ManageEngine
PasswordManager Pro

Addressing the Operational Challenges of Administrative Passwords

WHITE PAPER

V..Balasubramanian
ZOHO Corp.

Abstract

Enterprises making use of various IT systems (servers, devices, applications etc.) face numerous challenges due to the proliferation of administrative passwords (also called as privileged passwords). This white paper discusses the problems associated with administrative password proliferation with special reference to the issues related to shared administrative passwords and service accounts. The ways to tackle the challenge, the importance of effective password management, the need for enterprise password management applications to prevent unauthorized access to passwords and the vital requirements that one should consider before zeroing-in on a password management solution, have been dealt with.

The Challenge

Modern IT and other enterprises are heavily dependant on servers, databases, network devices, security infrastructure and other software applications for their day-to-day operations. These infrastructure are accessed and controlled through administrative passwords. Typically, the applications are used in a shared environment by a group of administrators.

The number of administrative passwords keep on growing as more and more servers, devices and applications are added to the enterprise. Administrators end up virtually struggling with a pile of passwords and face problems on securely storing, managing and sharing the passwords. Spreadsheets, flat files and even print-outs containing the passwords are circulated among the administrators.

This traditional practice brings with it a host of issues such as the following:

- When one administrator changes a password, it should be updated in all the 'copies'; otherwise, at the most needed time, one would be trying to login with an outdated or old password!
- Chances of security attacks on the IT infrastructure become very bright
- The business of the enterprise would be in jeopardy as sensitive passwords remain insecure

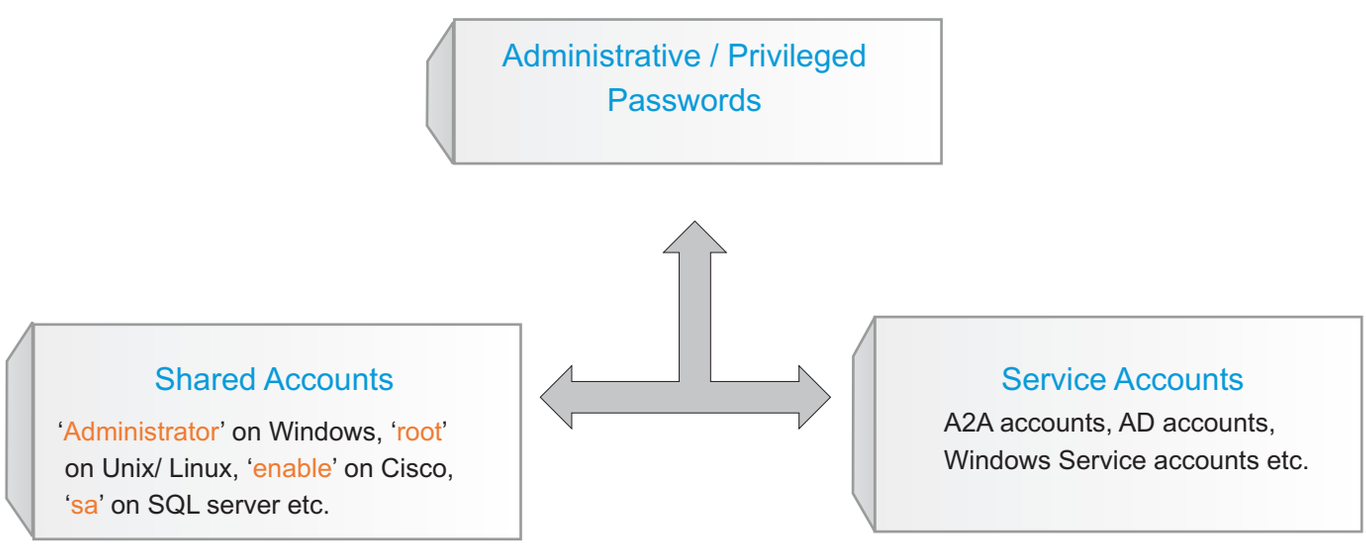

Fig. 1 - Types of Administrative Passwords

In most of the organizations, a common administrative account is created and all the administrators use the same account to access the infrastructure - for instance '**Administrator**' on Windows, '**root**' on Unix/Linux, '**enable**' on Cisco, '**sa**' on SQL server etc.

