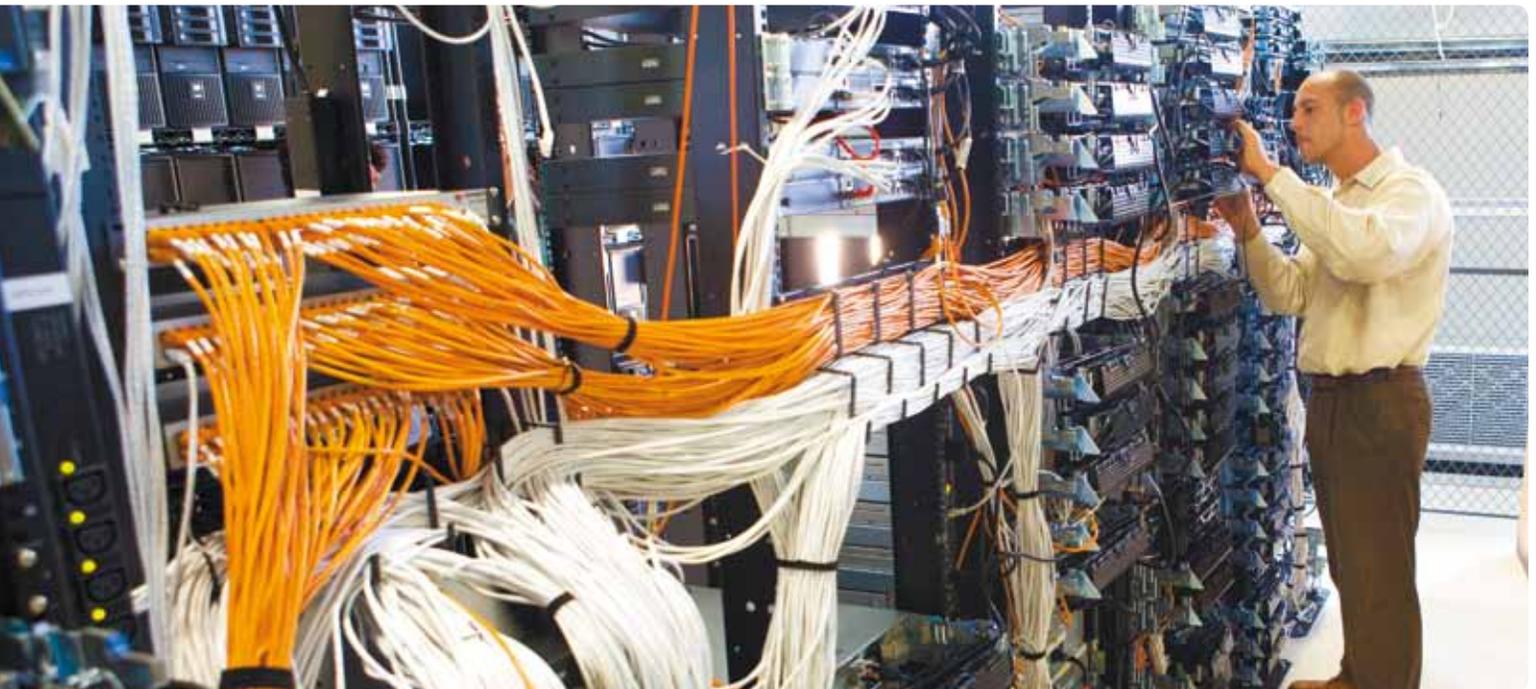


Changed Your Service Account Passwords Lately?

The Secure and Easy Way to Manage Service Accounts



Abstract

Services are a great feature of Windows – but one that most of us don't manage very well, or take full advantage of. Changing service account passwords regularly is important for security and regulatory compliance, and changing service account permissions can make the environment easier to manage. But

we tend not to change either very often, because it's tedious, time-consuming, error-prone and risky.

This paper explores the options available for managing service accounts – including one that makes the job easy, reliable and safe. You'll have no reason not to make your environment more secure and easier to manage.

