ManageEngine
ADAudit Plus

Kontensperrungen **verstehen** und **auflösen:**

Inhalt

Kontosperrungen bedürfen keiner weiteren Erläuterung … Ständige Helpdeskanrufe wegen dieses überwältigend verbreiteten Problems bereiten den meisten Technikern wahre Albträume. Die Quelle einer Kontosperrung herauszufinden, um damit das eigentliche Problem an der Wurzel zu packen, ist eine Herausforderung, der sich Administratoren und Helpdesktechnikern immer wieder gegenübersehen. Eine zuverlässige Entschleierung dieses Mysteriums, die zum nachhaltigen Versiegen permanenter Kontofreischaltungsanfragen führte, käme einem Eldorado gleich. Kontosperrungen können sich sehr negativ auf Sicherheit, Produktivität und Finanzen eines Unternehmens auswirken. In diesem E-Book beleuchten wir unterschiedliche Auswirkungsweisen von Kontosperrungen auf Organisationen. Und natürlich auch, wie man damit am besten umgeht.

Die geschäftlichen Auswirkungen von Kontensperrungen

*Kontosperrungen und Kennwortrücksetzungen machen bis zu **30 %** sämtlicher Helpdeskanfragen aus.*

- Gartner

Kontosperrungen zählen zu den wohl frustrierendsten Aufgaben, mit denen Helpdesktechniker oder Administratoren viel zu häufig konfrontiert werden. In den Stunden, die gewöhnlich vom Aufspüren der Sperrungsursache bis zur endgültigen Lösung vergehen, erfahren Administratoren und Helpdesktechniker aus erster Hand, welche Zeit- und Energieverschwendungen daraus erwachsen. Nicht selten zeigen sich auch die geschäftlichen Auswirkungen von Kontensperrungen als ernst genug, nicht nur Zeit und Geld zu verschwenden, sondern auch dem guten Ruf zu schaden.

Produktivitätsverluste

Bei zahlreichen Helpdeskanrufen rund um Kontosperrungen büßen sowohl Administratoren und Techniker als auch betroffene Anwender reichlich an Produktivität ein. Angenommen, die Auflösung einer einzigen Sperrung wäre in einer Stunde erledigt, würde dies das Unternehmen bereits zwei Arbeitsstunden kosten, zuzüglich der damit verbundenen Leerlaufzeit des ausgesperrten Anwenders. Zum mühsamen Ablauf zählen das Herausfinden der Kontosperrungsursache, Freischalten des Kontos, Ändern des Anwenderkennwortes, Aktualisieren des neuen Kennwortes bei sämtlichen Diensten, die mit dem Anwenderkonto zu tun haben, obendrein Ausschluss eines möglichen Cyberangriffs. Neben der verschwendeten Zeit kann sich dieser Ablauf auch mit gehörigen Kosten in den Büchern des Unternehmens auswirken.

Auswirkungen auf den Ertrag

Laut Gartner liegen die geschätzten Begleitkosten einer einzigen Kontosperrung bei rund 50 bis 100 $. Wenn ein reguläres Nutzerkonto entsperrt wird, ist es gewöhnlich mit der Entsperrung und einer Rücksetzung des Kennwortes getan. Wenn es sich allerdings um ein Dienstkonto handelt, braucht es Lösungen, die weit über eine einfache Kennwortänderung hinausreichen. Falls Systeme der Abteilungen ausfallen, die auf den Zugangsdaten des Dienstkontos beruhen, können sich die negativen Auswirkungen dieser Ausfallzeit auf die gesamte Organisation ausdehnen. Falls der Dienst beispielsweise mit Kundenkontakten zu tun hat, kann der Ausfall die Organisation in erster Linie ihren guten Ruf, in zweiter Linie auch unweigerlich Geld kosten.

Angriffe und potentielle Bedrohungen

Kontensperrungen können Anzeichen verdeckter Angriffsversuche auf das Netzwerk sein. Bei Sperrungen als Folge eines Brute-Force-Angriffs: Wenn die Sperrdauer in Active Directory zu niedrig (z. B. auf 30 Minuten) eingestellt ist, die Sperrung zu spät erkannt wird (vielleicht erst nach 90 Minuten oder später), kann der Hacker bereits lange mit einem fröhlichen Lied auf den Lippen sein Unwesen im Netzwerk treiben. Eine kürzere Sperrdauer verbessert die Erfolgschancen eines Angreifers. Angreifer können auch DoS-Angriffe ausführen, dabei die Dienstausfallzeit in Folge einer Sperrung ausnutzen.

