Beschreibung *nexthink*

IT Beilage E

Inhaltsverzeichnis

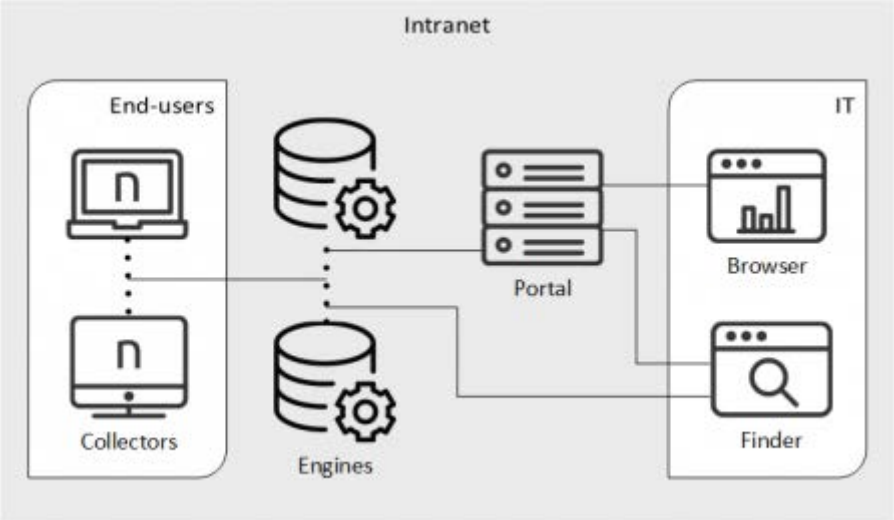
Mitgeltende Dokumente:

- IT-TK-004a_LKI_FO
- IT-TK-004b_HZN_FO
- IT-TK-004c_HA_FO
- IT-TK-004d_Schwaz_FO

The following contents are a summary of the manufacturer's specifications. More detailed information can be found under:
https://doc.nexthink.com/Documentation/Nexthink/latest/ProductOverview/Collector?_ga=2.268339854.1840072860.1561981741-1356225158.1561981741

1. General Overview

The following figure depicts the role of the Collector within the Nexthink solution.



2. Windows Collector

The Windows version of the Collector includes several features in addition to the gathering of user activity. These extra features require a comprehensive set of components.

Applies to platforms:

2.1. Windows Collector binaries

For all versions of Windows, the following components are installed:

- **Main driver**: A kernel mode driver that gathers valuable information from the device of the end-user.
- **Network specific driver**: A kernel mode driver that detects network connections.
- **Helper service**: A Windows service that complements the main driver by collecting additional information.
- **Printing info library**: A dynamic link library that is responsible for detecting printing activity.
- Optional **Command line configuration tool**: A tool to configure the Collector from the command line.
- Optional **Control Panel extension**: A tool to control the behaviour of the Collector that is added to the Control Panel of Windows.

- **Automatic updates**: A component of the Collector that is responsible for downloading new versions and updating the installed components.
- **Coordinator**: Coordination of the Collector with the Appliance for detecting new updates and communicating end-user feedback.
- **End-user feedback**: Components for presenting the questions of campaigns and getting answers from the end-users.

Component	File	Path
Main driver	nxtrdrv.sys	C:\Windows\System32\drivers
Network specific driver	nxtrdrv5.sys	C:\Windows\System32\drivers
Helper service	nxtsvc.exe 7.088k nxtsvc.exe_11.392k	C:\Windows\System32
Printing info helper library	nxtdll.dll	
Command line configuration tool	nxtcfg.exe	
Control Panel extension	nxtpanel.cpl (in Systemsteuerung sichtbar)	
Automatic updates	nxtupdater.exe	
Coordinator	nxtcoordinator.exe 2.332k	
End-user feedback	• nxteufb.exe • nxtray.exe • nxtray.exe.config	

Starting from **Windows 8**, these additional binaries are also installed:

- **Metro apps helper library:** A dynamic link library that detects the execution of Metro apps.

Component	File	Path
Metro apps helper library	nxtwrt.dll	C:\Windows\System32

2.2. Registry keys of the Windows Collector

On installation, the Collector creates the following keys in the Registry of Windows:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\nxtrdrv
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\nxtrdrv5
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Nexthink Service
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Nexthink Coordinator\Modules\Updater
- HKEY_LOCAL_MACHINE\SYSTEM\Nexthink\Updater
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Nexthink Coordinator
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Nexthink Coordinator\Modules\EndUserFeedback

- HKEY_USERS\S-1-5-21-2281471460-584676728-3927365163-1676\SOFTWARE\NEXThink\NxTray
- HKEY_CLASSES_ROOT\nxtrayproto

On **Windows 10**, this additional key is created, used and maintained by the Action Center:

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Notifications\Current\NexThink.NxTray.Messages

2.3. Additional files of the Windows Collector

Find the log files of the Collector here:

- C:\Windows\nxtsvc.log
- C:\Windows\nxtsvc.log.bk
- C:\Windows\nxtupdater.log
- C:\Windows\nxtupdater.log.bk
- C:\Windows\nxtcoordinator.log
- C:\Windows\nxtcoordinator.log.bk
- C:\Windows\nxteufb.log
- C:\Windows\nxteufb.log.bk
- %temp%\nxtray.log
- %temp%\nxtray.log.<timestamp>

Finally, Windows creates a cached copy of the kernel drivers in two folders whose names start with the name of the drivers (**nxtrdrv** and **nxtrdrv5**, respectively) followed by an unique identifier that depends on the version of the driver itself. Find the folders here:

- C:\Windows\System32\DRVSTORE

3. Mac OS Collector

The Mac OS version of the Collector has just the necessary components to report user activity.

Applies to platforms:

3.1. Mac Collector binaries

- Driver: A kernel mode driver that gathers valuable information from the device of the end-user.
- Helper service: A Mac Os daemon that complements the driver by collecting additional information.

Component	File	Path
Driver	nxtdrv.kext	/Library/Extensions
Helper service	nxtsvc	/Library/Application Support/Nexthink

3.2. Configuration files of the Mac Collector

Component	File	Path
Daemon registration file	com.nexthink.collector.driver.nxtsvc.plist	/Library/LaunchDaemons/
Daemon configuration file	config.plist	/Library/Application Support/Nexthink
Crash Guard file	crashguard	

3.3. Additional files of the Mac Collector

Find the log files of the Mac Collector here:

- /var/log/kernel.log
- /Library/Logs/nxtsvc.log
- /Library/Logs/nxtsvc.log.bk (when previous log is rotated)
- /Library/Logs/CrashReporter

RELATED TASKS

- Installing the Collector
- Updating the Collector

RELATED REFERENCES

- Collector MSI parameters reference table
- Nxtcfg - Collector configuration tool
- Collector (Product Overview)

4. Storage requirement:

CPU usage	Memory usage	Network traffic
• Less than 0.015% (in average)	• Kernel: Around 500 KB • User: Around 20 MB	• **UDP** (Optional) 0.1 - 0.3 Kbps (in average) • **TCP** Depending on o Campaigns o Remote actions o Updates In TCP-only configs o Add documented UDP traffic