Självständigt arbete (examensarbete), 9 hp för högskoleexamen med inriktning informationsteknologi
VT 2016

Linux i Micosoft AD-miljö

Ola Ettorsson
Tomas Nilsson

Sektionen för hälsa och samhälle

Högskolan Kristianstad | www.hkr.se

Författare
Ola Ettorsson
Tomas Nilsson

Titel
Linux i Windows AD-miljö

Handledare
Martin Nilsson, teknisk utbildare, HKR

Examinator
Fredrik Jönsson, universitetslektor i datavetenskap och teknik, HKR

Sammanfattning

Examensarbetet handlar om hur man kan integrera Linux i en Microsoft AD-miljö. De delar som har tagits upp är om det går att logga in från en Linux klient mot en Microsoft AD-miljö. Arbetet omfattar även hur det går att använda en Linux server för att kunna sätta upp en katalogtjänst liknande Microsoft AD. Tjänsterna som har inkluderats är de grundläggande tjänsterna så som inloggning och behörigheter gällande fildelning.

Ämnesord

Samba, Kerberos, Winbind, Linux Powerbroker, Windows, Microsoft, AD

Sammanfattning

Examensarbetet är en undersökning på hur det går att integrera Linux i en Microsoft AD-miljö. Detta genom att gå igenom de nödvändiga delarna för en lyckad autentisering. Arbetet tittar även på vissa skillnader mellan en Microsoft AD-miljö och en Samba AD-miljö vilket kan göra integreringen genomförbar eller inte. Undersökningen har gjorts med att ha Linux som klient mot en Microsoft AD-miljö men även att ha en Windows klient mot en Linux server installerad med Samba och dess AD-struktur. Tjänsterna som har inkluderats är de grundläggande tjänsterna så som inloggning och behörigheter gällande fildelning.

Innehållsförteckning

1 Introduktion

1.1 Bakgrund

Intresset för Linux har ökat men användningen av Linux ligger på en ganska stabil låg nivå jämfört med Windows höga nivå. Orsaken till att Linux inte ökar i användning skulle kunna bero på att en integration inte är möjlig eller att det tidigare har varit svår att göra. Anledningen till examensarbetet är att undersöka svårighetsgraden att integrera en dator med Linux i en Microsoft Active Directory miljö (Microsoft AD-miljö). Resultatet i detta arbete kan resultera till ett ökat användningsområde för Linux i en Microsoft AD-miljö.

1.2 Målsättning och syfte

Examensarbetets syfte är att ta reda om det är tekniskt möjligt att integrera en dator med Linux i en Windowsdomän. Det gäller både Linux som klient mot en Windowsserver och Windowsklient mot en Linuxserver. Målet med att försöka integrera Linux, är att Linux är fritt och anpassningsbart. Dessutom är de flesta distributioner fria att ladda ner, använda och modifiera efter behov.

1.3 Metodik

Information och guider har inhämtas på Internet för att hitta lösningar för att integrera de olika miljöerna. Lösningarna har sedan testats genom laborationer för att se hur lätt eller svårt det vara att få de olika miljöerna att samarbeta. När det har blivit fel under laborationerna har felsökning gjorts med hjälp av information som inhämtats från Internet.

1.4 Avgränsningar

I en Microsoft AD-miljö finns det väldigt många funktioner så vi har valt att avgränsa oss för att få ett genomförbart examensarbete. Vi valt att använda oss av operativsystemen Windows Server 2012 R2, Ubuntu 14.04 Desktop, Ubuntu 14.04 Server och Zentyal Server 4.2 Development Edition. Det vi har valt att titta på är möjligheten för en klient att kunna logga in mot en AD-server eller AD-liknande server. Med kriterierna att det ska fungera med ”Single Sign-On”[1] mot en filserver och att filbehörighet på utdelade filer och kataloger ska fungera. Valet av linuxdistribution föll på Ubuntu eftersom den är en av de mest populära distributionerna enligt websidan Distrowatch. [1]

[1] Single Sign-On innebär att enbart en inloggning för att komma åt flera system.

2 Utredning

2.1 Samba historik

När det var nytt med Personal Computer (PC) utvecklade IBM och Sytec gemensamt ett enkelt nätverkssystem designat för att bygga lokala nätverk (såkallade LAN, Local Area Network). I systemet fanns det något som kallades NetBIOS (Network Basic Input Output System) [2]. NetBIOS utgjordes av många program som laddades upp till minnet för att ge ett gränssnitt mellan mjukvaran och nätverksprogrammen. Arbetsstationerna och aktiva applikationer på nätverket identifierades med 16 bytes adresser. Microsoft utökade funktionerna i Disk Operating System (DOS) som tillät Input/Output (I/O) till och från disk att bli omdirigerade till NETBIOS i gränssnittet, vilket gjorde att diskutrymmet blev delbart på ett LAN. Fildelningsprotokollet som användes var Server Message Block (SMB) [2]. Nu används Common Internet File System (CIFS) som är publikt eller öppen variant på SMB protokollet [3].

Under tiden som NETBIOS utvecklades hade Andrew Tridgell ett problem, han behövde montera diskutrymme från en Unix server på hans DOS PC. Det var inget problem för han hade en NFS klient för DOS, problemet var att han även hade applikationer som krävde NetBIOS gränssnitt. Multipla protokoll under DOS kan vara problematiskt. Andrews lösning var att skriva en paketsniffare för att kunna dekonstruera SMB protokollet och implementera det på en Unix maskin. Unix systemet uppfattades då som en PC filserver, som tillät honom montera delade filsystem från Unix servern och samtidigt som ha möjlighet att köra NETBIOS applikationer. Tridgell publicerade koden 1992, under en begränsad tid gjorde han även buggfixar innan ha la projektet åt sidan. Två senare ville han länka sitt linuxsystem med fruns Windows PC, han plockade då fram sin kod till paketsniffaren[2] och blev överraskad att det fungerade.
Genom sina e-postkontakter upptäckte han att NetBIOS och SMB var dokumenterade även om det var marginellt. Då kom nästa problem nämligen att ett företag hade varumärkesrättigheterna till SMB som han ville använda på serverprogrammet han hade kod till sedan tidigare.
Han gjorde då en sökning i en ordlista på ord som innehöll bokstäverna s, m och b. Samba fanns med på listan och han valde då detta. [2].

[2] Ett program för att undersöka vilka paket som skickas runt i nätverket.

2.1.1 Kommunikation mellan server och klient

För att en kommunikation ska kunna ske mellan domänkontrollant och klienter används fram för allt tre olika protokoll. Dessa är Kerberos, LDAP och SMB. Kerberos används för säker autentisering mellan nätverkstjänster över obetrodda nätverksanslutningar. LDAP är till för att hitta användare och gruppinformation på domänkontrollanten. För att de olika datorerna ska kunna skicka dela med sig av olika resurser så som skrivare och filer används även SMB.

