Fünf Tipps zum Active Directory

Die Arbeit am Active Directory (AD) ist bisweilen recht komplex. Mit diesen Tipps rund um die AD-Lösungen von ManageEngine können IT-Mitarbeiter den Windows-Verzeichnisdienst noch effektiver nutzen.

TEXT: Daniel Seifert

Mit den von Microsoft bereitgestellten Bordmitteln lassen sich viele Monitoring- und Reporting-Aufgaben im Active Directory nicht oder oftmals nur umständlich bewerkstelligen. Deutlich einfacher geht es mit speziellen Management-Lösungen wie ADAudit Plus oder ADManager Plus von ManageEngine. Die folgende Auswahl an Tipps zeigt, wie umfassend die Möglichkeiten der Lösungen sind – und wie IT-Administratoren ganz konkret vom Einsatz dieser Lösungen profitieren können:

1. Ablaufdatum von User-Accounts überwachen

Ob Praktikant, Aushilfe oder Berater: Viele Benutzer-Accounts werden nur für einen bestimmten Zeitraum benötigt. Um sicherzustellen, dass der Zugang des jeweiligen Mitarbeiters nach Ablauf seiner Tätigkeit für das Unternehmen zuverlässig und unverzüglich gesperrt wird, lassen sich User-Accounts im Active Directory mit einem Ablaufdatum versehen.

Trotzdem sollten Administratoren zeitlich befristete Accounts im Blick behalten und nicht mehr benötigte Konten regelmäßig löschen, um die Angriffsfläche für Hacker so gering wie möglich zu halten. Mit den von Microsoft bereitgestellten AD-Werkzeugen ist das Aufspüren abgelaufener Accounts allerdings mühsam und zeitaufwändig.

Deutlich einfacher und schneller klappt es mit ADManager Plus von ManageEngine: Die Lösung enthält zahlreiche vorkonfigurierte Berichte, die IT-Teams bei Bedarf individuell anpassen können. Einer davon ist der „All Users Report", der sich quasi per Knopfdruck erstellen und – sofern gewünscht – auch ausdrucken lässt. Im Report sind zunächst die Attribute aller AD-User aufgelistet. Mit wenigen Klicks kann der Administrator anschließend die Spalten auswählen, die angezeigt werden sollen. Im konkreten Beispiel wären das „Account Name" sowie „Account Expiry Time" – und schon zeigt ADManager Plus eine Übersicht an, welches Konto wann abläuft.

