

سامبا

ترجمه و تالیف:

محمود تقی زاده

آناهی تا فی روزی

فهرست مطالب

مقدمه

فصل اول: به دست آوردن و نصب سامبا

مقدمه و ساختار سامبا و چگونگی نصب آن

تنظیم سامبا

ساختار سرویس دهنده سامبا

بررسی صحت فایل smb.conf با برنامه testparm

استفاده از ابزار مبتنی بر وب swat برای تنظیم و مدیریت سامبا

دیدن لیست منابع مشترک روی سامبا

دسترسی به منابع به اشتراک گذاشته شده

چند نکته قابل ذکر

برخی خطاهای معمول در راه اندازی سامبا

فصل دوم: مثالها

مقدمه

مثال ۱: راه اندازی یک Document Server

مثال ۲: راه اندازی یک Read Write Document server

مثال ۳: راه اندازی یک سرور چاپ

مثال ۴: راه اندازی یک read write file & print server امن

مثال ۵: Domain Member server

فصل سوم: مودهای امنیتی در سامبا و انواع مختلف سرورها

مقدمه

انواع سرورها

مودهای امنیتی در سامبا

سطح امنیتی کاربر (user level security)

سطح امنیتی share (share level security)

سطح امنیتی Domain (user level security)

سطح امنیتی ADS (user level security)

سطح امنیتی server (user level security)

فصل چهارم: Stand-alone servers

مقدمه

Document server و Print server مرکزی

Document server

Print Server

فصل پنجم: دیتابیس های مربوط به اطلاعات accountها

مقدمه

مزیت کلمات عبور رمز شده

مزیت کلمات عبور رمز نشده

تبدیل شناسه های کاربری ویندوز و یونیکس

ابزارهای مدیریت account

دستور passwd

دستور pdbedit

فصل ششم: کنترل دسترسی به فایل های و شاخه ها و منابع اشتراکی

مقدمه

کنترل دسترسی به فایل سیستم

مقایسه فایل سیستم NTFS و فایل سیستم لینوکس

کنترل دسترسی به فایل ها و شاخه ها

کنترل دسترسی به منابع اشتراکی

کنترل بر اساس user و group

کنترل بر اساس مجوزهای File , Directory

برخی کنترل های دیگر

کنترل دسترسی روی منابع مشترک

Full control

مدیریت مجوزهای منابع مشترک در سیستم عامل های ویندوز و یونیکس

Windows NT4 workstation /Server

Windows 200x/xp
MS Windows Access Control List and UNIX Interoperability
دیدن File Security روی منابع مشترک سامبا

دیدن File ownership

دیدن مجوزهای فایل و دایرکتوری‌ها

مجوزهای فایل

مجوزهای دایرکتوری

تصحیح یا تغییر مجوز فایل یا دایرکتوری

بررسی پارامتر mask در سامبا

فصل هفتم: Securing Samba

مقدمه

استفاده از host-based protection

استفاده از user-based protection

استفاده از interface protection

استفاده از Firewall

استفاده از IPC\$ Share-Based Denials

NTLMv2 security

به روز رسانی سامبا

فصل هشتم: Classical Printing Support and CUPS

مقدمه

مقدمهٔ تکنیکی

مراحل پردازش چاپ از سرویس‌گیرنده به سرویس‌دهندهٔ سامبا

پارامترهای مرتبط با تنظیمات چاپ در سامبا

تنظیمات سادهٔ چاپ

استفاده از برنامه Testparm

جزئیات بیشتر

نصب درایورها در [print\$]

ویزارد اضافه نمودن چاپگر

Common UNIX Printing System (CUPS)

مروری بر سیستم چاپ CUPS

تنظیمات پایه‌ای CUPS

تنظیمات پیچیده‌تر در CUPS

استفاده از اینترفیس وب

استفاده از command-line

حذف یک چاپگر

Start و Stop کردن یک چاپگر

قبول یا رد یک job مربوط به چاپگر

تنظیم Quota روی چاپگر در CUPS

محدود نمودن کاربران برای دسترسی به یک چاپگر

فصل نهم: استفاده از کاربران تعریف شده روی دامین وی‌اندوزی

مقدمه

Winbind چگونه کار می‌کند؟

Microsoft Remote Procedure Calls

Name Service Switch(NSS)

Pluggable Authentication Modules

User and Group Allocation

Result Caching

نصب و تنظیم Winbind

تنظیم nsswitch.conf و winbind Libraries روی لینوکس

تنظیم smb.conf برای Winbind

متصل نمودن سرور سامبا به دامین PDC

تنظیم winbind با PAM

تکنیکهای پشتیبان‌گیری

backup PC

Rsync

Amanda

BOBS: Browseable Online Backup System

فصل دهم: مهاجرت از سامبا نسخه قدیمی به سامبا نسخه ۳

مقدمه

فصل اول

به دست آوردن و نصب سامبا

مقدمه و ساختار سامبا و چگونگی نصب آن

معمولاً بسته سامبا در نسخه‌های ارائه شده توسط توزیع‌کنندگان لینوکس وجود دارد. برای استفاده از آن باید این بسته را روی پلت‌فرم دلخواه خود نصب نمایید. همچنین می‌توان این بسته را از سایت سامبا در آدرس `< http://samba.org >` نیز به دست آورد. به همراه بسته سامبا، فایل‌های کمکی و مستندات نیز برای راهنمایی نصب روی سیستم عامل وجود دارد که دارای جزئیات کافی برای نصب و تنظیم سامبا هستند. گاهی نیاز است که سامبا را از روی سورس^۱ آن کامپایل کرد که در فصل مربوط به آن به تفصیل آورده شده است. توجه کنید که معمولاً آخرین نسخه سامبا در سایت آن وجود دارد. برای شروع کار ابتدا باید از نصب سامبا روی سیستم عامل مطمئن شوید.

سامبا شامل سه بسته^۲ است:

۱. `samba-common`: که شامل فایل‌های مورد نیاز سرویس‌دهنده و سرویس‌گیرنده است.

^۱ Source

^۲ Package

۲. samba-server: که نسخه سرویس دهنده سامباست.

۳. samba-client: که شامل برنامه‌های smbprint و smbmount و smbclient

و مستندات مربوط به آنان است.

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

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

با وارد کردن دستور فوق هر دو بسته سرویس‌دهنده و سرویس‌گیرنده نصب خواهند شد. در

صورتی که فقط مایل به نصب سرویس‌گیرنده 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 سیستم عامل شما نصب شده است. حالا باید

به تنظیم آن پردازید.

تنظیم سامبا

کلیه تنظیمات مربوط به سامبا در فایل smb.conf ذخیره شده است. این فایل معمولاً در مسیر

/etc/samba/smb.conf و یا /usr/local/lib/samba/smb.conf قرار دارد. بسته به نظر

خودتان می‌توانید این فایل را دستی ویرایش کنید و یا اینکه از ابزارهایی که برای اینکار فراهم شده

است، مانند ایتترفیس مبتنی بر وب SWAT و یا linuxconf استفاده نمایید. توضیحات لازم در مورد

این ابزارها در پایان فصل به طور کامل آورده شده است.

شکل فایل smb.conf مانند فایل های قدیمی ini. در ویندوز 3.1 است. این فایل دارای

قسمتهای^۳ مختلفی است و با قرارگرفتن نام هر بخش درون علامت "[]" در یک خط جدید شروع

³ Section

می‌شود. هر بخش معرف یک منبع به اشتراک گذاشته شده روی سرویس‌دهنده سامبا است و شامل تنظیمات مربوط به همان بخش است. بخش "global" در فایل تنظیمات یک بخش ویژه و خاصی است که شامل تمام تنظیماتی است که روی کل سرویس‌دهنده سامبا اعمال می‌شود و مربوط به یک منبع به اشتراک گذاشته شده مجزا نمی‌باشد. در مثال زیر یک فایل 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 آنرا در فایل smb.conf وارد نمایید. البته این فقط ابتدای کار است. برای تنظیمات دقیقتر باید به پارامترهای دیگری که بعداً توضیح می‌دهیم دقت نمایید.

ساختار سرویس دهنده سامبا

سامبا شامل سه سرور⁴ است. هر سرور در لینوکس، یک برنامه کاربردی است که در پس زمینه⁵ سیستم عامل اجرا می‌شود و سرویس‌هایی را فراهم می‌کند. مثلاً این سرویسها می‌تواند سرویس وب باشد که

⁴ Daemon

⁵ Background

سرویس‌دهنده آن در لینوکس Apache است و در آنصورت سرور آن httpd خواهد بود. سرویس‌دهنده

سامبا نیز شامل سه سرور است که وجود دوتای آنها برای یک سرویس‌دهنده سامبا الزامی است:

nmbd: این سرور تمام درخواست‌های مربوط به Name Registration و Name Resolution را

مدیریت می‌کند و با وجود آن سرویس‌گیرندگان می‌توانند به سرویس‌دهنده‌ها و منابع مشترک آنها دسترسی

پیدا کنند. این سرور به عنوان WINS Server نیز می‌تواند عمل کند و تبدیل NetBIOSName به

آدرس IP را انجام دهد. علاوه بر این، nmbd تمام پروتکل‌های مبتنی بر UDP را اداره می‌کند و باید در

ابتدای کار سامبا اجرا شود.

smbd: این سرور نیز تمام سرویس‌های مبتنی بر TCP/IP را مدیریت می‌کند. همچنین کلیه کارهای

مربوط به تصدیق‌اصالت⁶ محلی سرویس‌گیرندگان را در صورت نیاز انجام می‌دهد و دسترسی به منابع مشترک

را فراهم می‌کند. smbd باید بلافاصله بعد از nmbd اجرا شود.

winbindd: وقتی سامبا عضوی در ویندوز NT4 و یا ADS Domain⁷ است، این سرور باید اجرا

شود. همچنین هنگامیکه سامبا یک ارتباط قابل اعتماد⁸ با دامین دیگری دارد، باید این سرور در حال اجرا

باشد. winbindd فایل smb.conf را برای وجود دو پارامتر idmap uid و idmap gid جستجو می‌کند.

اگر این دو پارامتر در فایل پیدا نشود، winbindd اصلاً اجرا نمی‌شود. جزئیات کار winbindd به طور کامل

در فصلهای بعد آورده شده است.

⁶ Authentication

⁷ Active Directory Server Domain

⁸ Trust Relationship

بررسی صحت فایل smb.conf با برنامه testparm

هر بار که در فایل smb.conf تغییری می‌دهید، بررسی درستی محتویات فایل smb.conf بعد از اعمال تغییرات در آن از اهمیت خاصی برخوردار است. با برنامه testparm می‌توان از صحت این فایل 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 به کار رفته در آن باید دستور زیر را وارد نمایید:

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

اگر هیچ مشکلی در فایل تنظیمات نباشد و testparm به درستی اجرا شود، این برنامه ابتدا پیغامی مبنی بر صحیح بودن فایل نمایش می‌دهد و سپس لیست منابع به اشتراک گذاشته شده‌ای را که در فایل تعیین کرده‌اید نشان می‌دهد. نحوه کار testparm به این صورت است که فایل smb.conf را به دقت تجزیه و تحلیل می‌کند^۹ و پارامترهای ناشناس و یا خطاهای syntax را گزارش می‌کند. بنابراین اکیداً توصیه می‌شود بعد از هر گونه تغییر در فایل smb.conf، برنامه testparm را اجرا نمایید و از صحیح بودن فایل اطمینان حاصل نمایید.

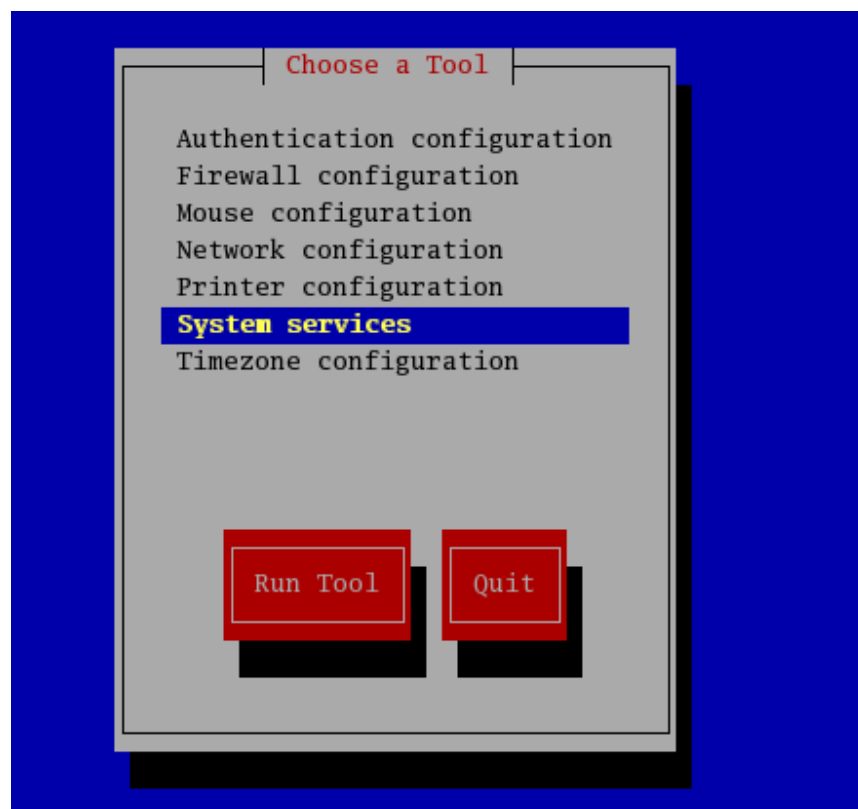
^۹ Parse

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

به غیر از تنظیم فایل `smb.conf` به طور دستی، 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 درباره SWAT در مستندات پلت فرم مورد علاقه شما آورده شده است. به `*/usr/doc/samba/` مراجعه کنید. همچنین در سایت `www.samba.org/doc` نیز این فایل توصیف شده است. برای استفاده از این ابزار باید ابتدا آنرا نصب نمایید، چون معمولاً این بسته به صورت پیش فرض نصب نمی شود. سپس در محیط `shell` مربوط به پلت فرم خود، دستور زیر را وارد نمایید:

```
# setup
```

با وارد نمودن دستور فوق؛ یک ویزارد گرافیکی مانند زیر مشاهده می کنید. دقت کنید که ما در اینجا از پلت فرم RedHat 9.0 استفاده کرده ایم و ممکن است در پلت فرم های مختلف در جزئیات، کمی تفاوت مشاهده کنید.



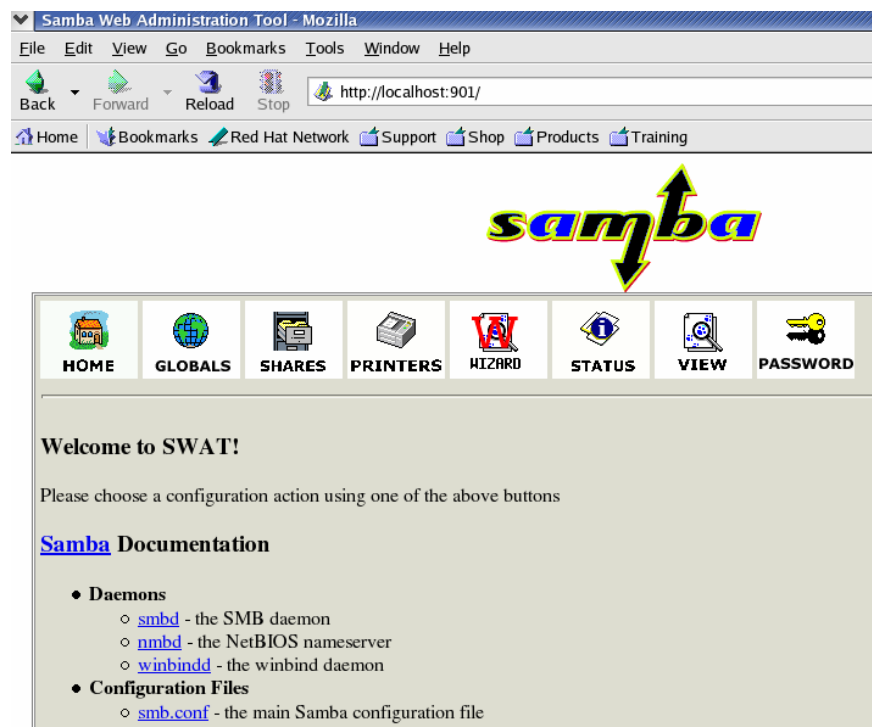
System services را انتخاب کرده و سپس در لیست، مقابل Swat را علامت بزنید:



حال باید سرویس xinetd را restart کنید: (در بعضی پلتفرمها ممکن است این سرویس به نام inetd باشد.)

```
# service xinetd restart
```

برای شروع کار با SWAT، ابتدا باید جستجوگر مورد نظر خود را باز کنید و آدرس <http://localhost:901> را تایپ نمایید. localhost را با نام کامپیوتری که سامبا روی آن درحال اجراست، جایگزین کنید. بعد از اینکه آدرس را وارد نمودید، یک اعلان برای Login مشاهده خواهید نمود. در اینجا باید نام کاربر و کلمه عبور صحیح را وارد نمایید. اگر با کاربر root وارد شوید، تمام تغییرات ممکن را می توانید انجام دهید. ولی اگر با یک کاربر عادی Login کنید، فقط می توانید تنظیمات را مشاهده کنید و تنها تغییری که می توانید بدهید کلمه عبور همان کاربر خواهد بود. تفاوت مشاهدات کاربر root و یک کاربر عادی را در دو شکل زیر ببینید:



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 آدرس IP با کامپیوتر سرویس‌دهنده سامبا در یک شبکه است، می‌تواند اجرا شود و مورد استفاده قرار بگیرد. اما در اینصورت باید مراقب مسائل امنیتی مثل استراق سمع¹⁰ کلمه عبور از روی شبکه باشید. به منظور داشتن امنیت بیشتر هنگام مدیریت سامبا از راه دور، می‌توان آنرا تحت SSL اجرا نمود. برای این کار کافی است مراحل زیر را طی کنید:

■ OpenSSL را نصب نمایید.

