ManageEngine
ADAudit Plus

Understanding and resolving account lockouts

Table of Contents

Account lockouts need no introduction; continuous help desk calls for this overwhelmingly common problem are a nightmare for most technicians. Finding the source of an account lockout to fix the root problem is a puzzle most admins and help desk technicians face. Demystifying these puzzles and getting rid of constant account unlock requests is a dream for many of them. Such account lockout issues affect your organization's security, productivity, and finances. This e-book will shed light on the various ways in which account lockouts impact an organization, and how to handle them.

The business impact of account lockouts

*Up to **30 percent** of help desk queries comprise account lockout complaints and password reset requests.* - Gartner

Account lockouts are one of the most frustrating tasks for a help desk technician or admin. From the hours spent figuring out the source of the lockout to finally resolving it, admins and help desk technicians know firsthand what a waste of time and energy they can be. Sometimes, the business impact of accounts lockouts is severe enough to cost not only time and money, but reputation as well.

Productivity loss

With so many help desk calls related to account lockouts, both the admins or technicians resolving the problem and the affected users face a blow to their productivity. Assuming it takes about one hour to resolve a single instance of lockout, this would cost the company two work hours, with the user's idle time included. This tiresome process includes finding the source of the account lockout, unlocking the account, changing the user's password, updating the new password on all services with the user's account, and ruling out the possibility of a cyberattack. Along with taking up a big chunk of time, this process can cost the company some big bucks.

The effect on an organization's revenue

According to Gartner, the approximate cost of a single account lockout instance is between $50 and $100. When an ordinary user's account gets locked, it just needs to be unlocked and the password reset. However, if it's a service account, the solution is well beyond just a simple password change. When systems for the departments using the service account's credentials fail, this downtime has adverse effects across the organization. For example, if the service involves customer interactions, this downtime might cost the organization its reputation and, inevitably, money.

Attacks and potential threats

Account lockouts could be a sign of an underlying attempt to attack the network. In case of lockout due to a brute-force attack, if the LockoutDuration in your AD is set too low (e.g. 30 minutes), and the lockout is noticed too late (after 90 minutes or later), the hacker could have already broken into the network. Setting a lower lockout duration increases the chance an attacker could be successful. Attackers could also perform a denial-of-service, essentially fulfilled by the service downtime caused by a lockout.

Continuous lockouts followed by a successful logon could indicate a successful attempt at hacking the user's account. Simply resolving the lockout would not suffice in this case; other anomalous activities by the same user need to be analyzed to identify patterns that are telltale signs of a breach. For example, an account lockout followed by a successful logon, followed by a large volume of file deletions.

Account lockouts aren't just an administrative problem any more. They need to be skilfully analyzed to uncover a potential threat to the organization's network. Here's a checklist of possible causes to account lockouts that need to be considered when performing an analysis:

Common causes of account lockouts

An attack was attempted

A simple brute-force attack or denial-of-service attack could be the reason for repeated account lockouts. The attacker will wait for the LockoutDuration to end and try again, so getting to the root of the lockout instantly is critical. If an account faces repeated lockouts, followed by a successful logon, analyze the user's activities to ensure they haven't been hacked. An attacker only needs to hack a single account to infiltrate the network and eventually gain complete control over it, so every lockout instance needs to be analyzed carefully.

Stale passwords

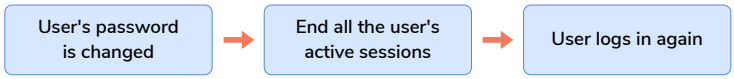
When a password change in a user's account is not replicated across the domain, these stale passwords cause account lockouts. Services using the service account's credentials may still use these stale passwords, causing authentication failures and user lockout. Admins and technicians need to check for stale passwords in applications and Windows components like Outlook Web App (OWA), Active Sync, Windows background services, COM objects (interprocess communication), and mapped network drives. Scheduled tasks may also use the user's cached credentials that weren't updated during replication.