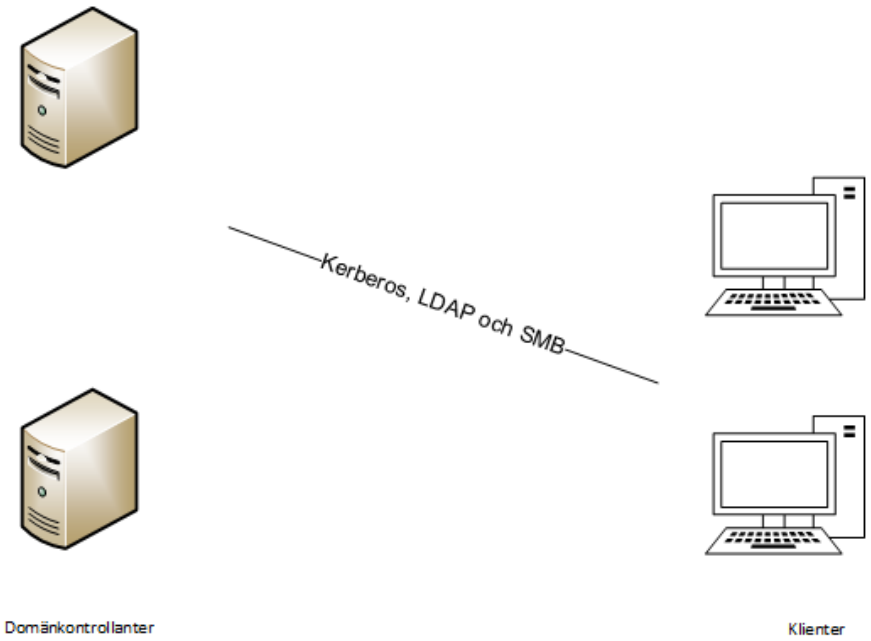

Bild 1 Översiktsbild hur kommunikationen mellan server och klient sker

2.1.2 Samba

Det är viktigt att kontrollera vilken Kerberos[3] som en linuxdistribution använder eftersom det finns två versioner. Dessa är MIT Kerberos och Heimdal och de använder sig av olika tekniker för att kommunicera. Alla distributioner kommer inte med stöd för domänkontrollanter[4]. Heimdal är den variant av Kerberos som finns med i Samba.

Samba stödjer inte Open Lightweight Access Protocol (OpenLDAP) eller andra LDAP servrar utan levereras med en egen implementering LDAP.

[3] Kerberos är ett protokoll för att tillåta autentisering till nätverkstjänster över osäkra kommunikationskanaler. Detta genom användning av säkra nycklar och betrodd tredje part.
[4] Domänkontrollant är den som har behörighet att göra ändringar i AD.

Samba AD domain controller (DC) och på svenska domänkontrollant kräver minst version 4.0.0 av Samba, det är rekommenderat av utvecklarna [4] att använda den senaste versionen. Det är viktigt att välja rätt NetBIOS-namn och Domain Name Service (DNS) -namn från början eftersom Samba inte stödjer modifiering av namnen i efterhand.
Det behövs ingen installation eller konfiguration av Kerberos Key Distribution Center (KDC) för att få Samba att fungera, i Samba finns det en kompatibel KDC med AD [5].

Samba består av två huvudprogram och dom är *smbd(Samba deamon[5])* och *nmbd(NetBIOS deamon)*. Dom implementerar de fyra basala moderna funktionerna:

- Fil och skrivartjänster
- autentisering[6] och auktorisation[7]
- namnuppslag
- tjänstmeddelanden(browsing).

Fil och skrivtjänsterna är hörnstenen i CIFS (Common Internet File System) sviten. Dom tillhandahålls av smbd. Smbd hanterar också "share mode"[8] och "user mode"[9] autentisering och auktorisation. Detta för att kunna skydda fil och skrivtjänster genom att kräva lösenord.

2.1.3 Pluggable Authentication Modules (PAM)

PAM är ett lager som finns på Linux och Unix liknade operativsystem som används till att möjliggöra autentisering mellan olika tjänster. [6]

Det enklaste sättet att använda ett AD till autentisering är att konfigurera PAM att använda LDAP, denna metod kallas LDAP bindning. Metoden är inte säker eftersom användarnamn och lösenord skickas i klartext över nätverket.

Det enda sättet att minska risken att överföra användaruppgifter öppet är att kryptera klient-AD kommunikationskanalen genom att använda t ex Secure Socket Layer (SSL). Det är möjligt att göra det, dock blir det ett extra arbete [7] att underhålla SSL certifikaten både på DC och linuxdatorn.

[5] Daemon är Linux svar på tjänst inom Microsoft Windows.
[6] När identitet kan visas t ex id-kort.
[7] Någon har fått tillträde.
[8] Share mode innebär att användare behöver autentiseras mot varje utdelning.
[9] User mode innebär att användaren authentiseras mot en server och får sedan tillgång till alla utdelning som användare har behörighet till.

2.1.4 Kerberos

Kerberos är ett protokoll för autentisering som använder en kombination av secret-key kryptering och betrodda tredje-parter för att tillåta säker autentisering till nätverkstjänster över obetrodda nätverksanslutningar.

Det finns flera implementeringar av Kerberos. Tidigare fanns det begränsningar i USA:s exportregler som gjorde att MIT Kerberos inte kunde användas hur som helst utanför USA:s gränser. Då skapades Heimdal. Både MIT Kerberos och Heimdal är utgivna under öppen källkods licens. I ett AD är KDC en av tjänsterna på en domänkontrollant.
Varje server som är med i Kerberos autentisering realm måste ha ett giltigt DNS uppslag med ett fullständigt Fully Qualified Domain Name (FQDN). [8].

För att kunna använda AD som Linux autentisering behöver PAM konfigureras så Kerberos autentisering används och Name Server Switch(NSS)[10] att använda LDAP för att hitta användare och gruppinformation i AD [7].

[10] NSS är en funktion som finns i många Unix system som t ex hitta host namn.

2.2 Linux som klient

2.2.1 Winbind

Winbind är en del av Samba, som är ett projekt licensierad som öppen källkod.

Winbind är en tjänst som kör på Sambaklienter och fungerar som en proxy[11] för kommunikation mellan PAM och NSS som körs på en linuxmaskin och AD på en domänkontrollant.

I detalj så används Kerberos av Winbind för att autentisera mot AD och LDAP för att hämta användar- och grupp information. Winbind tillhandahåller även andra tjänster såsom förmågan att lokalisera domänkontrollanter med en algoritm som liknar DCLOCATOR i AD och förmågan att återställa AD lösenord med kommunikation med domänkontrollant genom att använda Remote Procedure Call (RPC). DCLOCATOR är den mekanism som hittar en domänkontrollant när en applikationer vill ha tillgång till AD [9].

AD som autentisering kräver att konfigurering av PAM och NSS för att anropa winbind-daemon (tjänst). Winbind kommer att översätta dom olika PAM och NSS efterfrågningarna till motsvarande AD anrop. Genom att använda antingen LDAP, Kerberos eller RPC, beroende på det som är mest lämpligt. Kerberos PAM har några problem som undviks med Winbind [7].

Winbind väljer en DC genom att söka DNS locator records på liknade sätt som Microsoft DCLOCATOR module gör, däremot hårdkodar PAM Kerberos domänkontrollanten.

2.2.2 Powerbroker Open

Powerbroker Open är ett öppet källkodsprojekt för att ansluta icke Windows system till en AD-domän. Förutom att ansluta Linux, vilket är det som detta arbete handlar om, ska man även kunna använda det för att ansluta andra Unix system och Mac.

Första delen av PowerBroker Open är PowerBroker Identity Services (PBIS). PBIS är den modulen som hanterar autentiseringen mot AD-domänen.

PBIS använder sig av PAM och NSS för att autentisera och supporterar bland annat Kerberos och NTLM (NT LAN MANAGER) [10].

Powerbroker tillhandahålls av BeyondTrust Software och finns i två versioner. Det är Powerbroker Open och det är GPL/LGPL v2 licens och en kommersiell licens. Detta gör att BeyondTrust Software är huvudsponsor av Powerbroker Opens.

[11] Proxy är en dator som fungerar som en brygga mellan olika program eller tjänster. [16]

2.3 Linux som server

2.3.1 Samba

Microsoft AD schema innehåller definitionerna av varje objekt klass och attribut som skapas i AD forest. Definitionerna ändras och utökas för att få fler funktioner mellan de olika Windows server versionerna. Det gör att samba inte fungerar med alla Windows server versioner som finns idag [11].

Samba stödjer AD schema 47 som är Windows 2008 R2. Detta gäller om Windows servern ska vara domänkontrollant men inte member server. Vill man att datorn ska vara en member server så ska den installeras som klient och man behöver inte tänka på detta. De andra Windows serveroperativsystem och deras schemanivå finns i följande tabell.