■ یک گواهینامه¹¹ و یک کلید خصوصی (Private Key) تولید کنید:

¹⁰ Sniff

¹¹ Certificate

```
# /usr/bin/openssl req -new -x509 -days365 -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.

■ سرویس stunnel را start کنید.

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

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

<https://localhost:901>

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

دیدن لیست منابع مشترک روی سامبا

خب، حالا که توانستید یک سرویس دهنده سامبا را به طور خیلی ساده تنظیم کنید، باید بتوانید لیست منابع مشترک را روی آن مشاهده نمایید. همانطور که می دانید، سرویس گیرنده سامبا می تواند یا ویندوزی باشد و یا لینوکسی. برای دیدن لیست منابع به اشتراک گذاشته شده از روی یک سرویس گیرنده لینوکسی باید دستور زیر را وارد نمایید:

\$ smbclient -L *yourhostname*

که در آن *yourhostname* نام سرویس دهنده سامبا است. با وارد نمودن این دستور باید لیست تمام منابع به اشتراک گذاشته شده روی سرویس دهنده را مشاهده کنید. اگر موفق به دیدن آنها نشدید، حتماً در تنظیمات

اشتباهی رخ داده است. از این روش می‌توان برای دیدن منابع مشترک روی سرویس‌دهنده‌های SMB دیگر مانند ویندوز ۲۰۰۰ نیز استفاده کرد.

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

\$ smbclient -L yourhostname -N

در سرویس‌گیرندگان ویندوزی نیز با دستور net share می‌توان لیست منابع مشترک را دید.

دسترسی به منابع به اشتراک گذاشته شده

سرویس‌گیرندگان لینوکسی به دو صورت می‌توانند به این منابع مشترک دسترسی داشته باشند:

■ توسط برنامه smbclient که درواقع یک دسترسی مانند FTP به منابع را فراهم می‌کند. مثال :

\$ smbclient //yourhostname/aservice

به این نوع دسترسی، دسترسی محلی^{۱۲} گویند. yourhostname نام کامپیوتری است که smbdrive روی آن

نصب شده است و aservice نام هر منبع به اشتراک گذاشته شده است. مثال:

\$ smbclient //bambi/fred

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

■ توسط دستور smbmount که به کاربران اجازه می‌دهد یک فایل سیستم مشترک مانند

فایل سیستم‌های محلی، Mount کنند:

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

به این نوع دسترسی نیز دسترسی از راه دور^{۱۳} گفته می‌شود.

¹² Local

سرویس‌دهنده سامبا باید در لیست آیکن‌های موجود در Network Neighborhood روی تمام سرویس‌گیرندگان ویندوزی که در زیر شبکه^{۱۴} خودش هستند، دیده شود. بنابراین سعی کنید آنرا از روی یک سرویس‌گیرنده دلخواه جستجو کنید و یا اینکه آنرا mount نمایید. در ویندوز با استفاده از دستور net use می‌توان منابع مشترک را Mount کرد:

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

```
C:\> net use lpt1: \\servername\spoolservice
```

برای چاپ:

```
C:\> print filename
```

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

چند نکته قابل ذکر

بعد از تنظیم سامبا باید سرویس آن را Start کنیم. اینکار باید طبق دستورات هر پلت‌فرم انجام شود. مثلاً در

نسخه Redhat از لینوکس می‌توانید به صورت زیر عمل نمایید:

چون اسکریپت مربوط به مدیریت سامبا در `/etc/rc.d/init.d/smb` قرار دارد، باید برای راه‌اندازی

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

سرویس سامبا بنویسید:

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

و نیز برای Stop کردن سامبا می‌توانید بنویسید:

همچنین برای چک کردن وضعیت سامبا دستور زیر را به کار ببرید:

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

تمام مسائل مربوط به Start و Stop سرویس سامبا در فایل مربوط به log های سیستم، ثبت می‌شود.

فایل ثبت رخدادهای سیستم در مسیر `var/log/messages` قرار دارد. اما علاوه بر آن، سامبا یک فایل ثبت

¹³ Remote

¹⁴ subnet

رخداده مخصوص به خود نیز دارد که مسیر آن در فایل smb.conf در پارامتر Log file مشخص شده است. هر چند معمولاً این فایل در مسیر /var/log/samba قرار دارد. اگر سامبا به درستی عمل نکرد، فایل ثبت رخداد سامبا را چک و بررسی نمایید. معمولاً اکثر مشکلات مربوط به سامبا با دیدن این فایل و پیغام‌های آن حل می‌شود.

تعداد زیاد فرایند smbд :

گفتیم smbд سرور مربوط به Name Server است. اگر سامبا به عنوان WINS Server عمل نکند، فقط یک فرایند smbд روی سیستم شما در حال اجراست، در غیر اینصورت، یعنی اگر سامبا بخواهد WINS Server هم باشد باید دو فرایند smbд در حال اجرا داشته باشید که یکی برای مدیریت درخواستهای WINS اختصاص یابد. اما از طرف دیگر smbд باید تمام درخواستهای اتصال به سرور را اداره کند. برای اینکار، smbд به ازای هر اتصال سرویس‌گیرنده یک فرایند جدید ایجاد می‌کند. در واقع برای هر اتصال سرویس‌گیرنده باید یک برنامه smbд مخصوص به آن فعال باشد و به آن پاسخ دهد. بنابراین دلیل اینکه در یک زمان ممکن است تعداد زیادی فرایند smbд ببینید، همین مسأله است.

بعضی خطاهای معمول در راه اندازی سامبا

■ پیغام خطای "open-oplock-ipc":

شاید این پیغام خطا در هنگام شروع فرایند smbд در فایل ثبت رخداد به صورت زیر مشاهده شود:

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

Error was cannot assign requested .

در صورت مشاهده این خطا، احتمالاً کارت شبکه^{۱۵} شما به درستی کار نمی‌کند. باید مطمئن شوید که آن را درست تنظیم کرده‌اید.

■ پیام خطای "The network name cannot be found":

خطای فوق می‌تواند ناشی از یکی از موارد زیر باشد:

- در فایل smb.conf مسیری را که برای منبع به اشتراک گذاشته شده تعیین کرده‌اید وجود ندارد.
- با کاربری سعی در دسترسی به منابع مشترک دارید که مجوزهای کافی برای استفاده در آن مسیر را ندارد.
- در واقع برای استفاده از یک منبع مشترک توسط یک کاربر، آن کاربر باید دارای مجوزهای read و Execute باشد.

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

فصل دوم

مثالها

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

¹⁵ Loopback

شود نیز بیان شده است. توجه داشته باشید که مثالهای این بخش صرفاً برای آشنایی بیشتر شما با سامبا مطرح شده و برای تنظیمات خیلی دقیق 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 پلتفرم خاصی مدنظر نبوده است. قبل از پرداختن به مثالها، از صحیح نصب شدن سامبا اطمینان حاصل کنید.

مثال ۱: راه اندازی یک Document Server

می‌خواهیم یک فایل سرور 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 فایل کاربری به نام `jack Baumbach` است که نام کاربری آن `jackb` و کلمه عبورش `m0r3paln` است.

برای ایجاد این سرویس‌دهنده باید مراحل زیر را انجام دهید:

کاربر مورد نظر را به سیستم اضافه کنید به طوری که دایرکتوری `home` آن نیز ایجاد شود:

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

دایرکتوری `/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 فایل‌هایی را که می‌خواهید به اشتراک بگذارید به دایرکتوری `/export` کپی نمایید.

فایل smb.conf را مطابق زیر تغییر دهید:

```
# Global parameters
[global]
workgroup = MIDEARTH
netbios name = HOBBIT
security = share
[data]
comment = Data
path = /export
read only = yes
guest ok = yes
```

فایل smb.conf را با برنامه testparm تست کنید:

testparm

بعد از اجرای testparm ممکن است با پیغام‌های خطایی مواجه شوید. 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 پلت‌فرم خود، سرویس سامبا را start کنید.

سرویس گیرنده ویندوزی خود را به workgroup مشخص شده (در اینجا MIDEARTH) متصل

نمایید و نام آن را به ROBBINS تنظیم کنید. آن را reboot کرده و کمی منتظر بمانید. سپس جستجوگر

ویندوز خود را باز نموده و به قسمت Network Neighborhood بروید. در آنجا باید ماشین HOBBIT

را ببینید و با کلیک کردن روی آیکن آن، باید بتوانید داده‌های به اشتراک گذاشته شده روی آن را مشاهده کنید.
در آنجا دایرکتوری `/export` قابل مشاهده خواهد بود.

مثال ۲: راه اندازی یک Read write Document Server:

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 فایل `smbpasswd` اضافه کنیم. پس ابتدا دستورات زیر را وارد نمایید:

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

سپس فایل `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  
guest ok و force group و force user از پارامترهای استفاده می‌کنید با استفاده از پارامترهای  
دسترسی به فایل سرور را محدود کرده‌ایم.
```

مثال ۳: راه اندازی یک سرور چاپ

ساده‌ترین سرور چاپ هم به نصب درایور صحیح چاپگر روی workstation های ویندوزی نیاز دارد. سرور چاپ در واقع طوری طراحی شده است که تمام job های مربوط به چاپ را به spooler می‌فرستد و spooler نیز باید طوری تنظیم شده باشد که این job ها را به نوبت به چاپگر ارسال کند، بدون اینکه کمترین فرایندی یا فیلتری روی آنها انجام دهد. در این مثال به بررسی ویزارد مربوط به اضافه کردن چاپگر نمی‌پردازیم. برای داشتن یک سرور چاپ ساده باید فایل 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 دایرکتوری /var/spool/samba همانطور که انتظار دارید ظرفیت پذیرش job های چاپ را دارد و نیز مجوزهای لازم برای اینکار را دارد. برای این منظور به صورت زیر باید عمل نمائید:

دایرکتوری موردنظر باید تحت مالکیت superuser یا همان root باشد. هم گروه آن و هم کاربر آن:

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

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

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

مثال ۴ : راه اندازی یک Read-write File & print Server امن

این بار، باز هم مثال را کمی پیچیده تر می کنیم. سرور جدید یک محیط ذخیره داده خواهد بود که فقط کاربران تصدیق‌اصالت شده (مثل کاربران محلی سیستم) می توانند فایل‌هایی را در آن ذخیره کنند؛ مثل یک home directory. و در ضمن یک چاپگری خواهیم داشت که باید برای تمام کاربران قابل دسترسی باشد. کاربران این محیط فرضی jack Baumbach و Amed Sehkah و Mary Orville هستند و هر کدام یک کلمه عبور برای خود دارند. مدیر چاپ و محیط ذخیره داده نیز کاربر Mary خواهد بود. سطح امنیت را روی user-level Security که همان پیش فرض است می گذاریم. سپس کارهای زیر را انجام می دهیم:

کاربران را به صورت زیر به سیستم عامل اضافه می کنیم:

```
# 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
```

فایل smb.conf را به صورت زیر تنظیم می کنیم:

```
# 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 دیتابیس 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 سرویس سامبا را start کنید:

```
# nmbd; smbd;
```

تنظیم دایرکتوری /export :

```
# mkdir /export
# chown maryo.users /export
# chown u=rwx , g=rwx , o-rwx /export
```

چک 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 کاربر maryo 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
```

مثال ۵: Domain Member Server

در یک اداره با شرکت حسابداری می‌خواهیم یک نرم‌افراز بنام SpytFall که فقط روی یک سرور نصب

و در حال اجراست (به خاطر محدودیت license) روی یک Application Server مرکزی قرار بگیرد.

مدیر دپارتمان نیز کاربر maryo است. تمام کارمندان باید یک دایرکتوری home داشته باشند و نیز باید بتوانند پرینت بگیرند. درضمن سیستم حسابداری تنها یک سرور به نام valinor خواهد داشت و اطلاعات کاربران نیز روی Domain Controller قرار دارد و زیر نظر آن چاپ می‌شود. برای اینکه این سرور را تنظیم و راه‌اندازی کنید باید به نکات زیر توجه داشته باشید:

هیچ کاربری را به سرور لینوکس اضافه نکنید، زیرا تمام این کارها بر عهده Domain مرکزی خواهد بود. فایل 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 separator = +
winbind use default Domain = yes
use send file = yes
printinf = cups
[homes]
comment = Home Directories
valid users = %S
read only = No
browseable = No
[ 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 , maryl
create mask = 0600
guest ok = yes
printable = yes
use client driver = yes
browseable = No
```

باید به Domain مربوطه Join شوید: (توجه کنید که حتماً این مرحله کامل شود، سپس سرویس سامبا را start کنید).

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

Joined domain MIDEARTH.

از disable بودن سرور nsd روی سیستمی که winbind روی آن تنظیم شده و در حال اجراست مطمئن شوید. نکته دی‌گری که باید به آن توجه داشته باشید آن است که بسته به نسخه سامبای مورد استفاده دستور ملحق شدن به یک دامین ممکن است متفاوت باشد. در این مورد در بخشهای بعدی به تفصیل صحبت خواهد شد.

سرویس سامبا را start کنید.

باید فایل `/etc/nsswitch.conf` را ویرایش کنید و تغییرات زیر را در آن بدهید، این تغییرات به منظور انجام عمل resolve 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 resolve 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 دید که آیا

username resolving صحیح انجام می‌شود یا نه:

```
# getent passwd maryo
```

maryo:x:15003:15003:Mary Orville:/home/MIDEARTH/maryo:/bin/false

دستورات زیر را انجام دهید:

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

```
# chown maryo /export/a_file
```

```
# ls -la /export/ a_file
```

...

```
-rw-r-f-- 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 دایرکتوری این سایت 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

مودهای امنیتی در سامبا و انواع مختلف سرورها

مقدمه

در این فصل می‌خواهیم انواع سرورهای که سامبا می‌تواند طبق آن تنظیم شود را توضیح دهیم. همچنین

مرور مختصری بر مودهای امنیتی که سامبا قادر به برقراری آنهاست داریم و اینکه سرویس‌گیرندگان ویندوزی

چطور می‌توانند با سامبا در این مدها به برقراری ارتباط بپردازند.

انواع سرورها

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

- Doamin Controller
 - Primary Doamin Controller
 - Backup Domain Controller
 - ADS Domain Controller
- Domain Member Server
 - Active Directory Domain server
 - NT4 Style Domain Server
- Stand-alone Server

مودهای امنیتی در سامبا

هدف انواع مختلف مدهای امنیتی در سرویس دهنده سامبا چگونگی برقراری آن با سرویس گیرندگان و نیز اعمال سیاست‌های امنیتی موردنظر توسط مدیران سیستم است. در دنیای شبکه‌ای SMB CIFS فقط دو نوع مد (سطح) امنیتی وجود دارد:

- User level Security
- Share level Security

که در واقع User level Security به چهار صورت پیاده‌سازی می‌شود و share level security را فقط به یک صورت می‌توان پیاده‌سازی کرد. جمعاً به این پنج روش مختلف پیاده‌سازی سطح‌های امنیتی^{۱۶} گفته می‌شود و عبارتند از:

SERVER , ADS , DOMAIN , USER , SHARE

¹⁶ Security Modes

این مدهای مختلف را یک‌به‌یک شرح خواهیم داد. در واقع هنگامی که یک سرویس‌گیرنده سامبا بالا می‌-

آید، باید به SMB Server بگوید که در چه سطح امنیتی کار می‌کند. یعنی یا Share level یا User level. بر طبق سطح امنیتی که سرویس‌گیرنده دارد باید خودش را برای سرویس دهنده معرفی^{۱۷} کند.