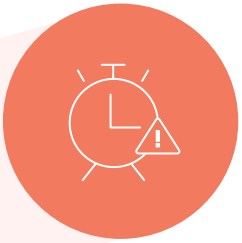
Failure to update a password on the service control manager

The service control manager caches service account passwords on computers running the service. When service account passwords are changed, those computers might not update the cached password, leading to a lockout. Admins and help desk technicians need to look for a pattern of failed logons in the AD Netlogon log files and the event log files on member servers. The security control manager also needs to be reconfigured to use the new password.

Users logged into multiple computers

A user may be logged into multiple computers simultaneously, with programs on those computers accessing network resources with this user's credentials. When users change their passwords, their active sessions on other machines might continue to use the old password. One way for admins and help desk technicians to avoid this situation is to end all the user's active sessions on other machines/applications when they change their password, and ask them to log in again.





False positives

If the LockoutThreshold is set too low, it could end up causing false positives. An ideal lockout threshold is 10-20 failed attempts. These false alarms waste time and reduce productivity, and may lead to actual threats being overlooked. A dynamic threshold based on individual user behavior is recommended.

Just another forgetful user!

The most common cause is simply a forgotten password. Most lockouts happen after a holiday or when a user returns from vacation as they perform too many login attempts due to forgotten passwords. Albeit frustrating, admins and technicians can breathe a sigh of relief, because this means the network is safe and the source of the lockout is just a forgetful user.

Resolving account lockouts

Check your event logs for lockout instances to locate the source. Look for the following events:

- 4740 - A user account was locked out.
- 4767- A user account was unlocked.
- 4625 - Logon failure due to unknown user name or bad password.
- 4793 - The Password Policy Checking API was called.
- 4776 - The domain controller attempted to validate the credentials for an account.
- 4471 - Kerberos pre-authentication failed.
- 4739 - Domain policy changed: Changes in account lockout and password policies.

Analyzing the above events and more to find out the source of account lockouts is a challenging task, and is almost impossible using the native AD tools offered by Microsoft. Here's why:

The clutter in native tools

If an attack occurs, by the time the user realizes their account was locked out, the hacker might reattempt their attack following the lockout duration. If it's too late, the attacker's attempt is successful and they may have infiltrated the network. The multitude of event logs also makes it difficult to spot a suspicious number of account lockouts in a short period of time. The user may be logged into multiple computers, services, and remote connections, and it could take a long time for an admin or technician to find the source of lockout in the tsunami of events!

Lack of sufficient storage space

The storage limit for the Windows Event Viewer is 4 GB, so it's easy for a lockout to go unnoticed. It's possible that the logs needed for analysis and investigation will already be long gone and overwritten during an investigation, making it impossible for a technician to identify the cause of the lockout. All they can do is reset the password for the user and check each component until they land on the right one. Users' recent logon data is also beneficial during an analysis to correlate these activities and understand the user's logon behavior, but there may not be enough logon events for an efficient analysis.

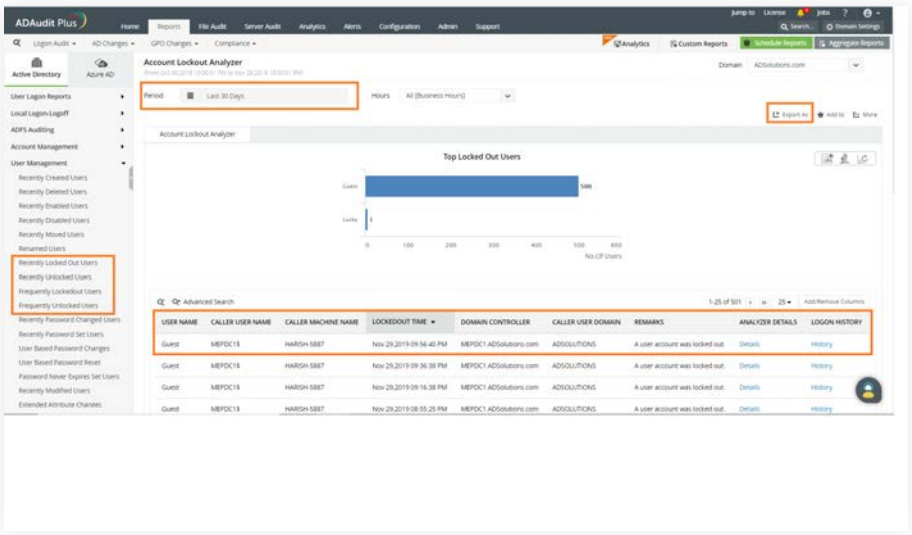
To put it simply, native AD tools don't have what it takes to resolve account lockouts quickly and efficiently.

