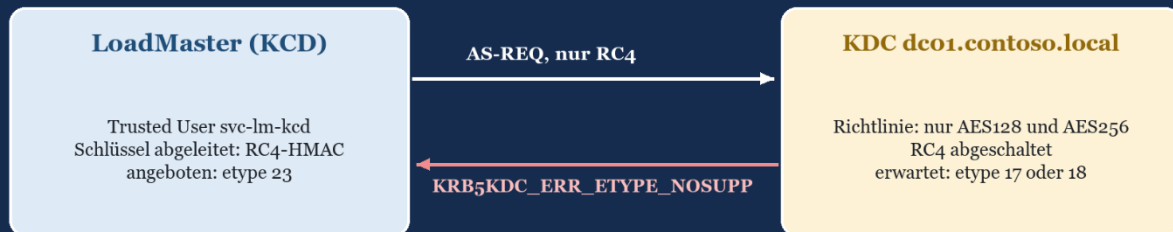


Die RC4-Falle: KCD-Keytab trifft AES-only-Domäne

Die RC4-Falle

Der LoadMaster spricht RC4, der Domänencontroller nur noch AES. Beide haben recht, keiner gibt nach.



Skizze: Fehlerbild am Beispiel der Domäne contoso.local

WISSEN

Alles zum Kemp LoadMaster mit Microsoft-Brille: Exchange, SharePoint, ADFS, RDS und Kerberos an einem Ort.

› [Kemp LoadMaster](#)

BERATUNG

RC4-Härtung steht an und der LoadMaster soll nicht der Grund für den Rollback sein? Wir prüfen Konten und KCD vorher.

› [Beratung zum Kemp LoadMaster](#)

SCHULUNG

Kerberos-Verschlüsselungstypen, KCD und ESP im Labor kaputt machen und reparieren, bevor es die Produktion tut.

› [Kemp-LoadMaster-Schulung](#)

Es gibt Projekte, bei denen alle alles richtig machen und trotzdem am Montagmorgen das Telefon klingelt. Das Security-Team härtet die Domäne, schaltet RC4 per Gruppenrichtlinie ab, liest stolz die Audit-Berichte vor. Das LoadMaster-Team hat vor drei Jahren eine wunderbar funktionierende Kerberos Constrained Delegation eingerichtet, die seitdem niemand mehr angefasst hat. Und dann treffen sich beide Welten am Domänencontroller, und der sagt ganz trocken: KRB5KDC_ERR_ETYPE_NOSUPP. Übersetzt: Ich kann mit deinem Schlüssel nichts anfangen, und ich habe auch keine Lust, es zu versuchen.

Der Grund ist banal und gemein zugleich. Der Progress Kemp LoadMaster verwendet für kemp kcd aes nicht automatisch AES. Ohne eine eigens zu setzende Option leitet er aus dem Kennwort des Trusted Users RC4-Schlüssel ab und bietet dem KDC genau diesen Verschlüsselungstyp an. Solange der Domänencontroller RC4 still als Rückfallebene akzeptiert, fällt das niemandem auf. Seit Microsoft RC4 im Laufe von 2026 abgekündigt und als Standard abgeschaltet hat, fällt es allen auf, und zwar gleichzeitig.

In diesem Beitrag erfährst du, warum die Falle zuschnappt, an welchen drei Stellen im KCD-Ablauf AES gefordert ist, wie du den Fehler sicher erkennst und in welcher Reihenfolge du LoadMaster und Active Directory umstellst, ohne zwischendurch alle Benutzer auszusperrern. Wie KCD am LoadMaster grundsätzlich funktioniert, steht in [Kerberos Constrained Delegation am LoadMaster: KCD und RBCD sauber einrichten](#). Den Überblick über alle LoadMaster-Themen mit Microsoft-Bezug findest du auf der Übersichtsseite [Kemp LoadMaster](#).

FAKTEN · Die RC4-Falle in fünf Sätzen

Der LoadMaster nutzt für KCD standardmäßig RC4, AES256 nur nach Aktivieren einer eigenen Option in der serverseitigen SSO-Konfiguration.

Härtungsrichtlinien und Microsofts RC4-Abkündigung sorgen dafür, dass Domänencontroller RC4-Anfragen ablehnen.

Das Ergebnis ist der Kerberos-Fehler KDC_ERR_ETYPE_NOSUPP, Fehlercode 14 beziehungsweise 0xE, und Benutzer landen trotz korrekter Anmeldung bei einem 401 oder einer Fehlerseite.

Die Heilung besteht aus drei Teilen: AES-Option am LoadMaster, AES-Verschlüsselungstypen am Dienstkonto und ein neu gesetztes Kennwort, damit überhaupt AES-Schlüssel existieren.

Die Reihenfolge entscheidet, ob die Umstellung fünf Minuten oder einen ganzen Vormittag dauert.

