



uberAgent 7.0

Contents

uberAgent 7.0	11
Quickstart	12
About uberAgent	14
Products: UXM & ESA	14
Components: Agents & Apps	15
System Requirements	16
Changelog and Release Notes	19
Default Configuration	29
uberAgent.conf	29
uberAgent-data-volume-optimized.conf	33
uberAgent-GPO-include.conf	38
New Release Information & Notifications	39
Planning	39
Architecture Options	39
Configuration Options	42
Antivirus Exclusions	43
Splunk Data Volume Calculation	44
Splunk Sizing Resources and Recommendations	46
uberAgent Feature Support on macOS	48
Installation	50
Backend	50
Installing Splunk	50
Configuring Splunk's HTTP Event Collector	52

Installing and Configuring Elasticsearch & Kibana	56
Configuring Microsoft Azure Monitor	58
Configuring Apache Kafka & Confluent REST Proxy	60
Installing uberAgent	65
Installing the Splunk Apps	66
Installing the Windows Endpoint Agent	68
Installing the macOS Endpoint Agent	72
Installing Splunk Universal Forwarder	76
Installing the Chrome Browser Extension	81
Installing the Firefox Browser Extension	83
Installing the Edge Browser Extension	86
Installing the Internet Explorer Browser Add-on	87
Upgrading uberAgent	90
Configuration via Group Policy	91
Configuration via Local Config Files	94
Config File Syntax	95
UXM Features & Configuration	97
Experience Score	97
Per-Application Network Monitoring	107
Web App Monitoring	110
Automatic Application Identification	115
Citrix NetScaler (ADC) Monitoring	119
Citrix Cloud Monitoring	123
Citrix Session Monitoring	125

Citrix Site Monitoring	128
Central License File Management	131
Event Data Filtering	132
Username and Configuration Setting Encryption	136
ESA Features & Configuration	137
Enabling ESA	137
Threat Detection Engine	138
MS Office & Acrobat Reader Monitoring	139
LOLBAS Monitoring	140
Network Monitoring	140
Process Tampering Monitoring	141
Remote Thread Monitoring	142
Root CA certificate monitoring	143
Security Descriptor & ACL Monitoring	144
Sigma Rules & Converter	144
Sysmon Rule Converter	145
Threat Detection Engine	146
Rule Syntax	148
Rule Editor: uAQL Studio	152
Event Types	156
Common Event Properties	158
DNS Query Event Properties	162
Image Load Event Properties	163
Network Event Properties	164

Registry Event Properties	165
Remote Thread Event Properties	167
Process.DirectorySdSddl	167
Hash Calculation of PE Images	171
Authenticode Signature Verification	172
DNS Query Monitoring	173
MITRE ATT&CK Integration	174
Process Tree Dashboard	178
Scheduled Task Monitoring	179
Splunk Enterprise Security Integration	180
UXM Metrics	183
Application Metrics	183
Application Crashes & Hangs Metrics	183
Application Inventory & Usage Metrics	188
Application Name to ID Mapping Metrics	191
Application & Process Performance Metrics	192
Application & Process Startup Metrics	202
Application UI Unresponsiveness Metrics	210
Software Update Metrics	212
Browser Metrics	213
Google Chrome Metrics	213
Internet Explorer Metrics	215
Web App Metrics	217
Citrix NetScaler (ADC) Metrics	221

Citrix Session Metrics	243
Citrix Virtual Apps & Desktops Site Metrics	253
Machine Metrics	280
Machine Blue Screens & Hangs Metrics	280
Machine Inventory Metrics	285
Machine Performance And Utilization Metrics	297
Computer Startup, Shutdown & Hibernation Metrics	306
Boot Processes Metrics	306
Computer Startup (Machine Boot) Metrics	310
Computer Shutdown Metrics	314
On/Off Transition Delay Metrics	315
Standby/Resume Duration Metrics	326
Network Metrics	331
Microsoft Office Metrics	337
Session Metrics	341
Performance Counter Metrics	353
uberAgent Licensing Metrics	354
User & Host Metrics	356
User Logoff Metrics	357
User Logon Metrics	364
ESA Metrics	375
Threat Detection Metrics	376
Generic Properties	382
DNS Query Monitoring Metrics	383

Process Stop Metrics	384
Scheduled Task Metrics	386
Advanced Topics	404
Multi-Tenancy With Splunk	404
Reducing the Data Volume	405
Demoing uberAgent With the Event Generator for Splunk	407
Recommendations for Custom Dashboards (Splunk)	409
Custom Scripts	410
Data Distribution and Separation (Routing to Multiple Backends)	413
User & Host Tags	415
uAQL - uberAgent Query Language	419
Persistent Output Queue With Intelligent Disk Buffering	424
Event Triggers for Timers	428
Troubleshooting	432
Creating an uberAgent Support Bundle	432
Log Files	435
uberAgent Log Collector Splunk App	440
uberAgent Browser Extensions	440
Creating an uberAgent Performance Recording	445
uberAgent's Driver Safety Net Feature	447
Knowledge Base	448
Architecture	448
Description of the uInSessionHelper/uberAgentHelper Process	448
Name or Version may be Inconsistent Between App Inventory & Usage	450

Using uberAgent With a Proxy	451
uberAgent vs. Splunk Template for XenDesktop 7	452
Configuration	453
Metric Dependencies	453
Custom Queries	454
Walkthrough: Building a Splunk Search	455
How to Implement Drilldowns on Custom Dashboards	459
How to Report on CPU Seconds & RAM GB Hours per User	461
Data Collection	463
Citrix Applications Are Still Displayed with Old Name After Renaming	463
Dashboards Have No Data	464
Differences between SessionPublishedAppsCtx and SessionPublishedName	465
How Application Startup Duration is Measured	465
How to Configure the Data Collection Frequency	467
Incomplete Boot Duration Metrics	468
No Data in Splunk Even Though uberAgent Sends Successfully	468
Reasons For Empty SessionFgBrowserActiveTabHost Field	470
Reported GPU Memory Usage per Process is Too High	471
Event Data Filtering Examples	472
PowerShell Constrained Language mode	473
Saving uberAgent Data to Disk on the Endpoint	475
Data Storage	477
How to Configure Data Retention	478
Data Volume	478

The Data Volume Dashboard Does Not Display Values For All Metrics	479
Footprint & Performance	480
Changing the Accelerated Time Range	481
Reuse of Open HTTP Connections	483
Installation & Upgrade	485
Directories and Registry Key Created by uberAgent's Installer	485
uberAgent macOS Installation Fails When Executed From a Network Drive	486
uberAgent With Splunk Cloud: Differences to On-Premises Splunk Enterprise	486
Using uberAgent With Self-Signed Certificates	488
Licensing	490
How to Enable uberAgent on a Subset of Machines Only	490
Supported License File Names & Multiple License Files	490
Storing uberAgent's License in Azure Files	491
Logon	492
"GP logon script" is longer than "Total duration"	492
Not all CSEs Used are Listed on the Dashboard "User Logon Duration - Group Policy"	493
What is the Definition of the Metric "Pre Logon Init"	494
Logon Data Arrives Late or Never in the Backend	494
Splunk	495
Configuring Alerts	495
How to Change uberAgent's Splunk Index Name	501
Splunk Product Editions (SKUs) Supported by uberAgent	502
What to Do When You Get Splunk License Errors	503
Workaround for Lookup Errors with Splunk Free	504

User Interface	507
How to Separate Data from Different Types of Machines	507
Remoting Protocol is Console Instead of ICA or RDP	508
The Dashboards Do Not Work Correctly in Internet Explorer	508
Practice Guides	509
Detecting Network Connectivity Problems	509
Citrix ADC Monitoring & Alerting	511
Generating Driver Version Inventory Reports	514
Querying Windows Performance Counters	519
Documenting Applied Computer GPOs	520
Identifying Applications That Use 100% of a CPU Core	523
Collecting the Processor Temperature With uberAgent	524
User & Host Tagging Examples	527
Querying Windows Event Log	530
Collecting More WiFi Details From WFH Employees	533
Monitoring Windows Update Performance	538
Creating a TPM Status Inventory Report	541
Building a Browser Extension Inventory Report (Chrome/Edge/Firefox)	545
Internet Explorer: Distinguish Standalone and Edge IE Mode Starts	549
Testing the Azure AD (Entra ID) Join Status	553
Addons and Tools	556
uberAgent Event Generator for Splunk	557
Changelog and Release Notes	557
Demoing uberAgent With the Event Generator for Splunk	562

uberAgent Helpdesk Splunk App	563
Changelog and Release Notes	564
uberAgent Helpdesk Splunk App	566
uberAgent Log Collector Splunk App	574
Changelog and Release Notes	575
uberAgent Log Collector Splunk App	576

uberAgent 7.0

July 23, 2024

What is uberAgent?

uberAgent is a User Experience Monitoring (UXM) and Endpoint Security Analytics (ESA) tool that provides in-depth visibility into user experience, system performance, and security across physical and virtual endpoints. It offers detailed insights into installed application usage - including installed web browsers, and network performance. The solution is capable of providing Endpoint Security Analytics (ESA) with its highly efficient and dynamic threat detection engine and rule engine.

Why uberAgent?

uberAgent makes performance and security diagnosis a lot easier by collecting vital KPIs like latency, jitter, and packet loss –per application - including the installed browser. One agent, one solution, across all physical and virtual Windows and macOS devices.

The agent is highly efficient looking at the amount of data that it reports, as well as looking at the footprint it adds on top: less than 0.5% CPU load and a minimal amount of RAM. Customers can complement the existing EDR solutions with uberAgent.

Application adoption and licensing reporting, crash analytics on process executable level, or pinpointing performance bottlenecks? You name it, uberAgent provides the metrics and comes with 70+ dashboards that visualize the collected data.

All of this sets us apart from other monitoring vendors in the EUC space, while we supplement existing observability platforms customers have in place today.

What can uberAgent do?

- Makes user experience measurable
- Helps you identify trends that otherwise would have gone unnoticed
- Simplifies troubleshooting by showing you everything you need to know in one place
- Detects threats, risky behavior, and insecure configurations
- Shows you which applications are used when –and where
- Makes Helpdesk and IT operations more effective

- Provides visibility into endpoint performance, reliability, and security
- Provides all the endpoint metrics and KPIs required by the business

Get Started

- [Quickstart](#)
- [Installation](#)

More Information

- [About uberAgent](#)
- [Changelog and Release Notes](#)
- [New Release Information & Notification](#)
- [Products: UXM & ESA](#)
- [System Requirements](#)

Quickstart

July 30, 2024

uberAgent is an innovative Windows and macOS **user experience** monitoring and **endpoint security** analytics product. You have come to the right place if you want to get it up and running in your environment.

Getting Started

1. Start by checking out the [system requirements](#) and take a look at the [release notes](#).
2. If you have not yet done so, [install Splunk](#) or one of the alternative supported [backends](#).
3. Next, you probably want to know how to [install and deploy](#) uberAgent.

Products

uberAgent comes in [two flavors](#): uberAgent UXM (**user experience** monitoring) and uberAgent ESA (**endpoint security** analytics).

Components

uberAgent's main [component](#) is a **lightweight agent** that collects data on the endpoints and sends it to a backend of your choice. The other component is a **Splunk dashboard app** that visualizes what has been collected by the agent.

Configuration and Metrics

Metrics

Here is a list of all the [metrics](#) collected by uberAgent, neatly organized by category.

Configuration

uberAgent can be configured by way of **config files** (all platforms) or via **Group Policy** (Windows). Details in [configuration options](#).

Here is a list of steps to take in order to [reduce uberAgent's data volume](#).

Troubleshooting

uberAgent's [log files](#) help you quickly find out what is going on. They are easy to read and have a wealth of information.

If you have a question, search the [documentation](#), ask a question in the [community forum](#) or [contact support](#).

Upgrading

When a new version of uberAgent is released you might want to upgrade your installation. Here's [how to do that](#).

More Information

Take a look at our [blog articles](#) or [follow us on Twitter](#).

About uberAgent

July 9, 2024

uberAgent is an innovative Windows and macOS user experience monitoring (UXM) and endpoint security analytics (ESA) product.

uberAgent UXM highlights include detailed information about **boot and logon duration**, application unresponsiveness detection, **network reliability** drill-downs, process startup duration, **application usage** metering, browser performance, **web app** metrics, and **Citrix** insights. These varied system performance and reliability aspects are smartly brought together in the Experience Score dashboard.

uberAgent ESA excels with a sophisticated **Threat Detection Engine**, endpoint security & compliance rating, the uAQL query language, detection of **risky activity**, DNS query monitoring, hash calculation, registry monitoring, and Authenticode signature verification. uberAgent ESA comes with **Sysmon and Sigma rule converters**, a graphical rule editor, and uses a simple yet powerful query language instead of XML.

Products: UXM & ESA

July 9, 2024

uberAgent is made up of **two products**: uberAgent **UXM** and uberAgent **ESA**.

uberAgent UXM: Digital Employee Experience (DEX)

uberAgent UXM covers all aspects of digital employee experience (DEX) on any Windows or macOS endpoint. uberAgent works equally well in virtual machines as on physical PCs. It has been optimized to meet the requirements of the world's most demanding organizations, with **proven scalability** to hundreds of thousands of endpoints.

uberAgent UXM determines **application reliability** KPIs, finds issues with network connectivity, collects detailed inventory information, and shows which applications are used when and how often, to name but a small subset of its impressive features. In addition to the above, uberAgent UXM has some of the most **comprehensive Citrix monitoring** capabilities. uberAgent's browser monitoring functionality provides detailed insights into **web app usage** and performance.

More Info on uberAgent UXM

Take a look at the [uberAgent UXM features and configuration documentation](#).

uberAgent ESA: Endpoint Security Analytics

uberAgent UXM and uberAgent ESA are deeply integrated. uberAgent UXM provides rich context and metadata, while uberAgent ESA adds deep security visibility. With the combination of ESA and UXM, you need **only one agent** for digital employee experience, performance, and security. This guarantees the smallest possible footprint on the endpoint. With its flexible and open architecture, uberAgent ESA is the **perfect complement to EDR/antivirus products**.

uberAgent ESA's powerful Threat Detection Engine helps businesses **identify risky behavior**, unusual communications, suspicious executables, and common vulnerabilities. The product ships with an extensive predefined ruleset covering some of the most significant endpoint security use cases. Extending ESA's rules is easily possible and highly encouraged.

More Info on uberAgent ESA

Take a look at the [uberAgent ESA features and configuration documentation](#).

Components: Agents & Apps

July 9, 2024

uberAgent consists of **two main components**: the actual agent runs on the endpoints you want to be monitored, sending the data it collects to the configured backend either directly or via Splunk's Universal Forwarder. The second main component, implemented as a set of Splunk apps, provides dashboards, visualizations, searches, and reports.

The Agent

uberAgent's data collecting component is a lightweight agent that runs independently of any run-times or frameworks. The agent's footprint is so small that it is truly unobtrusive on the monitored endpoints and does not affect user density.

Where other products rely on operating system sources such as performance counters, WMI, or similar unfiltered data, uberAgent comes with its own metrics. Instead of raw data uberAgent gives you **information that matters** (see uberAgent's [list of metrics](#)).

The agent is **highly configurable**: metrics can be turned on or off individually, the **data collection frequency** can be chosen freely, denylists and allowlists (supporting regular expressions) enable fine-grained control. This ensures that only data you really need is sent to the backend for indexing.

Browser Extensions

uberAgent's endpoint agent is complemented by browser extensions, which enable uberAgent to collect performance and usage metrics from web apps, too. Extensions are available for all major browsers.

The Splunk Apps

Multiple Splunk apps help process and visualize the data collected by the agent. The **indexer app** lives on Splunk indexers and mainly creates uberAgent's index and data input. **Dashboard apps** implement the user interface, providing different views into the collected data. uberAgent comes with two dashboard apps: one for **uberAgent UXM** and another for **uberAgent ESA**.

uberAgent's main apps are complemented by special-purpose apps that offer a different view of the existing uberAgent data, such as the **uberAgent Helpdesk** app.

Most dashboards are searchable and have extensive filtering capabilities to give you a fast and powerful way of isolating specific data. Time range pickers make it easy to go back to the exact time a problem occurred.

uberAgent makes full use of Splunk's advanced UI components to display a beautiful user interface that fluidly adapts to screen width and device type. As a result, it works equally well on a tablet as on a PC or Mac.

Alternative Backends

uberAgent supports several backends in addition to Splunk: Azure Monitor, Elasticsearch, and Apache Kafka. Please note that at this time support is limited to sending data from the endpoint agent to the backend. Dashboards are only available for Splunk.

System Requirements

July 9, 2024

Backend

Splunk

Operating system: all that are [supported by Splunk](#)

Splunk version: Splunk Enterprise 7.0 or newer or Splunk Cloud ([details](#)).

We only support uberAgent on Splunk software that is officially supported by Splunk ([details](#)).

Endpoints

Windows

Operating system:

- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

All Windows versions are supported in 32-bit (where applicable) and 64-bit. We only support uberAgent on Windows versions that are officially supported by Microsoft.

Windows Agent Service Account The main component of uberAgent's endpoint agent is a system service that needs to run as the local SYSTEM account because that is required by some APIs.

macOS

Operating system:

- macOS 10.15.6 (Catalina) or above

Citrix Virtual Apps and Desktops, Microsoft RDS, VMware Horizon View

Remote desktop session hosts (e.g. Citrix XenApp/CVAD, VMware Horizon View, Microsoft RDS) are explicitly supported. The same applies to any kind of virtual desktop (e.g. Citrix XenDesktop/CVAD, VMware View).

Windows Virtual Desktop

uberAgent supports Windows Virtual Desktop (WVD) environments running on Microsoft Azure.

IaaS (AWS EC2, Azure VMs)

uberAgent supports cloud infrastructure as a service offerings such as Amazon AWS EC2, Azure VMs, and similar in any region.

Browser Extensions

Chrome

Google Chrome 41 or newer

Edge

Microsoft Edge 80 or newer

Internet Explorer

Microsoft Internet Explorer 11

Firefox

Mozilla Firefox 50 or newer

Endpoint Agent Features

Citrix Virtual Apps and Desktops Site Monitoring

- CVAD delivery controller version 7.6 or newer

Citrix ADC Monitoring

- At least PowerShell version 3.0
- At least Citrix ADC firmware version 10.5

Citrix Cloud Monitoring

- Citrix Virtual Apps and Desktops Remote PowerShell SDK

Alternative Backends

Apache Kafka

- Confluent REST Proxy 5.4.x or newer
- Confluent Schema Registry 5.4.x or newer
- Any Apache Kafka version supported by the Confluent components above

Elasticsearch & Kibana

- At least Elasticsearch 7.12.x
- At least Kibana 7.12.x

Microsoft Azure Log Analytics

- No specific requirements

Changelog and Release Notes

July 9, 2024

Version 7.0

New features

- **Citrix session monitoring (Windows) [B19]:** uberAgent now determines bandwidth usage per Citrix HDX virtual channel, records applied Citrix session policies & collects important session state information (including video codec and color space).

- **Elasticsearch 8 [B274]:** added support for Elasticsearch 8 and Elasticsearch data streams.
- **Event triggers for timers (Windows) [B267]:** new event-based trigger option for timers to collect data when something happens, e.g., a user logs on. Event triggers are compatible with classic timers that collect data at fixed intervals.
- **Intelligent disk buffering [B636]:** evolution of the persistent output queue introduced with 6.2. Events are sent directly to the backend if possible; events are only buffered to disk if network connectivity is unavailable.
- **MITRE ATT&CK integration [B561]:** all uberAgent ESA rules now come with MITRE ATT&CK technique ID annotations. MITRE ATT&CK technique information is displayed in the *Activity Monitoring Events* dashboard.
- **Nutanix Frame integration (Windows) [B702]:** uberAgent now collects session metrics for Nutanix Frame sessions.
- **Performance counters (Windows) [B262, B674]:** new dashboard for Windows performance counters; support for wildcards in counter paths.
- **Process statistics (Windows) [B517]:** uberAgent now collects additional process information, e.g., handle count, private & virtual memory usage, priority, and page faults.
- **Protected processes (Windows) [B626]:** uberAgent now also collects data from protected processes (e.g., EDR & antivirus products).
- **Splunk Enterprise Security [B561]:** new Splunk *uberAgent ESA Enterprise Security companion app* to integrate ESA metrics in Splunk's *Risk Based Alerting* with support for event annotations (MITRE ATT&CK and others).
- **System time change resilience (Windows) [I87]:** durations and other time measurements are now determined correctly even if the interval overlaps with system time changes.

Improvements

- **Activity monitoring [B730]:** the converted Sigma ruleset has been updated.
- **Application errors (macOS) [B634]:** the sourcetype `uberAgent:Application:Errors` is now supported for application crashes with a corresponding system report in `.ips` format (Monterey).
- **Application errors (macOS) [B634]:** the sourcetype `uberAgent:Application:Errors` now supports the fields `ModulePath` and `ModuleVersion` on macOS as well.
- **Application errors (macOS) [B634]:** the sourcetype `uberAgent:Application:Errors` now contains two additional fields on macOS: `ProcImageUUID` and `ModuleImageUUID`. These fields allow the unique identification of a crashed binary image.
- **Application identification (macOS) [B686]:** application versions are now reported uniformly in the standard macOS format.
- **Authenticode signature verification [B705]:** new property `IsSignedByOSVendor` for `Process`, `Parent`, and `Image`.

- **Boot monitoring (Windows) [I736]:** improved determination of parent process properties.
- **Browsers [B579]:** when configuring full URL monitoring, query parameters in the component detail specification are now interpreted as regular expressions. This makes it possible to use wildcards or to specify more sophisticated patterns that define which query parameters are to be included in the collected data. This feature requires at least version 3.1.0 of the uberAgent browser extensions. The uberAgent Internet Explorer add-on does not support this.
- **Citrix Cloud monitoring [I593]:** avoid parallel determination of Citrix Cloud metrics and Citrix authentication token. This only resulted in an error within the log file if an invalid Cloud configuration exists.
- **Citrix Cloud monitoring [I605]:** use the `ConfigFlag: NetworkCommunicationTimeoutMs` for all Citrix Cloud network calls.
- **Citrix Cloud monitoring [B644]:** exchanged deprecated Trust Service Flow API with OAuth 2.0 API.
- **Citrix Cloud monitoring (Windows) [B687]:** use configuration option for disabling or ignoring TLS certificate revocation (CRL) checks for HTTPS transmissions.
- **Configuration (macOS) [B558]:** the timer setting `Persist interval` is now supported on macOS, too.
- **Configuration [B563, I638]:** any configuration stanza can now be platform-specific using `platform=Windows` or `platform=macOS` in its configuration.
- **Configuration (Windows) [B652]:** the new section `ActivityMonitoringRule_Filter` adds a new allow-/denylist to configure [ActivityMonitoringRule] entries.
- **Dashboards [B19]:** new dashboards *Citrix Session Protocol Insights*, *Citrix Session Configuration Details*.
- **Dashboards [B19]:** in case of a Citrix session, additional information is displayed on the *Analyze timechart* and *Single User Detail* dashboards.
- **Experience Score [B547]:** new individual dashboards for machine, session, and application scores for detailed analysis of scores.
- **Experience Score [B547]:** better search performance for score calculation.
- **Experience Score [B659]:** scores are no longer aggregated for the past day at midnight. Instead, scores stay in raw format in the score index.
- **Installer (macOS) [B627]:** templates for configuration files are now installed to `/Library/Application Support/uberAgent/Config Templates` and copied to the parent directory only if the file does not already exist in the parent directory.
- **Logging (Windows) [I733]:** removed unnecessarily logged messages if it is impossible to determine a Remote Desktop client IP.
- **Logon monitoring (Windows) [I570]:** improved logon/logoff monitoring for short-lived sessions.
- **Logon monitoring (Windows) [I570]:** fixed a rare circumstance where logon monitoring end is not detected correctly.

- **Machine inventory (Windows) [I530]:** determine correct user-friendly OS version string for in-place Windows upgrades.
- **Machine inventory (Windows) [B677]:** virtual machine detection is more accurate now and should not emit false positive results in VM hosts anymore.
- **Machine inventory (Windows) [B678]:** determine hypervisor vendor name and display it in single machine dashboard.
- **Machine inventory (macOS)[B693]:** in addition to the detection if macOS is running in a virtual machine, the hypervisor vendor is now detected as well.
- **Network monitoring (macOS) [B633]:** network connection failures are now determined on macOS, too.
- **Process details (macOS) [B557]:** the `uberAgent:Session:ProcessDetail` field `ProcNetKBPS` is now determined on macOS, too.
- **Service (Windows) [B728]:** increased default values for maximum number of elements in internal hashes list.
- **Service (Windows) [I622]:** stop error metrics are reported for Event Log events with IDs 1001 and 41.
- **Splunk [B607]:** implemented a new Splunk data model architecture.
- **Splunk [B666]:** enabled auto-skewing for all saved searches.
- **Splunk [B667]:** added `sc_admin` permissions to meet Splunk Cloud requirements.
- **Splunk [B679]:** added more CIM fields for the source types `uberAgent:Process:ProcessStartup` (uberAgent UXM) and `uberAgent:Process:ProcessStop` (uberAgent ESA). *Thanks to Alexander Schüller!*
- **Tagging (Windows) [B507]:** changed user/host tags determination from a hard-coded interval to a new timer metric `UserTags` and `HostTags`.
- **Tagging (Windows) [I657, I758]:** improved determination of user tags.
- **uAQL (Windows) [B592]:** added support for reading registry data in uAQL queries.

Bugfixes

- **Application errors (macOS) [I591]:** fixed very rare doubly reported crash of uberAgent itself.
- **Application errors (macOS) [I600]:** events with the sourcetype `uberAgent:Application:Errors` are now sent with the timestamp of the crash, not the timestamp of the detection of a crash.
- **Application errors (macOS) [I608]:** the field `FaultOffset` in the sourcetype `uberAgent:Application:Errors` was erroneously sent as an absolute address instead of an offset relative to the base image address.
- **Application errors (macOS) [I719]:** events of the sourcetype `uberAgent:Application:Errors` might have been empty in some rare cases in which multiple crashes occurred in a very short time frame.

- **Application identification (Windows) [I529]:** all Windows 11 UWP applications and their app names are now determined correctly.
- **Application identification (macOS) [I602]:** the formatting of the field `AppVersion` now follows the macOS versioning convention of `version (buildnumber)` e.g. `1.2.3 (4567)`.
- **Application identification (Windows) [I696]:** Java `AppName` and `AppID` identification was sometimes incorrect.
- **Authenticode signature verification (Windows) [B626]:** fixed a very rare case where no hash was calculated for an executable.
- **Authenticode signature verification (Windows) [I539]:** CPU usage for Authenticode validation of executables significantly reduced.
- **Boot monitoring (Windows) [I29]:** the field `AutostartServicesMs` was empty on Windows 10 or newer.
- **Browsers (macOS) [I626]:** fixed faulty filtering of invalid data sent from Firefox.
- **Citrix Cloud monitoring [I565]:** metrics collection was stopped for all Cloud instances if authentication failed for one such instance.
- **Citrix site/Cloud monitoring (Windows) [I574]:** Citrix metrics were not determined for older Citrix versions.
- **Daemon (macOS) [I540]:** introduced controlled shutdown of uberAgent, and fixed race condition in ES client.
- **Daemon (macOS) [I567]:** fixed cases where uberAgent would crash upon shutdown.
- **Dashboards [I545]:** fixed experience score chart error after drilldown from *User Sessions* to *Analyze Data Over Time* dashboard.
- **Dashboards [I577]:** fixed drilldown on the data table on the dashboard *Process UI Unresponsiveness*.
- **Dashboards [I582]:** fixed wrong distinct counts for applications and users on the dashboards *Application Network Issues* and *Machine Network Issues*.
- **Dashboards [I598]:** fixed wrong includes on *Machine Storage* dashboards that caused JavaScript errors with Splunk version 8.2.5.
- **Dashboards [I601]:** reimplemented custom single value visualization to fix JavaScript error in Splunk Cloud.
- **Dashboards [I651]:** filters were not applied on the chart *Average logon duration over time* on the dashboard *User Session Overview*.
- **Dashboards [I712]:** fixed wrong network and performance timechart calculations.
- **Dashboards [I743]:** the *Power button timestamp* field in the table *Stop error detail* on the dashboard *Stop Errors (Blue Screen & Power Loss)* showed a misleading timestamp when power button was not pressed.
- **Dashboards [I753]:** removed deprecated JS/CSS includes from various dashboards.
- **Dashboards [I778]:** fixed drilldown on the *Process DNS* dashboard for process names containing spaces.

- **DNS query monitoring (Windows) [I555]:** fixed high CPU load with many DNS entries.
- **DNS query monitoring [I727]:** the field `ProcGUID` of sourcetype `uberAgentESA:Process:DnsQuery` was empty.
- **Event data filtering [I546]:** clearing or changing fields now applies to each receiver individually.
- **Experience Score [B547]:** added missing application scores to the `Single Application Detail` dashboard.
- **Experience Score [I537]:** fixed errors in the machine and application score calculations.
- **GPU (Windows) [I721]:** fixed rare issue during determination of GPU metrics that caused a warning message about too high GPU compute usage.
- **GPU (Windows) [I760]:** the `GpuUsageEngine` field `GpuEngineComputeUsagePercent` was always zero if more than one graphic card is present.
- **GPU (Windows) [I771]:** the `GpuUsageEngine` metric was not sent on some non-English Windows systems.
- **In-session helper (macOS) [I735]:** fixed erroneous restarts if using multiple profiles under Chrome.
- **Installer (macOS) [I701]:** added a grace period of up to sixty seconds to allow uberAgent to send all pending events in case of a shutdown.
- **Kafka [I746]:** the schema was changed to avoid warnings in the REST log file like: *Ignored the uberAgent_Application_SoftwareUpdateInventory.time.logicalType property.*
- **License verification (macOS) [I569]:** fixed an issue where license files containing non-ASCII characters could not be verified.
- **Logging [I442]:** reduced CPU load by improving logger performance.
- **Logging [I490]:** logging of http receiver errors and warnings only once per host.
- **Logging [I564]:** `ConfigFlagTraceLogFilterExpression` is checked only for trace log messages.
- **Logon monitoring (Windows) [I617]:** fixed a rare issue where logon monitoring could crash the `uberAgent.exe` process.
- **Network monitoring (macOS) [I365]:** removed unreliable pcap statistics from logging.
- **Network monitoring (macOS) [I550]:** fixed rare cases of miscalculated values for `NetTargetSendJitterMs`, `NetTargetSendLatencyMs` and `NetTargetSendLatencyInitial`.
- **Network monitoring (macOS) [I589]:** fixed overflow in hash calculation, which could lead to memory corruption.
- **Network monitoring (macOS) [I610]:** fixed differing metrics between Windows and macOS.
- **Network monitoring (macOS) [I676]:** fixed wrong timestamps for DNS query events.
- **Network monitoring (Windows) [I687]:** uberAgent's network driver could slow down network transfers or freeze the system with some network drivers, e.g., Nutanix VirtIO Ethernet Adapter.
- **Persistent output queue [I527]:** events would be lost if Elasticsearch, Kafka or Azure Monitor

backends were not reachable at service shutdown.

- **Persistent output queue (Windows) [I528]:** updated the receiver server URL within the persistent output queue file if needed.
- **Persistent output queue [I729]:** fixed issue during service start if corrupt persistent output queue files exist.
- **Process monitoring (macOS) [I563]:** events could no longer be processed if more than 100k processes had been created within a short timeframe (PID wrapping).
- **Process monitoring (Windows) [I599]:** fixed rare issue during determination of process image path.
- **Process monitoring (macOS) [I705]:** fixed possible crash while handling events generated by the Endpoint Security framework.
- **Process startup (macOS) [I503]:** fixed missing process user for short-lived processes.
- **Process startup (macOS) [I516]:** fixed cases where short process lifetimes and faulty lookups created inconsistent AppIDs.
- **Process startup (macOS) [I628]:** fixed bug in retrieval of the process name for sourcetype `ProcessStartup`.
- **Process startup (macOS) [I749]:** the field `SessionID` is now available for sourcetype `uberAgent:Process:ProcessStartup`. Please also note the corresponding release notes.
- **Scheduled task monitoring [I559]:** made use of Splunk macros for each dataset's datamodel.
- **Service (Windows) [I776]:** fixed rare issue that trimmed whitespaces while parsing command line output of started scripts.
- **Sessions (Windows) [I584]:** fixed rare issue during determination of session connection information.
- **Sessions (Windows) [B702]:** when no data for the field `SessionClientHwIdCtx2` could be determined, the field's content was `0` instead of empty.
- **Splunk CIM data model [I560]:** added missing `report` tag for processes.
- **Splunk [I588]:** removed the usage of search macros in `eventtypes.conf`.

Release notes

- **Configuration [B521]:** the timer setting `Thread priority` was marked as deprecated and removed from the default configuration.
- **Configuration [B652]:** the configuration stanza `[ActivityMonitoringRule]` now has a new mandatory setting: `RuleId`.
- **Configuration [I605]:** new `ConfigFlag: NetworkCommunicationTimeoutMs`.
- **Configuration (macOS) [I749]:** the field `SessionID` of sourcetype `uberAgent:Process:ProcessStartup` is only available if both metrics `SessionDetail` and `ProcessStartup` are configured to run in the same timer. This also applies to `SessionDetail`

and `ProcessDetail(Full)`.

- **Dashboards [B19]:** removed dashboard *Session Info: Citrix* and merged its content into *Citrix Session Configuration Details*.
- **Elasticsearch 8 [B274]:** the field `time` was changed to `@timestamp` to support Elasticsearch data streams.
- **Libraries [B729]:** updated Boost to version 1.78.
- **Libraries [B729]:** updated curl to version 7.81.0.
- **Libraries [B729]:** replaced the stand-alone version of Asio with Boost Asio.
- **Libraries [B729]:** replaced the RapidJSON library with the nlohmann JSON library.
- **Persistent output queue [B636]:** intelligent disk buffering via the persistent output queue is now enabled by default. This can be changed through the receiver configuration setting `PersistentOutputQueue`.
- **Sourcetype [B19]:** new sourcetype `uberAgent:CitrixSession:VirtualChannelDetail` with fields: `SessionGUID, SessionUser, VirtualChannelVendorName, VirtualChannelData, VirtualChannelDataVolumeOutputMB`.
- **Sourcetype [B19]:** new sourcetype `uberAgent:CitrixSession:SessionConfig` with fields: `SessionGUID, SessionUser, AudioActualPriority, AudioPolicyAllowMicrophone, AudioPolicyAllowRedirection, AudioPolicyPriority, AudioPolicySoundQuality, CdmActualPriority, CdmVolumes, CdmPolicyAllowDriveRedirection, CdmPolicyPriority, CdmPolicyReadOnly, DisplayMode, ThinwireActualPriority, ThinwireColorDepth, ThinwireComponentEncoder, ThinwireHardwareEncodeInUse, ThinwireVideoCodecType, ThinwireColorspace, ThinwireVideoCodecUse, ThinwirePolicyFps, ThinwirePolicyPriority, ThinwirePolicyUseHardwareEncoding, ThinwirePolicyUseVideoCodec, ThinwirePolicyVisualQuality, FramehawkActualPriority, FramehawkPolicyPriority, D3DActualPriority, D3DPolicyAeroRedirection, D3DPolicyGraphicsQuality, D3DPolicyPriority, GraphicsActualPriority, GraphicsPolicyDisplayDegradeNotifyUser, GraphicsPolicyDisplayDegradePolicy, GraphicsPolicyPriority, NetworkConnectedVia, NetworkEdtMtu, NetworkPolicyAccept, NetworkPolicyICAListenerPortNumber, NetworkPolicySessionReliabilityPort, NetworkPolicySessionReliabilityTimeout, PrinterActualPriority, PrinterSessionPrinter, PrinterPolicyAllowRedirection, PrinterPolicyAutoCreate, PrinterPolicyPriority, USBActualPriority, USBPolicyAllowPNPRedirection, USBPolicyAllowUSBSupport, USBPolicyPriority`.
- **Sourcetype [B517]:** new sourcetype `uberAgent:Process:ProcessStatistics` with fields: `ProcHandleCount, ProcThreadCount, ProcPriority, ProcPrivateMB, ProcVirtualSizeMB, ProcPageFaultsPS, ProcPageFileMB, ProcName, ProcID, ProcGUID, ProcUser` and `AppId`.
- **Sourcetype [B674]:** new sourcetype `uberAgent:System:PerformanceCounter` with fields: `PerformanceCounterObject, PerformanceCounterInstance`,

PerformanceCounterName, PerformanceCounterValue.

- **Sourcetype [B678]:** `uberAgent:System:MachineInventory` has new field(s): `HwHypervisorVendor`.
- **Sourcetype [B19]:** `uberAgent:Session:SessionDetail` has new field(s): `SessionRoundTripTime`, `SessionFps`, `SessionTransportProtocols`.
- **Sourcetype (macOS) [B634]:** the sourcetype `uberAgent:Application:Errors` no longer contains data in the field `ProcTimestamp` on macOS, since this metric can be confusing, e.g., if an application crashes during an update or the binary on disk was deleted during runtime.
- **Sourcetype [B675]:** `uberAgent:Citrix:Applications` has new field(s): `CustomerId`.
- **Sourcetype [B675]:** `uberAgent:Citrix:Catalogs` has new field(s): `CustomerId`.
- **Sourcetype [B675]:** `uberAgent:Citrix:DesktopGroups` has new field(s): `CustomerId`.
- **Sourcetype [B675]:** `uberAgent:Citrix:Machines` has new field(s): `CustomerId`.
- **Sourcetype [B675]:** `uberAgent:Citrix:PublishedDesktops` has new field(s): `CustomerId`.
- **Sourcetype [B674]:** replaced KV sourcetype `uberAgent:PerformanceCounter:` with CSV sourcetype `uberAgent:System:PerformanceCounter`.
- **Sourcetype [B672]:** `uberAgent:Application:ApplicationUsage` has been removed (it was marked as deprecated as of version 6.1.1).
- **Sourcetype:** the sourcetypes `uberAgent:Citrix:Hypervisor`, `uberAgent:OnOffTransition:SlowSMSSInit` and `uberAgent:OnOffTransition:SlowUserPolicy` are now marked as deprecated. They have been removed from the uberAgent UXM data models.
- **Splunk:** the minimum required Splunk version is now 7.0 (formerly 6.6).
- **Splunk data models [B607]:** removed the data models `uberAgent`, `uberAgent_Score`, `uberAgent60m`, `uberAgent_ESA`.
- **Splunk data models [B607]:** added the uberAgent UXM data models `uberAgentUXM_Application`, `uberAgentUXM_Citrix`, `uberAgentUXM_CitrixADC`, `uberAgentUXM_CitrixSession`, `uberAgentUXM_License`, `uberAgentUXM_Logoff`, `uberAgentUXM_Logon`, `uberAgentUXM_OnOffTransition`, `uberAgentUXM_Process`, `uberAgentUXM_Score`, `uberAgentUXM_Session`, `uberAgentUXM_System`, `uberAgentUXM_Tags`.
- **Splunk data models [B607]:** added the uberAgent ESA data models `uberAgentESA_ActivityMonitoring`, `uberAgentESA_Process`, `uberAgentESA_System`.

Known issues

- **Boot duration (Windows):** the metrics `TotalBootTimeMs`, `MainPathBootTimeMs` and `PostBootTimeMs` cannot be determined for every system boot.
- **Browsers/IE add-on (Windows):** metrics are not collected on page reload.
- **Browsers/IE add-on (Windows):** metrics are collected incompletely for the configured start page.
- **Browsers/IE add-on (Windows):** monitoring does not work if IE is published from Citrix Virtual Apps. It does work from Citrix Virtual Desktops, however.
- **Browsers/Firefox add-on:** if the option `privacy.resistFingerprinting` is set to true, browser metrics are not available due to invalid data being sent from Firefox.
- **Citrix ADC:** in very rare cases, the content of the Virtual Server Performance field `vServerName` contains spaces in wrong places.
- **Citrix site monitoring (Windows):** data collection issue if the Citrix Remote Powershell SDK (required for Citrix Cloud monitoring) is installed on a CVAD controller.
- **Citrix XA/XD Machines (Windows):** when running the Citrix VDA on a Citrix Delivery Controller, some per-machine information is missing.
- **Experience score [I377]:** scheduled searches generate three warnings in Splunk's `_internal` index every 30 minutes. The messages look like the following: `DateParserVerbose - Failed to parse timestamp in first MAX_TIMESTAMP_LOOKAHEAD (128) characters of event..` However, there is no impact on uberAgent's functionality.
- **GPU (Windows) [I33]:** values for the fields `ComputeUsagePercentAllEngines`, `ComputeUsagePercentEngine0` and similar can be higher than 100 with Intel Iris GPUs on Windows Server 2016 1607.
- **Kafka [I291]:** in rare cases sending data to Kafka results in a `SEC_E_BUFFER_TOO_SMALL` error message in the logfile. This should have no effect; the transmission is repeated and succeeds on the second try.
- **Network monitoring (Windows) [I815]:** network metrics may be missing: 1) after resuming from a low-power state (e.g., suspend), or 2) after certain disastrous network events such as a crash of the default gateway.
- **Performance [I372] (macOS):** running uberAgent has a noticeable impact on I/O performance of small writes. If the config flag `DisableESFileSystemMonitoring` is enabled, performance is not impacted, but the fields `ProcIOWriteCount` and `ProcIOPSWrite` are not available in `uberAgent:Process:ProcessDetail`.
- **Update inventory (Windows):** not all installed Windows updates may be reported due to API limitations.
- **Volume inventory (macOS):** the encryption status of mounted read-only APFS snapshots may not be reported due to API limitations. This includes the root directory volume in a default installation of macOS.

Default Configuration

July 9, 2024

This page lists uberAgent's default configuration that is in effect if the endpoint agent is installed without making any changes.

uberAgent can be configured via config files or via Active Directory Group Policy (see [configuration options](#)).

uberAgent.conf

July 22, 2024

`uberAgent.conf` is uberAgent's main configuration file. It [includes](#) additional configuration files for uberAgent ESA which are maintained in the [uberAgent-ESA-rules GitHub repository](#) where they're updated frequently.

The content of the `uberAgent.conf` file that ships with uberAgent is listed below. An [alternative configuration file that is optimized for data volume](#) is available, too.

```
1 #
2 # This is the default configuration file for uberAgent
3 # On Windows, place it in the same directory as uberAgent.exe
4 #
5 # On macOS, this file must be located in /Library/Application Support/
6 # uberAgent. Make sure to save changes to this file as uberAgent.conf.
7 # uberAgent-default.conf serves as a fallback, and is overwritten with
8 # the most current default configuration during updates.
9 #
10 #
11 #
12 # Documentation: /en-us/uberagent/7-0-0/installation/configuration-
13 # through-config-file.html
14 #
15 #
16 # #####
17 #
18 # Products
19 #
20 # a) UXM (User Experience Monitoring)
21 #
22 # This is the default product. It is always enabled.
23 #
24 # b) ESA (Endpoint Security Analytics)
25 #
26 # ESA is an optional add-on product that requires UXM to work.
27 # Please note that ESA must be licensed independently of UXM.
```

```
23 #
24 # Configurable settings in this section:
25 #
26 #   Setting name: EnableESA
27 #   Description: Enables the Endpoint Security Analytics product
28 #   Valid values: true | false
29 #   Default: false
30 #   Required: no
31 #
32 #####
33
34 [ProductComponents]
35 EnableESA = true
36
37 #####
38 #
39 # General configuration
40 #
41 # Configurable settings in this section:
42 #
43 #   Setting name: DebugMode
44 #   Description: When in debug mode, uberAgent's log file is more
45 #   verbose, providing more detail on what is going on.
46 #   Valid values: true | false
47 #   Default: false
48 #   Required: no
49 #
50 #   Setting name: LogFileCount
51 #   Description: Number of log files to keep (current + historical).
52 #   When exceeded, the oldest log file is deleted.
53 #   Valid values: any positive integer
54 #   Default: 5
55 #   Required: no
56 #
57 #   Setting name: EncryptUserNames
58 #   Description: If enabled, user and domain names are encrypted in the
59 #   agent before being sent off to Splunk. This can be useful for
60 #   compliance with privacy regulations.
61 #   Valid values: true | false
62 #   Default: false
63 #   Required: no
64 #
65 #   Setting name: LicenseFilePath
66 #   Description: Path to a directory where uberAgent searches for
67 #   license files. For more details see /en-us/uberagent/7-0-0/uxm-
68 #   features-configuration/central-license-file-management.html
69 #   Valid values: Any valid path (local or UNC)
70 #   Default: empty
71 #   Required: no
72 #
73 #   Setting name: RegisterIEAddOn
74 #   Description: Register or deregister uberAgent's Internet Explorer
75 #   add-on through the service.
```



```
69 # Valid values: 0 = do nothing, 1 = register the add-on, 2 =
    # deregister the add-on
70 # Default: 0
71 # Required: no
72 #
73 # Setting name: BrowserDataCollection
74 # Description: Enable or disable data collection of uberAgent's
    # browser extensions. Currently this setting is used only in our
    # Firefox extension.
75 # Valid values: 0 = do nothing, 1 = enable data collection, 2 =
    # disable data collection
76 # Default: 1
77 # Required: no
78 #
79 # Setting name: RegistryMonitoring
80 # Description: When disabled (false), no registry monitoring is
    # performed. Registry monitoring requires ESA being enabled.
81 # Valid values: true | false
82 # Default: true
83 # Required: no
84 #
85 # Setting name: RemoteThreadMonitoring
86 # Description: When disabled (false), no remote thread monitoring is
    # performed. Remote Thread monitoring requires ESA being enabled and
    # Activity Monitoring being configured.
87 # Valid values: true | false
88 # Default: true
89 # Required: no
90 #
91 # Setting name: ConfigFlags
92 # Description: Define additional implementation defined flags.
93 # Valid values: A comma- or semicolon-separated list of any of the
    # following strings
94 #     - NoGatewayCheck                - disable the check for a
    # configured Default Gateway for non-PPP network interfaces
95 #     - IEIgnoreFrames                - disable determination of
    # performance data for frames in Internet Explorer
96 #     - RegMonSvcDebugOutput          - enable Registry
    # Monitoring debug output to ProcMon
97 #     - TLSRevocationChecksDisabled  - disable certificate
    # revocation checks, e.g. during testing with self-signed certificates
    # on the backend (Windows only)
98 #     - TLSRevocationChecksBestEffort - ignore certificate
    # revocation checks in case of missing or offline distribution points
    # (Windows only). If both revocation check options are configured, the
    # option above takes precedence. For more details on these two
    # options see https://curl.se/libcurl/c/CURLOPT\_SSL\_OPTIONS.html
99 #     - EnableESFileSystemMonitoring - collects data for the
    # fields ProcIOWriteCount and ProcIOPSWrite of the sourcetype
    # ProcessDetail on macOS. May increase uberAgent's CPU utilization.
100 #     - SessionHelperQueryDelayMs:NUMBER - delay between queries to
    # in-session helper processes. Replace NUMBER with any integer >= 0
    # to specify the delay in ms.
```



```
101 # - TraceLogFilterExpression:REGEX - include messages
    matching the regular expression REGEX in the log, regardless of
    their log level. This includes trace-level messages not included
    with DebugMode = true. REGEX must match the complete source string.
102 # - EnableSystemLog - send log entries to the
    system's native log system in addition to the log file. Only
    available on macOS.
103 # - CitrixSDKMaxRecordCount:NUMBER - defines the -
    MaxRecordCount parameter for each Citrix (Remote) PowerShell SDK
    call. Replace NUMBER with any integer >= 0 (default is 1000).
104 # - CitrixODataAPIMaximumAttempts:NUMBER - defines the maximum
    amount of repeating API queries if a query is responding with a not
    successful status code (default is 10).
105 # - POQSendWaitDelayMs:NUMBER - defines the delay
    between two send attempts if the persistent output queue is
    processed (default is 500ms). Valid values are between 100 and
    10000.
106 # - NetworkCommunicationTimeoutMs:NUMBER - defines a timeout for
    network communication (default is 100000ms). Valid values are between
    100 and 1000000.
107 # - LockEnterMaxWaitMs:NUMBER - defines a duration in
    milliseconds if an internal locking mechanism took too long to enter/
    succeed. A trace log message will be written. Valid values are >=
    100 (default is 1000).
108 # - LockHeldMaxWaitMs:NUMBER - defines a duration in
    milliseconds if an internal locking mechanism was held for more than
    the defined number. A trace log message will be written. Valid
    values are >= 100 (default is 1000).
109 # Default: empty
110 # Required: no
111 #
112 #####
113
114 [Miscellaneous]
115 DebugMode = true
116
117 #####
118 #
119 # Data receivers
120 #
121 # uberAgent sends data to the receivers configured here.
122 # If multiple [Receiver] sections are specified, data will be sent to
    EACH receiver. This can be overridden per Timer by specifying a
    comma-separated list of receivers.
123 # To load-balance and fail over between servers specify multiple comma-
    separated values for "Servers" in a SINGLE receiver section
124 #
125 # The documentation for the Persistent Output Queue options can be
    found here: /en-us/uberagent/7-0-0/advanced-topics/persistent-output
    -queue.html
126 #
127 # Configurable settings in this section:
128 #
```

```
129 # Setting name: Name
130 # Description: Arbitrary name for the data receiver. If no persistent
    # output queue is configured the name is used only internally.
    # Otherwise the name is used as an appendix for the persistent output
    # queue file name.
131 # Valid values: any string
132 # Default: empty
133 # Required: Required only if persistent output queue is activated for
    # this receiver. In this case the name must be unique for all
    # receivers.
134 #
135 # Setting name: Type
136 # Description: Receiver type.
137 # Valid values: Splunk | Elasticsearch | OMSLogAnalytics | Kafka
138 # Default: Splunk
139 # Required: yes
140 #
141 # Setting name: Protocol
142 # Description: How to send data to the backend.
143 #     TCP uses a direct TCP connection
144 #     HTTP sends to a REST endpoint via HTTP or HTTPS
145 #     For type Splunk use TCP or HTTP, for all other types use HTTP.
146 # Valid values: TCP | HTTP
147 # Default: TCP
148 # Required: no
149 #
150 # Setting name: Servers
151 # Description: List of target servers/URLs.
152 # Valid values:
153 #     TCP: comma-separated list of server:port, e.g.: localhost:19500,
    # splunksrv:12345
154 #     HTTP: comma-separated list of URLs starting with http or https.
155 #     Splunk example: http://server1:8088, https://server2:8088
156 #     OMS Log Analytics example: https://CUSTOMERID.ods.opinsights.
    # azure.com
157 # Default: empty
158 # Required: yes
159 #
160 # Setting name: RESTToken
161 # Description: Authentication token required by the Splunk HTTP Event
    # Collector and by OMS Log Analytics.
162 #     For Type OMSLogAnalytics use the primary or the secondary key for
    # the workspace.
163 #     For Type Elasticsearch credentials in format
```

uberAgent-data-volume-optimized.conf

July 22, 2024

The following is the `uberAgent-data-volume-optimized.conf` configuration file that ships with uberAgent. It can be used in place of the [default configuration file](#) if the data volume generated by the agent needs to be minimized ([details](#)).

```
1 #
2 # This is a configuration file for uberAgent optimized for small data
   volume.
3 # To use it on Windows in place of the default configuration:
4 #   - rename the default configuration file uberAgent.conf to uberAgent
   .conf.bak
5 #   - rename this file to uberAgent.conf
6 #   - place this file in the same directory as uberAgent.exe
7 #
8 # To use it on macOS in place of the default configuration:
9 #   - rename the default configuration file uberAgent.conf to uberAgent
   .conf.bak
10 #   - rename this file to uberAgent.conf
11 #   - place this file in the same directory as uberAgent.exe
12 #
13 #
14 # Documentation: /en-us/uberagent/7-0-0/installation/configuration-
   through-config-file.html
15 #
16 #
17 #####
18 #
19 # Products
20 #
21 # a) UXM (User Experience Monitoring)
22 #
23 #   This is the default product. It is always enabled.
24 #
25 # b) ESA (Endpoint Security Analytics)
26 #
27 #   ESA is an optional add-on product that requires UXM to work.
   Please note that ESA must be licensed independently of UXM.
28 #
29 # Configurable settings in this section:
30 #
31 #   Setting name: EnableESA
32 #   Description: Enables the Endpoint Security Analytics product
33 #   Valid values: true | false
34 #   Default: false
35 #   Required: no
36 #
37 #####
38 #
39 [ProductComponents]
40 EnableESA = true
41 #
42 #####
43 #
44 # General configuration
```

```
45 #
46 # Configurable settings in this section:
47 #
48 #   Setting name: DebugMode
49 #   Description: When in debug mode, uberAgent's log file is more
50 #   verbose, providing more detail on what is going on.
51 #   Valid values: true | false
52 #   Default: false
53 #   Required: no
54 #
55 #   Setting name: LogFileCount
56 #   Description: Number of log files to keep (current + historical).
57 #   When exceeded, the oldest log file is deleted.
58 #   Valid values: any positive integer
59 #   Default: 5
60 #   Required: no
61 #
62 #   Setting name: EncryptUserNames
63 #   Description: If enabled, user and domain names are encrypted in the
64 #   agent before being sent off to Splunk. This can be useful for
65 #   compliance with privacy regulations.
66 #   Valid values: true | false
67 #   Default: false
68 #   Required: no
69 #
70 #   Setting name: LicenseFilePath
71 #   Description: Path to a directory where uberAgent searches for
72 #   license files. For more details see /en-us/uberagent/7-0-0/uxm-
73 #   features-configuration/central-license-file-management.html
74 #   Valid values: Any valid path (local or UNC)
75 #   Default: empty
76 #   Required: no
77 #
78 #   Setting name: RegisterIEAddOn
79 #   Description: Register or deregister uberAgent's Internet Explorer
80 #   add-on through the service.
81 #   Valid values: 0 = do nothing, 1 = register the add-on, 2 =
82 #   deregister the add-on
83 #   Default: 0
84 #   Required: no
85 #
86 #   Setting name: BrowserDataCollection
87 #   Description: Enable or disable data collection of uberAgent's
88 #   browser extensions. Currently this setting is used only in our
89 #   Firefox extension.
90 #   Valid values: 0 = do nothing, 1 = enable data collection, 2 =
91 #   disable data collection
92 #   Default: 1
93 #   Required: no
94 #
95 #   Setting name: RegistryMonitoring
96 #   Description: When disabled (false), no registry monitoring is
97 #   performed. Registry monitoring requires ESA being enabled.
```

```
86 # Valid values: true | false
87 # Default: true
88 # Required: no
89 #
90 # Setting name: RemoteThreadMonitoring
91 # Description: When disabled (false), no remote thread monitoring is
    performed. Remote Thread monitoring requires ESA being enabled and
    Activity Monitoring being configured.
92 # Valid values: true | false
93 # Default: true
94 # Required: no
95 #
96 # Setting name: ConfigFlags
97 # Description: Define additional implementation defined flags.
98 # Valid values: A comma- or semicolon-separated list of any of the
    following strings
99 #     - NoGatewayCheck                - disable the check for a
    configured Default Gateway for non-PPP network interfaces
100 #     - IEIgnoreFrames                - disable determination of
    performance data for frames in Internet Explorer
101 #     - RegMonSvcDebugOutput          - enable Registry
    Monitoring debug output to ProcMon
102 #     - TLSRevocationChecksDisabled   - disable certificate
    revocation checks, e.g. during testing with self-signed certificates
    on the backend (Windows only)
103 #     - TLSRevocationChecksBestEffort - ignore certificate
    revocation checks in case of missing or offline distribution points
    (Windows only). If both revocation check options are configured, the
    option above takes precedence. For more details on these two
    options see https://curl.se/libcurl/c/CURLOPT\_SSL\_OPTIONS.html
104 #     - EnableESFileSystemMonitoring  - collects data for the
    fields ProcIOWriteCount and ProcIOPSWrite of the sourcetype
    ProcessDetail on macOS. May increase uberAgent's CPU utilization.
105 #     - SessionHelperQueryDelayMs:NUMBER - delay between queries to
    in-session helper processes. Replace NUMBER with any integer >= 0
    to specify the delay in ms.
106 #     - TraceLogFilterExpression:REGEX - include messages
    matching the regular expression REGEX in the log, regardless of
    their log level. This includes trace-level messages not included
    with DebugMode = true. REGEX must match the complete source string.
107 #     - EnableSystemLog                - send log entries to the
    system's native log system in addition to the log file. Only
    available on macOS.
108 #     - CitrixSDKMaxRecordCount:NUMBER - defines the -
    MaxRecordCount parameter for each Citrix (Remote) PowerShell SDK
    call. Replace NUMBER with any integer >= 0 (default is 1000).
109 #     - CitrixODataAPIMaximumAttempts:NUMBER - defines the maximum
    amount of repeating API queries if a query is responding with a not
    successful status code (default is 10).
110 #     - POQSendWaitDelayMs:NUMBER      - defines the delay
    between two send attempts if the persistent output queue is
    processed (default is 500ms). Valid values are between 100 and
    10000.
```

```
111 # - NetworkCommunicationTimeoutMs:NUMBER - defines a timeout for
    # network communication (default is 10000ms). Valid values are between
    # 100 and 1000000.
112 # - LockEnterMaxWaitMs:NUMBER - defines a duration in
    # milliseconds if an internal locking mechanism took too long to enter/
    # succeed. A trace log message will be written. Valid values are >=
    # 100 (default is 1000).
113 # - LockHeldMaxWaitMs:NUMBER - defines a duration in
    # milliseconds if an internal locking mechanism was held for more than
    # the defined number. A trace log message will be written. Valid
    # values are >= 100 (default is 1000).
114 # Default: empty
115 # Required: no
116 #
117 #####
118
119 [Miscellaneous]
120 DebugMode = true
121
122 #####
123 #
124 # Data receivers
125 #
126 # uberAgent sends data to the receivers configured here.
127 # If multiple [Receiver] sections are specified, data will be sent to
    # EACH receiver. This can be overridden per Timer by specifying a
    # comma-separated list of receivers.
128 # To load-balance and fail over between servers specify multiple comma-
    # separated values for "Servers" in a SINGLE receiver section
129 #
130 # The documentation for the Persistent Output Queue options can be
    # found here: /en-us/uberagent/7-0-0/advanced-topics/persistent-output
    # -queue.html
131 #
132 # Configurable settings in this section:
133 #
134 # Setting name: Name
135 # Description: Arbitrary name for the data receiver. If no persistent
    # output queue is configured the name is used only internally.
    # Otherwise the name is used as an appendix for the persistent output
    # queue file name.
136 # Valid values: any string
137 # Default: empty
138 # Required: Required only if persistent output queue is activated for
    # this receiver. In this case the name must be unique for all
    # receivers.
139 #
140 # Setting name: Type
141 # Description: Receiver type.
142 # Valid values: Splunk | Elasticsearch | OMSLogAnalytics | Kafka
143 # Default: Splunk
144 # Required: yes
145 #
```

```
146 # Setting name: Protocol
147 # Description: How to send data to the backend.
148 #     TCP uses a direct TCP connection
149 #     HTTP sends to a REST endpoint via HTTP or HTTPS
150 #     For type Splunk use TCP or HTTP, for all other types use HTTP.
151 # Valid values: TCP | HTTP
152 # Default: TCP
153 # Required: no
154 #
155 # Setting name: Servers
156 # Description: List of target servers/URLs.
157 # Valid values:
158 #     TCP: comma-separated list of server:port, e.g.: localhost:19500,
159 #     splunksrv:12345
160 #     HTTP: comma-separated list of URLs starting with http or https.
161 #     Splunk example: http://server1:8088, https://server2:8088
162 #     OMS Log Analytics example: https://CUSTOMERID.ods.opinsights.
163 #     azure.com
164 # Default: empty
165 # Required: yes
166 #
167 # Setting name: RESTToken
168 # Description: Authentication token required by the Splunk HTTP Event
169 # Collector and by OMS Log Analytics.
170 # For Type OMSLogAnalytics use the primary or the secondary key for
171 # the workspace.
172 # For Type Elasticsearch credentials in format
```

uberAgent-GPO-include.conf

July 9, 2024

The following is the `uberAgent-GPO-include.conf` configuration file that ships with uberAgent. This file is included in the default Group Policy configuration and contains settings that cannot be set via Group Policy.

```
1 #
2 # If uberAgent is configured using Group Policy,
3 # this file is included and processed by default to include additional
4 # configuration elements,
5 # that are not available in Group Policy configurations.
6 #
7 # Include the ESA config file
8 @ConfigInclude uberAgent-ESA.conf platform=Windows
9
10 # Include default event data filter rules
11 @ConfigInclude uberAgent-eventdata-filter.conf
```

New Release Information & Notifications

August 1, 2024

There are many ways to get notified about new uberAgent releases.

Citrix Blog

- Citrix uberAgent [blog URL](#)

Citrix Downloads

- Citrix Observability [feed URL](#)

Social Media

- Citrix [Twitter](#)
- Citrix [LinkedIn](#)
- Citrix [Facebook](#)
- Citrix [Instagram](#)

Email

You can subscribe to Citrix's newsletter on citrix.com/blogs.

Planning

July 9, 2024

The information in this section helps you plan uberAgent deployments.

Architecture Options

July 25, 2024

Backend Placement

Applies to: Splunk and alternative backends.

The backend service required by uberAgent can be installed or consumed in any setup that is supported by the backend product vendor. This includes:

- On-premises (physical or virtual machine)
- Backend vendor cloud offering such as Splunk Cloud
- Public cloud IaaS (virtual machine in a cloud such as AWS EC2, Azure VMs)

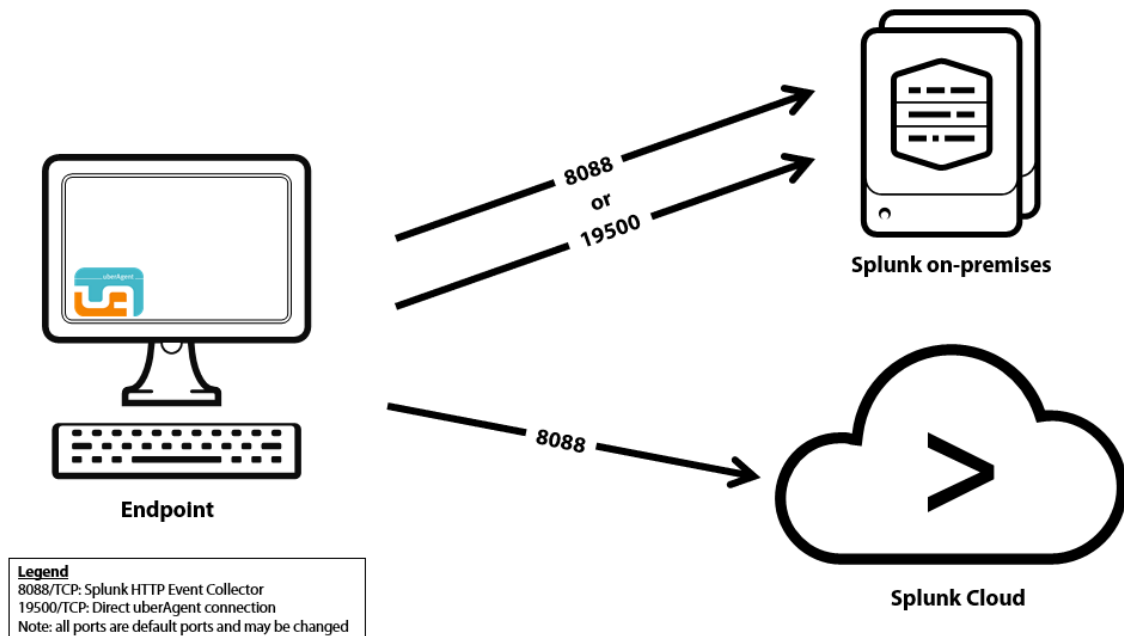
Note: vast limits does not operate backend servers for data storage and visualization. Backend servers such as Splunk are always operated by vast limits' customers or partners.

Endpoint to Backend Communication

Recommended: Direct

Applies to: Splunk and alternative backends.

In this recommended configuration uberAgent talks directly to the backend servers. This has the advantage that the overall footprint on the monitored endpoints is smaller compared to architecture options that require Splunk Universal Forwarder.



Configuration highlights

- **Communications:** uberAgent sends data directly from the endpoint to the backend servers
- **Splunk backends:** on the indexers, either a TCP port is opened or HTTP Event Collector is configured
- **Alternative backends:** uberAgent makes use of the backend's native REST API

Pros

- Smallest footprint
- Data can be transferred encrypted via HTTPS and authenticated with a REST token

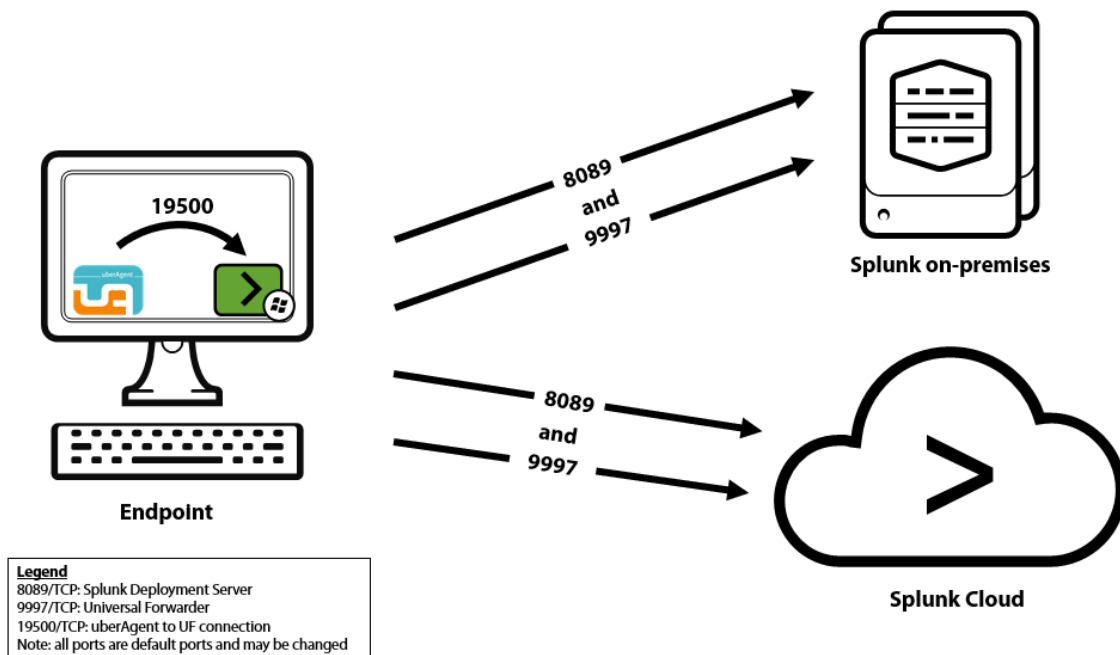
Alternative: Via Splunk Universal Forwarder

Applies to: Splunk backends only.

