

Incident - TLS CERTIFICATE CHANGED

Type d'erreur :



Suite à nos investigations et à l'appel auprès du support Wallix, les erreurs TLS_CERTIFICATE_CHANGED surviennent lorsque le serveur cible renouvelle son certificat de bureau à distance (RDP).

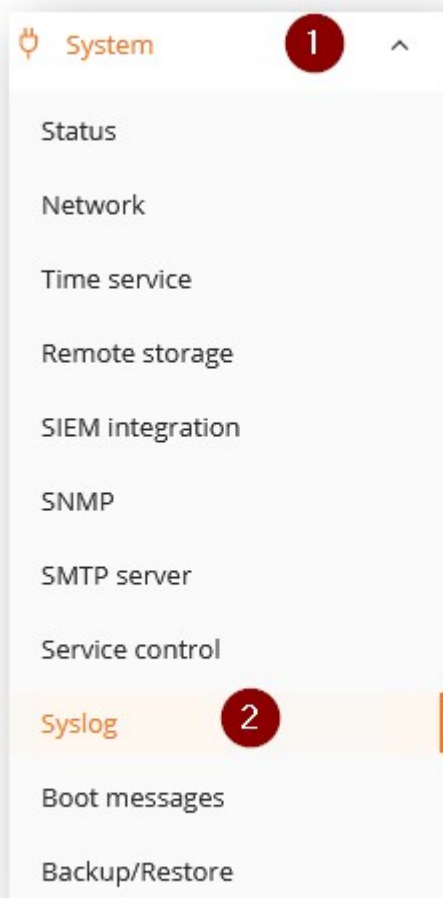
Le bastion ne remplace pas le certificat obsolète existant par le nouveau de la machine cible.

Le renouvellement est possible en supprimant en premier lieu le certificat dans le bastion et se reconnecter au serveur cible depuis l'accès utilisateur pour que le bastion récupère le nouveau certificat.

Il n'y a pas de réplication pour cette partie du certificat RDP pour la machine cible donc l'action de renouvellement du certificat RDP doit être effectuée sur les deux bastions.

Note : Les certificats sont stockés localement sur les bastions à l'emplacement : /var/wab/cert/

La connexion devrait être possible désormais pour les utilisateurs et le message TLS_CERTIFICATE_CHANGED ne devrait plus apparaître.
En complément, les détails de l'erreur apparaissent dans les logs du bastion dans System\Syslog.



Exemple de l'erreur :

```
Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- SSL_get_peer_certificate()
Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- certificate directory is:
'/var/wab/cert/18074c309afb7897005056a2a787'
Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- certificate file is:
'/var/wab/cert/18074c309afb7897005056a2a787/rdp,192.168.12.100,3389,X509.pem'
Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- nb1=1107 nb2=1107
Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- TLS::X509 existing::issuer=CN
= INTER
Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- TLS::X509 existing::subject=CN
= INTER
Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- TLS::X509
```

