راهنمای کارساز سامبا

ترجمه و تالیف:
مهندس محمود تقی زاده
مهندس آناهیتا فیروزی

ویرایش:
مهندس آرش معبودی
مهندس احسان کشتکاری

فهرست‌برگه

تقی زاده، محمود

راهنمای کارساز سامبا/ ترجمه و تالیف محمود تقی زاده ، آناهیتا فیروزی.--تهران شورای عالی انفورماتیک کشور، دبیرخانه، ۱۳۸۴.

۷۸ص.: مصور، جدول، نمودار.

ISBN:964-96535-3-8

فهرست نویسی براساس اطلاعات فیپا

۱.سامبا(فایل کامپیوتر). ۲. سیستمهای عامل(کامپیوتر). ۳. سیستم عامل لینوکس. الف. فیروزی، آناهیتا،- مترجم. ب. شورای عالی انفورماتیک کشور، دبیرخانه. ج.عنوان

۷ت۹۴س/۷۶/۷۶ **QA** ۰۰۵/۴۴۷۶

۱۳۸۴

کتابخانه ملی ایران ۸۴-۲۶۶۷۴م

راهنمای کارساز سامبا

ناشر: دبیرخانه شورای عالی انفورماتیک

ترجمه و تالیف: مهندس محمود تقی زاده، مهندس آناهیتا فیروزی

ویراستار فنی: مهندس آرش معبودی

ویراستار ادبی: مهندس احسان کشتکاری

حروف‌چینی: سارا مکی

صفحه آرایی: محمدمهدی بزرکار

ناظر چاپ: مریم مسعودی

طرح روی جلد: مهندس بهروز عبادی

چاپ و صحافی:

تیراژ: ۵۰۰ نسخه

قیمت: ۱۵۰۰۰ ریال

شابک: ۸-۳-۹۶۵۳۵-۹۶۴

طرح ملی نرم افزارهای آزاد/متن‌باز

(گنو/ لینوکس فارسی)

با هدایت علمی مرکز تحقیقاتی فناوری اطلاعات و ارتباطات پیشرفته

دانشگاه صنعتی شریف

و حمایت دبیرخانه شورای عالی اطلاع رسانی

امروزه فنّاوری اطّلاعات به عنوان یکی از مهمترین زیرساختهای توسعه در کشورهای دنیا شناخته شده است. رشد روزافزون این فناوری در کشورهای توسعه یافته، شکاف دیجیتال بین این کشورها و کشورهای در حال توسعه را افزایش می‌دهد.

یکی از حوزه‌هایی که در رشد فنّاوری اطّلاعات در دنیا تاثیر بسزایی داشته، مقوله نرم‌افزارهای آزاد/متن‌باز است. جنبش نرم‌افزارهای آزاد/متن‌باز پس از ۲۰ سال تلاش برای آزادی نرم‌افزار در سراسر دنیا امروزه به رشد و بالندگی رسیده است و باعث پیشرفت و تحولی عمیق در حوزه فناوری اطلاعات شده است.

کشورهای اتحادیه اروپایی، چین، ژاپن، برزیل، آرژانتین، پرو، آفریقای جنوبی و حتی افغانستان برنامه‌های مدونی برای بکارگیری و توسعه این نرم‌افزارها برای نیل به اهداف خود اعلام کردند، کسانی که به این نرم‌افزارها به دیدهٔ تردید می‌نگریستند، پی به اهمیت آن در سیاست‌گذاری توسعه فناوری اطلاعات در کشورها بردند. این‌گونه سیاست‌گذاری نیازمند همکاری و هماهنگی ارکان مختلف دولت در راستای تحقق آنهاست.

در ایران نیز این حرکت جهانی در قالب طرح ملی نرم‌افزارهای آزاد/متن‌باز (گنو/لینوکس فارسی) از حدود سه سال قبل با کارفرمایی دبیرخانه شورای عالی انفورماتیک و مدیریت مرکز تحقیقاتی فنّاوری اطّلاعات و ارتباطات پیشرفته دانشگاه صنعتی شریف و حمایت دبیرخانه شورای عالی اطلاع رسانی برای تولید جایگزین نرم‌افزارهای مهم و کاربردی داخل کشور بر مبنای بومی‌سازی نرم‌افزار آزاد و ایجاد تنوع نرم‌افزاری شروع شده است. این طرح بسترساز تولید سامانه عامل ملی کشور است که می‌تواند به خوبی به عنوان جایگزین سامانه‌عامل ویندوز استفاده شود. در حال حاضر با توجه به فعالیت انجام گرفته نسخه‌های اولیه جایگزین برای سامانه‌عامل، برنامه‌های دفتری و بانکهای اطلاعاتی تا حد خوبی انجام شده است، که این تلاش در جهت استقلال و خودکفایی کشور در صنعت نرم‌افزار قابل تقدیر است.

با توجه به جوان بودن این حرکت در کشور لزوم فرهنگ‌سازی و تولید محتویات آموزشی ضروری به نظر می‌رسد. دبیرخانه شورای عالی انفورماتیک بر خود واجب می‌داند که تا حد امکان بستر لازم برای گسترش این فعالیت را آماده نماید. در همین راستا این شورا اقدام به تهیه مجموعه کتابهایی با عنوان «مجموعه نرم‌افزارهای آزاد/متن‌باز» –با پوشش‌دادن طیف کلی از مخاطبین این حوزه مانند مدیران، کارشناسان رسته فرابری داده‌ها، کاربران نهایی، دانشجویان، توسعه‌دهندگان و برنامه‌نویسان– نموده است که کتاب حاضر نیز از همین مجموعه است. امید است این مجموعه کتابها بتواند کمکی در جهت بالابردن آگاهی عمومی جامعه در حوزه نرم‌افزارهای آزاد/متن‌باز شود.

دبیر شورای‌عالی انفورماتیک کشور
دی ۸۴

فهرست مطالب

فصل اول
نحوه دریافت و نصب سامبا
۱-۱- مقدمه و ساختار سامبا و چگونگی نصب آن

معمولاً بسته[1] سامبا در نسخه‌های ارائه شده توسط توزیع‌کنندگان لینوکس وجود دارد. برای استفاده از آن باید این بسته را روی بستر دلخواه خود نصب نمائید. همچنین می‌توان این بسته را از وب‌گاه سامبا در آدرس <http://samba.org> نیز به دست آورد. به همراه بسته سامبا، پرونده‌های کمکی و مستنداتی نیز برای راهنمایی نصب روی سامانه‌عامل وجود دارد که دارای جزئیات کافی برای نصب و تنظیم سامبا هستند. گاهی نیاز است که سامبا را از روی متن[2] آن ترجمه کرد که در فصل مربوط به آن به تفصیل آورده شده است. توجه کنید که معمولاً آخرین نسخه سامبا در وب‌گاه آن وجود دارد. برای شروع کار ابتدا باید از نصب سامبا روی سامانه‌عامل مطمئن شوید.

سامبا شامل سه بسته است:

۱. samba-common: که شامل پرونده‌های مورد نیاز کارساز و کارخواه است.
۲. samba-server: که نسخه کارساز سامباست.
۳. samba-client: که شامل برنامه‌های smbprint و smbmount و smbclient و مستندات مـربوط بـه آنان است.

برای نصب باید به شاخه شامل بسته بروید و سپس دستور زیر را وارد کنید:

```
# rpm -Uvh samba-*.rpm
```

با وارد کردن دستور فوق هر دو بسته کارساز و کارخواه نصب خواهند شد. در صورتی‌که فقط مایل به نصب کارخواه سامبا باشید باید دستور زیر را استفاده کنید:

```
# rpm -Uvh samba-common-*.rpm samba-client-*.rpm
```

در صورت عدم دریافت پیغام خطا، بسته سامبا روی سامانه‌عامل شما نصب شده است. حالا باید به تنظیم آن بپردازید.

۱-۲- تنظیم سامبا

کلیه تنظیمات مربوط به سامبا در پرونده smb.conf ذخیره شده است. این پرونده معمولاً در مسیر /etc/samba/smb.conf و یا /usr/local/lib/samba/smb.conf قرار دارد. بسته به نظر خودتان می‌توانید این پرونده را دستی ویرایش کنید و یا اینکه از ابزارهایی مانند واسط مبتنی بر وب SWAT و یا linuxconf که برای این کار فراهم شده است، استفاده نمایید. توضیحات لازم در مورد این ابزارها در پایان فصل به طور کامل آورده شده است.

شکل پرونده smb.conf مانند پرونده‌های قدیمی ini. در ویندوز ۳،۱ است. این پرونده دارای قسمتهای[3] مختلفی است و با قرارگرفتن نام هر بخش درون علامت "[ ]" در یک خط جدید شروع می‌شود. هر بخش معرف یک منبع به اشتراک گذاشته شده روی کارساز سامبا است و شامل تنظیمات

---

[1] Package
[2] Source
[3] Section

مربوط به همان بخش است. بخش "global" در پرونده تنظیمات یک بخش ویژه و خاصی است که شامل تمام تنظیماتی است که روی کل کارساز سامبا اعمال می‌شود و مربوط به یک منبع به اشتراک گذاشته شده مجزا نمی‌باشد. در مثال زیر یک پرونده بسیار ساده و کوچک از smb.conf را مشاهده می‌کنید:

```
[global]
Workgroup =WKG
Netbios name = MYNAME
[share1]
Path = /tmp
[share2]
Path = /my_share_folder
Comment = some random files
```

همانطور که در مثال نیز می‌بینید، دو منبع به نامهای share1 و share2 معرفی شده‌اند و مسیر آنها نیز در پارامتر Path مشخص شده است. در واقع برای به اشتراک گذاشتن یک منبع روی سامبا کافیست مانند مثال فوق ابتدا نام و سپس دیگر مشخصات آن را در پرونده smb.conf وارد نمایید. البته این فقط ابتدای کار است. برای تنظیمات دقیق‌تر باید به پارامترهای دیگری که بعداً توضیح داده می‌شود دقت نمود.

۱-۳- ساختار کارساز سامبا

سامبا شامل سه دایمون[1] است. هر دایمون در لینوکس، یک برنامه کاربردی است که در پس زمینه[2] سامانه‌عامل اجرا می‌شود و خدماتی را فراهم می‌کند. این خدمات می‌تواند خدمات وب باشد که کارساز آن در لینوکس Apache است و در آن‌صورت دایمون آن httpd خواهد بود. کارساز سامبا نیز شامل سه دایمون است که وجود دوتای آنها برای یک کارساز سامبا الزامی است:

nmbd: این دایمون تمام درخواستهای مربوط به Name Registration وName Resolution را مدیریت می‌کند و با وجود آن کارخواه‌ها می‌توانند به کارسازها و منابع مشترک آنها دسترسی پیدا کنند. این دایمون به عنوان WINS Server نیز می‌تواند عمل کند و تبدیل NetBIOSName به آدرسIP را انجام دهد. علاوه بر این، nmbd تمام پروتکلهای مبتنی برUDP را اداره کرده و باید در ابتدای کار سامبا اجرا شود.

smbd: این دایمون نیز تمام خدمات مبتنی بر TCP/IP را مدیریت می‌کند. همچنین کلیه کارهای مربوط به احرازهویت[3] محلی کارخواه‌ها را در صورت نیاز انجام می‌دهد و دسترسی به منابع مشترک را فراهم می‌کند. smbd باید بلافاصله بعد از nmbd اجرا شود.

---

[1] Daemon
[2] Background
[3] Authentication

winbindd: وقتی سامبا عضوی در ویندوز NT4 و یا دامنه ADS[1] است، این دایمون باید اجرا شود. همچنین هنگامیکه سامبا یک ارتباط قابل اعتماد[2] با دامنه دیگری دارد، باید این دایمون در حال اجرا باشد. winbindd پرونده smb.conf را برای وجود دو پارامتر idmap uid و idmap gid جستجو می‌کند. اگر این دو پارامتر در پرونده پیدا نشود، winbindd اصلاً اجرا نمی‌شود. جزئیات کار winbindd به طور کامل در فصلهای بعد آورده شده است.

۱-۴- بررسی صحت پرونده smb.conf با برنامه testparm

هر بار که در پرونده smb.conf تغییری داده می‌شود، بررسی درستی محتویات پرونده smb.conf بعد از اعمال تغییرات در آن از اهمیت خاصی برخوردار است. با برنامه testparm می‌توان از صحت این پرونده مطلع شد. مثال زیر را در نظر بگیرید:

```
[global]
workgroup = MIDEARTH
[homes]
guest ok = no
read only = no
```

در این مثال یک منبع به نام homes به اشتراک گذاشته شده است. در مورد پارامترهای به کار رفته در آن در فصلهای بعدی توضیح خواهیم داد. اما برای اطمینان از صحت تنظیمات به‌کار رفته در آن باید دستور زیر را وارد نمائید:

```
# testparm   /etc/samba/smb.conf
```

اگر هیچ مشکلی در پرونده تنظیمات نباشد و testparm به درستی اجرا شود، این برنامه ابتدا پیغامی مبنی بر صحیح بودن پرونده نمایش می‌دهد و سپس لیست منابعی که به اشتراک گذاشته شده است و در پرونده تعیین گردیده، نشان می‌دهد. نحوهٔ کار testparm به این صورت است که پرونده smb.conf را به دقت تجزیه و تحلیل می‌کند[3] و پارامترهای ناشناس و یا خطاهای نحوی[4] را گزارش می‌کند. بنابراین اکیداً توصیه می‌شود بعد از هر گونه تغییر در پرونده smb.conf، برنامه testparm را اجرا نمایید و از صحیح بودن پرونده اطمینان حاصل نمائید.

۱-۵- استفاده از ابزار مبتنی بر وب SWAT برای تنظیم و مدیریت سامبا

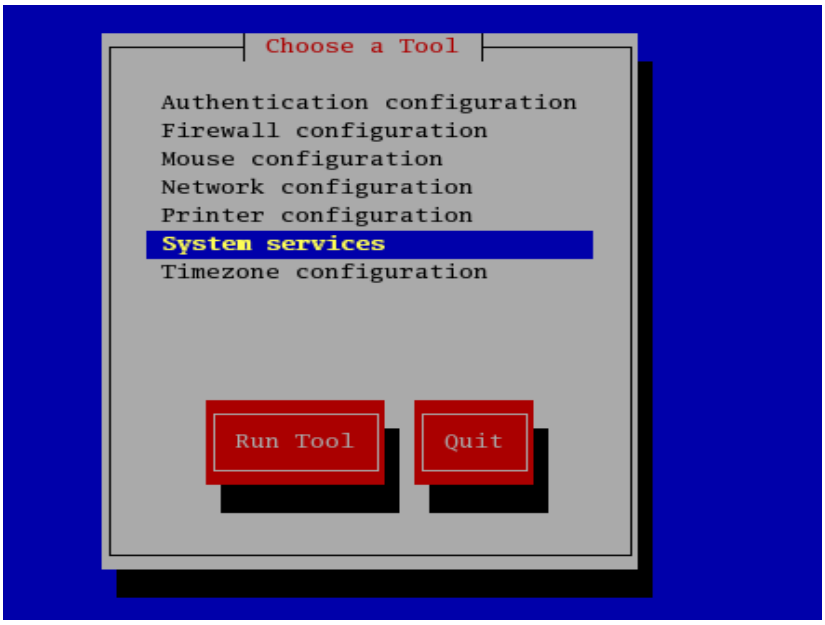
به غیر از تنظیم دستی پرونده smb.conf، ابزار گرافیکی نیز به نام SWAT وجود دارد. معمولاً SWAT در بسته سامبا وجود دارد، اما ممکن است به صورت یک بسته جدا نیز ارائه شود. توضیحاتی دربارهٔ SWAT در مستندات بستر مورد استفاده آورده شده است. (به*usr/doc/samba/ مراجعه شود). همچنین در وب‌گاه www samba.org/doc نیز توضیحاتی در باره این پرونده داده شده است. برای

[1] Active Directory Server Domain
[2] Trust Relationship
[3] Parse
[4] syntax

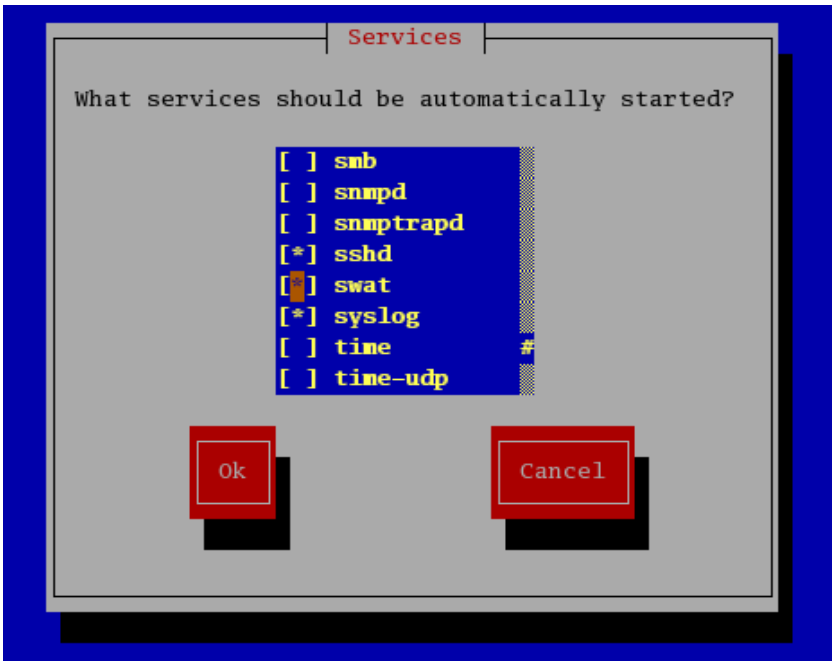
استفاده از این ابزار باید ابتدا آن را نصب نمایید (چون معمولاً این بسته به صورت پیش‌فرض نصب نمی‌شود) سپس در محیط shell مربوط به بستر خود، دستور زیر را وارد نمایید:

```
# setup
```

با وارد نمودن دستور فوق؛ یک ویزارد گرافیکی مانند زیر مشاهده می‌کنید. دقت کنید که در اینجا از بستر RedHat 9.0 استفاده شده و ممکن است در بسترهای مختلف در جزئیات، کمی تفاوت باشد.



System services را انتخاب کرده و سپس در لیست، مقابل swat را علامت بزنید:

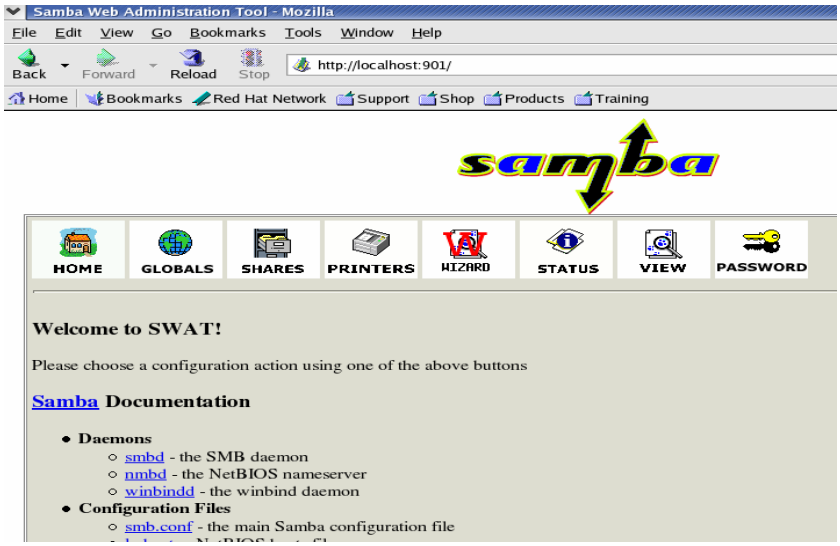


حال باید خدمت xinetd را مجددا راه‌اندازی کنید: (در بعضی بسترها ممکن است این خدمت به نام inetd باشد.)

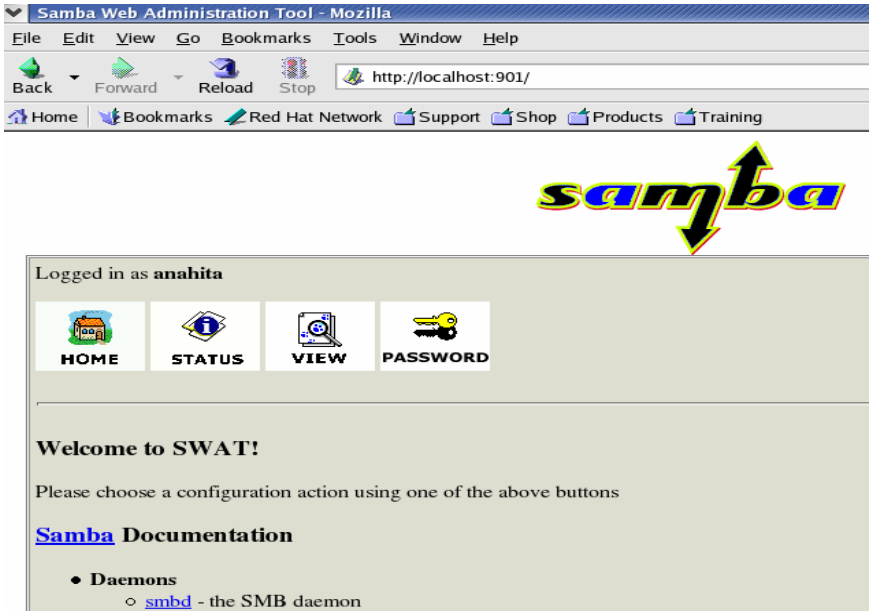
```
# service   xinetd   restart
```

برای شروع کار با SWAT، ابتدا باید مرورگر مورد نظر خود را باز کنید و آدرس <http://localhost:901> را تایپ نمایید. می‌توان localhost را با نام رایانه‌ای که سامبا روی آن درحال اجراست، جایگزین کرد. بعد از این که آدرس را وارد نمودید، یک اعلان برای ورود[1] مشاهده خواهید نمود. در اینجا باید نام کاربر و کلمهٔعبور صحیح را وارد نمایید. با کاربر root می‌توان، تمام تغییرات ممکن را انجام داد. ولی اگر با یک کاربر عادی وارد شوید، فقط می‌توانید تنظیمات را مشاهده کنید و تنها تغییری که می‌توانید بدهید کلمهٔعبور همان کاربر خواهد بود. تفاوت کاربر root و یک کاربر عادی در دو شکل بعدی نشان داده شده است:

[1] Login



صفحه تنظیمات SWAT با کاربر root



صفحه تنظیمات SWAT با کاربر عادی

به تفاوتهای بالای صفحه‌ها دقت نمایید. با استفاده از این محیط گرافیکی به راحتی می‌توانید تمام تنظیمات سامبا را انجام دهید. همچنین از اینجا به صفحات کمکی نیز دسترسی دارید. SWAT از روی هر ماشینی که از نظر آدرسIP با رایانه کارساز سامبا در یک شبکه است، می‌تواند اجرا شود و مورد استفاده قرار بگیرد. اما در این صورت باید مراقب مسائل امنیتی مثل استراق سمع[1] کلمهٔعبور از روی شبکه باشید. به منظور داشتن امنیت بیشتر هنگام مدیریت سامبا از راه دور، می‌توان آن را تحت SSL اجرا نمود. برای این کار کافی است مراحل زیر را طی کنید:

- OpenSSL را نصب نمایید.
- یک گواهینامه[2] و یک کلید خصوصی[3] تولید کنید:

```
# /usr/bin/openssl  req  -new -x509 -days 365 -nodes -config \
/usr/share/doc/packages/stunnel/stunnel.cnf \
-out /etc/stunnel/stunnel.pem -keyout /etc/stunnel/stunnel.pem
```

- Swat را از xinetd (inetd) حذف نمایید.
- خدمت stunnel را راه اندازی کنید.

```
# stunnel -p /etc/stunnel/stunnel.pem -d 901 \
-l /usr/local/samba/bin/swat swat
```

- بعد از انجام مراحل فوق به مرورگر خود رفته و سپس آدرس زیر را وارد نمایید:

```
<https://localhost:901>
```

- گواهینامه را قبول نموده و سپس اتصال SSL شما برقرار خواهد شد.

