

Re: Using Kerberos in Windows 2000 Clustering

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.clustering/2004-09/0331.html>

From: Shaun Rumbelow (*shaun.rumbelow_at_sth.nhs.uk.donotspam*)

Date: 09/21/04

Date: Tue, 21 Sep 2004 07:01:04 -0700

Thanks Mike,

This has helped to make it a bit clearer. However I'm still not 100% certain about what happens if servers and cluster nodes use a mixture of kerberos and non-kerberos.

The various articles I have read seem to suggest that Windows 2000 and Windows 2003 servers drop down to using LAN Manger (LM) authentication for windows 9x clients [1] & [2] rather than Kerberos.

However, the information about the cluster's use of Kerberos and LM isn't totally clear to me. The article [3] says that when Kerberos is enabled the client can use this authentication method. What happens if the client is a 9x based machine? Does the cluster software also drop down to using LM or will the connection fail? Is Kerberos used exclusively or is Kerberos used first and then drops down to a lower method of authentication if Kerberos fails.

We also have 2 Windows 2000 Advanced Server (SP4) email clusters, each one consisting of 2 exchange 2000 servers. In the near future we plan to remove one of the clusters and create a new cluster using Windows 2003 server and 2 Exchange 2003 servers. This will give us the following situation:

Cluster 1: Windows 2000
Email Server1: Exchange 2000
Email Server2: Exchange 2000

Cluster 2: Windows 2003
Email Server3: Exchange 2003
Email Server4: Exchange 2003

Note. All 4 exchange servers are part of the same email organisation.

>From article [5] it seems to suggest that if Kerberos is used on the network name of a Windows 2000 SP3+ server then Exchange 2000 server will not function correctly as it wasn't designed to use kerberos. As Kerberos is installed by default on Exchange 2003, we will have a mixture of Kerberos & non-kerberos authentication. We will be left with the following situation.

Cluster 1: Windows 2000

Email Server1: Exchange 2000 "non kerberos

Email Server2: Exchange 2000 "non kerberos

Cluster 2: Windows 2003

Email Server3: Exchange 2003 – kerberos

Email Server4: Exchange 2003 "Kerberos

Will all the various exchange servers still be able to communicate with each other and will all clients (operating systems and outlook) work with a mixture of Kerberos and non-Kerberos. Article [6] says that Outlook 2003 works with Kerberos, but what about other clients?

Our eventual plan, over a period of time, is to replace both clusters with Windows 2003 servers and Exchange 2003 servers.

I guess my ultimate question is, if Kerberos is enabled on some cluster nodes, will other clients/servers drop down automatically to an authentication method that is compatible?

Any help to clear up this would be appreciated.

Thanks

References:

[1] <http://support.microsoft.com/?id=299656>

Windows 2000-based servers and Windows Server 2003-based servers can authenticate users who connect from computers that are running all earlier versions of Windows. However, versions of Windows earlier than Windows 2000 do not use Kerberos for authentication. For backward compatibility, Windows 2000 and Windows Server 2003 support LAN Manager (LM) authentication, Windows NT (NTLM) authentication, and NTLM version 2 (NTLMv2) authentication. The NTLM, NTLMv2, and Kerberos all use the NT hash, also known as the Unicode hash. The LM authentication protocol uses the LM hash.

[2] Technet: Chapter 5 – Security Options

In Active Directory domains Kerberos is the default for authentication, but if Kerberos isn't negotiated for some reason Active Directory will use LM, NTLM, or NTLMv2

[3] <http://support.microsoft.com/?id=302389>

Click the Enable Kerberos Authentication option, click OK, right-click the Network Name resource, and then click Bring Online. A client can now use Kerberos authentication when it connects to the VirtualServer. If you view the Active Directory Users and Computers MMC, a new Computer object that correlates to the Network Name resource is visible.

[4] Technet: Chapter 7 – Deploying Exchange 2003 in a Cluster

Select the Enable Kerberos Authentication check box so that clients can use the Kerberos authentication protocol when making an authenticated connection to this Exchange Virtual Server's Network Name resource. Enabling Kerberos

may require coordination with your domain administrator

[5] <http://support.microsoft.com/?id=235529>

This article describes the Kerberos authentication support for Windows 2000-based server clusters that has been added in Windows 2000 Service Pack 3 (SP3). With versions of Windows 2000 earlier than SP3, the Cluster service does not publish Computer objects for virtual servers in Active Directory. This means that virtual servers authenticate only by using NTLM or NTLM version 2. With Windows 2000 SP3, you can configure virtual servers to permit clients to authenticate by using the Kerberos authentication protocol. If this is enabled, a Computer object is created for each corresponding Network Name resource.

