

1. Administrativer Zugriff von außen

Autor: Uwe Labs

Stand: 21.03.2008

Inhaltsverzeichnis

- 1.Administrativer Zugriff von außen.....1
 - 1.1. Überblick.....1
 - 1.2. iManager und RemoteManager.....1
 - 1.3. SecureCopy (SFTP).....2
 - 1.4. SSH-Zugriff.....3
 - 1.4.1. SSH-Zugriff von Windows aus.....4
 - 1.4.2. SSH Zugriff von Linux aus (textbasiert).....5
 - 1.4.3. SSH Zugriff von Linux aus (graphisch).....6
 - 1.5. Virtual Network Computing (VNC).....7
 - 1.5.1. VNC mit Client.....9
 - 1.5.2. VNC mit (javafähigem) Browser.....10
 - 1.6. Zugriff per Remote-Windows-XP-Arbeitsstation.....12

1.1. Überblick

In einer Reihe von Fällen muss man Arbeiten am Server durchführen. Dazu gehören Einstellung am eDirectory, Einstellungen im Linuxsystem, Kopieren von Dateien auf das Linux-Filesystem oder auf die NSS-Volumes, Prüfen von Dateien und Einstellungen und vieles mehr. Dabei ist es oft bequem, wenn man dies aus der Ferne und von zuhause aus mit verschiedenen, dem Zweck angepassten Mitteln per Remote-Zugriff tun kann.

Die paedML® 3.0 Novell bietet viele Möglichkeiten, administrativ auf den Gserver03 zuzugreifen. Acht Möglichkeiten sollen hier kurz aufgezählt und vorgestellt werden. Ausführlichere Beschreibungen finden Sie in einzelnen Dokumenten.

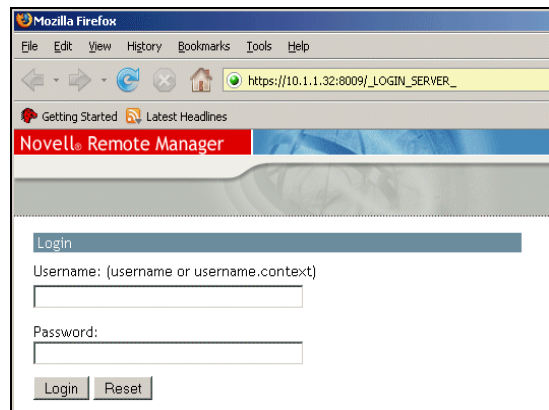
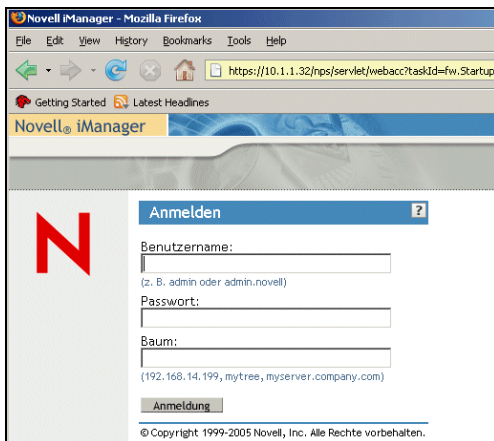
1.2. iManager und RemoteManager

Die schon aus den früheren Novell Musterlösungen bekannten browserbasierten und per SSL-verschlüsselten Zugriffe über den *iManager* bzw. den *RemoteManager* gibt es natürlich auch in der ML3, teils stark erweitert.

Die Aufrufe erfolgen mittels:

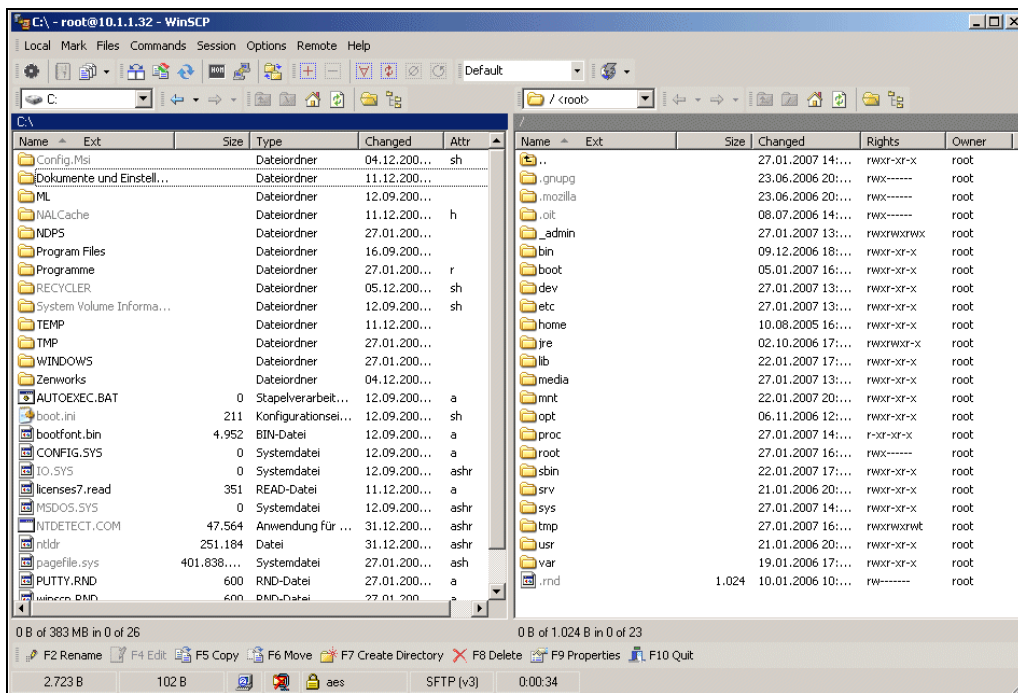
iManager: `https://<server>/nps/iManager`