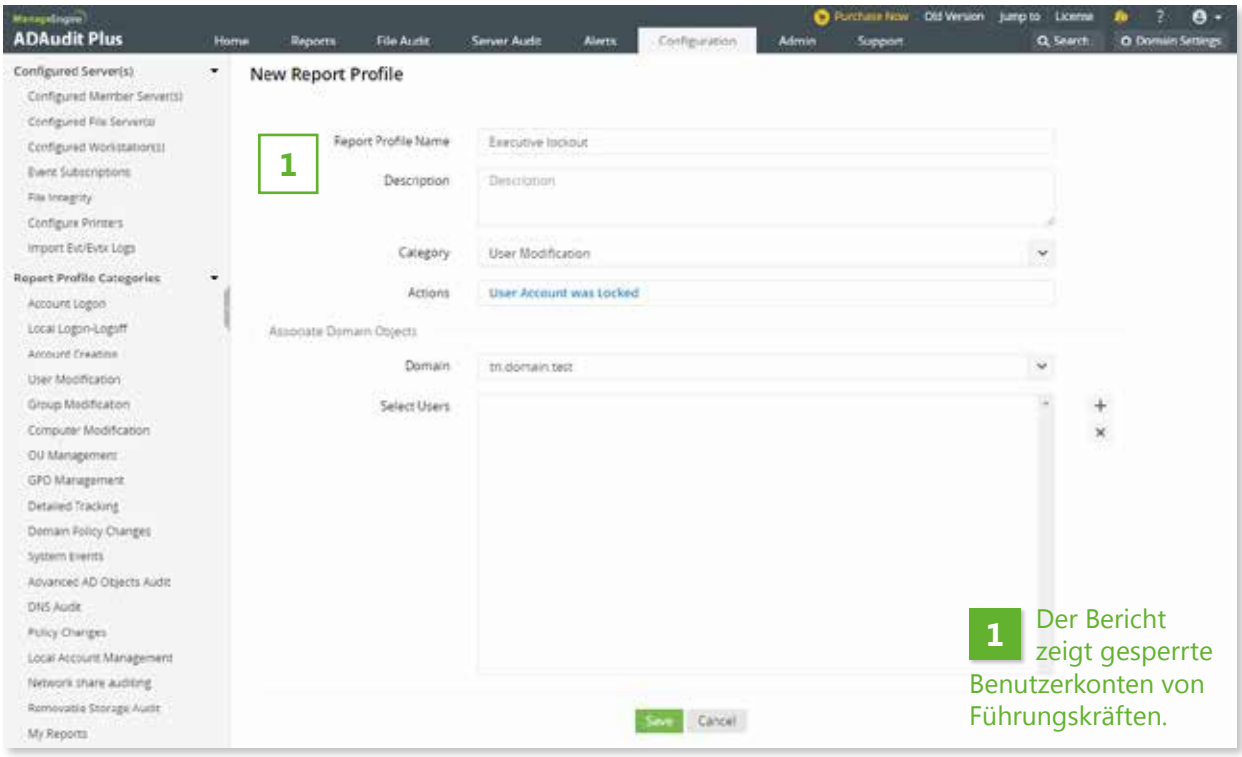
Übrigens: ADManager Plus bietet neben einer Komplettübersicht aller Accounts auch den vorkonfigurierten Bericht „Account Expired Users". Dieser enthält nur die Benutzerkonten, die bereits abgelaufen sind.

2. Autom. Benachrichtigung, wenn sich der Chef aussperrt

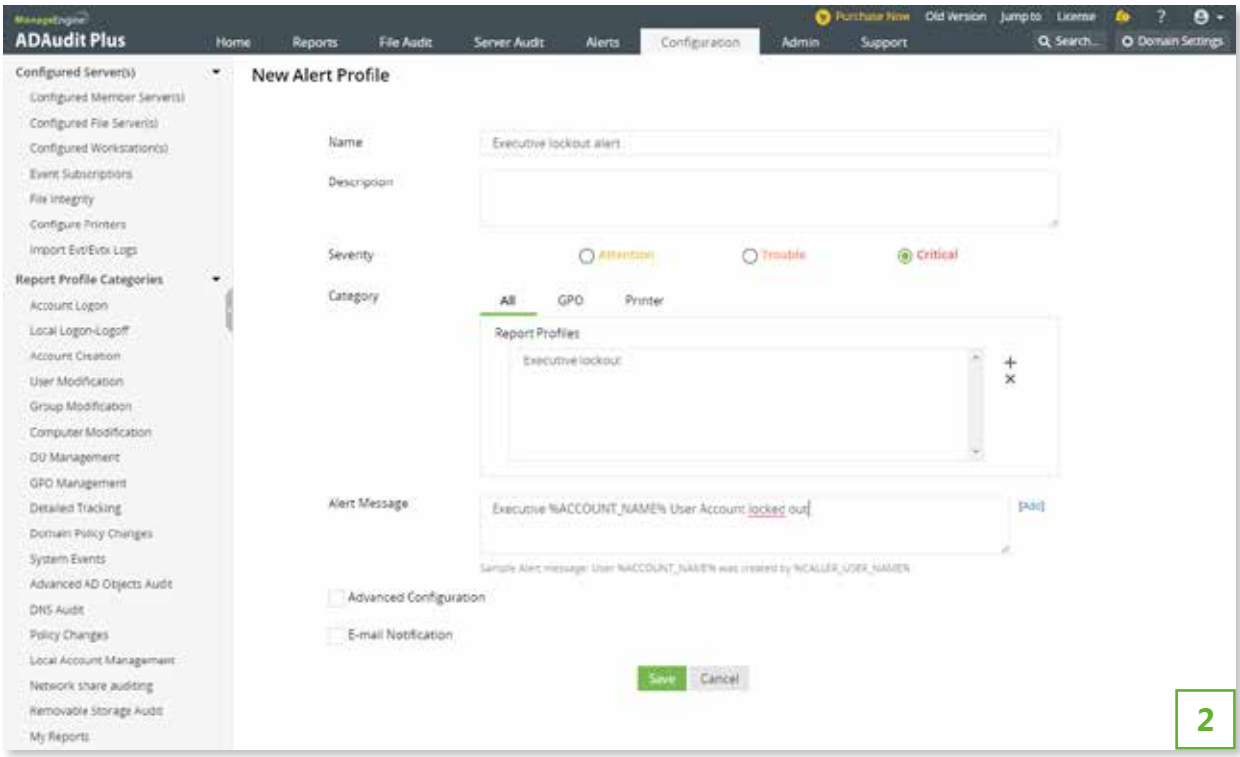
Ein Anruf vom Vorstandsvorsitzenden oder Geschäftsführer, der sich nicht in seinen Benutzer-Account einloggen kann: auf diese Erfahrung würden die meisten Helpdesk-Mitarbeiter wahrscheinlich gerne verzichten. Da Führungskräfte Budget- und Mitarbeiterverantwortung innehaben, ist es für sie besonders wichtig, dass sie zuverlässig Zugang zu allen erforderlichen Daten und Informationen haben – mit entsprechender Priorisierung durch die IT.

