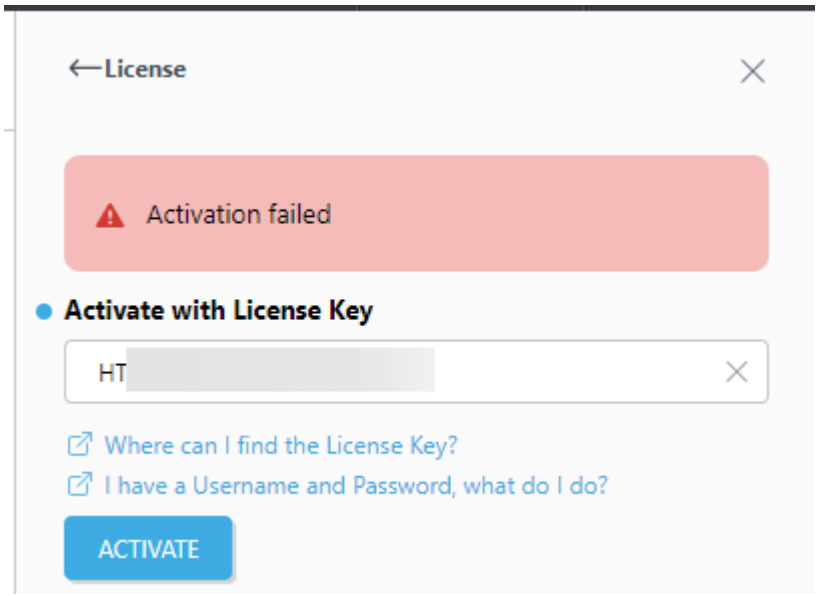
Activation of EFS7 via proxy fails on RHEL6/CentOS6 with SELinux enabled

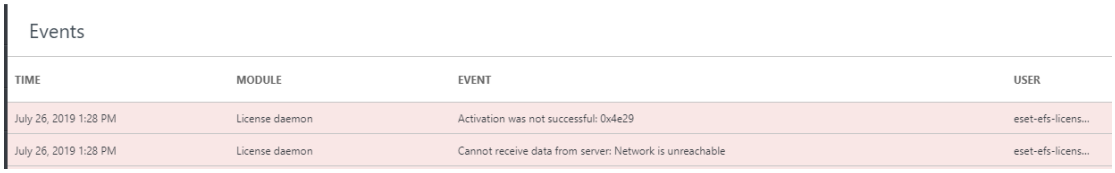
Mitchell | ESET Nederland - 2019-08-08 - Reacties (0) - EFS for Linux

Affected OS: RHEL6, CentOS6

Issue description:

If a proxy is configured and direct connection to the ESET activation servers is not possible (or "Use direct connection if HTTP proxy is not available" is disabled) it is not possible to activate the product.





The following is observed in /var/log/audit/audit.log

cat /var/log/audit/audit.log | grep licensed

```
type=AVC msg=audit(1564140527.218:93): avc: denied { name_connect } for
pid=11892 comm="licensed" dest=3128
scontext=unconfined_u:system_r:eset_efs_licensed_t:s0
tcontext=system_u:object_r:http_cache_port_t:s0 tclass=tcp_socket type=SYSCALL
msg=audit(1564140527.218:93): arch=c000003e syscall=42 success=no exit=-13 a0=d
a1=55d213d12d90 a2=10 a3=10 items=0 ppid=11885 pid=11892 auid=0 uid=498 gid=498
euid=498 suid=498 fsuid=498 egid=498 sgid=498 fsgid=498 tty=(none)
ses=1 comm="licensed" exe="/opt/eset/efs/lib/licensed"
subj=unconfined_u:system_r:eset_efs_licensed_t:s0 key=(null)
```

Cause:

The SELinux policy allows the eset license daemon (/opt/eset/efs/lib/licensed) to connect to the following ports.

allow eset_efs_licensed_t http_port_t : tcp_socket name_connect ;
allow eset_efs_licensed_t squid_port_t : tcp_socket name_connect ;

But, based on the above this allows only connection to:

```
squid_port_t                   tcp      3401, 4827
squid_port_t                   udp      3401, 4827
http_port_t                    tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
```

On RHEL7/CentOS7 based systems the value "squid_port_t" also contains port 3128 and thus this issue does not occur on those systems.

Solution:

```
ausearch -m AVC --comm licensed | audit2allow -M eset_http_cache
semodule -i eset_http_cache.pp
```