۱-۶- مشاهده لیست منابع مشترک روی سامبا

بعد از آنکه توانستید یک کارساز سامبا را به طور خیلی ساده تنظیم کنید، باید بتوانید لیست منابع مشترک را روی آن مشاهده نمائید. همانطور که می‌دانید، کارخواه سامبا می‌تواند یا ویندوزی باشد و یا لینوکسی. برای مشاهده لیست منابع به اشتراک گذاشته شده از روی یک کارخواه تحت لینوکس باید دستور زیر را وارد نمائید:

$ smbclient –L *yourhostname*

که درآن yourhostname نام کارساز سامبا است. با وارد نمودن این دستور باید لیست تمام منابع به اشتراک گذاشته شده روی کارساز را مشاهده کنید. اگر این مورد انجام نشد، حتماً در تنظیمات اشتباهی رخ داده است. از این روش می‌توان برای دیدن منابع مشترک روی کارسازهای دیگر مانند ویندوز ۲۰۰۰ نیز استفاده کرد.

توجه کنید که اگر در پرونده تنظیم، پارامتر security را طوری تنظیم کرده باشید که نیاز به تصدیق اصالت باشد در آن صورت یک پیغام جهت وارد کردن کلمهٔعبور به شما داده می‌شود. این امکان نیز وجود دارد که شما کارساز سامبا را مجبور کنید بدون درخواست کلمهٔعبور، لیست را نشان دهد:

---

[1] Sniff
[2] Certificate
[3] Private Key

$ smbclient -L *yourhostname* **-N**

در کارخواه‌ها تحت ویندوز نیز با دستور net share می‌توان لیست منابع مشترک را دید.

۱-۷- دسترسی به منابع به اشتراک گذاشته شده

کارخواه‌ها در لینوکس به دو صورت می‌توانند به این منابع مشترک دسترسی داشته باشند:

- توسط برنامهٔ smbclient که درواقع یک دسترسی مانند FTP به منابع را فراهم می‌کند.

مثال :

$ smbclient *//yourhostname/aservice*

به این نوع دسترسی، دسترسی محلی[1] گویند. yourhostname نام کامپیوتری است که smbd روی آن نصب شده است و aservice نام هر منبع به اشتراک گذاشته شده است. مثال:

$ smbclient //bambi/fred

در مثال فوق، نام کامپیوتر کارساز bambi و نام منبع مشترک fred است.

- توسط دستور smbmount که به کاربران اجازه می‌دهد یک سامانه پرونده مشترک مانند سامانه‌های پرونده محلی، سوار[2] کنند:

$ smbmount *//server/Share /mount-point*

به این نوع دسترسی نیز دسترسی از راه دور[3] گفته می‌شود.

کارساز سامبا باید در لیست شمایلهای موجود در Network Neighborhood روی تمام کارخواه-های تحت ویندوز که در زیر شبکه[4] خودش هستند، دیده شود. بنابراین سعی کنید آن را از روی یک کارخواه دلخواه جستجو کنید و یا این‌که آن را سوار نمایید. در ویندوز با استفاده از دستور net use می‌توان منابع مشترک را سوار کرد:

C:\> net use I: *\\yourhostname\aservices*

برای چاپ: **C:\> net use lpt1:** *\\servername\spoolservice*

C:\> print *filename*

نکته: برنامه printtool اجازه دسترسی به چاپگرهای مشترک سامبا را از روی کارخواه‌های لینوکس فراهم می‌کند.

---

[1] Local
[2] Mount
[3] Remote
[4] Subnet

۱-۸- چند نکته قابل ذکر

بعد از تنظیم سامبا باید خدمت آن را راه اندازی کنیم. این کار باید طبق دستورات هر بستر انجام شود. مثلاً در نسخهٔ RedHat از لینوکس می‌توانید به صورت زیر عمل نمائید:

چون دست‌نوشته[1] مربوط به مدیریت سامبا در /etc/rc.d/init.d/smb قرار دارد، باید برای راه‌اندازی، ایست و پی بردن به وضعیت خدمت سامبا دستورات زیر را اجرا کنید:

```
# /etc/rc.d/init.d/smb   start
# /etc/rc.d/init.d/smb   stop
# /etc/rc.d/init.d/smb   status
```

تمام مسائل مربوط به راه اندازی و ایست خدمت سامبا در پرونده مربوط به log های سامانه، ثبت می‌شود. پرونده ثبت رخدادهای سامانه در مسیر var/log/messages قرار دارد. اما علاوه بر آن، سامبا یک پرونده ثبت رخداد مخصوص به خود نیز دارد که مسیر آن در پرونده smb.conf در پارامتر Log file مشخص شده است. هر چند معمولاً این پرونده در مسیر /var/log/samba قرار دارد. اگر سامبا به درستی عمل نکرد، پرونده ثبت رخداد سامبا را بررسی نمائید. معمولاً اکثر مشکلات مربوط به سامبا با مشاهده این پرونده و پیغامهای آن حل می‌شود.

تعداد زیاد فرآیند smbd:

همان طور که گفته شد، nmbd دایمون مربوط به Name Server است. اگر سامبا به عنوان WINS Server عمل نکند، فقط یک فرآیند nmbd روی سامانه شما در حال اجراست، در غیر این صورت، یعنی اگر سامبا بخواهد WINS Server هم باشد باید دو فرآیند nmbd در حال اجرا داشته باشید که یکی برای مدیریت درخواستهای WINS اختصاص یابد. اما از طرف دیگر smbd باید تمام درخواستهای اتصال به دایمون را اداره کند. برای این کار، smbd به ازای هر اتصال کارخواه یک فرآیند جدید ایجاد می‌کند. در واقع برای هر اتصال کارخواه باید یک برنامهٔ smbd مخصوص به آن فعال باشد و به آن پاسخ دهد. بنابراین ممکن است در یک زمان تعداد زیادی فرآیند smbd دیده شود.

۱-۹- بعضی خطاهای معمول در راه اندازی سامبا

- *پیغام خطای "open-oplock-ipc":*

شاید این پیغام خطا در هنگام شروع فرآیند smbd در پرونده ثبت رخداد به صورت زیر مشاهده شود:

```
open-oplock-ipc : Failed to get local UDP socket for address 100007f.
```

Error was connot assign requested .

درصورت مشاهده این خطا، احتمالاً کارت شبکه[2] شما به درستی کار نمی‌کند. باید مطمئن شوید که آن را درست تنظیم کرده‌اید.

---

[1] Script
[2] Loopback

- *پیام خطای "The network name connot be found":*

خطای فوق می‌تواند ناشی از یکی از این موارد باشد:

– در پرونده smb.conf مسیری را که برای منبع به اشتراک گذاشته شده تعیین گردیده، وجود ندارد.

– با کاربری سعی در دسترسی به منابع مشترک دارید که مجوزهای کافی برای استفاده درآن مسیر را ندارد. (در واقع برای استفاده از یک منبع مشترک توسط یک کاربر، آن کاربر باید دارای مجوزهای خواندن و اجرا باشد).

– سعی در دسترسی به منبع مشترکی را دارید که اصلاً وجود ندارد.

فصل دوم
مثالها
۲-۱- مقدمه
در این بخش سعی می‌کنیم مثالهایی از تنظیم سامبا برای کارهای مختلف به منظور روشن‌تر شدن مطلب بیاوریم. مثالهای ذکر شده از ساده به مشکل طرح شده‌اند و در هر مورد تمام تغییرات و تنظیماتی که باید انجام شود، نیز بیان شده است. توجه داشته باشید که مثالهای این بخش صرفاً برای آشنایی بیشتر با سامبا مطرح شده و برای تنظیمات پیشرفته باید مطالب بیشتری بیان شود که در فصلهای آینده به آنها خواهیم پرداخت. نکته دیگر اینکه، تمرکز اصلی در مثالها فقط روی سامبا است و هیچ توجهی به بستر خاصی مدنظر نبوده است. قبل از پرداختن به مثالها، از نصب صحیح سامبا اطمینان حاصل کنید.

۲-۲- مثال ۱: راه اندازی یک کارساز سند[1]
می‌خواهیم یک پرونده کارساز داشته باشیم که تمام کاربران بتوانند به آن دسترسی داشته باشند. شرایط این محیط به اشتراک گذاشته شده به صورت زیر است:

نام منبع مشترک export/ را انتخاب کرده‌ایم.

صاحب پرونده کاربری به نام jack Baumbach است که نام کاربری آن jackb و کلمهٔعبورش m0r3paln است.

برای ایجاد این کارساز باید مراحل زیر را انجام دهید:

کاربر مورد نظر را به سامانه اضافه کنید. به طوری که شاخه home آن نیز ایجاد شود:

```
# useradd -c "Jack Baumbach" -m -g users -p m0r3plan jackb
```

شاخه export/ را ایجاد نمایید و مجوزهای آن را تنظیم کنید. همچنین صاحب آن را باید مشخص نمایید:

```
# mkdir /export
# chmod u+rwx , g+rx , o+rx /export
# chown jackb.users /export
```

کلیه پرونده‌هایی را که می‌خواهید به اشتراگ بگذارید به شاخه export/ کپی نمایید.

پرونده smb.conf را مطابق زیر تغییر دهید:

```
# Global parameters
[global]
workgroup = MIDEARTH
netbios name = HOBBIT
security = share
[data]
comment = Data
```

[1] Document Server

path = /export
read only = yes
guest ok = yes

پرونده smb.conf را با برنامه testparm آزمایش کنید: # testparm

بعد از اجرای testparm ممکن است پیغامهای خطایی ظاهر شود. تا از اجرای صحیح testparm و گرفتن نتیجه‌ای بدون خطا مطمئن نشده‌اید، ادامه ندهید. خروجی testparm باید شبیه زیر باشد:

```
Load smb config files from  /etc/samba/ smb.conf
Processing section "[data]"
Loaded services file ok
Server role : Role_STANDALONE
Press Enter to see a dump of your service definitions
[press enter]
#Global parameters
[global]
Workgrpup = MIDEARTH
netbios name  = HOBBIT
security = share
[data]
comment = Data
path = /export
read only = yes
guest ok = yes
```

با دستورات مناسب بستر مورد استفاده، خدمت سامبا را راه اندازی کنید.

کارخواه تحت ویندوز خود را به گروه کاری[1] مشخص شده (در اینجا MIDEARTH) متصل نمایید و نام آن را به ROBBINS تنظیم کنید. آن را مجدداً راه‌اندازی کرده و کمی منتظر بمانید. سپس مرورگر ویندوز خود را باز نموده و به قسمت Network Neighborhood بروید. در آنجا باید ماشین HOBBIT را مشاهده نمایید. با فشار روی شمایل آن، می‌توانید داده‌های به اشتراک گذاشته شده روی آن را مشاهده کنید. در آنجا شاخه export/ قابل مشاهـده خواهد بود.

۲-۳- مثال۲: راه اندازی یک کارساز خواندن-نوشتن سند[2] :

این مثال کمی پیشرفته‌تر از مثال قبلی است. تفاوت در اینجاست که دسترسی به منابع مشترک فقط از طریق یک کاربر خاص و گروهی که آن کاربر به آن متعلق است امکان‌پذیر خواهد بود. برای این کار باید آن کاربر مثلاً همان Jackb در مثال قبلی را به پرونده smbpasswd اضافه کنیم. پس ابتدا دستورات زیر را وارد نمایید:

[1] Workgroup
[2] Read–write Document Server

```
# smbpasswd -a Jackb
New SMB password : m03paln
Retype new SMB password : m03paln
Added user Jackb.
```

سپس پرونده smb.conf را به صورت زیر اصلاح کنید:

```
# Global parameters
[global]
workgroup = MIDEARTH
netbios name = HOBBIT
security = SHARE
[data]
comment = Data
path = /export
force user = Jackb
force group = users
read only = No
guest ok = yes
```

همانطور که مشاهده می‌کنید با استفاده از پارامترهای force user، force group و guest ok دسترسی به پرونده کارساز را محدود کرده‌ایم.

۲-۴- مثال ۳: راه اندازی یک کارساز چاپ

ساده‌ترین کارساز چاپ هم به نصب نرم‌افزار راه‌انداز صحیح چاپگر روی ایستگاه‌های کاری تحت ویندوز نیاز دارد. کارساز چاپ در واقع طوری طراحی شده است که تمام کارهای مربوط به چاپ رابه spooler می‌فرستد و spooler نیز باید طوری تنظیم شده باشد که این کارها را به نوبت به چاپگر ارسال کند، بدون اینکه کمترین فرآیندی یا فیلتری روی آنها انجام دهد. در این مثال به بررسی ویزارد مربوط به اضافه کردن چاپگر نمی‌پردازیم. برای داشتن یک کارساز چاپ ساده باید پرونده smb.conf را به صورت زیر تنظیم نمائیم:

```
# Global parameters
[global]
Workgroup = MIDEARTH
netbios name = LUTIEN
security = Share
printcap name = cups
disable spools = yes
show add printer wizard = No
printing = cups
[data]
comment =All printers
path = /var/spool/samba
guest ok = yes
```

printable = yes
use client driver = yes
browseable = No

مثال فوق یک مثال خیلی ساده و شاید کمی غیر واقعی است. اما کار چاپ را انجام می‌دهد.
در ضمن شما باید مطمئن شوید که شاخه /var/spool/samba همان طور که انتظار دارید ظرفیت پذیرش کارهای چاپ ومجوزهای لازم برای این کار را دارد. برای این منظور باید به صورت زیر عمل نمائید:
شاخه مورد نظر باید تحت مالکیت superuser یا همان root باشد. هم گروه آن و هم کاربر آن:

```
# chown  root.root  /var/spool/samba
```

مجوزهای شاخه باید برای همه به صورت read-write با تنظیم sticky-bit باشد:

```
# chmod  a+rw TX  /var/spool/samba
```

۲-۵- مثال ۴: راه اندازی یک کارساز پرونده و چاپ امن

در اینجا یک مثال پیچیده‌تر می‌کنیم. کارساز جدید یک محیط ذخیره داده خواهد بود که فقط کاربران احرازهویت شده (مثل کاربران محلی سامانه) می‌توانند پرونده‌هایی را در آن ذخیره کنند؛ مثل یک home directory. در ضمن یک چاپگری خواهیم داشت که باید برای تمام کاربران قابل‌دسترسی باشد. کاربران این محیط فرضی jack Baumbach و Amed Sehkah وMary Orville هستند و هر کدام یک کلمهٔعبور برای خود دارند. مدیر چاپ و محیط ذخیره داده نیز کاربر Mary خواهد بود. سطح امنیت را روی سطح امنیتی کاربر –که همان پیش‌فرض است– می‌گذاریم. سپس کارهای زیر را انجام می‌دهیم:
کاربران را به صورت زیر به سامانه عامل اضافه می‌کنیم:

```
# useradd  -c  " Jack Bumbach" -m   -g   users  -p  m0r3paln Jackb
# useradd  -c  " Mary orville "   -m   -g   users  -p  secret maryo
# useradd  -c  " Amed sehkah"  -m   -g   users  -p  secret ameds
```

پرونده smb.conf را به صورت زیر تنظیم می‌کنیم:

```
# Global parameters
[global]
workgroup = MIDEARTH
netbios name = OLORIN
printcap name = cups
disable spools = yes
show add printer wizard = No
printing = cups
[data]
```

comment = Home Directories
valid users = %S
read only = No
browseable = No
[public]
comment = Data
path = /export
force user = maryo
force group = users
guest ok = yes
[printers]
comment = All printers
path = /var/spool/samba
printer admin = root,, maryo
create mask = 0600
guest ok = yes
printable = yes
use client driver = yes
browseable = No

اضافه کردن کاربران مورد نظر به پایگاه داده کلمات عبور ویندوز:

smbpasswd -a root

password = Bigsecret

smbpasswd -a Jackb

password = m0r3paln

smbpasswd -a maryo

password = secret

smbpasswd -a ameds

password = mysecret

با دستورات مناسب سامبا را راه اندازی کنید:

nmbd; smbd;

تنظیم شاخه export/ :

mkdir /export

chown maryo.users /export

chown   u=rwx , g=rwx , o-rwx /export

بررسی کنید که آیا سامبا به درستی در حال اجراست یا خیر:

```
# smbclient  –L  localhost  –U %

Domain=[MIDEARTH] OS=[UNIX] Server=[Samba-3.0.0]

Sharename       Type      Comment
---------       ----      -------
public          Disk      Data
IPC$            IPC       IPC Service (Samba-3.0.0)
ADMIN$          IPC       IPC Service (Samba-3.0.0)
hplj4           Printer   hplj4

Server               Comment
---------            -------
OLORIN               Samba-3.0.0

Workgroup            Master
---------            -------
MIDEARTH             OLORIN
```

با کاربرmaryo به ماشین OROLIN وصل شوید:

```
# smbclient   //oroline/maryo  –Umaryo% secret

OS=[UNIX] Server=[Samba-3.0.0]
smb: \> dir
.                           D        0  Sat Jun 21 10:58:16 2003
..                          D        0  Sat Jun 21 10:54:32 2003
Documents                    D        0  Fri Apr 25 13:23:58 2003
DOCWORK                      D        0  Sat Jun 14 15:40:34 2003
OpenOffice.org               D        0  Fri Apr 25 13:55:16 2003
.bashrc                      H     1286  Fri Apr 25 13:23:58 2003
.netscape6                  DH        0  Fri Apr 25 13:55:13 2003
.mozilla                    DH        0  Wed Mar  5 11:50:50 2003
.kermrc                      H      164  Fri Apr 25 13:23:58 2003
.acrobat                    DH        0  Fri Apr 25 15:41:02 2003

      55817 blocks of size 524288. 34725 blocks available
smb: \> q
```

۲-۶- مثال ۵: کارساز دامنه اعضا[1]

در یک اداره با شرکت حسابداری می‌خواهیم یک نرم‌افزار به نام SpytFall –که به خاطر محدودیت مجوز– فقط روی یک کارساز نصب و در حال اجراست روی یک کارساز کاربردی[2] مرکزی قرار بگیرد. مدیر بخش نیز کاربر maryo است. تمام کارمندان باید یک شاخه home و امکان چاپ را داشته باشند. درضمن سامانه حسابداری تنها یک کارساز به نام valinor خواهد داشت و اطلاعات کاربران نیز روی کنترل‌کننده دامنه قرار دارد و زیر نظر آن چاپ می‌شود. برای تنظیم و راه‌اندازی این کارساز باید به نکات زیر توجه داشته باشید:

هیچ کاربری را به کارساز لینوکس اضافه نکنید، زیرا تمام این کارها بر عهده دامنه مرکزی خواهد بود.

پرونده smb.conf را به صورت زیر تنظیم کنیم:

```
[global]
workgroup = MIDEARTH
netbios name = VALINOR
security = DOMAIN
printcap name = cups
disable spools = yes
show add printer wizard = No
idmap uid = 15000-20000
idmap gid = 15000-20000
winbind seperator = +
winbind use default Domain = yes
use send file = yes
printinf = cups
[homes]
comment = Home Directories
valid users = %S
read only = No
browseable = No
```

[1] Domain Member Server
[2] Application Server

```
[ spytfull ]
comment = Accounting Application only
path = /export/spytfull
valid users = @ Accounts
admin users = maryo
read only = yes
[ public]
comment = Data
path = /export/ public
read only = No
[ printers]
comment = All printers
path = /var/spool/samba
printer admin = root , maryo
create mask = 0600
guest ok = yes
printable = yes
use client driver = yes
browseable = No
```

باید با دامنه مربوطه اتصال[1] حاصل کنید (توجه کنید که حتماً این مرحله کامل شود، سپس خدمت[2] سامبا را راه اندازی کنید.)

```
# net    rpc   join –U root% 'bigsecret '

Joined domain MIDEARTH.
```

از غیر فعال بودن دایمون nscd روی سامانه‌ای که winbind روی آن تنظیم شده و در حال اجراست مطمئن شوید. نکته دیگری که باید به آن توجه داشته باشید آن است که نسبت به نسخه سامبای مورد استفاده، دستور ملحق شدن به یک دامنه ممکن است متفاوت باشد. در این مورد در بخشهای بعدی به تفصیل صحبت خواهد شد.

[1] Join
[2] Service

خدمت سامبا را راه اندازی کنید.

باید پرونده /etc/nsswitch.conf را ویرایش کنید و تغییرات زیر را در آن بدهید، این تغییرات به منظور انجام عمل تطبیق[1] نام گروه و کاربر در winbind است.

```
passwd:  files winbind
group:  files winbind
hosts:  files  dns  winbind
```

باید یک کلمه عبور برای استفاده wbinfo اختصاص دهید:

```
# wbinfo  --set-auth-user=root%' bigsecret '
```

با اجرای دستورات زیر بررسی کنید که آیا اعتبارات کاربران و گروه‌ها به درستی منطبق می‌شود یا خیر:

```
# wbinfo  −u
MIDEARTH+maryo
MIDEARTH+Jackb
MIDEARTH+ameds
…
MIDEARTH+root
# wbinfo -g
MIDEARTH+Domain Users
MIDEARTH+Domain Admins
MIDEARTH+Domain Guests
…
MIDEARTH+Accounts
```

بررسی کنید که آیا winbind به درستی کار می‌کند یا خیر. با استفاده از getent می‌توان صحت انجام username resolving را بررسی کرد:

```
# getent passwd maryo
maryo:x:15003:15003:Mary Orville:/home/MIDEARTH/maryo:/bin/false
```

دستورات زیر را انجام دهید:

```
# touch /export/a_file
```

[1] Resolve

```
# chown maryo  /export/a_file
# ls  -la  /export/a_file
…
-rw-r--r--     1  maryo   users     11234 Jun  21 15:32      a_file
…
# rm  /export/a_file
```

تا اینجا تقریباً تنظیمات را به طور کامل انجام داده‌اید. حال فقط باید ساختار شاخه این وب‌گاه را تنظیم کنید:

```
# mkdir -p  /export/{spytfull, public}
# chmod ug=rwxS,o=x   /export/{spytfull, public}
# chown  maryo.Accounts  /export/{ spytfull, public}
```

بدین ترتیب کلیه مراحل را تکمیل نموده‌اید.

فصل سوم
سطوح امنیتی در سامبا و انواع مختلف کارسازها

۳-۱- مقدمه

در این فصل می‌خواهیم انواع کارسازهایی که سامبا می‌تواند طبق آن تنظیم شود را توضیح دهیم. همچنین مرور مختصری بر سطوح امنیتی که سامبا قادر به برقراری آنها است و به چگونگی ارتباط کارخواه‌ها تحت ویندوز با سامبا در این حالتها می‌پردازیم.