Permanente Sperrungen, die von einer erfolgreichen Anmeldung abgelöst werden, können auf einen erfolgreichen Versuch zum Hacken eines Nutzerkontos hindeuten. Eine einfache Auflösung der Sperre brächte in diesem Fall keine Besserung – weitere abweichende Aktivitäten desselben Nutzers müssen auf weitere Muster analysiert werden, die Anzeichen einer Sicherheitslücke sein können. Ein Beispiel: Kontosperrung, anschließend erfolgreiche Anmeldung, gefolgt von Dateilöschungen im großen Stil.

Kontosperrungen sind mittlerweile weit mehr als lediglich ein administratives Problem. Sperrungen müssen sorgfältig analysiert werden, damit potentielle Bedrohungen des Organisationsnetzwerkes nicht unter das Radar fallen. Hier eine Aufzählung mit möglichen Ursachen von Kontosperrungen, die bei Analysen berücksichtigt werden müssen:

Gängige Ursachen von Kontensperrungen

Versuchter Angriff

Ein einfacher Brute-Force- oder DoS-Angriff kann die Ursache wiederholter Kontensperrungen sein. Der Angreifer wartet das Ende der Sperrdauer ab, versucht es anschließend erneut. Daher ist es unerlässlich, den Ursachen der Sperrung unverzüglich auf den Grund zu gehen. Falls wiederholte Sperrungen eines Kontos auftreten, denen eine erfolgreiche Anmeldung folgt, müssen Sie die Aktivitäten des betroffenen Nutzers analysieren und sicherstellen, dass nichts gehackt wurde. Zum Eindringen in ein Netzwerk und zur vollen Kontrollübernahme genügt es oft, lediglich ein einzelnes Konto zu hacken. Daher muss jede Sperrung sorgfältig analysiert werden.

Verwaiste Kennwörter

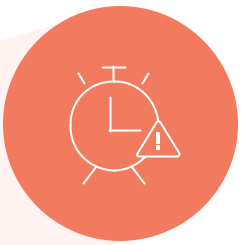
Wenn Kennwortänderungen eines Nutzerkontos nicht über die gesamte Domäne repliziert werden, können solche verwaisten Kennwörter zu Kontensperrungen führen. Dienste, die mit den Zugangsdaten des jeweiligen Kontos arbeiten, erwarten eventuell nach wie vor das alte Kennwort. Dies wiederum führt zu Authentifizierungsfehlschlägen und Aussperrungen. Administratoren und Techniker müssen Applikationen und Windows-Komponenten wie Outlook Web App (OWA), Active Sync, Windows-Hintergrunddienste, COM-Objekte (prozessübergreifende Kommunikation) und verknüpfte Netzwerklaufwerke auf verwaiste Kennwörter überprüfen. Auch geplante Aufgaben können auf zwischengespeicherte Zugangsdaten zurückgreifen, die im Rahmen der Replikation nicht aktualisiert wurden.

Unterlassen der Kennwortaktualisierung im Dienststeuerungsmanager

Der Dienststeuerungsmanager (auch „Dienststeuerungs-Manager“) speichert Dienstkontenkennwörter auf Computern zwischen, die mit dem Dienst arbeiten. Wenn Dienstkontenkennwörter geändert werden, wird das zwischengespeicherte Kennwort eventuell nicht bei diesen Computern aktualisiert, was zu einer Aussperrung führt. Administratoren und Helpdesktechniker müssen nach Mustern fehlgeschlagener Anmeldungen in den Protokolldateien des AD-Anmeldungsdienstes und in den Ereignisprotokolldateien der Mitgliedsserver suchen. Auch der Dienststeuerungsmanager muss zum Einsatz des neuen Kennwortes umkonfiguriert werden.

