LAUREA
UNIVERSITY OF APPLIED SCIENCES
Together we are stronger

Automating an IT environment with a service delivery platform

Valkama, Kim Juhani

Laurea University of Applied Sciences
Leppävaara

Automating IT-environment with a service delivery platform

Kim Valkama
Degree Programme in Business
Information Technology
Bachelor's Thesis
October, 2016

Laurea University of Applied Sciences **Abstract**
Degree Programme in Business Information Technology
Bachelor's Thesis

Valkama, Kim

Automating IT-environment with a service delivery platform

Year 2016 Pages 29

As business keeps growing, and the amount of technology needed to run a business grows, the need to maintain and update those devices becomes a project in itself. In this documentation different ways of maintaining, updating and repairing these devices will be explored. The project will focus on maintenance from a centralized point of view, instead of per device and for this reason it will be built around a platform named N-Central.

The following documentation includes general information about the different aspects of N-Central, as well as a separated network where the platform will be configured to update, repair and configure devices. The results gathered in the project are based on information found in the official information repository of the platform and a trial and error style of testing features. The documentation is set up in 5 parts, with an introduction, information about how the platform works, the project itself, an example case and a conclusion.

While the project was still underway a few live cases related to the project emerged. Although these cases were not directly related to the project network itself, a live case example is included to give context on how such a problem can be handled with the available technology.

Keywords: automation, enterprise network, windows, N-Central, administrator, business

Table of contents

1 Introduction

While companies grow bigger and computer networks become bigger part of the business world, the maintenance for those networks also requires more attention. A reliable way to ensure that these devices are kept up to date and functioning is by monitoring them. The aim of this project is to take it one step further and build a device network that is able to sustain and update itself, the idea behind it is to decrease the amount of work administrators have to focus on single devices, and give that task over to the device itself. To achieve this goal a mimicked version of an enterprise network will be built and the different solutions will be applied and results will be documented. The project will heavily focus on the technology available, and aims to follow the principles and ideology of the company. Although there is no clear finish line for the project, it aims to prove the different possibilities available and works as a guideline of how to create and use such a network environment.

1.1 Project background

When the topic of the thesis was first discussed with my current employee and thesis customer, the decision was stuck between two options; a deeper insight of the automation the N-Central platform we have in use, or a new service for patients and doctors to remotely connect. After some brainstorming it was finally decided that the automation was the right way to start. The reason automation was the higher priority was simply the fact that the automation technology was already in use, and this project would give a deeper insight on how it works, and allow the company to apply the technology better.

1.2 Project Goals

The goal for the project is very clear but unspecific, ease the work of administrators and create a more reliable and user friendly working environment for customers. Since the goal of the project is so unspecific and the result is based on 2 different points of view (administrators and customers) milestones were used as sub-goals, the milestones are as follows: Initial setup, Patch management, Self-Healing, task scheduling, monitoring and maintenance. After a milestone is complete it will be tested and monitored from both sides of view.

1.3 Personal goal

Personally I have always been interested in testing device capability, what other functions can devices have than the intended one. Automation is one way to test capabilities, how much can remotely be controlled on the device and how much can be automated. Besides my personal interest there is some other valuable knowledge to be learnt, how networks work. Networking has always been one of my weakest topics in IT and I think this project is a good opportunity to learn about device networking.

1.4 Integral Oy

Integral is a medium sized ICT-Integrator based in Finland. With around 50 employees and revenue of around 6 M €, the continuously growing company offers a wide variety of ICT services such as: programming, websites, IT-support, networking and hosting. Originally started in 2005 the company has made recent progression in expanding its market outside of Finland, as well as expands the customer base. Some of the new additional services offered by integral are data collection, analyzing and reporting. More information about the company can be found on their website www.integral.fi.

Figure 1: Integrals homepage with different products

2 N-Central

The N-Central platform is a system delivery platform designed for system administrators to maintain, administrate and update devices in a business network. The platform itself is very simple and comes with a variety of tools. These different tools can be used separately or be combined to create a service. Initial configuring is the key to using N-Central, it is very limited if not configured correctly, and vice versa, if the platform is configured correctly it has almost unlimited access to the intended domain or device network. N-central also includes 4 different services you can include in the agent; Security Manager, Backup Manager, Patch Manager and Remote support Manager. This project will focus mostly on 2 of them, Patch Manager and Remote support manager. The reason for the focus group is since we have backup software as well as security software in use.

A few keywords that will be used in this section are:

N-Central: The Administrators “side” of the platform. This is the section where the work is mostly done, since N-Central is web based it is a website.

Probe: The probe is the core software for any server, it enables monitoring tools for devices and can “discover” the network as well as add new devices.

Agent: The key feature of the platform. The agent is a little software that opens the connection between N-Central and the computer. The agent also gathers information about the device and runs command from a different user than the local logged in one, if configured right it can even control a locked/shut down computers.