۳-۲- انواع کارسازها

اغلب مدیران شبکه‌های ویندوز کارسازها را شامل سه دسته زیر می‌دانند:

- کنترل‌کننده دامنه (Doamin Controller)
  - کنترل‌کننده اولیه دامنه (Primary Doamin Controller)
  - کنترل‌کننده پشتیبان دامنه (Backup Domain Controller)
  - کنترل‌کننده ADS دامنه (ADS Domain Controller)
- کارساز دامنه اعضا (Domain Member Server)
  - کارساز AD دامنه (Active Directory Domain server)
  - کارساز سبک NT4 دامنه (NT4 Style Domain Server)
- کارساز خود اتکا (Stand-alone Server)

۳-۳- سطوح امنیتی در سامبا

هدف انواع مختلف سطوح امنیتی در کارساز سامبا چگونگی برقراری آن با کارخواه‌ها و نیز اعمال سیاستهای امنیتی مورد نظر توسط مدیران سامانه است. در دنیای شبکه‌ای SMB/CIFS فقط دو نوع سطح امنیتی وجود دارد:

- سطح امنیتی کاربر (User level Security)
- سطح امنیتی مشترک (Share level Security)

در واقع سطح امنیتی کاربر به چهار صورت پیاده‌سازی می‌شود و سطح امنیتی مشترک فقط به یک صورت می‌توان پیاده سازی کرد. جمعاً به این پنج روش مختلف پیاده‌سازی حالتهای امنیتی[1] گفته می‌شود و عبارتند از:

SERVER , ADS , DOMAIN , USER , SHARE

این سطوح مختلف را یک‌به‌یک شرح خواهیم داد. در واقع هنگامی که یک کارخواه سامبا بالا می‌آید، باید به کارساز سامبا بگوید که در چه سطح امنیتی کار می‌کند، سطح مشترک[1] یا سطح کاربر. طبق سطح امنیتی که کارخواه دارد باید خودش را برای کارساز معرفی کند.

[1] Security Modes

۳-۳-۱- سطح امنیتی کاربر (User level Security)

ساده‌ترین نوع سطح امنیتی، سطح امنیتی کاربر است. در اینجا کارخواه درخواست برقراری یک نشست[۲] را به کارساز می‌فرستد. در این درخواست نام کاربر و کلمهٔعبور نیز فرستاده می‌شود. کارساز سامبا می‌تواند این درخواست را با کلمهٔعبور و نام کاربر قبول یا رد نماید. در سطح امنیتی کاربر کارساز نمی‌تواند هیچ دخالتی در اینکه کارخواه به چه منبعی دسترسی پیدا می‌کند، داشته باشد و در واقع تنها معیار قبول و رد درخواست کارخواه فقط دو چیز است:

- نام کاربری و کلمهٔ عبور
- نام ماشین کارخواه

اگر کارساز این درخواست را قبول کند، کارخواه می‌تواند بدون دادن هیچ کلمهٔعبور دیگری منابع به اشتراک گذاشته شده را برای خود سوار کند، چون فرض بر این است که کلیهٔ حقوق و مجوزهای دسترسی در برقراری و تشکیل یک نشست به کارخواه داده شود.

همچنین ممکن است از سوی کارخواه چند درخواست تشکیل نشست ارسال شود. کارساز با قبول یک درخواست تشکیل نشست به کارخواه یک شناسه کاربری[۳] اختصاص می‌دهد که به عنوان پارامتر احرازهویت برای نام کاربر و کلمهٔعبور دریافت شده در نظر گرفته خواهد شد. بنابراین کارخواه به راحتی می‌تواند از همین شناسه کاربری برای نشستهای بعدی نیز استفاده کند. یک برنامه کاربردی که این کار را انجام می‌دهد WinDD نام دارد.

نحوهٔ تنظیم امنیت در سطح کاربر به این ترتیب است که باید در پرونده smb.conf، پارامتر security را به user مقداردهی کنید:

```
Security = user
```

نکته: از زمان samba-2-2.x پیش‌فرض سامانه user است.

۳-۳-۲- سطح امنیتی مشترک (Share level Security)

در این نوع تنظیم امنیت، هر کارخواه باید برای هر منبع به اشتراک گذاشته شده به طور جداگانه احرازهویت شود. در واقع برای استفاده از هر منبع مشترک باید یک کلمهٔعبور داشته باشد. نحوهٔ تنظیم در پرونده smb.conf به صورت زیر است:

```
security = share
```

---

[1] Share level
[2] Session
[3] UID

۳-۳-۳- سطح امنیتی دامنه (User level Security)

وقتی سامبا در حالت دامنه کار می‌کند، به این معنی است که کارساز سامبا یک حساب در یک دامنه دارد که تمام درخواستهای احرازهویت را به کنترل‌کننده دامنه[1] آن ارسال می‌کند. به عبارت دیگر با این تنظیم کارساز سامبا به عنوان عضوی از یک دامنه محسوب خواهد شد.

نحوه تنظیم :

به پرونده smb.conf رفته و تنظیمات زیر را انجام دهید:

```
security = domain
workgroup = MIDEARTH
```

برای اینکه این تنظیمات به درستی عمل کند، باید به دامنه مربوطه متصل[2] شوید. برای اتصال به دامنه کارهای زیر را انجام دهید:

روی کنترل‌کننده دامنه Win NT با استفاده از مدیر کارساز[3] یک حساب به نام ماشین کارساز سامبا ایجاد کنید.

روی سامانه لینوکس خود دستور زیر را اجرا نمائید:

```
# net rpc join -U administrator%password
```

نکته: در نسخه‌های سامبای ۲-۲-۴ و بعد از آن به طور خودکار می‌توان با دستور زیر به NT4-Style domain متصل شد:

```
# Smbpasswd -j DOMAIN-NAME -r PDC-NAME \ -U Administrator%password
```

در سامبای نسخه ۳ همین کار با اجرای دستور زیر انجام می‌شود:

```
# net rpc join –U Administrator%password
```

بنابراین لزومی به مشخص کردن نام دامنه یا PDC-NAME نیست و این تنظیمات در پرونده smb.conf انجام می‌شود.

وقتی از این مد استفاده می‌کنیم به یک حساب کاربری لینوکسی استاندارد برای هر کاربر نیاز داریم تا به یک شناسه کاربری احرازهویت شده توسط windows DC اختصاص یابد. برای جزئیات بیشتر به فصل عضویت دامنه[4] مراجعه کنید.

۳-۳-۴- سطح امنیتی ADS

سامبای ۲،۲ و ۳ هر دو می‌توانند به Active Directory Domain متصل شوند. البته هنگام یکه دامنه در حالت Native در حال اجرا باشد. Active Directory در حالت Native به تمام عضوهای دامنه با سامانه‌عامل NT4-Style اجازهٔ کار می‌دهد و فقط به ابزارهای کنترل‌کننده پشتیبان دامنه‌ای که

---

[1] Domain Controller
[2] Join
[3] Server Manager
[4] Domain Membership

NT4-Style هستند اجازهٔ کار نمی‌دهد. برای تنظیم سامبا در این حالت باید پرونده smb.conf را به صورت زیر تغییر دهید:

realm = your.kerberos.REALM

security = ADS

همچنین ممکن است به پارامتر زیر نیاز داشته باشید:

password server = your.kerberos.server

۳-۳-۵- سطح امنیتی کارساز

این پارامتر هنگامی مورد استفاده قرار می‌گیرد که کارساز سامبا به عنوان عضو کارسازی دامنه عمل کند. اکیداً توصیه می‌شود که از این پارامتر استفاده نشود. در واقع سطح امنیتی کارساز دارای مضرّات و مشکلات زیر است:

- پتانسیل تحریم حساب کاربری روی Windows NT4/200x password server.
- عدم اطمینان از کلمه عبوری که برای کارساز تعیین شده است.
- با Winbind نمی‌تواند کار کند و این به ویژه هنگامی که می‌خواهیم profile ها را از راه دور ذخیره کنیم، مشکل‌ساز می‌شود.
- این حالت ممکن است باعث شود اتصالاتی با کارساز کلمه عبور برقرار شود و آن را برای مدت طولانی باز نگه دارد.
- وقتی کارساز راه‌دور کلمه عبور به طور ناگهانی خاموش شود، امنیت کارساز سامبا به خطر می‌افتد.

در زیر تنظیمات مربوط به این حالت آورده شده است:

Encrypt passwords = yes

Security = server

Password server = "NetBIOS_name_of_a_DC"

فصل چهارم
کارساز خوداتکا
۴-۱- مقدمه

در این فصل سعی در معرفی کارساز خود اتکا[1] داریم. این کارسازها کاملاً از دامنه کنترل‌کننده‌های روی یک شبکه مستقل هستند و عضو دامنه نیستند و بیشتر شبیه کارسازهای یک گروه کاری عمل می‌کنند. یک کارساز خوداتکا می‌تواند با ملاحظات امنیتی و یا بدون آن پیاده‌سازی شود. در اغلب موارد یک کارساز خوداتکا با حداقل کنترلهای امنیتی تنظیم می‌شود که در نتیجهٔ آن تمام کاربران به داده‌های موجود روی آن دسترسی خواهند داشت.

اگر به یک کارساز-پرونده[2] فقط خواندنی یا به یک کارساز چاپ نیاز دارید، تنظیماتی که باید انجام دهید، پیچیده نخواهد بود. فرض کنید در یک اداره‌ای می‌خواهیم نقشه‌ها و پرونده‌های اطلاعاتی قدیمی را نگهداری کنیم. هیچکس حق نوشتن یا تغییر پرونده روی کارساز را ندارد. در این شرایط، بهترین راه حل استفاده از یک کارساز خوداتکا فقط خواندنی، که در حالت مشترک کار می‌کند، خواهد بود.

یک کارساز خوداتکا برای تمام منابع قابل دسترس از روی آن، تصدیق اصالت و کنترل دسترسی را به صورت محلی[3] فراهم می‌کند. برای این کار یک پایگاه داده از کاربران محلی وجود خواهد داشت. به عبارت دیگر، منابع موجود روی آن سامانه یا در حالت مشترک و یا در حالت کاربر قابل دسترس خواهند شد. بنابراین برای تنظیم آن، ایجاد کاربران تنها کار لازم است. البته با کارسازهای خوداتکا هیچ خدمتی برای ورود[4] روی شبکه ارائه نخواهد شد. یعنی ماشینهایی که از این کارساز استفاده می‌کند هیچ عمل ورود را روی دامنه انجام نمی‌دهند. هر چند لازم است که هر کاربر شبکه‌ای نام کاربرش با نام کاربری محلی روی کارساز مذکور منطبق باشد. یعنی روی کارساز یک عمل انطباق بین آنها انجام شود. چندین راه برای این کار وجود دارد:

پایگاه داده مربوط به احرازهویت کاربران به چند صورت می‌تواند باشد: یا به صورت محلی و یا یک کارساز راه‌دور[5] و یا حتی از طریق پروتکل SMB روی کارسازی که اصلاً عضوی از امنیت دامنه نیست.

به‌خاطر استفاده از[6] PAM و همچنین NSSWITCH (Name Service Switcher) که پایگاه داده مربوط به کاربران لینوکس است، منبع احرازهویت ممکن است روی کارساز دیگری باشد. اگر ما بخواهیم آن کارساز را فراخوانی کنیم، کارساز سامبا ممکن است از پایگاه داده کلمات‌عبور سامانه محلی لینوکس استفاده کند که در یا پرونده‌های /etc/passwd و /etc/shadow قرار دارد و یا ممکن

---

[1] Stand–alone Server
[2] File-Server
[3] Local
[4] Login
[5] Remote server
[6] Pluggable Authentication Modules

است از پرونده smbpasswd local یا LDAP و یا حتی از PAM و winbind روی یک کارساز CIFS/SMB دیگری استفاده کند.

۴-۲- کارساز سند[1] و کارساز چاپ[2] مرکزی

۴-۲-۱- کارساز سند

می‌خواهیم یک کارساز سند داشته باشیم. برای تنظیمات مربوط به آن در پرونده smb.conf باید تغییرات زیر را اعمال کنیم. فرض می‌کنیم که تمام مستندات در شاخه export/ قرار دارد. هیچ home directory به صورت مشترک وجود ندارد و کاربری نیز در پایگاه داده سامانه تحت لینوکس /etc/passwd وجود ندارد. پس:

```
# Global parameters
[global]
workgroup=MIDEARTH
netbios name =GANDALF
security= SHARE
passdb backend= guest
wins Server = 192.168.1.1
[data]
comment =Data
path=/export
guest only= Yes
```

در مثال فوق نام ماشین GANDALF است و گروه‌کاری آن نیز به MIDEARTH تنظیم شده است. بنابراین ماشین مورد نظر با سامانه‌های دیگر در یک جا ظاهر می‌شوند. با توجه به passdb backend که به guest تنظیم شده اجازهٔ دسترسی به همهٔ کاربران ناشناس داده شده است. یک WINS Server نیز به این منظور در شبکه ایجاد کرده‌ایم.

۴-۲-۲- کارساز چاپ مرکزی

برای داشتن خدمت چاپ نیز باید کارهای زیر را انجام دهیم؛ فرض کنید:

- کارساز چاپ نباید به مدیریتی نیاز داشته باشد.
- سامانه print spooling & processing روی کارساز چاپ مورد نظر، CUPS خواهد بود.
- این کارساز چاپ، فقط به چاپگرهای شبکه خدمت می‌دهد و مدیر شبکه باید تنظیمات مربوط به CUPS را برای چاپگرهای شبکه به درستی انجام دهد.
- همهٔ کارخواه‌ها فقط از نرم‌افزار راه‌اندازهای Postscript استفاده خواهند کرد.

در این مثال، کارساز چاپ هر کار[1] مربوط به چاپی را که دریافت می‌کند در /var/spool/samba جمع خواهد کرد تا در زمان مناسب که نوبت آن فرا رسید توسط پردازشگر چاپ CUPS سامبا پذیرفته شود. چون تمام اتصالات نیز توسط کاربران مهمان (guest) ایجاد می‌شود، دو چیز نیاز است:

[1] Document Server
[2] Print Server

در سامانه عامل لینوکس باید یک حساب کاربری برای guest داشته باشیم. معمولاً نام پیش‌فرض آن nobody خواهد بود. اگر می‌خواهید دقیقاً نامی که برای این حساب کاربری به‌طور پیش‌فرض در نسخهٔ سامبای در نظر گرفته شده را بدانید؛ دستور زیر را اجرا کنید:

```
$ testparm -s  -v | grep "guest account"
```

و مطمئن شوید که این کاربر در پایگاه داده (/etc/passwd) وجود دارد.

شاخه که سامبا می‌خواهد کارهای مربوط به چاپ را در آن نگهداری کند، باید دارای مجوز نوشتن برای کاربر guest باشد. با استفاده از دستورات زیر این کار را انجام دهید:

```
# mkdir /var/spool/samba

# chown nobody.nobody /var/spool/samba

# chmod a+rwt /var/spool/samba
```

سپس تغییرات لازم در پرونده smb.conf را مانند زیر انجام دهید:

```
# Global parameters
[global]
workgroup=MIDEARTH
netbios name =GANDALF
security=SHARE
passdb backend =guest
printing = cups
printcap name = cups
[ printers]
comment = All printers
path = /var/spool/samba
printer admin = root
guest ok = Yes
printable = Yes
use client driver = Yes
browseable = No
```

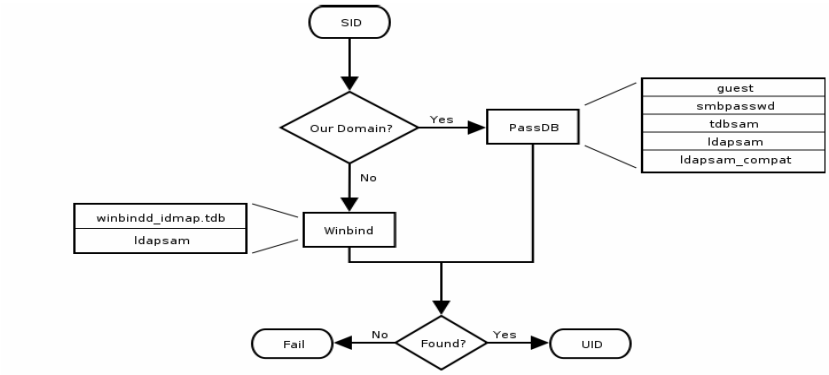
[1] job

فصل پنجم
پایگاه های داده مربوط به اطلاعات حسابها
۵-۱- مقدمه

در نسخه‌های قدیمی ویندوز، معمولاً کارخواه‌ها کلمات‌عبور را در طول شبکه و رسانه‌های[1] مورد استفاده خود به صورت متن ساده[2] یا رمز نشده، می‌فرستادند. سامبا با دریافت آنها و سپس رمزکردن کلمات‌عبور، نتیجه به‌دست آمده را با کلمات‌عبوری که در پایگاه داده کاربران لینوکس به صورت کد شده با الگوریتم hash نگهداری می‌شد، مقایسه می‌کرد.

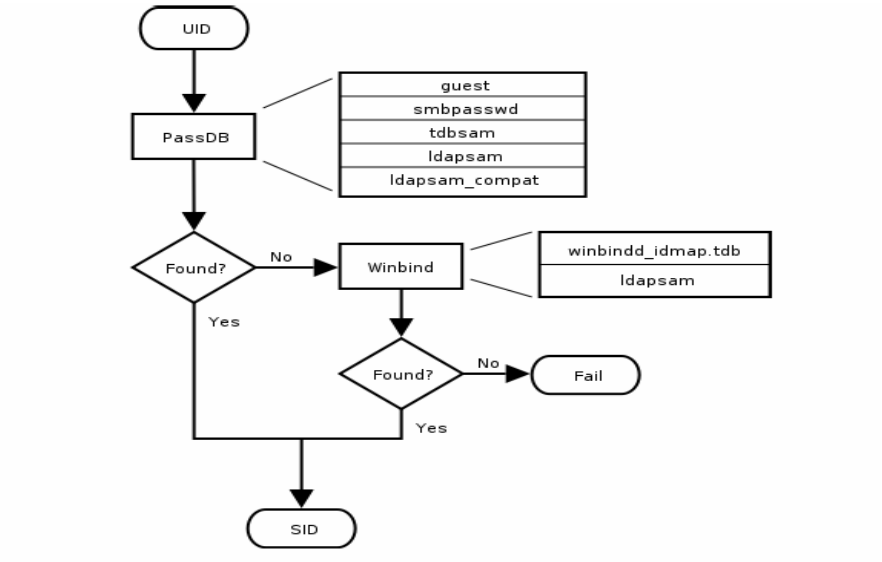
در ویندوزهایی که بعد از آنها روانه بازار شدند، روش کمی فرق کرد. در آنها کارخواه‌ها کلمات‌عبور را به صورت رمز شده روی شبکه می‌فرستادند. این کلمات عبور نمی‌توانند به کلمات رمز شده لینوکسی تبدیل شوند. به همین دلیل نمی‌توان از پایگاه داده استاندارد کاربران تحت لینوکس استفاده کرد و مجبوریم کلمات‌عبور را در جایی دیگر مثل LanMan و NT hashes نگهداری کنیم. بنابراین برای هر کاربر دو حساب کاربری داریم: یکی روی لینوکس و دیگری به عنوان حساب کاربری سامبا روی ویندوز. برای اینکه سامبا بتواند به طور صحیح کار کند، این دو باید بتوانند به هم تبدیل شوند. در واقع تبدیل این دو به هم پایهٔ کار سامبا است. حساب کاربری مربوط بـــه ویندوز را بـــا SID[3] و حساب کاربری مربوط بـــه لینوکس را بـا UID[4] می‌شناسیم. اگر winbindd در حال اجرا نباشد یا امکان تماس با آن وجود نداشته باشد، فقط یک map به صورت محلی بین SID و UID انجام می‌پذیرد.

دو نمودار ارائه شده مراحل انجام عملیات تبدیلSID بهUID و نیزUID بهSID را نشان می‌دهد:



IDMAP: Resolution of SIDs to UIDs.

[1] Media
[2] Plain text
[3] Security Identifier
[4] User Identifier



IDAMP: Resolution of UIDs to SIDs.

به نظر می‌رسد که فنون رمزنگاری در لینوکس و SMB برای کلمات‌عبور شبیه به هم باشند. این شباهت به طور کاملاً ظاهری و سطحی است. در لینوکس معمولاً وقتی کاربری وارد سیستم می‌شود، کلمهٔ‌عبور آن به صورت متن ساده روی شبکه فرستاده می‌شود که این کار اصلاً صحیح نیست. در SMB هرگز کلمهٔ‌عبوری به صورت متن ساده فرستاده نمی‌شود. بلکه قبل از فرستادن رمز می‌شود. اما مقدار آن به صورت یک hash شانزده بایتی روی دیسک ذخیره می‌شود. این کار نیز درست نیست؛ چون شانزده بایت hash شده معادل کلمات‌عبور است. درست است که نمی‌توان از روی آنها کلمهٔ‌عبور را تشخیص داد، اما به راحتی می‌توان از آنها برای شبیه سازی یک اتصال[1] و یا جازدن به جای یک کارخواه برای دسترسی به کارساز استفاده کرد. بنابراین باید بتوان با استفاده از فنون مناسبی از بروز حملاتی از این قبیل جلوگیری نمود. یعنی پرونده کلمات‌عبور باید کاملاً مخفی و محافظت شده باشد. در حالت ایده‌آل نباید کلمه‌های عبور به صورت متن ساده نه روی شبکه و نه روی دیسک نگهداری شوند.

۵-۲- مزیت کلمات عبور رمز شده

۱ـ کلمات‌عبور به صورت متن ساده در شبکه رد و بدل نمی‌شوند. این مانع از سوءاستفاده دیگران توسط برنامه‌های ثبت کلمه عبور مثل sniffer می‌شود.

۲ـ کلمات‌عبور به صورت متن ساده در حافظه و یا دیسک ذخیره نمی‌شوند.

[1] Connection

۳ـ با استفاده از کلمات‌عبور رمز شده امکان برقراری مجدد ارتباط به صورت خودکار برای منابع مشترک وجود دارد.

۴ـ کلمات عبور رمز شده اساس عملکرد PDC/BDC هستند.

۵-۳- مزیت کلمات عبور با متن ساده

۱ـ کلمات عبور به صورت متن ساده نه روی دیسک نگهداری می‌شوند و نه Cache می‌شوند.

۲ـ از همان پرونده کلمات عبور برای خدمات دیگر لینوکس مثل ورود و FTP می‌توان استفاده کرد.

۳ـ ....

۵-۴- تطبیق[1] بین شناسه‌های کاربری ویندوز و لینوکس

همان طور که گفته شد، هر عملیاتی در لینوکس نیاز به یک UID دارد، درست مانند ویندوز که به یک SID نیاز دارد و سامبا برای انجام کار خود باید بتواند این دو را به یکدیگر منطبق کند، برای این کار دو روش فراهم کرده است:

اول اینکه تمام حسابهای کاربری SAM[2] در سامبا به یک UID در لینوکس نیاز دارند که به آن منطبق شوند. وقتی یک کاربر به پایگاه داده مربوط به حساب ها اضافه می‌شود، سامبا واسط مربوط به دست‌نوشته اضافه کردن کاربر را برای ایجاد کاربر در سامانه عامل میزبان سامبا فرامی‌خواند. در اصل تمام حسابهای کاربری در Local SAM به یک حساب کاربری محلی نیاز دارند.

راه دوم نگاشت[3] بین UID و SID از طریق پارامترهایidmap gid، idmap uid درپرونده smb.conf است. وجود این پارامترها زمانی که کاربران از یک کارساز SAM راه دور می‌خواهند map شوند، ضروری است. برای اطلاعات بیشتر به پرونده smb.conf و صفحه‌های راهنمای[4] آن مراجعه کنید.