Warum der LoadMaster RC4 spricht, obwohl es niemand mehr hören will

Kerberos verschlüsselt fast alles mit Schlüsseln, die aus Kennwörtern abgeleitet werden. Für jedes Konto speichert Active Directory nicht einen, sondern mehrere Schlüssel, je einen pro Verschlüsselungstyp, kurz etype. RC4-HMAC hat den etype 23, AES128 den etype 17, AES256 den etype 18. Der RC4-Schlüssel ist dabei schlicht der NT-Hash des Kennworts, ohne Salz, ohne Iterationen. Wer ihn hat, braucht das Kennwort gar nicht mehr. Genau deshalb ist Kerberoasting gegen RC4-Tickets so beliebt und genau deshalb will Microsoft RC4 loswerden.

Der Trusted User und seine Schlüsseltabelle

Für KCD trägst du am LoadMaster in der serverseitigen SSO-Domäne den Kerberos Realm, einen oder zwei KDCs sowie Name und Kennwort des Trusted Users ein. Der LoadMaster hinterlegt kein Kennwort im Klartext für jede Anfrage, sondern baut daraus intern eine Kerberos-Schlüsseltabelle, gewissermaßen eine Keytab, mit der er sich am KDC authentifiziert. Welche Schlüssel in diese Tabelle wandern, bestimmt eine einzige Option: In der aktuellen Kemp-Dokumentation heißt sie „Use AES256 SHA1 KCD cipher“ und sitzt in der Verwaltung der serverseitigen Single-Sign-On-Konfigurationen. Ist sie nicht gesetzt, verwendet der LoadMaster RC4. Ältere Dokumentationsstände nennen als Standard RC4, DES und DES3; praktisch macht das keinen Unterschied, denn DES ist in jeder Domäne ab Windows Server 2008 R2 ohnehin abgeschaltet.

Eingeführt hat Kemp die AES-Option mit Firmware 7.2.48. Wer einen LoadMaster mit älterer Firmware betreibt, hat das Problem also nicht nur in der Konfiguration, sondern im Funktionsumfang. Dann steht vor allem anderen ein Update an, und wie du das ohne Herzzrasen erledigst, steht in [Firmware-Updates, Backup und Notfallplan: LoadMaster-Betrieb ohne Herzzrasen](#).

WICHTIG · Optionsnamen können je Firmware abweichen

Kemp hat die WUI über die Jahre mehrfach umgebaut. Die Bezeichnung „Use AES256 SHA1 KCD cipher“ stammt aus der aktuellen Konfigurationsanleitung der GA-Firmware. In älteren Ständen oder in LTSF-Versionen kann die Beschriftung leicht anders lauten oder an etwas anderer Stelle stehen. Suche im Zweifel in den Einstellungen der serverseitigen SSO-Domäne mit KCD nach einem Kontrollkästchen, das AES256 im Namen trägt. Findest du keines, ist deine Firmware zu alt.

Wie RC4 in der Domäne abgeschaltet wird

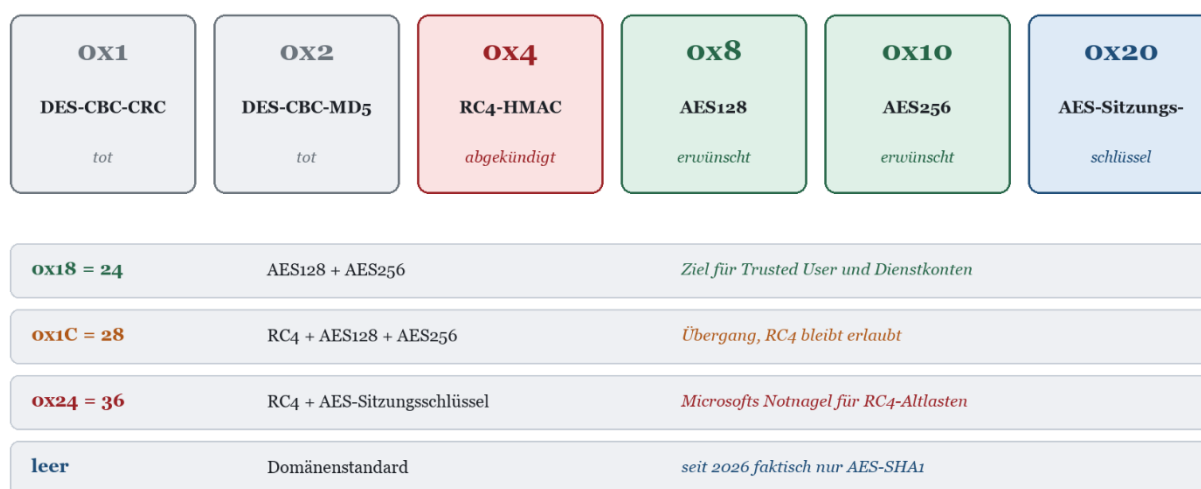
In härtinggetriebenen Umgebungen kommt die Abschaltung meist nicht von Microsoft, sondern vom eigenen Security-Team, oft Jahre vor dem offiziellen Zeitplan. Das Werkzeug der Wahl ist die Gruppenrichtlinie „Netzwerksicherheit: Für Kerberos zulässige Verschlüsselungstypen