Microsoft forest level	Samba Objekt version
Windows Server 2008	44
Windows Server 2008 R2	47
Windows Server 2012	56
Windows Server 2012 R2	69
Windows 2016 Technical Preview	82

2.3.2 Zentyal

Zentyal är en distribution som är färdig för att använda som bland annat domänkontrollant för en AD-miljö. Zentyal bygger på Ubuntu och har färdiga verktyg för att installera och konfigurera bland annat Samba som används när man ska göra den som domänkontrollant med dom funktionerna som behövs, så som DNS och replikering. I Zentyal finns det även möjlighet att sätta upp DHCP, e-postserver, filserver och mycket mera.

3 Genomförande

3.1 Labbmiljö

För att genomföra laborationerna har en virtualiseringsmiljö som har bestått av ett kluster byggt på Proxmox och FreeNas använts.
Proxmox är en Linux distribution som skapar en virtualiseringsmiljö. I Proxmox finns det två olika typer av hypervisor. Den ena är KVM och den andra är LXC. Den som används i dessa laborationer har varit KVM.
FreeNas är en freeBSD distribution som är specialiserad för fildelning. Denna har endast används för fillagring mellan virtualiseringsnoderna.
För att göra nyinstallationer i Linux behöver man ha root-rättigheter. Detta kan man få på lite olika sätt `sudo -i` eller `sudo su` gör att man loggar in som root och stannar där tills man loggar ut. I de exempel som kommer att nämnas används `sudo` tillsammans med kommandot. Detta gör att man endast kör det kommandot som root och sen återgår till sina vanliga rättigheter. Väljer man att logga in som root kan inte kommandot köras med `sudo` framför utan då tas bara det ordet bort.
Förutsättningarna som är satta för att kunna genomföra detta test är att det finns en dator som är installerad med Windows 2012 R2. På den ska det vara konfigurerat en fungerande AD-miljö datorn är satt som domänkontrollant. Utöver detta ska det även finnas utdelningar som har olika behörigheter för olika användare. Som är klient används Ubuntu 14.04 LTS Desktop med de senaste uppdateringarna vid labbtillfället. Versioner på enskilda paket som kan ha betydelse nämns i vardera beskrivning. För att ha ett lyckat resultat ska klienten kunna autentisera mot domänkontrollanten och behörigheterna på mapparna ska fungera.

3.2.1 Winbind

Förberedelser för att installera Winbind är att klienten ska ha rätt nätverksinställningar så att den kan komma åt nätverket. I de inställningarna ska man tänka på att ställa in rätt DNS och rätt FQDN i `/etc/hosts`. Det går i ett senare läge att justera datorns FQDN men det är fördelaktigt att ha rätt från början. Datorns DNS ska peka mot en DNS som har kännedom om domänkontrollanten, lämpligt kan vara att använda domänkontrollantens DNS.

När detta var säkerställt var det dags att påbörja installationen. Till att börja med behövs det installeras en del paket. De paketen som användes på klienten var `krb5-user libpam-krb5 winbind samba smbclient smbfs libnss-winbind libpam-winbind`. Dessa installeras genom att kommandot

```
sudo apt-get install krb5-user libpam-krb5 winbind samba smbclient smbfs libnss-winbind libpam-winbind
```

Paketen `smbclient` och `smbfs` är inte nödvändiga för att få en inloggning men kan vara bra att ha om man vill dela ut filer eller montera utdelningar från andra på din dator. `Winbind` är programmet vi ska använda och är beroende av `samba. krb5-user, libpam-krb5, libnss-winbind` och `libpam-winbind` är till för att det ska gå att autentisera med kerberos och winbind och för att kunna integrera autentiseringsmetoderna i PAM.

Första steget är att få Kerberos att fungera. Det var i detta steg som man kan ha stor fördel av att förbereda klienten med rätt DNS och FQDN. Under installationen var `krb5-user` så kom det upp rutor med inställningar som skulle göras. Har man då satt rätt FQDN och rätt DNS så hittade den inställningen själv och det var bara att klicka vidare. Annars fick man ange realm och då ska den skrivas in i versaler. För att kolla om Kerberos fungerar kan man köra

```
sudo kinit <Domainadmin>@<REALM>
```

Detta är inte nödvändigt att göra men man får en bekräftelse på att Kerberos fungerar och att den fungerar är nödvändigt för att komma vidare.

Efter att Kerberos är klar var det dags att editera konfigurationsfilen för samba och den ligger i `/etc/samba/smb.conf`. Ett exempel av en konfigurationsfil i sin helhet finns i bilaga 6.1.
Där är dock vissa saker som är viktiga och tänka på.
`Realm` är hela domännamnet och `workgroup` är en förkortat realm, bägge ska anges i versaler.
`Template homedir` är den som bestämmer var domänanvändarnas hemkataloger ska ligga. `%D` betyder = domänen och `%U` betyder användarnamnet. Alla som loggar in behöver ha en hemkatalog och för att skilja på lokala användare som sparas oftast direkt i `/home/%U` katalogen därför sattes `/home/%D/%U` som plats för de som loggar in på domänen.
`Winbind use default domain` är den variabeln som gör att man inte behöver ange domännamnet vid varje inloggning utan att den använder den som är nämnd som standard.

När man gör ändringar i smb.conf så behöver man starta om samba och winbind för att ändringarna ska slå igenom. Detta gör man genom att skriva.

```
sudo /etc/init.d/winbind stop
sudo /etc/init.d/samba restart
sudo /etc/init.d/winbind start
```

För att slutligen ansluta till domänen behöver man köra kommandot
`sudo net ads join -U <Domainadmin>%<Password>`
Det skulle kunna vara så att man får felmeddelandet
`Failed to join domain: failed to find DC for domain <DOMAIN>`
när man försöker ansluta till domänen. Detta beror på att `net ads join` inte hittar en domänkontrollant och det kan bero på att DNS inte är aktivt. Genom att lägga till variabeln `-S <servernamn>` så ställer man in vilken server anslutningen ska verifieras emot.

Det räcker dock inte med att ansluta datorn till domänen utan man måste ställa in hur datorn ska sköta autentiseringen. Detta måste man göra i lite olika filer.
Till att börja med kan man editera `/etc/nsswitch.conf` i den filen behöver man lägga till att dator känner till att man kan logga in via winbind. Detta görs genom att lägga till order winbind på tre av raderna så att det står som i exemplet nedan.

```
passwd:     compat winbind
group:      compat winbind
shadow:     compat winbind
```

För att inloggning ska fungera måste även PAM få ändrade konfigurationsfiler. Om man har installerat `libpam-winbind` räcker det med att köra `sudo pam-auth-update` för att få dessa filer uppdaterade. Är det så att man inte kan eller vill köra `sudo pam-auth-update` så kan man gå igenom filerna manuellt.

Filerna innehåller hur autentiseringsbiblioteken ska laddas. Det som ska göras är att uppdatera hur biblioteket laddades eller lägga till biblioteket. Ett bibliotek är den filen som slutar på `.so` som till exempel `pam_unix.so`.

```
/etc/pam.d/common-session
session required pam_unix.so
session required pam_mkhomedir.so umask=0022 skel=/etc/skel

/etc/pam.d/common-account
account sufficient       pam_winbind.so
account required         pam_unix.so

/etc/pam.d/common-auth
auth sufficient pam_winbind.so
auth sufficient pam_unix.so nullok_secure use_first_pass
auth required   pam_deny.so

/etc/pam.d/common-session
session required pam_unix.so
session required pam_mkhomedir.so umask=0022 skel=/etc/skel

/etc/pam.d/sudo
auth sufficient pam_winbind.so
auth sufficient pam_unix.so use_first_pass
auth required   pam_deny.so
@include common-account
```

Efter detta fungera det att logga in i terminalen med domänanvändare. För att aktivera det även till fönsterhanteraren behövs det göra en justering till i en konfigurationsfil. Det är i `/etc/lightdm/lightdm.conf` där får man lägga till raden eller ändra raden så att den ser ut så här

```
greeter-show-manual-login=true
```

Efter detta går det att logga in och sätta grupp- eller användarbehörigheter på utdelningarna från filservern.