۵-۵- ابزارهای مدیریت حساب[5]

سامبا برای مدیریت و نظارت حسابهای کاربران و ماشینها دو ابزار در اختیار دارد، این دو ابزار عبارتند از pdbedit، smbpasswd که در ادامه به بررسی عملکرد این دو ابزار می‌پردازیم.

۵-۵-۱- دستور smbpasswd

عملکرد برنامهٔ smbpasswd شبیه به برنامه‌های passwd و yppasswd است. smbpasswd، دو حوزه[6] ۳۲ بایتی password در پایگاه داده مربوط به کلمات عبور نگه می‌دارد و در حالت کارساز- کارخواه کار می‌کند. به این ترتیب که با smbd محلی برای تغییر کلمهٔعبور کاربر تماس می‌گیرد. این روش مزایای بی‌شماری دارد.

---

[1] Resolve
[2] Security Account Manager Database
[3] Mapping
[4] Man Page
[5] Account
[6] Field

Smbpasswd توانایی و قابلیت تغییر کلمهٔعبور روی کارسازهای ویندوزNT را دارد. (البته این کار فقط زمانی امکان‌پذیر است که درخواست به NT PDC فرستاده شود و جهت تغییر کلمهٔعبور کاربری روی دامنه NT باشد).

از Smbpasswd برای انجام کارهای زیر می‌توان استفاده کرد:

ـ اضافه کردن یک کاربر یا ماشین.
ـ حذف یک کاربر یا ماشین.
ـ فعال کردن یک کاربر یا ماشین.
ـ غیرفعال کردن یک کاربر یا ماشین.
ـ تنظیم کلمه عبور کاربر به NULL.
ـ مدیریت interdomain trust account.

برای استفاده و اجرای Smbpasswd به صورت زیر عمل می‌کنیم:

```
$ Smbpasswd
Old SMB password : secret
```

که در واقع secret کلمه عبور قدیمی است و سپس باید به درخواست تایپ کلمهٔعبور جدید پاسخ دهید:

```
New SMB password : new secret
Retype New SMB password : new secret
```

وقتی با کاربری عادی اقدام به اجرای Smbpasswd کنید، فقط کلمهٔعبور خود را می‌توانید تغییر دهید. ولی هنگامیکه با root آن را اجرا کنید، باید نام کاربری را که می‌خواهید کلمه عبورش را عوض کنید بدهید و سپس بدون سؤال دربارهٔ کلمهٔعبور قدیمی اجازه تغییر کلمهٔعبور را دارید. این کار برای زمانی که کاربران کلمهٔ عبور خود را فراموش کرده‌اند مفید است.

همان طور که مشاهده شد، Smbpasswd مانند passwd, yppasswd عمل می‌کند.

۵-۵-۲- دستور pdbedit

pdbedit فقط توسط root می‌تواند استفاده شود و برای مدیریت پایگاه داده کلمات‌عبور طراحی شده است. Pddbedit کارهای زیر را می‌تواند انجام دهد:

ـ افزودن، حذف و تغییر حسابهای کاربران.
ـ لیست نمودن حسابهای کاربران.
ـ انتقال حسابهای کاربران

درواقع pddbedit قادر به انجام عملیاتی است که Smbpasswd انجام می‌داد. یک مثال را در زیر بینید:

```
$ pdbedit -Lv met
UNIX username:        met
NT username:
Account Flags:        [UX         ]
User SID:             S-1-5-21-1449123459-1407424037-3116680435-2004
Primary Group SID:    S-1-5-21-1449123459-1407424037-3116680435-1201
Full Name:            Melissa E Terpstra
Home Directory:       \\frodo\met\Win9Profile
HomeDir Drive:        H:
Logon Script:         scripts\logon.bat
Profile Path:         \\frodo\Profiles\met
Domain:               MIDEARTH
Account desc:
Workstations:         melbelle
Munged dial:
Logon time:           0
Logoff time:          Mon, 18 Jan 2038 20:14:07 GMT
Kickoff time:         Mon, 18 Jan 2038 20:14:07 GMT
Password last set:    Sat, 14 Dec 2002 14:37:03 GMT
Password can change:  Sat, 14 Dec 2002 14:37:03 GMT
Password must change: Mon, 18 Jan 2038 20:14:07 GMT
```

یک هدف مهم و خاص pdbedit اجازه انتقال اطلاعات مربوط به حسابها از یک passdb به دیگری است. به عنوان مثال برای انتقال حسابها از یک پایگاه داده قدیمی Smbpasswd به tdbsam backend می‌توان کارهای زیر را انجام داد:

۱ـ پارامتر passdb backend را به Smbpasswd , tdbsam تنظیم کنید:

```
passdb backend = tdbsam , Smbpasswd
```

۲ـ دستور زیر را اجرا کنید:

```
# pdbedit  -i  Smbpasswd -e tdbsam
```

۳ـ حال باید Smbpasswd را از پارامتر passdb backend در پرونده smb.conf حذف کنید.

فصل ششم
کنترل دسترسی به پرونده‌ها و شاخه‌ها و منابع اشتراکی

۶-۱- مقدمه

یادآوری این نکته لازم است که سامبا به منظور تعامل و تبادل اطلاعات بین دو محیط یا سامانه عامل مختلف ایجاد شده است. توجه کنید که هدف سامبا تغییر لینوکس به بستر ویندوز نیست، بلکه فراهم نمودن یک سطح تبادل خوب از اطلاعات بین این دو محیط است. اغلب کاربران ویندوز وقتی متوجه می‌شوند پرونده‌ها و منابعی که توسط سامبا به اشتراک گذاشته شده آن طور که انتظار دارند رفتار نمی‌کنند، دچار ابهام می شوند و مدیران سامانه نیز نیاز دارند به دقت مجوزها و کنترلهایی که می‌خواهند را روی منابع به اشتراک گذاشته شده اعمال کنند، تا از نفوذ افراد غیر مجاز به این منابع ممانعت نمایند.

مساله اصلی تفاوت درچگونگی اعمال مجوزها وکنترلها بین دو محیط است. هدف این فصل ارائه نکاتی برای کنترل توسط سامبای ۳ برای مدیران شبکه است تا به کمک آنها بتوانند روش بهینه کنترل منابع مشترک را برای محیطهای تحت ویندوز پیدا کنند.

۶-۲- کنترل دسترسی به سامانه‌پرونده

یکی از مهمترین مطالب وجود تفاوت فناوری سامانه‌پرونده پیاده سازی شده در دو محیط ویندوز و لینوکس است. بنابراین بهتر است ابتدا کمی با این دو فناوری آشنا شویم و سپس ببینیم سامبا چطور به تبادل اطلاعات روی ایندو کمک می‌کند.

۶-۳- مقایسه سامانه پرونده ویندوز و لینوکس

سامبا طبق سامانه‌پرونده لینوکس عمل می‌کند، یعنی از قوانین و مجوزهای آن پیروی می‌کند. در زیر یک مقایسه بین سامانه‌پرونده لینوکس و ویندوز NT/200x انجام شده است:

فضای نام[1]: از لحاظ نام، نام پرونده‌ها در سامانه عامل ویندوز می‌تواند تا 254 کاراکتر باشد. ولی در لینوکس این مقدار تا 1023 کاراکتر است. در ویندوز پسوند پرونده مشخص کنندهٔ نوع پرونده است در صورتی که در لینوکس این طور نیست و داشتن پسوند اختیاری است. در آخر اینکه آنچه در ویندوز فولدر نامیده می‌شود، در لینوکس شاخه (دایرکتوری) گفته می‌شود.

حساسیت به حروف[2]: در لینوکس نامها به بزرگی و کوچکی حروف برعکس ویندوز حساس هستند. بنابراین سامبا باید از این جهت یک هماهنگی بین این دو سامانه عامل فراهم کند. سامبا این کار را با یک سری برنامه‌های کاربردی انجام می‌دهد که باعث مقداری سربار[3] روی آن می‌شود.

به مثال زیر توجه کنید از نظر ویندوز پرونده‌های زیر همه یک پرونده هستند ولی از نظر لینوکس سه پرونده مختلف :

MYFILE.TXT

---

[1] Name space
[2] Case Sensitivity
[3] Overhead

MyFile.txt

Myfile.txt

جداساز شاخه[1]: ویندوز و داس هر دو از « \» (backslash) به عنوان جدا کننده شاخه‌ها استفاده می‌کنند در حالی که در لینوکس از « / » برای این کار استفاده می‌کند. این مورد نیز توسط سامبا قابل حل و مدیریت است.

شناسایی گرداننده[2]: در ویندوز علامت یک افزار[3] با یک حرف مربوط به آن افزار مشخص می‌شود (مثل C:\). در لینوکس مفهوم یک جدا وجود ندارد. هر سامانه پرونده که Mount شده است بخشی از درخت شاخه سراسری است. این درخت شاخه با « / » شروع می‌شود که به آن root می‌گوئیم و بقیه از آن جدا می‌شوند مثل C:\ در داس.

File Naming Conventions: در ویندوز هیچ‌گاه نام پرونده‌ها با (۰) شروع نمی‌شوند. در صورتی که در لینوکس این قبیل پرونده‌ها در home Directory کاربران وجود دارند و معمولاً برای پرونده‌های شروع، برنامه‌ها یا پرونده‌های مختلف تنظیمی بکار می‌روند.

Links and Short-Cuts: معمولاً در ویندوز مفاهیمی مانند پیوند[4] و میان‌بر[5] وجود دارند که کار آنها اجرای یک پرونده را از پیوندی به محل واقعی خودش است. در واقع از یک مسیر غیر واقعی یک پرونده اجرا می‌شود. در لینوکس نیز این مفهوم وجود دارد. symbolLink پرونده‌هایی در لینوکس هستند که محتویات آنها مسیر واقعی پرونده اصلی است و عملیات (خواندن یا نوشتن) روی پرونده اصلی انجام می‌شود. به Symbollink ها Softlink نیز گفته می‌شود. علاوه بر این در لینوکس مفهوم دیگری به نام HardLink نیز داریم که کاملاً برای ویندوز ناآشنا است. در HardLink به یک پرونده می‌توان بیش از یک نام نسبت داد.

علاوه بر تفاوتهای فوق، موارد متعدد دیگری نیز وجود دارد که در اینجا فقط به ذکر مهمترین‌ها اکتفا نموده ایم.

مدیریت شاخه[6]: معمولاً برای عملیات اصلی روی شاخه‌ها و برای مدیریت آنها سه عملیات وجود دارد: ایجاد، حذف و تغییر نام. به جدول زیر دقت کنید:

Action	MS Windows Command	UNIX Command
create	md folder	mkdir folder
delete	rd folder	rmdir folder
rename	rename oldname newname	mv oldname newname

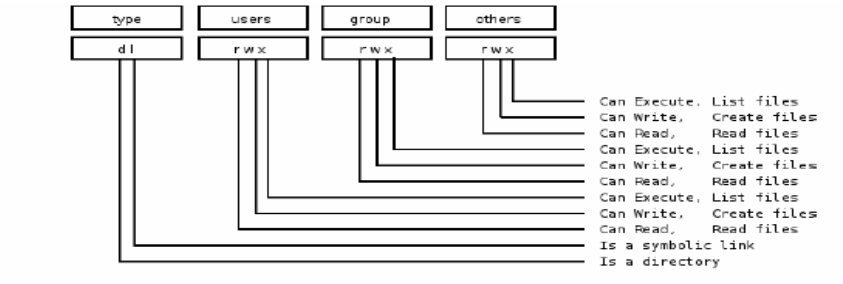
[1] Directory Separators
[2] Drive identification
[3] Partition
[4] Link
[5] Short-cut
[6] Managing Directory

۶-۴- کنترل دسترسی پرونده و شاخه

در لینوکس معمولاً مجوزهای مربوط به شاخه و پرونده به صورت زیر نمایش داده می‌شود:

```
$ ls -la
total 632
drwxr-xr-x   13 maryo   gnomes      816 2003-05-12 22:56 .
drwxrwxr-x   37 maryo   gnomes     3800 2003-05-12 22:29 ..
dr-xr-xr-x    2 maryo   gnomes       48 2003-05-12 22:29 muchado02
drwxrwxrwx    2 maryo   gnomes       48 2003-05-12 22:29 muchado03
drw-rw-rw-    2 maryo   gnomes       48 2003-05-12 22:29 muchado04
d-w--w--w-    2 maryo   gnomes       48 2003-05-12 22:29 muchado05
dr--r--r--    2 maryo   gnomes       48 2003-05-12 22:29 muchado06
drwsrwsrwx    2 maryo   gnomes       48 2003-05-12 22:29 muchado08
----------    1 maryo   gnomes     1242 2003-05-12 22:31 mydata00.lst
--w--w--w-    1 maryo   gnomes     7754 2003-05-12 22:33 mydata02.lst
-r--r--r--    1 maryo   gnomes    21017 2003-05-12 22:32 mydata04.lst
-rw-rw-rw-    1 maryo   gnomes    41105 2003-05-12 22:32 mydata06.lst
$
```

ستونهایی که در شکل فوق نشان داده شده‌اند از چپ به راست به ترتیب عبارتند از: مجوزها، تعداد HardLink به پرونده، صاحب پرونده، گروه پرونده، اندازه پرونده به بایت، تاریخ دسترسی، زمان دسترسی و نام پرونده. به طور خلاصه می‌توان مجوزهای مشخص شده در شکل فوق را به صورت زیر تعیین کرد:



در مجوزها هر پرچم[1] که با ـ نمایش داده شده به معنی عدم مجوز در آن مورد به خصوص است. مثلاً در مثال زیر خواهیم داشت:

-rwxr-x---

ـ صاحب پرونده می‌توان پرونده را بخواند و تغییر دهد و اجرا کند.
ـ گروه پرونده می‌تواند فقط آن را بخواند و اجرا کند.
ـ بقیه افراد هیچ مجوزی ندارند.

در ضمن اولین ستون از ستون مجوزها مشخص کننده نوع پرونده است. قرار داشتن هرکدام از حروف زیر در این ستون معنای خاص خود را دارد:

[1] Flag

- : پرونده عادی
d : شاخه
Symbol Link : l
Block Derice : b
Pipe Device : p
Linux Domain Socket : S

مثال: فرض کنید مجوز پرونده‌ای d-wx--x--- است. در این صورت داخل این پرونده را صاحب آن می‌تواند بخواند و ایجاد کنند (تغییر دهد) اما چون هیچ کس مجوز نوشتن را ندارد، این پرونده توسط هیچ کس در لیست شاخه دیده نخواهد شد. گروه پرونده نیز می‌تواند شاخه را بخواند اما نمی‌تواند در آن پرونده جدیدی ایجاد کند.

۶-۵- کنترل دسترسی به منابع اشتراکی

پارامترهایی که در زیر آورده‌ایم هر کدام در پرونده smb.conf یک سری تنظیمات مربوط به کنترل دسترسی به منابع به اشتراک گذاشته شده است. بهتر است قبل از مطالعه آنها به راهنماهای این پرونده مراجعه کنید.

۶-۵-۱- کنترل براساس کاربر و گروه

این نوع از کنترل دسترسی می‌تواند خیلی مفید باشد، چون دقیقاً می‌توان تعیین کرد که چه کسی به پرونده‌ها دسترسی داشته باشد. در جدول دقیقاً این کنترلها مشخص شده است.

Control Parameter	Description - Action - Notes
admin users	List of users who will be granted administrative privileges on the share. They will do all file operations as the super-user (root). Any user in this list will be able to do anything they like on the share, irrespective of file permissions.
force group	Specifies a UNIX group name that will be assigned as the default primary group for all users connecting to this service.
force user	Specifies a UNIX user name that will be assigned as the default user for all users connecting to this service. This is useful for sharing files. Incorrect use can cause security problems.
guest ok	If this parameter is set for a service, then no password is required to connect to the service. Privileges will be those of the guest account.
invalid users	List of users that should not be allowed to login to this service.
only user	Controls whether connections with usernames not in the user list will be allowed.
read list	List of users that are given read-only access to a service. Users in this list will not be given write access, no matter what the read only option is set to.
username	Refer to the `smb.conf` man page for more information – this is a complex and potentially misused parameter.
valid users	List of users that should be allowed to login to this service.
write list	List of users that are given read-write access to a service.

۶-۵-۲- کنترل بر اساس مجوزهای پرونده و شاخه

اگر این قبیل کنترلها به درستی اعمال نشود، باعث سختی در تشخیص تنظیمات انجام شده و نیز سردرگمی خواهد شد. بنابراین باید آنها را به‌دقت و البته به تـدریج به کار برد.

Control Parameter	Description - Action - Notes
create mask	Refer to the `smb.conf` man page.
directory mask	The octal modes used when converting DOS modes to UNIX modes when creating UNIX directories. See also: directory security mask.
dos filemode	Enabling this parameter allows a user who has write access to the file to modify the permissions on it.
force create mode	This parameter specifies a set of UNIX mode bit permissions that will always be set on a file created by Samba.
force directory mode	This parameter specifies a set of UNIX mode bit permissions that will always be set on a directory created by Samba.
force directory security mode	Controls UNIX permission bits modified when a Windows NT client is manipulating UNIX permissions on a directory.
force security mode	Controls UNIX permission bits modified when a Windows NT client manipulates UNIX permissions.
hide unreadable	Prevents clients from seeing the existence of files that cannot be read.
hide unwriteable files	Prevents clients from seeing the existence of files that cannot be written to. Unwriteable directories are shown as usual.
nt acl support	This parameter controls whether smbd will attempt to map UNIX permissions into Windows NT access control lists.
security mask	Controls UNIX permission bits modified when a Windows NT client is manipulating the UNIX permissions on a file.

۶-۵-۳- برخی کنترلهای دیگر

علاوه بر پارامترهایی که قبلاً برای کنترل دسترسی به پرونده‌ها ذکر کردیم موارد کنترلی دیگری نیز وجود دارند، جدول زیر به بررسی آنها پرداخته است.

Control Parameter	Description - Action - Notes
create mask	Refer to the `smb.conf` man page.
directory mask	The octal modes used when converting DOS modes to UNIX modes when creating UNIX directories. See also: directory security mask.
dos filemode	Enabling this parameter allows a user who has write access to the file to modify the permissions on it.
force create mode	This parameter specifies a set of UNIX mode bit permissions that will always be set on a file created by Samba.
force directory mode	This parameter specifies a set of UNIX mode bit permissions that will always be set on a directory created by Samba.
force directory security mode	Controls UNIX permission bits modified when a Windows NT client is manipulating UNIX permissions on a directory.
force security mode	Controls UNIX permission bits modified when a Windows NT client manipulates UNIX permissions.
hide unreadable	Prevents clients from seeing the existence of files that cannot be read.
hide unwriteable files	Prevents clients from seeing the existence of files that cannot be written to. Unwriteable directories are shown as usual.
nt acl support	This parameter controls whether smbd will attempt to map UNIX permissions into Windows NT access control lists.
security mask	Controls UNIX permission bits modified when a Windows NT client is manipulating the UNIX permissions on a file.

۶-۶- کنترل دسترسی روی منابع مشترک

در این بخش به بررسی تنظیم سامبا روی هر منبع مشترک برای کنترل دسترسی و محدود کردن آن می‌پردازیم. به طور پیش‌فرض، در سامبا هیچ تنظیمی و هیچ محدودیتی برای هر منبع مشترک ندارد. در ویندوزهای NT4/xp/200x روی منابع به اشتراک گذاشته شده می‌توان محدودیتهایی را به دلخواه تنظیم کرد. به عنوان مثال چه کسی اجازه دسترسی به آن منابع را دارد. به طور پیش‌فرض در ویندوز مجوز دسترسی به منابع به صورت کنترل کامل[1] برای تمام افراد[2] است.

[1] Full control
[2] Everyone

سامبا برای هر منبع مشترک، تنظیمات مربوط به کنترل دسترسی را در یک پرونده به نام share_info.tdb ذخیره می‌کند. محل این پرونده بستگی به چگونگی ترجمه[1] سامبا دارد. معمولاً محل آن و پرونده‌های tdb سامبا در /usr/local/samba/var است. اگر برنامهٔ tdbdump روی سامانه شما ترجمه و نصب شده باشد، با اجرای دستور زیر می‌توانید محتویات آن پرونده را بررسی و امتحان کنید:

در زیر شاخه پرونده‌های tdb این دستور را اجرا کنید:

```
tdbdump share_info.tdb
```

۶-۷- مدیریت مجوزهای منابع مشترک

برای مدیریت مجوزهای منابع مشترک، شما باید بسته به بستری که استفاده می‌کنید، بهترین ابزار را متناسب با آن انتخاب کنید. در ادامه برای دو بستر windows NT4 و windows xp/200x ابزارهای موجود و نحوهٔ کار با آنها را بررسی می‌کنیم.

۶-۷-۱- Windows NT4 workstation /Server

در اینجا ابزاری که برای مدیریت مجوزهای منابع مشترک نیاز دارید روی یک کارساز سامبا، NT Server Manager است. این ابزار معمولاً همراه نسخه‌های کارساز ویندوز NT است ولی در نسخه‌های ایستگاه کاری موجود نیست. بنابراین باید آن را از وب‌گاه مایکروسافت دریافت و نصب نمائید. سپس برای کار با آن به صورت زیر عمل نمائید:

برنامه NT4 Server Manager را اجرا کنید. روی کارساز سامبایی که می‌خواهید مدیریت کنید، کلیک نمائید: از منوی اصلی computer را انتخاب نمائید و روی Shared directories کلیک نمائید.

روی منبع مشترکی که می‌خواهید آن را مدیریت کنید، فشار دهید و سپس قسمت properties را انتخاب کنید. درآنجا به قسمت permission رفته و تنظیماتی را که در نظر دارید اعمال کنید.

۶-۷-۲- Windows 200x/xp

در ویندوز 200x و بعد از آن، ابزاری به نام Computer Management Snap-in برای MMC[2] می‌آید. این ابزار در Control panel > Administrative Tools> Computer Management قرار دارد. آن را اجرا کنید و به صورت ذکر شده عمل نمائید:

از منوی Action، Connect to another computer را انتخاب نمائید. اگر تحت دامنه وارد نشده‌اید با یک پیغام برای ورود مواجه می‌شوید. نام کاربری را که وارد می‌کنید، در دامنه احرازهویت خواهد شد. اگر با Administrator، وارد شده باشید، به این مرحله نیازی نیست.

اگر درصفحه مربوط به Select Computer، کارساز سامبا نشان داده نشده است، ابتدا رایانه کارساز سامبا را در فیلد Name وارد کنید. سپس روی علامت(+) و بعد روی + کنار Shared Folder در قسمت چپ صفحه فشار دهید.

---

[1] Compile
[2] Microsoft Management Console

در قسمت راست صفحه، روی منبع مشترکی که می‌خواهید روی آن مجوزهای دسترسی را تنظیم کنید، به صورت دوبار فشاردادن[1] اعمال نمائید. در Tab مربوط به Share permissions رفته و تنظیمات مورد نظر را اعمال کنید.

۶-۷-۳- MS Windows Access Control List and UNIX Interoperability

کارخواه‌ها ویندوز NT هرکدام می‌توانند از Security Setting dialog box برای مشاهده و تصحیح کردن مجوزهای لینوکس استفاده کنند. اما این ابزارها به دقت ابزارهای موجود در روی سامبا و لینوکس نیست.