An mehreren Computern angemeldete Nutzer

Nutzer können sich durchaus an mehreren Computern gleichzeitig anmelden, dabei über Programme dieser Computer mit ihren Zugangsdaten auf Netzwerkressourcen zugreifen. Wenn Nutzer ihre Kennwörter ändern, arbeiten aktive Sitzungen anderer Computer eventuell weiterhin mit dem alten Kennwort. Eine Möglichkeit zum Umschiffen dieser Situation besteht für Administratoren und Helpdesktechniker darin, sämtliche aktiven Sitzungen eines Nutzers auf anderen Geräten/bei anderen Anwendungen zu beenden, wenn das Kennwort geändert wird, anschließend zur erneuten Anmeldung auffordern.



Falsche Alarme

Falls der Sperrschwellenwert zu niedrig eingestellt wird, kann dies zu falschen Alarmen führen. Ein optimaler Sperrschwellenwert liegt bei 10 bis 20 fehlgeschlagenen Versuchen. Falsche Alarme verschwenden Zeit, behindern die Produktivität und können im Endeffekt dazu führen, dass tatsächliche Bedrohungen übersehen werden. Ein dynamischer Schwellenwert, der auf dem individuellen Nutzerverhalten beruht, ist sehr empfehlenswert.

Wieder jemand, der sich nichts merken kann!

Die häufigste Ursache liegt darin, dass ein Kennwort schlicht und einfach vergessen wurde. Die meisten Sperrungen passieren nach Feiertagen, Wochenenden oder Urlauben, wenn Kennwörter schlicht vergessen wurden, das Konto nach einigen Fehlversuchen gesperrt wird. Obwohl auch diese Sperrungsursache frustrierend ist, können Administratoren und Techniker aufatmen – denn dies bedeutet, dass das Netzwerk sicher ist, das Problem lediglich in der Vergesslichkeit des jeweiligen Anwenders liegt.

Kontosperrungen auflösen

Prüfen Sie zum Lokalisieren der Quelle Ihre Ereignisprotokolle auf Sperrungen. Schauen Sie nach folgenden Ereignissen:

- 4740 – Ein Benutzerkonto wurde gesperrt.
- 4767 – Die Sperrung eines Benutzerkontos wurde aufgehoben.
- 4625 – Anmeldungsfehler durch unbekannten Benutzernamen oder falsches Kennwort.
- 4793 – Die Kennwortrichtlinienprüfungs-API wurde aufgerufen.
- 4776 – Der Domänencontroller hat versucht, die Anmeldeinformationen für ein Konto zu bestätigen.
- 4471 – Fehler bei der Kerberos-Vorauthentifizierung.
- 4739 – Domänenrichtlinien geändert: Änderungen von Kontosperrungs- und Kennwortrichtlinien.

Analysen der obigen Ereignisse und mehr, um den Ursachen von Kontosperrungen auf die Schliche zu kommen, ist nicht selten ein gewaltiges – und mit den von Microsoft angebotenen nativen AD-Werkzeugen ein nahezu unmögliches Vorhaben. Dies liegt daran:

Durcheinander bei nativen Werkzeugen

Im Falle eines Angriffes kann der Hacker nach Ablauf der Sperrdauer gleich einen neuen Angriff ansetzen; in vielen Fällen noch bevor dem Nutzer aufgeht, dass sein Konto gesperrt wurde. Wenn es zu spät ist, erweist sich der Angriff als erfolgreich, der Angreifer ist ins Netzwerk eingedrungen. Die schier unüberschaubare Vielzahl von Protokolleinträgen trägt auch nicht unbedingt zum einfachen Auffinden verdächtiger Kontensperrungen bei; vor allem, wenn die Zeit läuft. Der Anwender ist eventuell an mehreren Computern, Diensten und Externverbindungen angemeldet, es kann ein gutes (oder eher schlechtes) Weilchen dauern, bis Administratoren oder Techniker die Quelle einer Sperrung in der Sintflut der Protokolleinträge auffinden.

