Software Assurance Planning Services

Windows Image Engineering and Deployment Planning
Agenda

- Managed Desktop
- Image Engineering
- Image Deployment
- Volume Activation
- Hardware Lifecycle Management
- Security Management
- Application Lifecycle
- User Settings
Managed Desktop
The Managed Desktop Solution

Enterprise Desktop Stack

- user settings
- individual applications
- role-based applications
- enterprise applications
- security configuration
- hardware-based software & drivers
- operating system master image

- user profile management
- security management
- image engineering
- image deployment

application lifecycle

hardware lifecycle
Managed Desktop Governance – Windows 7

- User settings
- Individual applications
- Role-based applications
- Enterprise applications
- Security configuration
- Hardware-based software & drivers
- Operating system
- Master image

Diagram elements:
- Configuration control board
- Desktop Operations Team
- Desktop Group Policy Administrators
- Security Operations Team
- Image Build Team
- Security desktop monitoring team
- Image deployment
- Network operations team
- Active directory administrations
- Helpdesk managed desktop support team
- Hardware council
- Enterprise role owner
- Role owners
- Application owner

Software distribution team

Hardware lifecycle
Managed Desktop Governance – Windows 8

Enterprise Desktop Stack
- User and app experience
- Individual applications
- Role-based applications
- Enterprise applications
- Security configuration
- Hardware-based software & drivers
- Operating system master image

Software distribution team
- Application owner
- Role owners
- Enterprise role owner

Consumerization
- Hardware council

Hardware lifecycle
- User-targeted Software

Image Optimizations
- Configuration control board
- Security Operations Team
- Image Build Team

Image deployment
- Security desktop monitoring team
- Helpdesk managed desktop support team
- Active directory administrations
- Network operations team

Use self-service imaging

Helpdesk managed desktop support team

Desktop Operations Team

Image engineering
- Security management

Enterprise role owner

Network operations team

Enterprise role owner

Security management

Image engineering

Desktop Operations Team

Security Operations Team

Configuration control board

Image build team
Windows 8 for the Enterprise

Devices & Experiences Users Love

- No Compromise Business Tablet*
- New Possibilities in Mobile Productivity
- Enhanced End-to-End Security
- Management and Virtualization

Enterprise-Grade Solutions

* x86 Tablets
Windows 8 Enhancements

- Touch Enabled
- Modern Application Experience
- Client Hyper-V
- Windows To Go
- Secure Boot
- Pre-Provisioning Bitlocker
- DirectAccess over IPv4
- Dynamic Access Controls
Image Engineering Process

- Process generates an enterprise image that can be deployed to desktops, laptops, x86 tablets, virtual machines

- Includes components of security baseline, look-and-feel, core applications and out-of-box drivers

- Components applied using a reference deployment and captured into a single image file (.wim)
Image Engineering
Common business concerns

- Building enterprise images is too complex, we have so much variation in our hardware. We need a more manageable solution.
- The enterprise image needs to be secure before it is put on our corporate network.
- We’ve decided to embrace virtualization to save costs but we don’t want to have to manage two different image engineering processes.
- We need to reduce the deployment time.
- We need to reduce the size of images because we have to distribute them to and store them at our branch offices.
- We need to reduce our training and support costs and provide a consistent, usable look and feel for all users.
Image Engineering
Business drivers

- Design for Manageability
  - A single enterprise image for all hardware platforms
- Design for Security
  - Ensure the image meets a security baseline from first boot
- Design for Portability
  - A single process to build and service images for both physical and virtual machines
- Design for Efficiency
  - Efficiently use network bandwidth and storage and reduce deployment time
- Design for Usability
  - A consistent look and feel for all users
Microsoft Deployment Toolkit 2012 Update 1

- **Purpose**
  - MDT is a Microsoft Solution Accelerator that allows you to automate the deployment of Operating Systems and applications in your organization
  - MDT is the Microsoft recommended process and toolset for automating image creation

