KDC_ERR_PREAUTH_REQUIRED

Was bedeutet diese Fehlermeldung „KDC_ERR_PREAUTH_REQUIRED"?

Der KDC erwartet grundsätzlich das sich alle Konten vorauthentifizieren (Pre-Authentication oder Präauthentifizierung), das ist Standard.

*Der Authentifizierungsserver setzt die Pre-Authentication ein, um sicherzustellen, dass der Principal (Benutzer oder System) der ist für den er sich ausgibt.

(Warum soll der AS die Tür öffnen, wenn sich jemand mit der Klingel vertan hat) 😉

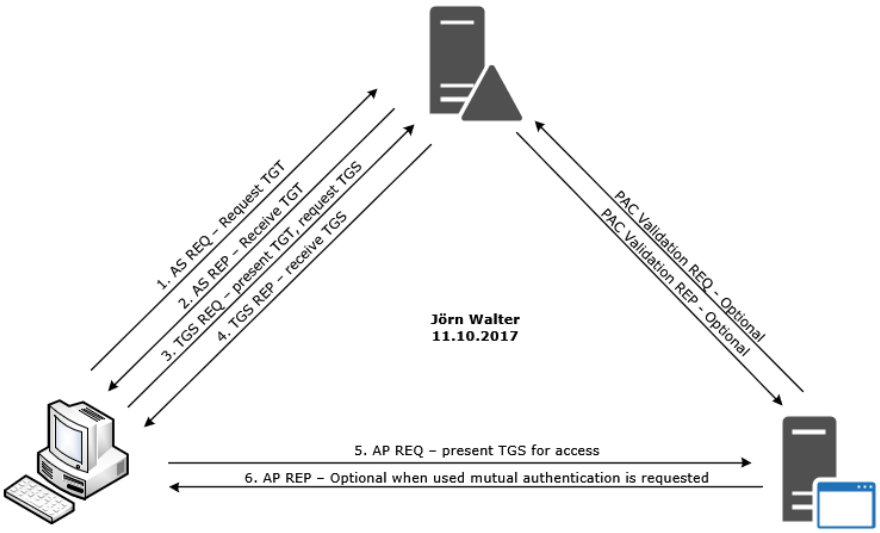
Dieser Mechanismus dient als Schutz vor böswilligen Angreifern, wobei im Verlauf (AS-Request) der Zeitstempel mit dem Benutzer-Password-Hash (LTK) verschlüsselt wird. Der KDC empfängt den Request, entschlüsselt diesen mit Benutzer-Password-Hash, und prüft daraufhin zuerst den Zeitstempel. Ist der Zeitstempel valide verarbeitet er den aktuellen Request mit weiteren Prüfmechanismen (Authenticator/Replay-Attacken) und sendet erst jetzt das TGT. (Erst gucken wer da ist, bevor man auf macht)

Im Active Directory ist diese Option auch standardmäßig auf allen Konten aktiviert, so dass eine Pre-Authentication stattfinden könnte.

Wenn auf der einen Seite etwas erwartet wird und auf der anderen Seite nicht geliefert wird/werden kann, so löst diese Aktion ein Event „KDC_ERR_PREAUTH_REQUIRED„ aus.

Bei Problemen kann sollte aber bitte nicht, die Pre-Authentication deaktiviert werden. Das erhöht zwar zum einen die Kompatibilität für diverse Authentifizierungsvorgänge (DES/3DES/AES) aber es wird auch kein Event mehr dazu geschrieben.

*Die Pre-Authentication läuft zwischen Schritt 1 und 2 des Diagramms.



1. AS Request – Request TGT = Der Client übermittelt seinen Benutzernamen in Klartext, die gewünschte Ticketlebensdauer, den Dienstnamen und eine Zufallszahl (Nonce)

2. Der AS antwortet mit einer AS REP Nachricht die unteranderem das TGT enthält. Dieses ist mit dem Master Secret des KDCs verschlüsselt, von dem der AS und TGS ein Teil sind. Das TGT enthält dem Benutzernamen, die Adresse, den Sitzungsschlüssel, die Gültigkeitsdauer, den Zeitstempel usw. und ist vom Client nicht einsehbar. Weiter enthält die Nachricht noch den Session-Key (User-KDC), die Nonce, den Namen, den Zeitstempel des KDCs und die TGT Länge. Diese Informationen sind ebenfalls mit dem Master Secret (User) vom Client verschlüsselt.

3. Das erhaltene TGT sendet der Client nun mit der Nachricht TGS REQ zum TGS. Diese Nachricht enthält nicht nur das TGT sondern auch den Namen der Ressource auf die zugegriffen werden soll, die Lebensdauer sowie eine Authenticator (nur einmal Gültig), der mit dem Sitzungsschlüssel verschlüsselt wurde. Der Authenticator enthält den Namen des Clients sowie einen Zeitstempel. Der Server gleicht nun die Zeitstempel ab (5 Minuten), prüft obb die Systemzeiten übereinstimmen.

4. Der TGS antwortet mit der Nachricht TGS REP, die das Ticket auf die Ressource enthält sowie den Namen des Client, die Netzwerkadresse des Clients, den Session-Key (User-Ressource), die Lebensdauer, den Zeitstempel, und den Servernamen. Verschlüsselt ist das Ticket mit dem Master Secret der Ressource. Geliefert wird auch noch der Session-Key (User-Ressource), Name der Ressource, die Ticket Lebensdauer, Zeitstempel des KDC oder auch eine Zufallszahl. Alles verschlüsselt mit dem Session-Key (Alice-KDC).

