Deploying a new computer management environment for Masaryk University

MASTER’S THESIS

Bc. Jan Grundmann

Brno, spring 2018
Declaration

Hereby I declare, that this paper is my original authorial work, which I have worked out on my own. All sources, references, and literature used or excerpted during the elaboration of this work are properly cited and listed in complete reference to the due source.

Bc. Jan Grundmann

Advisor: Mgr. Kamil Malinka, Ph.D.
Acknowledgment

I would like to thank my work advisor, Mgr. Kamil Malinka, Ph.D., for his patience and professional advisement. I would also like to thank all my colleagues who participated in this project. Lastly and most of all, I would like to thank my parents for their support during my whole studies.
Abstract

This thesis aims to deploy a new computer management environment at Masaryk University. The new environment will be based on System Center Configuration Manager. This thesis describes how the deployment was prepared, how the environment is configured and what the ways of joining or migrating into the new environment are.
Keywords

Institute of Computer Science, System Center Configuration Manager, Central Management Service, Active Directory, Microsoft PowerShell, Operating system deployment, Application management, Windows Update, Role-based administration, Endpoint Protection
# Table of contents

1  Introduction .................................................................................................................. 1
    1.1 Content of chapters................................................................................................. 1

2  Motivation ....................................................................................................................... 3
    2.1 Problem definition.................................................................................................... 3

3  Old CMS environment .................................................................................................. 6
    3.1 Central Management Service .................................................................................. 6
    3.2 CMS subservices and technologies ......................................................................... 8

4  Software choice ............................................................................................................. 12

5  System Center Configuration Manager ...................................................................... 14
    5.1 Application management ....................................................................................... 14
    5.2 SCCM client ............................................................................................................ 15
    5.3 Internet-based client management ......................................................................... 16
    5.4 Software updates ................................................................................................... 16
    5.5 Operating system deployment ................................................................................. 16
    5.6 Role-based administration ...................................................................................... 17

6  New CMS environment ............................................................................................... 18
    6.1 Integration of SCCM into CMS ............................................................................. 18
    6.2 Reused subservices ................................................................................................ 20

7  Installing the SCCM .................................................................................................... 21
    7.1 Designing the SCCM environment ......................................................................... 21
    7.2 Installation of SCCM .............................................................................................. 22

8  Configuration of SCCM .............................................................................................. 23
    8.1 Client Settings ....................................................................................................... 23
    8.2 Software updates ................................................................................................... 27
    8.3 Delegation model ................................................................................................... 28
1 Introduction

Institute of Computer Science [1] (ICS) besides research and development activities also ensures operation and development of ICT at Masaryk University (MUNI). For operations regarding desktop management, the Central Management Service [2] (CMS) has been designed and was formalized in Matěj Antol’s master’s thesis [3]. However, the CMS became outdated over the years. We as ICS administrators were not satisfied with how much workload operation of CMS takes, the more so seeing issues CMS has despite our best effort. CMS in its current form got to the point where it either must have been reworked or discontinued. We took this opportunity and prepared a concept of a new CMS built on the System Center Configuration Manager (SCCM). At this point, the scope of this thesis starts as it focuses on the deployment of such concept.

This thesis has multiple chapters but can be divided into three main parts; the first part is dedicated to the presentation of the current environment sometimes referred as an old CMS (chapters 2 and 3). The second part is about SCCM software itself, its technologies, how it was integrated, installed and configured (chapter 4-8) and the last part describes how the migration will be handled and how it is communicated with IT departments (chapters 9 and 10).

1.1 Content of chapters

The second chapter presents motivation that led us into making changes in central management. It also defines the issues that current central management had which we wanted to address and resolve.

In the third chapter which is devoted to a description of the current environment the Central Management Service (CMS) is presented. There are also described technologies and subservices which CMS uses.

The fourth chapter gives a brief explanation of how and why SCCM was chosen. This selection was not the aim of the thesis but is worth the mentioning.
Chapter five presents technologies in new CMS, primarily SCCM itself and its components and features.

Chapter six explains how the new CMS is compositied, what features it has, what subservices got reused and what is new.

In chapter seven, the design of SCCM’s infrastructure and installation process of SCCM in cooperation with Microsoft’s Premier Support is described.

Chapter eight covers all aspects of configuration that were done to prepare the new environment for computer management. The first part introduces the key features of SCCM and their respective configurations whereas in the second part of the chapter the configuration of different computer modes is outlined.

Chapter nine offers an overview of migration processes that were developed to serve as guidelines for IT administrators wanting to use new CMS.

In the tenth chapter is described how the cooperation and collaboration between IT departments of MUNI on the project went and what did we achieve through it.

Chapter eleven concludes this thesis and summarizes what was accomplished, what was not and what should come in the future of CMS.
2 Motivation

Computer management plays a significant role in organization’s IT. Thus, it is essential to do it efficiently. Masaryk University has over 5000 desktop computers connected to the network, but only 2840 [4] of these computers are managed through CMS provided by ICS. Rest of them is managed by various desktop management solutions depending on what each IT department uses. Not counting nearly 3000 notebooks that have no centralized management available, so they are managed manually one at a time. This fragmentation goes directly against efficiency and flexibility of operations. For example, switching to more advantageous software on university level would be complicated and costly because there is no universal software deployment tool set up right now and a considerable part of deployment would be manual. So, the goal is to unify the approach to computer management across MUNI with one ultimate solution used by all IT departments. Furthermore, the unified solution will create an environment for tighter collaboration between IT departments and enable sharing of resources between them.

Also, Central Management Service is outdated and has a negative performance impact on computers. The following section defines problems which the new solution must solve.

2.1 Problem definition

The most significant issue of existing Central Management Service (CMS) is a severe impact on computer’s performance; mainly startup time which is caused by Group Policy [5] startup scripts (GPSS) written in PowerShell [6] (PS) and Command prompt [7] (CMD). GPSS handle both software deployment and OS configuration. These scripts run sequentially every time computer starts up, so the more software computer has, the longer it takes to run these scripts, and thus startup takes longer. The startup time of study room computer at University Computer Centre (UCC) which is in CMS is around 5 minutes, non-CMS computer with identical hardware in a study
room starts up under 2 minutes. The 3-minute difference can be ascribed solely to GPSS.

Another downside of software deployment through GPSS is poor management of application lifecycle in the meaning of the process of installing, updating and uninstalling an application. The user has no possibility of choosing and installing the application on his own and must ask an administrator. The application is installed at next computer startup coming after the administrator links/enables Group Policy Object (GPO) for a specific computer. The whole logic of checking whether the installation was successful (and disabling installation at next startup) or not (and ensuring another installation attempt at next startup) is done in script. The administrator has no feedback on the result of deployment; he must either believe in faultlessness of script or ask the user for confirmation of successful deployment. Also, uninstallation of the application must be done similarly by the administrator; the user cannot do anything.

From the administrator’s point of view, creating a new application or updating an existent one in CMS requires extensive knowledge of CMD or PS and is time-consuming. Reduction of the workload in this process is needed for example by using solution providing an updated source of application packages.

CMS relies on computer’s membership in Active Directory; our ultimate goal for CMS is the management of every computer at Masaryk University. Thus, we need a solution which can also manage non-domain computers, non-Windows OSes and notebooks taken out of MUNI network.

