Ton Werner is werkzaam als trainer bij Info Support.

Services for UNIX 3.5

INTEGRATIE TUSSEN DE WINDOWS- EN UNIX-OMGEVING

Dit artikel bevat een globaal overzicht van de mogelijkheden van Windows Services for UNIX (SFU) 3.5 inzake de gehele of gedeeltelijke centralisatie van authenticatie en autorisatie van gebruikers. Ook worden aanwijzingen gegeven om de beschreven configuratie - centraal beheer van authenticatie en autorisatie van de gebruikers - snel aan de praat te krijgen. Verderop in dit blad beschrijft Erno de Weerd de development-aspecten van Services for Unix. In dit artikel beperkt de auteur zich tot de infrastructuur.

In 1999 introduceerde Microsoft de eerste versie van *Windows Services For UNIX*. SFU 1.0 was samengesteld uit verschillende producten, die alle waren gericht op de integratie tussen Windows- en Unix-omgevingen. Met ingang van versie 3.0, die uitkwam in 2002, is de utility- en shell-emulatielaag uit de vorige versies vervangen door Interix- technologie. Interix is te beschouwen als een native subsystem waarbinnen Unix-applicaties gecompileerd en uitgevoerd kunnen worden op Windows 2000, Windows Server 2003 en Windows XP-platforms.

Momenteel is SFU 3.5 de actuele versie van Windows Services for UNIX. SFU 3.5 kan worden gezien als een uitgebreide en geïntegreerde toolset, die kan worden gebruikt om een Unix-omgeving te creëren op een Windows- platform. SFU3.5 is geen Unix-emulatie of een Unix-lookalike, maar een volwaardige Unix-omgeving. Daarmee is het momenteel dé - gratis beschikbare - tool om Unix-omgevingen te integreren in de nix/Linux-platform kunnen samenwerken. In dit artikel is de term Unix te lezen als Unix/Linux.

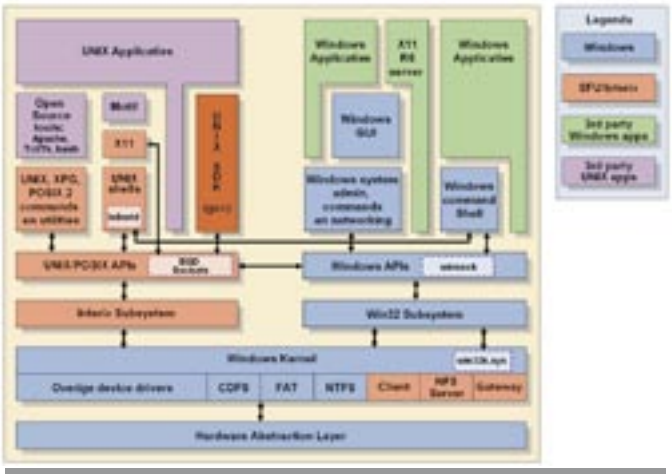
Natuurlijk is het leuk voor de Unix-adept om nu zijn *KornShell-scripts*, zijn *Perl-scripts* en tools als *grep* en *awk* te laten werken op een Windows-platform. Hij zal het heerlijk vinden om met zijn geliefde *vi* notepad-bestanden te editen. Een bestaansrecht van SFU 3.5 is de migratie van Unix-applicaties naar het Windows-platform. Dit artikel gaat echter in op de beheeraspecten inzake de integratie tussen Windows- en Unix-omgevingen en zal zich met name richten op authenticatie en autorisatie van de gebruikers.

In dit artikel geef ik een globaal overzicht gegeven van de mogelijkheden van SFU 3.5 inzake de gehele of gedeeltelijke centralisatie van authenticatie en autorisatie van gebruikers en geef ik aanwijzingen om de beschreven configuratie - het centraal beheer van authenticatie en autorisatie van de gebruikers - snel aan de praat te krijgen. In dit artikel ga ik niet in op allerlei security-gerelateerde aspecten van mogelijke configuraties. In feite is de hieronder beschreven configuratie als niet veilig te beschouwen. Gezien de in Windows geïmplementeerde standaarden inzake SSL, PKI, Kerberos, HTTPS en dergelijke is een goede beveiliging zeer wel mogelijk; alleen valt dit buiten de scope van dit artikel. Aan het eind van het artikel verwijs ik naar enkele documenten die de beveiliging van mogelijke configuraties als onderwerp hebben.