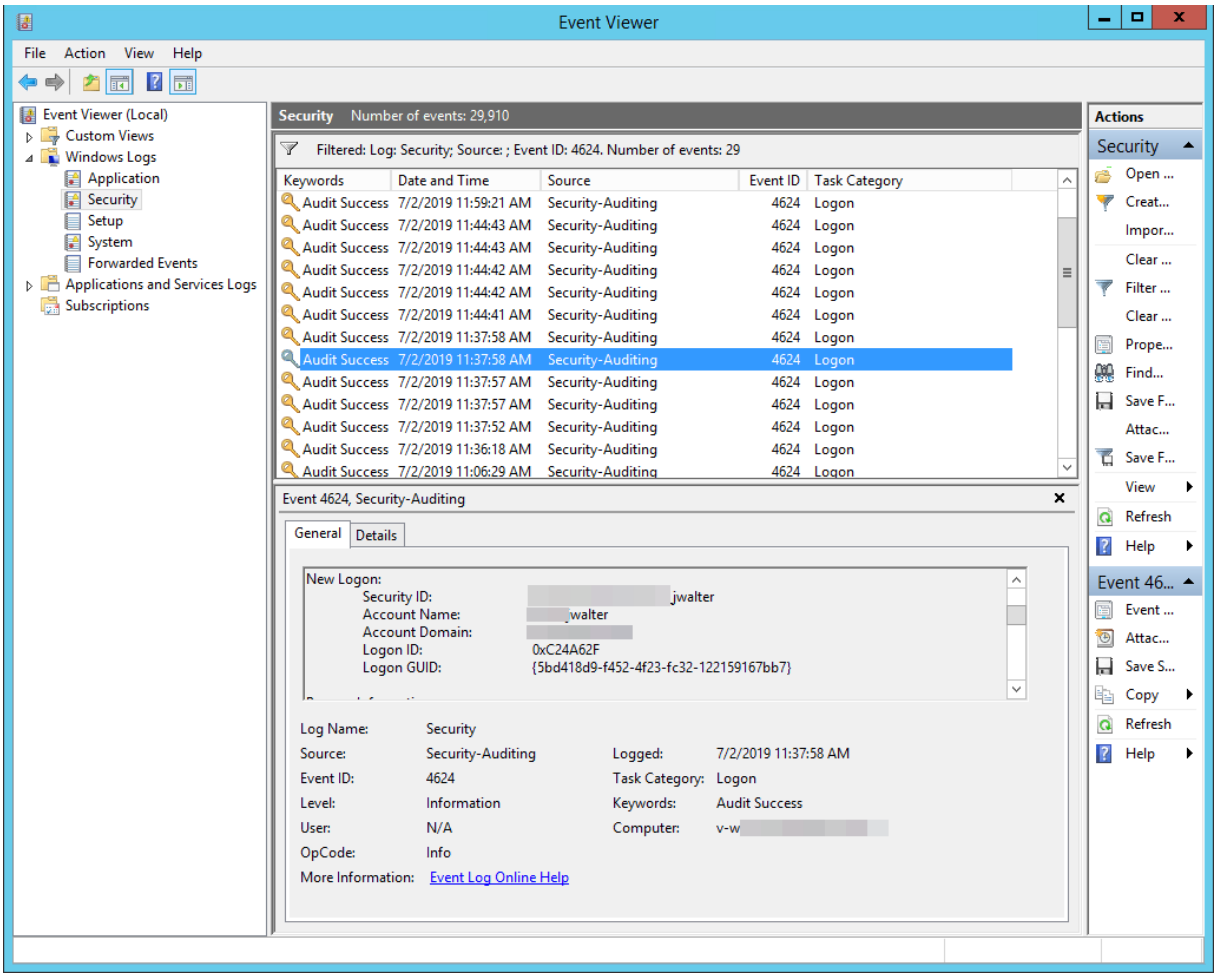
5. Jetzt hat der Client alle Informationen zusammen um auf die Ressource zugreifen zu können. Mit dem AP REQ sendet der Client der Ressource das TGT vom TGS zu sowie den Authenticator, der mit dem Session-Key verschlüsselt wurde.

6. Die weitere Kommunikation erfolgt mit AP REP, der ungeschützte Austausch von Anwendungsdaten.

Hier ein komplettes Beispiel als Vorgang:

KDC_ERR_PREAUTH_REQUIRED

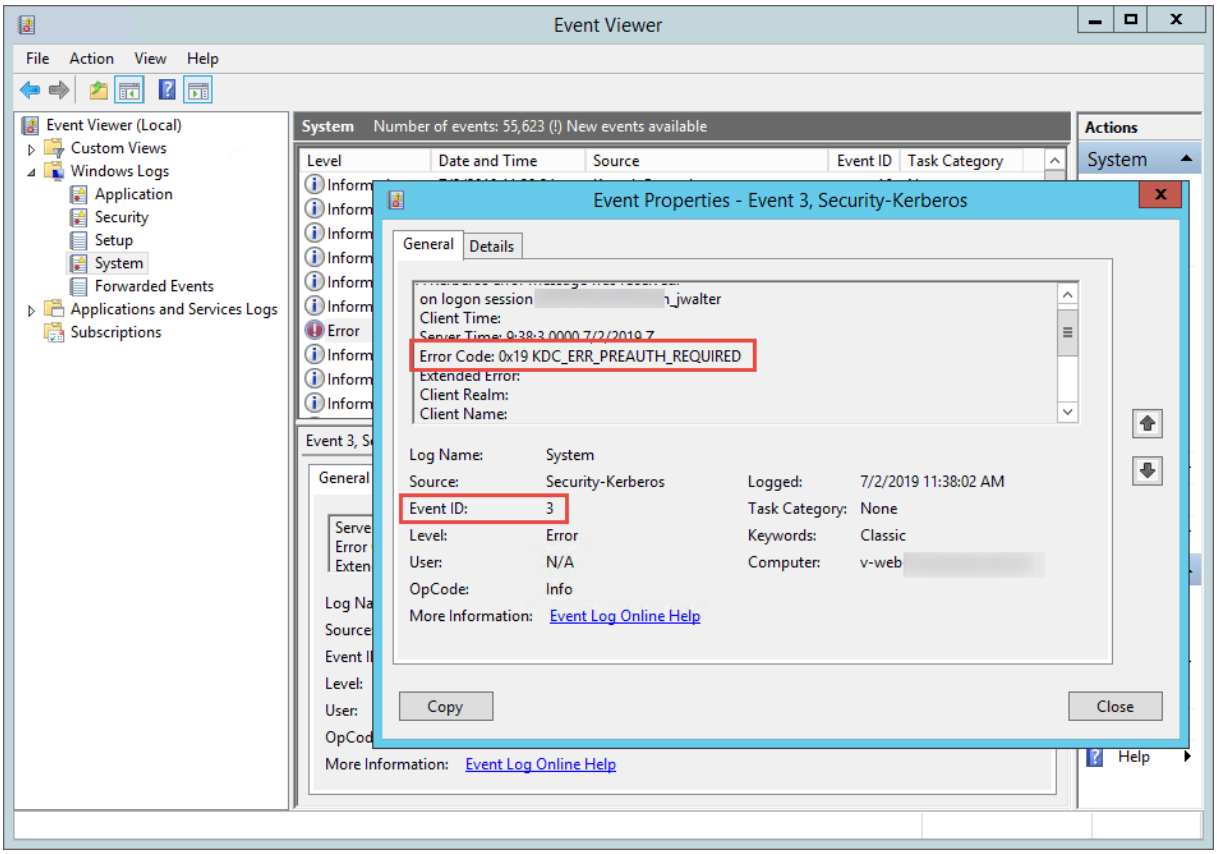
Es ist 11:37:58 Uhr - Logon auf Server



KDC_ERR_PREAUTH_REQUIRED

Bei eingeschaltetem Kerberos Logging wird mir das Event mit der ID 3 unter Windows Logs > System angezeigt. Wie vorher bereits erwähnt, erwartet Kerberos eine Pre-Authentication.

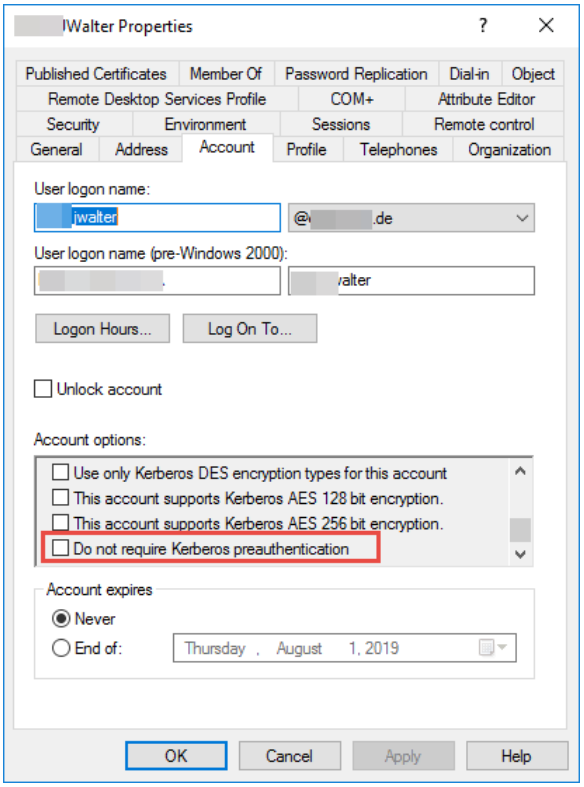
Es ist 11:38:02 Uhr.