سطح امنیتی کاربر (User level Security)

ساده‌ترین نوع سطح امنیتی، سطح امنیتی کاربر است. در اینجا سرویس‌گیرنده درخواست برقراری یک نشست^{۱۸} را به سرور می‌فرستد. در این درخواست نام کاربر و کلمه عبور نیز فرستاده می‌شود. سرویس‌دهنده سامبا می‌تواند این درخواست را با کلمه عبور و نام کاربر یا قبول کند و یا رد نماید. در سطح امنیتی کاربر سرویس‌دهنده نمی‌تواند هیچ دخالتی در اینکه سرویس‌گیرنده به چه منبعی دسترسی پیدا می‌کند، داشته باشد و در واقع تنها معیار قبول و رد درخواست سرویس‌گیرنده فقط دو چیز است:

■ نام کاربری و کلمه عبور

■ نام ماشین سرویس‌گیرنده

اگر سرویس‌دهنده این درخواست را قبول کند، سرویس‌گیرنده می‌تواند بدون دادن هیچ کلمه عبور دیگری منابع به اشتراک گذاشته شده را برای خود Mount کند، چون فرض بر این است که کلیه حقوق و مجوزهای دسترسی در برقراری و تشکیل یک نشست به سرویس‌گیرنده داده شود.

همچنین ممکن است از سوی سرویس‌گیرنده چند درخواست تشکیل نشست ارسال شود. سرویس‌دهنده با قبول یک درخواست تشکیل نشست به سرویس‌گیرنده یک uid اختصاص می‌دهد که به عنوان پارامتر تصدیق‌اصالت برای نام کاربر و کلمه عبور دریافت شده در نظر گرفته خواهد شد. بنابراین سرویس‌گیرنده به

¹⁷ Authenticate

¹⁸ Session

راحتی می‌تواند از همین uid برای نشستهای بعدی نیز استفاده کند. یک برنامه کاربردی که اینکار را انجام می‌دهد WinDD نام دارد.

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

Security = user

نکته: از زمان samba-2.2.x پیش‌فرض سیستم user است.

سطح امنیتی Share (Share level Security)

در این نوع تنظیم امنیت، هر سرویس‌گیرنده باید برای هر منبع به اشتراک گذاشته شده به طور جداگانه تصدیق‌اصال شود. در واقع برای استفاده از هر منبع مشترک باید یک کلمه عبور داشته باشد. نحوه تنظیم در فایل smb.conf به صورت زیر است:

security = share

سطح امنیتی Domain (User level Security)

وقتی سامبا در مد Domain کار می‌کند به این معنی است که سرویس‌دهنده سامبا یک account در یک Domain دارد که تمام درخواستهای تصدیق‌اصال را به Domain Controller های آن پاس می‌کند. به عبارت دیگر با این تنظیم سرویس‌دهنده سامبا به عنوان عضوی از یک Domain محسوب خواهد شد.

نحوه تنظیم :

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

security = domain

workgroup = MIDEARTH

برای اینکه این تنظیمات به درستی عمل کند، باید به Domain مربوطه متصل^{۱۹} شوید. برای متصل شدن به Domain کارهای زیر را انجام دهید:

روی Win NT Domain controller با استفاده از server Manager یک account به نام ماشین سرویس دهنده سامبا ایجاد کنید.

روی سیستم لینوکسی خود دستور زیر را اجرا نمایید:

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

نکته: در نسخه‌های سامبای ۲-۲-۴ و بعد از آن به طور اتوماتیک 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 Admin strator%password
```

یعنی لزومی به مشخص کردن نام domain یا PDC-NAME نیست و این تنظیمات در فایل

smb.conf انجام می‌شود.

وقتی از این مد استفاده می‌کنیم به یک حساب کاربری یونیکسی استاندارد برای هر کاربر نیاز داریم تا به

یک UID تصدیق‌اصالت شده توسط windows DC اختصاص یابد. برای جزئیات بیشتر به فصل

Domain Membership مراجعه کنید.

سطح امنیتی ADS (User level Security)

¹⁹ Join

هم سامبای ۲-۲ و هم سامبای ۳ می‌توانند به Active Directory Domain متصل شوند. البته هنگامیکه دامین در مد Native در حال اجرا باشد. Active Directory در مد Native به تمام عضوهای دامین با سیستم‌عامل NT4-Style اجازه کار می‌دهد و فقط به Backup Domain Controller هایی که NT4-Style هستند اجازه کار نمی‌دهد. برای تنظیم سامبا در این مد باید فایل 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
```

سطح امنیتی Server (User level security)

این پارامتر هنگامی مورد استفاده قرار می‌گیرد که سرویس‌دهنده سامبا به عنوان عضو سروری دامین عمل کند. اکیداً توصیه می‌شود که از این پارامتر استفاده ننمایید. در واقع سطح امنیتی Server دارای مضرات و مشکلات زیر است:

- پتانسیل تحریم حساب کاربری روی Windows NT4/200x password server.
- عدم اطمینان از اینکه password server همان است که تعیین شده است.
- با Winbind نمی‌تواند کار کند و این به ویژه هنگامیکه می‌خواهیم profile ها را از راه دور ذخیره کنیم مشکل‌ساز می‌شود.
- این مد ممکن است باعث شود اتصالاتی با password server برقرار شود و آنرا برای مدت طولانی باز نگه دارد.

- وقتی password server راه دور به طور ناگهانی shutdown شود، امنیت سرویس دهنده سامبا به خطر می افتد.

در زیر تنظیمات مربوط به این مد آورده شده است:

Encrypt passwords = yes

Security = server

Password server = "NetBIOS_name_of_a_DC"

فصل چهارم

Stand-alone Servers

مقدمه

در این فصل سعی در معرفی Stand-alone Server ها داریم. این سرورها کاملاً از دامین کنترلرهای روی یک شبکه مستقل هستند و عضو دامین نیستند و بیشتر شبیه سرویس دهنده های یک workgroup عمل می کنند. یک Stand-alone Server می تواند با ملاحظات امنیتی و یا بدون آن پیاده سازی شود. در اغلب موارد یک Stand-alone Server با حداقل کنترل های امنیتی تنظیم می شود که در نتیجه آن تمام کاربران به داده های موجود روی آن دسترسی خواهند داشت.

اگر به یک file-Server فقط خواندنی نیاز دارید و یا به یک print Server، تنظیماتی که باید انجام دهید، پیچیده نخواهد بود. فرض کنید در یک اداره‌ای می‌خواهیم نقشه‌ها و فایل‌های اطلاعاتی قدیمی را نگهداری کنیم. هیچکس حق نوشتن فایل روی سرویس‌دهنده و یا تغییر فایل‌های روی آن را ندارد. در این شرایط، بهترین راه حل استفاده از یک Stand-alone Server فقط خواندنی که در مد Shared کار می‌کند، خواهد بود.

یک Stand-alone Server برای تمام منابع قابل دسترس از روی آن، تصدیق اصالت و کنترل دسترسی را به صورت local فراهم می‌کند. به این معنی که برای اینکار یک دیتابیس از کاربران محلی خواهد داشت. به عبارت دیگر، منابع موجود روی آن سیستم یا در مد SHARE و یا در مد USER قابل دسترس خواهند شد. بنابراین برای تنظیم آن به کار خاصی به جز ایجاد کاربران نیازی نیست. یک مسأله واضح این است که با Stand-alone Server ها هیچ سرویسی برای login روی شبکه ارائه نخواهد شد. یعنی ماشین‌هایی که از این سرویس‌دهنده استفاده می‌کند هیچ عمل login را روی دامین انجام نمی‌دهند. هرچند لازم است که هر کاربر شبکه‌ای نام کاربرش با نام کاربری محلی روی سرویس‌دهنده مذکور منطبق باشد. یعنی روی سرویس-دهنده یک عمل انطباق بین آنها انجام شود. چندین راه برای این کار وجود دارد:

دیتابیس مربوط به تصدیق اصالت کاربران به چند صورت می‌تواند باشد: یا به صورت محلی و یا یک سرویس‌دهنده راه دور (remote server) و یا حتی از طریق پروتکل SMB روی سرویس‌دهنده‌ای که اصلاً عضوی از Domain Security نیست.

به‌خاطر استفاده از Pluggable Authentication Modules (PAM) و همچنین Name Service Switcher (NSSWITCH) که دیتابیس مربوط به کاربران یونیکس است، منبع تصدیق اصالت ممکن است روی سرویس‌دهنده دیگری باشد. اگر ما بخواهیم آن سرویس‌دهنده را فراخوانی کنیم، سرویس‌دهنده سامبا ممکن است از دیتابیس کلمات عبور سیستم local unix /linux استفاده کند که در

فایل `/etc/passwd` و یا `/etc/shadow` قرار دارد و یا ممکن است از فایل `smbpasswd local` یا `LDAP` و یا حتی از `PAM` و `winbind` روی یک سرور `CIFS SMB` دیگری استفاده کند.

مثال: **Document server** و **Print server** مرکزی

Document server

می‌خواهیم یک **Document Server** داشته باشیم. برای تنظیمات مربوط به آن در فایل `smb.conf` باید تغییرات زیر را اعمال کنیم. فرض می‌کنیم که تمام `document` ها در دایرکتوری `/export` قرار دارد. هیچ `home directory` به صورت `share` وجود ندارد و کاربری نیز در دیتابیس سیستم یونیکسی `/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 سیستم‌های دیگر در یک جا ظاهر می‌شوند. با توجه به `passdb backend` که به

`guest` تنظیم شده اجازه دسترسی به همه کاربران ناشناس داده شده است. یک `WINS Server` نیز به این

منظور در شبکه ایجاد کرده‌ایم.

Print server مرکزی

برای داشتن سرویس **print** نیز باید کارهای زیر را انجام دهیم؛ فرض کنید:

- **print Server** نباید به مدیریتی نیاز داشته باشد.
 - سیستم **print spooling & processing** روی سرویس‌دهنده چاپ مورد نظر، **CUPS** خواهد بود.
 - این سرویس‌دهنده چاپ، فقط به چاپگرهای شبکه سرویس می‌دهد و مدیر شبکه باید تنظیمات مربوط به **CUPS** را برای چاپگرهای شبکه به درستی انجام دهد.
 - همه سرویس‌گیرندگان فقط از درایورهای **Postscript** استفاده خواهند کرد.
- در این مثال، سرویس‌دهنده چاپ هر **job** 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 ناشناس (**guest**) ایجاد می‌شود، دو چیز نیاز است:
- در سیستم **unix /linux** باید یک حساب کاربری برای **guest** داشته باشیم. معمولاً نام پیش‌فرض آن **nobody** خواهد بود. اگر می‌خواهید دقیقاً نامی که برای این حساب کاربری به طور پیش‌فرض در نسخه 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 دیتابیس (**/etc/passwd**) وجود دارد.

دایرکتوری که سامبا می‌خواهد **job**های مربوط به چاپ را در آن نگهداری کند، باید دارای مجوز **write**

برای کاربر **guest** باشد. با استفاده از دستورات زیر اینکار را انجام دهید:

```
# mkdir /var/spool/samba
```

```
# chown nobody.nobody /var/spool/samba
```

