SCCM OSD

7-Nov-17

8:29 AM

Windows 10 Operating System Deployment

Architecture

Workstations apply a base Windows 10 image, then install customizations. Customizations fall under these categories:

* + Driver packages
  + Software Packages
  + Software Applications
  + Registry (HKLM)
  + Registry (Default User)
  + Group Policy

The base image is straight from Microsoft with only two modifications:

* + .NET 3.5
  + Telnet Client

Everything else is a customization being applied by either the Task Sequence, or Group Policy.

Re-imaging Process

Prerequisites:

* + Network connection is on an OPP subnet
  + Disk 0 must be unencrypted

A workstation boots from the SCCM boot image (USB drive or PXE in some areas). Password: **oppdsc**

It connects to the MP (SCCM.opp.gov.on.ca) and retrieves task sequence policy, then displays the available task sequences. Two will normally be available:

* + Apply image from WIM
  + Install Windows 10

Both options will partition and format Disk 0, and then prompt for a Computer Name. Active Directory is queried to determine if the computer name is valid.

'Apply image from WIM' is used when prestaged media is available on the USB drive. It puts the base image on along with all the packages already pre-downloaded (but not installed). Use this when bandwidth is limited and all the package content is not available on your LAN. After applying the WIM the workstation reboots and brings you back to the task sequence selection. At this point choose 'Install Windows 10'.

'Install Windows 10' is the main task sequence and applies all of the customizations. If prestaged media was not used then all package content (including the base image) will be downloaded from the local Distribution Point. It takes 2-3 hours for the task sequence to complete. Upon completion the workstation is left at the Windows login screen and is ready for end-users.\*

\*Laptops and tablets will need to have SecureDoc activated by hand before being released to end-users.

*Troubleshooting*

At any time while WinPE is loaded you can press F8 to bring up a command shell. You can use ping and ipconfig to verify network connectivity. You could run utilities from your USB drive, like HWEMNGR.exe for decrypting the hard drive. The task sequence

The task sequence log's location changes with time, but at this stage you can view it here:

cmtrace X:\Windows\temp\SMSTSLOG\smsts.log

Post-WinPE the log will be at C:\\_SMSTaskSequence\Logs\Smstslog\smsts.log until the SCCM client is installed, and then C:\Windows\CCM\logs\Smstslog\smsts.log while packages are installing, and then finalized to C:\Windows\CCM\logs\smsts.log once the task sequence is complete.

A custom log-parsing script has been made, TaskSequenceFailures.ps1. It checks the smsts.log files for known wordings that indicate an Application or Package failed to install, and outputs results to C:\OPPapps\Packages\TaskSequenceFailures.htm. If the file doesn't exist, no failures were found.

Logs are copied to [\\SCCM\TSLogs\<ComputerName>](file:///\\SCCM\TSLogs\%3cComputerName%3e) at the end of the task sequence for offline viewing.

Prestaged Media

Task sequences contain references to 1) packages and 2) operating system images. The idea with Prestaged Media is that you can have SCCM create a .WIM containing "pre-downloaded" task sequence references. When it comes time to run the task sequence all it needs to download is policy from the MP. Use Prestaged Media when there's no local Distribution Point, or when there is but it doesn't have all the content on it.

Prestaged Media is also what is provided to OEMs/Compucom/Compugen.

Prestaged Media should be re-generated once the package content or operating system image has significantly changed. *Software Library > Operating Systems > Task Sequences > Create Task Sequence Media*

(This takes a long time to process and chews up a lot of disk space in your temp folder.)

Wizard options are all defaults unless specified:

* + Prestaged media
  + Site-based media
  + Media file: the destination on your workstation for the new .WIM
  + Password protect the media: **oppdsc**
  + Task sequence: 'Install Windows 10'. Let it add all dependencies.
  + Boot image: Boot (x64). DP & MP = SCCM.opp.gov.on.ca
  + Image package: The appropriate Win10 image and index. DP = SCCM.opp.gov.on.ca
  + Applications / Packages / Driver Packages: accept defaults, they should all be populated already
  + Distribution Points: SCCM.opp.gov.on.ca, it should say it has all the packages
  + Customization: none

Once complete the new WIM can be distributed to DSCs.