Note

Please note that with this configuration option, data is transmitted unencrypted over TCP from uberAgent to Splunk's Universal Forwarder on the local machine. Therefore, we recommend that you use the direct connection as described before, which enables encrypted and authenticated data transmission.

Similar to Standalone mode, but uberAgent sends the data it collects to a locally installed Splunk Universal Forwarder. If you have deployed Universal Forwarder on your monitored endpoints anyway you might want the forwarder to handle all Splunk communications.



Configuration highlights

- **Communications:** uberAgent sends data to the local forwarder's TCP port which in turn sends data to the Splunk indexers
- **Splunk Universal Forwarder:** a TCP port is opened on each endpoint (for local access only)

Pros

- All Splunk communications are handled by Splunk components
- Additional data can be collected via Universal Forwarder (log files, Windows event logs, scripts)
- Collected data can optionally be persisted to disk before sending off to Splunk

Cons

- Larger footprint than the recommended architecture
- On the local machine, data is sent unencrypted and unauthenticated over TCP

Configuration Options

July 9, 2024

uberAgent can be configured by means of **configuration files** (all platforms) or via **Group Policy** (Windows).

Default Configuration

uberAgent's setup installs a default set of configuration files along with the agent binaries. This default configuration is maintained in the [uberAgent Configuration](#) GitHub repository. It is advisable to regularly check the GitHub repository for relevant configuration updates, specifically for uberAgent ESA's threat detections and security inventory checks.

Data Volume Optimized Configuration

A [configuration optimized for data volume](#) is available as an alternative to the default configuration.

Precedence

uberAgent looks for its configuration in the following locations.

Windows

1. **Group Policy**
2. **ProgramData:** `%ProgramData%\vast limits\uberAgent\Configuration\uberAgent.conf`
3. **Installation directory:** typically `C:\Program Files\vast limits\uberAgent\uberAgent.conf`

The first configuration found is used exclusively. In other words: Group Policy overrides `%ProgramData%`, which overrides the installation directory.

macOS

1. `/Library/Application Support/uberAgent/`

How to Configure uberAgent

Configuration via Group Policy

To configure uberAgent via Group Policy, please follow [these steps](#).

Configuration via Config Files

To configure uberAgent via configuration files, please follow [these steps](#).

Antivirus Exclusions

August 2, 2024

It is recommended that specific folders are excluded from scanning by your antivirus product to ensure smooth operation of your uberAgent deployment. Include the following items to reduce the risk of false positives.

Configuration Files & Scripts

Platform	Path	Filetype
Windows	%ProgramData%\vast limits\uberAgent\ Configuration\	.conf
Windows	%ProgramFiles%\vast limits\uberAgent\ Configuration\	.conf
macOS	/Library/Application Support/uberAgent/	.conf
macOS	/Library/Application Support/uberAgent/ Config Templates/	.conf

Persistent Output Queue

Exclude the location where the POQ stores its files. The items below assume the default location. If you choose to use a different path, adjust accordingly.

Platform	Path	Filetype
Windows	%ProgramData%\vast limits\uberAgent\ Output Queue*	.db .db-shm .db-wal
macOS	/Library/Application Support/uberAgent/ Output Queue/*	.db .db-shm .db-wal

Splunk Data Volume Calculation

September 30, 2024

When uberAgent is used with Splunk as a backend, a Splunk license is required. Splunk is licensed by daily indexed data volume, i.e., you pay for the total amount of data you send to Splunk per day. How long that data is stored does not matter, only how much new data you add. uberAgent is one of the potentially many data sources that put data into Splunk, contributing to the total data volume.

Estimate or Measure

Customers have a vested interest in knowing how much data each Splunk add-on generates, so they can estimate costs before they buy. In the case of uberAgent, the data volume per host depends greatly on the environment, the types of applications used, the desktop configuration, background processes, the type of browser used and many other variables. For that reason, it is not possible to calculate the data volume with any reasonable accuracy without doing an actual proof of concept implementation (see below). However, if you just want some figures for a **very rough first calculation**, use the following values for typical clients and servers:

uberAgent UXM data volume

- Typical data volume per **single-user** client and working day: **25 MB**
- Typical data volume per **multi-user** (Citrix CVAD/RDS) server and working day: **90 MB**

uberAgent ESA data volume

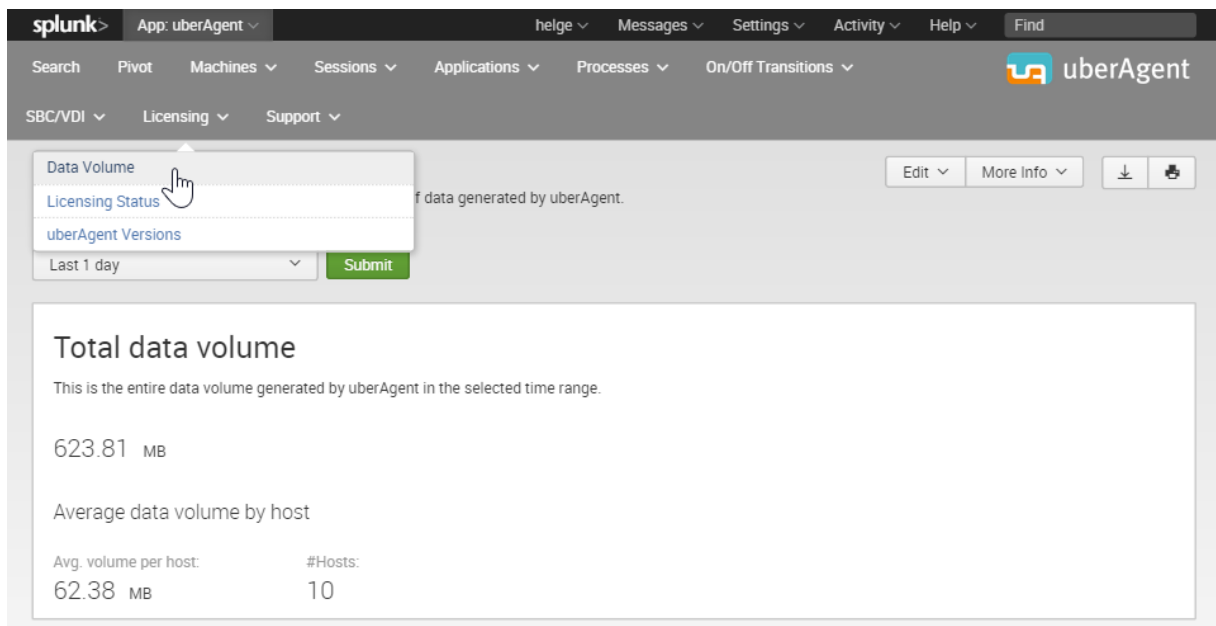
Using uberAgent ESA in addition to uberAgent UXM will approximately double the data volume per client/server and working day.

Accurate data volume numbers

To get accurate numbers install uberAgent and go to the *Data Volume* dashboard (see below). You can significantly reduce the data volume through an [optimized configuration](#).

Data Volume Dashboard

If you already have uberAgent installed, you can simply look up the generated data volume by going to the *Data Volume* dashboard:



Make sure you have [configured Splunk correctly](#) or the data volume dashboard may not be able to display values for all metrics.

Reducing the Data Volume

Once you have your first installation set up you might want to fine-tune and possibly reduce the data volume. Luckily that is easily possible. Here is [how to reduce uberAgent's data volume](#).

Splunk Sizing Resources and Recommendations

July 9, 2024

Sizing Splunk is not always trivial, especially if it is used for other use cases in addition to uberAgent. We generally recommend working with one of our [partners](#).

That being said, this page lists some basic recommendations as well as resources that should help with sizing Splunk. Before we start, please keep in mind that the only generic answer any good consultant will give is: "it depends". Because it does.

Splunk Sizing Considerations

Hardware Resources: CPU and Disk

Splunk needs CPU and disk resources, RAM not so much (compared to some other workloads). Make sure you have enough disk space for the planned retention time as well as a disk subsystem that delivers good IOPS numbers.

Accelerated Data Model

uberAgent's Splunk app makes use of an accelerated data model which speeds up searches by about 50-100x. The data model's high-performance analytics store (HPAS) is located on the indexers. Generating the HPAS incurs some additional indexer CPU load and requires additional disk storage.

Heavy Forwarders

Splunk Heavy Forwarders (HFs) can often be a useful third tier, logically situated between the uberAgent endpoints and the Splunk indexers. If you are deploying uberAgent to tens of thousands of endpoints, keep in mind that high numbers of simultaneous network connections may place a significant load on the HFs. Monitor heavy forwarder performance and be prepared to scale out.

Splunk Sizing Recommendations

1. Always **start with a PoC** and closely monitor Splunk performance during that phase.
2. [Measure uberAgent's data volume](#), keeping in mind that [optimization](#) is often possible.
3. Due to the accelerated data model, uberAgent's Splunk load profile is somewhat similar to Splunk's Enterprise Security (ES) app. When looking at sizing guides, base your calculations on the ES use case.

Splunk Sizing Resources

- Splunk's [Capacity Planning Manual](#) and its chapter on [reference hardware](#) and its [summary of performance recommendations](#)
- The [deployment planning](#) chapter from Splunk's Enterprise Security installation and upgrade manual
- Splunk's unofficial [storage sizing calculator](#)
- Hurricane Labs' Splunking Responsibly blog series. [Part 1: considerations for managing limited system resources](#) and [Part 2: sizing your storage](#)
- Aplura's [Splunk best practices](#)

uberAgent Feature Support on macOS

July 9, 2024

The long-term goal for uberAgent on macOS is to achieve feature-parity with its Windows counterpart. As long as this is not yet the case, this article helps you to see at a glance **which metrics are being collected and which dashboards contain macOS-specific information.**

More information about individual fields is available in the [metrics documentation](#).

User Experience Monitoring

Sourcetypes

- uberAgent:Application:AppNameldMapping
- uberAgent:Application:ApplicationInventory
- uberAgent:Application:ApplicationUsage
- uberAgent:Application:BrowserWebRequests2
- uberAgent:Application:Errors
- uberAgent:Application:NetworkConnectFailure
- uberAgent:License:LicenseInfo
- uberAgent:Process:NetworkTargetPerformance
- uberAgent:Process:ProcessDetail
- uberAgent:Process:ProcessStartup
- uberAgent:Session:SessionDetail
- uberAgent:System:DiskInventory
- uberAgent:System:MachineInventory
- uberAgent:System:MonitorInventory
- uberAgent:System:NetworkConfigInformation
- uberAgent:System:SystemPerformanceSummary2
- uberAgent:System:VolumeInventory

Dashboards

Experience Score

- Experience Score Overview
- Machine Scores
- Session Scores
- Application Scores

Machines

- Machine Performance
- Machine Network Communication
- Machine Network Configuration
- Machine Network Issues
- Machine Uptime
- Machine Inventory
- Machine Storage

Sessions

- User Session Overview
- User Sessions
- Session 0

Applications

- Application Performance
- Application Errors
- Application Network Communication
- Application Network Issues
- Browser Web App Performance
- Browser Web App Usage
- Application Inventory
- Application Usage

Processes

- Process Performance
- Process Network Communication
- Process Network Issues

Licensing

- Data Volume
- Licensing Status
- uberAgent Versions

Endpoint Security Analytics

Sourcetypes

- uberAgentESA:Process:DnsQuery

Dashboards

Processes

- Process DNS

Installation

July 9, 2024

Installing uberAgent is quick and easy. This section shows you how to install the two main uberAgent components: the actual agent that runs on the machines you want to monitor as well as the backend that stores and visualizes the collected data.

Backend

July 9, 2024

Supported Backends

While uberAgent has been designed to use **Splunk** as a backend from day one, it also works well with **Elasticsearch & Kibana**, **Apache Kafka**, and **Microsoft Azure Monitor**. Installing instructions for all backends are available in this section.

Installing Splunk

July 25, 2024

This page explains how to install a Splunk server for uberAgent.

Prerequisites

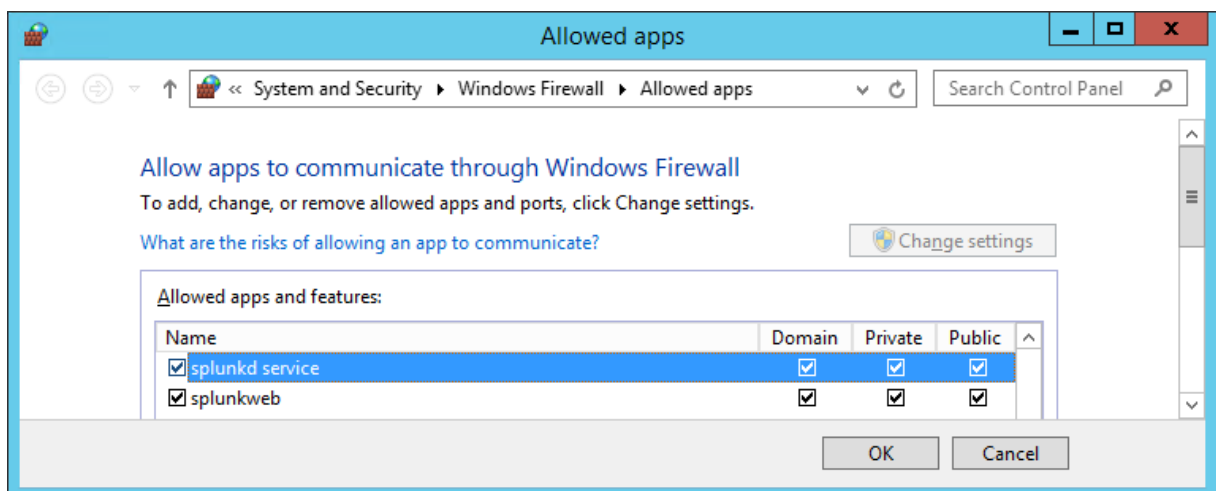
- Download [Splunk](#)
- Please see the KB article [supported Splunk versions](#)

Setup

Run through Splunk's setup on the designated Splunk server (in this simple tutorial we assume that you only have a single, Windows-based Splunk server). Choose *Local system user* when asked for a Splunk user.

Firewall

Once Splunk is installed: if you have a firewall enabled, make sure that communication is allowed for `splunkd.exe` and `splunkweb.exe` (both normally located in `C:\Program Files\Splunk\bin`). For Windows Firewall the recommended configuration looks like this:



Log On

Log on to the Splunk console by navigating to `http://servername:8000` in your browser.

License

If you plan to use Splunk Enterprise and already have a license, install it through **Settings > Licensing**. If you do not have a license yet: Splunk runs in Enterprise mode with an allowed daily data volume of 500 MB for 60 days. Then it switches to the free version.

Sending to Splunk's HTTP Event Collector

If you plan to have the endpoint agent send the collected data to Splunk's HTTP Event Collector [follow the steps in this article](#).

Install uberAgent

Read on about how to [install uberAgent](#).

Configuring Splunk's HTTP Event Collector

July 25, 2024

What is HTTP Event Collector

HTTP Event Collector (HEC) is a high-performance REST API data input. It accepts plain text or JSON data sent via HTTP or HTTPS.

Clients must authenticate with a token in order to be able to send data to a HEC input. Multiple tokens can be generated per HEC input if required.

When to Use HTTP Event Collector

HTTP Event Collector (HEC) is the only way to send uberAgent data to Splunk Cloud. But it is useful even with on-premises Splunk Enterprise. HEC forces clients to authenticate before being allowed to send and it can use HTTPS as data transport, which qualifies it for sending data over the internet.

uberAgent natively supports HEC. It can send the data it collects to HEC via HTTP or HTTPS.

Configuring HTTP Event Collector in Splunk Enterprise

Enabling HTTP Event Collector in the UI

To enable HTTP Event Collector (HEC) for uberAgent follow these steps:

- From the system bar, click **Settings > Data Inputs**
- On the left side of the page, click **HTTP Event Collector**

- In the upper right corner, click **Global Settings**. The following dialog comes up:

The screenshot shows the 'Edit Global Settings' dialog box. It features a title bar with the text 'Edit Global Settings' and a close button 'x'. The settings are as follows:

- All Tokens:** A toggle button with 'Enabled' selected and 'Disabled' unselected.
- Default Source Type:** A dropdown menu showing 'Select Source Type'.
- Default Index:** A dropdown menu showing 'Default'.
- Default Output Group:** A dropdown menu showing 'None'.
- Use Deployment Server:** An unchecked checkbox.
- Enable SSL:** An unchecked checkbox.
- HTTP Port Number?:** A text input field containing the value '8088'.

At the bottom of the dialog, there are two buttons: 'Cancel' on the left and 'Save' on the right.


- In the **All Tokens** toggle button, select **Enabled**
- Optionally change the HEC port or enable SSL/TLS
 - Note that Splunk’s default self-signed certificate is not trusted by uberAgent if it is not in the endpoint’s operating system certificate store.
 - HTTP Event Collector shares SSL settings with the Splunk management server so check your [server.conf](#) for SSL configuration details.
- Click **Save**

Creating an HTTP Event Collector Token in the UI

To use the HTTP Event Collector, you must configure at least one token. The token is what uberAgent uses when it connects to Event Collector to send data.

To create an HEC token for use with uberAgent follow these steps:

- From the system bar, click **Settings > Data Inputs**
- On the left side of the page, click **HTTP Event Collector**
- In the upper right corner, click **New Token**. The following dialog comes up:

Configure a new token for receiving data over HTTP. [Learn More](#) 

Name

Source name override?

Description?

Output Group (optional)

Enable indexer acknowledgement

- Enter a name (e.g. uberAgent) and click **Next**. The following dialog comes up:

Select Allowed Indexes

Available item(s) add all >	Selected item(s) remove all <
history main summary	

Select indexes that clients will be able to select from.

Default Index [Create a new index](#)

- Leave everything at the defaults and click **Review**
- On the next page click **Submit**
- Copy the token value displayed. In the following screenshot that would be: 10C2F38B-CA7A-4850-8124-7A3191F82DBE

✓ Token has been created successfully.

Configure your inputs by going to Settings > [Data Inputs](#)

Token Value

[Start Searching](#)

Search your data now or see [examples and tutorials](#). [↗](#)

[Add More Data](#)

Add more data inputs now or see [examples and tutorials](#). [↗](#)

[Download Apps](#)

Apps help you do more with your data. [Learn more](#). [↗](#)

[Build Dashboards](#)

Visualize your searches. [Learn more](#). [↗](#)

HTTP Event Collector Configuration Files

Splunk HTTP Event Collector can be configured through configuration files instead of the UI, which is often required for automation or for configuring settings that are not exposed in the UI. See Splunk's documentation [Set up and use HTTP Event Collector with configuration files](#) for details.

Configuring uberAgent to Send to an HTTP Event Collector Input

To configure uberAgent to send its collected data to HEC the following [configuration settings](#) are required:

- **Servers:** comma-separated list of URLs starting with http or https, e.g.: `http://server1:8088, https://server2:8088`
- **Protocol:** must be set to [HTTP](#) (even when sending via HTTPS)
- **RESTToken:** fill in the token created above. The token can optionally be encrypted with the `uAEncrypt` commandline tool.

Please make sure to review the KB document [Reuse of Open HTTP Connections](#).

Installing and Configuring Elasticsearch & Kibana

July 9, 2024

This document explains how to install and configure Elasticsearch/Kibana for uberAgent (in this simple tutorial, we assume that you only have a single node with Elasticsearch and Kibana).

Installation

Follow Elastic's [installation guide](#) to install Elasticsearch.

Configuration for uberAgent

Elasticsearch 6.x

Elasticsearch 6 is only supported by uberAgent version 6.2 and lower.

Run the following PowerShell command on the Elasticsearch server to create an index template for uberAgent with the required field definitions:

```
1 Invoke-RestMethod -Uri http://localhost:9200/_template/uberagent -
  Method Put -InFile .\elasticsearch-uberagent.json -ContentType "
  Application/json"
```

On Linux use:

```
curl -XPUT -H 'Content-Type: application/json' http://localhost:9200/
_template/uberagent -d@elasticsearch-uberagent.json
```

The file `elasticsearch-uberagent.json` is part of the uberAgent download package.

If you enabled X-Pack security, you need to pass the elastic user (configured during the setup) for the commands above. On Windows use the `-Credential` parameter, for Linux `-u`.

Elasticsearch 7.7 And Lower

Elasticsearch 7.7 and lower are only supported by uberAgent version 6.2 and lower.

Run the following PowerShell command on the Elasticsearch server to create an index template for uberAgent with the required field definitions:

```
1 Invoke-RestMethod -Uri http://localhost:9200/_template/uberagent?
  include_type_name=true -Method Put -InFile .\elasticsearch-uberagent
  .json -ContentType "Application/json"
```

On Linux use:

```
curl -XPUT -H 'Content-Type: application/json' http://localhost:9200/_template/uberagent?include_type_name=true -d@elasticsearch-uberagent.json
```

The file `elasticsearch-uberagent.json` is part of the uberAgent download package.

If you enabled X-Pack security, you need to pass the elastic user (configured during the setup) for the commands above. On Windows use the `-Credential` parameter, for Linux `-u`.

Elasticsearch 7.8 And Higher (Including 8.x)

Elasticsearch 7.8 and higher as well as 8.x are only supported by uberAgent version 6.3 and higher. Run the following PowerShell command on the Elasticsearch server to create an index template for uberAgent with the required field definitions:

```
1 Invoke-WebRequest -Uri http://localhost:9200/_index_template/uberagent -Method Put -InFile .\elasticsearch-uberagent.json -ContentType "Application/json"
```

On Linux use:

```
curl -XPUT -H 'Content-Type: application/json' http://localhost:9200/_index_template/uberagent -d@elasticsearch-uberagent.json
```

The file `elasticsearch-uberagent.json` is part of the uberAgent download package.

If you enabled X-Pack security, you need to pass the elastic user (configured during the setup) for the commands above. X-Pack security is enabled by default since Elasticsearch 8. On Windows use the `-Credential` parameter, for Linux `-u`.

If you want to use an Elasticsearch data stream instead of a classic index, add `"data_stream": { }`, to the file `elasticsearch-uberagent.json`. Example:

```
1 {
2
3   "priority": 100,
4   "index_patterns": [
5     "uberagent*"
6   ],
7   "data_stream": {
8   }
9 ,
10  "template": {
11
12    "mappings": {
13
14      "dynamic": "strict",
15      "properties":
16        {
```

```
17
18     "@timestamp" : {
19   "type" : "date" }
20
21     }
22
23   }
24
25 }
26
27 }
```

Kibana

Follow Elastic's [installation guide](#) to install Kibana

Dashboards

uberAgent only comes with Splunk dashboards. Nevertheless, there is a way to visualize uberAgent data in Elasticsearch using [XOAP's Kibana dashboard package](#).

XOAP's [GitHub repository](#) has 60+ dashboards that visualize a large part of the data set collected by uberAgent.

Install uberAgent

Read on about how to [install uberAgent](#).

To configure uberAgent to send data to Elasticsearch, a configuration section similar to the following is required:

```
1 [Receiver]
2 Name = Default
3 Type = Elasticsearch
4 Protocol = HTTP
5 Servers = http://servername:9200
6 # The setting RESTToken is required if X-Pack security is enabled. It
   is enabled by default since Elasticsearch version 8.
7 RESTToken = username:password
```

Configuring Microsoft Azure Monitor

December 9, 2024

This page explains how to configure uberAgent to send the collected data to Microsoft Azure Monitor.

Support/Status

Support for Microsoft Azure Monitor Logs is **experimental** and **and available exclusively on Windows platforms**.

Creating the Log Analytics Workspace

To use uberAgent with Microsoft Azure Monitor Logs, please follow these steps:

- Navigate to <https://portal.azure.com> and sign in with your Microsoft account or your Organizational account associated with your Microsoft Azure subscription.
- Navigate to the Azure service **Log Analytics workspaces** and create a new workspace by specifying a unique workspace name, subscription, resource group, location and pricing tier or use an existing workspace linked to your Microsoft Azure subscription.
- Open up the **Advanced settings** > **Connected sources** menu and note the **WORKSPACE-ID** and the **PRIMARY-KEY**.

Configuring uberAgent to Send to Azure Monitor Logs

To configure uberAgent to send its collected data to Azure Monitor Logs the following [Receiver configuration settings](#) are required:

- **Type:** `OMSLogAnalytics`
- **Protocol:** `HTTP`
- **Servers:** `https://WORKSPACE-ID.ods.opinsights.azure.com`
- **RESTToken:** `PRIMARY-KEY`

Example

```
1 [Receiver]
2 Name = Default
3 Type = OMSLogAnalytics
4 Protocol = HTTP
5 Servers = https://WORKSPACE-ID.ods.opinsights.azure.com
6 RESTToken = SECRET-PRIMARY-KEY
```

Configuring Apache Kafka & Confluent REST Proxy

July 9, 2024

Introduction

What is Apache Kafka

Apache Kafka is a high-performance distributed message queuing and event stream processing platform. Producers send data to Kafka, which buffers the incoming events to disk for a configurable period of time. Kafka logically groups events into topics, which Consumers subscribe to.

What is Confluent REST Proxy

Confluent is a Kafka distribution targeted at enterprises. It adds monitoring, security, and management components to open source Kafka.

While vanilla Kafka only accepts incoming data via a proprietary binary protocol, Confluent comes with a REST proxy that is similar in nature to Splunk HEC or Elasticsearch REST API. REST Proxy is part of the free community edition of Confluent.

When to Use Kafka with uberAgent

By routing uberAgent's data through Kafka, enterprises can make end-user computing metrics available to individual teams within the organization in a publish/subscribe kind of model. Once access has been granted for a topic, a team can start consuming that topic's metrics. While some teams might be interested in uberAgent's asset and inventory information, others might need access to application performance or browser web app usage data.

Kafka makes it possible to distribute uberAgent's metrics in a highly scalable manner, supporting hundreds of thousands of endpoints (data producers) and thousands of consumers. uberAgent natively supports Kafka via the Confluent REST proxy.

Prerequisites

In order for uberAgent to be able to send data to a Kafka backend the following is required:

- Confluent REST Proxy with Confluent Schema Registry
- Apache Kafka

Please see the [system requirements](#) for details.

Implementation Details

Topics

Kafka Topics and uberAgent Sourcetypes uberAgent uses Splunk's concept of sourcetypes to logically group events. uberAgent sourcetypes names always start with `uberAgent` followed by two additional sections concatenated by colons. Example:

```
1 uberAgent:Application:Errors
```

uberAgent sourcetypes are mapped to Kafka topics in a 1:1 relationship. Since colons are not allowed in topic names, they are replaced by underscores. The sourcetype from the above example maps to the following Kafka topic:

```
1 uberAgent_Application_Errors
```

Topic Creation uberAgent does not create Kafka topics. For uberAgent to be able to send data to Kafka, either topic auto-creation must be enabled (setting `auto.create.topics.enable`), or the topics needed by uberAgent must be created manually.

uberAgent's sourcetypes are [documented here](#). A listing of all sourcetypes is available in the file `uA_sourcetypes_metrics.csv` which is part of the uberAgent dashboard app (included in the [uberAgent download](#)).

Partitions

Kafka stores topic data in partitions that can be distributed across nodes in a Kafka cluster. One partition per consumer group is required.

Kafka producers like uberAgent can either select a specific partition for each event or have events be distributed randomly across partitions. uberAgent combines the two approaches: it specifies the hostname as key for each event. This ensures that all events from a specific host are always stored in the same partition.

Schema and Data Format

uberAgent uses Avro as data format when sending to Kafka. Avro requires a schema definition for every event. This guarantees high data quality and easier processing by downstream consumers.

In order to minimize network data volume, uberAgent sends the full schema definition only for the first event of a topic. All further events of the same topic reference the topic's schema definition by the ID returned from the schema registry in response to the first event.

Avro requires REST Proxy to be configured with a schema registry URL (configuration setting `schema.registry.url`).

Event Metadata Each uberAgent event has the same default metadata fields in Kafka as in Splunk:

- time
- host
- index
- source
- sourcetype

The sourcetype is used as the key for the Kafka partition selection (see above) and added to each event as a dedicated field.

REST Proxy API Details uberAgent sends data to the [Confluent REST Proxy API v2](#) via HTTP POST to `/topics/SOURCETYPE` ([docs](#)). The HTTP content type is `application/vnd.kafka.v2+json`.

Configuration

uberAgent

To configure uberAgent to send data to Kafka via Confluent REST Proxy a configuration section similar to the following is required:

```
1 [Receiver]
2 Name = Kafka
3 Type = Kafka
4 Protocol = HTTP
5 Servers = https://confluent-rest-proxy.company.com:8083/
6 TLSClientCertificate = LocalMachine\MY\
   abcd123456789123456789123456789123456789
```

The receiver `Name` can be any string. The `Protocol` must be `HTTP` - it stands for a REST endpoint accessed via `http` or `https`. The `Servers` parameter accepts a comma-separated list of REST proxies that are contacted in a round-robin fashion for fault tolerance and load sharing. `TLSClientCertificate` optionally specifies a client certificate to use for authentication (see below).

Kafka

Please see the implementation details section above for information on how to configure Confluent and Kafka for receiving data from uberAgent.

Authentication

Confluent REST Proxy supports authentication via an HTTPS client certificate on the endpoint. Make sure to specify the `TLSCliientCertificate` option in the [uberAgent configuration](#).

It is not necessary to issue individual certificates to clients. A single certificate with `CN=uberAgent` (or similar) might be best.

Confluent REST Proxy [propagates the client certificate](#) to the Kafka broker in one of two ways:

- TLS
- SASL

The following sections show the configuration steps for each option.

Client Certificate Propagation via TLS In order for certificate propagation from REST Proxy to the Kafka brokers to work, the following requirements must be met:

- REST Proxy and the Kafka brokers must be configured for TLS support
- A root CA that issues all required certificates and is trusted by all components is highly recommended
- REST Proxy's client certificate store must contain the certificate (including private key) uberAgent authenticates with

REST Proxy Configuration This example shows a simple configuration with all components on one server. In a real-world deployment that would most likely not be the case. Adjust the URLs accordingly.

Add the following to the file `/etc/kafka-rest/kafka-rest.properties`:

```
1 #####
2 #
3 # Schema registry
4 #
5 #####
6
7 schema.registry.url=http://localhost:8081
8
9 #####
10 #
```



```
11 # REST proxy to broker connection
12 #
13 #####
14
15 bootstrap.servers=localhost:9093
16 client.security.protocol=SSL
17
18 # The client keystore contains the client certificate (including the
19 #   private key) that is used by uberAgent to authenticate. REST proxy
20 #   passes it on to the broker.
21 client.ssl.keystore.location=/opt/vastlimits/certificates/kafka.
22 #   clientkeystore.jks
23 client.ssl.keystore.password=PASSWORD3
24 client.ssl.key.password=PASSWORD3
25
26
27 # The truststore contains the collection of CA certificates trusted by
28 #   this application
29 client.ssl.truststore.location=/opt/vastlimits/certificates/kafka.
30 #   truststore.jks
31 client.ssl.truststore.password=PASSWORD1
32
33 #####
34 #
35 # Miscellaneous
36 #
37 #####
38
39 # Listeners (port 8083 cannot be used for REST Proxy because it is used
40 #   by Confluent Connect)
41 listeners=https://0.0.0.0:8084
42
43 #####
44 #
45 # Security plugin
46 #
47 #####
48
49 # License for commercial edition (required for the security plugin)
50 confluent.license=LICENSE_KEY
51
52 # Enable the REST proxy security plugin
53 kafka.rest.resource.extension.class=io.confluent.kafkarest.security.
54 #   KafkaRestSecurityResourceExtension
55
56 # Whether or not to require the HTTPS client to authenticate via the
57 #   server's trust store (required if the security plugin is enabled)
58 ssl.client.auth=true
59
60 #####
61 #
62 # HTTPS from clients to REST proxy
63 #
64 #####
```

```
56
57 # Web server certificate for REST proxy
58 ssl.keystore.location=/opt/vastlimits/certificates/kafka.keystore.jks
59 ssl.keystore.password=PASSWORD2
60 ssl.key.password=PASSWORD2
61
62 # The truststore lists certificates that are allowed to connect.
   Specify either a single CA certificate or individual client
   certificates.
63 ssl.truststore.location=/opt/vastlimits/certificates/kafka.truststore.
   jks
64 ssl.truststore.password=PASSWORD1
```

Kafka Broker Configuration Add the following to the file `/etc/kafka/server.properties` :

```
1 # The truststore lists certificates that are allowed to connect.
   Specify either a single CA certificate or individual client
   certificates.
2 ssl.truststore.location=/opt/vastlimits/certificates/kafka.truststore.
   jks
3 ssl.truststore.password=PASSWORD1
4
5 # Server certificate for the broker
6 ssl.keystore.location=/opt/vastlimits/certificates/kafka.keystore.jks
7 ssl.keystore.password=PASSWORD2
8 ssl.key.password=PASSWORD2
9
10 # Both plaintext and SSL listeners on different ports. Plaintext can be
   used from the schema registry, for example.
11 listeners=PLAINTEXT://:9092,SSL://:9093
12
13 # Enforce authentication for clients connecting via SSL
14 ssl.client.auth=required
```

Client Certificate Propagation via SASL We are waiting for information from Confluent on some specifics of this configuration. We will update this section once that is available.

Installing uberAgent

July 30, 2024

Installing uberAgent is quick and straightforward. Due to the product's flexibility, there is often more than one way of doing things. In such a case we describe the recommended configuration and link to supported alternatives.

Prerequisites

- Read about the [architecture options](#).
- If you do not have a running Splunk installation yet [set up Splunk](#).
- Download [uberAgent](#) and extract the archive. You should have a directory [uberAgent components](#) with the following content:
 - A subdirectory [uberAgent_endpoint](#)
 - Packed Splunk app [uberAgent_indexer.tgz](#)
 - Packed Splunk app [uberAgent_searchhead.tgz](#)
 - Packed Splunk app [uberAgent_ESA_searchhead.tgz](#)

Installation Steps

Installing uberAgent consists of the following steps:

1. [Installing the Splunk apps](#)
2. [Installing the Windows endpoint agent](#)
3. [Installing the macOS endpoint agent](#)
4. [Installing Splunk Universal Forwarder](#) (optional)
5. [Installing the Chrome browser extension](#) (optional)
6. [Installing the Edge Browser Extension](#) (optional)
7. [Installing the Firefox Browser Extension](#) (optional)
8. [Installing the Internet Explorer Browser Extension](#) (optional)

Installing the Splunk Apps

July 30, 2024

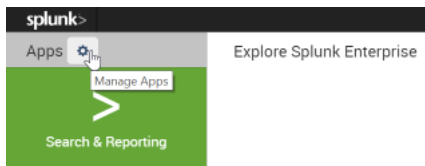
Upgrade

If you are upgrading from an earlier version of the uberAgent Splunk apps please make sure to follow the [upgrade instructions](#).

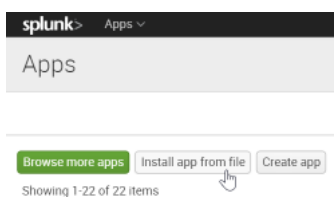
Please consult the [release notes](#) for possible changes in configuration or functionality.

Manual Installation

- Go to the Splunk console's home page by navigating to <http://servername:8000> in your browser.
- Click **Manage apps**:



- Click **Install app from file**:



- Select `uberAgent_indexer.tgz` and click **Upload**
- The uberAgent indexer app is now installed
- Install `uberAgent_searchhead.tgz` in the same way
- Optionally install the uberAgent ESA search head app `uberAgent_ESA_searchhead.tgz`, too
- Click **Settings > Server controls > Restart Splunk**

Splunk Enterprise Security

uberAgent ESA comes with [native support for Splunk Enterprise Security](#). Install the following apps on your Enterprise Security server to enjoy the benefits:

- `uberAgent_searchhead.tgz`
- `uberAgent_ESA_searchhead.tgz`
- `uberAgent_ESA_ES_companion.tgz`.

Available on [Splunkbase](#).

Using Splunk Cloud

The installation process is different when using uberAgent in combination with Splunk Cloud. This [knowledgebase article](#) contains all the necessary details.

Distributed Splunk Deployment

If you have a distributed Splunk deployment with separate search heads and indexers please deploy the **indexer app to all indexers as well as heavy forwarders** and the **search head app to all search heads**.

Alternative Architectures

Note: This is optional and not required for the [recommended architecture](#).

If you decided to have uberAgent send data to Splunk through a locally installed Universal Forwarder on the monitored endpoints you need to enable receiving Universal Forwarder data as described [here](#), i.e., through **Settings > Forwarding and receiving > Receive data > Add new > 9997 > Save**.

Sending to Splunk HTTP Event Collector

Note: This is only required when you want uberAgent to send directly to Splunk Cloud, but it can optionally be used with Splunk Enterprise, too.

uberAgent can send the data it collects via HTTP or HTTPS to a Splunk data input called HTTP Event Collector (HEC). Please follow [these steps](#) to enable and configure HTTP Event Collector.

Installing the Windows Endpoint Agent

July 9, 2024

The agent installer is available as an MSI package. The MSI can either be installed manually or unattended through existing software deployment tools or Splunk's Deployment Server.

Manual Installation

1. Run the batch file `uberAgent_endpoint\bin>manual-install.cmd`.
2. On the screen *Receiver Configuration* specify the name(s) of your Splunk indexer(s) and the port configured earlier (default: 19500).

Configuration

uberAgent can be configured very flexibly. By editing the [configuration](#) you can switch metrics on or off, change the data collection frequency and significantly [reduce the data volume](#).

License File

If you have a license file for uberAgent, copy it to the installation directory (default: `C:\Program Files\vast limits\uberAgent`). Without a license file, uberAgent displays a splash screen during logon. [Contact us](#) for an evaluation license.

Installation Through a Software Deployment Tool

Install the appropriate MSI file from the directory `uberAgent_endpoint\bin` depending on the bitness of your machine: `uberAgent-32.msi` or `uberAgent-64.msi`.

MSI Parameters

Specify the following MSI parameters:

SERVERS

- **Required:** yes
- **Description:** list of target servers/URLs
- **Valid values:**
 - **TCP input:** comma-separated list of `server:port`, e.g., `localhost:19500, splunksrv:12345`
 - **HEC input:** comma-separated list of URLs starting with `http` or `https`, e.g., `http://server1:8088, https://server2:8088`

INSTALLDIR

- **Required:** no
- **Description:** installation directory
- **Valid values:** any local file system path

RECEIVER_PROTOCOL

- **Required:** no
- **Description:** how to send data to the backend
- **Valid values:**
 - `TCP` uses a direct TCP connection. This is the default.
 - `HTTP` sends to Splunk HTTP Event Collector via HTTP or HTTPS

REST_TOKEN

- **Required:** only when sending to Splunk HTTP Event Collector
- **Description:** application token required by the Splunk HTTP Event Collector
- **Valid values:** authentication token created in Splunk

Note: see our documentation on [Configuring Splunk's HTTP Event Collector](#).

License File

If you have a license file for uberAgent, copy it to the installation directory (default: `C:\Program Files\vast limits\uberAgent`). Without a license file, uberAgent displays a splash screen during logon. [Contact us](#) for an evaluation license.

Installation Through Splunk Deployment Server

Note: Deployment Server can only be used with Splunk Enterprise and requires Splunk Universal Forwarder on the endpoint as deployment client.

uberAgent

Copy the directory `uberAgent_endpoint` from the unzipped uberAgent download package to `$(SPLUNK_HOME)\etc\deployment-apps` on your deployment server.

Edit `$(SPLUNK_HOME)\etc\deployment-apps\uberAgent_endpoint\bin\silent-install.cmd`, modifying the `servers` variable so that it contains a list of your Splunk servers.

Example:

```
set servers=splunk1:19500,splunk2:19500
```

Note: `$(SPLUNK_HOME)` refers to the base directory of the Splunk installation, typically `C:\Program Files\Splunk`.

Configuration

To deploy a customized configuration file, copy it into the directory `$(SPLUNK_HOME)\etc\deployment-apps\uberAgent_endpoint\bin`. This overwrites the default configuration file from the installation package.

License File

If you have a license file for uberAgent, copy it into the directory `$(SPLUNK_HOME)\etc\deployment-apps\uberAgent_endpoint\bin`.

Serverclass

Create a file called `serverclass.conf` in `$(SPLUNK_HOME)\etc\system\local` on your deployment server. `Serverclass.conf` defines what to deploy where. For a quick start paste the

following content into `Serverclass.conf` to deploy uberAgent to all Windows machines. You may want to fine-tune this to suit your needs.

```
1 # [global]
2 # We cannot match by machine type here. We'll do that on the app level
   below.
3 whitelist.0 = *
4
5 # Define a serverclass
6 [serverClass:windows]
7 # Deploy only to Windows machines
8 machineTypesFilter = windows-*
9
10 # Define which apps to deploy to the serverclass
11 [serverClass:windows:app:uberAgent_endpoint]
12 stateOnClient = enabled
13 restartSplunkd = true
```

To make Splunk read the new file `serverclass.conf`, run the following command:

```
1 $SPLUNK_HOME\splunk.exe reload deploy-server
```

Citrix Site Monitoring

If some or all of your endpoints are running the Citrix Virtual Apps and Desktops (CVAD) VDA, you should install uberAgent on the Citrix delivery controller(s), too. Please see [this page](#) for details.

Endpoint to Backend Communication Via Splunk Universal Forwarder

Note: This is optional and not required for the [recommended architecture](#).

If you decided to implement the alternative endpoint to backend communication path via Splunk Universal Forwarder, you need to [install Universal Forwarder](#) on each endpoint.

Imaging & Citrix PVS

If you intend to copy the agent installation via an imaging method or Citrix PVS, we recommend you remove instance-specific information. To do that, follow these steps right before capturing the image:

- Stop the service `uberAgent` (but leave the start type at `automatic`).
- Open an administrative command prompt.
- Run the command: `reg delete "HKLM\SOFTWARE\vast limits\uberAgent"/f /reg:64.`
- Prepare the machine for cloning as necessary, but do not reboot.

If you have Splunk Universal Forwarder installed, please follow the steps listed [here](#), too.

Installing the macOS Endpoint Agent

August 2, 2024

The agent installer is available as a PKG file. It can either be installed manually or unattended through existing software deployment tools. Also, most device management solutions support the distribution of such packages natively.

Note

Securing the Configuration Directory

To protect the configuration of uberAgent, **starting with version 6.1.2, the installer automatically sets the permissions for the agent's directory so that only root can read or access the installation directory.**

Requirements

uberAgent on macOS requires the entitlement for certain privacy privileges through Apple's Transparency, Consent and Control (TCC) Framework in order to run properly. These can either be assigned manually, as described below or distributed as part of a PPC profile. The latter can either be created manually by following the [documentation provided by Apple](#) or make use of tools like the [PPPC-Utility](#). An example profile is available at the bottom of this page.

Full Disk Access

uberAgent makes use of Apple's EndpointSecurity (ES) framework (available since macOS 10.15), which requires explicit user authorization. Authorization is granted manually, by adding `/Library/uberAgent/uberAgent.app` to **System Preferences > Security & Privacy > Privacy > Full Disk Access**.

Note: Without this permission uberAgent won't be able to start and will terminate itself. When this happens, you'll find an error log message indicating that the ES client could not be started due to a missing TCC approval.

Accessibility Access

uberAgent uses the Accessibility framework on macOS to determine parts of the Session Detail metrics. Authorization is granted manually, by adding `/Library/uberAgent/uberAgent.app` to **System Preferences > Security & Privacy > Privacy > Accessibility**.

Installation method

Interactive

- The installation of uberAgent can be started by opening `uberAgent.pkg` and following the instructions on the screen.
- Since uberAgent is installed as a system-wide daemon, the installer will ask for a password for elevated access rights to install it.

Command Line

- The Installer can also be used from the command line to install uberAgent using the command `installer -pkg uberAgent.pkg -target /`
- This requires root privileges. A command line installation can be executed locally or remotely, e.g., using SSH.

License File

If you have a license file for uberAgent, copy it to the following directory `/Library/Application Support/uberAgent`. Without a license file, uberAgent displays a splash screen during logon. [Contact us](#) for an evaluation license.

Installation Through Splunk Deployment Server

Note: Deployment Server can only be used with Splunk Enterprise and requires Splunk Universal Forwarder on the endpoint as deployment client. Please make sure that Splunk Universal Forwarder has **sufficient privileges** to perform system-wide installations, e.g. by [enabling boot-start](#).

uberAgent

Copy the directory `uberAgent_endpoint` from the unzipped uberAgent download package to `$(SPLUNK_HOME)/etc/deployment-apps` on your deployment server. Please make sure to apply the executable flag to the installation script by executing `chmod +x silent-install.sh`. Besides that, the `uberAgent_endpoint` folder is ready to use for deployment on Windows as well as macOS operating systems.

Note: `$(SPLUNK_HOME)` refers to the base directory of the Splunk installation, typically `/opt/splunk` on Linux.

Configuration

To deploy customized configuration files, copy them into the directory `$SPLUNK_HOME/etc/deployment-apps/uberAgent_endpoint/bin`. This overwrites existing files under `/Library/Application Support/uberAgent/`.

License File

If you have a license file for uberAgent, copy it into the directory `$SPLUNK_HOME/etc/deployment-apps/uberAgent_endpoint/bin`.

Serverclass

Create a file called `serverclass.conf` in `$SPLUNK_HOME/etc/system/local` on your deployment server. `serverclass.conf` defines what to deploy where. For a quick start, paste the following content into `serverclass.conf` to deploy uberAgent to all macOS machines. You may want to fine-tune this to suit your needs.

```
1 # [global]
2 # We cannot match by machine type here. We'll do that on the app level
   below.
3 whitelist.0 = *
4
5 # Define a serverclass
6 [serverClass:macOS]
7 # Deploy only to macOS machines
8 machineTypesFilter = darwin-x86_64
9
10 # Define which apps to deploy to the serverclass
11 [serverClass:macOS:app:uberAgent_endpoint]
12 stateOnClient = enabled
13 restartSplunkd = true
```

To make Splunk read the new file `serverclass.conf` run the following command:

```
1 $SPLUNK_HOME/bin/splunk reload deploy-server
```

Configuration

uberAgent can be configured very flexibly. By editing the [configuration](#), you can switch metrics on or off, change the data collection frequency and significantly [reduce the data volume](#).

Example uberAgent PPC Profile

This is an exemplary privacy preferences policy control (PPPC) profile to grant uberAgent the necessary TCC privileges.

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.
   com/DTDs/PropertyList-1.0.dtd">
3 <plist version="1.0">
4 <dict>
5   <key>PayloadContent</key>
6   <array>
7     <dict>
8       <key>PayloadDescription</key>
9       <string>uberAgent</string>
10      <key>PayloadDisplayName</key>
11      <string>uberAgent</string>
12      <key>PayloadIdentifier</key>
13      <string>5FD70527-9AC3-4667-82AF-8F8F44C95C94</string>
14      <key>PayloadOrganization</key>
15      <string>vast limits GmbH</string>
16      <key>PayloadType</key>
17      <string>com.apple.TCC.configuration-profile-policy</string>
18      <key>PayloadUUID</key>
19      <string>E86AC250-6BF9-4C91-BB0A-5890F000A48C</string>
20      <key>PayloadVersion</key>
21      <integer>1</integer>
22      <key>Services</key>
23      <dict>
24        <key>Accessibility</key>
25        <array>
26          <dict>
27            <key>Allowed</key>
28            <true/>
29            <key>CodeRequirement</key>
30            <string>anchor apple generic and identifier "
               com.vastlimits.uberAgent" and (certificate
               leaf[field.1.2.840.113635.100.6.1.9] /*
               exists */ or certificate 1[field
               .1.2.840.113635.100.6.2.6] /* exists */ and
               certificate leaf[field
               .1.2.840.113635.100.6.1.13] /* exists */ and
               certificate leaf[subject.OU] = "64N35HHH3F"
               )</string>
31            <key>Comment</key>
32            <string></string>
33            <key>Identifier</key>
34            <string>com.vastlimits.uberAgent</string>
35            <key>IdentifierType</key>
36            <string>bundleID</string>
37          </dict>
38        </array>
39      <key>SystemPolicyAllFiles</key>

```

```
40         <array>
41             <dict>
42                 <key>Allowed</key>
43                 <true/>
44                 <key>CodeRequirement</key>
45                 <string>anchor apple generic and identifier "
                    com.vastlimits.uberAgent" and (certificate
                    leaf[field.1.2.840.113635.100.6.1.9] /*
                    exists */ or certificate 1[field
                    .1.2.840.113635.100.6.2.6] /* exists */ and
                    certificate leaf[field
                    .1.2.840.113635.100.6.1.13] /* exists */ and
                    certificate leaf[subject.OU] = "64N35HHH3F"
                    )</string>
46                 <key>Comment</key>
47                 <string></string>
48                 <key>Identifier</key>
49                 <string>com.vastlimits.uberAgent</string>
50                 <key>IdentifierType</key>
51                 <string>bundleID</string>
52             </dict>
53         </array>
54     </dict>
55 </dict>
56 </array>
57 <key>PayloadDescription</key>
58 <string>uberAgent</string>
59 <key>PayloadDisplayName</key>
60 <string>uberAgent</string>
61 <key>PayloadIdentifier</key>
62 <string>5FD70527-9AC3-4667-82AF-8F8F44C95C94</string>
63 <key>PayloadOrganization</key>
64 <string>vast limits GmbH</string>
65 <key>PayloadScope</key>
66 <string>System</string>
67 <key>PayloadType</key>
68 <string>Configuration</string>
69 <key>PayloadUUID</key>
70 <string>F53E14C7-D9ED-4933-8A71-87FD74C9870D</string>
71 <key>PayloadVersion</key>
72 <integer>1</integer>
73 </dict>
74 </plist>
```

Installing Splunk Universal Forwarder

July 25, 2024

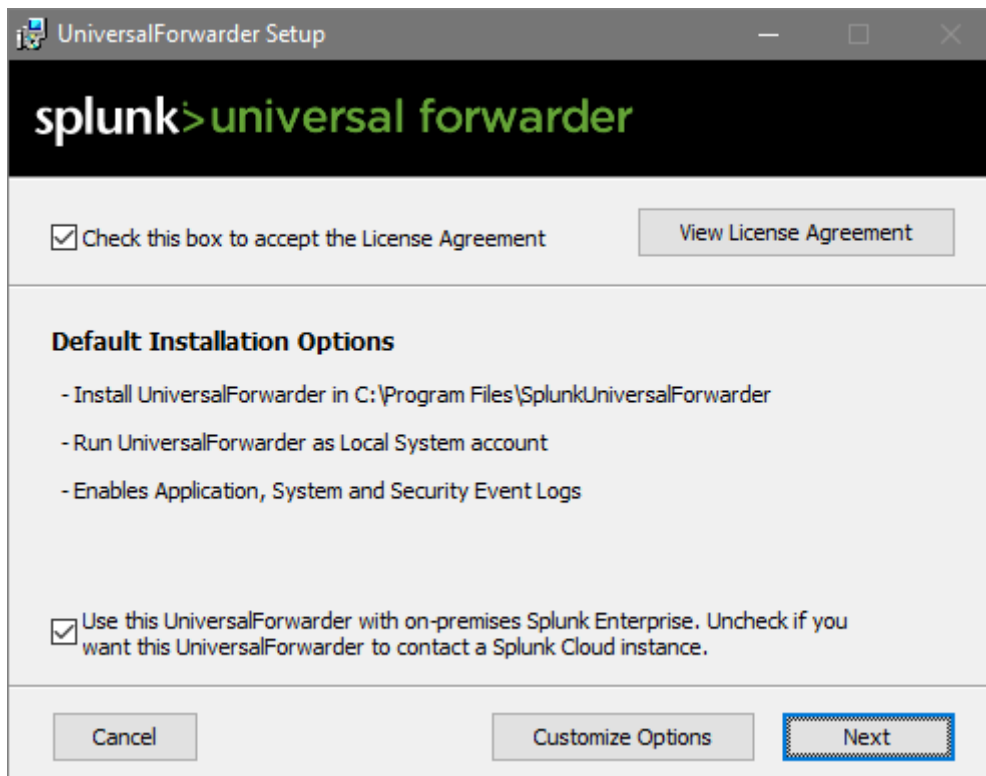
If you have chosen an [architecture option](#) where uberAgent interacts with Splunk through Splunk'

s Universal Forwarder you need to install Universal Forwarder on every machine along with uberAgent.

The following description shows you how to install and configure Universal Forwarder for uberAgent. In this example, the Splunk server's FQDN is `srv1.hk.test`.

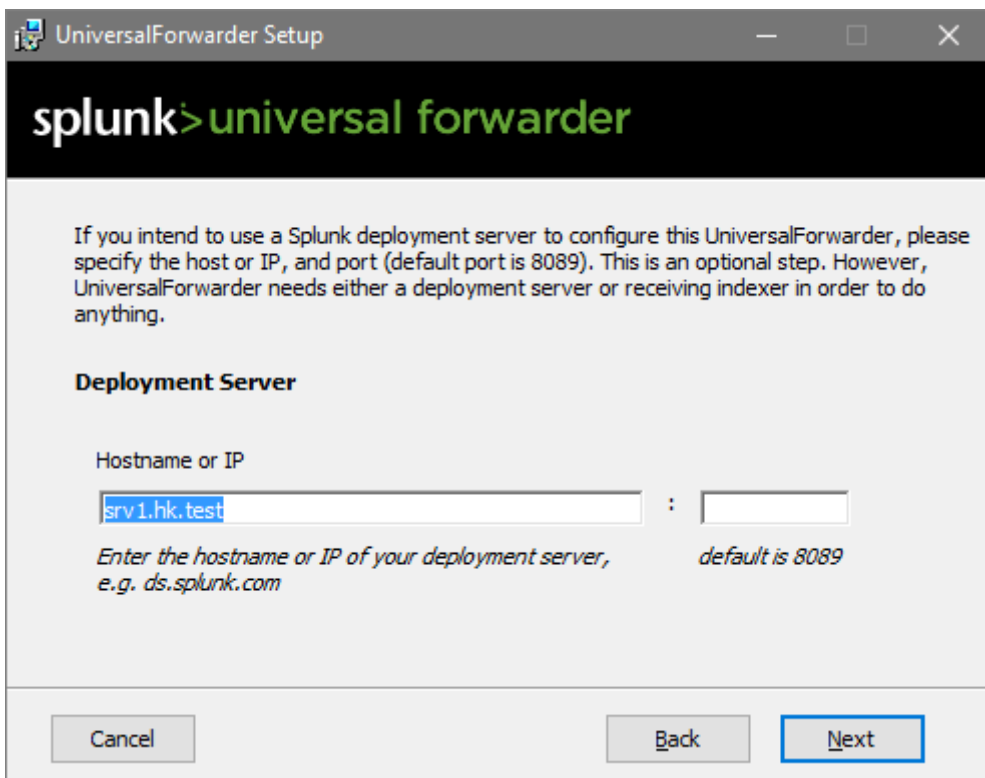
Installation

Launch the Universal Forwarder MSI file. Accept the license agreement and click **Next**.



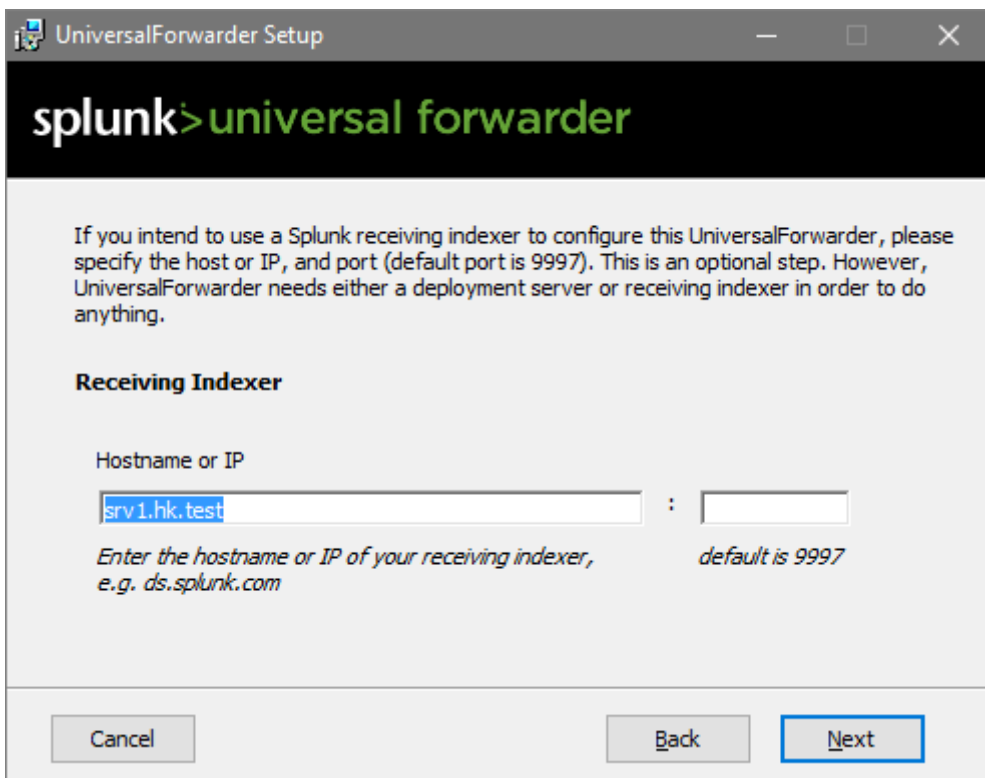
Deployment Server

If you have Splunk Enterprise, you can use Splunk's Deployment Server functionality to deploy apps. In that case, specify the Splunk server name. You can leave the port empty to use the default. If you have Splunk Free leave both fields empty.



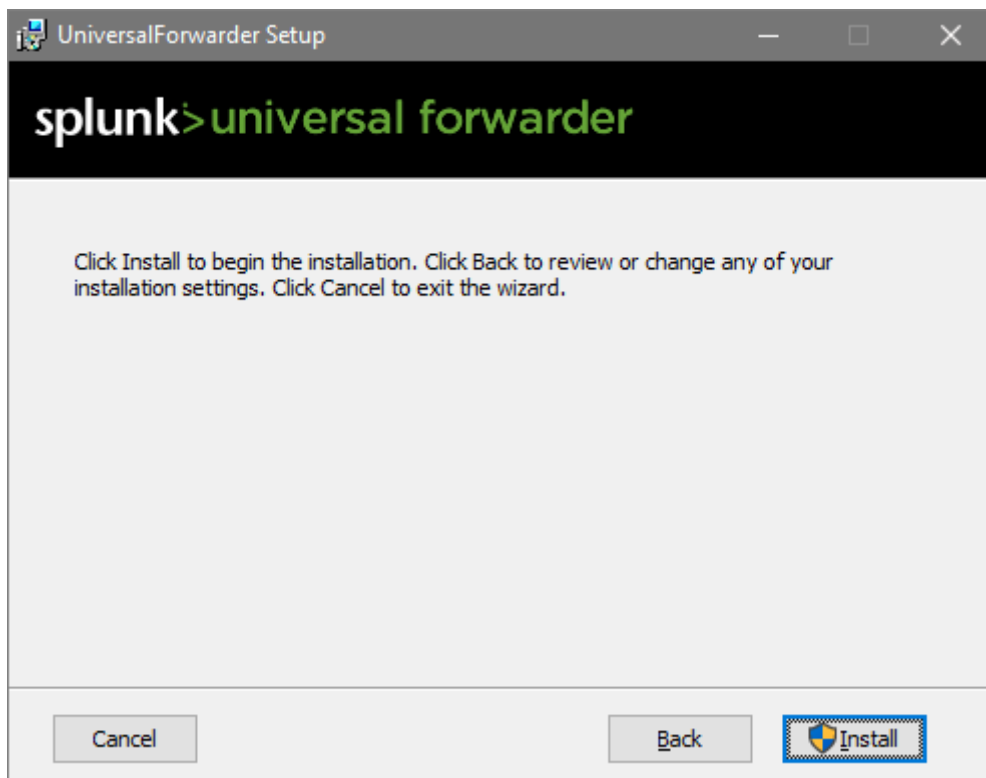
Indexer

Specify the name of your Splunk Indexer. In this simple walkthrough, our Splunk server also acts as an indexer. Again, the port is left at the default value:



Finished

That's all!



Configuration

Receive uberAgent Data via TCP Port

If you want Universal Forwarder to handle all Splunk communications, you need to configure uberAgent to pass its output to Universal Forwarder on the same machine. To do that, open a TCP port uberAgent can send data to by adding the following to `$$SPLUNK_HOME\etc\system\local\inputs.conf` on your Universal Forwarders:

```
1 [tcp://127.0.0.1:19500]
2 connection_host = none
3 sourcetype = dummy
4 listenOnIPv6 = no
5 acceptFrom = 127.0.0.1
```

Note: `$$SPLUNK_HOME` refers to the base directory of the Splunk (Forwarder) installation, typically `C:\Program Files\SplunkUniversalForwarder`.

If you are deploying the `uberAgent_endpoint` app, port 19500 is opened for you automatically ([details](#)).

Disable Universal Forwarder Eventlog Data Collection

A default installation of Universal Forwarder sends all data from the Windows Application, Security, and System event logs to Splunk. If you do not need that, edit `$SPLUNK_HOME\etc\apps\Splunk_TA_windows\local\inputs.conf` so that all stanzas are disabled as in the following example:

```
1 [WinEventLog://Application]
2 disabled = 1
3
4 [WinEventLog://Security]
5 disabled = 1
6
7 [WinEventLog://System]
8 disabled = 1
```

Unattended (Silent) Installation

You can find all the information required for automating the deployment of Universal Forwarder [here](#).

Preparation for Imaging/Citrix PVS

If you intend to copy the installation via an imaging method or Citrix PVS, you need to remove instance-specific information such as server name and GUID from the Universal Forwarder installation. To do that, follow these steps right before capturing the image:

- Stop the service `SplunkForwarder` (but leave the start type at `automatic`).
- Open an administrative command prompt.
- Run the command: `C:\Program Files\SplunkUniversalForwarder\bin\splunk clone-prep-clear-config`.
- Prepare the machine for cloning as necessary, but do not reboot.

Installing the Chrome Browser Extension

July 9, 2024

uberAgent's browser web app performance functionality requires a browser extension to be installed. This article lists the necessary steps.

Enabling the Agent Metric

To enable data collection from Chrome make sure uberAgent's [BrowserPerformanceChrome](#) metric is enabled in the [configuration](#). In the default configuration, [BrowserPerformanceChrome](#) is enabled.

Installing the Chrome Extension

The extension is available from two different channels: release and beta. The release channel gets only fully-tested versions of the extension, while the beta channel additionally gets beta-quality versions.

We recommend putting the majority of users on the release channel and a small minority on the beta channel.

Manual Installation

For tests and PoCs, it may be easiest to install uberAgent's Chrome extension manually from the Chrome Web Store.

Release Channel Install the extension from [release channel](#) on the Chrome Web Store.

Beta Channel Install the extension from [beta channel](#) on the Chrome Web Store.

Automated Deployment

Deployment of uberAgent's Chrome extension is easily possible with Group Policy. Follow the steps in the Chromium Documentation to configure the [ExtensionInstallForcelist](#) setting.

To configure Chrome to install the uberAgent extension from the standard Chrome Web Store update URL add the following to the [ExtensionInstallForcelist](#) setting:

Release Channel `cmcmennehclgdccnlmnjladhlmclbkb;https://clients2.google.com/service/update2/crx`

Beta Channel `lnjgkeibanadbijljjijogklikdblaom;https://clients2.google.com/service/update2/crx`

Offline Deployment

If your endpoints are not connected to the Internet and can't access Chrome's Web Store, you can also [pre-install the extensions](#). Please [contact us](#) for the CRX file or use an online CRX extractor.

Note that using the offline deployment you need to push updated CRX files manually.

Relevant Configuration Settings

Native Messaging

uberAgent's Chrome extension uses native messaging to communicate with the agent. In a default configuration of Chrome, native messaging is not restricted.

If native messaging has been restricted, for example via the [NativeMessagingBlocklist](#) Group Policy setting, an exception needs to be defined for the uberAgent extension, for example via the [NativeMessagingAllowlist](#) Group Policy setting.

Installing the Firefox Browser Extension

July 9, 2024

uberAgent's browser web app performance functionality requires a browser extension to be installed. This article lists the necessary steps for the Firefox extension. The requirements can be found [here](#).

Enabling the Agent Metric

To enable data collection from Firefox make sure uberAgent's [BrowserPerformanceFirefox](#) metric is enabled in the [configuration](#). In the default configuration, [BrowserPerformanceFirefox](#) is enabled.

Installing the Firefox Extension

The extension is available from two different channels: release and beta. The release channel gets only fully-tested versions of the extension, while the beta channel additionally gets beta-quality versions.

Manual Installation

For tests and PoCs, it may be easiest to install uberAgent's Firefox extension manually.

Release Channel Install the extension from release channel on the [Firefox Web Store](#).

Beta Channel To install the beta version of the extension:

1. In Firefox, click [here](#) and agree to the terms and conditions
2. When Firefox asks `Allow uberagent.com to install an add-on?` select `Continue to Installation`
3. When Firefox asks `Add uberAgent - beta?` select `Add`
4. Firefox shows a message indicating that the installation was successful

We recommend putting the majority of users on the release channel and a small minority on the beta channel.

Note: due to a change by Mozilla, beta versions prior to 2.6 cannot upgrade to 2.6+ automatically. Please uninstall older versions of the extension, and then install version 2.6+. This only applies to the beta channel.

User Consent The extension version 2.6 or newer initially does not collect any data. **To enable data collection click the uberAgent icon in the upper right corner.**

Automated Installation

Add-on Deployment Deployment of uberAgent's Firefox extension is easily possible with Group Policy (Firefox 60+ required). Please follow the steps in [Mozilla's documentation](#).

Below is an example JSON code to block the user from installing any extension but force the uberAgent extension installation through Group Policy. Put it in [Policies - Administrative Templates - Mozilla - Firefox - Extensions - Extension Management](#).