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

سپس تغییرات لازم در فایل `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
```

فصل پنجم

دیتابیس‌های مربوط به اطلاعات accountها

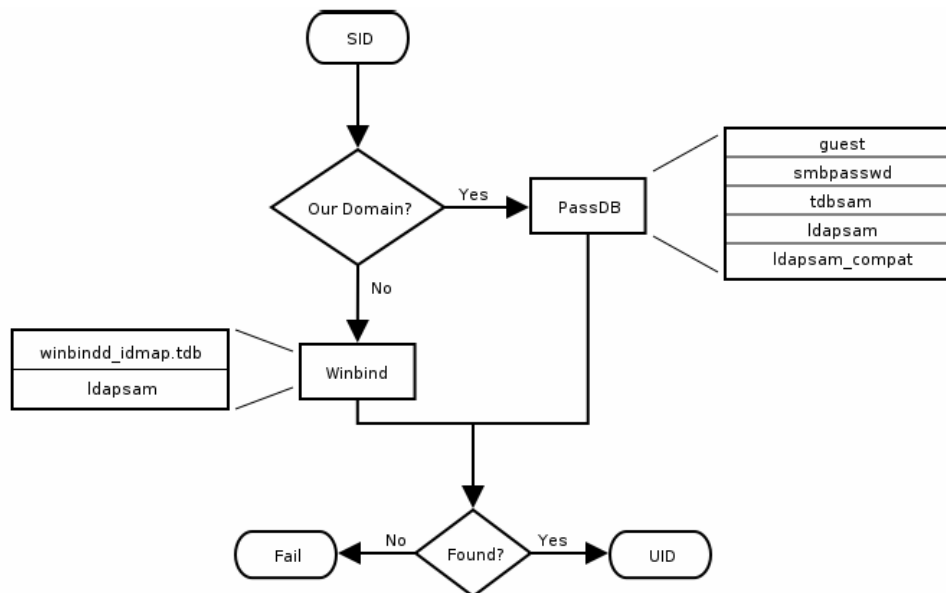
مقدمه

در ویندوزهای قدیمی، معمولاً سرویس‌گیرنده‌ها کلمات عبور را در طول شبکه و media های مورد استفاده خود به صورت متن واضح^{۲۰} یا رمز نشده، می‌فرستادند. سامبا با دریافت آنها و سپس رمزکردن کلمات عبور، نتیجه به دست آمده را با کلمات عبوری که در دیتابیس کاربران یونیکس به صورت hash شده نگهداری می‌شد، مقایسه می‌کرد.

²⁰ Plain text

در ویندوزهایی که بعد از آنها روانه بازار شدند روش کمی فرق کرد و در آنها، سرویس گیرنده ها کلمات- عبور را به صورت رمز شده روی شبکه می فرستادند. این کلمات عبور نمی توانند به کلمات رمز شده یونیکسی تبدیل شوند. به همین دلیل نمی توان از دیتابیس استاندارد کاربران یونیکسی استفاده کرد و مجبوریم آنها (کلمات عبور) را در جایی دیگر مثل LanMan و NT hashes نگهداری کنیم. بنابراین برای هر کاربر دو حساب کاربری داریم: یکی یونیکس 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 تبدیلی این دو به هم پایه کار سامبا است. حساب کاربری مربوط به ویندوز را با SID²¹ و حساب کاربری مربوط به یونیکس را با UID²² می شناسیم. اگر winbindd در حال اجرا نباشد یا نتوان با آن تماس گرفت فقط یک map به صورت محلی بین SID و UID انجام می پذیرد.

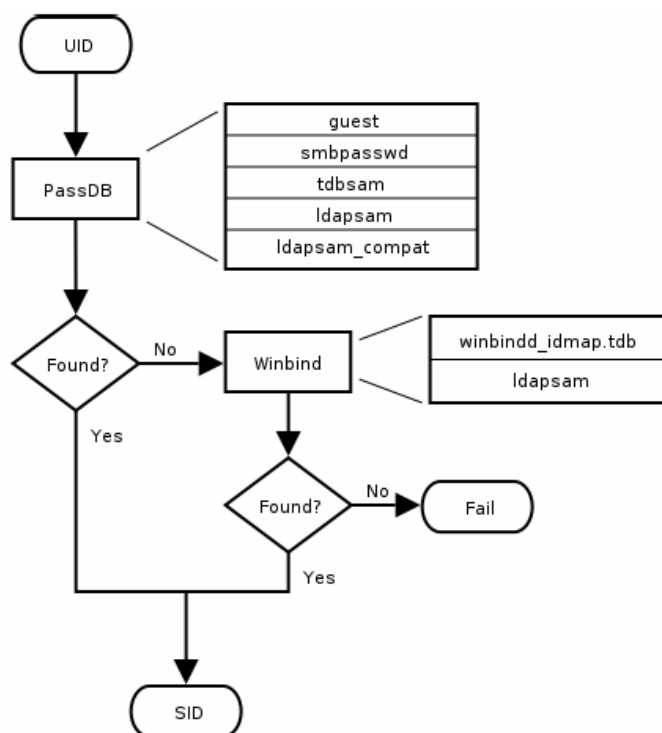
دو دیاگرام زیر مراحل انجام عملیات تبدیل SID به UID و نیز UID به SID را نشان می دهد:



IDMAP: Resolution of SIDs to UIDs.

²¹ Security Identifier

²² User identifier



IDAMP: Resolution of UIDs to SIDs.

به نظر می‌رسد که تکنیکهای رمزنگاری در یونیکس و SMB برای کلمات عبور شبیه به هم باشند. این شباهت وجود دارد اما به طور کاملاً ظاهری و سطحی. در یونیکس معمولاً وقتی کاربری login میکند، کلمه عبور آن به صورت متن واضح روی شبکه فرستاده می‌شود و این اصلاً خوب نیست. در SMB هرگز کلمه عبوری به صورت متن واضح فرستاده نمی‌شود. بلکه قبل از فرستادن رمز می‌شود. اما مقدار آن به صورت یک hash شانزده بیتی روی دیسک ذخیره می‌شود. این نیز خوب نیست؛ چون شانزده بایت hash شده معادل کلمات عبور است. درست است که نمی‌توان از روی آنها کلمه عبور را تشخیص داد، اما به راحتی می‌توان از آنها برای شبیه سازی یک اتصال^{۲۳} و یا جازدن به جای یک سرویس گیرنده برای دسترسی به سرویس دهنده استفاده کرد. بنابراین باید بتوان با استفاده از تکنیکهای مناسبی از بروز حملات این چنینی

²³ Connection

جلوگیری نمود. یعنی فایل کلمات عبور باید کاملاً مخفی (سری) و محافظت شده باشد. به طور ایده آل نمی‌خواهیم کلمه‌های عبور به صورت متن واضح نه روی شبکه و نه روی دیسک نگهداری شوند.

مزیت کلمات عبور رمز شده

- ۱- کلمات عبور به صورت متن واضح در شبکه رد و بدل نمی‌شوند. این مانع از سوءاستفاده دیگران توسط برنامه‌های ضبط کلمه عبور مثل sniffer می‌شود.
- ۲- کلمات عبور به صورت متن واضح در حافظه و یا دیسک ذخیره نمی‌شوند.
- ۳- با استفاده از کلمات عبور رمز شده امکان برقراری مجدد ارتباط به صورت اتوماتیک برای منابع مشترک وجود دارد.
- ۴- کلمات عبور رمز شده اساس عملکرد PDC/BDC هستند.

مزیت کلمات عبور با متن واضح

- ۱- کلمات عبور به صورت متن واضح نه روی دیسک نگهداری می‌شوند و نه Cache می‌شوند.
- ۲- از همان فایل کلمات عبور برای سرویس‌های دیگر یونیکس مثل login و FTP می‌توان استفاده کرد.
- ۳-

Resolve بین شناسه‌های کاربری ویندوز و یونیکس

همانطور که می‌دانید قبلاً نیز گفته‌ایم، هر عملیاتی در یونیکس نیاز به یک UID دارد، درست مانند ویندوز که به یک SID نیاز دارد و نیز گفتیم که سامبا برای انجام کار خود باید بتواند ایندو را به یکدیگر resolve کند، برای اینکار دو روش فراهم کرده است:

اول اینکه تمام حسابهای کاربری SAM²⁴ در سامبا به یک UID در Unix/Linux نیاز دارند که به آن resolve شوند. وقتی یک کاربر به دیتابیس مربوط به account ها اضافه می‌شود، سامبا ایتترفیس مربوط به اسکریپت اضافه کردن کاربر را برای ایجاد کاربر در سیستم عامل میزبان سامبا فرامی‌خواند. در اصل تمام حسابهای کاربری در Local SAM به یک حساب کاربری محلی نیاز دارند.

راه دوم mapping بین UID و SID از طریق پارامترهای idmap uid, idmap gid در فایل smb.conf است. وجود این پارامترها زمانیکه کاربران از یک سرور SAM راه دور می‌خواهند map شوند، ضروری است. برای اطلاعات بیشتر به فایل smb.conf و man page های آن مراجعه کنید.

ابزارهای مدیریت Account

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

دستور smbpasswd

عملکرد برنامه smbpasswd شبیه به برنامه‌های passwd و yppasswd است. smbpasswd، دو فیلد ۳۲ بیتی password در دیتابیس مربوط به کلمات عبور نگه می‌دارد و در مد client-server کار

²⁴ Security Account Manager Database

می‌کند. به این ترتیب که با `smbd` محلی برای تغییر کلمه عبور کاربر تماس می‌گیرد. این روش مزایای بیشماری دارد.

`Smbpasswd` توانایی و قابلیت تغییر کلمه عبور روی سرویس دهنده‌های ویندوز NT را دارد. (البته این کار فقط زمانی امکان پذیر است که درخواست به NT PDC فرستاده شود و جهت تغییر کلمه عبور کاربری روی NT Domain باشد.)

از `Smbpasswd` برای انجام کارهای زیر می‌توان استفاده کرد:

- اضافه کردن یک کاربر یا ماشین.
- حذف یک کاربر یا ماشین.
- enable کردن یک کاربر یا ماشین.
- disable کردن یک کاربر یا ماشین.
- تنظیم کلمه عبور کاربر به NULL.
- 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 کلمه عبور جدید پاسخ دهید:

New SMB password : new secret

Retype New SMB password : new secret

وقتی با کاربری عادی اقدام به اجرای `Smbpasswd` کنید، فقط کلمه عبور 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 درباره کلمه عبور قدیمی اجازه تغییر کلمه عبور را دارید. این کار برای زمانی که کاربران کلمه عبور خود را فراموش کرده اند به درد می خورد.

همانطور که دیدید، Smbpasswd مانند passwd, yppasswd عمل می کند.

دستور pddedit

pddedit فقط توسط root می تواند استفاده شود و برای مدیریت دیتابیس کلمات عبور طراحی شده

است. Pddedit کارهای زیر را می تواند انجام دهد:

- add ، remove و modify برای حسابهای کاربران.

- لیست کردن حسابهای کاربران.

- migrate user accounts

درواقع pddedit قادر به انجام عملیاتی است که Smbpasswd انجام می داد. یک مثال را در زیر ببینید:

```
$ 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 دیتابیس قدیمی **Smbpasswd** به **tdbsam backend**

می توان کارهای زیر را انجام داد:

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

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

۲- دستور زیر را اجرا کنید:

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

۳- حال باید **Smbpasswd** را از پارامتر **passdb backend** در فایل **smb.conf** حذف کنید.

فصل ششم

کنترل دسترسی به فایل‌های و شاخه‌ها و منابع اشتراکی

مقدمه

یادآوری این نکته لازم است که سامبا به منظور تعامل و تبادل اطلاعات بین دو محیط یا سیستم عامل مختلف ایجاد شده است. توجه کنید که هدف سامبا تغییر `unix /linux` به پلت فرم ویندوز نیست بلکه فراهم کردن یک سطح تبادل خوب از اطلاعات بین این دو محیط است. اغلب کاربران ویندوز وقتی متوجه می‌شوند فایل‌ها و منابعی که توسط سامبا به اشتراک گذاشته شده آنطور که انتظار دارند رفتار نمی‌کنند، دچار ابهام می‌شوند و مدیران سیستم 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 در چگونگی اعمال مجوزها و کنترل‌ها بین دو محیط است. هدف این فصل ارائه نکات کنترل ممکن توسط سامبای ۳ برای مدیران شبکه است تا به کمک آنها بتوانند روش بهینه کنترل منابع مشترک را برای محیط‌های ویندوزی پیدا کنند.

کنترل دسترسی به فایل سیستم

شاید مهمترین مطلب دانستن این نکته است که آنچه که در ویندوز به عنوان تکنولوژی File system پیاده سازی شده کاملاً با تکنولوژی File system در یونیکس متفاوت است. بنابراین بهتر است ابتدا کمی با این دو تکنولوژی آشنا شویم و سپس ببینیم سامبا چگونه به تبادل اطلاعات روی این دو کمک می کند.

مقایسه فایل سیستم ویندوز و یونیکس

سامبا طبق File system یونیکس عمل می کند. یعنی از قوانین و مجوزهای آن پیروی می کند. در زیر یک مقایسه بین فایل سیستم یونیکس و ویندوز NT/200x انجام شده است:

Name space: از لحاظ نام، نام فایل ها در سیستم عامل ویندوز می تواند تا 254 کاراکتر باشد. ولی در یونیکس تا 1023 کاراکتر می تواند باشد. در ویندوز پسوند فایل مشخص کننده نوع فایل است در صورتی که در یونیکس اینطور نیست و داشتن پسوند اختیاری است. در آخر اینکه آنچه در ویندوز فلدر نامیده می شود، در یونیکس دایرکتوری گفته می شود.

Case Sensitivity: در ویندوز معمولاً نام ها Case Sensitive نیستند، برعکس یونیکس. بنابراین سامبا باید یک هماهنگی بین این دو سیستم عامل از این جهت فراهم کند. سامبا اینکار را با یکسری برنامه های کاربردی انجام می دهد که باعث مقداری بار اضافی²⁵ روی آن می شود.

به مثال زیر توجه کنید از نظر ویندوز فایل های زیر همه یک فایل هستند ولی از نظر یونیکس سه فایل مختلف:

MYFILE.TXT

MyFile.txt

Myfile.txt

²⁵ Overhead

Directory Separators : ویندوز و Dos هر دو از « \ » (backslash) به عنوان جدا کننده

دایرکتوری ها استفاده می کنند در حالیکه یونیکس از « / » استفاده می کند . این نیز توسط سامبا قابل حل و مدیریت است.

Drive identification : در ویندوز علامت یک پارتیشن با یک حرف مربوط به آن پارتیشن مشخص

می شود. مثل C:\. در یونیکس مفهوم یک پارتیشن جدا وجود ندارد. هر فایل سیستم که Mount شده است بخشی از درخت دایرکتوری سراسری است. این درخت دایرکتوری با « / » شروع می شود که به آن root می گوئیم و بقیه از آن جدا می شوند مثل C:\ در Dos .

File Naming Conventions : در ویندوز هیچگاه نام فایل ها با (*) شروع نمی شوند. در صورتی

که در یونیکس این قبیل فایلها در home Directory کاربران وجود دارند و معمولاً برای فایل های شروع برنامه های مختلف یا فایل های مختلف تنظیم به کار می روند.

Links and Short-Cuts : معمولاً در ویندوز با مفهوم link , Short-cut آشنا هستید که در آنها

سعی می کنیم یک فایل را از لینکی به محل واقعی خودش اجرا کنیم. در واقع از یک مسیر غیر واقعی یک فایل را اجرا می کنیم. در یونیکس نیز این مفهوم وجود دارد اما کاملاً به شکلی متفاوت از ویندوز. symbolLink ها فایل هایی در یونیکس هستند که محتویات آنها مسیر واقعی فایل اصلی است و عملیات (خواندن یا نوشتن) روی فایل اصلی انجام می شود. به Symlink ها Softlink نیز گفته می شود. علاوه بر این در یونیکس مفهوم دیگری به نام HardLink نیز داریم که کاملاً برای ویندوز نا آشنا است. در HardLink به یک فایل می توان بیش از یک نام نسبت داد.

علاوه بر تفاوت های فوق، موارد متعدد دیگری نیز وجود دارد که در اینجا فقط به ذکر مهمترین ها اکتفا نموده ایم.

: Managing Directory

معمولاً برای عملیات اصلی روی دایرکتوری‌ها و برای مدیریت آنها سه عملیات وجود دارد: `rename`.

Create, Delete. 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

File and Directory Access control

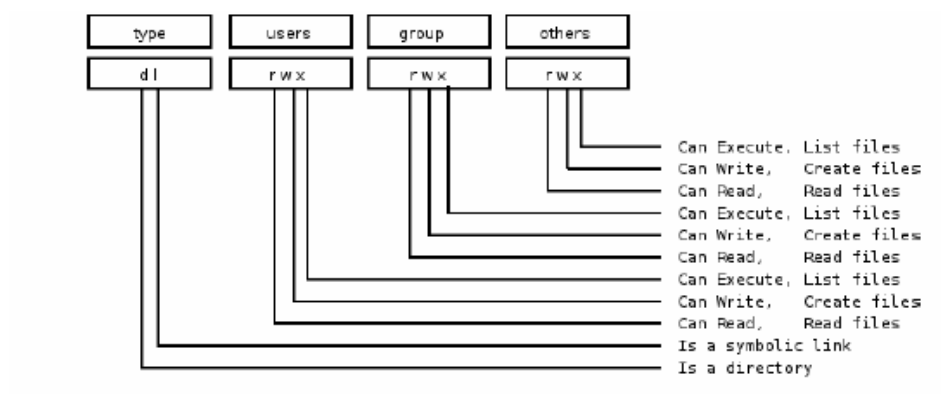
در یونیکس معمولاً مجوزهای مربوط به دایرکتوری و فایل به صورت زیر نمایش داده می‌شود:

```
$ 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 ها به فایل، صاحب فایل، گروه فایل، اندازه فایل به بایت، تاریخ دسترسی، زمان دسترسی و نام

فایل. به طور خلاصه می‌توان مجوزهای مشخص شده در شکل فوق را به صورت زیر تعیین کرد:



هر flag در مجوزها که با - نمایش داده شده به معنی عدم مجوز در آن مورد به خصوص است. مثلاً در

مثال زیر خواهیم داشت:

`-rwxr-x---`

- صاحب فایل می‌تواند فایل را بخواند و تغییر دهد و اجرا کند.

- گروه فایل می‌تواند فقط آن را بخواند و اجرا کند.

- بقیه افراد هیچ مجوزی ندارند.

در ضمن اولین ستون از ستون مجوزها مشخص کننده نوع فایل است. قرار داشتن هر کدام از حروف زیر

در این ستون معنای خاص خود را دارد:

- : فایل عادی

d : دایرکتوری

Symbol Link : l

Block Device : b

Pipe Device : p

Unix Domain Socket : S

مثال : فرض کنید مجوز فایلی `d-wx-x---` است. در اینصورت داخل این فایل را صاحب آن می‌تواند

بخواند و ایجاد کنند (تغییر دهد) اما چون هیچ کس مجوز `read` را ندارد، این فایل در لیست دایرکتوری دیده

نخواهد شد (توسط هیچ کس). گروه فایل نیز می تواند دایرکتوری را بخواند اما نمی تواند در آن فایل جدیدی ایجاد کند.

کنترل دسترسی به منابع اشتراکی

پارامترهایی که در زیر آورده ایم هر کدام در فایل `smb.conf` یک سری تنظیمات مربوط به کنترل دسترسی به منابع به اشتراک گذاشته شده است. بهتر است قبل از مطالعه آنها به `Manpage` های این فایل مراجعه کنید.

کنترل براساس User و Group

این نوع از کنترل دسترسی می تواند خیلی مفید باشد، چون دقیقاً می توان تعیین کرد که چه کسی به فایل ها دسترسی داشته باشد. در جدول زیر دقیقاً این کنترل ها 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 <code>smb.conf</code> 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.

کنترل بر اساس مجوزهای File , Directory

اگر این قبیل کنترل‌ها به درستی اعمال نشود، باعث سختی در تشخیص تنظیمات انجام شده و نیز سردرگمی خواهد شد. بنابراین به دقت باید آنها را به کاربرد و البته به تدریج. به جدول زیر دقت کنید:

Control Parameter	Description - Action - Notes
create mask	Refer to the <code>smb.conf</code> 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 <code>smbd</code> 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.

برخی کنترل‌های دیگر

علاوه بر پارامترهایی که قبلاً برای کنترل دسترسی به فایل‌ها 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 <code>smb.conf</code> 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 unwritable files	Prevents clients from seeing the existence of files that cannot be written to. Unwritable directories are shown as usual.
nt acl support	This parameter controls whether <code>smbd</code> 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.

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، 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 منظور اینکه مثلاً چه کسی اجازه دسترسی به آن منابع را دارد. به طور پیش‌فرض در ویندوز مجوز دسترسی به منابع به صورت Full control است. برای تمام افراد (Everyone).

سامبا برای هر منبع مشترک، تنظیمات مربوط به کنترل دسترسی را در یک فایل به نام `share_info.tdb` ذخیره می‌کند. محل این فایل بستگی به چگونگی کامپایل سامبا دارد. معمولاً محل آن و کلاً فایل های `tdb` ی سامبا در `/usr/local/samba/var` است. اگر برنامه `tdbdump` روی سیستم شما کامپایل و نصب شده باشد، شما با اجرای دستور زیر می‌توانید محتویات آن فایل را بررسی و امتحان کنید:

در زیر دایرکتوری فایل های `tdb` این دستور را اجرا کنید:

```
tdbdump share_info.tdb
```

مدیریت مجوزهای منابع مشترک

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

Windows NT4 workstation /Server

در اینجا ابزاری که شما برای مدیریت مجوزهای منابع مشترک نیاز دارید روی یک سرویس‌دهنده سامبا، `NT Server Manager` است. این ابزار معمولاً همراه نسخه های سرور ویندوز `NT` است ولی در نسخه های `workstation` نیست و باید آن را از سایت مایکروسافت دانلود و نصب نمائید. سپس برای کار با آن به صورت زیر عمل نمائید:

برنامه `NT4 Server Manager` را اجرا کنید. روی سرویس‌دهنده 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، کلیک کنید و سپس قسمت **properties** را انتخاب کنید. در آنجا به قسمت **permission** رفته و تنظیماتی را که در نظر دارید اعمال کنید.

Windows 200x/xp

در ویندوز 200x و بعد از آن، ابزاری به نام **ComputerManagement Snap-in** برای (MMC) **Microsoft Management Console** می‌آید. این ابزار در **Control panel > Administrative Tools > Computer Management** قرار دارد. آن را اجرا کنید و به صورت زیر عمل نمائید:

از منوی **Action**، **Connect to another computer** را انتخاب نمائید. اگر در دامین، **login** نکرده باشید با یک پیغام برای **login** مواجه می‌شوید. **User name** که وارد می‌کنید در دامین تصدیق‌اصالت خواهد شد. اگر با **Adminiistrator**، **login** کرده باشید، به این مرحله نیازی نیست.

اگر در صفحه مربوط به **Select Computer**، سرویس‌دهنده سامبا نشان داده نشده است، ابتدا کامپیوتر سرویس‌دهنده سامبا را در فیلد **Name** وارد کنید. سپس روی علامت (+) کلیک کنید و بعد روی + کنار **Shared Folder** در قسمت چپ صفحه کلیک کنید.

در قسمت راست صفحه، روی منبع مشترکی که می‌خواهید روی آن مجوزهای دسترسی را تنظیم کنید، **double click** نمائید. در **Tab** مربوط به **Share permissions** بروید. سپس تنظیمات مورد نظر را اعمال کنید.

MS Windows Access Control List and UNIX Interoperability

سرویس گیرندگان ویندوز NT هرکدام می توانند از Security Setting dialog box برای دیدن و تصحیح کردن مجوزهای یونیکس استفاده کنند. اما این ابزارها به دقت ابزارهای موجود در روی سامبا و یونیکس نیست.

دیدن File Security روی منابع مشترک سامبا

از روی یک سرویس گیرنده NT4/200x/xp، روی هر فایل یا دایرکتوری که روی سرویس دهنده 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 کلیک کنید. در آنجا سه دکمه Auditing، Ownership، Permissions را خواهید دید.

دیدن File ownership

روی دکمه ownership کلیک کنید. یک dialogbox باز خواهد شد که صاحب فایل را به شما معرفی می کند. مثلاً:

“SERVER \user (Long Name)”

SERVER، NetBIOS name، سرویس دهنده سامبا است. user نام کاربر یونیکسی است که صاحب فایل است و Long Name یک سری توضیحات درباره کاربر و معرفی اوست. (معمولاً این اطلاعات در فیلد GECOS از دیتابیس کلمات عبور یونیکس قرار دارد.) روی دکمه close کلیک کنید. توجه کنید که اگر پارامتر nt acl به false تنظیم شده باشد، صاحب فایل به عنوان کاربر Everyone از NT نشان داده خواهد شد. در ضمن دکمه Takeownership در اینجا کار نمی کند و شما اجازه تغییر صاحب فایل را نخواهید داشت. در واقع با انتخاب این دکمه، یک صفحه ظاهر شده و در آن گفته می شود که کاربری که با آن login کرده اید، پیدا نمی شود. علت این امر آنست که مجوز تغییر صاحب فایل فقط در اختیار کاربر root در یونیکس

است و کلیک کردن روی این دکمه باعث خواهد شد که صاحب فایل به کاربری که شما با آن در سرویس-گیرنده ویندوزی login کرده‌اید تغییر کند و این در سامبا کار نخواهد کرد.

دیدن مجوزهای فایل و دایرکتوری‌ها

اگر روی دکمه permission کلیک کنید، هم صاحب فایل و دایرکتوری و هم مجوزهای آنها را می‌توانید ببینید. مثلاً:

SERVER\ser (Long Name)

مانند قبل که توضیح داده شد. با این تفاوت که اگر پارامتر false nt acl باشد مجوزها نیز Full Control خواهد بود برای کاربران NT. اما نکته‌ای که وجود دارد این است که مجوزهای نشان داده شده برای فایل و دایرکتوری متفاوت است. بنابراین در ادامه این بخش به بررسی این مجوزها به طور مجزا می‌پردازیم.

مجوزهای فایل

سه‌بیتی‌های استاندارد user/group/world در یونیکس و مجوزهای سه تایی read.write.execute توسط سامبا باید به مجوزهای موجود در NT تبدیل شوند. به این ترتیب که مجوزهای مربوط به other در یونیکس با مجوز Everyone در NT منطبق می‌شود. مجوزهای مربوط به user، group نیز به ترتیب به NT user، NT local group برمی‌گردد. (یکسری توضیحات درباره Take ownership در NT)

مجوزهای دایرکتوری

دو مجموعه مجوزهای متفاوت برای دایرکتوری در فایل سیستم NTFS وجود دارند. یکی مربوط به خود دایرکتوری است و اینکه به خود دایرکتوری چه کسانی می‌توانند چه دسترسی‌هایی داشته باشند و دیگری مربوط به مجوزهای فایل‌های داخل دایرکتوری است.

نکته: اگر فایلی در یونیکس 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.

تصحیح یا تغییر مجوز فایل یا دایرکتوری

تغییر مجوزهای یک فایل یا دایرکتوری به راحتی با تغییر آنها در dialog box مربوط و تایید آنها با انتخاب دکمه 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 کلیک کردن روی دکمه Add است. با کلیک کردن 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). معنی آن این است که شما فقط می‌توانید مجوزهای مربوط به user/ group/ world های جاری سیستم را تغییر دهید که در dialog box لیست شده اند.

هنگامیکه یک مجوز از مجموعه سه‌تایی user/ group/ world در ویندوز حذف شود و سپس کلید ok زده شود، سامبا آن مجوز را در طرف یونیکس به عنوان نداشتن مجوز تفسیر می‌کند. چون یونیکس فقط بیت‌های r,w,x از nt acl را می‌فهمد و support 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. هنگامیکه شما مجوزی را روی یک دایرکتوری تعیین می‌کنید، این مجوز به کل دایرکتوری 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.

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 کلیک می‌کند، سامبا باید آن مجوزها را به مجموعه‌های سه‌تایی **rwx.user/group/world** در یونیکس ترجمه و تبدیل کند و سپس تغییر مجوزهای فایل 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 ۱ نباشد، آن تغییر مجوز فایل 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، بطور پیش-فرض همان مقدار پارامتر **Create mask** را خواهد داشت. برای اینکه به کاربری اجازه تصحیح همه مجوزهای **user/ group/ world** روی یک فایل 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 user/ group/ world را تغییر دهد

روی یک فایل باید این پارامتر به 000 تنظیم شود.

برای دایرکتوری، سامبا همانند چیزی که در مورد فایل 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 پیش فرض 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 فایل‌ها و

دایرکتوری‌هایشان full Control باشند، باید در فایل smb.conf دربخش 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

مقدمه

سه سطح برای فراهم کردن حداقل امنیت در یک سایت (شبکه) وجود دارد که عبارتند از: Firewall، تنظیم سرویس‌دهنده میزبانی که در حال اجرای سامباست و خود سامبا. 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 روش‌های مختلفی استفاده می‌کند؛ از جمله استفاده از همان ACL ها در روی هر منبع مشترک. در این بخش به بررسی این روش‌ها و امکانات می‌پردازیم. نکته قابل توجه این است که هرگز با رعایت این نکات امنیتی نباید تصور کنید که سرویس‌دهنده سامبای شما به یک دژ غیر قابل نفوذ تبدیل شده است.

استفاده از Host-Based Protection

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 host قبول می‌کند. یعنی اگر سامبایی که نصب کرده‌اید ناامن باشد و مستقیماً به اینترنت وصل باشد قطعاً نفوذپذیر^{۲۶} خواهد بود. یکی از ساده‌ترین راه‌های جلوگیری از این امر، استفاده از hostdeny و hostsallow است که می‌توان در فایل تنظیم سامبا اضافه کرد. به صورت زیر:

²⁶ Vulnerable

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 SMB که از خود سرویس‌دهنده^{۲۷} و دو شبکه 192.198.2. و 192.168.3. برقرار می‌شود، اجازه برقرای اتصال داده می‌شود و غیر از این موارد هیچ کس حق اتصال ندارد و به محض فرستادن اولین پکت ارسالی رد خواهند شد.

استفاده از User-Based Protection

می‌توان دسترسی به سرویس‌دهنده را با کاربران خاصی نیز محدود کرد. اگر بخواهید فقط کاربرانی که مد نظر دارید به سرویس‌دهنده وصل شوند، باید در بخش global از فایل تنظیم smb.conf به صورت زیر عمل کنید:

valid users = @smbusers , jacko

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

استفاده از Interface Protection

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

interfaces = eth lo*

bind interfaces only = yes

²⁷ localhost

با تنظیمات فوق، سامبا فقط به اتصالاتی که از روی اینترفیس هایی که با `eth` شروع می‌شوند و نیز `loopback`، برقرار می‌شود پاسخ می‌دهد. مثل `eth0`، `eth1`. البته نام اینترفیس ها به نوع سیستم عامل بستگی دارد. این نام هایی که گفتیم روی `Linux` کاربرد دارد.

بنابراین اگر یک اتصالی از روی اینترفیس `ppp0` صورت پذیرد، فوراً رد خواهد شد.

استفاده از Firewall

معمولاً از `Firewall` در مواقعی استفاده می‌کنیم که می‌خواهیم از خارج از شبکه بعضی از سرویس‌های خاص در دسترس باشند یا نه. این روش تکنیک خوبی برای داشتن امنیت در شبکه است. هرچند توصیه می‌شود حتماً برای امنیت بیشتر از روش‌های دیگر نیز در کنار `Firewall` استفاده شود.

برای تنظیم `Firewall` باید بدانید که چه پورتهایی را می‌خواهید باز بگذارید و چه پورتهایی را ببندید.

معمولاً سامبا از پورت‌های زیر استفاده می‌کند:

UDP/137- Used by nmbd

UDP/138- Used by nmbd

TCP/139- Used by smbd

TCP/445- Used by smbd

پورت آخر در سالهای اخیر مورد استفاده قرار گرفته است.

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 localhost و شبکه 192.168.115.0 امکانپذیر خواهد بود. و اگر سرویس گیرندگان دیگر بخواهند وصل شوند با پیغام Access denied مواجه خواهند شد و نمی توانند منابع مشترک را جستجو کنند و نیز قادر به دسترسی به Share های دیگر نیز نخواهند بود. استفاده از این روش پیشنهاد نمی شود مگر اینکه نتوانید از روشهای قبلی استفاده نمایید.

NTLMv2 security

روش تصدیق اصالت مبتنی بر NTLM یک روش پیشرفته هویت شناسی در وی‌ندوز می باشد. برای بررسی دقیقتر این روش به کتابهای موجود در این زمینه مراجعه کنید.

برای تنظیم تصدیق اصالت NTLMv2 باید Registry key های زیر را بدانید:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]

"Imcompatibilitylevel"=dword:00000003

مقدار 00000003 به این معنی است که NTLMv2 فقط response را می فرستد. سرویس گیرندگان

از تصدیق اصالت NTLMv2 استفاده می کنند. Domain Controller تصدیق اصالت های NTLM،

LM و NTLM v2 را قبول می کنند.

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

"NtlmMinClientSec"=dword:00080000

مقدار 00080000 به این معنی است که فقط NTLMv2 Session security ها 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.

به روز رسانی سامبا

توجه داشته باشید که همیشه به سایت سامبا^{۲۸} 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 به روز رسانی سامبا اکیداً توصیه می‌گردد.

²⁸ <http://www.samba.org/>

فصل هشتم

Classical Printing Support and CUPS

مقدمه

یکی از مهمترین و ضروری‌ترین سرویس‌هایی که باید به کاربران ارائه شود، سرویس چاپ است. سامبا می‌تواند این سرویس را برای سرویس‌گیرندگان شبکه شامل استفاده‌کنندگان ویندوزی با قابلیت اعتماد بالا فراهم کند. این سرویس چاپ سامبا هم می‌تواند روی یک سرور Stand-alone اجرا شود و هم روی یک سرور (Domain Member) عضو دامنه. تنظیماتی که روی این سرویس انجام می‌شود می‌تواند بسیار ساده یا پیچیده باشد و به طور کلی می‌توان آن را جایگزین سرور چاپ در ویندوز NT یا 2000 کرد و نیز قابلیت‌های متعددی را به آن افزود. سرویس‌گیرندگان نیز می‌توانند با استفاده از مکانیزم "Print'n'Print" چاپگر و درایوهای آنرا به دست آورده و نصب نمایند. اگر به یک Accounting مرکزی نیاز داشته باشیم، به طوری که برای هر صفحه مقداری از حساب کاربر کم شود، این کار را نیز می‌توان با Common UNIX (CUPS) Printing System به بهترین نحو انجام داد.

در این فصل به بررسی چگونگی تنظیم و راه‌اندازی سرویس چاپ در سامبا می‌پردازیم. اکثر مطالبی که در این فصل آورده‌ایم در مورد CUPS نیز کاربرد دارد. در ادامه فصل به چگونگی استفاده از سرویس CUPS می‌پردازیم.

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

مقدمه تکنیکی

سامبا یک “middleman” است. به این ترتیب که فایل‌هایی که باید چاپ شود، از سرویس‌گیرندگان ویندوز (یا دیگر SMB ها) می‌گیرد و آنها را به سیستم چاپ تحویل می‌دهد تا پردازش لازم روی آنها صورت پذیرد. بنابراین سامبا نیاز دارد تا با هر دو طرف ارتباط برقرار کند:

- سرویس‌گیرندگان چاپ ویندوز

- سیستم چاپ یونیکس

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

در واقع سامبا job مربوط به چاپ را از سرویس‌گیرنده چاپ می‌گیرد که این job ها نیز در یک فضای محلی spool شده‌اند. وقتی تمام job چاپ دریافت شد، سامبا دستور چاپ را می‌دهد و فایل مربوطه را نیز به آن ارسال می‌کند. (Local unix/Linux print).

مراحل پردازش چاپ از سرویس‌گیرنده به سرویس‌دهنده سامبا

چاپ موفقیت‌آمیز از یک سرویس‌گیرنده ویندوز به یک سرویس‌دهنده یونیکسی با استفاده از سرویس‌دهنده چاپ سامبا شامل شش یا نهایتاً هفت مرحله خواهد بود:

۱. یک اتصال از سوی ویندوز به چاپگر به اشتراک گذاشته شده باز می‌شود. (برقرار می‌شود)
۲. سامبا باید کاربر را شناسایی کند.
۳. ویندوز یک کپی از فایل 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 فایل به محیط Spooling چاپ یونیکس فرا می‌خواند.
۶. سیستم چاپ یونیکس job مربوط به چاپ را پردازش می‌کند.
۷. ممکن است نیاز باشد که فایل چاپ پاک شود (حذف شود). این آیتم به تنظیمات Spooler چاپ شما بستگی دارد.

پارامترهای مرتبط با تنظیمات چاپ در سامبا

- چند پارامتر در فایل smb.conf برای تنظیم چاپ وجود دارد. همانند پارامترها و تنظیمات قبلی دو سطح Service و Global از این پارامترها وجود دارد.
- Global Parameters : که به تعاریف اختصاصی اعمال نمی‌شود. اگر خطایی در آن باشد با برنامه testparm مشخص می‌شود و به شما گزارش داده می‌شود.
 - Service Level Parameters : این پارامترها می‌تواند (ممکن است) در بخش [global] در فایل smb.conf تعیین شوند. در این مورد، آنها رفتار پیش‌فرض همه سرویس‌های مشترک را تعریف می‌کنند.

تنظیمات ساده چاپ

در اینجا مثالی از یک تنظیم ساده چاپ در سامبا آورده شده است. که از تعداد کمی پارامتر برای تنظیم استفاده کرده است. با وجود این به راحتی سرویس چاپ را فراهم می‌سازد. وقتی شما یک پارامتر را در فایل `smb.conf` تعیین و مشخص می‌کنید، مقدار پیش‌فرض `overwrite` می‌شود. هنگامیکه `testparm` با مجوز `root` اجرا می‌شود، قادر است تمام تنظیمات را گزارش دهد. یعنی هم مقادیر پیش‌فرض و هم تنظیمات فایل `smb.conf` و ضمناً هشدارهایی برای پارامترهایی که تنظیم نشده‌اند اعلام می‌کند. خروجی برنامه `testparm` حدود ۳۴۰ خط و یا بیشتر است و بنابراین بهتر است هنگام اجرا آن را با یک برنامه صفحه‌بندی Pipe کنید.

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

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

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 دستورا برای نمونه می‌توانید در زیر ببینید :

```
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 برنامه `testparm` در سامبای 3 متفاوت از سامبای 2.2.x است.

