Microsoft System Center Deployment at The Shepherd Color Company

By Ian Iliff

Submitted to the Faculty of the Information Technology Program in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Information Technology

University of Cincinnati
College of Criminal Justice, Education, Human Services
June 2012
Microsoft System Center Deployment at The Shepherd Color Company

By
Ian Iliff

Submitted to the Faculty of the Information Technology Program
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Technology

© Copyright 2012 Ian Iliff

The author grants to the Information Technology Program permission
to reproduce and distribute copies of this document in whole or in part.

__________________________ __________________
Ian Iliff        Date

__________________________ __________________
Mark Stockman       Date
Acknowledgements/Dedication

This document is dedicated to two individuals who were instrumental to my education in the field of Information Technology. The first is my professor and senior design advisor, Mark Stockman. Professor Stockman is responsible for the majority of my technical learning while at the University of Cincinnati. The second individual I would like to acknowledge is Jeff Lane. Jeff is one of the other administrators at the Shepherd Color Company. Jeff’s guidance throughout the development of my professional technical career has been invaluable. Without the advice and instruction of Jeff and Mark, the project completed in this document would not have been possible.
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledgements</td>
<td>i</td>
</tr>
<tr>
<td>Table of Contents</td>
<td>ii</td>
</tr>
<tr>
<td>List of Figures</td>
<td>iii</td>
</tr>
<tr>
<td>Abstract</td>
<td>iv</td>
</tr>
<tr>
<td>1. Project Description and Intended Use</td>
<td>1</td>
</tr>
<tr>
<td>1. 1 Statement of the Problem</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Description of the Solution</td>
<td>3</td>
</tr>
<tr>
<td>1.3 User Profile</td>
<td>6</td>
</tr>
<tr>
<td>2. Design Protocols</td>
<td>8</td>
</tr>
<tr>
<td>3. Deliverables</td>
<td>11</td>
</tr>
<tr>
<td>4. Project Planning</td>
<td>12</td>
</tr>
<tr>
<td>4.1 Budget</td>
<td>12</td>
</tr>
<tr>
<td>4.2 Timeline</td>
<td>14</td>
</tr>
<tr>
<td>5. Proof of Design</td>
<td>14</td>
</tr>
<tr>
<td>5.1 Configuration Manager: Software Distribution</td>
<td>14</td>
</tr>
<tr>
<td>5.2 Configuration Manager: Windows Updates Deployment</td>
<td>16</td>
</tr>
<tr>
<td>5.3 Configuration Manager: Remote Administration</td>
<td>18</td>
</tr>
<tr>
<td>5.4 Forefront: Client Anti-Virus Protection</td>
<td>19</td>
</tr>
<tr>
<td>5.5 Forefront: Protection for Exchange</td>
<td>23</td>
</tr>
<tr>
<td>5.6 Virtual Machine Manager: Centralized VM management</td>
<td>24</td>
</tr>
<tr>
<td>5.7 Virtual Machine Manager: P2V Functionality</td>
<td>27</td>
</tr>
<tr>
<td>6. Testing</td>
<td>28</td>
</tr>
<tr>
<td>7. Conclusions and Recommendations</td>
<td>30</td>
</tr>
<tr>
<td>7.1 Conclusion</td>
<td>30</td>
</tr>
<tr>
<td>7.2 Recommendations</td>
<td>31</td>
</tr>
<tr>
<td>8. References</td>
<td>32</td>
</tr>
<tr>
<td>9. Appendices</td>
<td>34</td>
</tr>
<tr>
<td>8.1 Appendix A: Documentation on Completing Tasks</td>
<td>34</td>
</tr>
</tbody>
</table>
## List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1.</td>
<td>2</td>
</tr>
<tr>
<td>Figure 2.</td>
<td>5</td>
</tr>
<tr>
<td>Figure 3.</td>
<td>7</td>
</tr>
<tr>
<td>Figure 4.</td>
<td>8</td>
</tr>
<tr>
<td>Figure 5.</td>
<td>9</td>
</tr>
<tr>
<td>Figure 6.</td>
<td>10</td>
</tr>
<tr>
<td>Figure 7.</td>
<td>11</td>
</tr>
<tr>
<td>Figure 8.</td>
<td>12</td>
</tr>
<tr>
<td>Figure 9.</td>
<td>13</td>
</tr>
<tr>
<td>Figure 10.</td>
<td>14</td>
</tr>
<tr>
<td>Figure 11.</td>
<td>14</td>
</tr>
<tr>
<td>Figure 12.</td>
<td>15</td>
</tr>
<tr>
<td>Figure 13.</td>
<td>16</td>
</tr>
<tr>
<td>Figure 14.</td>
<td>17</td>
</tr>
<tr>
<td>Figure 15.</td>
<td>18</td>
</tr>
<tr>
<td>Figure 16.</td>
<td>19</td>
</tr>
<tr>
<td>Figure 17.</td>
<td>19</td>
</tr>
<tr>
<td>Figure 18.</td>
<td>20</td>
</tr>
<tr>
<td>Figure 19.</td>
<td>21</td>
</tr>
<tr>
<td>Figure 20.</td>
<td>22</td>
</tr>
<tr>
<td>Figure 21.</td>
<td>23</td>
</tr>
<tr>
<td>Figure 22.</td>
<td>24</td>
</tr>
<tr>
<td>Figure 23.</td>
<td>25</td>
</tr>
<tr>
<td>Figure 24.</td>
<td>26</td>
</tr>
<tr>
<td>Figure 25.</td>
<td>27</td>
</tr>
<tr>
<td>Figure 26.</td>
<td>28</td>
</tr>
</tbody>
</table>
Abstract