Statt in solchen Fällen nur reagieren zu können, ermöglicht ADAudit Plus IT-Abteilungen ein aktives Vorgehen: Ein schnell eingerichteter, benutzerdefinierter Alarm informiert die Administratoren automatisch, sobald ein Benutzerkonto gesperrt wurde (siehe Textkasten). So lässt sich der betroffene Account meist zurücksetzen, bevor die Führungskraft überhaupt bemerkt, dass das gewohnte Login nicht mehr funktioniert.

Hier noch ein Zusatztipp: Mit ADAudit Plus lassen sich für nahezu alle Änderungen an AD-Objekten Alarme einrichten. Da der Administrator dabei genau festlegen kann, welche Anwender, Gruppen oder Organisationseinheiten (OU) beobachtet werden sollen, erhält er nur die Informationen, die er wirklich benötigt.



1 Der Bericht zeigt gesperrte Benutzerkonten von Führungskräften.



2 In Kombination mit dem Report in Abbildung 1 informiert der Alarm den Administrator umgehend, falls der User-Account einer Führungskraft gesperrt wird.

Alarmierung bei Sperrung von Executive-Accounts

Zur Einrichtung des Alarms sind in ADAudit Plus lediglich zwei Schritte erforderlich:

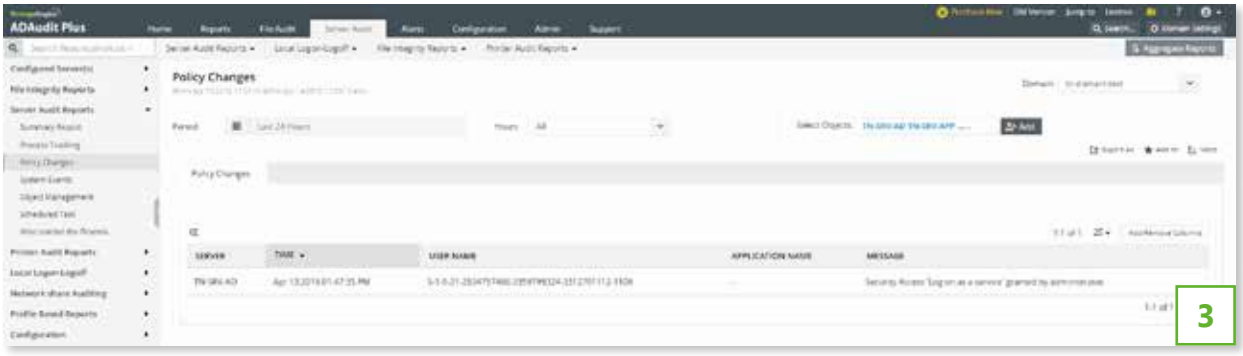
» **Benutzerdefinierten Report erstellen:** Legen Sie im Bereich „Configuration" einen neuen Report an und vergeben Sie einen Namen. Wählen Sie als Kategorie „User Modification" und als Aktion „User Account was locked" aus. Anschließend wählen Sie die für Sie relevanten Anwender, Gruppen oder Organisationseinheiten (OU) aus.