- **Overview**
  - MDT is available in x86 and x64 versions. Both versions of MDT 2012 support deployment of x86 and x64 Windows operating systems
  - MDT 2012 Update 1 supports the creation and deployment of Windows 8 images
  - MDT leverages the Windows Assessment and Deployment Kit for Windows 8 image creation and deployment
  - MDT does not require a license

- **Use MDT to create your reference image**
  - Provides most flexibility in customizing default profile
  - Lightweight and repeatable
Windows 8 Versions

- **Windows RT**
  - Embedded into ARM processor
  - Does not run legacy x86/x64 applications
  - Imaged by OEM, cannot create or deploy an image to it

- **Windows 8 Professional**
  - Intended for business use
  - Available in 32-bit/64-bit editions

- **Windows 8 Enterprise**
  - Intended for business use
  - Available in 32-bit/64-bit editions
  - Includes AppLocker, BranchCache, DirectAccess, and Windows To Go
What to Include in the Image?
Supporting Decisions

Considerations
Including applications ties the lifecycle of the image to those applications

Recommendations
Include applications critical to maintain a security baseline for the image

If the deployment time is your objective, include large enterprise-wide applications with high deployment times

Do not include applications with frequent updates
Look and Feel
Supporting decisions

Considerations

• The Windows 8 Start Screen offers some look-and-feel configuration capabilities when capturing an image
• Note that you cannot sysprep an image that has Windows Store applications in it
• This limits the applications that can be injected into the image to traditional desktop applications, or Windows Store applications that have been sideloaded
• Arranging the Start Screen requires pausing the image capture task sequence and arranging the tiles manually

Recommendations

• Use MDT to build and capture image; avoid heavy customization of Start Screen as there is no programmatic way to change the screen layout without re-snapping an image
• Use Group Policy to enforce required user and computer settings
• Use Group Policy preferences to set (but not enforce) user and computer settings
Image Engineering
Summary

- Operating Systems in Scope:
  - Version, Architecture, SKUs, Features

- Core Applications:
  - Security, Large Applications, Tools

- Look and Feel
  - User Profile, Branding, Performance Settings, Internet Explorer settings, Group Policy and Group Policy Preferences

- Regulations
  - Operational standards and compliance requirements, regulatory standards
Image Deployment
Image Deployment Process

- The image deployment process delivers the components of the enterprise desktop

- The process includes:
  - Capturing the user state from an old machine
  - Laying down a new master image
  - Configuring and installing applications
  - Restoring the user state
Common Business Concerns

- Our capacity to deliver desktops is too small
- We need to reduce the time to deploy a desktop
- We need our deployment process to produce a usable desktop customized for the specific user
- We need to ensure our deployments to branch offices do not require too much network bandwidth
- User impact and productivity loss needs to be minimized.
- Involving resources to start or debug the process costs us money.
- Managing who gets what configuration and applications is a costly process.
Business Drivers

- Design for Automation
  - Least manual intervention in the process as possible
- Design for Flexibility
  - Single deployment mechanism for all scenarios
- Design for Efficiency
  - Reduce network bandwidth and storage requirements
- Design for Scalability
  - Ability to meet deployment targets
- Design for Supportability
  - Non-destructive process with abilities to recover
- Design for Productivity
  - Minimized user impact during pilot and production migration
Deployment Approach

- Microsoft System Center 2012 Configuration Manager SP1
- Microsoft Deployment Toolkit 2012 Update 1 (MDT)
  - Windows Assessment and Deployment Kit
  - Windows PE 4.0
  - USMT 5.0
- Windows Server 2012
  - Windows Deployment Services with multicast
  - Branch Cache improvements
Deployment Approach - LTI

- LTI – Lite Touch Installation
- Only requires Microsoft Deployment Toolkit 2012 Update1 (free download)
- Contains tools and best practice guidance for deployment
- Used for Image Engineering and Image Deployment processes
- Includes MDT Database for role, location, computer and hardware-based configurations
- Does not provide lifecycle for desktop components after deployment
Microsoft Deployment Toolkit 2012 Update 1

What’s New?