```
1 {
2
3   "*": {
4
5     "blocked_install_message": "If you need this browser extension,
6       please contact the helpdesk.",
7     "installation_mode": "blocked"
8   }
9 ,
10  "{
11    2e53b2d2-1bdf-446a-8f9d-9be4173886fe }
12  ": {
13    "installation_mode": "force_installed",
14    "install_url": "https://addons.mozilla.org/firefox/downloads/
15      latest/uberagent/latest.xpi"
```

```
15     }  
16  
17 }
```

User Consent As of 2019-12-02, Mozilla enforces [showing a consent dialog](#) to users if an add-on collects information about visited URLs, even if the add-on was deployed through Group Policy.

This change **forces** us to publish a new version of the add-on that initially does not collect any data. To automatically enable data collection set the new managed storage setting [EnableBrowserDataCollection](#) to **true**. This can be achieved in one of two ways.

Automatically declare consent and enable data collection by running a script to set [EnableBrowserDataCollection](#) to **true**:

- Make sure that cookies are enabled and Firefox's setting `dom.storage.enabled` is set to **true**
- Download and unzip [this script](#)
- Run the script with elevated permissions on every endpoint:
`powershell.exe -executionpolicy bypass -file Set-uberAgentFFEnableBrowserDataCollection.ps1`
- Only upgrade to or install version 2.6+ of uberAgent's Firefox add-on once the script has been run on all endpoints

If you prefer to change things manually instead of using our script we have you covered, too:

1. Create the file `uAFirefoxSettings.json` in uberAgent's installation directory with the following content:

```
{ "name": "{ 2e53b2d2-1bdf-446a-8f9d-9be4173886fe } ", "description": "ignored", "type": "storage", "data": { "EnableBrowserDataCollection": true } }
```
2. Create the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\ManagedStorage\{ 2e53b2d2-1bdf-446a-8f9d-9be4173886fe }`
3. Set the key's default value to the full path of the JSON file from step one, e.g. `C:\ProgramFiles\vast limits\uberAgent\uAFirefoxSettings.json`

If you do not set [EnableBrowserDataCollection](#) to **true before upgrading to or installing version 2.6+ of uberAgent's Firefox extension users have to opt-in at first run. If they do not opt-in, uberAgent cannot collect any website metrics.**

Future versions of uberAgent (> 5.3) will set [EnableBrowserDataCollection](#) to **true** automatically unless this is specifically disabled in uberAgent's configuration.

Note that setting `ShowConsentDialog` to **false** has the same effect as setting `EnableBrowserDataCollection` to **true**.

Installing the Edge Browser Extension

July 9, 2024

uberAgent's browser web app performance functionality requires a browser extension to be installed. This article lists the necessary steps.

Enabling the Agent Metric

To enable data collection from Edge make sure uberAgent's `BrowserPerformanceEdge` metric is enabled in the [configuration](#). In the default configuration, `BrowserPerformanceEdge` is enabled.

Installing the Edge Extension

The extension is available from the Chrome Web Store from two different channels: release and beta. The release channel gets only fully-tested versions of the extension, while the beta channel additionally gets beta-quality versions.

We recommend putting the majority of users on the release channel and a small minority on the beta channel.

Manual Installation

For tests and PoCs, it may be easiest to install uberAgent's Edge extension manually from the Chrome Web Store. Please note that you need to [allow extensions from other stores](#).

Release Channel Install the extension from [release channel](#) on the Chrome Web Store.

Beta Channel Install the extension from [beta channel](#) on the Chrome Web Store.

Automated Deployment

Deployment of uberAgent's Edge extension is easily possible with Group Policy. Follow the steps in the Edge documentation to configure the [ExtensionInstallForcelist](#) setting. Extensions on the [ExtensionInstallForcelist](#) will also get installed if the Edge setting [Allow extensions from other stores](#) is not enabled.

To configure Edge to install the uberAgent extension from the standard Chrome Web Store update URL add the following to the [ExtensionInstallForcelist](#) setting:

Release Channel `cmcmennehc1gdccn1mnjladh1kmc1bkb;https://clients2.google.com/service/update2/crx`

Beta Channel `1njgkeibanadbij1jjijogklikdblaom;https://clients2.google.com/service/update2/crx`

Offline Deployment

If your endpoints are not connected to the Internet and can't access Chrome's Web Store, you can also [pre-install the extensions](#). Please [contact us](#) for the CRX file or use an online CRX extractor.

Note that using the offline deployment you need to push updated CRX files manually.

Relevant Configuration Settings

Native Messaging

uberAgent's Edge extension uses native messaging to communicate with the agent. In a default configuration of Edge, native messaging is not restricted.

If native messaging has been restricted, for example via the [NativeMessagingBlocklist](#) Group Policy setting, an exception needs to be defined for the uberAgent extension, for example via the [NativeMessagingAllowlist](#) Group Policy setting.

Installing the Internet Explorer Browser Add-on

July 9, 2024

uberAgent's browser web app performance functionality requires a browser add-on (aka extension) to be installed. This article lists the necessary steps.

Enabling and Configuring the Agent Metric

To enable data collection from Internet Explorer make sure uberAgent's [BrowserPerformanceIE](#) metric is enabled in the configuration. In the default configuration, [BrowserPerformanceIE](#) is enabled.

You can optionally disable the collection of performance data from embedded frames via the registry. The following setting is valid for 32-bit and 64-bit Windows systems:

```
1 Hive:           HKEY_LOCAL_MACHINE
2 Key:           SOFTWARE\vast limits\uberAgent
3 Value name:    IEAddonIgnoreFrames
4 Value type:    DWORD
5 Value data:    0 (default) - Collect performance data from each page
                 including embedded frames
6               1           - Do not collect performance data from embedded
                           frames
```

Installing the IE Add-on

The add-on's files are part of the uberAgent setup and placed in the installation directory automatically.

Note: the add-on is **not registered automatically** to prevent prompts asking the end-users for confirmation.

Registering the IE Add-on

Manual Registration

For tests and PoCs, it may be easiest to register uberAgent's Internet Explorer add-on manually. The installation directory contains the file `Register-uAIEExtension.cmd`. Run this file with elevated rights to register uberAgent's Internet Explorer add-on DLLs.

Alternatively, run the following commands with elevated rights:

```
1 regsvr32 /s "%ProgramFiles%\vast limits\uberAgent\uAIEExtension32.dll"
2 regsvr32 /s "%ProgramFiles%\vast limits\uberAgent\uAIEExtension64.dll"
```

Automated Registration - Software Deployment Tool

The automated registration of uberAgent's Internet Explorer add-on is easily possible with your software deployment tool of choice. Make sure to register the two DLLs using the `regsvr32` commands (see above) after uberAgent is installed.

Automated Registration - uberAgent Service

uberAgent's Internet Explorer add-on can be registered automatically through uberAgent's system service. Please note that this does not happen by default to prevent end-user prompts (see below).

To configure the uberAgent service to automatically register the IE add-on set the [RegisterIEAddOn](#) configuration value to 1.

Enabling the IE Add-on

Enable Manually

Internet Explorer will ask each user to enable the add-on once the DLLs are registered when the browser is started.

Enable Automatically

To avoid end-user prompts, configure the Group Policy setting [Add-on List](#) for automatic enablement. The setting can be found at **Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Security Features > Add-on Management > Add-on List**.

Add an entry with the following values:

```
1 Value name: {
2   82004312-5B53-46F1-B179-4FCE28048E6F }
3
4 Value data: 1
```

Relevant Configuration Settings

Protected Mode

The uberAgent Internet Explorer add-on has been tested successfully and is supported in protected mode.

Enhanced Protected Mode

The uberAgent Internet Explorer add-on has been tested successfully and is supported in enhanced protected mode.

Enterprise Mode

Internet Explorer enterprise mode allows customers to define URLs that are rendered with older versions of the IE engine (e.g., IE9 or IE10). uberAgent's Internet Explorer add-on requires IE11 and only works for sites rendered with version 11 of the IE engine.

Upgrading uberAgent

July 9, 2024

When a new version of uberAgent is available you need to do the following in order to update your existing installation.

Understand What is New and Changed

Please read the [changelog](#). Changes might affect uberAgent's configuration, for example.

Depending on the nature of the changes made for a new version it may be necessary to update custom apps that make use of the data collected by uberAgent.

uberAgent Splunk Indexer and Dashboard Apps

Before upgrading from version 6, delete the Splunk KV store lookup `lookup_hostinfo2` by running the following Splunk search:

```
1 | outputlookup lookup_hostinfo2
```

Also, run the following commands one after another to delete obsolete KV Store collections of the experience scores. Starting with 6.1, scores are stored in an index.

```
1 | outputlookup lookup_score_per_machine
```

```
1 | outputlookup lookup_score_historic_per_machine
```

```
1 | outputlookup lookup_score_per_session
```

```
1 | outputlookup lookup_score_historic_per_session
```

```
1 | outputlookup lookup_score_per_application
```

```
1 | outputlookup lookup_score_historic_per_application
```

Delete the uberAgent app directories:

- ```
1 $SPLUNK_HOME\etc\apps\uberAgent
2 $SPLUNK_HOME\etc\apps\uberAgent_ESA
3 $SPLUNK_HOME\etc\apps\uberAgent_indexer
```

**Install** the new versions of the Splunk apps as described [here](#).

**Restart** Splunk.

Starting with uberAgent 6.1, we added a second index called `score_uberagent_uxm` in addition to the existing index `uberAgent`.

This is because uberAgent now uses index storage for scores on the Experience Score dashboard instead of the KV Store. So please make sure to update the `uberAgent_indexer` app as well.

This is especially important when using Splunk Cloud. Details are available [here](#).

## uberAgent on the Endpoints

In uberAgent 7.0, host and user tags are collected through dedicated timers instead of a static interval. Please adjust your configuration and implement a timer as described [here](#) to continue collecting user and host tags after upgrading to uberAgent 7.0.

uberAgent's MSI installer has all the logic to upgrade an installation automatically preserving the current settings. Just run the installer again using your deployment method of choice as described [here](#).

**Note:** customizations to the [configuration](#) in the installation directory are not retained during an upgrade. Such customizations must be re-applied after the upgrade. We recommend to store the configuration files [outside the installation directory](#).

## Elasticsearch

New uberAgent versions generally come with additional fields. This makes it necessary to update the index template. To do that, [overwrite the existing index template](#) with the new version. Please note that templates are applied to new indexes only. Existing indexes keep their templates.

## Configuration via Group Policy

July 9, 2024

**Platforms:** Windows only

## Overview

To configure uberAgent via Group Policy, follow these steps:

- Copy the Group Policy AMDL/ADMX templates included in the uberAgent download package to your `PolicyDefinitions` directory.
- Create a new GPO that applies to the computers uberAgent is installed on.
- Import the default configuration from the directory `uberAgent components\Group Policy\GPO backup` of the download package, choosing either the default configuration or the version optimized for data volume.
- Adjust the imported default configuration as required.
- Local configuration files on the endpoints are ignored, and policy settings are used exclusively. If an additional configuration file is set via Group Policy, the settings of that file overwrite Group Policy settings.

## Detailed Description

### Preparation

In order to have the uberAgent settings show up in Group Policy Management Editor, you need to add uberAgent's Group Policy template (ADMX and ADML files) to your `PolicyDefinitions` directory. If you are using a Central Store for Group Policy administrative template files, then the location of the `PolicyDefinitions` directory is:

```
\\FQDN\SYSVOL\FQDN\policies\PolicyDefinitions
```

If you are not using a Central Store, administrative templates reside on the machines that are used to manage Group Policy in:

```
%Systemroot%\PolicyDefinitions
```

In any case, copy all files from this location in uberAgent's download package to your `PolicyDefinitions` directory:

```
uberAgent components\Group Policy\Administrative template (ADMX)
```

That directory should contain at least:

- `uberAgent.admx`
- `en\uberAgent.adml`

### Configuration

Once the administrative template files are in the correct location, choose a Group Policy Object (GPO) you want to configure uberAgent's settings in. uberAgent's configuration settings are located in **Com-**

## **Computer Configuration > Policies > Administrative Templates > uberAgent.**

**Settings Import** The easiest way to get a working configuration is to import the settings from the GPO backup included in the uberAgent download package.

To import the default configuration, follow these steps:

- In Group Policy Management Console (GPMC), navigate to the node **Group Policy Objects** (import is not available on a GPO link).
- Right-click the GPO you want to import the settings into.
- Select **Import Settings....**
- When asked for the **Backup location** from which settings will be imported select the directory `uberAgent components\Group Policy\GPO backup` from uberAgent's download package.
- Complete the **Import Settings** wizard.
- Open the GPO you imported the settings into in Group Policy Management Editor.
- Navigate to **Computer Configuration > Policies > Administrative Templates > uberAgent > Receivers > Receiver 01.**
- Adjust the setting **Servers (required)** according to your requirements.

**Manual Configuration** As an alternative to importing the default configuration (as described above), you can configure uberAgent's settings from scratch. Here are some recommendations:

- Enable on-demand metrics: **On-demand metrics > On-demand metrics.**
- Configure and enable a receiver: **Receivers > Receiver 01.**
- Configure and enable at least one timer: **Timers > Timer 01.**
- Do not forget to enable the setting **Configuration through Group Policy.**

## **Troubleshooting**

Verify in the registry that the machines running uberAgent have received the correct Group Policy settings. uberAgent's settings are stored in `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\vast limits`.

Verify that uberAgent is processing the settings correctly:

- Restart the uberAgent service.
- Open the [log file](#).
- Right after the service starts uberAgent logs in detail how it processes its configuration and what source (Group Policy, config file) is being used.

## Configuration via Local Config Files

July 9, 2024

**Platforms:** all

### Config File Location

#### Windows

The default configuration file `uberAgent.conf` is located in the installation directory, typically `C:\Program Files\vast limits\uberAgent`.

**Configuration Optimized for Data Volume** To switch to the configuration optimized for data volume back up `uberAgent.conf` and rename `uberAgent-data-volume-optimized.conf` to `uberAgent.conf`.

**Persisting Configuration Files in %ProgramData%** The agent installer completely removes the installation directory, including any configuration files, during uninstalls and upgrades.

To persist configuration files across agent upgrades, place them in `%ProgramData%\vast limits\uberAgent\Configuration`. As explained [here](#), configuration files in `%ProgramData%` take precedence over configuration files in the installation directory.

Please note that you **need to update** configuration files in `%ProgramData%` when rolling out new versions of the agent.

#### macOS

The default configuration file `uberAgent.conf` is located in `/Library/Application Support/uberAgent/`. During upgrades, files in this directory are not overwritten to preserve customizations. It is recommended to update the default configuration from the config file templates (see below) after an upgrade.

**Config File Templates** The installer copies config file templates to `/Library/Application Support/uberAgent/Config Templates/`. Changes to the template files have no effect - they are only meant to be used as a reference.

## Applying Configuration Changes

The agent reads the configuration upon startup of the `uberAgent` service/daemon. To apply configuration changes, restart the `uberAgent` service/daemon.

## Config File Syntax

July 9, 2024

uberAgent's configuration file supports several advanced syntax features.

### Windows

#### PATH\_REGEX

`PATH_REGEX` stands for a **regex** in which **environment variables** can be used. It is matched against a **file system** path. The following rules apply:

- Environment variables (enclosed in percent signs, e.g., `%ProgramFiles%`) are expanded first, regex matching happens second.
- Paths are specified as regular expressions.
- Backslashes must be escaped by prepending a second backslash.
- Matching is case-insensitive.
- Specifying only the file name without the full path works but is not recommended.

### Agents on All Operating Systems

#### ConfigInclude

A `@ConfigInclude` directive includes another configuration file. The other file is identified by name (without path) and must reside in the same directory as the configuration file including it. The additional `platform` parameter may be used to conditionally include a file on the selected platform (`Windows` or `macOS`). Platform matching is case-insensitive.

Examples:

```
1 #Include on all platforms
2 @ConfigInclude other-file.conf
```

```
1 # Include on Windows only
2 @ConfigInclude windows-specific.conf platform=Windows
```



## PROCESS\_NAME\_REGEX

`PROCESS_NAME_REGEX` stands for a **regex** that is matched against a **process name**. The following rules apply:

- Backslashes must be escaped by prepending a second backslash.
- Matching is case-insensitive.
- Only the file name is used for matching, not the full path.

## URL\_REGEX

`URL_REGEX` stands for a **regex** that is matched against a **URL**. The following rules apply:

- Backslashes must be escaped by prepending a second backslash.
- Matching is case-sensitive.

Format of the URLs matched against `URL_REGEX`:

- Origin and path (without query segment), e.g.: `https://uberagent.com/download/`
- Port numbers are stripped from the URL if they match the default port number.

## platform=

All configuration stanzas can optionally be limited to a specific platform using the `platform=` attribute.

- The platform is either **Windows** or **macOS**
- Stanzas without `platform=` are active on all supported platforms.

### Example

```
1 [Timer platform=Windows]
2 ...
3
4 [Timer platform=macOS]
5 ...
```

## Change configured setting values dynamically with uAQL

Some configuration settings are changeable using prefixed uAQL queries. This allows use cases where configuration values depend on environment variables, registry values or require string prefixes/suffixes. For now, the following configuration settings are changeable:

### [Receiver]

- RESTToken
- TLSClientCertificate
- ElasticIngestPipeline
- Index
- Host
- Source
- PersistentOutputQueuePathWindows
- PersistentOutputQueuePathMacOS
- KafkaTopicName

Consider the following **example** to configure a prefix string in any *KafkaTopicName* setting.

```
1 KafkaTopicName = uaql(set(KafkaTopicName, concat('vastlimits_',
KafkaTopicName)))
```

## UXM Features & Configuration

July 9, 2024

uberAgent uses sophisticated methods to collect **relevant data** from the operating system and applications. It then presents the data in an **easily understandable** and human-friendly way to give IT the information they actually need to improve **digital employee experience** and maintain **security**.

This section lists important features with their respective configuration options.

## Experience Score

July 25, 2024

The experience score is a single view that shows the current and past status of all devices, users, and applications monitored by uberAgent.

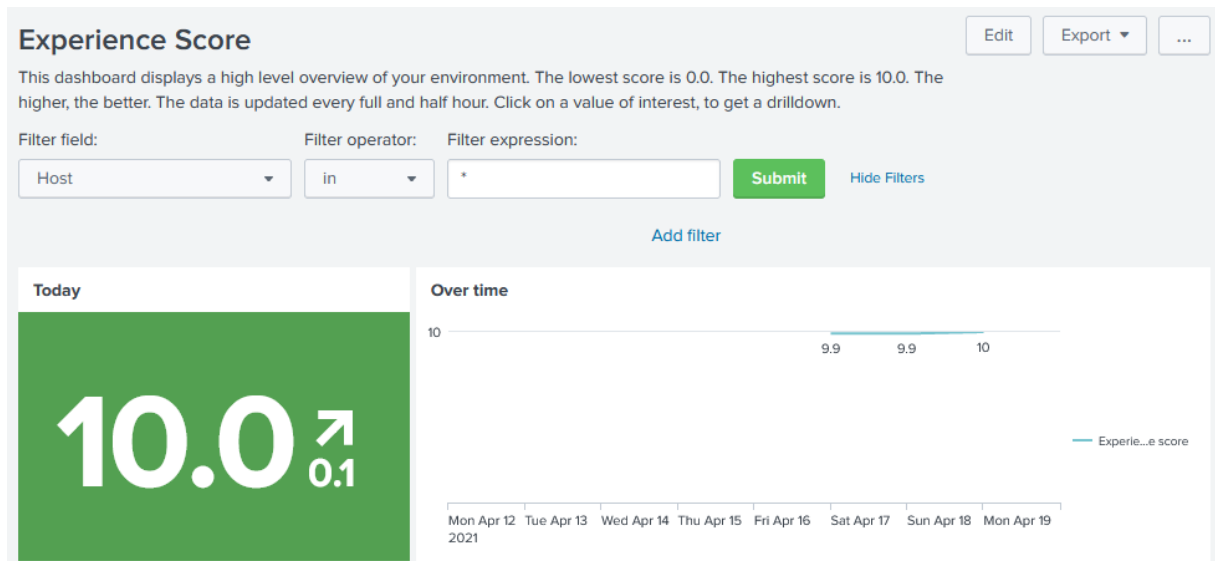
The score is evaluated every full and half hour. It ranges from **zero** to **ten**. The **higher** the **better**. Scores from zero to four are highlighted in red, scores from four to seven in yellow, and scores from seven to ten in green. The experience score is currently available for uberAgent UXM.

## Experience Score Dashboard

The experience score dashboard is the new entry point of the uberAgent UXM Splunk app. It calculates and visualizes experience scores for the entire estate, breaking the data down by category and component, highlighting components where potential issues are originating from.

The dashboard also provides quick access to important **KPIs** like logon duration, application responsiveness, or application errors.

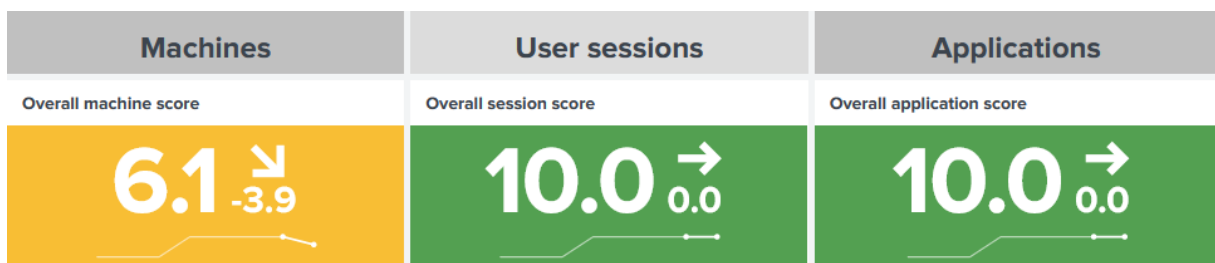
### Overall Score



The filter at the top allows filtering the dashboard to a subset of machines. By default, all machines are shown.

On the left in the second row one can see the overall score and the trend compared to yesterday. On the right the score development over time is visualized.

### Machine, User Session, and Application Scores

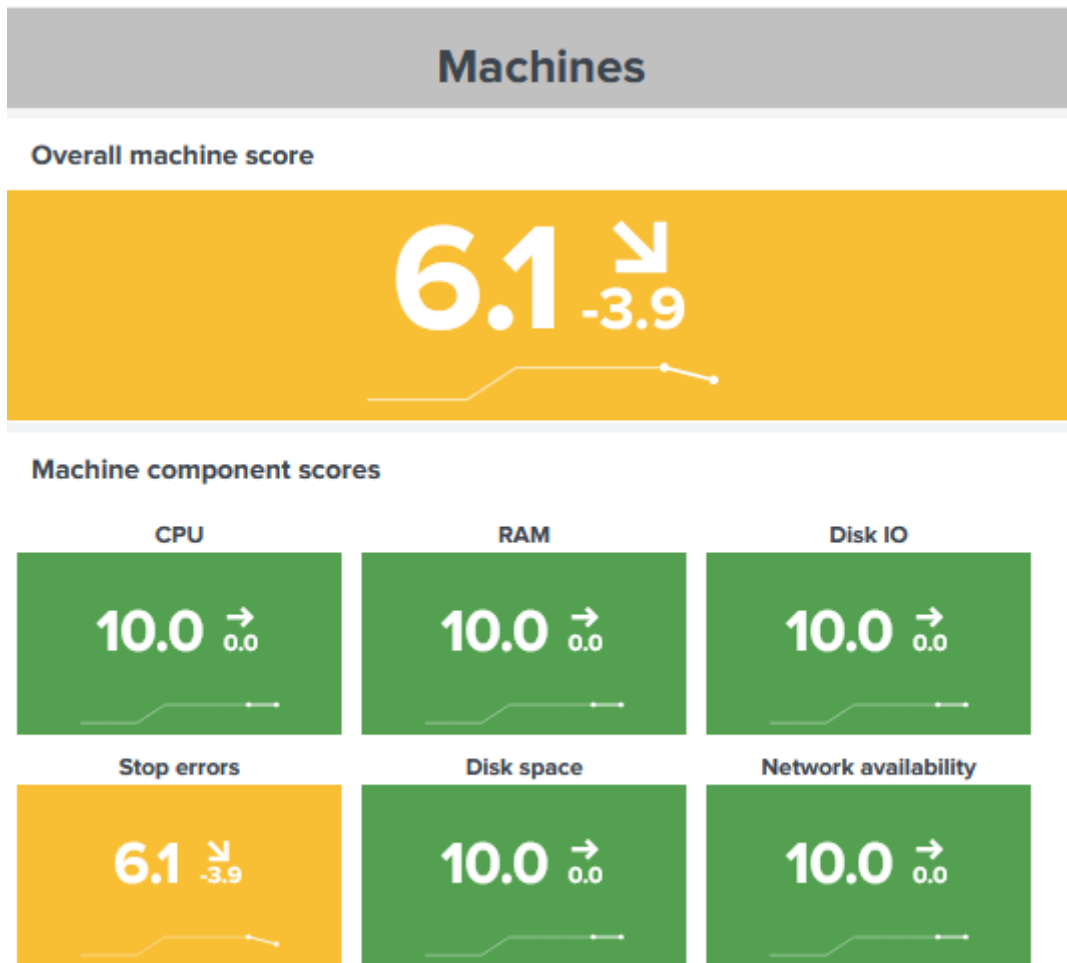


The overall score derives from three categories:

- **Machine score:** quality indicator for machine performance and health
- **User session score:** quality indicator for user session performance and health
- **Application score:** quality indicator for application performance and health

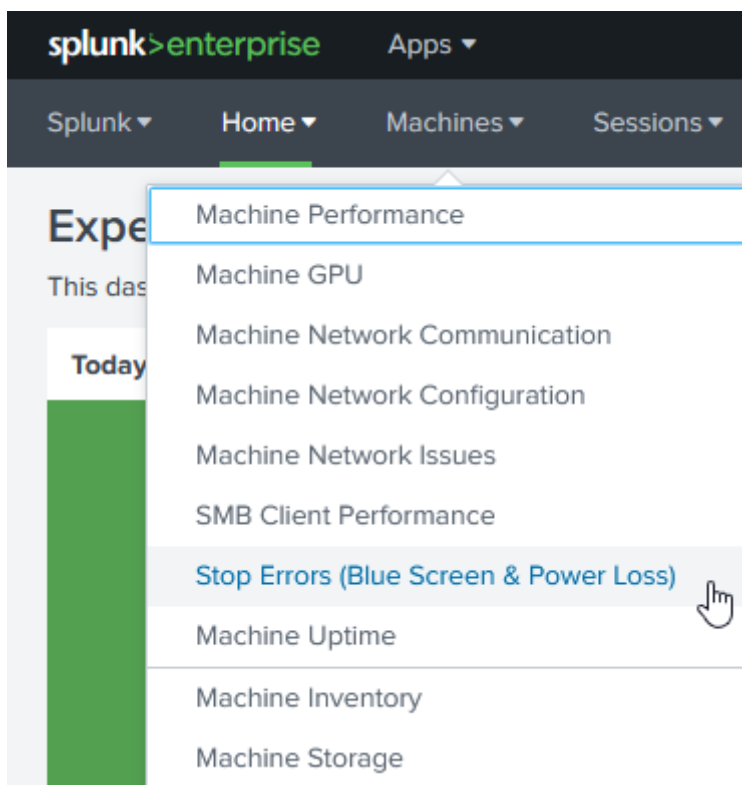
The charts show a trend indicator for the last day as well as a sparkline for the last seven days.

### Score Components



Each category is calculated by different components. Components differ per category. For example, *Stop errors* is a component solely for the machine category, while the *Protocol latency* component is only part of the user session category. There are also common components, like *CPU* or *RAM*.

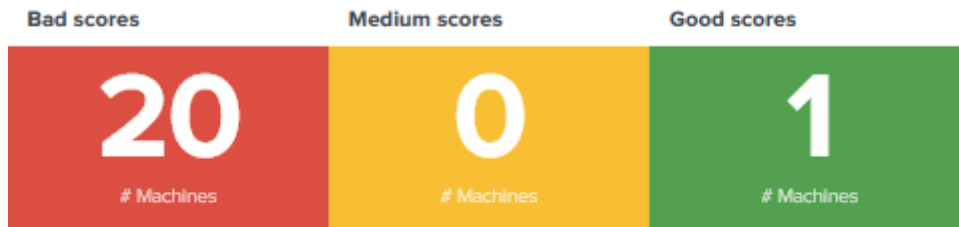
The categories allow to see issues in an environment and the components unveil the cause or causes. In the screenshot above, the low machine score is caused by a lot of stop errors.



In that case, checking the *Stop Errors (Blue Screen & Power Loss)* dashboard in the *Machine* menu shows the problematic machines.

## Analyzing Individual Machines, User Sessions, and Applications

### Machine analysis

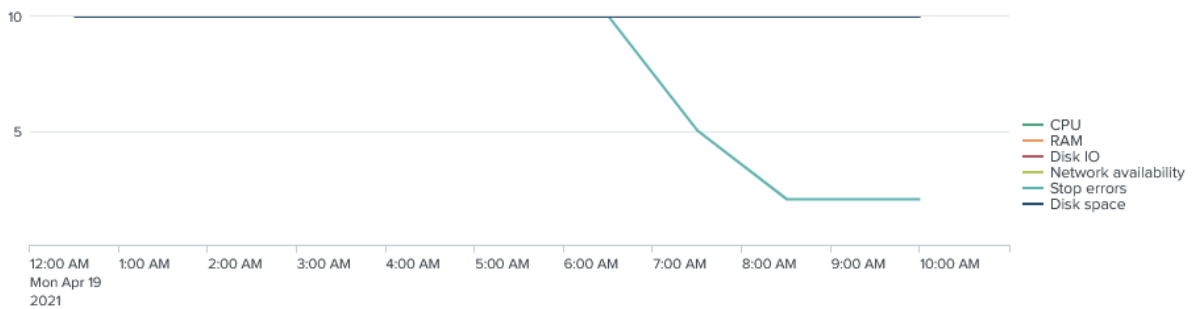


Filter:  Bad  Medium  Good

| Machine ↕ | Lowest ↕ | Daily average ↕ |
|-----------|----------|-----------------|
| demo1     | 2.0      | 2.0             |
| demo10    | 2.0      | 2.0             |
| demo11    | 2.0      | 2.0             |
| demo12    | 2.0      | 2.0             |
| demo13    | 2.0      | 2.0             |
| demo14    | 2.0      | 2.0             |
| demo15    | 2.0      | 2.0             |
| demo16    | 2.0      | 2.0             |
| demo17    | 2.0      | 2.0             |
| demo18    | 2.0      | 2.0             |
| demo19    | 2.0      | 2.0             |
| demo2     | 2.0      | 2.0             |
| demo20    | 2.0      | 2.0             |
| demo3     | 2.0      | 2.0             |
| demo4     | 2.0      | 2.0             |

The charts below are showing scores for individual machines, user sessions, and applications for today. Items with bad (red) or medium (yellow) scores may need attention the most. Click on an item in the table to get a drilldown.

Component scores for machine: "demo19"



Analyse "demo19"

A new chart opens showing the components over time for that item. That allows to see when the issue or the issues started. To analyze the item in detail, click on the **analyse button**, which redirects to a new page.

### More Details



Scores might be not enough to get an overview. One may want to see real numbers, for example login times, to get a better understanding of the performance.

Click on the plus sign next to the *More details* title to reveal charts with more details. Click an item of interest to get a drilldown.

### Score Calculation

Component scores are evaluated every full and half hour for the last 30 minutes. Calculations are done for a span of three minutes, resulting in 10 sections (30 minutes/3 minutes = 10). If a section is above a threshold, a threshold counter is incremented.

Each score has two thresholds. One for low severity, one for high severity. Each threshold has a weight.

A score is calculated as follows:  $10 - (\text{Low severity threshold counter} \times \text{low severity threshold weight} + \text{high severity threshold counter} \times \text{high severity threshold weight})$

Example 1: three sections above the low severity threshold as well as a weight of 0.5. The score would be:  $10 - (3 \times 0.5) = 8.5$

Example 2: three sections above the low severity threshold (weight = 0.5) and two sections above the high severity threshold (weight = 1). The score would be:  $10 - (3 \times 0.5 + 2 \times 1) = 6.5$

Note the following: the higher the weight, the lower the score.

Below is a list of default thresholds and weights. To modify the defaults, see [Modifying the Score Calculation](#).

**Machine**

| Threshold                            | Setting                                               | Default value | Unit  | Default weight |
|--------------------------------------|-------------------------------------------------------|---------------|-------|----------------|
| CPU usage. Low severity.             | ThresholdMachineCPUPercentLowerBound                  | 80            | %     | 0.5            |
| CPU usage. High severity.            | ThresholdMachineCPUPercentHigherBound                 | 90            | %     | 1              |
| RAM usage. Low severity.             | ThresholdMachineRAMPercentLowerBound                  | 80            | %     | 0.5            |
| RAM usage. High severity.            | ThresholdMachineRAMPercentHigherBound                 | 90            | %     | 1              |
| Disk IO usage. Low severity.         | ThresholdMachineIOPercentLowerBound                   | 80            | %     | 0.5            |
| Disk IO usage. High severity.        | ThresholdMachineIOPercentHigherBound                  | 90            | %     | 1              |
| Stop errors. Low severity.           | ThresholdStopErrorCountLowerBound                     | 1             | Count | 0.7            |
| Stop errors. High severity.          | ThresholdStopErrorCountHigherBound                    | 2             | Count | 1              |
| Disk usage. Low severity.            | ThresholdMachineDiskUsagePercentLowerBound            | 80            | %     | 0.2            |
| Disk usage. High severity.           | ThresholdMachineDiskUsagePercentHigherBound           | 90            | %     | 0.5            |
| Network availability. Low severity.  | ThresholdMachineNetworkAvailabilityPercentLowerBound  | 95            | %     | 0.5            |
| Network availability. High severity. | ThresholdMachineNetworkAvailabilityPercentHigherBound | 90            | %     | 0.2            |

*Note: higher is better*

*Note: higher is better*



**User session**

| Threshold                        | Setting                                 | Default value | Unit | Default weight |
|----------------------------------|-----------------------------------------|---------------|------|----------------|
| CPU usage. Low severity.         | ThresholdSessionCPUPercentLowerBound    | 30            | %    | 0.5            |
| CPU usage. High severity.        | ThresholdSessionCPUPercentHigherBound   | 90            | %    | 1              |
| RAM usage. Low severity.         | ThresholdSessionRAMPercentLowerBound    | 30            | %    | 0.5            |
| RAM usage. High severity.        | ThresholdSessionRAMPercentHigherBound   | 90            | %    | 1              |
| Disk IO latency. Low severity.   | ThresholdIOLatencyLowerBound            | 20            | ms   | 0.5            |
| Disk IO latency. High severity.  | ThresholdIOLatencyHigherBound           | 30            | ms   | 0.7            |
| Logon duration. Low severity.    | ThresholdLogonDurationLowerBound        | 30            | s    | 0.2            |
| Logon duration. High severity.   | ThresholdLogonDurationHigherBound       | 60            | s    | 0.4            |
| Protocol latency. Low severity.  | ThresholdSessionRpcLatencyMsLowerBound  | 100           | ms   | 0.2            |
| Protocol latency. High severity. | ThresholdSessionRpcLatencyMsHigherBound | 200           | ms   | 0.5            |

**Application**

| Threshold                 | Setting                           | Default value | Unit | Default weight |
|---------------------------|-----------------------------------|---------------|------|----------------|
| CPU usage. Low severity.  | ThresholdAppCPUPercentLowerBound  | 30            | %    | 0.5            |
| CPU usage. High severity. | ThresholdAppCPUPercentHigherBound | 90            | %    | 1              |
| RAM usage. Low severity.  | ThresholdAppRAMMBLowerBound       | 1024          | MB   | 0.1            |
| RAM usage. High severity. | ThresholdAppRAMMBHigherBound      | 2048          | MB   | 0.3            |

| Threshold                                                             | Setting                                           | Default value | Unit  | Default weight |
|-----------------------------------------------------------------------|---------------------------------------------------|---------------|-------|----------------|
| Disk IO. Low severity.                                                | ThresholdAppIOCountLowerBound                     | 200           | Count | 0.1            |
| Disk IO. High severity.                                               | ThresholdAppIOCountHigherBound                    | 400           | Count | 0.3            |
| Network availability. Low severity.<br><i>Note: higher is better</i>  | ThresholdAppNetworkAvailabilityPercentLowerBound  | 95            | %     | 0.5            |
| Network availability. High severity.<br><i>Note: higher is better</i> | ThresholdAppNetworkAvailabilityPercentHigherBound | 90            | %     | 0.2            |
| Network latency. Low severity.                                        | ThresholdAppSendLatencyMsLowerBound               | 100           | ms    | 0.2            |
| Network latency. High severity.                                       | ThresholdAppSendLatencyMsHigherBound              | 300           | ms    | 0.5            |
| Application UI delay. Low severity.                                   | ThresholdAppUIDelaySLowerBound                    | 5             | s     | 0.2            |
| Application UI delay. High severity.                                  | ThresholdAppUIDelaySHigherBound                   | 15            | s     | 0.5            |
| Application errors. Low severity.                                     | ThresholdApplicationErrorCountLowerBound          | 1             | Count | 0.5            |
| Application errors. High severity.                                    | ThresholdApplicationErrorCountHigherBound         | 2             | Count | 1              |

## Modifying the Score Calculation

The scores' default calculations are based on experiences in the field, but may not be applicable to your environment. Hence the calculations may be changed.

## Before Modifying

Before making changes, note the following:

- The lowest weight possible is 0
- The highest weight possible is 1
- The sum of all weights doesn't need to be 1. Each component is calculated separately.
- All components together form a total machine/user session/application score. The total score is always equal to the lowest component score.

## Modifying

To modify the score calculation, change the following three input lookup files in `$SPLUNK_HOME/etc/apps/uberAgent/lookups`. See Score Calculation for calculations and settings.

- **Machine:** `score_machine_configuration.csv`
- **User session:** `score_session_configuration.csv`
- **Application:** `score_application_configuration.csv`

## After Modifying

- Distribute the changed input lookup files to all search heads
- It is best to delete all previous scores as they cannot be compared to the new ones. See Deleting Scores for instructions.

New versions of uberAgent may introduce new scores or changes to calculations for existing scores, hence your score modifications will be overridden when updating uberAgent.

## Score Storage

Scores are stored in the Splunk index `score_uberagent_uxm`. The scores for the current date get aggregated at midnight (average per day) and then stored in the index as well.

If you want to delete the scores, see Deleting Scores.

## Deleting Scores

Scores are stored in the Splunk index `score_uberagent_uxm` and can be deleted via the CLI.

```
splunk clean eventdata -index score_uberagent_uxm
```

## Troubleshooting

If the Experience Score dashboard stays empty, try the following troubleshooting steps.

1. Scores are stored in an additional Splunk index `score_uberagent_uxm` since version 6.1. Check whether the index exists.
2. Scores are calculated through saved searches running on Splunk search heads. In a distributed Splunk environment, configure the [search heads to forward data to the indexer layer](#).

## Per-Application Network Monitoring

July 9, 2024

*This feature is supported on: Windows, macOS*

### What Is Per-Application Network Monitoring

uberAgent network monitoring keeps track of all incoming and outgoing network connections. uberAgent associates every network connection with the application handling it and determines metrics like **latency**, **packet loss**, **data volume**, and more. uberAgent network monitoring also records **failed connections** that may have been blocked by firewalls, for example.

uberAgent per-application network monitoring does not inspect packets and does not break TLS or other types of encryption.

### Use Cases for Per-Application Network Monitoring

By providing insights into network activity per application, uberAgent enables the following use cases:

- Network **availability** scoring
- Network **quality** monitoring
- Identification of network **issues** (jitter, packet loss, blocked ports)
- Mapping of network **targets** (who talks to whom)
- **Data volume** analytics (how much traffic is going where)

### Which Data is Collected by Per-Application Network Monitoring

The data collected as part of uberAgent per-application network monitoring is sent to the backend via the sourcetypes listed in the [network metrics documentation](#).

## **Name Resolution (IP Address to DNS Name)**

*Name resolution is supported on: Windows*

Network packets contain IP addresses, but not DNS names. In order to be able to associate each network target IP address with the corresponding DNS name, uberAgent also monitors DNS queries. By enriching network monitoring data with DNS query data, uberAgent ensures that each network event has the target's IP address as well as its DNS name.

Please note that uberAgent does not perform reverse DNS lookups, nor does it send its own DNS queries over the wire. uberAgent only generates network traffic to send the collected data from the endpoint to the backend servers.

## **Protocol Notes**

### **IPv6**

IPv6 is fully supported by uberAgent per-application network monitoring.

### **UDP**

UDP traffic is fully supported by uberAgent per-application network monitoring. However, due to the protocol's connectionless nature, latency cannot be determined.

### **TCP**

TCP traffic is fully supported by uberAgent per-application network monitoring. Since TCP is a connection-based protocol, latency, jitter, and packet loss can be determined.

Please note that latency detection is limited to send operations because otherwise a cooperating agent at the receiving side would be required.

### **QUIC**

QUIC traffic is treated as UDP by uberAgent per-application network monitoring.

### **ICMP**

ICMP traffic is ignored by uberAgent per-application network monitoring.

## Configuration

### Enabling or Disabling Per-Application Network Monitoring

uberAgent per-application network monitoring is enabled or disabled via the `NetworkTargetPerformancePr` timer metric in the [configuration](#). In the default configuration, network monitoring is enabled.

### Configuration Options for Per-Application Network Monitoring

Certain aspects of per-application network monitoring can be configured via the stanza [`NetworkTargetPerformanceProcess_Config`].

**Key** *This setting is supported on: Windows, macOS*

Internally, uberAgent records network activity by process instance. However, that level of detail is rarely required. In most cases, it is sufficient to visualize network activity per process name. This is an optimization that reduces the event count in the backend and the data volume. Optionally, the agent can be configured to record network activity by process ID for full granularity by switching to grouping per ID instead of per name.

```
1 Setting name: Key
2 Description: What to group by: process name or ID
3 Valid values: name | id
4 Default: name
5 Required: no
```

**IgnoreLowActivity** *This setting is supported on: Windows, macOS*

This is another setting targeted at reducing the event count and the data volume. By default, a threshold is applied below which per-application network activity is dropped (not sent to the backend).

```
1 Setting name: IgnoreLowActivity
2 Description: Whether to ignore processes with very low activity during
 a collection interval
3 Valid values: true | false
4 Default: true
5 Required: no
```

**NetworkDriverEnabled** *This setting is supported on: Windows*

Starting with uberAgent 6.0 (Windows), uberAgent monitors network activity with a kernel driver. This configuration option can be used to switch back to the older network data collection source ETW. ETW network monitoring has several limitations. Most notably, latency cannot be determined accurately.

```
1 Setting name: NetworkDriverEnabled
2 Description: Enables processing all network metrics by a driver instead
 of ETW.
3 Valid values: true | false
4 Default: true
5 Required: no
```

**NetworkDriverLegacyAPI** *This setting is supported on: Windows*

This setting is intended for internal use by vast limits. Only enable it if instructed by support.

```
1 Setting name: NetworkDriverLegacyAPI
2 Description: Use legacy WFP API to process packet streams in kernel
 mode.
3 Valid values: true | false
4 Default: false
5 Required: no
```

**TestCompareNetworkDriverAndETW** *This setting is supported on: Windows*

This setting is intended for internal use by vast limits. Only enable it if instructed by support.

```
1 Setting name: TestCompareNetworkDriverAndETW
2 Description: Collect network metrics using Windows ETW interfaces and
 the uberAgent network driver.
3 The ProcUser field of the metric
 NetworkTargetPerformanceProcess is extended by a suffix
 ETW or DRV to differentiate the type of network event.
4 Because of that, the network events are sent two times to
 the configured backend.
5 Use this feature to test unusual behavior in test
 environments. This is not intended to be used in a
 production environment.
6 Valid values: true | false
7 Default: false
8 Required: no
```

## Web App Monitoring

July 9, 2024

## What Is Web App Monitoring

uberAgent web app monitoring records page loads and XMLHttpRequests. For every such event, uberAgent collects the duration, the user, and the HTTP status code (plus some additional information). Web app monitoring works on every website and in all major browsers.

In the default configuration, uberAgent does not send full URLs to the backend. Instead, events are summarized per webserver (the host displayed in the browser's address bar). **Full URL monitoring** can optionally be enabled for specific domains or sites of interest.

## Use Cases for Web App Monitoring

By providing insights into browser and website usage, uberAgent web app monitoring enables the following use cases:

- Measuring web **page load performance**
- Calculating **web app usage**
- Collecting an **inventory of web apps**
- Tracking the **user journey** on a website

## Which Data is Collected by Web App Monitoring

The data collected as part of uberAgent web app monitoring is sent to the backend via the sourcetypes listed in the [browser metrics documentation](#).

Additionally, some fields in the `SessionDetail` sourcetype ([docs](#)) are populated through web app metrics.

## Requirements & Installation

Web App monitoring requires the [uberAgent browser extensions](#) to be installed in the end user's web browser. Please see the [installation instructions](#) for details on how to install the browser extensions.

## Enabling or Disabling Web App Monitoring

uberAgent web app monitoring is enabled or disabled via the `BrowserPerformance*` timer metrics in the [configuration](#). In the default configuration, web app monitoring is enabled for all supported browsers.



## Full URL Monitoring

### What Is Full URL Monitoring

Full URL monitoring optionally includes additional URL components in the following browser web app events or fields:

- the sourcetype `uberAgent:Application:BrowserWebRequests2` ([docs](#))
- the field `SessionFgBrowserActiveTabHost` of the sourcetype `uberAgent:Session:SessionDetail` ([docs](#))

**By default, full URL monitoring is disabled.** The path and query components are stripped from URLs sent to the backend, i.e., uberAgent only records the scheme (e.g., `https`), the host (e.g., `www.domain.com`) and the port (unless it's a standard port, e.g., 443 for https).

Example of the default behavior:

- Full URL in the browser: `https://splunk1.domain.com:8000/en-US/app/uberAgent/session_user_detail?earliest=-1h&latest=now`
- Shortened URL in uberAgent event: `https://splunk1.domain.com:8000`

### Configuring Full URL Monitoring

The default level of URL component detail can be changed by adding items in the `[BrowserWebAppURL_ComponentDetail]` stanza of the [configuration](#).

Please note that URL **allowlists and denylists** (`[BrowserWebAppURL_Filter]` stanza) have precedence over `[BrowserWebAppURL_ComponentDetail]`. In other words, the level of detail configuration only applies to URLs that are not filtered by a deny or allow list.

**BrowserWebAppURL\_ComponentDetail** Format of entries in the `[BrowserWebAppURL_ComponentDetail]` stanza:

```
1 URL_REGEX = COMPONENT_DETAIL_SPEC
2 or:
3 URL_REGEX = COMPONENT_DETAIL_SPEC_TAB;COMPONENT_DETAIL_SPEC_REQUEST
```

Note: see the [definition of URL\\_REGEX](#).

Tab URLs are matched against the regular expressions (`URL_REGEX`) of the items in the `[BrowserWebAppURL_ComponentDetail]` stanza. For matching URLs, `COMPONENT_DETAIL_SPEC` specifies which level of detail is recorded of the tab and request URLs.

Note:

- **Tab URLs** are URLs in the browser's address bar
- **Request URLs** are URLs the browser communicates with

Optionally, the detail level of the request URL can be set independently of the detail level of the tab URL by using the second format shown above.

Multiple URL component detail specs can be specified in a single `[BrowserWebAppURL_ComponentDetail]` stanza. Matching is performed in the order in which items are listed. The first matching item wins.

**COMPONENT\_DETAIL\_SPEC** Format of the URL component detail specification (`COMPONENT_DETAIL_SPEC`):

```
host[:path[(DEPTH)]][:query[(PARAMS)]]
```

with:

- **DEPTH:** the number of path elements to include. Without `DEPTH`, the entire path is included.
- **PARAMS:** comma-separated list of regular expressions specifying query parameters to include. Without `PARAMS`, all query parameters are included. Details:
  - Query parameters to be included are specified as regular expressions.
  - Matching is case-sensitive.

### Examples: Same Level of Detail for Tab URL and Request URL

The following examples show the effect of different configurations in a scenario where the tab URL and the request URL are identical:

- Tab URL: `https://splunk1.domain.com:8000/en-US/app/uberAgent/session_user_detail?earliest=-1h&latest=now`
- Request URL: `https://splunk1.domain.com:8000/en-US/app/uberAgent/session_user_detail?earliest=-1h&latest=now`

**Host and Path** Capture URLs on `splunk1.domain.com` including the path, but excluding the query:

```
.*\.?splunk1\.domain\.com/.*$ = host:path
```

Result:

```
https://splunk1.domain.com:8000/en-US/app/uberAgent/session_user_detail
```

**Host and 2 Path Elements** Capture URLs on `splunk1.domain.com` including the path, but only the first two elements:

```
.*\.?splunk1\.domain\.com/.*$ = host:path(2)
```

Result:

```
https://splunk1.domain.com:8000/en-US/app
```

**Host, Path, and Query** Capture URLs on `splunk1.domain.com` including the path and all query parameters:

```
.*\.?splunk1\.domain\.com/.*$ = host:path:query
```

Result:

```
https://splunk1.domain.com:8000/en-US/app/uberAgent/session_user_detail?earliest=-1h&latest=now
```

**Host, 1 Path Element, and 1 Query Parameter** Capture URLs on `splunk1.domain.com` including the first path element and the query parameter `earliest`:

```
.*\.?splunk1\.domain\.com/.*$ = host:path(1):query(earliest)
```

Result:

```
https://splunk1.domain.com:8000/en-US?earliest=-1h
```

**Host, 1 Path Element, and 1 Query Parameter Regex** Capture URLs on `splunk1.domain.com` including the first path element and all query parameters that match the regular expression `.+est`:

```
.*\.?splunk1\.domain\.com/.*$ = host:path(1):query(.+est)
```

Result:

```
https://splunk1.domain.com:8000/en-US?earliest=-1h&latest=now
```

### Examples: Different Level of Detail for Tab URL and Request URL

The following examples show the effect of different configurations in a scenario where the tab URL and the request URL are different:

- Tab URL: [https://splunk1.domain.com:8000/en-US/app/uberAgent/session\\_user\\_detail?earliest=-1h&latest=now](https://splunk1.domain.com:8000/en-US/app/uberAgent/session_user_detail?earliest=-1h&latest=now)
- Request URL: <https://www.example.org/images/uberAgent>

**Tab URL: Host Only, Request URL: Host and Path** Capture only the host of the tab URL, but the host and the path of the request URL:

```
.*\.?splunk1\.domain\.com/.*$ = host;host:path
```

Result:

```
1 Tab URL: https://splunk1.domain.com:8000/
2 Request URL: https://www.example.org/images/uberAgent
```

**Tab URL: Host and Path, Request URL: Host Only** Capture the host and the path of the tab URL, but only the host of the request URL:

```
.*\.?splunk1\.domain\.com/.*$ = host:path;host
```

Result:

```
1 Tab URL: https://splunk1.domain.com:8000/en-US/app/uberAgent/
 session_user_detail
2 Request URL: https://www.example.org
```

## Automatic Application Identification

July 25, 2024

### Applications

While it is pretty clear where machine and process data come from, this is not so obvious with applications. In fact, there is a tiny little bit of magic involved here - the operating system does not have a concept of applications, it only knows about processes. The fact that `receiver.exe`, `concentr.exe` and `wfcrun32.exe` form a logical application entity called `Citrix Receiver` is totally irrelevant to the OS. For that reason, other monitoring products do not bother with applications.

uberAgent is different. It automatically groups related processes to applications, because humans think in applications, not in processes - and uberAgent is designed for humans. When troubleshooting performance problems it is not enough to know that, say, `SelfService.exe` has a problem. You need to know that `Citrix Receiver` generates all those IOs. uberAgent shows you exactly that and makes it easy to analyze the impact your applications have on overall system performance.

## How It Works (Windows)

Automatic application identification works for classic Win32 apps just as well as it does for Java applications, Universal Windows Platform (UWP) apps, and Windows services.

### Win32

uberAgent determines the application names for all executables from properties of the MSI package the executable was installed from. Where that is not possible, uberAgent uses the information embedded in the executable.

| App name ↕      | Process name(s) ↕                             |
|-----------------|-----------------------------------------------|
| Adobe Reader XI | AcroRd32.exe<br>AdobeARM.exe<br>reader_sl.exe |

### Java

uberAgent extracts the class name or filename of a Java command line. This works for Java Web Start processes, too.

| Application ↕ | Process name(s) ↕ |
|---------------|-------------------|
| freemind      | javaw.exe         |

### UWP

uberAgent retrieves the information from the UWP package.

| App name ↕                | Process name(s) ↕         |
|---------------------------|---------------------------|
| 4DF9E0F8.Netflix          | WWAHost.exe               |
| Microsoft.BingWeather     | Microsoft.Msn.Weather.exe |
| Microsoft.People          | PeopleApp.exe             |
| Microsoft.Windows.Cortana | SearchUI.exe              |
| Microsoft.Windows.Photos  | Microsoft.Photos.exe      |

## Windows services

Starting with Windows 10 1703 each service gets a dedicated `svchost.exe` instance if certain minimum RAM conditions are met. uberAgent extracts the (localized) display name for services that run in a dedicated `svchost.exe` instance.

| App name ↕                      | Process name(s) ▼ |
|---------------------------------|-------------------|
| Network Connections             | svchost.exe       |
| Network List Service            | svchost.exe       |
| Network Location Awareness      | svchost.exe       |
| Network Store Interface Service | svchost.exe       |
| Network Virtualization Service  | svchost.exe       |
| Phone Service                   | svchost.exe       |
| Plug and Play                   | svchost.exe       |

Requirements:

- Windows 10 1703 or higher
- uberAgent 5.2 or higher

## How It Works (macOS)

### Bundles

uberAgent determines application names for executables that are part of a bundle folder structure by retrieving either bundle name, bundle identifier, or bundle executable name from the bundle's `Info.plist` file. Executables located in nested app bundles are identified as their top-level host app bundle. Executables located in nested framework bundles are identified as their nested framework bundle, except for XPC Services which are always identified as the application that initiated their launch.

| App name ↕ | Process name(s) ↕                                                                                                                                                        |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Safari     | CacheDeleteExtension<br>ImageIOXPCService<br>MTLCompilerService<br>Safari<br>com.apple.Safari.SearchHelper<br>com.apple.WebKit.Networking<br>com.apple.WebKit.WebContent |

## Executables

uberAgent extracts application names from executables that are not part of a bundle folder structure by retrieving either bundle name, bundle identifier, or bundle executable name from the embedded binary info plist. If an executable can not be identified this way but is located in a system directory it is mapped to app name `macOS`.

## Privileged Helper Tools

uberAgent determines application names for executables located in `/Library/PrivilegedHelperTools` by inspecting their respective host app bundles as described above.

| App name ↕              | Process name(s) ↕                                                                     | Process commandline ↕                                                                                                                                                                                                                                                                                                                                |
|-------------------------|---------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Microsoft<br>AutoUpdate | Microsoft AutoUpdate<br>Microsoft Update Assistant<br>com.microsoft.autoupdate.helper | "/Library/Application Support/Microsoft/MAU2.0/Microsoft AutoUpdate.app/Contents/MacOS/Microsoft AutoUpdate"<br>"/Library/Application Support/Microsoft/MAU2.0/Microsoft AutoUpdate.app/Contents/MacOS/Microsoft Update Assistant.app/Contents/MacOS/Microsoft Update Assistant"<br>"/Library/PrivilegedHelperTools/com.microsoft.autoupdate.helper" |

## Configuration

### Adding Your Own Mappings

uberAgent's sophisticated method to map processes to applications works nearly every time for every application. When it does not, you can adjust it in the [configuration](#) section [`ProcessToApplicationMapping`]. Enter the full path to the process as a regular expression. Environment variables can also be used (enclosed in percent signs: `%ProgramFiles%`). Then specify the application name. Specifying only the file name without the full path works but is not recommended.

```

1 [ProcessToApplicationMapping]
2 # App name for C:\Dir\my.exe is "MyApp"
3 ^C:\\DIR\\my\\.exe$ = MyApp
4
5 # App name for all executables in "C:\Program Files\Windows Defender"
 is "Windows Defender"
6 ^%ProgramFiles%\\Windows Defender\\.+\\.exe$ = Windows Defender

```

### Overriding Default Mappings

This configuration option also allows you to override uberAgent's default mapping. Let us take Microsoft Office as an example. uberAgent, by default, groups all Office processes like `WINWORD.EXE` and `EXCEL.EXE` into the application `Microsoft Office`.

Data table

Function:

average

| App name              | Process name(s)          | Total |
|-----------------------|--------------------------|-------|
| Microsoft Office 2016 | EXCEL.EXE<br>WINWORD.EXE |       |

By changing uberAgent's `[ProcessToApplicationMapping]` configuration settings as follows, you get individual applications per process.

```

1 [ProcessToApplicationMapping]
2 ^%ProgramFiles(x86)%\Microsoft Office\root\Office16\EXCEL*.EXE$ =
 Microsoft Excel 2016
3 ^%ProgramFiles(x86)%\Microsoft Office\root\Office16\WINWORD*.EXE$ =
 Microsoft Word 2016

```

Data table

Function:

average

| App name             | Process name(s) | Total |
|----------------------|-----------------|-------|
| Microsoft Excel 2016 | EXCEL.EXE       |       |
| Microsoft Word 2016  | WINWORD.EXE     |       |

### Ignoring Certain Processes

If you want uberAgent to ignore certain processes during application lookup, you can configure this with the option `[ApplicationMappingIgnoredProcesses]`.

## Citrix NetScaler (ADC) Monitoring

August 14, 2024



## What is Citrix NetScaler (ADC) Monitoring

With Citrix NetScaler (ADC) monitoring, uberAgent collects appliance & gateway performance, utilization, and inventory data from Citrix NetScaler Application Delivery Controllers ([metrics docs](#)).

The uberAgent endpoint agent needs to be installed on a machine from where it can reach the physical or virtual Citrix NetScaler (ADC) appliance(s). On Citrix Delivery Controllers (DDCs), the collection of NetScaler (ADC) metrics is enabled by default. Of course, NetScaler (ADC) metrics can also be retrieved from any other machine instead.

## Enabling or Disabling Citrix NetScaler (ADC) Monitoring

Citrix NetScaler (ADC) monitoring is activated by default only on Citrix Delivery Controllers, as explained above. You can modify this behavior through the configuration setting [`CitrixADC_Config`] in uberAgent's [configuration](#).

To completely disable collecting Citrix ADC metrics, disable the following metrics in the [configuration](#):

- CitrixADCPerformance
- CitrixADCvServer
- CitrixADCGateways
- CitrixADCInventory

## Installation and Configuration

If you have uberAgent already installed on one or more DDCs for Citrix site monitoring, it makes sense to also collect Citrix NetScaler (ADC) metrics there. Make sure that the DDCs can communicate with the Citrix NetScaler (ADC) management interface (NSIP) either through port 80 or, if you enabled [Secure Access Only](#) for the NSIP, through port 443.

While DDCs may be the ideal place to capture Citrix NetScaler (ADC) data for most customers, that may not be the case for everybody. As explained above, you can overwrite the setting `CollectADCInformation` in the stanza [`CitrixADC_Config`] to collect Citrix NetScaler (ADC) metrics from any installed uberAgent endpoint. Make sure that this setting is only distributed to the machines that are intended for this purpose. If you distribute it to all machines where uberAgent is installed, every endpoint communicates with the Citrix NetScaler (ADC) appliance(s), which could overload the appliance(s) and generate unnecessary data.

`CollectADCInformation=MachineList` in combination with a set of machines configured in `CollectADCInformationMachines`, defines on which machines the collection of ADC metrics will be performed.

## Citrix NetScaler (ADC) Configuration

Besides network access, uberAgent also needs credentials to be able to login into the Citrix ADC appliances. It only needs to read information; hence using a user with the command policy *read-only* bound is the recommended option. Users with more privileges are also supported, but not recommended from a security perspective.

Create a user with the command policy *read-only* bound from CLI:

```
1 add system user nsread Password -externalAuth DISABLED -timeout 900 -
 maxsession 20
2 bind system user nsread read-only 100
```

## uberAgent Configuration

This section explains the configuration via uberAgent's configuration file. The configuration via GPO works accordingly.

Use the stanza `[CitrixADC_Config]` to specify how uberAgent should connect to your appliance(s). If multiple `[CitrixADC_Config]` stanzas are specified, the configured metrics are determined for each of them. Use one `[CitrixADC_Config]` stanza per Citrix NetScaler (ADC) pair.

Following are some examples of valid Citrix ADC configurations. More information on the parameters is available in the configuration file itself. Note that passwords can be [encrypted](#).

**Example 1:** One Citrix NetScaler (ADC) appliance manageable through HTTP (port 80). Data collection happens on DDCs only

```
1 [CitrixADC_Config]
2 Server = 10.1.1.21
3 Username = nsread
4 Password = Password
5 Https = false
6 CollectADCInformation = DDCOnly
```

**Example 2:** A Citrix ADC high-availability pair manageable through HTTPS (port 443). Data collection happens not on a DDC.

- If HTTPS is used, the entries in the setting `Server` must match those in the certificate bound to the NSIP.
- uberAgent collects performance information for the primary appliance only. So for best collection performance, list the primary appliance first.

```
1 [CitrixADC_Config]
2 Server = CitrixADC1.domain.local,CitrixADC2.domain.local
3 Username = nsread
```

```
4 Password = Password
5 Https = True
6 CollectADCInformation = True
```

**Example 3:** A Citrix ADC high-availability pair manageable through HTTPS (port 443). Data collection happens on a set of machines.

```
1 [CitrixADC_Config]
2 Server = CitrixADC1.domain.local,CitrixADC2.domain.local
3 Username = nsread
4 Password = Password
5 Https = True
6 CollectADCInformation = MachineList
7 CollectADCInformationMachines = DDC01, DDC02
```

## Deployment Considerations

uberAgent's NetScaler integration sequentially queries the configured NetScalers with PowerShell through the NITRO API. This implementation method has pros and cons.

This section describes if the uberAgent implementation is for you, or if you should go with [NetScaler's builtin Observability integrations](#).

### When to Use uberAgent's Netscaler Integration

uberAgent's NetScaler integration is easy to use, comes with beautiful Splunk dashboards out-of-the-box, and is tailored to the Citrix CVAD/DaaS administrator who focuses on the quality of user sessions.

The NITRO API offers plenty of information about NetScaler, but comes with limitations. For example, it does not offer insights into failed AAA logins. In addition, not all existing NITRO API fields are queried by uberAgent, but only the ones that you see in the Splunk dashboards. Additional fields can be requested via feature requests.

uberAgent queries NetScaler sequentially. Querying lots of NetScaler boxes from one uberAgent endpoint can lead to performance issues and requires distributing the load to multiple endpoints.

Use uberAgent's NetScaler integration, when you have only a few NetScaler to monitor and want to benefit from pre-built Splunk dashboards and easy configuration.

### When to Use NetScaler's Built-in Observability Integrations

NetScaler can send metrics and logs to various backends natively. This includes [Splunk](#) with [example dashboards](#).

NetScaler Console, the monitoring and configuration tool for NetScaler from Citrix, [can send data to Observability platforms like Splunk, too.](#)

Sending data off the NetScaler instead of querying it externally through an API is more efficient. Also, NetScaler can send, more or less, data for every NetScaler setting that you see in the UI or via the Shell. It can also send log files which include information on failed AAA logins.

While NetScaler can send a lot to Observability platforms, you have to define which settings you would like to see. Also, you have to create your own visualizations or change the example dashboards.

Use NetScaler's and NetScaler Console's built-in Observability integrations when you require monitoring more than a handful NetScaler, when you need management logs or more data that is not available through uberAgent and the NITRO API.

## System Requirements

Please see the [system requirements page](#) for details.

## Citrix Cloud Monitoring

July 29, 2024

**Disclaimer: Citrix Cloud monitoring makes use of the Citrix Virtual Apps and Desktops OData APIs. These APIs are currently in Tech Preview state!**

### What Is Citrix Cloud Monitoring

Citrix Cloud monitoring refers to uberAgent's capability to monitor the Citrix Virtual Apps and Desktops (CVAD) control plane in Citrix Cloud. This is an exciting feature for customers who do not host delivery controllers on-premises but leverage Citrix Cloud instead.

### Which Metrics Are Collected By Citrix Cloud Monitoring

Citrix Cloud monitoring collects a rich set of metrics about many aspects of a Citrix Cloud deployment (see the [metrics documentation](#) for details):

- Published **applications**
- **Desktops**
- Desktop groups
- Machines
- Machine Catalogs

## Enabling or Disabling Citrix Cloud Monitoring

Citrix Cloud monitoring is **disabled by default**. You can enable the data collection through the configuration setting `[CitrixCloud_Config]` in uberAgent's [configuration](#).

To completely disable Citrix Cloud monitoring, disable the following metrics in the [configuration](#):

- CitrixDCDesktopGroup
- CitrixDCCatalog
- CitrixDCMachine
- CitrixDCGeneralInformation
- CitrixDCApplication
- CitrixDCPublishedDesktops

## Installation and Configuration

To enable the Citrix Cloud data collection, please configure the stanza `[CitrixCloud_Config]` in uberAgent's configuration. Make sure that this setting is only distributed to the machines that are intended for this purpose. If you distribute it with `CollectCitrixCloudInformation=True` to all machines where uberAgent is installed, every endpoint communicates with the Citrix Cloud APIs, which could overload the APIs and generate unnecessary data.

`CollectCitrixCloudInformation=MachineList` in combination with a set of machines configured in `CollectCitrixCloudInformationMachines`, defines on which machines the collection of Citrix Cloud metrics will be performed.

## uberAgent Configuration

This section explains the configuration via uberAgent's configuration file. The configuration via GPO works accordingly.

Use the stanza `[CitrixCloud_Config]` to specify how uberAgent should connect to the Citrix Cloud infrastructure. If multiple `[CitrixCloud_Config]` stanzas are specified, the configured metrics are determined for each of them. Use one `[CitrixCloud_Config]` stanza per Citrix Cloud tenant. The API endpoint option must contain to full URL to the Citrix Cloud server (e.g., `https://api-eu.cloud.com`). The appendix `/monitordata` is optional.

Following are some examples of valid Citrix Cloud monitoring configurations. More information on the parameters is available in the configuration file itself.

**Example 1:** one Citrix Cloud tenant. Data collection happens on all uberAgent endpoints.