» **Verknüpfung mit einem benutzerdefinierten Alarm:** Anschließend erstellen Sie einen neuen Alert, vergeben einen Namen und verknüpfen diesen mit dem gerade angelegten Report. Bei Bedarf können Sie im Feld „Alert Message" einen individuellen Nachrichtentext einfügen, der im Alarm angezeigt werden soll. Zum Schluss können Sie noch auswählen, ob der Alarm nur auf dem Dashboard von ADAudit angezeigt oder auch per E-Mail versendet werden soll.

3. Benutzerrechte auf Windows-Servern sichern

Auf jedem Windows-Server lassen sich mehr als 35 verschiedene Benutzerrechte einstellen beziehungsweise konfigurieren. Angesichts dieser Vielzahl an Möglichkeiten ist es für Administratoren hilfreich, genau zu wissen, welche davon bei einer Beeinträchtigung die größten Auswirkungen auf den Geschäftsbetrieb haben.

Das lässt sich folgendermaßen herausfinden: Zunächst kann sich der Administrator für jeden Server eine Liste mit den aktuellen Benutzerrechten anzeigen lassen. Dazu gibt es verschiedene Möglichkeiten, eine davon ist die Eingabe des Befehls „Secpol.msc" im Menü „Ausführen". Dadurch wird eine Liste der lokalen Sicherheitsrichtlinien angezeigt, inklusive aller auf dem Server konfigurierten User-Rechte. Per Rechtsklick auf den Knoten „User Rights Assignments" lässt sich die Übersicht schließlich als Liste exportieren und abspeichern.



3 Der Report „Policy Changes" in ADAudit Plus zeigt alle Änderungen an Benutzerrechten an.

Obwohl alle Benutzerrechte wichtig sind, scheinen – so die Erfahrung des Active-Directory-Experten Derek Melber – folgende besonders große Auswirklungen auf den Server zu haben:

- Herunterfahren des Systems
- Erzwungenes Herunterfahrens von einem Remote-System aus
- Anmelden als Stapelverarbeitungsauftrag
- Anmelden als Dienst
- Lokal anmelden zulassen
- Als Teil des Betriebssystem handeln
- Wiederherstellen von Dateien und Verzeichnissen
- Für Delegierungszwecke vertrauen
- Sicherheitsüberprüfung generieren
- Laden und Entfernen von Gerätetreibern
- Verwalten von Überwachungs- und Sicherheitsprotokollen
- Prozessebenen-Token ersetzen
- Synchronisieren von Verzeichnisdienstdaten
- Übernehmen des Besitzes von Dateien und Objekten

Daher ist es für Administratoren empfehlenswert, eben diese Punkte im nächsten Schritt auf jedem einzelnen Server genau unter die Lupe zu nehmen und korrekt zu konfigurieren – gefolgt von den übrigen Benutzerrechten. Damit ist der größte Teil der Aufgabe bereits erledigt und eine gute Ausgangsbasis in Punkto Sicherheit geschaffen. Anschließend gilt es lediglich, den Status Quo aufrecht zu erhalten beziehungsweise Änderungen zu überwachen. Dabei helfen beispielsweise die im nächsten Tipp vorgestellten Reports in ADAudit Plus.