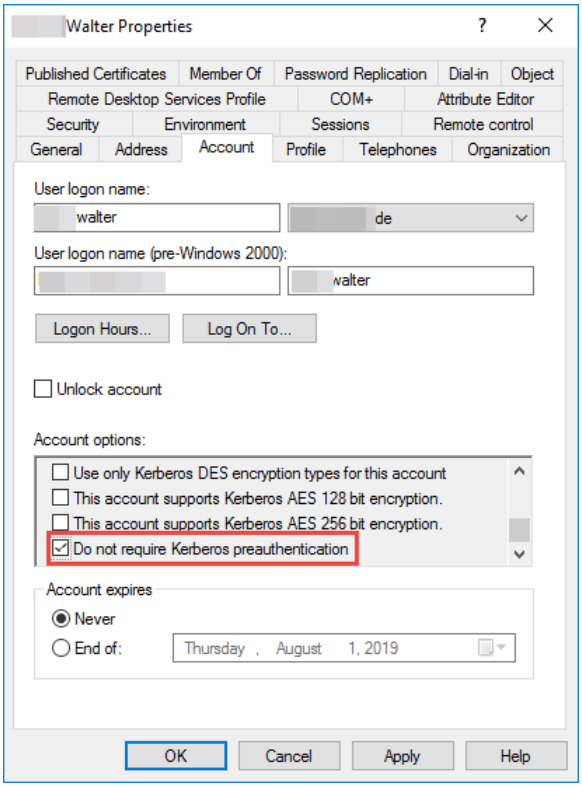


KDC_ERR_PREAUTH_REQUIRED

Jetzt stelle ich mein Konto so ein, dass keine Notwendigkeit für ein Pre-Authentication besteht (rechtes Bild).

Es ist 11:40 Uhr.

