Received error from KDC: -1765328318/Certificate mismatch

- Parallels Secure Workspace 5.5.1
- Parallels Secure Workspace 5.6.0

Symptoms

Some users are unable to sign in because SSO credentials can not be created.

In the **awingu-worker-smc.service.log** file, a similar error can be seen:

```
2023-09-27 12:50:25.060193+00:00 awingu-acc
awingu-worker-smc.service[manage.py:2852706]: Using specified cache:
/etc/awingu/domains/SOMEDOMAIN/b60cc05c-df5c-4564-b30b-850a5bff9eb3/kerberos/kerberc
Using principal: someusere\@SOMEDOMAIN.ORG@SOMEDOMAIN.ORG
PA Option X509_user_identity =
FILE:/etc/awingu/domains/SOMEDOMAIN/b60cc05c-df5c-4564-b30b-850a5bff9eb3/certificate
[2915407] 1695819024.671381: Getting initial credentials for
someusere\@SOMEDOMAIN.ORG@SOMEDOMAIN.ORG
[2915407] 1695819024.671383: Sending unauthenticated request
[2915407] 1695819024.671384: Sending request (240 bytes) to SOMEDOMAIN.ORG
[2915407] 1695819024.671385: Resolving hostname AD-01.SOMEDOMAIN.ORG
[2915407] 1695819024.671386: Sending initial UDP request to dgram
10.246.111.251:88
[2915407] 1695819024.671387: Received answer (246 bytes) from dgram
10.246.111.251:88
[2915407] 1695819024.671388: Sending DNS URI query for
_kerberos.SOMEDOMAIN.ORG.
[2915407] 1695819024.671389: No URI records found
[2915407] 1695819024.671390: Sending DNS SRV query for
_kerberos-master._udp.SOMEDOMAIN.ORG.
[2915407] 1695819024.671391: Sending DNS SRV query for
_kerberos-master._tcp.SOMEDOMAIN.ORG.
[2915407] 1695819024.671392: No SRV records found
[2915407] 1695819024.671393: Response was not from master KDC
[2915407] 1695819024.671394: Received error from KDC: -1765328359/Additional
pre-authentication required
[2915407] 1695819024.671397: Preauthenticating using KDC method data
[2915407] 1695819024.671398: Processing preauth types: PA-PK-AS-REQ (16),
PA-PK-AS-REP_OLD (15), PA-ETYPE-INFO2 (19), PA-ENC-TIMESTAMP (2)
[2915407] 1695819024.671399: Selected etype info: etype aes256-cts, salt
"SOMEDOMAIN.ORGsomeusere", params ""
[2915407] 1695819024.671400: PKINIT loading CA certs and CRLs from FILE
[2915407] 1695819024.671401: PKINIT client computed kdc-req-body checksum
9/CCA5CEA6F7BF4177460CAE81752BEAD95FC8CEB1
[2915407] 1695819024.671403: PKINIT client making DH request
[2915407] 1695819025.31886: Preauth module pkinit (16) (real) returned:
0/Success
[2915407] 1695819025.31887: Produced preauth for next request: PA-PK-AS-REQ
(16)
[2915407] 1695819025.31888: Sending request (5308 bytes) to SOMEDOMAIN.ORG
```

```
[2915407] 1695819025.31889: Resolving hostname AD-01.SOMEDOMAIN.ORG
[2915407] 1695819025.31890: Initiating TCP connection to stream
10.246.111.251:88
[2915407] 1695819025.31891: Sending TCP request to stream 10.246.111.251:88
[2915407] 1695819025.31892: Received answer (134 bytes) from stream
10.246.111.251:88
[2915407] 1695819025.31893: Terminating TCP connection to stream
10.246.111.251:88
[2915407] 1695819025.31894: Sending DNS URI query for
_kerberos.SOMEDOMAIN.ORG.
[2915407] 1695819025.31895: No URI records found
[2915407] 1695819025.31896: Sending DNS SRV query for
_kerberos-master._udp.SOMEDOMAIN.ORG.
[2915407] 1695819025.31897: Sending DNS SRV query for
_kerberos-master._tcp.SOMEDOMAIN.ORG.
[2915407] 1695819025.31898: No SRV records found
[2915407] 1695819025.31899: Response was not from master KDC
[2915407] 1695819025.31900: Received error from KDC: -1765328318/Certificate
mismatch
[2915407] 1695819025.31901: Retrying AS request with master KDC
[2915407] 1695819025.31902: Getting initial credentials for
someusere\@SOMEDOMAIN.ORG@SOMEDOMAIN.ORG
[2915407] 1695819025.31904: Sending unauthenticated request
[2915407] 1695819025.31905: Sending request (240 bytes) to SOMEDOMAIN.ORG
(master)
[2915407] 1695819025.31906: Sending DNS URI query for
_kerberos.SOMEDOMAIN.ORG.
[2915407] 1695819025.31907: No URI records found
[2915407] 1695819025.31908: Sending DNS SRV query for
_kerberos-master._udp.SOMEDOMAIN.ORG.
[2915407] 1695819025.31909: Sending DNS SRV query for
_kerberos-master._tcp.SOMEDOMAIN.ORG.
[2915407] 1695819025.31910: No SRV records found
kinit: Certificate mismatch while getting initial credentials
```

In the Windows Event Viewer of the domain controller(s), a similar error to the one below can be seen:

The Key Distribution Center (KDC) encountered a user certificate that was valid but contained a different SID than the user to which it mapped. As a result, the request involving the certificate failed.
See https://go.microsoft.com/fwlink/?linkid=2189925 to learn more.

Cause

Since version 5.5.1, the Single Sign-On (SSO) mechanism has been made more secure to comply with the increased security standards enforced by Microsoft. Therefore, user certificates now also contain the objectSid of the user account.

The objectSid is cached in Parallels Secure Workspace upon first sign-in.

However, when a user account uses the same sAMAccountName as a previous user account; Parallels Secure Workspace will consider this to be the same user and will not automatically update the objectSid. This is done by design, as a security measure (TOFU - Trust on first use) to avoid spoofing.

Resolution

Option 1 (requires version 5.6 or higher)

The version of Parallels Secure Workspace must at least be 5.6.

Then, the objectSid can be reset by deleting the user from **System Settings > Manage > Users.**

For subscriptions, this means the user will only be marked for deletion. When the user signs in again, the new objectSid will be accepted.

Option 2 (also works for version 5.5)

If the Recycle bin of the Active Directory is enabled, it may be possible to restore the account with the original objectSid instead.

In this case:

1. Delete the new user with the same sAMAccountName as a previous user.
2. Restore the original user with the original objectSid from the Recycle bin instead.

More info: https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/retore-deleted-accounts-and-groups-in-ad .
