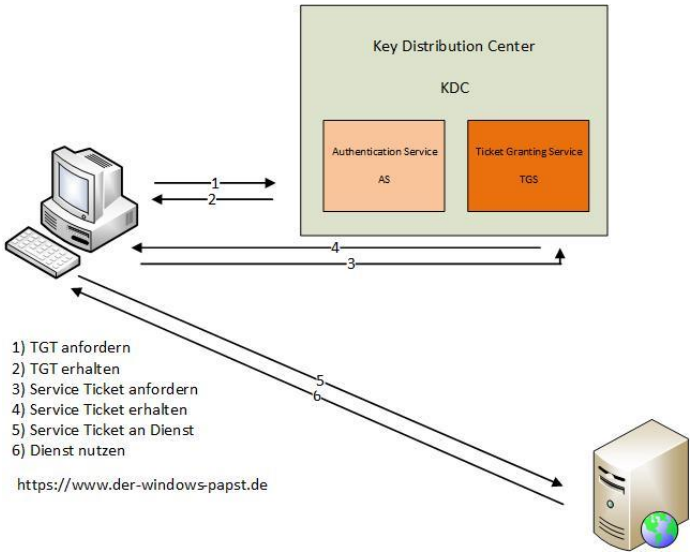
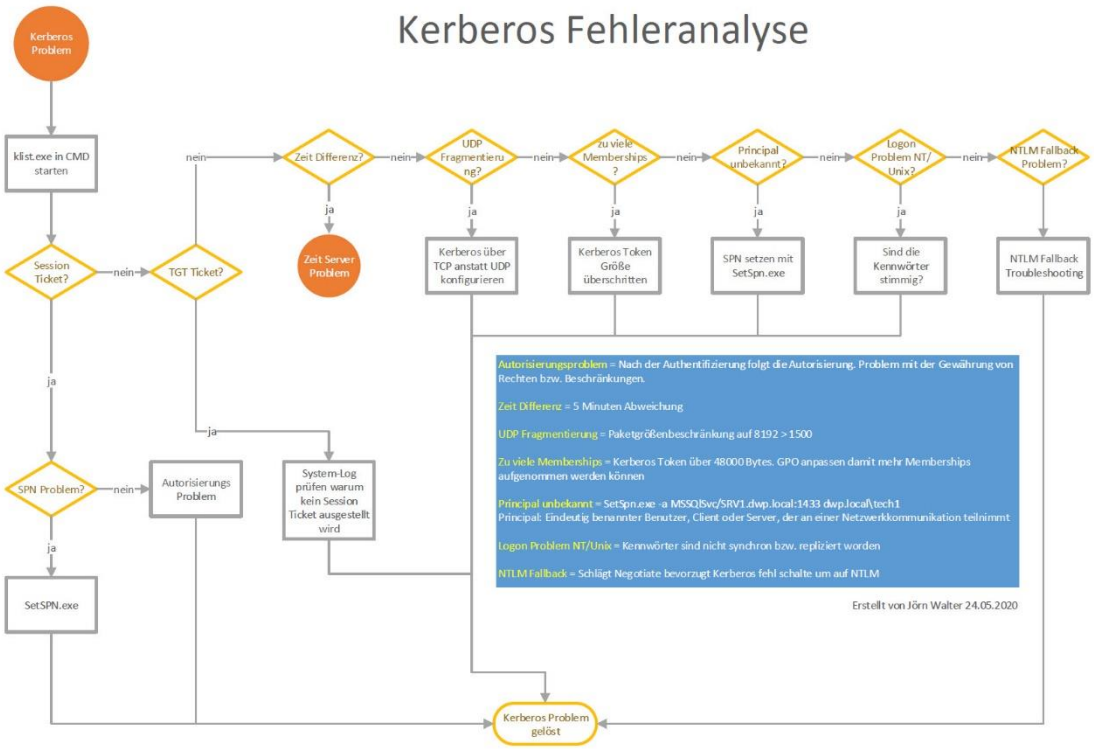
Authentication Auditing

Der einfache Ablauf einer Ticket-Granting-Ticket Anforderung.