konfigurieren“. Sie wirkt doppelt. Auf jedem Computer legt sie fest, welche Verfahren das System selbst verwendet, und schreibt den Wert in das Attribut msDS-SupportedEncryptionTypes des Computerkontos. Auf den Domänencontrollern bestimmt sie zusätzlich, welche Verfahren der KDC überhaupt annimmt und ausstellt. Steht dort nur AES128, AES256 und Zukünftige Verschlüsselungstypen, ist RC4 aus dem Rennen, egal was ein einzelnes Konto behauptet.

Für Benutzer- und Dienstkonten setzt die Richtlinie das Attribut nicht. Dort pflegst du msDS-SupportedEncryptionTypes selbst, per PowerShell oder über die Kontooptionen „Dieses Konto unterstützt Kerberos-AES-128-Bit-Verschlüsselung“ und das Gegenstück für 256 Bit. Ist das Attribut leer, greift der Domänenstandard, und der war jahrzehntelang RC4-freundlich. Genau dieser Standard ist 2026 gekippt.

msDS-SupportedEncryptionTypes: eine Zahl, sechs Schalter

Bits addieren, Ergebnis ans Konto schreiben, Kennwort neu setzen



Skizze: Bitwerte des Attributs msDS-SupportedEncryptionTypes, Auswahl

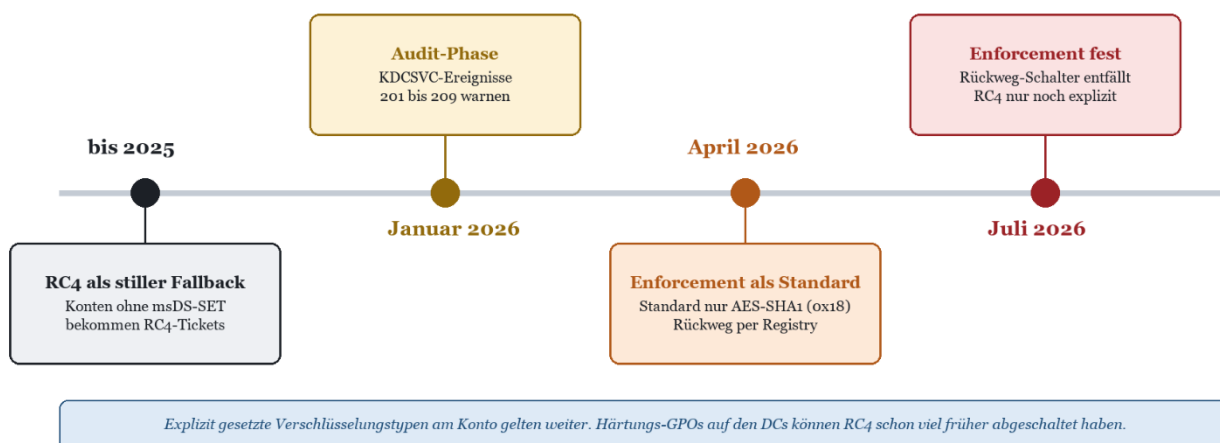
Wert	Bedeutung	Bewertung für KCD am LoadMaster
leer (nicht gesetzt)	Domänenstandard, seit der Härtung 2026 AES-SHA1	Funktioniert nur, wenn das Konto AES-Schlüssel besitzt
0x4 (4)	nur RC4	Sofortiger Fehler in einer AES-only-Domäne
0x18 (24)	AES128 und AES256	Empfohlen für Trusted User und Zielkonten
0x1C (28)	RC4, AES128 und AES256	Übergangswert, solange noch RC4-Clients existieren
0x24 (36)	RC4 mit AES-Sitzungsschlüsseln	Microsofts Ausnahmewert für Altgeräte, nicht für den LoadMaster gedacht

Microsofts RC4-Abkündigung: aus „sollte“ wurde „muss“

Lange war RC4 in Active Directory ein Untoter. Offiziell unerwünscht, praktisch überall noch erlaubt, weil Konten ohne gesetztes msDS-SupportedEncryptionTypes stillschweigend RC4-Tickets bekamen. Mit der Schwachstelle CVE-2026-20833 und dem Supportartikel KB5073381 hat Microsoft daraus einen Fahrplan gemacht, der inzwischen vollständig abgefahren ist.