• Support for Windows 8 and Server 2012 deployment
• Deployment Monitoring Functionality – view all LTI deployments performed from a specific deployment share
• Integration with System Center 2012 Configuration Manager – extends the functionality of OS deployment
• Integration with Diagnostic and Recovery Toolkit (DaRT) – available to organizations with access to the Microsoft Desktop Optimization Pack (MDOP)
• Integration with Windows Assessment and Deployment Kit (ADK) – tools to customize and automate the deployment of Windows 8
• Integration with Security Compliance Manager – apply security templates to clients during deployment
• Support for UEFI deployment
• Improved disk partitioning options
• Enhanced User Driven Installation (UDI) capabilities
What’s New?

- Replaces Windows AIK (Automated Installation Kit) for Windows 8 deployments

What’s in it?

- Windows Pre-Installation Environment (Windows PE) 4.0
- Windows System Image Manager (Windows SIM)
- User State Migration Tool (USMT) 5.0
- Deployment Imaging Servicing and Management (DISM)
- Application Compatibility Toolkit (ACT)
- Volume Activation Management Tool (VAMT)
Deployment Approach - OSD

- OSD – Operating System Deployment
- Requires Microsoft System Center 2012 Configuration Manager SP1 infrastructure
- Used for Image Deployment process
- Provides application, hardware, and security lifecycle after deployment
- Does not include MDT Database for role, location, computer or hardware-based configurations
What’s New?

- Improved Deployment Scalability – the functionality of the PXE Service Point and its configuration has been moved to the distribution point to increase scalability
- User Device Affinity (UDA) Support – you can associate a user with a client device to take advantage of User Device Affinity. UDA provides the ability to deploy the most suitable application type (virtual, MSI, remote) to a user based on the client device they are logged into
- Enhanced media deployment functionality – deploy client devices using media to anywhere in the System Center 2012 Configuration Manager SP1 hierarchy
- Update reference images offline in administrative console – apply Windows Updates to reference images using System Center 2012 Configuration Manager SP1 software library
Deployment Approach - WDS

- Windows Deployment Services in Standalone
- Requires Windows Deployment Services Feature installed on the server
- Can be used for Image Deployment process
- Does not provide lifecycle for desktop components after deployment
- Does not include MDT database for role, location, computer or hardware-based configurations
Deployment Approach - ZTI

- ZTI – Zero Touch Installation
- Combines the MDT database, OSD and WDS into a fully automated deployment solution
- Requires Microsoft Deployment Toolkit 2012 U1 integrated with Configuration Manager infrastructure
- Can be used for Image Deployment process
- Provides application, hardware and security lifecycle after deployment
- Includes MDT Database for role, location, computer and hardware-based configurations
System Center 2012 Configuration Manager SP1

Microsoft Deployment Toolkit 2012 Update 1 Integration

- Integration of MDT 2012 Update 1 and System Center 2012 Configuration Manager provides an easier path for users to migrate to a new Windows operating system
- New deployment methods – provides users with the option to select regional settings, preferred languages and administrator-defined applications to enable a customized migration to an approved client device that is suitable for deployment
- Store configuration information for centralized deployment – provide users with different requirements the same automated deployment experience
- Support for additional languages – enable more users to migrate with duplicating administrator effort
- Improved diagnostics, monitoring, error reporting, and recovery – troubleshoot and identify deployment problems as they happen
Deployment Approach
Supporting decisions

- **Considerations**
  - Trade-off infrastructure and administration cost automation and lifecycle

- **Recommendations**
  - In those enterprises with System Center 2012 Configuration Manager SP1, the ZTI approach provides the most automation, distribution efficiency and lifecycle features
  - In scenarios with less infrastructure, the LTI approach with Microsoft Deployment Toolkit 2012 U1 offers the most automation while using only a share
  - In both scenarios, automate as much of the process by providing configuration information in the MDT database
  - Use Windows Server 2008 R2 / Windows Server 2012 to take advantage of remote differential compression and BranchCache
## Deployment Approach - Core OS Scenarios