RemoteManager: `https://<server>:8009`

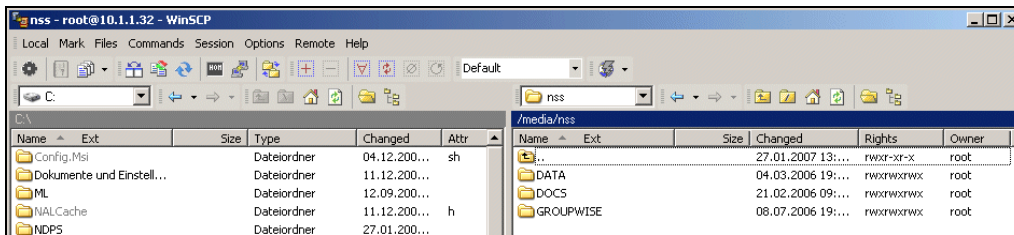


1.3. SecureCopy (SFTP)

Ein bequemer Weg, auf das Dateisystem des Servers ähnlich FTP, jedoch mit verschlüsselter Übertragung, zuzugreifen, ist das Secure Copy Verfahren. Unter Windows stehen dafür verschiedene Programme zur Verfügung, wie z.B. *FileZilla* oder *WinSecureCopy*. Das hier kurz beschriebene *WinSecureCopy* stellt sich standardmäßig wie der Explorer dar, auf der linken Seite ist das lokale Dateisystem, auf der rechten Seite das des Servers zu sehen.

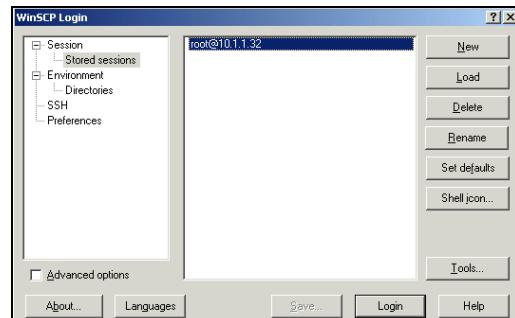
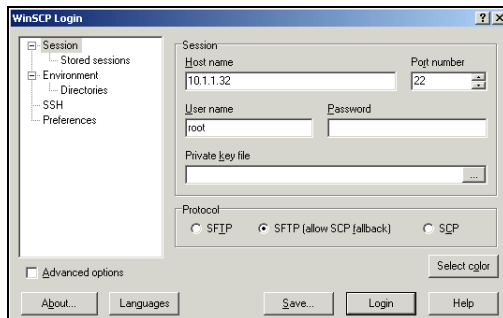


Auch ein Zugriff auf das NSS-Datei-System ist möglich, das unter `/media/nss` „eingehängt“ ist:

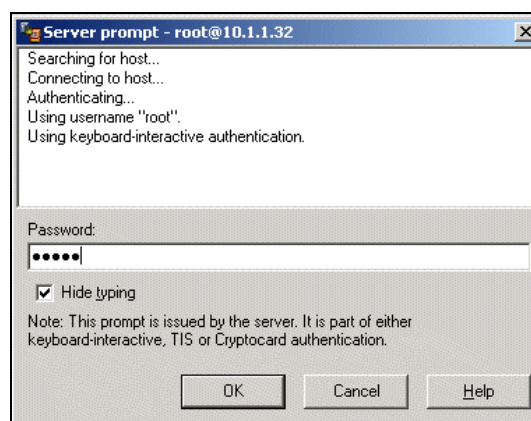


Bedenken sollte man jedoch eventuelle Rechteprobleme, die sich ergeben können, weil man hier als `root` im Linux-System eingeloggt ist, aber im NSS-Bereich, der Novellrechte besitzt, arbeitet.