I `/etc/lightdm/lightdm.conf` finns det även möjligheten att stänga av att det går att logga in som gäst på datorn. Detta görs genom att lägga till en rad eller ändra raden så att den ser ut så här

```
allow-guest=false
```

För kunna att administrera klienten med hjälp av en användare som finns i domänen behöves det läggas till en rad i `/etc/sudoers` . Denna fil är den fil som bestämmer vilken användare eller grupp som får lova att använda kommandot `sudo` och på det viset få root-rättigheter. Genom att

börja med ett %-tecken kan man ange en användargrupp. Det går att lägga till vilken grupp som helst men med tanke på att administrera en Linux dator är väldigt speciellt jämfört med en Windows dator kan det vara så att inte alla administratörer ska kunna göra allt med en Linux dator. Genom att lägga till raden

```
%linuxadmins ALL=(ALL:ALL) ALL
```

så ger man alla användare medlemmar i gruppen linuxadmins rättigheter att använda `sudo`.

Det är möjligt att automatisera hela installationsprocessen genom att göra ett script. Vi gjorde ett skript där även de specialanpassningarna som behövdes i laborationen är inlagda. Men för att scriptet ska fungera behöver man se till att datorn har rätt FQDN och DNS. Scriptet bifogar vi som bilaga 6.2.

3.2.2 Powerbroker

Versionen som är använd är PowerBroker Open och då version 8.3 som är den för närvarande senaste stabila versionen.
Att installera Powerbroker går snabbt och är enkelt. Man laddar ner ett skript från deras hemsida som man kör och det installerar allt man behöver. Det ända man behöver göra är att följa instruktionerna.
Man är dock tvungen att registrera sig för att få tillgång till länken för att kunna ladda ner.

Det finns vissa delar som man kan behöva komplettera installationen med.
Efter att installationen gå det bra att logga in i konsolläge, vill man även kunna logga in med hjälp av fönsterhanteraren behöver man redigera filen `/etc/lightdm/lightdm.conf`. I den filen behöver man redigera eller lägga till raden

```
greeter-show-manual-login=true
```

Detta gör att det går bra att skriva in sitt egna användanamn när man ska logga in. I samma fil kan man även stänga av gästkontot. Då får man redigera eller lägga till raden

```
allow-guest=false
```

För kunna att administrera klienten med hjälp av en användare som finns i domänen behöves det läggas till en rad i `/etc/sudoers` . Denna filen är den filen som bestämmer vilken användare eller grupp som får lova att använda kommandot `sudo` och på det viset få root-rättigheter. Genom att börja med ett %-tecken kan man ange en användargrupp. Det går att lägga till vilken grupp som helst men med tanke på att administrera en Linux dator är väldigt speciellt jämfört med en Windows dator kan det vara så att inte alla administratörer ska kunna göra allt med en Linux dator. Genom att lägga till raden

```
%linuxadmins ALL=(ALL:ALL) ALL
```

så ger man alla användare medlemmar i gruppen linuxadmins rättigheter att använda `sudo`.

När man ska gå med i domänen kan det vara så att det inte går. Efter lite efterforskningar visade det sig att `Avahi-deamon` var i konflikt med PowerBroker. `Avahi-deamon` är det paketet som gör det möjligt att upptäcka lokala nätverk med mDNS/DNS-SD protokoll sviten [12]. Konflikten går att avhjälpa genom att avinstallera `Avahi-deamon`. I så fall går det bra att använda `sudo apt-get remove avahi-deamon` för att ta bort paketet.

Det är möjligt att automatisera hela installationsprocessen genom att göra ett skript. Vi gjorde ett skript där även de specialanpassningarna som behövdes i laborationen är inlagda. Detta lämnar vi lämnar med som bilaga 6.3.

3.3 Linux som domänkontrollant

3.3.1 Samba

För att använda Linux som domänkontrollant kan man använda Samba. Detta installerar man genom att köra kommandot `sudo apt-get install samba` som även installerar fler paket som är beroende av varandra.
För att sen göra servern till en domänkontrollant kör man kommandot `samba-tool domain provision --use-rfc2307 –interactive.`

Samba-tool kan inte göra backup eller ta bort `/etc/samba/smb.conf` , vilket är en fil som den ska ersätta. Finns filen redan så kan inte samba-tool köras utan den kommer att avbryta sin körning och man får ett felmeddelande. För att lösa detta problem finns det två alternativ. Det ena är att flytta filen till en annan plats eller ta bort den.

Till `samba-tool` är det tilllagt lite olika växlar.
`domain provision` innebär att man vill göra servern till domänkontrollant.

`--use-rfc2307` möjliggör Network Information Service (NIS) anslutningar. NIS möjliggör en central hantering av UNIX attribut i AD. Rekommendationen är att använda sig av den här funktionaliteten under förberedelsen med att skapa en domän. Det finns inga nackdelar att inte använda den men det kan komma situationer där kravet är att använda central hantering. Detta kräver extra arbete t ex att manuellt utöka AD schema.

`--interactive` gör att konfigurationen blir lite mer interaktiv med frågor man ska svara på. Fördelen är att om man har ställt in servern med rätt domän och mot den DNS som man vill

använda sig av så hämtar `samba-tool` mycket från den befintliga konfigurationen. Dessa svar kommer inom hakparenteser och blir standardvärdet om man inte vill fylla i något annat.

Frågorna man ska svara på är `realm, domain, server role, DNS backend` och `DNS forwarder.`

`Realm` är Kerberos Realm och AD DNS skrivs i stora bokstäver. Realmen är domänen.

`Domain` är NT4 NetBIOS domännamn skrivs i stora bokstäver används för bakåtkompabilitet. Längsta tillåta namnlängd är 15 tecken och det rekommenderas av dom som har utvecklat Samba. Detta är den första delen av AD DNS namnet. Några skiljetecken är tillåtna som tex punkt, dessa kan orsaka problem och ska undvikas.

`Server role` är vilken roll servern ska ha. DC står för domänkontrollant.

`DNS backend` är vilken typ av DNS som servern ska använda sig av. `Samba internal DNS server` och `BIND9_DLZ` är dom som stöds av samba. Om det inte finns komplexa krav på DNS är det bästa valet internal DNS. `BIND9_DLZ` kräver setup och konfiguration av `BIND`. Det går att ändra valet i efterhand. `BIND9_FLATFILE` ska inte användas, den är inte dokumenterad och är inte stöd av samba. Det går inte att välja `NONE` eftersom AD förlitar sig på DNS, så den första domänkontrollant måste agera som DNS server. Väljer man `Samba internal DNS server` så sköter samba själva konfigureringen och man behöver inte göra mer själv.

`DNS forwarder IP address` är den adressen som servern ska skicka sina DNS-frågor till om den inte har det i sitt egna register. Parameter kommer bara upp för inmatning av parameter vid användning av Samba internal DNS som backend.

Slutligen frågar `samba-tool` efter vilket lösenord man vill ha på sin domänadministrator med användarnamnet `Administrator.`
Lösenordet måste uppfylla komplexa krav, minst 8 tecken, måste minst innehålla tre av fem av följande grupper:

- Stora bokstäver i de europeiska språken (A till Z, med diakritiska tecken, grekiska och krylliska tecken.
- Små bokstäver i de europeiska språken (A till Z, med diakritiska tecken, grekiska och kyrilliska tecken.
- Decimalt (0-9)
- Icke alfanumerisk: `~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/`

- Vilken unicode tecken som är katalogiserad som alfabetiskt tecken men inte är versal eller gemen. Detta inkluderar unicode tecken från asiatiska språken.