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Key Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>New computer</td>
<td>- Fresh install of a new operating system on client or server system</td>
</tr>
<tr>
<td></td>
<td>- New or repurposed hardware</td>
</tr>
<tr>
<td></td>
<td>- Bootable Media (CD or USB Flash Drive)</td>
</tr>
<tr>
<td>PXE boot</td>
<td>- Integrate with WDS PXE server</td>
</tr>
<tr>
<td></td>
<td>- Control deployment action with Configuration Manager deployments</td>
</tr>
<tr>
<td></td>
<td>- Self-provisioning via F12</td>
</tr>
<tr>
<td>Wipe-and-load</td>
<td>- Install new version of operating system on existing client or server hardware</td>
</tr>
<tr>
<td></td>
<td>- Reinstall applications under new operating system</td>
</tr>
<tr>
<td></td>
<td>- For clients, securely save/restore user state and settings (locally or on a file server)</td>
</tr>
<tr>
<td>Side-by-side</td>
<td>- Install new version of operating system on new client hardware for an existing user</td>
</tr>
<tr>
<td></td>
<td>- Reinstall applications on new computer under new operating system</td>
</tr>
<tr>
<td></td>
<td>- Move user state and settings from old computer to new computer via a file server</td>
</tr>
<tr>
<td>Offline with removable media</td>
<td>- Do operating system deployment from removable media (CD set, DVD, USB flash drive)</td>
</tr>
<tr>
<td></td>
<td>- Site with low bandwidth or no connectivity (no status reporting)</td>
</tr>
<tr>
<td></td>
<td>- Large software packages are on the media</td>
</tr>
<tr>
<td>Pre-staged media</td>
<td>- Optimized for network bandwidth and speeds up end to end deployment</td>
</tr>
<tr>
<td></td>
<td>- Works with existing processes</td>
</tr>
<tr>
<td></td>
<td>- Initial staging can be completed detached from ConfigMgr environment</td>
</tr>
</tbody>
</table>
Deployment Approach
Supporting decisions

Considerations

• Replace Scenarios involve a workflow: old machine to new machine association established, old machine data captured, new machine deployed, data restored
• Which locations are involved? Branch Offices? Disconnected?
• How does network connectivity influence the deployment method?

Recommendations

• Ensure a process is established for Replace scenarios
• Upgrade scenario is not recommended in large enterprises – instead, use an in-place refresh process (capture data, wipe drive, install new OS, restore data)
• For zero-data loss requirements, use Replace scenario
Distribution Strategy

Depot Strategy
Can build machines quickly using multicast
Need to ship machines to/from depot

BranchCache Strategy
Requires Server 2008 R2 or 2012 infrastructure
Can be used to obtain packages from local branch server or client machines
Requires initial transport of packages

Media Strategy
Requires no infrastructure
More difficult to customize machine to user
Need to regenerate media to update
Distribution Strategy
Supporting decisions

Considerations

- What locations are in scope and what infrastructure is available? BrancheCache can allow peer Windows 7 / Windows 8 machines to pull bits, but requires Windows Server 2008 R2 or Windows Server 2012.
- Is a depot scenario in scope? If so, does the depot have infrastructure to support multicast (at least Windows Server 2008)?
- Are there machines that are fully disconnected? If so, media is the only solution, however media cannot be customized easily.

Recommendations

- For branch scenarios without Windows Server 2008 R2 or 2012, consider a depot type model or media deployments; leverage BrancheCache for other branch deployments
- For depots with capacity concerns, leverage System Center 2012 Configuration Manager SP1 and Windows Server 2012 with multicast
- Use media deployments sparingly and for more homogeneous configurations
Windows 8 Enterprise Scenarios

- Productivity with Tablet
- Enterprise Windows 8 Apps
- Your Portable Workspace
- Work Anywhere*
- Your Data and Apps On Any Windows-based Device**
- Help Secure Your Devices & Data
- Help Secure Your Environment
- Embrace BYOD scenarios
- Support Mobile Workforce
- Virtual Desktops Simplified

*Internet access required
** x86
# Windows 8 Enterprise Scenarios with Deployment Methods