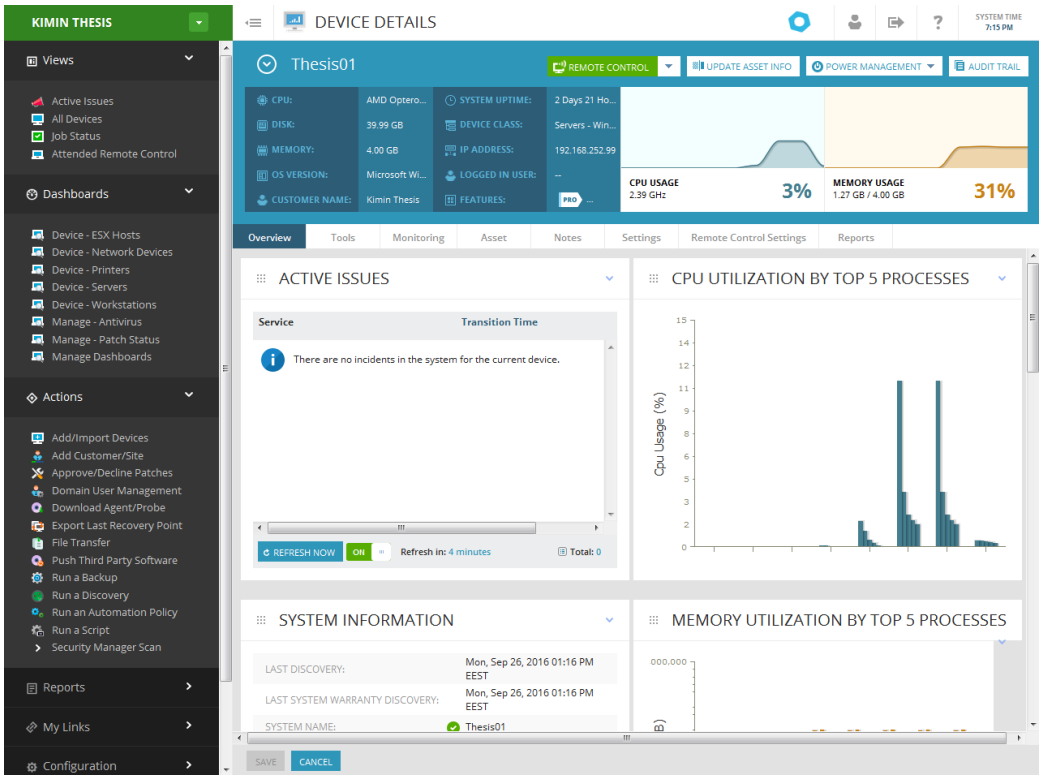


Figure 2: N-Central device overview

2.1 How it works

The N-Central website is hosted on a dedicated server or in a cloud, this server is in charge of administrators' login portal as well as sending and receiving data to all the different devices with an agent or probe installed. When a command is sent from the portal to a device, it is received and executed with the "run as..." command. The command changes user to a domain or local administrator specifically made for N-Central use. Since the agent is flagged as local system process it will execute at boot up instead of user login, this allows administrators to access the device before user login. Full control of the device before login can be useful for many different cases. Some examples would be a forgotten password without connection to domain or a broken local profile. Since the N-Central platform includes a lot of features sorted under different tabs that can be combined in different ways for different solutions, the next section will be basic information about each feature and generally how it has been used in this project.

2.1.1 Rules and service templates

Rules and service templates tell the different tools how behave. Service templates describe what should be monitored on which device, what the different thresholds are and what to do when a process fails. Rules describe how the agent should act on a device, and what devices to target.

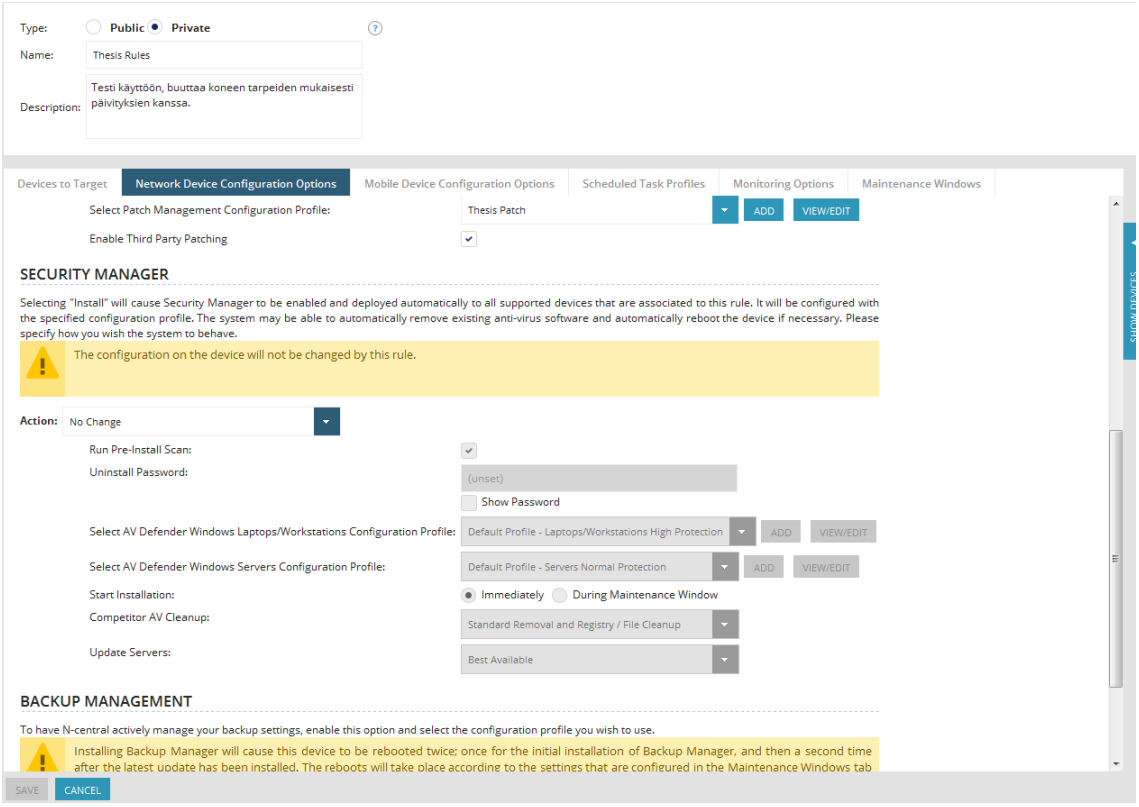


Figure 3: Editing rules

2.1.2 Tools

The tools section includes general support tools that directly connect to the customer computer. From the tools section it is easy to do quick fixes or changes. One of the core tools is the command prompt connection. As mentioned before the N-Central user is an administrator, and the command prompt is run as administrator. This is the simplest yet one of the most powerful tools, since command prompt with elevated rights have almost unlimited access to the device. Notable with the cmd tool is the possibility to open PowerShell with the command “powershell.exe”. Another notable tool is the task execution. Task execution is able to run an administrator created script or N-Central repository script without creating a rule. These two tools are the ones that will be used the most. Other tools available are file manager, registry editor, startup applications and printers.

