

Re: Replace Domain Controller

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2004-08/1844.html

From: John Savill (john_at_savilltech.com)

Date: 08/31/04

Date: Mon, 30 Aug 2004 21:37:14 -0500

Depending on your EFS recovery you may also want to backup your EFS private key which would be on the domain controller and restore to your new one (in case you need to recover any EFS files).

Following from an old KB article.

IN THIS TASK

SUMMARY

Export your Private Key from Recovery Agent

Troubleshooting

REFERENCES

SUMMARY

This article describes how to back up your Encrypting File System (EFS) private key so that you can recover encrypted data in the event that you lose the copy on your computer.

When you use EFS to encrypt the files on your computer, an EFS public key encrypts the files, and an EFS private key decrypts the files. If you lose the private key after a file is encrypted, the file cannot be recovered.

WARNING: After you export the private key to a disk, store the disk in a secure place. If someone gains access to your EFS private key, he or she can gain access to your encrypted data.

back to the top

Export your Private Key from Recovery Agent

Log on to your computer using the local Administrator account. **NOTE:** You must use the built-in Administrator account, not just an account with Administrator privileges.

Click Start, click Run, type secpol.msc, and then click OK.

Click the plus sign (+) next to Public Key Policies to expand this item.

Click the Encrypted Data Recovery Agents category.

In the right-hand pane, a certificate that is issued to "Administrator" with an intended purpose of "file recovery" is displayed. Right-click this item, and then click All tasks > export.

Click Next.

Ensure the Yes, export the private key option is selected, and then click Next.

In the Export File Format dialog box, if you want to remove the private key associated with the Administrator account, click to select the Delete the private key if the export is successful check box.

back to the top
Troubleshooting

If your computer is a member of a Windows domain, the domain administrator can designate certain users as EFS recovery agents, who can recover data even if a specific user's private key is lost.

If your computer is not participating in a Windows domain, (for example, a stand-alone computer, or a computer in a Microsoft Windows NT 4.0-based domain structure), the local Administrator account is the designated EFS recovery agent. Because of this, you can recover your encrypted data only if you previously backed up the local administrator's private key.

back to the top
REFERENCES

For additional information, click the article numbers below to view the articles in the Microsoft Knowledge Base:

Q223316 Best Practices for Encrypting File System

Q230520 How to Encrypt Data Using EFS in Windows 2000

Q242296 How to Restore an EFS Private Key for Encrypted Data Recovery

To download the "Encrypting File System for Windows 2000" white paper, please visit the following Microsoft Web site:

<http://www.microsoft.com/windows2000/techinfo/howitworks/security/encrypt.asp>

John

John Savill MCSE MVP

john@savilltech.com

<http://www.windows2000faq.com>

"DC" <DC@discussions.microsoft.com> wrote in message
news:F1B7C224-B9DD-4746-A3DB-97761E3E8AB5@microsoft.com...

> *I have only one domain controller running Windows 2000 server standard
> edition. Recently I need to replace it with with better performance
server.*

> *Beside those five Operations Master and Global Catalog need to transfer to
> new server, is there anything else need to be done prior to demote the
old*

microsoft.public.windows.server.active_directory: Re: Replace Domain Controller

> *server? Please help. Thanks.*

>