Preauth module pkinit (17) (real) returned: -1765328314/Failed to verify received certificate (depth 0): unable to get local issuer certificate

- Parallels Secure Workspace

Symptoms

First, see How to analyze the log files to identify single-sign on (SSO) issues .

Single sign-on fails. In **awingu-worker-smc.service.log**, a similar error can be seen:

```
2022-03-17 11:37:06.090662 HOST19124
awingu-worker-smc.service[manage.py:16443]: Using specified cache:
/etc/awingu/DOMAINS/WORKSPACEDOMAIN/ff65192e-57d0-44ab-bb87-88f361d89a44/kerberos/ke
Using principal: someuser\@somedomain.org@SOMEDOMAIN.ORG
PA Option X509_user_identity =
FILE:/etc/awingu/DOMAINS/WORKSPACEDOMAIN/ff65192e-57d0-44ab-bb87-88f361d89a44/certif
[20063] 1647517011.9606: Getting initial credentials for
someuser\@somedomain.org@SOMEDOMAIN.ORG
[20063] 1647517011.9608: Sending unauthenticated request
[20063] 1647517011.9609: Sending request (245 bytes) to SOMEDOMAIN.ORG
[20063] 1647517011.9610: Resolving hostname SOMEHOST.somedomain.org
[20063] 1647517011.9611: Sending initial UDP request to dgram 10.1.2.3:88
[20063] 1647517011.9612: Received answer (232 bytes) from dgram 10.1.2.3:88
[20063] 1647517011.9613: Sending DNS URI query for _kerberos.SOMEDOMAIN.ORG.
[20063] 1647517011.9614: No URI records found
[20063] 1647517011.9615: Sending DNS SRV query for
_kerberos-master._udp.SOMEDOMAIN.ORG.
[20063] 1647517011.9616: SRV answer: 0 100 88 "somehost.somedomain.org."
[20063] 1647517011.9617: Sending DNS SRV query for
_kerberos-master._tcp.SOMEDOMAIN.ORG.
[20063] 1647517011.9618: SRV answer: 0 0 88 "somehost.somedomain.org."
[20063] 1647517011.9619: Response was not from master KDC
[20063] 1647517011.9620: Received error from KDC: -1765328359/Additional
pre-authentication required
[20063] 1647517011.9623: Preauthenticating using KDC method data
[20063] 1647517011.9624: Processing preauth types: PA-PK-AS-REQ (16),
PA-PK-AS-REP_OLD (15), PA-ETYPE-INFO2 (19), PA-ENC-TIMESTAMP (2)
[20063] 1647517011.9625: Selected etype info: etype aes256-cts, salt
"SOMEDOMAIN.ORGsomeuser", params ""
[20063] 1647517011.9626: PKINIT loading CA certs and CRLs from FILE
[20063] 1647517011.9627: PKINIT client computed kdc-req-body checksum
9/53D75BED49E4B9D134A097FB4C9306DDAAA2B7DD
[20063] 1647517011.9629: PKINIT client making DH request
[20063] 1647517011.9630: Preauth module pkinit (16) (real) returned:
0/Success
[20063] 1647517011.9631: Produced preauth for next request: PA-PK-AS-REQ (16)
[20063] 1647517011.9632: Sending request (4991 bytes) to SOMEDOMAIN.ORG
[20063] 1647517011.9633: Resolving hostname SOMEHOST.somedomain.org
```

```
[20063] 1647517011.9634: Initiating TCP connection to stream 10.1.2.3:88
[20063] 1647517011.9635: Sending TCP request to stream 10.1.2.3:88
[20063] 1647517021.76416: Sending initial UDP request to dgram 10.1.2.3:88
[20063] 1647517024.77836: Sending retry UDP request to dgram 10.1.2.3:88
[20063] 1647517026.85287: Received answer (4778 bytes) from stream
10.1.2.3:88
[20063] 1647517026.85288: Terminating TCP connection to stream 10.1.2.3:88
[20063] 1647517026.85289: Sending DNS URI query for _kerberos.SOMEDOMAIN.ORG.
[20063] 1647517026.85290: No URI records found
[20063] 1647517026.85291: Sending DNS SRV query for
_kerberos-master._udp.SOMEDOMAIN.ORG.
[20063] 1647517026.85292: SRV answer: 0 100 88 "somehost.somedomain.org."
[20063] 1647517026.85293: Sending DNS SRV query for
_kerberos-master._tcp.SOMEDOMAIN.ORG.
[20063] 1647517026.85294: SRV answer: 0 0 88 "somehost.somedomain.org."
[20063] 1647517026.85295: Response was not from master KDC
[20063] 1647517026.85296: Processing preauth types: PA-PK-AS-REP (17)
[20063] 1647517026.85297: PKINIT OpenSSL error: Failed to verify received
certificate (depth 0): unable to get local issuer certificate
[20063] 1647517026.85298: PKINIT client could not verify DH reply
[20063] 1647517026.85299: Preauth module pkinit (17) (real) returned:
-1765328314/Failed to verify received certificate (depth 0): unable to get
local issuer certificate
[20063] 1647517026.85300: Produced preauth for next request: (empty)
[20063] 1647517026.85301: Getting AS key, salt "SOMEDOMAIN.ORGsomeuser",
params ""
kinit: Cannot read password while getting initial credentials
```

Cause

The Parallels Secure Workspace appliance does not trust the certificate (or one of the certificates in its certification path) presented by the Kerberos Domain Controller.

Resolution

The error is most likely on the Parallels Secure Workspace side. Parallels Secure Workspace that can not verify the certificate presented by the KDC.
Check whether the root CA (and any intermediate CA certificates) of the KDC are (also) included in the Trusted Roots file of the Workspace.

Make sure to include all certificates (intermediate and root) in the certification path of the Workspace subCA certificate; as well as for each of the certificates presented by the Kerberos Domain Controllers.