Wer *WinSecureCopy* zum ersten Mal benutzt, muss den Zugriff auf den `GServer03` konfigurieren. Der Hostname oder die IP ist einzugeben, die Portnummer 22 (*ssh*), bzw. 51222 bei Verwendung der Astaro-Firewall und der Username. Ein Passwort sollte hier aus Sicherheitsgründen nicht eingegeben werden.



Ein anschließender Start über den *Login*-Button führt zur Eingabe des Passwortes:



1.4. SSH-Zugriff

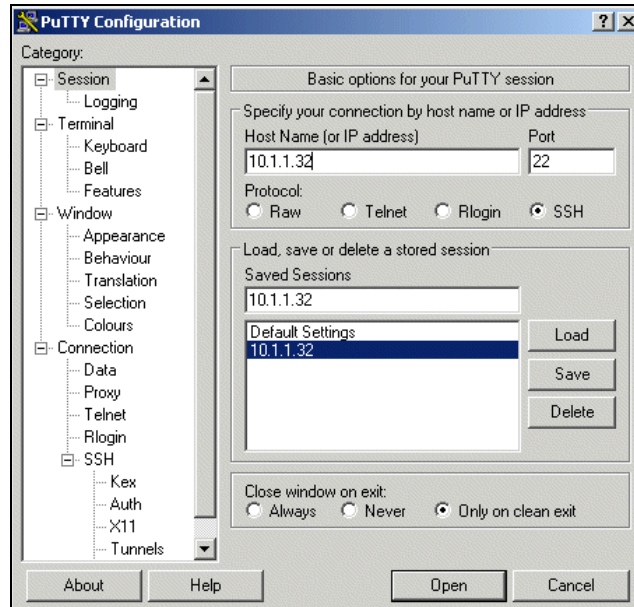
Im einfachen Fall sehen SSH-Zugriffe wie mit einem Terminal-Programm aus. Die Verbindung ist jedoch stark verschlüsselt.

Im Folgenden wird je ein Verfahren, einmal von Windows und einmal von Linux aus, vorgestellt.

1.4.1. SSH-Zugriff von Windows aus

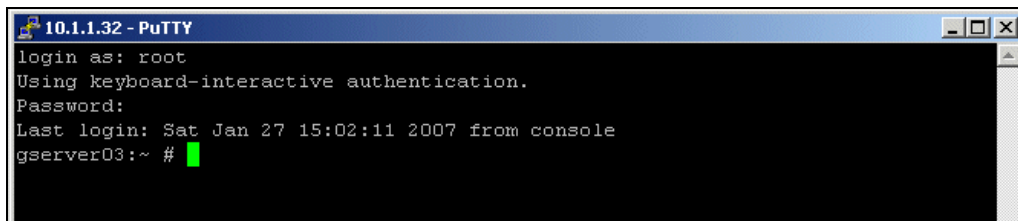
Auch hier gibt es mehrere Programme, die für diese Zugriffsart geeignet sind. Recht beliebt ist das Programm *PuTTY*, das hier als Beispiel dient.

Beim ersten Start muss *PuTTY* für den gewünschten Zugriff konfiguriert werden.

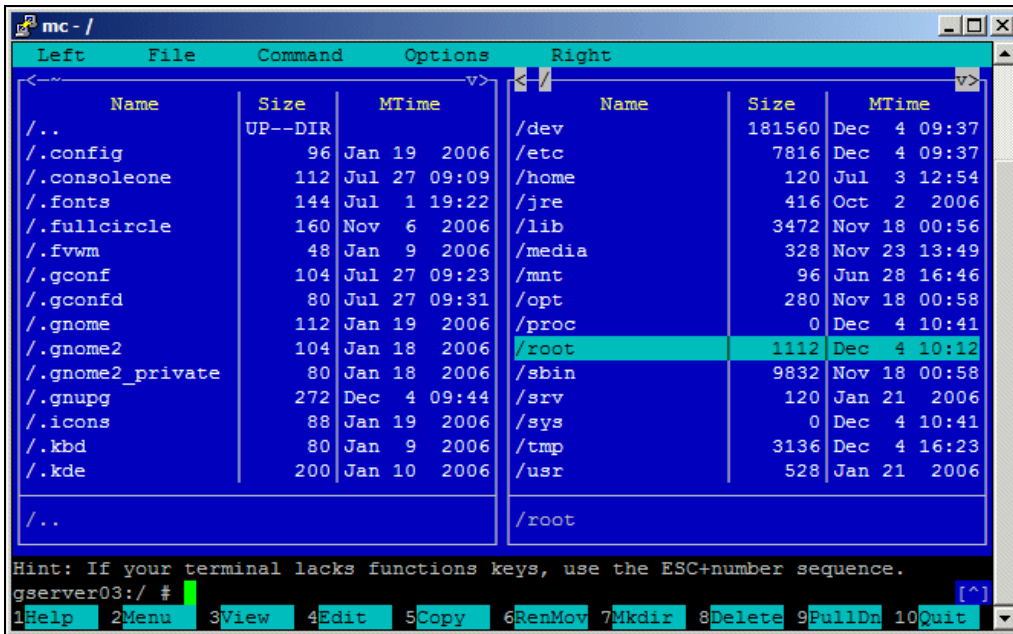


Der Hostname oder die IP ist einzugeben, die Portnummer 22 (*ssh*) bzw. 51222 bei Verwendung der Astaro-Firewall und der Username. Es gibt eine Fülle von Einstellmöglichkeiten, z.B. die Schriftdarstellung betreffend, mit der die Verbindung optimiert werden kann.

