

VMware VIEW 4 und Novell



Autor: Christian Johannsen <christian.johannsen@mightycare.de>

Erste Veröffentlichung: 22.02.10

Datum der letzten Änderung: 23.02.10

MightyCare Solutions GmbH
Philipp-Reis-Str. 15a
D-61130 Nidderau

Fon: +49 (0) 6187 900 156
Fax: +49 (0) 6187 900 157

<http://www.mightycare.de>

Historie:

Version	Änderung
0.1	Aufbau Gliederung und Beschreibung der Zielstellung
0.2	Beschreibung OES Installation und DSfW Erweiterung
0.3	Beschreibung der Funktionsüberprüfung DSfW
0.4	Beschreibung der OS Integration und der VIEW Konfiguration
0.5	Troubleshooting und Finalisierung

Inhaltsverzeichnis

1 Zusammenfassung	4
2 SLES und OES	4
2.1 Domain Services for Windows	5
2.1.1 Installation und Konfiguration	6
2.1.2 Test der Funktionen	8
2.2 Benutzermanagement	9
3 VMware VIEW	10
3.1 Konfiguration des OS (VIEW Manager)	10
3.2 Konfiguration des OS (VIEW Agent)	11
3.3 Konfiguration Benutzer	11
4 Troubleshooting	11
4.1 Domänen-Integration	12
4.2 Administrator-Account	12
4.3 vCenter Authentifizierung	13
5 Quellen und Nachweise	13
6 Begriffe und Abkürzungen	14

1 Zusammenfassung

Das nachfolgende Whitepaper beschreibt eine Möglichkeit der Integration einer VMware VIEW 4 Umgebung in einer Novell eDirectory. Der beschriebene Lösungsweg basiert auf Erfahrungen der Mightycare Solutions GmbH und stellt derzeit keinen offiziellen von VMware unterstützten Lösungsweg dar.

Die hier beschriebene Lösung zur Integration des VMware VIEW 4 Manager bzw. des connection broker basiert auf einer SuSe Linux Enterprise Server 10 SP3 Installation und dem Novell Open Enterprise Server 2 SP2. Zusätzlich wird der OES um eine Komponente erweitert die eine Integration erst möglich macht: Domain Services for Windows 1.0.

Anders als bei bekannten Workarounds zur Integration, wie dem Identity Manager oder Active-Directory Replika-Servern auf Windows Basis fallen bei dieser Lösung keine Microsoft Server Lizenzen oder Client-Access-Lizenzen (CALs) an.

2 SLES und OES

Basis für eine Integration der VMware VIEW Umgebung und Installation einer DSfW Erweiterung ist die SLES 10 SP3 Installation mit einem OES 2 SP2. In den meisten Umgebungen ist diese Basis bereits vorhanden, wenn eine eDirectory als Verzeichnisdienst eingesetzt wird. Für eine eventuelle Neu- oder Testinstallation können beide Komponenten unabhängig voneinander im Novell Download-Bereich (<http://download.novell.com/>) heruntergeladen werden.

Basierend auf der SLES Installation kann der OES als Add-On installiert werden. Dies geht auch per grafischer Oberfläche mittels YaST. Hier kann nach dem Mounten des OES Mediums eine Add-On Installation gestartet werden und danach können die jeweiligen Komponenten ausgewählt und installiert werden.