2.1.3 Monitoring

The monitoring tools available in N-Central generate information about the device based on how the administrator has configured the device. This section includes any N-Central related changes done to the device, such as any rules created in N-Central, Service Templates and any processes with self-healing applied. Notable from the monitoring section service templates can be created by copying chosen monitored processes. This eases the deployment for new customers. The monitoring section is also where self-healing processes are applied.

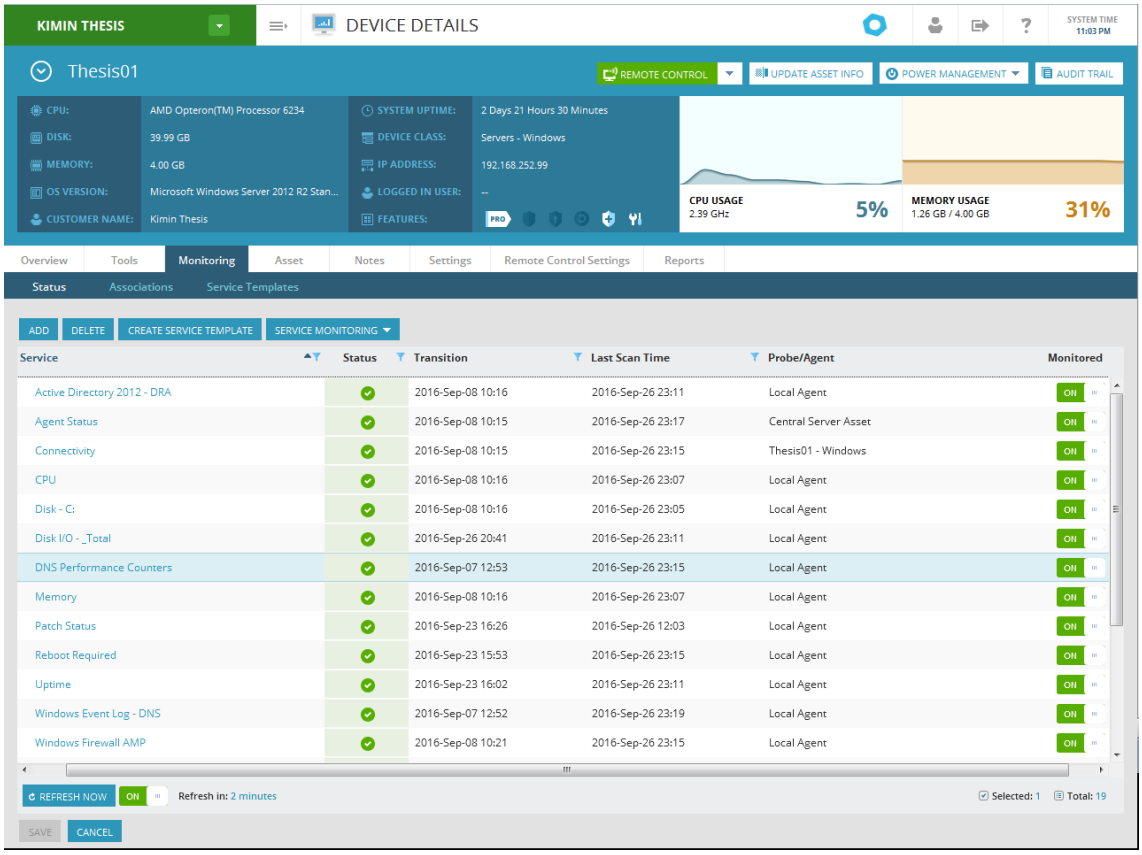
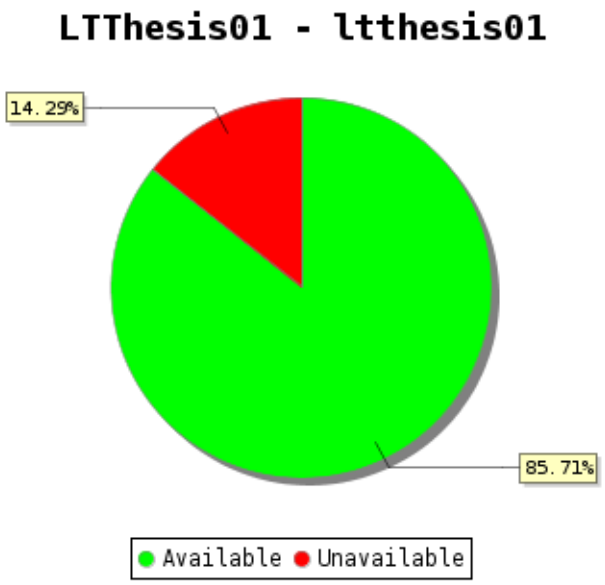


Figure 4: Service monitoring

2.1.4 Assets, Notes and Reports

Are the non-live tools of N-Central. Assets include information about what hardware the device has, different licenses, installed applications and general information that does not need to be updated live. Notes are personal or companywide notes of a certain device. Reports are one of the more useful sections. The report section logs all activity between the N-Central platform and the device. Reports can also be configured to be sent to a dedicated e-mail address.



Available (%)	Unavailable (%)
85,71	14,29

Table 1: Machine availability report

2.1.5 Administration Control

N-Central also includes tools to control N-Central itself and other miscellaneous tools that control different aspects. Almost all the tools mentioned so far are customizable to an extent. Some examples of small but invaluable tools are Service control, discovery defaults and Network share settings. The Service Control can enable or disable a certain service for a wide group of devices, discovery defaults include configurations about how auto discovery

works and network share settings allow you to map a device from where any customer can access files (optimal for bulk installations). These are just a few examples of small efficient tools that can be found around the N-Central platform.

2.2 Different Operating system

The N-able agent is available for the 3 major operating systems, Windows, Mac OS and Linux. Since N-Central is based around Windows most of the tools will not be available for Mac OS or Linux, however the remote control option is still available for both which is more than enough for maintenance. The administrator side of N-Central can be accessed as an app through the android and apple phones.