Because of historical issues with configuring Windows 10 Upgrades using Windows Software Update Services [8] (WSUS), upgrades are disabled. Majority of CMS workstations has Windows 10 Pro with version 1607 which servicing ended on April 10, 2018; this problem also needs to be addressed in the new solution.

Open PC Server Integration [9] (OPSI) used for operating system deployment (OSD) is used under a free license which means we cannot install computers with UEFI boot system, because this feature is available only through OPSI co-founding program. UEFI is necessary for using Windows 10’s advanced
security feature Secure Boot. In combination with GPT partitioning UEFI also reduces boot time, supports disk larger than 2TB and allows up to 128 partitions on the drive. Also, the feature of capturing the running OS and turning it into image available for installation is missing in the free license; this feature would be valuable for classroom mode which is described later in section 3.1.1.

To summarize the requirements for new CMS arising from issues mentioned above:

- manage application lifecycle
- get rid of startup scripts
- allow users to install available applications
- an efficient approach to the creation of application’s installation and update processes
- management of non-domain computers (possibly also non-Windows)
- management of clients on the Internet (typically notebooks)
- reliable Windows Update management
- UEFI and GPT support in OSD
- capture and install an OS image
3 Old CMS environment

The previous chapter identified issues in CMS, in this chapter CMS itself is described. This description gives insight into old CMS’s structure, what computers is it for, what features are there and what subservices are behind CMS. The insight is necessary for understanding the changes CMS have undergone.

3.1 Central Management Service

CMS is a service provided by ICS for management of workstations. Localities included in the CMS provide users with integrity and uniformity of working environment based on Microsoft Windows OS and a standardized set of installed software.

Figure 3.1 Diagram of the old Central Management Service
3.1.1 CMS computer modes

As shown in Figure 3.1 there are three modes of workstation use:

- Study rooms
- Classrooms
- Employee

Study rooms are computer rooms available to students anytime within opening hours; this means that there are no lectures taking place in these rooms. Computers are equipped with basic software including internet browsers, office suits and a defined set of software related to various subjects of study. The desktop environment is unified with classrooms and provides roaming user profiles, local and network storage and access to printing solution.

Classrooms are computer rooms dedicated to lectures. These lectures are scheduled, and in the free time, some classrooms are opened for students, so they can access licensed software installed only in these classrooms. The technical specification is like in study rooms, only having this limited license software on top of it.

The configuration of employee’s computer is somewhat similar to study room’s. It also has a basic set of software, and in addition to it, there is software associated with specifics of work assignment. Each employee has its workplace with workstation, so they have user profiles stored only locally. Employees have access to network storage used as a backup and for remote access to files. There is also printing solution available.
3.2 CMS subservices and technologies

These are the subservices and technologies used in CMS:

- Active Directory
- DHCP
- OPSI and PXE
- WSUS
- PCSM and PowerShell

3.2.1 Active Directory

Active Directory [10] (AD) is Microsoft’s directory service. Like other directory services, it stores information about network objects (e.g., users, groups, computers, printers, sites, networks and others) in a hierarchical structure.

In AD Microsoft implemented Lightweight Directory Access Protocol (LDAP) and its version of Kerberos.

ICS manages Microsoft Active Directory domain named ucn.muni.cz. UCN domain stores identities, groups, and computers. User identities are used for unified login to CMS workstations; this login consists of username in the form of UČO¹ and secondary password. The stored information can be accessed via LDAP protocol and used for authentication in other various services. CMS absolutely relies on functionalities of Active Directory UCN domain.

Group Policy (GP) is a feature which is used for management and configuration of workstations in UCN domain. GP object includes startup scripts which are used for application deployment.

As a part of CMS, centralized application maintenance for a set of most commonly used applications is provided. With two weeks period, we check for application updates and update our application installation packages accordingly.

¹ UČO is a unique identification number of MUNI students and staff
3.2.2 Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol [11] (DHCP) is TCP/IP protocol for dynamic assigning of network configuration (most notably IP address) to network devices. DHCP is client-server protocol in which server holds configuration settings, and at the end of DHCP session, the client is configured according to these settings.

Workstations are connected through ethernet to MUNI network, and each PC has DHCP reservation created which prevents unknown devices from accessing the network. For domain computers, there is also DNS suffix specified which is used in the process of computer joining AD domain.

DHCP server also allows setting DHCP options which are optional data that configure TCP/IP on a client. For PXE boot we configure option 66: *TFTP server name* and option 67: *Bootfile name*.

3.2.3 Preboot execution environment

Preboot execution environment [12] (PXE) is a client-server environment that boots software from a network source. The client computer must have enabled PXE boot in BIOS or UEFI and set network interface controller first in the boot order. The computer finds PXE/TFTP server which is done either using defined DHCP options (66 and 67) or via IP helper address on network infrastructure that points at PXE/TFTP server. PXE boot from OPSI is the only way how an administrator can initiate OSD in CMS.

3.2.4 Open PC Server Integration

Open PC Server Integration (OPSI) is an open source client management system. The OPSI server serves as a TFTP server for PXE boot. For the unattended installation computer boots Linux-based operating system via PXE which performs hardware inventory, disc formatting and partitioning, downloading the image. In the end, it deletes itself and initiates installation of Windows OS.

We are using OPSI only for unattended OSD, other features as application deployment are not used because of insufficient granularity of access rights.
In CMS a multi-language Windows OS installation is performed where the installed OS has both English and Czech language available, and the user can choose which one uses. This feature requires offline servicing [13] of the installation image which although that is scripted is time-consuming. Since Microsoft rolls out Windows 10 version every half a year, the offline servicing becomes rather aggravating method of customizing OS installation.

3.2.5 Windows Server Update Services

Windows Server Update Services (WSUS) is a role in Microsoft’s Windows Server. It enables administrators to manage the deployment of software updates. It is mandatory to have at least one WSUS server that can connect to Microsoft Update to synchronize update information. Client settings are configured in GPO which sets WSUS server and automatic updates properties as update check period, installation time and restart policy.

ICS operates two independent Windows Server 2012R2 servers with WSUS role installed. Both are synchronized directly with Microsoft Update and using Windows Internal Database as storage. WSUS.ucn.muni.cz is an upstream server which means it also serves as update source (update files are stored locally), WSUS2.ucn.muni.cz downloads only update metadata and its clients download updates directly from Microsoft Update.

3.2.6 PC State Manager

PC State Manager [14] (PCSM) is an application made by Mgr. Martin Čuchran as bachelor’s thesis. This PowerShell [6] application manages states of computer and allows performing changes between these states. PCSM uses data from the AD, DHCP, and OPSI. The main feature is Wake-on-LAN, which turns the computer on using magic packet sent to powered on network interface card (NIC). PCSM also remotely restarts and turns off computers. All these operations can be planned as one time or repeating events. PCSM is used for turning on study rooms PCs in the morning and off in the evening, it also manages Wednesday night update window in which it turns all computers on, so they can install updates, restarts them to apply updates and turns them off.
3.2.7 **PowerShell**

PowerShell is a task automation and configuration management framework. Formerly it was an abbreviation of Windows PowerShell, which consists of a command-line shell and scripting language built on .NET Framework. Nowadays it also implies PowerShell Core which is open-source and cross-platform equivalent of Windows PowerShell built on .NET Core.

