Brought to you by

thycotic

Service Account Security

for dummies®
A Wiley Brand

Identify your service account risks

Establish account security and governance

Safeguard service accounts

Joseph Carson, CISSP

Thycotic Special Edition

About Thycotic

Thycotic is the leading provider of cloud-ready privilege management solutions. Thycotic's security tools empower over 10,000 organizations, from small businesses to the Fortune 500, to limit privileged account risk, implement least privilege policies, control applications, and demonstrate compliance. Thycotic makes enterprise-level privilege management accessible for everyone by eliminating dependency on overly complex security tools and prioritizing productivity, flexibility, and control. Headquartered in Washington DC, Thycotic operates worldwide with offices in the UK and Australia. For more information, visit **www.thycotic.com.**

Service Account Security

Thycotic Special Edition

by Joseph Carson, CISSP

for dummies®
A Wiley Brand

Service Account Security For Dummies®, Thycotic Special Edition

Published by

John Wiley & Sons, Inc.

111 River St.

Hoboken, NJ 07030-5774

www.wiley.com

ISBN: 978-1-119-68605-7 (pbk); ISBN: 978-1-119-68606-4 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Carrie Burchfield-Leighton

Editorial Manager: Rev Mengle

Acquisitions Editor: Ashley Coffey

Business Development Representative: Yemily Lopez

Production Editor: Mohammed Zafar Ali

Introduction

Privileged service accounts are a top target for cybercriminals and malicious insiders because they allow the attacker to access sensitive data while staying hidden behind the disguise of legitimate services. This veil allows them to move around corporate networks and cloud environments undetected, carrying out malicious activity such as stealing sensitive information and conducting financial fraud. Service accounts allow attackers to elevate privileges to easily access sensitive databases and maintain persistent access.

Privileged service accounts represent major challenges for businesses. Service accounts exist in every organization, running in the background, helping automate applications and IT services that are critical to business success. Failure to properly manage service accounts leads to significant cybersecurity risks that organizations must prioritize and address. That's especially true for organizations with large active directory environments, large server farms, virtual environments, and DevOps teams. Most organizations' service accounts are too numerous to be managed manually, which leads to misconfigurations, inconsistent security, and default passwords that leave them vulnerable to compromise and exploitation.

About This Book

Almost all organizations suffer from service account sprawl, perpetuating the unmanaged, uncontrolled expansion of their privileged account attack surface. *Service Account Security For Dummies,* Thycotic Special Edition, is meant to help you and your organization get control of your service accounts, manage them more effectively, and reduce the risk of service accounts being compromised and abused. It also explains the nature of service accounts and the significant risks associated with them. It demonstrates how organizations typically manage service accounts today and where they come up short in properly managing and protecting them. I also give you recommended steps to take to implement service account security best practices and protect your organizations from a serious breach or insider abuse of privileges.

While privileged access management (PAM) covers all privileged access security, this book focuses on privileged service account security challenges and best practices.

I wrote this book for IT managers, administrators, systems administrators, and security professionals who are responsible for protecting their organizations from criminal hackers, cybercriminals, and malicious insider threats. This content assumes a basic level of IT expertise and experience, including familiarity with IT networks and the use of privileged accounts (human and non-human) across the organization.

Icons Used in This Book

This book uses the following icons to indicate special content.

REMEMBER

You don't want to forget this information. It's essential to gain a basic understanding of service account security.

WARNING

Watch out! Pay close attention to these details. They focus on serious issues that have a major impact on you and your organization's security.

TIP

The Tip icon points out practical advice that saves you time and effort in putting together your own service account security strategy.

Beyond the Book

Discovering and getting control of your service accounts only *begins* with this book. Many automated tools help you manage your service accounts — and within the limited resources that seem to constrain nearly every organization. To help you plan and execute your own service account management strategy, visit `www.thycotic.com` for free resources, including software tools, white papers, videos, and product information.

IN THIS CHAPTER

- Describing service accounts
- Seeing the risks service accounts pose

Chapter 1
Defining Service Accounts and Their Risks

Every organization has multiple IT services that have programs running in the background of operating systems and springing into action when called on by a user, an application, or other services. In many medium- to large-size organizations, hundreds or thousands of services may be running across a network that access equal numbers of resources. Just like human users, these services require access to servers, databases, and other resources, and therefore need the associated service accounts.