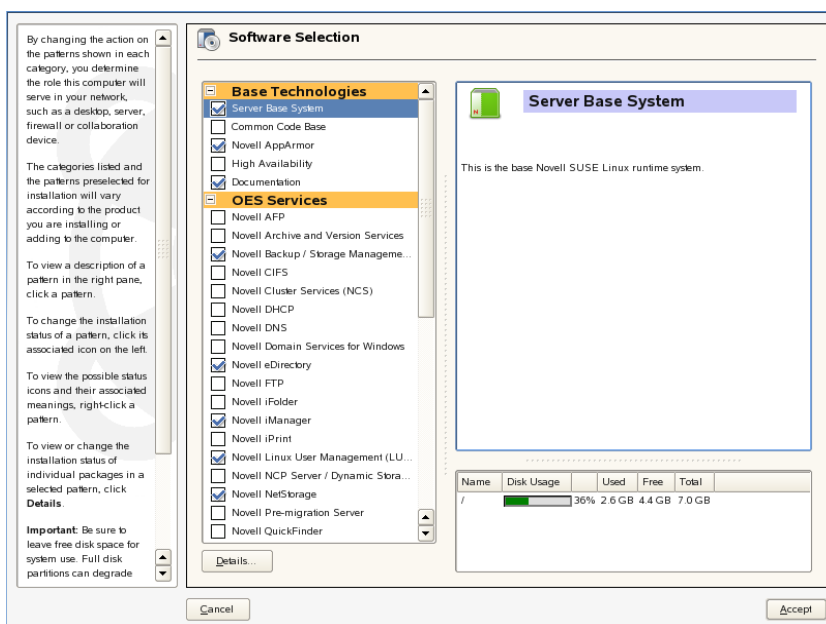


Abbildung 1 – Add-On Installation

Neben der reinen eDirectory Installation können hier schon weitere Services ausgewählt und installiert werden, unter anderem die Novell Domain Services for Windows. Eine Konfiguration wird nachfolgend automatisch gestartet und wird in Absatz 2.1.1 genauer erläutert.

2.1 Domain Services for Windows

Die Domain Services for Windows 1.0 ermöglichen den Windows-Anwendern und Applikationen den Zugriff auf den OES über die nativen Windows und Active-Directory Protokolle, ohne den sonst notwendigen Novell Client. Durch diese Möglichkeit des Zugriffs wird die Co-Existenz zwischen den beiden Verzeichnisdiensten bzw. Plattformen weiter verbessert.

DSfW basiert auf verschiedenen Komponenten (Abbildung 1) die im Zusammenspiel eine AD-ähnliche Bereitstellung ermöglichen.

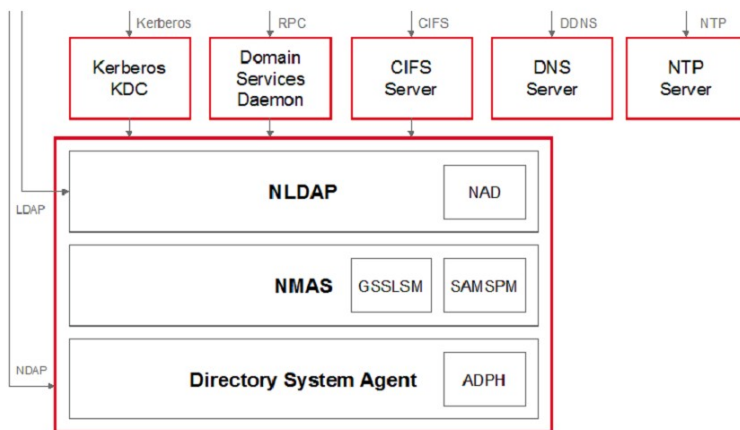


Abbildung 2 – DSfW Komponenten

Die Technologien zur Umsetzung sind:

- **eDirectory** als Verzeichnisdienst in Version 8.8 SP2 oder höher
- **KDC** als AD-ähnliche Authentifizierung
- **NMAS** Erweiterungen zur GSS-API Authentifizierung
- **ADPH** als Mittler für die Clientsysteme
- **Domain Services Daemon** für remote procedure calls und Sicherheitsmechanismen
- **NAD** virtualisiert das AD-Model in der eDirectory
- **CIFS** als Datei-Service-Protokoll
- **DNS** wurde modifiziert für den GSS-TSIG Support (Kerberos)
- **NTP** als Zeitserver für die Domäne

Das Zusammenspiel der einzelnen Technologien ermöglicht dann Mehrwerte wie das Client-lose Anmelden, das unabhängige User-Management, Cross-Domain/ -Forest Beziehungen und das Anmelden mit einem einzigen Passwort.

2.1.1 Installation und Konfiguration

Nachdem die DSfW während der Add-On Installation ausgewählt wurden kann die nachfolgende Konfiguration beginnen. Zuerst wird eine neue Domain Service for Windows Gesamtstruktur und deren DNS-Name für die „Windows-Domäne“ definiert.