These administrative passwords, also known as '**Shared Administrative Passwords**' give unlimited access to the infrastructure to the extent that the user can do virtually anything. This practice brings along with it accountability issues since the super-user is not role-based and actions could not be traced back to a particular user.

According to a research report of Gartner, the shared accounts with superuser privileges or other high-level access rights pose a significant risk in all organizations. Passwords are shared by multiple users who are sanctioned to use those accounts, or they're managed using fragile manual processes. High risks stem from passwords becoming known to others, as well as the lack of individual accountability. (**Source:** Gartner, Inc., "Toolkit: Password Management Tools for Shared Accounts and Service Accounts", Ant Allan, 11 January 2007).

There is yet another kind of administrative account, called the '**Service Accounts**'. These are **Application-Application accounts** and generally have unlimited privileges. Service accounts are used by applications internally - for instance, scripts.

While the access permissions will be defined in one application, the other application, which seeks to access this application will have to provide the credentials. These credentials are generally hard coded in the calling application for ease of use and this makes the organizations vulnerable to attacks.

Also, IT Managers often wish to enforce certain standard password policies - such as usage of strong passwords, curbs on usage of obvious passwords, rotating passwords at periodic intervals etc. The traditional password management lacks provision for all of these policies.

Governmental and industry regulations prescribe severe security measures for protecting passwords and require comprehensive audit records on each and every action on the passwords. In the traditional approach, there is no way to ensure compliance to such regulations.

In short, administrators of enterprises are drowning in a pile of administrative passwords and are struggling to store and manage them securely and effectively.

The issues at a glance

- Insecure storage of passwords & security vulnerabilities
- Uncontrolled super-user privileges
- Lack of role-based access control
- Lack of accountability for actions
- Lack of provision for enforcing standard password practices/policies
- Lack of centralized management

The Way Out

One of the effective ways to securely manage the administrative passwords is to store the passwords in a central, secure storage and automate password management tasks. Deploying 'Password Management Applications' or in simple words, the 'Enterprise Password Managers' can help organizations in controlling access to administrative passwords and in taking total control of the shared administrative passwords.

Enterprise Password Manager: Strategic Requirements

Before analyzing the requirements for an ideal password management application, it is worthwhile to have a look at the top questions that arise in the minds of IT administrators:

Top questions in the minds of IT administrators

- How do I keep a secure, central record of all my privileged/administrative accounts?
- How do I track who has access to which accounts?
- How do I make sure my users do not keep a copy of these passwords and float them around?
- How do I change passwords of these systems periodically without spending man days?
- How do I provide time-bound access to passwords on need basis?
- What happens if an administrator knowing all the passwords leaves the enterprise?
- How do I enforce standard management practices to my users?

A good enterprise password manager should be capable of addressing all the above issues. In addition, it should have the following capabilities:

Secure Password Storage

Should be capable of securely storing thousands of administrative passwords. The passwords should reside in 'safe custody' - encrypted using **Advanced Encryption Standard** (AES) algorithm, which is the strongest encryption available for password protection and also approved by the US Government. A very strong authentication mechanism should be in place to access the passwords.

Secure Data Communication

All data communication between the user interface and database should be encrypted. In the case of web interfaces, the communication should be through secure http.

Well-defined Password Ownership

The age-old practice of users with 'administrator' role getting access to all passwords, is no longer considered reasonable from the standpoint of information security. Specific users should take full ownership for specific passwords, which could be accessed only by them unless they decide to make the passwords accessible to others.

Selective Sharing of Passwords

On need basis, password owners should be able to share their passwords with others. Sharing should be governed by granular access control policies. The owner should be able to choose what type of access has to be provided just 'view only' access or 'view & edit' privilege. In extreme instances, there should be provision for sharing/delegating complete management of passwords.

Password Request-Release Mechanism

In the work environments that involve the usage of very sensitive applications, even password sharing or granular access restrictions alone may not viewed sufficient for certain accounts. To handle such cases, there should be provision for 'Request-Release' mechanism. When a user needs access to the password, a request for authorization would be sent to the administrator, who would validate the request and release the password. The 'request-release' mechanism should be a hassle-free process.

Password Lock

Even when passwords are shared on need basis, there may be requirements to reserve access to passwords exclusively for a single user at a time. That means, when one user is accessing a password, it would be locked and will not be available for others to view.