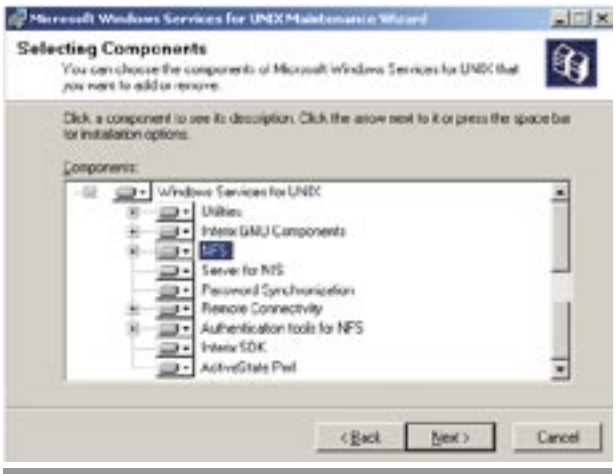
In het kader van dit artikel onderken ik drie vormen van integratie, waarvan de laatste mogelijkheid als voorbeeld wordt genomen.

1. **Beheer van het Windows– en Unix-platform is gescheiden.** De omgevingen zijn gekoppeld, maar autorisatie en authenticatie van gebruikers zijn per platform gescheiden. Gemeenschappelijke bestanden zijn vanuit beide omgevingen te benaderen. SFU 3.5 kan worden ingeschakeld om gebruik te maken van *NFS*.

2. **Beheer van het Windows- en Unix-platform is geïntegreerd.** Authenticatie is gescheiden per platform, autorisatie is geïntegreerd. Gemeenschappelijke bestanden zijn vanuit beide omgevin-



Afbeelding 1. Positionering Interix



Afbeelding 2. SFU 3.5 installatie

Afbeelding 3. SFU 3.5 admin console

Afbeelding 4. SFU 3.5 NIS-server

gen te benaderen. SFU 3.5 kan worden ingeschakeld om gebruik te maken van *NFS*, *UserName Mapping* en *Password Synchronisatie*.

3. Beheer van het Windows- en Unix platform is gecentraliseerd.
Authenticatie vindt plaats op het Windows-platform. Autorisatie is transparant en bestanden zijn gemeenschappelijk te benaderen. SFU 3.5 kan worden ingeschakeld om gebruik te maken van *NFS*, *NIS, User Name Mapping en Password Synchronisatie*.

Installatie SFU3.5

SFU 3.5 kan met 'Add or Remove Programs' worden geïnstalleerd, waarbij de diverse onderdelen al dan niet kunnen worden geselecteerd. Zie afbeelding 2. Er is de keuze uit de volgende onderdelen:
- Utilities
Hieronder vallen tal van Unix-utilities waaronder natuurlijk de KornShell, grep, awk, vi, sed en niet te vergeten Perl.
- Interix GNU Components
Deze componenten bevatten Interix GNU-utilities en de Interix GNU SDK met gcc, g++ compilers. Interix heeft een uitgebreide en goed onderhouden toolset.
- NFS
NFS server, client en gateway. NFS-gateway beheert de NFS-mounts en stelt ze beschikbaar aan Windows-clients. Installatie van de NFS-client op de Windows-machines is dan niet nodig.
- *Password-synchronisatie*
Synchronisatie van wachtwoorden tussen Unix en Windows. Bi-directional voor zowel local als domain-accounts.
- *Server for NIS*
Centraal beheer van netwerkobjecten.
- *Remote Connectivity*
Remote Shell-service (de remote r-commands)
- *Authentication Tools for NFS*
De User Name Mapping server, de server for NFS Authentication en de PCNFS-server
- *Interix SDK*
Compilers, yacc, cc en X11R5- en X11R6-libraries. Echter geen Xserver.
- *Active State Perl*
De standaard Perl-distributie voor Linux, Solaris en Windows.

SFU 3.5 beheerinterface

Na installatie van SFU 3.5 kunnen de diverse onderdelen worden geconfigureerd met een Microsoft Management Console, de *SFU3.5 admin console*; zie afbeelding 3.

