REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
3/14/2016	Process Analysis / Process Improvement	2/16/2016 - 3/4/2016

4. TITLE AND SUBTITLE
Operating System Deployment Analysis

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Jason Adsit
SSG/GS-11, Network Engineer
jason.l.adsit.mil@mail.mil

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Oregon Army National Guard
ATTN: NGOR-IMS-ISB
1776 Militia Way SE, PO Box
14350 Salem, OR 97301

8. PERFORMING ORGANIZATION REPORT NUMBER

NGOR-IMS-IM-2016-001

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Distribution Statement A. Approved for public release.

13. SUPPLEMENTARY NOTES
U.S. Government Work (17 USC §105) Not copyrighted in the U.S.

14. ABSTRACT

This paper is an analysis of the operating system deployment (OSD) methodologies in the Oregon Army National Guard. Many external sources were used in conjunction with the development efforts of the G6 staff to construct stable, usable process for the Information Services Branch to use going forward.

The lite-touch, high volume deployment setup that is now in production has doubled the productivity of the system imaging process. It is likely that when the ISB staff become more comfortable with the solution, productivity will take another similar jump.

15. SUBJECT TERMS

MDT, SCCM, ADK, WDS, OSD, Windows, SHB, PXE, Multicast, Microsoft, PowerShell

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Adsit, Jason L.
					19b. TELEPHONE NUMBER (Include area code)
U	U	U	UU	11	(503) 584-3945

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

This page is intentionally left blank.

Oregon Army National Guard

G6 - Information Management Branch

Operating System Deployment Analysis

Jason Adsit

14 March 2016

Abstract

This paper is an analysis of the operating system deployment (OSD) methodologies in the Oregon Army National Guard. Many external sources were used in conjunction with the development efforts of the G6 staff to construct stable, easy to use process for the Information Services Branch (ISB) to use going forward.

The lite-touch, high volume deployment setup that is now in production has doubled the productivity of the system imaging process. It is likely that when the ISB staff becomes more comfortable with the solution, productivity will take another similar jump.

UNCLASSIFIED

Contents

Figures

UNCLASSIFIED

iii

Introduction

It was identified that the Oregon Army National Guard's operating system deployment (OSD) process needed to be improved. The Information Services Branch (ISB) staff requested assistance in order to accomplish its goal of redesigning the OSD infrastructure to increase efficiency and consistency.

Problem

The following issues were raised to management concerning the current OSD process.

- It takes too long to image computers.
- The imaging process requires a lot of manual input, thus increasing errors.
- Freshly imaged systems are not fully patched and compliant.

Requirements

The project requirements included those defined by DCSIM leadership as well as several others discovered during design and implementation. The new OSD redesign project addresses the following:

- Design a lite-touch installation (LTI) OSD solution that is resilient and secure.
- Train the ISB staff and transition daily operations to the help desk.
- Attend the weekly Windows 10 working group with NGB G6.
- Identify systems that will not be upgradable to the new DoD Secure Host Baseline (SHB).

22 **Architecture**

23   The LTI solution leverages existing Microsoft technologies that are freely available for
24 use. The core component of the solution in the Microsoft Deployment Toolkit (MDT). It is
25 what is known as a solution accelerator. It leverages other Microsoft technologies and
26 orchestrates them in such a way that the user is not required to learn all of the
27 advanced scripting needed to automate operating system deployments. See Figure 1 –
28 MDT with WDS, for an overview for the new imaging logic.

