Solution Brief

Dynamic Password Controller

Ironsphere
A Krontech Company

Introduction

Today's corporate employees use two major types of accounts – Personal and Privileged accounts – with associated passwords to prevent unauthorized use. Their personal accounts are used to access their personal business emails, logging in to their personal computers, or accessing their company's internal applications.

What are privileged accounts?

Privileged accounts provide elevated, often non-restricted, access to the technology infrastructure. Organizations rely on privileged accounts to enable authorized users, such as IT and Network admins, to perform daily configuration, operation, administration, and maintenance duties. Those accounts are referred to as superuser accounts, technical accounts, service accounts, or admin accounts. They include local administrative accounts of servers, databases, and network devices, as well as domain, emergency, application management, and service accounts. These accounts are the keys to the IT kingdom, and a prime target for internal and external attackers who seek to gain access to them. Despite the critical nature of these accounts, organizations rarely have tools and processes in place to control how and why they are used. Organizations must improve their security posture to mitigate operational and business risk, by implementing processes and technologies to track and prevent the misuse of privileged accounts by external and internal actors.

Challenges

Technical admin users remotely access servers, hosts, and devices directly using privileged accounts in the course of their daily administration and maintenance operations, such as configuration changes, troubleshooting, upgrades, and backups.

Such user activities pose security threats for organizations, such as credential theft and privilege abuse, due to the lack of accountability, visibility, and excessive privileges.

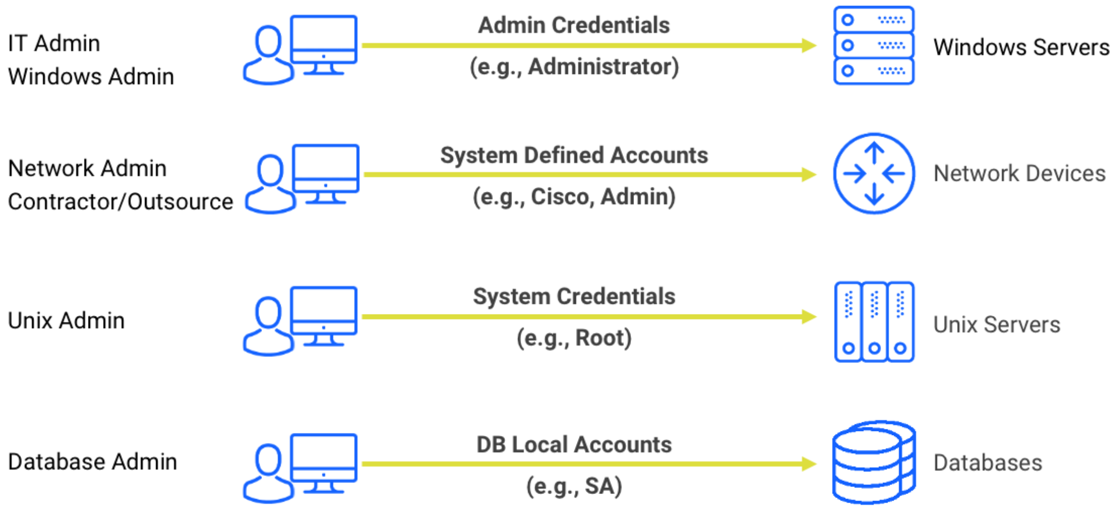

Figure 1 — Accessing Hosts/Devices without a PAM Solution

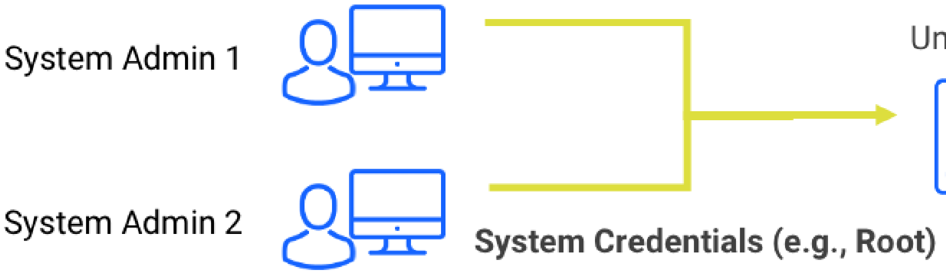

Figure 2 — Accountability

Accountability

Multiple users can connect to the same host/system with the same privileged account, at different times or at the same time. Since the privileged account is non-personal and shared, there is no way to track which real user accessed what and for what purpose. This situation hinders accountability.

Visibility

Most of the time, privileged user activities, such as which user accessed what and for what purpose, are not visible to the organization. This means those organizations have none or very limited tools to detect security incidents related to privileged credential theft or abuse.

Excessive Privileges

Administrators prefer to have an entire set of privileges assigned to them, for an easier and more convenient manual process. However, this also allows users to accidentally access servers/hosts or change configurations that are not within their responsibilities, enabling attackers to gain more control when they steal the credentials of such an account.

Stale Passwords

Privileged accounts are frequently non-personal and shared, causing users to not change its passwords because they do not feel responsible for them. This also makes it inconvenient to change passwords, as others will lose access to systems, causing delays or issues in daily operations. Such unchanged passwords increase the risk factor, allowing attackers to use the stolen passwords silently for an indeterminate period of time, resulting in data breaches or unauthorized access to other systems. Also, employees or contractors who left the company or moved to another department will continue to have knowledge of the passwords, and are able to access the organization’s systems.