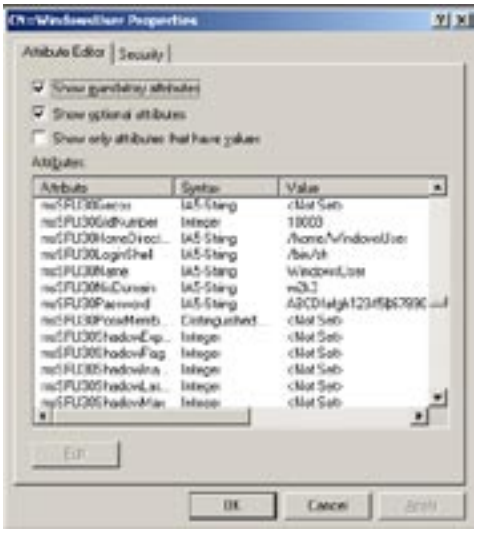
Alle onderdelen zoals *NFS*, *NIS*, *Telnet Server* en de *User Name Mapping Server* kunnen al dan niet apart worden ingezet om een zekere mate van integratie te bewerkstelligen. In dit artikel beperk ik mij tot de meest integrale oplossing, namelijk die van centraal beheer van authenticatie en autorisatie, waarbij *Active Directory*, *NIS, NFS* en de *User Name Mapping server* samenwerken. In dit voorbeeld is gekozen voor een Windows Server 2003 Enterprise Edition aan de ene kant en een Linux Fedora Core 1 machine aan de andere kant.
Eerst komt de NIS-configuratie aan de orde en de integratie van deze server in Active Directory, waarbij ook de configuratie van NIS aan de Linux-kant wordt behandeld. Daarna is het de beurt aan NFS. We mounten een in Windows geëxporteerde folder vanaf het Linux systeem, completeren de configuratie met de User Name Mapping server en controleren de eigenschappen van een (geïntegreerde) gebruiker aan de hand van zijn gebruikersidentificatie en de permissies op de door de gebruiker aangemaakte bestanden in de Windows- en de Unix-omgeving.

Network Information System (NIS)

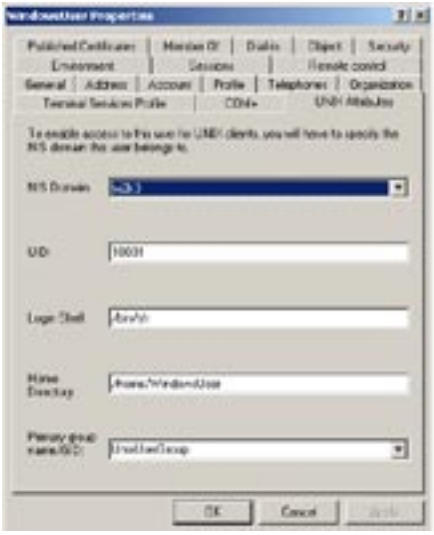
NIS is voor het gemak te beschouwen als een Active Directory 'avant la lettre'. Informatie over netwerkobjecten wordt centraal op een server in zogenaamde *NIS-maps* opgeslagen. Deze maps bevatten configuratie-informatie over gebruikers, groepen, printers, wachtwoorden, protocollen en dergelijke. Iedere map bevat informatie over een specifiek netwerkobject. Er kunnen in een NIS-domein meer NIS-servers aanwezig zijn, die in een master–slave configuratie de informatie over de netwerkobjecten repliceren. Clients kunnen informatie aangaande de netwerkobjecten aanvragen bij de NIS-servers; zie afbeelding 4.

De configuratie-instellingen van de SFU 3.5 NIS-server zijn met name gericht op de inpassing van deze NIS-server in een NIS-domein, waarin meer NIS-slave-servers zijn opgenomen. De SFU 3.5 NIS-server functioneert dan als een master-server. Om NIS voor onze doeleinden geschikt te maken is het voldoende om het Windows-domein te benoemen. De NIS-server dient overigens op een Domein Controller te worden geïnstalleerd vanwege de integratie van NIS met Active Directory.

Door installatie van SFU 3.5 wordt het *Active Directory Schema* uitgebreid met tal van msSFU-attributen. Zie afbeelding 5. In tegenstelling tot de Unix-georiënteerde NIS-servers kent de SFU 3.5 NIS-server geen centrale maps. In Active Directory worden geen NIS-maps gegenereerd, maar liggen de van belang zijnde attributen als het ware verspreid over de relevante objecten in het *Active Directory Schema*. Zo worden bij installatie de attributen van de domeingebruikers uitgebreid met enkele NIS-attributen. Dit is van belang, omdat deze attributen ook via LDAP-tools zijn te benaderen. Het is mogelijk de NIS-server niet te activeren en toch via eigen tooling gebruik te maken van de NIS-attributen. Is de NIS-server wel actief, dan betekent dit dat we beschikken over een centraal instrument - geïntegreerd in Active Directory - om gebruikers te authenticeren. Gebrui-