Automatic Reset of Passwords

When passwords are changed in the application, there should be provision for automatically reflecting the changes in the resource. Also, the application should be capable of automatically changing the passwords of thousands of accounts without any human intervention.

Comprehensive Audit

All access to passwords (who accessed what passwords and when) and all operations done by the users on any resource have to be captured in the audit trails. Strong accountability has to be established for all users and actions.

Tamper-proof audit logs

Audit trails recorded by the application should not only be accurate, but also tamper-proof. Otherwise, malicious users would delete the records to conceal their actions. Audit trails will then be of no use to fix accountability issues. Even when the permission to purge the trails rests with a most-trusted administrator, alarms should be generated when audit trails are deleted.

Password Policies

There should be provision for establishing password policies that help in defining the characteristics of passwords of various strengths, which can then be used to enforce strong passwords in the system.

Security Controls

Apart from enforcing standard password management practices, the application should have provision for various other security control measures such as monitoring failed login attempts, locking out login after a specified number of failed attempts, provision for granting access to the application only for a specified time-limit, termination of inactive user sessions, automatic passwords resets, setting password age etc.

Compliance & Reports

Apart from ensuring secure storage, secure data transmission, granular access restrictions and comprehensive auditing, there must be provision for checking compliance to government/industry regulations (HIPAA, Sarbanes-Oxley, EPHI, GLBA, PCI Data Security Requirements etc.) and certain other standard password management practices such as mandatorily changing passwords at frequent intervals, setting password age, non-usage of recently used passwords, compulsory usage of strong passwords etc. Intuitive reports should be generated whether the passwords/practices are compliant to the rules defined. Violations should be reported as alerts.

Alerts/Notifications

Owners of passwords should be notified of various password actions such as password access, change in access permissions, change in user roles, password expiry, when automatic password reset happens etc.

Managing A2A Passwords

There should be effective mechanism to deal with Application-to-Application (A2A) passwords of service accounts, which are used by applications without human intervention. One application (say Application A) would contact the password management application for the password to access another application (say Application B). On getting the password, 'A' would contact 'B' and all these have to happen without human intervention.

Storing Digital Certificates, Keys, Documents

The Password Management application should not just be for storing passwords. There should also be provision for securely storing documents, images, digital certificates, license keys and the like.

Disaster Recovery

However robust the application may be, there should always be provision for a reliable disaster recovery mechanism. Live backup of data is the best setup to have. At the least, there should be support for periodic backup and secure storage of data.

Centralized Control

Organizations generally have several functional groups and each group will have access to specific passwords. The passwords should be stored in a centralized repository and should be governed by centralized password policies and practices.

Access from Anywhere

The application should preferably be web-based providing access for authorized users from anywhere. In geographically distributed environments, the need for this would be very high.