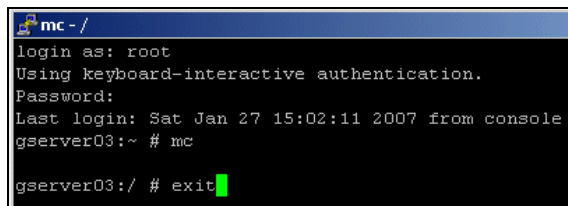
Ein Klick auf den *Open*-Button startet das „Terminal“-Fenster, in dem man sich im Textmodus am Server anmelden kann.



Ein beliebter Linux-Dateimanager ist der *Midnight-Commander*, der dem früheren *Norton-Commander* sehr ähnlich ist und viele Arbeiten erlaubt:



Geschlossen wird die Verbindung mit der Eingabe von exit:



1.4.2. SSH Zugriff von Linux aus (textbasiert)

Wer ein Linux-System (z.B. ein SuSE-System) hat, kann auch von dort bequem und verschlüsselt auf den ML3-Server zugreifen. Man öffnet eine Shell (ein Terminal-Fenster) startet die Verbindung mit

```
ssh <server/ip>
```

(In den folgenden Abbildungen unterscheidet sich das Linux-System (z.B. zu Hause) vom ML3-Server durch den Prompt:

```
linux:~ # z.B. häusliches Linux-System
```

```
gserver03:~ ML3-Server
```

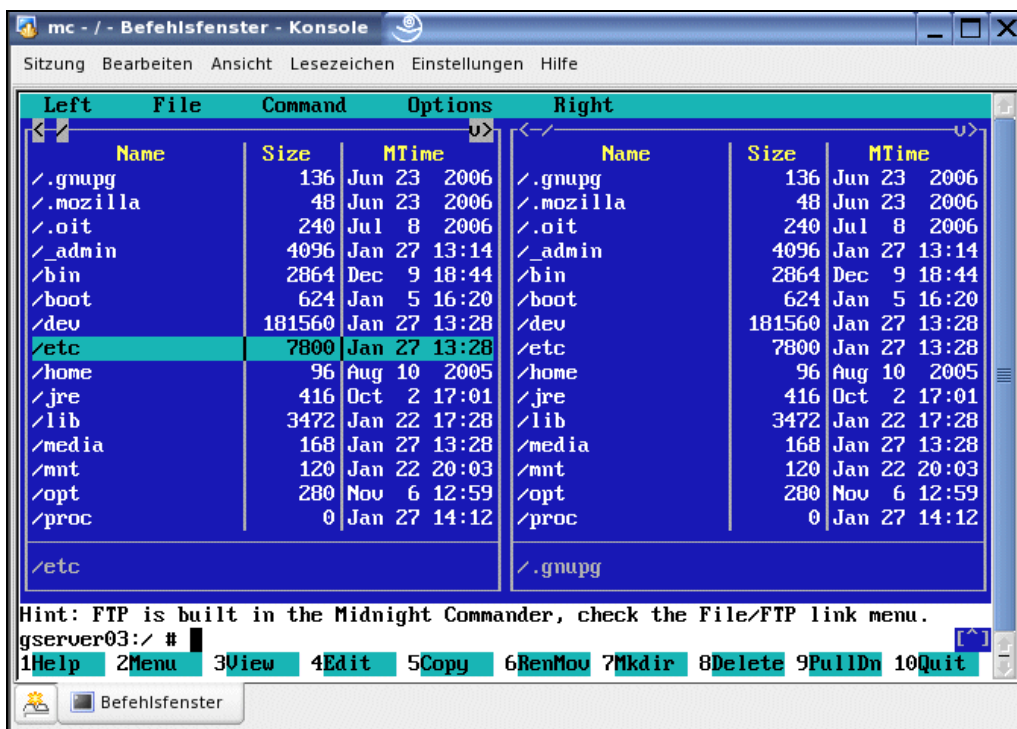
Ggf. muss beim ersten Verbinden die Verbindung mit `yes` bestätigt werden.

```

Befehlsfenster - Konsole
Sitzung Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe

linux:~ # ssh 10.1.1.32
The authenticity of host '10.1.1.32 (10.1.1.32)' can't be established.
RSA key fingerprint is a8:0a:fc:69:30:bb:6e:3a:2c:c5:1f:6d:7e:8c:42:80.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.1.1.32' (RSA) to the list of known hosts.
Password: █
    
```

Jetzt kann man so arbeiten, als säße man vor einem Terminal-Fenster direkt am ML3-Server. Auch der beliebte *Midnight-Commander* lässt sich benutzen:



Geschlossen wird die Verbindung mit der Eingabe von `exit`:

```

gserver03:/ # exit
logout
Connection to 10.1.1.32 closed.
linux:~ # █
    
```

Dann befindet man sich wieder im (z.B. heimischen) Linux-System.