29
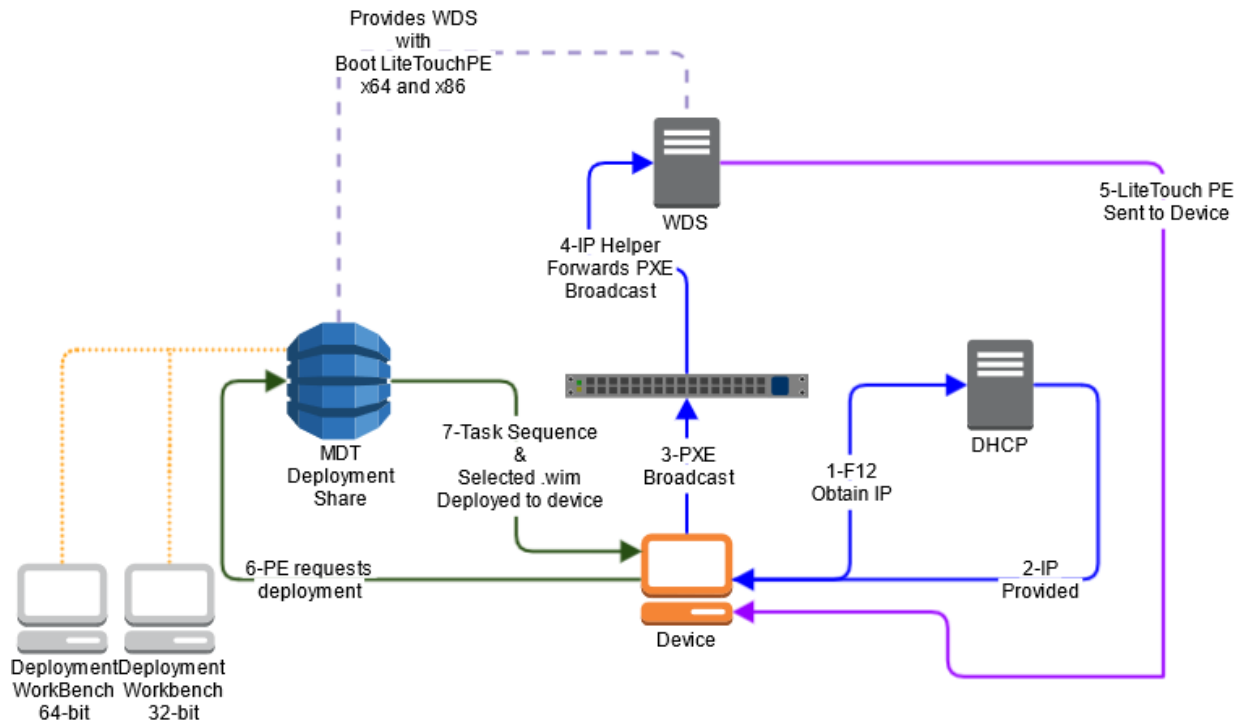
30
31   Figure 1 – MDT with WDS

32   Window Assessment and Deployment Toolkit (ADK) does the actual boot image
33 manipulation. Microsoft Deployment Toolkit (MDT) is the interface for the sysadmin to
34 manipulate the OS Deployment and Application Installation logic. Windows Deployment
35 Services (WDS) manages the transmission of images to the clients. This design does
36 require that the correct DHCP options have been configured to allow PXE booting. Also,
37 if multicast image transfer is desired, PIM must be enabled on the subnets where the
38 clients reside.

39   Multicast deployment is preferred because it allows the system imaging work load to
40 be massively parallelized without congesting the infrastructure. The servers hosting
41 deployment shares only ever have to serve up a maximum of three imaging data
42 streams. WDS dynamically detects the transfer speeds of the clients and divides them
43 into slow, medium, and fast imaging streams accordingly.

44

Platform Management

46 One of the primary concerns of the ISB staff was that drivers were cumbersome to
47 manage and difficult do deploy reliably. The new LTI solution removes this process from
48 the list of things for the ISB to worry about. Drivers are downloaded for each platform,
49 cataloged in a central store, and injected dynamically into the Windows during the
50 deployment process.

51 The WinPE image that has been provided also includes the Dell Command
52 Configuration toolkit. Using this tool, the system BIOS/UEFI can be upgraded from
53 WinPE before the OS is installed. This will be a critical task to master. Once the
54 organization begins rolling out the DoD SHB (Windows 10), up-to-date UEFI will be a
55 prerequisite for implementing secure boot.

