

1. NXQL Data Model 6.29	2
1.1 Definitions	2
1.2 Relationships	2
1.3 application object NXQL	4
1.4 binary object NXQL	5
1.5 destination object NXQL	7
1.6 device object NXQL	7
1.7 domain object NXQL	18
1.8 executable object NXQL	19
1.9 package object NXQL	20
1.10 port object NXQL	21
1.11 printer object NXQL	21
1.12 service object NXQL	22
1.13 url_path object NXQL	22
1.14 user object NXQL	22
1.15 connection event NXQL	23
1.16 device_activity event NXQL	24
1.17 device_error event NXQL	25
1.18 device_performance (Public Beta) event NXQL	25
1.19 device_warning event NXQL	26
1.20 execution event NXQL	26
1.21 execution_error event NXQL	27
1.22 execution_warning event NXQL	28
1.23 installation event NXQL	28
1.24 network_scan event NXQL	29
1.25 port_scan event NXQL	29
1.26 printout event NXQL	30
1.27 session_performance event NXQL	30
1.28 user_activity event NXQL	31
1.29 web_request event NXQL	31
1.30 connection aggregate NXQL	32
1.31 device_activity aggregate NXQL	34
1.32 device_error aggregate NXQL	34
1.33 device_performance aggregate NXQL	35
1.34 device_warning aggregate NXQL	35
1.35 execution aggregate NXQL	36
1.36 execution_error aggregate NXQL	37
1.37 execution_warning aggregate NXQL	38
1.38 installation aggregate NXQL	38
1.39 network_scan aggregate NXQL	39
1.40 package aggregate NXQL	40
1.41 port_scan aggregate NXQL	40
1.42 printout aggregate NXQL	41
1.43 session_performance aggregate NXQL	41
1.44 user_activity aggregate NXQL	41
1.45 web_request aggregate NXQL	42

NXQL Data Model 6.29

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.

Relationships

A relationship is a link between the object and the 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
- user

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

application object NXQL



















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























































Name	Type				Properties
company	string				
	Company producing the application				




database_usage	permill				
	Percentage of the database used by information related with the application				
description	string				
	Application description				
first_seen	datetime				NU
	First time activity of the application was recorded on any device.				
id	identifier				
	Unique application identifier				
known_packages	string				
	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				NU
	Last time activity of the application was recorded on any device.				
name	string				
	Application name				
platform	enum				
	The platform (operating system family) on which the application is running.				
storage_policy	enum				
	Indicates the event storage policy for the application. Possible values are: <ul style="list-style-type: none"> • all: web requests, connections and executions are stored; • connections and executions; • executions; • none: no activity is recorded. 				
total_active_days	day				
	Total number of days the application was active.				

binary object NXQL

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






















Name	Type				Properties
application_category	string				SE
	Indicates the category of the application: <ul style="list-style-type: none"> • '-': Not yet tagged; • Unknown: Not categorized by Nextthink Library. 				
application_company	string				
	Application company				
application_name	string				
	Application name				
architecture	enum				
	Executable architecture (32/64 bit)				
average_cpu_usage	permill				
	Average CPU usage for the binary				

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

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
















destination object NXQL





































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























































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




















































device object NXQL


























































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











































Name	Type				Properties
administrator_account_status	enum				
	Determines whether the local Administrator account is enabled or disabled.				
all_antispywares	string				
	Summary information about all the detected antispyware: <ul style="list-style-type: none"> • 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				
	Summary information about all the detected antiviruses: <ul style="list-style-type: none"> • 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				
	Summary information about all the detected firewalls: <ul style="list-style-type: none"> • 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'				
antispware_name	string				NU
	Name of the main antispware				
antispware_rtp	enum				
	Indicates whether the antispware real time protection (RTP) is active: <ul style="list-style-type: none"> • on: Indicates that RTP is active; • off: Indicates that either RTP is not active or no antispware 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. 				
antispware_up_to_date	enum				
	Indicates whether the antispware is up-to-date: <ul style="list-style-type: none"> • yes: Indicates that antispware is up-to-date; • no: Indicates that either the antispware is not up-to-date or no antispware 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				NU
	Name of the main antivirus				
antivirus_rtp	enum				
	Indicates whether the antivirus real time protection (RTP) is active: <ul style="list-style-type: none"> • 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				
	Indicates whether the antivirus is up-to-date: <ul style="list-style-type: none"> • 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				
	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				
	Determines whether to audit each event of account management on a computer.				
audit_directory_service_access	enum				
	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				
	Determines whether to audit each instance of a user logging on to or logging off from a computer.				
audit_object_access	enum				
	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				
	Determines whether to audit every incident of a change to user rights assignment policies, audit policies, or trust policies.				
audit_privilege_use	enum				
	Determines whether to audit each instance of a user exercising a user right.				
audit_process_tracking	enum				
	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				
	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				NU
	Full boot duration baseline				
average_fast_startup_duration	millisecond				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				NU
	User logon duration baseline				
bios_serial_number	string				NU
	BIOS serial number				
boot_disk_health_status	enum				NU
	Indicates the health of the disk from which the device is booting [from], as reported by the operating system.				
boot_disk_type	enum				NU
	Indicates the type of the disk from which the device is booting.				
chassis_serial_number	string				NU
	Chassis serial number				
cltr_ca_license_uid	string				NU
	Indicates the Collector assignment license UID				
cltr_ca_status	enum				NU
	Indicates whether Collector assignment service is enabled or disabled				
cltr_crash_guard_count	integer				NU
	Indicates the number of consecutive hard resets or system crashes of the device				
cltr_crash_guard_limit	integer				NU
	Indicates the Collector CrashGuard limit				
cltr_crash_guard_protection_interval	integer				NU
	Indicates the CrashGuard monitoring interval in minutes				
cltr_crash_guard_react_interval	integer				NU
	Indicates the Collector CrashGuard reactivation interval in hours				
cltr_custom_shells	enum				NU
	Indicates whether the Collector reports user logon events and user interactions in virtualized and embedded (kiosk mode) environments				

















