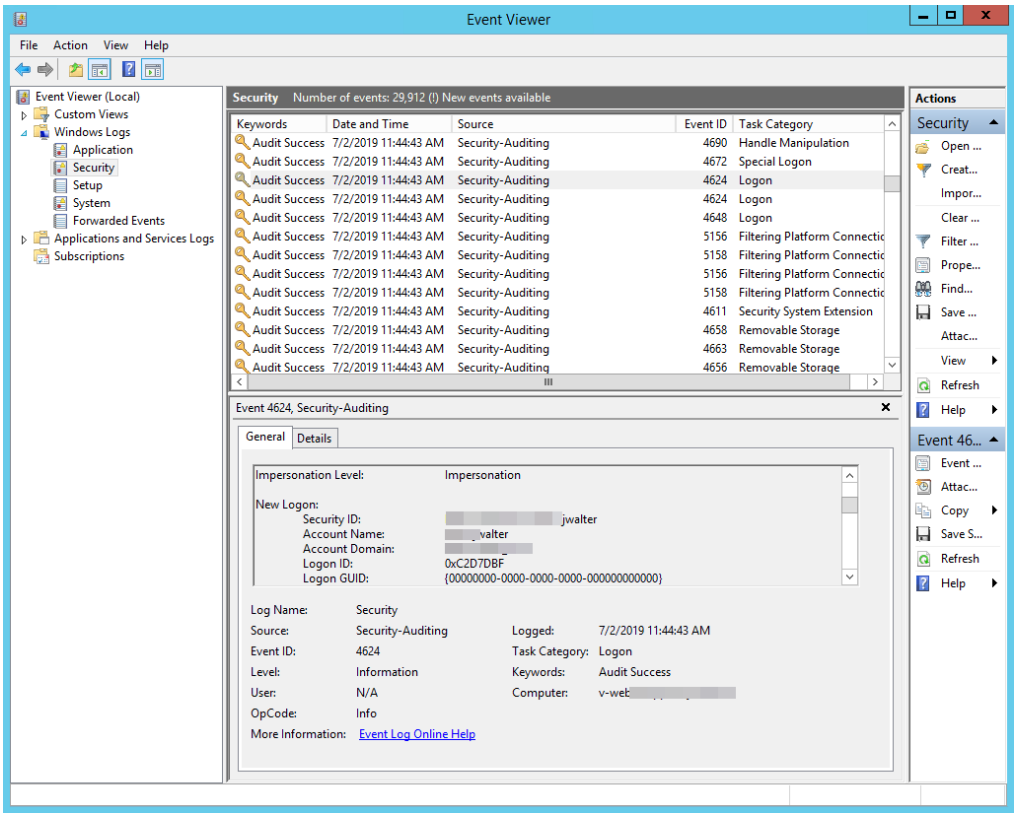




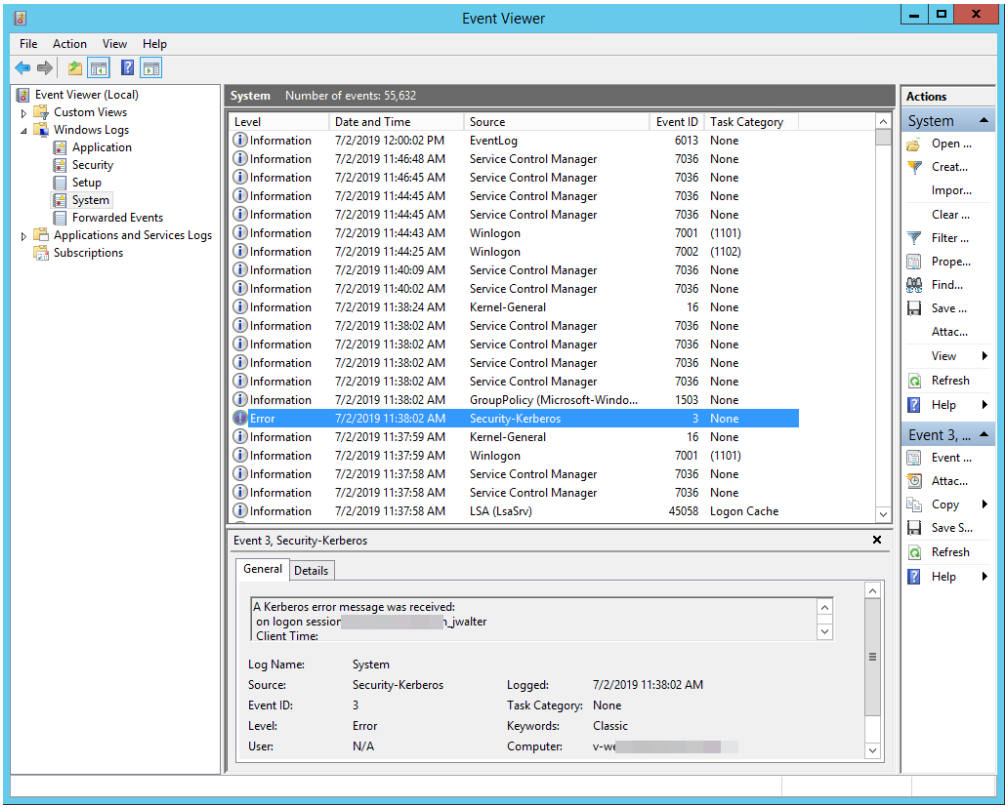
KDC_ERR_PREAUTH_REQUIRED

Zum Vergleich melde ich mich auf den gleichen Server wieder an und schaue ins Log.

Es ist 11:44:43 Uhr – Logon auf Server

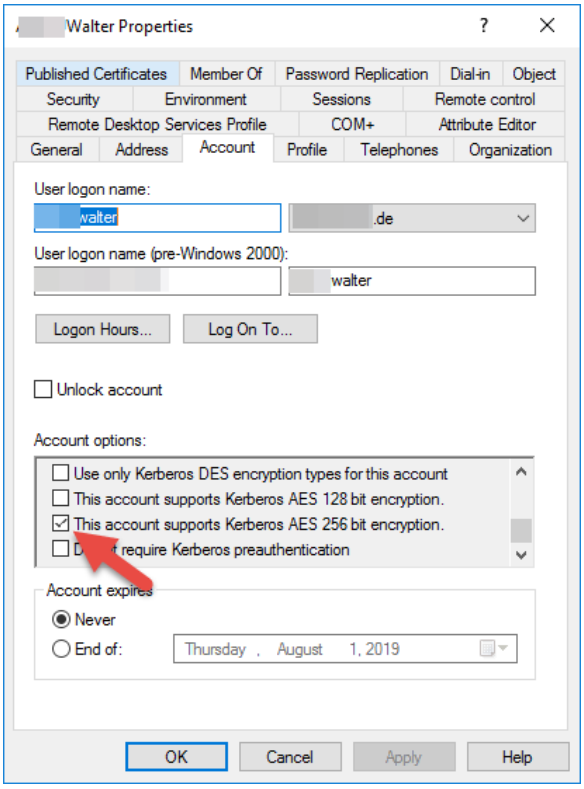


Es erscheint kein Event mehr mit der ID 3 nach 11:38:02 Uhr.

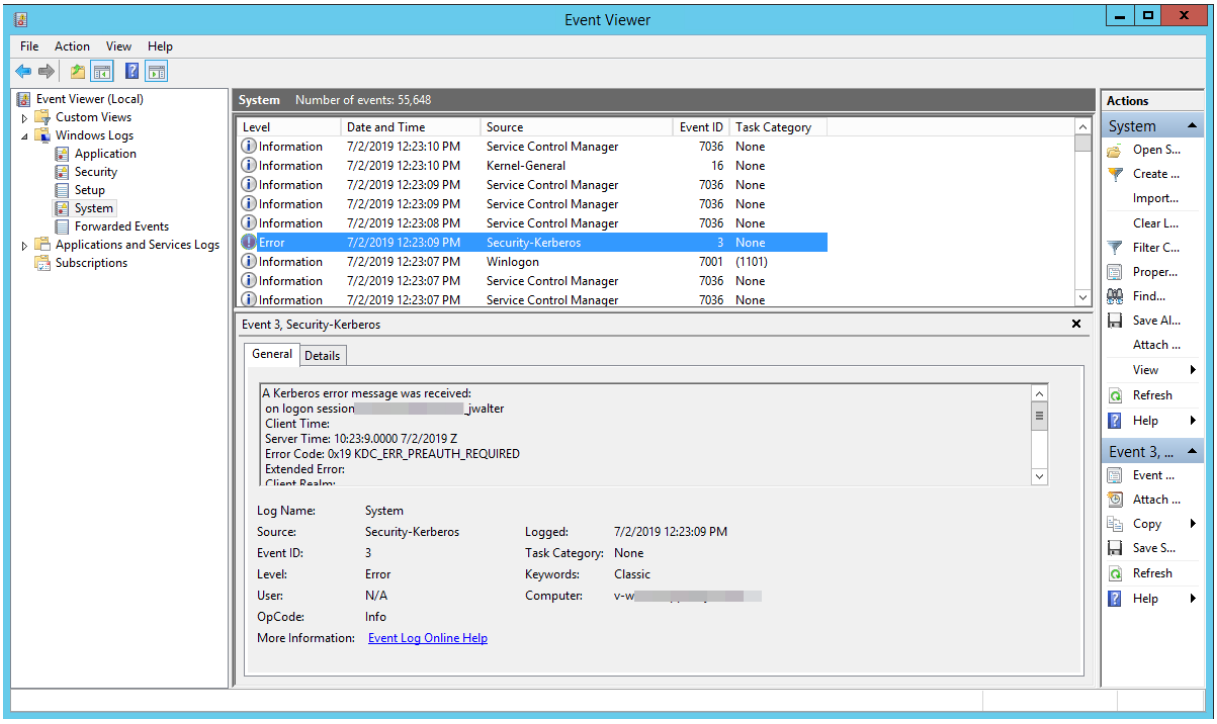


KDC_ERR_PREAUTH_REQUIRED

Jetzt stelle ich mein Konto so ein, das ich ausdrücklich eine Kerberos-AES-256-Bit Verschlüsselung präferiere.