<table>
<thead>
<tr>
<th></th>
<th>Efficient Mobile Workforce</th>
<th>Bring Your Own Device (BYOD)</th>
<th>My Data and Apps Follow Me</th>
<th>Windows 8 Companion Devices Ready for Business</th>
<th>Contractors Using Shared PCs / BYOD</th>
<th>Windows 8 Applications in the Enterprise</th>
<th>The Effective Developer / Administrator</th>
<th>Better Together</th>
<th>The Secure Workplace</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lite Touch Installation</strong></td>
<td></td>
<td>❖</td>
<td></td>
<td></td>
<td>❖</td>
<td></td>
<td></td>
<td></td>
<td>❖</td>
</tr>
<tr>
<td><strong>Zero Touch Installation</strong></td>
<td>❖</td>
<td>❖</td>
<td>❖</td>
<td>❖</td>
<td>❖</td>
<td>❖</td>
<td>❖</td>
<td>❖</td>
<td>❖</td>
</tr>
<tr>
<td><strong>User Driven Installation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>❖</td>
<td>❖</td>
<td>❖</td>
<td>❖</td>
<td>❖</td>
</tr>
<tr>
<td><strong>OEM Installation</strong></td>
<td>❖</td>
<td></td>
<td></td>
<td></td>
<td>❖</td>
<td></td>
<td></td>
<td></td>
<td>❖</td>
</tr>
<tr>
<td><strong>Offline Installation</strong></td>
<td>❖</td>
<td></td>
<td></td>
<td></td>
<td>❖</td>
<td></td>
<td></td>
<td></td>
<td>❖</td>
</tr>
<tr>
<td><strong>VDI</strong></td>
<td>❖</td>
<td>❖</td>
<td>❖</td>
<td>❖</td>
<td>❖</td>
<td></td>
<td></td>
<td>❖</td>
<td>❖</td>
</tr>
<tr>
<td><strong>Windows To Go</strong></td>
<td>❖</td>
<td>❖</td>
<td>❖</td>
<td>❖</td>
<td>❖</td>
<td></td>
<td></td>
<td>❖</td>
<td>❖</td>
</tr>
</tbody>
</table>
Volume Activation
What is Volume Activation?

- Automates and manages the activation process of Volume Licensing media
- Used strictly as a tool for activation and is not tied to license invoicing or billing
- Activation confirms the genuine status of a product and that the product key is not compromised
- Applies to Windows 8 and Office Professional Plus 2013
Activation Methods

- **Key Management Service (KMS)**
  - A server-client model in which a computer serves as the KMS host
  - A KMS host key must be installed and activated
  - This establishes a local activation service in your environment

- **Multiple Activation Key (MAK)**
  - If you use a MAK key, Office client computers are activated online by using the Microsoft hosted activation servers or by telephone

- **Active Directory-Based activation**
  - Available only for Office on Windows 8 and Windows Server 2012
  - Active Directory-Based activation can activate all Office Professional Plus 2013 volume license clients throughout a domain
  - Active Directory-Based activation is set up through Active Directory Domain Services (AD DS) from either a Windows 8 volume license edition computer or a Windows Server 2012 computer
Key Management Service (KMS)

- Install KMS on a host machine and activate once with KMS host key
- The KMS host key for Office is not specific to a particular operating system
- Supported operating systems for KMS host:
  - Volume License editions of Windows 7 & Windows 8
  - Windows Server 2008 R2 & Windows Server 2012
- No product keys are specified in Office configuration file (.msp or Config.xml) or post-setup routine
- Volume license clients detect KMS automatically
- KMS clients regularly reactivate
  - Non-perpetual activation (every 180-days) - completely transparent to customer
  - If activation does not occur during the 180-day period, Office 2013 goes into the out-of-tolerance state for 30 days - users then see notifications that request activation
  - If activation does not occur during the out-of-tolerance state, Office 2013 goes into the unlicensed notification state. Users then see notifications that request activation and a red title bar
  - Communication between KMS and Client never exposed to Microsoft
Multiple Activation Key (MAK)