```
1 [CitrixCloud_Config]
2 API endpoint = https://api-eu.cloud.com
```

```
3 CustomerId = <CustomerId>
4 ClientId = <ClientId>
5 ClientSecret = <ClientSecret>
6 CollectCitrixCloudInformation=True
```

**Example 2:** one Citrix Cloud tenant. Data collection happens on specific endpoints only.

```
1 [CitrixCloud_Config]
2 API endpoint = https://api-eu.cloud.com
3 CustomerId = <CustomerId>
4 ClientId = <ClientId>
5 ClientSecret = <ClientSecret>
6 CollectCitrixCloudInformation=MachineList
7 CollectCitrixCloudInformationMachines = MachineA,MachineB
```

## Requirements

- Create a Citrix Cloud API client as described [here](#).
- The Citrix Virtual Apps and Desktops [Remote PowerShell SDK](#) must be installed on the endpoint.
- PowerShell script execution is required by the Remote PowerShell SDK. Set the execution policy (machine scope) accordingly, for example, [RemoteSigned](#).

**Note:** the Remote PowerShell SDK must **not** be installed on:

- Citrix Virtual Apps and Desktops **delivery controllers**
- Citrix **Cloud Connector** machines

Please see the [system requirements page](#) for details.

## Citrix Session Monitoring

July 25, 2024

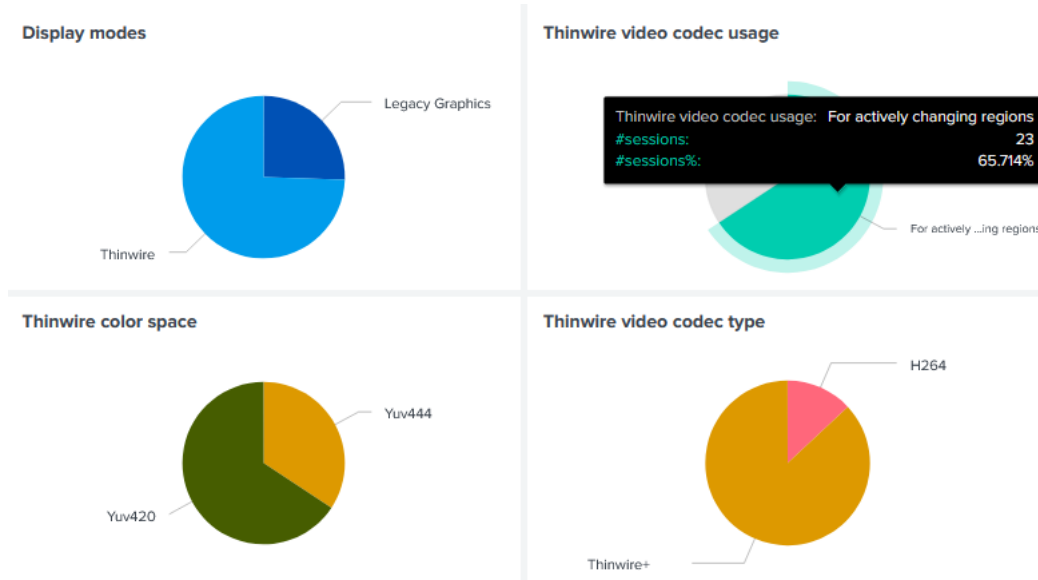
uberAgent provides unprecedented visibility into what's happening on the session level: bandwidth usage, protocol latency, Citrix policies, video encoding settings, and much more.

### Citrix Session Configuration Details

The session configuration dashboard lets you analyze almost any aspect of how users connect and what policies are being applied to their sessions. The dashboard pulls its data from live sessions, so it always reflects the current state. Historical values are available, too, of course.

### Video Codec, Display Mode, Color Space

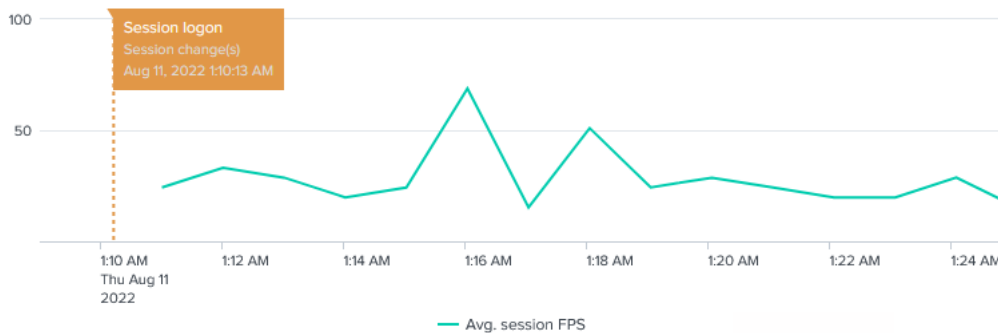
Many things need to be configured just right to achieve optimal visual quality in a remoting session. These include the video codec and color space, to pick just one set of essential session parameters. As you can see in the screenshot below, uberAgent shows you exactly which codecs and rendering algorithms are configured for your sessions:



### Frame Rate (FPS)

Another important metric that greatly influences rendering fidelity as experienced by end users is the frame rate, measured in frames per second. uberAgent continuously collects the frame rate for the entire duration of any session. This allows IT staff to proactively optimize the user experience without a single end-user having to call the help desk.

Session FPS over time



## Citrix Policies and Settings

The Citrix session configuration dashboard offers drilldown capabilities that allow you to inspect the policies and settings of every session individually. The following screenshot shows a small excerpt of what’s available:

| Citrix settings (last seen values) |                                  | Citrix policies (last seen values) |                                 |
|------------------------------------|----------------------------------|------------------------------------|---------------------------------|
| Setting ↕                          | Value ↕                          | Policy ↕                           | Value ↕                         |
| Audio channel actual priority      | RealTime                         | Audio channel priority             | RealTime                        |
| CDM channel actual priority        | Medium                           | Audio redirection                  | Allowed                         |
| Connected via                      | 10.1.1.104                       | Auto-create client printers        | Auto-create all client printers |
| Display mode                       | Thinwire                         | CDM channel priority               | Medium                          |
| EDT MTU                            | 1400                             | Client drive mapping               | Allowed                         |
| Mapped printers                    | Microsoft Print to PDF (from LOI | ICA listener port                  | 1494                            |
|                                    | OneNote for Windows 10 (from LOI | Microphone redirection             | Allowed                         |
|                                    | Microsoft Print to PDF (from LOI | Printer channel priority           | Low                             |
|                                    | OneNote for Windows 10 (from LOI | Printer redirection                | Allowed                         |
|                                    | Microsoft XPS Document Writer    | Read-only client drive access      | Prohibited                      |
| Mapped volumes                     | Local Disk (C: on LOGINLAUNCHER  | Session reliability connections    | Allowed                         |
| Printer channel actual priority    | Low                              |                                    |                                 |

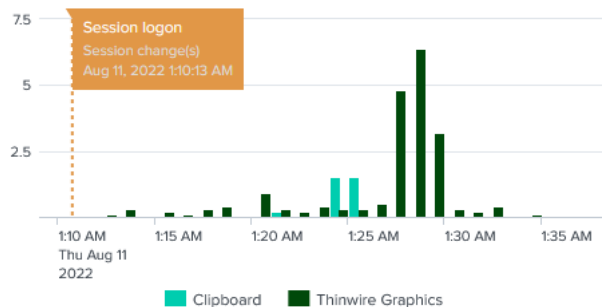
## Citrix Session Protocol Insights

The session protocol insights dashboard is focused on ICA/HDX remoting protocol analytics.

### Virtual Channel Bandwidth Usage

One of the dashboard’s highlights: it visualizes session bandwidth usage per virtual channel. This is crucial information for any Citrix admin, as it explains which kind of data is transferred in the encrypted Citrix HDX protocol. In the screenshot below, for example, the user seems to have copied a lot of data to or from the clipboard (virtual channel: [Clipboard](#)), followed by what may have been scrolling in a long document (virtual channel: [Thinwire Graphics](#)).

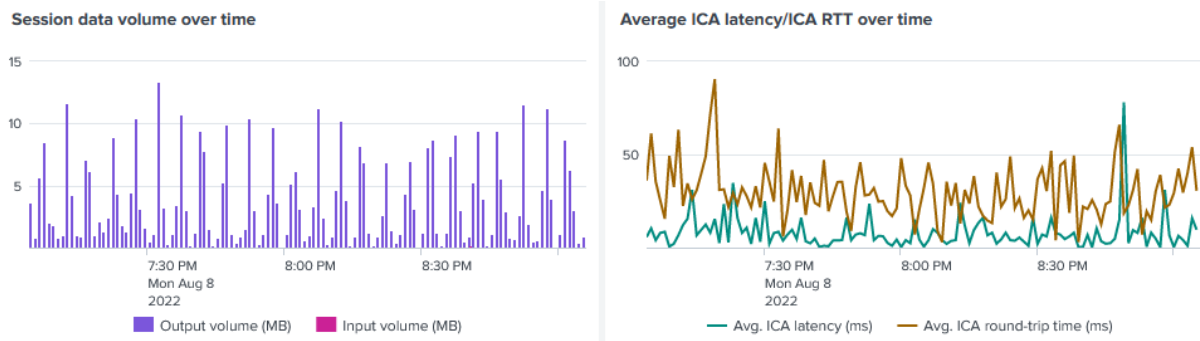
Virtual channel data volume (MB) over time





## ICA RTT

Another cool metric helps to get to the bottom of many networking issues: ICA round-trip time (RTT). A high round-trip time may be experienced by end users as screen lag. The session protocol insights dashboard visualizes ICA RTT along with ICA latency, which offers a lower-level view of network connectivity (think: an ICA/HDX version of ping). uberAgent also determines the total incoming and outgoing HDX data volume, of course:



## Configuration

Citrix session configuration details as well as policies and settings are configured through two metrics. The metrics are collected by default if uberAgent is running on a Citrix Virtual Apps and Desktops session host, but this behavior is customizable.

- `CitrixSessionVirtualChannelDetail`
- `CitrixSessionConfig`

## Requirements

- Citrix Virtual Apps and Desktops 7.6 LTSR and higher
- Citrix Cloud

Please see the [system requirements](#) page for supported product versions.

## Citrix Site Monitoring

July 9, 2024

## What is Citrix Virtual Apps and Desktops Site Monitoring

uberAgent detects if it is running on a Citrix Delivery Controller (DDC) or a Citrix Virtual Desktop Agent (VDA). On DDCs, **uberAgent automatically activates additional metrics** like machine registration status, license usage, and published application inventory.

## Which Metrics Are Collected By Citrix Site Monitoring

Citrix site monitoring collects a rich set of metrics about many aspects of Citrix CVAD sites (see the [metrics documentation](#) for details):

- Published **applications**
- Databases
- **Desktops**
- Desktop groups
- Hypervisors
- **Licenses**
- Machines
- Machine Catalogs

## Enabling or Disabling Site Monitoring

Citrix site monitoring is **enabled by default** but is only **activated on Citrix delivery controllers** as explained above. To disable Citrix site monitoring disable the following metrics in the [configuration](#):

- CitrixDCDesktopGroup
- CitrixDCCatalog
- CitrixDCMachine
- CitrixDCHypervisor
- CitrixDCGeneralInformation
- CitrixDCLicenseInformation
- CitrixDCApplication
- CitrixDCPublishedDesktops

## Installing & Configuring Citrix Site Monitoring

Install the uberAgent endpoint agent on at least one delivery controller per site. Installation on more than one controller is optional - it helps ensure uninterrupted data collection even when individual DDCs are unavailable.

## Required Permissions

uberAgent requires read-only administrator permissions for:

- each delivery controller's computer account
- the local SYSTEM account

## Permissions Script Template

The following script template can be used to grant the required permissions. Fill in the names of your domain and of your Citrix DDCs before running it in an elevated PowerShell console.

```
1 Add-PSSnapin Citrix.DelegatedAdmin.Admin.V1
2 New-AdminAdministrator -Sid S-1-5-18 -Enabled $true
3 Add-AdminRight -Role 0a05f0c6-0153-4852-a55a-989d6a95c0eb -
 Administrator S-1-5-18 -All
4 New-AdminAdministrator -Name
```

## Permissions Script Example

The following example script demonstrates how to grant the required permissions in an environment with two DDCs named `CTX-DDC1` and `CTX-DDC2` that are members of the `CONTOSO` domain. Note that you need to append a dollar sign (\$) to the computername.

```
1 Add-PSSnapin Citrix.DelegatedAdmin.Admin.V1
2 New-AdminAdministrator -Sid S-1-5-18 -Enabled $true
3 Add-AdminRight -Role 0a05f0c6-0153-4852-a55a-989d6a95c0eb -
 Administrator S-1-5-18 -All
4 New-AdminAdministrator -Name CONTOSO\CTX-DDC1$ -Enabled $true
5 Add-AdminRight -Role 0a05f0c6-0153-4852-a55a-989d6a95c0eb -
 Administrator CONTOSO\CTX-DDC1$ -All
6 New-AdminAdministrator -Name CONTOSO\CTX-DDC2$ -Enabled $true
7 Add-AdminRight -Role 0a05f0c6-0153-4852-a55a-989d6a95c0eb -
 Administrator CONTOSO\CTX-DDC2$ -All
```

## Sizing Guidelines

Sizing recommendations for delivery controllers with uberAgent:

- **1,000 machines:** minimal CPU usage, 30 MB RAM
- **25,000 machines:** 0.5 CPU cores, 500 MB RAM

## System Requirements

The following services need to be started on delivery controllers with uberAgent:

- Citrix Delegated Administration Service
- Citrix Monitor Service

Please see the [system requirements page](#) for supported product versions.

## Central License File Management

July 9, 2024

### Central License File Share

License file management is easy with uberAgent. All you have to do is set up a file share with read permissions for computer accounts, drop your uberAgent license file(s) there and configure the share path in uberAgent's configuration option `LicenseFilePath`. Endpoints periodically check `LicenseFilePath` for new licenses. If any are found that are not yet cached locally, the new license files are copied to the local license cache directory in `%ProgramData%\vast limits\uberAgent\License cache` (Windows) or in `/Library/Application Support/uberAgent/License Cache` (macOS) respectively.

### Storing uberAgent's License in Azure Files

uberAgent can also validate a license file stored in an Azure Files share. Our [knowledge base article](#) describes the necessary steps to set this up.

### Availability Requirements

There is **no need** for the configured license file path to be available all of the time. Endpoints always use the local license cache for license validation.

### Alternative: Local License Storage

Of course, there is no requirement to set up a central license file path. You can also distribute the license file to each endpoint. If the license file path is not specified uberAgent falls back to the installation directory (Windows) or to `/Library/Application Support/uberAgent` (macOS).

## Event Data Filtering

November 25, 2024

### What is Event Data Filtering

Event data filtering allows defining rules with conditions that are evaluated for every event before it is sent to the backend. This feature applies to all built-in metrics. With each matching rule, a pre-defined action is executed that controls whether the event is sent to the backend or not. Additionally, it allows clearing the contents of certain fields before the event is sent to the backend.

### Use Cases for Event Data Filtering

#### Data Volume Reduction

Depending on the requirements, one might only need a subset of the events generated by uberAgent for certain sourcetypes. Filtering out unnecessary data at the endpoint may reduce the data volume significantly (see the documentation for other [ways to reduce the data volume](#)).

**Example:** every time a `cmd.exe` process is started on Windows, an accompanying console host process is started too. These `conhost.exe` processes are rarely of interest and can be safely excluded.

```
1 [EventDataFilter]
2 # Exclude "conhost.exe" (typically started from the path: \\??\C:\
 WINDOWS\system32\conhost.exe)
3 Action = deny
4 Sourcetype = Process:ProcessStartup
5 Query = regex_match_path(ProcPath, r"^(\\\\?\\?\\)?%SystemRoot%\\System32
 \\conhost\\.exe$")
```

**Example:** compared to Windows, macOS runs significantly more concurrent processes. which can also lead to an increased data volume. One way to adjust this is to exclude the processes that belong to the operating system.

```
1 [EventDataFilter]
2 # Exclude processes belonging to the operating system
3 Action = deny
4 Sourcetype = Process:ProcessDetail
5 Sourcetype = Process:ProcessStartup
6 Sourcetype = Process:ProcessStop
7 Sourcetype = Process:ProcessStatistics
8 Sourcetype = Process:NetworkTargetPerformance
9 Query = AppId == "mcOS"
```

## Sensitive Data Removal

Some sourcetypes have fields with data that may be considered sensitive in nature, such as window titles. Event data filtering allows clearing such fields, on the endpoint, before the data is sent to the backend for indexing and searching.

**Example:** clear the contents of session detail window title metric.

```
1 [EventDataFilter]
2 # Clear the contents of window titles.
3 Action = clear
4 Sourcetype = Session:SessionDetail
5 Field = SessionFgWindowTitle
6 Query = true
```

The query above always evaluates to **true** and therefore the action **clear** is executed for this particular event and the field **SessionFgWindowTitle** is cleared to an empty value.

## Actions: allow, clear and deny

### allow

When an event matches a rule with the allow action, it is immediately sent to the backend. No further filtering rules are applied to the event.

### deny

When an event matches a rule with the deny action, it is immediately discarded and not sent to the backend. Like allow, no further rules are applied.

### clear

The clear action is used to overwrite the value of a specified field with an empty value. Filtering continues with subsequent rules after clear.

## Configuring Event Data Filtering

An event data filter is configured using the configuration file. The stanza `[EventDataFilter]` starts a new filter configuration, followed by multiple settings.

It's essential to note that filter rules are processed sequentially. Once a rule matches, the filtering process for that particular event stops. Therefore, the order of filters can be crucial for the desired outcome.

| Setting    | Description                                                                                                                                      | Valid Values                                                                                   |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Action     | Specifies the action to be taken if a query rule is matched.                                                                                     | <code>allow</code> , <code>deny</code> or <code>clear</code>                                   |
| Sourcetype | The category and name of the sourcetype.                                                                                                         | Please refer to the <a href="#">metrics documentation</a> for a list of available sourcetypes. |
| Query      | The query rule to filter using uAQL.                                                                                                             | Please refer to the <a href="#">uAQL documentation</a> .                                       |
| Field      | Optional setting to specify the field to be cleared if the current Action is <code>clear</code> . This setting can be configured multiple times. | This can be any field of the given metric.                                                     |

#### Example: Exclude DNS Monitoring Events Caused by Browsers

A browser can generate a significant number of DNS monitoring events that are rarely of interest. Such events can be easily ignored using the following event data filter.

```
1 [EventDataFilter]
2 # Deny any DNS event caused by browsers.
3 Action = deny
4 Sourcetype = Process:DnsEvent
5 Query = ProcName in ["chrome.exe", "iexplore.exe", "firefox.exe", "msedge.exe", "opera.exe"]
```

#### Example: Exclude Process Detail Metrics For Certain Processes

```
1 [EventDataFilter]
2 # Exclude processes whose name is exactly one of the given names.
3 Action = deny
4 Sourcetype = Process:ProcessDetail
5 Query = ProcName in ["cmd.exe", "conhost.exe", "csrss.exe", "lsm.exe", "smss.exe", "wininit.exe", "winlogon.exe"]
```

#### Example: Exclude Everything Except..

Consider a use case where one wants to exclude an entire metric, except for specific data in events. This is achievable by explicitly allowing certain processes but denying all others. The stanza ordering is important because filter processing stops after the first match.

```
1 [EventDataFilter]
2 # Allow network events caused by John Doe and Jane Doe.
3 Action = allow
4 Sourcetype = Process:NetworkTargetPerformance
5 Query = ProcUser in ["John Doe", "Jane Doe"]
6
7 [EventDataFilter]
8 # Deny any network event that was not allowed in a previous filter.
9 Action = deny
10 Sourcetype = Process:NetworkTargetPerformance
11 Query = true
```

## Per-Receiver Configuration

In addition to the fields of a sourcetype, certain built-in receiver fields may also be used. This allows creating event data filters that are active for certain receivers, only. Check the [documentation on routing to different backends](#) to learn more on the use case.

The available fields are `Receiver.Name` and `Receiver.Index`.

### Example: Clear Fields Per Receiver

For this example, we take a look at the Session Detail metric. Consider there are two receivers configured, one for most metrics and an extra receiver for sensitive content with restricted access.

```
1 [EventDataFilter]
2 # Clear the contents of window titles for any receiver except "
 uberagent_sensitive"
3 Action = clear
4 Sourcetype = Session:SessionDetail
5 Field = SessionFgWindowTitle
6 Query = Receiver.Name != "uberagent_sensitive"
```

This configuration will clear the contents of `SessionFgWindowTitle` in all receivers, except the receiver `uberagent_sensitive`.

### Example: Filter Events Per Receiver

We can also use almost the same rule to achieve a different use case: exclude events from all receivers, except `uberagent_sensitive`.

```
1 [EventDataFilter]
2 # Exclude this event from all receivers except "uberagent_sensitive"
3 Action = deny
4 Sourcetype = Session:SessionDetail
5 Query = Receiver.Name != "uberagent_sensitive"
```



Instead of clearing the field content for the non-matching receiver, we simply deny sending the event to all receivers, except `uberagent_sensitive`.

### More Examples

More examples including rules created by our support for our customers can be found in the knowledge base article [here](#).

## Username and Configuration Setting Encryption

July 25, 2024

uberAgent optionally encrypts user and domain names in the agent and has support to encrypt sensitive settings in its configuration.

### User and Domain Names

#### Encryption

User and domain names can be encrypted in the agent before being sent off to the backend. This can be useful for compliance with privacy regulations.

User and domain name encryption is disabled by default. If required, enable it via the configuration setting `EncryptUserNames`.

With encryption enabled, user and domain names show up in the backend and in dashboards like this:

| User ↕                           | Host ↕          |
|----------------------------------|-----------------|
| .ttkb=wt0?43n5.-eyzm>er1hgti3t&0 | VASTLIMITS-TIMM |

#### Decryption

uberAgent's download package comes with the command line-tool `uAEncrypt.exe`, which can be used to decrypt usernames as shown in the following example:

```
uAEncrypt.exe -decrypt -keyId 101 -data
```

## Configuration Settings

Configuration settings can optionally be obfuscated.

### Obfuscation

Sensitive settings like passwords can be obfuscated with the command-line tool `uAEncrypt.exe`, which is available in the uberAgent download package. The syntax is viewable by running `uAEncrypt.exe -?`.

To encrypt `MySecretPassword`:

```
uAEncrypt.exe -encrypt -keyId 1 -data PlaintextData
```

**De-Obfuscation** De-obfuscation is possible with:

```
uAEncrypt.exe -decrypt -keyId 1 -data ObfuscatedData
```

**Supported Settings** Obfuscation is supported for all configuration settings.

## ESA Features & Configuration

July 9, 2024

This section describes features that are part of the uberAgent ESA endpoint security analytics product. Please take a look at the [UXM and ESA products page](#) for an explanation what the two products are about and how they work together.

### Enabling ESA

July 9, 2024

uberAgent ESA is enabled or disabled through the configuration setting `EnableESA`. In the [default configuration](#), `EnableESA` is set to `true`. However, the endpoint agent enables ESA only if one of the following is also true:

- Valid UXM and ESA licenses are available (i.e., the product is properly licensed)
- Neither UXM nor ESA licenses are available (demo mode)

## ESA Enables EnableExtendedInfo

When ESA is enabled, `EnableExtendedInfo` is automatically enabled, too, irrespective of the configuration setting of the same name. `EnableExtendedInfo` ensures that GUIDs are added to process events so that individual process instances can be identified and tracked over time.

## Threat Detection Engine

July 9, 2024

uberAgent ESA Threat Detection **makes system activity traceable** and searchable.

When a Threat Detection rule matches a risky process, an unusual network connection, or similar activity, uberAgent ESA creates an event in your SIEM (e.g., Splunk). Threat Detection's comprehensive, extensible ruleset is powered by uAQL, a feature-rich query language that is both easy to read by humans and fast to process by computers.

uberAgent ESA comes with hundreds of predefined rules for many common attack vectors and converters for [Sysmon rules](#) and [Sigma signatures](#). Customizing and extending ESA's ruleset is explicitly encouraged.

### Rule Sources

uberAgent ESA ships with rules from two different sources: vast limits rules and third-party rules. The former are curated by vast limits, while the latter are converted from sources such as the [Sigma project](#).

### Rule Storage

uberAgent ESA Threat Detection rules are part of uberAgent's configuration, which is maintained in the [uberAgent Configuration GitHub repository](#).

### Metadata

#### Annotation (MITRE ATT&CK Technique ID)

Annotations add supplementary data to Threat Detection rules, notably [MITRE ATT&CK technique IDs](#).

## Tag & Risk Score

Every ESA Threat Detection rule comes with a tag and a risk score that are assigned to matching events.

## Sourcetype

ESA Threat Detection events are assigned the sourcetype `uberAgentESA:ActivityMonitoring:ProcessTagging` (see the [metrics documentation](#) for a description of the fields).

## Visualization

ESA Threat Detection events are visualized in the *Threat Detection Events* dashboard, which is part of the `uberAgent_ESA` Splunk searchhead app.

## MS Office & Acrobat Reader Monitoring

July 9, 2024

The ESA Threat Detection rules for monitoring Microsoft Office and Adobe Acrobat Reader are vast limits vendor rules.

### Microsoft Office Rules

The rules in this section detect suspicious behavior with MS Office applications.

- Detect macro execution with the default Office security configuration applied (“disable all macros with notification”)
- Detect child processes of Microsoft Office applications (dedicated rules for scripts and other types of child processes)
- Detect Microsoft Office download operations
- Detect Microsoft Office applications executing macros that access WMI to create child processes
- Suspicious DLL load by Office
- Detect loading of MAPI DLLs from processes other than Outlook

### Adobe Acrobat Reader Rules

The rules in this section detect suspicious behavior with Adobe Acrobat Reader.

- Detect child processes of Adobe Reader

## LOLBAS Monitoring

July 9, 2024

LOLBAS stands for Living Off the Land Binaries And Scripts, a type of activity that misuses tools and executables that are already there because they are part of the operating system. To cite the [LOLBAS' project's criteria](#), a LOLBin/lib/script must:

- Be a Microsoft-signed file, either native to the OS or downloaded from Microsoft.
- Have extra "unexpected" functionality. It is not interesting to document intended use cases.
- Have functionality that would be useful to an APT or red team.

The ESA Threat Detection rules for monitoring LOLBAS activity are vast limits vendor rules.

### LOLBAS Rules

The rules in this section detect suspicious behavior related to operating system binaries.

- Unusual child processes and DLL loads
- Detect starts from non-default locations
- Detect proxy execution
- Detect UAC bypass
- Detect csc/jsc compile
- Detect execute from alternate data streams
- Detect AWL bypass
- Detect encode and decode operations
- Detect copy operations
- Detect download operations

## Network Monitoring

July 9, 2024

The ESA Threat Detection rules for monitoring network activity are vast limits vendor rules.

## Network Rules

The rules in this section detect suspicious behavior related to network operations.

- Suspicious network target names
- PowerShell outbound network connections
- Suspicious outbound Kerberos connections
- PowerShell remoting
- Detect network connects from suspicious sources
- Detect network connects from Windows processes
- Detect network connects from third-party tools
- RDP connects from non-RDP software, indicating lateral movement
- Detect network connects to suspicious ports
- Detect network connects to 80 and 443 from non-browser applications

## Process Tampering Monitoring

July 30, 2024

uberAgent ESA detects several malicious attack techniques such as Process Herpaderping and Process Hollowing. We name these attack techniques Process Tampering events.

### Configuration

uberAgent ESA Process Tampering Monitoring is enabled or disabled through a configuration option. The related configuration Stanza is [[ProcessStartupSettings](#)].

Configure the setting `EnableProcessTampering = false` to disable process tampering monitoring.

By default, this option is enabled (requires ESA enabled, too).

### Detecting Process Tampering Events

Any process tampering action is queryable with [uAQL](#) and its [Threat Detection Engine](#) rules.

### Example Rule

The following example detects any Process Tampering event and forwards it to your backend, once triggered.

```
1 [ActivityMonitoringRule]
2 # Detects any Process Tampering action
3 RuleName = Detects any Process Tampering action
4 EventType = Process.TamperingEvent
5 Tag = process-tampering
6 RiskScore = 75
7 Query = true
```

This example rule forwards any tampering event. You may filter this with more advanced conditions using [Common Event Properties](#).

## Introduction to Process Tampering

While there are a couple of different techniques the outcome is most likely the same. A malicious process is running in the context of a non-malicious process and tries to hide malicious actions in the context of this good process. There are many good resources available that explain these techniques in detail. To get you a short summary please refer to the notes below.

### What is Process Hollowing

A process is launched in a suspended state and executable code is unmapped and replaced with malicious code and resumed.

### What is Process Herpaderping

This technique requires replacing an executable binary with a malicious file and launching it. Then, the original file is restored and the malicious executable pretends to be the original one.

## Remote Thread Monitoring

July 30, 2024

uberAgent ESA detects remote thread creation that may be used in malicious attack techniques or suspicious activities such as DLL injections or malicious code execution in remote processes.

### Configuration

uberAgent ESA Remote Thread Monitoring is enabled or disabled through a configuration option. The related configuration Stanza is [\[Miscellaneous\]](#).

Configure the setting `RemoteThreadMonitoring = false` to disable remote thread monitoring.

By default, this option is enabled (requires ESA enabled and Process Startup metrics enabled, too).

## Detecting Remote Thread Events

Any remote thread action is queryable with [uAQL](#) and its [Threat Detection Engine](#) rules.

### Example Rule

The following example detects any Remote Thread event and forwards it to your backend, once triggered.

```
1 [ActivityMonitoringRule]
2 # Detect any remote thread creation
3 RuleName = Detect remote thread creations
4 EventType = Process.CreateRemoteThread
5 Query = true
6 Tag = process-create-remote-thread
7 RiskScore = 75
8 GenericProperty1 = Thread.Id
9 GenericProperty2 = Thread.Timestamp
10 GenericProperty3 = Thread.StartAddress
11 GenericProperty4 = Thread.StartModule
12 GenericProperty5 = Thread.StartFunctionName
```

However, this general rule may include false positives. There are many cases where remote threads are used that are absolutely not malicious or suspicious. (e.g: debugging applications or OS remote threads)

Therefore it is recommended to filter this with more advanced conditions using [Common Event Properties](#) and [Remote Event Properties](#).

uberAgent ESA is shipped with many automatically converted rules from [Sigma](#). This ruleset already includes several useful Remote Thread detection rules.

## Root CA certificate monitoring

July 9, 2024

The ESA Threat Detection rules for monitoring changes to root CA certificates are vast limits vendor rules.



The rules detect certificate chain cloning and cloned root trust attacks by monitoring writes to user and machine registry keys. For details, check the following rules:

- [Detect AuthRoot, CA and Root certificate changes per machine](#)
- [Detect AuthRoot, CA and Root certificate changes per user](#)

## Security Descriptor & ACL Monitoring

July 30, 2024

The ESA Threat Detection rules for permissions (security descriptors and ACLs) are vast limits vendor rules.

### File System ACL Rules

The rules in this section detect suspicious behavior related to file system permissions (ACLs).

- Detect processes started from directories that are user-writeable
- Detect process starts from directories with a low mandatory integrity label

### Security Descriptor Monitoring Capabilities

uberAgent ESA has sophisticated features that make security descriptors, which can be a bit obscure and difficult to work with, much more accessible:

- SID to name lookup
- Conversion of hex access masks to permission strings

Please see [this document](#) for details.

## Sigma Rules & Converter

July 9, 2024

uberAgent ESA ships with Threat Detection rules derived from Sigma signatures. These rules are grouped by severity: critical, high, medium, and low.

By their nature, Sigma rules are pretty dynamic and may change quickly. Our [Sigma rule coverage explorer](#) web app lets you browse and explore which Sigma rules are supported in which uberAgent

version - and why. See below for instructions on how to convert Sigma rules yourself with our **Sigma converter**.

## Sigma Rules

Following is an excerpt of some Sigma rules that ship with uberAgent ESA:

- Detect Ryuk ransomware command lines
- Detect DNS tunnel activity for Muddywater actor
- Detect a suspicious PowerShell command-line combination as used by APT29 in a campaign against US think tanks
- Detect Russian group activity as described in Global Threat Report 2019 by CrowdStrike
- Detect a suspicious DLL loading from `AppData\Local` as described in BlueMashroom report
- Detect Chafer activity attributed to OilRig as reported in Nyotron report in March 2018
- Detect CrackMapExecWin activity as described by NCSC
- Detect Elise backdoor activity as used by APT32
- Detect the execution of DLL side-loading malware used by threat group Emissary Panda aka APT27
- Detect a specific tool and export used by EquationGroup
- Detects Golden Chickens deployment method as used by Evilnum in a report published in July 2020
- Detect tools and process executions as observed in a Greenbug campaign in May 2020
- Detect Judgement Panda activity as described in Global Threat Report 2019 by CrowdStrike
- Detect registry modifications performed by Ke3chang malware in campaigns running in 2019 and 2020
- Detects Trojan loader activity as used by APT28
- ...and hundreds more

Not all Sigma rules are enabled by default.

## Sigma Converter

vast limits maintains a [Sigma to uberAgent rule converter](#) as part of the Sigma project. The converter is implemented as a Sigma backend. Please see the header of [uberAgent's Sigma rule files](#) for instructions on how to invoke the conversion.

## Sysmon Rule Converter

July 9, 2024

The Sysmon to uberAgent rule converter **translates Sysmon rules into the format used by uberAgent ESA.**

Sysmon is one of the most popular endpoint detection tools. Numerous quality rulesets are maintained by the security community. The Sysmon converter makes those rulesets available for use with uberAgent ESA.

## uberAgent ESA as Sysmon Alternative

In addition to the Sysmon converter, vast limits also provides a [converter for Sigma rules](#). This makes uberAgent one of the most versatile detection tools on the market. Read on to find out [why you should consider uberAgent ESA as an alternative to Sysmon](#).

## Getting Started

### Download

To download the Sysmon converter, head over to the [releases section of its GitHub repository](#).

### Usage

Please see the Sysmon converter's [readme for usage information](#).

## Sysmon Converter Details

### Development Info

The [Sysmon converter](#) is developed as an open-source project on GitHub. Contributions are always welcome!

The Sysmon converter is written in C# .NET. Release builds are available for Windows.

## Threat Detection Engine

July 9, 2024

uberAgent ESA Threat Detection **makes system activity traceable** and searchable.

When a Threat Detection rule matches a risky process, an unusual network connection, or similar activity, uberAgent ESA creates an event in your SIEM (e.g., Splunk). Threat Detection's comprehensive,

extensible ruleset is powered by uAQL, a feature-rich query language that is both easy to read by humans and fast to process by computers.

uberAgent ESA comes with hundreds of predefined rules for many common attack vectors and converters for [Sysmon rules](#) and [Sigma signatures](#). Customizing and extending ESA's ruleset is explicitly encouraged.

## Rule Sources

uberAgent ESA ships with rules from two different sources: vast limits rules and third-party rules. The former are curated by vast limits, while the latter are converted from sources such as the [Sigma project](#).

## Rule Storage

uberAgent ESA Threat Detection rules are part of uberAgent's configuration, which is maintained in the [uberAgent Configuration GitHub repository](#).

## Metadata

### Annotation (MITRE ATT&CK Technique ID)

Annotations add supplementary data to Threat Detection rules, notably [MITRE ATT&CK technique IDs](#).

### Tag & Risk Score

Every ESA Threat Detection rule comes with a tag and a risk score that are assigned to matching events.

### Sourcetype

ESA Threat Detection events are assigned the sourcetype `uberAgentESA:ActivityMonitoring:ProcessTagging` (see the [metrics documentation](#) for a description of the fields).

## Visualization

ESA Threat Detection events are visualized in the *Threat Detection Events* dashboard, which is part of the `uberAgent_ESA` Splunk searchhead app.

## Rule Syntax

July 30, 2024

uberAgent ESA's Threat Detection rules are part of the [configuration](#). This page documents the rule syntax.

### Example

The following example shows a simple rule that is triggered whenever a process is started (`EventType = Process.Start`). The rule's query checks if the started process name is `wmiprvse.exe`. If that is the case, the rule matches, and an event with the tag `proc-start-wmiservice-child` is sent to the backend.

```
1 [ActivityMonitoringRule]
2 RuleId = 0a1bbfbc-e0d9-4c49-953e-e31c3aa3fc91
3 RuleName = Detect child processes of the WMI service
4 EventType = Process.Start
5 Annotation = {
6 "mitre_attack": ["T1071", "T1071.004"] }
7
8 Tag = proc-start-wmiservice-child
9 Query = Parent.Name == "wmiprvse.exe"
```

### Rule Stanzas

There can be any number of `[ActivityMonitoringRule]` stanzas, each defining one rule. Rules are processed in the order in which they are defined in the configuration. uberAgent ESA always processes all rules for every activity. This means that multiple events may be generated per activity.

### Rule Components

An `[ActivityMonitoringRule]` stanza may contain the following components.

#### RuleName

- Setting name: `RuleName`
- Description: any name to more easily identify a rule. Not used by uberAgent.
- Valid values: any string

- Default: empty
- Required: yes

### EventType

- Setting name: [EventType](#)
- Description: the type of event this rule applies to.
- Valid values: see the [event types page](#)
- Default: empty
- Required: yes

### Annotation

- Setting name: [Annotation](#)
- Description: one or more annotations for the event in JSON format
- Valid values:
  - Supported in Splunk Enterprise Security: [nist](#), [kill\\_chain\\_phases](#), [cis20](#), [mitre\\_attack](#), or any custom cyber security framework
  - Supported in uberAgent ESA: [mitre\\_attack](#)
- Default: empty
- Required: no

### Hive

[registry events](#).

This setting is only valid for [registry events](#).

- Setting name: [Hive](#)
- Description: a comma-separated list of registry hives that will be matched against before evaluating the query. For best performance, only the necessary hives should be specified.
- Valid values:
  - [HKLM](#), matches [HKEY\\_LOCAL\\_MACHINE](#)
  - [HKU](#), matches [HKEY\\_USERS](#)
  - [A](#), matches [application hives](#)
  - [WC](#), matches App-V packages and UWP apps

- \*, matches events in any hive. Note that \* has a high performance impact and should be avoided if possible.

- Default: empty
- Required: only if `EventType` is a registry event type.

### Query

- Setting name: `Query`
- Description: a `uAQL query` string that is matched against the `properties of the event`. A rule is considered matching if the query returns `true`.
- Valid values: any uAQL query string
- Default: empty
- Required: yes

### Tag

- Setting name: `Tag`
- Description: a tag assigned to events matching this rule.
- Valid values: any string
- Default: empty
- Required: yes

### RuleId

- Setting name: `RuleId`
- Description: an unique id assigned to this rule.
- Valid values: any string, e.g: 7098a059-4191-4a9e-973c-8976d61cddc0
- Default: empty
- Required: yes

### RiskScore

- Setting name: `RiskScore`
- Description: a risk score assigned to events matching this rule.
- Valid values: any number
- Default: 50
- Required: no

## VerboseLogging

- Setting name: `VerboseLogging`
- Description: if enabled, more detail is added to the log file, e.g., the full evaluated security descriptor if an SDDL rule is configured.
- Valid values: `true` or `false`
- Default: `false`
- Required: no

## Rule Evaluation

Rules are evaluated by evaluating a rule's query with the properties of an event that occurred.

## Reusable uAQL Queries

Threat Detection can store common queries in expressions that can then be used in other queries. This gives you the flexibility to write query code only once and use it multiple times.

### Example

The following declares the Threat Detection expression **ParentIsMsOffice** to identify Microsoft Office as a parent application.

```
1 [AddActivityMonitoringExpression name=ParentIsMsOffice]
2 Query = istartswith(Parent.Company, "Microsoft") and Parent.Name in ["
 excel.exe", "msaccess.exe", "onenote.exe", "outlook.exe", "powerpnt.
 exe", "winword.exe"]
```

The expression **ParentIsMsOffice** is used in the following Threat Detection rule to identify child processes of Microsoft Office.

```
1 [ActivityMonitoringRule]
2 Query = ParentIsMsOffice and (Process.Name in ["cmd.exe", "cscript.exe"
 , "wscript.exe", "ftp.exe"] or ProcessIsPowerShell)
```

Please note that expressions must be defined *before* usage. Ideally, expressions are defined at the top of the configuration file. Also, please make sure not to use [reserved keywords](#) as expression names.

## Disable default shipped rules

Rules can be filtered by their `RuleId` setting. This gives the flexibility to disable certain rules without merging changes in configuration files during updates. The `RuleId` field is unique and persistent over uberAgent releases.



The stanza `ActivityMonitoringRule_Filter` defines a deny list to ignore certain rules by their id.

```
1 [ActivityMonitoringRule_Filter]
2 7098a059-4191-4a9e-973c-8976d61cddc0 = uberAgent_denylist
3 d5b4d0b7-1bfe-4a6b-9664-7b321bfa4094 = uberAgent_denylist
4 21791409-7892-4122-9441-066955ee01b5 = uberAgent_denylist
```

## Rule Editor: uAQL Studio

July 30, 2024

uAQL Studio is a free online tool to learn, build and test uberAgent ESA [Threat Detection](#) rules.

### Quickstart

Follow these steps to get started with uAQL Studio quickly:

1. Open [uAQL Studio](#) in a new browser tab
2. Select an [event type](#)
3. Add events to test the uAQL query your going to write
4. Work on your [uAQL query](#) until it matches your test events correctly
5. Fill out the fields [Rule name](#), [Tag](#), [Risk score](#)
6. Copy the rule definition from the preview pane to the clipboard and paste it into your uberAgent ESA [configuration](#)

### Walkthrough

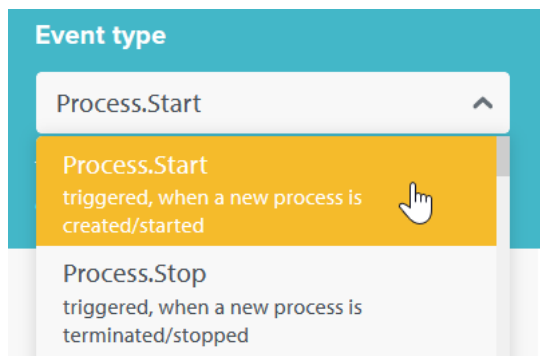
In this walkthrough, we're building a Threat Detection rule that detects script child processes of Microsoft Office applications.

### Launch uAQL Studio

Click the following link to launch uAQL Studio in a new browser tab: <https://uberagent.com/uaql-studio/>.

## Select an Event Type

uberAgent ESA Threat Detection supports many different [types of events](#), including process, network, registry, and DNS events. Select the **Process.Start** event type:

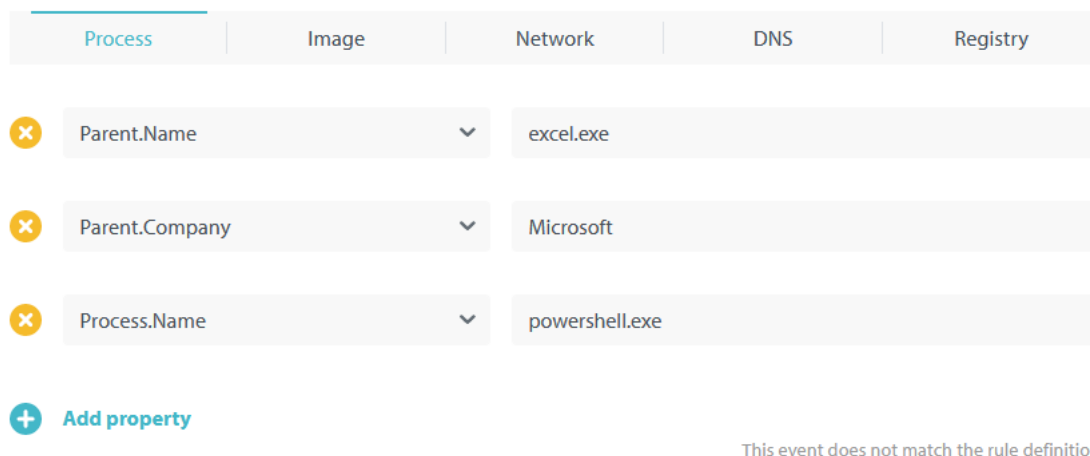


## Add a Test Event

Click **Add event** and specify the [properties](#) of an event you want uAQL Studio to match against the uAQL query you're going to write. Since we're creating a rule to detect script child processes of MS Office apps we're adding the properties of just such an event:

- **Parent.Name:** `excel.exe`
- **Parent.Company:** `Microsoft`
- **Process.Name:** `powershell.exe`

It should look similar to this:



As you can see in the lower right corner of the above screenshot, at this point the test event is not matched by the rule definition (aka, the query). That is correct, of course. After all, the query is still empty!

## Define the uAQL Query

**Detecting Child Processes of MS Office Apps** Let's start to work on our detection query by first creating a snippet that identifies child processes of MS Office apps. Please see the [documentation](#) for details. The following properties should work:

1. the company name of the parent process needs to start with `Microsoft` (which also covers "Microsoft Corporation" and variants like "Microsoft Corp.", all of which can be found in the wild)
2. the parent process name must be one of the following: `excel.exe`, `msaccess.exe`, `onenote.exe`, `outlook.exe`, `powerpnt.exe`, `winword.exe`

In uAQL code the above looks as follows:

```
1 istartswith(Parent.Company, "Microsoft") and Parent.Name in ["excel.exe", "msaccess.exe", "onenote.exe", "outlook.exe", "powerpnt.exe", "winword.exe"]
```

**Detecting Script Processes** We define the following executables as script runtimes:

1. **PowerShell:** `powershell.exe`, `pwsh.exe`
2. **Batch, VBS, miscellaneous:** `cmd.exe`, `cscript.exe`, `wscript.exe`, `ftp.exe`

In uAQL code the above looks as follows:

```
1 Process.Name in ["cmd.exe", "cscript.exe", "wscript.exe", "ftp.exe"] or Process.Name in ["powershell.exe", "pwsh.exe"]
```

**Putting the Query Together** We can now combine the two snippets into the complete uAQL query:

```
1 istartswith(Parent.Company, "Microsoft") and Parent.Name in ["excel.exe", "msaccess.exe", "onenote.exe", "outlook.exe", "powerpnt.exe", "winword.exe"] and (Process.Name in ["cmd.exe", "cscript.exe", "wscript.exe", "ftp.exe"] or Process.Name in ["powershell.exe", "pwsh.exe"])
```

**Paste the Query Into uAQL Studio** Copy the completed query from above and paste it into the **Query** field in uAQL Studio. The built-in syntax checking mechanism should show a green checkmark similar to the following:

**Query**

```

istartswith(Parent.Company, "Microsoft") and Parent.Name in ["excel.exe",
"msaccess.exe", "onenote.exe", "outlook.exe", "powerpnt.exe",
"winword.exe"] and (Process.Name in ["cmd.exe", "cscript.exe",
"wscript.exe", "ftp.exe"] or Process.Name in ["powershell.exe",
"pwsh.exe"])

```

This uAQL query string is matched against the properties of each event observed by the endpoint Activity Monitoring engine. A rule is considered matching if the query returns true. Ctrl+Space for code completion.

**Verify the Test Event Matches** Take a look at the test event we created earlier. The green border indicates that it matches the query. The text in the lower right corner has changed to *This event matches the rule definition*:

### Add Rule Metadata

The rule definition is now complete but we need to add some metadata to make it usable with uberAgent and Splunk. Please see the [documentation](#) for details. The following values work well:

- **Rule name:** Detect script child processes of Microsoft Office applications
- **Tag:** proc-start-msoffice-child
- **Risk score:** 100

The UI should now look similar to the following:

### Rule metadata

#### Rule name

Detect script child processes of Microsoft Office a

A name to more easily identify a rule. Not used by uberAgent.

#### Tag

proc-start-msoffice-child

The string tag assigned to events matching this rule.

#### Risk score

100

The numeric risk score assigned to events matching this rule.

### Copy the Rule Definition

With this, the rule definition is complete. We can copy it from the preview pane and use it with uberAgent ESA!

### Rule preview

Copy to clipboard 

```
[ActivityMonitoringRule]
Name = Detect script child processes of Microsoft Office applications
EventType = Process.Start
Tag = proc-start-msoffice-child
RiskScore = 100
Query = istartswith(Parent.Company, "Microsoft") and Parent.Name in ["excel.exe", "msaccess.exe", "onenote.exe", "outlook.exe", "powerpnt.exe", "winword.exe"] and (Process.Name in ["cmd.exe", "cscript.exe", "wscript.exe", "ftp.exe"] or Process.Name in ["powershell.exe", "pwsh.exe"])
```

### Event Types

August 21, 2024

uberAgent ESA's Threat Detection rules can be triggered by many different types of events.

Event types are specified in the `EventType` component of `[ActivityMonitoringRule]` stanzas ([rule syntax](#)).

## Process & Image Events

### Event Types

The following process event types are available:

- `Process.Start`: triggered, when a new process is created/started
- `Process.Stop`: triggered, when a new process is terminated/stopped
- `Process.CreateRemoteThread`: triggered, when a process is starting a thread in another process
- `Process.TamperingEvent`: triggered, when a process tampering event is being detected
- `Image.Load`: triggered, when an executable image (e.g., a DLL) is loaded

### Event Properties

Common event properties are available with all types of events. [Remote thread creation events](#) and [image load events](#) have additional properties.

## Network Events

### Event Types

The following network event types are available:

- `Net.Send`: triggered, when a network packet is sent
- `Net.Receive`: triggered, when a network packet is received
- `Net.Connect`: triggered, when a network connection is established
- `Net.Reconnect`: triggered, when a network connection is re-established
- `Net.Retransmit`: triggered, when a network packet is retransmitted (sent again)

### Event Properties

Please see the documentation for the [properties of network events](#).

## Registry Events

### Event Types

The following registry event types are available:

- `Reg.Key.Create`: triggered, when a registry key is created

- **Reg.Value.Write**: triggered, when a registry value is written. This includes registry value creation as well as changes to the value's name and data.
- **Reg.Delete**: triggered, when a registry key or value is deleted
- **Reg.Key.Delete**: triggered, when a registry key is deleted
- **Reg.Value.Delete**: triggered, when a registry value is deleted
- **Reg.Key.SecurityChange**: triggered, when a registry key's security descriptor is changed
- **Reg.Key.Rename**: triggered, when a registry key is renamed
- **Reg.Key.SetInformation**: triggered, when a registry key metadata is changed (e.g. last-write time, tags, virtualization, etc.)
- **Reg.Key.Load**: triggered, when a registry hive is loaded
- **Reg.Key.Unload**: triggered, when a registry hive is unloaded
- **Reg.Key.Save**: triggered, when a registry key is saved
- **Reg.Key.Restore**: triggered, when a registry key is restored
- **Reg.Key.Replace**: triggered, when a registry key is replaced
- **Reg.Any**: triggered for any of the above

### Event Properties

Please see the documentation for the [properties of registry events](#).

### DNS Query Events

#### Event Types

The following DNS query event types are available:

- **DNS.Query**: triggered, when an outgoing DNS query request has completed and a response has been received

### Event Properties

Please see the documentation for the [properties of DNS query events](#).

### Common Event Properties

July 30, 2024

The following event properties can be used with all types of events in uAQL queries.

---

| Property name                    | uAQL Data Type | Description                                                                  |
|----------------------------------|----------------|------------------------------------------------------------------------------|
| <code>Process.Id</code>          | String         | The process'id (e.g., 148)                                                   |
| <code>Parent.Id</code>           | String         | The process'parent's id (e.g., 4)                                            |
| <code>Process.Name</code>        | String         | The process'image file name (e.g., <code>Winword.exe</code> )                |
| <code>Parent.Name</code>         | String         | The process'parent's image file name (e.g., <code>Winword.exe</code> )       |
| <code>Process.User</code>        | String         | The process'user name in the format <code>domain\account</code>              |
| <code>Parent.User</code>         | String         | The process'parent's user name in the format <code>domain\account</code>     |
| <code>Process.Path</code>        | String         | The process'full path including the image file name                          |
| <code>Parent.Path</code>         | String         | The process'parent's full path including the image file name                 |
| <code>Process.CommandLine</code> | String         | The process'command line                                                     |
| <code>Parent.CommandLine</code>  | String         | The process'parent's command line                                            |
| <code>Process.AppName</code>     | String         | The process'application name (e.g., <code>Microsoft Office</code> )          |
| <code>Parent.AppName</code>      | String         | The process'parent's application name (e.g., <code>Microsoft Office</code> ) |
| <code>Process.AppVersion</code>  | String         | The process'application version                                              |
| <code>Parent.AppVersion</code>   | String         | The process'parent's application version                                     |
| <code>Process.Company</code>     | String         | The process'company (as stored in the PE image resources)                    |
| <code>Parent.Company</code>      | String         | The process'parent's company (as stored in the PE image resources)           |
| <code>Process.IsElevated</code>  | Boolean        | Is the process elevated?                                                     |
| <code>Parent.IsElevated</code>   | Boolean        | Is the parent process elevated?                                              |



| Property name                              | uAQL Data Type | Description                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>Process.IsProtected</code>           | Boolean        | Is the process protected?                                                                                                                                                                                                                                                                                                                                                                                       |
| <code>Parent.IsProtected</code>            | Boolean        | Is the parent process protected?                                                                                                                                                                                                                                                                                                                                                                                |
| <code>Process.SessionId</code>             | Integer        | The process's session ID                                                                                                                                                                                                                                                                                                                                                                                        |
| <code>Parent.SessionId</code>              | Integer        | The process's parent's session ID                                                                                                                                                                                                                                                                                                                                                                               |
| <code>Process.DirectorySdSddl</code>       | String         | The security descriptor (SD) of the process's directory. The SD is converted to the security descriptor string format (SDDL) for the match. NULL SDs, which grant full access to everyone, are represented as <code>[UA_NULL_SD]</code> . SIDs in the SD are looked up and replaced with names. Hex access masks are replaced with their string representations in SetACL's format ( <a href="#">details</a> ). |
| <code>Process.DirectoryUserWritable</code> | Boolean        | Is the process's directory writable by the user that is logged on the session the process is started in? Ignores processes in session 0.                                                                                                                                                                                                                                                                        |
| <code>Process.Hash.MD5</code>              | String         | MD5 hash of the process executable                                                                                                                                                                                                                                                                                                                                                                              |
| <code>Process.Hash.SHA1</code>             | String         | SHA1 hash of the process executable                                                                                                                                                                                                                                                                                                                                                                             |
| <code>Process.Hash.SHA256</code>           | String         | SHA256 hash of the process executable                                                                                                                                                                                                                                                                                                                                                                           |
| <code>Process.Hash.IMP</code>              | String         | Import-table hash of the process executable                                                                                                                                                                                                                                                                                                                                                                     |

| Property name                           | uAQL Data Type | Description                                                                                                                                                    |
|-----------------------------------------|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>Process.Hashes</code>             | String         | All enabled hashes for process are output comma-separated, e.g.: MD5= CFCD208495D565EF66E7DFF9F98764D , SHA1= B6589FC6AB0DC82CF12099D1C2D40AE                  |
| <code>Parent.Hash.MD5</code>            | String         | MD5 hash of the parent process executable                                                                                                                      |
| <code>Parent.Hash.SHA1</code>           | String         | SHA1 hash of the parent process executable                                                                                                                     |
| <code>Parent.Hash.SHA256</code>         | String         | SHA256 hash of the parent process executable                                                                                                                   |
| <code>Parent.Hash.IMP</code>            | String         | Import-table hash of the parent process executable                                                                                                             |
| <code>Parent.Hashes</code>              | String         | All enabled hashes for parent process are output comma-separated, e.g.: MD5= CFCD208495D565EF66E7DFF9F98764D , SHA1= B6589FC6AB0DC82CF12099D1C2D40AE           |
| <code>Process.IsSigned</code>           | Boolean        | Is the process signed? This evaluates to <b>true</b> even if the certificate was revoked or is expired.                                                        |
| <code>Process.IsSignedByOSVendor</code> | Boolean        | Is the process signed by the vendor of the operating system (e.g. Microsoft)? This evaluates to <b>true</b> even if the certificate was revoked or is expired. |
| <code>Process.Signature</code>          | String         | The signer name.                                                                                                                                               |
| <code>Process.SignatureStatus</code>    | String         | Evaluates to <b>Valid</b> for a valid certificate and <b>Invalid</b> for an invalid certificate. It is empty if the process is not signed.                     |

---

| Property name                          | uAQL Data Type | Description                                                                                                                                                           |
|----------------------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>Parent.IsSigned</code>           | Boolean        | Is the parent process signed? This evaluates to <b>true</b> even if the certificate was revoked or is expired.                                                        |
| <code>Parent.IsSignedByOSVendor</code> | Boolean        | Is the parent process signed by the vendor of the operating system (e.g. Microsoft)? This evaluates to <b>true</b> even if the certificate was revoked or is expired. |
| <code>Parent.Signature</code>          | String         | The signer name.                                                                                                                                                      |
| <code>Parent.SignatureStatus</code>    | String         | Evaluates to <b>Valid</b> for a valid certificate and <b>Invalid</b> for an invalid certificate. It is empty if the parent process is not signed.                     |

---

## DNS Query Event Properties

August 21, 2024

The following event properties can be used with DNS query events in uAQL queries (event type [DNS.Query](#)). In addition to the properties listed here, the [common properties](#) are applicable, too.

---

| Property name                  | uAQL Data Type | Description                                                                          |
|--------------------------------|----------------|--------------------------------------------------------------------------------------|
| <code>Dns.QueryRequest</code>  | String         | The requested DNS name.                                                              |
| <code>Dns.QueryResponse</code> | String         | Responses to the request. May be a semicolon ; separated list of multiple responses. |

---

## Image Load Event Properties

July 30, 2024

The following event properties can be used with image load events in uAQL queries (event type `Image . Load`). In addition to the properties listed here, the [common properties](#) are applicable, too.

| Property name                           | uAQL Data Type | Description                                                                                                                                                         |
|-----------------------------------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>Image . Name</code>               | String         | The image's file name (e.g., <code>userenv.dll</code> )                                                                                                             |
| <code>Image . Path</code>               | String         | The image's full path including the image file name                                                                                                                 |
| <code>Image . Hash . MD5</code>         | String         | MD5 hash of the image                                                                                                                                               |
| <code>Image . Hash . SHA1</code>        | String         | SHA1 hash of the image                                                                                                                                              |
| <code>Image . Hash . SHA256</code>      | String         | SHA256 hash of the image                                                                                                                                            |
| <code>Image . Hash . IMP</code>         | String         | Import-table hash of the image                                                                                                                                      |
| <code>Image . Hashes</code>             | String         | All enabled hashes for image are output comma-separated, e.g.: <code>MD5=CFCD208495D565EF66E7DFF9F98764D</code> , <code>SHA1=B6589FC6AB0DC82CF12099D1C2D40AE</code> |
| <code>Image . IsSigned</code>           | Boolean        | Is the image signed? This evaluates to <b>true</b> even if the certificate was revoked or is expired.                                                               |
| <code>Image . IsSignedByOSVendor</code> | Boolean        | Is the image signed by the vendor of the operating system (e.g. Microsoft)? This evaluates to <b>true</b> even if the certificate was revoked or is expired.        |
| <code>Image . Signature</code>          | String         | The signer name.                                                                                                                                                    |

| Property name                      | uAQL Data Type | Description                                                                                                                                          |
|------------------------------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>Image.SignatureStatus</code> | String         | Evaluates to <code>Valid</code> for a valid certificate and <code>Invalid</code> for an invalid certificate. It is empty if the image is not signed. |

## Network Event Properties

July 30, 2024

The following event properties can be used with network events in uAQL queries (event type `Net.*`). In addition to the properties listed here, the [common properties](#) are applicable, too.

| Property name                    | uAQL Data Type | Description                                                                                       |
|----------------------------------|----------------|---------------------------------------------------------------------------------------------------|
| <code>Net.Target.Ip</code>       | String         | The network target's IP address (IPv4 or IPv6)                                                    |
| <code>Net.Target.IpIsV6</code>   | Boolean        | Indicates whether the network target's IP address is IPv6 (true) or not (false).                  |
| <code>Net.Target.Name</code>     | String         | The network target's name. This is only available if it can be resolved from the local DNS cache. |
| <code>Net.Target.Port</code>     | Integer        | The network target's port                                                                         |
| <code>Net.Target.PortName</code> | String         | A textual representation of the network target port, e.g: https                                   |
| <code>Net.Target.Protocol</code> | String         | Either TCP or UDP                                                                                 |
| <code>Net.Source.Ip</code>       | String         | The network source IP address (IPv4 or IPv6)                                                      |
| <code>Net.Source.IpIsV6</code>   | Boolean        | Indicates whether the network source IP address is IPv6 (true) or not (false).                    |

---

| Property name                    | uAQL Data Type | Description                                                                                     |
|----------------------------------|----------------|-------------------------------------------------------------------------------------------------|
| <code>Net.Source.Name</code>     | String         | The network source name. This is only available if it can be resolved from the local DNS cache. |
| <code>Net.Source.Port</code>     | Integer        | The network source port                                                                         |
| <code>Net.Source.PortName</code> | String         | A textual representation of the network source port, e.g: https                                 |

---

## Registry Event Properties

July 30, 2024

The following event properties can be used with registry events in uAQL queries (event type `Reg.*`). In addition to the properties listed here, the [common properties](#) are applicable, too.

---

| Property name                    | uAQL Data Type | Description                                                                                                                                                     |
|----------------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>Reg.Key.Path</code>        | String         | The absolute path of the registry key (e.g., <code>^HKLM\\SYSTEM\\.*ControlSet.*\\Services\\lmhosts\$</code> ). Not supported for <code>Reg.Key.Rename</code> . |
| <code>Reg.Key.Name</code>        | String         | The name the registry key - the last path element of the full path (e.g., <code>^lmhosts\$</code> ). Not supported for <code>Reg.Key.Rename</code> .            |
| <code>Reg.Parent.Key.Path</code> | String         | The absolute path to the parent key (e.g., <code>^HKLM\\SYSTEM\\.*ControlSet.*\\Services\$</code> ). Not supported for <code>Reg.Key.Rename</code> .            |

---

| Property name                 | uAQL Data Type | Description                                                                                                                                                                               |
|-------------------------------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>Reg.Key.Path.New</code> | String         | The new absolute path of the registry key (e.g., <code>^HKLM\SYSTEM\*. *ControlSet.*\Services\lmhosts\$</code> ). Only supported for <code>Reg.Key.Rename</code> .                        |
| <code>Reg.Key.Path.Old</code> | String         | The old absolute path of the registry key (e.g., <code>^HKLM\SYSTEM\*. *ControlSet.*\Services\lmhosts\$</code> ). Only supported for <code>Reg.Key.Rename</code> .                        |
| <code>Reg.Value.Name</code>   | String         | The name of a key property (e.g., <code>RequiredPrivileges</code> ).                                                                                                                      |
| <code>Reg.File.Name</code>    | String         | A file path (e.g., <code>C:\TempHive.hiv</code> ). Supported for <code>Reg.Key.Load</code> , <code>Reg.Key.Restore</code> , <code>Reg.Key.Save</code> , or <code>Reg.Key.Replace</code> . |
| <code>Reg.Key.Sddl</code>     | String         | The security descriptor (SD) of a registry key.                                                                                                                                           |
| <code>Reg.Key.Hive</code>     | String         | The name of the Hive (e.g., <code>HKLM</code> ).                                                                                                                                          |
| <code>Reg.Key.Target</code>   | String         | The absolute path of the registry key. Takes <code>Reg.Key.Path.Old</code> or <code>Reg.Key.Path</code> and is thus never empty.                                                          |

---

## Remote Thread Event Properties

July 30, 2024

The following event properties can be used with create remote thread events in uAQL queries (event type `Process.CreateRemoteThread`). In addition to the properties listed here, the [common properties](#) are applicable, too.

---

| Property name                         | uAQL Data Type | Description                                                                  |
|---------------------------------------|----------------|------------------------------------------------------------------------------|
| <code>Thread.Id</code>                | Integer        | The thread identifier of the newly created thread.                           |
| <code>Thread.Timestamp</code>         | Integer        | Event Timestamp                                                              |
| <code>Thread.Process.Id</code>        | Integer        | The process identifier of the process that runs the newly created thread.    |
| <code>Thread.Parent.Id</code>         | Integer        | The process identifier of the process that has initiated the remote thread.  |
| <code>Thread.StartAddress</code>      | Integer        | The absolute address in virtual memory where the function is located.        |
| <code>Thread.StartModule</code>       | String         | The name of the library where the function that was started is located in.   |
| <code>Thread.StartFunctionName</code> | String         | The name of the function that was started as entry point for the new thread. |

---

## Process.DirectorySdSddl

July 30, 2024

The event property `Process.DirectorySdSddl` is a powerful tool: it makes the **file system permissions** of a process' directory available for regex matching and rule evaluation.



## Overview

Whenever an event occurs, uberAgent ESA checks if the event property `Process.DirectorySdSddl` is configured in at least one Threat Detection rule. If that is the case, uberAgent ESA does the following:

1. determine the **directory** of the process executable
2. read the directory's **security descriptor** (SD)
3. convert the SD to the **SDDL string** format
4. in the SDDL string, **replace SIDs** with user/group names
5. in the SDDL string, replace hex access masks with **readable permissions** strings
6. **match** the resulting string against the rule's regex

## Security Descriptor Components

Security Descriptors are structures that contain multiple components, some of which are optional:

- Owner
- Primary group (rarely used, if at all)
- DACL (permissions)
- SACL (auditing configuration)
- Attributes (claims)
- Mandatory integrity label
- Scoped policy ID

uberAgent ESA retrieves all of the SD components shown above.

## How It Works in Detail

### Converting the SD to the SDDL String Format

Security descriptors are binary structures. In order for humans to read or regular expressions to match their contents, SDs must be converted to strings. Microsoft established a common format for that purpose, the [Security Descriptor Definition Language](#).

uberAgent ESA converts all the security descriptor components to SDDL, but it does not stop there because **SDDL has shortcomings**.

### Converting User/Group SIDs to Names

SDDL strings are more or less 1:1 representations of the binary SD structure. This means that, with very few exceptions, users and groups are not shown by their names, but by their SIDs, for example

S-1-5-21-3803133166-2955000686-238773884-1029. Such a SID string is not very useful for regex matching, so uberAgent goes ahead and converts it to the well-known `domain\user` format before performing the regex matching.

### Converting Hex Access Masks to Permission Strings

The same is true for access masks, which store the actual permission in a 32-bit unsigned integer. In a raw SDDL string, an access mask might look like this: `0x1200a9`. That is not very useful for regex matching because multiple permissions can be combined in one access mask through bitwise OR. Again, uberAgent does the heavy lifting by converting access masks to a string format that is processed easily: `SetACL`'s. With this conversion, the cryptic access mask `0x1200a9` becomes the easily understandable string `read_execute`.

If an access mask contains a combination of multiple individual permissions, uberAgent's `SetACL` string lists all the individual permission names separated by commas.

### Example

SDDL string for `C:\Windows\System32` as obtained by the Windows API before uberAgent ESA's simplifications:

```
1 O:S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464G:S
 -1-5-80-956008885-3418522649-1831038044-1853292631-2271478464D:PAI(A
 ;;FA;;;S
 -1-5-80-956008885-3418522649-1831038044-1853292631-2271478464)(A;
 CIIIO;GA;;;S
 -1-5-80-956008885-3418522649-1831038044-1853292631-2271478464)(A;;0
 x1301bf;;;SY)(A;OICIIIO;GA;;;SY)(A;;0x1301bf;;;BA)(A;OICIIIO;GA;;;BA)(
 A;;0x1200a9;;;BU)(A;OICIIIO;GXGR;;;BU)(A;OICIIIO;GA;;;CO)(A;;0x1200a9
 ;;;AC)(A;OICIIIO;GXGR;;;AC)(A;;0x1200a9;;;S-1-15-2-2)(A;OICIIIO;GXGR
 ;;;S-1-15-2-2)S:AINO_ACCESS_CONTROL
```

The same string after uberAgent ESA replaced SIDs with names:

```
1 O:NT SERVICE\TrustedInstallerG:NT SERVICE\TrustedInstallerD:PAI(A;;FA
 ;;;NT SERVICE\TrustedInstaller)(A;CIIIO;GA;;;NT SERVICE\
 TrustedInstaller)(A;;0x1301bf;;;SY)(A;OICIIIO;GA;;;SY)(A;;0x1301bf;;;
 BA)(A;OICIIIO;GA;;;BA)(A;;0x1200a9;;;BU)(A;OICIIIO;GXGR;;;BU)(A;OICIIIO
 ;GA;;;CO)(A;;0x1200a9;;;AC)(A;OICIIIO;GXGR;;;AC)(A;;0x1200a9;;;
 APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES)(A
 ;OICIIIO;GXGR;;;APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED
 APPLICATION PACKAGES)S:AINO_ACCESS_CONTROL
```

The same string after uberAgent ESA additionally replaced hex access masks with permission strings:

```

1 O:NT SERVICE\TrustedInstallerG:NT SERVICE\TrustedInstallerD:PAI(A;;;full
;;;NT SERVICE\TrustedInstaller)(A;CIIIO;full;;;NT SERVICE\
TrustedInstaller)(A;;change;;;SY)(A;OICIIIO;full;;;SY)(A;;change;;;BA
)(A;OICIIIO;full;;;BA)(A;;read_execute;;;BU)(A;OICIIIO;read_execute;;;
BU)(A;OICIIIO;full;;;CO)(A;;read_execute;;;AC)(A;OICIIIO;read_execute
;;;AC)(A;;read_execute;;;APPLICATION PACKAGE AUTHORITY\ALL
RESTRICTED APPLICATION PACKAGES)(A;OICIIIO;read_execute;;;APPLICATION
PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES)S:
AINO_ACCESS_CONTROL

```

## Deconstructing the SDDL String

Here is a quick explanation of the security descriptor string format. For the full specifications please see [Microsoft's documentation](#).

Split into the SD's components, the SDDL string from the example above is already much more readable:

```

1 O:NT SERVICE\TrustedInstaller
2 G:NT SERVICE\TrustedInstaller
3 D:PAI(A;;;full;;;NT SERVICE\TrustedInstaller)(A;CIIIO;full;;;NT SERVICE\
TrustedInstaller)(A;;change;;;SY)(A;OICIIIO;full;;;SY)(A;;change;;;BA
)(A;OICIIIO;full;;;BA)(A;;read_execute;;;BU)(A;OICIIIO;read_execute;;;
BU)(A;OICIIIO;full;;;CO)(A;;read_execute;;;AC)(A;OICIIIO;read_execute
;;;AC)(A;;read_execute;;;APPLICATION PACKAGE AUTHORITY\ALL
RESTRICTED APPLICATION PACKAGES)(A;OICIIIO;read_execute;;;APPLICATION
PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES)
4 S:AINO_ACCESS_CONTROL

```

As you can see, the four main components of a security descriptor are prepended by the following:

- O:: owner
- G:: primary group
- D:: DACL
- S:: SACL

The DACL part of an SDDL string is a concatenation of **access control entries (ACEs)**, each wrapped in parentheses. In this example, there are 13 ACEs in the ACL:

```

1 (A;;;full;;;NT SERVICE\TrustedInstaller)
2 (A;CIIIO;full;;;NT SERVICE\TrustedInstaller)
3 (A;;change;;;SY)
4 (A;OICIIIO;full;;;SY)
5 (A;;change;;;BA)
6 (A;OICIIIO;full;;;BA)
7 (A;;read_execute;;;BU)
8 (A;OICIIIO;read_execute;;;BU)
9 (A;OICIIIO;full;;;CO)
10 (A;;read_execute;;;AC)

```

```
11 (A;OICIIIO;read_execute;;;AC)
12 (A;;;read_execute;;;APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED
 APPLICATION PACKAGES)
13 (A;OICIIIO;read_execute;;;APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED
 APPLICATION PACKAGES)
```

Please see [Microsoft's documentation](#) for an explanation of the ACE properties.

## Logging

As you saw above, SDDL strings can be complex. When writing regular expressions to match them, you need to know what you are dealing with. In other words, you need log samples.

**Tip:** while working on a Threat Detection rule involving the security descriptor, set the rule's [VerboseLogging](#) config element to **true**. With verbose logging enabled, uberAgent's write messages like the following to its [log file](#):

```
GetPermissionsSddl,Read the SD of <\\?\C:\WINDOWS\System32>:
```

## Hash Calculation of PE Images

July 9, 2024

uberAgent ESA calculates hashes of executables (e.g., `.exe`, `.dll` or `.sys` files). Whenever a process is started or a DLL is loaded, uberAgent calculates the hash of the file located on disk. uberAgent supports the hash variants `MD5`, `SHA-1`, `SHA-256`, and `ImpHash` both individually and simultaneously.

## Configuration

The uberAgent ESA hash calculation feature is configured through the process startup setting `EnableCalculateHash`. In the [default configuration](#), `MD5` hash calculation is enabled.

Process and library (DLL) hashes are cached to reduce CPU load. Cache lifetime is managed automatically. The cache's size can be configured (or disabled altogether) via the configuration setting `HashesCacheMaxSize`.

## Metadata

### Sourcetype

Process hashes are part of the sourcetypes `uberAgent:Process:ProcessStartup` and `uberAgentESA:Process:ProcessStop`. Please see the [metrics documentation](#) for a description of the fields.

Due to the huge amount of data being produced, hash values for image load events are not sent to the backend but can be used with the [Threat Detection Engine](#).

## Authenticode Signature Verification

July 9, 2024

uberAgent ESA verifies the Authenticode signature for every process that is started.

The following information is collected:

- Is the executable signed by the OS manufacturer, e.g., Microsoft?
- Is the Authenticode signature valid?
- The Authenticode signer's name

### Configuration

uberAgent ESA Authenticode verification is configured through the process startup setting `EnableAuthenticode`. In the [default configuration](#), Authenticode verification is enabled.

uberAgent ESA caches the results of Authenticode verifications. The number of cached results can be set via `AuthenticodeCacheMaxSize`, which is preset to 500 entries in the default configuration.

## Metadata

### Sourcetype

Authenticode signature information is part of the sourcetype `uberAgent:Process:ProcessStartup`. Please see the [metrics documentation](#) for a description of the fields.

## DNS Query Monitoring

July 9, 2024

uberAgent ESA monitors outgoing DNS queries and their responses. This includes all DNS queries that are processed by the operating system.

### Functionality

The implementation and functionality of DNS query monitoring differ between operating systems.

#### Windows

uberAgent uses the local DNS machine's DNS resolver as the data source. uberAgent sees all DNS requests that are handled by the OS, including requests via encrypted DNS (DoT or DoH). uberAgent doesn't see requests that bypass the OS resolver, e.g., requests from tools such as [nslookup](#).

uberAgent cannot differentiate between requests that go over the wire and requests that can be answered from the local DNS cache. Both types of requests are collected by uberAgent.

#### macOS

uberAgent monitors network traffic at the packet level. uberAgent sees any and all DNS requests, but it cannot process encrypted DNS (DoT or DoH). uberAgent only collects requests that go over the wire, it doesn't process requests that can be answered from the local DNS cache.

### Configuration

uberAgent ESA DNS query monitoring is enabled or disabled through the timer metric [DnsMonitoring](#). For Windows clients, this feature requires Windows 8.1 or newer versions of Windows since the data source for this event is not available in previous Windows versions, such as Windows 7. Enabling the metric on unsupported Windows versions has no effect. For macOS, all versions are supported.

### Metadata

#### Sourcetype

DNS query monitoring events are sent with the sourcetype [uberAgentESA:Process:DnsQuery](#) ([documentation](#)). This feature may significantly increase the data volume and can be limited us-

ing [event data filtering](#). uberAgent's configuration includes a comprehensive set of rules to exclude known and harmless DNS requests.

## Threat Detection

DNS monitoring events are also available via uberAgent's Threat Detection engine. This allows the creation of rules to report specific DNS events (e.g., malicious events or threat detection).

## Visualization

DNS query monitoring events are visualized in the *Process DNS* dashboard, which is part of the [uberAgent\\_ESA](#) Splunk searchhead app.

## MITRE ATT&CK Integration

July 30, 2024

### MITRE ATT&CK

The MITRE ATT&CK® framework is a knowledge base of adversary tactics and techniques based on real-world observations of cybersecurity threats. With the help of ATT&CK, different stakeholders (offense, defense, SOCs, third-party vendors, and so on) can speak the same language to describe attacks on enterprise IT and mobile devices. While there are other similar frameworks available, ATT&CK is the de-facto industry standard.

### Integration With uberAgent ESA

When an uberAgent ESA Threat Detection rule matches suspicious activity, uberAgent's endpoint agent sends an event to its configured SIEM backend. uberAgent annotates Threat Detection events with ATT&CK technique IDs.

Annotations are part of the ESA Threat Detection rule specification. Implementation details can be found [here](#). Below is a rule sample:

```
1 [ActivityMonitoringRule]
2 # Detects suspicious DNS queries known from Cobalt Strike beacons
3 RuleName = Cobalt Strike DNS Beaconing
4 EventType = Dns.Query
5 Tag = cobalt-strike-dns-beaconing
```

```

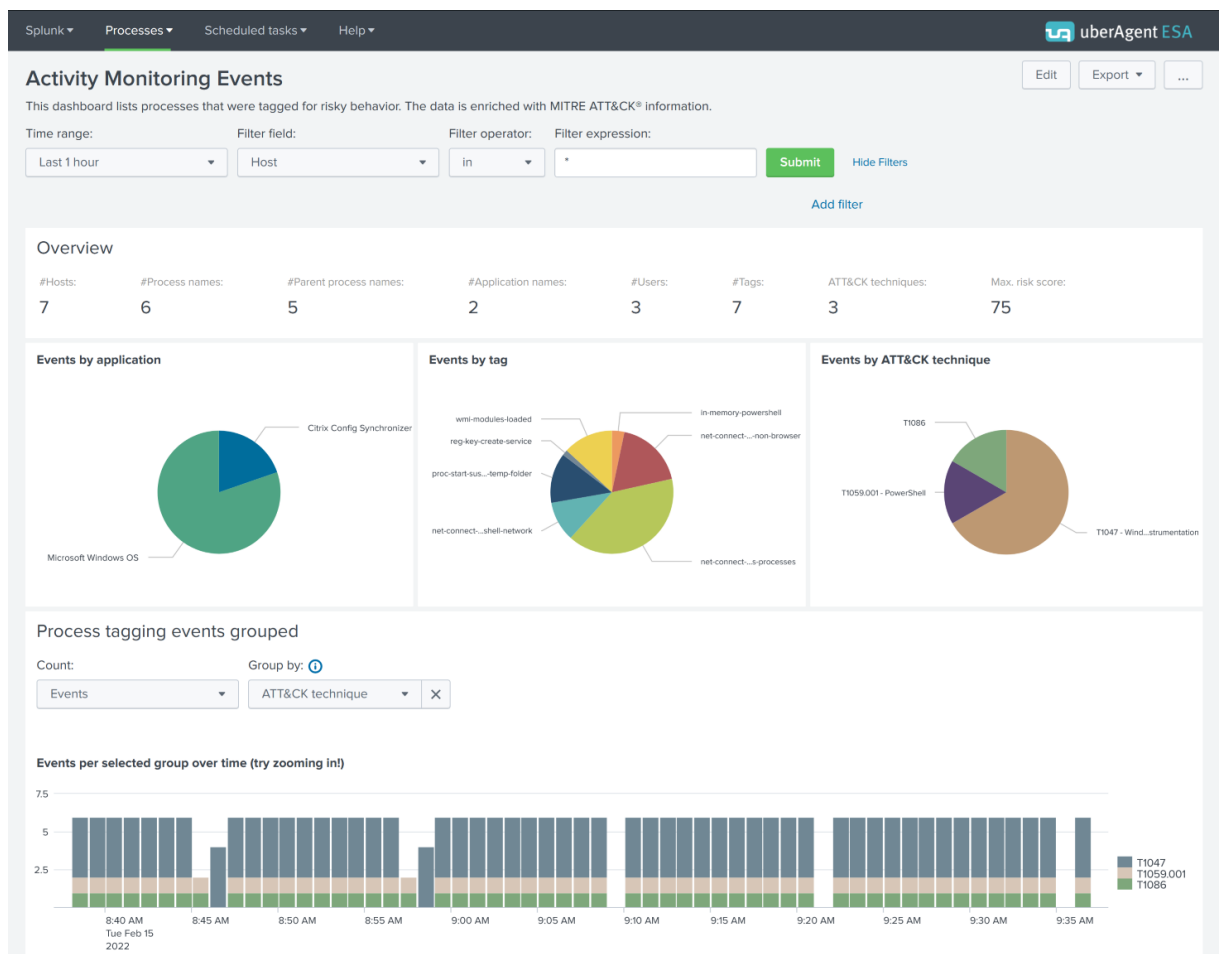
6 RiskScore = 100
7 Annotation = {
8 "mitre_attack": ["T1071", "T1071.004"] }
9
10 Query = (Dns.QueryRequest like r"aaa.stage.%" or Dns.QueryRequest like
11 r"post.1%")
12 GenericProperty1 = Dns.QueryRequest
13 GenericProperty2 = Dns.QueryResponse

```

### Visualization

The uberAgent ESA Splunk app processes the Threat Detection events with technique ID annotations and adds context like the technique’s name, its description and detection, and the URL to the technique on the MITRE website.

This processed information is visualized in the **Threat Detection Events** dashboard. In the screenshot below you can see the number of events by technique ID, and the distribution of events by ID over time.



The further you scroll down the more details you get. The first table in the screenshot below shows



details for each technique. A click on a technique row lists all events where the technique was detected in the second table in the screenshot below.

Events per selected group (effective interval: 2022-02-15 08:37:00 - 2022-02-15 09:38:00)

| ATT&CK technique | #Events | #Hosts | #Process names | #Parent process names | #Application names | #Users | #Tags | #ATT&CK techniques | Max. risk score |
|------------------|---------|--------|----------------|-----------------------|--------------------|--------|-------|--------------------|-----------------|
| T1047            | 228     | 1      | 1              | 1                     | 1                  | 1      | 1     | 1                  | 75              |
| T1059_001        | 55      | 1      | 1              | 1                     | 1                  | 1      | 1     | 1                  | 75              |
| T1086            | 55      | 1      | 1              | 1                     | 1                  | 1      | 1     | 1                  | 75              |

Explanation of the data in the table

Events in selected group: ATT&CK technique = T1047

Fields to display:

Name (ID) x Parent (ID) x Application (version) x User (session ID) x Elevated x Protected x Tag x ATT&CK techniques x

| Time                | Host     | Event type | #Events | Additional Data                                                                                                                                                                                                                                                                                                                         | Name (ID)                | Parent (ID)                  | Application (version)                  | User (session ID)   | Elevated | Protected | Tag                | ATT&CK techniques |
|---------------------|----------|------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|------------------------------|----------------------------------------|---------------------|----------|-----------|--------------------|-------------------|
| 2022-02-15 08:37:16 | NIGHTLY1 | Image.Load | 2       | Image.Name: wbencom.dll<br>Image.Path: C:\Windows\System32\wbencom.dll<br>Image.Hash_MD5: 3423A91671C32A82B0002582B184537<br>Image.Hash_SHA1: 828982AF8C8E964899C74854643AC921E7B7D424<br>Image.Hash_SHA256: 6F5C38519866A8E5E654CE80EF274A713C40DFB1D485D7584E278542A74D673<br>Image.Hash_IMP: 28FB09158B980F89CE95B63A6345ED98        | ConfigSyncRun.exe (8716) | ConfigSyncService.exe (2784) | Citrix Config Synchronizer (7.30.0.12) | NETWORK SERVICE (8) | 1        | 0         | wmi-modules-loaded | T1047             |
| 2022-02-15 08:37:16 | NIGHTLY1 | Image.Load | 2       | Image.Name: Fastprox.dll<br>Image.Path: C:\Windows\System32\wbem\Fastprox.dll<br>Image.Hash_MD5: 95C49381FE7852484D20866587DC8AF<br>Image.Hash_SHA1: B14E2EE95FD398E35E3114EE60FD0837DE620FA4<br>Image.Hash_SHA256: 079EE278C93E683FF7B01B26667FEC4E49E5F74A0B1CB731F521D88AE213E12<br>Image.Hash_IMP: E823F281398172902F3883C082375AF3 | ConfigSyncRun.exe (8716) | ConfigSyncService.exe (2784) | Citrix Config Synchronizer (7.30.0.12) | NETWORK SERVICE (8) | 1        | 0         | wmi-modules-loaded | T1047             |

Note that the rightmost column **ATT&CK techniques** is highlighted in blue. When you click on it you get detailed ATT&CK information on the technique ID in a pop-up.

Events per selected group (effective interval: 2022-02-15 08:37:00 - 2022-02-15 09:38:00)

| ATT&CK technique | #Events | #Hosts | #Process names | #Parent process names | #Application names | #Users | #Tags | #ATT&CK techniques | Max. risk score |
|------------------|---------|--------|----------------|-----------------------|--------------------|--------|-------|--------------------|-----------------|
| T1047            | 228     | 1      | 1              | 1                     | 1                  | 1      | 1     | 1                  | 75              |
| T1059_001        | 55      | 1      | 1              | 1                     | 1                  | 1      | 1     | 1                  | 75              |
| T1086            | 55      | 1      | 1              | 1                     | 1                  | 1      | 1     | 1                  | 75              |

Explanation of the data in the table

Events in selected group: ATT&CK technique = T1047

Fields to display:

Name (ID) x Parent (ID) x Application (version) x User (session ID) x Elevated x Protected x Tag x ATT&CK techniques x

| Time                | Host     | Event type | #Events | Additional Data                                                                                                                                                                                                                                                                                                                         | Name (ID)                | Parent (ID)                  | Application (version)                  | User (session ID)   | Elevated | Protected | Tag                | ATT&CK techniques |
|---------------------|----------|------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|------------------------------|----------------------------------------|---------------------|----------|-----------|--------------------|-------------------|
| 2022-02-15 08:37:16 | NIGHTLY1 | Image.Load | 2       | Image.Name: wbencom.dll<br>Image.Path: C:\Windows\System32\wbencom.dll<br>Image.Hash_MD5: 3423A91671C32A82B0002582B184537<br>Image.Hash_SHA1: 828982AF8C8E964899C74854643AC921E7B7D424<br>Image.Hash_SHA256: 6F5C38519866A8E5E654CE80EF274A713C40DFB1D485D7584E278542A74D673<br>Image.Hash_IMP: 28FB09158B980F89CE95B63A6345ED98        | ConfigSyncRun.exe (8716) | ConfigSyncService.exe (2784) | Citrix Config Synchronizer (7.30.0.12) | NETWORK SERVICE (8) | 1        | 0         | wmi-modules-loaded | T1047             |
| 2022-02-15 08:37:16 | NIGHTLY1 | Image.Load | 2       | Image.Name: Fastprox.dll<br>Image.Path: C:\Windows\System32\wbem\Fastprox.dll<br>Image.Hash_MD5: 95C49381FE7852484D20866587DC8AF<br>Image.Hash_SHA1: B14E2EE95FD398E35E3114EE60FD0837DE620FA4<br>Image.Hash_SHA256: 079EE278C93E683FF7B01B26667FEC4E49E5F74A0B1CB731F521D88AE213E12<br>Image.Hash_IMP: E823F281398172902F3883C082375AF3 | ConfigSyncRun.exe (8716) | ConfigSyncService.exe (2784) | Citrix Config Synchronizer (7.30.0.12) | NETWORK SERVICE (8) | 1        | 0         | wmi-modules-loaded | T1047             |

T1047 - Windows Management Instrumentation

**Description**

Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. WMI is an administration feature that provides a uniform environment to access Windows system components. The WMI service enables both local and remote access, though the latter is facilitated by Remote Services such as Distributed Component Object Model (DCOM) and Windows Remote Management (WinRM). (Citation: MSDN WMI) Remote WMI over DCOM operates using port 135, whereas WMI over WinRM operates over port 5985 when using HTTP and 5986 for HTTPS. (Citation: MSDN WMI) (Citation: FireEye WMI 2015)

An adversary can use WMI to interact with local and remote systems and use it as a means to execute various behaviors, such as gathering information for Discovery as well as remote Execution of files as part of Lateral Movement. (Citation: FireEye WMI SANS 2015) (Citation: FireEye WMI 2015)

**Detection**

Monitor network traffic for WMI connections; the use of WMI in environments that do not typically use WMI may be suspect. Perform process monitoring to capture command-line arguments of "wmic" and detect commands that are used to perform remote behavior. (Citation: FireEye WMI 2015)

**More Information**

<https://attack.mitre.org/techniques/T1047>

## Installation

The ATT&CK integration is enabled by default. You don't need to do anything except install the uberAgent ESA Splunk app on your Splunk search heads. The installation is documented [here](#).

## Keeping ATT&CK Up-to-Date

Every uberAgent release includes the latest ATT&CK information. If you notice that MITRE made changes to their ATT&CK framework and want the updated data in Splunk, you have two options:

1. Wait for the next uberAgent version and update the ESA Splunk app
2. Update the CSV file for the ATT&CK Splunk lookup manually
  - a) The current CSV is always accessible in our [GitHub repository](#). Download the file `annotation_mitre_attack.csv` from there.
  - b) Replace the file in `$SPLUNK_HOME/etc/apps/uberAgent_ESA/lookups`
  - c) Restart Splunk
3. Context: in the year 2021, MITRE made five changes to the source

### **uberAgent ESA and Splunk Enterprise Security**

Splunk Enterprise Security also has an ATT&CK integration and uberAgent integrates with ES, too. Below is a short summary of both integrations to avoid confusion.

#### **uberAgent MITRE ATT&CK Data in uberAgent ESA Dashboards**

The uberAgent ESA Splunk app visualizes the data collected by uberAgent's endpoint agents. The uberAgent ESA Splunk app is compatible with Splunk Enterprise and Cloud. It has an ATT&CK integration built-in that can be used without the need to purchase Splunk Enterprise Security.

Use it when:

- You don't have Splunk Enterprise Security
- You only need ATT&CK and no other cybersecurity framework

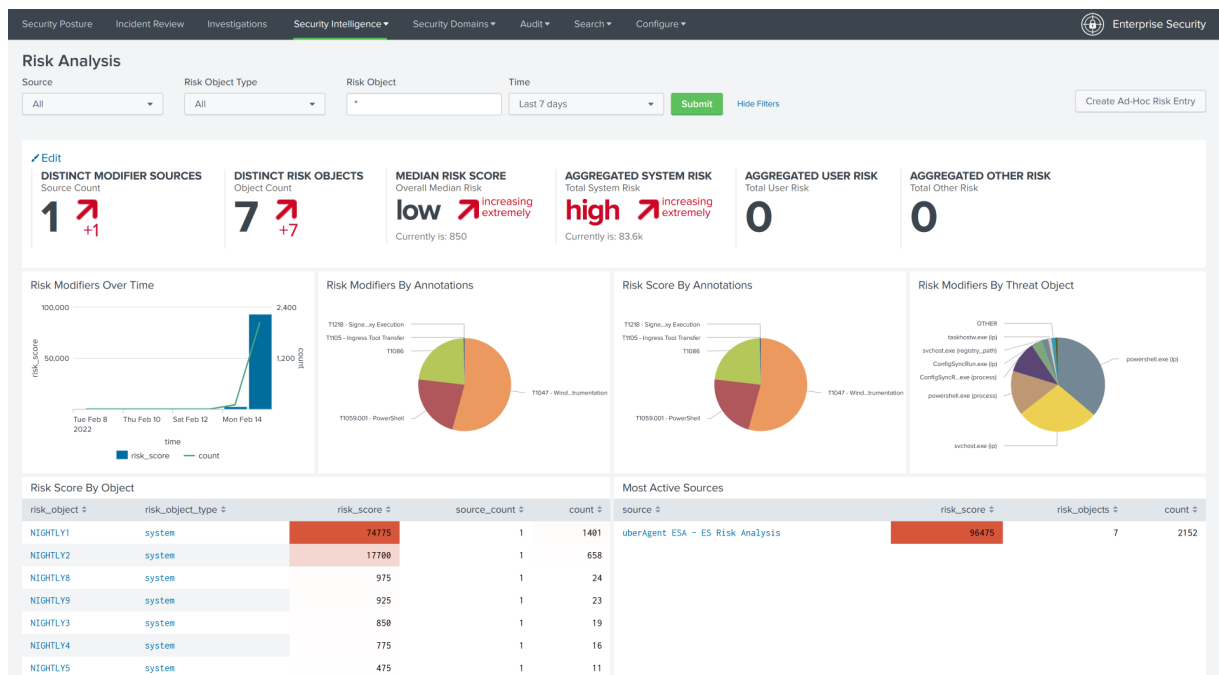
#### **uberAgent MITRE ATT&CK Data in Splunk Enterprise Security**

Splunk Enterprise Security is a paid premium app developed by Splunk that needs to be licensed on top of Splunk Enterprise or Cloud. It comes with support for multiple cybersecurity frameworks, ATT&CK is one of them. If you are an ES customer you may want to install the *uberAgent ESA ES companion* app to enjoy the benefits of uberAgent ESA data in Enterprise Security, enriched with data from cybersecurity frameworks ([more information](#)).

Use it when:

- You have Splunk Enterprise Security
- You need more cybersecurity frameworks than ATT&CK

**Note:** in this scenario, you can use both the uberAgent ESA app and Splunk's Enterprise Security dashboards.



## Process Tree Dashboard

July 25, 2024

## Tracking Process Lifetime & Child Creation

### Process GUID

uberAgent ESA assigns each process a GUID. Such a unique ID is necessary because the operating system's process IDs are reused. By leveraging process GUIDs, uberAgent can track processes throughout their lifetime, from the start (sourcetype `uberAgent:Process:ProcessStartup`) to the end (sourcetype `uberAgentESA:Process:ProcessStop`) as well as during the runtime (sourcetype `uberAgent:Process:ProcessDetail`).

### Process Parent

uberAgent ESA not only identifies unique process instances; it also keeps track of parent-child relationships. All process start and stop events include names and GUIDs of the parent process.

## Process Tree

A process tree is an essential tool for understanding process creation behavior. uberAgent ESA comes with a powerful Process Tree dashboard that makes it easy to identify a process' descendants, listing important process properties such as the process **lifetime**, the **command line**, the **elevation** status, or the name and **version** of the application the process is a part of. Additionally, the number of child processes is calculated, both direct children as well as their children recursively.

By selecting any process in the tree, it becomes the new root, and the table updates to show its child processes. This makes it possible to browse through process hierarchies.

The screenshot shows the 'Process Tree' dashboard in uberAgent ESA. At the top, there are navigation tabs for 'Splunk', 'Processes', 'Scheduled tasks', and 'Help'. The main title is 'Process Tree' with a subtitle 'This dashboard lists processes to visualize process creation behavior and process lifetime.' Below this, there are input fields for 'Time range' (15:00 to 16:00, 19 May 2021), 'Filter field' (Host), 'Filter operator' (In), and 'Filter expression'. A 'Submit' button and a 'Hide Filters' link are also present. A section titled 'Please start by selecting host(s)' shows a dropdown menu with 'UA-WKS-1 (CELSIUS\_1...)' selected. Below that is a bar chart titled 'Process start count over time (try zooming in!)' showing process starts from 15:00 to 15:57. A legend on the right of the chart lists various processes like Code.exe, Chrome.exe, etc. Below the chart is a section 'Process starts (select a process or parent to make it the new root)' with three filter input fields. The main part of the dashboard is a table with the following data:

| Lifetime # | Name (ID) #         | #Children (recursive) # | Parent (ID) #       | Application (version) #             | Elevated # | Protected # | Start #             | Stop #              | Lifetime [s] | Command Line #                                        |
|------------|---------------------|-------------------------|---------------------|-------------------------------------|------------|-------------|---------------------|---------------------|--------------|-------------------------------------------------------|
|            | explorer.exe (2836) | 3 (3)                   | explorer.exe (72)   | Internet Explorer (11.583.17763.0)  | 0          | 0           | 2021-05-19 15:29:09 | 2021-05-19 15:29:24 | 15.078       | ... \Internet Explorer\Iexplorer.exe http://uberag... |
|            | explorer.exe (2840) | 0 (0)                   | explorer.exe (2836) | Internet Explorer (11.583.17763.0)  | 0          | 0           | 2021-05-19 15:29:09 | 2021-05-19 15:29:24 | 15.078       | ... \Internet Explorer\IEXPLORE.EXE SCODEF:6600 CR... |
|            | explorer.exe (2844) | 0 (0)                   | explorer.exe (2836) | Internet Explorer (11.583.17763.0)  | 0          | 0           | 2021-05-19 15:29:09 | 2021-05-19 15:29:24 | 15.078       | ... \Internet Explorer\Iexplorer.exe www.heise.de     |
|            | explorer.exe (2848) | 0 (0)                   | explorer.exe (2836) | Internet Explorer (11.583.17763.0)  | 0          | 0           | 2021-05-19 15:29:09 | 2021-05-19 15:29:24 | 15.078       | ... \Internet Explorer\IEXPLORE.EXE SCODEF:8148 CR... |
|            | cscrip.exe (2856)   | 0 (0)                   | excel.exe (2852)    | Microsoft Windows OS                | 1          | 0           | 2021-05-19 15:29:29 | 2021-05-19 15:29:34 | 5            | ... \System32\cscrip.exe                              |
|            | excel.exe (2852)    | 0 (0)                   | explorer.exe (72)   | Microsoft Office (16.0.11981.20174) | 1          | 0           | 2021-05-19 15:29:29 | 2021-05-19 15:29:34 | 5            | ... \Microsoft Office\root\Office16\EXCEL.EXE         |
|            | Code.exe (2876)     | 0 (0)                   | Code.exe (2864)     | Visual Studio Code (1.51.1)         | 1          | 0           | 2021-05-19 15:29:41 | [after selected]    |              | ... \Microsoft VS Code\Code.exe --typeUtility         |

## Scheduled Task Monitoring

July 9, 2024

uberAgent ESA monitors changes to Windows scheduled tasks. Whenever a task is created, updated, or deleted, uberAgent generates an event with all available details. This includes properties that are not displayed in the Windows Task Scheduler UI, such as COM actions or custom triggers.

## Configuration

uberAgent ESA scheduled task monitoring is enabled or disabled through the on-demand metric [ScheduledTaskMonitoring](#). In the [default configuration](#), scheduled task monitoring is enabled.

## Metadata

### Sourcetype

ESA scheduled task monitoring events are assigned the sourcetypes:

- `uberAgentESA:System:ScheduledTasks`
- `uberAgentESA:System:ScheduledTaskActions`
- `uberAgentESA:System:ScheduledTaskTriggers`

Please see the [metrics documentation](#) for a description of the fields.

## Visualization

ESA scheduled task monitoring events are visualized in the *Scheduled Tasks* dashboard which is part of the `uberAgent_ESA` Splunk searchhead app.

## Splunk Enterprise Security Integration

July 30, 2024

### Splunk Enterprise Security

Splunk Enterprise Security (ES) solves a wide range of security analytics and operations use cases including continuous security monitoring, advanced threat detection, compliance, incident investigation, forensics, and incident response. Splunk ES delivers an end-to-end view of organizations' security postures with flexible investigations, unmatched performance, and the most flexible deployment options offered in the cloud, on-premises, or hybrid deployment models.

Source: [Splunk](#)

## Integrating uberAgent ESA

uberAgent ESA comes with native support for Splunk Enterprise Security. This article summarizes all related information in one place.

### Installation

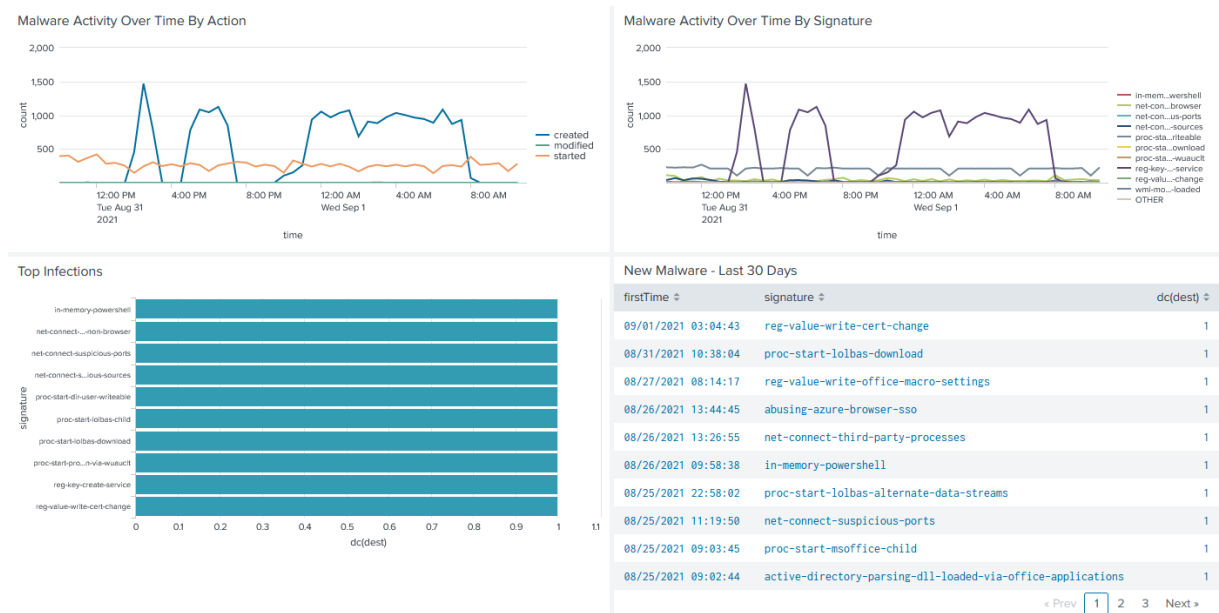
Detailed installation instructions can be found [here](#). In short, you need to install the following uberAgent apps on your ES server:

- **uberAgent\_searchhead.tgz**: contains uberAgent UXM CIM information
- **uberAgent\_ESA\_searchhead.tgz**: contains uberAgent ESA CIM information
- **uberAgent\_ESA\_ES\_companion.tgz**: required for Splunk’s risk-based alerting. Available on [Splunkbase](#).

### CIM Support

Splunk Enterprise Security works with data sources from many different vendors. This diverse data set needs to be normalized to allow users to search and interact with it in a standardized way. Splunk uses the [CIM data model](#) to achieve that.

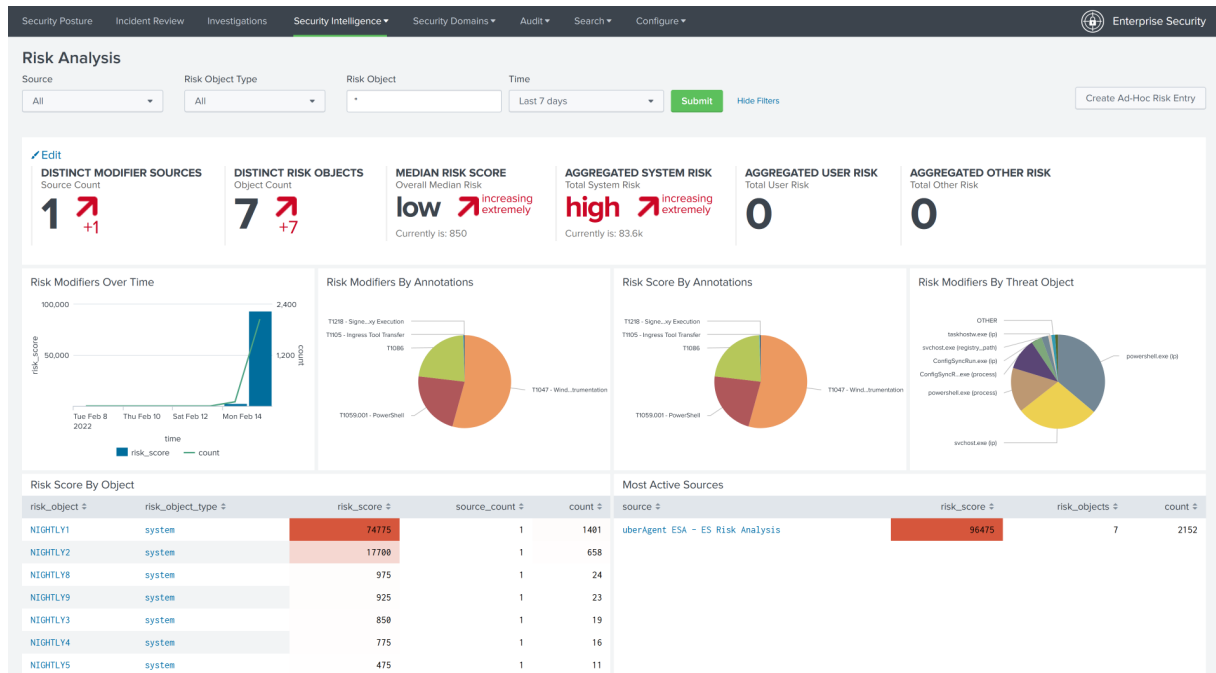
While uberAgent had CIM support for a long time, we have extended the integration greatly with uberAgent ESA. If you are used to working with Sysmon data in ES, you will notice no difference when switching to uberAgent. **uberAgent supports all CIM fields populated by popular Sysmon add-ons found in Splunkbase, and more!**



Visit our [blog post about the CIM integration](#) for details.

## Risk-Based Alerting

Splunk introduced **risk-based alerting (RBA)** in ES to reduce alert volume and enhance security operations. uberAgent supports RBA through the **uberAgent ESA ES companion** app. See the installation section above for installation instructions. When all requirements are met, the Splunk Enterprise Security dashboard **Risk Analysis** is populated automatically with uberAgent data:



**Security Frameworks** RBA supports annotations with cyber security frameworks like MITRE ATT&CK®, CIS 20, NIST Controls, and more. uberAgent does, too, and comes with ATT&CK annotation out-of-the-box. You may add other cyber security frameworks anytime.

Annotations are part of the ESA Threat Detection rule specification. Implementation details can be found [here](#). Below is a rule sample:

```

1 [ActivityMonitoringRule]
2 # Detects suspicious DNS queries known from Cobalt Strike beacons
3 RuleName = Cobalt Strike DNS Beacons
4 EventType = Dns.Query
5 Tag = cobalt-strike-dns-beacons
6 RiskScore = 100
7 Annotation = {
8 "mitre_attack": ["T1071", "T1071.004"] }
9
10 Query = (Dns.QueryRequest like r"aaa.stage.%" or Dns.QueryRequest like
11 r"post.1%")
12 GenericProperty1 = Dns.QueryRequest
13 GenericProperty2 = Dns.QueryResponse

```

## UXM Metrics

July 9, 2024

uberAgent UXM collects many different metrics, logically grouped into sourcetypes. All metrics are explained in detail in this chapter, including:

- Name and description
- Supported platform
- Unit and example
- Related source type and where to find it in the dashboards
- Calculated fields and their availability in Splunk's data model and/or "Search Processing Language" (SPL)
- Related settings in the [configuration file](#)

## Application Metrics

July 9, 2024

## Application Crashes & Hangs Metrics

November 25, 2024

### Application Errors

For every application error uberAgent collects metrics like application name and version, process lifetime as well as the exception code.

#### Notes:

- Processes are auto-grouped into applications, i.e., the application name is determined automatically. Information on how automatic application identification works is available [here](#).
- Field: `AppVersion` - uberAgent has an internal filter to minimize data volume by suppressing version information for system processes and system services. As a result, the `AppVersion` field is typically empty for most system processes and services.



## Details

- Source type: [uberAgent:Application:Errors](#)
- Used in dashboards: *Application Errors, Single Machine Detail, Single Application Detail, Single User Detail*
- Enabled through configuration setting: [ApplicationErrors](#)
- Related configuration settings: *n/a*
- Supported platform: *all* for application crashes, *Windows* for application hangs

## List of Fields in the Raw Agent Data

| Field         | Description                                                                                                        | Data type | Unit | Measurement |                                                             |          |
|---------------|--------------------------------------------------------------------------------------------------------------------|-----------|------|-------------|-------------------------------------------------------------|----------|
|               |                                                                                                                    |           |      | type        | Example                                                     | Platform |
| ErrorType     | Error type code.<br>Possible values: 1, 2.<br>Please take a look at the field <a href="#">ErrorTypeName</a> , too. | Number    |      | Snapshot    | 1                                                           | all      |
| ProcName      | Process name.                                                                                                      | String    |      | Snapshot    | chrome.exe                                                  | all      |
| ProcPath      | Process path.                                                                                                      | String    |      | Snapshot    | C:\Program Files (x86)\Google\Chrome\Application\chrome.exe | all      |
| ProcVersion   | Process version.                                                                                                   | String    |      | Snapshot    | 67.0.3396.99                                                | all      |
| ProcTimestamp | Build timestamp of the process binary, embedded PE header information.                                             | String    |      | Snapshot    | 2017-06-02 11:43:43.000 +0200                               | Windows  |

| Field              | Description                                                          | Data type | Unit | Measurement |                                     |          |
|--------------------|----------------------------------------------------------------------|-----------|------|-------------|-------------------------------------|----------|
|                    |                                                                      |           |      | type        | Example                             | Platform |
| ModuleName         | Faulting module name.                                                | String    |      | Snapshot    | msvcrt.dll                          | all      |
| ModulePath         | Faulting module path.                                                | String    |      | Snapshot    | C:\Windows\system32\msvcrt.dll      |          |
| ModuleVersion      | Faulting module version.                                             | String    |      | Snapshot    | 7.0.9600.17415                      | all      |
| ModuleTimestamp    | PE timestamp of the faulting module, embedded PE header information. | String    |      | Snapshot    | 2014-10-29 04:04:30.000 +0200       | Windows  |
| ProclD             | Process ID.                                                          | Number    |      | Snapshot    | 456                                 | all      |
| Proclifetime       | Process lifetime.                                                    | Number    | ms   | Sum         | 82744165                            | all      |
| ExceptionCode      | Exception code.                                                      | String    |      | Snapshot    | 0xc0000005                          | all      |
| FaultOffset        | An address offset relative to the base address of the crashed image. | String    |      | Snapshot    | 0x0000b5f0                          | all      |
| AppPackageFullName | UWP app full name. <a href="#">More information.</a>                 | String    |      | Snapshot    | Microsoft.XboxGameCallableUI_1000.1 | Windows  |

| Field                | Description                                                                                                          | Data type | Unit | Measurement |                                      |          |
|----------------------|----------------------------------------------------------------------------------------------------------------------|-----------|------|-------------|--------------------------------------|----------|
|                      |                                                                                                                      |           |      | type        | Example                              | Platform |
| AppPackageRelativeId | Microsoft UWP app relative ID. <a href="#">More information.</a>                                                     | String    |      | Snapshot    | xbox                                 | Windows  |
| AppId                | Associated application ID. Used by uberAgent to lookup application names and populate field <a href="#">AppName.</a> | String    |      | Snapshot    | GglChrm                              | all      |
| ProcUser             | Process user.                                                                                                        | String    |      | Snapshot    | Domain\JohnDoe                       | all      |
| SessionGUID          | Unique identifier that is generated by uberAgent when the session is created. Valid for this session only.           | String    |      | Snapshot    | 00000002-f295-9109-e7c7-c964011dd401 | all      |

| Field         | Description                                                                                                                                                                                                         | Data type | Unit | Measurement      |                                      |          |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------------|--------------------------------------|----------|
|               |                                                                                                                                                                                                                     |           |      | Measurement type | Example                              | Platform |
| ProcGUID      | Unique identifier that is generated by uberAgent when the process is started.                                                                                                                                       | String    |      | Snapshot         | 00000000-0599-6955-eb63-a00bb127d401 | all      |
| AppVersion    | Application version.                                                                                                                                                                                                | String    |      | Snapshot         | 67.0.3396.99                         | all      |
| HangType      | Hang type. Requires Windows 10 1903. Possible values: <a href="#">Cross-process</a> , <a href="#">Cross-thread</a> , <a href="#">Quiesce</a> , <a href="#">Top level window is idle</a> , <a href="#">Unknown</a> . | String    |      | Snapshot         | Cross-process                        | Windows  |
| ProclmageUUID | A unique identifier of the binary image that was executed.                                                                                                                                                          | String    |      | Snapshot         | D61D3713-69F9-32C3-B001-E509C0A8EE0A | macOS    |

| Field           | Description                                                        | Data type | Unit | Measurement type | Example                              | Platform |
|-----------------|--------------------------------------------------------------------|-----------|------|------------------|--------------------------------------|----------|
| ModuleImageUUID | Unique identifier of the binary image in which the crash occurred. | String    |      | Snapshot         | D61D3713-69F9-32C3-B001-E509C0A8EE0A | macOS    |

### List of Calculated Fields

| Field         | Description                                                                                                          | Data type | Unit | Measurement type | Where available               | Example        |
|---------------|----------------------------------------------------------------------------------------------------------------------|-----------|------|------------------|-------------------------------|----------------|
| ErrorTypeName | Display name of the <a href="#">ErrorType</a> field. Possible values: <a href="#">Crash</a> , <a href="#">Hang</a> . | String    |      | Snapshot         | Splunk data model, Splunk SPL | Hang           |
| User          | User name.                                                                                                           | String    |      | Snapshot         | Splunk data model             | Domain\JohnDoe |
| AppName       | Associated application name.                                                                                         | String    |      | Snapshot         | Splunk data model, Splunk SPL | Google Chrome  |

## Application Inventory & Usage Metrics

November 25, 2024

### Application Inventory

uberAgent collects application inventory information like name, publisher, version, and install date.

**Notes:**

- Processes are auto-grouped into applications, i.e. the application name is determined automatically without requiring any configuration. Information on how this works are available [here](#).
- Field: `AppVersion` - uberAgent has an internal filter to minimize data volume by suppressing version information for system processes and system services. As a result, the `AppVersion` field is typically empty for most system processes and services.

**Details**

- Source type: `uberAgent:Application:ApplicationInventory`
- Used in dashboards: *Application Inventory*, *Single Application Inventory*, *Single Machine Inventory*
- Enabled through configuration setting: `ApplicationInventory`
- Related configuration settings: *n/a*

**List of Fields in the Raw Agent Data**

| Field          | Description                                          | Data type | Unit | Measurement |          | Example       |
|----------------|------------------------------------------------------|-----------|------|-------------|----------|---------------|
|                |                                                      |           |      | type        | Platform |               |
| DisplayName    | Application name                                     | String    |      | Snapshot    | all      | Google Chrome |
| DisplayVersion | Application version                                  | String    |      | Snapshot    | all      | 67.0.3396.99  |
| Publisher      | Application publisher                                | String    |      | Snapshot    | all      | Google        |
| InstallDate    | Application installation date                        | String    |      | Snapshot    | all      | 2018-03-19    |
| Language       | Application language                                 | String    |      | Snapshot    | Win      | en-US         |
| IsMsiPackage   | Indicates if application was installed through a MSI | String    |      | Snapshot    | Win      | 1             |

| Field            | Description                                         | Data type | Unit | Measurement |          | Example                                 |
|------------------|-----------------------------------------------------|-----------|------|-------------|----------|-----------------------------------------|
|                  |                                                     |           |      | type        | Platform |                                         |
| IsMachineInstall | Indicates if application is installed for all users | String    |      | Snapshot    | all      | 1                                       |
| InstallLocation  | Application installation location                   | String    |      | Snapshot    | all      | C:\Program Files (x86)\Google\Chrome\Ap |

## Application Usage

**DEPRECATED:** this sourcetype is deprecated and will be removed in a future release. uberAgent's dashboards use the [ProcessDetail](#) sourcetype instead.

uberAgent collects application usage information like name (even for App-V, Java, and UWP apps), version, and number of concurrent users.

## Details

- Source type: [uberAgent:Application:ApplicationUsage](#)
- Used in dashboards: *Application Usage*
- Enabled through configuration setting: [ApplicationUsage](#)
- Related configuration settings: *n/a*

## List of Fields in the Raw Agent Data

| Field              | Description          | Data type | Unit | Measurement |          | Example        |
|--------------------|----------------------|-----------|------|-------------|----------|----------------|
|                    |                      |           |      | type        | Platform |                |
| AppName            | Application name     | String    |      | Snapshot    | all      | Google Chrome  |
| UserName           | User name            | String    |      | Snapshot    | all      | Domain\JohnDoe |
| AppVersion         | Application version  | String    |      | Snapshot    | all      | 67.0.3396.99   |
| RemotingClientName | Remoting client name | String    |      | Snapshot    | Win      | ThinClient1    |

## Application Name to ID Mapping Metrics

July 9, 2024

### Application Name to ID Mapping

uberAgent maps application names to IDs to save data volume sent over the network.

*Note:* processes are auto-grouped into applications, i.e. the application name is determined automatically without requiring any configuration. Information on how this works are available [here](#).

#### Details

- Source type: `uberAgent:Application:AppNameIdMapping`
- Used in dashboards: *n/a*
- Enabled through configuration setting: `AppNameIdMapping`
- Related configuration settings: *n/a*
- Supported platform: *all*

#### List of Fields in the Raw Agent Data

---

| Field   | Description                                                                                                              | Data type | Unit | Measurement type | Example          |
|---------|--------------------------------------------------------------------------------------------------------------------------|-----------|------|------------------|------------------|
| AppName | Application name.                                                                                                        | String    |      | Snapshot         | Google<br>Chrome |
| AppId   | Associated application ID.<br>Used by uberAgent to lookup application names and populate field <a href="#">AppName</a> . | Number    |      | Snapshot         | GlgChrm          |

---



## Application & Process Performance Metrics

November 25, 2024

### Process Detail

uberAgent collects rich metrics per process & per application. This includes the user and domain, CPU & RAM usage as well as network latency & throughput, to name just a few.

#### Notes:

- Processes are auto-grouped into applications, i.e., the application name is determined automatically. Information on how automatic application identification works is available [here](#).
- Field: `AppVersion` - uberAgent has an internal filter to minimize data volume by suppressing version information for system processes and system services. As a result, the `AppVersion` field is typically empty for most system processes and services.

#### Details

- Source type: `uberAgent:Process:ProcessDetail`
- Used in dashboards: *Process Performance, Application Performance, Machine Performance, Application Usage, Process GPU, Single Machine Detail, Single Application Detail, Single User Detail, Analyze data over time*
- Enabled through configuration setting: `ProcessDetailTop5` or `ProcessDetailFull`
- Related configuration settings: `[ProcessToApplicationMapping]`, `[ApplicationMappingIgnore]`, `[ProcessDetailFull_Filter]`, `[ProcessDetail_SendCommandline]`, `[ProcessStartupSettings]`

#### List of Fields in the Raw Agent Data

| Field    | Description   | Data type | Unit | Measurement |          |            |
|----------|---------------|-----------|------|-------------|----------|------------|
|          |               |           |      | type        | Platform | Example    |
| ProcName | Process name. | String    |      | Snapshot    | all      | chrome.exe |

| Field               | Description                                         | Data type | Unit | Measurement |          | Example |
|---------------------|-----------------------------------------------------|-----------|------|-------------|----------|---------|
|                     |                                                     |           |      | type        | Platform |         |
| ProcCPUTimeMs       | Process CPU usage (absolute usage in milliseconds). | Number    | ms   | Sum         | all      | 5000    |
| ProcCPUPercent      | Process CPU usage (relative usage in percent).      | Number    | %    | Average     | all      | 12      |
| ProcIOPSRead        | Process I/O read operations per second.             | Number    |      | Average     | Win      | 200     |
| ProcIOPSWrite       | Process I/O write operations per second.            | Number    |      | Average     | Win      | 200     |
| ProcIOPReadCount    | Process I/O read operation count.                   | Number    |      | Count       | Win      | 100     |
| ProcIOPWriteCount   | Process I/O write operation count.                  | Number    |      | Count       | Win      | 100     |
| ProcIOPReadMB       | Process I/O read data volume.                       | Number    | MB   | Sum         | all      | 150     |
| ProcIOPWriteMB      | Process I/O write data volume.                      | Number    | MB   | Sum         | all      | 150     |
| ProcIOLatencyReadMs | Rate of process I/O read operations.                | Number    | ms   | Average     | Win      | 300     |

| Field                 | Description                                                                                                               | Data type | Unit | Measurement |          | Example        |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------|-----------|------|-------------|----------|----------------|
|                       |                                                                                                                           |           |      | type        | Platform |                |
| ProcIOLatencyWriteMs  | Writes of process I/O write operations.                                                                                   | Number    | ms   | Average     | Win      | 300            |
| ProcWorkingSetMB      | Process RAM usage (working set).                                                                                          | Number    | MB   | Snapshot    | all      | 100            |
| ProcNetKBPS           | Process network traffic data volume per second.<br>macOS: includes payload + protocol overhead,<br>Windows: payload only. | Number    | KB/s | Sum         | all      | 500            |
| ProcUser              | Process user.                                                                                                             | String    |      | Snapshot    | all      | Domain\JohnDoe |
| ProcGpuComputePercent | Process GPU compute usage (relative usage in percent).                                                                    | Number    | %    | Average     | Win      | 20             |
| ProcGpuMemMB          | Process GPU memory usage.                                                                                                 | Number    | MB   | Average     | Win      | 150            |

| Field       | Description                                                                                                                                                      | Data type | Unit | Measurement |          | Example                                                                  |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-------------|----------|--------------------------------------------------------------------------|
|             |                                                                                                                                                                  |           |      | type        | Platform |                                                                          |
| AppId       | Associated application ID. Used by uberAgent to lookup application names and populate field <a href="#">AppName</a> .                                            | String    |      | Snapshot    | all      | GglChrm                                                                  |
| AppVersion  | Associated application version.                                                                                                                                  | String    |      | Snapshot    | all      | 67.0.3396.99                                                             |
| ProcID      | Process ID generated by the OS. Process IDs are reused and cannot be used to uniquely identify a process. Use <a href="#">ProcGUID</a> for that purpose instead. | Number    |      | Snapshot    | all      | 456                                                                      |
| ProcCmdline | The process' command line.                                                                                                                                       | String    |      | Snapshot    | all      | C:\Program Files (x86)\Google\Chrome\Ap<br>-url<br>http://vastlimits.com |

| Field                        | Description                                                              | Data type | Unit | Measurement |          | Example                                          |
|------------------------------|--------------------------------------------------------------------------|-----------|------|-------------|----------|--------------------------------------------------|
|                              |                                                                          |           |      | type        | Platform |                                                  |
| ProcGUID                     | Unique identifier for a process instance that is generated by uberAgent. | String    |      | Snapshot    | all      | 00000000-<br>ebe5-469c-<br>63ae-<br>f5a1de28d401 |
| ProcGpuEngineMostUsed        | The most used GPU engine (requires at least Windows 10 1709).            | Number    |      | Snapshot    | Win      | 1                                                |
| ProcGpuEngineMostUsedDisplay | The most used GPU engine (requires at least Windows 10 1709).            | String    |      | Snapshot    | Win      | 3D                                               |

| Field     | Description                                                                                                                                                         | Data type | Unit | Measurement |          | Example |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-------------|----------|---------|
|           |                                                                                                                                                                     |           |      | type        | Platform |         |
| SessionID | Session ID generated by the OS. Session IDs are reused and cannot be used to uniquely identify a session. Use <a href="#">SessionGUID</a> for that purpose instead. | Number    |      | Snapshot    | all      | 1       |

**Notes**

- The following fields are empty unless `EnableExtendedInfo` is set to true: `ProcGUID`.
- The following field is empty unless `EnableExtendedInfo` and `[ProcessDetail_SendCommandline]` are configured: `ProcCmdline`.

**List of Calculated Fields**

| Field       | Description                                                    | Data type | Unit | Measurement Where |                   | Example |
|-------------|----------------------------------------------------------------|-----------|------|-------------------|-------------------|---------|
|             |                                                                |           |      | type              | available         |         |
| ProcCPUTime | Process CPU usage (absolute usage in seconds).                 | Number    | s    | Sum               | Splunk data model | 5       |
| ProcIOCount | <code>ProcIOReadCount</code> + <code>ProcIOWriteCount</code> . | String    |      | Sum               | Splunk data model | 200     |

| Field                 | Description                                           | Data type | Unit | Measurement type | Where available   | Example        |
|-----------------------|-------------------------------------------------------|-----------|------|------------------|-------------------|----------------|
| ProcIOPS              | ProcIOPSRead<br>+<br>ProcIOPSWrite<br>.               | Number    |      | Sum              | Splunk data model | 400            |
| ProcIOMB              | ProcIOReadMB<br>+<br>ProcIOWriteMB<br>.               | Number    | MB   | Sum              | Splunk data model | 300            |
| ProcIOMBPS            | ProcIOMB<br>/<br>ProcIOCount<br>x<br>ProcIOPS<br>.    | Number    | MB   | Sum              | Splunk data model | 600            |
| ProcIOLatencyMs       | ProcIOLatencyReadMs<br>+<br>ProcIOLatencyWriteMs<br>. | Number    | ms   | Sum              | Splunk data model | 600            |
| ProcIODurationReadMS  | ProcIOLatencyRead<br>x<br>ProcIOCountRead<br>.        | Number    | ms   | Sum              | Splunk data model | 30000          |
| ProcIODurationWriteMS | ProcIOLatencyWrite<br>x<br>ProcIOCountWrite<br>.      | Number    | ms   | Sum              | Splunk data model | 30000          |
| ProcIODurationMS      | ProcIODurationRead<br>+<br>ProcIODurationWriteMS<br>. | Number    | ms   | Sum              | Splunk data model | 60000          |
| User                  | Alias for ProcUser<br>.                               | String    |      | Snapshot         | Splunk data model | Domain\JohnDoe |

| Field   | Description                    | Data type | Unit | Measurement type | Where available               | Example                       |
|---------|--------------------------------|-----------|------|------------------|-------------------------------|-------------------------------|
| AppName | Associated application name.   | String    |      | Snapshot         | Splunk data model, Splunk SPL | Google Chrome                 |
| time    | Alias for <code>_time</code> . | Number    |      | Snapshot         | Splunk data model             | 2018-07-31T18:34:32.451+02:00 |

## Process Statistics

uberAgent collects rich metrics per process. This includes the handle count, page faults, and priority, to name just a few.

### Notes:

- Processes are auto-grouped into applications, i.e., the application name is determined automatically. Information on how automatic application identification works is available [here](#).

### Details

- Source type: `uberAgent:Process:ProcessStatistics`
- Used in dashboards: *Process Performance*, *Application Performance*, *Single Application Detail*, *Analyze data over time*
- Enabled through configuration setting: `ProcessStatistics`
- Related configuration settings:

## List of Fields in the Raw Agent Data

| Field    | Description   | Data type | Unit | Measurement type | Platform | Example    |
|----------|---------------|-----------|------|------------------|----------|------------|
| ProcName | Process name. | String    |      | Snapshot         | Win      | chrome.exe |



---

| Field    | Description                                                                                                                                                      | Data type | Unit | Measurement |          | Example                                          |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-------------|----------|--------------------------------------------------|
|          |                                                                                                                                                                  |           |      | type        | Platform |                                                  |
| ProcID   | Process ID generated by the OS. Process IDs are reused and cannot be used to uniquely identify a process. Use <a href="#">ProcGUID</a> for that purpose instead. | Number    |      | Snapshot    | Win      | 456                                              |
| ProcGUID | Unique identifier for a process instance that is generated by uberAgent.                                                                                         | String    |      | Snapshot    | Win      | 00000000-<br>ebe5-469c-<br>63ae-<br>f5a1de28d401 |
| ProcUser | Process user.                                                                                                                                                    | String    |      | Snapshot    | Win      | Domain\JohnDoe                                   |
| AppId    | Associated application ID. Used by uberAgent to lookup application names and populate field <a href="#">AppName</a> .                                            | String    |      | Snapshot    | Win      | GglChrm                                          |

| Field             | Description                                                                                                                                                                       | Data type | Unit | Measurement |          | Example |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-------------|----------|---------|
|                   |                                                                                                                                                                                   |           |      | type        | Platform |         |
| ProcHandleCount   | Process handle count.                                                                                                                                                             | Number    |      | Snapshot    | Win      | 810     |
| ProcThreadCount   | Process thread count.                                                                                                                                                             | Number    |      | Snapshot    | Win      | 20      |
| ProcPriority      | Process priority.<br>Valid values: 0, 1, 2, 3, 4, 5 or 6. The numerical priority is used by uberAgent to look up and populate the field <a href="#">ProcPriorityDisplayName</a> . | Number    |      | Snapshot    | Win      | 4       |
| ProcPrivateMB     | Process allocated private memory.                                                                                                                                                 | Number    | MB   | Snapshot    | Win      | 512     |
| ProcVirtualSizeMB | Process allocated virtual memory.                                                                                                                                                 | Number    | MB   | Snapshot    | Win      | 128     |
| ProcPageFaultsPS  | Process page faults per second.                                                                                                                                                   | Number    | s    | Average     | Win      | 10      |
| ProcPageFileMB    | Process page file usage.                                                                                                                                                          | Number    | MB   | Snapshot    | Win      | 256     |

## List of Calculated Fields

| Field                     | Description                                                                                                                                                 | Data type | Unit | Measurement type | Where available               | Example      |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------------|-------------------------------|--------------|
| ProcPriorityDisplayAsName | Process priority display name (see also <a href="#">ProcPriority</a> ). Valid values: Above normal, Below normal, High, Idle, Normal, Realtime and Unknown. | String    |      | Snapshot         | Splunk data model, Splunk SPL | Above normal |

## Application & Process Startup Metrics

November 25, 2024

### Process Startup

For each application or process that is being launched, uberAgent collects metrics like startup performance (duration, IOPS), as well as process properties (e.g., elevation status). If the configuration setting [EnableExtendedInfo](#) is enabled, uberAgent also collects metrics like the full path to the process executable in the file system as well the full command line the process was launched with.

#### Notes:

- As with all other metrics, process startup duration is recorded automatically without requiring any configuration. uberAgent optionally only shows new processes never seen before in the Splunk dashboards.
- Processes are auto-grouped into applications, i.e., the application name is determined automatically. Information on how automatic application identification works is available [here](#).
- Field: `AppVersion` - uberAgent has an internal filter to minimize data volume by suppressing version information for system processes and system services. As a result, the `AppVersion` field is typically empty for most system processes and services.

### Details

- Source type: `uberAgent:Process:ProcessStartup`
- Used in dashboards: *Application Startup*, *Process Startup*, *Single Application Detail*, *Analyze data over time*
- Enabled through configuration setting: `ProcessStartup`
- Related configuration settings: [`ProcessStartupSettings`], [`ProcessStartupDurationWaitI` ]

### List of Fields in the Raw Agent Data

| Field                      | Description                                                         | Data type | Unit | Measurement |          | Example                     |
|----------------------------|---------------------------------------------------------------------|-----------|------|-------------|----------|-----------------------------|
|                            |                                                                     |           |      | type        | Platform |                             |
| <code>ProcName</code>      | Process name.                                                       | String    |      | Snapshot    | all      | <code>chrome.exe</code>     |
| <code>ProcUser</code>      | Process user.                                                       | String    |      | Snapshot    | all      | <code>Domain\JohnDoe</code> |
| <code>StartupTimeMs</code> | Startup time duration (how long it took the process to initialize). | Number    | ms   | Sum         | Win      | 300                         |

| Field       | Description                                                                                                                                                      | Data type | Unit | Measurement |          | Example |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-------------|----------|---------|
|             |                                                                                                                                                                  |           |      | type        | Platform |         |
| StartupIOPS | I/O operations per second generated during the process' startup phase (see <a href="#">StartupTimeMs</a> .                                                       | Number    |      | Count       | Win      | 150     |
| AppId       | Associated application ID. Used by uberAgent to look up the application name and populate the field <a href="#">AppName</a> .                                    | String    |      | Snapshot    | all      | GglChrm |
| ProcID      | Process ID generated by the OS. Process IDs are reused and cannot be used to uniquely identify a process. Use <a href="#">ProcGUID</a> for that purpose instead. | Number    |      | Snapshot    | all      | 456     |

---

| Field        | Description                                                                                                                                                                                                                                                                  | Data type | Unit | Measurement |          | Example |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-------------|----------|---------|
|              |                                                                                                                                                                                                                                                                              |           |      | type        | Platform |         |
| ProcParentID | Parent process ID (also see <a href="#">ProcID</a> ).                                                                                                                                                                                                                        | Number    |      | Snapshot    | all      | 789     |
| SessionID    | Session ID generated by the OS. Session IDs are reused and cannot be used to uniquely identify a session. Use <a href="#">SessionGUID</a> for that purpose instead. macOS: for consistency with Windows all non-user sessions are assigned to a fictitious system session 0. | Number    |      | Snapshot    | all      | 3       |

| Field          | Description                                                              | Data type | Unit | Measurement |          | Example                                                                        |
|----------------|--------------------------------------------------------------------------|-----------|------|-------------|----------|--------------------------------------------------------------------------------|
|                |                                                                          |           |      | type        | Platform |                                                                                |
| ProcGUID       | Unique identifier for a process instance that is generated by uberAgent. | String    |      | Snapshot    | all      | 00000000-<br>ebe5-469c-<br>63ae-<br>f5a1de28d401                               |
| SessionGUID    | Unique identifier for a session that is generated by uberAgent.          | String    |      | Snapshot    | Win      | 00000002-<br>f295-9109-<br>e7c7-<br>c964011dd401                               |
| ProcParentName | Parent process name.                                                     | String    |      | Snapshot    | all      | powershell.exe                                                                 |
| ProcPath       | Full path to the process executable in the file system.                  | String    |      | Snapshot    | all      | C:\Windows\System32\W                                                          |
| ProcCmdline    | The process' command line.                                               | String    |      | Snapshot    | all      | C:\Program<br>Files<br>(x86)\Google\Chrome\Ap<br>-url<br>http://vastlimits.com |
| IsElevated     | Indicates if the process is elevated (has admin rights).                 | String    |      | Snapshot    | all      | 1                                                                              |

| Field          | Description                                                                                                                                                        | Data type | Unit | Measurement |          | Example                              |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-------------|----------|--------------------------------------|
|                |                                                                                                                                                                    |           |      | type        | Platform |                                      |
| AppVersion     | Associated application version.                                                                                                                                    | String    |      | Snapshot    | all      | 67.0.3396.99                         |
| ProcParentGUID | Unique identifier of the parent process (the parent's <a href="#">ProcGUID</a> ).                                                                                  | String    |      | Snapshot    | all      | 00000000-ebe5-469c-54ae-f5a1de28d401 |
| IsProtected    | Indicates whether the process is protected ( <a href="#">PsProtectedTypeProtected</a> ) or protected light ( <a href="#">PsProtectedTypeProtectedLight</a> , PPL). | String    |      | Snapshot    | Win      | 1                                    |
| HashMD5        | MD5 hash of the process executable (requires ESA).                                                                                                                 | String    |      | Snapshot    | Win      | 7FFE122B109F1B586DEA                 |
| HashSHA1       | SHA1 hash of the process executable (requires ESA).                                                                                                                | String    |      | Snapshot    | Win      | 26DBC241A37881072689                 |



| Field              | Description                                                                                                                         | Data type | Unit | Measurement |          | Example              |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-------------|----------|----------------------|
|                    |                                                                                                                                     |           |      | type        | Platform |                      |
| HashSHA256         | SHA256 hash of the process executable (requires ESA).                                                                               | String    |      | Snapshot    | Win      | 95F0FBBAEF2899923859 |
| HashIMP            | Importable hash of the process executable (requires ESA).                                                                           | String    |      | Snapshot    | Win      | 188392D5FBCC485811BE |
| SignatureStatus    | Authenticode signature status. Can be 0, 1, 2, 3, 4, 5, 6 or 7. See also <a href="#">SignatureStatusDisplayName</a> . Requires ESA. | String    |      | Snapshot    | Win      | 1                    |
| IsSignedByOSVendor | Indicates whether the Authenticode signer is the OS manufacturer (e.g., Microsoft). Requires ESA.                                   | String    |      | Snapshot    | Win      | 1                    |
| SignerName         | Authenticode signer name (requires ESA).                                                                                            | String    |      | Snapshot    | Win      | Microsoft Windows    |

### Notes

- The following fields are empty unless `EnableExtendedInfo` is set to true: `ProcID`, `ProcParentID`, `SessionID`, `ProcGUID`, `SessionGUID`, `ProcParentName`, `ProcPath`, `ProcCmdline`, `ProcParentGUID`.
- The maximum supported timer `Interval` for the `ProcessStartup` metric is 300000 (5 minutes).

### List of Calculated Fields

| Field           | Description                                                                                                                                                                                                                  | Data type | Unit | Measurement type | Where available               | Example        |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------------|-------------------------------|----------------|
| User            | Alias for <code>ProcUser</code> .                                                                                                                                                                                            | String    |      | Snapshot         | Splunk data model             | Domain\JohnDoe |
| StartupTimeS    | Startup time duration.                                                                                                                                                                                                       | Number    | s    | Sum              | Splunk data model             | 0.3            |
| StartupIOCount  | $\text{StartupIOPS} * \text{StartupTimeMs} / 1000$ .                                                                                                                                                                         | Number    |      | Sum              | Splunk data model             | 45             |
| AppName         | Associated application name.                                                                                                                                                                                                 | String    |      | Snapshot         | Splunk data model, Splunk SPL | Google Chrome  |
| SignatureStatus | Display Name values: <code>Unknown</code> , <code>Ok</code> , <code>Revoked</code> , <code>Expired</code> , <code>InvalidHash</code> , <code>UntrustedRoot</code> , <code>TrustedRootNotInCA</code> and <code>Error</code> . | String    |      | Snapshot         | Splunk data model             | Ok             |

## Application UI Unresponsiveness Metrics

November 25, 2024

### UI Unresponsiveness

Whenever an application's user interface is unresponsive for more than a few hundred milliseconds uberAgent collects information like the application name (even for App-V, Java, and UWP apps), application version and the unresponsiveness duration.

#### Notes:

- Processes are auto-grouped into applications, i.e. the application name is determined automatically without requiring any configuration. Information on how this works are available [here](#).
- Field: `AppVersion` - uberAgent has an internal filter to minimize data volume by suppressing version information for system processes and system services. As a result, the `AppVersion` field is typically empty for most system processes and services.

#### Details

- Source type: `uberAgent:Application:UIDelay`
- Used in dashboards: *Application UI Unresponsiveness, Process UI Unresponsiveness, \_\_Single Machine Detail, Single Application Detail, Single User Detail*
- Enabled through configuration setting: `ApplicationUIDelay`
- Related configuration settings: *n/a*
- Supported platform: *Windows*

#### List of Fields in the Raw Agent Data

| Field       | Description                                                                                                           | Data type | Unit | Measurement type | Example                              |
|-------------|-----------------------------------------------------------------------------------------------------------------------|-----------|------|------------------|--------------------------------------|
| AppId       | Associated application ID. Used by uberAgent to lookup application names and populate field <a href="#">AppName</a> . | String    |      | Snapshot         | GglChrm                              |
| AppVersion  | Application version.                                                                                                  | String    |      | Snapshot         | 67.0.3396.99                         |
| ProcessName | Process name.                                                                                                         | String    |      | Snapshot         | chrome.exe                           |
| ProcessId   | Process ID.                                                                                                           | Number    |      | Snapshot         | 456                                  |
| UIDelayMs   | UI delay/unresponsiveness.                                                                                            | Number    | ms   | Sum              | 5000                                 |
| User        | User name.                                                                                                            | String    |      | Snapshot         | Domain\JohnDoe                       |
| SessionGUID | Unique identifier that is generated by uberAgent when the session is created. Valid for this session only.            | String    |      | Snapshot         | 00000002-f295-9109-e7c7-c964011dd401 |
| HasFocus    | Indicates if the application is in the foreground (is being used actively). Possible values: 0, 1.                    | String    |      | Snapshot         | 1                                    |

### List of Calculated Fields

| Field          | Description                                                                                        | Data type | Unit | Measurement type | Where available               | Example       |
|----------------|----------------------------------------------------------------------------------------------------|-----------|------|------------------|-------------------------------|---------------|
| AppName        | Associated application name.                                                                       | String    |      | Snapshot         | Splunk data model, Splunk SPL | Google Chrome |
| UIDelayS       | UI delay/un-responsiveness.                                                                        | Number    | s    | Sum              | Splunk data model             | 5             |
| HasFocusNumber | Indicates if the application is in the foreground (is being used actively). Possible values: 0, 1. | Number    |      | Snapshot         | Splunk data model             | 1             |
| ProcName       | Process name.                                                                                      | String    |      | Snapshot         | Splunk data model             | chrome.exe    |

## Software Update Metrics

July 9, 2024

### Software Update

uberAgent collects the name and install date per update.

#### Details

- Source type: [uberAgent:Application:SoftwareUpdateInventory](#)
- Used in dashboards: [Update inventory](#), [Single Machine Detail](#), [Single Update Detail](#)

- Enabled through configuration setting: [SoftwareUpdateInventory](#)
- Related configuration settings: *n/a*
- Supported platform: *Windows*

### List of Fields in the Raw Agent Data

| Field       | Description                                                                                                         | Data type | Unit | Measurement type | Example                                                             |
|-------------|---------------------------------------------------------------------------------------------------------------------|-----------|------|------------------|---------------------------------------------------------------------|
| Guid        | GUID.                                                                                                               | String    |      | Snapshot         | AC76BA86-7AD7-0000-2550-AC120B4E4800                                |
| DisplayName | Update name.                                                                                                        | String    |      | Snapshot         | KB2565063                                                           |
| ProductName | Product name.                                                                                                       | String    |      | Snapshot         | Microsoft Visual C++ 2010 x86 Re-distributable - 10.0.40219 applied |
| State       | Update state.<br>Possible values: <a href="#">applied</a> , <a href="#">superseded</a> , <a href="#">obsolete</a> . | String    |      | Snapshot         |                                                                     |
| InstallDate | Installation date.                                                                                                  | String    |      | Snapshot         | 2018-04-13                                                          |

### Browser Metrics

July 9, 2024

### Google Chrome Metrics

November 25, 2024

## Google Chrome

uberAgent collects performance data per Chrome (Edge) process type like Browser (main process) or GPU (graphics acceleration).

### Details

- Source type: `uberAgent:Application:BrowserPerformanceChrome`
- Used in dashboards: *Browser Performance: Chrome, Browser Performance: Edge, Analyse data over time*
- Enabled through configuration setting: `BrowserPerformanceChrome,BrowserPerformanceEdge,BrowserPerformanceCEB`
- Related configuration settings: *n/a*
- Supported platform: *Windows*

### List of Fields in the Raw Agent Data

| Field      | Description                                                                                                                                                                        | Data type | Unit | Example        |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|----------------|
| ProcUser   | User who ran the process.                                                                                                                                                          | String    |      | Domain\JohnDoe |
| ProcType   | Process type.<br>Possible values:<br><code>Browser</code> ,<br><code>Extension</code> ,<br><code>Flash</code> ,<br><code>GPU</code> ,<br><code>Java</code> ,<br><code>Tab</code> . | String    |      | Tab            |
| CPUTimeMs  | Consumed CPU time.                                                                                                                                                                 | Number    | ms   | 11859          |
| CPUPercent | Consumed CPU performance.                                                                                                                                                          | Number    |      | 5.05           |
| IOPS       | I/O operations per second.                                                                                                                                                         | Number    |      | 2000           |
| IOCount    | Count of I/O operations.                                                                                                                                                           | Number    |      | 500            |
| IOMB       | Amount of data I/O operation volume.                                                                                                                                               | Number    | MB   | 200            |

| Field        | Description                                                | Data type | Unit | Example |
|--------------|------------------------------------------------------------|-----------|------|---------|
| IOLatencyMs  | I/O operation duration divided by count of I/O operations. | Number    | ms   | 1.20    |
| WorkingSetMB | Consumed RAM.                                              | Number    | MB   | 68.08   |
| NetKBPS      | Generated network traffic.                                 | Number    | KB   | 19.06   |

### List of Calculated Fields

| Field        | Description                                     | Data type | Unit | Example        | Where available   |
|--------------|-------------------------------------------------|-----------|------|----------------|-------------------|
| User         | User who ran the process.                       | String    |      | Domain\JohnDoe | Splunk data model |
| CPUTimeS     | Consumed CPU time.                              | Number    | s    | 11.859         | Splunk data model |
| IOMBPS       | Amount of data I/O operation volume per second. | Number    | MB   | 2              | Splunk data model |
| IODurationMs | I/O operation duration.                         | Number    | ms   | 600            | Splunk data model |

## Internet Explorer Metrics

July 9, 2024

### Internet Explorer

Contains metrics per website (URL) like CPU and RAM usage.



**Details**

- Source type: `uberAgent:Application:BrowserPerformanceIE`
- Used in dashboards: *Browser Performance: Internet Explorer, Analyze data over time*
- Enabled through configuration setting: `BrowserPerformanceIE`
- Related configuration settings: *n/a*
- Supported platform: *Windows*

**List of Fields in the Raw Agent Data**

---

| Field        | Description                                                                                                    | Data type | Unit | Example                                                             |
|--------------|----------------------------------------------------------------------------------------------------------------|-----------|------|---------------------------------------------------------------------|
| ProcID       | Process ID.                                                                                                    | Number    |      | 456                                                                 |
| ProcType     | Process type.<br>Possible values:<br><code>frame</code> ,<br><code>undefined</code> ,<br><code>worker</code> . | String    |      | frame                                                               |
| URL          | URL.                                                                                                           | String    |      | <a href="https://www.vastlimits.com">https://www.vastlimits.com</a> |
| CPUTimeMs    | Consumed CPU time.                                                                                             | Number    | ms   | 11859                                                               |
| CPUPercent   | Consumed CPU performance.                                                                                      | Number    | %    | 5.05                                                                |
| IOPS         | I/O operations per second.                                                                                     | Number    |      | 2000                                                                |
| IOCount      | Count of I/O operations.                                                                                       | Number    |      | 500                                                                 |
| IOMB         | Amount of data I/O operation volume.                                                                           | Number    | MB   | 200                                                                 |
| IOLatencyMs  | I/O operation duration divided by count of I/O operations.                                                     | Number    | ms   | 1.20                                                                |
| WorkingSetMB | Consumed RAM.                                                                                                  | Number    | MB   | 68.08                                                               |
| NetKBPS      | Generated network traffic.                                                                                     | Number    | KB   | 19.06                                                               |

---

### List of Calculated Fields

| Field        | Description                                     | Data type | Unit | Example            | Where available   |
|--------------|-------------------------------------------------|-----------|------|--------------------|-------------------|
| URLHost      | URL host address.                               | String    |      | www.vastlimits.com | Splunk data model |
| CPUTimeS     | Consumed CPU time.                              | Number    | s    | 11.859             | Splunk data model |
| IOMBPS       | Amount of data I/O operation volume per second. | Number    | MB   | 2                  | Splunk data model |
| IODurationMs | I/O operation duration.                         | Number    | ms   | 600                | Splunk data model |

## Web App Metrics

November 25, 2024

### Browser Web Requests

uberAgent determines UX metrics for SaaS and web apps like page load and XMLHttpRequest duration for every web request made.

#### Details

- Source type: [uberAgent:Application:BrowserWebRequests2](#)
- Used in dashboards: *Browser Web App Performance*
- Enabled through configuration setting: [BrowserPerformanceChrome](#), [BrowserPerformanceEdge](#), [BrowserPerformanceFirefox](#), [BrowserPerformanceIE](#)
- Related configuration settings: [[BrowserWebAppURL\\_Filter](#)]
- Supported platforms: *all*

### List of Fields in the Raw Agent Data

| Field          | Description                                                                                                                                           | Data type | Unit | Example        |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|----------------|
| Browser        | Browser ID.<br>Possible values:<br>1, 2, 3,4. Also see<br>the field<br><a href="#">BrowserDisplayName</a><br>below.                                   | Number    |      | 1              |
| BrowserVersion | Browser version.                                                                                                                                      | String    |      | 69.0.3497.81   |
| IsFrame        | Indicates if a page<br>is a frame or not.<br>Possible values:<br>0, 1.                                                                                | String    |      | 1              |
| ProcUser       | User who ran the<br>process.                                                                                                                          | String    |      | Domain\JohnDoe |
| TabHost        | Host address of<br>the entered URL.                                                                                                                   | String    |      | vastlimits.com |
| TabUriScheme   | Uri scheme ID of<br>the entered URL.<br>Possible values:<br>0, 1, 2, 3, 4. Also<br>see the field<br><a href="#">TabUriSchemeDisplayName</a><br>below. | Number    |      | 3              |
| RequestType    | Type of the<br>requested URL.<br>Possible values:<br>0, 1, 2, 3. Also<br>see the field<br><a href="#">RequestTypeDisplayName</a><br>below.            | String    |      | 1              |
| RequestHost    | Host address<br>which was<br>requested by the<br><a href="#">TabHost</a><br>address.                                                                  | String    |      | uberagent.com  |

---

| Field                   | Description                                                                                                                               | Data type | Unit | Example |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|---------|
| RequestUriScheme        | Uri scheme ID of the requested URL. Possible values: 0, 1, 2, 3, 4. Also see the field <a href="#">RequestUriSchemeDisplayName</a> below. | Number    |      | 3       |
| RequestCount            | Total count of requests                                                                                                                   | Number    |      | 40      |
| WebRequestDuration      | Duration for all web requests. Does not work with Internet Explorer.                                                                      | Number    | ms   | 140     |
| PageLoadTotalDuration   | Total duration for page load.                                                                                                             | Number    | ms   | 300     |
| PageLoadNetworkDuration | Network duration for page load.                                                                                                           | Number    | ms   | 150     |
| PageLoadRenderDuration  | Render duration for page load.                                                                                                            | Number    | ms   | 150     |
| HttpStatusCount2xx      | Count of 2xx http errors.                                                                                                                 | Number    |      | 2       |
| HttpStatusCount3xx      | Count of 3xx http errors.                                                                                                                 | Number    |      | 3       |
| HttpStatusCount4xx      | Count of 4xx http errors.                                                                                                                 | Number    |      | 4       |
| HttpStatusCount5xx      | Count of 5xx http errors.                                                                                                                 | Number    |      | 5       |

---

### List of Calculated Fields

| Field                   | Description                                                                                           | Data type | Unit | Example        | Where available                  |
|-------------------------|-------------------------------------------------------------------------------------------------------|-----------|------|----------------|----------------------------------|
| BrowserDisplay          | Browser name.<br>Possible values:<br>Chrome,<br>Internet Explorer,<br>Firefox,<br>Edge.               | String    |      | Chrome         | Splunk data model,<br>Splunk SPL |
| User                    | User name.                                                                                            | String    |      | Domain\JohnDoe | Splunk data model                |
| TabUriSchemeDisplay     | URI scheme name of the entered URL.<br>Possible values:<br>Other, http,<br>https, ftp,<br>file.       | String    |      | https          | Splunk data model,<br>Splunk SPL |
| RequestUriSchemeDisplay | URI scheme name of the requested URL. Possible values:<br>Other, http,<br>https, ftp,<br>file.        | String    |      | https          | Splunk data model,<br>Splunk SPL |
| RequestTypeDisplay      | Type of the requested URL. Possible values:<br>Unknown,<br>XmlHttpRequest,<br>WebSocket,<br>PageLoad. | String    |      | XmlHttpRequest | Splunk data model,<br>Splunk SPL |

## Citrix NetScaler (ADC) Metrics

July 30, 2024

Citrix NetScaler (ADC) monitoring requires its metrics to be enabled on at least one machine. See the [documentation](#) for details.

### Appliance Inventory

uberAgent collects metrics like MAC address, model, and version for the primary as well as the secondary appliance.

#### Details

- Source type: `uberAgent:CitrixADC:ApplianceInventory`
- Used in dashboards: *CitrixADC Inventory*, *Single CitrixADC Inventory*
- Enabled through configuration setting: `CitrixADCInventory`
- Related configuration settings: `[CitrixADC_Config]`
- Supported platform: *Windows*

#### List of Fields in the Raw Agent Data

| Field         | Description                                                                                                | Data type | Unit | Example                                          |
|---------------|------------------------------------------------------------------------------------------------------------|-----------|------|--------------------------------------------------|
| HostName      | Appliance name.                                                                                            | String    |      | CitrixADC1                                       |
| Version       | Firmware version.                                                                                          | String    |      | NS12.0: Build 59.8.nc Date: Sep 12 2018 06:16:17 |
| License       | Installed license.                                                                                         | String    |      | Platinum                                         |
| Model         | Appliance model.                                                                                           | Number    |      | 1000                                             |
| LicensingMode | Configured licensing mode. Possible values: <code>Local</code> , <code>Pooled</code> , <code>CICO</code> . | String    |      | Local                                            |
| HwDescription | Hardware and its ports detail.                                                                             | String    |      | NetScaler Virtual Appliance.                     |

| Field                 | Description                                                     | Data type | Unit | Example                                 |
|-----------------------|-----------------------------------------------------------------|-----------|------|-----------------------------------------|
| SysId                 | System id.                                                      | String    |      | 450088                                  |
| ManufactureDay        | Day the appliance was manufactured.                             | Number    |      | 17                                      |
| ManufactureMonth      | Month the appliance was manufactured.                           | Number    |      | 2                                       |
| ManufactureYear       | Year the appliance was manufactured.                            | Number    |      | 2009                                    |
| CpuFrequency          | CPU frequency.                                                  | Number    |      | 3890                                    |
| SerialNo              | Serial number.                                                  | Number    |      | ABCDEFG12                               |
| EncodedSerialNo       | Encoded serial number.                                          | String    |      | 68310055cb267307ffg8                    |
| MACAddress            | MAC address.                                                    | String    |      | 00155d3d890d                            |
| HostId                | Host id.                                                        | String    |      | 123456789                               |
| LastConfigSaveTime    | Time when the configuration was last saved.                     | String    |      | 2018-12-07<br>12:06:36                  |
| Timezone              | Timezone.                                                       | String    |      | GMT+01:00-CET-Europe/Berlin<br>password |
| WeakPassword          | List of all weak passwords.                                     | String    |      |                                         |
| SystemType            | System type.<br>Possible Values:<br>Standalone,<br>HA, Cluster. | String    |      | HA                                      |
| LastConfigChangedTime | Time when the configuration was last changed.                   | String    |      | 2018-12-07<br>12:06:21                  |
| LastStartupTime       | Time when the appliance was last started.                       | String    |      | 2018-11-24<br>15:26:25                  |

| Field                  | Description                                                                                                                                           | Data type | Unit | Example                |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------------------|
| CurrentHAStatus        | Indicates the high availability state of the node.<br>Possible values:<br>Staysecondary<br>, Primary,<br>Secondary,<br>Claiming,<br>Force change<br>. | String    |      | Primary                |
| LastHAStatusChangeTime | Time when the last master state transition occurred.                                                                                                  | String    |      | 2018-12-04<br>10:34:51 |
| SSLCards2              | Number of available SSL cards.                                                                                                                        | Number    |      | 0                      |
| SSLCardsUp2            | Number of working SSL cards.                                                                                                                          | Number    |      | 0                      |

### List of Calculated Fields

| Field      | Description                    | Data type | Unit | Example | Where available   |
|------------|--------------------------------|-----------|------|---------|-------------------|
| SSLCards   | Number of available SSL cards. | Number    |      | 0       | Splunk data model |
| SSLCardsUp | Number of working SSL cards.   | Number    |      | 0       | Splunk data model |

### Appliance Performance

uberAgent collects metrics like CPU usage, RAM usage as well as network throughput for the primary appliance.



## Details

- Source type: `uberAgent:CitrixADC:AppliancePerformance`
- Used in dashboards: *CitrixADC Appliance Performance*
- Enabled through configuration setting: `CitrixADCPerformance`
- Related configuration settings: `[CitrixADC_Config]`
- Supported platform: *Windows*

## List of Fields in the Raw Agent Data

| Field                  | Description                      | Data type | Unit  | Example    |
|------------------------|----------------------------------|-----------|-------|------------|
| HostName               | Appliance name.                  | String    |       | CitrixADC1 |
| MemUsagePcnt           | Memory usage.                    | Number    | %     | 17.62      |
| MgmtCpuUsagePcnt       | Management CPU usage.            | Number    | %     | 14.6       |
| PktCpuUsagePcnt        | Packet CPU usage.                | Number    | %     | 3          |
| Disk0PerUsage          | /flash disk usage.               | Number    | %     | 41         |
| Disk0Size              | /flash disk size.                | Number    | MB    | 1585       |
| Disk0Used              | /flash disk allocated space.     | Number    | MB    | 598        |
| Disk0Avail             | /flash disk free space.          | Number    | MB    | 860        |
| Disk1PerUsage          | /var disk usage.                 | Number    | %     | 45         |
| Disk1Size              | /var disk size.                  | Number    | MB    | 14179      |
| Disk1Used              | /var disk allocated space.       | Number    | MB    | 5988       |
| Disk1Avail             | /var disk free space.            | Number    | MB    | 7056       |
| ApplianceBytesReceived | Amount of incoming network data. | Number    | Bytes | 608359     |
| ApplianceBytesSent     | Amount of outgoing network data. | Number    | Bytes | 616856     |
| NumCpus2               | Number of CPUs.                  | Number    |       | 3          |

| Field              | Description                                                                                                         | Data type | Unit | Example |
|--------------------|---------------------------------------------------------------------------------------------------------------------|-----------|------|---------|
| MemSizeMB2         | Memory size.                                                                                                        | Number    | MB   | 8096    |
| MemUseInMB2        | Memory usage.                                                                                                       | Number    | MB   | 196     |
| CpuFan0Speed       | CPU fan 0 speed.<br>Acceptable range is 3000 through 6000 RPM.                                                      | Number    |      | 5000    |
| CpuFan1Speed       | CPU fan 1 speed.<br>Acceptable range is 3000 through 6000 RPM.                                                      | Number    |      | 5000    |
| SystemFanSpeed     | System fan speed.<br>Acceptable range is 3000 through 6000 RPM.                                                     | Number    |      | 5000    |
| Cpu0Temp           | CPU 0 temperature.                                                                                                  | Number    |      | 80      |
| Cpu1Temp           | CPU 1 temperature.                                                                                                  | Number    |      | 80      |
| InternalTemp       | Internal temperature of health monitoring chip.                                                                     | Number    |      | 80      |
| PowerSupply1Status | Power supply 1 failure status.<br>Can be 0, 1, 2, 3, or 4. See also <a href="#">PowerSupply1StatusDisplayName</a> . | Number    |      | 1       |
| PowerSupply2Status | Power supply 2 failure status.<br>Can be 0, 1, 2, 3, or 4. See also <a href="#">PowerSupply2StatusDisplayName</a> . | Number    |      | 1       |

| Field                     | Description                                                                                                      | Data type | Unit | Example |
|---------------------------|------------------------------------------------------------------------------------------------------------------|-----------|------|---------|
| PowerSupply3Status        | Power supply 3 failure status. Can be 0, 1, 2, 3, or 4. See also <a href="#">PowerSupply3StatusDisplayName</a> . | Number    |      | 1       |
| PowerSupply4Status        | Power supply 4 failure status. Can be 0, 1, 2, 3, or 4. See also <a href="#">PowerSupply4StatusDisplayName</a> . | Number    |      | 1       |
| VoltageV33Main            | Main power supply +3.3V output. Acceptable range is 2.970 through 3.630 volts.                                   | Number    |      | 3.630   |
| ICAOnlySessions           | Number of ICA sessions.                                                                                          | Number    |      | 45      |
| ICAOnlyConnections        | Number of ICA connections.                                                                                       | Number    |      | 45      |
| SmartAccessSessions       | Number of VPN sessions.                                                                                          | Number    |      | 45      |
| SmartAccessICAConnections | Number of VPN ICA connections.                                                                                   | Number    |      | 45      |
| SSLSessions               | Number of SSL sessions.                                                                                          | Number    |      | 400     |

### List of Calculated Fields

| Field               | Description                      | Data type | Unit | Example | Where available   |
|---------------------|----------------------------------|-----------|------|---------|-------------------|
| ApplianceMBReceived | Amount of incoming network data. | Number    | MB   | 594.100 | Splunk data model |

| Field              | Description                                                                                                                                                           | Data type | Unit | Example | Where available               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|---------|-------------------------------|
| ApplianceMBSent    | Amount of outgoing network data.                                                                                                                                      | Number    | MB   | 602.39  | Splunk data model             |
| NumCpus            | Number of CPUs.                                                                                                                                                       | Number    |      | 3       | Splunk data model             |
| MemSizeMB          | Memory size.                                                                                                                                                          | Number    | MB   | 8096    | Splunk data model             |
| MemUseInMB         | Memory usage.                                                                                                                                                         | Number    | MB   | 196     | Splunk data model             |
| PowerSupply1Status | Power supply 1 failure status. Can be Unknown, Normal, Failed, Not present, or Not supported. Based on the lookup file <code>citrixadc_powersupplystatus.csv</code> . | Number    |      | Normal  | Splunk data model, Splunk SPL |
| PowerSupply2Status | Power supply 2 failure status. Can be Unknown, Normal, Failed, Not present, or Not supported. Based on the lookup file <code>citrixadc_powersupplystatus.csv</code> . | Number    |      | Normal  | Splunk data model, Splunk SPL |

| Field              | Description                                                                                                                                                         | Data type | Unit | Example | Where available               |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|---------|-------------------------------|
| PowerSupply3Status | PowerSupply3 failure status. Can be Unknown, Normal, Failed, Not present, or Not supported. Based on the lookup file <code>citrixadc_powersupplystatus.csv</code> . | Number    |      | Normal  | Splunk data model, Splunk SPL |
| PowerSupply4Status | PowerSupply4 failure status. Can be Unknown, Normal, Failed, Not present, or Not supported. Based on the lookup file <code>citrixadc_powersupplystatus.csv</code> . | Number    |      | Normal  | Splunk data model, Splunk SPL |

## Certificates

uberAgent collects certificate metrics like name, type, and expiration date for the primary as well as the secondary appliance.

### Details

- Source type: `uberAgent:CitrixADC:Certificate`
- Used in dashboards: *Single CitrixADC Inventory*

- Enabled through configuration setting: [CitrixADCInventory](#)
- Related configuration settings: [[CitrixADC\\_Config](#)]
- Supported platform: *Windows*

### List of Fields in the Raw Agent Data

| Field              | Description                                                                                                                                                                                    | Data type | Unit | Example                |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------------------|
| HostName           | Appliance name.                                                                                                                                                                                | String    |      | CitrixADC1             |
| CertName           | Certificate name.                                                                                                                                                                              | String    |      | nsmgmtcer              |
| CertFile           | Certificate file.                                                                                                                                                                              | String    |      | nsmgmt.cer             |
| CertType           | Certificate type.<br>Possible values:<br><a href="#">Client</a> ,<br><a href="#">Server</a> ,<br><a href="#">Client;</a><br><a href="#">Server,Root</a> ,<br><a href="#">Intermediate</a><br>. | String    |      | Client;Server          |
| CertExpirationDate | Certificate expiration date.                                                                                                                                                                   | String    |      | 2020-11-22<br>11:06:46 |

### Gateways

uberAgent collects gateway metrics like network throughput and SSL as well as authentication policies for the primary appliance.

### Details

- Source type: [uberAgent:CitrixADC:Gateway](#)
- Used in dashboards: [Citrix ADC Gateway Performance](#),[Single CitrixADC Inventory](#)
- Enabled through configuration setting: [CitrixADCGateway](#)
- Related configuration settings: [[CitrixADC\\_Config](#)]
- Supported platform: *Windows*

### List of Fields in the Raw Agent Data

| Field              | Description                               | Data type | Unit  | Example                   |
|--------------------|-------------------------------------------|-----------|-------|---------------------------|
| HostName           | Appliance name.                           | String    |       | CitrixADC1                |
| vServerName        | Gateway name.                             | String    |       | _XD_10.1.1.22_443         |
| PrimaryIpAddress   | IP address.                               | IPv4      |       | 10.1.1.22                 |
| PrimaryPort        | Port.                                     | Number    |       | 443                       |
| Type               | vServer type.<br>Possible values:<br>SSL. | String    |       | SSL                       |
| State              | vServer state.                            | String    |       | Up                        |
| RequestBytesRate   | Incoming network traffic.                 | Number    | Bytes | 1024                      |
| ResponseBytesRate  | Outgoing network traffic.                 | Number    | Bytes | 1024                      |
| AuthLDAPPolicies   | Bound LDAP authentication policies.       | String    |       | pol_ldap1;pol_ldap2       |
| AuthRadiusPolicies | Bound Radius authentication policies.     | String    |       | pol_radius1;pol_radius2   |
| AuthSAMLpolicies   | Bound SAML authentication policies.       | String    |       | pol_saml1                 |
| SessionPolicies    | Bound session policies.                   | String    |       | sp_storefront             |
| STAs               | Secure ticket authorities.                | String    |       | http://DDC.vastlimits.com |
| ResponderPolicies  | Bound responder policies.                 | String    |       | rp_storefront             |
| RewritePolicies    | Bound rewrite policies.                   | String    |       | rw_clientname             |
| Certificates       | Bound certificates.                       | String    |       | wildcard.vastlimits.com   |
| PortalTheme        | Bound portal theme.                       | String    |       | Default                   |
| SSL2*              | Indicates if SSL2 is enabled.             | String    |       | 0                         |

| Field            | Description                                                                                                                                                                                                                  | Data type | Unit | Example                         |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|---------------------------------|
| SSL3*            | Indicates if SSL3 is enabled.                                                                                                                                                                                                | String    |      | 0                               |
| TLS1*            | Indicates if TLS1 is enabled.                                                                                                                                                                                                | String    |      | 0                               |
| TLS11*           | Indicates if TLS1.1 is enabled.                                                                                                                                                                                              | String    |      | 0                               |
| TLS12*           | Indicates if TLS1.2 is enabled.                                                                                                                                                                                              | String    |      | 1                               |
| DiffeHellman*    | Indicates if Diffie-Hellman is enabled.                                                                                                                                                                                      | String    |      | 1                               |
| SSLProfile       | Name of the bound SSL profile.                                                                                                                                                                                               | String    |      | ns_default_ssl_profile_frontend |
| Ciphers*         | Bound ciphers.                                                                                                                                                                                                               | String    |      | DEFAULT                         |
| CipherSuites*    | Bound cipher suites.                                                                                                                                                                                                         | String    |      | DEFAULT                         |
| TotalRequests2   | Total number of requests received.                                                                                                                                                                                           | Number    |      | 456789                          |
| TotalResponses2  | Total number of responses.                                                                                                                                                                                                   | Number    |      | 456789                          |
| SessionTimeout2* | Session timeout.                                                                                                                                                                                                             | Number    |      | 120                             |
| HSTS             | State of HSTS protocol support for the SSL Virtual Server. Using HSTS, a server can enforce the use of an HTTPS connection for all communication with a client. Can be <a href="#">Enabled</a> or <a href="#">Disabled</a> . | String    |      | Disabled                        |



| Field           | Description                                                                                                                                                                        | Data type | Unit | Example |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|---------|
| HSTSMaxAge      | The maximum time, in seconds, in the strict transport security (STS) header during which the client must send only HTTPS requests to the server.                                   | Number    |      | 0       |
| HSTSIInclSubdom | Indicates if HSTS for subdomains is enabled or disabled. If set enabled, a client must send only HTTPS requests for subdomains. Can be <a href="#">Yes</a> or <a href="#">No</a> . | String    |      | No      |
| TLS13           | Indicates if TLS1.3 is enabled.                                                                                                                                                    | String    |      | Enabled |

\* If an SSL profile is bound, then these settings are taken from it.

### List of Calculated Fields

| Field                    | Description                                                       | Data type | Unit  | Example | Where available   |
|--------------------------|-------------------------------------------------------------------|-----------|-------|---------|-------------------|
| RequestResponseBytesRate | $\text{RequestBytesRate} + \text{ResponseBytesRate}$              | Number    | Bytes | 2048    | Splunk data model |
| RequestResponseRateMB    | $\frac{\text{RequestBytesRate} + \text{ResponseBytesRate}}{1024}$ | Number    | MB    | 2       | Splunk data model |

| Field           | Description                        | Data type | Unit | Example | Where available   |
|-----------------|------------------------------------|-----------|------|---------|-------------------|
| TotalRequests2  | Total number of requests received. | Number    |      | 456789  | Splunk data model |
| TotalResponses2 | Total number of responses.         | Number    |      | 456789  | Splunk data model |
| SessionTimeout2 | Session timeout.                   | Number    |      | 120     | Splunk data model |

## Ips

uberAgent collects Ip metrics like address, type, and if it is used for management access for the primary as well as the secondary appliance.

### Details

- Source type: [uberAgent:CitrixADC:Ip](#)
- Used in dashboards: [Single CitrixADC Inventory](#)
- Enabled through configuration setting: [CitrixADCInventory](#)
- Related configuration settings: [\[CitrixADC\\_Config\]](#)
- Supported platform: *Windows*

### List of Fields in the Raw Agent Data

| Field     | Description                                                                                                                                                             | Data type | Unit | Example     |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-------------|
| HostName  | Appliance name.                                                                                                                                                         | String    |      | CitrixADC1  |
| IpAddress | IP address.                                                                                                                                                             | IPv4      |      | 10.1.1.25   |
| IpNetmask | IP netmask.                                                                                                                                                             | String    |      | 255.255.0.0 |
| IpType    | IP type. Possible values: <a href="#">SNIP</a> , <a href="#">VIP</a> , <a href="#">NSIP</a> , <a href="#">GSLBsiteIP</a> , <a href="#">CLIP</a> , <a href="#">LSN</a> . | String    |      | VIP         |

---

| Field        | Description                                | Data type | Unit | Example |
|--------------|--------------------------------------------|-----------|------|---------|
| IpvServer    | Indicates if the IP is bound to a vServer. | String    |      | Yes     |
| IpMgmtAccess | Indicates if management access is allowed. | String    |      | 0       |

---

## Services

uberAgent collects service metrics like protocol, state as well as bound monitors for the primary appliance.

### Details

- Source type: [uberAgent:CitrixADC:Service](#)
- Used in dashboards: *Single Virtual Server Performance*
- Enabled through configuration setting: [CitrixADCvServer](#)
- Related configuration settings: [[CitrixADC\\_Config](#)]
- Supported platform: *Windows*

### List of Fields in the Raw Agent Data

---

| Field       | Description     | Data type | Unit | Example    |
|-------------|-----------------|-----------|------|------------|
| HostName    | Appliance name. | String    |      | CitrixADC1 |
| ServiceName | Service name.   | String    |      | webserver1 |

---

| Field            | Description                                                                                                                                                                                                                                                                                                                                                                             | Data type | Unit | Example   |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-----------|
| Protocol         | Service protocol.<br>Possible values:<br>HTTP, FTP, TCP,<br>UDP, SSL,<br>SSL_BRIDGE,<br>SSL_TCP, DTLS,<br>NNTP, DNS,<br>DHCPR, ANY,<br>SIP_UDP,<br>SIP_TCP,<br>SIP_SSL,<br>DNS_TCP, RTSP,<br>PUSH,<br>SSL_PUSH,<br>RADIUS, RDP,<br>MYSQL, MSSQL,<br>DIAMETER,<br>SSL_DIAMETER,<br>TFTP, ORACLE,<br>SMPP,<br>SYSLOGTCP,<br>SYSLOGUDP,<br>FIX, SSL_FIX,<br>USER_TCP,<br>USER_SSL_TCP<br>. | String    |      | HTTP      |
| PrimaryIpAddress | IP address.                                                                                                                                                                                                                                                                                                                                                                             | IPv4      |      | 10.1.1.11 |
| PrimaryPort      | Port.                                                                                                                                                                                                                                                                                                                                                                                   | Number    |      | 80        |

| Field           | Description                                                                                                                                                                                       | Data type | Unit | Example               |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-----------------------|
| State           | Service state.<br>Possible values:<br>UP, DOWN,<br>UNKNOWN,<br>OFS (Out of<br>Service),<br>TROFS (<br>Transition<br>Out of<br>Service),<br>TROFS_DOWN (<br>Down when<br>going Out of<br>Service). | String    |      | Up                    |
| vServerName     | Name of the<br>vServer the<br>service is bound<br>to.                                                                                                                                             | String    |      | lbvs_CompanyWebserver |
| ServiceMonitors | Bound service<br>monitors.                                                                                                                                                                        | String    |      | tcp-default           |

### List of Calculated Fields

| Field                | Description                         | Data type | Unit | Example | Where available   |
|----------------------|-------------------------------------|-----------|------|---------|-------------------|
| ServiceMonitorsSplit | ServiceMonitors split by semicolon. | Number    | MB   |         | Splunk data model |

### Service Groups

uberAgent collects service group metrics like protocol, state as well as bound monitors for the primary appliance.

**Details**

- Source type: `uberAgent:CitrixADC:ServiceGroup`
- Used in dashboards: *Single Virtual Server Performance*
- Enabled through configuration setting: `CitrixADCvServer`
- Related configuration settings: `[CitrixADC_Config]`
- Supported platform: *Windows*

**List of Fields in the Raw Agent Data**

---

| Field            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Data type | Unit | Example    |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------|
| HostName         | Appliance name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | String    |      | CitrixADC1 |
| ServiceGroupName | Service group name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | String    |      | sgr1       |
| Protocol         | Service group protocol: <code>ADNS</code> , <code>DNS</code> , <code>MYSQL</code> , <code>RTSP</code> , <code>SSL_DIAMETER</code> , <code>ADNS_TCP</code> , <code>DNS_TCP</code> , <code>NNTP</code> , <code>SIP_UDP</code> , <code>SSL_TCP</code> , <code>ANY</code> , <code>FTP</code> , <code>RADIUS</code> , <code>SNMP</code> , <code>TCP</code> , <code>DHCPRA</code> , <code>HTTP</code> , <code>RDP</code> , <code>SSL</code> , <code>TFTP</code> , <code>DIAMETER</code> , <code>MSSQL</code> , <code>RPCSVR</code> , <code>SSL_BRIDGE</code> , <code>UDP</code> . | String    |      | HTTP       |

| Field                | Description                                                                                                                                                     | Data type | Unit | Example           |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-------------------|
| State                | Service group state. Possible values: UP, DOWN, UNKNOWN, OFS (Out of Service), TROFS (Transition Out of Service), TROFS_DOWN (Down when going Out of Service).  | String    |      | Up                |
| EffectiveState       | Indicates the effective servicegroup state based on the state of the bound service items. Possible values: UP, DOWN, OUT OF SERVICE, PARTIAL-UP, PARTIAL-DOWN . | String    |      | Up                |
| vServerName          | Name of the vServer the service group is bound to.                                                                                                              | String    |      | lbvs_Storefront   |
| ServiceGroupMembers  | Services which are members of the service group.                                                                                                                | String    |      | Service1;Service2 |
| ServiceGroupMonitors | Bound service group monitors.                                                                                                                                   | String    |      | ping;tcp          |

## List of Calculated Fields

| Field                                 | Description         | Data type | Unit | Example              | Where available   |
|---------------------------------------|---------------------|-----------|------|----------------------|-------------------|
| ServiceGroupMembersSplitGroupNumbers  | split by semicolon. | Number    | MB   | Service1<br>Service2 | Splunk data model |
| ServiceGroupMonitorsSplitGroupNumbers | split by semicolon. | Number    | MB   | ping tcp             | Splunk data model |

## Virtual Server

uberAgent collects virtual server (load-balancing virtual server only) metrics like network throughput and bound policies for the primary appliance.

### Details

- Source type: `uberAgent:CitrixADC:vServer`
- Used in dashboards: *Citrix ADC Virtual Server Performance*, *Single Virtual Server Performance*, *Single CitrixADC Inventory*
- Enabled through configuration setting: `CitrixADCGateway`
- Related configuration settings: `[CitrixADC_Config]`
- Supported platform: *Windows*

## List of Fields in the Raw Agent Data

| Field            | Description          | Data type | Unit | Example       |
|------------------|----------------------|-----------|------|---------------|
| HostName         | Appliance name.      | String    |      | CitrixADC1    |
| vServerName      | Virtual server name. | String    |      | vs_Storefront |
| PrimaryIpAddress | IP address.          | IPv4      |      | 10.1.1.5      |
| PrimaryPort      | Port.                | Number    |      | 443           |



| Field             | Description                                                                                                                                                                                                                                                                                                                                                                         | Data type | Unit  | Example       |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------|---------------|
| Type              | vServer type.<br>Possible values:<br>HTTP, FTP, TCP,<br>UDP, SSL,<br>SSL_BRIDGE,<br>SSL_TCP, DTLS,<br>NNTP, DNS,<br>DHCPR, ANY,<br>SIP_UDP,<br>SIP_TCP,<br>SIP_SSL,<br>DNS_TCP, RTSP,<br>PUSH,<br>SSL_PUSH,<br>RADIUS, RDP,<br>MYSQL, MSSQL,<br>DIAMETER,<br>SSL_DIAMETER,<br>TFTP, ORACLE,<br>SMPP,<br>SYSLOGTCP,<br>SYSLOGUDP,<br>FIX, SSL_FIX,<br>USER_TCP,<br>USER_SSL_TCP<br>. | String    |       | SSL           |
| State             | vServer state.                                                                                                                                                                                                                                                                                                                                                                      | String    |       | Up            |
| RequestBytesRate  | Incoming<br>network traffic.                                                                                                                                                                                                                                                                                                                                                        | Number    | Bytes | 1024          |
| ResponseBytesRate | Outgoing<br>network traffic.                                                                                                                                                                                                                                                                                                                                                        | Number    | Bytes | 1024          |
| RewritePolicies   | Bound rewrite<br>policies.                                                                                                                                                                                                                                                                                                                                                          | String    |       | rw_clientname |
| ResponderPolicies | Bound responder<br>policies.                                                                                                                                                                                                                                                                                                                                                        | String    |       | rp_storefront |
| Certificates      | Bound<br>certificates.                                                                                                                                                                                                                                                                                                                                                              | String    |       | Cert1;Cert2   |

| Field            | Description                                                                                | Data type | Unit | Example                |
|------------------|--------------------------------------------------------------------------------------------|-----------|------|------------------------|
| SSL2*            | Indicates if SSL2 is enabled.                                                              | String    |      | 0                      |
| SSL3*            | Indicates if SSL3 is enabled.                                                              | String    |      | 0                      |
| TLS1*            | Indicates if TLS1 is enabled.                                                              | String    |      | 0                      |
| TLS11*           | Indicates if TLS1.1 is enabled.                                                            | String    |      | 0                      |
| TLS12*           | Indicates if TLS1.2 is enabled.                                                            | String    |      | 1                      |
| DiffeHellman*    | Indicates if Diffie-Hellman is enabled.                                                    | String    |      | 1                      |
| SSLProfile       | Name of the bound SSL profile.                                                             | String    |      | vastlimits_ssl_profile |
| Ciphers*         | Bound ciphers.                                                                             | String    |      | Secure_Cipher_Group    |
| CipherSuites*    | Bound cipher suites.                                                                       | String    |      | DEFAULT                |
| ActSvc2          | Active services.                                                                           | Number    |      | 2                      |