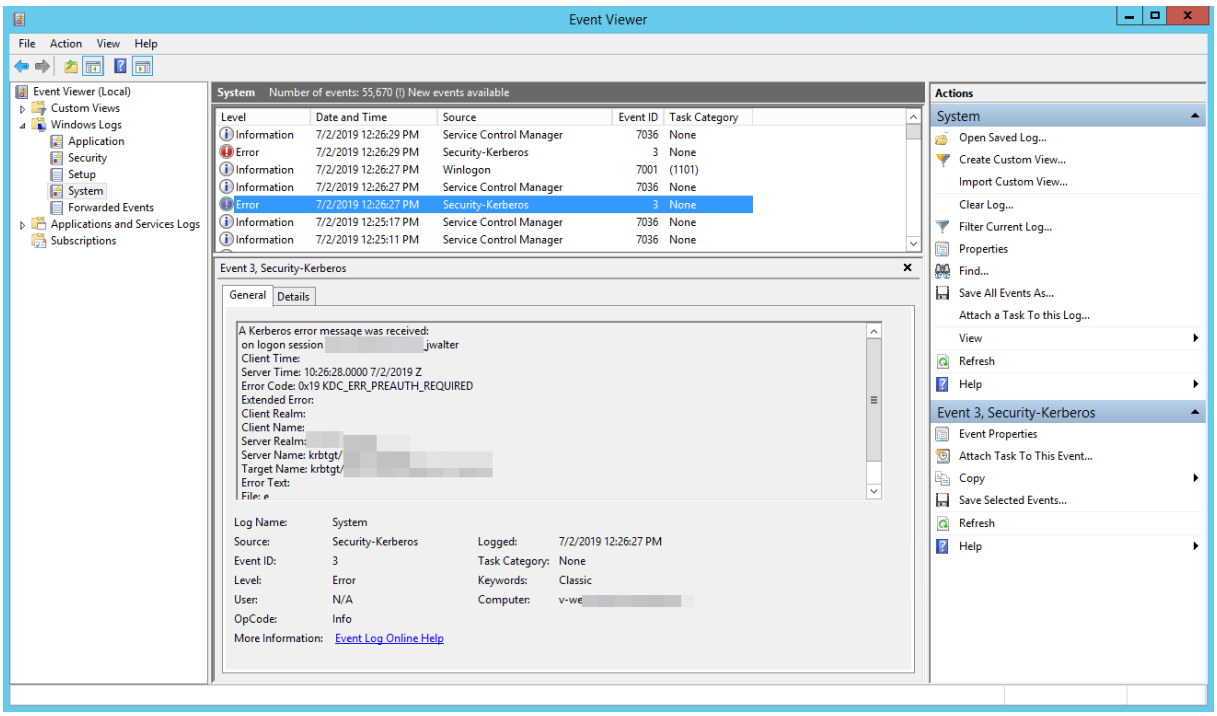


Die Fehlermeldung mit der Event ID 3 erscheint wieder.

