NXQL Data Model

Objects

application

An application is a set of executables e.g. 'Microsoft Office'.

Name	Type	Operating systems		Properties
company	string	Windows	macOS	
	Company producing the application			
database_usage	permill	Windows	macOS	
	Percentage of the database used by information related with the application			
description	string	Windows		
	Application description			
first_seen	datetime	Windows	macOS	NU
	First time activity of the application was recorded on any device.			
id	identifier	Windows	macOS	
	Unique application identifier			
known_packages	string	Windows	macOS	
	List of packages known to contain the application. This list is not exhaustive: The presence of a package does not necessarily imply that on a given device the application was installed through that package.			
last_seen	datetime	Windows	macOS	NU
	Last time activity of the application was recorded on any device.			
name	string	Windows	macOS	
	Application name			
platform	enum	Windows	macOS	
	The platform (operating system family) on which the application is running.			
storage_policy	enum	Windows	macOS	
	Indicates the event storage policy for the application. Possible values are: • all: web requests, connections and executions are stored; • connections and executions; • executions; • none: no activity is recorded.			
total_active_days	day	Windows	macOS	
	Total number of days the application was active.			

binary

A binary is an executable binary file identified by its hash code.

Name	Type	Operating systems		Properties
application_category	string	Windows	macOS	SE
	Indicates the category of the application: • '-': Not yet tagged; • Unknown: Not categorized by Nexthink Library.			
application_company	string	Windows	macOS	
	Application company			
application_name	string	Windows	macOS	

	Application name			
architecture	enum	Windows	macOS	
	Executable architecture (32/64 bit)			
average_cpu_usage	permill	Windows		
	Average CPU usage for the binary			
average_memory_usage	byte	Windows		NU
	Average memory usage for the binary			
average_number_of_graphical_handles	integer	Windows		NU
	Average number of graphical handles (GDI)			
company	string	Windows	macOS	
	Executable company			
database_usage	permill	Windows	macOS	
	Percentage of the database used by information related with the binary.			
description	string	Windows		
	Description as it appears in the binary file.			
executable_name	string	Windows	macOS	
	Executable name			
file_size	byte	Windows	macOS	
	Binary file size			
first_seen	datetime	Windows	macOS	NU
	First time activity of the binary was recorded on any device.			
hash	md5	Windows	macOS	
	Hash code of the binary (MD5)			
id	identifier	Windows	macOS	
	Unique binary identifier			
last_seen	datetime	Windows	macOS	NU
	Last time activity of the binary was recorded on any device.			
paths	path	Windows	macOS	
	List of paths of the binary			
platform	enum	Windows	macOS	
	The platform (operating system family) on which the binary is running.			
sha1	sha1	Windows	macOS	
	SHA-1 hash code of the binary			
sha256	sha256	Windows	macOS	
	SHA-256 hash code of the binary			
storage_policy	enum	Windows	macOS	
	Event storage policy for the binary (connection and execution, execution-only or none)			
threat_level	enum	Windows	macOS	SE
	Indicates the threat level of the binary: • '-': Not yet tagged; • none detected: No known threat; • low: low threat; • intermediate: Intermediate threat; • high: high threat.			
total_active_days	day	Windows	macOS	

	Total number of days the binary was active.			
user_interface	boolean	Windows		
	Application has interactive user interface			
version	version	Windows	macOS	
	Version of the binary			

destination

A destination is a device or server receiving TCP/UDP connections.

Name	Type	Operating systems		Properties
database_usage	permill	Windows	macOS	
	Percentage of the database used by information related with the destination			
first_seen	datetime	Windows	macOS	NU
	First time activity to the destination was recorded on any device.			
id	identifier	Windows	macOS	
	Unique destination identifier			
ip_address	ip_address	Windows	macOS	
	IP address for the destination			
last_seen	datetime	Windows	macOS	NU
	Last time activity to the destination was recorded on any device.			
name	string	Windows	macOS	
	Reverse lookup name			

device

A device is Windows physical or virtual machine monitored by a Nexthink Collector.

Name	Type	Operating systems		Properties
administrator_account_status	enum	Windows		
	Determines whether the local Administrator account is enabled or disabled.			
all_antispywares	string	Windows		
	Summary information about all the detected antispyware: • unknown: Indicates that the information could not be retrieved; • N/A: This field is not available on this operating system; • '-': No data, incompatible collector version or the data is not yet available.			
all_antiviruses	string	Windows		
	Summary information about all the detected antiviruses: • unknown: Indicates that the information could not be retrieved; • N/A: This field is not available on this operating system; • '-': No data, incompatible collector version or the data is not yet available.			
all_firewalls	string	Windows		
	Summary information about all the detected firewalls: • unknown: Indicates that the information could not be retrieved; • N/A: This field is not available on this operating system; • '-': No data, incompatible collector version or the data is not yet available.			
allow_non_provisionable_devices	boolean			NU
	Indicates whether a device which does not fully support the policy is still allowed to connect to the Exchange Exchange ActiveSync server. If 'yes', the security policy is not guaranteed to be applied, even if the field 'ActiveSync policy application status' value is 'applied in full'			

antispyware_name	string	Windows		NU
	Name of the main antispyware			
antispyware_rtp	enum	Windows		
	Indicates whether the antispyware real time protection (RTP) is active: • on: Indicates that RTP is active; • off: Indicates that either RTP is not active or no antispyware has been detected; • unknown: Indicates that the information could not be retrieved; • N/A: This field is not available on this operating system; • '-': No data, incompatible collector version or the data is not yet available.			
antispyware_up_to_date	enum	Windows		
	Indicates whether the antispyware is up-to-date: • yes: Indicates that antispyware is up-to-date; • no: Indicates that either the antispyware is not up-to-date or no antispyware has been detected; • unknown: Indicates that the information could not be retrieved; • N/A: This field is not available on this operating system; • '-': No data, incompatible collector version or the data is not yet available.			
antivirus_name	string	Windows		NU
	Name of the main antivirus			
antivirus_rtp	enum	Windows		
	Indicates whether the antivirus real time protection (RTP) is active: • on: Indicates that RTP is active; • off: Indicates that either RTP is not active or no antivirus has been detected; • unknown: Indicates that the information could not be retrieved; • N/A: This field is not available on this operating system; • '-': No data, incompatible collector version or the data is not yet available.			
antivirus_up_to_date	enum	Windows		
	Indicates whether the antivirus is up-to-date: • yes: Indicates that antivirus is up-to-date; • no: Indicates that either the antivirus is not up-to-date or no antivirus has been detected; • unknown: Indicates that the information could not be retrieved; • N/A: This field is not available on this operating system; • '-': No data, incompatible collector version or the data is not yet available.			
audit_account_logon_events	enum	Windows		
	Determines whether to audit each instance of a user logging on to or logging off from another computer in which this computer is used to validate the account.			
audit_account_management	enum	Windows		
	Determines whether to audit each event of account management on a computer.			
audit_directory_service_access	enum	Windows		
	Determines whether to audit the event of a user accessing an Active Directory object that has its own system access control list (SACL) specified.			
audit_logon_events	enum	Windows		
	Determines whether to audit each instance of a user logging on to or logging off from a computer.			
audit_object_access	enum	Windows		
	Determines whether to audit the event of a user accessing an object, e.g. a file, folder, registry key, printer, and so forth - that has its own system access control list (SACL) specified.			
audit_policy_change	enum	Windows		
	Determines whether to audit every incident of a change to user rights assignment policies, audit policies, or trust policies.			
audit_privilege_use	enum	Windows		
	Determines whether to audit each instance of a user exercising a user right.			
audit_process_tracking	enum	Windows		
	Determines whether to audit detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access.			