| TotHits2         | Total Hits.                                                                                | Number    |      | 456789                 |
| TotalRequests2   | Total number of requests received.                                                         | Number    |      | 31888                  |
| TotalResponses2  | Total number of responses.                                                                 | Number    |      | 31888                  |
| VSLBHealth2      | The health of the vserver. This gives the percentage of UP services bound to this vserver. | Number    | %    | 100                    |
| SessionTimeout2* | Session timeout.                                                                           | Number    |      | 120                    |

---

| Field          | Description                                                                                                                                                                                                                  | Data type | Unit | Example  |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|----------|
| HSTS           | State of HSTS protocol support for the SSL Virtual Server. Using HSTS, a server can enforce the use of an HTTPS connection for all communication with a client. Can be <a href="#">Enabled</a> or <a href="#">Disabled</a> . | String    |      | Disabled |
| HSTSMaxAge     | The maximum time, in seconds, in the strict transport security (STS) header during which the client must send only HTTPS requests to the server.                                                                             | Number    |      | 0        |
| HSTSInclSubdom | Indicates if HSTS for subdomains is enabled or disabled. If set enabled, a client must send only HTTPS requests for subdomains. Can be <a href="#">Yes</a> or <a href="#">No</a> .                                           | String    |      | No       |
| TLS13          | Indicates if TLS1.3 is enabled.                                                                                                                                                                                              | String    |      | Enabled  |

---

*\* If an SSL profile is bound, then these settings are taken from it.*

## List of Calculated Fields

| Field          | Description                                                                                | Data type | Unit | Example | Where available   |
|----------------|--------------------------------------------------------------------------------------------|-----------|------|---------|-------------------|
| RequestMBRate  | Incoming network traffic.                                                                  | Number    | MB   | 1       | Splunk data model |
| ResponseMBRate | Outgoing network traffic.                                                                  | Number    | MB   | 1       | Splunk data model |
| ActSvcs        | Active services.                                                                           | Number    |      | 2       | Splunk data model |
| TotHits        | Total Hits.                                                                                | Number    |      | 456789  | Splunk data model |
| TotalRequests  | Total number of requests received.                                                         | Number    |      | 31888   | Splunk data model |
| TotalResponses | Total number of responses.                                                                 | Number    |      | 31888   | Splunk data model |
| VSLBHealth     | The health of the vserver. This gives the percentage of UP services bound to this vserver. | Number    | %    | 100     | Splunk data model |
| SessionTimeout | Session timeout.                                                                           | Number    |      | 120     | Splunk data model |

## Citrix Session Metrics

July 9, 2024

### Virtual Channel Detail

uberAgent collects the input and output data volume for every virtual channel per Citrix session.

## Details

- Source type: `uberAgent:CitrixSession:VirtualChannelDetail`
- Used in dashboards: *Citrix Session Protocol Insights, Single User Detail, Analyze data over time*
- Enabled through configuration setting: `CitrixSessionVirtualChannelDetail`
- Related configuration settings: *CitrixSessionConfig*

## List of Fields in the Raw Agent Data

| Field                          | Description                                                                                                | Data type | Unit | Example                              | Platform |
|--------------------------------|------------------------------------------------------------------------------------------------------------|-----------|------|--------------------------------------|----------|
| SessionGUID                    | Unique identifier that is generated by uberAgent when the session is created. Valid for this session only. | String    |      | 00000002-f295-9109-e7c7-c964011dd401 | Windows  |
| SessionUser                    | User name.                                                                                                 | String    |      | Domain\JohnDoe                       | Windows  |
| VirtualChannelVendorName       | Vendor name identifier for a virtual channel.                                                              | String    |      | CTXTW                                | Windows  |
| VirtualChannelDataVolumeInput  | Data volume received by the session per virtual channel.                                                   | Number    | MB   | 1                                    | Windows  |
| VirtualChannelDataVolumeOutput | Data volume sent by the session per virtual channel.                                                       | Number    | MB   | 10                                   | Windows  |

## List of Calculated Fields

| Field                                   | Description                                                                                                                                                         | Data type | Unit | Example           | Where available   |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-------------------|-------------------|
| VirtualChannelDataVolumeInputOutputMB   | Total virtual channel data volume.                                                                                                                                  | Number    | MB   | 11                | Splunk data model |
| VirtualChannelDisplayName               | Display name of virtual channel name. Possible values: too many to list here. Please check the lookup file <code>citrixsession_virtualchannels.csv</code> .         | String    |      | Thinwire Graphics | SPL               |
| VirtualChannelVirtualChannelDisplayName | Content of <code>VirtualChannelDisplayName</code> . If <code>VirtualChannelDisplayName</code> is not filled, <code>VirtualChannelVendorName</code> is used instead. | String    |      | Thinwire Graphics | Splunk data model |

## Session Config

uberAgent collects detailed information about applied Citrix HDX policies and important active session settings.

### Details

- Source type: `uberAgent:CitrixSession:SessionConfig`
- Used in dashboards: *Citrix Session Configuration Details*, *Single User Detail*
- Enabled through configuration setting: `CitrixSessionConfig`
- Related configuration settings: *CitrixSessionVirtualChannelDetail*, *TriggerCitrixSessionConfig*

**List of Fields in the Raw Agent Data**

| Field                                 | Description                                                                                                | Data type | Unit | Example                              | Platform |
|---------------------------------------|------------------------------------------------------------------------------------------------------------|-----------|------|--------------------------------------|----------|
| SessionGUID                           | Unique identifier that is generated by uberAgent when the session is created. Valid for this session only. | String    |      | 00000002-f295-9109-e7c7-c964011dd401 | Windows  |
| SessionUser                           | User name.                                                                                                 | String    |      | Domain\JohnDoe                       | Windows  |
| AudioActualPriority                   | Applied virtual channel priority for audio.                                                                | String    |      | RealTime                             | Windows  |
| AudioPolicyAllowMicrophoneRedirection | Microphone redirection allow/deny.                                                                         | String    |      | 1                                    | Windows  |
| AudioPolicyAllowRedirection           | Redirection to allow/deny audio redirection.                                                               | String    |      | 1                                    | Windows  |
| AudioPolicyPriority                   | Cyrix policy to set the virtual channel priority.                                                          | String    |      | RealTime                             | Windows  |
| AudioPolicySoundQuality               | Quality policy to configure the sound quality.                                                             | String    |      | High                                 | Windows  |

| Field                        | Description                                                           | Data type | Unit | Example                     | Platform |
|------------------------------|-----------------------------------------------------------------------|-----------|------|-----------------------------|----------|
| CdmActualPriority            | Applied virtual channel priority for client drive mapping.            | String    |      | Medium                      | Windows  |
| CdmVolumes                   | Volumes the client mapped into the session.                           | String    |      | Local Disk (C: on MACHINE1) | Windows  |
| CdmPolicyAllowDriveDirection | Allow/deny client drive mapping.                                      | String    |      | 1                           | Windows  |
| CdmPolicyPriority            | Citrix policy to set the virtual channel priority.                    | String    |      | Medium                      | Windows  |
| CdmPolicyReadOnly            | Citrix policy to allow/deny read-only client drive access.            | String    |      | 1                           | Windows  |
| DisplayMode                  | Active display mode. See <a href="#">DisplayModeName</a> for details. | Number    |      | 4                           | Windows  |
| ThinwireActualPriority       | Applied virtual channel priority for this display mode.               | String    |      | High                        | Windows  |
| ThinwireColorDepth           | Applied session color depth.                                          | Number    | bit  | 24                          | Windows  |



| Field                             | Description                                                   | Data type | Unit | Example                       | Platform |
|-----------------------------------|---------------------------------------------------------------|-----------|------|-------------------------------|----------|
| ThinwireComponentEncoder          | Applied video component encoder.                              | String    |      | DeepCompressionVideoEncoder   | Windows  |
| ThinwireHardwareEncodeInUse       | Set if hardware encode is actually in use.                    | String    |      | 1                             | Windows  |
| ThinwireVideoCodecType            | Applied video codec type.                                     | String    |      | H264                          | Windows  |
| ThinwireColorspace                | Applied session color space.                                  | String    |      | Yuv420                        | Windows  |
| ThinwireVideoCodecUsage           | Applied video codec usage setting.                            | String    |      | For actively changing regions | Windows  |
| ThinwirePolicyFPS                 | Citrix policy to configure the maximum session FPS.           | Number    |      | 30                            | Windows  |
| ThinwirePolicyPriority            | Citrix policy to set the virtual channel priority.            | String    |      | High                          | Windows  |
| ThinwirePolicyUseHardwareEncoding | Set if hardware encoding is enable/disable hardware encoding. | String    |      | 1                             | Windows  |
| ThinwirePolicyUseVideoCodec       | Set if policy to configure the video codec.                   | String    |      | UseVideoCodecIfPreferred      | Windows  |
| ThinwirePolicyVisualQuality       | Citrix policy to configure the visual quality.                | String    |      | Medium                        | Windows  |

| Field                    | Description                                             | Data type | Unit | Example | Platform |
|--------------------------|---------------------------------------------------------|-----------|------|---------|----------|
| FrameworkActualPriority  | Applied virtual channel priority for this display mode. | String    |      | High    | Windows  |
| FrameworkPolicyPriority  | Citrix policy to set the virtual channel priority.      | String    |      | High    | Windows  |
| D3DActualPriority        | Applied virtual channel priority for this display mode. | String    |      | High    | Windows  |
| D3DPolicyAeroRedirection | Citrix policy to enable/disable DCR aero redirection.   | String    |      | 1       | Windows  |
| D3DPolicyGraphicsQuality | Citrix policy to configure the DCR graphics quality.    | String    |      | Medium  | Windows  |
| D3DPolicyPriority        | Citrix policy to set the virtual channel priority.      | String    |      | High    | Windows  |
| GraphicsActualPriority   | Applied virtual channel priority for this display mode. | String    |      | High    | Windows  |

| Field                                 | Description                                                                                   | Data type | Unit | Example                  | Platform |
|---------------------------------------|-----------------------------------------------------------------------------------------------|-----------|------|--------------------------|----------|
| GraphicsPolicyDisplayDegradedNotify   | Use to notify the user about display quality degradation.                                     | String    |      | 1                        | Windows  |
| GraphicsPolicyDisplayDegradedPolicy   | Configure the display quality degradation.                                                    | String    |      | DEGRADE_RESOLUTION_FIRST | Windows  |
| GraphicsPolicyPriority                | Policy to set the virtual channel priority.                                                   | String    |      | High                     | Windows  |
| NetworkConnectAddress                 | Address the session connected from. This is the same information as shown in Citrix Director. | String    |      | 10.1.1.150               | Windows  |
| NetworkEdtMtu                         | Applied Enlightened Data Transport MTU size.                                                  | Number    |      | 1400                     | Windows  |
| NetworkPolicyAcceptSessionReliability | enable/disable session reliability.                                                           | String    |      | 1                        | Windows  |
| NetworkPolicyICAListenerPort          | Configure the ICA listener port.                                                              | Number    |      | 1494                     | Windows  |

| Field                                  | Description                                                                                                        | Data type | Unit | Example                                             | Platform |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------|-----------|------|-----------------------------------------------------|----------|
| NetworkPolicySessionReliabilityPort    | configure the session reliability port.                                                                            | Number    |      | 2598                                                | Windows  |
| NetworkPolicySessionReliabilityTimeout | configure the session reliability timeout.                                                                         | Number    | s    | 180                                                 | Windows  |
| PrinterActualPriority                  | Applied virtual channel priority for printing.                                                                     | String    |      | Low                                                 | Windows  |
| PrinterSessionPrinters                 | mapped session printers.                                                                                           | String    |      | Microsoft Print to PDF (from MACHINE1) in session 9 | Windows  |
| PrinterPolicyAllowRedirection          | allow/deny printer redirection.                                                                                    | String    |      | 1                                                   | Windows  |
| PrinterPolicyAllowRedirection          | allow/deny printer redirection.                                                                                    | String    |      | Allowed                                             | Windows  |
| PrinterPolicyAutoCreateClientPrinters  | configure printer auto-creation. See <a href="#">PrinterPolicyAutoCreateClientPrintersDisplayName</a> for details. | Number    |      | 3                                                   | Windows  |

| Field                        | Description                                        | Data type | Unit | Example | Platform |
|------------------------------|----------------------------------------------------|-----------|------|---------|----------|
| PrinterPolicyPriority        | Citrix policy to set the virtual channel priority. | String    |      | Low     | Windows  |
| USBActualPriority            | Applied virtual channel priority for USB devices.  | String    |      | Medium  | Windows  |
| USBPolicyAllowPNPRedirection | Allow/deny PNP redirection.                        | String    |      | 1       | Windows  |
| USBPolicyAllowUSBSupport     | Allow/deny USB support.                            | String    |      | 1       | Windows  |
| USBPolicyPriority            | Citrix policy to set the virtual channel priority. | String    |      | Medium  | Windows  |

**List of Calculated Fields**

| Field           | Description                                                                                                                                                    | Data type | Unit | Example  | Where available |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|----------|-----------------|
| DisplayModeName | Descriptive display mode name. Possible values: <a href="#">Thinwire</a> , <a href="#">Framehawk</a> , <a href="#">DCR</a> , <a href="#">Legacy Graphics</a> . | String    |      | Thinwire | SPL             |

| Field                                                 | Description                                                                                                                                                                                                                                   | Data type | Unit | Example                                       | Where available |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-----------------------------------------------|-----------------|
| PrinterPolicyAutoCreateClientPrinterStringDisplayName | name of how client printer creation is configured. Possible values: Do not auto-create client printers, Auto-create the client's default printer only, Auto-create local (non-network) client printers only, Auto-create all client printers. | String    |      | Auto-create the client's default printer only | SPL             |

## Citrix Virtual Apps & Desktops Site Metrics

July 9, 2024

Citrix Virtual Apps and Desktops site metrics can be determined from on-premises machines or from the Citrix Cloud.

Citrix site monitoring requires its metrics enabled on at least one machine. See the [documentation](#) for details.

## Applications

uberAgent collects metrics like application name, site name as well as several application properties (is enabled, creation date, modification date, type) for each published application.

### Details

- Source type: [uberAgent:Citrix:Applications](#)
- Used in dashboards: *Citrix Virtual Apps and Desktops*
- Enabled through configuration setting: [CitrixDCApplication](#)
- Related configuration settings: *n/a*
- Supported platform: *Windows, Citrix Virtual Apps and Desktops on-premises, Citrix Cloud*

### List of Fields in the Raw Agent Data

| Field            | Description                                    | Data type | Unit | Example                              |
|------------------|------------------------------------------------|-----------|------|--------------------------------------|
| Id               | Application ID.                                | String    |      | 10                                   |
| Name             | Application name.                              | String    |      | GoogleChrome                         |
| PublishedName    | Application published name.                    | String    |      | Google Chrome                        |
| SiteName         | Related Citrix site name.                      | String    |      | vl-Site                              |
| SiteGuid         | Related Citrix site GUID.                      | String    |      | 0a0fda60-aebf-4ac0-920d-44bd509ca927 |
| DesktopGroupId   | Desktop group ID.                              | String    |      | 05bddbe7-cf12-4ee2-ab02-93d0428d3847 |
| DesktopGroupName | Desktop group name.                            | String    |      | Finance users                        |
| ApplicationType  | Application type.<br>Possible values:<br>0, 1. | Number    |      | 0                                    |

| Field                | Description                                                 | Data type | Unit | Example                              |
|----------------------|-------------------------------------------------------------|-----------|------|--------------------------------------|
| Enabled              | Indicates if application is enabled. Possible values: 0, 1. | String    |      | 1                                    |
| AdminFolder          | Application admin folder.                                   | String    |      | Finance                              |
| Tags                 | Configured tags.                                            | String    |      | Germany France                       |
| ApplicationGroupId   | Application group ID.                                       | String    |      | f5411e59-bc4f-4dfa-a893-c54015aa4a66 |
| ApplicationGroupName | Application group name.                                     | String    |      | Finance apps                         |
| CustomerId           | Citrix Cloud CustomerId.                                    | String    |      | a230abcdej1e                         |

### List of Calculated Fields

| Field                      | Description                                                                                                         | Data type | Unit | Example                    | Where available               |
|----------------------------|---------------------------------------------------------------------------------------------------------------------|-----------|------|----------------------------|-------------------------------|
| ApplicationTypeDisplayName | Application type name. Possible values:<br><a href="#">HostedOnDesktop</a> ,<br><a href="#">InstalledOnClient</a> . | String    |      | HostedOnDesktop            | Splunk data model, Splunk SPL |
| TagsSplit                  | Tags split by semicolon.                                                                                            | String    |      | Germany;France             | Splunk data model             |
| SiteNameExtended           | Site name including the Citrix Cloud CustomerId.                                                                    | String    |      | cloudxdsite (a230abcdej1e) | Splunk data model             |



## Databases

uberAgent collects information like name and data store about databases configured in a site.

### Details

- Source type: [uberAgent:Citrix:Databases](#)
- Used in dashboards: *Citrix Virtual Apps and Desktops Databases*
- Enabled through configuration setting: [CitrixDCGeneralInformation](#)
- Related configuration settings: *n/a*
- Supported platform: *Windows, Citrix Virtual Apps and Desktops on-premises*

### List of Fields in the Raw Agent Data

---

| Field               | Description                                                                          | Data type | Unit | Example                              |
|---------------------|--------------------------------------------------------------------------------------|-----------|------|--------------------------------------|
| SiteName            | Related Citrix site name.                                                            | String    |      | vl-Site                              |
| SiteGuid            | Related Citrix site GUID.                                                            | String    |      | 0a0fda60-aebf-4ac0-920d-44bd509ca927 |
| DataStore           | Datastore type.<br>Possible values:<br>1, 2, 3 (1 = Site, 2 = Logging, 3 = Monitor). | Number    |      | 1                                    |
| IntegratedSecurity  | Database authentication method. Possible values: 1 (1 = <b>true</b> ).               | String    |      | 1                                    |
| MirrorServerAddress | Mirror database server address.                                                      | String    |      | DB2.domain.ad                        |
| Name                | Database name.                                                                       | String    |      | CitrixSiteDB                         |
| ServerAddress       | Database server address.                                                             | String    |      | DB1.domain.ad                        |

---

## Desktops

uberAgent collects metrics like desktop name, site name as well as tags for each published desktop.

### Details

- Source type: [uberAgent:Citrix:PublishedDesktops](#)
- Used in dashboards: *Citrix Virtual Apps and Desktops*
- Enabled through configuration setting: [CitrixDCPublishedDesktops](#)
- Related configuration settings: *n/a*
- Supported platform: *Windows, Citrix Virtual Apps and Desktops on-premises, Citrix Cloud*

### List of Fields in the Raw Agent Data

| Field            | Description                              | Data type | Unit | Example                              |
|------------------|------------------------------------------|-----------|------|--------------------------------------|
| Id               | Published desktop ID.                    | String    |      | 10                                   |
| Name             | Published desktop name (internal).       | String    |      | Finance Desktop                      |
| PublishedName    | Published desktop name (published).      | String    |      | Finance Desktop                      |
| SiteName         | Related Citrix site name.                | String    |      | vl-Site                              |
| SiteGuid         | Related Citrix site GUID.                | String    |      | 0a0fda60-aebf-4ac0-920d-44bd509ca927 |
| DesktopGroupId   | Related desktop group ID.                | String    |      | 05bddbe7-cf12-4ee2-ab02-93d0428d3847 |
| DesktopGroupName | Related desktop group name.              | String    |      | Finance users                        |
| BrowserName      | Unique published desktop name in a site. | String    |      | FinanceDesktop                       |

| Field                     | Description                                                                                   | Data type | Unit | Example                      |
|---------------------------|-----------------------------------------------------------------------------------------------|-----------|------|------------------------------|
| ColorDepth                | Color depth.<br>Possible values:<br>0, 1, 2, 3.                                               | Number    |      | 3                            |
| Description               | Description.                                                                                  | String    |      | Desktop for<br>finance users |
| Enabled                   | Indicates if the<br>published<br>desktop is<br>enabled. Possible<br>values: 0, 1.             | String    |      | 1                            |
| ExcludedUserFilterEnabled | Indicates if the<br>excluded user<br>filter is enabled.<br>Possible values:<br>0, 1.          | String    |      | 1                            |
| ExcludedUsers             | Excluded users.                                                                               | String    |      | AD\Marketing<br>AD\HR        |
| IncludedUserFilterEnabled | Indicates if the<br>included user<br>filter is enabled.<br>Possible values:<br>0, 1.          | String    |      | 1                            |
| IncludedUsers             | Included users.                                                                               | String    |      | AD\Finance                   |
| LeasingBehavior           | Leasing behavior.<br>Possible values:<br>0, 1.                                                | Number    |      | 1                            |
| RestrictToTag             | Indicates if a<br>published<br>desktop is<br>restricted to<br>machines with<br>specific tags. | String    |      | Finance                      |
| SecureIcaRequired         | Indicates if<br>SecureICA is<br>required.<br>Possible values:<br>0, 1.                        | String    |      | 1                            |

| Field               | Description                                                             | Data type | Unit | Example        |
|---------------------|-------------------------------------------------------------------------|-----------|------|----------------|
| SessionReconnection | Indicates the session reconnection behaviour. Possible values: 0, 1, 2. | Number    |      | 2              |
| Tags                | Configured tags.                                                        | String    |      | Germany France |
| CustomerId          | Citrix Cloud CustomerId.                                                | String    |      | a230abcdej1e   |

### List of Calculated Fields

| Field                 | Description                                                                 | Data type | Unit | Example            | Where available               |
|-----------------------|-----------------------------------------------------------------------------|-----------|------|--------------------|-------------------------------|
| ColorDepthBits        | Color depth. Possible values: 4, 8, 16, 24.                                 | Number    |      | 24                 | Splunk data model, Splunk SPL |
| ColorDepthDisplayName | Color depth. Possible values: FourBit, EightBit, SixteenBit, TwentyFourBit. | String    |      | TwentyFourBit      | Splunk data model, Splunk SPL |
| ExcludedUsersSplit    | Excluded user split by semicolon.                                           | String    |      | AD\Marketing;AD\HR | Splunk data model             |
| IncludedUsersSplit    | Included users split by semicolon.                                          | String    |      | AD\Finance         | Splunk data model             |

| Field                      | Description                                                                                                                                                       | Data type | Unit | Example                    | Where available                  |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|----------------------------|----------------------------------|
| LeasingBehaviorDisplay     | Display behavior.<br>Possible values:<br><a href="#">Allowed</a> ,<br><a href="#">Disallowed</a>                                                                  | String    |      | Allowed                    | Splunk data model,<br>Splunk SPL |
| SessionReconnectionDisplay | Display session reconnection behaviour.<br>Possible values:<br><a href="#">Always</a> ,<br><a href="#">DisconnectedOnly</a> ,<br><a href="#">SameEndpointOnly</a> | String    |      | SameEndpointOnly           | Splunk data model,<br>Splunk SPL |
| TagsSplit                  | Tags split by semicolon.                                                                                                                                          | String    |      | Germany;France             | Splunk data model                |
| SiteNameExtendedSite       | Site name including the Citrix Cloud CustomerId.                                                                                                                  | String    |      | cloudxdsite (a230abcdej1e) | Splunk data model                |

## Desktop Groups

uberAgent collects metrics like desktop group name and tags for each desktop group in a site.

### Details

- Source type: [uberAgent:Citrix:DesktopGroups](#)
- Used in dashboards: *Citrix Virtual Apps and Desktops*, *Citrix Virtual Apps and Desktops Machines*
- Enabled through configuration setting: [CitrixDCDesktopGroup](#)
- Related configuration settings: *n/a*
- Supported platform: *Windows, Citrix Virtual Apps and Desktops on-premises, Citrix Cloud*

**List of Fields in the Raw Agent Data**

| Field          | Description                                                                            | Data type | Unit | Example                              |
|----------------|----------------------------------------------------------------------------------------|-----------|------|--------------------------------------|
| Id             | Desktop group ID.                                                                      | String    |      | 10                                   |
| Name           | Desktop group name.                                                                    | String    |      | Finance                              |
| SiteName       | Related Citrix site name.                                                              | String    |      | vl-Site                              |
| SiteGuid       | Related Citrix site GUID.                                                              | String    |      | 0a0fda60-aebf-4ac0-920d-44bd509ca927 |
| IsRemotePC     | Indicates if a desktop group is configured for Remote PC.<br>Possible values:<br>0, 1. | String    |      | 0                                    |
| DesktopKind    | Kind of contained desktops.<br>Possible values:<br>0, 1.                               | Number    |      | 1                                    |
| LifecycleState | Lifecycle state.<br>Possible values:<br>0, 1, 2, 3.                                    | Number    |      | 1                                    |
| SessionSupport | Indicates a desktop group's session support.<br>Possible values:<br>0, 1, 2.           | Number    |      | 1                                    |
| DeliveryType   | Desktop group delivery type.<br>Possible values:<br>0, 1, 2.                           | Number    |      | 2                                    |
| Tags           | Configured tags.                                                                       | String    |      | Germany France                       |
| CreatedDate    | Desktop group creation date.                                                           | String    |      | 2018-03-16<br>14:16:07.008<br>+0200  |

| Field        | Description                      | Data type | Unit | Example                             |
|--------------|----------------------------------|-----------|------|-------------------------------------|
| ModifiedDate | Desktop group modification date. | String    |      | 2018-03-16<br>14:16:07.008<br>+0200 |
| CustomerId   | Citrix Cloud CustomerId.         | String    |      | a230abcdej1e                        |

**List of Calculated Fields**

| Field                 | Description                                                                                                                              | Data type | Unit | Example                                          | Where available                  |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|--------------------------------------------------|----------------------------------|
| DesktopGroupId        | Content of field <code>Id</code> .                                                                                                       | String    |      | 05bddbe7-<br>cf12-4ee2-<br>ab02-<br>93d0428d3847 | Splunk data model,<br>Splunk SPL |
| DesktopKindDisplay    | KindName contained desktops. Possible values: <code>Private</code> , <code>Shared</code> .                                               | String    |      | Shared                                           | Splunk data model,<br>Splunk SPL |
| LifecycleStateDisplay | LifecycleState name. Possible values: <code>Active</code> , <code>Deleted</code> , <code>RequiresResolution</code> , <code>Stub</code> . | String    |      | Active                                           | Splunk data model,<br>Splunk SPL |

| Field                     | Description                                                                                                                       | Data type | Unit | Example                    | Where available               |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-----------|------|----------------------------|-------------------------------|
| SessionSupportDisplayname | desktop group's session support. Possible values: <code>Unknown</code> , <code>SingleSession</code> , <code>MultiSession</code> . | String    |      | SingleSession              | Splunk data model, Splunk SPL |
| DeliveryTypeDisplayname   | desktop group delivery type. Possible values: <code>DesktopsOnly</code> , <code>AppsOnly</code> , <code>DesktopAndApps</code> .   | String    |      | DesktopAndApps             | Splunk data model, Splunk SPL |
| TagsSplit                 | Tags split by semicolon.                                                                                                          | String    |      | Germany;France             | Splunk data model             |
| SiteNameExtended          | Site name including the Citrix Cloud CustomerId.                                                                                  | String    |      | cloudxdsite (a230abcdej1e) | Splunk data model             |

## Hypervisors

**DEPRECATED:** this sourcetype is deprecated and will be removed in a future release.

uberAgent collects information like name and lifecycle state about hypervisors configured in a site.

### Details

- Source type: `uberAgent:Citrix:Hypervisors`
- Used in dashboards: *n/a*



- Enabled through configuration setting: [CitrixDCHypervisor](#)
- Related configuration settings: *n/a*
- Supported platform: *Windows*

### List of Fields in the Raw Agent Data

| Field          | Description                                         | Data type | Unit | Example                              |
|----------------|-----------------------------------------------------|-----------|------|--------------------------------------|
| Id             | Hypervisor ID.                                      | String    |      | 10                                   |
| Name           | Hypervisor name.                                    | String    |      | XenServer1                           |
| SiteName       | Related Citrix site name.                           | String    |      | vl-Site                              |
| SiteGuid       | Related Citrix site GUID.                           | String    |      | 0a0fda60-aebf-4ac0-920d-44bd509ca927 |
| LifecycleState | Lifecycle state.<br>Possible values:<br>0, 1, 2, 3. | Number    |      | 2                                    |
| CustomerId     | Citrix Cloud CustomerId.                            | String    |      | a230abcdej1e                         |

### List of Calculated Fields

| Field                     | Description                                                                                                                                                          | Data type | Unit | Example                    | Where available                  |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|----------------------------|----------------------------------|
| LifecycleStateDisplayname | Lifecycle state name.<br>Possible values:<br><a href="#">Active</a> ,<br><a href="#">Deleted</a> ,<br><a href="#">RequiresResolution</a> ,<br><a href="#">Stub</a> . | String    |      | Active                     | Splunk data model,<br>Splunk SPL |
| SiteNameExtended          | Site name including the Citrix Cloud CustomerId.                                                                                                                     | String    |      | cloudxdsite (a230abcdej1e) | Splunk data model                |

## Licenses

uberAgent collects metrics like site name and ID as well as license server for each active license in a site.

### Details

- Source type: `uberAgent:Citrix:Licenses`
- Used in dashboards: *Citrix Virtual Apps and Desktops Licensing*
- Enabled through configuration setting: `CitrixDCLicenseInformation`
- Related configuration settings: *n/a*
- Supported platform: *Windows, Citrix Virtual Apps and Desktops on-premises*

### List of Fields in the Raw Agent Data

| Field                            | Description                                                                                                                      | Data type | Unit | Example                              |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-----------|------|--------------------------------------|
| SiteName                         | Related Citrix site name.                                                                                                        | String    |      | vl-Site                              |
| SiteGuid                         | Related Citrix site GUID.                                                                                                        | String    |      | 0a0fda60-aebf-4ac0-920d-44bd509ca927 |
| LicenseServer                    | License server.                                                                                                                  | String    |      | licsrv1                              |
| LicenseProductName               | License product name. Possible values: <code>XDS</code> , <code>XDT</code> , <code>MPS</code> .                                  | String    |      | XDT                                  |
| LicenseEdition2                  | License edition. Possible values: <code>PLT</code> , <code>ENT</code> , <code>APP</code> , <code>STD</code> , <code>ADV</code> . | String    |      | PLT                                  |
| LicenseExpirationDate            | License expiration date.                                                                                                         | String    |      | 2019-04-16<br>02:00:00.000<br>+0200  |
| LicenseSubscriptionAdvantageDate | License subscription advantage date.                                                                                             | String    |      | 2019-03-16<br>02:00:00.000<br>+0200  |
| LicenseType                      | License type.                                                                                                                    | String    |      | NFR                                  |

| Field                | Description                                                                                      | Data type | Unit | Example        |
|----------------------|--------------------------------------------------------------------------------------------------|-----------|------|----------------|
| LicenseTypeLocalized | license type localized.                                                                          | String    |      | Not For Resale |
| LicensesInUse        | Indicates how many licenses were in use.                                                         | Number    |      | 5              |
| LicensesAvailable    | Indicates how many licenses were available.                                                      | Number    |      | 100            |
| LicenseOverdraft     | Indicates how many overdraft licenses were in use.                                               | Number    |      | 0              |
| LicenseModel         | License model. Possible values: <a href="#">CCS</a> , <a href="#">UD</a> , <a href="#">CCU</a> . | String    |      | UD             |

### List of Calculated Fields

| Field                     | Description                                                                                                                | Data type | Unit | Example    | Where available               |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------|-----------|------|------------|-------------------------------|
| LicenseProductDisplayName | Product name. Possible values: <a href="#">XenDesktop (Legacy)</a> , <a href="#">XenDesktop</a> , <a href="#">XenApp</a> . | String    |      | XenDesktop | Splunk data model, Splunk SPL |

| Field                 | Description                                                                                                                           | Data type | Unit | Example          | Where available                  |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------------|----------------------------------|
| LicenseEditionDisplay | License edition.<br>Possible values:<br>Platinum Edition,<br>Enterprise Edition,<br>App Edition,<br>VDI Edition,<br>Advanced Edition. | String    |      | Platinum Edition | Splunk data model,<br>Splunk SPL |
| LicenseModelDisplay   | License model.<br>Possible values:<br>Concurrent,<br>,<br>User/Device,<br>Concurrent.                                                 | String    |      | User/Device      | Splunk data model,<br>Splunk SPL |

## Machines

uberAgent collects metrics like machine name and ID as well as the load index for each machine in a site. The terms "desktop group" and "delivery group" are used interchangeably.

### Details

- Source type: `uberAgent:Citrix:Machines`
- Used in dashboards: *Citrix Virtual Apps and Desktops Machines*, *Citrix Virtual Apps and Desktops*
- Enabled through configuration setting: `CitrixDCMachine`
- Related configuration settings: *n/a*

- Supported platform: *Windows, Citrix Virtual Apps and Desktops on-premises, Citrix Cloud*

**List of Fields in the Raw Agent Data**

---

| Field              | Description                                   | Data type | Unit | Example                                       |
|--------------------|-----------------------------------------------|-----------|------|-----------------------------------------------|
| Id                 | Machine ID.                                   | String    |      | 10                                            |
| Sid                | Machine SID.                                  | String    |      | S-1-5-21-3286265390-2319899195-874027928-2628 |
| Name               | Machine name with Active Directory domain.    | String    |      | Domain\VM1                                    |
| NameHost           | Machine name without Active Directory domain. | String    |      | VM1                                           |
| SiteName           | Related Citrix site name.                     | String    |      | vl-Site                                       |
| SiteGuid           | Related Citrix site GUID.                     | String    |      | 0a0fda60-aebf-4ac0-920d-44bd509ca927          |
| EffectiveLoadIndex | Effective load index.                         | Number    |      | 10000                                         |
| DnsName            | Machine name with full qualified domain name. | String    |      | VM1.domain.ad                                 |
| LifecycleState     | Lifecycle state. Possible values: 0, 1, 2, 3. | Number    |      | 1                                             |
| IPAddress          | IP address.                                   | String    |      | 10.1.1.100                                    |
| HostedMachineId    | Hypervisor identifier for this Machine.       | String    |      | F8143B4F-7371-4efa-868A-54787EF9F64E          |

| Field               | Description                                                                                                           | Data type | Unit | Example              |
|---------------------|-----------------------------------------------------------------------------------------------------------------------|-----------|------|----------------------|
| HostingServerName   | DNS name of the hypervisor that is hosting the machine if managed.                                                    | String    |      | XenServer1.domain.ad |
| HostedMachineName   | The friendly name of a hosted machine as used by its hypervisor. This is not necessarily the DNS name of the machine. | String    |      | XenServer1           |
| IsAssigned          | Indicates if machine is assigned. Possible values: 0, 1.                                                              | String    |      | 1                    |
| IsInMaintenanceMode | Indicates if machine is in maintenance mode. Possible values: 0, 1.                                                   | String    |      | 0                    |
| IsPendingUpdate     | Indicates if machine is in pending update state. Possible values: 0, 1.                                               | String    |      | 0                    |
| AgentVersion        | Citrix VDA version.                                                                                                   | String    |      | 7.15.1000.150        |

| Field                    | Description                                                                                                                                                                   | Data type | Unit | Example             |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|---------------------|
| AssociatedUserFullNames  | Full names of the users that have been associated with the machine. Associated users are the current user(s) for shared machines and the assigned users for private machines. | String    |      | Testuser 1          |
| AssociatedUserNames      | Ussernames of the users that have been associated with the machine. Associated users are the current user(s) for shared machines and the assigned users for private machines. | String    |      | AD\Testuser1        |
| AssociatedUserUPNs       | The User Principal Names of the users associated with the machine. Associated users are the current user(s) for shared machines and the assigned users for private machines.  | String    |      | Testuser1@domain.ad |
| CurrentRegistrationState | Current registration state. Possible values: 0, 1, 2.                                                                                                                         | Number    |      | 1                   |

| Field                       | Description                                                                                                                                                   | Data type | Unit | Example                             |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-------------------------------------|
| RegistrationStateChangeDate | Date when the registration state changed.                                                                                                                     | String    |      | 2018-07-29<br>03:03:43.953<br>+0200 |
| LastDeregisteredCode        | Machine's last deregistration code. Possible values: too many to list here. Please have a look at the <a href="#">citrix_deregistrationreasoncode</a> lookup. | Number    |      | 207                                 |
| LastDeregisteredDate        | Machine's last deregistration date.                                                                                                                           | String    |      | 2018-07-29<br>02:33:34.037<br>+0200 |
| CurrentPowerState           | Current power state. Possible values: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.                                                                                       | Number    |      | 9                                   |
| CurrentSessionCount         | Current session count.                                                                                                                                        | Number    |      | 20                                  |
| ControllerDnsName           | Controller name.                                                                                                                                              | String    |      | DDC1.domain.ad                      |
| PoweredOnDate               | Date when machine was powered on.                                                                                                                             | String    |      | 2018-03-16<br>15:18:27.407<br>+0200 |
| PowerStateChangeDate        | Date when power state changed.                                                                                                                                | String    |      | 2018-03-16<br>15:18:27.407<br>+0200 |
| FunctionalLevel             | Functional level. Possible values: 0, 1, 2, 3, 4, 5, 6.                                                                                                       | Number    |      | 6                                   |
| FailureDate                 | Date when machine failed.                                                                                                                                     | String    |      | 2018-03-16<br>15:18:27.407<br>+0200 |



| Field                     | Description                                                            | Data type | Unit | Example                              |
|---------------------------|------------------------------------------------------------------------|-----------|------|--------------------------------------|
| WindowsConnectionSettings | Windows connection setting. Possible values: 0, 1, 2, 3, 4.            | Number    |      | 1                                    |
| IsPreparing               | Indicates if the machine is in preparing state. Possible values: 0, 1. | String    |      | 0                                    |
| FaultState                | Fault state. Possible values: 0, 1, 2, 3, 4, 5.                        | Number    |      | 1                                    |
| CatalogId                 | Related catalog ID.                                                    | String    |      | 10                                   |
| DesktopGroupId            | Related desktop group ID.                                              | String    |      | 05bddbe7-cf12-4ee2-ab02-93d0428d3847 |
| HypervisorId              | Related hypervisor ID.                                                 | String    |      | 10                                   |
| Hash                      | Hash.                                                                  | String    |      | CC7380E01A5FD3403708B7D3             |
| MachineRole               | Machine role. Possible values: 0, 1, 2.                                | Number    |      | 2                                    |
| HypervisorDisplayName     | Related hypervisor name.                                               | String    |      | XenServer1                           |
| CatalogDisplayName        | Related catalog name.                                                  | String    |      | Finance machines                     |
| DesktopGroupDisplayName   | Related desktop group name.                                            | String    |      | Finance                              |
| CreatedDate               | Machine creation date.                                                 | String    |      | 2018-03-16<br>14:16:07.008<br>+0200  |
| ModifiedDate              | Machine modification date.                                             | String    |      | 2018-03-16<br>14:16:07.008<br>+0200. |
| Tags                      | Configured tags.                                                       | String    |      | Germany France                       |

| Field      | Description              | Data type | Unit | Example      |
|------------|--------------------------|-----------|------|--------------|
| CustomerId | Citrix Cloud CustomerId. | String    |      | a230abcdej1e |

### List of Calculated Fields

| Field                     | Description                                                                                                                                                        | Data type | Unit | Example | Where available               |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|---------|-------------------------------|
| LifecycleStateDisplayName | Lifecycle state name. Possible values: <a href="#">Active</a> , <a href="#">Deleted</a> , <a href="#">RequiresResolution</a> , <a href="#">Stub</a> .              | String    |      | Active  | Splunk data model, Splunk SPL |
| IsVDA                     | Indicates if machine is a VDA. Possible values: 0, 1. Is 1 if field <a href="#">MachineRoleDisplayName</a> is either <a href="#">Vda</a> or <a href="#">Both</a> . | String    |      | 1       | Splunk data model             |
| IsVDANumber               | Indicates if machine is a VDA. Possible values: 0, 1. Is 1 if field <a href="#">MachineRoleDisplayName</a> is either <a href="#">Vda</a> or <a href="#">Both</a> . | Number    |      | 1       | Splunk data model             |

| Field                    | Description                                                                                                                                               | Data type | Unit | Example    | Where available               |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------|-------------------------------|
| IsDDC                    | Indicates if machine is a DDC. Possible values: 0, 1. Is 1 if field <code>MachineRoleDisplayName</code> is either <code>Ddc</code> or <code>Both</code> . | String    |      | 1          | Splunk data model             |
| IsRegistered             | Indicates if machine registered. Possible values: 0, 1. Is 1 if field <code>CurrentRegistrationState</code> is 1.                                         | String    |      | 1          | Splunk data model             |
| IsRegisteredNumber       | Indicates if machine registered. Possible values: 0, 1. Is 1 if field <code>CurrentRegistrationState</code> is 1.                                         | Number    |      | 1          | Splunk data model             |
| CurrentRegistrationState | Current registration state. Possible values: <code>Unknown</code> , <code>Registered</code> , <code>Unregistered</code> .                                 | String    |      | Registered | Splunk data model, Splunk SPL |

| Field                  | Description                                                                                                                                                                                                                                                                                                                                      | Data type | Unit | Example     | Where available               |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-------------|-------------------------------|
| LastDeregisteredCode   | Code displayed at deregistration code. Possible values: too many to list here. Please have a look at the <a href="#">citrix_deregistrationreasoncode</a> lookup.                                                                                                                                                                                 | String    |      | ContactLost | Splunk data model, Splunk SPL |
| CurrentPowerState      | Current power state. Possible values: <a href="#">Unknown</a> , <a href="#">Unavailable</a> , <a href="#">Off</a> , <a href="#">On</a> , <a href="#">Suspended</a> , <a href="#">TurningOn</a> , <a href="#">TurningOff</a> , <a href="#">Suspending</a> , <a href="#">Resuming</a> , <a href="#">Unmanaged</a> , <a href="#">NotSupported</a> . | String    |      | Unmanaged   | Splunk data model, Splunk SPL |
| FunctionalLevelDisplay | Functional level. Possible values: <a href="#">Unknown</a> , <a href="#">L5</a> , <a href="#">L7</a> , <a href="#">L7_6</a> , <a href="#">L7_7</a> , <a href="#">L7_8</a> , <a href="#">L7_9</a> / <a href="#">MAX</a> .                                                                                                                         | String    |      | L7_9 / MAX  | Splunk data model, Splunk SPL |

| Field                            | Description                                                                                                        | Data type | Unit | Example                    | Where available               |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------|-----------|------|----------------------------|-------------------------------|
| WindowsConnectivityDisplayString | Windows connection setting. Possible values: Unknown, LogonEnabled, Draining, DrainingUntilRestart, LogonDisabled. | String    |      | Unknown                    | Splunk data model, Splunk SPL |
| FaultStateDisplayName            | Fault state. Possible values: Unknown, None, FailedToStart, StuckOnBoot, Unregistered, MaxCapacity.                | String    |      | None                       | Splunk data model, Splunk SPL |
| MachineRoleDisplayName           | Machine role. Possible values: Vda, Ddc, Both.                                                                     | String    |      | Both                       | Splunk data model, Splunk SPL |
| TagsSplit                        | Tags split by semicolon.                                                                                           | String    |      | Germany;France             | Splunk data model             |
| SiteNameExtended                 | Site name including the Citrix Cloud CustomerId.                                                                   | String    |      | cloudxdsite (a230abcdej1e) | Splunk data model             |

## Machine Catalogs

uberAgent collects metrics like catalog name and ID as well as site name for each machine catalog in a site.

### Details

- Source type: `uberAgent:Citrix:Catalogs`
- Used in dashboards: *Citrix Virtual Apps and Desktops Machines*
- Enabled through configuration setting: `CitrixDCCatalog`
- Related configuration settings: *n/a*
- Supported platform: *Windows, Citrix Virtual Apps and Desktops on-premises, Citrix Cloud*

### List of Fields in the Raw Agent Data

| Field                 | Description                                                                             | Data type | Unit | Example                              |
|-----------------------|-----------------------------------------------------------------------------------------|-----------|------|--------------------------------------|
| Id                    | Machine catalog ID.                                                                     | String    |      | 10                                   |
| Name                  | Machine catalog name.                                                                   | String    |      | Finance machines                     |
| SiteName              | Related Citrix site name.                                                               | String    |      | vl-Site                              |
| SiteGuid              | Related Citrix site GUID.                                                               | String    |      | 0a0fda60-aebf-4ac0-920d-44bd509ca927 |
| LifecycleState        | Lifecycle state.<br>Possible values:<br>0, 1, 2, 3.                                     | Number    |      | 0                                    |
| ProvisioningType      | Provisioning type.<br>Possible values:<br>0, 1, 2, 3.                                   | Number    |      | 1                                    |
| PersistentUserChanges | Indicates if and where user changes should be saved.<br>Possible values:<br>0, 1, 2, 3. | Number    |      | 1                                    |

| Field                | Description                                                                           | Data type | Unit | Example                              |
|----------------------|---------------------------------------------------------------------------------------|-----------|------|--------------------------------------|
| IsMachinePhysical    | Indicates if machine catalog contains physical machines.<br>Possible values:<br>0, 1. | String    |      | 0                                    |
| AllocationType       | Allocation type.<br>Possible values:<br>0, 1, 2, 3.                                   | Number    |      | 2                                    |
| SessionSupport       | Indicates a machine catalog's session support.<br>Possible values:<br>0, 1, 2.        | Number    |      | 1                                    |
| ProvisioningSchemeId | Associated provisioning scheme Id.                                                    | String    |      | 0a0fda60-aebf-4ac0-920d-44bd509ca927 |
| CreatedDate          | Machine catalog creation date.                                                        | String    |      | 2018-03-16<br>14:16:07.008<br>+0200  |
| ModifiedDate         | Machine catalog modification date.                                                    | String    |      | 2018-03-16<br>14:16:07.008<br>+0200  |
| CustomerId           | Citrix Cloud CustomerId.                                                              | String    |      | a230abcdej1e                         |

### List of Calculated Fields

| Field     | Description                           | Data type | Unit | Example | Where available   |
|-----------|---------------------------------------|-----------|------|---------|-------------------|
| CatalogId | Content of field <a href="#">Id</a> . | String    |      | 10      | Splunk data model |

| Field                             | Description                                                                                               | Data type | Unit | Example | Where available                  |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------|-----------|------|---------|----------------------------------|
| LifecycleStateDisplayNames        | State name.<br>Possible values:<br>Active,<br>Deleted,<br>RequiresResolution,<br>Stub.                    | String    |      | Active  | Splunk data model,<br>Splunk SPL |
| ProvisioningTypeDisplayNames      | Display name type. Possible values:<br>Unknown,<br>MCS, PVS,<br>Manual.                                   | String    |      | MCS     | Splunk data model,<br>Splunk SPL |
| PersistentUserChangesDisplayNames | and where user changes should be saved.<br>Possible values:<br>Unknown,<br>Discard,<br>OnLocal,<br>OnPvd. | String    |      | Discard | Splunk data model,<br>Splunk SPL |
| AllocationTypeDisplayNames        | Allocation type. Possible values:<br>Unknown,<br>Static,<br>Random,<br>Permanent.                         | String    |      | Random  | Splunk data model,<br>Splunk SPL |



| Field                     | Description                                                                                                                                             | Data type | Unit | Example                    | Where available               |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|----------------------------|-------------------------------|
| SessionSupportDisplayname | Display name of the machine catalog's session support. Possible values: <code>Unknown</code> , <code>SingleSession</code> , <code>MultiSession</code> . | String    |      | SingleSession              | Splunk data model, Splunk SPL |
| SiteNameExtendedSite      | Site name including the Citrix Cloud CustomerId.                                                                                                        | String    |      | cloudxdsite (a230abcdej1e) | Splunk data model             |

## Machine Metrics

July 9, 2024

## Machine Blue Screens & Hangs Metrics

July 9, 2024

### Blue Screens and Hangs

uberAgent collects information on every blue screen and hang, like the type of error (blue screen, hard power off or hang) and the stop error code.

**Details**

- Source type: [uberAgent: System: Bugcheck](#)
- Used in dashboards: *Stop Errors (Blue Screen & Power Loss)*
- Enabled through configuration setting: [ApplicationErrors](#)
- Related configuration settings: *n/a*
- Supported platform: *Windows*

**List of Fields in the Raw Agent Data**

---

| Field             | Description                                                                                                                                                                           | Data type | Unit | Example        |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|----------------|
| BugcheckCode      | Stop error code ID. Possible values: too many to list here. Please check the lookup file <a href="#">bugcheck_codes.csv</a> or <a href="#">Microsoft's bug check code reference</a> . | Number    |      | 0x1            |
| BugcheckParameter | Stop error parameter 1. The meaning of this value depends on the bugcheck code and can be looked up in <a href="#">Microsoft's bug check code reference</a> .                         | String    |      | 0x7ffd8e8c7864 |

---

| Field              | Description                                                                                                                                                   | Data type | Unit | Example            |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|--------------------|
| BugcheckParameter2 | Stop error parameter 2. The meaning of this value depends on the bugcheck code and can be looked up in <a href="#">Microsoft's bug check code reference</a> . | String    |      | 0x1                |
| BugcheckParameter3 | Stop error parameter 3. The meaning of this value depends on the bugcheck code and can be looked up in <a href="#">Microsoft's bug check code reference</a> . | String    |      | 0x0                |
| BugcheckParameter4 | Stop error parameter 4. The meaning of this value depends on the bugcheck code and can be looked up in <a href="#">Microsoft's bug check code reference</a> . | String    |      | 0xffffe181ead22b80 |
| SleepInProgress    | Indicates if the machine was in sleep mode when stop error occurred.<br>Possible values:<br>0, 1.                                                             | Number    |      | 0                  |

| Field                      | Description                                                                                                                                                                         | Data type | Unit | Example            |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|--------------------|
| PowerButtonTimestamp       | Indicates if the power button on the computer was pushed and held for at least four seconds. Possible values: 0 or Windows FILETIME timestamp of when the power button was pressed. | Number    |      | 131768171003182508 |
| PowerButtonTimestampEpoch  | Indicates if the power button on the computer was pushed and held for at least four seconds. Possible values: 0 or Unix epoch timestamp of when the power button was pressed.       | Number    |      | 1532343500318      |
| BootAppStatus              | n/a                                                                                                                                                                                 | String    |      | 0                  |
| Checkpoint                 | n/a                                                                                                                                                                                 | Number    |      | 0                  |
| ConnectedStandbyInProgress | Indicates if the machine was in connected standby mode when a stop error occurred. Possible values: 0, 1.                                                                           | String    |      | 0                  |

| Field                          | Description                                                                                                             | Data type | Unit | Example |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------|-----------|------|---------|
| SystemSleepTransitionIndicates | Indicates if the machine was in the transition from sleep to on mode when a stop error occurred. Possible values: 0, 1. | Number    |      | 0       |
| CsEntryScenarioInstance        |                                                                                                                         | Number    |      | 0       |

### List of Calculated Fields

| Field                    | Description                                                                                                                                                                               | Data type | Unit | Example        | Where available   |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|----------------|-------------------|
| BugcheckCodeDisplay Name | Display Name code name. Possible values: too many to list here. Please check the lookup file <a href="#">bugcheck_codes.csv</a> or <a href="#">Microsoft's bug check code reference</a> . | String    |      | Hard power off | Splunk data model |

### Interpreting the Data

The data collected by uberAgent helps to identify three different types of blue screens and hangs:

**”Normal” Bugcheck** Conditions:

- `BugcheckCode > 0`

Explanation: the bugcheck code can be determined and written to disk before the computer shuts down or restarts.

**Hard Power Off** Conditions:

- `PowerButtonTimestamp > 0`

Explanation: the machine was turned off by pressing and holding the power button for at least 4 seconds.

**Random Restart** Conditions:

- `BugcheckCode = 0`
- `PowerButtonTimestamp = 0`

Explanation: power loss or hard hang.

## Machine Inventory Metrics

July 9, 2024

### Machine Inventory

Contains inventory metrics for machines like operating system name and hardware manufacturer.

#### Details

- Source type: `uberAgent:System:MachineInventory`
- Used in dashboards: *Machine Inventory*, *Single Machine Inventory*, *Single Application Inventory*, *Update Inventory*
- Enabled through configuration setting: `MachineInventory`
- Related configuration settings: *n/a*

#### List of Fields in the Raw Agent Data

| Field                 | Description                                                                                                                                                                    | Data type | Unit | Example              | Platform |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|----------------------|----------|
| OsName                | Operating system name.                                                                                                                                                         | String    |      | Windows 7 Enterprise | all      |
| OsSpName              | Operating system service pack name.                                                                                                                                            | String    |      | Service Pack 1       | Win      |
| OsVersion             | Operating system version.                                                                                                                                                      | Number    |      | 6.1                  | all      |
| OsBuild               | Operating system build.                                                                                                                                                        | Number    |      | 7601                 | Win      |
| OsBuildString         | Operating system build.                                                                                                                                                        | String    |      | 19D76                | Mac      |
| OsUpdateBuildRevision | Operating system Update Build Revision number. <a href="#">More information.</a>                                                                                               | Number    |      | 165                  | Win      |
| OsArchitecture        | Operating system architecture.                                                                                                                                                 | String    |      | x64                  | all      |
| OsSpVersion           | Operating system service pack version.                                                                                                                                         | Number    |      | 1.0                  | Win      |
| OsType                | Operating system type.<br>Possible values:<br><a href="#">Client</a> ,<br><a href="#">Domain Controller</a> ,<br><a href="#">Server</a> ,<br><a href="#">Terminal Server</a> . | String    |      | Client               | all      |

| Field                 | Description                           | Data type | Unit | Example                                                           | Platform |
|-----------------------|---------------------------------------|-----------|------|-------------------------------------------------------------------|----------|
| OsInstallDate         | Operating system installation date.   | String    |      | 2018-04-13                                                        | Win      |
| HwManufacturer        | Hardware manufacturer.                | String    |      | LENOVO                                                            | all      |
| HwModel               | Hardware model.                       | String    |      | ThinPad T470s                                                     | all      |
| HwBiosVersion         | Hardware bios version.                | String    |      | N1WET46W (1.25)                                                   | Win      |
| AdDomainDns           | Active Directory DNS domain name.     | String    |      | vastlimits.com                                                    | Win      |
| AdDomainNetBios       | Active Directory NetBios name.        | String    |      | VASTLIMITS                                                        | Win      |
| AdSite                | Active Directory site.                | String    |      | Default-First-Site-Name                                           | Win      |
| AdOu                  | Active Directory organizational unit. | String    |      | vast limits/Computers/Clients                                     | Win      |
| ComputerNameDn        | Computer name Dn formatted.           | String    |      | CN=Client1,OU=Clients,OU=Computers,OU=limits,DC=vastlimits,DC=com | Win      |
| ComputerNameCanonical | Computer name canonical formatted.    | String    |      | vastlimits.com/Computers/Clients/Client1                          | Win      |
| CtxFarmName           | Citrix farm name.                     | String    |      | vast limits Farm                                                  | Win      |
| CtxMachineCatalogName | Citrix machine catalog name.          | String    |      | Machine Catalog 1                                                 | Win      |
| CtxDeliveryGroupName  | Citrix delivery group name.           | String    |      | Delivery Group 1                                                  | Win      |
| RAMSizeGB             | RAM size.                             | Number    | GB   | 15.86                                                             | all      |



| Field                         | Description                                                                          | Data type | Unit | Example | Platform |
|-------------------------------|--------------------------------------------------------------------------------------|-----------|------|---------|----------|
| PowerSupportsConnectedStandby | Indicates if the operating system supports Connected Standby. Possible values: 0, 1. | String    |      | 0       | Win      |
| PowerSupportsS1               | Indicates if the operating system supports sleep state S1. Possible values: 0, 1.    | String    |      | 0       | Win      |
| PowerSupportsS2               | Indicates if the operating system supports sleep state S2. Possible values: 0, 1.    | String    |      | 0       | Win      |
| PowerSupportsS3               | Indicates if the operating system supports sleep state S3. Possible values: 0, 1.    | String    |      | 0       | Win      |
| PowerSupportsS4               | Indicates if the operating system supports sleep state S4. Possible values: 0, 1.    | String    |      | 1       | Win      |

| Field             | Description                                                                                 | Data type | Unit | Example                                           | Platform |
|-------------------|---------------------------------------------------------------------------------------------|-----------|------|---------------------------------------------------|----------|
| PowerSupportsS5   | Indicates if the operating system supports sleep state S5. Possible values: 0, 1.           | String    |      | 1                                                 | Win      |
| IsUpsPresent      | Indicates if there is an uninterruptible power supply (UPS) present. Possible values: 0, 1. | String    |      | 0                                                 | all      |
| IsBatteryPresent  | Indicates if there is a battery present. Possible values: 0, 1.                             | String    |      | 1                                                 | all      |
| BatteryWearLevel  | Percent of battery capacity gone. The accuracy strongly depends on the built-in hardware.   | Number    | %    | 7.8                                               | all      |
| CPUName           | CPU name.                                                                                   | String    |      | Intel(R)<br>Core(TM)<br>i7-7500U CPU<br>@ 2.70GHz | all      |
| CPU.Sockets       | CPU sockets.                                                                                | Number    |      | 1                                                 | Win      |
| CPU.CoresPhysical | CPU physical cores.                                                                         | Number    |      | 2                                                 | all      |
| CPU.CoresLogical  | CPU logical cores.                                                                          | Number    |      | 4                                                 | all      |

| Field              | Description                                                       | Data type | Unit | Example      | Platform         |
|--------------------|-------------------------------------------------------------------|-----------|------|--------------|------------------|
| CPUMaxMhz          | CPU base frequency.                                               | Number    | MHz  | 2904         | all              |
| HwHypervisorVendor | Detected hypervisor technology for this system.                   | String    |      | Microsoft Hv | Win, Mac (Intel) |
| HwIsVirtualMachine | Indicates if machine is a virtual machine. Possible values: 0 ,1. | String    |      | 0            | all              |
| BIOSerial          | BIOS serial number.                                               | String    |      | YM5S012345   | Win              |
| BaseboardSerial    | Baseboard serial number.                                          | String    |      | 50123445     | Win              |
| IsSipEnabled       | Status of the System Integrity Protection.                        | String    |      | 1            | Mac              |

### List of Calculated Fields

| Field               | Description                                                                                                                                             | Data type | Unit | Example               | Where available   |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-----------------------|-------------------|
| OsBuildUbr          | Operating system build and Update Build Revision combined. For operating systems lower than Windows 10 it is just the content of <code>OsBuild</code> . | Number    |      | 17134.165             | Splunk data model |
| HwManufacturerModel | Hardware manufacturer and model combined.                                                                                                               | String    |      | LENOVO ThinkPad T470s | Splunk data model |

## Disk Inventory

Contains inventory metrics for physical disks like disk name and capacity.

### Details

- Source type: `uberAgent:System:DiskInventory`
- Used in dashboards: *Machine Storage*
- Enabled through configuration setting: `MachineInventory`
- Related configuration settings: *n/a*

### List of Fields in the Raw Agent Data

| Field | Description | Data type | Unit | Example                    | Platform |
|-------|-------------|-----------|------|----------------------------|----------|
| Name  | Disk name.  | String    |      | SAMSUNG MZVLW1T0HMLH-000L7 | all      |

---

| Field       | Description                                                | Data type | Unit | Example | Platform |
|-------------|------------------------------------------------------------|-----------|------|---------|----------|
| Enumerator  | Disk enumerator (e.g., IDE, SCSI, USBSTOR).                | String    |      | SCSI    | all      |
| DiskNumber  | Disk number.                                               | Number    |      | 0       | all      |
| CapacityMB  | Disk capacity.                                             | Number    | MB   | 976762  | all      |
| IsWritable  | Indicates if the disk is writable. Possible values: 0, 1.  | String    |      | 1       | all      |
| IsRemovable | Indicates if the disk is removable. Possible values: 0, 1. | String    |      | 0       | all      |

---

## Monitor Inventory

Contains inventory metrics for monitors like resolution and color depth.

### Details

- Source type: [uberAgent:System:MonitorInventory](#)
- Used in dashboards: *Machine Inventory*, *Single Machine Inventory*
- Enabled through configuration setting: [MachineInventory](#)
- Related configuration settings: *n/a*
- The fields "MonitorColorDepth" and "MonitorDisplayName" contain generic values for ARM-based systems under macOS.

### List of Fields in the Raw Agent Data

| Field              | Description                                                       | Data type | Unit | Example             | Platform |
|--------------------|-------------------------------------------------------------------|-----------|------|---------------------|----------|
| MonitorIndex       | Monitor index.                                                    | Number    |      | 1                   | all      |
| MonitorHRes        | Monitor horizontal resolution.                                    | Number    |      | 3440                | all      |
| MonitorVRes        | Monitor vertical resolution.                                      | Number    |      | 1440                | all      |
| MonitorColorDepth  | Monitor color depth.                                              | Number    |      | 32                  | all      |
| MonitorIsPrimary   | Indicates if a monitor is the primary one. Possible values: 0, 1. | String    |      | 1                   | all      |
| MonitorDisplayName | Monitor name.                                                     | String    |      | Generic PnP Monitor | all      |

## Network Configuration Information

Contains inventory metrics for network connections like interface type and SSIDs.

### Details

- Source type: [uberAgent:System:NetworkConfigInformation](#)
- Used in dashboards: *Machine Inventory*, *Single Machine Inventory*, *Machine Network Configuration*
- Enabled through configuration setting: [NetworkConfigInformation](#)
- Related configuration settings: *n/a*

### List of Fields in the Raw Agent Data

| Field                     | Description            | Data type | Unit | Example | Platform |
|---------------------------|------------------------|-----------|------|---------|----------|
| NetworkConfigFriendlyName | Network friendly name. | String    |      | WiFi    | all      |

| Field                                 | Description                                                                   | Data type | Unit | Example                                 | Platform |
|---------------------------------------|-------------------------------------------------------------------------------|-----------|------|-----------------------------------------|----------|
| NetworkConfigDescription              | Network description.                                                          | String    |      | Intel(R) Dual Band Wireless-AC 8265     | all      |
| NetworkConfigInterfaceType            | Interface type ID. Possible values: 0, 6, 23, 63, 71, 243.                    | Number    |      | 71                                      | all      |
| NetworkConfigInterfaceTypeDisplayName | Interface type name. Possible values: Other, Ethernet, VPN, ISDN, WiFi, WWAN. | String    |      | WiFi                                    | all      |
| NetworkConfigDNSSuffix                | DNS suffix.                                                                   | String    |      | fritz.box                               | all      |
| NetworkConfigSSID                     | Network SSID.                                                                 | String    |      | HomeWiFi                                | all      |
| NetworkConfigConnectedToInternet      | Whether the network is connected to the Internet. Possible values: 0, 1.      | String    |      | 1                                       | all      |
| NetworkConfigIPv4Address              | IPv4 address.                                                                 | IPv4      |      | 192.168.178.40                          | all      |
| NetworkConfigIPv6Address              | IPv6 address.                                                                 | String    |      | 2001:0db8:85a3:0000:0000:8a2e:0370:7334 | all      |
| NetworkConfigMACAddress               | MAC address.                                                                  | String    |      | AC-ED-5C-02-F0-30                       | all      |
| NetworkConfigWiFiSignalQuality        | WiFi signal quality.                                                          | Number    | %    | 100                                     | all      |
| NetworkConfigWiFiType                 | WiFi connection type.                                                         | Number    |      | 7                                       | all      |

| Field                                 | Description                 | Data type | Unit | Example | Platform |
|---------------------------------------|-----------------------------|-----------|------|---------|----------|
| NetworkConfigWiFiAuthenticationNumber | WiFi authentication method. | Number    |      | 7       | all      |

### List of Calculated Fields

| Field                                      | Description                       | Data type | Unit | Example        | Where available   |
|--------------------------------------------|-----------------------------------|-----------|------|----------------|-------------------|
| Ipv4Address                                | Ipv4 address.                     | IPv4      |      | 192.168.178.40 | Splunk data model |
| NetworkConfigWiFiTypeDisplayName           | WiFi type display name.           | String    |      | IEEE 802.11n   | Splunk data model |
| NetworkConfigWiFiAuthenticationDisplayname | WiFi authentication display name. | String    |      | WPA2           | Splunk data model |

### Volume Inventory

Contains inventory metrics for volumes like capacity and filesystem.

#### Details

- Source type: [uberAgent:System:VolumeInventory](#)
- Used in dashboards: *Machine Storage*
- Enabled through configuration setting: [MachineInventory](#)
- Related configuration settings: *n/a*

### List of Fields in the Raw Agent Data



| Field            | Description                                                    | Data type | Unit | Example                                | Platform |
|------------------|----------------------------------------------------------------|-----------|------|----------------------------------------|----------|
| Guid             | Volume GUID.                                                   | String    |      | {d4eadd95-6dce-426e-b55b-521800346789} | all      |
| DeviceName       | Device name.                                                   | String    |      | DeviceHarddiskVolume3                  | all      |
| Label            | Volume label.                                                  | String    |      | Windows                                | all      |
| FileSystem       | Volume file system.                                            | String    |      | NTFS                                   | all      |
| MountPoints      | Volume mount points.                                           | String    |      | C                                      | all      |
| DiskNumbers      | Disk numbers.                                                  | String    |      | 0                                      | all      |
| FreeMB           | Volume free capacity.                                          | Number    |      | 695395                                 | all      |
| CapacityMB       | Volume capacity.                                               | Number    |      | 975485                                 | all      |
| UsedSpacePercent | Volume used space.                                             | Number    | %    | 29                                     | all      |
| PartitionStyle   | Volume partition style.                                        | String    |      | GPT                                    | all      |
| IsSystemVolume   | Indicates if volume is a system volume. Possible values: 0, 1. | String    |      | 1                                      | Win      |
| IsBootVolume     | Indicates if volume is a boot volume. Possible values: 0, 1.   | String    |      | 1                                      | all      |

---

| Field   | Description                                                                                        | Data type | Unit | Example | Platform |
|---------|----------------------------------------------------------------------------------------------------|-----------|------|---------|----------|
| IsDirty | Indicates if volume has a dirty bit. If yes, the volume might be corrupted. Possible values: 0, 1. | String    |      | 0       | Win      |

---

### List of Calculated Fields

---

| Field              | Description                                                                                        | Data type | Unit | Example | Where available   |
|--------------------|----------------------------------------------------------------------------------------------------|-----------|------|---------|-------------------|
| IsBootVolumeNumber | Indicates if volume is a boot volume. Possible values: 0, 1.                                       | Number    |      | 1       | Splunk data model |
| IsDirtyNumber      | Indicates if volume has a dirty bit. If yes, the volume might be corrupted. Possible values: 0, 1. | Number    |      | 0       |                   |

---

## Machine Performance And Utilization Metrics

July 9, 2024

### GPU Usage

uberAgent collects information about GPU compute and memory usage.

## Details

- Source type: `uberAgent:System:GpuUsage`
- Used in dashboards: *Machine GPU, Analyze data over time*
- Enabled through configuration setting: `GpuUsage`
- Related configuration settings: *n/a*
- Supported platform: *Windows*

## List of Fields in the Raw Agent Data

| Field                         | Description                | Data type | Unit | Example                  |
|-------------------------------|----------------------------|-----------|------|--------------------------|
| DisplayAdapterName            | GPU name.                  | String    |      | Intel(R) HD Graphics 520 |
| DisplayAdapterIndex           | GPU index.                 | Number    |      | 1                        |
| MemorySharedMB                | Shared memory usage.       | Number    | MB   | 512                      |
| MemoryDedicatedMB             | Dedicated memory usage.    | Number    | MB   | 64                       |
| MemorySharedPercent           | Shared memory usage.       | Number    | %    | 50                       |
| MemoryDedicatedPercent        | Dedicated memory usage.    | Number    | %    | 50                       |
| MemorySharedSizeMB            | Shared memory size.        | Number    | MB   | 1024                     |
| MemoryDedicatedSizeMB         | Dedicated memory size.     | Number    | MB   | 128                      |
| ComputeUsagePercentAllEngines | GPU usage for all engines. | Number    | %    | 10.00                    |

## List of Calculated Fields

| Field                           | Description            | Data type | Unit | Example | Where available   |
|---------------------------------|------------------------|-----------|------|---------|-------------------|
| DisplayAdapterIndex - validated | GPU index - validated. | Number    |      | 1       | Splunk data model |

## GPU Usage per Engine

uberAgent collects information about GPU compute usage per engine. This requires Windows 10 1709 or newer. On older versions of Windows `ComputeUsagePercentEngineN` is populated instead.

### Details

- Source type: `uberAgent:System:GpuUsageEngine`
- Used in dashboards: *Machine GPU*
- Enabled through configuration setting: `GpuUsage`
- Related configuration settings: *n/a*
- Supported platform: *Windows*

### List of Fields in the Raw Agent Data

---

| Field                                     | Description                                                     | Data type | Unit | Example |
|-------------------------------------------|-----------------------------------------------------------------|-----------|------|---------|
| <code>DisplayAdapterIndex</code>          | GPU index.                                                      | Number    |      | 1       |
| <code>GpuEngineIndex</code>               | GPU engine index.                                               | Number    |      | 8       |
| <code>GpuEngineType</code>                | GPU engine type ID. Possible values: 0, 1, 2, 3, 4, 5, 6, 7, 8. | Number    |      | 4       |
| <code>GpuEngineComputeUsagePercent</code> | GPU engine compute usage.                                       | Number    | %    | 10.00   |

---

### List of Calculated Fields

| Field                    | Description                                                                                                                                                                        | Data type | Unit | Example                  | Where available   |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|--------------------------|-------------------|
| GpuEngineCombined        | <pre> "GPU" + DisplayAdapterIndex + "-E" + GpuEngineIndex + " - " + GpuEngineTypeDisplayName           </pre>                                                                      | String    |      | GPU1-E8-Video processing | Splunk data model |
| GpuEngineTypeDisplayName | <p>GPU engine type name.</p> <p>Possible values:</p> <pre> Other, 3D, Video decode, Video encode, Video processing, Scene assembly, Copy, Legacy overlay, Crypto.           </pre> | String    |      | Video processing         | Splunk data model |

## SMB Client Performance

uberAgent collects metrics per network share the endpoint is connected to, such as share path and latency.

### Details

- Source type: `uberAgent:System:SmbClient`
- Used in dashboards: *SMB Client Performance*, *Machine Storage*, *Machine Uptime*, *Analyze data over time*

- Enabled through configuration setting: [SMBClientSharePerformance](#)
- Related configuration settings: *n/a*
- Supported platform: *Windows*

### List of Fields in the Raw Agent Data

---

| Field            | Description                                | Data type | Unit | Example   |
|------------------|--------------------------------------------|-----------|------|-----------|
| SharePath        | Share path.                                | String    |      | \dc1\home |
| IOPSRead         | I/O operations read.                       | Number    |      | 100       |
| IOPSWrite        | I/O operations write.                      | Number    |      | 100       |
| IOPSMetadata     | I/O operations metadata.                   | Number    |      | 100       |
| IOCountRead      | Count of read I/O operations.              | Number    |      | 20        |
| IOCountWrite     | Count of write I/O operations.             | Number    |      | 20        |
| IOCountMetadata  | Count of metadata I/O operations.          | Number    |      | 20        |
| IOMBRead         | Amount of read I/O operation data volume.  | Number    | MB   | 30        |
| IOMBWrite        | Amount of write I/O operation data volume. | Number    | MB   | 30        |
| IOLatencyMsRead  | Latency of read I/O operations.            | Number    | ms   | 5         |
| IOLatencyMsWrite | Latency of write I/O operations.           | Number    | ms   | 5         |

---

### List of Calculated Fields

| Field             | Description                            | Data type | Unit | Example | Where available   |
|-------------------|----------------------------------------|-----------|------|---------|-------------------|
| IOPSRW            | $IOPSRead + IOPSWrite.$                | Number    |      | 200     | Splunk data model |
| IOCountRW         | $IOCountRead + IOCountWrite$           | Number    |      | 40      | Splunk data model |
| IODurationReadMs  | $IOLatencyMsRead \times IOCountRead$   | Number    | ms   | 100     | Splunk data model |
| IODurationWriteMs | $IOLatencyMsWrite \times IOCountWrite$ | Number    | ms   | 100     | Splunk data model |
| IODurationRWMs    | $IODurationReadMs + IODurationWriteMs$ | Number    | ms   | 200     | Splunk data model |
| IOMBRW            | $IOMBRead + IOMBWrite.$                | Number    | MB   | 60      | Splunk data model |
| IOMBPSRW          | $IOMBRW / IOCountRW \times IOPSRW.$    | Number    | MB   | 300     | Splunk data model |
| IOLatencyMsRW     | $IOLatencyMsRead + IOLatencyMsWrite$   | Number    | ms   | 10      | Splunk data model |

## System Performance Summary

### Details

- Source type: `uberAgent:System:SystemPerformanceSummary2`
- Used in dashboards: *Machine Performance, SBC Sizing and Capacity Planning, Single Machine*

*Detail, Analyze data over time*

- Enabled through configuration setting: [SystemPerformanceSummary](#)
- Related configuration settings: *n/a*

### List of Fields in the Raw Agent Data

| Field             | Description                                | Data type | Unit | Platform | Example |
|-------------------|--------------------------------------------|-----------|------|----------|---------|
| CPUUsagePercent   | CPU usage.                                 | Number    | %    | all      | 20.45   |
| RAMUsagePercent   | RAM usage.                                 | Number    | %    | all      | 12      |
| RAMUsageGB        | RAM usage.                                 | Number    | GB   | all      | 50      |
| IOPSRead          | I/O operations read.                       | Number    |      | all      | 200     |
| IOPSWrite         | I/O operations write.                      | Number    |      | all      | 200     |
| IOCountRead       | Count of read I/O operations.              | Number    |      | all      | 100     |
| IOCountWrite      | Count of write I/O operations.             | Number    |      | all      | 100     |
| IOMBRead          | Amount of read I/O operation data volume.  | Number    | MB   | Windows  | 150     |
| IOMBWrite         | Amount of write I/O operation data volume. | Number    | MB   | Windows  | 150     |
| IOLatencyMsRead   | Latency of read I/O operations.            | Number    | ms   | all      | 300     |
| IOLatencyMsWrite  | Latency of write I/O operations.           | Number    | ms   | all      | 300     |
| IOPercentDiskTime | Disk utilization.                          | Number    | %    | Windows  | 20      |



| Field                 | Description                                                                                                                                                                                                              | Data type | Unit | Platform | Example |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|----------|---------|
| NetUtilizationPercent | Network utilization.                                                                                                                                                                                                     | Number    | %    | Windows  | 15      |
| KernelPagedMB         | Kernel paged memory usage.                                                                                                                                                                                               | Number    | MB   | all      | 100     |
| KernelNonPagedMB      | Kernel non-paged memory usage.                                                                                                                                                                                           | Number    | MB   | all      | 300     |
| HandleCount           | On Windows: Handle count.<br>On macOS: Number of open file descriptors.                                                                                                                                                  | Number    |      | all      | 17      |
| ThreadCount           | Thread count.                                                                                                                                                                                                            | Number    |      | all      | 63      |
| IdlenessPercent       | Status of the idle timer expressed as a percentage. When this value reaches 100%, the system is considered completely idle, and the OS shows the screen saver or turns the display off (depending on the configuration). | Number    | %    | Windows  | 50      |

| Field                | Description                                                                                              | Data type | Unit | Platform | Example |
|----------------------|----------------------------------------------------------------------------------------------------------|-----------|------|----------|---------|
| CPURelativeFrequency | Percent actual CPU frequency as a Percentage of the base frequency.<br><a href="#">More information.</a> | Number    | %    | Windows  | 21      |
| PagefileTotalSize    | Pagefile total size.                                                                                     | Number    | GB   | all      | 8       |
| PagefileUsagePercent | Pagefile usage.                                                                                          | Number    | %    | all      | 60      |
| PagefileIOPSRead     | Pagefile I/O operations read.                                                                            | Number    |      | Windows  | 300     |
| PagefileIOPSWrite    | Pagefile I/O operations write.                                                                           | Number    |      | Windows  | 300     |

### List of Calculated Fields

| Field      | Description                                                  | Data type | Unit | Example | Where available   |
|------------|--------------------------------------------------------------|-----------|------|---------|-------------------|
| TotalRamGb | Total RAM size.                                              | Number    | ms   | 24      | Splunk data model |
| IOPS       | <a href="#">IOPSRead</a> + <a href="#">IOPSWrite</a> .       | Number    |      | 400     | Splunk data model |
| IOCount    | <a href="#">IOCountRead</a> + <a href="#">IOCountWrite</a> . | Number    |      | 200     | Splunk data model |
| IOMB       | <a href="#">IOMBRead</a> + <a href="#">IOMBWrite</a> .       | Number    | MB   | 300     | Splunk data model |

| Field             | Description                            | Data type | Unit | Example | Where available   |
|-------------------|----------------------------------------|-----------|------|---------|-------------------|
| IOMBPS            | $\frac{IOMB}{IOCount} \times IOPS.$    | Number    |      | 600     | Splunk data model |