- A MAK key is used for one-time activation with the Microsoft hosted activation services.
- Each MAK key has a predetermined number of allowed activations.
- Each MAC activation counts toward the activation limit.
- Once Office is activated, no re-activation is required unless the hardware changes significantly.
- MAK activation requires that a MAK key is installed on a client computer and instructs that computer to activate itself against Microsoft hosted activation servers over the Internet – this can be configured in an .msp using OCT.
- There are two ways to activate computers by using a MAK key:
  - MAK Independent Activation - requires that each computer independently connect and be activated with Microsoft, either over the Internet or by telephone.
  - MAK Proxy Activation by using Volume Activation Management Tool - enables a centralized activation request on behalf of multiple computers that have one connection to Microsoft.
Active Directory-Based activation

- Active Directory Domain Service must be at the Windows Server 2012 schema level to store activation objects - domain controllers running earlier versions of Windows Server can activate clients after their schemas have been updated using the Windows Server 2012 version of Adprep.exe
- Active Directory-Based activation activates Office VL clients within the domain
- Available for Office 2013 on Windows 8 or Server 2012 – activation occurs automatically without user intervention
- A successful Active Directory-Based activation grants a license to the Office client for 180 days
- Activation is distributed throughout the domain and remains as long as machine is a member of the domain
Windows 8 clients can use Active Directory-based activation or KMS

Windows 7 must use KMS

Disconnected machines can use MAK activation
Considerations

• Active Directory-based Activation simplifies the process of activating clients that are running Windows 8 or Windows Server 2012
  • Requires the Windows Server 2012 AD DS schema
  • Activation objects themselves are not editable but can be view/deleted using AD DS tools

Recommendations

• Use KMS If you there are multiple versions of Windows client and server operating systems deployed
  • KMS is the default key for volume activation clients, regardless of the Windows version running
  • Ensure that the firewall ports for KMS activation are opened
• Use MAK for disconnected machines from CorpNet
• Use the Volume Activation Management Tool (VAMT) for bulk activation
• Ensure there are the right keys available prior deployment
Hardware Lifecycle Management
Windows 8 - Great Experience Across Hardware

- Touch
- Long Battery Life
- Thinner, Lighter, Faster
- Modern Security
- Sensors
- New Form Factors
Hardware Lifecycle Management

- Hardware Lifecycle Management is the set of processes that introduce, update and decommission hardware into the enterprise.
- When new hardware is introduced, drivers and hardware based software must be certified before they are deployed.
- Configuration of hardware at deploy-time can have significant effects on the manageability of the desktop.
- Setting Bring Your Own Device (BYOD) guidelines.

Enterprise Desktop Stack

- User settings
- Individual applications
- Role-based applications
- Enterprise applications
- Security configuration
- Hardware-based software & drivers
- Operating system master image
Hardware Lifecycle
Discovery and assessment

- What information do you already have?
  - Makes and Models currently in the enterprise
  - Configuration Manager inventory (Upgrade Assessment)

- Assessment and Tools
  - Microsoft Assessment and Planning Tool (MAP)
  - Contact vendors
  - Engage Hardware Council
Common Business Concerns

- We have a varied set of hardware and a continuous refresh cycle.
- We need our deployment solution to deploy the correct drivers for each solution without regenerating images.
- We need to ensure our hardware supports Windows 8.
- We need to ensure our machines conserve power when they are not utilized.
- We have a large number of peripherals in the enterprise. We cannot test each one individually, we need to collect data about these during a pilot phase.
- We need to ensure our machines are configured and patched even when they have been turned off.
Hardware Management Technologies
Supporting decisions

Considerations

• Machines not configured correctly at deploy time may require desk-side visits
• AMT requires infrastructure and Intel vPro chipsets
• Wake on LAN (WoL) requires network infrastructure to be set correctly
• PXE requires WDS infrastructure and BIOS configuration set correctly

Recommendations

• Ask vendor or asset management team to set initial configuration settings
• Consider using AMT, if available, to configure hardware management going forward
• Engage network team early to identify WoL and PXE blockers
Security Management
Security Management is the set of processes that ensure the security baseline of an enterprise desktop.

