
Mail Gateway Synchronization with HA

<https://campus.barracuda.com/doc/43847136/>

You can configure mail gateway synchronization for a Barracuda NG Firewall in an HA cluster.

In this article:

Automatic Email Synchronization

Automatic email traffic synchronization is quite similar to the transparent failover that is available for the Forwarding Firewall (see [Transparent Failover for an HA Firewall](#)). When mails are spooled, they are synchronized on the HA partner after a maximum of 10 seconds. However, the synchronization procedure itself is one-way only. That means that changes made to the mail log and envelope on the partner unit are lost when the primary unit takes back the mail gateway. When synchronized mail is delivered, it is deleted on the HA partner. If a synchronization attempt fails, it is stored in a transaction log for pending actions and is retried as soon as possible.

Manual Email Synchronization after an HA Takeover

During an HA takeover, the mail gateway service on the server of the secondary unit starts and performs the mail delivery. After successful recovery of the primary unit, the server of the primary unit takes over mail delivery again and the mail gateway running on the secondary unit stops delivering mail. If the HA takeover happens during mail delivery, mail delivery might not be finished because some mail could be left in the mail queue of the secondary HA server. In other words, HA takeover can be initiated while the spooling process of mails is active. This occurs especially during heavy loads when lots of emails are processed by the mail gateway service.

In this case, you must manually move leftover mail from the secondary unit to the primary HA partner and initiate the delivery so that no mail is lost after an HA takeover. The following description shows step-by-step what must be done in such a case:

While connected via SSH, do not enter any commands unless you know exactly what you are doing.

Step 1. Connecting

Establish a connection to the secondary HA unit using Barracuda NG Admin. Now select SSH from the unit menu and log into the secondary HA unit as root. Change to the spool directory of the mail gateway by using the following command line:

```
cd /var/phion/spool/mgw//spool/
```

For , type in the name of the server, and for , type in the name of the mail gateway service you have configured when introducing the service.

Step 2. Check for Undelivered Mails

This check is done by listing the content of the spool directory. Therefore, enter the following command:

```
ls -l
```

If the result of this command is Total 0, there are no undelivered mails left, and it is not necessary to continue. In this case, type "exit" to close your SSH session. However, if there are files with the extension .body and .env, continue with the next step.

Step 3. Copy the Spool Directory

Copy all files to the mail input directory of the active (primary) mail gateway service. To do so, use the following command line:

```
scp * IP:/var/phion/spool/mgw/_ /input/
```

The parameter indicates the box management IP of the primary HA unit where the mail gateway service is active. You will be prompted to enter the root password of the primary unit.

Step 4. Copy the vscan Directory (optional)

If the virus scanning for mails is active, it is necessary to copy this directory, too. Therefore, change to the vscan directory of the mail gateway by using the following command line:

```
cd ../vscan/
```

Now copy all files to the mail input directory of the active (primary) mail gateway service. To do so, use the following command line:

```
scp * :/var/phion/spool/mgw/_ /input/
```

Step 5. Initiating Delivery Manually

As soon as Step 3 and Step 4 (optionally) are complete, the manually initiated delivery can be started on the primary HA unit. For this purpose, you need a SSH session to the active unit. This session is established by using the following command line:

```
ssh
```

For , type in the box management IP of the primary HA unit where the mail gateway service is active. You will be prompted to enter the root password of the primary unit. After that, the prompt of the primary unit appears. Now initiate the mail insertion and delivery of the copied mail in the input directory:

```
/bin/kill -s SIGUSR2 _
```

For , type in the name of the server, and for , type in the name of the mail gateway service you have configured at the time you [introduced the service on the unit](#).

Note that these names are case sensitive.

This command inserts the imported mails from the input directory to spooling process of the active mail gateway, and performs the delivery. Active mail jobs in the current spooling queue are not affected by this action. In order to verify that the mails have really been inserted, check the mail gateway logs through **Logs > *servername* > *servicename* > mailgw**. For each newly inserted mail, a log file entry, containing the text "SPOOLER new mail inserted (id=#####-#####-#####)", is generated. After that, normal delivery of inserted mails is initiated and can be checked via the operative mail gateway GUI (MailGW).

Step 6. Removing the Obsolete Mails

After successful delivery, remove mails left in the /spool/and /vscan/ directories of the inactive mail gateway on the secondary unit to avoid duplicate delivery. To do so, terminate the SSH session to the primary unit by entering exit. The system prompt of the secondary unit now appears displaying the message: Connection to closed.

Repeat Step 1 if the bash prompt of the secondary unit does not contain the path /var/phion/spool/mgw/_/spool (for example, in case you changed to a different directory).

Now remove all mails in the current directory by using the following command within the /spool/ directory of the secondary unit:

```
rm * -f
```

Using this command permanently removes all files in the current directory. Make sure that you have not changed to another directory before entering `rm * -f`.

If Step 4 was performed, it is also necessary to remove obsolete mails from the `/vscan/` directory.

Step 7. Exit

Enter the command `exit` to terminate the SSH session. This concludes the email synchronicity after HA handover.

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.