Understanding a Service Account

Service accounts are specialized non-human privileged accounts typically used within operating systems to execute applications or other services so they can access data and network resources to perform specific tasks. Service accounts operate with associated privileges (or a defined account created during the installation of an application) that require certain local system privileges to function and/or to connect with other network resources. With this in mind, the operation of service accounts often requires elevated privileges and access to business-critical applications and data.

Because service accounts have high-level system and network privileges, they're an attractive high-valued target for cybercriminals. Within certain systems, service accounts are named differently:

- **In UNIX and Linux:** Service accounts are known as *init* or *inetd* and can execute applications.
- **In the cloud:** Service accounts are referred to as *cloud service account, cloud compute service accounts,* or *virtual service accounts.*
- **In Windows:** Service accounts are known by the most common types listed here:
  - LocalSystem
  - NetworkService
  - Local user account
  - Domain user account


WARNING

Gaining control of a service account opens a pathway to attaining sensitive data, allowing an attacker to freely roam and explore your network while remaining undetected for weeks, months, or even years. Cybercriminals target service accounts because they prefer the easiest technique for gaining persistent access and appearing to be part of your normal IT operations.

Posing Major Security Risks

The person responsible for managing your *services* is likely not the one responsible for your *service accounts*. Unlike many types of privileged accounts, service accounts aren't tied to a unique human identity and often fly under IT's radar. There may not be a named person responsible (and held accountable) for service account management, which means that managing service accounts is often ignored or neglected. Service accounts run in the background and can easily go unnoticed and unmanaged for long periods due to various reasons:

- The original person who set up the service account may leave and neglect to pass on vital information about its purpose.
- The original system tied to a service account may no longer be needed, but the account may live on with no control or supervision.

- Service accounts may have been set up for temporary purposes, such as software installation or system maintenance, but left in place long after their use.
- Cloud-based service accounts used to accelerate development cycles or as part of a DevOps workflow can be particularly difficult to find and manage. Containers and microservices get provisioned quickly and are often abandoned quickly after use without proper disposal. Many containers also reuse credentials or have hardcoded keys that allow attackers to repeatedly gain access.

Typically, no records are kept as to why a specific service account exists, who has access, what services depend on it, and when it should be reviewed, disabled, or deprovisioned.

Updating or changing credentials for service accounts is risky because this practice can affect running services with a chain of dependencies. Service accounts are difficult to map to business services that rely on them. Also former employees, contractors, or consultants can remember credentials and reuse them for other companies, meaning the credentials are no longer unique and possibly already exposed. Or even worse? They can use them for unauthorized access.

WARNING

With limited options for managing service accounts, many organizations have developed poor security practices:

- Giving excessive privileges or overprivileged service accounts
- Never rotating or changing service account passwords
- Leaving default passwords in place that are never changed
- Leaving interactive logon enabled
- Using the same account for multiple services — violating the principle of least privilege
- Using poor service account naming conventions
- Hardcoding passwords or storing them in plain text
- Sharing an account between services and people and using the same password for multiple accounts

Any one of these practices can pose significant risks, yet they are commonly found in most organizations because security is often sacrificed for convenience. When security becomes too large of a management burden, it takes a back seat to keeping systems up and running smoothly for business users. This trade-off must

be resolved if you are to effectively secure service accounts and reduce business risks.


TIP

Ideally, organizations should strive for a 1:1 service account to service relationship with every account set to only the privileges that the corresponding service requires. Service accounts are often reused for multiple services, so it's easier to give them elevated admin-level privileges, which violates the concept of least privilege.

IT admins are often reluctant to decommission service accounts because their dependencies can be difficult to ascertain, and their removal can lead to "catastrophic" service disruptions. This reluctance leads to runaway service account sprawl, expanding the privileged account attack surface to proportions that are hard to manage without automated tools.

SERVICE ACCOUNTS: A FAVORITE TARGET

In the *2019 Black Hat Survey Report* conducted by Thycotic, hackers and security professionals were asked about current practices and risks associated with service accounts. Twenty-four percent of security professionals said service accounts were their most vulnerable targets for attacks by cybercriminals.

According to both security professionals and hackers alike, the top reasons why service accounts are such an attractive target for exploitation are

- Easily elevated privileges
- Access to valuable/sensitive data
- Persistent access
- Under-the-radar movement across the IT environment

Among survey respondents, both hackers and security professionals agree that the best ways to protect service accounts from compromise include

- Removal of unnecessary service accounts
- Frequent credential rotation
- Privileged account activity monitoring to detect suspicious behavior

IN THIS CHAPTER

- Following the PAM life cycle approach
- Being service account compliant

Chapter 2
Achieving Success with Automated Governance

Standardizing, provisioning, tracking, maintaining, and decommissioning of service accounts is virtually impossible without the proper tools to automate the process. Therefore, those responsible for managing service account privileges and access need a solution to discover, document, secure, establish governance, monitor, and eventually decommission service accounts.