۶-۸- مشاهده امنیت پرونده روی منابع مشترک سامبا

از روی یک کارخواه NT4/200x/xp، روی هر پرونده یا شاخه که روی کارساز سامبا به اشتراک گذاشته شده، راست کلیک کنید. از منوی باز شده properties را انتخاب کنید تا پنجره مربوط به properties باز شود. روی Security Tap فشار دهید. درآنجا سه دکمهٔ Ownership، Auditing ، Permissions را خواهید دید.

۶-۹- مشاهده مالکیت پرونده[2]

روی دکمه ownership فشار دهید. یک dialogbox باز خواهد شد که صاحب پرونده را به شما معرفی می‌کند. مثلاً:

" SERVER\ user (Long Name)"

SERVER ، NetBIOS name کارساز سامبا است. user نام کاربر تحت لینوکس صاحب پرونده است و Long Name یک سری توضیحات دربارهٔ کاربر و معرفی اوست. (معمولاً این اطلاعات در فیلد GECOS از پایگاه داده کلمات عبور لینوکس قرار دارد). روی دکمهٔ close فشار دهید. توجه کنید که اگر پارامتر nt acl به false تنظیم شده باشد، صاحب پرونده به عنوان کاربر EveryOne از NT نشان داده خواهد شد. در ضمن دکمهٔ Takeownership در اینجا فعال نیست و شما اجازهٔ تغییر صاحب پرونده را نخواهید داشت. در واقع با انتخاب این دکمه، یک صفحه ظاهر شده و در آن گفته می‌شود که کاربری که با آن وارد شده اید ، موجود نیست. علت این امر آن است که مجوز تغییر صاحب پرونده فقط در اختیار کاربر root در لینوکس است و فشار دادن روی این دکمه باعث خواهد شد که صاحب پرونده به کاربری که شما با آن در کارساز تحت ویندوز وارد شده‌اید، تغییر کند و این در سامبا اجرا نخواهد شد.

۶-۱۰- مشاهده مجوزهای پرونده و شاخه‌ها

اگر روی دکمه permission فشار دهید، هم صاحب پرونده و شاخه و هم مجوزهای آنها را می‌توانید ببینید. مثلاً:

SERVER\user (Long Name)

---

[1] Double click
[2] File ownership

اگر پارامتر nt acl، false باشد مجوزها نیز برای کاربرانNT به صورت مجوز کنترل کامل خواهد بود. اما نکته قابل توجه این است که مجوزهای نشان داده شده برای پرونده و شاخه متفاوت است. بنابراین در ادامه این بخش به بررسی این مجوزها به طور مجزا می‌پردازیم.

۶-۱۰-۱- مجوزهای پرونده

حوزه‌های سه‌بیتی استاندارد کاربر/گروه/دیگران[1] در لینوکس و مجوزهای سه تایی خواندن-نوشتن-اجرا[2] توسط سامبا باید به مجوزهای موجود درNT تبدیل شوند. به این ترتیب که مجوزهای مربوط به دیگران در لینوکس با مجوز همه افراد[3] در NT منطبق می‌شود. مجوزهای مربوط به کاربر و گروه نیز به ترتیب به کاربر NT و گروه محلی NT بر می‌گردد. (یک سری توضیحات دربارهٔ Take ownership در NT)

۶-۱۰-۲- مجوزهای شاخه

دو مجموعهٔ مجوزهای متفاوت برای شاخه در سامانه پرونده NTFS وجود دارند. یکی مربوط به خود شاخه است و این که به خود شاخه چه کسانی می‌توانند چه دسترسی‌هایی داشته باشند و دیگری مربوط به مجوزهای پرونده‌های داخل شاخه است.

نکته: اگر پرونده‌ای در لینوکس هیچ مجوزی برای هیچ کس نداشته باشد، در آن صورت سامبا مجوز آن را در NT به Takeownership تبدیل می‌کند و به آن Zero Permission گفته می‌شود.

۶-۱۱- تصحیح یا تغییر مجوز پرونده یا شاخه

تغییر مجوزهای یک پرونده یا شاخه به راحتی با تغییر آنها درdialog box مربوط و تایید آنها با انتخاب دکمهٔ ok انجام می‌شود. اگر پارامتر nt acl همانطور که قبلاً نیز گفتیم به false تنظیم شده باشد، هنگام تلاش برای تغییر مجوزها با پیغام"Access denied" مواجه خواهید شد.

در تغییر مجوزها به اولین نکته‌ای که باید توجه کنید، هنگام فشار دادن روی دکمهٔ Add است. با فشار دادن روی Add لیست کاربران سامبا به شما نشان داده نخواهد شد (احتمالاً با پیغامهای شبیه The remote percedure call failed and did not Execute مواجه خواهید شد). بدین معنی که شما فقط می‌توانید مجوزهای مربوط به کاربر/گروه/دیگران جاری سامانه را تغییر دهید که در dialog box لیست شده اند.

هنگامی که یک مجوز از مجموعه سه‌تایی کاربر/گروه/دیگران در ویندوز حذف شود و سپس کلید ok زده شود، سامبا آن مجوز را در طرف لینوکس به عنوان نداشتن مجوز تفسیر می‌کند. چون لینوکس فقط بیتهای r،w،x از nt acl را پشتیبانی می‌کند، اگر یک خصوصیت مربوط به مجوز دیگری غیر از اینها مثل Delete Access در NT انتخاب شود، این مجوز هنگام اعمال توسط سامبا نادیده گرفته خواهد شد. هنگامی که شما مجوزی را روی یک شاخه تعیین می‌کنید، این مجوز به کل شاخه

[1] user/group/world
[2] Read-write-Execute
[3] Everyone

اعمال می‌شود و این چیزی نیست که شما می‌خواهید. بنابراین باید check box مربوط به Replace Permission on Existing file را قبل از اینکه کلید ok را بزنید، بردارید.

۶-۱۲- بررسی پارامتر mask در سامبا

چهار پارامتر زیر وجود دارند که برای کنترل تعامل با پارامترهای استاندارد create mask سامبا به کار می‌روند:

- Security mask
- Force Security mode
- Directory Security mask
- Force Directory Security mode

هر بار که کاربری برای اعمال مجوزهای مورد نظرش کلید ok را فشار می‌دهند، سامبا باید آن مجوزها را به مجموعه‌های سه‌تایی کاربر/گروه/دیگران، خواندن-نوشتن-اجرا در لینوکس ترجمه و تبدیل کند و سپس تغییر مجوزهای پرونده را با مجموعه بیتهایی که در پارامتر Security mask تنظیم شده‌اند، بررسی کند. هر بیتی در مجوز که تغییر داده شده است اگر پارامتر Security mask آن یک نباشد، آن تغییر مجوز پرونده اعمال نخواهد شد. اصولاً، صفر بودن بیت در Security mask به معنی این است که کاربر حق تغییر ندارد. یک بودن آن به بدین معنی است که اجازه تغییر به کاربر داده شده است. اگر صریحاً این پارامتر تنظیم نشده باشد، به‌طور پیش‌فرض همان مقدار پارامتر Create mask را خواهد داشت. برای اینکه به کاربری اجازه تصحیح همه مجوزهای کاربر/گروه/دیگران روی یک پرونده را بدهیم، باید Create mask را به 0777 تنظیم کنیم.

بعد از این مرحله، سامبا بررسی می‌کند که مجوزهای تغییر داده شده برخلاف بیتهای تنظیم شده در پارامتر Force Security mode نباشد. اصولاً همیشه این بیتها باید طوری تنظیم شوند که کاربر بتواند مجوزهای Security را تغییر دهد. برای اینکه یک کاربر بتواند مجوزهای تمام کاربر/گروه/دیگران را تغییر دهد روی یک پرونده باید این پارامتر به 000 تنظیم شود.

برای شاخه، سامبا همانند چیزی که در مورد پرونده در بالا گفته شد عمل می‌کند با این تفاوت که به جای پارامتر Security mask از پارامتر Directory Security mask و به جای Force Security mode از Force Directory Security mode استفاده می‌کند. پارامتر Directory Security mask به طور پیش‌فرض همان مقدار پارامتر Directory mask را دارد و پارامتر Force Directory Security mode نیز به طور پیش فرض مقدار پارامتر Force Directory mode را دارد.

اگر شما بخواهید منابع مشترک را طوری تنظیم کنید که کاربران در تغییر مجوزها روی پرونده‌ها و شاخه‌های آنها مجوز کنترل کامل باشند، باید در پرونده smb.conf در بخش مربوط به آن منبع تنظیمات زیر را انجام دهید:

Security mask =0777

Force Security mode= 0

Directory Security mask= 0777

Force Directory Security mode= 0

فصل هفتم
امن کردن سامبا
۷-۱- مقدمه
سه سطح برای فراهم کردن حداقل امنیت در یک سایت (شبکه) وجود دارد که عبارتند از: دیواره آتش، خود سامبا و تنظیم کارساز میزبانی که در حال اجرای سامبا است.

سامبا از نظر فراهم کردن امکانات امنیتی در شبکه بسیار قابل انعطاف است و تا آنجائیکه ممکن است از پروتکل‌های مطمئن استفاده می‌کند. برای این منظور سامبا از روش های مختلفی استفاده می‌کند؛ از جمله استفاده از همان ACL در روی هر منبع مشترک. در این بخش به بررسی این روش ها و امکانات می‌پردازیم. نکتهٔ قابل توجه این است که هرگز با رعایت این نکات امنیتی نباید تصور کنید که کارساز سامبای شما به یک دژ غیر قابل نفوذ تبدیل شده است.

۷-۲- استفاده از حفاظت مبتنی بر میزبان[1]
در موارد زیادی که سامبا را نصب می‌کنیم، اکثر رفتارهای غیر عادی از خارج از شبکه صورت می‌پذیرد. به طور پیش‌فرض سامبا تمام درخواستهایی را از هر میزبان قبول می‌کند. یعنی اگر سامبایی که نصب کرده‌اید ناامن باشد و مستقیماً به اینترنت وصل باشد قطعاً نفوذپذیر[2] خواهد بود.

یکی از ساده‌ترین راه‌های جلوگیری از این امر، استفاده از hostsdeny وhostsallow است که می‌توان در پرونده تنظیم سامبا به صورت زیر اضافه کرد.:

hosts allow = 127.0.0.1 192.198.2.0/24 192.168.3.0/24

hosts deny = 0.0.0.0/0

در مثال بالا فقط به اتصالات سامبا که از خود کارساز[3] و دو شبکه .192.198.2 و192.168.3 برقرار می‌شود، اجازه برقراری اتصال داده می‌شود و غیر از این موارد هیچ کس حق اتصال ندارد و به محض فرستادن اولین بسته ارسالی رد خواهند شد.

۷-۳- استفاده از حفاظت مبتنی بر میزبان کاربر[4]
می‌توان دسترسی به کارساز را با کاربران خاصی نیز محدود کرد. اگر بخواهید فقط کاربرانی که مد نظر دارید به کارساز وصل شوند، باید در بخش global از پرونده تنظیم smb.conf به صورت زیر عمل کنید:

valid users = @smbusers , jacko

به این ترتیب اجازه دسترسی به کارساز یا از طریق کاربر jacko و یا اعضای گروه smbuser امکان پذیر خواهد بود.

---
[1] Host-Based Protection
[2] Vulnerable
[3] Localhost
[4] User-Based Protection

۷-۴- استفاده از حفاظت مبتنی بر واسط[1]

به طور پیش‌فرض، سامبا تمام اتصالات را روی هر واسط شبکه‌ای که روی سامانه پیدا کند می‌پذیرد. یعنی اگر اتصال ISDN یا PPP به اینترنت داشته باشد، سامبا آنها را قبول خواهد کرد. ولی برای اینکه این تنظیمات را نیز به دلخواه خود تغییر دهید باید به صورت زیر عمل کنید:

interfaces = eth lo*

bind interfaces only = yes

با تنظیمات فوق، سامبا فقط به اتصالات روی واسطهایی که با eth شروع شده و loopback برقرار می‌شود، پاسخ می‌دهد. مانند eth0،eth1. البته نام واسطها به نوع سامانه‌عامل بستگی دارد. این نامهایی که گفته شد روی لینوکس کاربرد دارد. بنابراین اگر یک اتصالی از روی واسطppp0 صورت پذیرد، فوراً رد خواهد شد.

۷-۵- استفاده از دیواره آتش

معمولاً از دیواره آتش در مواقعی استفاده می‌شود که دسترسی به بعضی خدمات خاص خارج از شبکه مد نظر باشد. این روش فن خوبی برای داشتن امنیت در شبکه است. هرچند توصیه می‌شود حتماً برای امنیت بیشتر از روش‌های دیگر نیز در کنار دیواره آتش استفاده شود.

برای تنظیم دیواره آتش باید بدانید، که چه درگاه‌هایی[2] باز چه درگاه‌هایی بسته باشد. معمولاً سامبا از درگاه‌های زیر استفاده می‌کند:

UDP/137- Used by nmbd
UDP/138- Used by nmbd
TCP/139- Used by smbd
TCP/445- Used by smbd

درگاه آخر در سالهای اخیر مورد استفاده قرار گرفته است.

۷-۶- استفاده از IPC$ Share-Based Denials

علاوه بر روشهای فوق می‌توانید دسترسی به IPC$ Share را نیز محدود کنید. یعنی:

[IPC$]

hosts allow = 192.168.115.0/24 127.0.0.1

hosts deny = 0.0.0.0/0

با توجه به دستورات و تنظیمات فوق، فقط اتصالات IPC$ از میزبان محلی[3] و شبکه 192.168.115.0 امکان‌پذیر خواهد بود. اگر کارخواه‌ها دیگر بخواهند به میزبان محلی وصل شوند با پیغام Access denied مواجه خواهند شد و نمی‌توانند منابع مشترک را جستجو کنند و نیز قادر به

[1] Interface Protection
[2] Port
[3] Localhost

دسترسی به منابع مشترک دیگر نیز نخواهند بود. استفاده از این روش پیشنهاد نمی‌شود، مگر اینکه امکان استفاده از روشهای قبلی مهیا نباشد.

۷-۷- NTLM v2 security

روش احرازهویت مبتنی بر NTLM یک روش پیشرفته احرازهویت در ویندوز می‌باشد. برای بررسی دقیق‌تر این روش به کتابهای موجود در این زمینه مراجعه کنید.

برای تنظیم احرازهویت NTLMv2 باید کلیدهای ثباتی[1] زیر را بدانید:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]

"Imcompatibilitylevel"=dword:00000003

مقدار 00000003 به این معنی است که NTLMv2 فقط پاسخ[2] را می‌فرستد. کارخواه‌ها از احرازهویت NTLVMv2 استفاده می‌کنند. کنترل‌کننده‌های دامنه احرازهویت NTLM، LM و NTLMv2 را قبول می کنند.

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control \Lsa\MSV1_0]

"NtlmMinClientSec"= dword:00080000

مقدار 00080000 به این معنی است که فقط موارد NTIMv2 Session security مجازند. اگر هر کدام از دو طرف NtlmMinClientSec و NtlmMinServerSec به مقدار 0x00080000 تنظیم شده باشند، در آن صورت اگر NTLMv2 Session Security تشخیص داده نشود، اتصال برقرار نخواهد شد.

۷-۸- بروز رسانی سامبا

برای بروز رسانی سامبا همیشه به وب‌گاه سامبا[3] سری بزنید و از وجود نسخه‌ها و یا رفع بعضی عیوب امنیتی جدید مطلع شوید. گاهی اوقات نکات امنیتی جدیدی ایجاد می‌شود که در آن صورت بروز رسانی سامبا اکیداً توصیه می‌گردد.

[1] Registry key
[2] Response
[3] http://www.samba.org/

فصل هشتم
پشتیبانی از چاپ کلاسیک[1] و CUPS[2]

۸-۱- مقدمه

یکی از مهمترین و ضروری‌ترین خدماتی که باید به کاربران ارائه شود، خدمت چاپ است. سامبا می‌تواند این خدمت را برای کارخواه‌های شبکه شامل استفاده‌کنندگان ویندوز با قابلیت اعتماد بالا فراهم کند. این خدمت چاپ سامبا می‌تواند هم روی یک کارساز خوداتکا و هم روی یک کارساز عضو دامنه اجرا شود. تنظیماتی که روی این خدمت انجام می‌شود می‌تواند بسیار ساده یا پیچیده باشد. البته می‌توان آن را جایگزین کارساز چاپ در ویندوز NT یا 2000 کرد و قابلیتهای متعددی را به آن افزود. کارخواه‌ها نیز می‌توانند با استفاده از روش "Print'n'Print" چاپگر و نرم‌افزارهای راه‌انداز آن را به دست آورده و نصب نمایند. اگر به یک حسابداری[3] مرکزی نیاز داشته باشیم، به طوری که برای هر صفحه مقداری از حساب کاربر کم شود، این کار را نیز می‌توان با CUPS به بهترین نحو انجام داد.

در این فصل به بررسی چگونگی تنظیم و راه‌اندازی خدمت چاپ در سامبا پرداخته می‌شود. اکثر مطالبی که در این فصل آورده شده است در مورد CUPS نیز کاربرد دارد. در ادامهٔ فصل به چگونگی استفاده از خدمت CUPS می‌پردازیم.

نکته: اغلب مثالهایی که آورده شده است، طبق کارخواه در حال اجرای WindowsXP professional است. در نظر داشته باشید که ویندوزهای 200x/xp کاملاً شبیه هم هستند و فقط در جزئیات کمی متفاوتند.

۸-۲- مقدمهٔ فنی

نقش سامبا به عنوان یک واسطه[4] است. به این ترتیب که پرونده‌هایی که باید چاپ شود، از کارخواه‌های ویندوز می‌گیرد و آنها را به سامانه چاپ تحویل می‌دهد تا پردازش لازم روی آنها صورت پذیرد. بنابراین سامبا نیاز دارد تا با هر دو طرف ارتباط برقرار کند:

- کارخواه‌های چاپ ویندوز
- سامانه چاپ لینوکس

امروزه یکی از جنبه‌های مساله‌ساز مدیریت سامبا، تنظیمات چاپ است. تعداد زیادی از مدیران سامبا تصور می‌کنند که سامبا پردازشهای چاپی خاصی را روی پرونده‌ها انجام می‌دهد. البته این تصور کاملاً اشتباه است. سامبا هیچ‌گونه فیلترینگ یا فرآیند دیگری را روی پرونده‌های چاپ اعمال نمی‌کند.

---

[1] Classical Printing Support
[2] Common UNIX Printing System
[3] Accounting
[4] Middleman

در واقع سامبا کار مربوط به چاپ را از کارخواه چاپ می‌گیرد. این کارها نیز در یک فضای محلی به صورت صف ذخیره[1] شده‌اند. وقتی تمام کار چاپ دریافت شد، سامبا دستور چاپ را می‌دهد و پرونده مربوطه را نیز به آن ارسال می‌کند.

۸-۳- مراحل پردازش چاپ از کارخواه به کارساز سامبا

چاپ موفقیت‌آمیز از یک کارخواه ویندوز به یک کارساز لینوکس با استفاده از کارساز چاپ سامبا شامل شش یا نهایتاً هفت مرحله خواهد بود:

۱. یک اتصال از سوی ویندوز به چاپگر به اشتراک گذاشته شده برقرار می‌شود.
۲. سامبا باید کاربر را شناسایی کند.
۳. ویندوز یک کپی از پرونده مورد نظر برای چاپ، به محیط Spooling سامبا می‌فرستد.
۴. اتصال برقرار شده از سوی ویندوز بسته می‌شود.
۵. سامبا دستور چاپ را برای دادن پرونده به محیط Spooling چاپ لینوکس فرا می‌خواند.
۶. سامانه چاپ لینوکس کار مربوط به چاپ را پردازش می‌کند.
۷. ممکن است نیاز باشد که پرونده چاپ پاک شود (حذف شود). این فقره[2] به تنظیمات ذخیره کننده کار در صف[3] چاپ بستگی دارد.

۸-۴- پارامترهای مرتبط با تنظیمات چاپ درسامبا

چند پارامتر در پرونده smb.conf برای تنظیم چاپ وجود دارد. همانند پارامترها و تنظیمات قبلی دو سطح Service و Global از این پارامترها وجود دارد.

- **پارامترهای سراسری[4]:** که به تعاریف اختصاصی اعمال نمی‌شود. اگر خطایی در آن باشد با برنامه testparm مشخص می‌شود و به شما گزارش داده می‌شود.
- **پارامترهای سطح خدمات[5]:** این پارامترها می‌تواند (ممکن است) در بخش [global] در پروندهsmb.conf تعیین شوند. در این مورد، آنها رفتار پیش‌فرض همهٔ خدمات مشترک را تعریف می‌کنند.

[1] Spool
[2] Item
[3] Spooler
[4] Global Parameters
[5] Service Level Parameters

۸-۵- تنظیمات سادهٔ چاپ

در اینجا مثالی از یک تنظیم ساده چاپ در سامبا است که از تعداد کمی پارامتر برای تنظیم استفاده کرده است. با وجود این به راحتی خدمت چاپ را فراهم می‌سازد. وقتی شما یک پارامتر را در پرونده smb.conf تعیین و مشخص می‌کنید، مقدار پیش‌فرض جای‌نوشت[1] می‌شود. هنگامی که testparm با مجوز root اجرا می‌شود، قادر است تمام تنظیمات را گزارش دهد. این مورد تمام مقادیر پیش‌فرض و تنظیمات پرونده smb.conf را شامل می‌شود. ضمناً هشدارهایی برای پارامترهایی که تنظیم نشده‌اند، اعلام می‌کند. خروجی برنامهٔ testparm حدود ۳۴۰ خط و یا بیشتر است و بنابراین بهتر است هنگام اجرا آن را با یک برنامه صفحه‌بندی لوله[2] کنید.

```
[global]
        printing = bsd
        load printers = yes

[printers]
        path = /var/spool/samba
        printable = yes
        public = yes
        writable = no
```

۸-۶- استفاده از برنامه Testparm

برای اینکه بتوانید تمام تنظیمات مربوط به چاپ در سامبا را مشاهده کنید، دستور زیر را اجرا کنید:

```
# testparm  -s -v | egrep " ( lp | print | spool | driver | ports | \[ )"
```

خروجی این دستور را می‌توانید برای نمونه ببینید:

[1] Overwrire
[2] Pipe

```
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[printers]"

[global]
        smb ports = 445 139
        lpq cache time = 10
        load printers = Yes
        printcap name = /etc/printcap
        disable spoolss = No
        enumports command =
        addprinter command =
        deleteprinter command =
        show add printer wizard = Yes
        os2 driver map =
        printer admin =
        min print space = 0
        max print jobs = 1000
        printable = No
        printing = bsd
        print command = lpr -r -P'%p' %s
        lpq command = lpq -P'%p'
        lprm command = lprm -P'%p' %j
        lppause command =

         lpresume command =
         printer name =
         use client driver = No

[homes]

[printers]
        path = /var/spool/samba
        printable = Yes
```

نکته: نتیجه اجرای برنامهٔ testparm در سامبای ۳ متفاوت از سامبای ۲،۲. x است.

توجه داشته باشید که همیشه لازم است به عقب برگردید و خروجی برنامهٔ testparm را به دقت بررسی کنید. این کار در واقع عیب‌یابی[1] است و توصیه می‌شود که هرگاه تنظیم خاصی مورد نظر است، حتماً صریحاً آن را ذکر و تنظیم کنید و به پیش‌فرض بودن حالت تنظیم مورد نظر خود اعتماد نکنید. با استفاده از برنامه testparm خیلی از تنظیماتی که در نظر گرفته شده و خلاف نظر شماست مشخص می‌شود.