PowerShell provides access to COM\(^2\) and WMI\(^3\), enabling administrators to perform administrative tasks on both local and remote Windows systems as well as WS-Management and CIM\(^4\) enabling management of remote Linux systems and network devices.

PowerShell is not a feature of CMS rather technology necessary for providing those features. It is used in GPSS, PCSM and daily tasks administrators perform.

---

\(^2\) Component Object Model  
\(^3\) Windows Management Instrumentation  
\(^4\) Common Information Model
4 Software choice

This thesis does not aim to find the best solution for computer management, but to describe how the one chosen is prepared, configured, put into operation and migrated into. This chapter outlines what the selection process of such solution was. The result of this process was taken as input in this thesis.

Initially, we were searching for software that would solve the issues with computer startup performance, application lifecycle, and deployment creation process as were mentioned in section 2.1. The result of such search were two software solutions: PDQ [15] and Chocolatey [16]. PDQ consists of two independent programs. PDQ Deploy which is a software deployment tool and PDQ Inventory that gathers data about software, hardware, and configuration from workstations. Using trial license PDQ features were thoroughly tested.

At the same time, the usefulness of Chocolatey, which is package management solution for Windows platform (like apt-get or yum is for Linux), was also tested.

In the feature comparison between both products PDQ came out as better, but the licensing policy where every single admin accessing PDQ console had to have its license in combination with our intention to give access to admins from all IT departments was unacceptable. The price was too high. On the other hand, Chocolatey was free to use but lacked any central management features, and the enterprise edition that would have them was still in a development phase.

The requirements were reconsidered, and solutions which do not offer a source of pre-created application packages but still solve our main issues in computer startup performance and application lifecycle were included. The System Center Configuration Manager [17] (SCCM) meets these requirements but since the beginning of CMS there was a discussion about using SCCM, and it was always ruled out as too expensive. Matěj Antol was in his master’s thesis [3] searching for unattended OSD solution, but OPSI with free licensing turned out being a better choice than SCCM. Martin Čuchran mentions SCCM as a possible solution in his bachelor thesis [14] where he was looking for a
solution that manages states of workstations and in this case SCCM was expensive too. However, they were both looking only for specific features that SCCM provides, so it was concluded overpriced as it also provides other features that were not valuable at the time. This time it would be the same counting SCCM as a solution only for application management, but knowing other features in SCCM, all issues in CMS were defined (as are in section 2.1) and SCCM was evaluated whether it could solve them or not. The outcome was that SCCM provides means to resolve all the issues we had and also provides features we would be happy to introduce in CMS.
5 System Center Configuration Manager

In the previous chapter, the software was chosen its features and functionalities are described in this chapter. System Center Configuration Manager (SCCM, ConfigMgr), previously known as Systems Management Server is a system for management of computers in large environments no matter their operating system. It provides tools for OSD, software distribution, patch management, settings management, hardware and software inventory, remote control and malware protection. Everything is accessible within a single console. SCCM is deployed on Windows Server infrastructure.

The key parts of SCCM that are described here and will be used in CMS are:

- Operating system deployment
- Software updates
- SCCM client
- Application management
- Role-based administration

5.1 Application management

Application in SCCM is an object which holds a description of an application together with an application deployment type which is the actual definition of installation properties like what the installation files are, how are they executed, what is the indication of correct installation, what requirements computer has to meet.

The process of creating an application is fully automated when an application uses Windows Installer [18]. The administrator only has to specify network share path where installation files are located, and SCCM itself reads application description and installations properties from installation file (package), and application is ready for deployment.

Unfortunately, not every application uses Windows Installer, in fact, the minority does. Majority of applications are just executable files that either install themselves or initiate the start of Windows Installer. Executable files
are typically used because Windows Installer framework has specific rules for managing installation, upgrade and uninstallation of product, which are inadequate for an application creator to have their application installed correctly. For these applications, the administrator has to manually specify everything that application object contains in an application creation wizard. When creating an application, there are two key components in its deployment type: installation command and detection method. If the application uses Windows Installer, both these components are filled automatically, but otherwise, the administrator must define them. Installation command tells what the installation file is and how it should be executed, there is also an option to run a script as an installation command. SCCM uses detection method to check whether the application is present or not. There are multiple options how detection rule can be composed, using file check, registry check, MSI code\(^5\) check or run a custom script. All these methods can be combined into complex detection rules.

### 5.2 SCCM client

SCCM client is a program that is installed on the device and communicates with the server. It also handles all operations that are performed on the client computer.

There are multiple ways of a client deployment. It can be installed during OSD, or using Group Policy Software installation, or using WSUS, or by client push using SMB over IP at port 445 and administrative share (Windows OS feature), or by the interactive manual installation.

Basic interactions and settings of SCCM client are managed with the Client settings. Each site has “Default Client Settings” which are automatically applied to all clients of this site and have lowest possible priority. The administrator can define his “Custom Clients Settings” which are deployed to either device or user collection. Priorities serve for merging multiple client settings when the same setting is set differently the one with highest priority wins.

\(^5\) Windows Installer package-specific GUID
5.3 **Internet-based client management**

The Internet-based client management [19] (IBCM) feature relies on a server to which clients connect from the Internet. This feature requires PKI\(^6\) and does not support all functionalities of SCCM. When a client is on the Internet the client push installation and software update-based installation do not work, the OSD does not work, and the remote control does not work. The clients can be configured for internet only client management if they never connect to the intranet, but more there is also the possibility to configure them as Internet and intranet client management where client switches servers based on the type of the network. Non-domain computers must be Internet-only.

5.4 **Software updates**

Software updates is a name for a feature that serves for managing Windows updates using SCCM’s Software Update Point which is, in fact, a WSUS role integrated into SCCM. SUP properties are defined at SCCM site level. These properties specify what and when SUP synchronizes with Windows Update (sometimes referred to as Microsoft Update).

The deployment of updates to computers is controlled with Automatic Deployment Rule (ADR). ADR defines filters by which updates are chosen for deployment, a period of its run and specifies deployment settings. The result of each ADR’s run is a Software Update Group (SUG) which contains all updates that match the filter. This SUG is deployed to a collection that is defined in ADR.

5.5 **Operating system deployment**

OSD is in SCCM managed through Task Sequence (TS), which is a receipt (set of steps) that are sequentially performed and where at the start, there is either a bare metal computer or a computer with old OS, and in the end, the computer has a freshly installed OS running. The steps inside TS are usually: disk partitioning, downloading and applying OS image, network

---

\(^6\) Public Key Infrastructure
configuration, driver management, OS configuration, SCCM client and other SW installation performed typically but not necessarily in this order. There is also a possibility to run custom CMD or PS script. Each step can have conditions which are dynamically evaluated during the run and decide whether the step will be performed or skipped.

5.6 Role-based administration


Security role groups multiple objects with their permissions to reduce the complexity of permission management. The role itself then represents a typical task that would be performed inside SCCM console. SCCM includes set predefined roles to cover basic management operations.