2.2.1 Windows

As mentioned the Agent software is built around windows, and hence it is also easiest to set up in windows. The agent on windows is stable as long as configured right. However a notable setback is local firewalls. Sometimes a local firewall can require local authentication before the agent can run its command, and if no one is locally at the device the command cannot be ran until authenticated. Generally firewall setbacks can be worked around with volume licensing and a control point for the administrators where local settings can be modified, or by using the provided firewall that can be enabled with N-Central.

2.2.2 Mac OS

As mentioned before the tools available for Mac OS are very limited. The installation on a mac device requires a lot more configuration to get working, and hence is suggested to be done locally on the device. As mentioned the only available tool for Mac OS computers is the remote desktop tool. This somewhat reduces the amount of control administrators have for the device, but still enables the administrators to work on the machine if required.

2.2.3 Linux

Linux also has limited support for the agent but like Mac OS the remote connection is still available. Since very few customers use Linux as workstation OS there is little to no need for Linux automation and Linux will mostly only be mentioned in this section. Although limited process self-healing is also applied.

2.2.4 Mobile Devices

Since mobile devices are generally seen as more stable and less configurable than workstation computers, the maintenance needs are different. The 3 key features to the mobile agent are; remote support, remote wipe and application/software updating. With these 3 tools automation is unfortunately not possible, but instead the mobile agent aims to centralize the maintenance of mobile devices and works as a safeguard to ensure no information on a mobile device is compromised.

2.3 Remote Support

Remote Support is one of the key features of N-Central as well as the currently most used tool at Integral. Remote support includes a variety of different tools to establish a remote desktop connection. As remote desktop connections give you the same graphical user interface as the customer it is easy to understand and troubleshoot the problem. Since remote desktop connection is not part of automation it will not be used for this project, but still is a feature worth documenting. Remote support can be customized to use different default settings depending on assigned service template, and since not all the different technologies used are windows dependent it is easy to configure and setup for a workstation different than windows.

3 The Project

As the project is mostly focused on automation, and some of the features available at N-Central are provided by another software, some otherwise essential features will not be configured on N-Centrals side. These features are security management (N-Centrals own version of a local firewall and antivirus) and backup management (a backup client). The project is divided into 5 milestones. The 5 different milestones are; the initial setup, patch management, self-Healing, task scheduling, monitoring and maintenance.

3.1 Limitations

Due to limitations in available resources some devices that usually are found in an enterprise network will not be included for this project. Out of these devices some have been replaced with alternatives that mimic the original device. An example of this would be printers, there are no printers connected to the network, some of the devices have a .pdf file printer installed. This allows automation on a software level, and is sufficient enough for this project.

Other devices such as firewalls and routers are neither dedicated to the project network. The network uses the company firewall and routers, but these devices are not as essential and are not configurable through N-Central.

3.2 The initial setup

To start off the project a group of devices and a network was in need. A smaller version of an enterprise network was built. During the initial setup there were some complications with the connection and devices. At some point midway through part of the devices were switched out to less demanding workstations, so the original workstations could be used for more demanding tasks. The location of the project was also changed, but the server stayed in the same network.

3.2.1 The network

The network is totally separated from the rest of the company network and some configuration had to be done. It was decided that a VLAN with a few physical ports at the office was the best solution. The VLAN was given an IP range of 192.168.252.0-254. The three different workstations in the network have dynamic IP addresses ranging from 192.168.100-254 and the server has a static address of 192.168.252.99. Since most customer computers use dynamic IP addresses it was decided it would be more suitable for this project. After the IP configurations were done all connection from the project server were blocked on the company firewall.

3.2.2 Devices and User

To ensure that the configurations done would work on different kinds of devices and different users, all of the users and devices differ. 2 of the machines are windows 7, one is windows 10 and the server is a windows 2012 r server. The server works as an Active director and DNS server. All of the devices are in the server's domain, and have a domain user with different user policies. 2 of the users have local administrator rights for the workstation they are signed in on. Out of the 4 devices 2 are virtual, one of the windows 7 machines and the server.

Name:	Virtual/Physical:	OS:	Local admin:	IP:
LTThesis01	Virtual	Windows 7	Yes	Dynamic
KONE	Physical	Windows 10	Yes	Dynamic
KONE2	Physical	Windows 7	No	Dynamic
Thesis01	Virtual	Server 2012 RS	Yes	192.168.262.99

Table 2: Device Specifications

3.2.3 Applying the N-Central probe

After everything was set up to mimic an enterprise network the probe was installed on to the server. When the installation was complete and the server had registered on N-Central auto discovery was enabled. Auto discovery is a feature of the probe. It scans the network for devices, and if the N-Central user's credentials work it installs the agent on to the target device. When the agent is installed and registered at N-Central, the default workstation service template was assigned. Since all the devices differ a little and there is no reason to create a template for one device, the default templates were only modified separately for each device.

3.3 Patch management

Patch management is one of N-Centrals core features. The patch manager is made to easily approve or decline patches based on patch or device. The manager itself is controlled by a patching profile which decides how the manager acts, what patches will be installed and when the patching will be done. Some patches by 3rd party vendor require an accepted EULA to install. Unfortunately these patches have to be approved manually through N-Central. If manual approval is not possible there is also the possibility to use a 3rd party package manager or software updater.