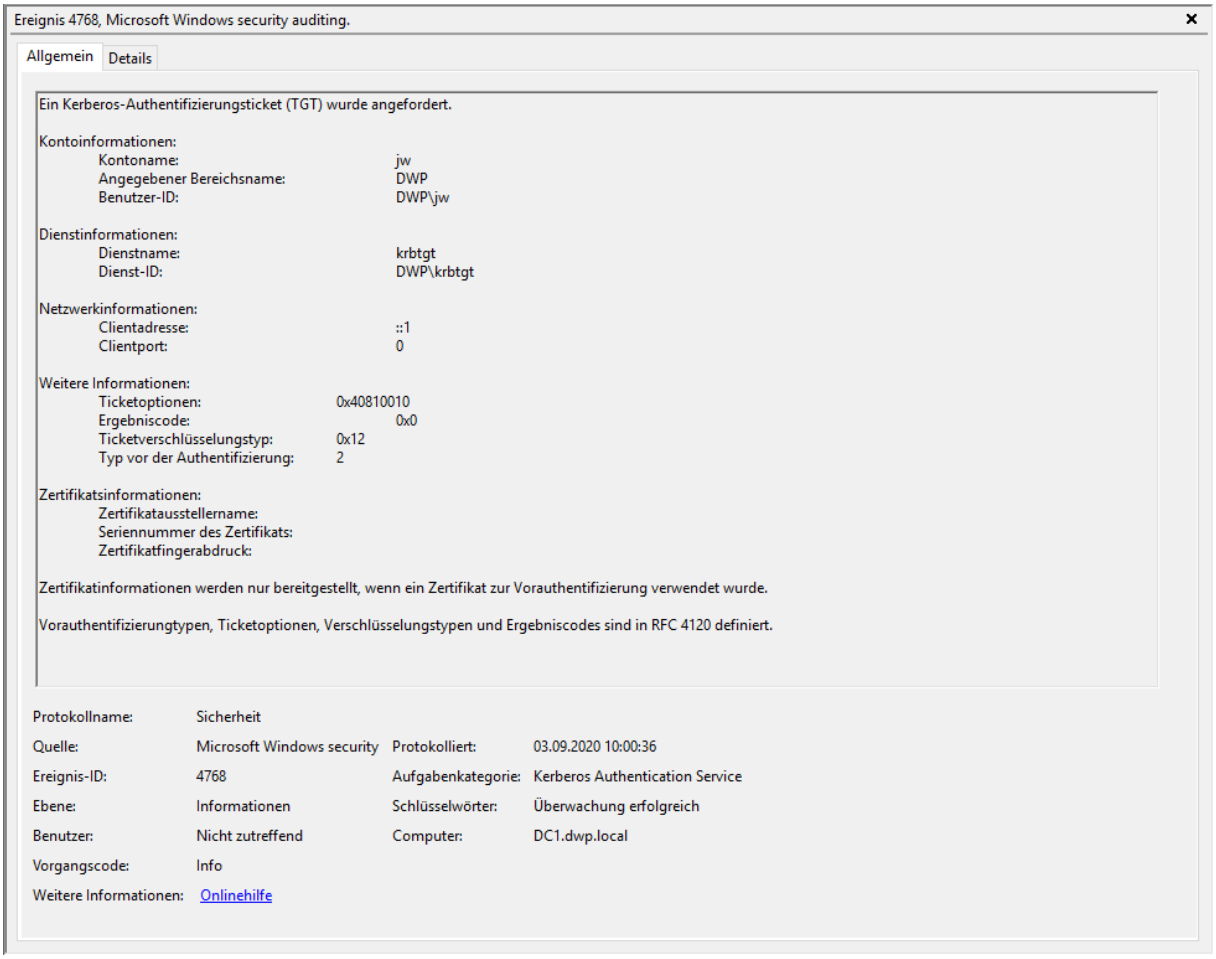


Was tun bei einem Kerberos Problem?



Authentication Auditing

Das Event-Log mit der ID 4768 kurz mal erklärt



Kontoinformationen

- Kontoname
  - Der Name des Kontos für das eine TGT angefordert wurde
- Angegebener Bereichsname
  - Ist das Kerberos Realm zu dem der User oder der Computer gehört
- Benutzer-ID
  - Es kann auch nur die SID angezeigt werden, sofern diese zuvor von der Ereignisanzeige nicht aufgelöst werden konnte.

Dienstinformation

- Dienstname
  - Das Ziel an, dass die TGT Anforderung gesendet wurde
- Dienst-ID
  - Das Ziel des Kontos an das die TGT Anforderung gesendet wurde

Netzwerkinformation

- Clientadresse
  - Die IP-Adresse des DCs von dem die TGT Anforderung empfangen wurde
- Clientport
  - Der Quell-Port des Clients. 0 steht für localhost

Authentication Auditing

Weitere Informationen

- Ticketoption
  - Hexadezimale Ticket-Flags
    - 0x40810010 - Weiterleitbar, erneuerbar, kanonisch, erneuerbar-ok
    - 0x40810000 - weiterleitbar, erneuerbar, kanonisch
    - 0x60810010 - weiterleitbar, weiterleitbar, erneuerbar, kanonisch, erneuerbar-ok
- Ergebniscode
  - Hexadezimale Fehlercodes

Code	Code Name	Beschreibung	Mögliche Ursachen
0x0	KDC_ERR_NONE	Kein Fehler	Es wurden keine Fehler gefunden.
0x1	KDC_ERR_NAME_EXP	Der Eintrag des Clients in der KDC-Datenbank ist abgelaufen	Keine Information.
0x2	KDC_ERR_SERVICE_EXP	Der Servereintrag in der KDC-Datenbank ist abgelaufen	Keine Information.
0x3	KDC_ERR_BAD_PVNO	Angeforderte Kerberos-Versionsnummer wird nicht unterstützt	Keine Information.
0x4	KDC_ERR_C_OLD_MAST_KVNO	Client-Schlüssel in altem Hauptschlüssel verschlüsselt	Keine Information.
0x5	KDC_ERR_S_OLD_MAST_KVNO	Serverschlüssel in altem Hauptschlüssel verschlüsselt	Keine Information.
0x6	KDC_ERR_C_PRINCIPAL_UNKNOWN	Client nicht in Kerberos-Datenbank gefunden	Der Benutzername existiert nicht.
0x7	KDC_ERR_S_PRINCIPAL_UNKNOWN	Server nicht in Kerberos-Datenbank gefunden	Der Domänencontroller kann den Servernamen in Active Directory nicht finden.
0x8	KDC_ERR_PRINCIPAL_NOT_UNIQUE	Mehrere Haupteinträge in der KDC-Datenbank	Es gibt doppelte Hauptnamen. Eindeutige Hauptnamen sind entscheidend für die gegenseitige Authentifizierung. Doppelte Hauptnamen sind strengstens verboten, auch in mehreren Bereichen. Ohne eindeutige Prinzipalnamen kann der Client nicht sicherstellen, dass der Server, mit dem er kommuniziert, der richtige ist.
0x9	KDC_ERR_NULL_KEY	Der Client oder Server hat einen	Für den Client oder Server wurde kein Hauptschlüssel gefunden. Dies bedeutet normalerweise, dass der