cltr_data_channel_protocol	enum				NU
	Specifies if the Collector data is sent over TCP or UDP				
cltr_dns_res_preference	enum				NU
	Indicates the DNS resolution preference for Collector in terms of IP protocol version on the device				
cltr_engage_service_status	enum				NU
	Indicates whether Engage is enabled or disabled				
cltr_freezes_monitoring	enum				NU
	Indicates whether the Collector is monitoring for unresponsive applications on the device				
cltr_installs_scan_interval	integer				NU
	Indicates the interval, in hours, after which the Collector checks for newly installed packages and updates				
cltr_is_visible	enum				NU
	Indicates whether Collector is hidden in the "Add or Remove Programs"				
cltr_log_level	enum				NU
	Indicates the Collector log level				
cltr_max_segment_size	integer				NU
	Indicates the maximum segment size of packets sent by Collector				
cltr_ra_execution_policy	enum				NU
	Indicates the Powershell script execution policy				
cltr_smb_print_mon_status	enum				NU
	Indicates whether SMB printing monitoring is enabled or disabled				
cltr_string_tag	string				NU
	Indicates the Collector string tag				
cltr_web_mon_status	enum				NU
	Indicates whether Web & Cloud monitoring is enabled or disabled				
collector_distinguished_name	string				NU
	Indicates the distinguished name (DN) as seen: <ul style="list-style-type: none"> • 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				NU
	Link to the last Nextthink Collector installation error log				
collector_package_target_version	version				NU
	Indicates the Collector package version that is targeted.				
collector_print_monitoring_status	enum				NU
	Indicates whether the Collector printing monitoring is enabled or disabled				
collector_status	enum				NU
	Indicates the status of the Nextthink Collector package installed on the device: <ul style="list-style-type: none"> • 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				
	Collector installation tag				
collector_update_status	enum				
	Current status of Nextthink Collector Updater				
collector_version	version				
	Version number of Nextthink Collector installation				
cpu_frequency	mhz				NU
	CPU frequency				
cpu_model	string				NU
	CPU model				
database_usage	permill				
	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				NU
	Indicates the device manufacturer.				
device_model	string				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				NU
	Device product ID				
device_product_version	string				NU
	Device product version				
device_serial_number	string				NU
	Indicates the device serial number.				
device_type	enum				
	Type of device (desktop, laptop, server, mobile)				
device_uid	md5				
	Indicates the universally unique identifier (based on Engine name and device ID)				
device_uuid	string				
	Indicates the device universally unique identifier (UUID)				
directory_service_site	string				NU
	Site (or location) of an Active Directory (AD) service				
disks_manufacturers	string				
	Hard disks manufacturers				
disks_smart_index	percent				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				NU
	<p>Indicates the distinguished name (DN) as seen:</p> <ul style="list-style-type: none"> 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				
	<p>Indicates whether the device can access the Exchange ActiveSync server. The possible states are:</p> <ul style="list-style-type: none"> 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				
	<p>Indicates the reason for the device access state. The possible values are:</p> <ul style="list-style-type: none"> 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				
	<p>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.</p>				
eas_device_identity	string				
	<p>Indicates the identity of the device in Exchange ActiveSync Server.</p>				
eas_exemption	enum				
	<p>Indicates whether a personal exemption is set for the device and its user. Possible values are:</p> <ul style="list-style-type: none"> none; allow; block. 				
eas_policy_application_status	enum				
	<p>Indicates whether the Exchange ActiveSync policy is applied or not. Possible values are:</p> <ul style="list-style-type: none"> 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				
	<p>Indicates the name of the Exchange ActiveSync policy applied to the user's mailbox.</p>				
eas_policy_update	datetime				
	<p>Indicates the last time the Exchange ActiveSync policy was updated on the device.</p>				
email_attachment_enabled	boolean				NU
	<p>Indicates whether attachments can be downloaded to the mobile device through the Exchange ActiveSync protocol.</p>				
enforce_password_history	integer				NU
	<p>Indicates the number of unique passwords that have to be associated with a user account before an old password can be reused.</p>				
entity	string				
	<p>Entity</p>				
extended_logon_duration_baseline	millisecond				NU
	<p>Extended logon duration baseline</p>				
firewall_name	string				NU
	<p>Name of the main firewall</p>				
