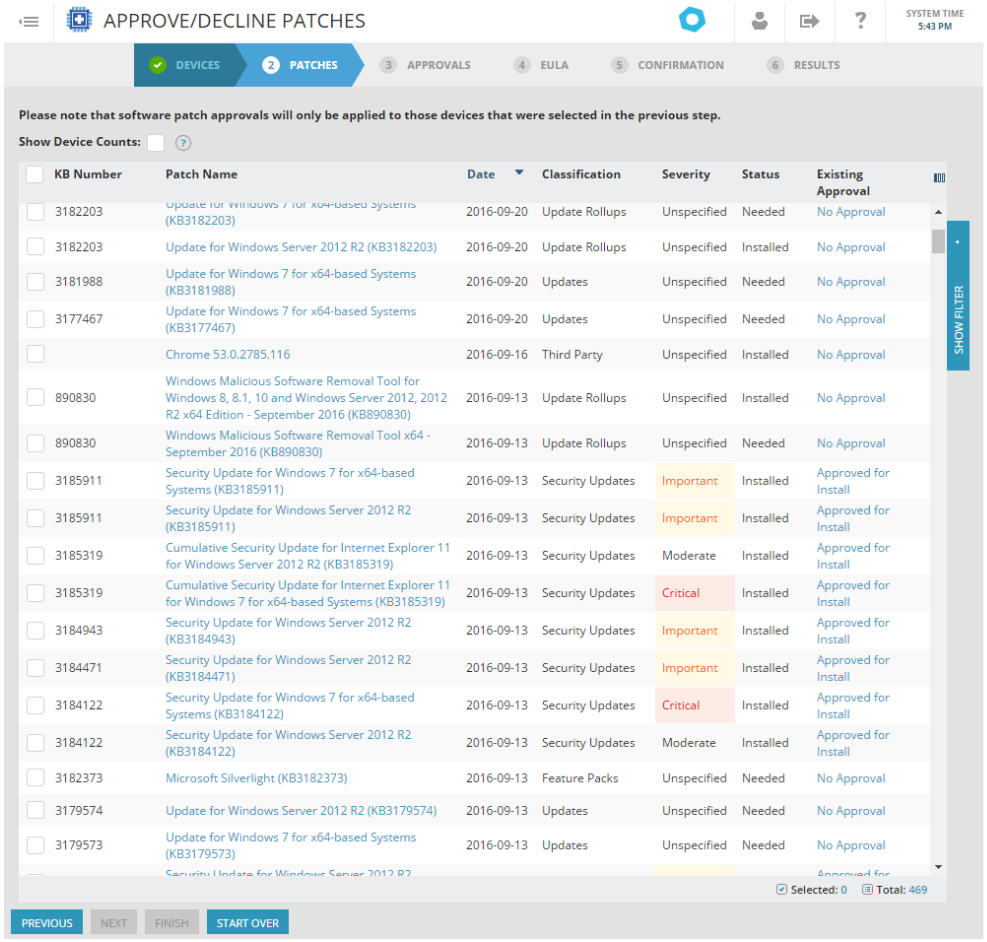


Figure 5: patch manager

3.3.1 How it was applied

When the server was initially setup patch management could be applied. Since the old profile found at N-Central included all essential updates, there was no need to create a new profile from scratch. The old profile includes patches for any freeware customers' use, generally this patch should be used by default and modified per customer basis. After patch management was applied a service template was created to monitor the patched services and to ensure they work as corrected. When creating a service template there is the possibility to enable self-heal, the next section of the documentation will have a deeper insight on how self-heal works. After the service temple was applied, self-heal was applied to some of the different services. As mentioned N-Central uses system credentials if not specified to use logged in ones, for this reason only part of the services are under the control of self-heal. If the device only has one user self-heal could also be applied to user specific processes, such as any network browser or explore.exe. Since new software patches sometimes include bugs or other unwanted software, it was decided that no 3rd party patching would be used. It adds an extra

layer of security to manually ensure the patches are viable and working with the current system setup.

3.4 Self-Healing

The self-healing tool in N-Central is the most essential tool for computer maintenance after initial setup. The tool allows administrators to decide how the device behaves based on process state changes. The standard type of self-heal would scan the process status every 5 minutes, if a process does not match the defined normal status (1 running process) the status would be changed to warning or failure. Warning and failure are by default configured as 0 processes running or more than 1 process running. After the status has changed it is rescanned a few times to verify that the process is not working correctly. If the status is still not back to normal the self-healing process starts. The agent shuts down all processes or the whole process tree for a certain process, verifies it is not running and restarts it. After the process has been restarted and scanned a few times to ensure it is running a report log is sent to the dedicated e-mail if there is one. This is generally the working fix for most cases, but since the administrators have full control of what processes to scan and what to do if the state is changed there are a variety of things that can be achieved with the self-healing tool. N-Central has a great Script repository for normal administrator tasks such as renewing target computer IP or killing a process.

3.4.1 How it was applied

As mentioned self-healing was applied to part of the patched processes combined with patch management, the reason to apply them was not to ensure that the processes keep running, but more so to discover the power of self-healing. After the self-healing was applied to patching some other self-heal processes were edited to fit the devices in use. A few examples of processes with changes are connectivity and disk usage. The standard connectivity process contacts the N-Central platform and verifies all the packages are moving. Since the devices in use are connected over LAN and can work without connection to the Platform the command was tweaked to contact the local server instead of the platform. The settings on the server side were tweaked to contact the platform and renew the network settings if connection was not possible. Since problems with network connections can sometimes take hours to resolve, a timeout timer for the self-heal was set for 1 hour and a scheduled task was saved as a manual alternative for resetting the connection. Scheduled tasks and automation policies will be discussed in the next topic. The disk usage process was changed on one of the virtual devices with dynamic disk allocation enabled. Dynamic disk allocation gives the virtual hard drive more space depending on how much space is required. Since the Agent is not aware that the hard drive is virtual it would keep notifying the user that the disk is full. The applied work

around for the disk was to edit the thresholds to only notify when there was 0% left of disk space. The reason to still keep the process enabled was to get a notification when if the disk started taking up a lot of space within a short period of time.

3.5 Automation Policies and Scheduled tasks

Automation Policies and scheduled tasks are aimed at running a task on a schedule, or running a task to more than 1 device at once. The automation policy focuses more on the network as whole and executing devices, task handler and target device can be defined. These policies are generally something evolving around transferring information between devices or changing device policies. Scheduled tasks work with the same principle as self-healing, but instead of a threshold that has to be met it runs on a schedule. The tasks that can be run are scripts made by administrators or from the N-Central repository. When applying N-Central automation policies to a network it is important to ensure that all target devices have PowerShell version 2.0 or higher in use, otherwise the policies will return a stale state.

3.5.1 How it was applied

When the company relocated to Espoo some of the devices were switched out, this was a perfect possibility to test out the N-Central automation policies. After auto discovery was run to add the new devices to the domain a command was run to add the 3 different users as local administrators for the devices. After it was verified to work and the devices were back on the network a few scheduled tasks were set up. The first scheduled task enabled was a script to lock any running windows devices after 17.00. After the lockdown script was verified to work another script was to create a zip of a folder on the server and save it to another location. The copyzip script was set to run every Friday at 18.00. Since these were all tasks that could be handled within the LAN the probe was set as the task handler. In the case of devices being outside the network it is preferred to use the devices own Agent as the task handler.