In September of 2011, the enterprise network at The Shepherd Color Company had expanded to the point in which it was nearly impossible to manage by the company’s three administrators. With nearly two hundred clients and servers, efficient network management was a daunting task. Furthermore, the organization was paying a substantial sum of money for Symantec security products to protect systems at the organization. This project details the implementation of the Microsoft System Center family of products to remedy some of the infrastructure problems present at Shepherd Color. System Center Configuration Manager provided a centralized management point for all of the systems on the Shepherd Color network. Microsoft Forefront Endpoint Protection and Forefront for Exchange replaced the antiquated and expensive Symantec products which were running on clients and servers on the network. Finally, Virtual Machine Manager was implemented to provide a centralized point to manage the company’s 70+ virtual servers. The implementation of this project has resulted in increased administrative productivity, reduced annual licensing fees, and established better network continuity.
Microsoft System Center Deployment at The Shepherd Color Company

1. Project Description and Intended Use

1.1 Statement of the Problem

In the diverse network infrastructure that is a cooperate network, there are many best practices that need to be followed in order to maintain a secure, efficient, and accessible network. The world of Information Technology is changing at such a degree that it may be difficult for organizations to keep up with these best practices as much as they should. Sometimes all it takes is a compelling business need and a brilliant software innovation to spark the move to migrate from one technology to another.

The Shepherd Color Company once used several different standalone technologies to complete different administrative tasks. For example: if an administrator would have wanted to monitor an anti-virus client running on a server on their network, they needed to log on to a dedicated server running third party anti-virus management software (Symantec Endpoint Protection). If that same administrator wanted to check the current patch status of Windows Updates on that server, they needed to log into yet another server in charge of Windows Update Services (1, 9). The use of some of these third party technologies required the need for expensive and complex licensing scenarios, which required considerable resources in both time and capitol to address. Another drawback to the use of software which requires multiple licensing scenarios, was keeping compliant with the terms of use expressly indicated in the licensing agreement. It was not uncommon for an administrator to dedicate his or her time to research the details of licensing, and then verify that each system fell within the limitations of the terms of use (11).
Previous to the implementation of this project, there were multiple dedicated servers in charge of providing both anti-virus and Windows Update services. Shepherd Color had three different anti-virus servers responsible for deploying and monitoring clients on the network. A fourth server was also required to provide Windows updates to servers and workstations to insure that they are protected from the most recent security threats prevalent on the web. Each one of these servers required the use of a Windows server license in order to fall within the legal confines of Shepherd Color’s Enterprise License Agreement. Figure 1 shows a network diagram of the anti-virus and Windows update servers which were running on Shepherd Color’s network.

Figure 1: AV and Windows update servers previously running on Shepherd Color’s Network
As the network at The Shepherd Color Company expands, the vast majority of new servers running at The Shepherd Color Company are being created in a virtual environment. The addition of these new servers caused management problems in the sense that there was no centralized point for administrators to oversee virtual machines (2). Virtual servers run on physical machines known as virtual host servers. Shepherd Color currently has seven virtual host servers running roughly 72 virtual servers. Furthermore, the virtual hosts ran on both Microsoft HyperV platforms, and VMWare platforms, farther complicating administration and licensing. Previous to this project, there was no way to uniformly manage all of these devices from one management console. Administrators also faced the problem that some older physical servers were running on aging hardware. In the event that one of these servers goes down, there was no plan in place or redundant system to take of the services provided by these servers. The Shepherd Color Company also had no way to monitor the health of these servers; short of logging on to each server individually to perform administrative tasks. Technology needed to be implemented which could provide centralized health monitoring of these servers, and even the means to convert the boxes from their physical forms into virtual servers.

