Dovecot Diffie-Hellman

Introduction

The default key size for the DH group in Dovecot is 2048. In some cases, users may wish to increase this size for security purposes. This article discusses how this can be adjusted through the terminal.

Procedure

To increase the DH group key size you will need to alter the dh.pem file that Dovecot uses to determine this. By default this is configured to be /etc/dovecot/dh.pem in the dovecot.conf configuration. You can use the following command to verify the current setting for this value.

```
doveconf -S |  grep '^ssl_dh'
```

To check the current size use the following command on the dh.pem returned from the above command. Since the default is 2048 in size, it would return output like "DH Parameters: (2048 bit)". This command can also be used to verify the change was successful.

```
openssl dhparam -in /etc/dovecot/dh.pem -text -noout
```

To update the length you will need to alter with the following command. You would replace the 2048 value with the desired length. Please note that this command may take a long time to complete and should be allowed to finish.

```
openssl dhparam 2048 > /etc/dovecot/dh.pem
```

That's it, now your Dovecot service will use the new DH group key size!

For additional information regarding this change and the Dovecot configurations, see the official documentation from the upstream providers below.

https://wiki.dovecot.org/SSL/DovecotConfiguration

https://support.cpanel.net/hc/en-us/articles/1500002760162-How-to-change-DH-group-key-size-in-Dovecot

---

Version #2
Erstellt: 25 April 2023 17:22:37 von Harald Geritzer
Zuletzt aktualisiert: 25 April 2023 17:36:55 von Harald Geritzer