

# Postfix-Courier/Cyrus mit DES/AES-Verschlüsselung

cplinux // 03.10.2009 13:18

Kategorie: [E-Mail-Server](#)

Die beiden Tutorials

[www.cplinux.de/e-mail-server/postfix-mit-mysql-courier-konfiguration.html](http://www.cplinux.de/e-mail-server/postfix-mit-mysql-courier-konfiguration.html)

[www.cplinux.de/e-mail-server/postfix-mit-mysql-cyrus-konfiguration.html](http://www.cplinux.de/e-mail-server/postfix-mit-mysql-cyrus-konfiguration.html)

beschreiben, wie man eine Basis-Konfiguration mit Postfix & Courier bzw. Postfix & Cyrus in Verbindung mit MySQL aufsetzt.

Das Ganze hat prinzipiell nur einen kleinen Nachteil. Derjenige, der Zugriff auf die Datenbank bekommt (normalerweise sollte das nur über localhost und den Benutzer postfix z.B. möglich sein), kann natürlich die Passwörter im Klartext auslesen.

Um das zu ändern, ohne dass man auf die Encrypt-Option zurückgreifen muß (die nicht in allen Versionen der Betriebssysteme ohne Patch verfügbar ist), kann man z.B. auf die DES-Verschlüsselung zurückgreifen, die von MySQL unterstützt wird.

So kann man mit Hilfe eines Schlüssels, den man selbst definieren kann, ein bestimmtes Passwort verschlüsseln und wieder entschlüsseln.

Im Folgenden gehe ich davon aus, dass die E-Mail-Adresse selbst für die Verschlüsselung des Passworts verwendet wird. Aus der E-Mail-Adresse könnte man natürlich auch vorher noch einen Hash erzeugen oder diese anderweitig verschlüsseln (z.B. md5(email), sha1(email), password(email), etc., siehe unten). Das könnte natürlich auch z.B. ein Hash sein, der sich in der gleichen oder einer anderen Tabelle befindet.

Das sollen erst einmal Anregungen sein, um zu zeigen, was man machen könnte.

Folgende Dateien ändern sich demnach:

*/etc/postfix/sasl/smtp\*.conf: (Zeile austauschen)*

```
select DES_DECRYPT(password,email) from users where email='%u@%r' and status='1'
```

*/etc/postfix/mysql\_auth.cf: (komplett)*

```
user = postfix
password = post
dbname = postfix
table = users
select_field = email
where_field = DES_DECRYPT(password,email)
additional_conditions = and status='1'
hosts = localhost
```

*/etc/courier/authmysqlrc: (Zeile austauschen)*

```
MYSQL_CLEAR_PWFIELD DES_DECRYPT(password,email)
```

## Anmerkung:

Möchte man nicht nur die E-Mail-Adresse verwenden, sondern z.B. vorher daraus einen MD5-Hash erzeugen, ersetzt man alle *DES\_DECRYPT(password,email)*

durch

*DES\_DECRYPT(password,MD5(email))*

Legt man einen neuen User an, muß man das Passwort natürlich verschlüsseln:

```
INSERT INTO users (user_login, user_password, user_email, user_status) VALUES ('testuser', DES_ENCRYPT('testpassword', 'testuser@example.net'), 'testuser@example.net', '1');
```

bzw.

```
INSERT INTO users (user_login, user_password, user_email, user_status) VALUES ('testuser', DES_ENCRYPT('testpassword', MD5('testuser@example.net')), 'testuser@example.net', '1');
```

Statt DES\_ENCRYPT kann man natürlich auch AES\_ENCRYPT verwenden.

Als Resultat kann man die Passwörter nun nicht mehr im Klartext aus der Datenbank auslesen, man kann sie aber entschlüsseln, wenn man den Schlüssel kennt.

Danach noch einmal die Dienste neu starten:

```
/etc/init.d/courier-authdaemon restart
```

```
/etc/init.d/courier-imap restart
```

```
/etc/init.d/postfix restart
```

**That's it.**