Conway's IT Blog

Blog for Windows IT Pro tips, tricks & best practices.

Minimum Permissions Required for Account Used to Join Computers to a Domain During OS Deployment

Posted on 20/10/2011

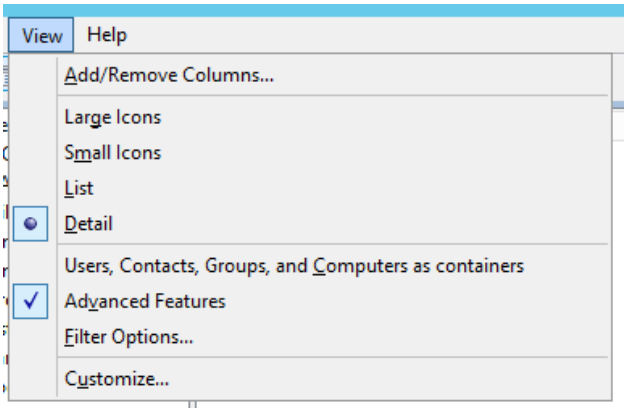
This account can be used during either MDT Lite Touch deployments using MDT or Zero Touch Deployments via SCCM.

The account requires the following permissions delegated on the OU's/domain required using the Delegation of Administration wizard or (as in this example) by directly changing the security on particular OUs within the domain.

The account **SHOULD NOT** be given "Domain Admins" privileges.

In this example I will use a domain account called "**CM_DJ**" (short for ConfigMgr Domain Join) which starts out with no special permissions other than being a member of "**Domain Users**". The account should be restricted from logging into computers via a GPO using the "**Allow log on locally**" User Rights Assignment item.

In order to view the Security tab in Active Directory Users and Computers enable "**View Advanced Features**" from the view menu.



The bullet points below summarise what permissions are required during deployment activities:

- Add/Remove new computers ("Bare Metal" scenarios)
- Update existing ones ("Refresh" scenarios)

Open the security tab of the OU you want to give permissions on – this can be done at the domain level if required but for security reasons it is best to limit this to certain parts of

Social

Recent Posts
- Check TPM Status from the Command Line (Enabled | Activated | Owned)
- Confirm Service Account Credentials The Easy Way with PowerShell (e.g. SCCM Network Access Account)
- Add CMTrace.exe to Computers Being Deployed via Task Sequence
- Use Task Scheduler to Schedule Server Reboot Out of Hours
- MBAM Client Deployment PowerShell Error 0x803d0006 – SCCM OSD in Disconnected/Offline Environments

Top Posts & Pages
- Command Line to Display UUID or MAC Address of a Computer
- Testing Connectivity Over Any TCP Port
- "Finish Installing Device Software" in Windows 10 Action Center
- How to Manually Set an IP Address in WinPE
- Minimum Permissions Required for Account Used to Join Computers to a Domain During OS Deployment
- SCCM Windows 10 Upgrade Task Sequence: BitLocker PIN Protector Issues on Laptops
- WinPE Versions Linked to Full OS Versions
- RoboCopy a Single File to See Accurate Progress/
- Add CMTrace.exe to Computers Being Deployed via Task Sequence
- Increase the Speed of PXE Boot/TFTP When Using SCCM Distribution Point

Follow

Archives
- November 2017
- June 2017
- May 2017
- March 2017
- February 2017
- January 2017
- September 2016

Active Directory.

Right-Click the relevant OU and select Properties.

Navigate to the Security tab.

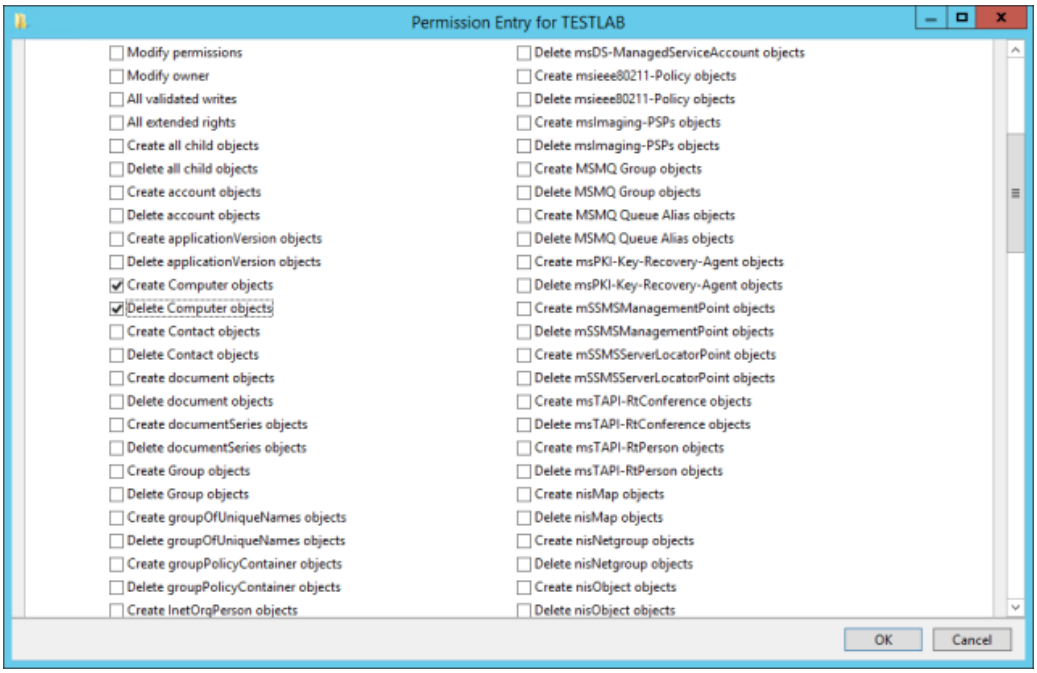
Click on "**Advanced**".

