ManageEngine
PAM360

Securing Windows Service Accounts with effective access management controls

Service accounts are privileged domain accounts, which are used by critical applications or services to interact with their operating systems, and to execute batch files, scheduled tasks, and applications hosted across databases, file systems, and devices. These accounts are controlled by "non-human" users, such as systems, scripts, applications, and are typically provided with elevated privileges to business-critical applications, databases, web services, APIs, and so on.

Categories of service accounts

Account Type	Description
Shared	Accounts that are used by two or more users on a system. Account credentials are shared among the users.
System	Also known as "Superuser" or privileged accounts. These administrative accounts are used to enable communications and processes within the operating system (e.g., root on UNIX).
Non-Interactive	Accounts that are used to execute system processes and services, such as running automated scripts, batch files, and scheduled tasks. End users can not log into these accounts.

Note: There could be more sub-classifications of accounts that might fall under the OS and service account categories.

Security risks associated with service accounts

There are several reasons why mismanagement of service accounts can pose significant security risks to organizations.

Too complex for manual management

Service accounts, albeit simple to configure and use, are tightly interconnected, and shared with several applications and services. Further, they are referenced in multiple instances across multiple assets and applications, which makes the management of these accounts so complex that even the slightest oversight with the chain of dependencies could cause cascading system failures.

Backdoor to privileged information

Service accounts are, more often than not, tied to business-critical applications, and hence can require privileged access to servers, databases, and other assets. With a single compromised account, attackers can gain complete control over privileged assets, endpoints, and shared sensitive information.

High-value, easy target for attackers

Since service accounts are mostly used by non-human entities to perform operations, security controls such as two-factor authentication (TFA) cannot be applied, as it requires human interaction for authentication purposes. To complicate this, passwords of service accounts are set to remain permanent because frequent password rotation of these accounts can cause unforeseen lockouts and disruptions. As a result, service accounts become an easy and lucrative target for attackers.

Service account management lifecycle: Getting started

As organizations grow, manual management of service accounts becomes overwhelming and laborious because of the number of applications and services accessed by them. Due to the pervasiveness and proliferation of service accounts, and the increasing risk of them being an easy target, it is important to actively monitor, administer, and audit the use of these accounts. For organizations to identify and thwart possible service account exploitations, they will have to implement a course of action that strikes a fine balance between operations and security.

While identity governance and administration (IGA) tools aid in managing credentials of privileged individual accounts, they do not provide management of service accounts that are tied to non-human entities. Here are some best practices to help you effectively manage and safeguard your service accounts from attacks.

1. Discover your organization's service accounts.

You can not protect your service accounts if you have not identified them yet. The first step in securing service accounts is to discover them throughout the network and within applications, and to identify the activities tied to them. This will help IT admins uncover and fortify the security loopholes that provide a backdoor entry to privileged data.

2. Build an inventory of service account credentials and dependencies.

To establish accountability and control over service accounts, IT admins need to develop an inventory of associated applications, users, and services that depend on the respective service accounts. Organizations should take the following steps to build a service accounts inventory:

- Establish a clear-cut workflow for service account creation, onboarding, and usage tracking.
- Scan the application environment periodically to discover newer service accounts, and the services, applications, and other service accounts they are connected to.
- Ensure that service account credentials are regularly rotated and updated based on standard password policies.
- Review the status of service accounts: active, inactive, and deleted. Ensure that expired service accounts are removed from the network.

3. Secure access to service accounts.

To counter the risks of service account abuse, organizations should strongly consider investing in privileged access management (PAM) solutions, which aid in streamlining the management of the service account lifecycle. PAM tools enable IT admins to develop strong governance over the service accounts spread across the corporate network using effective automations to discover, secure, and monitor access to these accounts. A strong PAM solution provides a secure vault to store and rotate the credentials of service accounts, and allows sharing of passwords to non-admin users based on specific requirements. This helps prevent unauthorized access to service accounts, and safeguards these accounts from privilege misuse.

Integrating PAM tools with SIEM tools and IT analytics tools enables IT admins to monitor user activity with these accounts, identify and contain abnormal behaviour, and adhere to compliance policies by generating real-time reports.

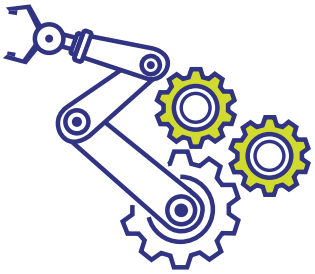
4. Establish sound governance of service accounts.

It is important for organizations to assert governance over service accounts and passwords by building specific security controls based on existing policies and standards. This includes assigning ownership, roles and responsibilities for privileged users, and delegating ownership with a role-based sharing system for users, owners, admins, and superadmins (approvers). Besides user training and education, organizations need to establish a well-defined workflow for service account creation, review, and mapping processes to gain complete visibility over these accounts.

The service account workflow should address these questions:

- Who should create service accounts, and who should approve access to them?
- Who will be the default owner of service accounts?
- How often will these accounts be reviewed? Will the review process be aligned with internal policy and/or compliance requirements?
- What will be the password policy for service accounts?
- If a service account has to be renewed, does it have to go through an approval process that is similar to account creation?
- Is there a provision to automatically decommission expired/inactive service accounts?

5. Embrace automation.



Establishing a tangible workflow can streamline the management of service accounts, but it is almost impossible to manage the entire lifecycle of every account in a large scale environment. This is where automation comes into play.

Once a well-defined workflow is put in place, organizations can leverage automation tools that can centralize the management of service accounts. These tools help IT admins gain granular control over service accounts, and aid in managing the complete account lifecycle from automatic discovery, to building workflow templates that comply with internal policies, to providing compliance reports to meet security objectives.

Automating service account management empowers privileged admins to create and review designated users, groups, and roles, as well as secure access to service accounts. Some automation tools enable admins to provision and de-provision service accounts automatically, and provide admins with options to customize their workflows based on specific business requirements, and type of service account request.

To proactively prevent misuse, automation tools provide real-time status reports for service accounts, and help admins decommission expired or inactive accounts without disruptions in operations. In addition, these tools notify admins whenever service accounts are created, approved, renewed, and deleted.

ManageEngine PAM360

ManageEngine PAM360 is a unified privileged access management solution for enterprises. It enables IT administrators and privileged users to gain granular and complete control over critical IT resources, such as passwords, digital signatures and certificates, license keys, documents, images, service accounts, and more.

Recognized by Gartner and Forrester as one of the top PAM vendors of 2020, ManageEngine PAM360 includes contextual integrations with SIEM, ticketing and analytics solutions to help IT teams build user behaviour models to identify and terminate anomalous activities, generate comprehensive audit and compliance reports, and take data-driven security decisions.

www.manageengine.com/pam360

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.manageengine.com/pam360

ManageEngine
PAM360