Proposal: Allow HostKeyAlias to be used in hostname check against certificate principal.

Charles Duffy charles at dyfis.net
Fri Feb 20 05:37:03 AEDT 2015

- Previous message: [PATCH] Unbreak compilation with --without-ssh1
- Next message: Proposal: Allow HostKeyAlias to be used in hostname check against certificate principal.
- **Messages sorted by:** [date] [thread] [subject] [author]

Howdy --

I have a number of servers with host keys validated by certificates.
These systems are behind a load-balanced frontend, and the
certificates are signed as valid for the DNS name used by that common
frontend address.

This works well for the primary use case of the systems; however, when
wishing to address only a single unit within the pool, the certificate
cannot be used to validate that host's legitimacy, as the individual
address of that host does not match against the name listed in the
principal.

>*From the perspective of the end user, wishing to connect against a*
specific address (as specified in the HostName option), but perform
validation against a user-specified name that differs from that
address seems a legitimate request -- one may also have a situation
where name resolution is not available, for instance, and wish to
connect to a system whose name is known by IP without the situation
posited above.

I'd like to propose that if HostKeyAlias is set, this be used as a
second name against which a certificate may be considered valid,
should it match.

A trivial patch implementing this behavior is attached.

- Previous message: [PATCH] Unbreak compilation with --without-ssh1
- Next message: Proposal: Allow HostKeyAlias to be used in hostname check against certificate principal.
- **Messages sorted by:** [date] [thread] [subject] [author]

More information about the openssh-unix-dev mailing list