1.4.3. SSH Zugriff von Linux aus (graphisch)

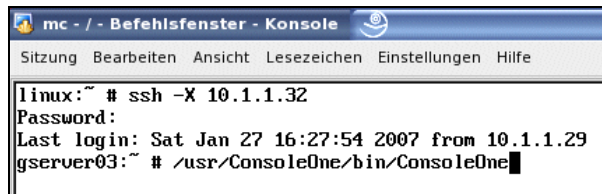
Sehr angenehm wäre der oben beschriebene Zugriff, wenn er erlauben würde, graphische Programme zu starten. Und genau das ist möglich. Die einzige Einschränkung ist, dass man wissen muss, wie die graphischen Programme, textbasiert aufgerufen werden müssen.

Dem `ssh`-Aufruf von oben ist lediglich der Kommandoschalter `-X` hinzuzufügen:

```
ssh -X <server/ip>
```

In der folgenden Abbildung wird die linuxbasierte ConsoleOne auf dem ML3-Server gestartet. Diese liegt im Verzeichnis

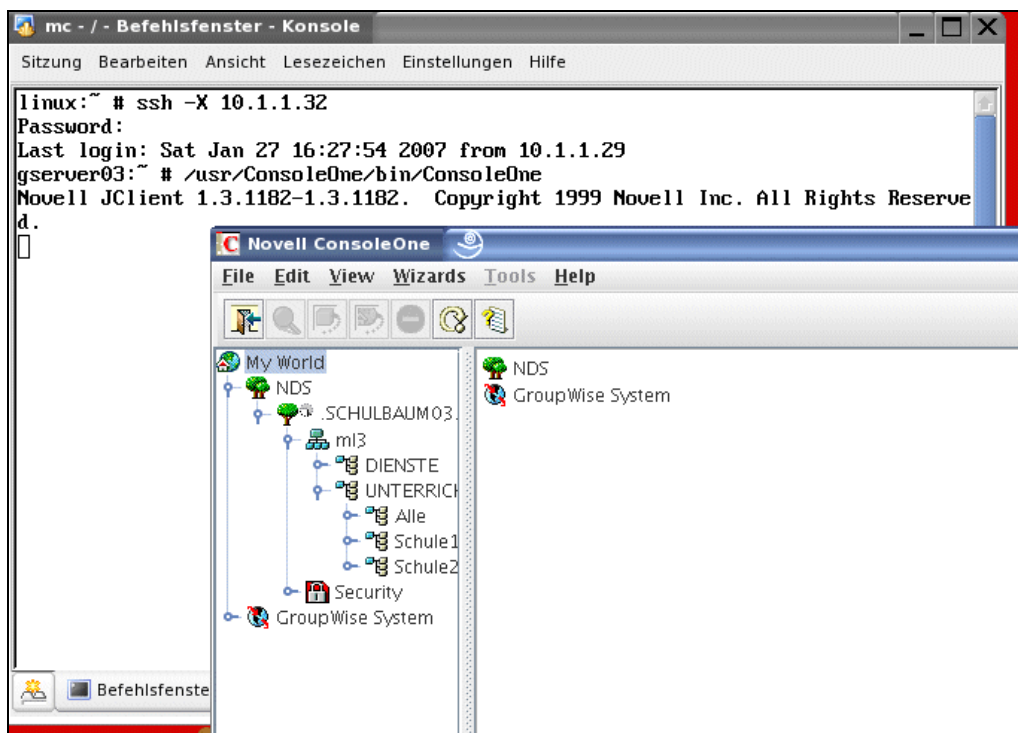
```
/usr/ConsoleOne/bin
```



```
mc - / - Befehlsfenster - Konsole
Sitzung Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe

linux:~ # ssh -X 10.1.1.32
Password:
Last login: Sat Jan 27 16:27:54 2007 from 10.1.1.29
gserver03:~ # /usr/ConsoleOne/bin/ConsoleOne
```

Danach öffnet sich ein GUI-Fenster mit der graphischen Ansicht der *ConsoleOne*. In der folgenden Abbildung ist im Hintergrund das Terminalfenster und ein Stück vom Desktop (zu Hause) auf dem Linux-System zu sehen, im Vordergrund die *ConsoleOne* auf dem ML3-Server:



1.5. Virtual Network Computing (VNC)

Auf dem ML3-Server ist der VNC-Dienst installiert. Mit einem geeigneten VNC-Client oder mit einem Java-fähigen Browser, sei es von einem Windows- oder Linux-System aus, kann man auf den vollständigen Desktop des ML3-Servers zugreifen. Die Verbindung wird per SSL verschlüsselt und ist deswegen nicht ganz so sicher, wie die SSH-Methode.