Skulle det vara så att något av stegen fallerade och man blev tvungen att starta om `samba-tool` fick man inte glömma att ta bort `smb.conf` eller byta plats på den. Annars fick man samma problem som om man glömde göra det i början. [5]

3.3.2 Zentyal

Zentyal är en distribution som är tänkt att användas som bland annat domänkontrollant. Så för att installera denna laddar man ner distributionen från Zentyals hemsida. Den versionen som är använd för laborationen är Zentyal 4.2 Development Edition. När sen installationen var klar får man gå in i administrationsgränssnittet som är en hemsida som finns lokalt på servern. I första steget kommer det upp en fråga om vilka tjänster man vill installera på sin server. För att ha servern som domänkontrollant räcker det med att installera rollerna `Domain Controler and File Sharing` och `DNS server`. Genom att administrationsgränssnittet är upplagt som en hemsida går det även bra att fjärradministrera servern genom att gå in på sidan från vilken dator som helst i nätverket. Det man måste se till då är att det är tillåtet i brandväggen. Detta kan även vara bra att känna till om det är så att man vill ha en annan säkerhet på server, så att vem som helst inte ska kunna administrera den.
Ett problem som stöttes på var att det blev fel på den iso-filen som laddades ner för Zentyal 4.2. Detta avhjälptes genom att ladda ner Zentyal 4.1 och installera den. Efter installationen fick man sen uppdatera den till Zentyal 4.2 innan laborationen fortsatte.

3.4 Resultat

3.4.1 Linux som klient

Att ha Linux som en klient till en Windows domänkontrollant var i dessa laborationer inga större problem. Autentiseringen fungerade och det gick bra att logga in mot domänkontrollanten. Det fungerade även med att ha utdelningar med olika behörigheter. Det som inte fungerade så bra var att i Ubunuts fönsterhanterare finns det ställe att hitta utdelade kataloger men där fanns inte det som var utdelat. Använde man istället Samba för att montera utdelningarna i Ubuntu så fungerade det felfritt. Detta gällde både Winbind och Powerbroker.

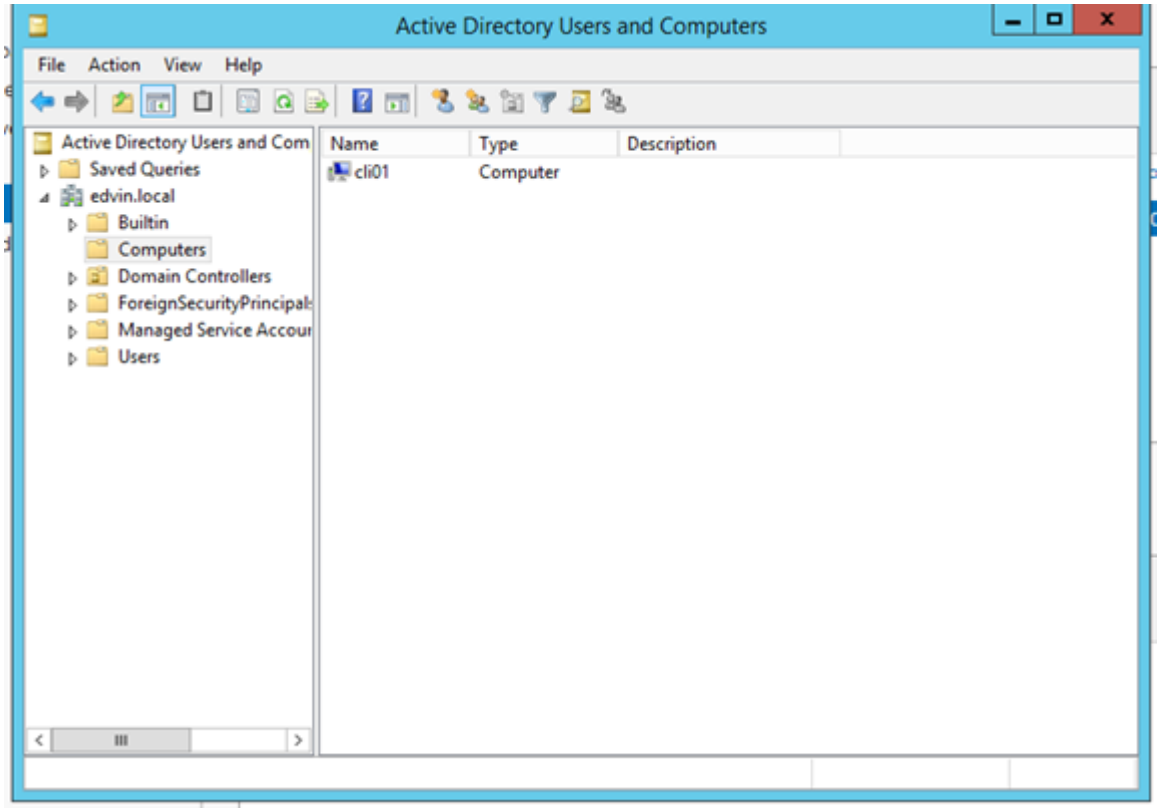

Bild 2 Bilden visar på hur man kan se klienten inlagd i AD-miljön

3.4.2 Linux som domänkontrollant

Det gick att sätta upp en Linux som domänkontrollant få Windows klienter att ansluta till den. Att dela ut filer med olika behörigheter var inte heller några problem. Något som man måste tänka på med att sätta upp en Linux som domänkontrollant är att replikering mellan kontrollanter inte fungerar per automatik utan detta är någon man är tvungen att lösa på annat sätt. Zentyal har vissa saker som replikeras men inte Samban.

