

ESX - Active Directory Integration: ...



[hharold](#) 147 posts since

Oct 18, 2004 Hi all,

We are setting up AD integration for SSH accounts on ESX 3.5 U3.

esxcfg-auth --enablead works just fine:

```
esxcfg-auth --enablead --addomain=our.domain.com --addc=our.domain.com
```

For some reason there was already an extra line in the configuration script: **esxcfg-auth --enablekrb5**

```
esxcfg-auth --enablekrb5 --krb5realm=our.domain.com --krb5kdc=our.domain.com  
--krb5adminserver=our.domain.com
```

As soon as this last command is entered things go wrong.

When adding a local account with this powershell command, we get this error:

```
New-VMHostAccount : 5/12/2009 10:17:11 AM New-VMHostAccount 52976ebb-2d24  
-f493-9aa3-bca7894ef581 A general system error occurred: passwd: Authenticat  
ion token manipulation error
```

The local account is actually created, but the Active Directory equivalent gets locked out, after several of these events:

```
Pre-authentication failed
```

```
User Name: TEST-USER
```

```
User ID: DOMAIN\TEST-USER
```

```
Service Name: kadmin/changepw
```

```
Pre-Authentication Type: 0x0
```

```
Failure Code: 0x19
```

```
Client Address: 10.10.120.16
```

Now I have two questions for you:

1. Does anyone know how to solve the lock-out problem
2. Is **--enablekrb5** necessary? What does it give me extra besides the **--enablead**

Thanks for your help!

Regards,

Harold



[kjb007](#) 5,486 posts since

Sep 18, 2006 **1. Re: ESX - Active Directory Integration: Kerberos?** May 12, 2009 10:46 AM

enablekrb5 is not required. The enablead will setup your kerberos configuration to talk to ad. the krb5 option is to be used when you're using a KDC that is not active directory. Also, when you create an account on the ESX side, it is pretty much an account with no password. At least no password from the UNIX shadow file perspective. The authentication works by checking the local files for the username (since ad is not being used for the user db, only authentication), then checking the password against local files, which have no password, so failure there, and then continuing to ad through kerberos, for a successful check. If you are trying to create an account with a password on the ESX system, then that is the problem. You don't need to set that, in fact, that needs to be no password, so without ad, the user can not effectively log into the system through ssh or console.

-KjB

VMware vExpert



[hharold](#) 147 posts since

Oct 18, 2004 2. **Re: ESX - Active Directory Integration: Kerberos?** May 12, 2009 11:00 AM

 in response to: [kjb007](#) Thanks a lot for your answer

This explains a lot. I've inherited the --enablekrb5 command, and could not explain what this could add to the --enablead command.

It only gave us errors and account lockouts.

Now I can explain why to let it out.

Thanks and kind regards,

Harold