Properly managing service accounts must include discovering and maintaining an inventory of the type of credentials they use, and where and how they're stored and managed. They also need to secure, monitor, and track where and how the service accounts are used to prevent, detect, and suppress unauthorized usage and decommission safely when appropriate.

Taking a PAM Life Cycle Approach

Service account governance falls under the umbrella of privileged access management (PAM). As you establish your plan for service account management, you should apply the broader PAM life cycle approach to guide decisions and implementation. In Figure 2-1, you see the key stages of the PAM life cycle approach, providing

a framework for any organization to manage its privileged access as a continuous program.

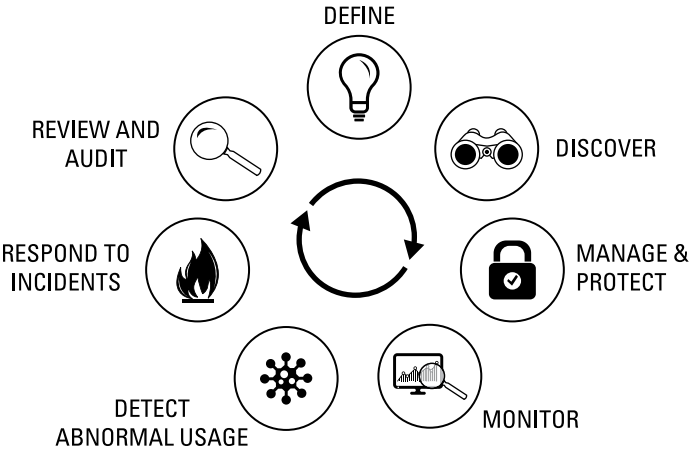

FIGURE 2-1: The key stages of PAM life cycle management.

Within this broader context, there are certain considerations you should incorporate that relate specifically to service accounts:

- **Creation/approval process:** As new applications are being deployed, ensure you have an automated service account creation and approval process. Align this with your review and audit process to ensure that more sensitive applications have strict security controls.
- **Service dependency mapping:** Map and record dependencies as part of your privilege management plan because making changes to one service account generally impacts others.
- **Continuous discovery:** Discover service accounts that may have been created outside of an approved process or life cycle. After that, include them in the standard workflow, so they are properly reviewed to ensure the correct security policies have been applied.
- **Security and governance risk assessments:** Map compliance requirements to the appropriate security access controls, implement them, and report on governance.
- **Automated auditing and reporting:** Monitor, record, and report on service accounts usage and changes as part of

your privileged access review and audit. This helps distinguish between authorized and unauthorized changes.

- **Updated and reviewed security controls:** Group service accounts according to similar risks and categories. Review along with other privileged accounts to ensure that the correct security controls are set for each service account.
- **Expiration/review process:** Set a review date or expiration date to determine whether the application is still required. This should be done as part of the creation process as well as part of continuous discovery.
- **Removal of unused/expired service accounts:** Continuously remove unused services accounts to reduce the privileged security attack surface. Deprovisioning is a critical stage of the life cycle that's often overlooked with service accounts.

TIP

For further information on the PAM life cycle, visit `thycotic.com/resources/experts-guide-to-advanced-pam-success`.

Demonstrating Service Account Compliance

Managing service accounts, like other privileged accounts, is critical to meet regulatory and compliance requirements for access security controls. This means your organization must demonstrate compliance for password management, privilege access management, as well as use clear naming conventions and regularly audit. Implementing the principle of least privilege for service accounts along with life cycle management should be the guiding principles for assuring you can meet policy and regulatory requirements.

TIP

To help ensure that you can demonstrate compliance, check out these resources:

- `thycotic.com/ciso-quick-guide`: CISO's Quick Guide to Access Control and Cyber Security Compliance gives you key access control requirements for your businesses MFA, Auditing, and Discovery practices.
- `thycotic.com/StateOfPAMCompliance`: The Global State of Privileged Access Management Risk and Compliance

provides recommendations for developing a PAM life cycle security program.