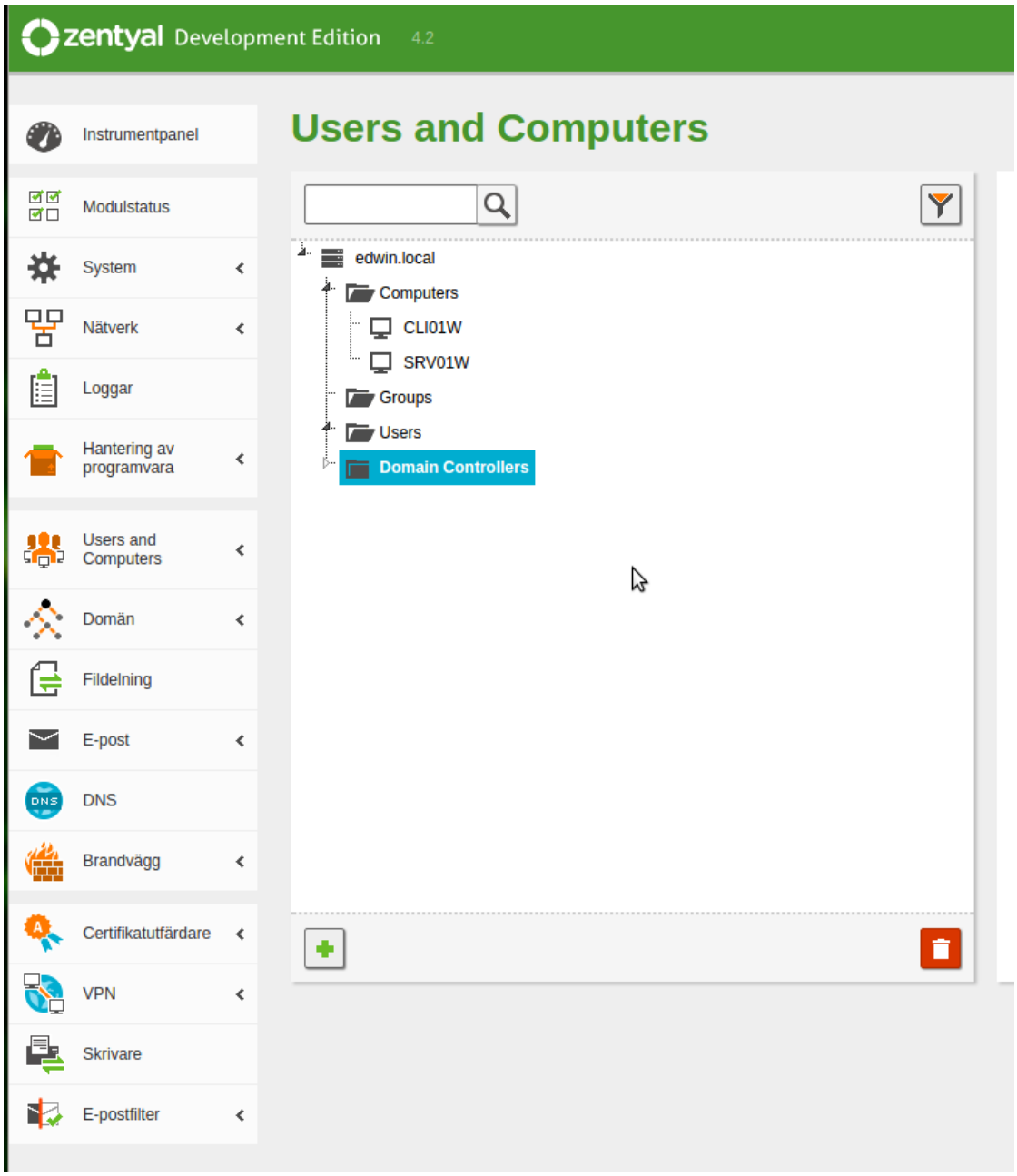

Bild 3 Bilden visar hur det ser ut på en Zentyal server när man har lagt till klienter i domänen.

4 Diskussion

4.1 Analys av resultat

Vi kan konstatera av våra resultat att det är fullt möjligt att använda Linux i en Windows AD-miljö. Det är dock lättare att sätta en Linux maskin som klient eller member server än att ha Linux som domänkontrollant. Detta är för att Windows alltid kommer att ha ett försprång när det gäller AD. Det är Microsoft som utvecklar AD-strukturen och implementerar det direkt i sina serveroperativsystem. När Linux ska använda AD behöver man göra det med Samba. Utvecklarna på Samba måste vänta på Microsoft för att återskapa något liknande med sin programvara.

Att veta att man kan ha en Linux maskin som member server kan vara en stor fördel. Detta då det finns en del tjänster som kan vara med lämpade att ha på en Linux som till exempel filserver eller webbserver. Skulle man inte kunnat använda den som member server hade det varit svårt att få den till att använda behörigheterna som finns med i ens inloggning.

Vårt examensarbete har handlat om Linux i AD-miljö men det finns många andra katalogtjänster som kan skapa liknande miljöer. En del av katalogtjänsterna är utvecklade för Linux. Vi tror att en katalogtjänst utvecklad för Linux skulle fungera bättre än en Windows AD om tanken är att man ska ha Linux som domänkontrollant.

Det vi tror är mest lämpligt är att använda Samba då det är mer aktuellt än Powerbroker i versionshanteringen. Powerbroker bygger vissa av sina delar på samba så det är naturligt att Powerbroker ligger lite efter.

4.2 Förslag till fortsatt arbete

Vi kan se tre delar av vårt arbete som vi själva skulle vilja utveckla men inte ser att vi har haft tid med. En del är att försöka kombinera en Linux domänkontrollant med en Windows domänkontrollant och se hur det fungera bland annat med replikeringar. Något annat vi skulle velat testa är att integrera fler tjänster i AD för att se om resultatet blir annorlunda. Som till exempel att skjuta ut program eller styra klienter med GPO. Till sist hade det varit intressant att se resultatet med att jämföra en Windows AD med en mer anpassad katalogtjänst till Linux som till exempel OpenLDAP.

5 Källförteckning

[1] ”Distrowatch,” 09 maj 2016. [Online]. Available: http://distrowatch.com/. [Använd 11 april 2016].

[2] ”Samba: An Introduction,” the open group, 27 November 2001. [Online]. Available: https://www.samba.org/samba/docs/SambaIntro.html. [Använd 08 april 2016].

[3] ”Techtarget,” 2000-2016. [Online]. Available: http://searchstorage.techtarget.com/definition/Common-Internet-File-System-CIFS. [Använd 20 april 2016].

[4] ”https://www.samba.org/samba/docs/FAQ/,” samba.org, [Online]. Available: https://www.samba.org/samba/docs/FAQ/. [Använd 19 maj 2016].

[5] ”Setup a Samba Active Directory Domain Controller,” samba.org, 2 april 2016. [Online]. Available: https://wiki.samba.org/index.php/Setup_a_Samba_Active_Directory_Domain_Controller.

[6] ”https://www.digitalocean.com/community/tutorials/how-to-use-pam-to-configure-authentication-on-an-ubuntu-12-04-vps,” Digital Ocean Community, 3 Oktober 2013. [Online]. Available: https://www.digitalocean.com/community/tutorials/how-to-use-pam-to-configure-authentication-on-an-ubuntu-12-04-vps. [Använd 8 april 2016].

[7] ”Authenticate Linux Clients with Active Directory,” Technet Magazine, december 2008. [Online]. Available: https://technet.microsoft.com/en-us/magazine/2008.12.linux.aspx#id0060010.

[8] ”https://help.ubuntu.com/community/Kerberos,” ubuntu documentation, 18 November 2014. [Online]. Available: https://help.ubuntu.com/community/Kerberos. [Använd 8 april 2016].

[9] ”Domain Controller Locator,” Microsoft, 2016. [Online]. Available: https://technet.microsoft.com/en-us/library/cc961830.aspx. [Använd 19 maj 2016].

[10] ”https://www.powerbrokeropen.org/,” PowerBroker Open Project, 2015. [Online]. Available: https://www.powerbrokeropen.org/. [Använd 20 maj 2016].

[11] ”Active Directory Schema,” Microsoft, 2016. [Online]. Available: https://msdn.microsoft.com/en-us/library/ms675085(v=vs.85).aspx. [Använd 20 maj 2016].

[12] ”Avahi.org,” 2014. [Online]. Available: www.avahi.org. [Använd 2 april 2016].

[13] ”https://help.ubuntu.com/community/ActiveDirectoryWinbindHowto,” ubuntu documentation, 24 September 2015. [Online]. Available: https://help.ubuntu.com/community/ActiveDirectoryWinbindHowto. [Använd 8 april 2016].

[14] ”Chapter 3. Server Types and Security Modes,” Samba team, [Online]. Available: https://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/ServerType.html. [Använd 19 maj 2016].

[15] ”Chapter 24. Winbind: Use of Domain Accounts,” Samba Team, 15 juni 2005. [Online]. Available: https://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/winbind.html. [Använd 19 maj 2016].

[16] ”Vad är ewn proxyserver,” Microsoft, 2016. [Online]. Available: http://windows.microsoft.com/sv-se/windows-vista/what-is-a-proxy-server. [Använd 19 maj 2016].

