Beschreibung *nexthink*

IT Beilage E

Inhaltsverzeichnis

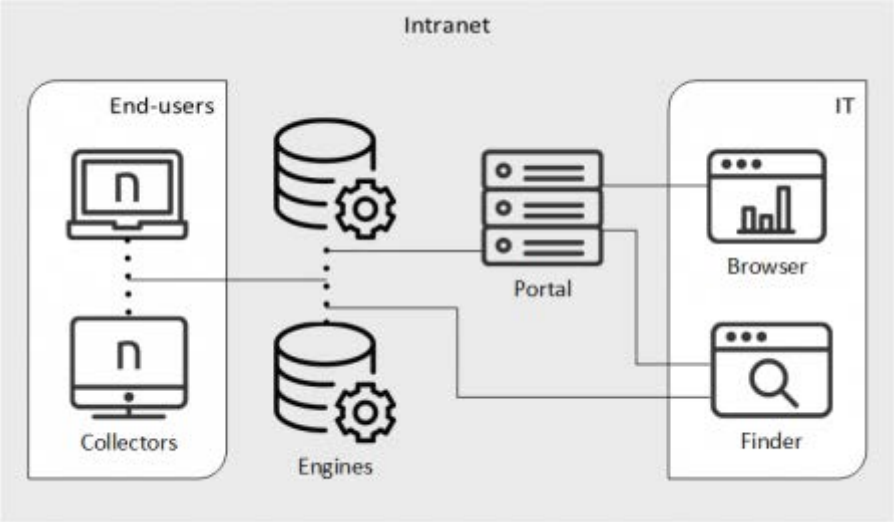
Mitgeltende Dokumente:

- 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: Collector | Nexthink Documentation

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.
- **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 to detect new updates, engage with end-users, and execute remote actions.
- **Nexthink Engage**
  Components for presenting the questions of campaigns and getting answers from the end-users.
- **Nexthink Act**
  Components that manage the execution of remote actions.
- **Nexthink Reporter**
  A troubleshooting tool that creates debug reports for specific support cases.
- **Nexthink Event Log Provider**
  A component for logging events in the Windows Event Log.
- **Nexthink Business Services**
  A component for monitoring business applications.
- **Command line configuration tool** (optional)
  A tool to configure the Collector from the command line.
- **Control Panel extension** (optional)
  A tool to control the behaviour of the Collector that is added to the Control Panel of Windows.

Component	File	Path
Main driver	nxtrdrv.sys	%Windows%\System32\drivers
Network specific driver	nxtrdrv5.sys	
Helper service	nxtsvc.exe	%ProgramFiles%\Nexthink\Collector\Collector
Printing info helper library	nxtdll.dll	
Nexthink Event Log Provider	nxteventprovider.dll	
Immersive apps	nxtwrt.dll	
Application start time	nxtwpm.dll	
Application start time (32 bit)	nxtwpm32.dll nxtusm.exe	%Windows%\SysWOW64
Application start time	nxtwpm.dll	
Coordinator service	nxtcoordinator.exe	%ProgramFiles%\Nexthink\Collector\Coordinator
Engage coordinator	nxteufb.exe	
Act coordinator	nxtcod.exe	
Updates coordinator	nxtupdater.exe	

Component	File	Path
OpenSSL (64 bit)	libcrypto-1_1-x64.dll libssl-1_1-x64.dll	
OpenSSL (32 bit)	libcrypto-1_1.dll libssl-1_1.dll	
Nexthink Engage	nxtray.exe nxtray.exe.config	%ProgramFiles%\Nexthink\Collector\Engage
Nexthink Act	Google.Protobuf.dll nxtcampaignaction.dll nxtremoteactions.dll	%ProgramFiles%\Nexthink\Collector\Remote Actions
Nexthink Reporter	nxtreporter.exe	%ProgramFiles%\Nexthink\Collector\Reporter
Nexthink Business Services	nxtbsm.exe	%ProgramFiles%\Nexthink\Collector\BSM
Command line configuration tool	nxtcfg.exe	%Windows%\System32
Control Panel extension	nxtpanel.cpl	

2.2. Registry keys of the Windows Collector

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

- HKEY_CLASSES_ROOT\nxtrayproto
- HKEY_LOCAL_MACHINE\SOFTWARE\Nexthink\Collector
- HKEY_LOCAL_MACHINE\SOFTWARE\Nexthink\Collector\AppStartTime
- HKEY_LOCAL_MACHINE\SOFTWARE\Nexthink\DN
- HKEY_LOCAL_MACHINE\SOFTWARE\Nexthink\RebootMarker
- HKEY_LOCAL_MACHINE\SOFTWARE\Nexthink\RemoteActions
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\Nexthink Collector
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Nexthink Coordinator
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Nexthink Coordinator\params
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Nexthink Coordinator\Modules\COD
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Nexthink Coordinator\Modules\EndUserFeedback
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Nexthink Coordinator\Modules\Updater
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Nexthink Service
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Nexthink Service\runtime_stats

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\nxtrdrv
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\nxtrdrv\params
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\nxtrdrv5
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\nxtrdrv5\Parameters\Wdf
- HKEY_LOCAL_MACHINE\SYSTEM\Nexthink\Updater
- HKEY_USERS\S-1-5-21-[X-X-X-X]\SOFTWARE\NEXThink\NxTray

2.3. Additional files of the Windows Collector

Find the log files of the Collector here:

- %windir%\nxtsvc.log
- %windir%\nxtsvc.1.log
- %windir%\nxtsvc.2.log
- %windir%\nxtupdater.log
- %windir%\nxtupdater.1.log
- %windir%\nxtupdater.2.log
- %windir%\nxtcoordinator.log
- %windir%\nxtcoordinator.1.log
- %windir%\nxtcoordinator.2.log
- %windir%\nxteufb.log
- %windir%\nxteufb.1.log
- %windir%\nxteufb.2.log
- %windir%\nxtcod.log
- %windir%\nxtcod.1.log
- %windir%\nxtcod.2.log
- %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:

- %windir%\System32\DRVSTORE

The Nexthink Reporter tool creates its logs and reports here:

- %temp%\nxtreporter[reportID].log
- %temp%\nxtreport-[hostname]-[reportID].zip

3. Storage requirement:

CPU usage	Memory usage	Network traffic
Less than 0.015% (on average)	• **Kernel** 500 KB • **User** 30-40 MB Temporary memory spikes are possible during campaigns.	• **UDP (Optional)** 0.1 - 0.3 Kbps (on average) • **TCP** Depending on ☐ Campaigns ☐ Remote actions ☐ Updates ☐ In TCP-only configs ☐ Add documented UDP traffic