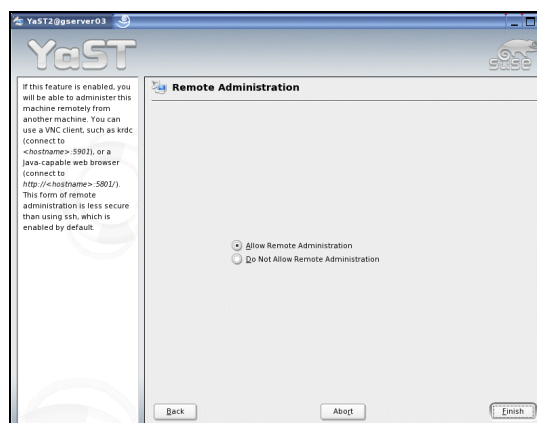
ACHTUNG: Im Folgenden werden die Einstellungen beschrieben, mit denen der VNC-Zugriff möglich ist. Nach Fertigstellung der Einstellungen startet der Server bei einem Neustart nicht mehr in den Textmodus, sondern in den graphischen Modus, und zwar dauerhaft!

(Um den Server wieder im Textmodus starten zu lassen, müssen die unten angegebenen Yast-Einstellungen rückgängig gemacht werden. Außerdem muss in der Datei `/etc/inittab` der Eintrag `id:5:initdefault:` auf `id:3:inidefault:` zurückgesetzt werden.)

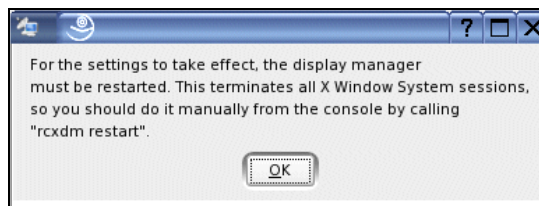
Auf Ihrem ML3-Server ist der VNC-Dienst aus Sicherheitsgründen noch nicht eingeschaltet. Dies können Sie mit *YaST* erledigen. Starten Sie *YaST* und wählen die Menüpunkte *Networkservices/Remote Administration*



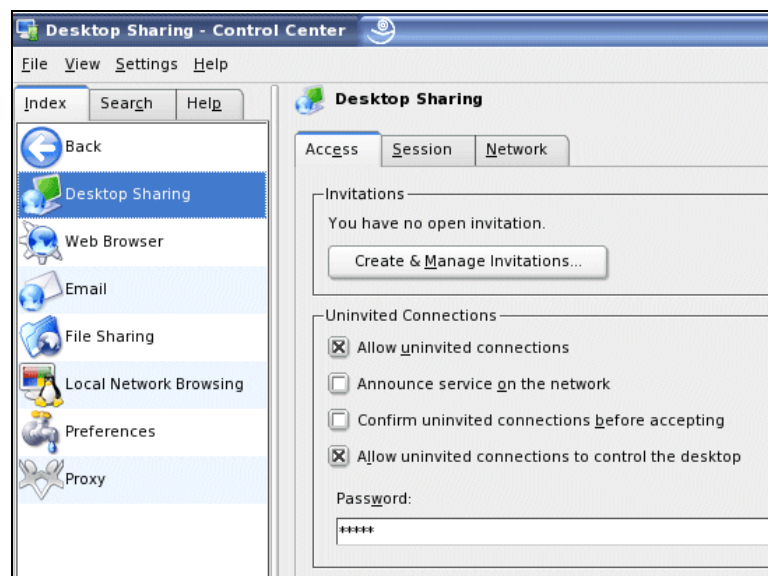
und dann *Allow Remote Administration*. Beenden Sie mit dem *Finish*-Button.



Es erscheint noch die Meldung,



die Sie befolgen können. Besser jedoch starten Sie anschließend den ML3-Server neu. Für die VNC-Client-Zugriffe sollten Sie jetzt noch die Art des Zugriffs und ein Passwort vergeben. Dazu starten Sie das KDE-Control-Center und wählen nacheinander die Menüpunkte *Internet & Network*, *Desktop Sharing*. Rechts im Fenster sollten Sie die Kreuze z.B. so setzen, wie angezeigt (damit wird kein „Erlaubnisfenster“ am Server angezeigt, dass dort bestätigt werden müsste, was ja nicht so leicht wäre, wenn Sie die VNC-Sitzung von zu Hause aus machen wollen; es sei denn per *ssh* (siehe oben)). Außerdem sollten Sie ein starkes Passwort wählen.

