

Samba-Server liest Benutzerdaten aus dem Active Directory



Full-Service

Dass ein Samba-Server seinen Dienst als Datei- und Druckerserver neben einem Windows 2003 Server versieht, ist keine Besonderheit mehr. Interessant wird die Aufgabenstellung, wenn der Druckerserver als Ausgabe eine PDF-Datei erzeugen, diese per Email an den Eigentümer des Druckauftrags verschicken soll und dabei weder die Mitarbeiter, noch ihre Email-Adressen kennt.

Die Prominent Dosiertechnik GmbH ist eine Hersteller von Komponenten und System der Fluid-Dosiertechnik und bietet Lösungen für die Wasseraufbereitung. Die IT-Landschaft besteht aus der weitverbreiteten Mischung aus Windows- und Linux-Servern.

Die Arbeitsplätze sind mit Windows 2000 Rechnern ausgestattet, die sich an einem Windows 2003 Server, der als Primary Domain Controller dient, anmelden. Der Versand von Dokumenten an Lieferanten und Kunden sollte nach Möglichkeit ausschließlich im PDF-Format erfolgen. Die Lizenzkosten für die Anschaffung der dafür notwendigen Software, schließlich sollte eine größere Anzahl von Arbeitsplätzen damit ausgestattet werden, ließ das Unternehmen nach einer anderen Lösung für diese Anforderung suchen.

Ein in die Domäne integrierte Samba-Server sollte im Netzwerk einen Drucker zur Verfügung stellen, der die Erzeugung eines PDF-Dokuments aus einer beliebigen Windows-Anwendung ermöglicht. Damit die Benutzer auf dem Samba-Server nicht nach den erstellten PDF-Dateien suchen müssen, sollen die fertigen PDF-Dateien an den jeweiligen Besitzer per Email verschickt werden.

Es galt somit zwei Aufgaben zu lösen: Zum einen muß ein Skript entwickelt werden, das beim Aufruf die Druckdaten übernimmt und daraus eine PDF-Datei erstellt. Zum anderen muß die Email-Adresse des Eigentümers der PDF-Datei aus dem Active Directory des Windows 2003 Server ermittelt und die Datei an diese Adresse verschickt werden.

Samba

Zunächst einmal wird der Samba-Server für die Anbindung an das Active Directory konfiguriert und dabei auch der erforderliche Postscript-Drucker bereitgestellt, aus dessen Druckdatei anschließend das PDF-Dokument erzeugt wird. Eine Einführung in die Anbindung eines Samba-Servers an das Active Directory findet man beispielsweise unter [1]. Bei der Einbindung des PS/PDF-Drucker unter Windows als Netzwerkdrucker sollte als Druckertreiber der Minolta Color PageWorks/Pro PS gewählt werden. Generell verwendet der Samba-Server CUPS als Drucksystem. Für die Erzeugung des PS-Dokuments

Samba-Server liest Benutzerdaten aus dem Active Directory



ist es jedoch erforderlich, als Drucksystem *printing=bsd* anzugeben. Zudem darf die Zeile *lpq command = /bin/true* nicht fehlen. Andernfalls wird der Drucker als offline angezeigt und die Druckaufträge werden nicht aus der Druckerwarteschlange gelöscht.

Samba-Konfiguration

```
;/etc/samba/smb.conf
[global]
    workgroup = ADS
    netbios name = pc103.ads.local
    realm = ADS.LOCAL
    security = ADS
    password server = win2ksrv.ads.local
    winbind separator = +
    idmap uid = 10000-20000
    idmap gid = 10000-20000
    winbind enum users = yes
    winbind enum groups = yes
    winbind enable local accounts = yes
    template shell = /bin/bash
    log file = /var/log/samba/log.smb.%U
    max log size = 500
    printcap name = cups
    cups options = raw

[pdfprinter]
    comment = Minolta Color PageWorks/Pro PS
    path = /samba/pdfprinter
    printing = bsd
    lpq command=/bin/true
    print command = /samba/pdfprinter/pdfscript "%s"
    printable = yes
    public = yes
    writeable = yes
```

Samba-Server liest Benutzerdaten aus dem Active Directory



PS zu PDF

Das in der Konfigurationsdatei aufgerufene Skript pdfscript ist wie folgt aufgebaut [2]:

```
#!/bin/bash
#
#
# Ermitteln des Dateinamens
FILE=$(egrep "^%%Title:" "$1" | head -n 1 | sed -e 's/^%%Title: //g' | sed -e 's/^(//g' | \
sed -e 's/(.*)\..*$\1/g' | tr -d "\r\n")
DATE=`date +%Y-%m-%d_%H.%M.%s`
FILE=`echo -n -e $FILE-$DATE`

# Entfernen von ueberfluessigen Daten am Anfang und am Ende der PS-Datei
POS_S=`egrep -n "^!PS-Adobe" "$1" | cut -d : -f 1`
POS_E=`egrep -n "%EOF" "$1" | cut -d : -f 1`
sed 1,$[POS_S - 1]d "$1" | head -n $[POS_E - POS_S + 1] > "${FILE}.ps"

# Loeschen der Druckdatei (smbprn.xxxx)
rm -f "$1"

# Erzeugen der PDF-Datei
gs -q -dCompatibilityLevel=1.3 -dNOPAUSE -dBATC H -sDEVICE=pdfwrite \
-sOutputFile="${FILE}.pdf" -c save pop -f "${FILE}.ps"

# Loeschen der Postscript-Datei
rm -f "${FILE}.ps"
```