		Nullschlüssel (Hauptschlüssel)	Administrator das Kennwort für das Konto zurücksetzen sollte.
0xA	KDC_ERR_CANNOT_POSTDATE	Ticket (TGT) kann nicht nachdatiert werden	Ein Kunde hat die Nachdatierung eines Kerberos-Tickets angefordert (Festlegen der Startzeit des Tickets auf ein zukünftiges Datum / eine zukünftige Uhrzeit), oder es besteht ein Zeitunterschied zwischen dem Kunden und dem KDC.
0xB	KDC_ERR_NEVER_VALID	Die angeforderte Startzeit ist später als die Endzeit	Es gibt einen Zeitunterschied zwischen dem KDC und dem Client.
0xC	KDC_ERR_POLICY	Die angeforderte Startzeit ist später als die Endzeit	Es gibt Anmeldebeschränkungen für das Benutzerkonto, z. B. eine Workstation-Einschränkung, eine Smartcard-Authentifizierungsanforderung oder eine Einschränkung der Anmeldezeit.
0xD	KDC_ERR_BADOPTION	KDC kann die angeforderte Option nicht berücksichtigen	Das TGT läuft bald ab. Der Client versucht, Anmeldeinformationen an einen SPN zu delegieren, der nicht in der Liste "Zulässig delegieren an" enthalten ist.
0xE	KDC_ERR_ETYPE_NOTSUPP	KDC unterstützt den Verschlüsselungstyp nicht	Das KDC oder der Client hat ein Paket empfangen, das nicht entschlüsselt werden kann.
0xF	KDC_ERR_SUMTYPE_NOSUPP	KDC unterstützt den Prüfsummentyp nicht	Das KDC, der Server oder der Client hat ein Paket erhalten, für das es keinen geeigneten Verschlüsselungsschlüssel hat, sodass das Ticket nicht entschlüsselt werden kann.
0x10	KDC_ERR_PADATA_TYPE_NOSUPP	KDC unterstützt den PADATA-Typ (Vorauthentifizierungsdaten) nicht.	Die Smartcard-Anmeldung wird versucht und das richtige Zertifikat kann nicht gefunden werden. Dies kann passieren, weil die falsche Zertifizierungsstelle abgefragt wird oder die richtige Zertifizierungsstelle nicht kontaktiert werden kann. Auf dem Domänencontroller ist kein Zertifikat für Smartcards installiert (Domänencontroller- oder Domänencontroller-Authentifizierungsvorlagen). Dieser Fehlercode kann in Ereignis 4768 nicht auftreten, kann jedoch in 4771 auftreten.
0x11	KDC_ERR_TRTYPE_NO_SUPP	KDC unterstützt keine Transit-Typen	Keine Information.
0x12	KDC_ERR_CLIENT_REVOKED	Die Anmeldeinformationen	Es kann explizite Einschränkungen für das Konto geben. Das Konto

		des Kunden wurden widerrufen	kann auch deaktiviert, abgelaufen oder gesperrt werden.
0x13	KDC_ERR_SERVICE_REVOKED	Anmeldeinformationen für den Server wurden widerrufen	Keine Information.
0x14	KDC_ERR_TGT_REVOKED	TGT wurde widerrufen	Da das entfernte KDC möglicherweise seinen PKCROSS-Schlüssel ändert, während noch PKCROSS-Tickets aktiv sind, sollte es die alten PKCROSS-Schlüssel zwischenspeichern, bis das zuletzt ausgestellte PKCROSS-Ticket abläuft. Andernfalls antwortet das Remote-KDC einem Client mit diesem Fehlercode. Weitere Informationen finden Sie in RFC1510.
0x15	KDC_ERR_CLIENT_NOTYET	Client noch nicht gültig - versuchen Sie es später erneut	Keine Information.
0x16	KDC_ERR_SERVICE_NOTYET	Server noch nicht gültig - versuchen Sie es später erneut	Keine Information.
0x17	KDC_ERR_KEY_EXPIRED	Passwort ist abgelaufen - ändern Sie das Passwort zum Zurücksetzen	Das Passwort des Benutzers ist abgelaufen. Dieser Fehlercode kann in Ereignis 4768 nicht auftreten, tritt jedoch in Ereignis 4771 auf.
0x18	KDC_ERR_PREAUTH_FAILED	Die Informationen vor der Authentifizierung waren ungültig	Das falsche Passwort wurde angegeben. Dieser Fehlercode kann in Ereignis 4768 nicht auftreten, tritt jedoch in Ereignis 4771 auf.
0x19	KDC_ERR_PREAUTH_REQUIRED	Zusätzliche Vorauthentifizierung erforderlich	Tritt häufig in UNIX-Interoperabilitätsszenarien auf. MIT-Kerberos-Clients fordern keine Vorauthentifizierung an, wenn sie eine KRB_AS_REQ-Nachricht senden. Wenn eine Vorauthentifizierung erforderlich ist (Standardeinstellung), senden Windows-Systeme diesen Fehler. Die meisten MIT-Kerberos-Clients reagieren auf diesen Fehler mit einer Vorauthentifizierung. In diesem Fall kann der Fehler ignoriert werden.