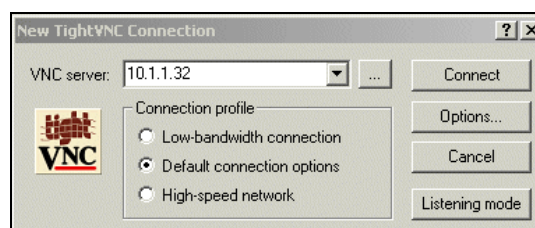


Damit sind die Vorbereitungen zur VNC-Nutzung abgeschlossen.

1.5.1. VNC mit Client

Es gibt unzählige VNC-Clients, sowohl für Windows als auch für Linux. In der Novell-OES-Dokumentation zum OES wird der *TightVNC-Client* erwähnt, den wir hier als Beispiel benutzen. Dieser Client muss auf dem Windows-Computer nicht einmal installiert werden; ein Kopieren reicht, vielleicht noch mit einer Verknüpfung.

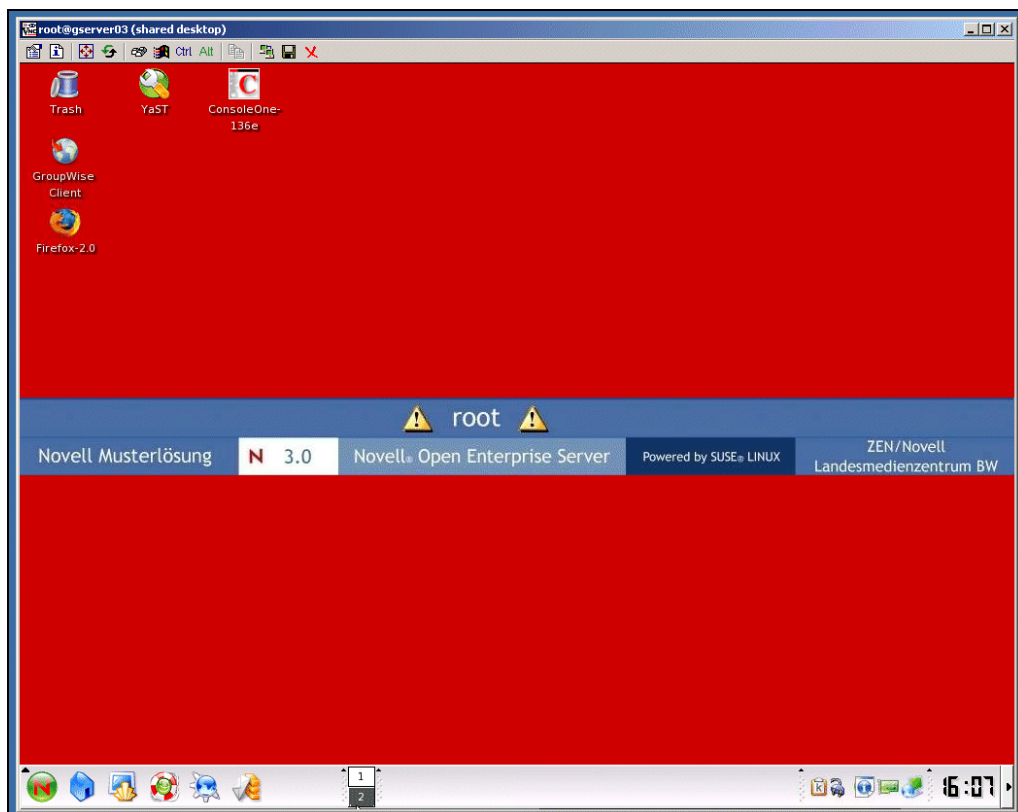
Der Start von *vncclient.exe* führt zum Fensterchen:



Nach Eingabe des Servernamens oder der IP wird die Verbindung mit dem *Connect*-Button hergestellt. Zwei weitere Fensterchen erscheinen, eines, mit dem man den Client verstecken kann, eines für die Passwordeingabe, des Passwortes, welchen oben im KDE-Control-Center festgelegt wurde.