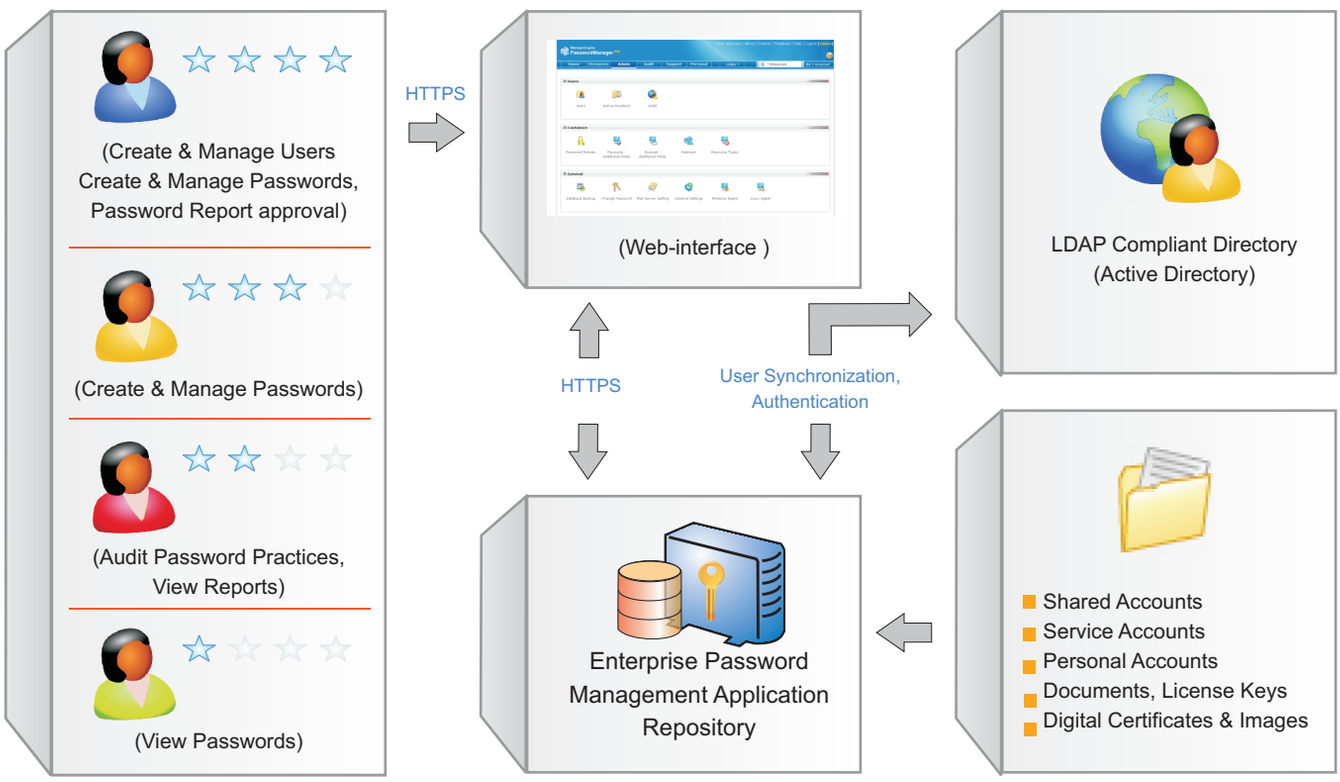

Fig. 2 - Password Management - Workflow

Support for External Identity Stores

The password management application should be capable of importing users/user groups as such from external identity stores such as Windows Active Directory or an LDAP directory. Also, it should be capable of using the authentication service provided by the external identity stores.

High Availability

Once a Password Manager is deployed in production in an enterprise, IT administrators/system administrators would be heavily Dependant on the application availability for retrieving passwords. Continuous availability of the password management application would be crucial in such scenarios. Otherwise, at the most wanted time, administrator would end up in not getting the required password.

Resources/Systems Support

Password Managers should be able to support servers, network devices, databases, workstations and any other application.

Easy to setup and use

Password Management Applications should be very easy to install and use. They should just act as a tool at the hands of the administrators not demanding cumbersome installation procedure and usage.

Affordable Price

Though Password Management Applications provide high value for your buck, the cost of the solution should not be too high to damage your pockets.

Some users tell why they use a Password Manager ...

"For effectively managing IT systems in an organisation with multiple domains and applications, it's become essential to store passwords in a safe, secure and functional way. Password Manager helps us in achieving our password security goals".

Phill Charlton
Infrastructure Specialist
Sara Lee Information Centre of Excellence
Australia & New Zealand

"Our attorneys and staff need password manager to securely store all the passwords required by them to use with court filings".

Kevin Davidson
Director of Information Security
Stinson Morrison Hecker LLP

"We require password manager to store, track, manage and secure our key production system passwords. In addition, the auditing of who retrieve what passwords and when allows us to meet internal and external auditing policies as set forth by SAS70, Sarbanes and other mandates".

Ken Wilkey
Euronet Worldwide Inc.
Kansas, USA

Conclusion

Organizations face an increasing security threat due to the proliferation of administrative passwords. Deploying a Password Management Application would prove to be invaluable, particularly in heterogeneous environments with multiple applications and multi-user scenario. Secure storage, selective sharing, granular access, centralized management and access-from-anywhere are the key ingredients of an effective password management system. With such an application in place, enterprises can be protected from various security threats and could save a great deal of time of the administrators.

About ManageEngine PasswordManager Pro

PasswordManager Pro (PMP) is a web-based Password Management Solution for enterprises to control the access to shared administrative/privileged 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. For more details on PMP, visit http://www.passwordmanagerpro.com

ZOHO Corp .
4900 Hopyard Rd., Suite 310 , Pleasanton, CA 94588, USA
Phone: +1-925-924-9500 Fax: +1-925-924-9600

Website: http://www.passwordmanagerpro.com
For Queries on Product: passwordmanagerpro-support@manageengine.com