0x1A	KDC_ERR_SERVER_NOMATCH	KDC kennt den angeforderten Server nicht	Keine Information.
0x1B	KDC_ERR_SVC_UNAVAILABLE	KDC ist nicht verfügbar	Keine Information.
0x1F	KRB_AP_ERR_BAD_INTEGRITY	Integritätsprüfung für entschlüsseltes Feld fehlgeschlagen	Der Authentifikator wurde mit etwas anderem als dem Sitzungsschlüssel verschlüsselt, sodass der Client die resultierende Nachricht nicht entschlüsseln kann. Die Änderung der Nachricht kann das Ergebnis eines Angriffs oder eines Netzwerkrauschens sein.
0x20	KRB_AP_ERR_TKT_EXPIRED	Das Ticket ist abgelaufen	Je kleiner der Wert für die Kerberos-Richtlinieneinstellung *Maximale Lebensdauer* für Benutzertickets ist, desto wahrscheinlicher ist es, dass dieser Fehler auftritt. Da die Ticketerneuerung automatisch erfolgt, sollten Sie nichts tun müssen, wenn Sie diese Nachricht erhalten.
0x21	KRB_AP_ERR_TKT_NYV	Das Ticket ist noch nicht gültig	Die Uhren auf dem KDC und dem Client sind nicht synchronisiert. Wenn eine bereichsübergreifende Kerberos-Authentifizierung versucht wird, sollten Sie die Zeitsynchronisation zwischen dem KDC im Zielbereich und dem KDC im Clientbereich überprüfen.
0x22	KRB_AP_ERR_REPEAT	Die Anfrage ist eine Wiederholung	Ein bestimmter Authentifikator tauchte zweimal auf. Mit anderen Worten, das KDC hat festgestellt, dass dieses Sitzungsticket eines dupliziert, das es bereits erhalten hat.
0x23	KRB_AP_ERR_NOT_US	Das Ticket ist nicht für uns	Der Server hat ein Ticket erhalten, das für einen anderen Bereich bestimmt war.
0x24	KRB_AP_ERR_BADMATCH	Ticket und Authentifikator stimmen nicht überein	Der KRB_TGS_REQ wird an das falsche KDC gesendet.
0x25	KRB_AP_ERR_SKEW	Der Zeitversatz ist zu groß	Ein Clientcomputer hat einen Zeitstempel gesendet, der die Wertdifferenz überschritten hat, die in der Kerberos-Richtlinie unter der Einstellung *Maximale* Toleranz für die *Synchronisierung* der Computeruhr zulässig ist .

0x26	KRB_AP_ERR_BADADDR	Die Netzwerkadresse im Header der Netzwerkschicht stimmt nicht mit der Adresse im Ticket überein	Die Adresse des Computers, der das Ticket sendet, unterscheidet sich von der gültigen Adresse im Ticket. Eine mögliche Ursache hierfür könnte eine Änderung der IP-Adresse sein Das Ticket wurde über einen Proxyserver oder NAT weitergeleitet. Dem Client ist das vom Proxyserver verwendete Adressschema nicht bekannt. Wenn das Programm den Client nicht veranlasst, ein Proxyserver-Ticket mit der Quelladresse des Proxyservers anzufordern, ist das Ticket möglicherweise ungültig.
0x27	KRB_AP_ERR_BADVERSION	Protokollversionsnummern stimmen nicht überein (PVNO)	Eine Anwendung überprüft die KRB_SAFE-Nachricht, um sicherzustellen, dass die Felder für die Protokollversion und den Typ mit der aktuellen Version bzw. KRB_SAFE übereinstimmen. Eine Nichtübereinstimmung generiert diesen Fehlercode.
0x28	KRB_AP_ERR_MSG_TYPE	Der Nachrichtentyp wird nicht unterstützt	Der Zielserver stellt fest, dass das Nachrichtenformat falsch ist. Dies gilt für KRB_AP_REQ-, KRB_SAFE-, KRB_PRIV- und KRB_CRED-Nachrichten. Das UDP-Protokoll wird mit Benutzer-zu-Benutzer-Authentifizierung versucht.
0x29	KRB_AP_ERR_MODIFIED	Nachrichtenstrom geändert und Prüfsumme stimmte nicht überein	Die Authentifizierungsdaten wurden mit dem falschen Schlüssel für den vorgesehenen Server verschlüsselt. Die Authentifizierungsdaten wurden während der Übertragung durch einen Hardware- oder Softwarefehler oder durch einen Angreifer geändert. Falsche DNS-Daten haben dazu geführt, dass der Client die Anforderung an den falschen Server gesendet hat.
0x2A	KRB_AP_ERR_BADORDER	Nachricht nicht in Ordnung (mögliche Manipulation)	Dieses Ereignis wird von KRB_SAFE- und KRB_PRIV-Nachrichten generiert, wenn eine falsche Sequenznummer enthalten ist oder wenn eine Sequenznummer erwartet wird, aber nicht vorhanden ist. Weitere Informationen finden Sie in RFC4120.
0x2C	KRB_AP_ERR_BADKEYVER	Die angegebene Version des Schlüssels ist nicht verfügbar	Dieser Fehler kann auf der Serverseite beim Empfang einer ungültigen KRB_AP_REQ-Nachricht generiert werden. Der Server kann die im Ticket in KRB_AP_REQ angegebene Schlüsselversion nicht verwenden (z. B. zeigt er einen alten