Account lockout analysis made easier

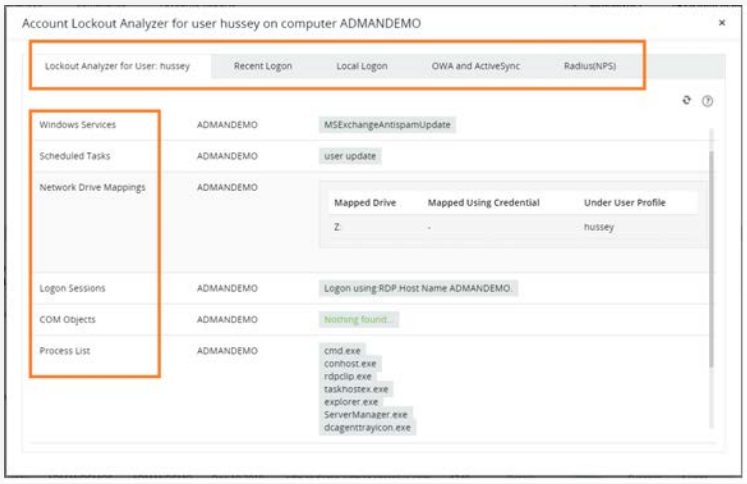
ManageEngine's ADAudit Plus has an account lockout analyzer with everything you need. With continuous monitoring and real-time log collection, neat reports are provided with all the necessary information needed to conduct a complete account lockout analysis.

This includes:

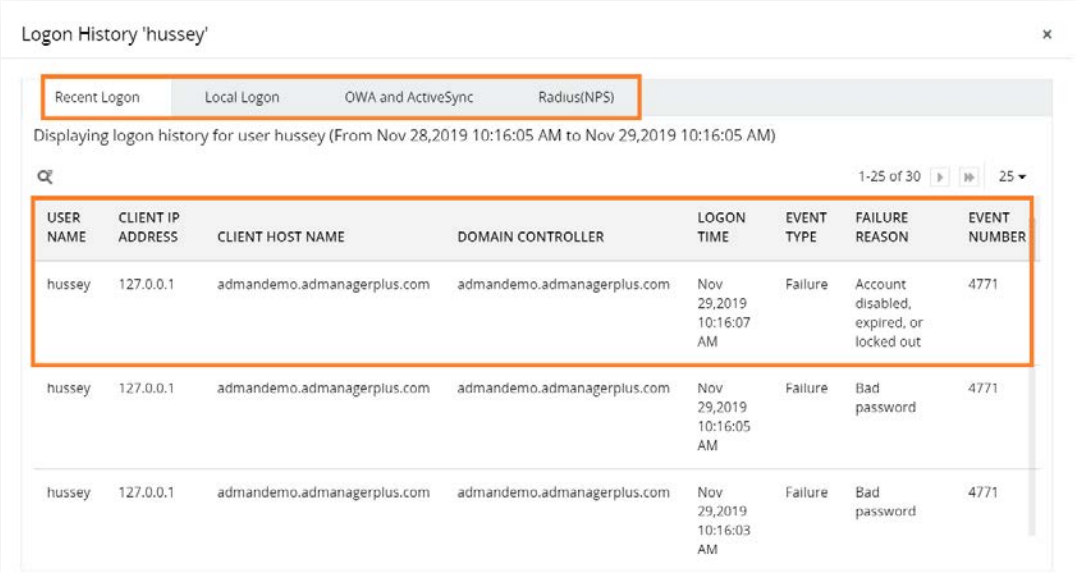
- The who, when, where, and why of every lockout instance. These reports are collected in real time and can be exported to formats like CSV, PDF, XML, and HTML. A single click is all it takes to pull up the complete details of every lockout that has happened in the specified time frame. Use these to avoid hours of filtering out events from the Event Viewer and typing out PowerShell scripts.