Plenty of organizations just let sleeping dogs lie, leaving service account passwords unchanged for months or years at a time. There's obviously risk in doing so.

The challenge of service account management

One of the more awkward aspects of Windows administration is the management of service accounts. Even some of the most security-conscious organizations will sheepishly admit that they don't change service account passwords all that often, primarily due to the pain involved in doing so. Changing the password is easy enough, of course – but finding and changing every service that uses the account can be time-consuming, error-prone, and fraught with risk: one mistake and critical services suddenly won't start, leaving users in the lurch.

So plenty of organizations just let sleeping dogs lie, leaving service account passwords unchanged for months or years at a time. There's obviously risk in doing so; the reasons we make users change their passwords every so often apply equally to services, after all. Organizations dealing with legal and industry-mandated compliance run the additional risk of being caught and fined.

It's the same story with service account permissions, which can be used to make your environment easier to operate and support. But if you don't like changing service account passwords manually, there's no way you're going to get excited about changing service permissions by hand.

In short, services are one of those great features that we often don't manage very well, or take full advantage of, because there's no real interface for doing so. Sure, if you've got one server, or maybe two or three, it isn't a big deal to go around to each one and change things. But start expanding that out to a dozen servers, or 50, or 100, and you start wishing that service accounts didn't exist.

Admit it. You've set up services to run as LocalSystem, even though you knew you shouldn't, just so you wouldn't have to create and manage a service account. We all do it: we slack off on service

management because there just doesn't seem to be a better way.

We could build a better way...

The DIY solution

More than a few organizations have sought to address the problem by writing scripts to automate the process of changing passwords. For example, given a list of computers in a file named C:\Uses-AccountA.txt, the following Windows PowerShell command will change the password that the service "ServiceD" uses to log on:

```
Gwmi Win32_Service -Filter "Name='ServiceD'"  
-computer (Gc C:\Uses-AccountA.txt) |  
% {  
  $_.Change($null,$null,$null,$null,$null,$null,$null,"NewPass") }
```

Did you get all that?

Even this approach – which is about the best you can do for a home-built solution – has its downsides. Computers are contacted individually, in sequence, which means changing a large number of computers can be very time-consuming. Moreover, this technique relies on Windows Management Instrumentation (WMI) Remote Procedure Calls (RPCs) for its communications, and RPCs are often thwarted by locally-installed firewalls on server computers.

This technique also assumes that the person running the command is a local administrator on every machine being made. Feedback for errors is minimal, consisting of cryptic numeric codes that aren't completely documented anywhere. In other words, there's likely to still be a decent amount of manual effort involved to handle any exceptions. There's also a real risk in missing machines, because the list of computers must be manually maintained. You essentially have to keep track of which computers are running a particular service under a particular account name – and that can be a lot of lists to keep up with.

You could certainly beef this up a bit, making it into a full script instead of a standalone command. You could add some error-handling to catch errors and log them for manual correction (although the whole point of the exercise was to eliminate manual effort). But no matter what you do, it's never going to be perfect, foolproof or painless.

And there's no way you're going to use a technique like this to modify service permissions. Just no way. So maybe there's a cheap way to do the work manually...

Using the "intern net"

Of course, there's always the time-honored approach to this kind of problem: cheap college labor called "interns." Give one the right permissions and a list of instructions, and let them do the work of logging onto all of your servers, opening the right console, finding the right service, and changing the password. It'll be an afternoon (or two) of Remote Desktop Connection excitement! What could possibly go wrong?

Plenty. This kind of mind-numbingly boring work is the kind most likely to incorporate some human error. A server that didn't make it onto the list of instructions. A mistyped password. Double-clicking the wrong service and changing its configuration. It's almost impossible for a normal human being to complete a task like this without making a simple mistake – and a simple mistake will result in downtime the next time a service (or the whole server) is restarted.

