ManageEngine Password Manager Pro

Overcoming the Perils of Password Sharing in Enterprises

White Paper

V Balasubramanian
ZOHO Corp

Abstract

Administrative passwords are literally 'aplenty' in enterprises of all sizes. They are mostly insecurely shared and lie scattered in the enterprise leaving little scope for any internal controls. This white paper discusses the security threats associated with the password sharing in enterprises. Though the security and operational problems caused by shared administrative passwords are so obvious, no organization can afford to eliminate them altogether. The ways to tackle this challenge, the importance of effective Shared Account Password Management and the need for enterprise password management solutions have been dealt with.

Contents

Shared Passwords – The Challenge

Administrative passwords are omnipresent and all pervasive in enterprises of all sizes – big and small. Organizations depend on a variety of IT resources to sustain their businesses. Servers, databases, network devices and numerous other IT applications are controlled through administrative passwords, which are aplenty.

Needless to say, administrative passwords are very powerful and accord unlimited privilege to the users. Those who login through the privileged mode could access absolutely anything with ease.

Typically, enterprises have thousands of privileged passwords, majority of which are used in shared environment. That means, a group of administrators use the common privileged account to access the resource. The privileged accounts are accessible to all the members of a team.

Apart from the 'officially shared' passwords, users often tend to reveal administrative passwords to their colleagues for some reason or other. The most common reason for such an 'unofficial share' is to cater to an emergency on one's absence – IT Manager revealing the password to a senior member when he has gone on vacation.

Whether it is official or casual, sharing of privileged passwords in enterprises could have disastrous repercussions on the security of the enterprise. Mismanagement of administrative passwords leads to information theft, manipulations and sabotage without a trace.

It is always good to avoid sharing of administrative passwords. Unfortunately, it is just an ideal situation. Practical needs are mostly the opposite. Business requirements demand selective sharing of passwords with others and yet not compromising on enterprise security. Thus, enterprises find themselves in a catch-22 situation!

Whether it is official or casual, sharing of privileged passwords in enterprises could have disastrous repercussions on the security of the enterprise. Mismanagement of administrative passwords leads to information theft, manipulations and sabotage without a trace.

The Traditional Approach

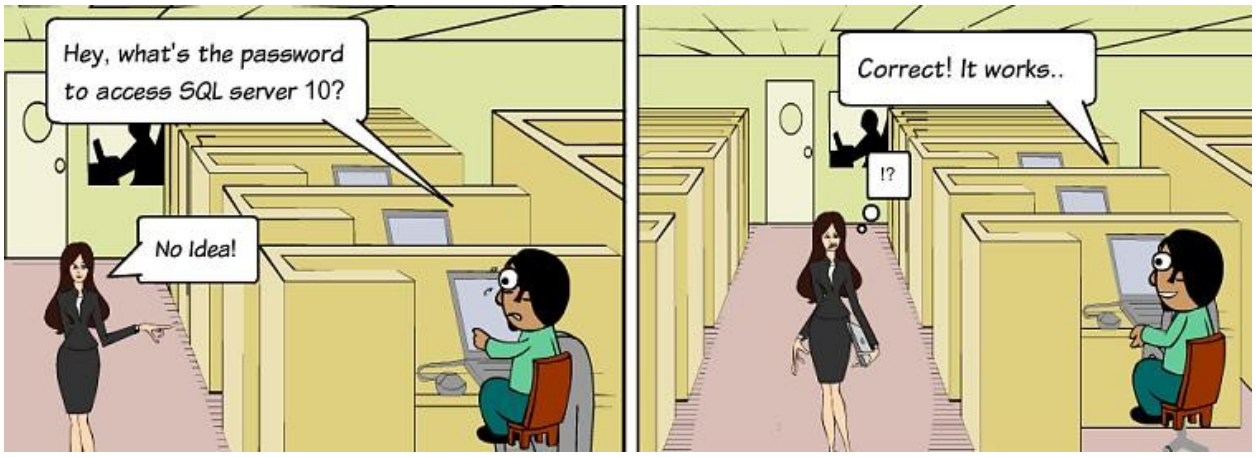
Administrative/Privileged passwords are literally 'aplenty' in enterprises. Just a single instance of a database could have as many as 30 administrative accounts. Servers, switches, routers and any other hardware or software, could have equally large number of administrative passwords. So, easily, even a small enterprise having a modest number of devices and applications will have thousands of privileged passwords.

A group of administrators in a team would require access to the same set of privileged passwords and hence, in reality, the passwords are just left open to be managed by the group.

Most of the administrators will have access to all the privileged accounts. This is called 'shared environment', where privileged passwords remain virtually in utter disorder.

Developers, help desk technicians and in certain cases, some third party vendors who require access to privileged passwords purely on temporary basis, are supplied with the required passwords mostly orally or through emails. There is no process to revoke temporary access and reset the password after the temporary usage, which leaves a big security hole.

