Secant

WHITE PAPER

SERVICE ACCOUNTS

Publication No. 101
Version: November 28, 2011

Service Accounts

OVERVIEW

An account used by an application (rather than a user) can be referred to as a service account. Many network applications such as backup software require a saved set of credentials to run. This standard identifies best practices for creating, configuring, and documenting service accounts.

APPROACH

Security

Many applications require administrative level credentials to run, such as backup software. In order to ensure services run uninterrupted and still maintain the highest levels of security, service accounts should be configured with very strong passwords (that will not be susceptible to brute force attacks). These passwords should then be set to never expire (unless an automated password management solution is implemented) to avoid potential service disruptions.

Consider the requirements of the service account carefully and factor in the principle of least privilege to determine whether the service account should be created locally on one or more systems or created in a directory service (such as Active Directory, eDirectory, or Open Directory). If the service account requires access to the directory service, then it must be created in the directory. If the service account requires access to more than two systems (such as backup software that uses client agents), then the account should be created in the directory. If the service account requires access to two or less systems and does not need access to directory resources, then it is generally recommended to create the account locally. Remember also that if the service account is created in the directory, then the directory must be available for it to authenticate. When an outage occurs the startup order and network availability become important when a service account in the directory is used to start a service. If the directory is not accessible when the server starts, then the service will fail to start. Assign appropriate permissions to each service account by referring to the application's documentation for details on what privileges are required.

Flexibility

To ensure the highest levels of security, it is best practice to change user credentials on a regular basis. Changing passwords is especially important for built-in administrative level credentials because those accounts are the most frequently attacked. One barrier to changing administrative level credentials on built-in accounts on a regular basis however is the usage of those credentials within applications such as backup software or database software, etc. When administrative credentials are used in this way, changing the password to such an account can result in application failures, backup failures, and scheduled maintenance routine failures. Thus, it is best practice when configuring applications with saved credentials, to always use a designated service account rather than a built-in administrative level account. This ensures the flexibility of changing built-in administrative level passwords on a regular basis and on an as-needed basis without impacting network services.

AUDITING

To support detailed security auditing, it is recommended that each application that requires saved credentials be configured with its own set of credentials. Thus, for example, if a server shuts down for an unknown reason, then security logs can be examined to determine which account initiated the shut down and determine if it was initiated by a particular application.

IMPLEMENTATION

Naming Convention

The service account naming convention for an application is **svc-applicationname**. For systems that do not support hyphens in the username, then omit the hyphen (example: **svcapplicationname**). Note that no spaces should be used in the username. If the service account is not being used by a specific application, then instead of applicationname, use a description of how the account is being used. For example, **svc-sql1scripts**.

Service Account Usernames

The following are recommended Service Account usernames for the specified applications. This is not a complete list by any means but does provide guidelines for some common applications.

Application	Service Account Username
CA ARCserve Backup	svc-arcserve
HP SIM	svc-hpsim
Secant Email Defender	svc-defender
Sophos	svc-sophos
Symantec Backup Exec	svc-backupexec
Veeam Backup	svc-veeam
Vizioncore vRanger	svc-vranger
VMWare Capacity Planner	svc-cplanner
VMWare vCenter	svc-vcenter

Group Membership

Appropriate permissions should be assigned to each service account using group membership. Use the principle of least privilege to assign permissions. For example, if an application requires administrative level permissions on only one server, then assign administrative group membership on that server only.

Passwords

Service account passwords must be strong passwords and must meet the following minimum requirements:

- 12 characters in length
- Three of the following four attributes
  - Contains one or more lowercase alphabetic characters
  - Contains one or more uppercase alphabetic characters
  - Contains one or more number characters
  - Contains one or more non-alphanumeric characters
- Passwords must not be composed of one or more dictionary words

Passwords must be documented appropriately.

Changing service account passwords every 18 to 24 months is recommended.

800.875.4222 | SECANTCORP.COM