Boot Image

*Software Library > Operating Systems > Boot Images> Boot (x64)*

A boot image (x64 only) has been created within SCCM. To generate an ISO from it:

*Software Library > Operating Systems > Task Sequences > Create Task Sequence Media*

Wizard options:

* + Bootable Media
  + Site-based media
  + Media type is up to you
  + Password protect the media: **oppdsc**
  + Boot image: Boot (x64); DP & MP = SCCM.opp.gov.on.ca
  + Customization: none

It has some customizations that would need to be re-applied if you're creating any new boot images from scratch.

* + Custom background ([\\SCCM\Packages\OSD\boot\OPPflash.jpg](file:///\\SCCM\Packages\OSD\boot\OPPflash.jpg))
  + Select drivers (see the Drivers tab of the boot image properties)
  + Components: WinPE-Scripting; WinPE-SecureStartup; WinPE-WDS-Tools; WinPE-WMI
  + Optional components: WinPE-NetFx; WinPE-PowerShell
  + Active Directory module was manually merged offline using script, see <https://daviddawsonsblog.wordpress.com/2017/03/03/powershell-active-directory-module-in-winpe-10/>

If you have a new hardware model of workstation and find it won't boot from this boot image, or it doesn't have network connectivity, then you likely need

'Install Windows 10' Task Sequence

*Software Library > Operating Systems > Task Sequences > Install Windows 10*

'Edit' the task sequence to see and configure its steps. Here are some pointers to help with understanding its flow:

* + Every step has an 'Options' tab that can have conditions to determine whether or not it will execute. i.e. this is how it knows not to re-wipe the drive if you used prestaged media.
  + The 'Computer Name' section relies on the scripts in the 'WinPE Scripts' package, whose source content is [\\SCCM\Packages\OSD\Scripts\Set-OSDComputerName\_x64](file:///\\SCCM\Packages\OSD\Scripts\Set-OSDComputerName_x64)
  + Many other steps rely on the 'OPPWIN10RUN ####' package, i.e. [\\SCCM\Packages\OSD\Scripts\Win10\_1709\OPP-WIN10RUN](file:///\\SCCM\Packages\OSD\Scripts\Win10_1709\OPP-WIN10RUN). The main script that runs is OPPWIN10RUN.ps1, but there are other steps calling their own scripts within the same package. These include customizations like:
    - Applying wallpapers (Set-OPPWallpaper.ps1; \OPP-wallpapers\)
    - Copying favourites and shortcuts (Copy-IconsShortcuts.ps1; \Icons\; \Shortcuts\)
    - Registry settings for the machine (HKLM.reg)
    - Registry settings for the default user profile (DefaultUser.reg)
    - Removing Microsoft AppX packages (MS Provisioned Apps Blacklist.txt; Remove-MSApps.ps1)
    - Providing the Windows setup unattended answer file (answerfile.xml)
    - Setting default app associations (OPPWIN10RUN.ps1; appassoc.xml)
    - Setting DCOM permissions (Set-DCOMperms.ps1)
    - Setting default power settings (PowerCfg.bat; PowerCfg-Mobile.bat)
    - Copying the hosts file (hosts)

If you're searching for a customization check HKLM.reg, DefaultUser.reg, OPPWIN10RUN.ps1, and the GPO 'OPP Workstation Policy v#'.

* + Driver Packages rely on WMI queries to determine the computer model. Many driver packages support multiple models. A query for those can look like this:

SELECT SystemSKUNumber FROM Win32\_ComputerSystem WHERE SystemSKUNumber LIKE "%P410%" OR SystemSKUNumber LIKE "%P510%" OR SystemSKUNumber LIKE "%P710%" OR SystemSKUNumber LIKE "%P910%"

* + Software Applications can install anything from SCCM's regular Applications repository, but beware their reboot behavior. If an installer is going to request a reboot it is strongly recommended to duplicate it as a Package instead for OSD. This is why Cisco AnyConnect and the PKI apps have their own packages. Task sequence results are inconsistent when applications request reboots.

Task sequences will fail if any of the referenced packages are not available on the Distribution Point. Select the task sequence and check the References tab to make sure all the content has been distributed.