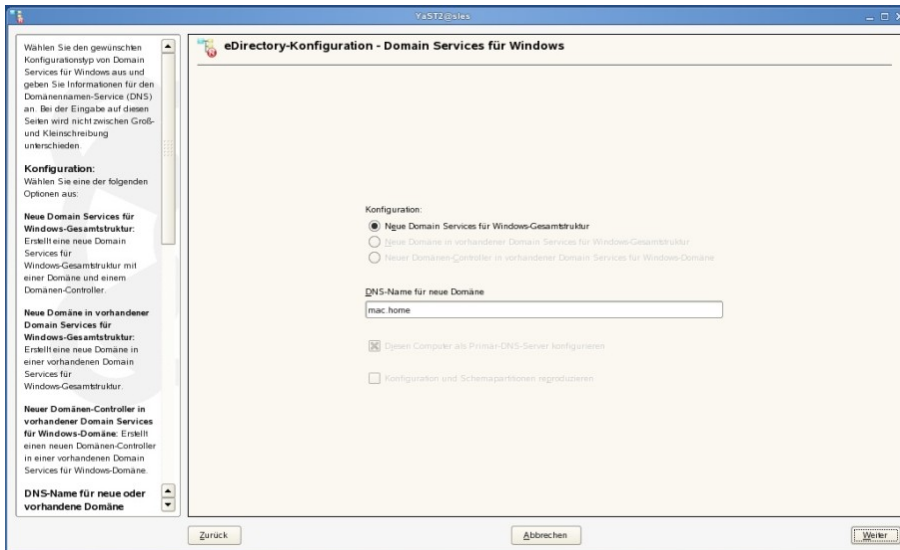


Abbildung 3 – DSfW Start

Nachfolgend muss in einem weiteren Fenster der Domänen-NetBIOS Name definiert werden und im nachfolgenden Installationsschritt muss ein Passwort für den Administrator der neuen Domäne definiert werden.

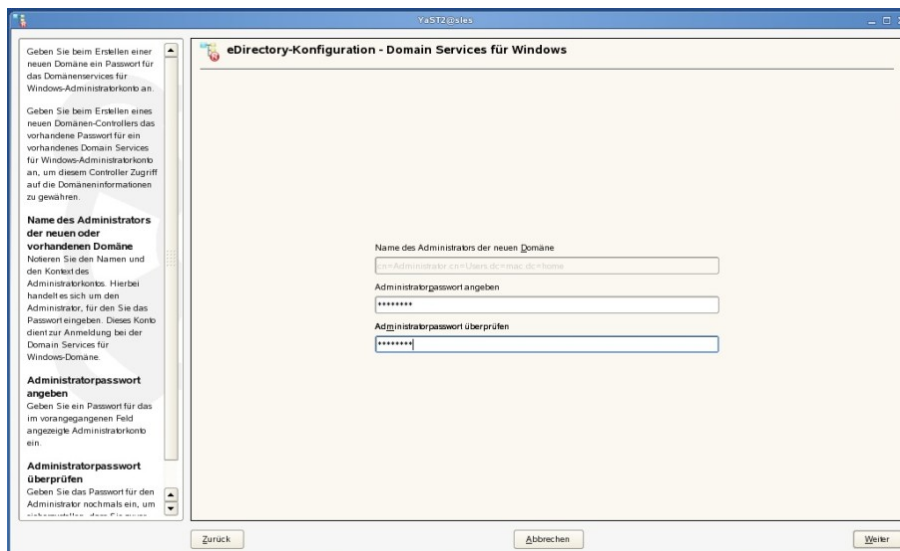


Abbildung 4 – DSfW Administrator-Passwort

Dieser Account ist in der späteren „Windows-Domäne“ der Domänen-Administrator. Eine versehentliche Löschung bzw. ein zu einfaches Passwort erfordern im Problemfall einen hohen Änderungsaufwand.

Im nächsten Installationsschritt kann der eDirectory DIB Pfad angepasst werden und eventuelle Port-Veränderungen vollzogen werden. Danach folgt die DNS-Konfiguration, die einen wichtigen Teil der DSfW Umgebung darstellt.