3.6 Monitoring

After everything was installed and verified working it was time to let the network to be tested as a unit. N-Centrals platform has well-built monitoring options for both devices and the network. When monitoring the network there are 4 main views, Active Issues, All Devices, Job Status and Attended Remote Control. Out of the 4 main view Active Issues is the main focus. The Active Issues include any monitored processes that have gone from a normal state to failed, warning, stale or misconfigured. Out of these 4 Stale and misconfigured are rarely see. Misconfigured means that something went wrong in the configuration of the self-heal

monitoring, and has to be reapplied. The stale state means that the process has been updated since the last time it was configured, but N-Central has not received any information about it.

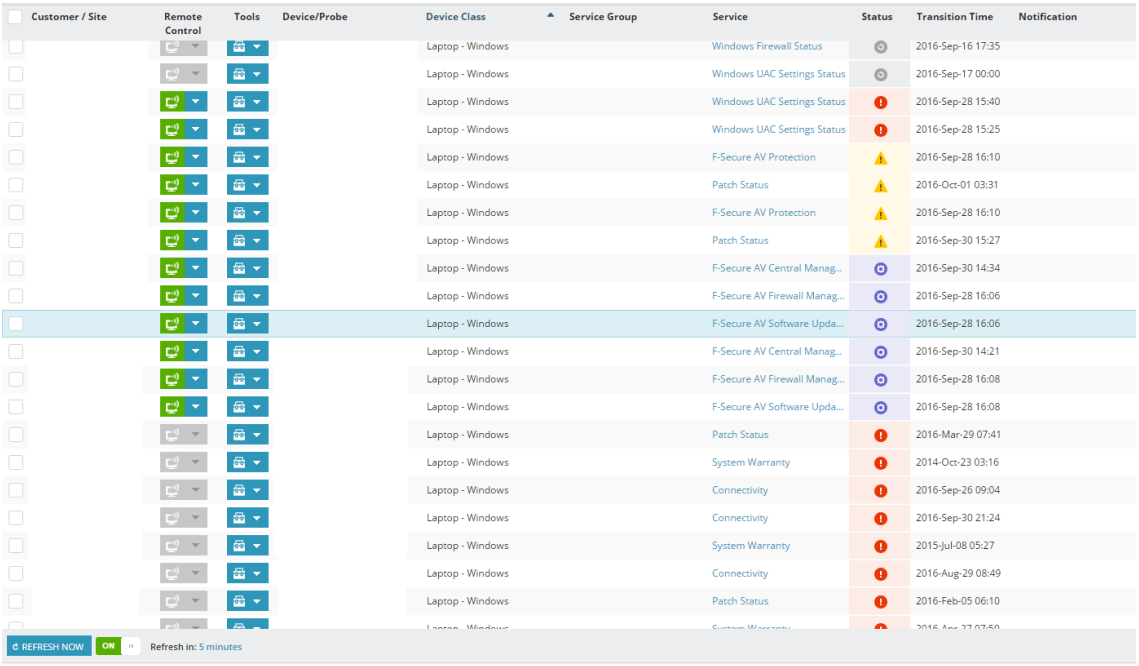


Figure 6: Active Issues of devices without self-healing configured

When a process is listed on active issues and self-healing has not been applied to the process, it is very easy to navigate to the logs of the process and manually fix the error. Under the all devices tab the same principle works as with active issues. The difference is instead of showing devices based on active issues all devices are shown and their current status is shown. The Job Status tab works like a logging service. All changes done by N-Central to devices in the network are logged under job status. The individual device overview is also very clean and simple. It includes any essential information and is modifiable to an extent. If some information is not found on the overview page it is found in one of the monitoring tabs.