56 Hardware vendors' websites have a vast amount of information regarding platform
57 specific driver packages. The deployment share is currently stocked with the latest
58 driver packs as of the date of this report. The update process currently requires a
59 sysadmin to download the drivers and import them into the deployment share.

60 When the SCCM 2012 roll-out is complete, the drivers and firmware will be managed
61 by SCCM using a System Center Update Publisher (SCUP) catalog. SCCM can retrieve
62 drivers and BIOS/UEFI updates directly from hardware vendors.

PowerShell

64 The entire build and deployment process can be accomplished without using MDT's
65 graphical user interface at all. Simply installing MDT includes the PowerShell code
66 needed to automate the OSD workflow.

67 The PowerShell code called by the graphical user interface is surfaced to the
68 sysadmin via "View Script" buttons. These allow the code to be captured for later re-use
69 without using the graphical UI. Figure 2 shows the PowerShell code that is being called
70 when a deployment share is updated.

71

72
```
Import-Module "C:\Program Files\Microsoft Deployment Toolkit\bin\MicrosoftDeploymentToolkit.psd1"

New-PSDrive -Name "DS001" -PSProvider MDTProvider -Root "C:\DeploymentShare"

Update-MDTDeploymentShare -path "DS001:" -Compress -Verbose
```

Figure 2 – Example MDT PowerShell Code Snippet

73 **Automation**

74   The MDT workbench allows the sysadmin to skip panes in the deployment wizard
75 and pre-answer the normal questions presented to the user. This allows the sysadmin
76 to make the process repeatable and free from human error. It also doesn't let end-users
77 opt out of mandatory applications. See Figure 2 – Example CustomSettings.ini.

```
[Settings]
Priority=INSTALL, Default
Properties=MyCustomProperty

[INSTALL]
SkipDeploymentType=YES
DeploymentType=NEWCOMPUTER
SkipApplications=YES
MandatoryApplications001={e7971139-8a85-4fe0-97e4-ec541843a887}
MandatoryApplications002={6e2dc470-690e-4a05-af84-b322d046290a}
MandatoryApplications003={6678a2c2-847b-4b4c-9eb7-ecfe0a1bbaf7}
MandatoryApplications004={1b93e53f-701a-4cf2-b09b-de1c7a09aa95}
MandatoryApplications005={7c3afe82-7408-4ea2-8ca5-8e5a4f9b99e2}
MandatoryApplications006={aa1237d4-0e56-441c-9169-b168d3a96d1a}
MandatoryApplications007={9fae0369-9069-4cf3-a5e8-a4884599d5a8}
MandatoryApplications008={de1b51a4-2e5d-49ef-ad12-1f955f429b7e}
MandatoryApplications009={ed9fbfa8-3499-46ff-b2cf-185c22235eb7}
MandatoryApplications010={d029409a-0c66-4df6-9b9c-cae08dd6ea73}
MandatoryApplications011={72fe3e2d-b11e-46a9-9848-d499f10ef87d}
MandatoryApplications012={382750c3-3630-45b0-9e5f-77c7768a987f}
MandatoryApplications013={a03fc9d9-2881-4933-91a7-07d019774dde}
MandatoryApplications014={646942cc-78ec-4b82-9e64-da2ec1c0148a}
MandatoryApplications015={cacad724-bfe9-4f96-85f2-f0f11a243efd}
MandatoryApplications016={0611969c-5d22-4a84-9fc3-b76176bfe3d2}
SkipComputerName=YES
OSDComputerName=mdt-%SerialNumber%
SkipUserData=YES
WSUSServer=https://wsus-server/
SkipPackageDisplay=YES

[Default]
OSInstall=Y
SkipBDDWelcome=YES
SkipWizard=NO
SkipTaskSequence=NO
SkipApplications=YES
SkipCapture=YES
SkipAdminPassword=YES
SkipComputerBackup=YES
SkipBitLocker=YES
BitLocker=NO
SkipDomainMembership=YES
JoinWorkgroup=WORKGROUP
NetworkLocation=Work
SkipComputerName=NO
SkipProductKey=YES
SkipBuild=YES
SkipAdminAccounts=YES
SkipRoles=YES
SkipSummary=YES
SkipFinalSummary=YES
OrgName=Some Organization
FullName=Someone
BitsPerPel=32
Xresolution=1
Yresolution=1
Vrefresh=60
FinishAction=REBOOT
SkipTimeZone=YES
TimeZoneName=Pacific Standard Time
SkipLocaleSelection=YES
KeyboardLocale=en-US
KeyboardLocalePE=0409:00000409
_SMSTSORGNAME=Name of Your IT Department
_SMSTSPackageName=OS Deployment Task Sequence
SLShare=\\mdt-server\DeploymentShare$\Logs
SLShareDynamicLogging=\\mdt-server\DeploymentShare$\Logs\%ComputerName%
EventService=http://mdt-server:9800
OSHome_Page=https://www.google.com/
```