Mangelnder Speicherplatz

Bei der Windows-Ereignisanzeige ist der Speicher auf 4 GB begrenzt. Daher kann es an der Tagesordnung sein, dass Sperrungen unbemerkt auftreten, entsprechende Einträge bald wieder aus dem Protokoll entschwinden. Nicht selten kommt es vor, dass zur Analyse und Nachforschung benötigte Protokolle schon lange verschwunden sind oder noch im Zuge der Nachforschung überschrieben werden. Dies macht es Technikern unmöglich, die Ursache einer Sperrung herauszufinden. Technikern bleibt nur noch übrig, das Kennwort des Nutzers rückzusetzen, anschließend jede einzelne Komponente im Auge zu behalten, bis sie – womöglich durch Zufall – auf die Richtige stoßen. Auch Daten zu letzten Nutzeranmeldungen erweisen sich bei Analysen häufig als hilfreich. Solche Aktivitäten lassen sich korrelieren, um Rückschlüsse auf das Anmeldungsverhalten zu ziehen. Allerdings fehlt es zur effizienten Analyse oft an ausreichend vielen Anmeldungsereignissen.

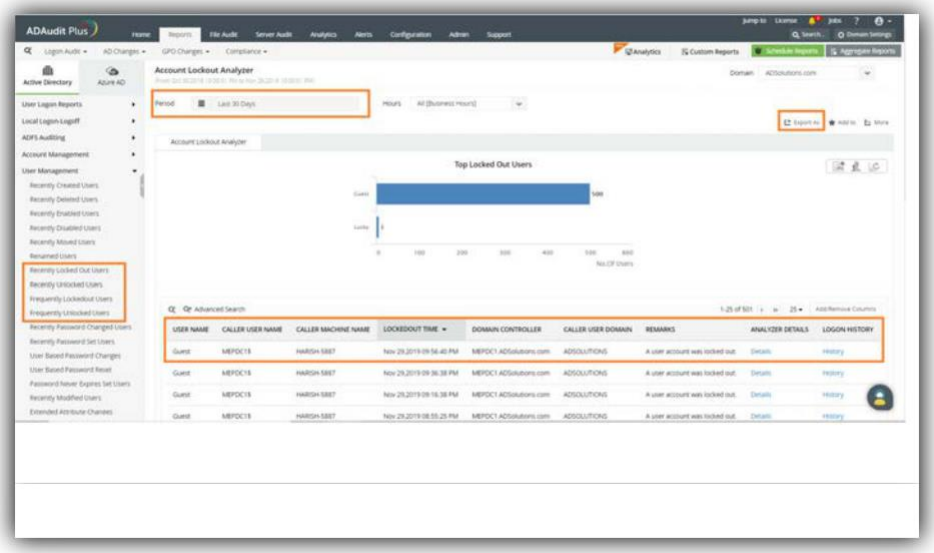
Oder etwas schonungsloser ausgedrückt: Native AD-Werkzeuge haben nicht das Zeug, das es zum schnellen und effektiven Auflösen von Kontosperrungen braucht.

Kontosperrungsanalyse leicht gemacht

ManageEngines ADAudit Plus bietet einen Kontosperrungsanalysator mit allem, was Sie wirklich brauchen. Mit kontinuierlicher Überwachung, Protokollsammlung in Echtzeit, adretten Berichten mit sämtlichen nötigen Informationen, die es zu einer lückenlosen Kontosperrungsanalyse braucht.

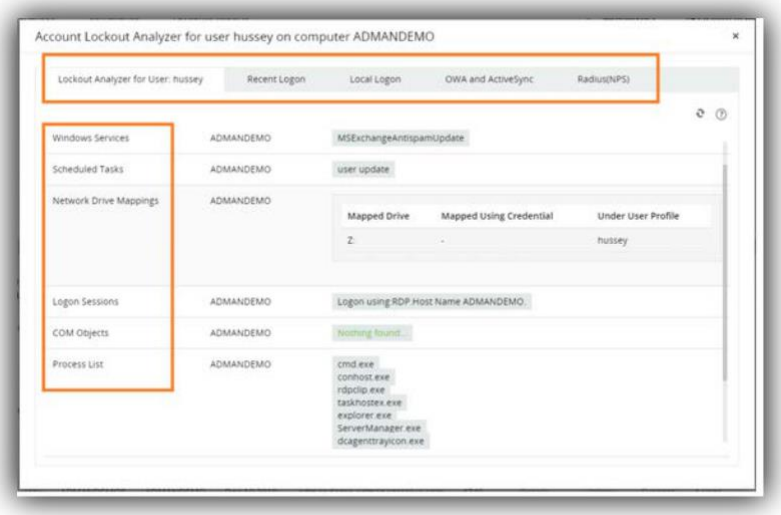
Dazu zählen:

- Das Wer, Wann, Wo und Warum jeder einzelnen Kontosperrung. Die Berichte werden in Echtzeit zusammengestellt, lassen sich in Formaten wie CSV, PDF, XML und HTML exportieren. Ein einfacher Klick ist alles, was es zum Abruf vollständiger Details zu jeder Sperrung braucht, die im festgelegten Zeitraum erfolgte. Mit Hilfe dieser Informationen ersparen Sie sich stundenlanges Herausfiltern von Ereignissen aus der Ereignisanzeige und langwieriges Eintippen komplexer PowerShell-Skripte.

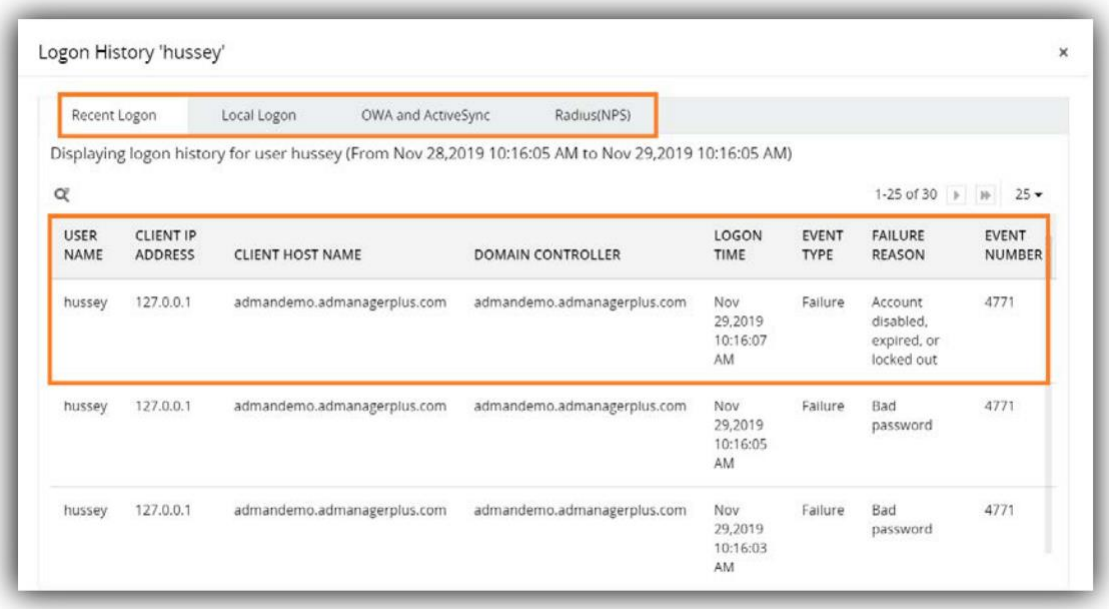


- Details zu sämtlichen Diensten und Windows-Komponenten, die auf die Nutzerzugangsdaten (oder „Anmeldeinformationen“) zurückgreifen.

  Auf diese Weise lässt sich der Ursprung verwaister Kennwörter in nur wenigen Sekunden herausfinden.



- Kürzlicher Anmeldungsverlauf des Nutzers; nützlich zum Entschlüsseln der Kontensperrungsursache. Durch Korrelieren des Anmeldungsverlaufes können Administratoren und Helpdesktechniker potentielle Bedrohungen bei verdächtigen Anmeldungen erkennen.