Microsofts Fahrplan zum Abschied von RC4

Härtung zu CVE-2026-20833: aus der Warnung wurde im Laufe von 2026 die Regel



Skizze: Phasen laut Microsoft-Artikel KB5073381, vereinfacht

Zeitpunkt	Phase	Was sich am KDC ändert
13. Januar 2026	Audit	Neue KDCSVC-Ereignisse 201 bis 209 im System-Log warnen vor RC4-Abhängigkeiten. Der Registry-Wert RC4DefaultDisablementPhase steuert die Phase.
14. April 2026	Enforcement mit Rückweg	Der Standard für Konten ohne explizite Verschlüsselungstypen wird AES-SHA1 (0x18). Ein Rollback per Registry bleibt möglich.
Juli 2026	Enforcement	Der Schalter RC4DefaultDisablementPhase wird nicht mehr ausgewertet. RC4 gibt es nur noch, wo es ausdrücklich am Konto oder per DefaultDomainSupportedEncTypes erlaubt ist.

Für den LoadMaster heißt das: Selbst wer nie eine Härtungs-GPO gesehen hat, sitzt seit dem Sommer 2026 in einer faktisch AES-only-Domäne, sofern die Domänencontroller gepatcht sind. Ein Trusted User ohne gesetzte Verschlüsselungstypen, der nur RC4 anbietet, fällt dann unter genau das Szenario, das Microsoft mit den Ereignissen 203 beziehungsweise 208 blockiert.

Die Ereignisse, die du kennen solltest

Ereignis	Typ	Bedeutung
KDCSVC 201	Warnung	Client bietet nur RC4 an, Zieldienst ohne msDS-SET, Audit-Phase
KDCSVC 202	Warnung	Dienstkonto hat keine AES-Schlüssel, Audit-Phase
KDCSVC 203	Fehler	Anfrage blockiert, weil der Client nur RC4 anbietet
KDCSVC 204	Fehler	Anfrage blockiert, weil das Dienstkonto nur RC4-Schlüssel hat
KDCSVC 205	Warnung	DefaultDomainSupportedEncTypes erlaubt mehr als AES-SHA1
KDCSVC 206 bis 209	Warnung und Fehler	wie oben, aber für Konten, die ausdrücklich auf AES-SHA1 gesetzt sind
Security 4768 / 4769	Fehlerüberwachung	Ergebniscode 0xE bei AS- beziehungsweise TGS-Anfragen, Feld Ticketverschlüsselungstyp zeigt das ausgehandelte Verfahren

TIPP · Die Audit-Ereignisse sind dein Frühwarnsystem

Hast du die Audit-Phase verschlafen, ist das kein Drama: Suche auf allen Domänencontrollern in den Ereignissen 4768 und 4769 nach dem Kontonamen deines Trusted Users und schau auf den Ticketverschlüsselungstyp. Steht dort 0x17, also RC4, weißt du Bescheid, bevor die Gruppenrichtlinie es dir mitteilt. Microsoft weist ausdrücklich darauf hin, dass fehlende Ereignisse keine Garantie für Nicht-Windows-Clients sind. Der LoadMaster ist genau so ein Nicht-Windows-Client.

WARNUNG · DefaultDomainSupportedEncTypes ist keine Lösung

Microsoft erlaubt als letzten Ausweg, RC4 über den Registry-Wert DefaultDomainSupportedEncTypes auf allen KDCs wieder einzuschalten. Das öffnet die Schwachstelle für jedes Konto der Domäne, nur damit ein LoadMaster sein Häkchen nicht setzen muss. Wer das in einer gehärteten Domäne vorschlägt, sollte vorher seinen Lebenslauf aktualisieren. Auch die kontobezogene Ausnahme 0x24 ist für Altgeräte gedacht, die AES nicht beherrschen, nicht für ein System, das AES kann und nur nicht darf.