4. Änderungen von Benutzerrechten überwachen

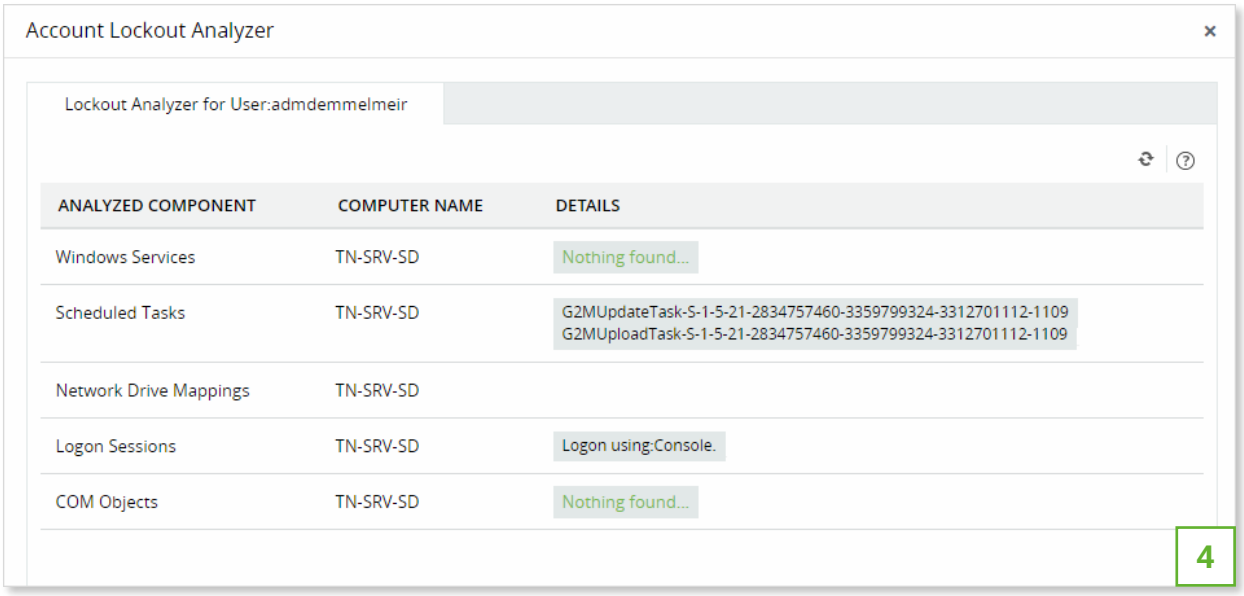
Prinzipiell gibt es zwei Möglichkeiten, wie sich Benutzerrechte auf einem Windows-Server ändern lassen: Zum einen kann das Anlegen eines Gruppenrichtlinienobjekts (Group Policy Object (GPO)) Auswirkungen auf die User-Rechte auf einzelnen oder mehreren Servern haben. Zum anderen kontrolliert der lokale Administrator eines Servers fast jede Einstellung – und kann sie folglich auch ändern.

Um sicherzustellen, dass die korrekt konfigurierten User-Rechte auch langfristig auf den Windows-Servern beibehalten werden, benötigen Administratoren Werkzeuge, die sie zuverlässig über Änderungen informieren. Die standardmäßig bereitgestellten Tools bieten allerdings keine Möglichkeit, alle Veränderungen in einem Report darzustellen oder eine automatische Alarmierung per E-Mail einzurichten.

Eine spezielle AD-Management-Lösung wie ADAudit Plus bietet hier natürlich Vorteile. Die ManageEngine-Software verfügt beispielsweise „ab Werk" über einen vorkonfigurierten „Policy Changes Report", der alle Änderungen an den Benutzerrechten komfortabel in einer Liste anzeigt (siehe Abbildung 3). Die Voraussetzung dafür: Der Administrator richtet hierfür die Audit-Richtlinien auf jedem Windows-Server zunächst einmalig ein, indem er die Einstellung „Audit Policy Change" aktiviert (beziehungsweise „Policy Change: Audit Authorization Policy Change" in den erweiterten Einstellungen). Anschließend ist es empfehlenswert, die Konfiguration der Windows-Server in ADAudit Plus im Reiter „Configuration" zu überprüfen.