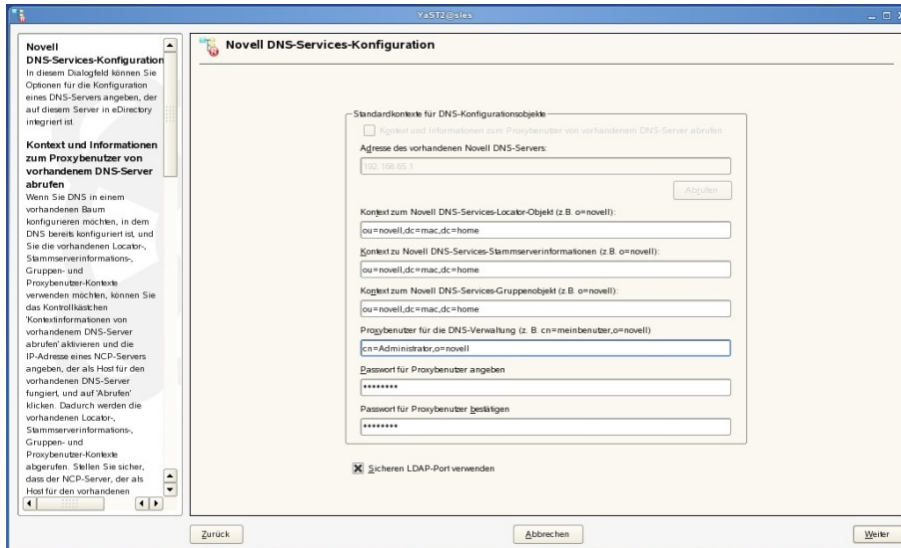


Abbildung 5 – Novell DNS-Konfiguration

Neben der reinen DNS-Konfiguration muss noch ein Proxy-Benutzer für die DNS-Verwaltung hinterlegt werden.

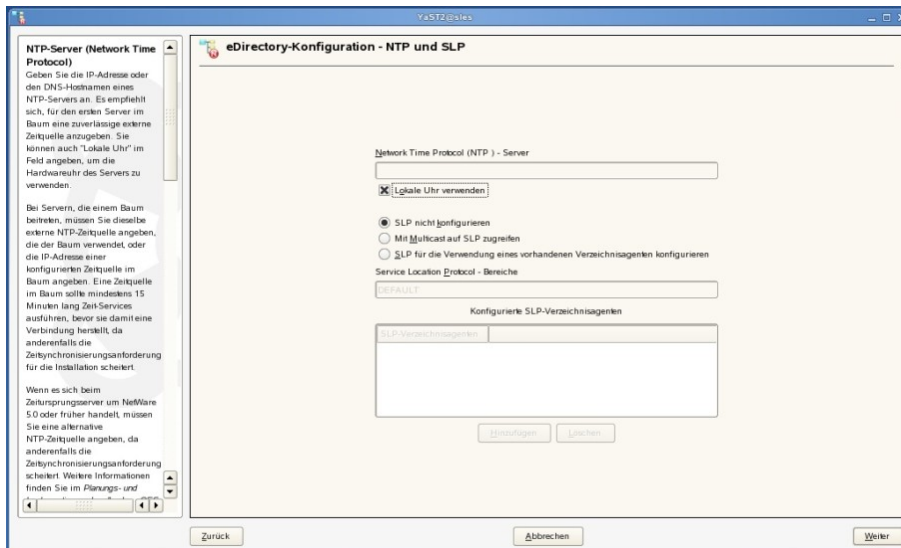


Abbildung 6 – Novell NTP, SLP Konfiguration

Abschließend kann nun der NTP Server hinterlegt werden oder die lokale „Hardware-Uhr“ verwendet werden. Es ist jedoch ratsam den NTP-Server zu wählen (Achtung bei virtualisierten Systemen und dem „Timekeeping“ Problem), da eine AD-Synchronisation auch hier bei zu starken Zeitdifferenzen (>5 Minuten) zum Problem werden kann. Zusätzlich kann auch noch Novell SLP (erforderlich in großen Umgebungen) konfiguriert werden.

Abschließend übernimmt YaST die abschließende Konfiguration (Abbildung 7).

