Resources

https://social.technet.microsoft.com/Forums/lync/en-US/3478c201-26a8-4bb1-a5e3-20c2521e321b/difference-between-service-account-and-user-account?forum=winserverDS

https://unix.stackexchange.com/questions/314725/what-is-the-difference-between-user-and-service-account

https://serverfault.com/questions/713108/distinguish-between-users-and-service-accounts-in-active-directory

https://delinea.com/blog/service-accounts-vs-user-accounts

Service Accounts vs User Accounts

A service account, a.k.a. technical account is an account that is designed to only be used by a service / application, not by a regular user. User accounts are used by real users, service accounts are used by system services such as web servers, mail transport agents, databases etc. Application and service developers want these accounts to restrict the associated processes rights and privileges instead of running their processes as root. Services as started by init, systemd or similar, which run as root, quickly downgrade to the service account to limit the risks. Service accounts can be created like ordinary user accounts (e.g. using useradd). However, service accounts are typically created and configured by the package manager upon installation of the service software. So, even as an administrator you should be rarely directly concerned with the creation of service accounts.

For good reason: In contrast to user accounts, service accounts often don't have a "proper" login shell, i.e. they have /usr/sbin/nologin as login shell (or, back in the old days, /bin/false). Moreover, service accounts are typically locked, i.e. it is not possible to login (for traditional /etc/passwd and /etc/shadow this can be achieved by setting the password hash to arbitrary values such as * or x). This is to harden the service accounts against abuse. Having individual service accounts for each service serves two main purposes: It is a security measure to reduce the impact in case of an incident with one service (*compartmentalization*), and it simplifies administration as it becomes easier to track down what resources belong to which service.

Service accounts and user accounts are prime targets for cyberattacks, and every organization has a combination of both types of accounts. Once one of these accounts is compromised, a cyberattacker can move laterally, infiltrate the business, and access critical data. Let’s go over the fundamentals of user accounts and service accounts. To best protect against cyberattacks, it’s important to understand the basics of user accounts and service accounts—they are not the same thing!

What is a service account?

A service account, sometimes referred to as a system account, is a non-human privileged account usually located within operating systems and used to run applications or services. As a type of privileged account, service accounts have associated privileges, including local system privileges. Service accounts require elevated privileges to function, connect to resources on the network, and access sensitive data and applications. Cybercriminals target service accounts because they have access to business-critical IT infrastructure and data.

Service account nomenclature

In Windows: Service accounts are referred to as:

- LocalSystem
- NetworkSystem
- Local user account
- Domain user account

In Unix & Linux: Service accounts are referred to as:

- Init
- Inetd

In the cloud: Service accounts are known as:

- Cloud service account
- Cloud computer service accounts
- Virtual service accounts

Service account risks

Service accounts pose an interesting yet troubling risk to organizations. Service accounts are not associated with any human identity and may not be directly managed by a human. On top of this, service accounts' privileges and functions make them critical to IT infrastructure and business applications. It's no exaggeration to say that service accounts are digital phantoms, as organizations usually do not keep records on existing service accounts.

It's no surprise business leaders are terrified of directly managing their service accounts, lest something goes wrong and a business function is crippled—or worse! Changing service account credentials can have a chain reaction on dependencies. It's challenging for organizations to deal with their service accounts when there are no records detailing what the accounts do and what they affect.

Service accounts go unchecked because:

- The person who created the service account left and did not give anyone any information about the service account
- The service account's original system no longer exists but the account still remains, uncontrolled
- A service account was originally created for a temporary reason like a program install, but the account remains in place after the task is complete
- Cloud-based service accounts used in development or DevOps are hard to manage, with microservices and containers getting spun up with privileges and burned down quickly without proper cleanup
- Containers used in DevOps often hardcode or reuse credentials

What is a user account?

User accounts are the accounts you are most likely familiar with. Simply put, a user account is an account tied to a human identity. Securing user accounts is critical in safeguarding an organization's systems and data. Let's take a closer look at the two primary kinds of IT user accounts: standard and privileged.

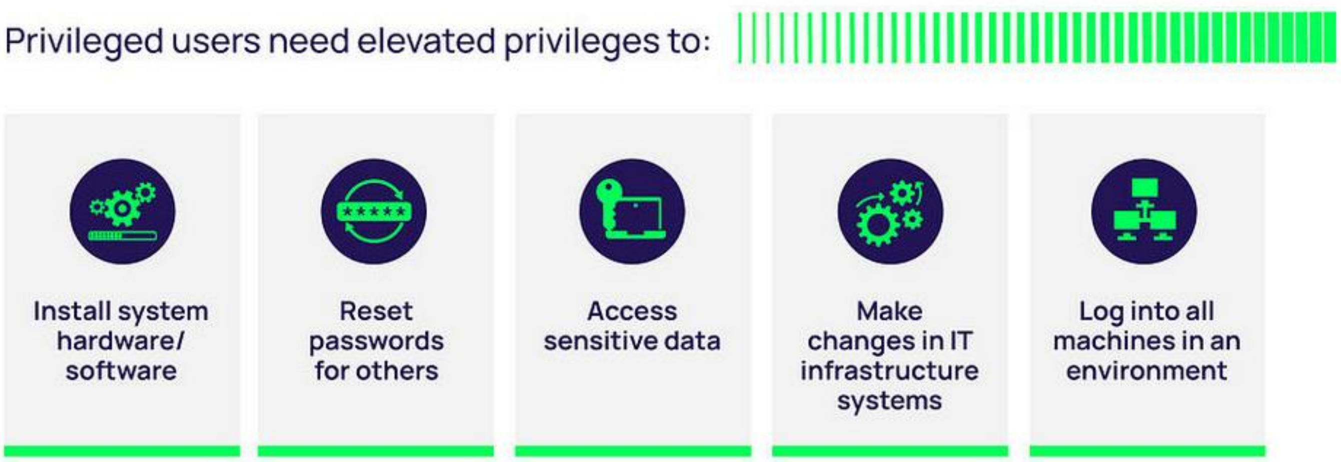
Standard user accounts:

This is the user account you are most likely familiar with—a standard user account represents a human identity and typically has an associated password to prevent authorized access. Active Directory user accounts are an example of standard user accounts. You probably have a number of these accounts yourself both at work and at home. In a typical organization, most employees have standard user accounts as they don't require special data or elevated access rights.

Privileged user accounts:

While securing standard user accounts is important, privileged user accounts have access to sensitive information and elevated privileges. Organizations can have three times more privileged user accounts than physical employees, which requires a balancing act between security and productivity. Privileged user accounts provide administrative access to enterprise systems, according to the permissions levels.

Privileged user accounts are typically used by system administrators, as they manage particular systems, environments, or other IT infrastructure. Privileged users require elevated privileges to do the following:



Privileged users need elevated privileges to:

- Install system hardware/ software
- Reset passwords for others
- Access sensitive data
- Make changes in IT infrastructure systems
- Log into all machines in an environment

While most non-IT employees only have standard user accounts to do their jobs, IT staff can have multiple accounts. An IT administrator could have multiple standard user accounts and privileged accounts, allowing them to access different systems and perform different tasks.