			Schlüssel an, von dem der Server keine Kopie hat).
0x2D	KRB_AP_ERR_NOKEY	Serviceschlüssel nicht verfügbar	Dieser Fehler kann auf der Serverseite beim Empfang einer ungültigen KRB_AP_REQ-Nachricht generiert werden. Der Server verfügt nicht über den richtigen Schlüssel zum Entschlüsseln des Tickets. Da der Server in mehreren Bereichen mit unterschiedlichen Schlüsseln in jedem Bereich registriert werden kann, wird im Bereich des Bereichs im unverschlüsselten Teil des Tickets in KRB_AP_REQ angegeben, mit welchem geheimen Schlüssel der Server dieses Ticket entschlüsseln soll.
0x2E	KRB_AP_ERR_MUT_FAIL	Die gegenseitige Authentifizierung ist fehlgeschlagen	Keine Information.
0x2F	KRB_AP_ERR_BADDIRECTION	Falsche Nachrichtenrichtung	Keine Information.
0x30	KRB_AP_ERR_METHOD	Alternative Authentifizierungsmethode erforderlich	Laut RFC4120 ist diese Fehlermeldung veraltet.
0x31	KRB_AP_ERR_BADSEQ	Falsche Sequenznummer in der Nachricht	Keine Information.
0x32	KRB_AP_ERR_INAPP_CKSUM	Unangemessene Art der Prüfsumme in der Nachricht (Prüfsumme wird möglicherweise nicht unterstützt)	Wenn das KDC eine KRB_TGS_REQ-Nachricht empfängt, entschlüsselt es diese. Anschließend muss die vom Benutzer bereitgestellte Prüfsumme im Authenticator anhand des Inhalts der Anforderung überprüft und die Nachricht zurückgewiesen werden, wenn die Prüfsummen nicht übereinstimmen (mit dem Fehlercode KRB_AP_ERR_MODIFIED) oder wenn die Prüfsumme nicht kollidiert. Beweis (mit dem Fehlercode KRB_AP_ERR_INAPP_CKSUM).
0x33	KRB_AP_PATH_NOT_ACCEPTED	Gewünschter Weg ist nicht erreichbar	Keine Information.
0x34	KRB_ERR_RESPONSE_TOO_BIG	Zu viele Daten	Die Größe eines Tickets ist zu groß, um zuverlässig über UDP übertragen zu werden. In einer Windows-Umgebung dient diese Nachricht nur zur Information. Ein Windows-Computer

			versucht automatisch TCP, wenn UDP fehlschlägt.
0x3C	KRB_ERR_GENERIC	Allgemeiner Fehler	Die Gruppenmitgliedschaft hat das Privilege Account Certificate (PAC) überlastet. Mehrere kürzlich vorgenommene Kennwortänderungen wurden nicht weitergegeben. Krypto-Subsystemfehler durch Speichermangel. Der SPN ist zu lang Der SPN hat zu viele Teile.
0x3D	KRB_ERR_FIELD_TOOLONG	Das Feld ist für diese Implementierung zu lang	Wenn ein KDC, der nicht versteht, wie ein gesetztes High-Bit der Längencodierung zu interpretieren ist, eine Anforderung mit dem höherwertigen Bit der eingestellten Länge empfängt, muss er eine KRB-ERROR-Nachricht mit dem Fehler KRB_ERR_FIELD_TOOLONG zurückgeben und das schließen TCP-Stream. Jeder Anforderung (KRB_KDC_REQ) und Antwort (KRB_KDC_REP oder KRB_ERROR), die über den TCP-Stream gesendet wird, geht die Länge der Anforderung als 4 Oktette in der Reihenfolge der Netzwerkbytes voraus. Das hohe Bit der Länge ist für zukünftige Erweiterungen reserviert und muss derzeit auf Null gesetzt werden.
0x3E	KDC_ERR_CLIENT_NOT_TRUSTED	Die Client-Vertrauensstellung ist fehlgeschlagen oder nicht implementiert	Das Smartcard-Zertifikat eines Benutzers wurde widerrufen, oder die Stammzertifizierungsstelle, die das Smartcard-Zertifikat (in einer Kette) ausgestellt hat, wird vom Domänencontroller nicht als vertrauenswürdig eingestuft.
0x3F	KDC_ERR_KDC_NOT_TRUSTED	Die KDC-Serververtrauensstellung ist fehlgeschlagen oder konnte nicht überprüft werden	Das Feld *trustCertifiers* enthält eine Liste der vom Client vertrauenswürdigen Zertifizierungsstellen für den Fall, dass der Client nicht über das Public-Key-Zertifikat des KDC verfügt. Wenn das KDC kein von einem der vertrauenswürdigen Zertifizierer signiertes Zertifikat hat, gibt es diesen Fehlercode zurück. Weitere Informationen finden Sie in RFC1510 .
0x40	KDC_ERR_INVALID_SIG	Die Signatur ist ungültig	Dieser Fehler hängt mit PKINIT zusammen. Wenn eine PKI-Vertrauensstellung besteht, überprüft das KDC die Signatur des Clients auf AuthPack (TGT-