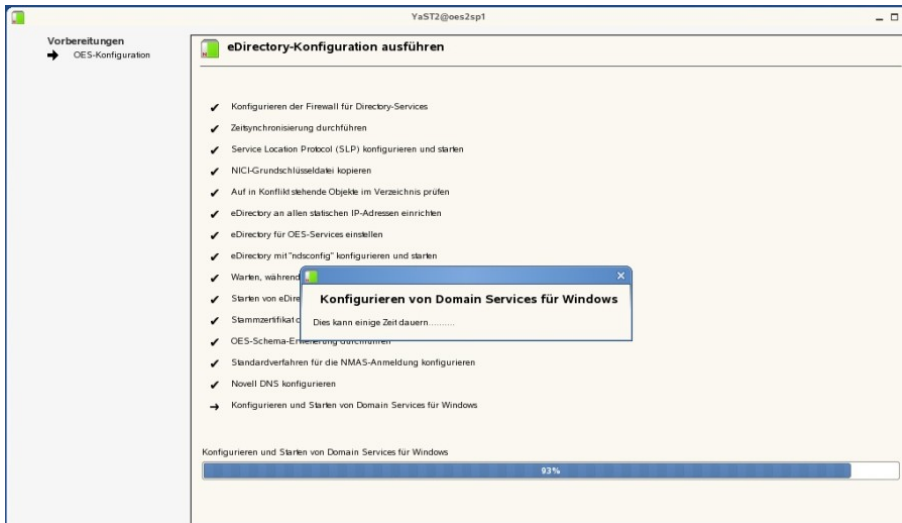


Abbildung 7 – abschließende Konfiguration

2.1.2 Test der Funktionen

Nachdem die Installation und Konfiguration erledigt ist, kann die Funktion der DSfW geprüft werden. Nach Prüfung der `/etc/hosts` und `/etc/resolv.conf` kann der DNS-Deamon mittels `rcnovell-named restart` neu gestartet werden. Nachdem der Deamon erfolgreich neu gestartet wurde sollte die Funktion der eDirectory geprüft werden:

```
/opt/novell/eDirectory/bin/ndsstat -h localhost
```

und bei erfolgreicher Ausführung folgendes Ergebnis zu sehen sein:

```
Tree Name: MAC
Server Name: .CN=sles.OU=novell.dc=mac.dc=home.T=MAC.
Binary Version: 20217.06
Root Most Entry Depth: 0
Product Version: eDirectory for Linux v8.8 SP4 [DS]
```

Die eigentliche Dienst kann jederzeit mittels `xadcntrl status` geprüft werden und sollte in etwa folgendes Ergebnis ausgeben:

```
Tree Name: MAC
Server Name: .CN=sles.OU=novell.dc=mac.dc=home.T=MAC.
Binary Version: 20217.06
Root Most Entry Depth: 0
Product Version: eDirectory for Linux v8.8 SP4 [DS]
```

```
Checking for nameserver BIND
number of zones: 2
debug level: 0
xfers running: 0
xfers deferred: 0
soa queries in progress: 0
```



```

query logging is OFF
recursive clients: 0/1000
tcp clients: 0/100
server is up and running
zone details are dumped at /var/opt/novell/log/named/named_zones.info
running
Checking for Name Service Cache Daemon: running
Checking for RPC Endpoint Mapper Service running
Checking for Kerberos KDC Service running
Checking for Kerberos Password Change Server running
Checking for Domain Services Daemon running
Checking for Samba NMB daemon running
Checking for Samba WINBIND daemon running
Checking for Samba SMB daemon running

```

Zusätzlich sollte das Novell Schema Tool im YaST ausgeführt werden und die Schema-Erweiterungen für die DSfW und LUM installiert werden. Abschließend kann alles per `xadcntrl restart` neu gestartet werden.

2.2 Benutzermanagement

Wie bereits erwähnt unterscheiden sich die Nutzer der eDirectory von denen der DSfW, so dass beide eigenständig zu verwalten sind. Um einen Microsoft Windows-Anwender anzulegen kann zum einen der Novell iManager auf dem OES verwendet werden, zum Anderen die bekannte MMC der Windows-Umgebung.