توجه داشته باشید که همیشه لازم است به عقب برگردید و خروجی برنامه `testparm` را به دقت بررسی کنید. اینکار در واقع عیب‌یابی یا همان Troubleshooting است و توصیه می‌شود که هرگاه تنظیم خاصی مورد نظر شما 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.

جزئیات بیشتر

به مثال زیر که یک فایل تنظیم برای چاپ در یک سیستم BSD است دقت کنید. انتخاب سیستم BSD

به دلیل رایج بودن آن سیستم 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 [global].[printers] 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 سرور اعمال می‌شوند، در این بخش آورده می‌شود.

■ **printing=bsd** : این پارامتر باعث می‌شود تا از دستورات مربوط به سیستم BSD 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 فایل **printcap** مشخص می‌شوند و همه چاپگرها

قابل **browse** 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 آنصورت 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 پیش فرض **yes** است، تعیین

می‌کنید که آیاکن مربوط به **Add printer wizard** در دایرکتوری **printers** از میزبان سامبا

(که در **Network Neighborhood** دیده می‌شود و یا با دستور **net view** می‌بینید) ظاهر گردد.

با **Add printer wizard** شما می‌توانید درایور چاپگر را تعیین کنید.

■ **Max print jobs=100** : حداکثر تعداد **job** هایی که در یک زمان می‌تواند روی سرور سامبا فعال

باشد را تعیین می‌کند. در اینجا این تعداد به ۱۰۰ تنظیم شده است. اگر بیش از این تعداد به سرور

فرستاده شود، در آن صورت سرویس گیرنده با پیغام خطای **no more space available on**

server مواجه خواهد بود. اگر این مقدار را به ۰ (پیش فرض هم ۰ است) تنظیم کنید، به این معنی

است که هیچ محدودیتی در تعداد **job** های همزمان وجود ندارد.

■ `Printcap name=/etc/printcap` : سامبا در این فایل به دنبال فایل چاپگرهای در دسترس می‌گردد.

■ `Printer admin=@ntadmin` : اعضای گروه `@ntadmin` باید قادر باشند درایوهای 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 یونیکسی باشد) به طور ضمنی کاربر `root` همیشه عضو `admin` چاپگر است. علامت `@` باعث می‌شود تا سامبا به نام گروه‌های موجود در فایل `/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 سرور چاپگر کاهش یابد.

■ `Use client driver= no` : `yes` بودن این پارامتر فقط روی ویندوزهای `NT/200x/xp` (و نه `95/98/ME`) تاثیر دارد. و نباید آن را در سرور سامبایی که درایورهای معتبری روی آن نصب است، به `yes` تنظیم کنید. برای توضیحات بیشتر به فایل کمکی `smb.conf` مراجعه کنید.

بخش `[printer]`

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

■ `Comment=All printers` : این توضیح به سرویس‌گیرندگانی که می‌خواهند از چاپگرهای به اشتراک گذاشته شده استفاده کنند، نشان داده می‌شود.

■ **Printable=yes** : سرویس [printers] باید بعنوان **printable** اعلام شود. اگر غیر از این باشد

smbd در هنگام **startup** برای بازشدن با مشکل مواجه خواهد شد. این پارامتر به سرویس‌گیرندگان

اجازه می‌دهد تا فایل‌های **spool** را بتواند در دایرکتوری مشخص شده در پارامتر **path** بازکنند و یا

بنویسند. این پارامتر جهت جداکردن چاپگرهای به اشتراک گذاشته شده از فایل های مشترک توسط

سامبا به کار می‌رود.

■ **Path=/var/spool/samba** : این پارامتر به دایرکتوری استفاده شده توسط سامبا برای **spool**

کردن فایل چاپ رسیده، اشاره می‌کند، که آن دایرکتوری باید **writable** باشد و بیت **stickey** نیز

در آن **set** شده باشد. همچنین این دایرکتوری نباید همان دایرکتوری **spool** تعیین شده در تنظیمات

زیر سیستم چاپ یونیکس 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. دز تعداد زیادی از سیستم‌ها حساب کاربری **guest** به کاربری به نام “**nobody**”

منطبق می‌شود. این کاربر در فایل **passwd** در یونیکس با کلمه عبور خالی (**Empty**) وجود دارد

ولی توجه کنید که نمی‌توان با آن روی یونیکس **login** کرد. در بعضی از سیستم‌ها کاربر **guest**

مجاز استفاده از چاپ را ندارد. شما می‌توانید این محدودیت را به طریق زیر امتحان کنید. ابتدا با

کاربر **guest** با استفاده از **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.

■ **Read only=yes** : وجود این پارامتر باعث می‌شود تا کاربران دیگری که از منابع مشترک دیگر

استفاده می‌کنند، نتوانند در دایرکتوری مخصوص این سرویس (چاپ) تغییری دهند. (هرچند

printable بودن این سرویس همیشه اجازه **write** را در این دایرکتوری می‌دهد، اما فقط در طول

عملیات مربوط به چاپ اگر کاربران مجوز اتصال را داشته باشند و به طور عادی عملیات **write**

اجازه داده نمی‌شود).

■ **writable=no** : این پارامتر مترادف پارامتر **read only = yes** است

هربخش [my-printer-name]

در این بخش که می‌تواند به تعداد چاپگرهای به اشتراک گذاشته شده شما باشد، تنظیمات اختصاصی هر

چاپگر را انجام می‌دهید. باید سعی کنید نامی که به چاپگر اشتراک گذاشته شده می‌دهید با نام منبع دیگر یکی

نباشد. چون در آن صورت وقتی درخواستی از طرف سرویس گیرنده به سامبا فرستاده شود، سامبا ابتدا به دنبال

آن نام در بین فایل‌های به اشتراک گذاشته شده می‌رود. در صورتی که آنرا پیدا کند شما را به آن متصل می‌کند

و نه به چاپگر.

■ **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 دایرکتوری پیش فرض.

■ **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 سرویس‌گیرندگان به راحتی بتوانند چاپگر مورد

نظر را در Network Neighborhood 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 سرویس‌گیرندگان می‌توان دسترسی به

چاپگر را محدود کرد. این کار اصلاً تاثیری در ایجاد امنیت ندارد. فقط یک کنترل ساده روی

دسترسی‌ها است.

■ **Host deny= turbo-xp,10.10.160.33,10.10.161.65** : سرویس‌گیرندگان مشخص شده

در این پارامتر، به هیچوجه اجازه دسترسی به چاپگر را ندارند. همانطور که مشاهده می‌کنید، در اینجا

هم می‌توان نام کامپیوتر و یا IP آن را آورد.

■ **Guest ok=no** : با این پارامتر دیگر هیچ کاربر guest نمی‌تواند به آن دسترسی داشته باشد.

سؤالی که در این بخش مطرح می‌شود این است که آیا لازم است درایوهای چاپگر روی یک سیستم سامبا

به منظور پشتیبانی از سرویس‌گیرندگان ویندوز نصب شود یا خیر؟

جواب این است: خیر، لازم نیست.

سرویس‌گیرندگان ویندوز NT/2000 می‌توانند (Add Printer Wizard)APW هایشان را برای

نصب درایورها به طور محلی اجرا کنند. این همان روش استفاده شده در سرویس‌گیرندگان 9x/Me است.

(هرچند در سامبای نسخه 2.2.0 یک bug وجود داشت که باعث می‌شد سرویس‌گیرندگان ویندوز

NT/2000 نیاز داشته باشند سرور سامبا یک درایور درست برای چاپگر را فراهم کند که این اشکال در نسخه

2.2.1 برطرف شد) اما با این همه یکی از قابلیت‌های جدید در سامبا برای نصب درایو چاپگر، استفاده از

بخش [printers] در سرور سامبا است که کار را بسیار آسان کرده است. با وجود این قابلیت، تمام سرویس-گیرندگان (شامل 95/98/Me) درایور نصب شده را در هنگام اولین اتصال به چاپگر به اشتراک گذاشته شده دریافت می کنند. depositing , uploading درایور به بخش [printers] و کارهای بعدی آن به چند طریق می تواند انجام شود:

اجرای APW روی یک سرویس گیرنده 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 command-line هستند.

استفاده از Cupsaddsmb (که فقط برای سیستم چاپ CUPS کار می کند و نه برای

LPRng,LDR/LPD و ...)

در ویندوزهای 98/Me وقتی یک چاپگر به اشتراک گذاشته می شود، نام [printers] به آن سرویس داده می شود. این سرویس در سامبای 2.2 در این بخش پارامترهایی نیز برای تنظیم آن در نظر گرفته می شد. اما در سامبای 3 این پارامترها حذف شدند. در واقع نام جدید [print\$] برای محل به دست آوردن درایورهای 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 Upload و download فایل های درایور چاپگر، باید ابتدا یک بخش به نام [print\$] ایجاد کنیم. دقت کنید نام این بخش یعنی [print\$] در سرویس گیرندگان ویندوزی یک hardcode است و نمی تواند تغییر کند. چون سرویس گیرندگان ویندوزی طوری برنامه نویسی شده اند

که دقیقاً این اسم را در لیست سرویس‌های به اشتراک گذاشته شده جستجو می‌کنند تا فایل‌های درایور چاپگر را به دست آورند. در این بخش که پارامترهای آن را معرفی می‌کنیم باید دایرکتوری را که فایل‌ها در آن قرار دارد را مشخص کنیم.

پارامترهای زیر در قسمت [print\$] نیاز است:

```
[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 هنگام لیست شدن در

سرویس‌گیرنده ظاهر می‌گردد (معمولاً سرویس‌گیرندگان ویندوزی این توضیح را نمی‌بینند ولی این توضیح در

خروجی دستور Smbclient -L samba Server ظاهر می‌شود).

Path = /etc/ samba/ Printers : مسیری که فایل‌های درایور ویندوز در آن قرار می‌گیرند برای

deposit از Unix.

browseable= no : باعث می‌شود که بخش به اشتراک گذاشته شده [print\$] برای سرویس‌گیرندگان

از Network Neighborhood قابل دیدن نباشد. هرچند بار هم شما می‌توانید آن را با استفاده از دستور:

از `Connect network drive menu` یا `Dosprompt` در `Net use g:\ Samba server\printer` جستجوگر ویندوز `Mount` کنید.

`read only = yes` : چون ما نمی‌خواهیم هرکسی به فایل‌های درایورها 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 (`write`) برای کاربران خاص مثل `root` ایجاد کنید. این لیست با پارامتر فوق ایجاد می‌شود.

Share Directory [print\$]

در قسمت قبل گفتیم به منظور ایجاد محل برای به‌دست آوردن درایور چاپگر توسط سرویس‌گیرندگان، بخش `[print$]` را ایجاد کرده‌ایم. حال این منبع مشترک باید دارای درایورهای چاپگر برای معماری‌های مختلف سرویس‌گیرندگان باشد. بنابراین باید در دایرکتوری که در پارامتر `path` مشخص کردیم، چند زیردایرکتوری ایجاد نماییم. یک نکته مهم این است که درست مثل نام بخش `[print$]` که یک `hardcode` بود و نباید تغییری در آن می‌دادیم، نام زیر دایرکتوری‌ها نیز `hardcode` است و دقیقاً به همین شکلی که در زیر آورده‌ایم باید ایجاد شوند:

```
[print$] --+
|--W 32X86      # Server drivers to windows NT x86
|-- WIN40       # Server drivers to windows 95/98
|--W 32ALPHA    # Server drivers to windows NT Alpah_Axp
|--W 32MIPS     # Server drivers to windows NT R4000
|--W 32PPC      # Server drivers to windows NT Power PC
```

بعد از اینکه از درستی تنظیمات فوق مطمئن شدید، به یکی از سیستم‌های سرویس‌گیرنده 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 بایستی چاپگرهایی را که می‌توانند با چاپگرهای به اشتراک گذاشته شده منطبق شوند ببینید.

نصب درایورها در [print\$]

خوب، حتماً تا الآن تمام مراحل را به خوبی پشت سر گذاشته‌اید. فایل‌های درایور چاپگر بعد از در دسترس بودن باید نصب شوند، چون در غیراینصورت چاپگر قابل استفاده نخواهد بود. دو راه برای نصب فایل درایور چاپگر در بخش [print\$] وجود دارد:

با استفاده از دستور rpcclient و زیر دستورهایش (در اینجا : Setdriver , adddriver) از روی هر سیستم یونیکسی.

با اجرای یک GUI (Add Printer Wizard ,Printer Properties) از روی هر سرویس‌گیرنده ویندوز NT/200x/XP که البته گزینه دوم شاید آسانتر باشد. در ادامه به بررسی این دو راه می‌پردازیم.

ویژارد اضافه نمودن چاپگر

روی ویندوزهای NT/200x/XP، برنامه گرافیکی Add Printer Wizard به نصب درایورهای چاپگر روی سرویس‌گیرندگان کمک می‌کند و با این شرایط نصب آنها چندان مشکل نخواهد بود. شما باید Properties چاپگری را که می‌خواهید درایور آن را نصب کنید، ببینید. یعنی جستجوگر ویندوز Network

Neighborhood را باز کنید و منابع به اشتراک گذاشته شده مربوط به سرور سامبای خود را ببینید. دایرکتوری مربوط به چاپگر(Printers) را باز کرده و روی آیکن چاپگر راست کلیک کنید و سپس Properties را انتخاب کنید. در صورتی که درایور نصب نشده باشد با پیغام خطای زیر روبرو خواهید شد:

Device Setting Cannot 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 اینصورت فقط

صفحه مربوط به Properties چاپگر را خواهید دید. در اینجا دو راه برای نصب داریم:

انتخاب درایور از لیست درایورهای نصب شده که این لیست در ابتدای کار خالی خواهد بود.

کلیک روی New Driver برای نصب یک درایور چاپگر جدید، که در اینصورت یک ویزارد شروع به

کار می‌کند و مراحل کاری آن دقیقاً شبیه نصب درایورهای دیگر در سیستم‌عامل ویندوز است.

ما فرض را بر این داریم که شما با مراحل نصب درایور در ویندوز آشنا هستید. از اینکه اتصال شما با

سرور سامبا با یک کاربر ممتاز است مطمئن شوید. اگر در این مورد شک دارید، می‌توانید با کمک دستور

smbstatus شرایط را چک کنید. در صورتیکه بخواهید درایور چاپگر را روی سیستم‌عامل دیگری غیر از

ویندوز نصب کنید (NT &6)، باید از sharing tab از Properties چاپگر استفاده کنید.

Common UNIX Printing System (CUPS)

CUPS²⁹ یک سیستم مدیریت چاپ برای پلتفرم‌های یونیکس است که توسط Easy Software Production به منظور ترویج یک استاندارد برای چاپ روی تمام نسخه‌های یونیکس و کاربران آن توسعه داده شده است. CUPS از IPP³⁰ به عنوان مبنای مدیریت jobها و Queueهای چاپ استفاده می‌کند. همچنین در آن از پروتکل‌های LPD³¹، SMB³² و Appsocket به منظور سهولت بیشتر در انجام توابع استفاده می‌شود. CUPS برای پشتیبانی از عملیات چاپ تحت یونیکس، جستجوگر چاپگرهای شبکه و PPD³³ را نیز اضافه کرده است. همچنین شامل یک Image File RIP است که برای چاپگرهای non-Postscript به کار می‌رود. CUPS تحت لیسانس GNU General Public Licanse و GNU Library General Public Licanse است.

مروری بر سیستم چاپ CUPS

مسئله چاپ در یونیکس برای چند سال مشکل‌آفرین بود. بر خلاف ویندوز و Mac Os، یونیکس دارای اینترنتیست استاندارد برای چاپگرها نبود. به همین منظور CUPS برای حذف مشکلات چاپ طراحی شد. در واقع CUPS یک سیستم چاپ مشترک بین تمام نسخه‌های یونیکس است که نیازهای چاپ را برای کاربران برطرف می‌کند. CUPS دارای featureهای قوی و منحصر به فردی است که سعی داریم در این بخش به برخی از آنان بپردازیم.

همانطور که گفتیم CUPS بر مبنای استاندارد اینترنتیسی که IPP نامیده می‌شود پابرجاست. IPP یک پروتکل استاندارد برای چاپ و مدیریت jobهای چاپ و تنظیمات چاپگر مثل resolution, media size و

²⁹ Common UNIX Printing System

³⁰ Internet Printing Protocol

³¹ Line Printer Daemon

³² Server Message Block

³³ Postscript Printer Description

... تعریف می‌کند. مانند تمام پروتکل‌های 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 برخلاف پروتکل‌های دیگر، در IPP می‌توان از Authentication، access control و encryption استفاده کرد و در نتیجه آن را کاراتر و امن‌تر از دیگر سرویس‌های چاپ ساخت.

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

کلیه مستندات مربوط به CUPS را می‌توانید در سایت <http://www.cups.org/> مشاهده نمایید. معمولاً CUPS در سامبای 3 و 2.2.x به طور پیش‌فرض نصب است و برای استفاده از آن کفایت به فایل smb.conf رفته و تنظیمات موردنظر خود را انجام دهید. اما اگر CUPS روی سیستم شما نصب نبود، به چند طریق می‌توانید آن را نصب یا کامپایل کنید. به عنوان مثال روی سیستم redhat می‌توانید rpm آن را دانلود 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 start و stop نمودن سرویس CUPS معمولاً بسته به پلت‌فرمی 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 پلت‌فرم‌ها انتخاب کرد و به کار برد.

تنظیمات پایه‌ای CUPS

برای استفاده از سرویس چاپ CUPS، در ساده‌ترین حالت فقط کافیست به فایل `smb.conf` رفته و دو

تنظیم زیر را انجام دهید:

`Printing = cups`

`Printcap name = cups`

برای نوشتن شدن نحوه تنظیمات به مثال زیر که یک مثال بسیار ساده از سیستم 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 فایلها با فرمتهای گرافیکی، `text`، `PDF` و `Postscript` را

که از سرویس گیرندگان ویندوز دریافت می‌کنید، چاپ نمایید. مثال بعدی کمی پیچیده‌تر از مثال قبلی است و

با استفاده از آن قادر خواهید بود سرویس CUPS را برای همه تعریف کنید. اما یک چاپگر را به طور متفاوت

با تنظیمات خاص خودش تعریف نمایید. به تنظیمات آن در فایل `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

