

Re: Service Login Account query

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-01/msg01359

- *From:* "Joe Richards [MVP]" <humorexpress@xxxxxxxxxxxx>
 - *Date:* Thu, 18 Jan 2007 00:33:47 -0500
-

First different services shouldn't share an ID, an attack on a single ID or a mistake and you lock out all of your services. Preferably services should try to run as networkservice or even better localservice then you don't worry about accounts and passwords.

1. No there is no central location maintaining where IDs are being used unless you are manually keeping a list.
2. There is a script written by a friend of mine that will scan your servers. You can get it here

<http://www.jsifaq.com/SF/Tips/Tip.aspx?id=5721>

3. No services will not be using passport in the future. I am not aware of any major changes in how services are running in Longhorn.

The main thing about handling service ids securely and properly is discipline and control. Also do not allow people to set the accounts to non-expiring so you are forced to regularly go out and change them so

- a. you know how
- b. you know where
- c. because they tend to have more rights and powers than most IDs that you wouldn't think of allowing to not get changed
- d. the more people who know a secret, the less likely it is not a secret

—
Joe Richards Microsoft MVP Windows Server Directory Services
Author of O'Reilly Active Directory Third Edition
www.joeware.net

—O'Reilly Active Directory Third Edition now available—

<http://www.joeware.net/win/ad3e.htm>

AdrianDev wrote:

Re: Service Login Account query

Hi,

A domain has several Windows 2003 services installed on windows serverd, all configured to login with a Domain user account. The domain user password gets stored encryted in the local registries of all the servers according to the documentation. And so if the domain user password changes, all the service properties will have to alter to update the locally stored passwords to synchronise them else the service wont restart.

Fine.

But if I dont have the list of server names, is there a central method of listing the server names that have services that are using a particular domain user?

I am aware that it can be done the long way by running sc remotely on every server to list every service user and cross checked, but is there a function or command to achive this I can run from a single Windows 2003 server on the domain?

Moreover, what is the future for windows services, is there any change planned here to use passports or something else?

Thanks, Adrian