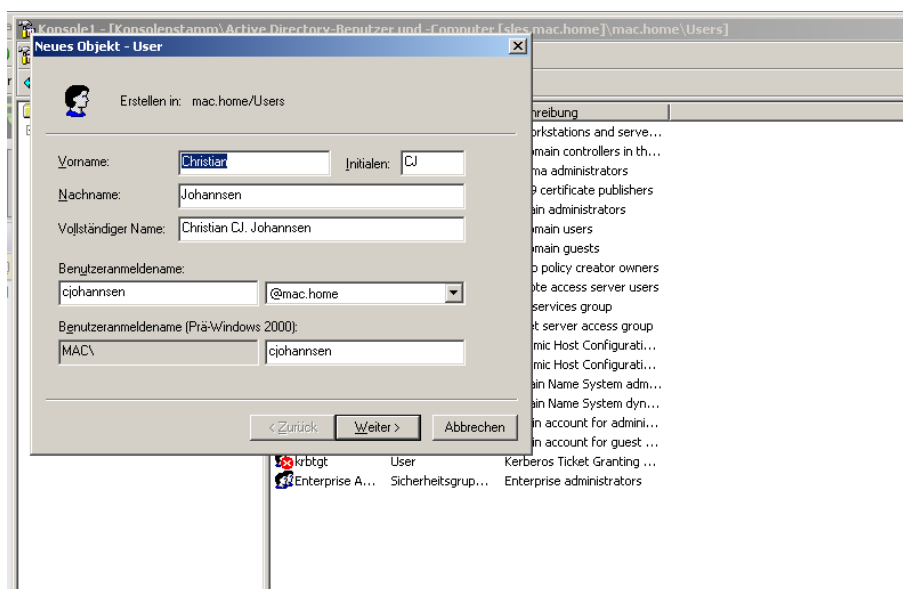


Abbildung 8 – MMC Administration

Der Vorteil in der MMC-Nutzung liegt in einer, für Windows-Administratoren und -Anwender bekannten Struktur und Optik. Über das Hinzufügen des Snap-Ins „Active Directory Benutzer und Computer“ kann die Administration gestartet werden. Mittels des Anlegen eines neuen Benutzers

per Wizard kann nun der entsprechende Nutzer angelegt werden. Es kann auch eine OU angelegt werden um eine Unterteilung zu ermöglichen.

3 VMware VIEW

Nachfolgend wird die Integration einer neuen VMware VIEW 4 Installation in die DSfW beschrieben. Nach der Integration des VIEW Manager Server in die DSfW können die Benutzer und Rollen genauso verwaltet werden wie in einer Active-Directory Umgebung. Lediglich die Authentifizierung des vCenter Server muss angepasst werden. Diese Beschreibung ist in Punkt 4 Troubleshooting näher erläutert.

3.1 Konfiguration des OS (VIEW Manager)

Der VMWare VIEW Manager basiert auf einem Microsoft Windows Betriebssystem der folgenden Varianten:

- Windows Server 2003 32bit R2 Standard Edition with SP2
- Windows Server 2003 32bit Standard Edition with SP2
- Windows Server 2003 32bit R2 Enterprise Edition with SP2
- Windows Server 2003 32bit Enterprise Edition with SP2

Um die Integration des VIEW Servers in die DSfW zu ermöglichen muss lediglich der DNS-Server auf den entsprechenden OES Server eingestellt sein. Am Besten kann eine Auflösung per Windows-Console und `nslookup` getestet werden. Für die Installation des VIEW Server ist später eine feste IP-Adresse notwendig, die hier schon eingesetzt werden kann.

Nach erfolgreichem Test der Namensauflösung kann das System wie gewohnt per Systemsteuerung der Domäne hinzugefügt werden. Als Name der Domäne reicht das NetBIOS Kürzel und der Administrator-Account. In einzelnen Fällen kann eine Schreibweise *Administrator@domänen.name* notwendig sein.

Nach erfolgreicher Aufnahme in die Domäne verhält sich das System wie in einer Windows-Active-Directory Umgebung.

Auszug auf `/var/log/messages` für eine erfolgreiche Domänen-Integration:

```
Feb  4 11:53:47 sles xadsd: [SECURITY] Impersonated user
MAC\Administrator
Feb  4 11:53:47 sles krb5kdc: [KDC] Regenerating authorization data for cross-
realm client Administrator@MAC.HOME
Feb  4 11:53:47 sles krb5kdc: [KDC] Regenerating authorization data for cross-
realm client Administrator@MAC.HOME
Feb  4 11:53:47 sles xadsd: [SECURITY] Impersonated user MAC\Administrator
Feb  4 11:53:47 sles xadsd: [SECURITY] Impersonated user MAC\Administrator
Feb  4 11:53:48 sles krb5kdc: [KDC] Regenerating authorization data for cross-
realm client Administrator@MAC.HOME
Feb  4 11:53:48 sles krb5kdc: [KDC] Regenerating authorization data for cross-
realm client Administrator@MAC.HOME
Feb  4 11:53:48 sles xadsd: [DRS] Bound NTDS API client
Feb  4 11:53:48 sles xadsd: [SECURITY] Impersonated user Administrator@MAC.HOME
```