The Shepherd Color Company was under the implementation of the old network management/network security model. In the past, security and management have existed as two separate entities in the cooperate network (1). However, new software innovations by Microsoft have enabled some corporations to integrate all aspects of network management into one simple one stop solution: Microsoft System Center.

1.2 Description of the Solution

Microsoft System Center family of products has several components to greatly enhance the management, control, and security of Shepherd Color’s cooperate network. The plan of this
deployment scenario was to install the base elements of System Center known as System Center Configuration Manager. The prerequisite steps needed to install Configuration Manager created a foundation for the rest of the System Center products. Once System Center Configuration Manager was installed, other System Center products could be installed and rolled out through Configuration Manager. The System Center deployment at Shepherd Color consists of several components of System Center. The following is a list of some of these components and their benefits to the network infrastructure at Shepherd Color.

1. System Center Configuration Manager: (1, 2, 3, 9)
   - Server and Workstation Patch Management
   - Inventory Management
   - Application Deployment
   - Workstation Image Deployment
   - Remote Administration Tools

2. System Center Virtual Machine Manager: (2, 5)
   - Streamline of Virtual Machine Management
   - Integration of VMware and Microsoft HyperV environments
   - Advanced Physical to Virtual Machine support

2. Microsoft Forefront Client Security: (9) (10) (11)
   - Enterprise Level Endpoint Anti-Virus features
   - Cost Savings when moving from Symantec Products
Figure 2 shows a logical layout of the Servers and Clients on the Shepherd Color network after the System Center implementation. The following diagram provides an overview of the specialized servers used in this deployment. It should be noted that ShCo-CM1 houses services for both Forefront and Configuration Manager:

**Figure 2: MSSC Logical Network Diagram:**

*Note: The Configuration Manager server provides all the roles of the servers seen in Figure 1*
1.3 User Profile

Microsoft System Center has one group of primary users: The Network Administrators at the Shepherd Color Company. In reality, any user who connects to a computer network at Shepherd Color indirectly benefits from the System Center deployment. Figure 3 shows two actors interacting with The System Center use case diagram. The first actor, the MSSC admin, can be any network administrator already present at The Shepherd Color Company. The MSSC admin will be responsible for performing administrative tasks inside System Center. These tasks include, but are not limited to:

1. Deploying various software packages to end user clients (MSSCCM).
2. Managing and installing Windows Updates on server and workstation clients (MSSCCM).
3. Deploying Anti-Virus clients to end user workstations and servers. (MSSCF).
4. Managing and configuring virtual machines across the network (MSSCVM).

The second actor in this use case scenario is the MSSC Technician. The MSSC Tech is the user who installed and performed the initial configuration of System Center. It should be noted that the MSSC Technician mentioned throughout this document was Ian Iliff. In the case of this scenario, one particular user performed both the roles of MSSC Tech and MSSC Administrator (Ian Iliff). This deployment procedure was done “in house”; however, there was an outside contractor available in case of the event that unforeseen problems should arise. The outside contractor would have also acted as both a MSSC Tech and a MSSC Administrator due to the fact that particular individual would need administrative access to multiple areas of the
project. Luckily, the services of an outside actor were never needed to any large degree during the implementation of this project.

End users also indirectly interact with the System Center deployment. Their client System is managed though System Center Configuration Manager. Furthermore, they also have the Microsoft Forefront Client installed on their client PC to provide anti-virus protection. It was the intention of this project for the end user to be unaware of any changes to his or her workstation, but also to receive the full benefits of System Center. These benefits come in the form of increased productivity due to increased system performance and management.

FIGURE 3: Active Users and Their Administrative Functions
2. Design Protocols

Configuration Manager and Forefront Endpoint Protection can all be accessed and administered from a central location: The Configuration Manager Console.

Features of Configuration Manager and Forefront

This section focuses on some of the explicit features and added benefits of a System Center Deployment at The Shepherd Color Company. Examples provided in this section are taken from the live environment currently running at Shepherd Color. The Configuration Manager Console is a MMC snap in that provides a centralized point for features such as:

1. Software Deployment: Software can be deployed to clients or collections of clients interactively though the console. This eliminates the need to push software though complex group policy objects or manual installations.

