White Paper:
Service Management and the Logon Cache

Rev 2 – June 1, 2006

Lieberman Software Corporation
http://www.liebsoft.com

Abstract

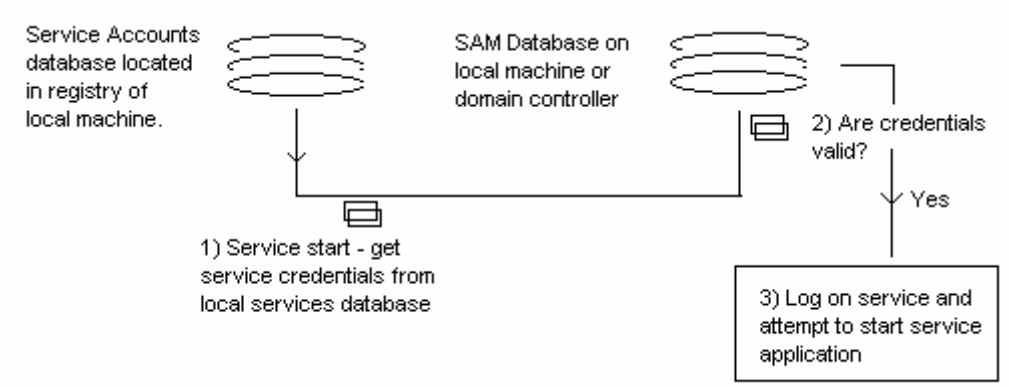
Updating the service accounts on laptops and other machines that periodically disconnect from their domain controller opens a can of worms unless special tactics are taken at the time of change.

Many organizations use services on their laptops that reference domain administrator accounts. When the laptop disconnects from the network, the service can fail immediately, or at the next system restart when the remote domain controller cannot be found (they are kind of hard to find at 35,000 feet on an airplane). In this article we will explain the problem and solution to this conundrum.

Contents

1. Service Logon Authentication

Each service on a machine stores its logon credentials in an encrypted area of the registry. If the service uses the Local System account or a locally stored administrator account, there are usually no problems if the credentials are changed (other than handling off-line machines). Shown below, are the authentication steps that a service takes when starting.

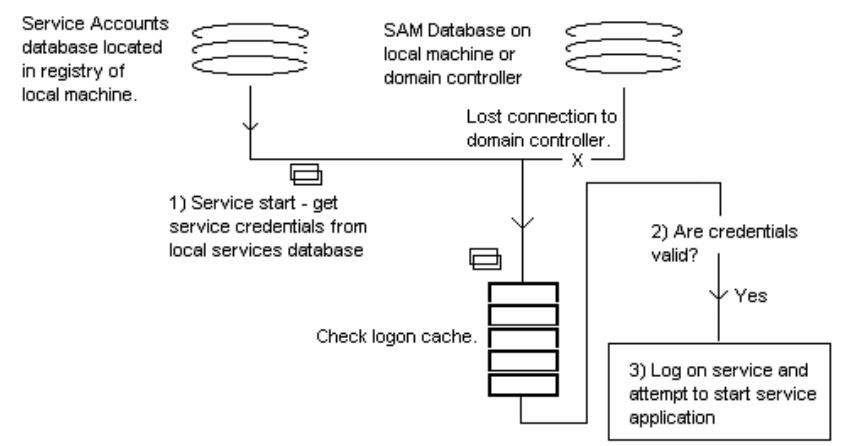


2. Domain Controller Problems and Laptops

When a service uses a domain administrator account, it must contact a domain controller and verify that the account and password specified are correct before the service can start. What would you imagine happens if the domain controller is unavailable or if you are running from a laptop that is disconnected from the network? Right, the service fails to start due to no way to authenticate the service.

The problem can be even worse for production servers that temporarily lose their connection to a domain controller and cause their working services to fail.

The trick to solving this problem is to logon interactively at each and every machine with each domain administrator account used by services on each machine. By performing an interactive logon, you can put the domain administrator credentials in the "logon cache" of the machine. When the domain controller cannot be found, the service will automatically check the logon cache to verify the credentials, and if they are correct, the service will start correctly and operate as though the domain controller is actually there.