firewall_rtp	enum				
	<p>Indicates whether the firewall real time protection (RTP) is active:</p> <ul style="list-style-type: none"> • 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				NU
	<p>Indicates the first time when the activity of the device was recorded:</p> <ul style="list-style-type: none"> • 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				NU
	Amount of RAM of the graphical card with most RAM				
graphical_cards	string				
	Installed graphical cards				
group_name	string				NU
	Name of computer domain or workgroup				
guest_account_status	enum				
	Determines if the Guest account is enabled or disabled.				
hard_disks	string				NC
	List of all hard disks				
id	identifier				
	Unique device identifier				
internet_security_settings	enum				
	Internet security settings (ok, at risk or unknown)				
ip_addresses	ip_address				
	List of IP addresses for the device				
is_collector_distinguished_name_truncated	boolean				
	Flag indicating whether the collector DN is truncated or not				
is_directory_service_site_truncated	boolean				
	Flag indicating whether the DS site is truncated or not				
last_boot_duration	millisecond				NU
	Last boot time duration				
last_extended_logon_duration	millisecond				NU
	Last extended logon duration				
last_ip_address	ip_address				NU
	Last IP address assigned to the device				
last_known_connection_status	enum				NU

	Indicates the last known connection status of the device:				
	<ul style="list-style-type: none"> • 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				NU
	Last local IP address assigned to the device				
last_logged_on_user	string				NU
	Last logged on user				
last_logon_duration	millisecond				NU
	Last user logon duration				
last_logon_time	datetime				NU
	Last logon time				
last_seen	datetime				NU
	Indicates the last time that activity on the device was reported:				
	<ul style="list-style-type: none"> • 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				NU
	Indicates the last time that the device was successfully connected through the TCP channel.				
	<ul style="list-style-type: none"> • '-': The Collector is an older version that does not support TCP. 				
last_system_boot	datetime				NU
	Last boot time				
last_update	datetime				NU
	Indicates the last Collector update time.				
last_update_status	enum				NU
	Indicates the status of the last Collector update:				
	<ul style="list-style-type: none"> • '-': 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 Nextthink 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				NU
	Last time Nextthink Updater checked for updates				
last_windows_update	datetime				NU
	Time of last system Update				
local_administrators	string				
	Users and groups which are members of the Local Administrators group on the device.				
local_power_users	string				
	Users and groups which are members of the Local Powers Users group on the device.				
logical_cpu_number	integer				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				
	List of all logical drives				
mac_addresses	mac_address				
	List of MAC addresses for the device				
maximum_password_age	integer				NU
	<p>Indicates the period in time (in days) during which the password can be used before the system requires the user to change it:</p> <ul style="list-style-type: none"> • Windows: As set up in the group policy; • Mobile: As set up in security policies. 				
membership_type	enum				
	Type of computer membership (domain/workgroup)				
minimum_password_age	integer				NU
	Period of time (in days) that a password must be used before the user can change it.				
minimum_password_length	integer				NU
	Least number of characters that a password for a user account may contain.				
monitor_models	string				
	Models of connected monitors				
monitor_resolutions	string				
	Screen resolutions of connected monitors				
monitors	string				
	Connected monitors				
monitors_serial_numbers	string				
	Serial numbers of connected monitors (ordered as in 'Monitors')				
name	string				
	<p>Indicates the name of the device:</p> <ul style="list-style-type: none"> • 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				
	<p>Number of antispyware detected:</p> <ul style="list-style-type: none"> • 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				
	<p>Number of antiviruses detected:</p> <ul style="list-style-type: none"> • 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				NU
	Number of cores				
number_of_cpus	integer				NU
	Number of CPUs				
number_of_days_since_first_seen	integer				NU































						Number of days since activity of the device was first recorded in the system.
number_of_days_since_last_boot	integer					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					NU
						Number of days since last logon
number_of_days_since_last_seen	integer					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: <ul style="list-style-type: none"> • 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					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					NU
						Number of days since last system Update
number_of_firewalls	enum					
						Number of firewalls detected: <ul style="list-style-type: none"> • 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					
						Number of installed graphical cards
number_of_monitors	integer					
						Number of connected monitors
os_architecture	enum					
						Architecture of device operating system (x86/x64)
os_build	version					
						Indicates the build number of the operating system.
os_version_and_architecture	string					NU
						Indicates name, version and architecture (when applicable) of the operating system. <ul style="list-style-type: none"> • unknown: the OS version could not be retrieved or it could not be mapped to a recognized value.
password_complexity_requirements	enum					
						Indicates whether password complexity is required: <ul style="list-style-type: none"> • 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					
						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: <ul style="list-style-type: none"> • Windows; • Mac OS; • Mobile.