Collections are groups of resources that consist of computers, users, and user groups. Most management task performed in SCCM rely on or require using a collection as a target. SCCM includes several collections by default which cannot be modified. For computers these are: All Systems which is the ultimate collection that contains all device resources in SCCM; All Unknown Computers is collection with generic computer records for x86 and x64 computer platforms, can be used for deploying an OS by using task sequence and PXE boot; All Desktop and Server Clients contains desktop and server devices having SCCM client installed. On top of this administrator can create custom collections with his own membership rules.

Security scopes encompass securable objects as applications, packages, task sequences, boot images, OS images, SUGs, SCCM sites and distribution points. SCCM has two built-in scopes Default and All which contains default and every custom created scope.

Combinations of the security role, security scope and collection define the administrative scope for each administrator, this combination is assigned to SCCM user who is either local or domain user or group.
6 New CMS environment

Chapter 4 talks about choosing a suitable software which meets our requirements to be integrated into CMS and chapter 5 presents SCCM with its features. This chapter describes how the new CMS service will be composited and how the integration of SCCM into CMS is designed.

6.1 Integration of SCCM into CMS

At the end of chapter 4 the verification of SCCM meeting our requirements is mentioned but the selection process described there did not deal with the question of integrating SCCM into CMS. The integration was driven by implementing the requirements summarized at the end of chapter 2.1 and is explained in the following sections.

6.1.1 Application management

The requirements for application lifecycle management, getting rid of startup scripts and users installing available applications could be all answered using Application management feature in SCCM, so this feature is planned to be implemented allowing to drop application management from AD Group Policy completely.

As already mentioned in chapter 4 the requirement for a source of pre-created packages for applications that would only need to be deployed was dropped, but the requirement for efficient approach to the processes of creating application’s installation and update can be still fulfilled in Application management as it offers automated process for creation of Windows Installer applications.

6.1.2 SCCM client

The management of non-domain computers is possible thanks to SCCM client which is essential for every computer being managed in SCCM. After the client is installed and Windows Firewall rule allowing connection with SCCM server added on the local computer, all features of SCCM are available. For
non-Windows OSes, the client installation is possible on Mac OS and mainstream Linux distributions [21]. Not every feature of SCCM will be available to these OSes for example updates from SUP are just for OS Windows but exact list of available features is not prepared yet because support for non-Windows OSes is planned to be introduced into CMS after all computers are migrated from the old CMS.

6.1.3 Internet-based client management
The requirement for management of computers taken out from the MUNI network to the Internet is solved by using the IBCM feature. These computers are mostly notebooks which users take home or on business and sometimes also connect them into MUNI network, so the clients would preferably be in Internet and intranet client management mode, but these notebooks are not typically joined in the AD, so the Internet-only client management is a must.

6.1.4 Software updates
Reliable management of Windows Update together with receiving upgrades for Windows 10 is available through Software updates feature of SCCM, this feature must be implemented and will replace the WSUS subservice of the old CMS.

6.1.5 Operating system deployment
The last two requirements for UEFI and GPT support and OS image capture and install can be fulfilled in OSD feature. SCCM server allows OSD through PXE boot, so everything we were doing with OPSI is possible to achieve in SCCM too, so we can stop using OPSI in the new CMS.

6.1.6 Role-based administration
Role-based administration enables having a single instance of SCCM for all IT departments of MUNI without worries about administrator accessing a computer that does not belong to his administrative scope.
6.2 Reused subservices

Subservices that will be used in the new CMS and were already present in the old one are:

- PCSM with PowerShell
- Active Directory
- DHCP

PCSM will be still managing states of AD computers, it used OPSI database for accessing MAC addresses, but these addresses are available in DHCP too. Active Directory will also be part of the new CMS as it stores identities used for logging into computers in AD domain modes and configuration in Group Policy makes certain tasks in SCCM more seamless as they would be without it, for example, SCCM client installation and Windows Firewall rules for SCCM server.

DHCP gets reused because it is necessary for PCSM and PXE boot-based installation.

Figure 6.1 depicts the new Central Management Service in full composition.

![Diagram of the new Central Management Service](image)
7 Installing the SCCM

In the previous chapter, the composition of the new CMS is drafted together with defining which the key features are and what requirement do they fulfill. In this chapter, this is turned into the installation of an SCCM on-premise instance.

7.1 Designing the SCCM environment

Since for everyone on our team, this was the first experience with SCCM deployment we reached out to Microsoft for help with designing the SCCM environment. Thanks to ICS having Microsoft’s Premium Support\textsuperscript{7} service consultation with Microsoft’s technician Mr. Robert Novák took place where we presented our requests for functionalities and specifications of our current environment, and he suggested the appropriate SCCM hierarchy for our case. He proposed keeping it simple, having a single site called “MU1” with only one server being used for managing intranet clients and one server for internet clients. There is also a single MSSQL\textsuperscript{8} database server for SCCM.

Then the network segment was selected. For all three servers, we used segment designed for university-wide services with firewall rules allowing incoming communication from 147.251.0.0/16\textsuperscript{9} and allowing outgoing communication everywhere. The intranet server sccm-01.ucn.muni.cz has no custom rules applied, but the internet one sccm-ibcm-01.ucn.muni.cz has custom rule adding an allowance of an incoming communication from outside of university network at TCP port 443.

\textsuperscript{7} Paid support service providing access to various resources that are not publicly available
\textsuperscript{8} Microsoft SQL Server
\textsuperscript{9} Public network subnet of Masaryk University
7.2 Installation of SCCM

Also, as a part of Premium Support, we were able to get Mr. Novák on site to do the actual installation process with us as we wanted to avoid learner’s mistakes that could have come if we would have done it on our own.

Our task was to prepare everything beforehand, so technician only needed to go just through SCCM installation process. The preparations included creating virtual machines, installing and configuring the operating system according to technician’s requirements and configuring network stack. All three servers are running in VMware virtualization environment provided by ICS with Windows Server 2016 installed. MSSQL Server is also in version 2016.

When the technician arrived, we spent four days installing everything that was necessary. The only issue came up with notebook management. It requires PKI, but SCCM does not perform certificate management as we expected and relies on other solution of certificate management. Because of our notebooks not being joined in Active Directory that can manage certificates, certificates would need to be manually issued and renewed. That was not foreseen from our side and would mean a substantial workload for the IBCM feature. However, it did not change anything in the setup of SCCM, so we proceeded to continue with installation procedure as planned and decided to discuss possible solutions later.

The rest went smoothly, so we had few hours at the end of the session to ask the technician in person about SCCM best practices in role-based access management, Windows Update deployment, and some other SCCM functionalities.
8  Configuration of SCCM

Chapter 7 outlines how the installation of SCCM went, and in this chapter, the steps necessary for having the new CMS fully operational are described. The initial plan of quickly releasing support for notebook management through IBCM feature was postponed until a new scalable solution would be chosen.

Next planned functionality was a study room mode support. At the same time talks began about the possibility of renewing all computers in Masaryk University study rooms via MUNI4STUDENTS project. It accelerated our effort to making study room mode work as soon as possible.

Our original thought was that we would transfer all the settings from Group Policy into SCCM, having everything at one place. However, Mr. Novák did not recommend it. We followed his advice and in SCCM only implemented settings which as he said: “made sense”. It would mean hybrid model of environment configuration where a significant part of OS configuration is still done in Group Policy which meant a significant reduction of the workload that needed to be done to have new CMS computer modes ready.

Before the mode-dependent configuration was done, following mode-independent functionalities were prepared.