audit_system_events	enum	Windows		
	Determines whether to audit when a user restarts or shuts down the computer or when an event occurs that affects either the system security or the security log.			
average_boot_duration	millisecond	Windows		NU
	Full boot duration baseline			
average_fast_startup_duration	millisecond	Windows		NU
	Indicated the fast startup boot duration averaged over the fast startups. In the calculation, recent boots weigh more than older boots (exponentially weighted moving average).			
average_logon_duration	millisecond	Windows		NU
	User logon duration baseline			
bios_serial_number	string	Windows	macOS	NU
	BIOS serial number			
boot_disk_health_status	enum	Windows		NU
	Indicates the health of the disk from which the device is booting [from], as reported by the operating system.			
boot_disk_type	enum	Windows	macOS	NU
	Indicates the type of the disk from which the device is booting.			
chassis_serial_number	string	Windows		NU
	Chassis serial number			
cltr_ca_license_uid	string	Windows	macOS	NU
	Indicates the Collector assignment license UID			
cltr_ca_status	enum	Windows	macOS	NU
	Indicates whether Collector assignment service is enabled or disabled			
cltr_crash_guard_count	integer	Windows		NU
	Indicates the number of consecutive hard resets or system crashes of the device			
cltr_crash_guard_limit	integer	Windows		NU
	Indicates the Collector CrashGuard limit			
cltr_crash_guard_protection_interval	integer	Windows		NU
	Indicates the CrashGuard monitoring interval in minutes			
cltr_crash_guard_react_interval	integer	Windows		NU
	Indicates the Collector CrashGuard reactivation interval in hours			
cltr_custom_shells	enum	Windows		NU
	Indicates whether the Collector reports user logon events and user interactions in virtualized and embedded (kiosk mode) environments			
cltr_data_channel_protocol	enum	Windows	macOS	NU
	Specifies if the Collector data is sent over TCP or UDP			
cltr_dns_res_preference	enum	Windows		NU
	Indicates the DNS resolution preference for Collector in terms of IP protocol version on the device			
cltr_engage_service_status	enum	Windows	macOS	NU
	Indicates whether Engage is enabled or disabled			
cltr_freezes_monitoring	enum	Windows		NU
	Indicates whether the Collector is monitoring for unresponsive applications on the device			
cltr_installs_scan_interval	integer	Windows		NU
	Indicates the interval, in hours, after which the Collector checks for newly installed packages and updates			
cltr_is_visible	enum	Windows		NU

	Indicates whether Collector is hidden in the "Add or Remove Programs"			
cltr_log_level	enum	Windows	macOS	NU
	Indicates the Collector log level			
cltr_max_segment_size	integer	Windows		NU
	Indicates the maximum segment size of packets sent by Collector			
cltr_ra_execution_policy	enum	Windows		NU
	Indicates the Powershell script execution policy			
cltr_smb_print_mon_status	enum	Windows		NU
	Indicates whether SMB printing monitoring is enabled or disabled			
cltr_string_tag	string	Windows	macOS	NU
	Indicates the Collector string tag			
cltr_web_mon_status	enum	Windows		NU
	Indicates whether Web & Cloud monitoring is enabled or disabled			
collector_distinguished_name	string	Windows		NU
	Indicates the distinguished name (DN) as seen: • For Windows: In Active Directory (AD). if no connection with AD is set up, a '-' is displayed; • For Mobile: In the Exchange ActiveSync server Note that this DN is reported by the Collector.			
collector_installation_log	string	Windows		NU
	Link to the last Nexthink Collector installation error log			
collector_package_target_version	version	Windows	macOS	NU
	Indicates the Collector package version that is targeted.			
collector_print_monitoring_status	enum	Windows		NU
	Indicates whether the Collector printing monitoring is enabled or disabled			
collector_status	enum	Windows	macOS	NU
	Indicates the status of the Nexthink Collector package installed on the device: • unmanaged: the Collector is not automatically updated • up-to-date: the Collector is up-to-date • outdated: a newer Collector version is available.			
collector_tag	integer	Windows		
	Collector installation tag			
collector_update_status	enum	Windows		
	Current status of Nexthink Collector Updater			
collector_version	version	Windows	macOS	
	Version number of Nexthink Collector installation			
cpu_frequency	mhz	Windows	macOS	NU
	CPU frequency			
cpu_model	string	Windows	macOS	NU
	CPU model			
database_usage	permill	Windows	macOS	
	Percentage of the database used by information related with the device			
device_encryption_required	boolean			NU
	Indicates whether device encryption is required.			
device_manufacturer	string	Windows	macOS	NU
	Indicates the device manufacturer.			

device_model	string	Windows	macOS	NU
	Indicates the model of the device.			
device_password_required	boolean			NU
	Indicates whether a password is required on the device.			
device_product_id	string	Windows	macOS	NU
	Device product ID			
device_product_version	string	Windows	macOS	NU
	Device product version			
device_serial_number	string	Windows	macOS	NU
	Indicates the device serial number.			
device_type	enum	Windows	macOS	
	Type of device (desktop, laptop, server, mobile)			
device_uid	md5	Windows	macOS	
	Indicates the universally unique identifier (based on Engine name and device ID)			
device_uuid	string	Windows	macOS	
	Indicates the device universally unique identifier (UUID)			
directory_service_site	string	Windows		NU
	Site (or location) of an Active Directory (AD) service			
disks_manufacturers	string	Windows		
	Hard disks manufacturers			
disks_smart_index	percent	Windows		NU
	Lowest S.M.A.R.T. index of installed hard disks (index is based on S.M.A.R.T. attributes)			
distinguished_name	string	Windows		NU
	Indicates the distinguished name (DN) as seen: • For Windows: In Active Directory (AD). if no connection with AD is set up, a '-' is displayed; • For Mobile: In the Exchange ActiveSync server			
eas_access_state	enum			
	Indicates whether the device can access the Exchange ActiveSync server. The possible states are: • allowed: the device has access; • blocked: the device is blocked; • discovery: the device is temporary quarantined while it is being identified by the Exchange ActiveSync server; • quarantined: the device is waiting for Exchange ActiveSync administrator approval.			
eas_access_state_reason	enum			
	Indicates the reason for the device access state. The possible values are: • global: caused by the global access settings; • device rule: caused by a device access rule; • individual: caused by an individual exemption; • policy: caused by Exchange ActiveSync policy.			
eas_device_access_rule	string			
	Indicates the name of the access rule. An access rule allows, blocks or quarantines devices based on the device type, model, OS or user agent characteristics.			
eas_device_identity	string			
	Indicates the identity of the device in Exchange ActiveSync Server.			
eas_exemption	enum			
	Indicates whether a personal exemption is set for the device and its user. Possible values are: • none; • allow; • block.			

eas_policy_application_status	enum			
	Indicates whether the Exchange ActiveSync policy is applied or not. Possible values are: • not applied; • applied in full: the policy is applied (unless the field 'Allow non provisionable devices' value is 'yes'); • partially applied.			
eas_policy_name	string			
	Indicates the name of the Exchange ActiveSync policy applied to the user's mailbox.			
eas_policy_update	datetime			
	Indicates the last time the Exchange ActiveSync policy was updated on the device.			
email_attachment_enabled	boolean			NU
	Indicates whether attachments can be downloaded to the mobile device through the Exchange ActiveSync protocol.			
enforce_password_history	integer	Windows		NU
	Indicates the number of unique passwords that have to be associated with a user account before an old password can be reused.			
entity	string	Windows	macOS	
	Entity			
extended_logon_duration_baseline	millisecond	Windows		NU
	Extended logon duration baseline			
firewall_name	string	Windows		NU
	Name of the main firewall			
firewall_rtp	enum	Windows		
	Indicates whether the firewall real time protection (RTP) is active: • on: Indicates that RTP is active; • off: Indicates that either RTP is not active or no firewall has been detected; • unknown: Indicates that the information could not be retrieved; • N/A: This field is not available on this operating system; • '-': No data, incompatible collector version or the data is not yet available.			
first_seen	datetime	Windows	macOS	NU
	Indicates the first time when the activity of the device was recorded: • For Windows and Mac OS: The first time Collector reported activity; • For Mobile: The first time the device was reported with a successful synchronization.			
graphical_card_ram	byte	Windows		NU
	Amount of RAM of the graphical card with most RAM			
graphical_cards	string	Windows		
	Installed graphical cards			
group_name	string	Windows	macOS	NU
	Name of computer domain or workgroup			
guest_account_status	enum	Windows		
	Determines if the Guest account is enabled or disabled.			
hard_disks	string	Windows	macOS	NC
	List of all hard disks			
id	identifier	Windows	macOS	
	Unique device identifier			
internet_security_settings	enum	Windows		
	Internet security settings (ok, at risk or unknown)			
ip_addresses	ip_address	Windows	macOS	