privileges_of_last_logged_on_users	enum				
	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				NU
	Windows security identifier for the device.				
storage_policy	enum				
	Indicates the event storage policy for the device. Possible values are: <ul style="list-style-type: none"> • 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				
	Total capacity of system drive				
system_drive_free_space	byte				
	Total available free space on system drive				
system_drive_usage	percent				NU
	Use percentage of system drive				
total_active_days	day				
	Total number of days the device was active.				
total_drive_capacity	byte				
	Total capacity of all drives				
total_drive_free_space	byte				
	Total free space on all drives				
total_drive_usage	permill				NU
	Total use percentage of all drives				
total_nonsystem_drive_capacity	byte				
	Total capacity of all non-system drives				
total_nonsystem_drive_free_space	byte				
	Total free space on all non-system drives				
total_nonsystem_drive_usage	percent				NU
	Total use percentage of all non-system drives				
total_ram	byte				NU
	Total amount of RAM				
updater_error	string				
	Last Nextthink Collector Updater error				
updater_version	version				
	Nextthink Collector Updater version				

upgrade_group	enum				NU
	Indicates the update group of Nextthink Collector: <ul style="list-style-type: none"> • 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				
	User account control status (ok, at risk or unknown)				
windows_license_key	string				NU
	Windows license key				
windows_updates_status	enum				
	Windows update status (ok, at risk or unknown)				
wmi_status	enum				
	Windows WMI service status (ok, failure)				

domain object NXQL





































A domain is a domain name e.g. www.nextthink.com




Name	Type				Properties
database_usage	permill				
	Percentage of the database used by information related with the domain				
domain_category	string				SE
	Indicates the category of the domain: <ul style="list-style-type: none"> • '-': Not yet tagged or internal domain. 				
first_seen	datetime				NU
	The first time the domain has been seen.				
hosting_country	string				SE
	Indicates in which country the domain is hosted: <ul style="list-style-type: none"> • '-': Not yet tagged, internal domain or not known by Nextthink Library. 				
hostname	string				NU
	The hostname of the fully qualified domain name				
id	identifier				
	Unique domain identifier				
internal_domain	boolean				
	Indicates whether the domain is considered internal: <ul style="list-style-type: none"> • yes: The domain is not reported to Nextthink Library and subdomains are not compressed using the '*' pattern; • no: The domain is reported to the Nextthink Library (if the license includes the Security module); complex subdomains are compressed using the '*' pattern. 				
last_seen	datetime				NU
	The last time the domain has been seen.				
name	string				
	The fully qualified domain name				

protocol	enum				
	Protocols used in web requests (HTTP, TLS, HTTP/TLS)				
response_size	byte				
	Total web incoming traffic				
storage	enum				
	Event storage policy for the domain (web request or none)				
threat_level	enum				SE
	<p>Indicates the threat level of the domain:</p> <ul style="list-style-type: none"> • '-': Not yet tagged or internal domain; • none detected: No known threat; • low: low threat; • intermediate: Intermediate threat; • high: High threat. 				

executable object NXQL











































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

Name	Type				Properties
application_company	string				
	Application company				
application_name	string				
	Application name				
database_usage	permill				
	Percentage of the database used by information related with the executable.				
description	string				
	Executable description				
first_seen	datetime				NU
	First time activity of the executable was recorded on any device.				
id	identifier				
	Unique executable identifier				
known_packages	string				
	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				NU
	Last time activity of the executable was recorded on any device.				
name	string				
	Executable name				
platform	enum				
	The platform (operating system family) on which the executable is running.				
storage_policy	enum				

	Indicates the event storage policy for the executable. Possible values are: <ul style="list-style-type: none"> • all: web requests, connections and executions are stored; • connections and executions; • executions; • none: no activity is recorded. 				
total_active_days	day				
	Total number of days the executable was active.				

package object NXQL

A package is a software packages (programs or updates)






















Name	Type				Properties
first_installation	datetime				NU
	Time of first installation				
first_seen	datetime				NU
	The first time the package has been seen.				
id	identifier				
	Unique package identifier				
name	string				
	Package name				
number_of_updates	integer				
	Number of updates (for programs)				
platform	enum				
	The platform (operating system family) on which the package is installed.				
program	string				
	Package program				
publisher	string				NU
	Package publisher				
status	enum				
	Package status (installed/removed)				
type	enum				
	Package type (program/update)				
version	string				NU
	Package version				
windows_7_32bit_compatibility	string				DE
	Indicates the Windows 7 (32-bit) compatibility of the package: <ul style="list-style-type: none"> • '-': Not yet tagged; • No information available: Not known by Nextthink Library; • Compatible: Compatible with Windows 7. 				
windows_7_64bit_compatibility	string				DE

Indicates the Windows 7 (64-bit) compatibility of the package:

- '-': Not yet tagged;
- No information available: Not known by Nextthink Library;
- Compatible: Compatible with Windows 7.




























port object NXQL




A port is a TCP or UDP connection ports.