Click on "**Add**" and browse to your account e.g. TESTLAB\CM_DJ (DomainName\JoinAccount)

Choose the following settings:

Choose "**This object and all descendant objects**"

- **Create Computer Objects**
- **Delete Computer Objects**



Click "**OK**"

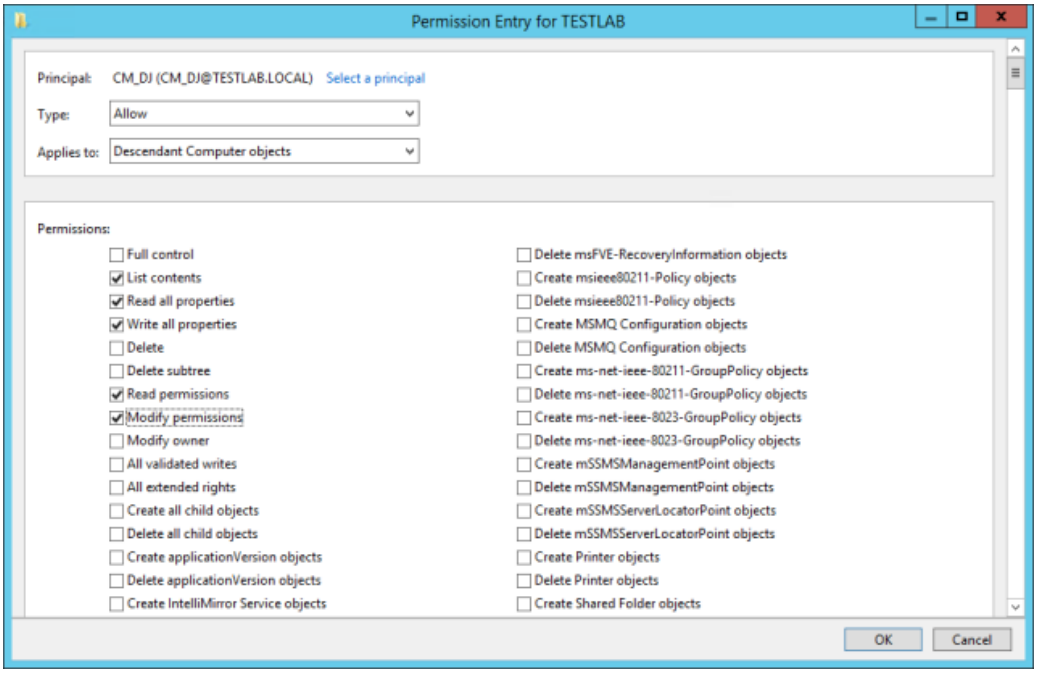
Click "**Add**" again and once more select the "JoinAccount" user.