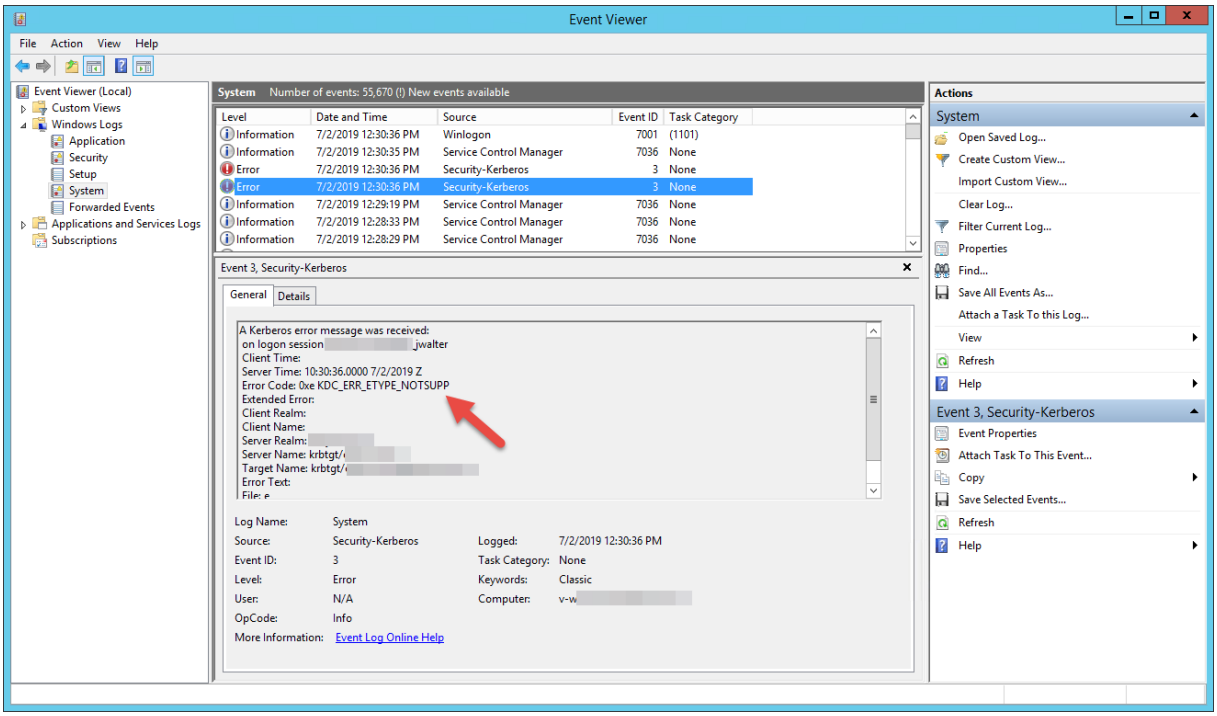


KDC_ERR_PREAUTH_REQUIRED

Das gleiche teste ich nun mit einer Kerberos-AES-128-Bit Verschlüsselung, gleicher Fehlercode.



Und nun mit einer Kerberos-DES Verschlüsselung, gleicher Fehlercode aber NOTSUPP. Das war zu erwarten, weil die DES-Verschlüsselung untersagt ist.



Hinweis: Bei einer fehlgeschlagenen Authentifizierung wäre der Fehlercode KDC_ERR_PREAUTH_FAILED.

KDC_ERR_PREAUTH_REQUIRED

Fazit:

Die Fehlermeldung kann insoweit ignoriert werden, weil man technisch davon ausgehen kann, dass die Authentifizierungsvorgänge funktionieren.

Auch wenn keine sensiblen Daten während der Pre-Authentication übermittelt werden, so sollte der Grund für die Fehlermeldung trotzdem ermittelt werden.

Ist die Pre-Authentication eingeschaltet, so wird das Paket (TGT-Anforderung) mit dem privaten Schlüssel des Anforderers verschlüsselt.

Microsoft schreibt dazu das es sich hierbei um ein false>positve Error handeln kann.

Optional:

NETLOGON LOG ERROR CODE	DESCRIPTION
0x0	Successful login
0xC0000064	The specified user does not exist
0xC000006A	The value provided as the current password is not correct
0xC000006C	Password policy not met
0xC000006D	The attempted logon is invalid due to a bad user name
0xC000006E	User account restriction has prevented successful login
0xC000006F	The user account has time restrictions and may not be logged onto at this time
0xC0000070	The user is restricted and may not log on from the source workstation
0xC0000071	The user account's password has expired
0xC0000072	The user account is currently disabled

0xC000009A	Insufficient system resources
0xC0000193	The user's account has expired
0xC0000224	User must change his password before he logs on the first time
0xC0000234	The user account has been automatically locked

LOGON EVENT ID	DESCRIPTION
528	A user successfully logged on to a computer. For information about the type of logon, see the Logon Types table below.
529	Logon failure. A logon attempt was made with an unknown user name or a known user name with a bad password.
530	Logon failure. A logon attempt was made, but the user account tried to log on outside of the allowed time.
531	Logon failure. A logon attempt was made using a disabled account.
532	Logon failure. A logon attempt was made using an expired account.
533	Logon failure. A logon attempt was made by a user who is not allowed to log on at this computer.
534	Logon failure. The user attempted to log on with a type that is not allowed.
535	Logon failure. The password for the specified account has expired.
536	Logon failure. The Netlogon service is not active.

537	Logon failure. The logon attempt failed for other reasons. *Note: In some cases, the reason for the logon failure may not be known.*
538	The logoff process was completed for a user.
539	Logon failure. The account was locked out at the time the logon attempt was made.
540	A user successfully logged on to a network.
541	Main mode Internet Key Exchange (IKE) authentication was completed between the local computer and the listed peer identity (establishing a security association), or quick mode has established a data channel.
542	A data channel was terminated.
543	Main mode was terminated. *Note: This might occur as a result of the time limit on the security association expiring, policy changes, or peer termination. (The default expiration time for security associations is eight hours.)*
544	Main mode authentication failed because the peer did not provide a valid certificate or the signature was not validated.
545	Main mode authentication failed because of a Kerberos failure or a password that is not valid.
546	IKE security association establishment failed because the peer sent a proposal that is not valid. A packet was received that contained data that is not valid.
547	A failure occurred during an IKE handshake.
548	Logon failure. The security identifier (SID) from a trusted domain does not match the account domain SID of the client.