	List of IP addresses for the device			
is_collector_distinguished_name_truncated	boolean	Windows		
	Flag indicating whether the collector DN is truncated or not			
is_directory_service_site_truncated	boolean	Windows		
	Flag indicating whether the DS site is truncated or not			
last_boot_duration	millisecond	Windows		NU
	Last boot time duration			
last_extended_logon_duration	millisecond	Windows		NU
	Last extended logon duration			
last_ip_address	ip_address	Windows	macOS	NU
	Last IP address assigned to the device			
last_known_connection_status	enum	Windows	macOS	NU
	Indicates the last known connection status of the device: • udp: the device successfully connected via UDP but not TCP. • tcp: the device successfully connected via TCP but not UDP. • udp_tcp: the device successfully connected via both UDP and TCP. • '-': Collector version is below V6.6.			
last_local_ip_address	ip_address	Windows	macOS	NU
	Last local IP address assigned to the device			
last_logged_on_user	string	Windows		NU
	Last logged on user			
last_logon_duration	millisecond	Windows		NU
	Last user logon duration			
last_logon_time	datetime	Windows		NU
	Last logon time			
last_seen	datetime	Windows	macOS	NU
	Indicates the last time that activity on the device was reported: • For Windows and Mac OS: The last time Collector reported activity through the UDP channel, • For Mobile: The last time the device successfully synchronized with the Mobile Bridge.			
last_seen_on_tcp	datetime	Windows	macOS	NU
	Indicates the last time that the device was successfully connected through the TCP channel. • '-': The Collector is an older version that does not support TCP.			
last_system_boot	datetime	Windows	macOS	NU
	Last boot time			
last_update	datetime	Windows	macOS	NU
	Indicates the last Collector update time.			
last_update_status	enum	Windows	macOS	NU
	Indicates the status of the last Collector update: • '-': the Collector was never updated • successful installation: the last Collector installation was successful • package download error: the Collector was not able to download the Collector package from Nexthink Appliance • package digital signature error: the Collector was not able to check the Collector package digital signature • device reboot required: the device needs to be rebooted to complete the Collector installation • package error: the Collector package installation has failed • internal error: the Collector package installation has failed for an unexpected reason.			
last_updater_request	datetime	Windows		NU
	Last time Nexthink Updater checked for updates			

last_windows_update	datetime	Windows		NU
	Time of last system Update			
local_administrators	string	Windows		
	Users and groups which are members of the Local Administrators group on the device.			
local_power_users	string	Windows		
	Users and groups which are members of the Local Powers Users group on the device.			
logical_cpu_number	integer	Windows	macOS	NU
	Indicates the number of cores multiplied by the number of threads that can run on each core through the use of hyperthreading.			
logical_drives	string	Windows	macOS	
	List of all logical drives			
mac_addresses	mac_address	Windows	macOS	
	List of MAC addresses for the device			
maximum_password_age	integer	Windows		NU
	Indicates the period in time (in days) during which the password can be used before the system requires the user to change it: • Windows: As set up in the group policy; • Mobile: As set up in security policies.			
membership_type	enum	Windows		
	Type of computer membership (domain/workgroup)			
minimum_password_age	integer	Windows		NU
	Period of time (in days) that a password must be used before the user can change it.			
minimum_password_length	integer	Windows		NU
	Least number of characters that a password for a user account may contain.			
monitor_models	string	Windows		
	Models of connected monitors			
monitor_resolutions	string	Windows		
	Screen resolutions of connected monitors			
monitors	string	Windows		
	Connected monitors			
monitors_serial_numbers	string	Windows		
	Serial numbers of connected monitors (ordered as in 'Monitors')			
name	string	Windows	macOS	
	Indicates the name of the device: • For Windows: NetBios Name; • For Mac OS: Computer name used on the network; • For Mobile: Composed by mailbox name and device friendly name.			
number_of_antispyware	enum	Windows		
	Number of antispyware detected: • unknown: Indicates that the information could not be retrieved; • N/A: This field is not available on this operating system; • '-': No data, incompatible collector version or the data is not yet available.			
number_of_antiviruses	enum	Windows		
	Number of antiviruses detected: • unknown: Indicates that the information could not be retrieved; • N/A: This field is not available on this operating system; • '-': No data, incompatible collector version or the data is not yet available.			
number_of_cores	integer	Windows	macOS	NU
	Number of cores			

number_of_cpus	integer	Windows	macOS	NU
	Number of CPUs			
number_of_days_since_first_seen	integer	Windows	macOS	NU
	Number of days since activity of the device was first recorded in the system.			
number_of_days_since_last_boot	integer	Windows	macOS	NU
	Number of days since last full boot			
number_of_days_since_last_eas_policy_update	integer			NU
	Indicates the number of days since the last Exchange ActiveSync policy update.			
number_of_days_since_last_logon	integer	Windows		NU
	Number of days since last logon			
number_of_days_since_last_seen	integer	Windows	macOS	NU
	Indicates the number of days since the last time the device was seen by Nexthink. The field is updated whenever device activity is detected: • For Windows and Mac OS: seen through the UDP channel, • For Mobile: seen through the Mobile Bridge.			
number_of_days_since_last_seen_on_tcp	integer	Windows		NU
	Indicates the number of days since the last time the device was successfully connected through the TCP channel. '-': The Collector is an older version that does not support TCP.			
number_of_days_since_last_windows_update	integer	Windows		NU
	Number of days since last system Update			
number_of_firewalls	enum	Windows		
	Number of firewalls detected: • unknown: Indicates that the information could not be retrieved; • N/A: This field is not available on this operating system; • '-': No data, incompatible collector version or the data is not yet available.			
number_of_graphical_cards	integer	Windows		
	Number of installed graphical cards			
number_of_monitors	integer	Windows	macOS	
	Number of connected monitors			
os_architecture	enum	Windows	macOS	
	Architecture of device operating system (x86/x64/ARM64)			
os_build	version	Windows		
	Indicates the build number of the operating system.			
os_version_and_architecture	string	Windows	macOS	NU
	Indicates name, version and architecture (when applicable) of the operating system. • unknown: the OS version could not be retrieved or it could not be mapped to a recognized value.			
password_complexity_requirements	enum	Windows		
	Indicates whether password complexity is required: • Windows: The password must meet complexity requirements as defined in the group policy; • Mobile: No simple passwords are allowed or a minimum password length is set, as defined in the security policy.			
platform	enum	Windows	macOS	