			Anforderungssignatur). Wenn dies fehlschlägt, gibt das KDC diesen Fehlercode zurück.
0x41	KDC_ERR_KEY_TOO_WEAK	Eine höhere Verschlüsselungsstufe ist erforderlich	f das *clientPublicValue* Feld ausgefüllt, was darauf hinweist , dass der Kunde wünscht , Diffie-Hellman - Schlüsselvereinbarung zu verwenden, dann die Kontrollen KDC , um zu sehen , dass die Parameter ihre Politik erfüllen. Wenn dies nicht der Fall ist (z. B. ist die Primgröße für den erwarteten Verschlüsselungstyp nicht ausreichend), gibt das KDC diesen Fehlercode zurück.
0x42	KRB_AP_ERR_USER_TO_USER_REQUIRED	Eine Benutzer-zu-Benutzer-Autorisierung ist erforderlich	Der Client weiß nicht, dass ein Dienst eine *Benutzer-zu-Benutzer-Authentifizierung* erfordert. Daher fordert er einen herkömmlichen KRB_AP_REP an, empfängt ihn und leitet ihn an den Server weiter. Der Server generiert diesen Fehlercode als Antwort.
0x43	KRB_AP_ERR_NO_TGT	Es wurde kein TGT vorgestellt oder verfügbar	Ein Dienst verfügt nicht über eine TGT für die Benutzer-zu-Benutzer- *Authentifizierung.*
0x44	KDC_ERR_WRONG_REALM	Falsche Domain oder Principal	Der Client präsentiert eine bereichsübergreifende TGT einem anderen als dem in der TGT angegebenen Bereich. Dieser Fehler tritt selten auf, wird jedoch normalerweise durch ein falsch konfiguriertes DNS verursacht.

Ticketverschlüsselungstyp

- Gibt die Cyphersuite an mit der die Ausgabe verschlüsselt wurde

Art	Modellname	Beschreibung
0x1	DES-CBC-CRC	Ab Windows 7 und Windows Server 2008 R2 standardmäßig deaktiviert.
0x3	DES-CBC-MD5	Ab Windows 7 und Windows Server 2008 R2 standardmäßig deaktiviert.
0x11	AES128-CTS-HMAC-SHA1-96	Unterstützt ab Windows Server 2008 und Windows Vista.
0x12	AES256-CTS-HMAC-SHA1-96	Unterstützt ab Windows Server 2008 und Windows Vista.

0x17	RC4-HMAC	Standardsuite für Betriebssysteme vor Windows Server 2008 und Windows Vista.
0x18	RC4-HMAC-EXP	Standardsuite für Betriebssysteme vor Windows Server 2008 und Windows Vista.
0xFFFFFFFF oder 0xffffffff	- -	Dieser Typ wird in *Audit Failure*- Ereignissen *angezeigt* .

Typ der Authentifizierung

- Der Code gibt den Vorauthentifizierungstyp an

Fehlercode	Beschreibung	Beschreibung
0	- -	Anmeldung ohne Vorauthentifizierung.
2	PA-ENC-TIMESTAMPS	Standard-Passwortauthentifizierung.
11	PA-ETYPE-INFO	Zusätzliche Vorauthentifizierung erforderlich (zusammen mit KRB-ERROR vom KDC). Wird normalerweise verwendet, um einen Client zu benachrichtigen, welcher Schlüssel für die Verschlüsselung verwendet werden soll, während ein Vorauthentifizierungswert für PA-ENC-TIMESTAMP gesendet wird. Nie in Microsoft Active Directory-Umgebungen gesehen.
fünfzehn	PA-PK-AS-REP_OLD	Wird für die Smartcard-Anmeldeauthentifizierung verwendet.
17	PA-PK-AS-REP	Wird für die Smartcard-Authentifizierung verwendet. In bestimmten Active Directory-Umgebungen nie gesehen.
19	PA-ETYPE-INFO2	Zusätzliche Vorauthentifizierung erforderlich (zusammen mit KRB-ERROR vom KDC). Wird normalerweise verwendet, um einen Client zu benachrichtigen, welcher Schlüssel für die Verschlüsselung verwendet werden soll, während ein Vorauthentifizierungswert für PA-ENC-TIMESTAMP gesendet wird. Nie in Microsoft Active Directory-Umgebungen gesehen.
20	PA-SVR-REFERRAL-INFO	Wird in KDC Referrals Tickets verwendet.

138	PA-ENCRYPTED-CHALLENGE	Melden Sie sich mit Kerberos Armoring (FAST) an. Unterstützt in Domänencontrollern mit Windows Server 2012 und höher sowie in Clients mit Windows 8 und höher.
- -	- -	*Wird* in *Audit Failure*- Ereignissen *angezeigt*.