Figure 3 – Example CustomSettings.ini

78 **Remote Systems and DaRT**

79   The MDT server has the Microsoft Diagnostics and Repair Tools (DaRT) installed
80 which allows for remote control of systems once the WinPE environment has booted
81 into memory via PXE. The systems to be imaged will show up under the monitoring
82 node in MDT. The temporary computer names are suffixed with the value returned by
83 the "%SerialNumber%" variable in the OSD environment running on a given computer.
84 This way the sysadmin can correlate the system waiting to be imaged to a help desk
85 ticked via the serial number.

86   Another advantage of using DaRT in the ability to remotely support systems that fail
87 to boot into Windows or that have fallen off the domain. The sysadmin can simply
88 instruct the user to power on the system, press F12, and go to lunch. Once the WinPE
89 boots and DaRT remote control starts, the sysadmin can lock the remote system's
90 keyboard and mouse to prevent interference. The DaRT tools enable many advanced
91 support scenarios including things like password reset, file recovery, and hotfix uninstall.

92 **State Migration Points**

93   The matter of user profiles and data will be addressed when the SCCM 2012
94 migration is complete. Sysadmins will use the User State Migration Tool to save user
95 state to the network location defined in a task sequence. The process flow that will take
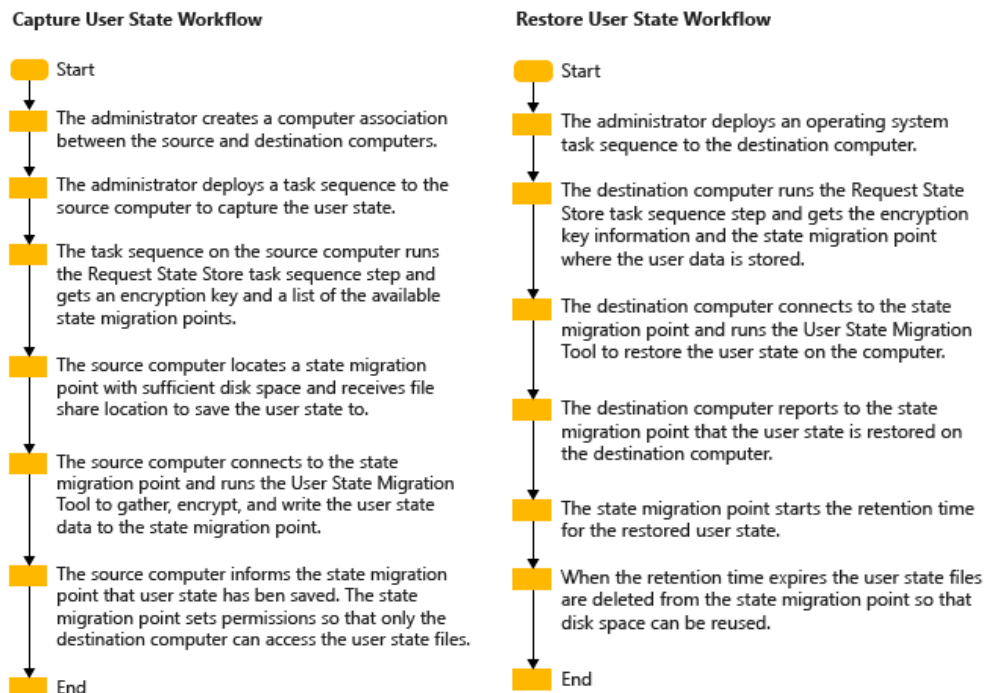96 place is illustrated by Figure 1 below.