	Indicates the platform of the device. A platform is a set of operating system families on which the same objects, activities, events and properties can be retrieved. The possible values are: • Windows; • Mac OS; • Mobile.			
privileges_of_last_logged_on_users	enum	Windows		
	Privileges of the last logged on user (user, power user, administrator)			
sd_card_encryption_required	boolean			NU
	Indicates whether SD card encryption is required.			
sid	sid	Windows		NU
	Windows security identifier for the device.			
storage_policy	enum	Windows	macOS	
	Indicates the event storage policy for the device. Possible values are: • all: web requests, connections and executions are stored • connections and executions; • executions; • none: no activity is recorded; • remove: The device will be removed from Engine during the next cleanup, as long as it is no longer sending data; Note that available events depend on the device platform.			
system_drive_capacity	byte	Windows	macOS	
	Total capacity of system drive			
system_drive_free_space	byte	Windows	macOS	
	Total available free space on system drive			
system_drive_usage	percent	Windows	macOS	NU
	Use percentage of system drive			
total_active_days	day	Windows	macOS	
	Total number of days the device was active.			
total_drive_capacity	byte	Windows	macOS	
	Total capacity of all drives			
total_drive_free_space	byte	Windows	macOS	
	Total free space on all drives			
total_drive_usage	permill	Windows	macOS	NU
	Total use percentage of all drives			
total_nonsystem_drive_capacity	byte	Windows	macOS	
	Total capacity of all non-system drives			
total_nonsystem_drive_free_space	byte	Windows	macOS	
	Total free space on all non-system drives			
total_nonsystem_drive_usage	percent	Windows	macOS	NU
	Total use percentage of all non-system drives			
total_ram	byte	Windows	macOS	NU
	Total amount of RAM			
updater_error	string	Windows		
	Last Nexthink Collector Updater error			
updater_version	version	Windows		
	Nexthink Collector Updater version			

upgrade_group	enum	Windows	macOS	NU
	Indicates the update group of Nexthink Collector: • manual: the Collector is manually updated • pilot: the Collector is updated as part of the pilot group • main: the Collector is updated as part of the main group.			
user_account_control_status	enum	Windows		
	User account control status (ok, at risk or unknown)			
windows_license_key	string	Windows		NU
	Windows license key			
windows_updates_status	enum	Windows		
	Windows update status (ok, at risk or unknown)			
wmi_status	enum	Windows		
	Windows WMI service status (ok, failure)			

domain

A domain is a domain name e.g. http://www.nexthink.com.

Name	Type	Operating systems		Properties
database_usage	permill	Windows	macOS	
	Percentage of the database used by information related with the domain			
domain_category	string	Windows	macOS	SE
	Indicates the category of the domain: • '-': Not yet tagged or internal domain.			
first_seen	datetime	Windows	macOS	NU
	The first time the domain has been seen.			
hosting_country	string	Windows	macOS	SE
	Indicates in which country the domain is hosted: • '-': Not yet tagged, internal domain or not known by Nexthink Library.			
hostname	string	Windows	macOS	NU
	The hostname of the fully qualified domain name			
id	identifier	Windows	macOS	
	Unique domain identifier			
internal_domain	boolean	Windows	macOS	
	Indicates whether the domain is considered internal: • yes: The domain is not reported to Nexthink Library and subdomains are not compressed using the '*' pattern; • no: The domain is reported to the Nexthink Library (if the license includes the Security module); complex subdomains are compressed using the '*' pattern.			
last_seen	datetime	Windows	macOS	NU
	The last time the domain has been seen.			
name	string	Windows	macOS	
	The fully qualified domain name			
protocol	enum	Windows	macOS	
	Protocols used in web requests (HTTP, TLS, HTTP/TLS)			
response_size	byte	Windows	macOS	
	Total web incoming traffic			
storage	enum	Windows	macOS	

	Event storage policy for the domain (web request or none)			
threat_level	enum	Windows	macOS	SE
	Indicates the threat level of the domain: • '-': Not yet tagged or internal domain; • none detected: No known threat; • low: low threat; • intermediate: Intermediate threat; • high: High threat.			

executable

An application is an executable program e.g. 'winword.exe'.

Name	Type	Operating systems		Properties
application_company	string	Windows	macOS	
	Application company			
application_name	string	Windows	macOS	
	Application name			
database_usage	permill	Windows	macOS	
	Percentage of the database used by information related with the executable.			
description	string	Windows		
	Executable description			
first_seen	datetime	Windows	macOS	NU
	First time activity of the executable was recorded on any device.			
id	identifier	Windows	macOS	
	Unique executable identifier			
known_packages	string	Windows	macOS	
	List of packages known to contain the executable. This list is not exhaustive: The presence of a package does not necessarily imply that on a given device the executable was installed through that package.			
last_seen	datetime	Windows	macOS	NU
	Last time activity of the executable was recorded on any device.			
name	string	Windows	macOS	
	Executable name			
platform	enum	Windows	macOS	
	The platform (operating system family) on which the executable is running.			
storage_policy	enum	Windows	macOS	
	Indicates the event storage policy for the executable. Possible values are: • all: web requests, connections and executions are stored; • connections and executions; • executions; • none: no activity is recorded.			
total_active_days	day	Windows	macOS	
	Total number of days the executable was active.			

package

A package is a software package (programs or updates).

Name	Type	Operating systems		Properties
first_installation	datetime	Windows		NU

	Time of first installation			
first_seen	datetime	Windows	macOS	NU
	The first time the package has been seen.			
id	identifier	Windows	macOS	
	Unique package identifier			
name	string	Windows	macOS	
	Package name			
number_of_updates	integer	Windows		
	Number of updates (for programs)			
platform	enum	Windows	macOS	
	The platform (operating system family) on which the package is installed.			
program	string	Windows	macOS	
	Package program			
publisher	string	Windows	macOS	NU
	Package publisher			
status	enum	Windows	macOS	
	Package status (installed/removed)			
type	enum	Windows	macOS	
	Package type (program/update)			
version	string	Windows	macOS	NU
	Package version			
windows_7_32bit_compatibility	string	Windows		DE
	Indicates the Windows 7 (32-bit) compatibility of the package: • '-': Not yet tagged; • No information available: Not known by Nexthink Library; • Compatible: Compatible with Windows 7.			
windows_7_64bit_compatibility	string	Windows		DE
	Indicates the Windows 7 (64-bit) compatibility of the package: • '-': Not yet tagged; • No information available: Not known by Nexthink Library; • Compatible: Compatible with Windows 7.			

port

A port is a TCP or UDP connection port.

Name	Type	Operating systems		Properties
first_seen	datetime	Windows	macOS	NU
	First time activity of the port was recorded on any device.			
id	identifier	Windows	macOS	
	Unique port identifier			
last_seen	datetime	Windows	macOS	NU
	Last time activity of the port was recorded on any device.			
port_number	integer	Windows	macOS	
	Port number			
port_type	enum	Windows	macOS	
	Port type (tcp, udp, tcp port scan, udp port scan)			

port_value	port	Windows	macOS	
	Port value for tagging			

printer

A printer is an installed printer (local, network, shared or virtual).

Name	Type	Operating systems		Properties
first_seen	datetime	Windows		NU
	First time activity of the printer was recorded on any device.			
host_name	string	Windows		
	Host name			
id	identifier	Windows		
	Unique print identifier			
last_seen	datetime	Windows		NU
	Last time activity of the printer was recorded on any device.			
location	string	Windows		NU
	Printer location			
model	string	Windows		
	Printer model			
name	string	Windows		
	Printer name			
real_name	string	Windows		
	Most frequently seen display name			
type	enum	Windows		
	Printer type (local/remote)			

service

A service represents an IT service in your organization, such as the mail service or the directory service. Services are either based on TCP connections (for Windows and Mac devices) or on web requests (for Windows devices only).

Name	Type	Operating systems		Properties
id	integer	Windows	macOS	
	Unique service identifier			
name	string	Windows	macOS	
	Service name			
status	enum	Windows	macOS	
	Service status (active, error)			
type	enum	Windows	macOS	
	Type of service (network, web)			

url_path

A url_path is a URL path after the domain name e.g. [http://www.nexthink.com]/awards/.

Name	Type	Operating systems		Properties
id	identifier	Windows	macOS	
	Unique url path identifier			

path	string	Windows	macOS	
	The URL path			

user

A user is an object that represents an individual account in a device (local user) or in a group of devices (domain user). The account may identify a physical user or a system user.