2. Agent Deployment: Program agents can be configured and deployed through the management console. These agents are responsible for administrative tasks such as hardware inventory of clients, software status metering, power management, and much more. Figure 4 shows some of the program agents available in Configuration Manager.

![Figure 4: Available Configuration Manager Agents](image-url)
3. System Collections: Collections are containers of client servers and workstations similar to OUs in Active Directory. Configuration Manager uses collections to group clients according to similar features. For example: an administrator may want to deploy an application simultaneously to all Windows XP clients they would have to do is right click the Windows XP collection, and select “Deploy Package”.

4. Windows Update Point Management: The Configuration Manager Console contains a centralized point to configure and approve updates from Microsoft. From this point, administrators can approve and distribute updates to the appropriate collections of clients.

6. Microsoft Forefront Endpoint Protection: Forefront Endpoint Protection is also administered though the Configuration Manager Console. From this point: administrators receive interactive reports about the status of malware and virus definitions on the network, create and manage specific policies for each collection of like clients, Create
custom client deployment packages to be pushed through software deployment, and much more. Figure 6 shows an example of some of the information that can be obtained from this point.

Figure 6: The Forefront Endpoint Protection Dashboard
**Virtual Machine Manager**

Virtual Machine manager has two intended functions in relation to this project: to provide a centralized management point for all virtual machines across the network, and to easily enable administrators convert physical machines into virtual machines. Figure 7 shows the Virtual Machine Management interface. Once implemented the interface in figure 7 will be populated with all of the virtual machines across the company:

![Virtual Machine Manager Admin Console](image)

**Figure 7: Virtual Machine Manager Admin Console**

3. Deliverables

The following changes/additions have been made to The Shepherd Color Enterprise Network:

1. All Symantec Anti-Virus clients have been removed from the Shepherd Color Network.
2. Microsoft Forefront clients have been deployed Network-Wide to replace the removed Symantec clients.
3. Hardware and Software can be interactively inventoried from ShCo-CM1. Software inventory provides a centralized point for administrators to oversee the status of
software licenses and version information. Hardware inventory can allow administrators to detect aging hardware and mitigate the risk of failure.

4. Microsoft Virtual Machine Manager is installed and functioning, providing administrators with centralized access to their virtual machines. Administrators will then be able to easily convert physical systems to virtual machines.

5. Four (4) unneeded servers have been shutdown (AV1-3, Update1).

6. Windows Updates are deployed from ShCo-CM1.

7. Documentation of all processes and installation steps have been created and given to the Shepherd Color Company.

4. Project Planning

4.1 Budget

It is difficult to address the exact cost of a Full System Center Deployment. This is due to the fact that Microsoft enterprise licensing schemes include a packages of software, rather than individual pieces of software themselves. The System Center Suite was purchased along with other Microsoft products, therefore, the cost of licensing has already been accounted for in Shepherd Color’s yearly Microsoft subscription (In fact, the notion that Shepherd Color is paying for software that is not used, could be seen as a waste of funds).

The original project proposal for a Microsoft System Center deployment at the Shepherd Color Company was prepared by an outside consulting organization. Shepherd Color uses this IT consulting group for advanced network configuration procedures (such as router and firewall configurations). Figure 9 shows the proposed project cost presented to Shepherd Color by this particular consulting group. Figure 9 also shows the actual cost of the project done “in house” rather than an outside consulting organization.
The availability of a System Center engineer in the event of unforeseen issues during deployment employs a “Best of Both Worlds” approach to the System Center deployment. It keeps the project costs “in house” rather than contracted out to an outside consultant firm; while it provides a safety net in the event of project snags. Furthermore, the availability of a MSSC engineer to review deployment plans before the project is actually implemented adds a certain level of assurance that the deployment will go smoothly. Mitigation of risks early in the project should ensure that no outside consultants need be present (or summoned in the case of a project snag) during the actual deployment.