It is quite common to see administrators assigning some familiar words or short phrases as passwords, for ease of use. The passwords are maintained in text files, spread sheets, homegrown tools or even in physical vaults. And, it is not uncommon to see UNIX administration team having full access to the Windows passwords, developers having full access to database passwords and so on.



Apart from the shared accounts, even the 'personalized accounts' of the top brass in the IT team are often revealed to the team members to tackle emergency issues. Many surveys by industry analysts have time and again pointed out that administrators often tend to casually 'tell' the passwords to their colleagues to carry out certain work in proxy.

Thus, administrative passwords are insecurely shared and lie scattered in the enterprise leaving little scope for any internal controls.

Security Threats and Drawbacks of Traditional Approach

- Every single privileged account will be accessed by multiple administrators, who, in reality, access the privileged mode anonymously. At the end of the day, all you will know is that someone has logged in as 'Administrator'. But, who is that 'someone'? This naturally leads to a kind of disorder in the enterprise, especially when a large number of administrators share the same account.

- Internal controls become fragile. Organizations might have secured their external face against attacks, but a still bigger attack might just be waiting to happen from within.

- Mistakes – accidental or intentional, could never be traced to individuals. Enterprises virtually lack accountability for actions.

- If the text file or spreadsheet containing the shared administrative passwords reaches the hands of a malicious user, data security and business reputation would be thrown to winds.

- When passwords are not kept secret and revealed to others, the very purpose of having an authentication mechanism to grant access to the resources is defeated.

- Passwords of the resources are often changed by one administrator without the knowledge of other administrators. Without close cooperation among administrators, day-to-day operations would become messy. Resource lockout events could become common.

Organizations might have secured their external face against attacks, but a still bigger attack might just be waiting to happen from within, as internal controls become fragile.

- Given the complex nature of sharing, it would be cumbersome to find who has access to what resources. When someone leaves the organization, changing all the privileged passwords of the enterprise is the only solution to rule out any possible access or intrusion by that person in future.

- Manually changing the passwords of the thousands of resources would demand 'man-years' to complete the task.

- In worst cases, if an administrator leaves without revealing a privileged password that was changed by him, the device/application might remain locked out for a prolonged period.

- Government regulations, compliance policies and industry best practices mandate strict access controls, clear-cut role definition, frequent password rotation and comprehensive audit trails on 'who' accessed 'what' resources and 'when'. The traditional approach has no provision for this.

The security and operational problems caused by shared administrative passwords are so obvious; but, no organization can afford to eliminate them altogether. Without compromising security, shared administrative passwords have to be used.

The Solution

All the threats associated with the shared administrative passwords, can be easily mitigated using a good **'Shared Account Password Management' (SAPM) software** available in the market. The SAPM solutions act as the alternative for the traditional, inefficient and insecure password management processes. They provide an automated, policy-driven solution for shared administrative password management.

It is pertinent to quote here a recent research report by Gartner:

"SAPM tools have emerged as a best-practice choice for managing shared-account passwords across all sizes of organization and all vertical industries. They provide efficient and effective password management for shared superuser and firecall accounts in a robust, controlled and accountable manner, enabling any enterprise to meet regulatory compliance requirements for restricted access and individual accountability".