Kerberos authentication for the Network Name resource on which Microsoft Exchange 2000 depends is not supported on a server cluster. Exchange 2000 was not tested with the expectation that a cluster virtual server would support Kerberos authentication; this configuration may not function properly. Future versions of Exchange Server may take advantage of Kerberos authentication for server clusters.

[6] Technet: Exchange Server 2003 Client Access Guide

Exchange 2003 allows Outlook 2003 clients to authenticate to Exchange 2003 servers by using Kerberos authentication.

"Mike Rosado [MSFT]" wrote:

> *Hi Shaun,*
>
> *As stated in the following article, clients prior to Windows 2000 do not*
> *support Kerberos. Because Kerberos was implemented as of Windows 2000 SP3*
> *and later.*
>
> *299656 How to prevent Windows from storing a LAN manager hash of your*
> *password*
> <http://support.microsoft.com/?id=299656>
>
> *I'm by no means an expert in this subject matter of Exchange, but I'll try*
> *to assist you to the best of my ability. My understanding is that Exchange*
> *does support Kerberos if it's installed or client OS are Windows 2000 SP3*
> *and greater.*
>
> --
> *Hope this helps,*
> *Mike Rosado*
> *Windows 2000 MCSE + MCDBA*
> *Microsoft Enterprise Platform Support*
> *Windows NT/2000/2003 Cluster Technologies*
>
> =====
> *When responding to posts, please "Reply to Group" via your newsreader so*
> *that others may learn and benefit from your issue.*

> =====
>
> *This posting is provided "AS IS" with no warranties, and confers no rights.*
> *<<http://www.microsoft.com/info/cpyright.htm>>*
>
> -----Original Message-----
>
> "Shaun Rumbelow" <shaun.rumbelow@sth.nhs.uk.donotspam> wrote in message
> news:70B4A9A3-060B-4259-8627-F3B1E416FC9D@microsoft.com...
> > Hi,
> >
> > *We have several clusters running Windows 2000 Advanced Server SP3. The*
> > *various clusters run Exchange 2000, SQL 2000 and File shares. KB235529*
> > *mentions that the clusters can use kerberos (if turned on) as stated*
> > *below. I*
> > *also believe that Windows 2003 clustering has Kerberos turned on by*
> > *default –*
> > *we are planning to upgrade some of the clusters to Windows 2003 and*
> > *Exchange*
> > *2003.*
> >
> > *My questions are:*
> >
> > *1) Can 95 and 98 clients still use the cluster resources such as file*
> > *shares*
> > *– can the clients still use LM rather than Kerberos? If so does this apply*
> > *to*
> > *Windows 2000 and Windows 2003.*
> >
> > *2) Am I correct in thinking that Exchange 2000 doesn't use kerberos and*
> > *thus*
> > *kerberos couldn't be configured on the cluster servers? Does Exchange 2003*
> > *allow for kerberos and again can 9x clients use this.*
> >
> > *Any help would be appreciated*
> >
> > *KB235529*
> > *"This article describes the Kerberos authentication support for Windows*
> > *2000–based server clusters that has been added in Windows 2000 Service*
> > *Pack 3*
> > *(SP3). With versions of Windows 2000 earlier than SP3, the Cluster service*
> > *does not publish Computer objects for virtual servers in Active Directory.*
> > *This means that virtual servers authenticate only by using NTLM or NTLM*
> > *version 2. With Windows 2000 SP3, you can configure virtual servers to*
> > *permit*
> > *clients to authenticate by using the Kerberos authentication protocol. If*
> > *this is enabled, a Computer object is created for each corresponding*
> > *Network*
> > *Name resource.*
> >
> > *Kerberos authentication for the Network Name resource on which Microsoft*

> > *Exchange 2000 depends is not supported on a server cluster. Exchange 2000*
> *was*
> > *not tested with the expectation that a cluster virtual server would*
> *support*
> > *Kerberos authentication; this configuration may not function properly.*
> *Future*
> > *versions of Exchange Server may take advantage of Kerberos authentication*
> *for*
> > *server clusters. "*
> >
> >
> >
> > --
> > *Thanks for your help*
> > *Shaun Rumbelowshaun.rumbelow@sth.nhs.uk.donotspam*
>
>
>