<table>
<thead>
<tr>
<th>Installation</th>
<th>MS Partner Time</th>
<th>Total Project Cost</th>
<th>&quot;In House&quot; Project Time</th>
<th>&quot;In House Project Cost&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Manager</td>
<td>80 Hours</td>
<td>$11,600.00</td>
<td>140 Hours</td>
<td>$2,660.00</td>
</tr>
<tr>
<td>VM Manager</td>
<td>40 Hours</td>
<td>$5,400.00</td>
<td>80 Hours</td>
<td>$1,520.00</td>
</tr>
<tr>
<td>Forefront</td>
<td>est 40 Hours</td>
<td>est $5,400</td>
<td>60 Hours</td>
<td>$1,140.00</td>
</tr>
<tr>
<td>Totals</td>
<td>160 Hours</td>
<td>$22,400.00</td>
<td>280 Hours</td>
<td>$5,320.00</td>
</tr>
</tbody>
</table>

**Figure 9: Cost Savings of In House System Center Deployment at The Shepherd Color Company**

*Note: Fields marked with an “est” are estimations*

An annual savings is also incurred as a result of this project. The result of ending license agreements with Symantec will save the company a substantial sum of money on a yearly basis. (10, 11) Furthermore, cooling and energy savings are now possible with the impending shutdown of several physical servers in the datacenter. (5) These servers will be converted into virtual machines by way of Virtual Machine Manager. Figure X below details a rough estimation of yearly re-occurring cost savings as a result of this project.
4.2 Timeline

Figure 10: Annual Re-Ocurring Cost Savings

5. Proof of Design

This section details the new features available now that System Center has been implemented at Shepherd Color. This section will explore all three new technologies, provide descriptions of their respective abilities, and provide examples of their effective use.

5.1 Configuration Manager: Software Distribution

Software distribution empowers administrators to deploy a certain piece of software to multiple groups of systems from a centralized point. The Configuration Manager console can target one or more systems with pre-made software packages created by an administrator. These
packages can be customized to run with certain scripts which will allow the administrators to set special parameters for their deployment. Some of these properties include:

- The Ability to be deployed on a schedule.
- The ability to be installed manually by the user. The use can be passed administrative rights to run the particular task.
- The ability to run in the background without the user being aware of the task.
- The ability to uninstall other products before the package is installed. This feature was particularly useful with deploying Forefront. The installation package was able to remove the Symantec clients before installing Forefront, preventing the complication of having multiple AV clients on one machine.

![Figure 12: Configuration Manager Software Distribution Dashboard](image-url)
Figure 13 shows some of the available packages which can be deployed via Configuration Manager Software deployment. The properties of these packages can be tweaked or modified by administrators to suit their specific needs during deployment.

### Figure 13: Configuration Manager Software Distribution Packages

<table>
<thead>
<tr>
<th>Packages</th>
<th>Systems Found</th>
</tr>
</thead>
<tbody>
<tr>
<td>Look For:</td>
<td>in All Columns</td>
</tr>
<tr>
<td>Name</td>
<td>Manufacturer</td>
</tr>
<tr>
<td>.NET</td>
<td>Citrix</td>
</tr>
<tr>
<td>Citrix Client Push</td>
<td></td>
</tr>
<tr>
<td>FOGST</td>
<td>Fossil</td>
</tr>
<tr>
<td>Lenovo Driver Update</td>
<td>Lenovo</td>
</tr>
<tr>
<td>Configuration Manager Client Upgrade</td>
<td>Microsoft</td>
</tr>
<tr>
<td>Office 2010 LT Edition</td>
<td>Microsoft</td>
</tr>
<tr>
<td>FEP - Deployment</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>FEP - Operations</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>FEP - Policies</td>
<td>Microsoft Corporation</td>
</tr>
</tbody>
</table>

5.2 Configuration Manager: Windows Updates Deployment

Previous to the implementation of this project, Windows Updates were deployed from an old WSUS server: Update1. Update1 was an aging physical server, which needed to be replaced. Windows updates are now deployed from the Software Update Point running from Configuration Manager. Software Updates are automatically downloaded on a weekly basis and stored on a repository running on the Configuration Manager server (ShCo-CM1).

Configuration Manager’s software updates provide advanced logging and reporting abilities which were not available with the WSUS server. Like Software Deployment packages, custom Software Update packages were created by administrators to streamline and customize deployment of Windows Updates. Features of these custom packages are as follows:

- Scheduled Windows Updates.
• Suppression of system restart after installation of updates. Updates can also be set to be automatically downloaded, automatically installed, or both.

• Deployment to specific collections or software types.

• Deployment of groups of updates in order to apply a “mass update” of a spectrum of products at a time.