Several of these processes involve configuration and decisions at the time of deployment, including how to apply the latest patches, GPOs, firewall and anti-malware settings as well as which encryption strategy to use.
Application Lifecycle
Application Lifecycle

Processes used to introduce, update and remove applications and their assignments to roles which feed into the image deployment process.
Application Lifecycle
Common business concerns

- We have too many applications in our enterprise and this is causing management, cost and compliance issues
- We don’t know which of our applications require remediation and/or packaging
- Some of our applications cannot coexist even if they are needed by the same user
- Managing which applications are assigned to which user or computer is difficult, we need a better way of determining this
- Determining what user settings to configure and how to maintain is overwhelming
Two Most Common Reasons for Application Failure

- **Standard User Accounts**
  - It costs less to manage standard user accounts, however many applications break when you remove administrator rights
  - If you are running Vista or 7 with UAC you have already overcome most of these issues
  - UAC is required in Windows 8 to support Windows Store applications, so you must not disable UAC in Windows 8
  - If you are moving from XP, you will need to address running applications as standard users

- **Version Checks**
  - Windows 8 maintains the same major version number as Vista and Windows 7 (6). The minor version has changed.
  - Some applications perform version checks only for a specific version instead of “this version or later”
  - This is an easy issue to mitigate
Application Compatibility

- Can require the most time and effort for any OS deployment project
- Generates the most serious blocking issues
- Keep in mind – application compatibility is a risk-management activity
  - The higher percentage of applications that are likely to fail, the more work you should invest in proactive testing to verify a critical application is not one of them
  - As the percentage decreases, the number of applications for which exhaustive testing is worthwhile shrinks
Managing Application Readiness

- Application Discovery
- Analyze Applications
- Assess and Mitigate
- Explore Delivery Options

Sequence Testing, Piloting and Deployment Efforts
Prioritization of applications has largest impact on project

In some cases it makes sense to start with inventory of applications

In other cases, it may be more sensible to build the list manually by just asking

Try to discover all of the applications that should be managed (but not just every application)
Application Analysis

- Eliminate Redundant or Unused Applications
- Remove Multiple Versions of Same Application / Standardize
- Prioritize Based on Business Use
Application Compatibility Toolkit 6.0

- Installed as part of the Windows Assessment and Deployment Kit (ADK)
- Supports Windows 8 application compatibility, focused on operating system deployment
- URL support for IE 10 site testing
- Deploy data collection packages as part of Install Launch Testing on Windows 8 before performing any UAT or pilot
- Obtain compatibility information from the ACT Community
- Standard User Analyzer and Compatibility Administrator to provide analysis and remediation (shimming)
Assess Incompatibilities & Mitigation Options

Does the vendor support the application on Windows 8?
Don’t spend the money to test and remediate if you will not receive vendor support!

Use UAT as the final arbiter of compatibility
Let your users determine if any bugs exist that impact user scenarios

Mitigation Options
Replace non-compatible app with a new version
Create shims for existing applications
Use Group Policy to change offending behavior of the application
Prepare for New Application Delivery Options

- An OS upgrade project is a great time to rethink how you package and deliver applications.
- Windows 8 opens up additional capabilities with the Windows Store and sideloading Store applications.
- Include applications in the new OS image.
- AppV 5.0 provides a very flexible and powerful application packaging and delivery model.
Packaging and Sequencing Strategy
Supporting Decisions

- Considerations
  - Packaging software vs. sequencing software
  - In house packaging vs. factory outsourcing
  - Compatibility and remediation assessments require involvement of application owners

- Recommendations
  - Create an application compatibility lab and test using the current enterprise image from the Image Engineering process
  - Engage application owners early in the process and maintain a lab to Q/A packages
  - Virtual (sequence) applications wherever feasible
Application Targeting & Assignment Strategy

- **Role-based Targeting**
  - Can reduce variants of desktops
  - Requires process to maintain going forward
  - Easier to manage application dependencies
  - Segues naturally into deployment sequencing