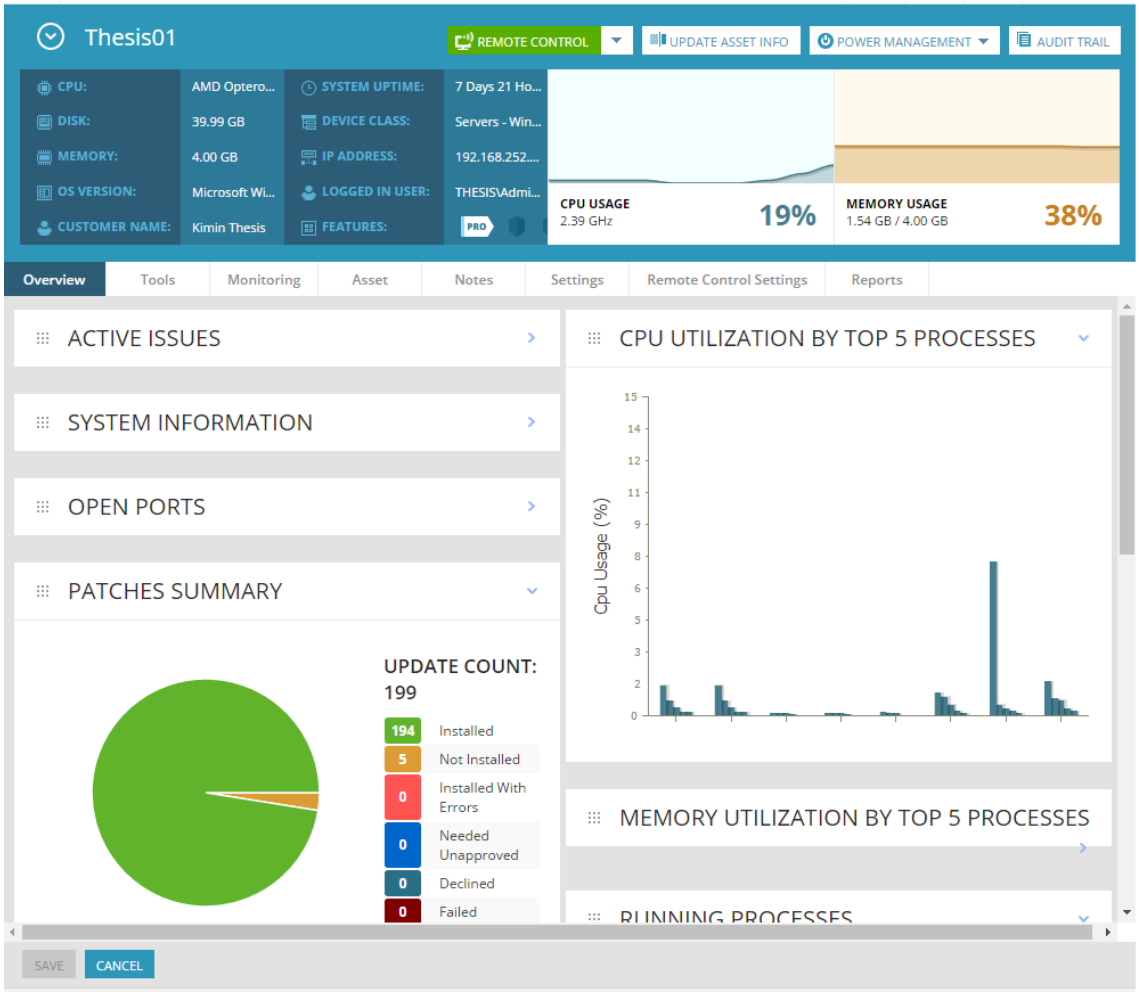


Figure 7: Device overview with patches and CPU usage visible

Besides the information what is running on the computer N-Central also logs activity about the device. The Reports section includes more detailed information about the device and how the agent is acting on it.

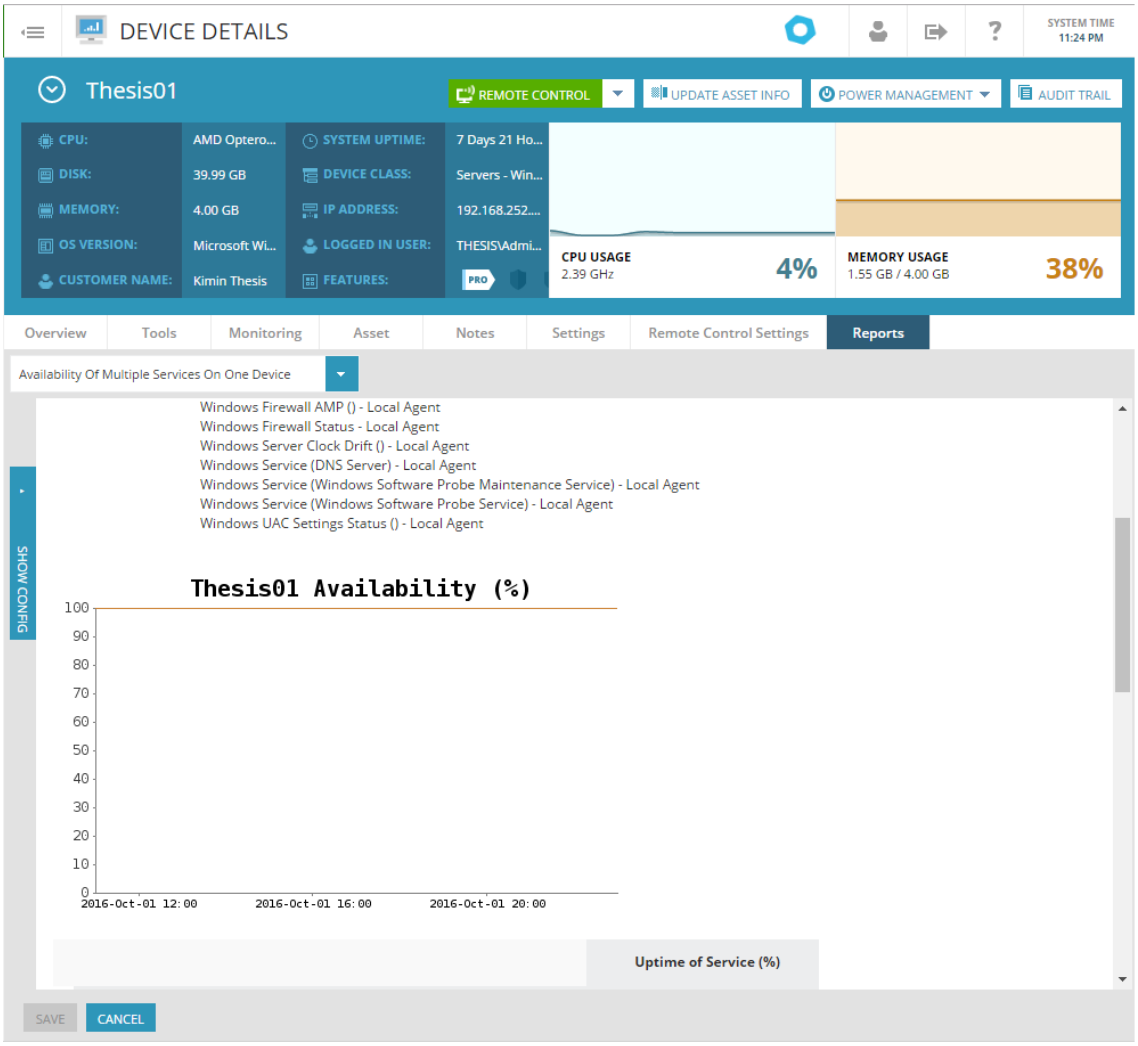


Figure 8: Report Section of N-Central

3.7 Maintenance

Maintaining the N-Central system requires maintenance of two types, maintaining the network and maintaining the N-Central platform and parts. Maintaining N-Central can be managed through the maintenance manager. The maintenance manager is a useful tool that controls what the agent does on the device. It can be used to activate different features for different devices. The maintenance manager can also be used for other tasks such as scheduled power management. Maintenance on the network side usually consists of reboots done through the maintenance manager. For this project the maintenance manager has been set to reboot devices Friday at 16.00, when the device restarts it updates the N-Central software as well as any other software that requires a reboot. The software has also been set to update if the device is shut down or rebooted by a user. At 15.30 Friday a prompt will show that will inform the user of the reboot. If the current user is logged in as an administrator the reboot can be postponed. Notable for maintenance management, if it is enabled it is

suggested to disable users' access to the Windows Update Service. The reason to disable the access is to reduce redundancy, if a user starts a windows update scheduled for later, it might be installed twice and can cause problems.