Afbeelding 5. msSFU-attributen



Afbeelding 6. Unix-attributen

Afbeelding 7. NIS-configuratie Fedora

kersinformatie en wachtwoorden worden centraal en op een veilige manier opgeslagen. Een bijkomend voordeel is dat ook het beleid rond wachtwoorden met Group Policy centraal kan worden geregeld. Aangezien Unix-platformen Kerberos ondersteunen, kan Kerberos volledig worden gebruikt.

Na authenticatie krijgen de gebruikers via Active Directory en NIS de *AccessTokens* die voor de desbetreffende omgeving gelden teneinde zich te kunnen autoriseren. Met andere woorden: in de Unix-omgeving dient een gebruiker in het bezit te zijn van een UserID en een GroupID; in de Windows-omgeving dient een gebruiker in het bezit te zijn van een SecurityID, en de SecurityID's van de security-groepen waarvan de gebruiker lid is. Met deze zaken kan een gebruiker zich in de desbetreffende omgeving identificeren en zich autoriseren. Een Domain Controller genereert automatisch SecurityID's indien een gebruiker wordt aangemaakt. Hierna moeten UserID's en GroupID's worden toegekend. Door installatie van NIS is er de mogelijkheid bijgekomen om per gebruiker de voor de Unix-omgeving vereiste gebruikersidentificaties te specificeren.
De gebruikerskenmerken in de Unix-omgeving bevatten naast de LoginShell en de HomeDirectory ook de Primary Group. Zie afbeelding 6. Dit is de groep die men bij het inloggen in een Unix-omgeving automatisch krijgt toegewezen. Om een gebruiker lid te maken van zo'n Unix-groep moet deze eerst aangemaakt zijn in de Windows-omgeving en zijn voorzien van de betreffende NIS-eigenschappen, te weten het NIS-domain van de groep en de GroupID van de groep.

Als Unix-omgeving is een Fedora Core 1 machine uitgekozen. Overigens lopen alle hier beschreven machines als vpc-image binnen Microsofts' VPC2004. In de autorisatiemodule op de Unix-machine is aangegeven dat NIS moet worden gebruikt voor authenticatie en zijn de relevante parameters ingebracht, te weten de naam van het NIS-domain en de Domeinnaam (FQDN) van de NIS-server. Zowel bij gebruikersinformatie als authenticatie kunnen meer zaken worden ingesteld, maar in dit artikel beperk ik me tot een minimale configuratie. Verder is pre-authentication uitgeschakeld bij de gebruikerseigenschappen van de domeingebruiker. Zie afbeelding 7. Het is een goed idee om op de Unix-machine de Domain Controller als Time Server in te stellen; bij gebruik van Kerberos is dit een noodzakelijke voorwaarde. In SFU 3.0 diende de DES-wachtwoordenoptie nog te worden ingeschakeld. Bij SFU 3.5 is dit niet meer nodig. Is de NIS-client op de Unix-machine correct ingesteld, dan kan men inloggen op de Unix-machine. Authenticatie zal dan verlopen via de met Active Directory geïntegreerde NIS-server.

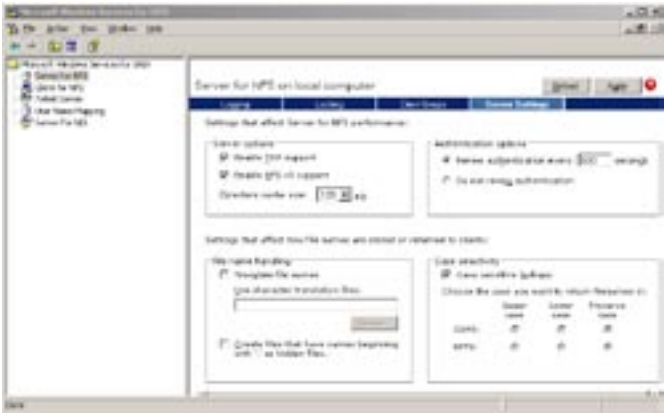
Het resultaat is nu dat in de Windows-omgeving het wachtwoord is geverifieerd en de gebruiker – in dit voorbeeld Fedorauser - de bij hem behorende SecurityID's heeft verkregen. Zie afbeelding 8. In de Unix-omgeving heeft de ingelogde gebruiker een UserID en een GroupID - noodzakelijke attributen voor de identificatie - verkregen. In het begin is het raadzaam om in de Unix-omgeving eerst de gebruikersomgeving aan te maken en daarna de gebruiker weer te verwijderen, omdat een Unix-login een gebruikersomgeving verwacht. Via scripting kunnen later nieuwe gebruikersomgevingen automatisch worden aangemaakt, indien men de gebruiker binnen Active Directory initialiseert.