8.1  Client Settings

The following section will mention and explain some of the Client Setting we configured and why.

8.1.1  Background Intelligent Transfer Service

This service allows throttling network bandwidth used for SCCM during defined throttling windows. Because the majority of clients have 1Gbps and the rest have at least 100Mbps network we have this feature disabled.
8.1.2  **Client Cache**

This setting configures the maximum size of SCCM client cache on a local drive. The default value is 5GB; we increased it to 25GB, this is crucial parameter because everything SCCM installs is firstly downloaded from Distribution Point to the local cache and then run. If the file is larger than the maximum size of the cache, the deployment will fail, if there is not enough free space in the cache, the client will delete other cached files to make a space for download.

There is also the possibility to enable BranchCache which allows sharing local cache between the computer in the subnet. This feature is disabled because we do not need to reduce load and save network bandwidth of Distribution Point.\(^{10}\)

8.1.3  **Client Policy**

There is a client policy polling interval set to 30 minutes, with this period the client checks for changes that server or administrator created. This is how client gets information about the new application, update or OSD.

8.1.4  **Cloud Services**

Allows to cooperate with Azure cloud services; this is disabled.

8.1.5  **Compliance Settings**

Compliance settings are enabled as they allow to set a desired state of the configuration, perform periodical checks and eventually remediate noncompliant items. Compliance settings feature concept is closely related to Group Policy as it delivers and ensures specific configuration on the client but offers more possibilities than templates in Group Policy.

\(^{10}\) SCCM’s role that serves as a point from which clients download packages
8.1.6 **Computer Agent**

Specifies general setting for communication between server and client. It defines that all users have to install permissions in Software Center. Sets PowerShell script execution policy to Bypass for PowerShell scripts run by SCCM client and sets organization name in Software Center to “Masarykova univerzita”.

8.1.7 **Computer Restart**

Manages restart behavior on client computers. Restarts are allowed only during maintenance windows, here is specified how the user is notified about the restart. We set a popup notification 90 minutes before the restart and a permanent dialog box that user cannot close at 15 minutes before restart.

8.1.8 **Endpoint Protection**

Endpoint Protection is not configured in Default Client Policy as we currently use it in pilot operation. So, it is configured in Custom Clients Policy and deployed only to selected computers. It will be discussed in section 8.9.

8.1.9 **Hardware Inventory**

Hardware inventory is a feature which collects information about client device that is stored in the registry and WMI. It is set to run once a week. Data from hardware inventory are one of the most valuable assets of SCCM client.

8.1.10 **Power Management**

We did not configure it yet. We set power settings in Group Policy and don’t need to rework them into SCCM. However, after we analyze data from hardware inventory about power management it is likely we will implement power management in SCCM to save electricity because it offers more flexibility and better manageability than Group Policy.

---

11 Application on client computer that user can install applications from
8.1.11 Remote Tools

Remote tools configure settings for remote access to SCCM client computers. We enabled both Remote Control and Remote Assistance. Both features enable connection to user’s session where the user must grant permission for connection and potential elevation from view only to full control access for the administrator. Remote Control on top of that offers the ability to connect to an unattended computer and Remote Assistance to send a request ticket to the administrator.

8.1.12 Software Deployment

Only configures re-evaluation schedule for deployments, during re-evaluation client does check all detection rules for deployed software according to latest Computer Policy. If any of it is not detected as installed, installs it back.

8.1.13 Software Inventory

Software inventory scans client computer filesystem for defined file types and names, collects them and copy to the server. This feature is turned off as Microsoft’s technician recommended because it loads the client’s computer disk and CPU and doesn’t provide any value.

8.1.14 Software Metering

Software metering collects data about applications ending in .exe. This allows monitoring use of applications. We run this feature to monitor use of licensed software to optimize licenses.

8.1.15 Software Updates

This setting specifies how client deploys software updates (Windows Update). We have configured scan period as once a week even though updates from the server only come once in two weeks when ADR runs, but sometimes we could push update manually, so we need a computer to pick it up. The installation of Express installation files for Windows 10 updates is disabled
since this caused the slow download of files and the updates would never install. There is also Office 365 Client agent management enabled which tells, that we can push updates to O365 installation through SCCM.

8.1.16 State Messaging

There is a period of state message reporting cycle defined to 15 minutes at which client sends various data in the form of state message to the server.

8.2 Software updates

In our configuration of software updates, we have chosen to synchronize Windows 10, Office 2016 and Office 365 Client products in Czech and English language.

For Windows 10 we have 3 ADRs, they all have the same filter which selects updates for Windows 10 from last 14 days, they all run with the same period 14 days, the difference is in deployment schedule. Different schedule for each ADR deployment creates rings of SUG. The first one is a testing ring, and its deployment deadline is immediate, test ring collection contains virtual machines which are used only for testing various stuff during our daily routine. The second ring is pilot which has deployment available two days and deadline seven days after ADR runs; pilot collection contains few selected workstations which are in daily use. The last ring is rollout which contains remaining computers, and the deployment has updates available ten days and deadline 14 days from ADR’s run.

The time of availability means that updates show up in Software Center and the user can initiate installation (when deployment is configured as visible to the user) and the deadline is a point in time when the installation is forced.

Both Office products updates are configured similarly to Windows 10’s but there are only two rings - test and rollout, test ring contains the same computers as a pilot ring of Windows 10. This is because on virtual machines there is no one using Office products.
8.2.1 SUP issues

WSUS thus SUP is easy to bloat with updates because of this there is WSUS cleanup wizard that periodically performs cleaning procedure during which superseded and expired updates are declined and later deleted. This WSUS cleanup wizard is included in WSUS and SUP but is not recommended to rely on. Instead, community suggests using WSUS Automated Maintenance [22] (WAM) which extends WSUS cleanup wizard features with database maintenance and logging options. WAM is PowerShell script that runs as a scheduled task every day, it performs daily routines as declining updates, cleaning WSUS synchronization logs and database maintenance. On the first of every month, it also removes declined and obsolete updates. The WAM is easy to set up and then maintenance-free, but it also backfired at us when Microsoft released Windows 10 version 1803 feature updates because at the same time the 1709 feature updates were marked as superseded and expired which meant WAM declined them, so they were not deployed in SCCM anymore. It needed to be manually repaired by un-declining 1709 and deploying them manually also the configuration of WAM was changed not to decline updates automatically but declining will be done manually when we switch to new Windows 10 version. At the same time, we also stopped using Windows 10 Servicing feature in SCCM, which until then managed feature updates deployment. It was essentially ADR for feature updates, but it did not do that much, because manual control over feature updates is more suitable.

8.3 Delegation model

As mentioned in chapter 2.1 SCCM is meant to be used university-wide which means we need to give access to it for administrators from multiple departments.

In our delegation model we are using these built-in roles: Full Administrator that grants all permission in SCCM; Read-only Analyst which grants permissions only to read objects; Operations Administrator which has permission to all actions except for the permission to manage security
settings; Remote Tools Operator that grants permissions to use various remote tools within SCCM console; Application Administrator which allows to create, modify and retire applications and to manage their deployment; Operating System Deployment Manager that grants permission to create and deploy OS images; Asset Manager which grants permissions to software and hardware inventory, software metering and asset intelligence.