Figure 14: Configuration Manager Software Updates Dashboard

Figure 15 shows a list of current lists of updates and deployment templates created by the administrators at Shepherd Color. Additional deployment lists can be created in order to consolidate updates into single tasks.
5.3 Configuration Manager: Remote Administration

One of the most useful new tools for administrators is the group of remote tools available with Configuration Manager. Administrators now have direct control of remote clients as if they were sitting right behind the computer. The list below details some of the many beneficial features of this particular piece of Configuration Manager:

- The ability to open the event logs of a remote machine with two clicks of the mouse. This enables administrators to review logging of errors to aid in the troubleshooting of any particular issues that may have arisen on that particular machine.
- The ability to see what types of hardware and software are present on the client. With a click of a mouse the Administrator is able to get a report of installed software, including versions and update levels.
- The ability to remotely control the client. Remote Control is very different than remote desktop. The remote control tool allows administrators to shadow a user’s active session. This essentially puts the administrator in the room with the end user and empowers him
or her to control their screen in real time. The remote control tool has made troubleshooting on user workstations significantly easier.

- The ability to start a remote desktop session into any client with one click of the mouse.

![Figure 16: Configuration Manager Client Options](image)

![Figure 17: Configuration Manager Remote Options](image)

### 5.4 Forefront: Client Anti-Virus Protection

Microsoft Forefront Endpoint Protection has replaced the currently running Symantec Endpoint Protection products running at Shepherd Color. Instead of having its own proprietary console, Forefront Endpoint Protection is manager from Configuration Manager. Configuration Manager deploys Forefront clients and provides advanced reporting of Virus and Malware activities which may be occurring on the network.
The forefront dashboard provides a centralized point from which administrators can review all malware activity on the network. From here, administrators can keep an eye on the virus definition status of all clients on the network. Although clients should be receiving updates on a regular basis, certain conditions may prevent this from happening, which need to be addressed for security concerns. Administrators can also monitor the deployment status of both the Forefront Client and the respective Forefront policy which each client receives.

Figure 19 shows a list of custom forefront policies which have been deployed to various systems on Shepherd Color’s Network. Custom polices must be created for certain groups of servers and workstations to accommodate existing software and features running on the systems. Some examples of such custom policies are as follows:
- Custom Backup Server Policy: Backup servers have huge directories containing backups of company data, and information from every server on the network. If Forefront were to scan these directories during its weekly scan, the scan would take hours to complete.

- Exchange Server Policy: Exchange servers contain all user’s e-mail mailboxes, scanning these boxes would also take a considerable amount of time and resources. Forefront Protection For Exchange was implemented on the Exchange servers to perform active mailbox scanning since Endpoint Protection is not being used for this task.

Figure 19: Configuration Manager Forefront Deployed Policies

Figure 20 shows a tab from one of the pre-configured Forefront policies. Each policy is configured to use Configuration Manager as the primary source for definition updates. However, in the event that the client cannot reach Configuration Manager, back up resources are available for updates. Custom policies also allow for the exclusion of certain file types during scans,
limitation of local resources during scans, and can interactively set the frequency of scans.

Policies also control what happens when malware is found.

![ShCo File Server Policy Properties](image)

**Figure 20: Configuration Manager Forefront Policy Functions**

On client workstations, the Forefront client icon sits on the taskbar of the user’s desktop. User Desktop and Laptop policies are configured in such a way that the user is unable to make any modifications to the Forefront client. Policies for servers allow for administrative intervention. This is so administrators can tweak any settings they may need to change from the servers themselves, rather than needing to log in to the CM console and change an entire policy.

Figure 21 shows what a user sees when she or he opens the Forefront graphical user interface.
Shepherd Color also used Symantec’s Exchange mailbox scanner. This was removed in favor of Microsoft’s Forefront for Exchange. Forefront for Exchange allows administrators to create filtering rules on outgoing and incoming mail. This is a line of defense to stop malware from entering the network via e-mail. Administrators are able to configure what types of file extensions are blocked in email attachments, and what happens with those blocked attachments once they have been found. Scanning every single e-mail as it arrives mitigates the need to have the Exchange mailboxes scanned themselves on a regular basis.
Figure 22: Configuration Manager Forefront For Exchange Client Interface

5.6 Virtual Machine Manager: Centralized VM management

Virtual Machine Manager is similar to the Configuration Manager console, only specifically for Virtual Machines. Virtual Machine manager provides interactive health and resource monitoring as well as advanced logging of events. Figure X shows some of the reporting features available in Virtual Machine Manager. Reports can be run against either the individual VMs themselves, or the virtual hosts in which they run on.
Both VMware and Microsoft HyperV hosts are present in the Virtual Machine Manager interface. Figure X shows the six Microsoft HyperV hosts and the two VMware hosts. The VMWare hosts show up as IP addresses because they are running on ESX servers which are not included in Active Directory. From the dashboard shown in the figure below, several tasks can be executed. Some of these tasks include:

- Creating a new VM: This task will create a new Virtual Machine on one of the Microsoft HyperV virtual hosts. The VM is created from a template stored in the Library. Templates are pre-configured images which provide all of the basic elements of the Operating System.
- Adding Virtual Hosts to Virtual Machine Manager (VMware or HyperV)
- Converting a Physical Server (P2V): See section 5.8
Figure 24: Virtual Machine Manager Active Virtual Hosts

Figure X shows an overview of each virtual server being managed by Virtual Machine Manager. From this window, servers can be live migrated between virtual hosts. Full stats and log reports of VM health can also be ascertained from this location.
Figure 25: Virtual Machine Manager Virtual Servers

5.7 Virtual Machine Manager: P2V Functionality

Figure 26 shows the Virtual Machine Manager P2V wizard which is responsible for the process of converting physical servers into virtual machines. The eventual shutdown of physical servers is responsible for a great deal of the annual cost savings made possible by the implementation of this project (5). Alternately, the V2V wizard also functions in a similar fashion, allowing administrators to migrate VMWare VMs to their existing HyperV hosts.
6. Testing

Microsoft recommends that System Center deployments be created in a prototype environment which emulates the actual production network in which they are to be deployed. Due to the network configuration at The Shepherd Color Company, this scenario was not possible to implement. The current prototype environment, which was recommended by an outside consultant, is set up in such a fashion in which it can be present on the production network without causing interruption.

A Windows 2008R2 sever was set up on one of Shepherd Color’s virtual host servers to host the System Center installation. Configuration Manager was the first System Center
installation installed. Prior to installation, a week was spent configuring needed prerequisite server roles such as IIS (Internet Information Services) and WebDAV. Shepherd Color’s Active Directory schema also had to be updated with a special script included with Configuration Manager. This script had to be run from the primary forest domain controller. Once the Pre-requisites were installed and configured, Configuration Manager was installed to ShCo-CM1.

After installation, various Configuration Manager services were turned on and configured before the testing environment was to be configured. Special boundaries had to be set to prevent Configuration Manager from detecting clients on the domain outside of Shepherd Color (The Shepherd family of companies have several locations all on the same domain). Once these boundaries were set, special LDAP queries had to be created to populate discovered clients into their respective test collections. (10)

Test collections were created to provide centralized locations to segregate newly added clients from the production clients. These collections were created to test both servers and workstations, as each group had to be configured differently. Specific ports had to be opened on client firewalls before the Configuration Manager client could be rolled out. This was done via group policy which was applied to the computers added to the test collections.

Once the System Center client was installed and functioning, the Forefront client could then be pushed through software distribution. The Forefront client was configured to automatically uninstall the existing Symantec Antivirus client. Before the Forefront client could actually be deployed however, special anti-virus policies had to be created for each server group already existing in the Symantec Endpoint Protection console. Each policy had to be copied and modified to fit the policy parameters required in Forefront. Once the policies were created, they
were assigned to the specific test collections, and the Forefront client was deployed via software push. (2)

Software updates were tested in a similar manner as the Forefront Deployment. Test collections were created containing a spectrum of various clients and servers. The collection was created to represent most of the systems across the network, so updates could be tested before they are pushed network wide. This special testing collection will remain for years to come as the default collection in which new updates are targeted to.

There was no testing done for Virtual Machine Manager. A period of two weeks was spent researching the best practice for implementation, and then that practice was followed. Virtual Machine Manager was installed during a network down, due to the potential of a service interruption. Once the Virtual hosts were added to Virtual Machine Manager, no farther configuration was required.

7. Conclusions and Recommendations

7.1 Conclusion

The implementation of System Center at The Shepherd Color Company has significantly impacted the IT infrastructure in several positive ways. With the remote administration tools available in Configuration Manager, administrators are now able to provide a superior level of end user technical support. Configuration Manager now also provides administrators with a centralized point to manage all servers and workstations across the network.

Forefront Endpoint Protection and Forefront Protection for Exchange have replaced the aging and expensive Symantec clients network wide. Forefront Endpoint Protection can be centrally administered through the Configuration Manager Console, providing administrators an
in-depth view of any malware activity that may be occurring on the network. Forefront for Exchange provides real-time Exchange mailbox scanning to prevent malware from entering the network via E-Mail.