6 Bilagor

Bilagor

6.1 Konfigurationsfiler för klient

6.2 Installationsscript i bash för att installera Winbind.

6.3 Installationsscript i bash för att installera Powerbroker.

6.4 Förkortningslista

6.1 Konfigurationsfiler för klient

/etc/samba/smb.conf

```
[global]
security = ads
realm = EDVIN.LOCAL
########################################################################
#If the system doesn't find the domain controller automatically,       #
#you may need the following line                                       #
########################################################################
#password server = 172.20.1.110

#######################################################
# note that workgroup is the 'short' domain name      #
#######################################################
workgroup = EDVIN

#####################################################################
# kommer alla domän användare att se alla tillgängliga utdelningar,  #
# detta är eqvialent som att #allowing “Everyone” att läsa alla utdelningar.  #
#####################################################################
users = @”Domain Users”

idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
winbind enum groups = yes
template homedir = /home/%D/%U
template shell = /bin/bash
client use spnego = yes
client ntlmv2 auth = yes
encrypt passwords = yes
winbind use default domain = yes
restrict anonymous = 2
```

6.2 Installationsscript i bash för att installera Winbind.

```
#!/bin/bash


		##########Kontrollera om scriptet körs med root-rättigheter##########
if (( $EUID != 0 )); then
    echo "Skriptet behöver köras med root-rättigheter."
    exit
fi
		################################Slut##############################


		##########Mata in data##########
echo "Ange ditt Domännamn:"
read DOMAIN
echo "Anger IP-nummer till Domänkontrollanten:"
read DOMAIN_IP
echo "Ange ditt DomänAdministatörsnamn:"
read DOMAIN_ADMIN
echo "Lösenord för DomänAdministratören:"
read -s DOMIAN_PASSWD
		##################Slut#############

		##############Peka rätt DNS##################

		#################Slut########################

		###########Sätt fulständig FQDN på host##################
	FILE="/etc/hosts"
	FIND_STR=$(hostname)
	NEW_TEXT="$(hostname).${DOMAIN^^} $(hostname)"
                                        sed -i "s/$FIND_STR/$NEW_TEXT/" "$FILE"
		##################Slut#######################33

		##########Installera nödvändiga paket##########
apt-get -y install krb5-user libpam-krb5 winbind samba smbclient libnss-winbind libpam-winbind
		#####################Slut########################

#kinit $DOMAIN_ADMIN@${DOMAIN^^}

		########Gör bakup på smb.conf#########
mv /etc/samba/smb.conf /etc/samba/smb.conf.old
		#################Slut##################


		##########Ta bort TLD##########
WORKGROUP=${DOMAIN%.*}
		##############Slut###############

		##########Skapa ny smb.conf anpassad för winbind##############
cat > /etc/samba/smb.conf << EOF

[global]

security = ads
realm = ${DOMAIN^^}
```

```
#########################################################################
#If the system does not find the domain controller automatically,#
#you may need the following line, type IP-number of the first DC #
#########################################################################

#password server = $DOMIAN_IP

################################################
# note that workgroup is the "short" domain name#
################################################

workgroup = ${WORKGROUP^^}

#########################################################################
# File sharing is allowed to be shown to users members of the group typed in  #
# variable "users"                                                ´ #
#########################################################################
users = @"Domain Users"

idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
winbind enum groups = yes
template homedir = /home/%D/%U
template shell = /bin/bash
client use spnego = yes
client ntlmv2 auth = yes
encrypt passwords = yes
winbind use default domain = yes
restrict anonymous = 2

EOF

                ######################################Slut#####################

                ####################Starta om tjänsterna####################
                service winbind stop
                service samba restart
                service winbind start
                ############################Slut############################


                ########################Anslut till domänen#################
                net ads join -U $DOMAIN_ADMIN%$DOMIAN_PASSWD
                ############################Slut############################


    ##########Sök upp rätt rad och lägg till winbind i filen nsswitch##########
        FILE="/etc/nsswitch.conf"
        FIND_STR="passwd:"
        ADD_TEXT="winbind"

                                        sed -i "s/$FIND_STR.*/& $ADD_TEXT/" "$FILE"

        FIND_STR="group:"
```

```
        sed -i "s/$FIND_STR.*/& $ADD_TEXT/" "$FILE"


    FIND_STR="shadow:"

        sed -i "s/$FIND_STR.*/& $ADD_TEXT/" "$FILE"
        ##############################Slut#################################

  #Sök rad och ändra om den finns eller lägg till ny rad i common-session#
FILE="/etc/pam.d/common-session"
                        FIND_STR="pam_unix.so"
    NEW_TEXT="session required pam_unix.so"

    FIND=$(grep -n $FIND_STR $FILE)

    NO=${FIND%:*}

    if [ "$NO" != "" ]; then
        NEW_NO=$NO"s"
        sed -i "$NEW_NO/.*/$NEW_TEXT/" "$FILE"
    else
        echo $NEW_TEXT >> $FILE
    fi

                        FIND_STR="pam_mkhomedir.so"
    NEW_TEXT="session required pam_mkhomedir.so umask=0022 skel=/etc/skel"

    FIND=$(grep -n $FIND_STR $FILE)

    NO=${FIND%:*}

    if [ "$NO" != "" ]; then
        NEW_NO=$NO"s"
        sed -i "$NEW_NO,.*,$NEW_TEXT," "$FILE"
    else
        echo $NEW_TEXT >> $FILE
    fi

        #################Slut##############################


        #############Ändra rad eller lägg till rad i common-account#########
    FILE="/etc/pam.d/common-account"
                        FIND_STR="pam_winbind.so"
    NEW_TEXT="account sufficient pam_winbind.so"

    FIND=$(grep -n $FIND_STR $FILE)

    NO=${FIND%:*}

    if [ "$NO" != "" ]; then
        NEW_NO=$NO"s"
        sed -i "$NEW_NO/.*/$NEW_TEXT/" "$FILE"
    else
        echo $NEW_TEXT >> $FILE
    fi
```

```
FIND_STR="pam_unix.so"
NEW_TEXT="account required pam_unix.so"

FIND=$(grep -n $FIND_STR $FILE)

NO=${FIND%:*}

if [ "$NO" != "" ]; then
        NEW_NO=$NO"s"
        sed -i "$NEW_NO/.*/$NEW_TEXT/" "$FILE"
else
        echo $NEW_TEXT >> $FILE
fi
       ######################Slut#####################################

       ######Ändra eller lägg till rad i common-auth#####################
FILE="/etc/pam.d/common-auth"
                        FIND_STR="pam_winbind.so"
NEW_TEXT="auth sufficient pam_winbind.so"

FIND=$(grep -n $FIND_STR $FILE)

NO=${FIND%:*}

if [ "$NO" != "" ]; then
        NEW_NO=$NO"s"
        sed -i "$NEW_NO/.*/$NEW_TEXT/" "$FILE"
else
        echo $NEW_TEXT >> $FILE
fi

FIND_STR="pam_unix.so"
NEW_TEXT="auth sufficient pam_unix.so nullok_secure use_first_pass"

FIND=$(grep -n $FIND_STR $FILE)

NO=${FIND%:*}

if [ "$NO" != "" ]; then
        NEW_NO=$NO"s"
        sed -i "$NEW_NO/.*/$NEW_TEXT/" "$FILE"
else
        echo $NEW_TEXT >> $FILE
fi

FIND_STR="pam_deny.so"
NEW_TEXT="auth required pam_deny.so"

FIND=$(grep -n $FIND_STR $FILE)

NO=${FIND%:*}

if [ "$NO" != "" ]; then
        NEW_NO=$NO"s"
        sed -i "$NEW_NO/.*/$NEW_TEXT/" "$FILE"
```

```
else
        echo $NEW_TEXT >> $FILE
fi

        ######################Slut#########################


        ######Ändra rad eller lägg till rad i /etc/pam.d/sudo########
FILE="/etc/pam.d/sudo"
                        FIND_STR="pam_winbind.so"
NEW_TEXT="auth sufficient pam_winbind.so"

FIND=$(grep -n $FIND_STR $FILE)

NO=${FIND%:*}

if [ "$NO" != "" ]; then
        NEW_NO=$NO"s"
        sed -i "$NEW_NO/.*/$NEW_TEXT/" "$FILE"
else
        echo $NEW_TEXT >> $FILE
fi

FIND_STR="pam_unix.so"
NEW_TEXT="auth sufficient pam_unix.so use_first_pass"

FIND=$(grep -n $FIND_STR $FILE)

NO=${FIND%:*}

if [ "$NO" != "" ]; then
        NEW_NO=$NO"s"
        sed -i "$NEW_NO/.*/$NEW_TEXT/" "$FILE"
else
        echo $NEW_TEXT >> $FILE
fi

FIND_STR="pam_deny.so"
NEW_TEXT="auth required pam_deny.so"

FIND=$(grep -n $FIND_STR $FILE)

NO=${FIND%:*}

if [ "$NO" != "" ]; then
        NEW_NO=$NO"s"
        sed -i "$NEW_NO/.*/$NEW_TEXT/" "$FILE"
else
        echo $NEW_TEXT >> $FILE
fi


FIND_STR="@include common-account"
NEW_TEXT="@include common-account"

FIND=$(grep -n $FIND_STR $FILE)
```

```
        NO=${FIND%:*}

        if [ "$NO" != "" ]; then
                NEW_NO=$NO"s"
        else
                echo $NEW_TEXT >> $FILE
        fi



                ####################Slut#####################


                ############Starta om tjänsterna#################
                service winbind stop
                service samba restart
                service winbind start
                ##############################Slut##########################

mkdir /home/${WORKGROUP^^}

##########Lägg till möjligheten att ange eget användarnamn##########
        FILE="/etc/lightdm/lightdm.conf"
        FIND_STR="greeter-show-manual-login"
        NEW_TEXT="greeter-show-manual-login=true"

        FIND=$(grep -n $FIND_STR $FILE)

        NO=${FIND%:*}

        if [ "$NO" != "" ]; then
                NEW_NO=$NO"s"
                sed -i "$NEW_NO/.*/$NEW_TEXT/" "$FILE"

        else
                echo $NEW_TEXT >> $FILE
        fi

##########Inaktivera möjligheten att logga in som gäst##########

        FIND_STR="allow-guest"
        NEW_TEXT="allow-guest=false"

        FIND=$(grep -n $FIND_STR $FILE)

        NO=${FIND%:*}

        if [ "$NO" != "" ]; then
                NEW_NO=$NO"s"
                sed -i "$NEW_NO/.*/$NEW_TEXT/" "$FILE"

        else
                echo $NEW_TEXT >> $FILE
        fi
```