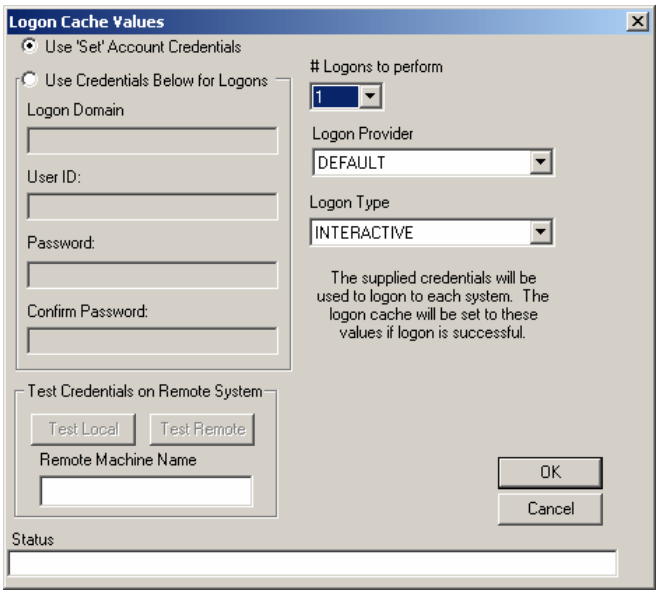
The problem with this strategy is that Microsoft provides no published method of writing a program to update the logon cache of each machine other than walking up to each machine.

Tip! If you are evaluating third party tools for service management, check if they are capable of managing the logon cache of the systems.

3. Solution to the Logon Cache Problem

In Lieberman Software's **Service Account Manager™**, an additional option called Update Logon Cache is available.

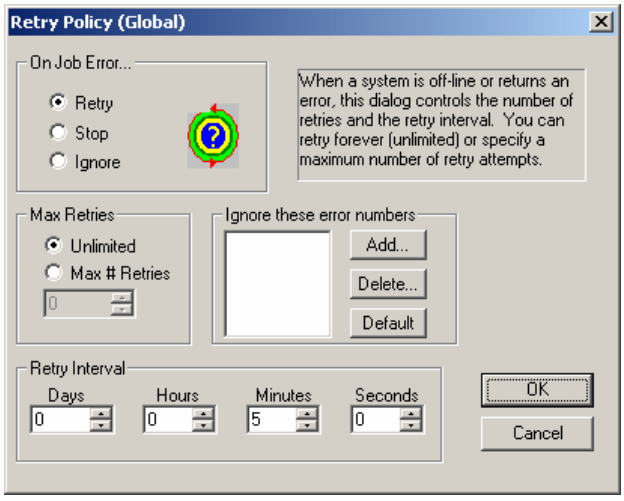
This feature allows the administrator to perform a remote logon with the new service account credentials. The type of logon as well as the number of logons to perform is controllable. By controlling the number of logons, the administrator can assure that all changed services will find their credentials locally in the cache.



4. Hitting Off-Line Machines with Auto Retry

There is no point to worrying about the logon cache if the laptop is not connected to the network at the time you are attempting to make a change. The solution to this problem is the inclusion in **Service Account Manager** of an auto-retry feature in the service management program.

Using this feature, an administrator makes a request to change all machines at the same time. At the end of the operation, all of the machines detected as off-line are put onto an auto-retry queue. The administrator can then forget about the missed machines knowing that they will be changed as soon as they are detected on the network.



5. Summary

The tools provided by Microsoft and third parties essentially ignore the logon cache and off-line machine problem when managing services. This leaves administrators on their own when attempting to change the services on laptops. Lieberman Software's **Service Account Manager** provides an elegant transparent solution to all of these challenges.

Our support staff is available to answer your technical questions whether you are a customer or not.

Voice: 800.829.6263 (USA/Canada) Voice: (01) 310.550.8575 (Worldwide) Fax: (01) 310.550.1152 (Worldwide)
Web: www.liebsoft.com Email: support@liebsoft.com

Microsoft GOLD CERTIFIED Partner