[1] Trubleshooting

۸-۷- جزئیات بیشتر

به مثال زیر که یک پرونده تنظیم برای چاپ در یک سامانه BSD است دقت کنید. (انتخاب سامانه BSD به دلیل رایج بودن آن سامانه در بسیاری از محیطهای کاری است)

```
[global]
        printing = bsd
        load printers = yes
        show add printer wizard = yes
        printcap name = /etc/printcap
        printer admin = @ntadmin, root
        max print jobs = 100
        lpq cache time = 20
        use client driver = no

[printers]
        comment = All Printers
        printable = yes
        path = /var/spool/samba
        browseable = no
        guest ok = yes
        public = yes
        read only = yes
        writable = no

[my_printer_name]
        comment = Printer with Restricted Access
        path = /var/spool/samba_my_printer
        printer admin = kurt
        browseable = yes
        printable = yes
        writable = no
        hosts allow = 0.0.0.0
        hosts deny = turbo_xp, 10.160.50.23, 10.160.51.60
        guest ok = no
```

در مثال فوق بخشهای [my-printer-name] و [printers]،[global] آورده شده است که در ادامه به تفصیل پارامترهای ذکر شده در هر یک را بررسی می‌کنیم.

بخش[global]

تمام پارامترهایی که به طور کلی روی کارساز اعمال می‌شوند، در این بخش آورده می‌شود.

- **printing=bsd:** این پارامتر باعث می‌شود تا از دستورات مربوط به سامانهBSD برای عملیات چاپ استفاده شود. قابل ذکر است که چون این پارامتر در بخش global آورده شده

است، روی تمام چاپگرهایی که به اشتراک گذاشته شده‌اند و به طور جداگانه تنظیم نشده‌اند، تاثیر دارد.

- **Load printers=yes**: این پارامتر به سامبا می‌گوید که تمام چاپگرهای به اشتراک گذاشته شده را ایجاد کند. این چاپگرها با بررسی و اسکن کردن پرونده printcap مشخص می‌شوند و همه چاپگرها قابل مرور هم می‌باشند. اگر این پارامتر را تنظیم کنید، دیگر نیازی به تنظیم جداگانه هر چاپگر به اشتراک گذاشته شده نیست. اگر این پارامتر را برابر با no بگذارید، در آن صورت باید هر چاپگری را که می‌خواهید به اشتراک بگذارید، به طور جداگانه تنظیم و تعیین کنید و چاپگری را هم که مایل نیستید به اشتراک بگذارید، تنظیمی به آن اعمال نخواهد شد و غیر قابل دسترس خواهد بود.
- **Show add printer wizard=yes**: با این پارامتر نیز که به طور پیش‌فرض yes است، تعیین می‌کنید که شمایل مربوط به Add printer wizard در شاخه printers از میزبان سامبا (که در Network Neignborhood یا با دستور net view دیده می‌شود) ظاهر گردد. با Add printer wizard شما می‌توانید نرم‌افزار راه‌انداز چاپگر را تعیین کنید.
- **Max print jobs=100**: حداکثر تعداد کارهایی که در یک زمان می‌تواند روی کارساز سامبا فعال باشد را تعیین می‌کند. در اینجا این با تعداد مقدار ۱۰۰ به عنوان مقدار حداکثر تنظیم شده است. اگر بیش از این تعداد به کارساز فرستاده شود، در آن صورت کارخواه با پیغام خطای "no more space available on server " مواجه خواهد بود. اگر این مقدار را به صفر (پیش‌فرض هم ۰ است) تنظیم کنید، به این معنی است که هیچ محدودیتی در تعداد کارهای همزمان وجود ندارد.
- **Printcap name=/etc/printcap**: سامبا در این پرونده به دنبال پرونده چاپگرهای در دسترس می‌گردد.
- **Printer admin=@ntadmin**: اعضای گروه @ntadmin باید قادر باشند نرم‌افزارهای راه‌انداز لازم را اضافه کنند و یا خصوصیات چاپگر را تغییر دهند (ntadmin فقط یک نام و مثال است و لازم است که یک نام متغیر از یک گروه لینوکس باشد). به طور ضمنی کاربر root همیشه عضوadmin چاپگر است. علامت @ باعث می‌شود تا سامبا به نام گروه‌های موجود در پرونده /etc/group مراجعه کند.
- **Lpq cache time=20**: با این پارامتر زمان Cache نتایج دستور lpq کنترل می‌شود و باعث می‌شود بار ایجاد شده روی کارساز چاپگر کاهش یابد.
- **Use client driver= no**: yes بودن این پارامتر فقط روی ویندوزهای NT/200x/xp تاثیر دارد. البته نباید آن را در کارساز سامبایی که نرم‌افزارهای راه‌انداز معتبری روی آن نصب است، به yes تنظیم کنید. برای توضیحات بیشتر به راهنمای کمکی smb.conf مراجعه کنید.

بخش[printers]

اگر بخشی با این نام در پرونده smb.conf آورده شود، کاربران قادر خواهند بود به هر چاپگری که در پروندهPrintCap مشخص شده است وصل شوند. چون بعد از شروع کار سامبا یک چاپگر به اشتراک گذاشته شده به ازای هر نام چاپگر موجود در پرونده PrintCap ایجاد می‌شود. در واقع این بخش یک تنظیمات عمومی مربوط به همهٔ چاپگرها را در بردارد. حال به بررسی پارامترهای این قسمت بپردازیم:

- **Comment=All printers:** این توضیح به کارخواه‌هایی که می‌خواهند از چاپگرهای به اشتراک گذاشته شده استفاده کنند، نشان داده می‌شود.
- **Printable=yes:** خدمت [printers] باید به‌عنوان printable اعلام شود. اگر غیر از این باشد smbd در هنگام راه‌اندازی برای بازشدن با مشکل مواجه خواهد شد. این پارامتر به کارخواه‌ها اجازه می‌دهد تا پرونده‌های ذخیره شده در را بتواند در شاخه مشخص شده در پارامتر path، باز کرده و یا بنویسند. این پارامتر جهت جداکردن چاپگرهای به اشتراک گذاشته شده از پرونده های مشترک توسط سامبا به کار می‌رود.
- **Path=/var/spool/samba:** این پارامتر به شاخه استفاده شده توسط سامبا برای ذخیره نمودن در صف پرونده چاپ رسیده، اشاره می‌کند، که آن شاخه باید قابل نوشتن[1] باشد و بیت stickey نیز در آن فعال شده باشد. همچنین این شاخه نباید همان شاخه spool تعیین شده در تنظیمات زیر سامانه چاپ لینوکس شما باشد.
- **Browseable=no:** معمولاً وقتی پارامتر printable به yes تنظیم شده باشد، این پارامتر همیشه به no تنظیم می‌شود و باعث می‌شود تا چاپگرهای به اشتراک گذاشته شده در لیست مخفی باشند.
- **guest ok=yes:** در صورت yes بودن این پارامتر، برای اتصال به چاپگر مورد نظر هیچ کلمه عبوری نیاز نیست. در اکثر سامانه‌ها حساب کاربری guest به کاربری به نام "nobody" منطبق می‌شود. این کاربر در پرونده passwd در لینوکس با کلمهٔعبور خالی (Empty) وجود دارد. ولی توجه کنید که نمی‌توان با آن تحت لینوکس وار شد. در بعضی از سامانه‌ها کاربر guest مجوز استفاده از چاپ را ندارد. شما می‌توانید این محدودیت را به طریق زیر امتحان کنید. ابتدا با کاربر guest با استفاده از دستور su - guest وارد شوید و دستوری مانند دستور زیر برای چاپ اجرا کنید:

```
$ lpr -P printername    /etc/motd
```

- **public=yes:** این پارامتر در واقع یک مترادف برای پارامتر guest ok= yes است و نیازی نیست که در صورت وجود آن، این پارامتر را دوباره بیاوریم.

[1] writable

- **Read only=yes:** وجود این پارامتر باعث می‌شود تا کاربران دیگری که از منابع مشترک دیگر استفاده می‌کنند، نتوانند در شاخه مخصوص خدمت چاپ تغییری دهند. (هرچند printable بودن این خدمت همیشه اجازه نوشتن را در این شاخه می‌دهد، اما فقط در طول عملیات مربوط به چاپ اگر کاربران مجوز اتصال را داشته باشند و به طور عادی برای عملیات نوشتن اجازه داده نمی‌شود.)
- **writable=no:** این پارامتر مترادف پارامتر read only = yes است

هر بخش [my-printer-name]

در این بخش می‌توان به تعداد چاپگرهای به اشتراک گذاشته شده تنظیمات اختصاصی هر چاپگر را انجام داد. باید سعی کنید نامی که به چاپگر اشتراک گذاشته شده می‌دهید با نام منبع دیگر یکی نباشد. چون در آن صورت وقتی در خواستی از طرف کارخواه به سامبا فرستاده شود، سامبا ابتدا به دنبال آن نام در بین پرونده‌های به اشتراک گذاشته شده می‌رود. در صورتی نام مشابه نام چاپگر پیدا کند به آن منبع متصل می‌شود و امکان دسترسی به چاپگر وجود ندارد.

- **Comment= Printer with Restricted Access:** توضیحی که به همه نشان داده می‌شود.
- **Path=/var/spool/samba-my-printer:** تنظیم فضای spooling برای این چاپگر در مسیری غیر از شاخه پیش‌فرض.
- **Printer admin=kurt:** تعریف یک admin جدا از دیگر چاپگرهای به اشتراک گذاشته شده برای این چاپگر خاص.
- **Browseable=yes:** این پارامتر باعث می‌شود تا کارخواه‌ها به راحتی بتوانند چاپگر مورد نظر را در Network Neigborhood ببینند.
- **Printable=yes:** همان کار پارامتر موجود در بخش [printers] را انجام می‌دهد.
- **Writable=no:** همان کار پارامتر موجود در بخش [printers] را انجام می‌دهد.
- **Host allow=10.10.160.,10.10.161.:** در این بخش یک کنترل دسترسی به چاپگر با استفاده از این پارامتر ساخته می‌شود. در واقع با دادن آدرس IP کارخواه‌ها، می‌توان دسترسی به چاپگر را محدود کرد. این کار اصلاً تاثیری در ایجاد امنیت ندارد. فقط یک کنترل ساده روی دسترسی است.
- **Host deny= turbo-xp,10.10.160.33,10.10.161.65:** کارخواه‌های مشخص شده در این پارامتر، به هیچ وجه اجازهٔ دسترسی به چاپگر را ندارند. همان طور که مشاهده می‌کنید، در اینجا هم می‌توان نام کامپیوتر و یا IP آن را آورد.
- **Guest ok=no:** با این پارامتر دیگر کاربر guest نمی‌تواند به آن دسترسی داشته باشد.

نکته مهم این است که لازم نیست درایوهای چاپگر روی یک سامانه سامبا به منظور پشتیبانی از کارخواه‌های ویندوز نصب شود.

کارخواه‌های ویندوز NT/2000 می‌توانند Add Printer Wizard)APW) مربوط به خود را برای نصب نرم‌افزار راه‌انداز ها به طور محلی اجرا کنند. این همان روش استفاده شده در کارخواه-های9x/Me است. (هرچند در سامبای نسخهٔ ۲،۲،۰ یک اشکال[1] وجود داشت که باعث می‌شد کارخواه‌های ویندوزNT/2000 نیاز داشته باشند کارساز سامبا یک نرم‌افزار راه‌انداز درست برای چاپگر را فراهم کند که این اشکال در نسخه ۲،۲،۱ برطرف شد) اما با این همه یکی از قابلیتهای جدید در سامبا برای نصب نرم‌افزار راه‌انداز چاپگر، استفاده از بخش [printers] در کارساز سامبا است که کار را بسیار آسان کرده‌است. با وجود این قابلیت، تمام کارخواه‌های (شامل 95/98/Me) نرم‌افزار راه‌انداز نصب شده را در هنگام اولین اتصال به چاپگر به اشتراک گذاشته شده دریافت می‌کنند. بارگذاری[2] و سپردن[3] نرم‌افزار راه‌انداز به بخش [printers] و کارهای بعدی آن به چند طریق می‌تواند انجام شود:

- اجرای APW روی یک کارخواه NT/200x/xp professional (این راه در ویندوزهای 95/98/Me عملی نیست.)
- استفاده از مجموعه ابزار Imprints.
- استفاده از مجموعه ابزار smbclient, rpcclient که به صورت خط فرمان هستند.
- استفاده از Cupsaddsmb (که فقط برای سامانه چاپ CUPS کار می‌کند و نه برای LPRng,LDR/LPD و...)

در ویندوزهای 98/Me وقتی یک چاپگر به اشتراک گذاشته می‌شود، نام [printers] به آن خدمت داده می‌شود. این خدمت در سامبای ۲،۲ در این بخش پارامترهایی نیز برای تنظیم آن در نظر گرفته می‌شد. اما در سامبای ۳ این پارامترها حذف شدند. در واقع نام جدید [print$] برای محل به دست آوردن نرم‌افزارهای راه‌انداز چاپگر در نظر گرفته شد. که این نام در ویندوزهای NT برای چاپگر به اشتراک گذاشته شده در نظر گرفته شده است.

Creating the [print$] share

همانطور که گفتیم برای پشتیبانی از بارگذاری و دریافت پرونده‌های نرم‌افزار راه‌انداز چاپگر، باید ابتدا یک بخش به نام [print$] ایجاد کنیم. دقت کنید نام این بخش یعنی [print$] در کارخواه‌های تحت ویندوز یک hardcode است و نمی‌تواند تغییر کند. چون کارخواه‌های تحت ویندوز طوری برنامه‌نویسی شده‌اند که دقیقاً این اسم را در لیست خدمات به اشتراک گذاشته شده جستجو می‌کنند تا پرونده‌های نرم‌افزار راه‌انداز چاپگر را به دست آورند. در این بخش که پارامترهای آن را معرفی می‌کنیم باید شاخه را که پرونده‌ها در آن قرار دارد را مشخص کنیم.

پارامترهای زیر در قسمت[print$] نیاز است:

---

[1] Bug
[2] Uploading
[3] Depositing

```
[global]
# members of the ntadmin group should be able to add drivers and set
# printer properties. root is implicitly always a 'printer admin'.
        printer admin = @ntadmin
...

[printers]
...

[print$]
        comment = Printer Driver Download Area
        path = /etc/samba/drivers
        browseable = yes
        guest ok = yes
        read only = yes
        write list = @ntadmin, root
```

comment = Printer Driver Download Area: توضیحی که هنگام لیست شدن در کارخواه ظاهر می‌گردد (معمولاً کارخواه‌های ویندوزی این توضیح را نمی‌بینند ولی این توضیح در خروجی دستور Smbclient –L samba Server ظاهر می‌شود.)

Path =/etc/ samba/ Printers: مسیری که پرونده‌های نرم‌افزار راه‌انداز ویندوز برای سپردن از لینوکس در آن قرار می‌گیرند.

browseable= no: باعث می‌شود که بخش به اشتراک گذاشته شدهٔ [print$] برای کارخواه‌های از Network Neighborhood قابل مشاهده نباشد. هرچند بار هم شما می‌توانید آن را با استفاده از دستور: Net use g:\\ Samba server\printer در Dosprompt یا Connect network drive menu از مرورگر ویندوز سوار کنید.

read only = yes: چون ما نمی‌خواهیم هرکسی به پرونده‌های نرم‌افزارهای راه‌انداز در این محل دسترسی داشته باشد و یا حتی تنظیمات آن را تغییر دهد، بنابراین با این پارامتر آن را به صورت فقط خواندنی به اشتراک می‌گذاریم.

write list =@ ntadmin ,root: با توجه به پارامتر قبلی چون [print$] فقط خواندنی شده است و کسی نمی‌تواند هیچ تغییری روی آن اعمال کند، شما باید یک لیستی با مجوز نوشتن برای کاربران خاص مثلroot ایجاد کنید. این لیست با پارامتر فوق ایجاد می‌شود.

Share Directory [print$]

در قسمت قبل گفتیم به منظور ایجاد محل برای به‌دست آوردن نرم‌افزار راه‌انداز چاپگر توسط کارخواه‌ها، بخش [print$] را ایجاد کرده‌ایم. حال این منبع مشترک باید دارای نرم‌افزارهای راه‌انداز

چاپگر برای معماریهای مختلف کارخواه‌ها باشد. بنابراین باید در شاخه که در پارامتر path مشخص کردیم، چند زیرشاخه ایجاد نماییم. یک نکته مهم این است که درست مثل نام بخش [print$] که یک hardcode بود و نباید تغییری در آن داده شود، نام زیر شاخه‌ها نیز hardcode است و باید دقیقاً به همین شکلی که در زیر آورده‌شده، ایجاد شوند:

```
[print$] --+
          |-- W32X86        # Server drivers to windows NT x86
          |-- WIN40         # Server drivers to windows 95/98
          |-- W32ALPHA      # Server drivers to windows NT Alpah_Axp
          |-- W32MIPS       # Server drivers to windows NT R4000
          |-- W32PPC        # Server drivers to windows NT Power PC
```

بعد از اینکه از درستی تنظیمات فوق مطمئن شدید، به یکی از سامانه‌های کارخواه که ویندوز NT 4.0/200x/xp دارد مراجعه کنید. سپس به محیط Network Neighborhood یا My Network Place بروید و به دنبال میزبان سامبا بگردید و روی آن به قسمت Printers and Faxes بروید. در آنجا باید چاپگرهایی را که می‌توانند با چاپگرهای به اشتراک گذاشته شده منطبق شوند، ببینید.

۸-۷-۱- نصب نرم‌افزار راه‌انداز در [print$]

حتماً تا الآن تمام مراحل را به خوبی پشت سرگذاشته‌اید. پرونده‌های نرم‌افزار راه‌انداز چاپگر بعد از در دسترس بودن باید نصب شوند، چون در غیر این صورت چاپگر قابل استفاده نخواهد بود. دو راه برای نصب پرونده نرم‌افزار راه‌انداز چاپگر در بخش [print$] وجود دارد:

با استفاده از دستور rpcclient و زیر دستورهای آن (دراینجا: adddriver, Setdriver) از روی هر سامانه لینوکس.

با اجرای یک GUI (Add Printer Wizard ,Printer Properties) از روی هر کارخواه ویندوز NT/200x/XP که البته گزینه دوم شاید آسان‌تر باشد.

در ادامه به بررسی این دو راه می‌پردازیم.

۸-۷-۲- ویزارد اضافه نمودن چاپگر

روی ویندوزهای NT/200x/XP، برنامه گرافیکی Add Printer Wizard به نصب نرم‌افزارهای راه‌انداز چاپگر روی کارخواه‌ها کمک می‌کند و با این شرایط نصب آنها چندان مشکل نخواهد بود. شما باید Properties چاپگری را که می‌خواهید نرم‌افزار راه‌انداز آن را نصب کنید، ببینید. یعنی مرورگر ویندوز Network Neighborhoodرا باز کنید و منابع به اشتراک گذاشته شده مربوط به کارساز سامبای خود را ببینید. شاخه مربوط به چاپگر (Printers) را باز کرده و روی شمایل چاپگر راست کلیک کنید و سپس Properties را انتخاب کنید. در صورتی که نرم‌افزار راه‌انداز نصب نشده باشد با پیغام خطای زیر روبرو خواهید شد:

Device Setting Connot be displayed .The driver for the specified Printer is not installed , Only spooler Properties will be displayed .Do you want to install the driver now?

در صورت مشاهده این پیغام روی yes کلیک نکنید و در عوض No را انتخاب کنید. در این صورت فقط صفحهٔ مربوط بهProperties چاپگر را خواهید دید. در اینجا دو راه برای نصب داریم:

- انتخاب نرم‌افزار راه‌انداز از لیست نرم‌افزارهای راه‌انداز نصب شده که این لیست در ابتدای کار خالی خواهد بود.
- فشار روی New Driver برای نصب یک نرم‌افزار راه‌انداز چاپگر جدید. در این صورت یک ویزارد شروع به کار می‌کند و مراحل کاری آن دقیقاً شبیه نصب نرم‌افزارهای راه‌انداز دیگر در سامانه‌عامل ویندوز است.

ما فرض را بر این داریم که شما با مراحل نصب نرم‌افزار راه‌انداز در ویندوز آشنا هستید. از اینکه اتصال شما با کارساز سامبا با یک کاربر قوی است، مطمئن شوید. اگر در این مورد شک دارید، می‌توانید با کمک دستور smbstatus شرایط را بررسی کنید. در صورتی که بخواهید نرم‌افزار راه‌انداز چاپگر را روی سامانه‌عامل دیگری غیر از ویندوز نصب کنید (NT x86)، باید از sharing tab از Properties چاپگر استفاده کنید.

CUPS[1] -۸-۸

CUPS یک سامانه مدیریت چاپ برای بسترهای لینوکس است که توسط Easy Software Production به منظور ترویج یک استاندارد برای چاپ روی تمام نسخه‌های لینوکس و کاربران آن توسعه داده شده است. CUPS از IPP[1] به عنوان مبنای مدیریت کارها و صفهای چاپ استفاده می‌کند. همچنین در آن از قراردادهای LPD[2]، SMB[3] و Appsocket به منظور سهولت بیشتر در انجام توابع استفاده می‌شود. CUPS برای پشتیبانی از عملیات چاپ تحت لینوکس، جستجوگر چاپگرهای شبکه و PPD[4] را نیز اضافه کرده است. همچنین شامل یک Image File RIP است که برای چاپگرهای non-Postscript به کار می‌رود. CUPS تحت مجوز GPL[5] است.

[1] Internet Printing Protocol
[2] Line Printer Daemon
[3] Server Message Block
[4] Postscript Printer Description
[5] GNU General Public Licanse

۸-۸-۱- مروری بر سامانه چاپ CUPS

مسالهٔ چاپ در لینوکس برای چند سال مشکل‌آفرین بود. بر خلاف ویندوز و Mac Os، لینوکس دارای واسط استانداردی برای چاپگرها نبود. به همین منظور CUPS برای حذف مشکلات چاپ طراحی شد. در واقع CUPS یک سامانه چاپ مشترک بین تمام نسخه‌های لینوکس است که نیازهای چاپ را برای کاربران برطرف می‌کند. CUPS دارای ویژگیهای قوی و منحصربه‌فردی است که سعی داریم در این بخش به برخی از آنان بپردازیم.

همان‌طور که گفتیم CUPS بر مبنای استاندارد واسطی که IPP نامیده می‌شود، پابرجاست. IPP یک قرارداد استاندارد برای چاپ و مدیریت کارهای چاپ و تنظیمات چاپگر مثل اندازه رسانه[1]، دقت[2] و ... تعریف می‌کند. مانند تمام قراردادهای IP-Based، IPP می‌تواند هم به صورت محلی و هم به صورت از راه دور یعنی در طول اینترنت روی چاپگرها با هزاران مایل فاصله استفاده شود و بر خلاف قراردادهای دیگر، در IPP می‌توان ازکنترل دسترسی، احرازهویت و رمزبندی[3] استفاده کرد و در نتیجه آن را کاراتر و امن‌تر از دیگر خدمات چاپ می‌سازد.

IPP یک لایه بالاتر از HTTP است. این پروتکل به کاربران اجازه می‌دهد تا مستندات خود را ببینند و وضعیت اطلاعات خود را روی چاپگر یا کارساز با استفاده از جستجوگرشان چک کنند.