##########Lägg till gruppen linuxadmins i sudoers##########

```
FIND_STR="linuxadmins"
NEW_TEXT="%linuxadmins ALL=(ALL:ALL) ALL"

FIND=$(grep -n $FIND_STR $FILE)

NO=${FIND%:*}

if [ "$NO" != "" ]; then
        NEW_NO=$NO"s"
        sed -i "$NEW_NO,.*,$NEW_TEXT," "$FILE"

else
        echo $NEW_TEXT >> $FILE
fi
```

6.3 Installationsscript i bash för att installera Powerbroker.

```
#!/bin/bash


##########Kontrollera om scriptet körs med root-rättigheter##########
if (( $EUID != 0 )); then
   echo "Skriptet behöver köras med root-rättigheter."
   exit
fi


##########Mata in data##########
echo "Ange ditt Domännamn:"
read DOMAIN
echo "Ange ditt DomänAdministatörsnamn:"
read DOMAIN_ADMIN


##########Installera paketet wget##########
apt-get -y install wget


##########Ta bort paketet avahi-daemon##########
#Detta då det skapar konflikter med Powerbroker
apt-get -y remove avahi-daemon



##########Kontrollera om det är 32 eller 64-bitars version av operativsystemet##########
if [ `getconf LONG_BIT` = "64" ]


      then
            ##########64-bit##########
            wget http://download.beyondtrust.com/PBISO/8.3/pbis-open-
8.3.0.3287.linux.x86_64.deb.sh                                  #Ladda ner installations-scriptet
            chmod 755 pbis-open-8.3.0.3287.linux.x86_64.deb.sh
                                                                  #Gör filen körbar
            ./pbis-open-8.3.0.3287.linux.x86_64.deb.sh --noexec
                                                                  #Packa upp installationen
            ./pbis-open-8.3.0.3287.linux.x86_64.deb/install.sh --legacy install
                                                #Kör installationen och installera Legacy
      else
            ##########32-bit##########
            wget http://download.beyondtrust.com/PBISO/8.3/pbis-open-
8.3.0.3287.linux.x86.deb.sh                     #Ladda ner installations-scriptet
            chmod 755 pbis-open-8.3.0.3287.linux.x86.deb.sh
                                                                                  #Gör filen körbar
            ./pbis-open-8.3.0.3287.linux.x86.deb.sh --noexec
                                                #Packa upp installationen
            ./pbis-open-8.3.0.3287.linux.x86.deb/install.sh --legacy install
                                          #Kör installationen och installera Legacy


      fi
```

```
##########Lägg till möjligheten att ange eget användarnamn##########

echo greeter-show-manual-login=true >> /etc/lightdm/lightdm.conf
##########Inaktivera möjligheten att logga in som gäst##########
echo allow-guest=false >> /etc/lightdm/lightdm.conf


##########Anslut till domänen##########
/opt/pbis/bin/domainjoin-cli join ${DOMAIN^^} $DOMAIN_ADMIN


##########Förkorta domännamnet##########
WORKGROUP=${DOMAIN%.*}

                                /opt/pbis/bin/config UserDomainPrefix ${WORKGROUP,,}


                ##########Sätt Defaultdomän##########
                                /opt/pbis/bin/config AssumeDefaultDomain true
                                ##########Ändra default loginscript##########
                                /opt/pbis/bin/config LoginShellTemplate /bin/bash
                                ##########Uppdatera DNS##########
                                /opt/pbis/bin/update-dns
                                ##########Töm cachen##########
                                /opt/pbis/bin/ad-cache --delete-all

    ##########Byt ut eller lägg till i PAM hur datorn ska logga in##########
                                FILE="/etc/pam.d/common-session"
        FIND_STR="pam_lsass.so"
        NEW_TEXT="session [success=ok default=ignore] pam_lsass.so"


        FIND=$(grep -n $FIND_STR $FILE)


        NO=${FIND%:*}


        if [ "$NO" != "" ]; then
                NEW_NO=$NO"s"
                sed -i "$NEW_NO/.*/$NEW_TEXT/" "$FILE"
        else
                echo $NEW_TEXT >> $FILE
        fi



######Lägg till så att alla användare i säkerhetsgruppen "linuxadmins" har sudorättigheter#####
                                echo "%linuxadmins ALL=(ALL:ALL) ALL" >> /etc/sudoers
                                ##########Skriv ut information om möjligheten som raden ovanför
ger##########
                                echo "Skapa global security group på servern med namnet
linuxadmins och lägg in de"
                                echo "grupper och/eller användare som ska ha sudorättigheter på
denna maskinen"
#EOF


##########Gör avslutnings-scriptet körbart##########
echo "Starta om datorn"
```

6.4 Förkortningslista

AD (Active Directory)

LAN (Local Area Network)

NETBIOS (Network Basic Input Output System)

I/O (Input/Output)

SMB (Server Message Block)

CIFS (Common Internet File System)

DOS (Disk Operating System)

OpenLDAP (Open Lightweight Directory Protocol)

DC (Domain Controller)

DNS (Domain Name Service)

KDC (Key Distribution Center)

LDAP (Lightweight Directory Access Protocol)

FQDN (Fully Qualified Domain Name)

PAM (Pluggable Authentication Modules)

SSL (Secure Socket Layer)

RPC (Remote Procedure Call)

PBIS (PowerBroker Identity Services)

NTLM (NT LAN Manager)

DHCP (Dynamic Host Configuration Protocol)

LTS (Long Term Support) det är versioner av Ubuntu som har får säkerhetsuppdateringar i tre år för klienter och fem år för server mot annars nio månader.

KVM Kernel-based Virtual Machine

LXC Linux containers