Das Fehlerbild: KRB5KDC_ERR_ETYPE_NOSUPP und seine Verkleidungen

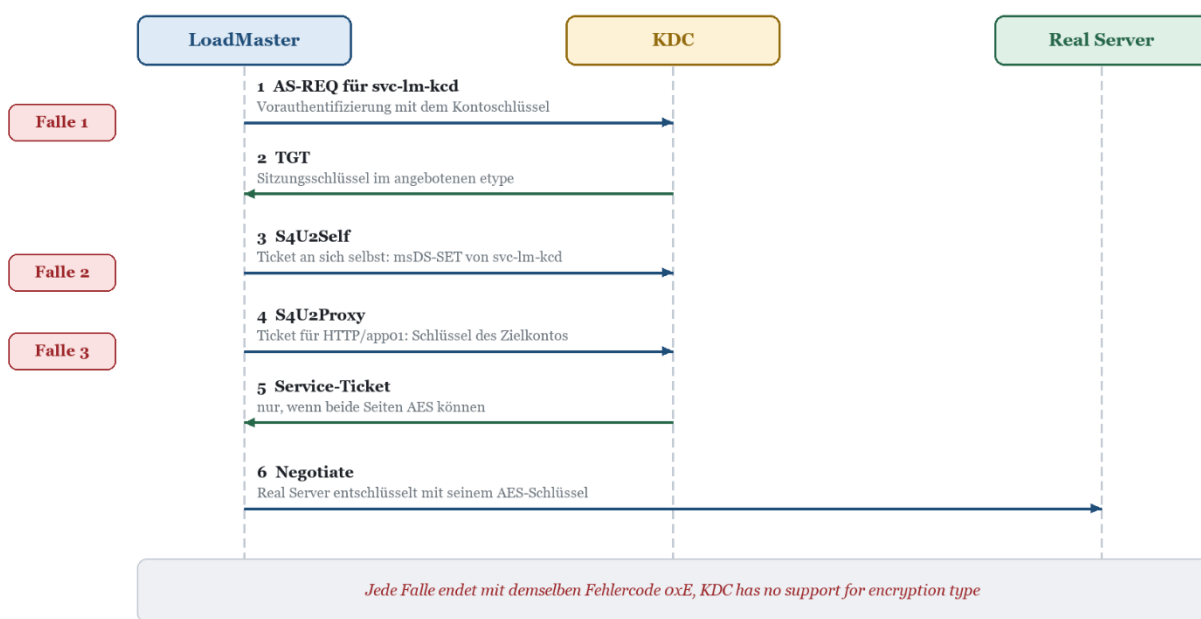
Das Tückische an der RC4-Falle ist, dass sie selten so heißt. Der Benutzer sieht das Anmeldeformular des ESP, meldet sich erfolgreich an und landet dann bei einem 401, einer leeren Seite oder einer erneuten Kennwortabfrage der Anwendung. Für ihn sieht das aus wie ein falsches Kennwort. Für den Helpdesk auch. Und für den Anwendungsbetreuer sieht es aus wie ein Problem des LoadMasters, das er sich nicht ansehen kann.

Drei Stellen, an denen AES fehlen kann

KCD am LoadMaster besteht aus mehreren Kerberos-Austauschen. Bei jedem einzelnen kann ein RC4-Rest die Kette reißen lassen, und jedes Mal kommt derselbe Fehlercode zurück.

Wo AES überall gefragt ist

Drei Kerberos-Austausche, drei Stellen, an denen ein RC4-Rest die Kette reißen lässt



Skizze: vereinfachter Ablauf von KCD mit Protocol Transition, Beispielnamen aus contoso.local

- **Falle 1, die Anmeldung des Trusted Users:** Der LoadMaster schickt einen AS-REQ und bietet nur RC4 an. Der KDC darf kein RC4 mehr und antwortet mit ETYPE_NOSUPP. Im Sicherheitsprotokoll erscheint 4768 mit Fehlercode 0xE. Das ist der häufigste Fall.
- **Falle 2, S4U2Self:** Das Ticket, das der Trusted User für sich selbst im Namen des Benutzers holt, wird mit seinem eigenen Schlüssel verschlüsselt. Hat das Konto keine AES-Schlüssel, scheitert es hier, auch wenn der LoadMaster längst AES anbietet.
- **Falle 3, S4U2Proxy:** Das Service-Ticket für den Real Server wird mit dem Schlüssel des Zielkontos verschlüsselt. Ein uraltes Dienstkonto für die Eigenentwicklung, dessen Kennwort seit 2007 niemand geändert hat, besitzt womöglich gar keinen AES-Schlüssel. Dann ist der LoadMaster unschuldig, aber trotzdem derjenige, der den Fehler meldet.

Wo du den Fehler findest

Am LoadMaster schreibt der SSO-Manager die Kerberos-Kommunikation ins Log, ausführlich erst mit erhöhter Debug-Stufe für ESP. Dort taucht die Meldung sinngemäß als „KDC has no support for encryption type“ auf. Wie du an die Logs kommst, die Debug-Stufe hochdrehst und einen Mitschnitt des Kerberos-Verkehrs zum KDC ziehst, beschreibt [Troubleshooting am LoadMaster: Logs, L7-Debug und TCP-Dump](#). Im TCP-Dump siehst du im AS-REQ die Liste der angebotenen etypes; steht dort nur 23, ist die Sache klar.

Auf der Gegenseite liefern die Domänencontroller die Bestätigung: Ereignis 4768 oder 4769 mit Fehlercode 0xE im Sicherheitsprotokoll, sofern die Überwachung der Kerberos-Authentifizierung und der Kerberos-Dienstticketvorgänge für Fehler aktiviert ist, dazu je nach Phase die KDCSVC-Ereignisse im System-Log. Ältere KDC-Meldungen wie Ereignis 14 oder 16 im System-Log, „das Konto hat keinen passenden Schlüssel“, zeigen dir Falle 2 und 3 besonders deutlich.