3.8 Testing

The last section of the project is testing the functionality of the network. With no major errors occurred at the monitoring phase the testing should also go as intended. The first part that was important to test was patch management. This was easily done by approving the current patches and monitoring the installation. The patch manager worked as intended and all the devices got updated. For the self-healing part it was a little harder to do some actual testing. A scenario had to be made where a windows service stopped working and the agent would take over. One of the devices has a self-healing process for the windows printer spooler service, the service was stopped and the device was left running. Within a few minutes the platform had a report of a dropped windows service that was restarted. The same process was done to a few other services that were also re-started by the local agent. While the agent is working in the background keeping processes running when they are shut down, the only notification of it the device user will get is a few minute time off the service. The testing of the system was a challenge, as the end result was based on if the device can run for longer periods of time without needing maintenance from an administrator. The most efficient test that could be done is by actively using the workstations for a long period of time.

4 Example case during project

During the project a real case for one of our customers showed up. To give some context on how the atomization could benefit in a real situation this section will be an example of how it was handled. The customer uses financial management software, located on their main server. Once in a while the software gets "overloaded" and stops taking requests. Since the software is not developed by our company, and there is no access to the source code, there is no possibility to change the program itself. The problem reoccurs every few weeks it is worth looking into for automation. The root of the problem was found to be the windows service "Financial Communications Server", and restarting the service is usually the solution for the problem. To work around manually disabling and enabling the service every time, a self-heal was created. The process was added to the devices service template, and the threshold set to 0 as Failed and 2-10 as Warning. If the service changed status from normal to warning or Failed, the service would be rescanned 5 times with 10 second intervals after 2 minutes. If the windows service still was at a Failed or Warning state the service would be shut down and restarted a minute later. Since the initial self-healing setup there have been no major

problems with the service and the customer has not contacted our IT-support regarding problems with the program.

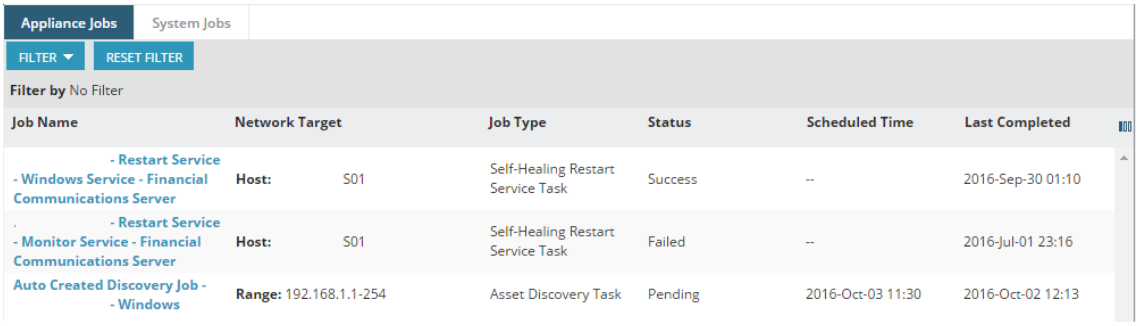


Figure 9: Last failed and successful attempt for the self-heal

From the picture above the last date for a successful self-heal is 30 September, this is 2 days before the screen capture was taken. The last failed attempt is July 01, this is the first attempt after the initial setup for the service. The reason the self-heal failed was a misconfiguration, the credentials applied on N-Central did not match the domain credentials. With this evidence it is reasonable to say that the self-healing process has been working as intended and has also come to use in this case.

5 Conclusion

The conclusion is based on 3 different sections, analysis of N-Central, the result of the project and conclusion of the customer company. Out of the 3 the customer company's response is the one with most value.

The N-central platform has been confirmed as a reliable tool for automation in a network environment. Although the platform has some tools that could be improved on, it also comes with a lot of tools that feel complete to use, and work as intended. Since no other tools that are comparable to N-Central have been used for this project, it is hard to do a benchmarking or comparison. But the N-Central tool has provided enough to deem useful if not essential for such a project.

The results of the project support the claim about the platform. Even though a few relocations have been made while the project was underway, the majority of time the platform has acted as expected on the network. While working with the devices a lot of new knowledge has been learned that can be taken into use to customers, to decrease downtime and increase the quality of their service at Integral Oy.

After the project was finished and presented to the customer company, the feedback and future implementation were discussed. A list of key points of how this technology will impact the company's workflow as well as reputation with customers was created:

- Less maintenance work with higher reliability
- Automatic incident tracking with a knowledge base
- Higher quality services for customer
- Better business value for both Integral and the customer
- Possibility of growth in the support department without personnel increase

Personally I feel like the goals set for myself have been achieved. Although the networking part was mostly focused in the beginning, it has given me a clearer picture of how different devices act with different network settings, and what functionality different settings have. Since completing the project the idea behind centralized management and automation, and the situation where it can be used is easier to determine and how to apply such a solution is clear. Personally I would see the project as a success.

References

Parker, S. 2015. Optimizing and Maintaining your N-central Environment. Accessed 15th June 2016. https://secure.nable.com/webhelp/ncentralpdfs/Optimizing_and_maintaining_your_N-central_environment

N-central Runbook. Accessed 06th June 2016. https://secure.n-able.com/Runbook/

N-Central Community forums and product documentation Accessed 06th June 2016. https://nrc.n-able.com/

Stackoverflow Accessed 06th June 2016. www.stackoverflow.com

Secure by Design 2012. Integrating NinitePro with N-Central. Accessed 06th June 2016. https://ninite.com/help/enterprise/nable.html

Figures

Tables