کلیهٔ مستندات مربوط به CUPS را می‌توانید در وب‌گاه http://www.cups.org/ مشاهده نمایید.

معمولاً CUPS در سامبای ۳ و ۲،۲.x به طور پیش‌فرض نصب است و برای استفاده از آن کافی است به پرونده smb.conf رفته و تنظیمات موردنظر خود را انجام دهید. اما اگر CUPS روی سامانه شما نصب نبود، به چند طریق می‌توانید آن را نصب یا ترجمه کنید. به عنوان مثال روی سامانه RedHat می‌توانید پرونده rpm آن را دریافت نموده و با دستور زیر آن را اجرا نمایید:

```
# rpm –e lpr
# rpm –i cups-1.1.linux-M.m.n-intel.rpm
```

البته برای اجرای دستور فوق باید با کاربر root وارد شده باشید.

برای راه اندازی و ایست نمودن خدمت CUPS معمولاً بسته به بستری که استفاده می‌کنید، از دستورات زیر استفاده می‌شود:

```
# /etc/software/init.d/cups restart
# /etc/rc.d/init.d/cups restart
# /etc/init.d/cups restart
# /sbin/init.d/cups restart
```

دستورات فوق را باید مناسب انواع بسترها انتخاب کرد و به کار برد.

---

[1] media size
[2] resolution
[3] encryption

۸-۸-۲- تنظیمات پایه‌ای CUPS

برای استفاده از خدمت چاپ CUPS، در ساده‌ترین حالت فقط کافی است به پرونده smb.conf رفته و دو تنظیم زیر را انجام دهید:

Printing = cups

Printcap name = cups

برای روشن‌تر شدن نحوهٔ تنظیمات به مثال زیر که یک مثال بسیار ساده از سامانه چاپ CUPS است دقت نمایید:

```
[global]
        load printers = yes
        printing = cups
        printcap name = cups

[printers]
        comment = All Printers
        path = /var/spool/samba
        browseable = no
        public = yes
        guest ok = yes
        writable = no
        printable = yes
        printer admin = root, @ntadmins
```

با تنظیمات مثال فوق به راحتی می‌توانید تمام پرونده‌ها با قالبهای گرافیکی، متنی، PDF و Postscript را که از کارخواه‌های ویندوز دریافت می‌کنید، چاپ نمایید. مثال بعدی کمی پیچیده‌تر از مثال قبلی است و با استفاده از آن قادر خواهید بود خدمت CUPS را برای همه تعریف کنید. اما یک چاپگر را به طور متفاوت با تنظیمات خاص خودش تعریف نمایید. به تنظیمات آن در پرونده smb.conf دقت نمایید:

```
[global]
        printing = cups
        printcap name = cups
        load printers = yes

[printers]
        comment = All Printers
        path = /var/spool/samba
        public = yes
        guest ok = yes
        writable = no
        printable = yes
        printer admin = root, @ntadmins

[special_printer]
        comment = A special printer with his own settings
        path = /var/spool/samba-special
        printing = sysv
        printcap = lpstat
        print command = echo "NEW: `date`:  printfile %f" \
>> /tmp/smbprn.log ; \
echo " `date`:  p-%p s-%s f-%f" >> /tmp/smbprn.log ; \
echo " `date`:  j-%j J-%J z-%z c-%c" >> /tmp/smbprn.log ; rm %f
        public = no
        guest ok = no
        writable = no
        printable = yes
        printer admin = kurt
        hosts deny = 0.0.0.0
        hosts allow = turbo_xp, 10.160.50.23, 10.160.51.60
```

همان طور که در مثال مشاهده می‌کنید در تعریف و تنظیم چاپگر خاص، پارامترهای printing به sysv و printcap به lpstat تنظیم شده است. علاوه بر آن، admin چاپگر kurt است و نه admin@ و guest نیز اجازهٔ چاپ روی آن را ندارد و در لیست Network Neighborhood نیز ظاهر نمی‌شود. بنابراین برای استفاده از آن باید بدانید که این چاپگر وجود دارد. در ضمن طبق تنظیمات انجام شده فقط سه سامانه به آن دسترسی دارند.

۸-۸-۳- تنظیمات پیچیده‌تر در CUPS

برای انجام تنظیمات CUPS دو راه وجود دارد:

۱. استفاده از واسط وب

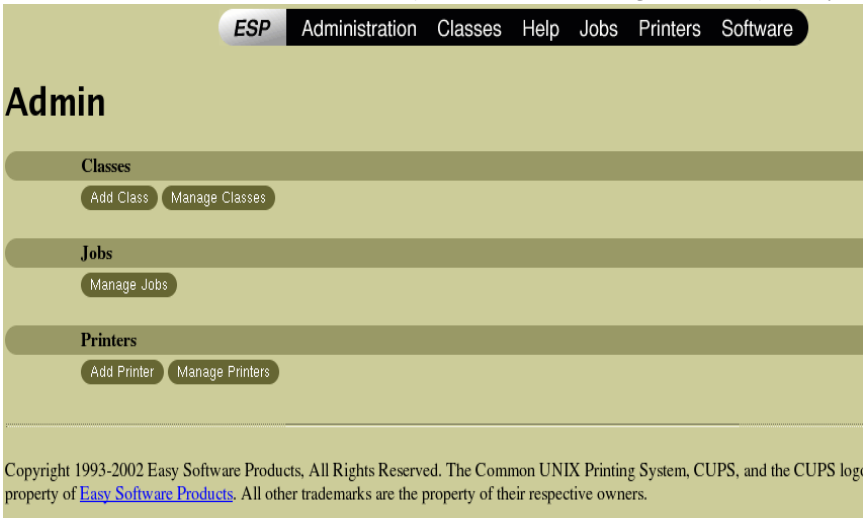
۲. استفاده از خط فرمان

۸-۹- استفاده از واسط وب

کارساز وب CUPS یک واسط خوب برای برخی تنظیمات CUPS ایجاد نموده است. برای استفاده از این واسط باید مرورگر مورد نظر خود را باز نموده و آدرس زیر را وارد نمایید:

http://localhost:631/admin

در صورت اجرای درست آن باید صفحه‌ای شبیه زیر مشاهده کنید:



با توجه به صفحهٔ فوق، باید برای اضافه کردن چاپگر، روی Add Printer کلیک نمایید و به تنظیمات خواسته شده پاسخ دهید. بقیهٔ تنظیمات نیز به همین ترتیب با واسط انجام می‌پذیرد.

۸-۱۰- استفاده از خط فرمان

همانطور که در ابتدای فصل نیز گفتیم، CUPS قابلیتهای فراوانی در مدیریت چاپ و کاربران آن دارد. برای استفاده از این قابلیتها و تنظیم آنها به کمک خط فرمان از دستور lpadmin می‌توان استفاده نمود. این دستور در شاخه /usr/sbin قرار دارد.

۸-۱۰-۱- اضافه کردن یک چاپگر

از دستور lpadmin با سوئیچ p– به منظور تصحیح و یا اضافه نمودن چاپگر استفاده می‌شود. برای اضافه نمودن یک چاپگر به CUPS باید از این دستور استفاده نمایید:

```
# /usr/sbin/lpadmin -p printer -E -v device -m ppd
```

مثلاً برای یک چاپگر HP DeskJet که به درگاه parallel متصل شده دستور فوق به صورت زیر به کار می‌رود:

```
# /usr/sbin/lpadmin  -p DeskJet -E  -v  parallel:/dev/lp1  -m  deskjet.ppd
```

و یا اضافه کردن یک چاپگر HP LaserJet با استفاده از واسط شبکه‌ای با آدرس 11.22.33.44 به صورت زیر است:

```
# /usr/sbin/lpadmin  -p LaserJet  -E –v  socket://11.22.33.44  -m laserjet.ppd
```

به طور کلی این دستور دارای سوئیچ‌های زیر است:

- -c *class*: اضافه کردن یک چاپگر به یک کلاس از چاپگرها. اگر آن کلاس وجود نداشته باشد، ایجاد می‌شود.
- -m *model*: یک نرم‌افزار راه‌انداز چاپگر استاندارد که معمولاً یک پرونده PPD است، را مشخص می‌کند. PPD معمولاً در مسیر /usr/share/cups/model قرار دارند. لیست کامل تمام مدلهای در دسترس را می‌توانید با استفاده از دستور lpinfo و سوئیچ m– روی سامانه خود مشاهده کنید.
- -r *class*: چاپگر مورد نظر را از لیست class مشخص شده حذف می‌کند. اگر آن class خالی باشد آن class را حذف می‌کند.
- -v *device-uri*: ابزاری که می‌خواهد با چاپگر ارتباط برقرار کند را تعیین می‌کند.
- -E: چاپگر را فعال ساخته و کارها را می‌پذیرد.
- -P *ppd-file*: یک پروندهPPD محلی برای نرم‌افزار راه‌انداز چاپگر تعیین می‌کند.
- -d *printer* : به منظور پیش‌فرض نمودن یک چاپگر.

۸-۱۰-۲- حذف یک چاپگر

برای حذف یک چاپگر از لیست چاپگرهای CUPS دستور زیر را به کار ببرید:

```
# /usr/sbin/lpadmin –x printer
```

۸-۱۰-۳- راه اندازی و ایست کردن یک چاپگر

دستورات enable و disable روی یک چاپگر، صف‌های[1] آن چاپگر را راه اندازی و ایست می‌کند. در واقع هر چاپگری که غیرفعال است، کارهایی که به آن می‌رسد را دریافت می‌کند اما تا مجدداً راه‌اندازی نشود، نمی‌تواند آن را چاپ کند. این قابلیت برای زمانی مفید است که نیاز دارید یک چاپگر را که به درستی کار نمی‌کند، اصلاح کنید. بعد از تعمیر آن، کلیهٔ کارهایی که به آن رسیده چاپ خواهند شد.

```
# /usr/bin/enable printer
# /usr/bin/disable printer
```

[1] queue

۸-۱۰-۴- قبول یا رد یک کار مربوط به چاپگر

برای قبول یا رد یک کار روی یک چاپگر خاص می‌توانید از دستورات زیر استفاده کنید:

```
# /usr/sbin/accept printer
# /usr/sbin/reject printer
```

۸-۱۱- تنظیم Quota روی چاپگر در CUPS

با استفاده از خدمت CUPS می‌توانید از لحاظ اندازه و تعداد صفحات روی هر چاپگر محدودیت ایجاد نمایید. دقت نمایید که این محدودیتهایی که تعیین می‌کنید روی تمام کاربران به طور یکسان اعمال می‌شود و نمی‌توانید یک کاربر خاص را از این محدودیت استثنا نمایید. به عنوان مثال می‌توانید تعیین کنید که هر کاربر فقط بتواند ۵ برگ چاپ کند. این محدودیتها با پارامترهای job-k-limit ، job-quota-period و job-page-limit تعیین می‌شود.

پارامتر job-quota-period مدت زمان پیگیری quota را تعیین می‌کند. این زمان به ثانیه است. بنابراین یک روز ۸۶۴۰۰ و یک هفته ۶۰۴۸۰۰ و یک ماه ۲۵۹۲۰۰۰ ثانیه خواهد بود. پارامتر job-k-limit محدودیت اندازهٔ کارها را به کیلو بایت مشخص می‌کند. بالاخره با پارامتر job-page-limit نیز می‌توانید تعداد صفحاتی را که کاربران می‌توانند چاپ کنند تعیین کنید. به مثال زیر توجه نمایید:

```
#/usr/sbin/lpadmin -p printer -o job-quota-period=604800 -o job-k-limit=1024
#/usr/sbin/lpadmin -p printer -o job-quota-period=604800 -o job-page-limit=10
```

۸-۱۱-۱- محدود نمودن کاربران برای دسترسی به یک چاپگر

علاوه بر تنظیمات فوق، امکان محدود نمودن دسترسی یک کاربر به یک چاپگر خاص نیز با دستور lpadmin با سوئیچ u- وجود دارد. البته به طور پیش‌فرض تمام کاربران به چاپگر دسترسی دارند.

```
# /usr/sbin/lpadmin -p printer  -u allow:all
```

اگر بخواهید اجازه دهید سه کاربر peter،paul و mary اجازهٔ چاپ داشته باشند، باید به صورت زیر عمل کنید:

```
# /usr/sbin/lpadmin -p printer  -u allow:peter,paul,mary
```

و اگر بخواهید برعکس عمل کنید:

```
# /usr/sbin/lpadmin -p printer  -u deny:peter,paul,mary
```

همچنین می‌توانید محدودیت را بر یک گروه خاص اعمال کنید:

```
# /usr/sbin/lpadmin -p printer  -u allow:peter,paul,mary, @printgods
```

در بالا علاوه بر سه کاربر مورد نظر، به اعضای گروه printgods نیز مجوز چاپ داده شده است.

نکته: توجه داشته باشید که CUPS در هر زمان فقط از یک لیست مجوز کاربران استفاده می‌کند. این لیست می‌تواند لیست allow و یا deny باشد. یعنی اگر شما یک لیست allow تعریف کنید و سپس یک لیست deny، لیست deny جایگزین لیست allow خواهد شد. یعنی **در هر زمان فقط یک لیست فعال خواهد بود.** به این ترتیب به راحتی می‌توانید چاپگرهای خود را مدیریت نمایید.

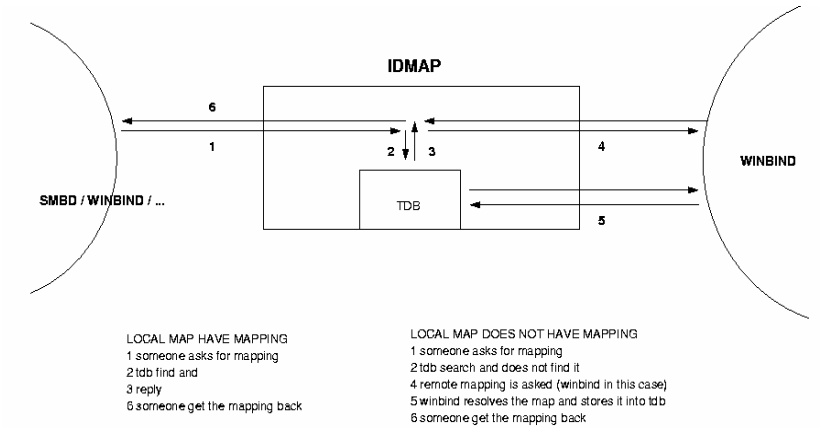
فصل نهم
استفاده از کاربران تعریف شده روی دامنه ویندوز
۹-۱- مقدمه

Winbind یکی از اجزای سامباست که مسالهٔ وارد شدن چندگانه را روی دامنه حل می‌کند. Winbind از پیاده‌سازی لینوکس برای فراخوانی RPC[1] تحت ویندوز، PAM[2] و NSS[3] به منظور اینکه کابران دامنه ویندوز NT بتوانند به عنوان کاربران لینوکس روی ماشین لینوکس کار کنند، استفاده می‌کند. در این فصل سامانه Winbind را توصیف می‌کنیم. و کارهایی را که می‌تواند انجام دهد را توضیح می-دهیم. همچنین به چگونگی تنظیم درست آن می‌پردازیم و اینکه چطور کار می‌کند.

Winbind سه کار مختلف زیر را انجام می‌دهد:

- احرازهویت و بررسی اعتبار کاربران با PAM
- تبدیل شناسه‌ها با NSS
- Winbind یک پایگاه داده به نام winbind_idmap.tdb نگهداری می‌کند که تبدیل بین شناسه‌های کاربری و گروهی لینوکس و شناسه‌های کاربری ویندوز NT را ذخیره می‌کند. این تبدیل فقط برای کاربران و گروه‌هایی استفاده می‌شود که هیچ UID/GID محلی ندارند.

همانطور که قبلاً نیز گفتیم، smbd است که winbind را فراخوانی می‌کند. حال اگر winbindd در حال اجرا نباشد، smbd از اطلاعات محلی /etc/passwd و/etc/group استفاده خواهد کرد و از هیچ نگاشت پویایی استفاده نخواهد کرد. به شکل دقت کنید:



1 Remote Procedure Calls
2 Pluggable Authentication Module
3 Name Service Switch

به خوبی می‌دانید که لینوکس و مایکروسافت ویندوز NT مدلهای متفاوتی را برای نمایش اطلاعات کاربر و گروه‌ها به کار می‌گیرند و نیز از فناوریهای مختلفی برای پیاده‌سازی آنها استفاده می‌کنند. به همین دلیل یکی نمودن آنها (دو سامانه) به طرز قابل قبول، مشکل خواهد بود. یک روش معمول که امروزه استفاده می‌شود این است که حسابهای کاربری با نامهای یکسان روی هر دو سامانه لینوکس و ویندوز ایجاد نموده و از برنامه‌های سامبا[1] برای فراهم نمودن تبادل خدمات پرونده و چاپ بین دو سامانه استفاده می‌کنند. اما در این روش چون به دو پایگاه داده مختلف نیاز است؛ کار کمی برای اضافه نمودن و حذف کاربران مشکل می‌شود. گاهی‌اوقات به مشکلات همزمان‌سازی[2] عملیات روی پایگاه‌های داده بر می‌خوریم. می‌توان مسائل مربوط به Unified logon برای سامانه-های لینوکس را به سه مسالهٔ کوچکتر تقسیم کرد:

- بدست‌آوردن اطلاعات گروه و کاربران ویندوز NT
- احرازهویت کاربران ویندوزی
- تغییر کلمهٔعبور برای کاربران ویندوز NT

با سامانه winbind یک راه‌حل ساده و خوب برای تمام مسائل فوق می‌توان ایجاد کرد.

از winbind در سازمانهایی استفاده می‌شود که یک ساختار دامنه مبتنی بر NT دارند و می‌خواهند در آن از کارسازها و ایستگاه‌های کاری لینوکس استفاده کنند. Winbind به این سازمانها اجازه می‌دهد تا سامانه‌های لینوکس خود را به دامنه اضافه کنند، بدون اینکه نیازی به نگهداری یک ساختار جدا برای حسابهای کاربری باشد. این مساله باعث سادگی بسیاری در مدیریت شبکه خواهد شد و از ایجاد سربار می‌کاهد.

۹-۲- Winbind چگونه کار می‌کند؟

سامانه winbind بر اساس معماری کارخواه/کارساز[3] است. هنگامی که کارساز winbindd در حال اجراست، به دامنه لینوکس گوش می‌دهد و منتظر رسیدن درخواست است. این درخواستها توسط کارخواه‌های NSS و PAM تولید می‌شوند و به طور مرتب فرآیند می‌شوند.

مواردی که winbind از آنها استفاده می‌کند آورده شده است:

۹-۳- Microsoft Remote Procedure Calls

همان طور که می‌دانید، از RPC برای عملیات مختلف مرتبط با شبکه بین ماشینهای ویندوز از قبیل مدیریت راه‌دور، احرازهویت کاربران و عملیات spooling چاپ استفاده می‌شود. Winbind از RPC مختلفی برای تعیین گروه‌ها و کاربران دامنه و بدست آوردن اطلاعات جزئی آنها استفاده می‌کند. وقتی یک درخواست برای بدست آوردن اطلاعات کاربر و گروه مستقیماً به یک PDC ویندوز فرستاده می‌شود، winbind اطلاعات حساب کاربری NT را به نام کاربری و گروه در لینوکس تبدیل می‌کند.

---

[1] Samba Suit
[2] Synchronize
[3] client/server

۹-۴- Name Service Switch

NSS یکی از ویژگیهایی است که امروزه در اکثر سامانه‌های عامل لینوکس وجود دارد. این خدمت کنترل چگونگی دسترسی به پایگاه‌های داده اطلاعاتی مورد نیاز توسط mail aliases، اطلاعات کاربران، نام میزبانها و غیره را بر عهده دارد. مثلاً یک ایستگاه کاری لینوکس می‌تواند اطلاعات مورد نیازش را از یکسری پرونده‌ها روی یک سامانه پرونده محلی بدست آورد. یک سامانه شبکه‌ای ممکن است در ابتدا تلاش کند تا اطلاعاتش را از روی پرونده‌های محلی بدست آورد، سپس با یک پایگاه داده NIS برای اطلاعات کاربری مشاوره کند و یا از یک کارساز DNS برای اطلاعات hostname کمک بگیرد. برنامه‌های واسط کاربردی NSS به winbind اجازه می‌دهد تا خود را به عنوان یک منبع اطلاعاتی در هنگام تطبیق نام کاربری و نام گروه در لینوکس معرفی کند. Winbind از این واسطه‌ها استفاده می‌کند و اطلاعات بدست آمده از کارساز ویندوز NT توسط RPC را برای تهیهٔ اطلاعات جدید کاربران به کار می‌گیرد. به این ترتیب، می‌توان اطلاعات کاربران یک دامنه NT را از روی یک ماشین لینوکس که در حال اجرای winbind است، بدست آورد. همچنین می‌توان اطلاعات کاربران دامنه‌هایی که به دامنه مورد نظر اعتمادسازی شده‌اند، را نیز دید.

پرونده کنترل اولیهٔ NSS، etc/nsswitch.conf/ است. وقتی یک خدمت در لینوکس درخواستی برای گرفتن اطلاعات می‌دهد، کتابخانهٔ C پرونده etc/nsswitch.conf/ و خطی که مربوط به تنظیمات آن خدمت مورد نظر است را بررسی می‌کند. به عنوان مثال برای خدمت passwd اگر در پرونده nsswitch.conf به صورت زیر تنظیم شده باشد:

Passwd: file example

کتابخانهٔ C اول پیمانه lib/libnss_files.so/ و سپس پیمانه lib/libnss_example.so/ را فراخوانده و در آنها به دنبال اطلاعات درخواستی می‌گردد و از هر کدام که توانست اطلاعات را بگیرد به درخواست مورد نظر پاسخ می‌دهد.

این واسط NSS یک راه آسان برای winbind مهیا می‌کند که همهٔ آنچه قرار بود از طریق فوق انجام شود، در پرونده libnss_winbind.so در شاخه lib/ قرار داده می‌شود و "winbind" در پرونده etc/nsswitch.conf/ در مکان مناسب قرار داده می‌شود. از این به بعد کتابخانهٔ C برای پاسخگویی به درخواستهای تطبیق اطلاعات نام کاربران و گروه‌ها، winbind را صدا می‌زند.

۹-۵- Pluggable Authentication Modules

Pluggable Authentication Modules که PAM نیز خوانده می‌شود، یک سامانه مجزا برای احرازهویت و مجوزدهی است. با PAM می‌توان بدون ترجمه دوبارهٔ برنامه‌های کاربردی مختلف برای آنها روشهای احرازهویت متفاوتی تعیین کرد. PAM همچنین برای سیاست‌گذاریهای خاص مجوزدهی مفید خواهد بود.

Winbind از واسط PAM مربوط به مدیریت کلمات‌عبور و مدیریت احرازهویت برای یکی کردن سیاستهای ویندوز و لینوکس استفاده می‌کند. در نتیجهٔ این امر، کاربران ویندوز NT می‌توانند روی یک ماشین لینوکس وارد شده‌اند و در برابر یک PDC مناسب احرازهویت شوند و همچنین می‌توانند کلمات‌عبور خود را تغییر دهند.

PAM توسط پرونده‌های کنترلی در شاخه /etc/pam.d تنظیم می‌شود. البته برای هر خدمتی که نیاز به احرازهویت دارد. وقتی یک درخواست احرازهویت از یک برنامهٔ کاربردی صادر می‌شود، کدهای PAM در کتابخانهٔ C در قسمت مربوطه بررسی می‌شود. مانند NSS، در اینجا نیز یک واسط به Winbind اختصاص می‌یابد و کارهای بررسی به او واگذار می‌شود و همهٔ آنچه که باید بررسی شود در پرونده pam_winbind.so در شاخه /lib/security قرار داده می‌شود.