Ist die initiale Konfiguration der Server abgeschlossen, lässt sich der Report in ADAudit Plus jederzeit in der Kategorie „Server Audit Reports" im Tab „Server Audit" aufrufen. So sehen Administratoren auf einen Blick, welche Änderungen an den Benutzerrechten vorgenommen wurden – und das für alle Windows-Server im Unternehmensnetzwerk.

Übrigens: Wie alle anderen Reports in ADAudit Plus lässt sich der „Change Policy Report" mit einem Alarm verknüpfen. Das stellt sicher, dass der Administrator bei kritischen Änderungen unverzüglich per E-Mail alarmiert wird.



4 Mit dem „Account Lockout Analyzer" lässt sich schnell herausfinden, ob ein gesperrtes Konto auf einem bestimmten Computer als Service-Account fungiert.

5. Gesperrte Service-Accounts aufspüren

Viele der Services, die auf Windows-Servern laufen, benötigen Benutzerkonten im Active Directory. Die sogenannten Service-Accounts sind beispielsweise für die Authentifizierung des Dienstes auf dem Domain-Controller erforderlich. Schlägt die Authentifizierung fehl, führt das zu einer Unterbrechung des Services. Passiert das mehrmals hintereinander, wird der Account in der Regel automatisch gesperrt. Die Folge: Der Service fällt komplett aus, bis die IT-Abteilung – meist durch die Beschwerde eines Anwenders – davon erfährt und das Passwort des Service-Accounts zurücksetzt.

In nahezu allen Fällen ist ein falsches Passwort für die Sperrung verantwortlich (die für den jeweiligen Domain-Controller eingestellten Passwortrichtlinien lassen sich über den in Tipp 3 vorgestellten Befehl „Secpol.msc" aufrufen). Da die Kennwörter der Services fest im Code auf dem Windows-Server programmiert sind, werden im Active Directory vorgenommene Passwortänderungen nicht automatisch übernommen. So kann es gerade bei auf mehreren Servern verwendeten Service-Accounts schnell passieren, dass ein Server bei der Passwortsynchronisation übersehen wird.

Um gesperrte Service-Accounts möglichst schnell und effizient aufzuspüren, können IT-Abteilungen auf Lösungen wie ADAudit Plus setzen, die neben Berichten auch individuelle Alarme bieten. Einmal eingerichtet, informiert die ManageEngine-Software den Administrator unverzüglich per E-Mail, sobald ein Service-Account-Passwort geändert und/oder ein Account gesperrt wurde. Dadurch lässt sich das Problem meist beheben, bevor die Anwender etwas von den Problemen merken. Das Ergebnis: weniger User-Anfragen beim Helpdesk.

Mit dem „Account Lockout Analyzer" (unter „Reports" / „User Management") lässt sich zudem einfach und schnell herausfinden, ob ein gesperrtes Konto auf dem Computer, auf dem die Sperrung initiiert wurde, als Service-Account fungiert (Abbildung 4). Auf diese Weise erkennt der Administrator sofort, welcher Service auf welchem Rechner durch die Sperrung unterbrochen wurde – schnelle Abhilfe ist dann möglich.

Fazit

Die vorgestellten Tipps zeigen, dass die Arbeit am Active Directory einfacher sein kann. Mit geeigneten Lösungen wie ADAudit Plus und AD-Manager Plus lassen sich viele, bislang umständlich zu lösende Aufgaben mit Hilfe von Reports und Alarmen deutlich schneller und einfacher beheben. Das minimiert den Zeitaufwand für die IT-Abteilung und hilft dabei, die Servicequalität zu verbessern und die Anzahl der Helpdesk-Anfragen zu reduzieren – für zufriedenere Kollegen.