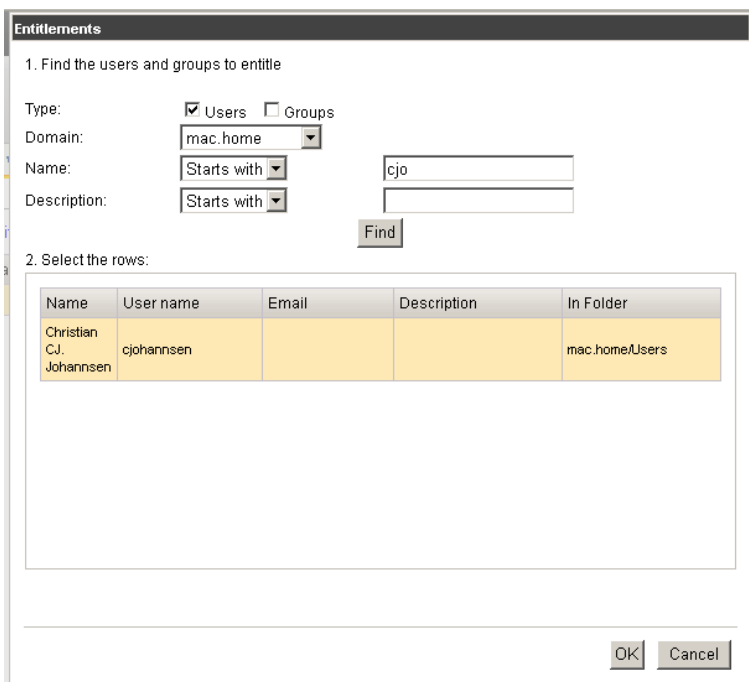
```
Feb  4 11:53:49 sles xadsd: [SECURITY] Impersonated user MAC\Administrator
Feb  4 11:53:56 sles xadsd: [NETLOGON] VIEW4$ opened secure channel
```

3.2 Konfiguration des OS (VIEW Agent)

Für die VMware VIEW Client-Systeme (Agent) gilt dasselbe Vorgehen zur Integration in die DSfW wie beim VIEW Manager Server. Auch hier wird das System in die Domäne per Windows-Administration integriert. Die Benutzer der Maschine werden dann per VIEW Manager definiert und freigeschaltet.

3.3 Konfiguration Benutzer

Nachdem der VIEW Server installiert wurde kann die Administration wie auch aus den Microsoft-A-D-Umgebungen bekannt erfolgen. Nachdem der vCenter Server integriert wurde können die entsprechenden virtuellen Maschinen ausgewählt und der Agent ausgerollt werden.



Name	User name	Email	Description	In Folder
Christian C.J. Johannsen	cjohannsen			mac.home/Users

Die entsprechenden Benutzer werden dann den virtuellen Maschinen zugeordnet und mit dem entsprechenden Domänen-Namen angezeigt.

4 Troubleshooting

Teilweise kommt es auch bei einer DSfW Installation und VIEW Integration zu Problemen die manuell gelöst werden müssen. Nachfolgend werden die bekanntesten beschrieben, zum Einen bei der Integration in die Domäne, zum Anderen die Initialisierung des Administrator-Account und die Authentifizierung des vCenter Server an den DSfW.

4.1 Domänen-Integration

Bei der Installation und Konfiguration der DSfW Erweiterung kam es vereinzelt zu Kerberos Problemen, da die Clients in der neuen Domäne mit dem Administrator-Account nicht berechtigt waren:

```
xadsd: [SAMSS] SampCreateUserInDomain: failed to create machine account
'VIEW4' in domain <dc=mac,dc=home>: Insufficient access
```

Dieses Problem lies sich mit einem Anpassen der Rechte und der Gruppenzugehörigkeit auf und einem zusätzlichen Link auf die Kerberos Datenbank lösen. Generell können solche Probleme auch auf dem Client-System in dessen `\Windows\Debug\NetSetup.log` geprüft werden.

```
chmod 640 /var/opt/novell/xad/ds/krb5kdc/krb5.keytab
chgrp named /var/opt/novell/xad/ds/krb5kdc/krb5.keytab
ln -sf /var/opt/novell/xad/ds/krb5kdc/krb5.keytab /etc
```

Nachdem diese Änderungen durchgeführt wurden sollte die Anmeldung erfolgen können.

```
Feb 4 11:53:48 sles krb5kdc: [KDC] Regenerating authorization data for
cross-realm client Administrator@MAC.HOME
Feb 4 11:53:48 sles xadsd: [DRS] Bound NTDS API client
Feb 4 11:53:48 sles xadsd: [SECURITY] Impersonated user
Administrator@MAC.HOME
Feb 4 11:53:49 sles xadsd: [SECURITY] Impersonated user MAC\Administrator
Feb 4 11:53:56 sles xadsd: [NETLOGON] VIEW4$ opened secure channel
```

Weitere Informationen bei Problemen können aus den Standard-logfiles sowie aus den in der `/etc/krb5.conf` hinterlegten Lokationen entnommen werden.