- The details of all the services and Windows components using the user's credentials. This way, the source of any stale password can be spotted in just a few seconds.



- The recent logon history of users, which is useful for deciphering the source of an account lockout. By correlating the user's logon history, admins and help desk technicians can understand potential threats in case of suspicious logons.



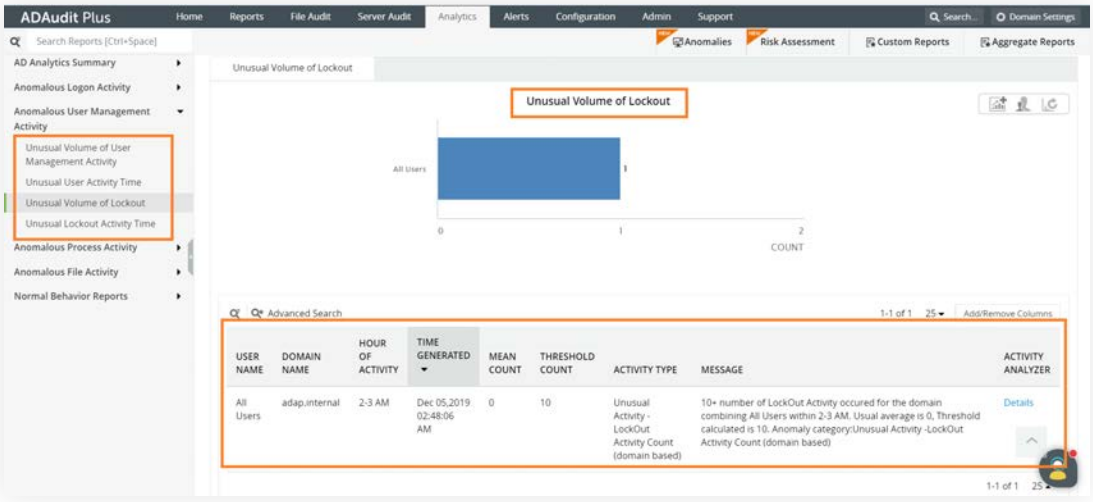
- Instant alerts when a privileged user is locked out, or if the volume of lockouts is too high. These alerts can also be sent straight to the admin's or technician's email, or by phone from ADAudit Plus.

In fact, to help admins and technicians better understand the account lockout status in their domain, ADAudit Plus offers a host of reports, including:

- Recently locked out users
- Frequently locked out users
- Recently unlocked users
- Frequently unlocked users

All these reports list the user accounts that were locked out, along with critical details like the time and domain controller from which they were locked out. These reports help admins track and keep a close eye on user accounts that are locked out frequently. In case of an investigation, if the admins or help desk technicians need to discover which user account could have been compromised as part of the attacker's initial entry, they can check the recently locked out users.

The user behavior analytics module of ADAudit Plus leverages machine learning to spot suspicious volumes or durations of user logon activities by employing dynamic thresholds.



Don't stop at just account lockout analysis; strengthen your AD security from every angle with these ADAudit Plus features:

- Real-time, continuous audit of all changes made in your domain
- Consolidated compliance reports
- Real-time alerts sent straight to your email or phone
- Complete user logon auditing
- Monitoring for all your servers, including Netapp clusters and EMC servers, and preserve data integrity

ManageEngine
ADAudit Plus

ManageEngine ADAudit Plus is an IT security and compliance solution. With over 200 event-specific reports and real-time email alerts, it provides in-depth knowledge about changes effected to both the content and configuration of Active Directory, Azure AD and Windows servers. Additionally it also provides thorough access intelligence for workstations and file servers (including NetApp and EMC).

To learn more about how ADAudit Plus can help you with all your Active Directory auditing needs, please visit: https://www.manageengine.com/products/active-directory-audit/

$ Get Quote ⬇ Download