The model was designed with two primary ideas. Firstly, our ICS team will have unrestricted permissions; this is done by assigning Full Administrator role with All scope and All Systems and All Users and User Groups collections to AD domain group UCN\SCCM_admins where all our accounts are. Secondly, each department must have its sphere which other departments cannot interfere with, but also must be able to use objects we offer them for use without the ability to modify. Each department has its AD domain group in which are accounts of actual administrators. This group is then tied with custom security scope and custom collection to which roles are assigned.

### 8.3.1 Example of model

Administrators from Faculty of Law which is in ucn.muni.cz AD forest, their accounts are in UCN\SCCM_law group which gives them permission to run SCCM console and what they seen in there is based on actual role, scope, and collection.

The scope is called law.ucn.muni.cz, the collection is WKS – OC – law.ucn.muni.cz and the roles are Application Administrator, Remote Tools Operator, and Operating System Deployment Manager.

The WKS – OC – law.ucn.muni.cz collection has membership rule based on AD domain name which is law.ucn.muni.cz this means that all computers in this domain are members of this collection. The security scope is automatically assigned according to the user who creates the specific object. It means every application, task sequence, etc. that is created by law-administrator has law.ucn.muni.cz security scope. When creating a custom collection law-administrator needs to specify WKS – OC – law.ucn.muni.cz directly as limiting collection or other custom collection which has WKS – OC – law.ucn.muni.cz specified as limiting collection transitively. In other words, all collections law-
administrator has permission to have WKS – OC – law.ucn.muni.cz as limiting collection directly or transitively.

8.4 Application management

The biggest issue of old CMS was application lifecycle thus configuring application management in SCCM was the primary concern. It involved redoing all applications from Group Policy into SCCM.

8.4.1 Application redo

Old CMS used Group Policy startup scripts in which application was scripted to be silently installed during computer startup. Script also included a check of application’s presence. It was done in various ways from checking the presence of file created during application installation to checking the registry for application key.

The process of redoing involves putting application installation files on SCCM’s network share and creating application object either automatically or manually depending on the type of installation files.

Since we already use scripts in Group Policy, we could’ve copied those old scripts and paste them into SCCM application installation command. However, as already said, old scripts also contained checks for application presence and generally were outdated, so we took just the installation commands from them. Typical installation command is “setup.exe /s”, where “setup.exe” is the name of file and “/s” is a silent installation option (switch).

Proper detection rules must have been created for each application. Formation of detection rule required the installation of an old version and reinstalling to a newer version of the application to determine what exactly changes and how we can determine whether the application is installed and which version of it. Windows OS has Uninstall register key [23] which stores information about installed programs. All correctly installed programs should have subkey in here, and we used it for most of our detection rules. However, we were forced to define file checks or develop a custom script for detection rule for few exceptions.
8.4.2 Application updates

When an application requires an update a new application should be created and set as superseding the previous version of the application with specifying whether the old one must be uninstalled before the new one is installed or upgrade (direct installation of the new one) is possible. We simplified the process by creating a copy of the old application object. The copy is stripped of deployments, but everything else remains which means administrator only needs to update source of installation files, detection method, and supersedence.

8.4.3 Application deployment

After the application is created, it can be deployed to a collection, and all objects in this collection will receive it and perform installation according to settings of deployment and application. So, when making centrally managed applications available to other departments, administrators need to have read permission on security scope in which applications are, and they can deploy them themselves to computers under their supervision. However, when performing application update, the new version of an application has no deployments, and they must be defined anew. This would have created excessive workload during application updates and to bypass this, a custom collection hierarchy was designed. Each centrally managed application has three corresponding collections created and is deployed only to those three. One is for testing purpose, other two for actual deployment either as a Required or Available application. Each of these two collections has membership rule set to contain department specific collection of the application and in this collection’s department administrator can edit membership. The reason why there are department specific collections is that if they would edit membership directly in application’s collection, they could edit membership of computers from other departments. For example, when law administrator wants to install VLC player as required to a computer, he only adds this computer to a collection WKS - SD - VLC - Required – law which is a member of WKS - SD - VLC – Required that has VLC
deployed. The membership of computer in subcollection gets propagated in the collection above, and the computer gets the deployment that targets the collection above.

Design with an application having corresponding deployment collections also simplifies the process of application deployment into a single step and is recommended to use for all applications that administrators will create in future even just for their department.

The drawback of this approach is a large number of collections needed. Having 30 applications centrally prepared in SCCM means 90 top-level application collections with each having 8 (currently) department subcollections. So initially this design required the creation of 720 collections which was scripted using SCCM’s PowerShell cmdlet. There is also the possibility of new departments and new centrally managed applications, for both these cases, PowerShell scripts are prepared to automate collection creation.

8.5 Study room mode

After having the client settings and software updates configured and basics of delegation model and application management set up, work on specifics for study room mode began where two functionalities were left to implement: OSD and specific applications.

8.5.1 Operating system deployment

We started with OSD. Study rooms usually have dozens of computers, so the OSD installation method needed to be zero-touch\(^\text{12}\). Task sequence (TS) if deployed as Required runs zero-touch. For study rooms the TS steps are in following order: formatting and partitioning disk as MBR with only single partition for OS; downloading and applying OS image of Windows 10 Pro in Czech language customized with unattended file specifying language options, this is used for support of switching OS languages between Czech and English; installation of CMTrace.exe which is software for better

\(^{12}\) Installation which runs without any user interaction
readability of log files; adding computer to Active Directory domain, which is chosen according to computers DNS domain suffix configuration received from DHCP; SCCM client is installed; drivers from Windows Update are downloaded and applied; .NET3.5 is installed; English language pack is installed if the OS is in the Czech language. After all these steps, the logon screen comes up, and the computer is ready for usage. Remaining mandatory applications are installed afterward, so it needs to be communicated that after installation it takes another hour until all applications are installed. We could include them as a step in TS, and we may do it in the future, but it would mean much longer OS installation time.

The support for UEFI and GPT was also implemented, the TS engine automatically recognizes whether PC boots via BIOS or UEFI and assigns a value into native TS variable, this variable is then used for conditional steps during disk partitioning.

8.5.2 Application management

After the OSD was prepared, we revised Group Policy and identified GPOs responsible for the installation of applications which needed to be migrated into SCCM’s Application management. We ended up with a set of 10 applications which were not in SCCM yet and were one by one redone in SCCM and tested. All applications are marked as Required so the user cannot manage installations in Software Center. It ensures a consistent desktop environment for all computers in study rooms.

8.6 Employee mode

After the study room mode was done, we moved to the employee mode. The first task was to find all differences employee mode has over study room. The biggest one was the usage of two partitions on a single disk at employee’s PC. One partition is used for OS and the second one has user profiles and the user data. It is used since Windows 7 for the ability to reinstall OS without loss of any user data. A similar feature of keeping user data during OS reinstallation was introduced in Windows 10, every version upgrade uses it, and it works
well. So, with Windows 10, there is no need for separate partitions for user profiles and data. However, since users and administrators are used to having a separate OS and user data partitions, we decided to try whether Windows 10 reinstallation supports this unique configuration of partitions. The tests were successful, so we decided to support both alternatives having just a single partition or having the user profile partition separate.