Virtual Machine Manager has completely changed the way administrators manage Virtual Machines at The Shepherd Color Company. Administrators can now manage Microsoft HyperV and VMWare Virtual Hosts from one location. The functionality is now available to convert physical servers into Virtual machines via Virtual Machine Manager. This ability will allow administrators to shut down physical servers running on aging hardware, thus saving a significant sum of money on energy and cooling costs. Furthermore, The VMWare Virtual Hosts can be migrated to Microsoft HyperV hosts, allowing Shepherd Color to cancel their annual licensing agreement with VMWare.

In the end, the bottom line in running a business comes down to money. The more money a project can save or make for a business the more valuable it becomes. The roll out of this project has saved Shepherd Color over $17,000 in implementation costs, with an additional $10,000 in re-occurring annual savings. Furthermore, the energy savings numerated from reducing the number of servers in Shepherd Color’s datacenter cannot be ignored. Perhaps the biggest benefactors of this project are the end users at Shepherd Color. Administrators can now spend less time managing servers, and more time developing new ways to make end users more productive.

7.2 Recommendations

Since Shepherd Color owns the licenses for the remaining System Center Products, it would be in their best interest to pursue implementing some other technologies included in the
System Center Enterprise suite. The following list contains three products which would be immediately beneficial to the network at Shepherd Color:

- **System Center Data Protection Manager**: Data Protection Manager is Microsoft’s solution to managing server and workstation backups. Currently, Shepherd Color uses Symantec’s Backup Exec software. Since backup Exec is the last piece of Symantec software to be removed from the network, it would be beneficial to pursue its removal in favor of a Microsoft solution.

- **System Center Operations Manager**: Operations Manager integrates with other System Center products already running on Shepherd Color’s network. Operations Manager provides advanced logging and reporting capabilities for many different services running on the network. It also aids in administrative task automation.

- **System Center Service Manager**: Service Manager is an advanced helpdesk and asset management program. It could be used to replace Shepherd Color’s ancient custom helpdesk program. Service Manager has the ability to tie into other System Center products and automatically resolve helpdesks based on a library of previous resolutions.

8. **References**


9. Appendices

9.1 Appendix A: Documentation on Completing Tasks

Software Update Procedure

Go to Computer Management | Software Updates | Update Repository

- Several Subgroups are present displaying updates for each Microsoft technology. Select the desired updates, right-click and select Deploy.
- Under Deployment Template, Select the Use an existing template radio box and select the Deploy Win Updates template.
- Under Deployment Package, select the Select deployment package radio box and click Browse. Select the Push Win Updates package.
- Under Schedule, specify when the updates are to be deployed and whether or not they are to be forcibly installed.

Adding Clients to CM

Clients must first be discovered by CM before they can have the Configuration Manager client Agent installed. This is done through the use of a LDAP Query.

Note: Step 1 is NOT necessary if Client already appears in “All Systems” Collection.

1. Go to Site Settings | Discovery Methods | Active Directory System Discovery
   - Add new LDAP query:
     On the Polling tab, select “Run full discovery ASAP”
     Enable Delta Discovery

Once Clients have been discovered by CM, they must be moved to a collection for administrative tasks. Collections are similar to Active Directory OUs, as they are containers where specific policies can be applied.
2. Go to Computer Management | Collections | [Desired Collection] right-click and select “add resources”.
   - Select clients to be added to collection.
     - NOTE: The two base collections are “WSUS Updates” and “NO WSUS UPDATES” each collection has custom policies applied pertaining to Windows Updates.
   - From the Actions Pane on the right, select refresh collection membership.
3. Add Client to desired Forefront collection.
4. Deploy Configuration Manager Client:
5. Navigate to Computer Management | Collections | [Desired Collection] right-click the desired system and select “Install Client”.
   - A wizard will appear prompting for parameters in which the client is to be deployed, accept the defaults.
   - NOTE: It is possible that a restart may be required after client installation.
   - The Forefront Endpoint Protection Client will be installed automatically
   - It may take as long as 30 minutes for the systems to show up in Configuration Manager as installed and approved. To expedite this process, manually log on to the client and force a sync:
     - Go to: Control Panel | Configuration Manager (32 bit)
     - On the Actions tab, initiate the list of Actions by selecting each action and pressing the “Initiate Action” button. Technically, only the bottom five actions are required in Shepherd Color’s environment.

**Deploying Operating Systems Via CM**

Operating Systems can now be pushed out via Configuration Manager. The process below describes how to discover clients by MAC address, and push a pre-configured image to the client via PXE.

Note: A write up on how to set up and configure OS Deployment can be found at:

The steps in the above article have already been performed.