۹-۶- User and Group Allocation

هر گاه در ویندوز NT/200x یک کاربر یا گروه ایجاد می‌شود، یک شناسه نسبی[1] به آن اختصاص می‌یابد که این شمارهٔ شناسه نسبی کمی با شماره‌ای که لینوکس به کاربر و گروه اختصاص می‌دهد متفاوت است. کار Winbind تبدیل شناسه نسبی به شناسه لینوکس و بالعکس است. نتیجهٔ این تبدیلها به طور دائمی در یک پایگاه داده مربوط به نگاشت شناسه در یک پایگاه داده tdb ذخیره می‌شود و در نتیجه یک روش ثابت و پایداری برای تبدیل شناسه‌های نسبی به شناسه‌های لینوکس خواهد شد.

۹-۷- Result Caching

در یک سامانه فعال عمل جستجو و تبدیل نام کاربر و گروه مرتباً در حال انجام است. برای کاهش هزینه‌ای که شبکه بدین منظور صرف می‌کند، Winbind می‌تواند از یک سامانه Caching استفاده نماید. بدین ترتیب اطلاعاتی که از PDC دریافت می‌شود به همراه یک شماره از PDC توسط Winbind، Cache می‌شود. این شماره هر بار که اطلاعات هر کاربر یا گروهی تغییر می‌کند، اضافه می‌شود. هر بار که اطلاعات Cache قدیمی[2] می‌شود، شمارهٔ مورد نظر با آنچه روی PDC است، مقایسه می‌شود. اگر با هم یکسان نبودند، اطلاعات موجود روی Cache کنار گذاشته می‌شود و مستقیماً از روی PDC اطلاعات دریافت می‌شوند.

۹-۸- نصب و تنظیم Winbind

در این بخش تنظیمات و کارهای مربوط به نصب Winbind را بررسی می‌کنیم. قبل از شروع به نصب و تنظیم، لازم است به نکات زیر دقت نمایید:

اول اینکه اگر پرونده تنظیمات سامبای شما در حال حاضر به درستی کار می‌کند، از آن یک پشتیبان تهیه نمایید. اگر سامانه شما از PAM استفاده می‌نماید از کل محتویات شاخه /etc/pam.d پشتیبان تهیه نمایید و در آخر اینکه اگر دیسکت راه‌انداز نساخته‌اید، الآن آن را بسازید!

دلیل پشتیبان گرفتن از موارد فوق این است که در مورد PAM، اگر پرونده تنظیمات آن بهم بریزد تقریباً login کردن روی سامانه شما غیر ممکن است. آخرین نسخهٔ سامبای ۳ شامل خدمت Winbind است که می‌توانید آن را از وب‌گاه بدست آورید.

برای اینکه کاربران دامنه بتوانند به پرونده‌ها و منابع به اشتراک گذاشته شده سامبا و کلاً خدماتی که توسط کارساز سامبا ارائه می‌شود دسترسی داشته باشند، باید PAM روی سامانه شما به درستی

---

[1] Relative Identifier (RID)
[2] Expire

نصب و تنظیم شده باشد. برای ترجمه پیمانه‌های Winbind شما باید حداقل کتابخانهٔ PAM را نصب شده روی سامانه خود داشته باشید. (PAM development libraries) به وب‌گاه PAM مراجعه کنید:
http://www.kernel.org/linux/libs/pam/

همچنین لازم است قبل از تنظیم، تمام خدمات سامبا که در حال اجرا هستند را متوقف کنید. مثل nmbd، smbd و winbindd و نیز مطمئن شوید که بسته‌های استاندارد PAM در شاخه /etc/pam.d قرار دارند.

۹-۹- تنظیم nsswitch.conf و winbind Libraries روی لینوکس

PAM یک جز استاندارد در نسخه‌های سامانه‌عامل لینوکس است ولی متأسفانه فقط تعداد کمی از این سامانه‌ها کتابخانه‌های مربوط به pam-devel را که برای سامبا و تنظیماتش نیاز است نصب می‌کند. به علاوه سامبای۳ به طور خودکار پرونده‌های winbind را در محلهای مناسب روی سامانه شما نصب می‌کند. پس ممکن است برای تنظیمات فقط به تغییر در پرونده nsswitch.conf نیاز داشته باشید.

کتابخانه‌های مورد نیاز برای اجرای صحیح خدمت winbind با nsswitch لازم است در محلهای صحیح کپی شوند. با دستور زیر این کار را انجام دهید:

```
# cp ../samba/source/nsswitch/libnss_inbind.so      /lib
```

همچنین خوب است symbol link زیر را نیز ایجاد کنید:

```
# ln –s /lib/libnss_winbind.so /lib/libnss_winbind.so.2
```

حال، به عنوان کاربر root باید پرونده /etc/nsswitch.conf را ویرایش کرده و اجازه دهید تا گروه‌ها و کاربران توسط خدمت winbind قابل رویت باشند. پس به پرونده nsswitch.conf رفته و آن را به شکل زیر تنظیم کنید:

```
passwd  :  files winbind
shadow  :  files
group   :  files winbind
```

کتابخانه‌های مورد نیاز خدمت winbind بعد از هر بار راه‌اندازی مجدد سامانه به طور خودکار به Idconfig Cache وارد می‌شوند. ولی برای اینکه این کار سریع‌تر انجام شود و نیاز به راه‌اندازی مجدد سامانه نباشد، می‌توانید با دستور زیر به طور دستی این کار را انجام دهید:

```
# /sbin/Idconfig  -v | grep winbind
```

دستور فوق، libnss_winbind را برای خدمت winbindd قابل دسترس می‌کند.

۹-۱۰- تنظیم smb.conf برای Winbind

برای کنترل نحوهٔ عملکرد winbindd چند پارامتر در پرونده smb.conf نیاز است. این پارامترها در صفحات کمکی مربوط به winbindd(8) به طور جزیی آورده شده‌اند. به شکل زیر که قسمت global از پرونده smb.conf است دقت کنید. پارامترهایی که باید تنظیم شوند در شکل مشخص شده‌اند:

```
[global]
# separate domain and username with '\', like DOMAIN\username
        winbind separator = \
# use uids from 10000 to 20000 for domain users
        idmap uid = 10000-20000
# use gids from 10000 to 20000 for domain groups
        idmap gid = 10000-20000
# allow enumeration of winbind users and groups
        winbind enum users = yes
        winbind enum groups = yes
# give winbind users a real shell (only needed if they have telnet access)
        template homedir = /home/winnt/%D/%U
        template shell = /bin/bash
```

۹-۱۱- اتصال کارساز سامبا به دامنه PDC

دستور زیر را برای اتصال کارساز سامبا به یک دامنه PDC به کار ببرید: PDC نام دامنه و Administrator نام کاربری است که در دامنه مجوز لازم را برای این کار دارد:

```
# /usr/local/samba/bin/net rpc join  -S  PDC  -U  Administrator
```

پاسخ مناسب دستور فوق از سوی سامانه به صورت زیر باید باشد:

"joined the domain DOMAIN."

که DOMAIN نام دامنه مورد نظر شماست.

برای اینکه خدمت winbindd را راه اندازی کنید، کافی است دستور زیر را به کار ببرید:

```
# / usr/local/samba/sbin/winbindd
```

نکته: در توضیحات فوق فرض شده است که سامبا در شاخه /usr/local/samba نصب شده است. ممکن است نیاز باشد محل نصب سامبا روی سامانه خود را پیدا کنید.

جالب است بدانید که winbindd می‌تواند در حالت dual[1] اجرا شود. یعنی دو فرآیند در حال اجرا باشد. اولی فقط برای پاسخگویی به در خواستها به کمک cache که سریع‌تر به کارخواه پاسخ داده شود و دومی به منظور بروز رسانی cache برای درخواستهایی که در cache نیستند و برای اولین بار پرسیده می‌شوند. کار کردن winbindd در این حالت باعث می‌شود نتیجه کار آن دقیق‌تر و سریع‌تر باشد. برای اینکه winbindd را به حالت dual ببرید باید از B- استفاده نمایید:

```
# /usr/local/samba/sbin/winbindd  -B
```

اگر می‌خواهید از در حال اجرا بودن winbind مطمئن شوید، دستور زیر را اجرا کنید و در لیست خروجی از وجود winbindd مطمئن شوید.

[1] Dual daemon mode

```
# ps  -ae | grep winbindd
```

در صورت وجود آن باید خطی شبیه خط زیر در خروجی مشاهده کنید:

```
3025  ?          00 : 00 : 00  winbindd
```

حال می‌توانید یکسری اطلاعات درباره کاربران دامنه خود ببینید:

```
# /usr/local/samba/bin/wbinfo   -u
```

دستور فوق باید لیستی از کاربران روی ویندوز PDC بدهد، مثلاً:

```
CEO\Administrator
CEO\burdell
CEO\Guest
CEO\jt-ad
CEO\krbtgt
CEO\TsInternetUser
```

واضح است که نام دامنه مثال فوق CEO و جدا کنندهٔ winbind هم "\" است.
با سوئیچ g- گروه‌ها را می‌بینید:

```
# /usr/local/samba/bin/wbinfo –g
```

```
CEO\Domain Admins
CEO\Domain Users
CEO\Domain Guests
CEO\Domain Computers
CEO\Domain Controllers
CEO\Cert Publishers
CEO\Schema Admins
CEO\Enterprise Admins
CEO\Group Policy Creator Owners
```

با تابع getent نیز می‌توانید تمام کاربران روی PDC و نیز سامانه خود را مشاهده کنید. به صورت زیر:

```
# getent passwd
# getent group
```

۹-۱۲- تنظیم winbind با PAM

اگر بخواهید از winbind برای احرازهویت خدمات دیگر استفاده کنید باید در پرونده‌های تنظیم PAM تغییراتی را بدهید باز هم تأکید می‌کنم که اگر تا به حال از شاخه /etc/pam.d پشتیبانی نگرفته‌اید، حال وقت آن است که این کار را انجام دهید.

برای استفاده winbindd با خدمات دیگر به یک پیمانه PAM نیاز دارید که این پیمانه باید با دستور زیر در شاخه source/nsswitch/.. کامپایل شود.

```
# make   nsswitch/pam-winbind.so
```

پرونده pam-winbind.so باید در محل پیمانه‌های دیگر PAM Security کپی شود. این محل در بستر های مختلف فرق می‌کند. مثلاً در RedHat شاخه lib/security/ و در solaris شاخه usr/lib/security/ خواهد بود.

```
# cp  ../samba/source/nsswitch/pam-winbind.so    /lib/security
```

در اینجا برای بسترهای Linux/FreeBSD-specific تنظیمات PAM را انجام می‌دهیم. پرونده etc/pam.d/samba/ نیازی به تغییر ندارد.

برای اینکه اجازه دهیم خدمات دیگر نظیر Telnet، ورود معمولی و FTP با winbind احرازهویت شوند، باید تغییراتی را در اطلاعات ورودی etc/xientd/ (یا etc/inetd.conf/) بدهیم. در RedHat7.1 و بعد از آن برای تغییرات باید خطهای enable=no از پرونده‌های etc/xientd.d/telnet/ و etc/xinetd.d/wuftp/ را به enable=yes تغییر دهید.

برای اینکه خدمت ftp به درستی کار کند همچنین نیاز است که یا شاخه‌های خاص کاربران دامنه را روی کارساز داشته باشید و یا اینکه home directory template را به یک شاخه general برای تمام کاربران دامنه تغییر دهید. این کار به راحتی با استفاده از پارامتر global template homedir انجام می‌شود.

پرونده etc/pam.d/ftp/ می‌تواند به صورت زیر برای اینکه winbind ftp به پرونده سامبا دسترسی داشته باشد تغییر کند:

```
auth       required     /lib/security/pam_listfile.so item=user sense=deny \
    file=/etc/ftpusers onerr=succeed
auth       sufficient   /lib/security/pam_winbind.so
auth       required     /lib/security/pam_stack.so service=system-auth
auth       required     /lib/security/pam_shells.so
account    sufficient   /lib/security/pam_winbind.so
account    required     /lib/security/pam_stack.so service=system-auth
session    required     /lib/security/pam_stack.so service=system-auth
```

همچنین می‌توانید پرونده /etc/pam.d/login را به صورت زیر تغییر دهید:

```
auth       required     /lib/security/pam_securetty.so
auth       sufficient   /lib/security/pam_winbind.so
auth       sufficient   /lib/security/pam_unix.so use_first_pass
auth       required     /lib/security/pam_stack.so service=system-auth
auth       required     /lib/security/pam_nologin.so
account    sufficient   /lib/security/pam_winbind.so
account    required     /lib/security/pam_stack.so service=system-auth
password   required     /lib/security/pam_stack.so service=system-auth
session    required     /lib/security/pam_stack.so service=system-auth
session    optional     /lib/security/pam_console.so
```

در شکل فوق، ابتدا خط auth sufficient /lib/security/pam-winbind.so و سپس خط reguired pam-securetty.so که باعث می‌شود کاربر root روی شبکه وارد نشود، اضافه شده است. همچنین خط sufficient/lib/security/pam-unix.so use-first-pass بعد از خط winbind.so اضافه شده است، که شناسه نسبی را می‌گیرد.

با توجه به مطالب فوق، winbind با استفاده از NSS، PAM و RPC مناسب باعث یکی بودن سیاستهای دو بستر ویندوز و لینوکس شده و بدین ترتیب در کاهش هزینه‌های مدیریت و پیچیدگی آنها تاثیر بسیاری خواهد داشت.

۹-۱۳- فنون پشتیبان‌گیری

پروژهٔ سامبا، پروژهٔ ۱۰ سال اخیر است که سازندگان اصلی آن مدیران سامانه‌ها هستند. مدیران سامانه‌های لینوکس از ابزارهای لینوکس برای پرونده سامانه‌های آن استفاده می‌کنند. در چهارسال گذشته شمار مدیران سامانه شبکه‌های ویندوز که به سامبا علاقه پیدا کرده‌اند، افزایش یافته است. که این مساله باعث بروز سوالات زیادی در مورد چگونگی تهیه پشتیبان شده است.

سه نرم افزار مجانی که در ادامه توضیح داده شده‌اند، می‌توانند برای فنون تهیهٔ پشتیبان، مفید واقع شوند.

۹-۱۳-۱- Backup PC

Backup PC نسخهٔ ۲،۰،۰ در sourceforge منتشر شده است. ویژگیهای جدید در وب‌گاه <http://backuppc.sourceforge.net> شامل حمایت از /sync/rsyncd و واسطهای CGI به منظور جهانی‌سازی آن است. (شامل انگلیسی، فرانسوی، اسپانیولی و آلمانی)

Backup PC یک بسته مبتنی بر زبان برنامه‌نویسی Perl با کارایی بسیار بالا جهت گرفتن پشتیبان از لینوکس، یونیکس و یا رایانه‌های شخصی و قابل حمل ویندوز، به یک دیسک کارساز است. این نرم‌افزار را به طور دقیق می‌توان تنظیم نمود و نیز از نظر نصب و نگهداری راحت و آسان است.

Backup PC تحت مجوز GPL است و روی کارخواه‌های لینوکس/یونیکس/Freenix اجرا می‌شود و روی لینوکس، یونیکس، ویندوز 9x/ME، win 98، win xp و Mac osx آزمایش شده است.

۹-۱۳-۲- Rsync

Rsync یک برنامه انعطاف‌پذیر برای گرفتن پشتیبان پرونده‌ها یا شاخه‌هاست. Rsync، گزینه‌های زیادی برای چگونگی کپی پرونده‌ها و انتقال آنها دارد و از آن می‌توان برای ftp و http، scp یا rcp استفاده کرد.

قرارداد rsync remote-update به آن اجازه می‌دهد که فقط اختلاف بین دو مجموعه از پرونده‌ها را در روی شبکه منتقل کند. این کار را با استفاده از یک الگوریتم کارای checksum-search که در بستهٔ rsync توضیح داده شده است، انجام می‌دهد.

بعضی از ویژگیهای اضافه در rsync به قرار زیر هستند:

- حمایت از کپی پیوند، ابزار، مالکیت، گروه و مجوزها
- نیازی به مجوز root ندارد. (privilege)
- توسط ssh یا rsh می‌تواند استفاده شود.

۹-۱۳-۳- Amanda[1]

Amanda یک سامانه تهیهٔ پشتیبان است که به مدیران LAN اجازه می‌دهد تا یک کارساز پشتیبان master را برای تهیهٔ پشتیبان از چند میزبان به یک فضای حافظه بزرگ مثل Tape drive تنظیم کنند. Amanda می‌تواند از شمار زیادی از ایستگاه‌های کاری که دارای نسخه‌های مختلف از لینوکس هستند، پشتیبان تهیه کند. نسخه‌های اخیر آن حتی می‌تواند از سامبا برای تهیهٔ پشتیبان از میزبانهای ویندوز نیز استفاده کند.

برای اطلاعات دقیق‌تر می‌توانید به وب‌گاه http://www.amanda.org مراجعه نمائید.

۹-۱۳-۴- BOBS[2]

BOBS نیز یک سامانه تهیهٔ پشتیبان برخط[3] کامل است که از یک دیسک بزرگ (حجیم) برای ذخیرهٔ پشتیبانها استفاده می‌کند و کاربران پرونده‌ها را با استفاده از یک مرورگر وب جستجو می‌کند. وب‌گاه آن هم به آدرس زیر است:

<http://bobs.sourceforge.net/>

[1] Advanced Maryland Automatic Network Disk Archive
[2] Browseable Online Backup System
[3] Online

فصل دهم
مهاجرت از نسخه های قدیمی سامبا به نسخه ۳
۱۰-۱- مقدمه
در این فصل به تفاوتهای بین دو نسخهٔ ۲،۲،۸ و ۳،۰،۰ سامبا می‌پردازیم و بررسی می‌کنیم که کدامیک از پارامترهای تنظیم در آن تغییر کرده است و نیز چگونگی حرکت از ۲،۲.x به ۳،۰،۰ را بیان می‌نمائیم.

رفتار پیش‌فرض نسخهٔ ۳،۰،۰ تقریباً شبیه رفتار نسخهٔ ۲،۲.x است. در واقع وقتی پارامترهای جدید passdb backend در پرونده smb.conf تعریف شده‌اند، سامبای ۳ همان سامبای ۲،۲.x با پارامتر encrypt passwords = yes است و از پایگاه داده smbpassed استفاده می‌کند. یک نکتهٔ جالب و خوب این است که در طول upgrade دو نسخه به هم، دامنه و machine SID حفظ می‌شوند.

۱۰-۲- امکانات جدید در سامبای ۳
حداقل چهارده ویژگی جدید در سامبای ۳ وجود دارند:

۱. حمایت از Active Directory. این نسخه قادر است به یک ADS realm به عنوان عنصر کارساز متصل شود و با استفاده از LDAP/Kerberos کاربران را احرازهویت کند.
۲. حمایت از یونی کد[1].
۳. سامانه جدید احرازهویت. سامانه احرازهویت داخلی تقریباً به طور کامل بازنویسی شده است.
۴. سامانه جدید filename mangling که کاملاً بازنویسی شده است و دیگر یک پایگاه داده داخلی mangling map را به طور دائمی ذخیره می‌کند.
۵. دستور جدید "net" اضافه شده است که تا حدی شبیه دستور "net" در ویندوز است. سعی شده است تا دسته‌ای از برنامه‌ها و دستورات کاربردی مثل smbpassad با زیر دستورات net جایگزین شوند.
۶. سامبا در نسخهٔ ۳ می‌تواند با کدهای NT-style status32 در طور کابل شبکه مذاکره کند که این مساله به طور قابل ملاحظه‌ای مدیریت خطاها را بهتر می‌کند.
۷. حمایت بهتر از خدمت چاپ WIN XP/200X.
۸. پیمانه‌هایRPC قابل بارگذاری جدید برای passdb backend و مجموعه‌های کاراکتری[2].
۹. کار کردن winbindd در حالت dual به طور پیش‌فرض به منظور کارایی بهتر.
۱۰. حمایت برای انتقال یا بروز رسانی از یک دامنه win NT 4.0 به دامنه سامبا با نگهداری و حفظ کاربران و گروه‌ها و شناسه‌های امنیتی دامنه.
۱۱. حمایت از تشکیل ارتباطات معتمد[1] با NT 4.0 DomainController

[1] Unicode
[2] Character set

۱۲.حمایت اولیه و ابتدایی از معماری winbind توزیع شده[2] با استفاده از شاخه LDAP جهت ذخیرهٔ تبدیل SID به UID/GID.
۱۳.بروز رسانی به samba documentation tree
۱۴.حمایت کامل از امضای کارسازها و کارخواه‌های SMB برای اطمینان از سازگاری با تنظیمات امنیتی ویندوز 2003.

علاوه بر موارد فوق موارد بسیار دیگری نیز وجود دارد.

یک لیست مختصر از گزینه‌هایی که در پرونده smb.conf در نسخهٔ ۳،۰،۰ تغییر کرده‌اند، در اینجا آورده شده است.

همچنین می‌توانید به صفحات کمکی smb.conf نیز مراجعه کنید.

پارامترهای که حذف شده‌اند:

- admin log
- alternate permissions
- character set
  - client codepage
  - code page directory
  - coding system
  - domain admin group
  - domain guest group
  - force unknown acl user
  - nt smb support
  - post script
  - printer driver
  - printer driver file
  - printer driver location
  - status
  - strip dot
  - total print jobs
  - use rhosts
  - valid chars
  - vfs options

[1] Trust
[2] Distributed

پارامترهایی که جدید اضافه شده اند:

این پارامترها بسته به نوع کارشان دسته‌بندی شده اند

Remote Management

- abort shutdown script
- shutdown script

User and Group Account Management:

- add group script
- add machine script
- add user to group script
- algorithmic rid base
- delete group script
- delete user from group script
- passdb backend
- set primary group script

Authentication:

- auth methods
- realm

Protocol Options:

- client lanman auth
- client NTLMv2 auth
- client schannel
- client signing
- client use spnego
- disable netbios
- ntlm auth
- paranoid server security
- server schannel
- server signing
- smb ports
- use spnego

File Service:

- get quota command
- hide special files
- hide unwriteable files
- hostname lookups
- kernel change notify
- mangle prefix
- map acl inherit
- msdfs proxy
- set quota command
- use sendfile
- vfs objects

Printing:

- max reported print jobs

Unicode and Character Sets:

- display charset
- dos charset
- unicode
- UNIX charset

SID to UID/GID Mappings:

- idmap backend
- idmap gid
- idmap uid
- winbind enable local accounts
- winbind trusted domains only
- template primary group
- enable rid algorithm

LDAP:

- ldap delete dn
- ldap group suffix
- ldap idmap suffix
- ldap machine suffix
- ldap passwd sync
- ldap user suffix

General Configuration:

- preload modules
- privatedir

پارامترهایی که اصلاح شده اند یا تغییر کرده‌اند:

- encrypt passwords (enabled by default)
- mangling method (set to hash2 by default)
- passwd chat
- passwd program
- password server
- restrict anonymous (integer value)
- security (new ads value)
- strict locking (enabled by default)
- winbind cache time (increased to 5 minutes)
- winbind uid (deprecated in favor of idmap uid)
- winbind gid (deprecated in favor of idmap gid)