```

همانطور 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

اجازه 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 سیستم به آن

دسترسی دارند.

تنظیمات پیچیده تر در CUPS

برای انجام تنظیمات CUPS دو راه وجود دارد:

۱. استفاده از اینترفیس وب

۲. استفاده از command-line

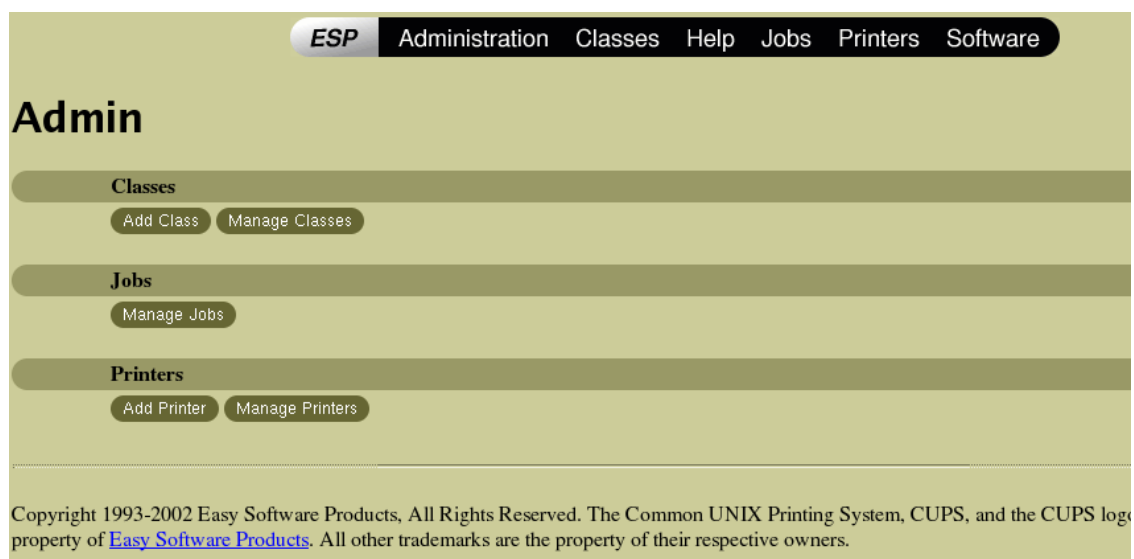
استفاده از اینترفیس وب

وب سرور CUPS یک اینترفیس خوب برای برخی تنظیمات CUPS ایجاد نموده است. برای استفاده از

این اینترفیس باید جستجوگر موردنظر 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 صفحه فوق، باید برای Add کردن چاپگر، روی Add Printer کلیک نمایید و به تنظیمات

خواسته شده پاسخ دهید. بقیه تنظیمات نیز به همین ترتیب با اینترفیس انجام می‌پذیرد.

استفاده از command-line

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 command-line از دستور `lpadmin` می‌توان استفاده نمود. این دستور در دایرکتوری `/usr/sbin` قرار دارد.

اضافه کردن یک چاپگر

از دستور `lpadmin` با سوئیچ `-p` به منظور تصحیح و یا اضافه نمودن چاپگر استفاده می‌شود. برای `add` نمودن یک چاپگر به CUPS باید از دستور زیر استفاده نمایید:

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

مثلاً برای یک چاپگر HP DeskJet که به پورت `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 `add` کردن یک چاپگر HP LaserJet با استفاده از اینترفیس 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 درایور چاپگر استاندارد که معمولاً یک فایل `PPD` است، را مشخص می‌کند.

`PPD`ها معمولاً در مسیر `/usr/share/cups/model/` قرار دارند. لیست کامل مدل‌های در

دسترس را می‌توانید با استفاده از دستور `lpinfo -m` و سوئیچ `-m` روی سیستم خود مشاهده کنید.

- **class -r**: چاپگر مورد نظر را از لیست **class** مشخص شده حذف می‌کند. اگر آن **class** خالی باشد آن **class** را حذف می‌کند.
- **device-uri -v**: **device** ی که می‌خواهد با چاپگر ارتباط برقرار کند را تعیین می‌کند.
- **E**: چاپگر را فعال ساخته و **job**ها را می‌پذیرد.
- **ppd-file -P**: یک فایل **PPD** محلی برای درایور چاپگر تعیین می‌کند.
- **printer -d**: به منظور پیش‌فرض نمودن یک چاپگر.

حذف یک چاپگر

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

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

Start و Stop کردن یک چاپگر

دستورات **enable** و **disable** روی یک چاپگر، **queue** های آن چاپگر را **Start** و **Stop** می‌کند. در واقع هر چاپگری که **disable** است، **job**هایی که به آن می‌رسد را دریافت می‌کند اما تا **restart** 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، کلیه **job**هایی که به آن رسیده چاپ خواهند شد.

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

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

قبول یا رد یک **job** مربوط به چاپگر

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

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

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

تنظیم Quota روی چاپگر در CUPS

با استفاده از سرویس CUPS می‌توانید از لحاظ اندازه و تعداد صفحات روی هر چاپگر محدودیت ایجاد نمایید. دقت نمایید که این محدودیت هایی 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 اندازه jobها را به کیلوبایت 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
```

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 پیش فرض تمام کاربران به چاپگر دسترسی دارند.

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

اگر بخواهید اجازه دهید سه کاربر `paul`، `peter` و `mary` اجازه چاپ داشته باشند و بقیه نه، 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. 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 دامین وی‌ندوز

مقدمه

Winbind یکی از اجزای سامباست که مسألهٔ logon متحد را روی دامین حل می‌کند. Winbind از پیاده‌سازی یونیکسی برای فراخوانی RPC‌های ویندوزی، PAM³⁴ و NSS³⁵ به منظور اینکه کاربران دامین ویندوز NT بتوانند به عنوان کاربران UNIX روی ماشین یونیکس کار کنند، استفاده می‌کند. در این فصل سیستم Winbind را توصیف می‌کنیم. و کارهایی را که می‌تواند انجام دهد را توضیح می‌دهیم. همچنین به چگونگی تنظیم درست آن می‌پردازیم و اینکه چگونه کار می‌کند.

Winbind سه کار مختلف زیر را انجام می‌دهد:

تصدیق‌اصالت و بررسی اعتبار کاربران (با PAM)

تبدیل شناسه‌ها (با NSS)

Winbind یک دیتابیس به نام winbind_idmap.tdb نگهداری می‌کند که تبدیل بین Unix

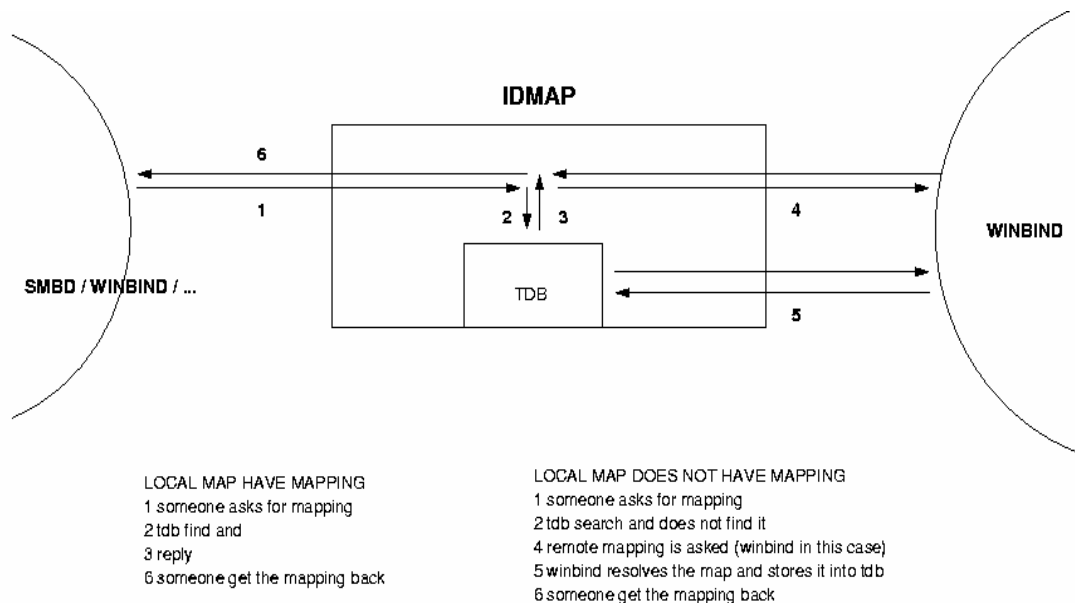
UIDs/GIDs و WindowsNT SIDs را ذخیره می‌کند. این تبدیل فقط برای کاربران . گروههایی

استفاده می‌شود که هیچ UID/GID محلی ندارند.

³⁴ Pluggable Authentication Module

³⁵ Name Service Switch

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 `mapping` دینامیکی استفاده نخواهد کرد. به شکل زیر دقت کنید:



به خوبی می‌دانید که یونیکس و میکروسافت ویندوز NT مدل‌های متفاوتی را برای نمایش اطلاعات کاربر و گروه‌ها به کار می‌گیرند و نیز از تکنولوژی‌های مختلفی برای پیاده‌سازی آنها استفاده می‌کنند. به همین دلیل یکی نمودن آنها (دو سیستم) 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 سیستم یونیکس و ویندوز ایجاد نموده و از برنامه‌های سامبا^{۳۶} برای فراهم نمودن تبادل سرویس‌های فایل و چاپ بین دو سیستم استفاده می‌کنند. اما در این روش چون به دو دیتابیس مختلف نیاز است؛ کار کمی برای اضافه نمودن و حذف کاربران مشکل می‌شود.

³⁶ Samba Suit

گاهی اوقات به مشکلات همزمان سازی³⁷ عملیات روی دیتابیس ها بر می خوریم. می توان مسائل مربوط به

Unified logon برای سیستم های یونیکس را به سه مسأله کوچکتر تقسیم کرد:

- بدست آوردن اطلاعات گروه و کاربران ویندوز NT

- تصدیق اصالت کاربران ویندوزی

- تغییر کلمه عبور برای کاربران ویندوز NT

با سیستم winbind یک راه حل ساده و خوب برای تمام مسائل فوق می توان ایجاد کرد.

از winbind در سازمانهایی استفاده می شود که یک ساختار دامین مبتنی بر NT دارند و می خواهند در آن

از سرویس دهنده ها و workstation های یونیکسی استفاده کنند. Winbind به این سازمانها اجازه می دهد

تا سیستمهای یونیکسی خود را به دامین 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 overhead می -

کاهد.

Winbind چگونه کار می کند؟

سیستم winbind بر اساس معماری client/server است. هنگامیکه سرور winbindd در حال

اجراست، به دامین یونیکسی گوش می دهد و منتظر رسیدن درخواست است. این درخواستها توسط سرویس -

گیرندگان NSS و PAM تولید می شوند و به طور مرتب فرایند می شوند.

مواردی که winbind از آنها استفاده می کند در زیر آورده شده است:

³⁷ Synchronize

Microsoft Remote Procedure Calls

همانطور که می‌دانید، از RPC برای عملیات مختلف مرتبط با شبکه بین ماشینهای ویندوزی از قبیل مدیریت راه‌دور، تصدیق‌اصالت کاربران و عملیات spooling چاپ استفاده می‌شود. Winbind از RPCهای مختلفی برای تعیین گروهها و کاربران دامین و بدست آوردن اطلاعات جزئی آنها استفاده می‌کند. وقتی یک درخواست³⁸ برای بدست آوردن اطلاعات کاربر و گروه مستقیماً به یک windows PDC فرستاده می‌شود، winbind اطلاعات حساب کاربری NT را به نام کاربری و گروه در unix تبدیل می‌کند.

Name Service Switch

NSS یکی از featureهایی است که امروزه در اکثر سیستم‌عامل‌های یونیکسی وجود دارد. این سرویس کنترل چگونگی دسترسی به دیتابیس‌های اطلاعاتی مورد نیاز توسط mail aliases، اطلاعات کاربران، hostnameها و غیره را بر عهده دارد. مثلاً یک workstation یونیکسی می‌تواند اطلاعات مورد نیازش را از یکسری فایلها روی یک فایل‌سیستم محلی بدست آورد. و یک سیستم شبکه‌ای اول ممکن است تلاش کند اطلاعاتش را از روی فایلهای محلی بدست آورد، سپس با یک دیتابیس NIS برای اطلاعات کاربری مشاوره کند و یا از یک سرویس‌دهنده DNS برای اطلاعات hostname کمک بگیرد. برنامه‌های واسط کاربری NSS به winbind اجازه می‌دهد تا خود را به عنوان یک منبع اطلاعاتی در هنگام resolve نام کاربری و نام گروه در یونیکس معرفی کند. Winbind از این واسطه‌ها استفاده می‌کند و اطلاعات بدست آمده از سرویس-دهنده ویندوز NT توسط RPCها را برای تهیه اطلاعات جدید کاربران به کار می‌گیرد. به این ترتیب، می‌توان اطلاعات کاربران یک دامین NT را از روی یک ماشین یونیکسی که در حال اجرای winbind است، بدست آورد. همچنین می‌توان اطلاعات کاربران دامین‌هایی که به دامین مورد نظر Trust شده‌اند را نیز دید.

فایل کنترل اولیه NSS، /etc/nsswitch.conf است. وقتی یک سرویس در یونیکس درخواستی برای گرفتن اطلاعات می‌دهد، کتابخانه C فایل /etc/nsswitch.conf و خطی که مربوط به تنظیمات آن سرویس

مورد نظر است را بررسی می‌کند. به عنوان مثال برای سرویس `passwd` اگر در فایل `nsswitch.conf` به صورت زیر تنظیم شده باشد:

Passwd: file example

کتابخانه C اول `/lib/libnss_files.so` و سپس `/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 اینترفیس NSS یک راه آسان برای `winbind` مهیا می‌کند و آن این است که همه آنچه قرار بود از طریق فوق انجام شود در فایل `libnss_winbind.so` در دایرکتوری `/lib` قرار داده می‌شود و `“winbind”` در فایل `/etc/nsswitch.conf` در مکان مناسب قرار داده می‌شود. از این به بعد کتابخانه C برای پاسخگویی به درخواستهای `resolve` اطلاعات نام کاربران و گروهها، `winbind` را صدا می‌زند.

Pluggable Authentication Modules

Pluggable Authentication Modules که PAM نیز خوانده می‌شود، یک سیستم مجزا برای هویت‌شناسی و مجوزدهی است. با PAM می‌توان بدون کامپایل کردن دوباره برنامه‌های کاربردی مختلف برای آنها روشهای هویت‌شناسی متفاوتی تعیین کرد. PAM همچنین برای سیاستگذاری‌های خاص مجوزدهی مفید خواهد بود.

Winbind از اینترفیس PAM مربوط به مدیریت کلمات عبور و مدیریت هویت‌شناسی برای یکی کردن سیاستهای ویندوز و یونیکس استفاده می‌کند. در نتیجه این امر، کاربران ویندوز NT می‌توانند روی یک ماشین یونیکسی `login` کنند و در برابر یک PDC مناسب تصدیق‌اصالت شوند و همچنین می‌توانند کلمات عبور خود را تغییر دهند.

PAM توسط فایل‌های کنترلی در دایرکتوری `/etc/pam` تنظیم می‌شود. البته برای هر سرویسی که نیاز به تصدیق‌اصالت دارد. وقتی یک درخواست تصدیق‌اصالت از یک برنامه کاربردی صادر می‌شود، کدهای PAM در کتابخانه C در قسمت مربوطه بررسی می‌شود. مانند NSS، در اینجا نیز یک اینترفیس به Winbind اختصاص می‌یابد و کارهای بررسی به او واگذار می‌شود و همه آنچه که باید بررسی شود در فایل `pam_winbind.so` در دایرکتوری `/lib/security` قرار داده می‌شود.

User and Group Allocation

هر گاه در ویندوز NT/200x یک کاربر یا گروه ایجاد می‌شود، یک RID^{۳۸} به آن اختصاص می‌یابد که این شماره RID کمی با شماره‌ای که یونیکس به کاربر و گروه اختصاص می‌دهد فرق می‌کند و متفاوت است. کار Winbind تبدیل RIDها به Unix IDها و بالعکس است. نتیجه این تبدیل‌ها به طور دائمی در یک دیتابیس مربوط به ID mapping در یک دیتابیس tdb ذخیره می‌شود و در نتیجه یک روش ثابت و پایداری برای تبدیل RIDها به Unix IDها خواهد شد.

Result Caching

در یک سیستم 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 سیستم 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^{۳۹} می‌شود، شماره مورد نظراً آنچه روی PDC است، مقایسه می‌شود. اگر با هم یکی نبودند، اطلاعات موجود روی Cache کنار گذاشته می‌شود و مستقیماً از روی PDC اطلاعات دریافت می‌شوند.

³⁸ Relative Identifier

³⁹ Expire

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 فایل تنظیمات سامبای شما در حال حاضر به درستی کار می‌کند، از آن یک پشتیبان تهیه نمایید. اگر سیستم شما از PAM استفاده می‌نماید از کل محتویات دایرکتوری `/etc/pam.d` پشتیبان تهیه نمایید و در آخر اینکه اگر دیسکت بوت نساخته‌اید، الآن آنرا بسازید!

دلیل پشتیبان گرفتن از موارد فوق این است که در مورد PAM، اگر فایل تنظیمات آن بهم بریزد تقریباً login کردن روی سیستم شما غیر ممکن است. آخرین نسخه سامبای ۳ شامل سرویس Wibind است که می‌توانید آن را از سایت بدست آورید.

برای اینکه کاربران دامین بتوانند به فایلها و منابع به اشتراک گذاشته شده سامبا و کلاً سرویسهایی که توسط سرویس‌دهنده سامبا ارائه می‌شود دسترسی داشته باشند، باید PAM روی سیستم شما به درستی نصب و تنظیم شده باشد. برای کامپایل کردن ماژولهای Winbind شما باید حداقل کتابخانه PAM را نصب شده روی سیستم خود داشته باشید. (PAM development libraries) به وب سایت PAM مراجعه کنید:

<http://www.kernel.org/linux/libs/pam/>

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

تنظیم `nsswitch.conf` و `winbind Libraries` روی لینوکس

PAM یک جز استاندارد در نسخه‌های سیستم‌عامل Unix/Linux است ولی متأسفانه فقط تعداد کمی از این سیستمها کتابخانه‌های مربوط به `pa-devel` را که برای سامبا و تنظیماتش نیاز است نصب می‌کند. به

علاوه سامبای ۳ به طور اتوماتیک فایل‌های winbind را در محل‌های مناسب روی سیستم شما نصب می‌کند.

پس ممکن است برای تنظیمات فقط به تغییر در فایل nsswitch.conf نیاز داشته باشید.

کتابخانه‌های مورد نیاز برای اجرای صحیح سرویس winbind با nsswitch لازم است در محل‌های

صحیح کپی شوند. با دستور زیر اینکار 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، شما به عنوان کاربر root باید فایل /etc/nsswitch.conf را ویرایش کرده و اجازه دهید تا

گروه‌ها و کاربران توسط سرویس winbind قابل رویت باشند. پس به فایل nsswitch.conf رفته و آن را

به شکل زیر تنظیم کنید:

```
passwd : files winbind
```

```
shadow : files
```

```
group : files winbind
```

کتابخانه‌های مورد نیاز سرویس winbind بعد از هر بار راه‌اندازی مجدد سیستم به طور خودکار به

Idconfig Cache وارد می‌شوند ولی برای اینکه اینکار سریعتر انجام شود و نیاز به راه‌اندازی مجدد سیستم

نباشد می‌توانید با دستور زیر به طور دستی اینکار را انجام دهید:

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

دستور فوق، libnss_winbind را برای سرویس winbindd قابل دسترسی می‌کند.

تنظیم smb.conf برای Winbind

برای کنترل نحوه عملکرد winbindd چند پارامتر در فایل smb.conf نیاز است. این پارامترها در صفحات کمکی مربوط به winbindd(8) به طور جزئی آورده شده‌اند. به شکل زیر که قسمت global از فایل 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
```

متصل نمودن سرور سامبا به دامین PDC

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

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

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

“joined the domain DOMAIN.”

که DOMAIN نام دامین مورد نظر شماست.

برای اینکه سرویس winbindd را start کنید کافی است دستور زیر را به کار ببرید:

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

نکته: در توضیحات فوق فرض شده است که سامبا در دایرکتوری `/usr/local/samba` نصب شده است.

ممکن است نیاز باشد محل نصب سامبا روی سیستم خود را پیدا کنید.

جالب است بدانید که `winbindd` می‌تواند در مد `dual`⁴⁰ اجرا شود. یعنی دو پراسس در حال اجرا باشد. اولی فقط برای پاسخگویی به درخواستها به کمک `cache` که سریعتر به سرویس‌گیرنده پاسخ داده شود و دومی به منظور به‌روزرسانی `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 مد `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.

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

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

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

خب ، حال می‌توانید یکسری اطلاعات درباره کاربران دامین خود ببینید:

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

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

⁴⁰ Dual daemon mode

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

واضح است که نام دامین مثال فوق CEO و جدا کننده 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 سیستم خود (local) را مشاهده کنید. به

صورت زیر:

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

تنظیم winbind با PAM

اگر بخواهید از winbind برای تصدیق‌اصالت سرویس‌های دیگر استفاده کنید باید در فایل‌های تنظیم

PAM تغییراتی را بدهید باز هم تأکید می‌کنم که اگر تا به حال از دایرکتوری `/etc/pamd` پشتیبانی

نگرفته‌اید، حال وقت آن است که این کار را انجام دهید.

برای استفاده winbind با سرویس‌های دیگر به یک ماژول PAM نیاز دارید که این ماژول باید با دستور زیر در دایرکتوری `../source/nsswitch` کامپایل شود.

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

فایل `.so pamwinbind` باید در محل ماژول‌های دیگر PAM Security کپی شود. این محل در پلت‌فرم‌های مختلف فرق می‌کند. مثلاً در RedHat دایرکتوری `lib security` و در solaris دایرکتوری `usr/lib security` خواهد بود.

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

در اینجا برای پلت‌فرم‌های Linux/FreeBSD-specific تنظیمات PAM را انجام می‌دهیم. فایل `/etc/pam/samba` نیازی به تغییر ندارد.

برای اینکه اجازه دهیم سرویس‌های دیگر نظیر Telnet، Login معمولی و FTP با winbind تصدیق-اصالت شوند، باید تغییراتی را در entry های `/etc/xinetd.d` (یا `/etc/inetd.conf`) بدهیم. در redhat7.1 و بعد از آن برای تغییرات باید خطهای `enable=no` از فایل‌های `/etc/xinetd.d/telnet` و `/etc/xinetd.d/wuftp` را به `enable=yes` تغییر دهید.

برای اینکه سرویس ftp به درستی کار کند همچنین نیاز است که یا دایرکتوری‌های خاص کاربران دامین را روی سرور داشته باشید و یا اینکه `home directory template` را به یک دایرکتوری `general` برای تمام کاربران دامین تغییر دهید. اینکار به راحتی با استفاده از پارامتر `global template homedir` انجام می‌شود.

فایل `/etc/pam/ftp` می‌تواند به صورت زیر برای اینکه `winbind ftp` به فایل 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 فایل `/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

`required pam-securetty.so` باعث می‌شود کاربر `root` روی شبکه `Login` نکند، اضافه شده است.

همچنین خط `sufficient lib/security/pam unix.so use-first-pass` بعد از خط `winbind.so`

اضافه شده است که `rid` را می‌گیرد.

با توجه به مطالب فوق، `winbind` با استفاده از `PAM`، `NSS` و `RPC` های مناسب باعث یکی بودن

سیاست های روی دو پلت فرم ویندوز و یونیکس شده و بدین ترتیب در کاهش هزینه‌های مدیریت و کمتر

شدن پیچیدگی آنها تاثیر بسیاری خواهد داشت.

تکنیکهای پشتیبان‌گیری

پروژه سامبا، پروژه ۱۰ سال اخیر است که سازندگان اصلی آن مدیران سیستمها هستند. مدیران سیستمهای یونیکس از ابزارهای یونیکس برای فایل سیستمهای آن استفاده می‌کنند. در چهارسال گذشته شمار مدیران سیستمی شبکه‌های ویندوزی 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 تکنیکهای تهیه پشتیبان، مفید واقع شوند.

backup PC

Backup PC نسخه 2.0.0 در sourceforge منتشر شده است. Feature های جدید در سایت <http://backuppc.sourceforge.net> شامل حمایت از /sync/rsyncd و اینترفیس های CGI به منظور جهانی سازی آن است. (شامل انگلیسی، فرانسوی، و اسپانیولی و آلمانی)

Backup PC یک بسته مبتنی بر زبان برنامه نویسی Perl با کارایی بسیار بالا جهت گرفتن پشتیبان از Linux و Unix و یا PC های ویندوز و Laptop به یک دیسک سرور است. این نرم افزار را به طور دقیق می‌توان تنظیم نمود و نیز از نظر نصب و نگهداری راحت و آسان است.

Backup PC تحت لیسانس GNUGPL است و روی سرویس دهندگان Linux / unix / freenix اجرا می‌شود و روی Linux ، Unix ، Windows 9x/ME ، win 98 ، win xp و Mac osx تست شده است.

Rsync

Rsync یک برنامه انعطاف پذیر برای کپی گرفتن فایل ها یا دایرکتوری هاست. Rsync ، گزینه های زیادی برای انتخاب اینکه چه فایل هایی کپی شوند و چگونه قرار است منتقل شوند، دارد و از آن می توان برای ftp و http ، scp یا rcp استفاده کرد.

پروتکل rsync remote-update به آن اجازه می دهد که فقط اختلاف بین دو مجموعه از فایل ها را در روی شبکه منتقل کند. که اینکار را با استفاده از یک الگوریتم کارای checksum-search که در بسته rsync توضیح داده شده است انجام می دهد.

بعضی از feature های اضافه در rsync به قرار زیر هستند:

حمایت از کپی Link ، device ، owners ، groups و permission ها.

نیازی به مجوز root ندارد. (privilege)

توسط ssh یا rsh می تواند استفاده شود.

Amanda

Amanda که مخفف Advanced Maryland Automatic Network Disk Archive است،

یک سیستم تهیه پشتیبان است که به مدیران LAN اجازه می دهد تا یک سرویس دهنده پشتیبان master را

برای تهیه پشتیبان از چند host به یک فضای حافظه بزرگ مثل Tape drive تنظیم کنند. Amanda

می تواند از شمار زیادی از Workstation ها که دارای نسخه های مختلف از Unix هستند، پشتیبان تهیه کند.

نسخه های اخیر آن حتی می تواند از سامبا برای تهیه پشتیبان از host های ویندوزی نیز استفاده کند.

برای اطلاعات دقیقتر می توانید به سایت <http://www.amanda.org> مراجعه نمایید.

BOBS: Browseable Online Backup System

BOBS نیز یک سیستم تهیه پشتیبان online کامل است که از یک دیسک بزرگ (حجیم) برای ذخیره

پشتیبانها استفاده می کند و کاربران فایل ها را با استفاده از یک جستجوگر وب جستجو می کند. سایت اینترنتی

آن هم به آدرس زیر است:

[<http://bobs.sourceforge.net/>](http://bobs.sourceforge.net/)

فصل دهم

مهاجرت از نسخه های قدیمی سامبا به نسخه ۳

مقدمه

در این فصل به تفاوت‌های بین دو نسخه 2.2.8 و 3.0.0 سامبا می‌پردازیم و بررسی می‌کنیم که کدامیک از پارامترهای تنظیم در آن تغییر کرده است و نیز چگونگی حرکت از 2.2.x به 3.0.0 را بیان می‌نمائیم. رفتار پیش‌فرض نسخه 3.0.0 تقریباً شبیه رفتار نسخه 2.2.x است. در واقع وقتی پارامترهای جدید `passdb backend` در فایل `smb.conf` تعریف شده‌اند، سامبای 3 همان سامبای 2.2.x با پارامتر `encrypt` `passwords = yes` است و از دیتابیس `smbpasswd` استفاده می‌کند. یک نکته جالب و خوب این است که در طول `upgrade` دو نسخه به هم، `domain` و `machine SID` ها حفظ می‌شوند.

امکانات جدید در سامبای 3

حداقل چهارده Feature جدید در سامبای 3 وجود دارند:

۱. حمایت از Active Directory. این نسخه قادر است به یک ADS realm به عنوان عنصر

سرویس‌دهنده متصل شود و با استفاده از Kerberos / LDAP کاربران را تصدیق‌اصالت کند.

۲. حمایت از Unicode.

۳. سیستم جدید تصدیق‌اصالت. سیستم تصدیق‌اصالت داخلی تقریباً به طور کامل بازنویسی شده است.

۴. سیستم جدید filename mangling که کاملاً بازنویسی شده است و دیگر یک دیتابیس داخلی mangling map ها 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 دسته‌ای از برنامه‌ها و دستورات کاربردی مثل smbpasswd با زیر دستورات net جایگزین شوند.

۶. سامبا در نسخه 3 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 سرویس چاپ WIN XP/200X.

۸. ماژول‌های rpc قابل بارگذاری جدید برای passdb backend و مجموعه‌های کاراکتری^{۴۱}.

۹. کار کردن winbindd در مد dual به طور پیش‌فرض به منظور کارایی بهتر.

۱۰. حمایت برای انتقال یا به روز رسانی از یک دامین win NT 4.0 به دامین سامبا با نگهداری و حفظ کاربران و گروه‌ها و SID های دامین.

۱۱. حمایت از تشکیل ارتباطات معتمد^{۴۲} با NT 4.0 DomainController

۱۲. حمایت اولیه و ابتدایی از معماری winbind توزیع شده^{۴۳} با استفاده از دایرکتوری LDAP

جهت ذخیره تبدیل SID به UID/GID.

۱۳. به روز رسانی به samba documentation tree

⁴¹ Character set

⁴² Trust

⁴³ Distributed

۱۴. حمایت کامل از امضای سرویس‌دهندگان و سرویس‌گیرندگان 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 فایل smb.conf در نسخه 3.0.0 تغییر کرده‌اند، در اینجا آورده

شده است.

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

پارامترهای که حذف شده‌اند:

به ترتیب حروف الفبا :

- 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

پارامترهایی که جدید اضافه شده اند:

این پارامترها بسته به نوع کارشان دسته بندی (گروه بندی) 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)