- `https://go.thycotic.com/nist-fisma-compliance`: FISMA/NIST Privilege Management Mandate Compliance helps you meet requirements for steps that federal agencies and government contractors must take to comply with privilege management in FISMA/NIST SP 800-53.
- `https://go.thycotic.com/iso-compliance`: PAM Mapping to ISO 27001 Controls meets the ISO 27001 standard for implementing an InfoSec Management System, which applies a risk management process and gives confidence that risks are adequately managed.
- `https://go.thycotic.com/pci-dss-compliance`: PAM Mapping to PCI DSS 3.2 meets PCI DSS requirements for accepting, storing or transmitting credit card data with guidelines for privilege management and a framework to protect cardholder data.
- `https://go.thycotic.com/hipaa-compliance`: PAM Compliance Requirements for HIPAA help any organization that creates, receives, maintains, or transmits electronic protected health information (ePHI) in the U.S. that must meet HIPAA requirements for access control and data sharing.

IN THIS CHAPTER

- Starting with service account discovery
- Establishing governance and accountability
- Evaluating automated tools

Chapter 3
Five Best Practices to Control Service Accounts

Implementing service account governance can often seem like an overwhelming task. This chapter gives you the five best practices to get you started. By focusing on these areas, you begin to get control of your service accounts, continuously manage them, and automate where possible. These five key activities you need to implement are shortened and simplified for this book.


TIP

For a complete list of best practices, check out this webinar: thycotic.com/company/blog/event/top-10-service-account-management-best-practices.

Discover Your Service Accounts

Without knowing where all your privileged service accounts are, you may have "backdoor accounts" that allow users and cybercriminals to bypass proper controls and auditing to compromise accounts. Malicious insiders can also create service accounts to gain access to sensitive information, and these accounts can go undetected for months or even years.

TIP

Use an automated solution to discover privileged accounts initially and on a continuous schedule. Scan your entire network and identify dependencies to avoid potential disruptions.

Document, Classify, and Inventory All Service Accounts

IT staffers often don't have the time, tools, or inclination to inventory all service accounts. This means many service accounts may exist without oversight or accountability. You must create a record that explains why accounts exist, which employees have credentials to access them, and which service(s) depend on this service account.

REMEMBER

Don't forget to include in the record when the service account should be reviewed, deactivated, or deleted.

Secure Access to Each Service Account

Customized credentials need to be associated with each service account. You should already have them in a centralized vault, and credentials should be limited only for necessary access. If you're just discovering the account, change passwords immediately and put them on a rotation schedule along with a "heartbeat" running to make sure that someone else hasn't gained access or changed them outside the system. Using an automated privileged access management (PAM) solution is a must to accomplish this.

REMEMBER

Keep in mind that not all service accounts use passwords; some are set to system and some use SSL KEYS, which are commonly used means of authentication within enterprise IT environments. Given their lack of visibility, IT groups often overlook these credentials when building a privileged access security strategy.

Establish Governance and Assign Accountability

Establish a governance plan for managing service accounts. Assign ownership to individuals and build a role-based permission

system that encompasses administrators, requesters/owners, and approvers.

Administrators should standardize when service accounts are created in accordance with company policy. Which organizational unit should they be assigned to? What other attributes should be required? Administrators need to answer these questions when setting up an account.

Provide the appropriate workflows for people who need to create service accounts, and ensure they go through the appropriate approval process. This process is where ownership should be assigned. Who will approve the requests for new accounts? Often one or a combination of the requestor's manager, a business owner, IT admin, or security personnel is responsible for approving new account creation.

Achieve Service Account Automation

When planning to automate service account security from provisioning through decommissioning, start by asking these key questions:

- How often should the service account be reviewed? This can be internal policy or dictated by compliance requirements.
- If the account can be renewed, can the account owner do it themselves or should the renewal go through the same approval process as when it was first created?
- Are there options for decommissioning an account? Do you want it disabled, expired, or deleted?
- When it comes time to decommission a service account, what is the appropriate process? Should it be up to the owner to do it, or should an automated tool be used?

After that, when evaluating and implementing your service account automation solution, keep in mind the following key capabilities:

- **Establish workflow.** Using automated tools, you need to establish workflows for tighter control over service accounts. Start with workflow templates to get familiar with what

works for you and then apply customizations to provide further visibility and control.