- **Active Directory Group Membership**
  - Configuration Manager can discover and import Active Directory group membership
  - Group membership can drive collection membership

- **Application Model**
  - In previous versions of Configuration Manager, collection membership rules and program “Run before” were required to manage deployments
  - Now with the Application Model, rules and conditions can be declared natively inside of Configuration Manager and target users
Sequence Your testing, Piloting and Deployment Efforts

- Deploy by Role
- Identify applications per Role
- Prioritize Roles based on small number of applications, or where the user base is more tolerant of change
- Begin piloting within the Role
- Build momentum Role by Role
User Settings
The User Profile Management group of processes are responsible for management of user data and settings as well as migration of this data and settings to new machines.
Common Business Concerns

- We have regulatory requirements for user data
- Our users have a significant amount of data, we only want to store data on the network on machine replaces
- Our users store data everywhere on the machine and we cannot ensure backup and version control
- We want to preserve settings that relate to user productivity
- We do not want to migrate non-business data
User Data and User State Migration

- USMT 5.0 is available as part of the Windows Assessment and Deployment Kit (Windows ADK) for Windows 8
  - Includes version 6.2 of loadstate, scanstate and usmtutils
  - Full support for Windows 8

- Hard-link migration
  - USMT 5.0 continues to support local storage of user data during an in-place refresh
  - Minimal network traffic, very fast process to hard-link local data

- Offline Capture
  - Captures file offline – no connectivity needed
  - Reduces chances of files being open or in use

- Document Finder
  - Simplified migration rules
What to Migrate
Supporting decisions

Considerations

• Migrating more files takes more space but not migrating something could yield in data loss
• Some settings do not translate well to Windows 8, such as the start menu
• Some file types such as mp3s may seem as non-business related but may actually have legitimate business value
• Application related settings migration is usually not well documented

Recommendations

• Engage business units to discover business critical file-types
• Use document finder to find documents across the machines
• Exclude network and attached storage
• Ensure application “personality” is documented by application owners
Where to Store Data
Supporting decisions

Considerations

- Network speed and storage of user data can often be the bottleneck in deployment capacity
- Hard-link migration can only be performed on refresh scenarios

Recommendations

- Run USMT estimates well before migration to determine scale for storage
- Leverage hard-links for refresh scenarios
- Consider regulatory requirements for retention
- Redirect “My Documents” to lessen load
Where to Perform Capture
Supporting decisions

Considerations

- Offline vs. Online Capture
- During maintenance window or ahead of time during the day
- Lock out user or communicate?

Recommendations

- Ensure appropriate user communication to minimize impact
- Perform capture at time of deployment to ensure up-to-date data
- Use offline capture if appropriate as it requires customization to invoke with tools
User Experience Virtualization (UE-V)

- New for Microsoft Desktop Optimization Pack (MDOP) subscribers
- Provides a consistent settings experience for end users as they roam between devices and between operating systems
- Custom templates can be generated on an application-by-application basis
  - Defines which application settings and files migrate with the end user

- UE-V Settings (per user)
- UE-V Templates (per application)
## User Experience Virtualization (UE-V)

### Supported OS

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Minimum Service Pack</th>
<th>Supported Architectures</th>
<th>.NET Framework Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7</td>
<td>SP1</td>
<td>32-bit or 64-bit</td>
<td>.NET 4.0 or .NET 3.5 SP1</td>
</tr>
<tr>
<td>Windows 8</td>
<td>None</td>
<td>32-bit or 64-bit</td>
<td>.NET 4.0 or .NET 3.5 SP1 (agent)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>.NET 4.0 (template generator)</td>
</tr>
<tr>
<td>Windows Server 2008 R2</td>
<td>SP1</td>
<td>64-bit</td>
<td>.NET 4.0 or .NET 3.5 SP1</td>
</tr>
<tr>
<td>Windows Server 2012</td>
<td>None</td>
<td>64-bit</td>
<td>.NET 4.0 or .NET 3.5 SP1 (agent)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>.NET 4.0 (template generator)</td>
</tr>
</tbody>
</table>
Thank you