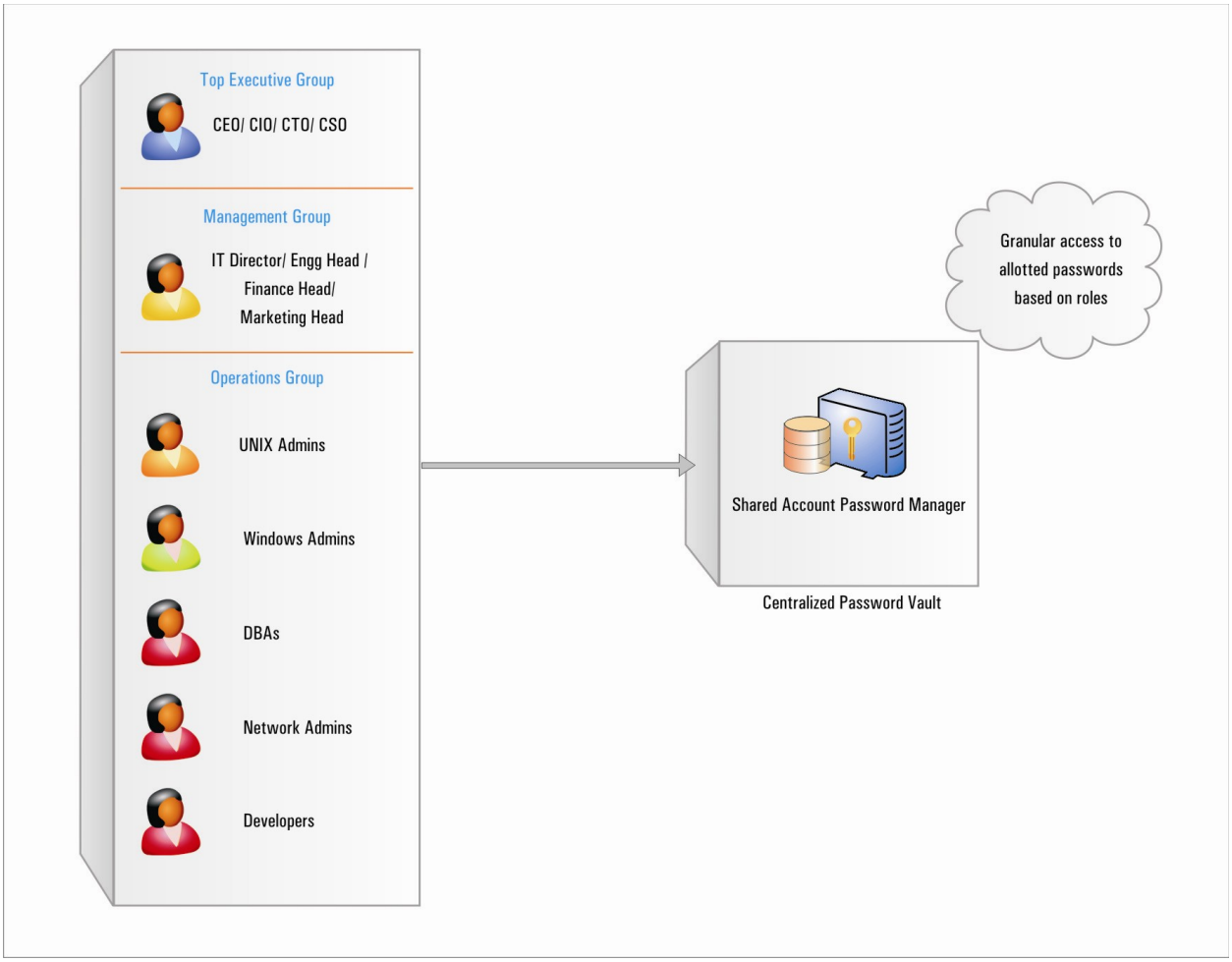
(**Source:** Gartner, Inc., "MarketScope for Shared-Account/Software-Account Password Management", Ant Allan, Perry Carpenter, 16 June 2009).

The SAPM solutions enable enterprises to establish a secure process for the entire life-cycle of administrative password management. They help securely store administrative passwords in a centralized vault and provide access through a web-interface. Access controls are well-defined – users will be allowed to retrieve only those passwords that are allotted to them; NOT all

The SAPM solutions act as the alternative for the traditional, inefficient and insecure password management practices. Through the automated, policy-driven approach, they help establish a secure process for the entire life-cycle of Shared Account Password Management.

passwords of the enterprise.

All passwords will have well-defined ownership – the owner alone will have absolute privilege on the passwords. Unless the owner shares the passwords, no other user will be permitted to view the passwords. The owner can share the passwords with others granting granular permission for various actions – password retrieval, reset etc., If an administrator leaves the organization, de- provisioning of passwords can be done instantly.



A Typical SAPM Solution

At any point of time, one can get a clear picture of 'who' has access to 'what' resources. When an administrator accesses a shared privileged password, audit trails are generated.

Thus the anonymity and the disorder created due to the traditional process are completely eliminated. If something goes wrong, user actions could be easily traced to individual users.

The SAPM solutions help establish a secure connection to the target systems and reset the passwords whenever required or automatically through scheduled tasks.

In summary, with an SAPM solution in place, IT Managers can ensure strict internal controls and comply with regulations; enforce standard policies, processes and practices. Whatever be the number of privileged passwords - thousands or millions, storing, sharing, accessing and changing them will be a breeze. Security threats arising due to password sharing are completely eliminated.

Introducing ManageEngine Password Manager Pro

Password Manager Pro (PMP) is a web-based, **Shared Account Password Management (SAPM) Solution** for enterprises to control the access to shared administrative passwords of any 'enterprise resource' such as servers, databases, network devices, applications etc. PMP enables IT managers to enforce standard password management practices such as maintaining a central repository of all passwords, usage of strong passwords, frequent changing of sensitive passwords and controlling user access to shared passwords across the enterprise. It is available at costs affordable to SMBs.

For more details on PMP, visit *http://www.passwordmanagerpro.com*

ManageEngine

ZOHO Corp. (formerly AdventNet Inc.)
Phone: +1-925-924-9500 **Website:** http://www.passwordmanagerpro.com
For Queries: passwordmanagerpro-support@manageengine.com