Tipps und Tricks

In diesem Bereich des Wikis werden sporadisch Kurzanleitungen, Workarounds usw. zu verschiedenen Themenbereichen auftauchen.

VirtualBox

Da der invis Server auch in Form virtueller Maschinen nutzbar ist und wir auf Messen gelegentlich entsprechende Images verteilen, beginnt die Tipps und Tricks Ecke mit einem Verweis auf VirtualBox - unserem favorisierten Virtualisierungssystem. Da mit einigen Einträgen zum Thema VirtualBox zu rechnen sein wird, widme ich diesem Thema eine eigene Wiki-Seite.

Tipps und Tricks zu VirtualBox

Linux-Clients und NFS-Fileserver

Die Gruppen-basierte Zusammenarbeit auf einem Linux-Fileserver gestaltet sich schwierig, wenn diese per NFS auf den Fileserver zugreifen. Zwar lassen sich mit gesetztem SGID-Bit auf den Freigabe-Verzeichnissen Gruppen-Besitzrechte auf alle Objekte im Ordner vererben, nicht aber die Zugriffsrechte. Letztere sind von der „umask“ abhängig.

Auf openSUSE-Systemen ist die vorgegebene umask „022“, was bedeutet, das neu angelegte Dateien und Verzeichnisse für die besitzende Gruppe kein Schreibrecht gewähren:

```
Verzeichnis
         | u | g | o |
----------------------
Default  | 7 | 7 | 7 |
umask    | 0 | 2 | 2 |
----------------------
Ergebnis | 7 | 5 | 5 | = rwx,r-x,r-x

Datei
Default  | 6 | 6 | 6 |
umask    | 0 | 2 | 2 |
----------------------
Ergebnis | 6 | 4 | 4 | = rw-,r--,r--
```

Um pauschal auch für die besitzende Gruppe Schreibrecht zu gewähren muss die umask auf den Wert „002“ geändert werden:

```
Verzeichnis
         | u | g | o |
----------------------
Default  | 7 | 7 | 7 |
```

```
umask    | 0 | 0 | 2 |
----------------------
Ergebnis | 7 | 7 | 5 | = rwx,rwx,r-x

Datei
Default  | 6 | 6 | 6 |
umask    | 0 | 0 | 2 |
----------------------
Ergebnis | 6 | 6 | 4 | = rw-,rw-,r--
```

Die umask ist prinzipiell Benutzer-bezogen. Sie kann an mehreren Stellen im System geändert werden. Wichtig dabei ist, dass die Änderung auf dem Fileserver-Client wirksam ist. Eine Änderung auf dem Server selbst, etwa in /etc/profile o.ä. bleibt wirkungslos.

Da openSUSE mit dem „pam_umask“ Modul arbeitet, kann die umask auch in den Einstellungen der einzelnen Benutzerkonten vorgenommen werden. Eingetragen wird eine persönliche umask in das „Gecos-Feld“. Hier ein Auszug aus einer entsprechend angepassten passwd-Datei:

```
...
stefan:x:10000:100:Stefan Schäfer,umask=002:/local/home/fump:/bin/bash
...
```

Da invis Server eine LDAP-basierte zentrale Benutzerverwaltung anbieten, **muss** die gezeigte Anpassung selbstverständlich im LDAP-Verzeichniseintrag der einzelnen Benutzer vorgenommen werden.

Melden Sie sich dazu über den Link „Verzeichnisdienst“ auf der Administrationsseite des Portals am LDAP-Verzeichnis an und ändern Sie das Feld „gecos“ betroffenen Benutzereinträge wie folgt ab:

DN: uid=**username**,ou=Users,ou=Benutzerverwaltung,dc=**invis-net**,dc=loc

Von: „System User“ zu „System User,umask=002“

Ab invis Version 6.7-R3 entspricht dies der Vorgabe, wenn Benutzer über das invis-Portal angelegt werden. Die Vorgabe kann in der Datei „/srv/www/htdocs/portal/config.php“ an die eigenen Wünsche angepasst werden.

Group-e Samba Dateimanager auch unter openSUSE

Out of the Box lässt sich der Samba Dateimanager von Group-e unter openSUSE nicht nutzen.

Das hat zwei Gründe:

1. Die smbclient-Methode funktioniert nicht, weil der PTY-Support in PHP seit einiger Zeit nicht mehr aktiviert ist. Dies zu lösen würde bedeuten PHP selbst neu zu übersetzen. Das wurde im Group-e Forum schon mehrfach diskutiert und stellt definitiv keine Lösung dar!!!!
2. Die smbmount-Methode funktioniert nicht, da ***smbmount*** schlicht in openSUSE nicht mehr enthalten ist. (Dürfte bei anderen Distris möglicherweise auch schon so sein) ***smbmount*** bzw. smbfs wird nicht mehr wirklich gepflegt. Als Ersatz ist das Paket cifs-mount mit den Kommandos ***mount.cifs*** und ***umount.cifs*** enthalten.

Im Gegensatz zu den alten Kommandos ***smbmount*** und ***smbumount*** ist bei den neuen aus Sicherheitsgründen das SUID-Bit nicht gesetzt.