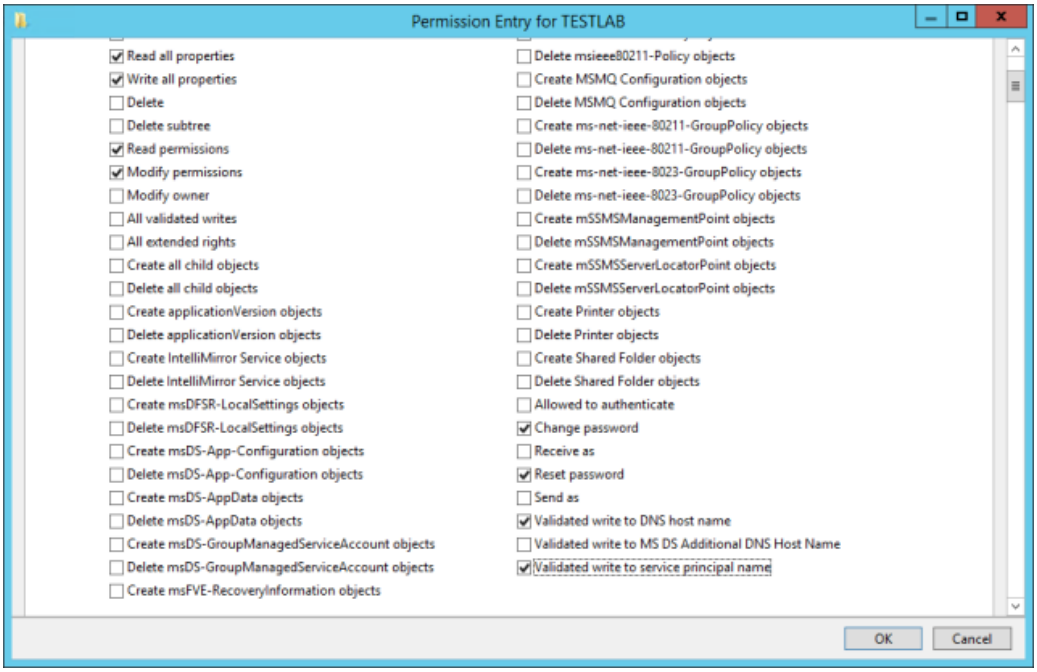
This time, limit the "**Apply Onto**" scope to "**Descendant Computer objects**" and choose the following settings:

- **Read All Properties**
- **Write All Properties**
- **Read Permissions**
- **Modify Permissions**
- **Change Password**
- **Reset Password**
- **Validated write to DNS host name**

- August 2016
- July 2016
- March 2016
- February 2016
- August 2015
- June 2015
- March 2015
- February 2015
- November 2014
- October 2014
- September 2014
- August 2014
- March 2014
- January 2014
- August 2013
- July 2013
- November 2011
- October 2011

- **Validated write to service principle name**





Once this has been done the “JoinAccount” (in this example TESTLAB\CM_DJ) will have the required permissions to add, modify and remove computer accounts in the locations you specify and nothing over and above that.

/ JC

Edit 09/03/2017

Updated to reflect the updated GUI in Windows Server 2012 and later.

Edit 24/02/2015

To automate this process, check out Johan Arwidmark's blog where you can download a script that he and Mikael Nystrom wrote to automate the permissions required:

Script to Set AD Permissions for OSD

Share this:

Related

MDT Deployment Power Plan Settings (Sleep, Hibernate etc.) Without GPO
With 3 comments

Increase the Speed of PXE Boot/TFTP When Using SCCM Distribution Point
In "SCCM 2012 R2"

How To Deploy & Run PowerShell Scripts via SCCM CB
In "Batch File"

This entry was posted in Microsoft Deployment Toolkit (MDT), SCCM 2007 and tagged Config Manager, MDT, SCCM. Bookmark the permalink.

← Welcome to Conway's IT Blog

How to Manually Set an IP Address in WinPE →

8 Responses to *Minimum Permissions Required for Account Used to Join Computers to a Domain During OS Deployment*

Tony *says:*
23/03/2012 at 01:29

Thank you for this. I have been looking for minimal settings for hours now. Your page had exactly what i was looking for.

Reply

London Lodge Reserving * *says:*
03/05/2013 at 05:57

I like the valuable information you supply to your articles.
I will bookmark your weblog and take a look at once more right here frequently.
I am relatively certain I'll learn many new stuff proper right here! Good luck for the following!

Reply

Jeff *says:*
23/05/2013 at 18:53

Pretty! This was an extremely wonderful article. Many thanks
for supplying this info.

Reply

How To Find Special discounts Upon Accommodations *says:*
30/05/2013 at 11:43

Its like you read my mind! You appear to know a lot about
this, like you wrote the book in it or something.
I think that you could do with a few pics to drive the message home a little bit, but instead of that,
this is wonderful blog. An excellent read. I'll definitely be back.

Reply

Olive *says:*
03/06/2013 at 15:31

You really make it seem so easy along with your presentation but I find this
topic to be actually one thing which I think I might
never understand. It sort of feels too complicated
and extremely vast for me. I'm having a look ahead on your next publish, I will attempt to get the cling of it!

Reply

Pingback: *Permissions for MDT deployment account | Technology Librarian Does Stuff*

m88 *says:*
26/06/2016 at 09:25

Wow, that's what I was seeking for, what a material! existing here at
this blog, thanks admin of this site.

Reply

Pingback: *Using Citrix PVS to stream Linux VDA (RHEL 7 Workstation) | magicalyak*

Leave a Reply