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

printer object NXQL
















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

Name	Type				Properties
first_seen	datetime				NU
	First time activity of the printer was recorded on any device.				
host_name	string				
	Host name				
id	identifier				
	Unique print identifier				
last_seen	datetime				NU
	Last time activity of the printer was recorded on any device.				
location	string				NU
	Printer location				
model	string				
	Printer model				
name	string				
	Printer name				
real_name	string				
	Most frequently seen display name				

type	enum				
	Printer type (local/remote)				

service object NXQL

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






















url_path object NXQL














































An url_path is an URL path after the domain name e.g. [www.nextthink.com/awards/].

Name	Type				Properties
id	identifier				
	Unique url path identifier				
path	string				
	The URL path				

user object NXQL










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				Properties
country	string				
	Country of user as listed in active directory				
database_usage	permill				
	Percentage of the database used by information related with the binary				
department	string				
	User department as listed in active directory				
distinguished_name	string				NU
	Active directory distinguished name (DN)				
first_seen	datetime				NU
	First time activity of the user was recorded on any device.				
full_name	string				NU
	Full user name as listed in active directory				

id	identifier				
	Unique user identifier				
job_title	string				NU
	Job title as listed in active directory				
last_seen	datetime				NU
	Last time activity of the user was recorded on any device.				
locality	string				
	Locality of user as listed in active directory				
location	string				
	Location of user as listed in active directory				
name	string				
	User logon name				
number_of_days_since_last_seen	integer				NU
	Indicates the number of days since the last time the user was seen by Nextthink. The field is updated whenever user activity is detected.				
org_unit	string				
	Organisational unit of User as listed in active directory				
seen_on_mac_os	boolean				
	Indicates if the user has been seen on a Mac device.				
seen_on_mobile	boolean				
	Indicates if the user has been seen on a Mobile device.				
seen_on_windows	boolean				
	Indicates if the user has been seen on a Windows device.				
sid	sid				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				
	Total number of days the user was active.				
type	enum				
	Type of user (local/domain/system)				
user_uid	md5				
	Indicates the universally unique identifier				

connection event NXQL

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				Properties
cardinality	integer				
	Number of underlying connections, consolidated over time				
destination_ip_address	ip_address				
	IP address of the connection destination				

device_ip_address	ip_address				
	IP address of the connection source				
duration	millisecond				
	The time between the start of the first connection and the end of the last underlying connection.				
end_time	datetime				
	Connection end time, corresponding to the moment when the last underlying connection was closed.				
id	identifier				
	Unique connection identifier				
incoming_bitrate	bps				NU
	Average incoming bitrate of all underlying connections, consolidated over time				
incoming_traffic	byte				
	Incoming traffic				
network_interface_iana_code	string				
	(beta) Indicates the network interface IANA code.				
network_interface_index	integer				
	(beta) Indicates the network interface index.				
network_interface_type	enum				
	(beta) Indicates the network interface type. Possible values are: <ul style="list-style-type: none"> wifi ethernet mobile other unknown: the Collector is not supporting interface type. 				
network_response_time	microsecond				
	TCP connection establishment time				
outgoing_bitrate	bps				NU
	Average outgoing bitrate of all underlying connections, consolidated over time				
outgoing_traffic	byte				
	Outgoing traffic				
start_time	datetime				
	Connection start time				
status	enum				
	Status of the connection (established, rejected, no service, no host, closed)				
type	enum				
	Type of the connection (tcp, udp)				

device_activity event NXQL



















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

Name	Type				Properties
boot_type	enum				NU

	Boot type of the boot activity				
duration	millisecond				
	Boot duration (timed between kernel start and launch of 'logonui.exe' process) or online duration				
id	identifier				
	Boot event identifier				
time	datetime				
	Time of boot				
type	enum				
	Activity event information				



















device_error event NXQL
















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

Name	Type				Properties
error_code	integer				
	Error code				
error_label	string				
	Error label				
id	identifier				
	Problem identifier				
start_time	datetime				
	Time of error				
type	enum				
	Indicates the device error type, with the following possible values:				
	<ul style="list-style-type: none"> • 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 (Public Beta) event NXQL




























A device_performance reports the average IOPS, CPU and memory of a device during one hours.