Een voordeel dat niet is te veronachtzamen, is dat de wachtwoorden van de geïntegreerde Unix-gebruikers onder het wachtwoordbeleid vallen zoals in Active Directory is gespecificeerd. Hierbij moet overigens in de gaten worden gehouden dat synchronisatie van ActiveDirectory naar NIS automatisch gaat, maar dat synchronisatie van de wachtwoorden in een omgekeerde richting niet vanzelfsprekend is. Als aan de Unix-kant *yppasswd* wordt gebruikt om het wachtwoord van de Unix-gebruiker te wijzigen, wordt dit wel correct opgeslagen in de NIS-map, maar dient men nog altijd met het vorige wachtwoord in te loggen in de Windows-omgeving, omdat synchronisatie niet heeft plaatsgevonden. Het is dan ook raadzaam om de Windows-omgeving inzake het gebruikersbeheer als beheerplatform aan te wijzen.

Network File System (NFS)

NFS is een gedistribueerd filesysteem; bestanden kunnen platformonafhankelijk over het netwerk worden gedeeld. Een NFS-server deelt zijn filesysteem of directory met NFS- clients. De NFS-client 'mount' de op de server beschikbare structuur en ziet deze structuur als onderdeel van zijn lokale filesysteem.
Zoals we hierboven hebben gezien, is het mogelijk de authenticatie van gebruikers in een Windows- en Unix-omgeving met ActiveDirectory te centraliseren. Nogmaals merk ik op dat bovengenoemde configuratie minimaal is. De bedoeling van deze configuratie is om te laten zien dat - out of the box - de implementatie weinig of geen moeite kost. Ook het inschakelen van Kerberos (waarbij de

Afbeelding 8. Fedorauser ID



Afbeelding 9. SFU 3.5 NFS

Afbeelding 10. UserNameMapping 2

pam-kerb5 PAM-module van belang is aan de Unix-kant) levert in het algemeen vrij weinig problemen op. De implementatie van een veilige omgeving, waarin allerlei security-zaken moeten worden geïntroduceerd, is wel wat veeleisender. Ook geldt dat hoe complexer de gewenste configuratie is, de implementatie van SFU 3.5 ook complexer is.

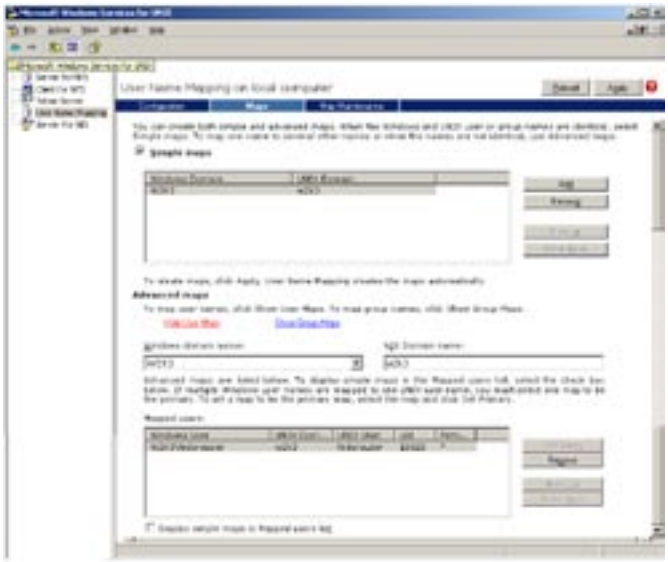
Nadat de gebruiker is geauthenticeerd, dient deze vanaf de Unix-omgeving toegang te krijgen tot resources in de Windows-omgeving op basis van verkregen AccesTokens. Met andere woorden: de Unix-identificatie moet worden vertaald naar de Windows-identificatie. Op basis van deze identificatie krijgt de gebruiker permissie om al dan niet met de resources om te gaan. Om dit op een eenvoudige manier te realiseren moet de NFS Server, de NFS Authorisation Server en de User Named Mapping Server worden geïnstalleerd en geconfigureerd. Zie afbeelding 9.