Name	Type	Operating systems		Properties
country	string	Windows	macOS	
	Country of user as listed in active directory			
database_usage	permill	Windows	macOS	
	Percentage of the database used by information related with the binary			
department	string	Windows	macOS	
	User department as listed in active directory			
distinguished_name	string	Windows	macOS	NU
	Active directory distinguished name (DN)			
first_seen	datetime	Windows	macOS	NU
	First time activity of the user was recorded on any device.			
full_name	string	Windows	macOS	NU
	Full user name as listed in active directory			
id	identifier	Windows	macOS	
	Unique user identifier			
job_title	string	Windows	macOS	NU
	Job title as listed in active directory			
last_seen	datetime	Windows	macOS	NU
	Last time activity of the user was recorded on any device.			
locality	string	Windows	macOS	
	Locality of user as listed in active directory			
location	string	Windows	macOS	
	Location of user as listed in active directory			
name	string	Windows	macOS	
	User logon name			
number_of_days_since_last_seen	integer	Windows	macOS	NU
	Indicates the number of days since the last time the user was seen by Nexthink. The field is updated whenever user activity is detected.			
org_unit	string	Windows	macOS	
	Organisational unit of User as listed in active directory			
seen_on_mac_os	boolean	Windows	macOS	
	Indicates if the user has been seen on a Mac device.			
seen_on_mobile	boolean	Windows	macOS	
	Indicates if the user has been seen on a Mobile device.			
seen_on_windows	boolean	Windows	macOS	
	Indicates if the user has been seen on a Windows device.			
sid	sid	Windows	macOS	NU

	Indicates the Windows security identifier for the user. For Mac OS, '-' means that the user is not in Active Directory.			
total_active_days	day	Windows	macOS	
	Total number of days the user was active.			
type	enum	Windows	macOS	
	Type of user (local/domain/system)			
user_uid	md5	Windows	macOS	
	Indicates the universally unique identifier			

Events

connection

A connection is a TCP connection or a UDP packet. Several identical TCP connections or UDP packets are merged when in close succession.

Name	Type	Operating systems		Properties
cardinality	integer	Windows	macOS	
	Number of underlying connections, consolidated over time			
destination_ip_address	ip_address	Windows	macOS	
	IP address of the connection destination			
device_ip_address	ip_address	Windows	macOS	
	IP address of the connection source			
duration	millisecond	Windows	macOS	
	The time between the start of the first connection and the end of the last underlying connection.			
end_time	datetime	Windows	macOS	
	Connection end time, corresponding to the moment when the last underlying connection was closed.			
id	identifier	Windows	macOS	
	Unique connection identifier			
incoming_bitrate	bps	Windows	macOS	NU
	Average incoming bitrate of all underlying connections, consolidated over time			
incoming_traffic	byte	Windows	macOS	
	Incoming traffic			
network_interface_iana_code	string	Windows	macOS	
	(beta) Indicates the network interface IANA code.			
network_interface_index	integer	Windows	macOS	
	(beta) Indicates the network interface index.			
network_interface_type	enum	Windows	macOS	
	(beta) Indicates the network interface type. Possible values are: • wifi • ethernet • mobile • other • unknown: the Collector is not supporting interface type.			
network_response_time	microsecond	Windows	macOS	
	TCP connection establishment time			
outgoing_bitrate	bps	Windows	macOS	NU
	Average outgoing bitrate of all underlying connections, consolidated over time			
outgoing_traffic	byte	Windows	macOS	

	Outgoing traffic			
start_time	datetime	Windows	macOS	
	Connection start time			
status	enum	Windows	macOS	
	Status of the connection (established, rejected, no service, no host, closed)			
type	enum	Windows	macOS	
	Type of the connection (tcp, udp)			

device_activity

A device_activity is a device activity (boot or activity).

Name	Type	Operating systems		Properties
boot_type	enum	Windows	macOS	NU
	Boot type of the boot activity			
duration	millisecond	Windows	macOS	
	Boot duration (timed between kernel start and launch of 'logonui.exe' process) or online duration			
id	identifier	Windows	macOS	
	Boot event identifier			
time	datetime	Windows	macOS	
	Time of boot			
type	enum	Windows	macOS	
	Activity event information			

device_error

A device_error is a critical system error (system crash, hard reset, or disk error).

Name	Type	Operating systems		Properties
error_code	integer	Windows	macOS	
	Error code			
error_label	string	Windows	macOS	
	Error label			
id	identifier	Windows	macOS	
	Problem identifier			
start_time	datetime	Windows	macOS	
	Time of error			
type	enum	Windows	macOS	
	Indicates the device error type, with the following possible values: • system crash: Windows bluescreen or macOS kernel panic; • hard reset: the device was abruptly stopped and then rebooted. It might be caused by pressing the reset button, a power failure or a crash; • SMART disk failure: a disk error was detected on a disk with SMART technology.			

device_performance

A device_performance reports the average IOPS, CPU and memory of a device for one hour.

Name	Type	Operating systems		Properties
average_cpu_usage	permill	Windows		

	Average CPU usage on the period			
average_memory_usage	byte	Windows		
	Average memory usage on the period			
cpu_queue_length	integer	Windows		
	Average CPU queue length on the period			
duration	millisecond	Windows		
	Total report duration			
end_time	datetime	Windows		
	Report end time			
id	identifier	Windows		
	Unique report identifier			
normalized_cpu_usage	permill	Windows		
	Average CPU usage on the period normalized by the available logical CPUs			
read_operations	integer	Windows		NU
	Total disk read operations accumulated during the period			
start_time	datetime	Windows		
	Start time			
write_operations	integer	Windows		NU
	Total disk write operations accumulated during the period			

device_warning

A device_warning is a peak in device resource usage (CPU, memory or I/O).

Name	Type	Operating systems		Properties
duration	millisecond	Windows	macOS	
	Performance event duration			
end_time	datetime	Windows	macOS	
	Performance event end time			
id	identifier	Windows	macOS	
	Unique performance event identifier			
info	string	Windows	macOS	
	Performance event information			
start_time	datetime	Windows	macOS	
	Performance event start time			
type	enum	Windows	macOS	
	Type of the device warning, one of: • 'high overall cpu usage' • 'high cpu usage' (deprecated) • 'high io usage' • 'high memory usage' • 'high number of page faults'.			
value	percent	Windows	macOS	
	Performance percentage			
warning_duration	millisecond	Windows	macOS	
	Indicates the duration of the warning. This duration can be shorter than the event duration when the warning is not continuous.			

execution

An execution is a process executing on a device. Several executions of the same process are merged when in close succession.

Name	Type	Operating systems		Properties
average_memory_usage	byte	Windows	macOS	
	Average memory usage per execution			
binary_path	path	Windows	macOS	
	Executed binary path			
cardinality	integer	Windows	macOS	
	Number of underlying processes, consolidated over time			
duration	millisecond	Windows	macOS	
	Total execution duration			
end_time	datetime	Windows	macOS	
	Execution end time			
focus_time	millisecond	Windows	macOS	NU
	Focus time			
id	identifier	Windows	macOS	
	Unique execution identifier			
incoming_tcp_traffic	byte	Windows	macOS	
	Incoming TCP traffic			
incoming_udp_traffic	byte	Windows	macOS	
	Incoming UDP traffic			
memory_usage	byte	Windows	macOS	
	Average memory usage			
outgoing_tcp_traffic	byte	Windows	macOS	
	Outgoing TCP traffic			
outgoing_udp_traffic	byte	Windows	macOS	
	Outgoing UDP traffic			
privilege_level	enum	Windows	macOS	
	Privilege level of the execution (user, power user, administrator)			
start_time	datetime	Windows	macOS	
	Execution start time			
startup_duration	millisecond	Windows		NU
	Startup duration			
status	enum	Windows	macOS	
	Status of the execution (started, stopped)			
total_cpu_time	millisecond	Windows	macOS	
	Total CPU time			

execution_error

An execution_error is an application error (crash or not responding).

Name	Type	Operating systems		Properties
id	identifier	Windows	macOS	
	Error identifier			

info	string	Windows	macOS	
	Error event information			
time	datetime	Windows	macOS	
	Time of error			
type	enum	Windows	macOS	
	Type of the execution error (application not responding, crash)			

execution_warning

An execution_warning is a peak in application resource usage (CPU or memory).

Name	Type	Operating systems		Properties
duration	millisecond	Windows	macOS	
	Performance event duration			
end_time	datetime	Windows	macOS	
	Performance event end time			
id	identifier	Windows	macOS	
	Unique performance event identifier			
info	string	Windows	macOS	
	Performance event information			
start_time	datetime	Windows	macOS	
	Performance event start time			
type	enum	Windows	macOS	
	Type of the execution warning (high cpu usage, high memory usage)			
value	percent	Windows	macOS	
	Performance percentage			
warning_duration	millisecond	Windows	macOS	
	Indicates the duration of the warning. This duration can be shorter than the event duration when the warning is not continuous.			

installation

An installation is the installation or uninstallation of a software package (programs or updates).