- **Delegate ownership.** Delegate ownership with role-based permissions. Role-based permissions should govern user access, setup, and the request workflow. You should select automated tools that empower you to create users, groups, and roles aligned to the needs of your business.
- **Provision service accounts.** Look for tools that allow you to provision service accounts seamlessly and automatically. Administrators should be able to define workflows for the provisioning process by setting required approvals for each type of service account request.
- **Enforce governance.** An effective automated tool should allow you to enforce governance with designated accountability and ownership over every service account.
- **Decommission accounts.** To minimize sprawl and reduce your attack surface, you need to decommission accounts automatically without causing disruption through notifications that trigger when accounts should be renewed, reapproved, or even deleted. Decommissioning is more than simply deprovisioning. You need to review, disable, expire, and then delete/deprovision all service accounts.

REMEMBER

Before you start implementing your service account security strategy, you must evaluate your options for automated solutions that enable these best practices. Only through automation can you control your service account sprawl and properly protect your organization from the perils of compromised privileged credentials — whether they're on-premises or in the cloud.

FREE RESOURCES FOR
SERVICE ACCOUNT SECURITY

WHITEPAPERS AND REPORTS

KuppingerCole: "Privileged Access Governance"
Understand the shortfalls of IAM/IGA and SIEM tools to govern non-human service accounts and prevent insecure service account sprawl. See how a new generation of automated Privileged Access Governance solutions can help you implement service account control and security.

https://thycotic.com/why-thycotic/analysts-opinions/kuppingercole-whitepaper-privileged-access-governance/

Black Hat 2019 Hacker Survey Report
Thycotic surveyed attendees at Black Hat 2019 focusing on cyber security issues associated with privileged account access, particularly for service accounts. Hackers and security pros strongly agree service accounts are an attractive target because hackers can easily elevate privileges and gain access to sensitive information.

https://thycotic.com/resources/black-hat-2019-hacker-survey-report/

Privileged Account Management (PAM) For Dummies
Gain a practical understanding of privileged account management. This book describes what privileged accounts are, where they reside and how they function. It also explains the risks associated with these accounts and how you can best protect them.

https://thycotic.com/resources/wiley-dummies-privileged-account-management/

SERVICE ACCOUNT TOOLS AND TRIALS FOR IT PROFESSIONALS

Service Account Discovery Tool For Windows
Thycotic's free tool, Service Account Discovery Tool for Windows, measures the state of privileged access entitlements in your Active Directory service accounts and exposes areas of highest concern in your attack surface. After running the Snapshot tool you'll receive a customized, prioritized risk report you can download and share.

https://thycotic.com/solutions/free-it-tools/service-account-discovery-tool/

Free Trial of Thycotic's Account Lifecycle Manager
Thycotic's Account Lifecycle Manager is a solution that automates and streamlines the full privileged account lifecycle of service accounts, finally allowing you to control service account sprawl. Now you can easily secure, provision and decommission service accounts to harden and ultimately shrink your attack surface with Account Lifecycle Manager. The free trial includes the full version of Account Lifecycle Manager, with all features enabled and access for 10 users, for 30 days.

https://thycotic.com/products/account-lifecycle-manager/start-a-trial/

Free Privileged Account Management (PAM) Risk Assessment Tool
Here is a fast and easy way to assess your privileged account security risks. This free tool from Thycotic takes less than 10 minutes to complete, providing you an immediate Risk Score to help evaluate your current PAM practices.

https://thycotic.com/solutions/free-pam-risk-assessment-tool/

Protect your service accounts!

Service accounts abound in every IT environment, but typically are managed manually with little oversight and no accountability. They're a favorite target for cybercriminals who can exploit them to roam your network undetected. This book helps you get control of service account sprawl and develop a strategy to properly protect service accounts. You gain key insights into how best to implement service account governance and day-to-day management practices with the help of automated cybersecurity tools.

Inside...

- Understand the role of service accounts
- Why service accounts pose major risks
- Protecting service account credentials
- Following a PAM life cycle approach
- Best practices to control service accounts
- Success through automated governance

thycotic

Joseph Carson, an infosec award winner, has 25+ years of experience in enterprise security. He's authored *PAM For Dummies* and *Least Privilege Cybersecurity For Dummies*. Joseph is an active member of the cyber community and speaks at global conferences, advising governments and critical infrastructure, financial, and maritime industries.

Go to Dummies.com™
for videos, step-by-step examples, how-to articles, or to shop!

ISBN: 978-1-119-68605-7
Not For Resale

for dummies®
A Wiley Brand

Also available as an e-book

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.