White Paper:
Service Account Lockouts

Rev 2 – June 1, 2006

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

Abstract

Trying to change service-based applications such as Microsoft Exchange is not as simple as it seems. Many administrators find themselves with locked out domain administrators and no idea what happened. Changing a Domain Administrator account that is used by a service is not as simple as it seems. The steps for the change are pretty well understood, but many administrators neglect to take into consideration issues of replication time to backup domain controllers and account lockout policies. In this article we will examine all of these issues and present a strategy for making service changes successfully.

Contents

1. Changing an Existing Domain Administrator Account

If an existing domain administrator account is already in use and it is desired to just change the password of the account (for security purposes), the administrator must first change it at the domain controller, and then change the services that reference the account, except all passwords must be updated.

This seemingly simple procedure of changing the domain controller then the services that reference the just modified account is fraught with many problems. First, changing the domain controller information does not mean this change is instantaneously replicated to all other domain controllers. If you change a service log on account, start the service, and it tries to authenticate to a domain controller that has not yet received the updated information, the service will fail to start due to bad credentials.

Some services that use a domain administrator account are constantly logging on and off with different credentials (i.e. Microsoft Exchange). If you have just changed a domain administrator account used by a service at the domain controller, but have not gotten around to updating the service that is logging on and off constantly, the service will begin to fail and shut down due to its using old credentials.

Another scenario involves so-called good security policies. Many companies implement account lockout. Some go so far as to implement permanent lockout of administrator accounts if they exceed a fixed number of bad password attempts. If you are in the middle of changing domain administrator accounts for services, some of the services will inadvertently log on with bad credentials causing an almost instantaneous lock out of the account and subsequent cascaded failure of services throughout the organization since even the correctly configured services will be unable to authenticate to a locked out account.

2. How to Properly Change Domain Administrator Accounts Used by Services

1) At the domain level, turn off account lockout. This can be done in NT 4.0 via User Manager for Domains. In Windows 2000, you will want to make the change in the domain controller policy and force this change immediately.

2) Change the domain-wide account used by the service in User Manager for Domains (NT 4.0), or in the Active Directory of Windows 2000/XP.

3) Force replication of the new account to all BDCs (NT 4.0) via Server Manager, or via the MMC plug-in to force domain replication in 2000.

4) Use the fastest mass management tool possible to change the affected service log on accounts.

5) Once all of the services are confirmed up and running (you may want to do a few refreshes of the changed services to confirm their new account and operational status), go ahead and turn account lockout back on again.

Tip: You may want to leave account lockout off for a little while and examine the Event logs of your domain controllers to confirm that there are no stray services still running with the wrong account settings.

3. Service Accounts that Refuse to Change – Forced Reboots

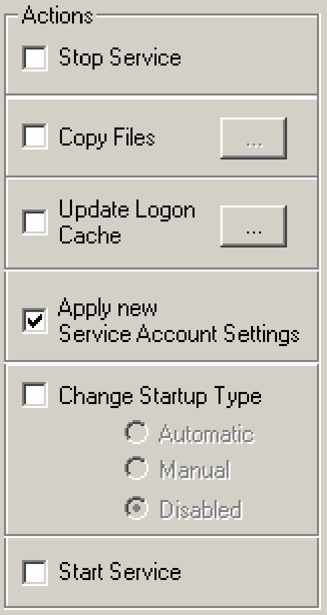
Due to incorrect coding of some application services, after changing the service account, the service will refuse to start correctly. The only solution in these cases is to change the service account without restarting the services (yes, you can change a service account without restarting the service, but the new account is not used until the service starts again). After the service settings have been changed, you can then reboot the systems using the restart option. We have seen this as a necessary procedure for some older versions of Veritas BackupExec. For proper management of these cases, your service management tool should allow service settings changes without restarts as well as a method for specifying a reboot at a specified time

4. Using Service Account Manager™

In Lieberman Software's **Service Account Manager™** you can change the service account settings for any number of services on an unlimited number of machines without restarting (no start or stop service action) the services. Using this strategy you can setup the services to use the new service information when each system restarts or the affected services are restarted (both can be accomplished by **Service Account Manager**). Before restarting the services or restarting the systems, make sure that the new credentials have fully replicated to all domain controllers.

When handling Microsoft Exchange it is sometimes desirable to do a forced restart of the system when changing the service accounts. With **Service Account Manager** you can schedule the restart of the changed systems at a time where you are assured that the new credentials for the service(s) have been fully replicated.

After changing your services it is a good idea to perform a refresh (Get) of all the affected services within **Service Account Manager** to confirm that they have been changed successfully and the account has not been locked out due to a missed credential setting of a service or other application.



Actions

☐ Stop Service

☐ Copy Files ...

☐ Update Logon Cache ...

☑ Apply new Service Account Settings

☐ Change Startup Type

○ Automatic

○ Manual

● Disabled

☐ Start Service

5. Summary

When it comes time to change domain administrator accounts you must turn off account lockouts until the changes have been completed. Take into account domain replication delays and also be on the alert for failed services that may have attempted to use stale credentials. If after performing all the correct steps, it is a good idea to check the event logs of all domain controllers to confirm that no services or other credential users are attempting to use the old credentials. In general we suggest that you do not implement permanent account lockouts since this opens your organization to a denial of service attack that is trivial to implement.

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