Name	Type	Operating systems		Properties
id	identifier	Windows	macOS	
	Unique deployment identifier			
time	datetime	Windows	macOS	
	Installation start time			
type	enum	Windows	macOS	
	Type of operation (installation, uninstallation)			

network_scan

A network scan is a sequence of failed TCP connections or UDP packets made to the same port to more than 50 destinations within a few seconds.

Name	Type	Operating systems		Properties
cardinality	integer	Windows	macOS	

	Number of underlying connections, consolidated over time			
device_ip_address	ip_address	Windows	macOS	
	IP address of the connection source			
duration	millisecond	Windows	macOS	
	The time between the start of the first connection and end of the last underlying connection			
end_time	datetime	Windows	macOS	
	Scanning end time, corresponding to the moment when the last underlying connection was closed.			
id	identifier	Windows	macOS	
	Unique scanning identifier			
network	ip_network	Windows	macOS	
	Minimum IP network including all scanned destinations			
start_time	datetime	Windows	macOS	
	Scanning start time			
status	enum	Windows	macOS	
	Status of the Scanning (established, closed)			
type	enum	Windows	macOS	
	Type of the port scanning (tcp, udp)			

port_scan

A port scan is a sequence of failed TCP connections or UDP packets made to the same destination to more than 50 ports within a few seconds.

Name	Type	Operating systems		Properties
cardinality	integer	Windows	macOS	
	Number of underlying connections, consolidated over time			
destination_ip_address	ip_address	Windows	macOS	
	IP address of the scanned destination			
device_ip_address	ip_address	Windows	macOS	
	IP address of the connection source			
duration	millisecond	Windows	macOS	
	The time between the start of the first connection and end of the last underlying connection.			
end_time	datetime	Windows	macOS	
	Scanning end time, corresponding to the moment when the last underlying connection was closed.			
first_scanned_port	port	Windows	macOS	
	First port scanning			
id	identifier	Windows	macOS	
	Unique scanning identifier			
last_scanned_port	port	Windows	macOS	
	Last port scanning			
start_time	datetime	Windows	macOS	
	Scanning start time			
status	enum	Windows	macOS	
	Status of the Scanning (established, closed)			
type	enum	Windows	macOS	
	Type of the port scanning (tcp, udp)			

printout

A printout is a print job processed by a printer.

Name	Type	Operating systems		Properties
color_print	boolean	Windows		
	Color print			
document_type	string	Windows		
	Type of printed document			
duplex	boolean	Windows		
	Indicates whether the pages are printed on both sides of the sheet.			
id	identifier	Windows		
	Unique print job identifier			
number_of_printed_pages	integer	Windows		NU
	Number of printed pages			
page_size	string	Windows		
	Paper size for printed pages			
print_quality	enum	Windows		
	Print quality			
size	byte	Windows		NU
	Print job size in bytes			
status	enum	Windows		
	Print job status(success, error, timeout)			
time	datetime	Windows		
	Print job time			

session_performance

Sessions of a user logged on a device.

Name	Type	Operating systems		Properties
cardinality	integer	Windows		
	Number of underlaying sessions consolidated in a bucket period			
citrix_rtt	millisecond	Windows		NU
	Citrix RTT			
client_ip	ip_address	Windows		
	Client IP			
duration	millisecond	Windows		
	Session performance bucket period duration			
end_time	datetime	Windows		
	Session performance bucket end time			
id	identifier	Windows		
	Unique session performance identifier			
session_network_latency	millisecond	Windows		NU
	Session network latency			
session_protocol	enum	Windows		NU

	User input delay			
start_time	datetime	Windows		
	Execution start time			

user_activity

A user_activity is a user activity (logon or interactive activity).

Name	Type	Operating systems		Properties
duration	millisecond	Windows	macOS	
	Indicates the time between the user logging on and the desktop being shown.			
id	identifier	Windows	macOS	
	User logon event identifier			
real_duration	millisecond	Windows	macOS	
	Indicates the time between the user logging on and the device being ready to use. Desktops and laptops are considered fully functional once the CPU usage drops below 15% and the disk usage drops below 80%, and servers once the CPU usage of all processes belonging to the corresponding user drops below 15%.			
time	datetime	Windows	macOS	
	Time of user logon			
type	enum	Windows	macOS	
	Activity event information			

web_request

A web_request is an HTTP or TLS request.

Name	Type	Operating systems		Properties
cardinality	integer	Windows	macOS	
	Number of underlying web requests, consolidated over time			
connections_duration	millisecond	Windows	macOS	
	The time between start of the first connection and end of the last underlying connection			
end_time	datetime	Windows	macOS	
	Web request end time, corresponding to the moment when the last underlying TCP connection was closed.			
http_status	http_status_code	Windows	macOS	NU
	HTTP response status code			
id	identifier	Windows	macOS	
	Unique request identifier			
incoming_traffic	byte	Windows	macOS	
	Incoming web traffic of all underlying web requests, consolidated over time			
network_response_time	microsecond	Windows	macOS	
	Average TCP connection establishment time of all underlying connections, consolidated over time			
outgoing_traffic	byte	Windows	macOS	
	Outgoing web traffic of all underlying web requests, consolidated over time			
protocol	enum	Windows	macOS	
	Web request protocol (HTTP, TLS)			
protocol_version	enum	Windows	macOS	
	Web request protocol version			
service_related	boolean	Windows	macOS	

	Indicates whether the web request is related to a configured service: • yes: These requests are always visible by all users; • no: Depending on the privacy settings, requests not related to a service might not be visible by everyone.			
start_time	datetime	Windows	macOS	
	Web request start time			
web_request_duration	millisecond	Windows	macOS	
	Average time between request and last response byte of all underlying requests, consolidated over time			

Relationships

A relationship is a link between object and event tables and is specified in a **with** clause.

connection

- device
- user
- binary
- executable
- application
- destination
- port
- service

device_activity

- device

device_error

- device

device_performance

- device

device_warning

- device

execution

- device
- user
- binary
- executable
- application

execution_error

- device
- user
- binary

- executable
- application

execution_warning

- device
- user
- binary
- executable
- application

installation

- device
- package

network_scan

- device
- user
- binary
- executable
- application
- port

port_scan

- device
- user
- binary
- executable
- application
- destination

printout

- device
- user
- printer

session_performance

- device
- user

user_activity

- device
- user

web_request

- device
- user
- binary
- executable
- application
- destination
- port
- domain
- url_path
- service

package

- device
- package

Aggregates

connection

Name	Type	Operating systems		Properties
number_of_devices	integer	Windows	macOS	FP
	Number of devices			
number_of_users	integer	Windows	macOS	FP
	Number of users			
number_of_applications	integer	Windows	macOS	FP
	Number of applications			
number_of_executables	integer	Windows	macOS	FP
	Number of executables			
number_of_binaries	integer	Windows	macOS	FP
	Number of binaries			
number_of_destinations	integer	Windows	macOS	
	Number of destinations			
number_of_ports	integer	Windows	macOS	
	Number of ports			
number_of_connections	integer	Windows	macOS	
	Number of connections			
cumulated_connection_duration	millisecond	Windows	macOS	
	Cumulated duration of TCP connections			
activity_start_time	datetime	Windows	macOS	NU
	Start time of investigated activity			
activity_stop_time	datetime	Windows	macOS	NU
	Stop time of investigated activity			
incoming_traffic	byte	Windows	macOS	NU
	Total network incoming traffic			