549	Logon failure. All SIDs that correspond to untrusted namespaces were filtered out during an authentication across forests.
550	A denial-of-service attack may have taken place.
551	A user initiated the logoff process.
552	A user successfully logged on to a computer using explicit credentials while already logged on as a different user.
672	An authentication service (AS) ticket was successfully issued and validated.
673	A ticket-granting service (TGS) ticket was granted.
674	A security principal renewed an AS ticket or TGS ticket.
675	Preauthentication failed. This event is generated on a Key Distribution Center (KDC) when a user types in an incorrect password.
676	Authentication ticket request failed. This event is not generated in Windows XP or in the Windows Server 2003 family.
677	A TGS ticket was not granted. This event is not generated in Windows XP or in the Windows Server 2003 family.
678	An account was successfully mapped to a domain account.
681	Logon failure. A domain account logon was attempted. This event is not generated in Windows XP or in the Windows Server 2003 family.
682	A user has reconnected to a disconnected terminal server session.
683	A user disconnected a terminal server session without logging off. *Note: This event is generated when a user is connected to a terminal server session over the network. It appears on the terminal server.*

KDC_ERR_PREAUTH_REQUIRED

Event ID Field	Comments
Event Type, Source,Category,ID,Date,and Time	self-explanatory
User	The user account performing the logon. For example, this might be NT AUTHORITYSYSTEM,which is the LocalSystem account used to start many Windows 2000 services.
Computer	The computer on which the event occurred
Reason	Applies to logon failures only; it's the reason the account failed to log on.
User Name	The name of the user account attempting to log on
Domain	The domain of the user account attempting to log on.
Logon Type	A numeric value indicating the type of logon attempted. Possible values are: 2 – Interactive (interactively logged on) 3 – Network (accessed system via network) 4 – Batch (started as a batch job) 5 – Service (a Windows service started by service controller) 6 – Proxy (proxy logon; not used in Windows NT or Windows 2000) 7 – Unlock (unlock workstation) 8 – NetworkCleartext (network logon with cleartext credentials) 9 – NewCredentials (used by RunAs when the /netonly option is used)
Logon Process	The process performing the logon. The following are some example logon processes: – Advapi (triggered by a call to LogonUser; LogonUser calls LsaLogonUser, and one of the arguments to LsaLogonUser, OriginName, identifies the origin of the logon attempt)

	– User32 (normal Windows 2000 logon using WinLogon) – SCMgr (Service Control Manager started a service) – KsecDD (network connections to the SMB server-for example, when you use a NET USE command) – Kerberos (the Kerberos Security Support Provider [SSP]) – NtlmSsp (the NTLM SSP) – Seclogon (Secondary Logon-that is, the RunAs command) – IIS (IIS performed the logon; generated when logging on the IUSR_machinename account or when using Digest or Basic authentication)
Authentication Package	The security package called to attempt to log on the account. An authentication package is a dynamic-link library (DLL) that analyzes logon data and determines whether to authenticate an account. Most common examples are Kerberos, Negotiate, NTLM, and MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 (also called MSV1_0; authenticates users in the SAM database, supports pass-through authentication to accounts in trusted domains, and supports subauthentication packages) Workstation Name Workstation name, if known, used by the principal during logon.

KERBEROS ERROR NUMBER	KERBEROS ERROR CODE	DESCRIPTION
0x3	KDC_ERR_BAD_PVNO	Requested protocol version number not supported.
0x6	KDC_ERR_C_PRINCIPAL_UNKNOWN	Client not found in Kerberos database.
0x7	KDC_ERR_S_PRINCIPAL_UNKNOWN	Server not found in Kerberos database.

0x8	KDC_ERR_PRINCIPAL_NOT_UNIQUE	Multiple principal entries in database.
0xA	KDC_ERR_CANNOT_POSTDATE	Ticket not eligible for postdating.
0xB	KDC_ERR_NEVER_VALID	Requested start time is later than end time.
0xC	KDC_ERR_POLICY	KDC policy rejects request.
0xD	KDC_ERR_BADOPTION	KDC cannot accommodate requested option.
0xE	KDC_ERR_ETYPE_NOSUPP	KDC has no support for encryption type.
0xF	KDC_ERR_SUMTYPE_NOSUPP	KDC has no support for checksum type.
0x10	KDC_ERR_PADATA_TYPE_NOSUPP	KDC has no support for pre-authentication data type.
0x12	KDC_ERR_CLIENT_REVOKED	Client's credentials have been revoked.
0x17	KDC_ERR_KEY_EXPIRED	Password has expired – change password to reset.
0x18	KDC_ERR_PREAUTH_FAILED	Pre-authentication information was invalid.
0x19	KDC_ERR_PREAUTH_REQUIRED	Additional pre-authentication required.

0x1B	KDC_ERR_MUST_USE_USER2USER	Server principal valid for user-to-user only.
0x1C	KDC_ERR_PATH_NOT_ACCPETED	KDC Policy rejects transited path.
0x1D	KDC_ERR_SVC_UNAVAILABLE	A service is not available.
0x1F	KRB_AP_ERR_BAD_INTEGRITY	Integrity check on decrypted field failed.
0x20	KRB_AP_ERR_TKT_EXPIRED	Ticket expired.
0x21	KRB_AP_ERR_TKT_NYV	Ticket not yet valid.
0x22	KRB_AP_ERR_REPEAT	Request is a replay.
0x23	KRB_AP_ERR_NOT_US	The ticket isn't for us.
0x24	KRB_AP_ERR_BADMATCH	Ticket and authenticator do not match.
0x25	KRB_AP_ERR_SKEW	Clock skew too great.
0x28	KRB_AP_ERR_MSG_TYPE	Invalid message type.
0x29	KRB_AP_ERR_MODIFIED	Message stream modified.
0x34	KRB_ERR_RESPONSE_TOO_BIG	Response too big for UDP, retry with TCP.
0x3C	KRB_ERR_GENERIC	Generic error (description in e-text).

0x44	KDC_ERR_WRONG_REALM	User-to-user TGT issued different KDC.