You can't even reliably test the changes that are being made, because doing so would involve stopping and starting each service. Not only would that add precious minutes to each server you had to touch, it would also disable key services for users. "Yeah, we know email is offline – we were changing a password." See how that goes over with your user population!

There's also the shocking inefficiency of this manual approach: It might take

an experienced administrator 6 to 8 minutes to log on to the server, open the right console, find the right service, make the right change, and log back off again. Multiply that by a few servers and you start seriously eating away at someone's productivity.

Imagine that you need to update service logon passwords for 100 servers, with just two services per server. That's probably at least 10 minutes per server – or more than eight hours. A day of someone's life. If that someone is an administrator, that's at least a couple of hundred dollars in salary – and you're going to have to do this, what, every 60 or 90 days? It's not hard to spend a few thousand dollars a year managing service passwords, if you're doing it manually. You'd better hope the local tech college has a couple of free kids they can loan you every quarter!

There just has to be a better way.

Better service management through automation

There is a better way, and it's Security Explorer. It takes a different approach to service account management.

Search and discovery

First, Security Explorer starts by identifying every service running on every computer. It uses that information to create a report, which is incredibly useful all by itself. It shows you which services are running where, what permissions are applied to those services, and what account each service is using to log on.

Using this seek-and-identify technology, Service Explorer can also change nearly any configuration setting associated with a service – including passwords, start modes, the logon account, and more. These changes can be targeted at the result of any Security Explorer search, meaning you can target every computer running a given service, limit your change to specific machines, or change

It's almost impossible for a normal human being to complete a task like this without making a simple mistake – and a simple mistake will result in downtime the next time a service (or the whole server) is restarted.

Security Explorer
can make the job
easy, reliable
and safe.

only services known to be running with a given user account.

How useful is that? Don't even worry about what computers are running what services. You've gone into Active Directory and changed the password for account "ServiceAccount1"; just let Security Explorer find every service using that account, and change their password setting. Easy.

Security Explorer's "search and discovery" mechanism avoids one of the biggest potential risks about service management: missing one. Now, you'll not only have definitive documentation about what's running where and under what account, you'll be able to target actions to ensure everything is touched when the time comes.

Changing passwords

Changing passwords couldn't be easier – or more automated – than Security Explorer makes it. Just tell it which service account you're looking for, and let it find all of the services, on all of your servers, using that account. Then tell Security Explorer what the new password is. Mission accomplished.

You'll see the operation happening live, so any problems – like a server that can't be contacted – are immediately apparent so that you can take whatever corrective action is necessary.

Changing more than just passwords

Did you know that services themselves have an Access Control List (ACL) that governs who can do what to the service? Almost nobody ever messes with the default permissions, but they're pretty granular: you can control who can stop a service, who can start it, who can check its status, and much more. With the right permissions, for example, you can give your help desk the ability to start a stopped service, while preventing them from stopping it or reconfiguring it. Of course, the reason nobody messes with those settings is because managing them is such a painful, manual process. Without Security Explorer.

With Security Explorer, it's easy. Just pick the services and the permissions you want to apply, and let Security Explorer do the work of actually applying those permissions. In no time, you can have a better set of permissions that enable and delegate a variety of key administrative tasks.

Be a better service manager

So don't try to avoid eye contact the next time someone asks you how long it's been since you changed your service account passwords. Don't rely on tedious manual labor or dodgy scripts that you downloaded from someone's Internet blog. Security Explorer can make the job easy, reliable and safe.

For more information on Security Explorer, including links to a free trial, visit www.quest.com/security-explorer today.

© 2012 Dell, Inc. ALL RIGHTS RESERVED. This document contains proprietary information protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose without the written permission of Dell, Inc. ("Dell").

Dell, Dell Software, the Dell Software logo and products—as identified in this document—are registered trademarks of Dell, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN DELL'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT,

DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

About Dell

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.dell.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software

5 Polaris Way
Aliso Viejo, CA 92656
www.dell.com

Refer to our Web site for regional and international office information.