outgoing_traffic	byte	Windows	macOS	NU
	Total network outgoing traffic			
average_network_response_time	microsecond	Windows	macOS	
	Average TCP connection establishment time			
successful_connections_ratio	permill	Windows	macOS	NU
	Percentage of successful TCP connections			
network_availability_level	availability_level	Windows	macOS	NU
	Graded ratio of successful TCP connections (high, medium, low)			
average_incoming_bitrate	bps	Windows	macOS	NU
	Average incoming network bitrate			
average_outgoing_bitrate	bps	Windows	macOS	NU
	Average outgoing network bitrate			
highest_local_privilege_reached	privileges_level	Windows	macOS	NU
	Highest local privilege level reached for executions (user, power user, administrator)			
number_of_events	integer	Windows	macOS	NU
	Number of events			
incoming_network_traffic_per_device	byte	Windows	macOS	NU
	Device average incoming network traffic			
outgoing_network_traffic_per_device	byte	Windows	macOS	NU
	Device average outgoing network traffic			
total_network_traffic	byte	Windows	macOS	NU
	Network traffic			

device_activity

Name	Type	Operating systems		Properties
number_of_devices	integer	Windows	macOS	
	Number of devices			
average_boot_duration	millisecond	Windows		NU
	Average boot duration			
average_logon_duration	millisecond	Windows		NU
	Average user logon duration			
average_extended_logon_duration	millisecond	Windows		NU
	Average extended logon duration			
number_of_boots	integer	Windows	macOS	NU
	Number of boots			
activity_start_time	datetime	Windows	macOS	NU
	Start time of investigated activity			
activity_stop_time	datetime	Windows	macOS	NU
	Stop time of investigated activity			
uptime	millisecond	Windows	macOS	NU

	Amount of time the machine has been running			
cumulated_interaction_duration	millisecond	Windows	macOS	NU
	Cumulated time with user interaction (mouse or keyboard events)			
number_of_events	integer	Windows	macOS	NU
	Number of events			

device_error

Name	Type	Operating systems		Properties
number_of_devices	integer	Windows	macOS	
	Number of devices			
number_of_errors	integer	Windows	macOS	
	Number of system errors			
activity_start_time	datetime	Windows	macOS	NU
	Start time of investigated activity			
activity_stop_time	datetime	Windows	macOS	NU
	Stop time of investigated activity			
number_of_events	integer	Windows	macOS	NU
	Number of events			

device_performance

Name	Type	Operating systems		Properties
average_read_operations	integer	Windows		
	Average read IPOS			
average_write_operations	integer	Windows		
	Average write IPOS			
average_cpu_queue_length	integer	Windows		
	Average CPU queue length			
average_memory_usage	byte	Windows		NU
	Average memory usage			
average_cpu_usage	percent	Windows		
	Average CPU usage			
average_normalized_cpu_usage	percent	Windows		
	Average normalized CPU usage			

device_warning

Name	Type	Operating systems		Properties
number_of_devices	integer	Windows	macOS	
	Number of devices			
number_of_warnings	integer	Windows	macOS	
	Number of warnings			
cumulated_warning_duration	millisecond	Windows	macOS	NU

	Cumulated duration of the warning events			
activity_start_time	datetime	Windows	macOS	NU
	Start time of investigated activity			
activity_stop_time	datetime	Windows	macOS	NU
	Stop time of investigated activity			
number_of_events	integer	Windows	macOS	NU
	Number of events			
high_device_overall_cpu_time_ratio	permill	Windows	macOS	NU
	Indicates the ratio between the time the device is in high overall CPU usage and its uptime.			
high_device_memory_time_ratio	permill	Windows	macOS	NU
	Indicates the ratio between the time the device is in high memory usage and its uptime.			
high_device_io_throughput_time_ratio	permill	Windows		NU
	Indicates the ratio between the time the device is in high IO throughput and its uptime.			
high_device_page_faults_time_ratio	permill	Windows		NU
	Indicates the ratio between the time the device is in high page faults and its uptime.			

execution

Name	Type	Operating systems		Properties
number_of_devices	integer	Windows	macOS	FP
	Number of devices			
number_of_users	integer	Windows	macOS	FP
	Number of users			
number_of_applications	integer	Windows	macOS	FP
	Number of applications			
number_of_executables	integer	Windows	macOS	FP
	Number of executables			
number_of_binaries	integer	Windows	macOS	FP
	Number of binaries			
number_of_executions	integer	Windows	macOS	
	Number of executions			
cumulated_execution_duration	millisecond	Windows	macOS	NU
	Cumulated duration of executions			
activity_start_time	datetime	Windows	macOS	NU
	Start time of investigated activity			
activity_stop_time	datetime	Windows	macOS	NU
	Stop time of investigated activity			
incoming_traffic	byte	Windows	macOS	NU
	Total network incoming traffic			
outgoing_traffic	byte	Windows	macOS	NU
	Total network outgoing traffic			

highest_local_privilege_reached	privileges_level	Windows	macOS	NU
	Highest local privilege level reached for executions (user, power user, administrator)			
number_of_events	integer	Windows	macOS	NU
	Number of events			
average_memory_usage_per_execution	byte	Windows	macOS	NU
	Average memory usage per execution			
memory_usage	byte	Windows	macOS	NU
	Memory usage			
focus_time	millisecond	Windows	macOS	NU
	Focus time			
cpu_usage_ratio	permill	Windows	macOS	NU
	Average CPU usage			
total_cpu_time	millisecond	Windows	macOS	NU
	Total CPU time			
average_process_start_time	millisecond	Windows		NU
	Average process start time			
incoming_network_traffic_per_device	byte	Windows	macOS	NU
	Device average incoming network traffic			
outgoing_network_traffic_per_device	byte	Windows	macOS	NU
	Device average outgoing network traffic			
total_network_traffic	byte	Windows	macOS	NU
	Network traffic			

execution_error

Name	Type	Operating systems		Properties
application_not_responding_event_ratio	permill	Windows	macOS	NU
	Application not responding event ratio			
application_crash_ratio	permill	Windows	macOS	NU
	Application crash ratio			
number_of_application_not_responding_events	integer	Windows	macOS	
	Number of application not responding events			
number_of_application_crashes	integer	Windows	macOS	
	Number of application crashes			
number_of_devices	integer	Windows	macOS	
	Number of devices			
number_of_users	integer	Windows	macOS	
	Number of users			
number_of_applications	integer	Windows	macOS	
	Number of applications			

number_of_executables	integer	Windows	macOS	
	Number of executables			
number_of_binaries	integer	Windows	macOS	
	Number of binaries			
number_of_errors	integer	Windows	macOS	
	Number of errors			
activity_start_time	datetime	Windows	macOS	NU
	Start time of investigated activity			
activity_stop_time	datetime	Windows	macOS	NU
	Stop time of investigated activity			
number_of_events	integer	Windows	macOS	NU
	Number of events			

execution_warning

Name	Type	Operating systems		Properties
number_of_devices	integer	Windows	macOS	
	Number of devices			
number_of_users	integer	Windows	macOS	
	Number of users			
number_of_applications	integer	Windows	macOS	
	Number of applications			
number_of_executables	integer	Windows	macOS	
	Number of executables			
number_of_binaries	integer	Windows	macOS	
	Number of binaries			
number_of_warnings	integer	Windows	macOS	
	Number of warnings			
cumulated_warning_duration	millisecond	Windows	macOS	NU
	Cumulated duration of the warning events			
activity_start_time	datetime	Windows	macOS	NU
	Start time of investigated activity			
activity_stop_time	datetime	Windows	macOS	NU
	Stop time of investigated activity			
number_of_events	integer	Windows	macOS	NU
	Number of events			
high_application_thread_cpu_time_ratio	permill	Windows	macOS	NU
	High application thread CPU time ratio			

installation

Name	Type	Operating systems		Properties
number_of_packages	integer	Windows	macOS	
	Number of packages			

number_of_devices	integer	Windows	macOS	
	Number of devices			
activity_start_time	datetime	Windows	macOS	NU
	Start time of investigated activity			
activity_stop_time	datetime	Windows	macOS	NU
	Stop time of investigated activity			
number_of_installations	integer	Windows	macOS	
	Number of installations			
number_of_events	integer	Windows	macOS	NU
	Number of events			