In de configuratie van de NFS-server kunnen we de logfile specificeren, client-locks vrijgeven, client-groups definiëren en de serverinstellingen inzake transportprotocol, filename translations, case-sensitivity en authentication-renewal specificeren. Bij de eigenschappen van Windows Services for Unix moet de User Name Mapping Server gericht zijn op 'localhost'. Zie afbeelding 10.

Bij de configuratie van de User Name Mapping moeten we aangeven dat de NIS-server wordt gebruikt. Onder de tab *Maps* kunnen simple maps en advanced maps worden gespecificeerd, zowel op gebruikers- als groepsniveau. Simple maps geven de koppelingen weer tussen de Windows- en Unix-gebruikers, waarbij de namen in de diverse omgevingen dezelfde zijn. Zijn de namen verschillend of wil men meer gebruikers op één groep 'mappen', dan kan van advanced maps gebruik worden gemaakt.

De gebruiker in afbeelding 11 genaamd 'Fedorauser' is lid van de groep UnixUsers. Om ook groepen te 'mappen' is een *Global Security Group* UnixUsers aangemaakt die 'gemapt' is op de groep UnixUsers.

Door de NFS-server te installeren in SFU 3.5 is het op een zeer simpele manier mogelijk geworden een NTFS-folder als NFS-export te definiëren. *Allow Anonymous Access* wordt uitgevinkt en de permissies worden gezet op ALL_MACHINES read-write. *Root-access* is niet toegestaan.



Afbeelding 11. User Name Mapping 1

In de security-tab van de NFS-share wordt de gebruiker Fedorauser alle rechten gegeven. Hierna moeten de User Name Mapping server en de NFS-server worden gestopt en gestart. De NFS-share is nu ingericht zodat de gebruiker Fedorauser deze kan benaderen van de Unix-kant. Aan de Unix-kant moeten we ook enkele zaken regelen. Hier behoort de NFS-share te worden 'gemount' en moet de gebruiker Fedorauser inloggen en naar de NFS-share gaan. De 'root'-gebruiker moet 'mounten' met het commando *mount –t nfs w2k3server:/NFSShareOpW2K3 /mnt/nfs*. In de Windows-omgeving is een Windows-folder aangemaakt, met daarin de bestanden wordpad.doc en notepad.txt.

In de Unix-omgeving is hetzelfde gedaan. Het resultaat is dat er enkele verschillen bestaan tussen de directories/bestanden. Het verschil in permissies wordt veroorzaakt doordat in de Unix-omgeving de *umask* op 022 is ingesteld. Wordt de *umask* op 000 gezet, dan komen de permissies met elkaar overeen. De niet benoemde groep kan worden vervangen door de juiste Unixgroep met het *chgrp*-commando.

Eenvoud

Al met al is de out-of-the-box-installatie van de NFS-server en de integratie van NIS in Active Directory, samen met het activeren van de User Name Mapping server en enkele simpele configuratie-instellingen, voldoende om een platform te creëren voor centraal beheer van gebruikers inzake authenticatie en autorisatie.

Ton Werner
is werkzaam als trainer bij Info Support. Zijn e-mailadres is tonw@infosupport.com

Nuttige internetadressen

White papers, artikelen, nieuwsgroepen en de laatste informatie inzake SFU 3.5 kan worden gevonden op http://www.microsoft.com/windows/sfu
Solutions Guide for Windows Security on Directory Services for Unix: http://www.microsoft.com/technet/itsolutions/migration/unix/usecdirw/default.mspx
Windows & Unix Interoperability door Martin Poulin (GIAC Certified Windows -Security Administrator– Practical Assignment, Version 3,2 Option 2): http://www.giac.org/practical/GCWN/Martin_Poulin_GCWN.pdf
Replacing NIS with Kerberos & LDAP: http://www.ofb.net/~jheiss/krbldap/howto.html
Step-by-step Guide to Kerberos Interoperability: www.microsoft.com/windows2000/techinfo/planning/security/kerbsteps.asp
Centralized User Management with Kerberos and LDAP: http://itso.vit.edu./~travis/kerberos
Migrating UNIX Applications to Windows: http://www.microsoft.com/technet/itsolutions/interop/sfu/migun2wi.mspx