Zertifikatsinformation

- Zertifikatsausstellername
  - Ist gleich der Name der Zertifizierungsstelle
- Seriennummer des Zertifikats
  - z.B. einer Smartcard
- Zertifikatfingerabdruck
  - z.B. einer Smartcard

Authentication Auditing

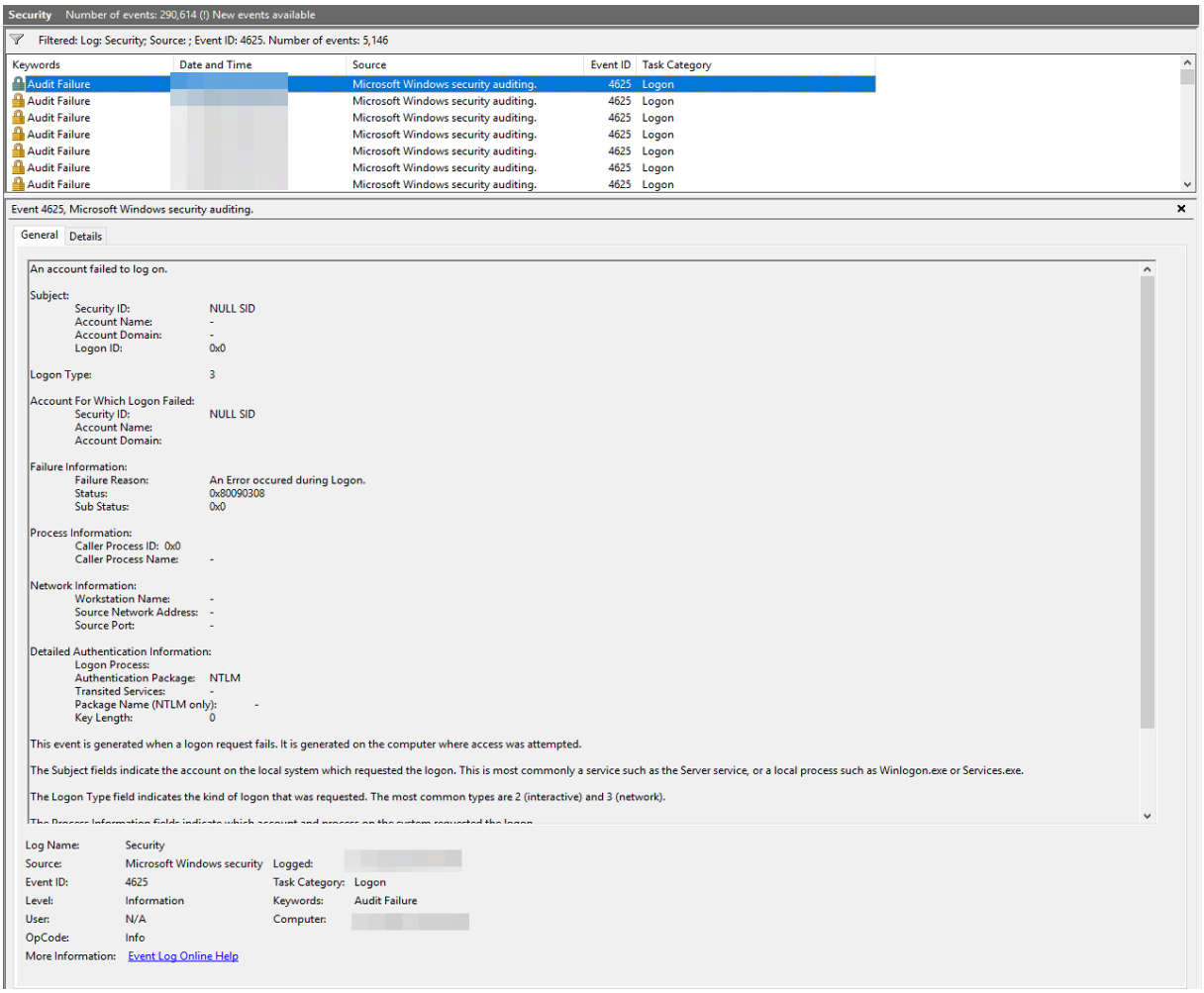
Event-Logs die man kennen sollte

Event-Log-ID 4625 = An account failed to log on

Event 4625 kommt nur auf den Betriebssystemen

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2008 R2
- Windows 10
- Windows 8.1/7

Event-Log-ID 4624 = An account was successfully logged on
Event-Log-ID 4634 = An account was logged of
Event-Log-ID 4771 = Kerberos Pre-Authentication failed
Event-Log-ID 4768 = Kerberos Authentication Ticket was requested (abgelaufen)



Authentication Auditing

Wichtige Informationen zu dem Event 4625 sind:

Anmeldetyp

- Gibt die Art der Anmeldung des Users aus
    - Typ 2 - wenn ein User sich lokal anmeldet
    - Typ 3 - wenn ein User sich remote an einen Drucker oder Dateiserver oder IIS anmeldet
    - Typ 4 - wenn der Taskplaner eine Batch-geplante Aufgabe ausführt
    - Typ 5 - wenn ein Dienst oder ein Dienstkonto sich anmeldet
    - Typ 7 - wenn ein User seinen Computer entsperrt
    - Typ 8 - wenn eine Klartext Anmeldung durchgeführt/gesendet wurde (Basisauthentifizierung)
    - Typ 9 - wenn ein User oder eine Anwendung RunAs/netonly gestartet hat
    - Typ 10 - gibt eine RDP Anmeldung, Terminalserver oder Remoteunterstützung aus