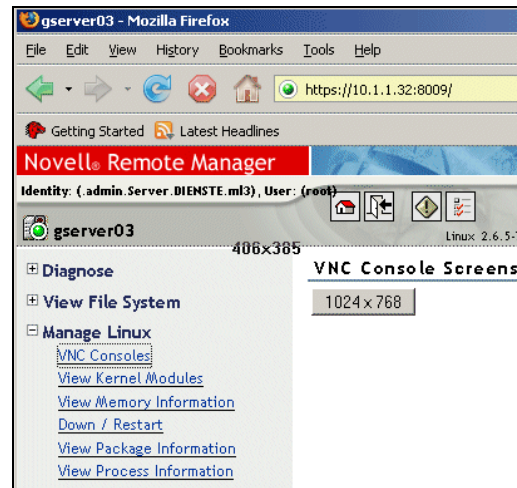
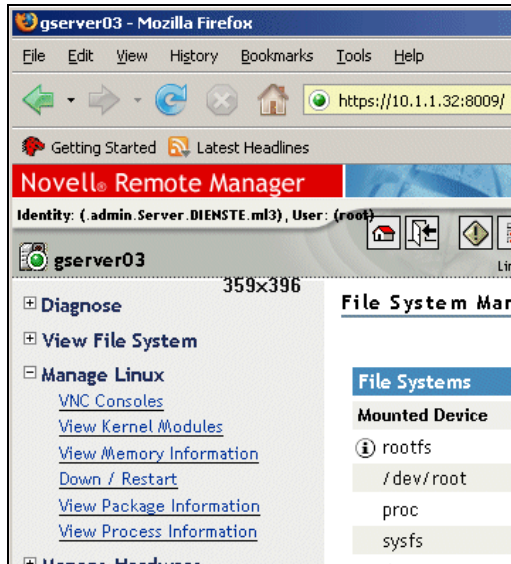
Dann öffnet sich ein Fenster, das den kompletten Desktop des ML3-Servers in dem Zustand zeigt, in dem er sich gerade befindet:



Nach Ihrer Arbeit beenden Sie die Sitzung mit einem *Disconnect* (rotes Kreuz oben rechts in der Toolbar-Leiste).

1.5.2. VNC mit (javafähigem) Browser

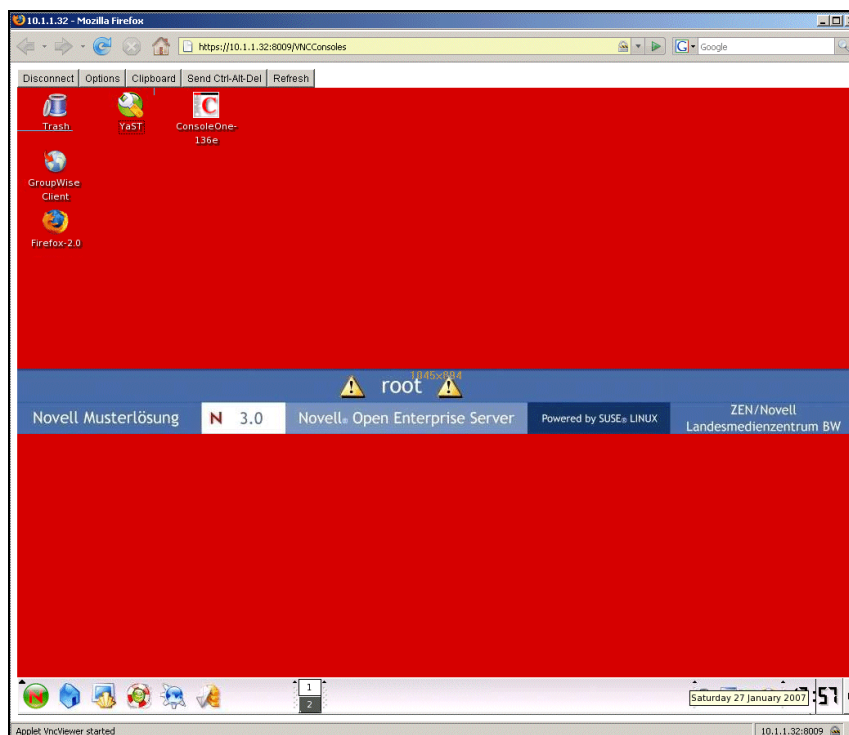
Öffnen Sie auf irgendeinem Computer einen javafähigen Browser, z.B. Firefox. Starten Sie den Novell RemoteManager mit `https://<server>:8009` und wählen Sie den Menüpunkt *Manage Linux/VNC Consoles* und klicken Sie auf den Button *1024x768*:



Daraufhin öffnet sich ein neues Browserfenster, das den ML3-Desktop zeigt:



und nach den Einloggen



Jetzt kann man so arbeiten, als säße man vor dem ML3-Server. Selbst eine 1024/128-DSL Verbindung ist noch ausreichend, jedenfalls für wichtige Arbeiten. Beendet wird die Sitzung durch einen Klick auf den *Disconnect*-Reiter oben.

1.6. Zugriff per Remote-Windows-XP-Arbeitsstation

Eine weitere sehr elegante Methode ist ein Zugriff über eine ferngesteuerte in der Schule stehende Windows-XP-Arbeitsstation. Bei dieser Methode, bei der Sie z.B. von zu Hause aus eine Windows-XP-Arbeitsstation in Ihrem Schulnetz fernsteuern, sitzen Sie quasi vollständig im Schulnetz und haben daher alle Möglichkeiten, wie in der Schule. Diese „Falksche Methode“ ist ausführlich in einem Dokument auf dem Support-Server beschrieben. (<http://www.support-netz.de/nml-remotedesktop.html>)