Die Suche

Im nächsten Schritt wird die Tatsache genutzt, daß sich im Active Directory des Windows 2003 Servers auch die Email-Adressen der Mitarbeiter befinden (sollten). Die vom Skript erzeugte Postscript-Datei gehört dem Mitarbeiter, der den Druckjob veranlaßt hat. Im Dateisystem befindet sich beispielsweise die folgende Datei:

```
-rw-r--r-- Firma+mmueller Firma+Domänenbenutzer smbprn.wkoad.pdf
```

Um nun den Namen des Mitarbeiters zu ermitteln, wird das Skript um die folgende Zeile erweitert:

```
# Ermitteln des Besitzers der Datei
OWNER=$(ls -l \x{FFFD}${FILE}.pdf\x{FFFD} | cut -f 4 -d " " | cut -f 2 -d "+")
```

Samba-Server liest Benutzerdaten aus dem Active Directory



Die Ausgabe von ls wird mittels cut in einzelne Felder zerlegt, wobei das Leerzeichen als Trennzeichen dient. Im vierten Feld befindet sich der Name des Eigentümers, mit vorangestelltem Domännennamen und dem Pluszeichen. Dieser String wird mit dem zweiten cut zerteilt, das zweite Feld enthält den Namen des Eigentümers und der Wert wird der Variablen OWNER zugewiesen. Der Name des Mitarbeiters dient nun als Filter für eine Suche im Active Directory. Das Active Directory basiert auf dem LDAP-Protokoll und läßt sich mit den Befehlen aus dem OpenLDAP-Paket problemlos abfragen:

```
ldapsearch -LLL -h 192.168.0.106 -P 3 -x -D "cn=Administrator,cn=users,dc=ads,dc=local" -w root12 -b \
"dc=ads,dc=local" „(&(&(objectClass=user)(objectCategory=person))§§(sAMAccountName=$OWNER))" mail
```

Tabelle 1: Die Bedeutung der Parameter:

-LLL	keine Ausgabe von Kommentaren oder der LDIF-Version, damit sich die Ausgabe leichter weiterverarbeiten läßt.
-h 192.168.0.106	Die IP-Adresse oder der Name des Active Directory Servers.
-P 3	Die zu verwendende Version des LDAP-Protokolls, im Falle von Windows 200x ist es die Version 3.
-x	Verwendung der einfachen Authentifizierung anstelle von SASL
-D "cn=Administrator,cn=users,dc=ads,dc=local"	Der Distinguished Name (DN), der "Benutzername", mit dem die Anmeldung am Active Directory.
-w root12	Angabe des Passworts für den mit dem Parameter -D übergebenen Anmelde-DN
-b "dc=adc,dc=local"	Punkt im Verzeichnisbaum des Active Directorys, an dem die Suche beginnen soll.
(&(&(objectClass=user)(objectCategory=person))\ (sAMAccountName=\$OWNER))	Der Suchfilter, wobei der zu findende Eintrag drei Bedingungen zwingend erfüllen muß: Er muß eine Objektklasse vom Typ user und die Objektkategorie person besitzen, zudem muß der Wert des Attributs sAMAccountName dem Wert der Variablen OWNER entsprechen. Auch wenn die Schreibweise etwas ungewöhnlich ist, die beiden führenden & sorgen für eine logische UND-Verknüpfung der drei Filter.
mail	Das Attribut, dessen Wert ausgegeben werden soll.

Aus Sicherheitsgründen sollte für den Abruf der Email-Adresse ein eigener Account angelegt werden und nicht der Account des Administrators benutzt werden.

Samba-Server liest Benutzerdaten aus dem Active Directory



Das PDF kommt

Das vom Samba-Server aufzurufende Drucksript wird nun um die Abfrage des Active Directorys, den Versand der PDF-Datei und das anschließende Löschen der PDF-Datei. Die Ausgabe von `ldapsearch` enthält nicht nur die Email-Adresse. Daher wird die Ausgabe mit Hilfe der Pipe an den Befehl `grep` weitergeleitet, welcher die Zeile erfaßt, die mit `mail` beginnt und daher die Email-Adresse enthält. Mit dem anschließenden Befehl `cut` wird die Zeile in einzelne Felder zerlegt, wobei das Leerzeichen als Trennzeichen dient. Das zweite Feld dieser Zerlegung enthält die Email-Adresse.

Abfrage und Versand

Abfrage des Active Directory, zur Ermittlung der Email-Adresse

```
email=$(ldapsearch -LLL -h 192.168.0.106 -P 3 -x -D "cn=Administrator,cn=users,dc=ads,dc=local" \  
-w root12 -b "dc=ads,dc=local" "(&(&(objectClass=user)(objectCategory=person)) \  
(sAMAccountName=$OWNER))" mail | grep "^mail:" | cut -f 2 -d " ")
```

Versand der fertigen Datei an die zuvor ermittelte Adresse

```
mutt -s "PDF-File" -a "${FILE}.pdf" $email < /dev/null
```

Loeschen der PDF-Datei

```
rm -f "${FILE}.pdf"
```

Zu guter Letzt muß sichergestellt werden, dass die Email auch zugestellt werden kann. Wenn der Samba-Server nicht zugleich der Mailserver ist, dann muß in der Konfiguration des lokalen MTA angegeben werden, an welchen Mail-Server die Email weiterzuleiten ist. Im Falle von Postfix setzt man dazu in der `main.cf` den Parameter `relayhost` auf die IP-Adresse oder den Rechnernamen des gewünschten Mail-Servers.

[1] Markus Klinke "Fenster-Öffnung", Linux-Magazin 05/05, S. 48

[2] Martin Rode "Drucken mal anders", iX 3/2003, S. 139