Backups are taken whenever a task sequence is changed: [\\sccm\c$\scripts\ExportedTaskSequences](file:///\\sccm\c$\scripts\ExportedTaskSequences)

To restore one, import the XML as a new task sequence. The backup mechanism uses \scripts\TS-Change-Tracking.ps1, which is triggered by a Status Filter Rule: *Administration > Site Configuration > Sites > 'OP2' > Status Filter Rules > 'Task Sequence Changes'*

Driver Packages

OEMs typically provide driver packs that can be imported into SCCM. Lenovo: <https://support.lenovo.com/ca/en/solutions/ht074984>

Importation process:

* + Install/extract the driver pack to your workstation. Copy the source folders to an appropriate model folder under [\\SCCM\Packages\OSD\Drivers](file:///\\SCCM\Packages\OSD\Drivers).
  + *SCCM > Software Library > Operating Systems > Drivers > Import Driver*
  + Provide the source folder you just copied them to, click Next and let it enumerate everything (Slow.)
  + Create a new category for the discovered drivers and assign them to it
  + **Do not** assign drivers to a boot image
  + **Do** assign drivers to a new Driver Package; name it after all of the models it applies to (Slow.)
  + Do a Distribute Content on the new package

The driver package can now be added to the 'Install Windows 10' task sequence. Copy/paste an existing Apply Driver Package step and modify it appropriately.

Operating System Images

When a new build of Windows 10 comes out you'll need to obtain the ISO, then copy \sources\install.wim to [\\SCCM\Packages\OSD\Win10\_####\_Ref\Win10\_####.wim](file:///\\SCCM\Packages\OSD\Win10_%23%23%23%23_Ref\Win10_%23%23%23%23.wim). Install .NET 3.5 and the Telnet Client using the script. You'll need to know the right index number for your edition (Education, Pro, Enterprise); use DISM /Get-WimInfo /WimFile:install.wim

* + Import it into SCCM: *Software Library > Operating Systems > Operating System Images > Win10 > Add Operating System Image*
  + Copy the previous build's task sequence to a new one.
  + Copy the OPPWIN10RUN package source to a new folder ([\\SCCM\Packages\OSD\Scripts\Win10\_####](file:///\\SCCM\Packages\OSD\Scripts\Win10_%23%23%23%23))
  + Create a new OPPWIN10RUN package with the new version number and source location. No program is needed. Distribute content.
  + Edit the new task sequence and update all package references to the new OPPWIN10RUN. You can check the References tab to make sure you got them all.
  + Deploy the new task sequence to your test collection and begin testing.

Microsoft Office

Office was packaged using this guide: <https://gallery.technet.microsoft.com/office/How-to-Deploying-Office-0f954e7f>

Run setup.exe /admin; customizations were saved to \Updates\OPP.msp.

Raw source: [\\SCCM\Packages\Office2013](file:///\\SCCM\Packages\Office2013) (no updates)

Package source: [\\SCCM\Packages\Office2013Pkg](file:///\\SCCM\Packages\Office2013Pkg) (updates)

Office Updates can be extracted and then copied into the package's Updates folder. The Office installer automatically enumerates and installs them. To extract the updates, manually prepare a workstation. Uninstall any old versions of Office, install the new one from the Raw source, then get it fully patched from Windows Update. Then run the extraction script, which will copy them to $env:temp\Updates. Use 7zip to replace all the .MSPs in the package with the new ones. (Leave OPP.msp.) Update content.

Internet Explorer

IE settings are generated using the Internet Explorer Administration Kit. Prepare a workstation with the correct settings, then run the IEAK to capture them. You only need the IE11-Setup-Branding.msi. Create a package for it ([\\SCCM\Packages\OSD\Settings\IE11](file:///\\SCCM\Packages\OSD\Settings\IE11)), with a program (msiexec /i IE11-Setup-Branding.msi), and add it to the task sequence. Making changes means re-running the IEAK capture, copying over the new msi, and redistributing content.