8.6.1 Operating system deployment

Two partition support was implemented into TS using variables. Each computer or collection can have assigned a custom variable with a value in it. These variables are available during TS, so if the computer needs to have user profile at separate partition, it must have defined variable UserProfile with value “D” together with OSPartitionSize set to size in GB. Otherwise, the single partition is created. The user profile location is via unattended file applied to OS during OSD alike language options are.

When installing a computer with two hard drives during OSD, it is recommended to only connect the one where OS partition will be, because it is impossible to know which drives gets which index. We may later introduce advanced logic into TS which will be able to decide where to put OS based on drive size and type, but this is not a priority as there are just a few computers with multiple hard drives and technicians can initialize the other drive after OS installation is done.

Other things remained same as for study room mode. So, we used the same TS for both modes with appropriate conditions on steps differentiating between study room and employee modes. Having single TS for multiple purposes simplifies its maintenance, but introduces complexity inside TS, we may switch to having separate TS for each mode in the future.

The employee OSD does not necessarily need to be zero-touch, there are no mass installations of employee’s computers. However, the support is already there from study room mode. We plan to offer an interactive installation where OSD configuration properties are filled through GUI wizard during OSD, but this feature is time-consuming to prepare, and we did not have the
time needed because we rushed to make employee mode available before April 2018 when new computers would arrive.

8.6.2 Application management

Also, in employee mode, we identified applications which needed to be redone in SCCM before the mode was complete. This included work on Office 365 Click2Run installer which is a new method of installing Office suite. We used Office 2016 MSI installer so far, but it is not up to date with the Office 365 one and installer itself is poorly manageable. The most difficult was to enable migration from Office 2016 to Office 365, but with the help of deployment tools and scripts from Office developers GitHub page [24] it works without any restart needed.

8.6.3 Upgrade possibilities

The last step before releasing employee mode was the preparation of an upgrade to Windows 10 version 1709. It was motivated by the expiration of support in April/May 2018 for Windows 10 versions currently installed in our environment. Since we knew the majority of employee’s computers would be migrated from old CMS to the new one without clean OS installation (unlike study rooms where clean OS installation would come at the latest before next semester) we needed to perform version upgrade on them. We decided to make it during the migration process so all computers in the new CMS would have Windows 10 version that is supported. The version upgrade has “Feature update” classification in Windows Update, so we created a collection which has this feature update deployed on and includes all migrated computers with OS version older than 1709 which is the one we are updating to.
8.7 Classroom mode

The classroom mode is not prepared yet. This mode is demanding for application preparation. Each classroom has its ever-changing specific set of applications which would need to be redone in SCCM and prepared before the start of the semester which was in the middle of February 2018. The next semester starts in the middle of September 2018 which leaves us time to focus on more important things that need to be done before this.

The plan for classroom mode is that each classroom has its responsible person and this person would be in charge of manual installation of specific software on a single computer which we would later clone using imaging to other computers in the classroom. The image would be kept for whole semester allowing us to reinstall OS quickly.

8.8 Notebooks

Mode for notebooks is not prepared yet too. It relies on working IBCM which has been redesigned and is undergoing tests; it solves the certificate management issue by notebooks joining AD and using the Always-on-VPN feature of Windows 10 when they are outside of MUNI network. Membership in the AD also enables the Internet and intranet client management which would not work for non-domain notebooks.

8.9 Endpoint Protection antivirus

SCCM has built-in antivirus software called Endpoint Protection (EP) based on Windows Defender [25] which is already present at Windows 10 computers. EP licensing is separate from SCCM license, and device client access licenses (CALs) [26] must be purchased. MUNI has been using ESET Endpoint Antivirus [27] for several years. With EP being integrated into SCCM and Windows 10, we decided to give it a try and evaluate features of EP to be able to compare both products. After this decision, 150 licenses were bought, and EP was set up to start with SCCM pilot at UCC (described later in section 9.1.1).
EP is enabled through custom client settings which were deployed only to the collection with UCC computers. The configuration was made to be similar to what is configured in ESET’s antivirus, but there are two interesting setting we set up. The first one is advanced membership in Cloud Protection Service [28]. This service in real time assesses files which are suspicious but not yet in rules and definitions of EP. The second one is periodic check for EP definition updates with 4 hours interval directly at Microsoft Update and Microsoft Malware Protection Center, so computers stay up to date with currently released definitions. The other way would be updating definitions using SUP, but since SUP updates once a day, the definitions would be outdated before they would arrive at the client computer.
9  Migration processes

Chapter 8 outlines how the SCCM was configured to be able to manage computers according to our demands. After the configuration, everything was prepared for the deployment of the new CMS. This chapter aims to describe what are the ways of either joining or migrating to the new CMS. Before any migration process can start every department must do a preparation works. As seen in Figure 9.1 they include creating firewall rules on network infrastructure for SCCM servers, creating new subtree in AD tree structure with linking appropriate GPO’s and creating necessary collections in SCCM. This preparation process is for localities using AD domain computer modes.

Figure 9.1 Diagram of preparation work process
9.1 Study room

As was said at the beginning of chapter 8 the project MUNI4STUDENTS motivated us to start with study room configuration. Thanks to the project hundreds of new computers will replace older hardware in study rooms. It resulted in choosing clean OS installation using SCCM as the way of study room’s migration. Also, there are no data on computers that would anyone miss so even non-replaced computers can be migrated using clean OS installation.

9.1.1 Pilot operation at UCC

Since the beginning, we planned to use UCC as a location for pilot SCCM management having February 2018 as the deadline for starting the pilot. After OSD and application deployment configurations were done during January 2018, we performed migration of UCC from old CMS to the new one. This migration involved moving computer objects in AD structure to the new organizational unit which had appropriate GPO linked. Then the reinstallation using PXE boot was performed. The whole migration took four days because of minimizing the impact on UCC continuous operation. Each day one of four rooms in UCC was closed for 3-4 hours during which we initiated and monitored OS reinstallation on-site. Migration was successful as we did not run into any significant issues. The minor ones involved 10 PCs with older hardware which had outdated NIC driver without supporting Wake-on-LAN and missing driver for EPSON scanners. Both drivers were deployed into running OS few hours after migration.

This UCC pilot served as a trial locality for new CMS operation and the migration process was for study rooms was created from experiences gained there.

9.1.2 Migration from old CMS

Majority of study rooms are replacing hardware before migration but even for those who are not the process is identical.
Typically, the new computer takes the place of the replaced one so network configuration, AD computer objects, and DNS records can be reused. However, in DHCP settings MAC addresses for reservations and options 66 and 67 must be changed accordingly. If there’s no hardware replacement just option 66 and 67 change is needed.

The next step is to move computer objects in AD tree structure and to update the AD OU in PCSM. The new AD location is configured in SCCM’s AD system discovery, so these computers are added into SCCM and placed in the collection with permissions for study room’s administrator. Then administrator imports MAC addresses into SCCM which are paired with the records discovered from the AD. Then in SCCM, he assigns these computers into the collection with TS deployed and OS installation is prepared.

OS installation starts through PXE boot (must be enabled in BIOS) and is configured as zero touch and installs SCCM client. After OS installation is done, the administrator removes computers from OS installation collection.