Symptom	Wahrscheinliche Ursache	Prüfung
Alle KCD-Anmeldungen scheitern seit dem Patchtag	LoadMaster bietet nur RC4 an (Falle 1)	4768 mit 0xE für den Trusted User, AES-Option am LoadMaster
Nach Aktivieren der AES-Option geht gar nichts mehr	Trusted User hat keine AES-Schlüssel	Datum der letzten Kennwortänderung, msDS-SET am Konto
Ein Virtual Service geht, ein anderer nicht	Zielkonto ohne AES-Schlüssel (Falle 3)	4769 mit 0xE, Dienstkonto des betroffenen Real Servers
Fehler nur an einem Domänencontroller	Härtungs-GPO oder Patchstand uneinheitlich	Reihenfolge der KDCs am LoadMaster, GPO-Ergebnis je DC
Kein Fehler, aber Fallback auf Formular oder NTLM	Anwendung fällt still zurück	Authentifizierungsart am Real Server protokollieren

AUS DER PRAXIS · Die Stadtverwaltung und der Mittwoch nach dem Patchday

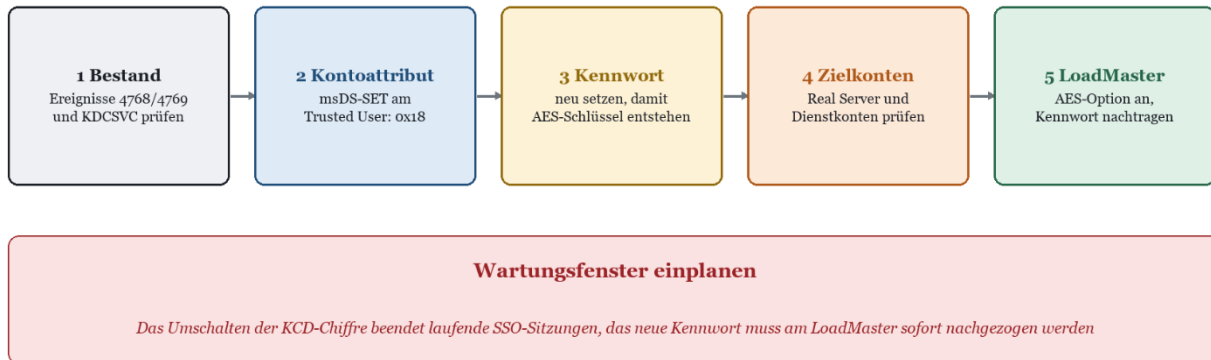
Eine mittelgroße Verwaltung betreibt OWA und ein selbst entwickeltes Antragsportal hinter einem LoadMaster mit ESP und KCD. Am Mittwoch nach dem Aprilpatch melden sich die ersten Kolleginnen und Kollegen aus dem Homeoffice: Anmeldung klappt, danach Fehlerseite. Das Security-Team verweist auf die GPO, die RC4 bereits seit einem Jahr auf den DCs verbietet, und wundert sich, warum es überhaupt je funktioniert hat. Die Antwort: Die GPO war nur auf einem Teil der DCs wirksam, und der LoadMaster hatte zufällig immer einen nicht gehärteten DC als ersten KDC eingetragen. Der Aprilpatch hat dieses Glück beendet. Lösung nach Lehrbuch, Dauer der Umstellung im Wartungsfenster: zwanzig Minuten. Dauer der Ursachensuche: zwei Tage.

Die Kur: AES für Trusted User, Zielkonten und LoadMaster

Die gute Nachricht: Die Umstellung ist technisch trivial. Die schlechte: Sie hat eine Reihenfolge, und wer sie ignoriert, produziert zwischendurch genau den Ausfall, den er vermeiden wollte.

Die Kur in fünf Schritten

Reihenfolge einhalten, sonst behebst du den Fehler zweimal



Skizze: empfohlene Reihenfolge der Umstellung von RC4 auf AES für KCD

Schritt 1 und 2: Bestand prüfen und Verschlüsselungstypen setzen

Zuerst schaust du dir den Trusted User an: Welche Verschlüsselungstypen stehen im Attribut, und wann wurde das Kennwort zuletzt gesetzt? Dasselbe gilt für alle Konten, an die delegiert wird, also Computerkonten der Real Server oder dedizierte Dienstkonten mit HTTP-SPN. Welches Konto zu welchem SPN gehört, klärt [SPN-Probleme hinter dem Load Balancer: ein Name, mehrere Server](#).

```
Get-ADUser svc-lm-kcd -Properties msDS-SupportedEncryptionTypes, pwdLastSet,
PasswordLastSet |
    Select-Object Name, msDS-SupportedEncryptionTypes, PasswordLastSet
```

```
# AES128 und AES256 erlauben, RC4 ausschließen
Set-ADUser svc-lm-kcd -Replace @{msDS-SupportedEncryptionTypes' = 0x18}
```

Alternativ setzt du in Active Directory-Benutzer und -Computer auf der Registerkarte Konto die beiden Haken für AES 128 und AES 256. Das Ergebnis ist dasselbe Attribut mit dem Wert 24.

