

# Re: krbtgt Account

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2006-06/msg00025.html>

---

- *From:* [v-xuwen@xxxxxxxxxxxxxxxxxxxxxx](mailto:v-xuwen@xxxxxxxxxxxxxxxxxxxxxx) (Vincent Xu [MSFT])
  - *Date:* Tue, 06 Jun 2006 03:08:22 GMT
- 

Hi,

Roger provided greate information. I just want to provide following article in case it can help also.

Key Distribution Center  
<[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secauthn/security/key\\_distribution\\_center.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secauthn/security/key_distribution_center.asp)>

Kerberos Technical Supplement for Windows  
<[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnpag2/html/wss\\_ch7\\_kerbtechsupp.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnpag2/html/wss_ch7_kerbtechsupp.asp)>

Have a good day!

Best regards,

Vincent Xu  
Microsoft Online Partner Support

=====  
Get Secure! – [www.microsoft.com/security](http://www.microsoft.com/security)  
=====

When responding to posts, please "Reply to Group" via your newsreader so that others may learn and benefit from this issue.

=====  
This posting is provided "AS IS" with no warranties,and confers no rights.  
=====

-----  
From: "Roger Abell [MVP]" <[mvpNoSpam@xxxxxxx](mailto:mvpNoSpam@xxxxxxx)>  
References:  
<[EE83BD50-A084-4CB2-AF84-5740E87F9F7B@xxxxxxxxxxxxxx](mailto:EE83BD50-A084-4CB2-AF84-5740E87F9F7B@xxxxxxxxxxxxxx)>

<[eiAvPfliGHA.1612@xxxxxxxxxxxxxxxxxxxxxx](mailto:eiAvPfliGHA.1612@xxxxxxxxxxxxxxxxxxxxxx)>

Re: krbtgt Account

<D4DE2D68-36C1-4578-A0EA-DD1C540F1365@xxxxxxxxxxxxxxxx>

Subject: Re: krbtgt Account  
Date: Mon, 5 Jun 2006 17:46:39 -0700  
Lines: 44  
X-Priority: 3  
X-MSMail-Priority: Normal  
X-Newsreader: Microsoft Outlook Express 6.00.2900.2869  
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2869  
X-RFC2646: Format=Flowed; Original  
Message-ID: <eOgvqKQiGHA.3588@xxxxxxxxxxxxxxxxxxxxxxxx>  
Newsgroups: microsoft.public.win2000.security  
NNTP-Posting-Host: ppp\_149\_169\_167\_253.inre.asu.edu 149.169.167.253  
Path:  
TK2MSFTNGXA01.phx.gbl!TK2MSFTNGP01.phx.gbl!TK2MSFTNGP02.phx.gbl  
Xref: TK2MSFTNGXA01.phx.gbl microsoft.public.win2000.security:41390  
X-Tomcat-NG: microsoft.public.win2000.security

It is normal to see that account disabled.

As its properties state, it is used for the KDC service, which is the heart of Kerberos, the default auth technology in AD.

You are posting into the W2k newsgroups, so I assume your DCs are W2k. If your domain is W2k3 based, then there is utility to reset the two default GPOs back to their as first set up state  
dcpofix /?

It might be worth considering, if you have just inherited a potentially mismanaged AD to get to a know state. In general I recommend that people define GPOs and make their policy adjustments in them rather than using the two shipped default GPOs.  
IIRC there are now KB articles outlining resetting of these for a W2k.

You could first copy the existing to new GPOs (using GPMC on an XP or W2k3), link these at domain and DC OU with higher priority than the default GPOs, then revert the defaults. Then, using the report capability after getting reports for the copied and the reverted you could do simple text/xml compare to see what they had changed.  
etc.

Roger

"George Schneider" <georgedschneider@xxxxxxxxxxxxxxxx> wrote in message

[news:D4DE2D68-36C1-4578-A0EA-DD1C540F1365@xxxxxxxxxxxxxxxx](mailto:news:D4DE2D68-36C1-4578-A0EA-DD1C540F1365@xxxxxxxxxxxxxxxx)

The previous network admin had disabled it. I was wondering if I

should

Re: krbtgt Account

have  
it enabled. What does this account do?

"Roger Abell [MVP]" wrote:

Leave the account as it is.  
This is the credential under which the  
issuance of initial Kerberos  
service tickets happens.

"George Schneider"  
<georgedschneider@xxxxxxxxxxxxxxxx>  
wrote in message  
[news:EE83BD50-A084-4CB2-AF84-5740E87F9F7B@xxxxxxxxxxxxxxxx](mailto:news:EE83BD50-A084-4CB2-AF84-5740E87F9F7B@xxxxxxxxxxxxxxxx)

Currently in our domain the  
krbtgt user account is  
disabled. Should

this

account be enabled?