Name	Type				Properties
average_cpu_usage	percent				
	Average CPU usage on the period				
average_memory_usage	byte				
	Average memory usage on the period				
duration	millisecond				
	Total report duration				
end_time	datetime				
	Report end time				
id	identifier				

	Unique report identifier				
read_bytes	byte				NU
	Total disk read bytes accumulated during the period				
read_operations	integer				NU
	Total disk read operations accumulated during the period				
time	datetime				
	Start time				
write_bytes	byte				NU
	Total disk write bytes accumulated during the period				
write_operations	integer				NU
	Total disk write operations accumulated during the period				























































device_warning event NXQL

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

Name	Type				Properties
duration	millisecond				
	Performance event duration				
end_time	datetime				
	Performance event end time				
id	identifier				
	Unique performance event identifier				
info	string				
	Performance event information				
start_time	datetime				
	Performance event start time				
type	enum				
	Type of the device warning, one of: <ul style="list-style-type: none"> 'high overall cpu usage' 'high cpu usage' (deprecated) 'high io usage' 'high memory usage' 'high number of page faults'. 				
value	percent				
	Performance percentage				
warning_duration	millisecond				
	Indicates the duration of the warning. This duration can be shorter than the event duration when the warning is not continuous.				













execution event NXQL

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

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




execution_error event NXQL

An execution_error is application errors (crash or not responding).

Name	Type				Properties
id	identifier				
	Error identifier				
info	string				
	Error event information				
time	datetime				
	Time of error				
type	enum				
	Type of the execution error (application not responding, crash)				

execution_warning event NXQL

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

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

installation event NXQL

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

Name	Type				Properties
id	identifier				
	Unique deployment identifier				
time	datetime				

	Installation start time				
type	enum				
	Type of operation (installation, uninstallation)				



















network_scan event NXQL



















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

port_scan event NXQL


































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				Properties
cardinality	integer				
	Number of underlying connections, consolidated over time				
destination_ip_address	ip_address				
	IP address of the scanned destination				
device_ip_address	ip_address				
	IP address of the connection source				
duration	millisecond				
	The time between the start of the first connection and end of the last underlying connection.				
end_time	datetime				

	Scanning end time, corresponding to the moment when the last underlying connection was closed.				
first_scanned_port	port				
	First port scanning				
id	identifier				
	Unique scanning identifier				
last_scanned_port	port				
	Last port scanning				
start_time	datetime				
	Scanning start time				
status	enum				
	Status of the Scanning (established, closed)				
type	enum				
	Type of the port scanning (tcp, udp)				











printout event NXQL

A printout is a print job processed by a printer.

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



















session_performance event NXQL

Sessions of a user logged on a device.

Name	Type				Properties
cardinality	integer				
	Number of underlying sessions consolidated in a bucket period				
citrix_rtt	millisecond				NU
	Citrix RTT				
client_ip	ip_address				
	Client IP				
duration	millisecond				
	Session performance bucket period duration				
end_time	datetime				
	Session performance bucket end time				
id	identifier				
	Unique session performance identifier				
session_network_latency	millisecond				NU
	Session network latency				
session_protocol	enum				NU
	User input delay				
start_time	datetime				
	Execution start time				








































user_activity event NXQL

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

Name	Type				Properties
duration	millisecond				
	Indicates the time between the user logging on and the desktop being shown.				
id	identifier				
	User logon event identifier				
real_duration	millisecond				
	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				
	Time of user logon				
type	enum				
	Activity event information				


























































web_request event NXQL

A web_request is a HTTP or TLS requests.

Name	Type				Properties
cardinality	integer				
	Number of underlying web requests, consolidated over time				
connections_duration	millisecond				
	The time between start of the first connection and end of the last underlying connection				
end_time	datetime				
	Web request end time, corresponding to the moment when the last underlying TCP connection was closed.				
http_status	http_status_code				NU
	HTTP response status code				
id	identifier				
	Unique request identifier				
incoming_traffic	byte				
	Incoming web traffic of all underlying web requests, consolidated over time				
network_response_time	microsecond				
	Average TCP connection establishment time of all underlying connections, consolidated over time				
outgoing_traffic	byte				
	Outgoing web traffic of all underlying web requests, consolidated over time				
protocol	enum				
	Web request protocol (HTTP, TLS)				
protocol_version	enum				
	Web request protocol version				
service_related	boolean				
	Indicates whether the web request is related to a configured service: <ul style="list-style-type: none"> • 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				
	Web request start time				
web_request_duration	millisecond				
	Average time between request and last response byte of all underlying requests, consolidated over time				


































connection aggregate NXQL

Name	Type				Properties
number_of_devices	integer				FP
	Number of devices				
number_of_users	integer				FP
	Number of users				
number_of_applications	integer				FP



