Schritt 3: Kennwort neu setzen, damit AES-Schlüssel entstehen

Hier liegt der Teil, den fast alle vergessen. Active Directory berechnet die AES-Schlüssel eines Kontos nur in dem Moment, in dem das Kennwort gesetzt wird, und auch nur, wenn die Domäne zu diesem Zeitpunkt mindestens auf der Funktionsebene Windows Server 2008 lief. Ein Trusted User, der 2012 angelegt und damals in einer Domäne mit 2003-Funktionsebene mit Kennwort versorgt wurde, hat schlicht keine AES-Schlüssel. Das Attribut zu ändern erzeugt keine Schlüssel, es verspricht nur, dass es welche gibt. Der KDC glaubt das Versprechen und scheitert dann beim Verschlüsseln.

Die Lösung ist so simpel, dass sie fast beleidigend wirkt: Kennwort neu setzen. Gern auf einen neuen, langen Zufallswert, denn ein Konto mit Protocol Transition ist ein Generalschlüssel. Ob du das Kennwort zweimal setzen solltest, hängt eher an deiner Kennwortrichtlinie als an Kerberos; einmal genügt, damit alle Schlüsseltypen neu berechnet werden. Warte anschließend die AD-Replikation ab oder trage am LoadMaster vorübergehend den DC ein, auf dem du die Änderung gemacht hast.

WARNUNG · Kennwort ändern heißt LoadMaster anfassen

Sobald das neue Kennwort gilt, scheitert der LoadMaster mit dem alten. Plane die Änderung deshalb im selben Wartungsfenster wie die Umstellung am LoadMaster, und trage das neue Kennwort in der serverseitigen SSO-Domäne sofort nach. Im HA-Paar synchronisiert sich die Konfiguration, prüfe es trotzdem auf beiden Einheiten.

Schritt 4: Zielkonten nicht vergessen

Computerkonten sind meist unkritisch, weil Windows ihr Kennwort standardmäßig alle 30 Tage selbst erneuert und dabei AES-Schlüssel erzeugt. Kritisch sind klassische Dienstkonten, unter denen ein IIS-Anwendungspool oder eine Eigenentwicklung läuft. Hat eines davon ein Kennwort aus grauer Vorzeit, bekommt es denselben Dreiklang: Attribut auf 0x18, Kennwort neu setzen, Anwendung mit neuem Kennwort versorgen. Gruppenverwaltete Dienstkonten erledigen den letzten Teil von selbst und sind ohnehin die bessere Wahl.

Schritt 5: AES-Option am LoadMaster aktivieren

Erst jetzt schaltest du in der serverseitigen SSO-Konfiguration mit KCD die Option für AES256 ein, in aktueller Firmware „Use AES256 SHA1 KCD cipher“. Der LoadMaster verwendet dann AES256-CTS-HMAC-SHA1-96, also etype 18, und verzichtet auf RC4 und DES. Laut Kemp fragt die Oberfläche beim Umschalten nach: Mit OK wird die Änderung sofort aktiv, der SSO-Cache geleert und bestehende Sitzungen beendet. Mit Abbrechen wartet der LoadMaster, bis seine Kerberos-Schlüsseltabelle ohnehin abläuft. Im Wartungsfenster nimmst du OK, denn ein Fehler, der irgendwann von allein auftritt, ist das Gegenteil von kontrolliert.

TIPP · Warum AES256 genügt

Die Option am LoadMaster kennt nur AES256 mit SHA1. Das reicht, denn jedes Konto mit neu gesetztem Kennwort besitzt neben dem AES128- auch einen AES256-Schlüssel. Setze am Konto trotzdem 0x18 statt nur 0x10, damit Windows-Clients und andere Dienste das Konto weiterhin mit beiden AES-Varianten ansprechen können.

Erfolgskontrolle

Nach der Umstellung meldest du dich als Testbenutzer an und prüfst drei Dinge: Die Anwendung öffnet sich ohne zweite Kennwortabfrage, im Sicherheitsprotokoll der DCs erscheinen 4768 und 4769 für den Trusted User mit Ticketverschlüsselungstyp 0x12, und auf dem Real Server zeigt das Anmeldeereignis 4624 Kerberos als Authentifizierungspaket. Ist das der Fall, kannst du die Härtungs-GPO auf allen DCs in Ruhe durchziehen. Taucht stattdessen NTLM auf, hat die Anwendung still auf ein anderes Verfahren umgeschaltet, und das ist ein eigenes Kapitel.