Um diese Kommandos für group-e nutzbar zu machen muss zunächst allen Sicherheitsbedenken zum Trotz das SUID-Bit für beide Kommandos gesetzt werden:

```
chmod u+s /sbin/mount.cifs
chmod u+s /sbin/umount.cifs
```

Da Group-e leider immer noch die alten Kommandos voraussetzt und vermutlich niemand bei jeder neuen Version den Quellcode anfassen möchte, müssen noch zwei symbolische Links angelegt werden:

```
ln -s /sbin/mount.cifs /usr/bin/smbmount
ln -s /sbin/umount.cifs /usr/bin/smbumount
```

Das wars, danach funktioniert der Samba-Dateimanager auch unter openSUSE, wenn auch mit ein paar Abstrichen in Sachen Sicherheit.

Ergänzung:

Wenn es nicht funktioniert bitte die /etc/hosts kontrollieren. Wenn dort eine wie im folgenden Beispiel gezeigte Zeile zu finden ist, ist diese entweder zu löschen oder die 127.0.0.2 gegen die tatsächliche IP-Adresse zu tauschen.

```
127.0.0.2      invis65.invis-net.loc     invis65
```

(Bitte nicht mit der 127.0.0.1 verwechseln.).

Es sollte ein korrekter Eintrag direkt unter „127.0.0.1 localhost“ stehen:

```
127.0.0.1            localhost
192.168.200.10       invis65.invis-net.loc     invis65
```

Erläuterung:

smbmount fragt die /etc/hosts nach der IP des Servers ab und gibt sich mit der ersten zutreffenden Antwort zufrieden. Wenn dies mit 127.0.0.2 beantwortet wird und Samba mit der Option „bind interfaces only“ an bestimmte IPs gebunden ist, verweigert es einfach den Mount-Versuch.

Gibt man in der Freigaben-Konfiguration von Group-e statt des Hostnamens die IP-des Samba-Servers ein, funktioniert es immer.

Nein Danke Zensursula

Achtung, der folgende Text ist nicht ganz neutral. Er enthält persönliche Meinugsäußerungen. Ich bitte dies zu entschuldigen.

Ab Oktober 2009 soll das Web-Sperren-Gesetz gegen die Verbreitung von Kinderpornographie in Kraft treten. Da dieses Gesetzt, trotz des sicherlich aufrichtigen Ansatzes, am Thema vorbei geht und

allenfalls eine Zensurinfrastruktur im Internet etabliert, zeigen wir hier eine Möglichkeit auf, es zu umgehen. Möglicherweise hilft das ja dabei die Wirkungslosigkeit dieses Gesetzes zu verdeutlichen.

Wer einen invis-Server im eigenen Netz betreibt und sich (zumindest vorerst) sicher sein möchte, dass seine Nameserverabfragen nicht von „manipulierten“ Nameservern beantwortet werden, kann dies durch Ändern der „forwarders“ in der bind-Konfiguration umgehen.

Ändern Sie einfach in der Datei „/etc/named.conf“ die Einträge hinter „forwarders“:

```
        # The forwarders record contains a list of servers to which queries
        # should be forwarded.  Enable this line and modify the IP address
to
        # your provider's name server.  Up to three servers may be listed.
        # Die folgende Zeile ist um die IP-Adresse des fuer Sie zustaendigen
DNS
        # zu erweitern.

        forwarders { 194.25.2.129; 192.168.178.1; };

        # Enable the next entry to prefer usage of the name server declared
in
        # the forwarders section.

        forward first;
```

Tragen Sie statt des T-Online Nameservers und etwa dem einer Fritzbox (wie hier gezeigt) bis zu drei Nameserver aus der unter http://www.ungefiltert-surfen.de zu findenden Liste ein und starten Sie ***bind*** mit:

```
Kommandozeile: /etc/init.d/named restart
```

neu.

Deeplinks verhindern

Wenn der Webserver eines invis Servers auch via HTTPs aus dem Internet erreichbar ist, können die einzelnen Applikationen derzeit noch durch direkte Eingabe der Zieladresse im Browser ohne Umweg über das invis Portal erreicht werden.

Dieses Verhalten ist aus Sicherheitsgründen eher bedenklich und in der Regel nicht erwünscht. Um dies zu verhindern muss die Apache-Konfigurationsdatei /etc/apache2/vhosts.d/i7ssl.conf erweitert werden.

Tragen Sie dort für jede Applikation die nicht direkt angesprochen werden soll folgenden Eintrag ein:

```
    # Deeplinks verhindern
    <Directory /srv/www/htdocs/phpMyAdmin>
        SetEnvIfNoCase Referer "^http://invis.invis-net.loc" dontblock
        SetEnvIfNoCase Referer "^https://your.dyndns-domain.net" dontblock
```

```
        Order Deny,Allow
        Deny from all
        Allow from env=dontblock
    </Directory>
```

Das Beispiel zeigt den Deeplink-Schutz für das Verzeichnis von phpMyAdmin. Sie müssen lediglich die Domain-Namen an Ihre Gegebenheiten anpassen und den Apache neustarten. Danach sind die geschützten Applikationen nur noch über das invis-Portal erreichbar.

Die gezeigten Einträge werden ab invis Release 6.6-R4 generell für alle Applikationen Standard sein.