**Internet Explorer Configuration (Nov 2017)**

Connections > LAN settings > Use automatic configuration script:

<http://proxy2.gonet.gov.on.ca:9001/proxy.pac>

Local Intranet

Local Intranet Zone - Enable Automatically detect intranet network

Sites

[http://\*.ad.gov.on.ca](http://*.ad.gov.on.ca)

[http://\*.cihs.ad.gov.on.ca](http://*.cihs.ad.gov.on.ca)

[http://\*.jus.gov.on.ca](http://*.jus.gov.on.ca)

<http://hris.opp.gov.on.ca>

<http://intra.busineeintelligence.jus.gov.on.ca>

<http://jus00aas0121>

<http://jus00aas0277>

<http://oppweb.sgc.gov.on.ca>

[https://\*.ad.gov.on.ca](https://*.ad.gov.on.ca)

[https://\*.apps.rus.mto.gov.on.ca](https://*.apps.rus.mto.gov.on.ca)

[https://\*.cihs.ad.gov.on.ca](https://*.cihs.ad.gov.on.ca)

<https://hris.opp.gov.on.ca>

<https://intra.mysse.gov.on.ca>

<https://intra.oppapss.jus.gov.on.ca>

<https://intra.pmbi.gov.on.ca>

<https://intranet.opp.gov.on.ca>

<https://jus000as5071.justice.gov.on.ca>

<https://oppweb.sgc.gov.on.ca>

<https://sse.gov.on.ca>

<https://www.osor.mcscs.jus.gov.on.ca>

Security Level for this Zone

Custom

Change

ActiveX Controls and Plugins

Allow ActiveX Filtering - Enable

Miscellaneous

Access data sources across domains - Prompt

Allow Dragging of Content Between domains into separate windows - Enable

Allow Dragging of Content Between domains into the same windows - Enable

Trusted Sites (Zone)

Sites

[http://\*.gov.on.ca](http://*.gov.on.ca)

[http://\*.projectcentre.jus.gov.on.ca](http://*.projectcentre.jus.gov.on.ca)

<http://intra.catalogue.its.gov.on.ca>

<http://intra.servicedesk.its.gov.on.ca>

<http://office.microsoft.com>

<http://sccm.opp.gov.on.ca>

[https://\*.gov.on.ca](https://*.gov.on.ca)

[https://\*.juscertify.ca](https://*.juscertify.ca)

<https://epsc.csc-scc.gc.ca>

<https://epscdr.csc-scc.gc.ca>

<https://infologindv1.rcmp-grc.gc.ca>

<https://intra.apps.rus.mto.gov.on.ca>

<https://intra.ops.myops.gov.on.ca>

<https://jus00as5103.justice.gov.on.ca>

<https://sor.jus.gov.on.ca>

<https://wi.csc-scc.gc.ca>

Restricted Sites (Zone)

.NET Framework Reliant Components

Permission for components with Manifests - Disable

Miscellaneous

Allow Dragging of content between domains into Separate windows - Enable

Allow Dragging of content between domain into the same window - Enable

Prevent Prompting about Add-Ons

Run PreventPromptingAboutAddOns.reg and PreventPromptingAboutAddOns-WOW6432Node.reg to added registry keys

Default Home page

Set <http://oppweb.sgc.gov.on.ca> as Home Page

Compatibility View Settings

unselect "Display intranet sites in Compatibility View"

Unselect "Use Microsoft compatibility lists"

Tools\Manage Add-Ons\Accelerators\E-mails with Windows Live "REMOVE"

Open Internet Options\Content\AutoComplete\Settings - Uncheck "Forms"

Run "RemoveIE\_Smiley.reg ([HKEY\_CURRENT\_USER\SOFTWARE\Policies\Microsoft\Internet Explorer\Restrictions] "NoHelpItemSendFeedback"=dword:00000001)

What's Taking So Long?

It can normally take 2-3 hours to reimage a workstation with an SSD. Without any customizations the baseline is about 20-30 minutes. The biggest time hit is from Office and all its updates. Using prestaged media also extends the time needed because of:

* + The need to go through the extra task sequence, which applies the WIM
  + The need for the SCCM client to compute hashes on every package that was integrated into the WIM (to ensure the content is still valid)

However, the majority of this time is unattended, and the only post-install task to complete is to activate SecureDoc (if applicable).

<<InstallActiveDirectoryModule.ps1>>

<<Install NetFx3 and TelnetClient.ps1>>

<<ExtractOfficeUpdates.ps1>>