network_scan

Name	Type	Operating systems		Properties
number_of_devices	integer	Windows	macOS	
	Number of devices			
number_of_users	integer	Windows	macOS	
	Number of users			
number_of_applications	integer	Windows	macOS	
	Number of applications			
number_of_executables	integer	Windows	macOS	
	Number of executables			
number_of_binaries	integer	Windows	macOS	
	Number of binaries			
number_of_ports	integer	Windows	macOS	
	Number of ports			
number_of_connections	integer	Windows	macOS	
	Number of connections			
cumulated_scan_duration	millisecond	Windows	macOS	NU
	Cumulated duration of the network scan			
activity_start_time	datetime	Windows	macOS	NU
	Start time of investigated activity			
activity_stop_time	datetime	Windows	macOS	NU
	Stop time of investigated activity			
incoming_traffic	byte	Windows	macOS	NU
	Total network incoming traffic			
outgoing_traffic	byte	Windows	macOS	NU
	Total network outgoing traffic			
number_of_events	integer	Windows	macOS	NU
	Number of events			
incoming_network_traffic_per_device	byte	Windows	macOS	NU
	Device average incoming network traffic			
outgoing_network_traffic_per_device	byte	Windows	macOS	NU

	Device average outgoing network traffic			
total_network_traffic	byte	Windows	macOS	NU
	Network traffic			

package

Name	Type	Operating systems		Properties
number_of_devices	integer	Windows	macOS	FP
	Number of devices			
number_of_packages	integer	Windows	macOS	FP
	Number of packages			

port_scan

Name	Type	Operating systems		Properties
number_of_devices	integer	Windows	macOS	
	Number of devices			
number_of_users	integer	Windows	macOS	
	Number of users			
number_of_applications	integer	Windows	macOS	
	Number of applications			
number_of_executables	integer	Windows	macOS	
	Number of executables			
number_of_binaries	integer	Windows	macOS	
	Number of binaries			
number_of_connections	integer	Windows	macOS	
	Number of connections			
number_of_destinations	integer	Windows	macOS	
	Number of destinations			
cumulated_scan_duration	millisecond	Windows	macOS	NU
	Cumulated duration of the network scan			
activity_start_time	datetime	Windows	macOS	NU
	Start time of investigated activity			
activity_stop_time	datetime	Windows	macOS	NU
	Stop time of investigated activity			
incoming_traffic	byte	Windows	macOS	NU
	Total network incoming traffic			
outgoing_traffic	byte	Windows	macOS	NU
	Total network outgoing traffic			
number_of_events	integer	Windows	macOS	NU
	Number of events			
incoming_network_traffic_per_device	byte	Windows	macOS	NU
	Device average incoming network traffic			
outgoing_network_traffic_per_device	byte	Windows	macOS	NU

	Device average outgoing network traffic			
total_network_traffic	byte	Windows	macOS	NU
	Network traffic			

printout

Name	Type	Operating systems		Properties
number_of_devices	integer	Windows		
	Number of devices			
number_of_users	integer	Windows		
	Number of users			
number_of_printers	integer	Windows		
	Number of printers			
number_of_printed_pages	integer	Windows		
	Number of printed pages			
number_of_printouts	integer	Windows		
	Number of print jobs			
activity_start_time	datetime	Windows		NU
	Start time of investigated activity			
activity_stop_time	datetime	Windows		NU
	Stop time of investigated activity			
number_of_events	integer	Windows	macOS	NU
	Number of events			

session_performance

Name	Type	Operating systems		Properties
session_duration	millisecond	Windows		NU
	Session duration			
average_citrix_rtt	millisecond	Windows		NU
	Average Citrix RTT			
average_session_network_latency	millisecond	Windows		NU
	Average session network latency			

user_activity

Name	Type	Operating systems		Properties
number_of_devices	integer	Windows		
	Number of devices			
number_of_users	integer	Windows	macOS	
	Number of users			
number_of_logons	integer	Windows		
	Number of user logons			
activity_start_time	datetime	Windows		NU
	Start time of investigated activity			

activity_stop_time	datetime	Windows		NU
	Stop time of investigated activity			
cumulated_interaction_duration	millisecond	Windows		NU
	Cumulated time with user interaction (mouse or keyboard events)			
average_logon_duration	millisecond	Windows		NU
	Average user logon duration			
average_extended_logon_duration	millisecond	Windows		NU
	Average extended logon duration			
number_of_events	integer	Windows	macOS	NU
	Number of events			

web_request

Name	Type	Operating systems		Properties
total_web_traffic	byte	Windows	macOS	NU
	Web traffic			
outgoing_web_traffic_per_device	byte	Windows	macOS	NU
	Outgoing web traffic per device			
incoming_web_traffic_per_device	byte	Windows	macOS	NU
	Incoming web traffic per device			
number_of_devices	integer	Windows	macOS	FP
	Number of devices			
number_of_domains	integer	Windows	macOS	FP
	Number of domains			
number_of_users	integer	Windows	macOS	FP
	Number of users			
number_of_applications	integer	Windows	macOS	FP/NU
	Number of applications			
number_of_executables	integer	Windows	macOS	FP
	Number of executables			
number_of_binaries	integer	Windows	macOS	FP
	Number of binaries			
number_of_destinations	integer	Windows	macOS	
	Number of destinations			
number_of_ports	integer	Windows	macOS	
	Number of ports			
activity_start_time	datetime	Windows	macOS	NU
	Start time of investigated activity			
activity_stop_time	datetime	Windows	macOS	NU
	Stop time of investigated activity			
average_network_response_time	microsecond	Windows	macOS	

	Average TCP connection establishment time			
highest_local_privilege_reached	privileges_level	Windows	macOS	NU
	Highest local privilege level reached for executions (user, power user, administrator)			
number_of_web_requests	integer	Windows	macOS	
	Number of web requests			
protocols_used_in_requests	web_protocol_combination	Windows	macOS	NU
	Protocols used in web requests (HTTP, TLS, HTTP/TLS)			
lowest_protocol_version	min_web_protocol_version	Windows	macOS	NU
	Lowest protocol version observed in web requests (excluding web requests with unknown protocol version)			
incoming_traffic	byte	Windows	macOS	NU
	Total web incoming traffic			
outgoing_traffic	byte	Windows	macOS	NU
	Total web outgoing traffic			
average_incoming_bitrate	bps	Windows	macOS	NU
	Average incoming bitrate of all underlying web requests, consolidated over time			
average_outgoing_bitrate	bps	Windows	macOS	NU
	Average outgoing bitrate of all underlying web requests, consolidated over time			
cumulated_web_request_duration	millisecond	Windows	macOS	NU
	Cumulated duration of web requests			
cumulated_web_interaction_duration	millisecond	Windows	macOS	NU
	Cumulated time during which web requests occurred, counted with a 5 minutes resolution.			
average_request_size	byte	Windows	macOS	NU
	Average size of web requests			
average_response_size	byte	Windows	macOS	NU
	Average size of web responses			
average_request_duration	millisecond	Windows	macOS	
	Average time between request and last response byte			
successful_http_requests_ratio	permill	Windows	macOS	NU
	Percentage of successful HTTP requests (1xx, 2xx and 3xx)			
number_of_events	integer	Windows	macOS	NU
	Number of events			

Definitions

The following document lists all objects, fields and aggregates available through NXQL. Each field and aggregate have a name, a type, properties and a description.

Platforms can have the following values:

- **W**: The field, aggregate or table is available on the Windows platform.
- **X**: The field, aggregate or table is available on the Mac OS platform.
- **M**: The field, aggregate or table is available on the Mobile platform.

Properties can have the following values:

- **DE**: The field or aggregate is deprecated.
- **PB**: The field or aggregate is in Public Beta.
- **FP**: The field or aggregate can be used without a between clause.
- **NU**: The field or aggregate can be nil.

- **SE**: The field or aggregate is only available with a license containing the **security** feature.
- **WE**: The field or aggregate is only available with a license containing the **web monitoring** feature.
- **NC**: The field is not comparable.