This process is included in more general OS installation process which is illustrated in Figure 9.2.
9.1.3 New study room

In case of adding a new study room, the migration process is longer because computers need to be added to other services of CMS like an AD, DNS, DHCP and PCSM which is performed in collaboration between study room’s administrator and our team. When this is done, the process is the same as described in the previous chapter.

9.2 Employee

With employee’s computers, the situation is different from study room PC’s. There is no massive hardware replacement coming, and PC’s have data which shouldn’t be lost thus clean OS installation does not suit well here.

Figure 9.3 Process of employee PC migration
9.2.1 Migration from old CMS

Without OS installation this migration process has a different way of deploying SCCM client to PC. It is done by client-push installation, and the goal was that employee leaves workplace with a computer in old CMS and the next day morning comes to a computer which is already managed by new CMS.

Since there is a problem with computers having unsupported Windows 10 version we decided to include Windows 10 version upgrade in migration process so there is an OS reinstallation but one that keeps user data and applications intact.

Because of upgrading OS, the process requires cooperation between administrator/technician and employee. Together they arrange that an employee leaves PC running after work, and on this day administrator/technician moves computer object in the AD to a new location and selects to install SCCM client. After the client is installed, the computer belongs to a collection which has Windows 10 upgrade assigned as required and maintenance window set from 8 PM to 5 AM. The upgrade will run only in this maintenance window. It results in computer starting to download upgrade files at 8 PM then performing upgrade which has the whole night to run. Upgrade takes from 20 minutes to few hours depending on hardware. When an administrator needs to perform migration earlier, he must add a new maintenance window that starts at his desired time and ends at 8 PM.

Apart from moving computer object in the AD, the migration process requires to prepare collection hierarchy in SCCM especially application collections so when the PC is migrated in automatically belongs to appropriate collections thus have all software managed by SCCM that it should’ve.

This process is represented by the model in Figure 9.3.
9.2.2 New PC hardware

There’s also the possibility that migration will be performed during installation of new hardware, then the migration is performed according to process model shown in Figure 9.2.

9.2.3 New locality

When adding a new employee locality to CMS, the process is like the one with a new study room. It is based on cooperation between the department’s administrators and us and depends on how much integration into CMS they want. It will follow the process illustrated in Figure 9.2 too.
10 IT departments participation

In chapter 9 were presented migration scenarios which emerged from our experiences and a discussion between our team, ICS technicians, and IT departments administrators. This chapter describes how the cooperation started, developed and what are the results of it. From the very beginning, the solution was planned to be used university-wide, bringing new IT departments into CMS. It was reflected when the choice of SCCM as software for new CMS was discussed at meeting with all IT departments of MUNI. The discussion resulted in conformity of all IT departments that they want not only use CMS but also contribute to it. However, since none of them had any experience with SCCM, we agreed that the initial configuration would be in the hands of our team and then after basics being done, the collaboration would start.

At some point in the time, the knowledge about how they can do the operations they need to perform in the new CMS had to be transferred to all IT departments. Knowing how big change CMS is undergoing, we decided to not overload administrators with training courses of SCCM, but rather prepare and give them processes easy to follow that will guide them in migrations and during which they will naturally get to know basics of SCCM. Moreover, after the migration is over, we plan to start regular training to broaden their SCCM knowledge and skills.

10.1 SCCM MUNI team

As soon as the study room mode was set up, it was presented to IT departments at the workshop that ICS conducts. The SCCM MUNI team, in which administrators voluntarily took part and got access into SCCM which was still undergoing improvements, was established there too. We prepared the test environment for them in which they could learn basics of SCCM without worries about breaking anything, expecting they would help us with the configuration of SCCM to speed it up. However, it turned out that the learning process of working in SCCM is difficult and slow, so they did not
help up us with configuration. However, their activity was beneficial because within SCCM MUNI team the migration scenarios shown in the previous chapter were prepared and tested. It was significant help having immediate feedback on what scenario the process does not cover, what is unclear and what doesn’t work typically because of incorrectly set permissions.

10.2 Access hand over

After the migration processes were prepared, the on-site meetings with each IT department were scheduled. They served for handing over access into SCCM, doing preparation works, explaining essentials, helping them during the first tries of the migration processes and resolving issues that came up. As first, we did the IT departments that had members in SCCM MUNI team because they had all the preparation work already done. These meetings took just a few hours in which questions and minor issues were resolved. Later we visited the other IT departments without members in SCCM MUNI team; these visits usually took 2-3 days depending what issues came up. We are not done yet the meetings are planned until the end of May 2018. After that, they should be able to perform migration tasks on their own, with our help in resolving problems that they cannot deal with yet. This migration period is expected to span over summer holidays when IT administrators usually perform changes utilizing lower PC occupancy.
11 Conclusion

At the beginning of the thesis, motivations are described which lead to searching new technology and solution for CMS. From the motivations that were mainly technological issues emerged requirements for the new CMS. The search and selection of such solution are also described but only briefly as it was not the goal of this thesis.

This thesis aimed to configure and deploy SCCM at MUNI and prepare migration plans for devices joining new CMS. SCCM itself is a valuable tool, but in conjunction with other technologies as an AD, it becomes superb for device management and therefore was SCCM integrated into existing CMS creating a new version of CMS meant to be used by every MUNI computer. Such integration required to get to know current CMS, to identify and reuse only necessary CMS subservices and to explore SCCM features which could be brought into CMS making it state of the art centralized management service. After it was done, the SCCM environment was designed and installed with the help of Microsoft’s Premier Support.

The main part of this thesis refers to how the configuration for different computer modes was done, what issues came up and how we resolved them. There is also outlined how we dealt with the requirements for cooperation between IT departments inside SCCM console by designing delegation model and custom collection hierarchy for application deployment.

However, configuration itself was not the final goal; we needed to design and create processes which administrators could follow to join or migrate into new CMS, these processes were created in collaboration inside SCCM MUNI team that was established during this project. Communication with members of the team during development of processes and later during handing over of these processes, access rights, and resolving issues established better contact between IT departments administrators and us and between IT departments themselves. It is promising that having unified central management solution also helps to unite IT departments into collaboration.

An important aspect of the project was the time constraint, because of MUNI4STUDENTS project everything had to be done before new hardware would arrive. The exact date was unknown, but May 2018 was estimated as the time when first computers needed to be installed. We were successful as on April 12th the workshop presenting prepared CMS was held. The hand over
meetings were then arranged according to requirements of IT departments depending when they plan their installations and migrations. There are still notebook and classroom modes that were planned but are not done yet. Notebook solution is in testing; Classrooms will be done after notebook support is released.

The work described in this thesis is the result of team collaboration from several departments of ICS MUNI and other IT departments of MUNI. However, most of the effort was made by a team of two Ing. Martin Lebeda and myself. Martin was the project manager, and his knowledge of old CMS was crucial. I was designing and developing configurations and processes, presenting at workshops and helping administrators in resolving issues.
References


A Attachments

The attached *archive.zip* contains four folders.

- **CMS diagrams** – diagrams of the old and the new CMS compositions.
- **CMS poster** – a poster that was created for internal ICS presentation.
- **PowerShell scripts** – contains scripts that were created during configuration of the application management in SCCM. There is also `install_jre.ps1` which is a sample of complex installation that has been implemented as script installer.
- **Process models** – contains models of processes designed for migration purpose.