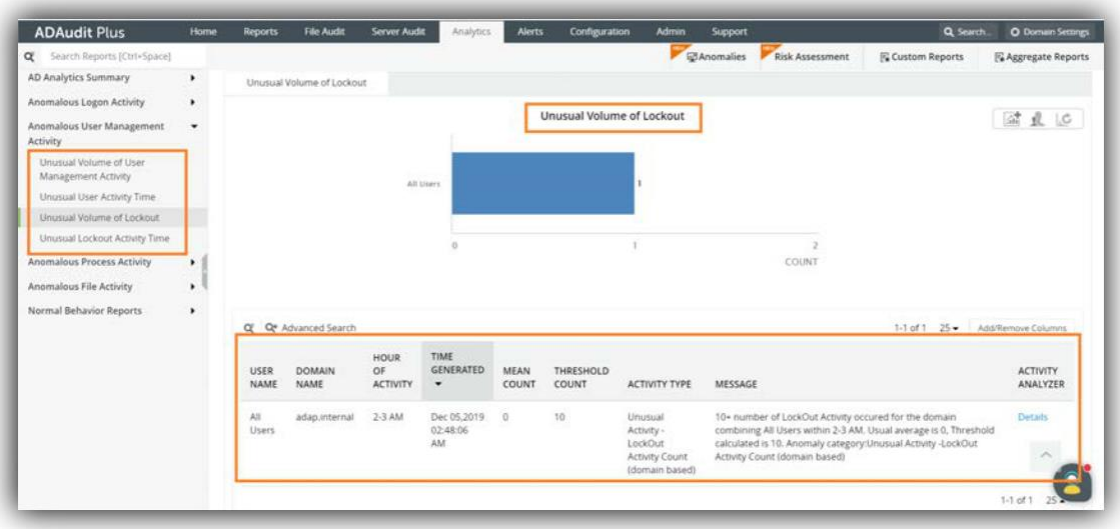
- Sofortige Alarmierungen bei Aussperrungen privilegierter Nutzer oder wenn die Anzahl der Aussperrungen über die Ufer tritt. Solche Alarmierungen können direkt an die E-Mail-Adresse des Administrators oder Technikerapps gesendet werden, auch telefonisch mit ADAudit Plus.

Um Administratoren und Technikern ein besseres Verständnis des Kontensperrungsstatus Ihrer Domäne zu vermitteln, bietet ADAudit Plus zahlreiche Berichte. Unter anderem:

- Kürzlich ausgesperrte Nutzer
- Häufig ausgesperrte Nutzer
- Kürzlich entsperrte Benutzer
- Häufig entsperrte Nutzer

Diese Berichte listen gesperrte Nutzerkonten auf, nennen zusätzlich wichtige Details wie Uhrzeiten und Domänencontroller, von denen die Sperrung ausging. Mit Unterstützung solcher Berichte können Administratoren häufig gesperrte Nutzerkonten einfach und bequem im Auge behalten. Wenn Administratoren oder Helpdesktechniker im Rahmen einer Nachforschung herausfinden müssen, welche Nutzerkonten beim Eindringen eines Angreifers kompromittiert wurden, erweist sich ein Blick auf kürzlich gesperrte Nutzerkonten oftmals als goldrichtig.

Das Nutzerverhaltensanalyse-Modul von ADAudit Plus setzt maschinelles Lernen zum Erkennen verdächtiger Häufigkeiten oder Zeitspannen von Anmeldungsaktivitäten unter Berücksichtigung dynamischer Schwellenwerte ein.



Lassen Sie es nicht bei der Kontosperrungsanalyse bewenden. Mit diesen ADAudit-Plus-Funktionen stärken Sie Ihre AD-Sicherheit aus jedem Blickwinkel:

- Kontinuierliche Echtzeitanalyse sämtlicher Veränderungen Ihrer Domäne.
- Konsolidierte Konformitätsberichte
- Direkt per E-Mail oder ans Smartphone gesendete Echtzeitalarmierungen
- Lückenlose Nutzeranmeldungsüberwachung
- Überwachung sämtlicher Server einschließlich NetApp-Clustern und EMC-Servern Datenintegritätsschutz

ManageEngine
ADAudit Plus

ManageEngine ADAudit Plus ist eine leistungsstarke IT-Sicherheits- und -Konformitätslösung. Mit mehr als 200 ereignisspezifischen Berichten und Echtzeitalarmierungen bietet die Lösung tiefgehende Einblicke in Änderungen an Inhalten und Konfigurationen von Active Directory, Azure AD und Windows-Servern. Zusätzlich ermöglicht die Software gründliche Zugriffaufklärung bei Workstations und Dateiservern (einschließlich NetApp und EMC).

Wenn Sie erfahren möchten, wie Ihnen ADAudit Plus bei Ihrem gesamten Active-Directory-Überwachungsbedarf tatkräftig unter die Arme greift, schauen Sie einmal hier vorbei:

https://www.manageengine.com/products/active-directory-audit/

$ Get Quote ⬇ Download