	Number of applications				
number_of_executables	integer				FP
	Number of executables				
number_of_binaries	integer				FP
	Number of binaries				
number_of_destinations	integer				
	Number of destinations				
number_of_ports	integer				
	Number of ports				
number_of_connections	integer				
	Number of connections				
cumulated_connection_duration	millisecond				
	Cumulated duration of TCP connections				
activity_start_time	datetime				NU
	Start time of investigated activity				
activity_stop_time	datetime				NU
	Stop time of investigated activity				
incoming_traffic	byte				NU
	Total network incoming traffic				
outgoing_traffic	byte				NU
	Total network outgoing traffic				
average_network_response_time	microsecond				
	Average TCP connection establishment time				
successful_connections_ratio	permill				NU
	Percentage of successful TCP connections				
network_availability_level	availability_level				NU
	Graded ratio of successful TCP connections (high, medium, low)				
average_incoming_bitrate	bps				NU
	Average incoming network bitrate				
average_outgoing_bitrate	bps				NU
	Average outgoing network bitrate				
highest_local_privilege_reached	privileges_level				NU
	Highest local privilege level reached for executions (user, power user, administrator)				
number_of_events	integer				NU
	Number of events				
incoming_network_traffic_per_device	byte				NU
	Device average incoming network traffic				
outgoing_network_traffic_per_device	byte				NU

	Device average outgoing network traffic				
total_network_traffic	byte				NU
	Network traffic				

device_activity aggregate NXQL




























Name	Type				Properties
number_of_devices	integer				
	Number of devices				
average_boot_duration	millisecond				NU
	Average boot duration				
average_logon_duration	millisecond				NU
	Average user logon duration				
average_extended_logon_duration	millisecond				NU
	Average extended logon duration				
number_of_boots	integer				NU
	Number of boots				
activity_start_time	datetime				NU
	Start time of investigated activity				
activity_stop_time	datetime				NU
	Stop time of investigated activity				
uptime	millisecond				NU
	Amount of time the machine has been running				
cumulated_interaction_duration	millisecond				NU
	Cumulated time with user interaction (mouse or keyboard events)				
number_of_events	integer				NU
	Number of events				

device_error aggregate NXQL











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







Number of events

device_performance aggregate NXQL

















































Name	Type				Properties
total_read_bytes	byte				NU
	Total read bytes				
total_write_bytes	byte				NU
	Total write bytes				
total_read_operations	integer				NU
	Average read IPOS				
total_write_operations	integer				NU
	Average write IPOS				
cumulated_measured_duration	millisecond				NU
	Average read/write IPOS				
average_memory_usage	byte				NU
	Average memory usage				
average_cpu_usage	percent				NU
	Average CPU usage				
number_of_events	integer				NU
	Number of events				



device_warning aggregate NXQL

Name	Type				Properties
number_of_devices	integer				
	Number of devices				
number_of_warnings	integer				
	Number of warnings				
cumulated_warning_duration	millisecond				NU
	Cumulated duration of the warning events				
activity_start_time	datetime				NU
	Start time of investigated activity				
activity_stop_time	datetime				NU
	Stop time of investigated activity				
number_of_events	integer				NU
	Number of events				
high_device_overall_cpu_time_ratio	permill				NU
	Indicates the ratio between the time the device is in high overall CPU usage and its uptime.				
high_device_memory_time_ratio	permill				NU





































	Indicates the ratio between the time the device is in high memory usage and its uptime.				
high_device_io_throughput_time_ratio	permill				NU
	Indicates the ratio between the time the device is in high IO throughput and its uptime.				
high_device_page_faults_time_ratio	permill				NU
	Indicates the ratio between the time the device is in high page faults and its uptime.				

execution aggregate NXQL

Name	Type				Properties
number_of_devices	integer				FP
	Number of devices				
number_of_users	integer				FP
	Number of users				
number_of_applications	integer				FP
	Number of applications				
number_of_executables	integer				FP
	Number of executables				
number_of_binaries	integer				FP
	Number of binaries				
number_of_executions	integer				
	Number of executions				
cumulated_execution_duration	millisecond				NU
	Cumulated duration of executions				
activity_start_time	datetime				NU
	Start time of investigated activity				
activity_stop_time	datetime				NU
	Stop time of investigated activity				
incoming_traffic	byte				NU
	Total network incoming traffic				
outgoing_traffic	byte				NU
	Total network outgoing traffic				
highest_local_privilege_reached	privileges_level				NU
	Highest local privilege level reached for executions (user, power user, administrator)				
number_of_events	integer				NU
	Number of events				
average_memory_usage_per_execution	byte				NU
	Average memory usage per execution				
memory_usage	byte				NU
	Memory usage				





































focus_time	millisecond				NU
	Focus time				
cpu_usage_ratio	permill				NU
	Average CPU usage				
total_cpu_time	millisecond				NU
	Total CPU time				
average_process_start_time	millisecond				NU
	Average process start time				
incoming_network_traffic_per_device	byte				NU
	Device average incoming network traffic				
outgoing_network_traffic_per_device	byte				NU
	Device average outgoing network traffic				
total_network_traffic	byte				NU
	Network traffic				

execution_error aggregate NXQL


Name	Type				Properties
application_not_responding_event_ratio	permill				NU
	Application not responding event ratio				
application_crash_ratio	permill				NU
	Application crash ratio				
number_of_application_not_responding_events	integer				
	Number of application not responding events				
number_of_application_crashes	integer				
	Number of application crashes				
number_of_devices	integer				
	Number of devices				
number_of_users	integer				
	Number of users				
number_of_applications	integer				
	Number of applications				
number_of_executables	integer				
	Number of executables				
number_of_binaries	integer				
	Number of binaries				
number_of_errors	integer				
	Number of errors				
activity_start_time	datetime				NU