Trust-Based Processes

Organizations trust users to own a privileged account and use it only for business purposes. Additionally, users trust their coworkers and easily share such privileged accounts with them. Those coworkers can trust and share with others as well, and soon after, the organization cannot track and control who has access/knowledge of which privileged accounts.

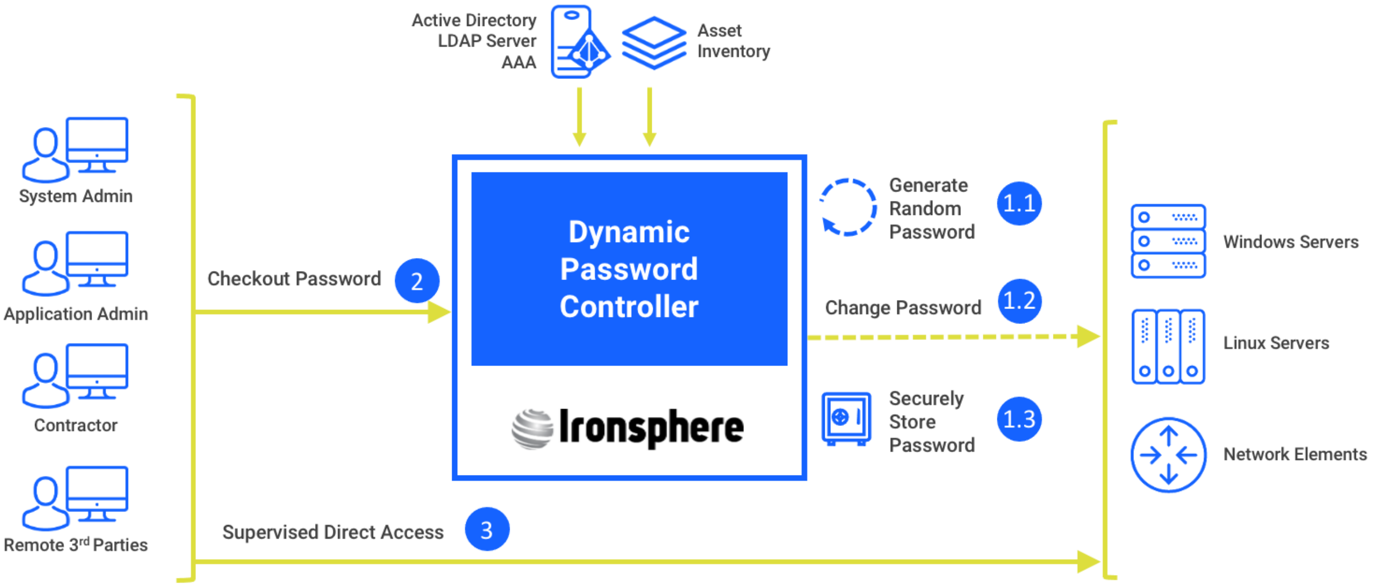

Figure 3 — Ironsphere Dynamic Password Controller, High Level Topology

Solution

Ironsphere provides centralized and unified management of privileged accounts. Accounts are stored securely and encrypted in a digital vault, and passwords are auto changed (rotated) regularly. When a user needs privileged credentials to perform essential IT operations, the user can retrieve them from Ironsphere's digital vault, after ensuring that the he/she really is who they claim to be and the operation is a legitimate business activity.

Enables Accountability

Users log in to Ironsphere with their own personal accounts instead of a shared account, so Ironsphere can detect and verify who the real user is. Ironsphere then displays the list of privileged accounts that specific user is authorized to use. When a user checks out a privileged (shared) account from the digital vault, Ironsphere logs that activity and provides unified audit trails of which users used which privileged accounts.

Provides Unified Visibility

Ironsphere provides unified and centralized visibility of privileged accounts in the IT infrastructure by auto discovering and onboarding those accounts across the board, including servers, databases, applications, and appliances. Authorization policies regarding who can retrieve which privileged accounts are configured, tracked, and governed on Ironsphere.

When a user attempts to retrieve a privileged credential from the Ironsphere digital vault, the required level of clearance must be met, such as the purpose of the activity, approval from a manager, or verifying it is linked to a valid and approved support ticket. Ironsphere logs all user activity and provides audit trails with details of who accessed which server/host, when, and for what purpose.

Eliminates Excessive Privileges

Ironsphere stores and changes all privileged credentials in an organization, and is effectively the owner of all privileged accounts. Since users no longer know the privileged credentials, these cannot be shared among employees without permission. Also, authorization policies regarding who can access what are centrally managed on Ironsphere, enabling organizations to implement least privilege management best practices to improve their security posture.

Eliminates Stale Passwords

Ironsphere remotely accesses target servers/systems at configurable regular intervals and auto changes the passwords with randomly populated strong passwords, eliminating manual processes and ensuring privileged credentials are always fresh and strong.

Eliminates Trust-Based Processes

The governance of privileged accounts and authorization policies are managed on Ironsphere. All activities are tracked and logged for audit trail purposes, limiting the human-factor in the process.

Conclusion

Malicious external actors can access critical systems and sensitive data once they gain unauthorized access to privileged accounts. There are also incidents where internal actors, such as employees or contractors, abuse their privileges or sometimes cause damage, exposure, or downtime by accident. It is critical for organizations to implement processes and tools to track, control, and manage the use of privileged accounts. Ironsphere helps organizations by auto discovering and onboarding privileged accounts in the technology infrastructure, securely storing them in an encrypted vault, and auto changing and generating random strong passwords at regular intervals.