du logiciel	7.1.4.4	
Version du matériel	∨4.0	
Version du pilote	1.2.4.35	
Interruption	5	
Adresse mémoire	0xFAFEF000	
Point d'accès obligatoire	Aucun	
Version CCX	2.0.0	
Puissance de transmission actuelle	40 mW	1.0
Nivoeu do nuiscenco disponiblo	6 10 16 /0 mW	
<		>

How to check if a user connects without going to the laptop:

- 1. Open a session to the FreeRadius server (Putty or local).
- 2. Run this command:

grep -- ir user-name /var/log/radius/radact/access-point-IP-address/reply-details-XXXXYYZZ

where XXXXYZZ is the date of the file. You should see a list of user's names. Normally, these are successfully connected users! If no user connected, 'Reply' files are not created.

3. Now run this command:

grep –ir "login ok" /var/log/radius/radius.log

Each line with "Login OK" means a successful connection.

Known problems (laptops)

1.<u>Symptom</u>:

WiFi connection seems to be established, but no network application works.
<u>Cause</u>:
IP address of WiFi card is 0.0.0.0
<u>Solution</u>:
Go to WiFi connection properties (My Network Places) and check if the TCP/IP protocol is associated with the card.

2. Symptom:

Everything seems to be configured correctly, but the user still can't connect.

Cause:

Most probably there is something wrong with Universal/NDS Password.

Solution:

On the FreeRadius server, stop the RADIUS service (rcradiusd stop) and re-launch it in debug mode (radiusd -X - A)

Find the exact error. Then:

-- Make sure you followed step 16 of the FreeRadius Server Configuration section of this document, especially the last point (NDS password expiration). Normally, when you change NDS password, UP is

synchronized.

-- If not, change the NDS password once again from a workstation that has the Novell Client installed with the NMAS/NICI option, or from iManager/C1/NWAdmin32.

-- After that, normally, the WiFi connection should be established. It was for us. Don't forget to stop the debug mode of the RADIUS service (press Ctrl-C) and re-launch it normally (rcradiusd start).