	Start time of investigated activity				
activity_stop_time	datetime				NU
	Stop time of investigated activity				
number_of_events	integer				NU
	Number of events				

execution_warning aggregate NXQL














































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

installation aggregate NXQL

Name	Type				Properties
number_of_packages	integer				
	Number of packages				
number_of_devices	integer				
	Number of devices				
activity_start_time	datetime				NU

	Start time of investigated activity				
activity_stop_time	datetime				NU
	Stop time of investigated activity				
number_of_installations	integer				
	Number of installations				
number_of_events	integer				NU
	Number of events				

network_scan aggregate NXQL








































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













outgoing_network_traffic_per_device	byte				NU
	Device average outgoing network traffic				
total_network_traffic	byte				NU
	Network traffic				

package aggregate NXQL




















Name	Type				Properties
number_of_devices	integer				FP
	Number of devices				
number_of_packages	integer				FP
	Number of packages				

port_scan aggregate NXQL





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

number_of_events	integer				NU
	Number of events				
incoming_network_traffic_per_device	byte				NU
	Device average incoming network traffic				
outgoing_network_traffic_per_device	byte				NU
	Device average outgoing network traffic				
total_network_traffic	byte				NU
	Network traffic				

printout aggregate NXQL




























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

session_performance aggregate NXQL































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























































user_activity aggregate NXQL







Name	Type				Properties
------	------	--	--	--	------------

number_of_devices	integer				
	Number of devices				
number_of_users	integer				
	Number of users				
number_of_logons	integer				
	Number of user logons				
activity_start_time	datetime				NU
	Start time of investigated activity				
activity_stop_time	datetime				NU
	Stop time of investigated activity				
cumulated_interaction_d uration	millisecond				NU
	Cumulated time with user interaction (mouse or keyboard events)				
average_logon_duration	millisecond				NU
	Average user logon duration				
average_extended_logon_d uration	millisecond				NU
	Average extended logon duration				
number_of_events	integer				NU
	Number of events				

web_request aggregate NXQL

Name	Type				Properties
total_web_traffic	byte				NU
	Web traffic				
outgoing_web_traffic_pe r_device	byte				NU
	Outgoing web traffic per device				
incoming_web_traffic_p er_device	byte				NU
	Incoming web traffic per device				
number_of_devices	integer				FP
	Number of devices				
number_of_domains	integer				FP
	Number of domains				
number_of_users	integer				FP
	Number of users				
number_of_applications	integer				FP/NU
	Number of applications				
number_of_executables	integer				FP
	Number of executables				
number_of_binaries	integer				FP
	Number of binaries				

	Number of binaries				
number_of_destinations	integer				
	Number of destinations				
number_of_ports	integer				
	Number of ports				
activity_start_time	datetime				NU
	Start time of investigated activity				
activity_stop_time	datetime				NU
	Stop time of investigated activity				
average_network_response_time	microsecond				
	Average TCP connection establishment time				
highest_local_privilege_reached	privileges_level				NU
	Highest local privilege level reached for executions (user, power user, administrator)				
number_of_web_requests	integer				
	Number of web requests				
protocols_used_in_requests	web_protocol_combination				NU
	Protocols used in web requests (HTTP, TLS, HTTP/TLS)				
lowest_protocol_version	min_web_protocol_version				NU
	Lowest protocol version observed in web requests (excluding web requests with unknown protocol version)				
incoming_traffic	byte				NU
	Total web incoming traffic				
outgoing_traffic	byte				NU
	Total web outgoing traffic				
average_incoming_bitrate	bps				NU
	Average incoming bitrate of all underlying web requests, consolidated over time				
average_outgoing_bitrate	bps				NU
	Average outgoing bitrate of all underlying web requests, consolidated over time				
cumulated_web_request_duration	millisecond				NU
	Cumulated duration of web requests				
cumulated_web_interaction_duration	millisecond				NU
	Cumulated time during which web requests occurred, counted with a 5 minutes resolution.				
average_request_size	byte				NU
	Average size of web requests				
average_response_size	byte				NU
	Average size of web responses				
average_request_duration	millisecond				
	Average time between request and last response byte				

successful_http_request s_ratio	permill				NU
	Percentage of successful HTTP requests (1xx, 2xx and 3xx)				
number_of_events	integer				NU
	Number of events				