4.2 Administrator-Account

Wenn der Administrator-Account nicht akzeptiert wird bzw. im logfile Probleme auftauchen, kann dessen ordnungsgemäße Anlage und Funktion auf dem OES geprüft werden.

Zuerst kann der Administrator-Account initialisiert mittels `kinit Administrator` und nachfolgend kann dessen Rolle geprüft mit `klist` geprüft werden. Bei ordnungsgemäßer Funktion sollte folgendes Ergebnis zu sehen sein:

```
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: Administrator@MAC.HOME

Valid starting      Expires            Service principal
02/23/10 16:56:40  02/24/10 02:56:40  krbtgt/MAC.HOME@MAC.HOME
        renew until 02/24/10 16:56:37
```

Generell stehen verschiedene logfiles zur Verfügung die eine genauere Sichtung bei Problemen erlauben. Ein Großteil sind in der `/etc/krb5.conf` definiert:

```
[logging]
kdc = FILE:/var/opt/novell/xad/log/kdc.log
admin_server = FILE:/var/opt/novell/xad/log/adm.log
kpasswd = FILE:/var/opt/novell/xad/log/kpasswd.log
kcm = FILE:/var/opt/novell/xad/log/kcm.log
```

Zusätzlich kann `/var/log/messages` eine schnelle Sicht auf die Probleme erlauben.

4.3 vCenter Authentifizierung

Beim Zusammenspiel zwischen vCenter Server und DSfW kann es zu einem Problem bei der Kerberos-Authentifizierung kommen. Novell hat für diesen Fall einen eigenen KB-Artikel (7004209) veröffentlicht.

Der VMware vCenter Server verlangt ein Kerberos Ticket für den Service Principal Namen: "ldap/<ip address of DSfW DC>". Sollte keine korrekte SPN Authentifizierung übermittelt werden scheitert die Authentifizierung.

Um einen entsprechenden SPN anzulegen ist folgender Workaround hilfreich:

1. Editieren Sie das Domain Controller Objekt mittels iManager oder ConsoleOne.
2. Das DC Objekt ist der Name des DSfW Server befindet sich in "ou=domain controllers,<dc=...>".
3. Gehen Sie auf den „Other“ Reiter und editieren Sie das servicePrincipalName Attribut.
4. Ergänzen Sie das ldap/<ipaddress> Attribut im servicePrincipalName Attribut.
5. Starten Sie DSfW Services erneut mittels "xadcctrl reload"

Nachfolgend sollte die Authentifizierung des vCenter Server an den DSfW funktionieren und der vCenter Server kann in den VIEW Manager integriert werden.

5 Quellen und Nachweise

Novell OES 2 SP2 Installation:

<http://www.novell.com/documentation/oes2/>

Novell DSfW 1.0 Installation Guide:

http://www.novell.com/documentation/oes2/acc_dsfw_lx/data/bookinfo.html#bookinfo

vCenter Server cannot authenticate (KB 7004209):

<http://www.novell.com/support/viewContent.do?externalId=7004290&slicId=1>

Cannot connect DC after upgrade OES (KB 7004976):

<http://www.novell.com/support/viewContent.do?externalId=7004976&slicId=1>

VIEW Community Artikel:

<http://www.thatsmyview.net/>

Vmware VIEW Reference Architecture:

<http://www.vmware.com/files/pdf/resources/vmware-view-reference-architecture.pdf>

6 Begriffe und Abkürzungen

OES	Open Enterprise Server (Novell)
SLES	SuSe Linux Enterprise Server (Linux Betriebssystem)
AD	Active-Directory (Microsoft Verzeichnisdienst)
DSfW	Domain Service for Windows
KDC	Kerberos Distribution Center
NMAS	Novell Modular Authentication Service
NTP	Network Time Protocol
CIFS	Common Internet File System
DNS	Domain Name Service
ADPH	Active-Directory Provisioning Handler
DIB	Directory Information Database
MMC	Microsoft Management Console
OU	Organizational Unit
SLP	Service Location Protocol
SPN	Service Principal Name