97

Capture User State Workflow

- Start
- The administrator creates a computer association between the source and destination computers.
- The administrator deploys a task sequence to the source computer to capture the user state.
- The task sequence on the source computer runs the Request State Store task sequence step and gets an encryption key and a list of the available state migration points.
- The source computer locates a state migration point with sufficient disk space and receives file share location to save the user state to.
- The source computer connects to the state migration point and runs the User State Migration Tool to gather, encrypt, and write the user state data to the state migration point.
- The source computer informs the state migration point that user state has ben saved. The state migration point sets permissions so that only the destination computer can access the user state files.
- End

Restore User State Workflow

- Start
- The administrator deploys an operating system task sequence to the destination computer.
- The destination computer runs the Request State Store task sequence step and gets the encryption key information and the state migration point where the user data is stored.
- The destination computer connects to the state migration point and runs the User State Migration Tool to restore the user state on the computer.
- The destination computer reports to the state migration point that the user state is restored on the destination computer.
- The state migration point starts the retention time for the restored user state.
- When the retention time expires the user state files are deleted from the state migration point so that disk space can be reused.
- End

98   Figure 4 – User State Migration

Follow-On Support

There will be an additional requirement for assistance when the ISB staff implements SCCM 2012 in April 2016. The integration of the provided OSD system with SCCM will require collaboration with the IMB and NGB G6. Once complete, the OSD process with move to what is known as zero-touch installation (ZTI). When the ISB is ready to begin engineering on the ZTI solution, they will request assistance from the IMB branch chief.

General Observations

The OSD process needs to be maintained on an ongoing basis to remain efficient, compliant, and secure. There are several lines of effort that are vital to the continued success of the new OSD process. They can be addressed by the following measures.

- Participate in the weekly Windows 10 working group with NGB.
- Use PowerShell daily.
- Tightly integrate the sysadmins responsible for OSD and SCCM.
- Deploy early and deploy often.
- Servers should be treated as cattle, not pets.
- Infrastructure as code. Do not make configuration adjustments manually. If the configuration is a process in your head, you're doing it wrong.
- Manage expectations honestly. If your leadership is not fully informed of the state of your activities, they tend to hover.
- Challenge organizational norms. Everyone has valuable input.
- If it would be easier to do via group policy, then do it via group policy. Work-arounds are not a good solution at scale.
- Communicate intent as well as process. Rapid information flow is critical.

References

Alphabet Soup Deployment: Understanding MDT, WDS, MAP, ACT, SCCM, and USMT. (2016, March 7). Retrieved from https://technet.microsoft.com/en-us/windows/hh215959

Build a distributed environment for Windows 10 deployment. (2015, November 12). Retrieved from https://technet.microsoft.com/en-us/library/mt297527(v=vs.85).aspx

Dell Catalog to Support Microsoft System Center Configuration Manager for Dell Hardware Updates. (2011, November 2). Retrieved from http://www.dell.com/downloads/global/solutions/Dell%20Catalog%20for%20Microsoft%20System%20Center%20Configuration%20Manager.pdf

Dell Command | Deploy - Driver Packs for Enterprise Client OS Deployment. (2016, March 8). Retrieved from http://en.community.dell.com/techcenter/enterprise-client/w/wiki/2065.dell-driver-cab-files-for-enterprise-client-os-deployment

Dell Drivers Direct Download Page. (n.d.). Retrieved from https://downloads.dell.com/published/Pages/index.html

Deploy Windows 10 with System Center 2012 R2 Configuration Manager. (2015, November 12). Retrieved from https://technet.microsoft.com/library/mt297520.aspx