Status und Sub Codes

Status- und Substatuscodes	Beschreibung
0xC0000064	Der Benutzername ist falsch geschrieben oder existiert nicht.
0xC000006A	Das Passwort des Benutzers ist falsch.
0xC000006D	Der Benutzername oder die Authentifizierungsinformationen sind falsch.
0xC0000234	Der Benutzer ist derzeit gesperrt.
0xC0000072	Das Benutzerkonto ist derzeit deaktiviert.
0xC000006F	Der Benutzer hat versucht, sich außerhalb der autorisierten Zeiten anzumelden.
0xC0000070	Der Benutzer hat versucht, sich von einer nicht autorisierten Workstation aus anzumelden.
0xC0000193	Das Benutzerkonto ist abgelaufen.
0xC0000071	Das Passwort des Benutzers ist abgelaufen.
0xC0000133	Die Zeiten des Domänencontrollers und des Computers sind nicht synchron.
0xC0000224	Der Benutzer muss sein Passwort bei der nächsten Anmeldung ändern.
0xc000015b	Dem Benutzer wurde der angeforderte Anmeldetyp auf diesem Computer nicht gewährt.

Die Gründe für die Überwachung des Events 4625 sind

- Erkennung von Brute-Force-Attacken
    - Nutzung von Wörterbüchern, ergibt eine hohe Anzahl an Fehlversuchen
- Böswillige interne Aktivitäten
    - Ein Anmeldeversuch trotz deaktiviertem Konto, eines nicht autorisierten Clients oder außerhalb der festgelegten Anmeldezeit

Authentication Auditing

Wichtige Informationen zu dem Event 4771 sind:

- Fehlercode
    - Hexadezimale Ausgabe der Fehler bedeuten

Code	Code Name	Beschreibung	Mögliche Ursachen
0x10	KDC_ERR_PADATA_TYPE_NOSUPP	KDC unterstützt den PADATA-Typ (Vorauthentifizierungsdaten) nicht.	Die Smartcard-Anmeldung wird versucht und das richtige Zertifikat kann nicht gefunden werden. Dies kann passieren, weil die falsche Zertifizierungsstelle (CA) abgefragt wird oder die richtige Zertifizierungsstelle nicht kontaktiert werden kann, um Domänencontroller-Authentifizierungszertifikate für den Domänencontroller abzurufen. Dies kann auch passieren, wenn auf einem DC kein Zertifikat für Smartcards installiert ist.
0x17	KDC_ERR_KEY_EXPIRED	Passwort ist abgelaufen - ändern Sie das Passwort zum Zurücksetzen.	Das Passwort des Benutzers ist abgelaufen.
0x18	KDC_ERR_PREAUTH_FAILED	Die Informationen vor der Authentifizierung waren ungültig.	Das falsche Passwort wurde angegeben.

- Vorauthentifizierungstyp
    - Der Typ der in der Vorauthentifizierung der TGT Anforderung verwendet wurde

Art	Modellname	Beschreibung
0	- -	Dieser Code zeigt eine Anmeldung ohne Vorauthentifizierung an.
2	PA-ENC-TIMESTAMP	Dieser Code ist der normale Typ für die Standardkennwortauthentifizierung.
11	PA-ETYPE-INFO	Dieser Code wird vom KDC in einem KRB-ERROR gesendet, was darauf hinweist, dass eine zusätzliche Vorauthentifizierung erforderlich ist. Es wird normalerweise verwendet, um einem Client mitzuteilen, welcher Verschlüsselungsschlüssel zum Verschlüsseln eines Zeitstempels beim Senden eines PA-ENC-TIMESTAMP-Vorauthentifizierungswerts verwendet werden soll.
fünfzehn	PA-PK-AS-REP_OLD	Dieser Code wird für die Smart Card-Anmeldeauthentifizierung verwendet.
17	PA-PK-AS-REP	Dieser Code sollte auch für die Smartcard-Authentifizierung verwendet werden, wird jedoch in bestimmten Active Directory-Umgebungen nie angezeigt.
19	PA-ETYPE-INFO2	Dieser Code wird vom KDC in einem KRB-ERROR gesendet, der angibt, dass eine zusätzliche Vorauthentifizierung erforderlich ist. Normalerweise wird es verwendet, um einen Client darüber zu informieren, welcher Schlüssel für die Verschlüsselung eines

		verschlüsselten Zeitstempels zum Senden eines PA-ENC-TIMESTAMP-Vorauthentifizierungswerts verwendet werden soll.
20	PA-SVR-REFERRAL-INFO	Dieser Code wird in KDC Referrals-Tickets verwendet.
138	PA-ENCRYPTED-CHALLENGE	Dieser Code wird verwendet, um eine Anmeldung mit Kerberos Armoring (FAST) anzuzeigen. Die Unterstützung für diesen Code wurde mit Windows Server 2012 und Windows 8 gestartet.
- -		Dieser Code wird in Audit Failure-Ereignissen angezeigt.

Ein gutes Auditing Tool ist Manage Engine AD Audit Plus.