Baustein	Vorher (RC4-Falle)	Nachher (AES)
Option am LoadMaster	nicht gesetzt, RC4	Use AES256 SHA1 KCD cipher aktiv
msDS-SET Trusted User	leer oder 0x4	0x18
Kennwort Trusted User	uralt, nur RC4-Schlüssel	neu gesetzt, AES-Schlüssel vorhanden
Zielkonten	teils ohne AES-Schlüssel	0x18, Kennwort erneuert oder gMSA
Ticketverschlüsselung in 4769	0x17	0x12
Abhängigkeit von RC4-Ausnahmen	DefaultDomainSupportedEncTypes oder 0x24	keine

FAQ: kemp kcd aes und die RC4-Falle

Warum hat KCD jahrelang funktioniert, obwohl RC4 schon unsicher war?

Weil Active Directory RC4 für Konten ohne gesetzte Verschlüsselungstypen still als Standard akzeptiert hat. Erst Härtungs-GPOs auf den DCs oder die Microsoft-Updates ab April 2026 haben diesen Standard auf AES-SHA1 umgestellt.

Reicht es, die AES-Option am LoadMaster zu setzen?

Nur, wenn der Trusted User bereits AES-Schlüssel besitzt. Fehlen sie, tauschst du den Fehler RC4 nicht erlaubt gegen den Fehler AES nicht vorhanden. Deshalb gehören Kontoattribut und Kennwortänderung zur Umstellung dazu.

Muss ich das Kennwort des Trusted Users wirklich ändern?

Wenn es gesetzt wurde, bevor die Domäne auf der Funktionsebene Windows Server 2008 oder höher lief, ja. Im Zweifel ja, denn eine Kennwortänderung schadet nicht und beseitigt die Unsicherheit. Vergiss nicht, das neue Kennwort am LoadMaster einzutragen.

Kann ich RC4 für den LoadMaster einfach wieder erlauben?

Technisch ja, über 0x24 oder 0x1C am Konto oder über DefaultDomainSupportedEncTypes auf den DCs. Sinnvoll ist es nicht, denn der LoadMaster beherrscht AES. Jede RC4-Ausnahme hält genau die Schwachstelle offen, die Microsoft mit CVE-2026-20833 schließen will.

Beendet das Umschalten der Chiffre laufende Sitzungen?

Ja, wenn du die Rückfrage mit OK bestätigst. Dann wird der SSO-Cache geleert. Plane die Umstellung deshalb in einem Wartungsfenster und informiere die Benutzer, dass sie sich einmal neu anmelden müssen.

Betrifft das auch RBCD?

Ja. Bei ressourcenbasierter Delegation ändert sich nur, wo die Erlaubnis gespeichert ist, nicht die Verschlüsselung der Tickets. Trusted User und Zielkonten brauchen auch dort AES-Schlüssel, und der LoadMaster braucht die AES-Option.

Was ist, wenn meine Firmware die Option nicht anbietet?

Dann ist sie älter als 7.2.48, und ein Firmware-Update ist Pflicht. Eine dauerhafte RC4-Ausnahme ist in einer gepatchten Domäne keine tragfähige Alternative.

Fazit: ein Häkchen, ein Attribut, ein Kennwort

Die RC4-Falle ist kein Fehler im LoadMaster und keiner in Active Directory. Sie ist das Ergebnis zweier Standardwerte, die jahrelang gut zusammengepasst haben und es seit 2026 nicht mehr tun. Der LoadMaster bietet ohne Zutun RC4 an, die Domäne nimmt nur noch AES. Wer die Lücke schließen will, braucht drei Dinge: die AES-Option am LoadMaster, AES-Verschlüsselungstypen am Trusted User und an den Zielkonten und ein frisch gesetztes Kennwort, damit die versprochenen Schlüssel auch existieren. In der richtigen Reihenfolge und im Wartungsfenster ist das eine Sache von Minuten.

Schwarzhumorig betrachtet hat die Falle sogar etwas Gutes: Sie zwingt dich, das mächtigste Konto deines LoadMasters endlich einmal anzusehen, sein Kennwort zu erneuern und zu dokumentieren, wohin es delegieren darf. Mehr über die Kerberos-Grundlagen, von Verschlüsselungstypen bis zur Ticketstruktur, findest du im Bereich [Microsoft Kerberos](#).

TIPP · Unterstützung bei Härtung und Umstellung

Wenn du die RC4-Abschaltung domänenweit planst und sichergehen willst, dass LoadMaster,

Dienstkonten und Delegationen mitziehen, hilft dir die [Beratung zum Kemp LoadMaster](#). Wer KCD, Verschlüsselungstypen und ESP mit dem eigenen Team im Labor durchspielen möchte, findet das in der [Kemp-LoadMaster-Schulung](#).

WEITERLESEN • Weiter im Thema

- › [Kerberos Constrained Delegation am LoadMaster: KCD und RBCD sauber einrichten](#)
- › [Troubleshooting am LoadMaster: Logs, L7-Debug und TCP-Dump](#)
- › [SPN-Probleme hinter dem Load Balancer: ein Name, mehrere Server](#)
- › [Microsoft Kerberos](#)