Deploying Windows 7 - Part 7: Automated LTI Deployment. (2009, August 27). Retrieved from http://www.windowsnetworking.com/articles-tutorials/windows-7/Deploying-Windows-7-Part7.html

End-to-End Deployment of Updates in SCCM 2012 Using Dell Business Client Catalog. (2012, December). Retrieved from http://en.community.dell.com/techcenter/extras/m/white_papers/20266738

Example Scenario for PXE-Initiated Operating System Deployment by Using Configuration Manager. (2015, May 14). Retrieved from https://technet.microsoft.com/en-us/library/jj134267.aspx

Getting Started with Windows Deployment for Windows Server 2012 or Windows 8 Using Microsoft Deployment Toolkit (MDT). (2013, September 16). Retrieved from https://blogs.technet.microsoft.com/askpfeplat/2013/09/16/getting-started-with-windows-deployment-for-windows-server-2012-or-windows-8-using-microsoft-deployment-toolkit-mdt/

HP Driver Packs (64-bit). (2016, March 8). Retrieved from http://ftp.hp.com/pub/caps-softpaq/cmit/HP_Driverpack_Matrix_x64.html

Integrated MDT into SCCM for better OSD task sequence. (2014, March 6). Retrieved from http://www.rickygao.com/integrated-mdt-into-sccm-for-better-osd-task-sequence/

Introduction to Operating System Deployment in Configuration Manager. (2015, May 14). Retrieved from https://technet.microsoft.com/en-us/library/gg682108.aspx

Lite-Touch, High-Volume Deployment. (2015, March 8). Retrieved from https://technet.microsoft.com/en-us/library/dd919179(v=ws.10).aspx

MDT 2013 Documentation. (2013, November 5). Retrieved from http://download.microsoft.com/download/B/F/5/BF5DF779-ED74-4BEC-A07E-9EB25694C6BB/MDT%202013%20Documentation.zip

MDT with WDS Integration Overview. (2015, February 20). Retrieved from http://techthoughts.info/mdt-with-wds-integration-overview/

Official Microsoft System Center Configuration Manager Sub-Reddit. (2016, March 8). Retrieved from https://www.reddit.com/r/SCCM/

Operating System Deployment with SCCM 2012. (2016, February 10). Retrieved from \\ngeea0-sccm00\osd_resources\SCCM 2012 (OSD)NGB_V1.docx

OSD – How make PXE work in ConfigMgr OSD, MDT and WDS work perfectly fine – Stop using DHCP Option 66 & 67. (2016, February 29). Retrieved from http://deploymentbunny.com/2016/02/29/osd-how-make-pxe-work-in-configmgr-osd-mdt-and-wds-work-perfectly-fine-stop-using-dhcp-option-66-67/

Overview of DoD SHB. (2016, March 2). Retrieved from https://disa.deps.mil/ext/cop/iase/dod-images/Documents/Win10/U_1_Overview_of_DoD_SHB_v1.0_20160302.pdf

Prepare for Zero Touch Installation of Windows 10 with Configuration Manager. (2015, August 6). Retrieved from https://technet.microsoft.com/en-us/library/mt297524(v=vs.85).aspx

Replace a Windows 7 SP1 client with Windows 10 using Configuration Manager. (2016, August 6). Retrieved from https://technet.microsoft.com/en-us/library/mt297532(v=vs.85).aspx

SHB Design Guide. (2016, March 2). Retrieved from https://disa.deps.mil/ext/cop/iase/dod-images/Documents/Win10/U_2_SHB_Design_Guide_v1.0_20160302.pdf

SHB Installation Guide. (2016, March 2). Retrieved from https://disa.deps.mil/ext/cop/iase/dod-images/Documents/Win10/U_3_SHB_Installation_Guide_v1.0_20160302.pdf

Windows ADK for Windows 10 scenarios for IT Pros. (2015, October 6). Retrieved from https://technet.microsoft.com/library/mt280162.aspx

Zero-Touch, High-Volume Deployment. (2015, March 8). Retrieved from https://technet.microsoft.com/en-us/library/dd919178(v=ws.10).aspx