| IOLatencyMs       | $IOLatencyMsRead + IOLatencyMsWrite$   | Number    |      | 600     | Splunk data model |
| IODurationReadMs  | $IOLatencyMsRead \times IOCountRead$   | Number    | ms   | 30000   | Splunk data model |
| IODurationWriteMs | $IOLatencyMsWrite \times IOCountWrite$ | Number    | ms   | 30000   | Splunk data model |
| IODurationMs      | $IODurationReadMs + IODurationWriteMs$ | Number    | ms   | 60000   | Splunk data model |
| User              | User name.<br>Always empty.            | Number    |      |         | Splunk data model |

## Computer Startup, Shutdown & Hibernation Metrics

July 9, 2024

## Boot Processes Metrics

October 11, 2024

## Boot Processes

uberAgent collects detailed information about each process running during the boot process like the command line and latency.

### Note

This metric is only available on client operating systems.

## Details

- Source type: `uberAgent:OnOffTransition:BootProcesses`
- Used in dashboards: *Single Boot Duration*
- Enabled through configuration setting: `BootDetail`
- Related configuration settings: *n/a*
- Supported platform: *Windows*

## List of Fields in the Raw Agent Data

| Field                   | Description                                        | Data type | Unit | Example                                          |
|-------------------------|----------------------------------------------------|-----------|------|--------------------------------------------------|
| ProcName                | Process name.                                      | String    |      | svchost.exe                                      |
| ProcID                  | Process ID.                                        | Number    |      | 456                                              |
| ProcParentID            | Parent process ID.                                 | Number    |      | 789                                              |
| ProcStartTimeRelativeMs | Relative process start time.                       | Number    | ms   | 100                                              |
| ProcLifetimeMs          | Process lifetime.                                  | Number    | ms   | 50                                               |
| ProcCmdline             | Process commandline.                               | String    |      | C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p |
| ProcIOReadCount         | Count of process I/O read operations.              | Number    |      | 91                                               |
| ProcIOWriteCount        | Count of process I/O write operations.             | Number    |      | 97                                               |
| ProcIOReadMB            | Amount of process I/O read operations data volume. | Number    | MB   | 50                                               |

| Field                | Description                                                                                                                        | Data type | Unit | Example                              |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------|-----------|------|--------------------------------------|
| ProclOWriteMB        | Amount of process I/O write operations data volume.                                                                                | Number    | MB   | 50                                   |
| ProclOLatencyReadMs  | Process I/O read operations latency.                                                                                               | Number    | ms   | 30                                   |
| ProclOLatencyWriteMs | Process I/O write operations latency.                                                                                              | Number    | ms   | 30                                   |
| SessionID            | Unique identifier that is generated by the machine when the session is created. Will be reassigned to other sessions after logoff. | Number    |      | 3                                    |
| TotalBootDurationMs  | Total boot duration.                                                                                                               | Number    | ms   | 500000                               |
| SortOrder2           | Sort order number to sort the table <i>Boot process performance</i> on the <i>Single Boot</i> dashboard correctly.                 | Number    |      | 29                                   |
| BootUID              | Unique UID for a boot generated by uberAgent.                                                                                      | String    |      | 00000408-0049-004b-0bb9-8ed17e25d401 |

### List of Calculated Fields

| Field     | Description                                                                                                    | Data type | Unit | Where available   | Example |
|-----------|----------------------------------------------------------------------------------------------------------------|-----------|------|-------------------|---------|
| SortOrder | Sort order number to sort the table<br><i>Boot process performance on the Single Boot dashboard correctly.</i> | Number    |      | Splunk data model | 1       |

### Boot Process Detail

uberAgent collects detailed information about each process running during the boot process like the disk IO and latency.

#### Note

This metric is only available on client operating systems.

### Details

- Source type: [uberAgent:OnOffTransition:BootProcessDetail](#)
- Used in dashboards: *Single Boot Duration*
- Enabled through configuration setting: [BootDetail](#)
- Related configuration settings: *n/a*
- Supported platform: *Windows*

### List of Fields in the Raw Agent Data

| Field              | Description                           | Data type | Unit | Example     |
|--------------------|---------------------------------------|-----------|------|-------------|
| ProcessName        | Process name.                         | String    |      | svchost.exe |
| ProcessIOReadCount | Count of process I/O read operations. | Number    |      | 91          |

| Field               | Description                                         | Data type | Unit | Example                              |
|---------------------|-----------------------------------------------------|-----------|------|--------------------------------------|
| ProcessIOWriteCount | Count of process I/O write operations.              | Number    |      | 97                                   |
| ProcessIOReadMB     | Amount of process I/O read operations data volume.  | Number    | MB   | 50                                   |
| ProcessIOWriteMB    | Amount of process I/O write operations data volume. | Number    | MB   | 50                                   |
| ProcessIOLatencyMs  | Process I/O operations latency.                     | Number    | ms   | 60                                   |
| BootUID             | Unique UID for a boot generated by uberAgent.       | String    |      | 00000408-0049-004b-0bb9-8ed17e25d401 |

### List of Calculated Fields

| Field          | Description                               | Data type | Unit | Where available   | Example    |
|----------------|-------------------------------------------|-----------|------|-------------------|------------|
| ProcessIOCount | ProcessIOReadCount + ProcessIOWriteCount. | Number    |      | Splunk data model | 188        |
| ProcName       | Process name.                             | String    |      | Splunk data model | chrome.exe |

## Computer Startup (Machine Boot) Metrics

July 9, 2024

## Boot Detail

uberAgent collects metrics about computer startup duration including Smss initialization as well as autostart services. The metrics in this section are based on the Microsoft document [Windows On/Off Transitions Solutions Guide](#).

### Details

- Source type: `uberAgent:OnOffTransition:BootDetail2`
- Used in dashboards: *Boot Duration, Single Boot Duration*
- Enabled through configuration setting: `BootDetail`
- Related configuration settings: *n/a*
- Supported platform: *Windows*

### List of Fields in the Raw Agent Data

---

| Field            | Description                                                                                                   | Data type | Unit | Example |
|------------------|---------------------------------------------------------------------------------------------------------------|-----------|------|---------|
| KernellnitTimeMs | Time from the beginning to the start of the first smss.exe process.                                           | Number    | ms   | 1683    |
| SmssInitTimeMs   | Time from the start of the first smss.exe process to the start of the second smss.exe process (in session 0). | Number    | ms   | 4007    |
| AutoCheckTimeMs  | Auto check time. <a href="#">More information.</a>                                                            | Number    | ms   | 20      |



| Field                  | Description                                                                                                                  | Data type | Unit | Example |
|------------------------|------------------------------------------------------------------------------------------------------------------------------|-----------|------|---------|
| Session0InitDurationMs | Session 0 initialization duration: from the start of the second smss.exe process to the start of wininit.exe.                | Number    | ms   | 9572    |
| Session1InitDurationMs | Session 1 initialization duration: from the start of the third smss.exe process (in session 1) to the start of winlogon.exe. | Number    | ms   | 71      |
| WininitInitDurationMs  | Wininit initialization duration: from the start of wininit.exe to the start of services.exe.                                 | Number    | ms   | 61      |
| WinlogonInitDurationMs | Winlogon initialization duration: from the start of winlogon.exe to the start of logonui.exe.                                | Number    | ms   | 369     |
| AutostartServicesMs    | Autostart services: from the start of services.exe to the start of the first taskhost.exe.                                   | Number    | ms   | 13269   |

---

| Field                     | Description                                                                                                                                                 | Data type | Unit | Example |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|---------|
| ComputerStartupMsComputer | startup: from the beginning to the start of LogonUI.exe. The user is now able to log in to the computer.                                                    | Number    | ms   | 15700   |
| MainPathBootTimeMs        | Main path boot time: from the beginning to the start of the shell (typically explorer.exe). The user has successfully logged in, and the shell is starting. | Number    | ms   | 28361   |
| PostBootTimeMs            | Post boot time: from shell start to the system reaching an 80% idle state. The desktop is now ready to use.                                                 | Number    | ms   | 6882    |

---

| Field           | Description                                                                                                                                                                                                                                                                                                                                    | Data type | Unit | Example                              |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|--------------------------------------|
| TotalBootTimeMs | The time from Windows start to the desktop being shown and the system reaching an 80% idle state. This is the sum of <code>MainPathBootTimeMs</code> and <code>PostBootTimeMs</code> . If <code>TotalBootTimeMs</code> is empty, it means that Windows stopped collecting data too early, or because the user waited longer before logging in. | Number    | ms   | 130765                               |
| BootUID         | Unique UID for a boot created by uberAgent.                                                                                                                                                                                                                                                                                                    | String    |      | 00000408-0049-004b-0bb9-8ed17e25d401 |

---

## Computer Shutdown Metrics

October 11, 2024

### Computer Shutdown

uberAgent collects the duration of the major phases as well as the total duration for each shutdown.

**Note**

This metric is only available on client operating systems.

**Details**

- Source type: `uberAgent:OnOffTransition:ShutdownDetail`
- Used in dashboards: *Shutdown Duration*
- Enabled through configuration setting: `ShutdownDetail`
- Related configuration settings: *n/a*
- Supported platform: *Windows*

**List of Fields in the Raw Agent Data**

---

| Field                         | Description                      | Data type | Unit | Example |
|-------------------------------|----------------------------------|-----------|------|---------|
| TotalShutdownTimeMs           | Total shutdown time.             | ms        |      | 700     |
| UserSessionTimeMs             | User session time.               | ms        |      | 100     |
| UserPolicyTimeMs              | User policy time.                | ms        |      | 100     |
| UserProfilesTimeMs            | User profiles time.              | ms        |      | 100     |
| SystemSessionsTimeMs          | System sessions time.            | ms        |      | 100     |
| PreShutdownNotificationTimeMs | Pre-shutdown notifications time. | ms        |      | 100     |
| ServicesTimeMs                | Services time.                   | ms        |      | 100     |
| KernelTimeMs                  | Kernel time.                     | ms        |      | 100     |

---

**On/Off Transition Delay Metrics**

October 11, 2024

## Slow App Startup

uberAgent records which applications are responsible for delays during system boot. For each delay, uberAgent collects metrics like application name and version.

### Note

This metric is only available on client operating systems.

## Details

- Source type: `uberAgent:OnOffTransition:SlowAppStartup`
- Used in dashboards:
- Enabled through configuration setting: `BootDetail`
- Related configuration settings: *n/a*
- Supported platform: *Windows*

## List of Fields in the Raw Agent Data

| Field             | Description                                        | Data type | Unit | Example                               |
|-------------------|----------------------------------------------------|-----------|------|---------------------------------------|
| Name              | Application name.                                  | String    |      | explorer.exe                          |
| FriendlyName      | Friendly application name.                         | String    |      | Windows Explorer                      |
| Version           | Application version.                               | String    |      | 6.2.9200.16384 (win8_rtm.120725-1247) |
| TotalTimeMs       | Total time.                                        | Number    | ms   | 100                                   |
| DegradationTimeMs | Degradation (how much longer it took than normal). | Number    | ms   | 20                                    |

## Slow App Shutdown

uberAgent records which applications are responsible for delays during system shutdown. For each delay, uberAgent collects metrics like application name and version.

**Note**

This metric is only available on client operating systems.

**Details**

- Source type: `uberAgent:OnOffTransition:SlowAppShutdown`
- Used in dashboards:
- Enabled through configuration setting: `ShutdownDetail`
- Related configuration settings: *n/a*
- Supported platform: *Windows*

**List of Fields in the Raw Agent Data**

---

| Field             | Description                                        | Data type | Unit | Example                               |
|-------------------|----------------------------------------------------|-----------|------|---------------------------------------|
| Name              | Application name.                                  | String    |      | explorer.exe                          |
| FriendlyName      | Friendly application name.                         | String    |      | Windows Explorer                      |
| Version           | Application version.                               | String    |      | 6.2.9200.16384 (win8_rtm.120725-1247) |
| TotalTimeMs       | Total time.                                        | Number    | ms   | 100                                   |
| DegradationTimeMs | Degradation (how much longer it took than normal). | Number    | ms   | 20                                    |

---

**Slow App Standby**

uberAgent records which applications are responsible for delays during standby. For each delay, uberAgent collects metrics like application name and version.

**Note**

This metric is only available on client operating systems.

**Details**

- Source type: `uberAgent:OnOffTransition:SlowAppStandby`
- Used in dashboards:
- Enabled through configuration setting: `StandbyDetail`
- Related configuration settings: *n/a*
- Supported platform: *Windows*

**List of Fields in the Raw Agent Data**

---

| Field             | Description                                        | Data type | Unit | Example                               |
|-------------------|----------------------------------------------------|-----------|------|---------------------------------------|
| Name              | Application name.                                  | String    |      | stisvc                                |
| FriendlyName      | Friendly application name.                         | String    |      | Still Image Devices Service           |
| Version           | Application version.                               | String    |      | 6.2.9200.16384 (win8_rtm.120725-1247) |
| TotalTimeMs       | Total time.                                        | Number    | ms   | 100                                   |
| DegradationTimeMs | Degradation (how much longer it took than normal). | Number    | ms   | 20                                    |

---

**Slow Service Startup**

uberAgent records which services are responsible for delays during system boot. For each delay, uberAgent collects metrics like service name and version.

**Note**

This metric is only available on client operating systems.

**Details**

- Source type: `uberAgent:OnOffTransition:SlowServiceStartup`
- Used in dashboards:

- Enabled through configuration setting: [BootDetail](#)
- Related configuration settings: *n/a*
- Supported platform: *Windows*

### List of Fields in the Raw Agent Data

---

| Field             | Description                                        | Data type | Unit | Example                               |
|-------------------|----------------------------------------------------|-----------|------|---------------------------------------|
| Name              | Service name.                                      | String    |      | stisvc                                |
| FriendlyName      | Friendly service name.                             | String    |      | Still Image Devices Service           |
| Version           | Service version.                                   | String    |      | 6.2.9200.16384 (win8_rtm.120725-1247) |
| TotalTimeMs       | Total time.                                        | Number    | ms   | 100                                   |
| DegradationTimeMs | Degradation (how much longer it took than normal). | Number    | ms   | 20                                    |

---

### Slow Service Shutdown

uberAgent records which services are responsible for delays during system shutdown. For each delay, uberAgent collects metrics like service name and version.

#### Note

This metric is only available on client operating systems.

### Details

- Source type: [uberAgent:OnOffTransition:SlowServiceShutdown](#)
- Used in dashboards:
- Enabled through configuration setting: [ShutdownDetail](#)
- Related configuration settings: *n/a*
- Supported platform: *Windows*



### List of Fields in the Raw Agent Data

| Field             | Description                                        | Data type | Unit | Example                               |
|-------------------|----------------------------------------------------|-----------|------|---------------------------------------|
| Name              | Service name.                                      | String    |      | stisvc                                |
| FriendlyName      | Friendly service name.                             | String    |      | Still Image Devices Service           |
| Version           | Service version.                                   | String    |      | 6.2.9200.16384 (win8_rtm.120725-1247) |
| TotalTimeMs       | Total time.                                        | Number    | ms   | 100                                   |
| DegradationTimeMs | Degradation (how much longer it took than normal). | Number    | ms   | 20                                    |

### Slow Service Hybrid Standby

uberAgent records which services are responsible for delays during hybrid standby. For each delay, uberAgent collects metrics like service name and version.

#### Note

This metric is only available on client operating systems.

### Details

- Source type: `uberAgent:OnOffTransition:SlowServiceHybridStandby`
- Used in dashboards:
- Enabled through configuration setting: [StandbyDetail](#)
- Related configuration settings: *n/a*
- Supported platform: *Windows*

### List of Fields in the Raw Agent Data

| Field | Description   | Data type | Unit | Example |
|-------|---------------|-----------|------|---------|
| Name  | Service name. | String    |      | stisvc  |

| Field             | Description                                        | Data type | Unit | Example                               |
|-------------------|----------------------------------------------------|-----------|------|---------------------------------------|
| FriendlyName      | Friendly service name.                             | String    |      | Still Image Devices Service           |
| Version           | Service version.                                   | String    |      | 6.2.9200.16384 (win8_rtm.120725-1247) |
| TotalTimeMs       | Total time.                                        | Number    | ms   | 100                                   |
| DegradationTimeMs | Degradation (how much longer it took than normal). | Number    | ms   | 20                                    |

## Slow Driver Startup

uberAgent records which drivers are responsible for delays during system boot. For each delay, uberAgent collects metrics like driver name and version.

### Note

This metric is only available on client operating systems.

## Details

- Source type: `uberAgent:OnOffTransition:SlowDriverStartup`
- Used in dashboards:
- Enabled through configuration setting: `BootDetail`
- Related configuration settings: *n/a*
- Supported platform: *Windows*

## List of Fields in the Raw Agent Data

| Field        | Description           | Data type | Unit | Example                         |
|--------------|-----------------------|-----------|------|---------------------------------|
| Name         | Driver name.          | String    |      | \Driver\pci                     |
| FriendlyName | Friendly driver name. | String    |      | NT Plug and Play PCI Enumerator |

| Field             | Description                                        | Data type | Unit | Example                                  |
|-------------------|----------------------------------------------------|-----------|------|------------------------------------------|
| Version           | Driver version.                                    | String    |      | 6.2.9200.16384<br>(win8_rtm.120725-1247) |
| TotalTimeMs       | Total time.                                        | Number    | ms   | 100                                      |
| DegradationTimeMs | Degradation (how much longer it took than normal). | Number    | ms   | 20                                       |

## Slow Driver Shutdown

uberAgent records which drivers are responsible for delays during system shutdown. For each delay, uberAgent collects metrics like driver name and version.

### Note

This metric is only available on client operating systems.

## Details

- Source type: `uberAgent:OnOffTransition:SlowDriverShutdown`
- Used in dashboards:
- Enabled through configuration setting: *ShutdownDetail*
- Related configuration settings: *n/a*
- Supported platform: *Windows*

## List of Fields in the Raw Agent Data

| Field        | Description           | Data type | Unit | Example                                  |
|--------------|-----------------------|-----------|------|------------------------------------------|
| Name         | Driver name.          | String    |      | \Driver\pci                              |
| FriendlyName | Friendly driver name. | String    |      | NT Plug and Play<br>PCI Enumerator       |
| Version      | Driver version.       | String    |      | 6.2.9200.16384<br>(win8_rtm.120725-1247) |

| Field             | Description                                        | Data type | Unit | Example |
|-------------------|----------------------------------------------------|-----------|------|---------|
| TotalTimeMs       | Total time.                                        | Number    | ms   | 100     |
| DegradationTimeMs | Degradation (how much longer it took than normal). | Number    | ms   | 20      |

## Slow Driver Standby

uberAgent records which drivers are responsible for delays during standby. For each delay, uberAgent collects metrics like driver name and version.

### Note

This metric is only available on client operating systems.

## Details

- Source type: [uberAgent:OnOffTransition:SlowDriverStandby](#)
- Used in dashboards:
- Enabled through configuration setting: [StandbyDetail](#)
- Related configuration settings: *n/a*
- Supported platform: *Windows*

## List of Fields in the Raw Agent Data

| Field        | Description           | Data type | Unit | Example                               |
|--------------|-----------------------|-----------|------|---------------------------------------|
| Name         | Driver name.          | String    |      | \Driver\pci                           |
| FriendlyName | Friendly driver name. | String    |      | NT Plug and Play PCI Enumerator       |
| Version      | Driver version.       | String    |      | 6.2.9200.16384 (win8_rtm.120725-1247) |
| TotalTimeMs  | Total time.           | Number    | ms   | 100                                   |

| Field              | Description                                        | Data type | Unit | Example                             |
|--------------------|----------------------------------------------------|-----------|------|-------------------------------------|
| DegradationTimeMs  | Degradation (how much longer it took than normal). | Number    | ms   | 20                                  |
| DeviceFriendlyName | Device friendly name.                              | String    |      | Ricoh PCIe SDXC/MMC Host Controller |

## Slow Driver Resume

uberAgent records which drivers are responsible for delays during resume. For each delay, uberAgent collects metrics like driver name and version.

### Note

This metric is only available on client operating systems.

## Details

- Source type: [uberAgent:OnOffTransition:SlowDriverResume](#)
- Used in dashboards:
- Enabled through configuration setting: [StandbyDetail](#)
- Related configuration settings: *n/a*
- Supported platform: *Windows*

## List of Fields in the Raw Agent Data

| Field        | Description           | Data type | Unit | Example                               |
|--------------|-----------------------|-----------|------|---------------------------------------|
| Name         | Driver name.          | String    |      | \Driver\pci                           |
| FriendlyName | Driver friendly name. | String    |      | NT Plug and Play PCI Enumerator       |
| Version      | Driver version.       | String    |      | 6.2.9200.16384 (win8_rtm.120725-1247) |
| TotalTimeMs  | Total time.           | Number    | ms   | 100                                   |

| Field              | Description                                        | Data type | Unit | Example                             |
|--------------------|----------------------------------------------------|-----------|------|-------------------------------------|
| DegradationTimeMs  | Degradation (how much longer it took than normal). | Number    | ms   | 20                                  |
| DeviceFriendlyName | Device friendly name.                              | String    |      | Ricoh PCIe SDXC/MMC Host Controller |

## Slow User Policy

**DEPRECATED:** this sourcetype is deprecated and will be removed in a future release.

uberAgent records which user policies are responsible for delays during system boot. For each delay, uberAgent collects metrics like name and total time.

### Details

- Source type: [uberAgent:OnOffTransition:SlowUserPolicy](#)
- Used in dashboards:
- Enabled through configuration setting: [BootDetail](#)
- Related configuration settings: *n/a*
- Supported platform: *Windows*

### List of Fields in the Raw Agent Data

| Field             | Description                                        | Data type | Unit | Example      |
|-------------------|----------------------------------------------------|-----------|------|--------------|
| Name              | User policy name.                                  | String    |      | PreShellInit |
| TotalTimeMs       | Total time.                                        | Number    | ms   | 100          |
| DegradationTimeMs | Degradation (how much longer it took than normal). | Number    | ms   | 20           |

## Slow SMSS Initialization

**DEPRECATED:** this sourcetype is deprecated and will be removed in a future release.

uberAgent records SMSS initialization is responsible for delays during system boot. For each delay, uberAgent collects metrics like name and total time.

### Details

- Source type: `uberAgent:OnOffTransition:SlowSMSSInit`
- Used in dashboards:
- Enabled through configuration setting: `BootDetail`
- Related configuration settings: *n/a*
- Supported platform: *Windows*

### List of Fields in the Raw Agent Data

---

| Field             | Description                                        | Data type | Unit | Example  |
|-------------------|----------------------------------------------------|-----------|------|----------|
| Name              | SMSSInit name.                                     | String    |      | SMSSInit |
| TotalTimeMs       | Total time.                                        | Number    | ms   | 100      |
| DegradationTimeMs | Degradation (how much longer it took than normal). | Number    | ms   | 20       |

---

## Standby/Resume Duration Metrics

October 11, 2024

### Standby Detail

uberAgent collects information about each standby/resume like duration, the reason for waking up as well as pages written to the hibernation file.

**Note**

This metric is only available on client operating systems.

**Details**

- Source type: `uberAgent:OnOffTransition:StandbyDetail2`
- Used in dashboards: *Standby/Resume Duration*
- Enabled through configuration setting: `StandbyDetail`
- Related configuration settings: *n/a*
- Supported platform: *Windows*

**List of Fields in the Raw Agent Data**

| Field               | Description                                  | Data type | Unit | Example                             |
|---------------------|----------------------------------------------|-----------|------|-------------------------------------|
| SleepTime           | Time the sleep started.                      | String    |      | 2018-07-31<br>19:02:37.582<br>+0200 |
| WakeTime            | Time the wake completed.                     | String    |      | 2018-07-32<br>07:31:58.434<br>+0200 |
| EnterStandbyMs      | Duration of the standby process.             | Number    | ms   | 5737                                |
| ResumeFromStandbyMs | Duration of the resume process.              | Number    | ms   | 1269                                |
| DriverInitDuration  | Duration of driver initialization at resume. | Number    | ms   | 897                                 |
| BiosInitDuration    | Duration of BIOS initialization at resume.   | Number    | ms   | 0                                   |
| HiberWriteDuration  | Duration of write to hibernation file.       | Number    | ms   | 8034                                |
| HiberReadDuration   | Duration of read from hibernation file.      | Number    | ms   | 4419                                |



| Field                | Description                                                                                                                                                                   | Data type | Unit | Example  |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|----------|
| HiberPagesWritten    | Memory pages written to the hibernation file.                                                                                                                                 | Number    |      | 738245   |
| Attributes           | n/a                                                                                                                                                                           | Number    |      | 33571073 |
| TargetState          | Target sleep state.<br>Possible values:<br>0-7. For a string representation see the calculated field <a href="#">TargetStateDisplayName</a> .                                 | Number    |      | 5        |
| EffectiveState       | Actual sleep state.<br>Possible values:<br>0-7. For a string representation see the calculated field <a href="#">EffectiveStateDisplayName</a> .                              | Number    |      | 5        |
| WakeSourceType       | Source of a wake up (what woke the machine up?).<br>Possible values:<br>0-6. For a string representation see the calculated field <a href="#">WakeSourceTypeDisplayName</a> . | Number    |      | 1        |
| WakeSourceTextLength | Number of characters in the field <a href="#">WakeSourceText</a> .                                                                                                            | Number    |      | 125      |

| Field                    | Description                                                          | Data type | Unit | Example                                                                                                |
|--------------------------|----------------------------------------------------------------------|-----------|------|--------------------------------------------------------------------------------------------------------|
| WakeSourceText           | Description of the source of a wake up                               | String    |      | Windows will execute 'NT TASK\Microsoft\Windows\Upd scheduled task that requested waking the computer. |
| WakeTimerOwnerLength     | Number of characters in the field <a href="#">WakeTimerOwner</a> .   | Number    |      | 52                                                                                                     |
| WakeTimerContextLength   | Number of characters in the field <a href="#">WakeTimerContext</a> . | Number    |      | 18                                                                                                     |
| NoMultiStageResumeReason | Reason                                                               | Number    |      | 0                                                                                                      |
| WakeTimerOwner           | If a wake up was caused by a timer: owner of the timer.              | String    |      | \Device\HarddiskVolume4\Win                                                                            |
| WakeTimerContext         | If a wake up was caused by a timer: additional information.          | String    |      | SystemEventsBroker                                                                                     |

### List of Calculated Fields

| Field                 | Description                                                                                                                                                                                | Data type | Unit | Example   | Where available                  |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-----------|----------------------------------|
| TargetStateDisplay    | String representation of the field<br>TargetState<br>. Possible values:<br>undefined,<br>S0/working,<br>S1, S2,<br>S3/standby,<br>Hibernate,<br>Shutdown,<br>Maximum enumeration value.    | String    |      | Hibernate | Splunk data model,<br>Splunk SPL |
| EffectiveStateDisplay | String representation of the field<br>EffectiveState<br>. Possible values:<br>undefined,<br>S0/working,<br>S1, S2,<br>S3/standby,<br>Hibernate,<br>Shutdown,<br>Maximum enumeration value. | String    |      | Hibernate | Splunk data model,<br>Splunk SPL |

| Field          | Description                                                                                                                                                                                          | Data type | Unit | Example | Where available                  |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|---------|----------------------------------|
| WakeSourceType | Display name presentation of the field<br><a href="#">WakeSourceType</a><br>. Possible values:<br>unknown,<br>Power<br>Button,<br>S4 Doze to Hibernate<br>, Device,<br>Device or<br>Timer,<br>Timer. | String    |      | Timer   | Splunk data model,<br>Splunk SPL |

## Network Metrics

November 25, 2024

### Network Communication

uberAgent collects metrics like source process (process sending/receiving data on the machine uberAgent is running on) as well as IP address and port per network target and sending/receiving process. A network target is a communication endpoint from the point of view of the machine uberAgent is running on. uberAgent distinguishes between different services on the target machine and can show latencies for, say, SMB and SQL Server independently. Of course, uberAgent supports both IPv4 and IPv6! uberAgent optionally only shows new ports and targets never seen before.

#### Notes:

- Field: [AppVersion](#) - uberAgent has an internal filter to minimize data volume by suppressing version information for system processes and system services. As a result, the [AppVersion](#) field is typically empty for most system processes and services.

## Details

- Source type: [uberAgent:Process:NetworkTargetPerformance](#)
- Used in dashboards: *Application Network Issues, Citrix XA/XD Databases, Process Network Communication, Application Network Communication, Machine Network Communication, Single Application Performance, Single Machine Detail, Single User Detail*
- Enabled through configuration setting: [NetworkTargetPerformanceProcess](#)
- Related configuration settings: [[NetworkTargetPerformanceProcess\\_Filter](#)], [[NetworkTargetPerformanceProcess\\_Config](#)]
- Supported platform: *all*

## List of Fields in the Raw Agent Data

| Field                  | Description                                              | Data type | Unit | Example        |
|------------------------|----------------------------------------------------------|-----------|------|----------------|
| ProcName               | Process name.                                            | String    |      | chrome.exe     |
| ProcUser               | Process user.                                            | String    |      | Domain\JohnDoe |
| NetTargetRemoteAddress | Network target remote address.                           | String    |      | 138.201.31.60  |
| NetTargetRemoteName    | Network target remote name.                              | String    |      | vastlimits.com |
| NetTargetRemotePort    | Network target remote port.                              | Number    |      | 443            |
| NetTargetSendCount     | Count of packets to network target containing payload.   | Number    |      | 15             |
| NetTargetReceiveCount  | Count of packets from network target containing payload. | Number    |      | 14             |
| NetTargetConnectCount  | Count of connects to network target.                     | Number    |      | 1              |
| NetTargetSendKBPS      | Kilobytes per second sent to network target.             | Number    | KB/s | 1024           |

| Field                     | Description                                                                                          | Data type | Unit | Example |
|---------------------------|------------------------------------------------------------------------------------------------------|-----------|------|---------|
| NetTargetReceiveKBps      | Kilobytes per second received from network target.                                                   | Number    | KB/s | 1024    |
| NetTargetSendMB           | Amount of data volume send to network target. Payload only, no protocol overhead.                    | Number    | MB   | 1       |
| NetTargetReceiveMB        | Amount of data volume received from network target. Payload only, no protocol overhead.              | Number    | MB   | 1       |
| NetTargetSendLatencyms    | Latency to network target.                                                                           | Number    | ms   | 100     |
| NetTargetProtocols        | Protocols used.                                                                                      | String    |      | TCP     |
| NetTargetSendLatencyCount | Count of events with latency.                                                                        | Number    |      | 2       |
| AppId                     | Associated application ID. Used by uberAgent to lookup application names and populate field AppName. | String    |      | GglChrm |
| NetTargetReconnectCount   | Count of reconnects to network target.                                                               | Number    |      | 3       |
| NetTargetRetransmitCount  | Count of retransmits to network target.                                                              | Number    |      | 3       |

| Field                       | Description                                        | Data type | Unit | Example      |
|-----------------------------|----------------------------------------------------|-----------|------|--------------|
| AppVersion                  | Application version.                               | String    |      | 67.0.3396.99 |
| NetTargetSendJitter         | Waiter to network target.                          | Number    | ms   | 5            |
| NetTargetSendJitterCount    | Count of events with jitter.                       | Number    |      | 1            |
| NetTargetSourceAddress      | Network source IP.                                 | String    |      | 127.0.0.1    |
| NetTargetSendLatencyInitial | Initial latency to network target (TCP handshake). | Number    | ms   | 100          |
| NetTargetSendLatencyCount   | Count of events with initial latency.              | Number    |      | 1            |
| NetTargetSourcePort         | Network source port.                               | Number    |      | 43021        |

**List of Calculated Fields**

| Field                          | Description                                                                                                | Data type | Unit | Example            | Where available   |
|--------------------------------|------------------------------------------------------------------------------------------------------------|-----------|------|--------------------|-------------------|
| NetTargetRemoteNameAddress     | <p>NetTargetRemoteName . If NetTargetRemoteName is not filled, NetTargetRemoteAddress is used instead.</p> | String    |      | vastlimits.com     | Splunk data model |
| NetTargetRemoteNameAddressPort | <p>NetTargetRemoteNameAddress and NetTargetRemotePort .</p>                                                | String    |      | vastlimits.com:443 | Splunk data model |

| Field                                  | Description                                        | Data type | Unit | Example          | Where available                  |
|----------------------------------------|----------------------------------------------------|-----------|------|------------------|----------------------------------|
| <code>NetTargetSendReceiveMB</code>    | NetTargetSendReceiveMB + NetTargetReceiveMB        | Number    | MB   | 2                | Splunk data model                |
| <code>NetTargetSendReceiveCount</code> | Number of sends and receive events combined.       | Number    |      | 29               | Splunk data model                |
| <code>NetTargetSendReceiveKBPS</code>  | NetTargetSendReceiveKBPS                           | Number    | KB/s | 2048             | Splunk data model                |
| <code>NetTargetSendLatencyMs</code>    | NetTargetSendLatencyMs x NetTargetSendLatencyCount | Number    | ms   | 200              | Splunk data model                |
| <code>AppName</code>                   | Associated application name.                       | String    |      | Google<br>Chrome | Splunk data model,<br>Splunk SPL |
| <code>ProcUser</code>                  | Process user.                                      | String    |      | Domain\JohnDoe   | Splunk data model,<br>Splunk SPL |
| <code>User</code>                      | User name.                                         | String    |      | Domain\JohnDoe   | Splunk data model                |
| <code>ProcessName</code>               | Process name.                                      | String    |      | chrome.exe       | Splunk data model                |

## Network Connection Failures

uberAgent collects metrics like source application name as well as protocols used whenever a network connection attempt fails.

### Details

- Source type: `uberAgent:Application:NetworkConnectFailure`
- Used in dashboards: *Application Network Issues, Machine Network Issues, Process Network Issues*



- Enabled through configuration setting: [NetworkTargetPerformanceProcess](#)
- Related configuration settings: [\[NetworkTargetPerformanceProcess\\_Filter\]](#), [\[NetworkTargetPerformanceProcess\\_Config\]](#)
- Supported platform: *all*

### List of Fields in the Raw Agent Data

| Field                  | Description                                                                                                | Data type | Unit | Example                              |
|------------------------|------------------------------------------------------------------------------------------------------------|-----------|------|--------------------------------------|
| AppId                  | Associated application ID. Used by uberAgent to lookup application names and populate field AppName.       | String    |      | GglChrm                              |
| AppVersion             | Application version.                                                                                       | String    |      | 67.0.3396.99                         |
| ProcessName            | Process name.                                                                                              | String    |      | chrome.exe                           |
| ProcessId              | Process ID.                                                                                                | Number    |      | 456                                  |
| SessionGUID            | Unique identifier that is generated by uberAgent when the session is created. Valid for this session only. | String    |      | 00000002-f295-9109-e7c7-c964011dd401 |
| NetTargetRemoteAddress | Network target remote address.                                                                             | String    |      | 138.201.31.60                        |
| NetTargetRemoteName    | Network target remote name.                                                                                | String    |      | vastlimits.com                       |
| NetTargetRemotePort    | Network target remote port.                                                                                | Number    |      | 443                                  |
| NetTargetProtocols     | Protocols used. The only protocol supported is TCP.                                                        | String    |      | TCP                                  |

| Field                  | Description          | Data type | Unit | Example   |
|------------------------|----------------------|-----------|------|-----------|
| NetTargetSourceAddress | Network source IP.   | String    |      | 127.0.0.1 |
| NetTargetSourcePort    | Network source port. | Number    |      | 43021     |

### List of Calculated Fields

| Field               | Description                                                                                                          | Data type | Unit | Example          | Where available                  |
|---------------------|----------------------------------------------------------------------------------------------------------------------|-----------|------|------------------|----------------------------------|
| AppName             | Associated application name.                                                                                         | String    |      | Google<br>Chrome | Splunk data model,<br>Splunk SPL |
| ProcName            | Process name.                                                                                                        | String    |      | chrome.exe       | Splunk data model                |
| User                | User name.                                                                                                           | String    |      | Domain\JohnDoe   | Splunk data model,<br>Splunk SPL |
| NetTargetRemoteName | Remote name. If <code>NetTargetRemoteName</code> is not filled, <code>NetTargetRemoteAddress</code> is used instead. | String    |      | vastlimits.com   | Splunk data model                |

\* Fields only available when `NetworkDriverEnabled = true`.

\*\* In cases of high network activity combined with a large number of retransmissions, uberAgent may not detect all retransmissions. This design choice ensures minimal overhead and avoids any negative impact on system performance.

## Microsoft Office Metrics

July 9, 2024

## Outlook Plugin Load

uberAgent collects Outlook plugin load duration and related information like the ProgID and GUID.

### Details

- Source type: `uberAgent:Application:OutlookPluginLoad`
- Used in dashboards: *Outlook Plugin Load Performance*
- Enabled through configuration setting: `OutlookPerformanceEvents`
- Related configuration settings: *n/a*
- Supported platform: *Windows*

### List of Fields in the Raw Agent Data

| Field        | Description                                                     | Data type | Unit | Measurement type | Example                              |
|--------------|-----------------------------------------------------------------|-----------|------|------------------|--------------------------------------|
| Name         | Plugin name (may change with version and language).             | String    |      | Snapshot         | Egnyte Outlook Add-In                |
| ProgID       | Unique plugin ID (language-independent).                        | String    |      | Snapshot         | EgnyteAddin.Connect                  |
| GUID         | Plugin GUID (language-independent).                             | String    |      | Snapshot         | CEBEF5C6-2F24-4EC1-A005-A04E55EF0C52 |
| LoadBehavior | Plugin load behavior ID. Possible values: 0, 1, 2, 3, 8, 9, 16. | Number    |      | Snapshot         | 3                                    |

---

| Field      | Description                                                                | Data type | Unit | Measurement type | Example |
|------------|----------------------------------------------------------------------------|-----------|------|------------------|---------|
| HKLM       | Indicates if plugin is configured for all users.<br>Possible values: 0, 1. | Number    |      | Snapshot         | 0       |
| BootTimeMs | Plugin load duration.                                                      | Number    | ms   | Sum              | 6000    |

---

### List of Calculated Fields

| Field                  | Description                                                                                                                                                                                                                                                | Data type | Unit | Measurement type | Where available   | Example             |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------------|-------------------|---------------------|
| LoadBehaviorPluginName | Plugin name behavior name. Possible values:<br>Do not load automatically (0),<br>Do not load automatically (1),<br>Load at startup (2),<br>Load at startup (3),<br>Load on demand (8),<br>Load on demand (9),<br>Load first time then load on demand (16). | String    |      | Snapshot         | Splunk data model | Load at startup (3) |
| BootTimeS              | Plugin load duration.                                                                                                                                                                                                                                      | Number    | s    | Sum              | Splunk data model | 6.00                |

## Session Metrics

July 9, 2024

### Session Detail

uberAgent collects metrics like the session ID, connection state, protocol latency, and foreground application per user session.

#### Details

- Source type: [uberAgent:Session:SessionDetail](#)
- Used in dashboards: *Application Usage, Machine Uptime, SBC Sizing and Capacity Planning, Session 0, Session Info: Citrix, Session Info: VMware, User Session Overview, User Sessions, Single Application Performance, Single Machine Performance, Single User Performance, Analyze data over time*
- Enabled through configuration setting: [SessionDetail](#)
- Related configuration settings: *n/a*

#### List of Fields in the Raw Agent Data

| Field     | Description                                                                                                                                                         | Data type | Unit | Example | Platform |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|---------|----------|
| SessionID | Session ID generated by the OS. Session IDs are reused and cannot be used to uniquely identify a session. Use <a href="#">SessionGUID</a> for that purpose instead. | Number    |      | 3       | all      |

---

| Field            | Description                                                                                                                                                                                                                         | Data type | Unit | Example                             | Platform |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-------------------------------------|----------|
| SessionLogonTime | Time when the user logged on.                                                                                                                                                                                                       | String    |      | 2018-07-23<br>10:06:02.123<br>+0200 | all      |
| SessionProtocol  | Remoting protocol used to connect to the session.<br>Possible values on Windows:<br>Console,<br>ICA, RDP,<br>PCoIP,<br>Blast,<br>Frame,<br>Protocol [ ID].<br>Possible values on macOS:<br>Console,<br>RFB, SSH,<br>Protocol [ ID]. | String    |      | ICA                                 | all      |

| Field                  | Description                                                                                                                                                                      | Data type | Unit | Example | Platform |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|---------|----------|
| SessionConnectionState | Session connection state. Possible values: active, connected, connecting, shadowing, disconnected, idle, listening, reset, down, initializing, unknown, Unsupported state: [ID]. | String    |      | active  | Win      |
| SessionProcessCount    | Number of processes that are running in the session.                                                                                                                             | Number    |      | 34      | all      |
| SessionCPUTimeMs       | Session CPU usage (absolute usage in milliseconds).                                                                                                                              | Number    | ms   | 3000    | all      |
| SessionCPUUsagePercent | Percent CPU usage (relative usage in percent).                                                                                                                                   | Number    | %    | 29      | all      |
| SessionIOPS            | I/O operations per second of all processes in the session combined.                                                                                                              | Number    |      | 500     | Win      |



| Field             | Description                                                                              | Data type | Unit | Example                              | Platform |
|-------------------|------------------------------------------------------------------------------------------|-----------|------|--------------------------------------|----------|
| SessionIOCount    | I/O operation count of all processes in the session combined.                            | Number    |      | 300                                  | Win      |
| SessionIOMB       | I/O data volume of all processes in the session combined.                                | Number    | MB   | 20                                   | all      |
| SessionIOLatency  | Latency of I/O operations.                                                               | Number    | ms   | 300                                  | Win      |
| SessionWorkingSet | SRW usage (working set) of all processes in the session combined.                        | Number    | MB   | 450.2                                | all      |
| SessionNetKBPS    | Process network traffic data volume per second of all processes in the session combined. | Number    | KB   | 21                                   | Win      |
| SessionUser       | User name.                                                                               | String    |      | Domain\JohnDoe                       | all      |
| SessionGUID       | Unique identifier for a session that is generated by uberAgent.                          | String    |      | 00000002-f295-9109-e7c7-c964011dd401 | all      |

| Field               | Description                                                                                                                                                                                                                                                                                                  | Data type | Unit | Example           | Platform |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-------------------|----------|
| SessionRplLatencyMs | Remote client protocol latency. This field is filled with the latency in ms at collection time. If the protocol is ICA, uberAgent uses the perfmon counter <a href="#">Latency - Last Recorded</a> as the source. This metric is different from Citrix Round-Trip-Time ( <a href="#">more information</a> ). | Number    | ms   | 30                | Win      |
| SessionClientMac    | Remote client MAC address. Only collected for VMware sessions.                                                                                                                                                                                                                                               | String    |      | AC-ED-5C-02-F0-30 | Win      |
| SessionClientIp     | Remote client IP address.                                                                                                                                                                                                                                                                                    | String    |      | 192.168.178.40    | all      |
| SessionClientName   | Remote client name.                                                                                                                                                                                                                                                                                          | String    |      | Client1           | Win      |
| SessionClientDomain | Remote client Active Directory domain.                                                                                                                                                                                                                                                                       | String    |      | vastlimits.com    | Win      |

| Field                   | Description                                                                         | Data type | Unit | Example       | Platform |
|-------------------------|-------------------------------------------------------------------------------------|-----------|------|---------------|----------|
| SessionClientUser       | Remote client user name.                                                            | String    |      | JohnDoe       | Win      |
| SessionClientUserDomain | Remote client user Active Directory domain.                                         | String    |      | Domain        | Win      |
| SessionHRes             | Horizontal resolution.                                                              | String    |      | 1920          | Win      |
| SessionVRes             | Vertical resolution.                                                                | String    |      | 1080          | Win      |
| SessionColorDepth       | Color depth.                                                                        | String    |      | 32            | Win      |
| SessionClientPlatform   | Remote client platform.                                                             | String    |      | Windows       | Win      |
| SessionClientVersion    | Remote client version.                                                              | String    |      | 13.0.0.256735 | Win      |
| SessionClientOsLanguage | Remote client operating system language.                                            | String    |      | en-us         | Win      |
| SessionPublishedName    | Published resource name. This resource was used to start or connect to the session. | String    |      | Google Chrome | Win      |
| SessionPublishedApps    | Citrix published apps in the session.                                               | String    |      | Word Excel    | Win      |

| Field                | Description                                                                                                                  | Data type | Unit | Example                  | Platform |
|----------------------|------------------------------------------------------------------------------------------------------------------------------|-----------|------|--------------------------|----------|
| SessionAppState      | Citrix application state. Possible values: n/a, active, pre-launched, lingering, app not running, unsupported                | String    |      | lingering                | Win      |
| SessionEncryption    | Citrix remoting protocol encryption. Possible values: unknown, basic, logon, 40 bit, 56 bit, 128 bit, SecureICA, unsupported | String    |      | SecureICA                | Win      |
| SessionClientType    | Citrix client type. Possible values: WI, ICA Client                                                                          | String    |      | WI                       | Win      |
| SessionBrokerDnsName | VMware broker DNS name.                                                                                                      | String    |      | HorizonCS.vastlinits.com | Win      |
| SessionBrokerUrl     | VMware broker URL.                                                                                                           | String    |      | https://192.168.8.143    | Win      |

| Field                  | Description                                                                            | Data type | Unit | Example                             | Platform |
|------------------------|----------------------------------------------------------------------------------------|-----------|------|-------------------------------------|----------|
| SessionBrokerTunnel    | VMware indicates if session is tunneled. Possible values: <b>true</b> , <b>false</b> . | String    |      | true                                | Win      |
| SessionBrokerTunnelURL | VMware URL of the View Connection Server tunnel connection.                            | String    |      | https://HorizonCSWastlimits.com:443 | Win      |
| SessionBrokerRemoteIP  | VMware broker remote IP address.                                                       | String    |      | 192.168.178.40                      | Win      |
| SessionBrokerUserName  | VMware broker user name.                                                               | String    |      | John                                | Win      |
| SessionBrokerDomain    | VMware broker user domain name.                                                        | String    |      | Doe                                 | Win      |
| SessionClientTimezone  | VMware client timezone.                                                                | String    |      | Europe/Italy                        | Win      |
| SessionClientID        | VMware client ID.                                                                      | String    |      | c47c60cf41ec44820ff91e1822b24dd8    | Win      |
| SessionType            | VMware session type. Possible values: <b>application</b> , <b>desktop</b> .            | String    |      | application                         | Win      |

| Field                | Description                                                                                                                                             | Data type | Unit | Example      | Platform |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|--------------|----------|
| SessionBrokerType    | Remote broker type.<br>Possible values:<br>Citrix,<br>Microsoft,<br>VMware,<br>Nutanix<br>Frame, none,<br>unknown,<br>Unsupported<br>broker: [ number]. | String    |      | Citrix       | Win      |
| SessionFgAppId       | Foreground application ID.<br>Used by uberAgent to look up application names and populate the field<br><a href="#">SessionFgAppName</a> .               | String    |      | GglChrm      | all      |
| SessionFgAppVersion  | Foreground application version.                                                                                                                         | String    |      | 67.0.3396.99 | all      |
| SessionFgProcessName | Foreground process name.                                                                                                                                | String    |      | chrome.exe   | all      |
| SessionFgProcessId   | Foreground process ID.                                                                                                                                  | Number    |      | 456          | all      |

| Field                         | Description                                                                                                                                         | Data type | Unit | Example                               | Platform |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|---------------------------------------|----------|
| SessionFgBrowserType          | Type of foreground window is a browser: browser type. Possible values: 1, 2, 3, 4. Also see the field <a href="#">SessionFgBrowserDisplayName</a> . | Number    |      | 1                                     | Win      |
| SessionFgBrowserActiveTabHost | URL of active tab. See this <a href="#">KB article</a> for troubleshooting empty values.                                                            | String    |      | uberagent.com                         | Win      |
| SessionFgWindowTitle          | Title of the active foreground window.                                                                                                              | String    |      | Search   Splunk 7.2.1 - Google Chrome | all      |
| SessionClientHardwareID       | Client hardware ID.                                                                                                                                 | Number    |      | 409D39C2                              | Win      |
| SessionRoundTripTime          | Session round trip time.                                                                                                                            | Number    | ms   | 50                                    | Win      |

| Field                    | Description                                                                                                   | Data type | Unit | Example     | Platform |
|--------------------------|---------------------------------------------------------------------------------------------------------------|-----------|------|-------------|----------|
| SessionFps               | Remoting protocol frames per second at collection time. Only available for Citrix and Nutanix Frame sessions. | Number    |      | 20          | Win      |
| SessionTransportProtocol | Protocol chain used for this connection. Only available for Citrix sessions.                                  | String    |      | UDP-CGP-ICA | Win      |

### List of Calculated Fields

| Field          | Description                                                         | Data type | Unit | Example       | Where available               |
|----------------|---------------------------------------------------------------------|-----------|------|---------------|-------------------------------|
| AppName        | Application name. Source is the field <code>SessionFgAppId</code> . | String    |      | Google Chrome | Splunk data model, Splunk SPL |
| SessionCPUTime | Session CPU usage (absolute usage in seconds).                      | Number    | s    | 3             | Splunk data model             |



| Field                             | Description                                               | Data type | Unit | Example          | Where available                  |
|-----------------------------------|-----------------------------------------------------------|-----------|------|------------------|----------------------------------|
| SessionIODuration                 | Percentage of the machine's RAM used by the session.      | Number    | ms   | 90000            | Splunk data model                |
| SessionRAMUsage                   | Alias for SessionUser                                     | String    |      | Domain\JohnDoe   | Splunk data model                |
| User                              | User name converted to lower case.                        | String    |      | domain\johndoe   | Splunk data model                |
| SessionUserLower                  | SessionHRes + "x" + SessionVRes + "x" + SessionColorDepth | String    |      | 1920x1080x32     | Splunk data model                |
| SessionDisplaySpec                | AppsCtxSplit split by semicolon.                          | String    |      | Word;Excel       | Splunk data model                |
| SessionPublishedAppsCtxSplit      | AppsCtxSplit converted to lower case.                     | String    |      | word;excel       | Splunk data model                |
| SessionPublishedAppsCtxSplitLower | Foreground application name.                              | String    |      | Google<br>Chrome | Splunk data model,<br>Splunk SPL |
| SessionFgAppName                  |                                                           |           |      |                  |                                  |

| Field                       | Description                                                                  | Data type | Unit | Example  | Where available               |
|-----------------------------|------------------------------------------------------------------------------|-----------|------|----------|-------------------------------|
| SessionFgBrowserDisplayname | Front browser name.                                                          | String    |      | Chrome   | Splunk data model, Splunk SPL |
|                             | Possible values:<br>Chrome,<br>Internet Explorer,<br>Firefox,<br>Edge.       |           |      |          |                               |
| SessionClientHardwareId     | SessionClientHardwareId or SessionClientHardwareIdCtx, whichever is present. | Number    | Ctx2 | 409D39C2 | Splunk data model             |

## Performance Counter Metrics

July 9, 2024

uberAgent can be configured to collect the values of Windows performance counters. Please see [this document](#) for more information.

### Details

- Source type: `uberAgent:System:PerformanceCounter`
- Used in dashboards: *Windows Performance Counters*
- Enabled through configuration setting: `Perf counter`
- Related configuration settings: *n/a*
- Supported platform: *Windows*

### List of Fields in the Raw Agent Data

| Field                      | Description                   | Data type | Unit | Example      |
|----------------------------|-------------------------------|-----------|------|--------------|
| PerformanceCounterObject   | Performance counter object.   | String    |      | Process      |
| PerformanceCounterInstance | Performance counter instance. | String    |      | conhost      |
| PerformanceCounterName     | Performance counter name.     | String    |      | Handle Count |
| PerformanceCounterValue    | Performance counter value.    | Number    |      | 100          |

## uberAgent Licensing Metrics

July 9, 2024

### uberAgent Licensing

Information on uberAgent licenses.

#### Details

- Source type: `uberAgent:License:LicenseInfo`
- Used in dashboards: *Licensing Status, uberAgent Versions*
- Enabled through configuration setting: *n/a*
- Related configuration settings: *n/a*
- Supported platform: *all*

#### List of Fields in the Raw Agent Data

| Field          | Description                                                                                  | Data type | Unit | Example  |
|----------------|----------------------------------------------------------------------------------------------|-----------|------|----------|
| LicensingState | Licensing state.<br>Possible values:<br><code>licensed</code> ,<br><code>unlicensed</code> . | String    |      | licensed |

| Field                 | Description                                                                                                | Data type | Unit | Example                              |
|-----------------------|------------------------------------------------------------------------------------------------------------|-----------|------|--------------------------------------|
| LicenseId             | License ID.                                                                                                | String    |      | 407d288f-02f7-4375-ae44-ea36654772fa |
| LicenseCountTotal     | Total number of licenses.                                                                                  | Number    |      | 2000                                 |
| LicensingModel        | Licensing model. Possible values: <a href="#">device</a> , <a href="#">user</a> , <a href="#">site</a> .   | String    |      | device                               |
| LicensingModelDetails | Contains more detailed information about the licensing model like if server or client licenses are in use. | String    |      | server                               |
| LicensingType         | Licensing type. Possible values: <a href="#">eval</a> , <a href="#">NFR</a> , <a href="#">full</a> .       | String    |      | full                                 |
| MaintenanceEnd        | Maintenance end. Only for perpetual licenses.                                                              | String    |      | 2018-07-07 01:59:59.000 +0200        |
| Expiration            | Expiration date. Only for one-year term, eval, and community licenses.                                     | String    |      | 2018-07-07 01:59:59.000 +0200        |
| LicensedComponents    | licensed components.                                                                                       | String    |      | unrestricted                         |
| ProductVersion        | Product version.                                                                                           | String    |      | 5.0.1.1609                           |

## User & Host Metrics

July 9, 2024

### User & Host Tags

uberAgent can collect custom tags for users and machines ([more information](#)).

#### Details

- Source type: `uberAgent:Tags:UserHost`
- Used in dashboards: *All except Citrix XA/XD and ADC dashboards*
- Related configuration settings: `[UserHostTagging]`
- Supported platform: *Windows*

#### List of Fields in the Raw Agent Data

---

| Field     | Description                                                                     | Data type | Unit | Example      |
|-----------|---------------------------------------------------------------------------------|-----------|------|--------------|
| User      | The name of the user (in the case of a user tag).                               | String    |      | domain\User1 |
| TagType   | The type of tag (User or Host).                                                 | String    |      | User         |
| TagName   | The user-defined name of the tag.                                               | String    |      | Department   |
| TagSource | The source of the tag (AD, <code>Environment</code> or <code>Registry</code> ). | String    |      | Registry     |

---

| Field    | Description                                                                                                                                                                                 | Data type | Unit | Example                              |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|--------------------------------------|
| TagValue | Defines the complete path of the tag. This can be an AD attribute, an environment variable or the full path to a registry value. The latter must include the registry hive, key, and value. | String    |      | HKCU/Software/vast limits/Department |
| TagData  | The determined value for the current tag.                                                                                                                                                   | String    |      | Development                          |

---

## User Logoff Metrics

November 25, 2024

### Logoff Detail

uberAgent collects various details about logoffs like profile unload time, Group Policy logoff script time as well as process performance.

#### Notes:

- Field: [AppVersion](#) - uberAgent has an internal filter to minimize data volume by suppressing version information for system processes and system services. As a result, the [AppVersion](#) field is typically empty for most system processes and services.

#### Details

- Source type: [uberAgent:Logoff:LogoffDetail](#)

- Used in dashboards: *User Logoff Duration, Single Logoff*
- Enabled through configuration setting: [LogonDetail](#)
- Related configuration settings: *n/a*
- Supported platform: *Windows*

### List of Fields in the Raw Agent Data

| Field             | Description                                                                                                                        | Data type | Unit | Measurement type | Example                              |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------------|--------------------------------------|
| SessionGUID       | Unique identifier that is generated by uberAgent when the session is created. Valid for this session only.                         | String    |      | Snapshot         | 00000002-f295-9109-e7c7-c964011dd401 |
| SessionID         | Unique identifier that is generated by the machine when the session is created. Will be reassigned to other sessions after logoff. | Number    |      | Snapshot         | 3                                    |
| User              | User name.                                                                                                                         | String    |      | Snapshot         | Domain\JohnDoe                       |
| SessionLogoffTime | Time when the user logged off.                                                                                                     | String    |      | Snapshot         | 2018-07-23<br>10:06:02               |
| SessionEndTime    | Time when the session ended.                                                                                                       | String    |      | Snapshot         | 2018-07-23<br>10:08:02               |

| Field                         | Description                                                          | Data type | Unit | Measurement |         |
|-------------------------------|----------------------------------------------------------------------|-----------|------|-------------|---------|
|                               |                                                                      |           |      | type        | Example |
| SessionDurationMs             | Session duration.                                                    | Number    | ms   | Sum         | 25000   |
| ProfileUnloadTimeMs           | MSI profile unloading time.                                          | Number    | ms   | Sum         | 300     |
| GroupPolicyLogoffScriptTimeMs | Group Policy logoff script processing time.                          | Number    | ms   | Sum         | 358     |
| TotalLogoffTimeMs             | Logoff duration combined for all phases.                             | Number    | ms   | Sum         | 40000   |
| ProcessStartCount             | Number of processes started.                                         | Number    |      | Count       | 8       |
| IOCountRead                   | Count of read I/O operations.                                        | Number    |      | Count       | 100     |
| IOCountWrite                  | Count of write I/O operations.                                       | Number    |      | Count       | 100     |
| IOMBRead                      | Amount of read data volume.                                          | Number    | MB   | Sum         | 50      |
| IOMBWrite                     | Amount of write data volume.                                         | Number    | MB   | Sum         | 50      |
| IOLatencyReadMs               | I/O read operation duration divided by count of read I/O operations. | Number    | ms   | Average     | 358     |



| Field           | Description                                                            | Data type | Unit | Measurement type | Example |
|-----------------|------------------------------------------------------------------------|-----------|------|------------------|---------|
| IOLatencyWriteM | I/O write operation duration divided by count of write I/O operations. | Number    | ms   | Average          | 358     |

## Logoff processes

Detailed performance data about all processes active during user logoff like process start time and lifetime duration, commandline, executable path, and CPU footprint.

### Details

- Source type: [uberAgent:Process:LogoffProcesses](#)
- Used in dashboards: *Single Logoff*
- Enabled through configuration setting: [LogonProcesses](#)
- Related configuration settings: *n/a*
- Supported platform: *Windows*

### List of Fields in the Raw Agent Data

| Field          | Description               | Data type | Unit | Measurement type | Example        |
|----------------|---------------------------|-----------|------|------------------|----------------|
| ProcName       | Process name.             | String    |      | Snapshot         | chrome.exe     |
| ProcID         | Process ID.               | Number    |      | Snapshot         | 456            |
| ProcParentName | Parent process name.      | String    |      | Snapshot         | PowerShell.exe |
| ProcParentID   | Parent process ID.        | Number    |      | Snapshot         | 789            |
| ProcUser       | User who ran the process. | String    |      | Snapshot         | Domain\JohnDoe |

| Field                   | Description                                                                                                                                                                | Data type | Unit | Measurement type | Example                                                                    |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------------|----------------------------------------------------------------------------|
| AppId                   | Associated application ID. Used by uberAgent to lookup application names and populate field <a href="#">AppName</a> .                                                      | String    |      | Snapshot         | GglChrm                                                                    |
| AppVersion              | Associated application version.                                                                                                                                            | String    |      | Snapshot         | 67.0.3396.99                                                               |
| LogoffProcType          | uberAgent groups processes running during logon into types. Possible values: <a href="#">Other</a> , <a href="#">GP logoff script</a> , <a href="#">Session teardown</a> . | String    |      | Snapshot         | Other                                                                      |
| ProcStartTimeRelativeMs | Process relative start time.                                                                                                                                               | Number    | ms   | Snapshot         | 16764                                                                      |
| ProcLifetimeMs          | Process lifetime.                                                                                                                                                          | Number    | ms   | Sum              | 73615                                                                      |
| ProcCmdline             | Process command line.                                                                                                                                                      | String    |      | Snapshot         | C:\Program Files (x86)\Google\Chrome\Appl<br>-url<br>http://vastlimits.com |

| Field              | Description                                                                                                | Data type | Unit | Measurement type | Example                                   |
|--------------------|------------------------------------------------------------------------------------------------------------|-----------|------|------------------|-------------------------------------------|
| ProcPath           | Process path.                                                                                              | String    |      | Snapshot         | C:\Program Files (x86)\Google\Chrome\Appl |
| ProcIOReadCount    | Process I/O operation read count.                                                                          | Number    |      | Count            | 2000                                      |
| ProcIOWriteCount   | Process I/O operation write count.                                                                         | Number    |      | Count            | 990                                       |
| ProcIOReadMB       | Process I/O operation read data volume.                                                                    | Number    | MB   | Sum              | 100.05                                    |
| ProcIOWriteMB      | Process I/O operation write data volume.                                                                   | Number    | MB   | Sum              | 16.06                                     |
| ProcIOLatencyRead  | Process I/O operation read latency.                                                                        | Number    | ms   | Average          | 300                                       |
| ProcIOLatencyWrite | Process I/O operation write latency.                                                                       | Number    | ms   | Average          | 300                                       |
| ProcNetKBPS        | Process generated network traffic.                                                                         | Number    | KB   | Sum              | 19.18                                     |
| SessionGUID        | Unique identifier that is generated by uberAgent when the session is created. Valid for this session only. | String    |      | Snapshot         | 00000002-f295-9109-e7c7-c964011dd401      |

| Field               | Description                                                                                                                        | Data type | Unit | Measurement type | Example |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------------|---------|
| SessionID           | Unique identifier that is generated by the machine when the session is created. Will be reassigned to other sessions after logoff. | Number    |      | Snapshot         | 3       |
| TotalLogoffDuration | Total logoff duration.                                                                                                             | Number    | ms   | Sum              | 40000   |
| SortOrder2          | Sort order number to sort the table <i>Boot process performance</i> on the <i>Single Boot</i> dashboard correctly.                 | Number    |      | Snapshot         | 29      |

**List of Calculated Fields**

| Field   | Description                  | Data type | Unit | Measurement type | Where available               | Example       |
|---------|------------------------------|-----------|------|------------------|-------------------------------|---------------|
| AppName | Associated application name. | String    |      | Snapshot         | Splunk data model, Splunk SPL | Google Chrome |

---

| Field     | Description                                                                                                        | Data type | Unit | Measurement type | Where available   | Example |
|-----------|--------------------------------------------------------------------------------------------------------------------|-----------|------|------------------|-------------------|---------|
| SortOrder | Sort order number to sort the table <i>Boot process performance</i> on the <i>Single Boot</i> dashboard correctly. | Number    |      | Snapshot         | Splunk data model | 29      |

---

## User Logon Metrics

November 25, 2024

### Logon Detail

uberAgent collects various details about logons like profile load time, Group Policy processing time as well as process performance.

#### Notes:

- Field: [AppVersion](#) - uberAgent has an internal filter to minimize data volume by suppressing version information for system processes and system services. As a result, the [AppVersion](#) field is typically empty for most system processes and services.

#### Details

- Source type: [uberAgent:Logon:LogonDetail](#)
- Used in dashboards: *Session Info: Citrix*, *Session Info: VMware*, *User Logon Duration*, *User Logon Duration - Group Policy*, *User Session Overview*, *User Sessions*, *Single Machine Detail*, *Single Logon*, *Single User Detail*
- Enabled through configuration setting: [LogonDetail](#)
- Related configuration settings: *n/a*
- Supported platform: *Windows*

**List of Fields in the Raw Agent Data**

| Field            | Description                                                                                                                        | Data type | Unit | Measurement type | Example                              |
|------------------|------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------------|--------------------------------------|
| SessionGUID      | Unique identifier that is generated by uberAgent when the session is created. Valid for this session only.                         | String    |      | Snapshot         | 00000002-f295-9109-e7c7-c964011dd401 |
| SessionID        | Unique identifier that is generated by the machine when the session is created. Will be reassigned to other sessions after logoff. | Number    |      | Snapshot         | 3                                    |
| User             | User name.                                                                                                                         | String    |      | Snapshot         | Domain\JohnDoe                       |
| SessionLogonTime | Time when the user logon started.                                                                                                  | String    |      | Snapshot         | 2018-07-23 08:50:14                  |
| SiteName         | Active Directory site name.                                                                                                        | String    |      | Snapshot         | Default-First-Site-Name              |
| LogonServer      | Authenticating Active Directory domain controller.                                                                                 | String    |      | Snapshot         | DC1                                  |

| Field                            | Description                                                                                                                  | Data type | Unit | Measurement |         |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------|-----------|------|-------------|---------|
|                                  |                                                                                                                              |           |      | type        | Example |
| ProfileLoadTimeMs                | User profile loading time - Microsoft user profile service.                                                                  | Number    | ms   | Sum         | 40000   |
| CitrixPMLoadTimeMs               | User profile loading time - Citrix Profile Management.                                                                       | Number    | ms   | Sum         | 40000   |
| GroupPolicyTotalProcessingTimeMs | Possible Group Policy processing time.                                                                                       | Number    | ms   | Sum         | 250     |
| DcDiscoveryTimeMs                | Domain controller discovery time                                                                                             | Number    | ms   | Sum         | 10      |
| LoopbackMode                     | Group Policy loopback mode. Possible values: <a href="#">replace</a> , <a href="#">merge</a> , <a href="#">no loopback</a> . | String    |      | Snapshot    | replace |
| ADLogonScriptTimeMs              | Active Directory logon script processing time.                                                                               | Number    | ms   | Sum         | 358     |
| GroupPolicyLogonScriptTimeMs     | Group Policy logon script processing time.                                                                                   | Number    | ms   | Sum         | 358     |

| Field               | Description                                                                                             | Data type | Unit | Measurement |         |
|---------------------|---------------------------------------------------------------------------------------------------------|-----------|------|-------------|---------|
|                     |                                                                                                         |           |      | type        | Example |
| ResWmProcessingTime | Time spent in the workspace shell startup time.                                                         | Number    | ms   | Sum         | 358     |
| ShellStartupTime    | Shell startup time. Typically Windows Explorer.                                                         | Number    | ms   | Sum         | 358     |
| TotalLogonTime      | Total logon duration is defined as the time from the actual logon until the shell is fully initialized. | Number    | ms   | Sum         | 40000   |
| ProcessStartCount   | Number of processes started.                                                                            | Number    |      | Count       | 8       |
| IOCountRead         | Count of read I/O operations.                                                                           | Number    |      | Count       | 100     |
| IOCountWrite        | Count of write I/O operations.                                                                          | Number    |      | Count       | 100     |
| IOMBRead            | Amount of read I/O operation data volume.                                                               | Number    | MB   | Sum         | 50      |
| IOMBWrite           | Amount of write I/O operation data volume.                                                              | Number    | MB   | Sum         | 50      |



---

| Field          | Description                                                          | Data type | Unit | Measurement type | Example |
|----------------|----------------------------------------------------------------------|-----------|------|------------------|---------|
| IOLatencyReadM | I/O read operation duration divided by count of read I/O operations. | Number    | ms   | Average          | 358     |

---

### Group Policy CSE Detail

uberAgent collects detailed information about Client-Side-Extensions (CSEs) like name, duration, and return code.

#### Details

- Source type: [uberAgent:Logon:GroupPolicyCSEDetail2](#)
- Used in dashboards: *Session Info: Citrix, Session Info: VMware, User Logon Duration, User Logon Duration - Group Policy, User Session Overview, User Sessions, Single Machine Detail, Single Logon, Single User Detail*
- Enabled through configuration setting: [LogonDetail](#)
- Related configuration settings: *n/a*
- Supported platform: *Windows*

#### List of Fields in the Raw Agent Data

| Field        | Description                                                                                                                        | Data type | Unit | Measurement type | Example                              |
|--------------|------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------------|--------------------------------------|
| SessionGUID  | Unique identifier that is generated by uberAgent when the session is created. Valid for this session only.                         | String    |      | Snapshot         | 00000002-f295-9109-e7c7-c964011dd401 |
| SessionID    | Unique identifier that is generated by the machine when the session is created. Will be reassigned to other sessions after logoff. | Number    |      | Snapshot         | 3                                    |
| User         | User name.                                                                                                                         | String    |      | Snapshot         | Domain\JohnDoe                       |
| CseName      | Client-side extension name.                                                                                                        | String    |      | Snapshot         | Citrix Group Policy                  |
| CseDurationS | Client-side extension processing time.                                                                                             | Number    | s    | Sum              | 5.40                                 |
| CseGPONames  | Group Policy where client-side extension is configured.                                                                            | String    |      | Snapshot         | Default Domain Policy                |

| Field         | Description                                                               | Data type | Unit | Measurement type | Example |
|---------------|---------------------------------------------------------------------------|-----------|------|------------------|---------|
| CseReturnCode | Client-side extension processing return code. Everything except 0 is bad. | Number    |      | Snapshot         | 0       |

## Logon Processes

Detailed performance data about all processes active during user logon like process start time and lifetime duration, commandline, executable path, and CPU footprint.

### Details

- Source type: [uberAgent:Process:LogonProcesses](#)
- Used in dashboards: *Single Logon*
- Related configuration settings: *n/a*
- Supported platform: *Windows*

### List of Fields in the Raw Agent Data

| Field                | Description               | Data type | Unit | Measurement type | Example        |
|----------------------|---------------------------|-----------|------|------------------|----------------|
| ProcName             | Process name.             | String    |      | Snapshot         | chrome.exe     |
| ProcID               | Process ID.               | Number    |      | Snapshot         | 456            |
| ProcParentNameParent | Parent process name.      | String    |      | Snapshot         | PowerShell.exe |
| ProcParentID         | Parent process ID.        | Number    |      | Snapshot         | 789            |
| ProcUser             | User who ran the process. | String    |      | Snapshot         | Domain\JohnDoe |

---

| Field      | Description                                                                                                           | Data type | Unit | Measurement type | Example      |
|------------|-----------------------------------------------------------------------------------------------------------------------|-----------|------|------------------|--------------|
| AppId      | Associated application ID. Used by uberAgent to lookup application names and populate field <a href="#">AppName</a> . | String    |      | Snapshot         | GglChrm      |
| AppVersion | Associated application version.                                                                                       | String    |      | Snapshot         | 67.0.3396.99 |

| Field         | Description                                                                                                                                                                                                                                                                                                                                                                    | Data type | Unit | Measurement type | Example         |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------------|-----------------|
| LogonProcType | uberAgent groups processes running during logon into types. Possible values:<br>Other<br>,Userinit<br>,AppSetup<br>,Active Setup,AD logon script,GP logon script<br>,Shell,RES Workspace Manager shell,RES Workspace Manager shell child,GP software installation<br>,Run once<br>,Initial program, User profile<br>,Group Policy<br>,Session setup<br>,First logon animation. | String    |      | Snapshot         | GP logon script |

| Field                   | Description                              | Data type | Unit | Measurement |                                                                            |
|-------------------------|------------------------------------------|-----------|------|-------------|----------------------------------------------------------------------------|
|                         |                                          |           |      | type        | Example                                                                    |
| ProcStartTimeRelativeMs | Process relative start time.             | Number    | ms   | Snapshot    | 16764                                                                      |
| ProcLifetimeMs          | Process lifetime.                        | Number    | ms   | Sum         | 73615                                                                      |
| ProcCmdline             | Process command line.                    | String    |      | Snapshot    | C:\Program Files (x86)\Google\Chrome\Appl<br>-url<br>http://vastlimits.com |
| ProcPath                | Process path.                            | String    |      | Snapshot    | C:\Program Files (x86)\Google\Chrome\Appl                                  |
| ProcCPUTimeMs           | Process consumed CPU time.               | Number    | ms   | Sum         | 11859                                                                      |
| ProcIOReadCount         | Process I/O operation read count.        | Number    |      | Count       | 2000                                                                       |
| ProcIOWriteCount        | Process I/O operation write count.       | Number    |      | Count       | 990                                                                        |
| ProcIOReadMB            | Process I/O operation read data volume.  | Number    | MB   | Sum         | 100.05                                                                     |
| ProcIOWriteMB           | Process I/O operation write data volume. | Number    | MB   | Sum         | 16.06                                                                      |
| ProcIOLatencyReadMs     | Process I/O operation read latency.      | Number    | ms   | Average     | 300                                                                        |
| ProcIOLatencyWriteMs    | Process I/O operation write latency.     | Number    | ms   | Average     | 300                                                                        |

| Field                   | Description                                                                                                                        | Data type | Unit | Measurement |                                      |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-------------|--------------------------------------|
|                         |                                                                                                                                    |           |      | type        | Example                              |
| ProcWorkingSetMB        | Process consumed RAM.                                                                                                              | Number    | MB   | Snapshot    | 500.06                               |
| ProcNetKBPS             | Process generated network traffic.                                                                                                 | Number    | KB   | Sum         | 19.18                                |
| SessionGUID             | Unique identifier that is generated by uberAgent when the session is created. Valid for this session only.                         | String    |      | Snapshot    | 00000002-f295-9109-e7c7-c964011dd401 |
| SessionID               | Unique identifier that is generated by the machine when the session is created. Will be reassigned to other sessions after logoff. | Number    |      | Snapshot    | 3                                    |
| TotalLogonDurationTotal | Total logon duration.                                                                                                              | Number    | ms   | Sum         | 40000                                |

| Field      | Description                                                                                                    | Data type | Unit | Measurement type | Example |
|------------|----------------------------------------------------------------------------------------------------------------|-----------|------|------------------|---------|
| SortOrder2 | Sort order number to sort the table <i>Logon process performance_on the _Single Logon dashboard correctly.</i> | Number    |      | Snapshot         | 29      |

**List of Calculated Fields**

| Field     | Description                                                                                                 | Data type | Unit | Measurement type | Where available               | Example       |
|-----------|-------------------------------------------------------------------------------------------------------------|-----------|------|------------------|-------------------------------|---------------|
| AppName   | Associated application name.                                                                                | String    |      | Snapshot         | Splunk data model, Splunk SPL | Google Chrome |
| SortOrder | Sort order number to sort the table <i>Boot process performance on the Single Boot dashboard correctly.</i> | Number    |      | Snapshot         | Splunk data model             | 1             |

**ESA Metrics**

July 9, 2024

uberAgent ESA collects many different metrics, logically grouped into sourcetypes. All metrics are explained in detail in this chapter, including:



- Name and description
- Supported platform
- Unit and example
- Related source type and where to find it in the dashboards
- Calculated fields and their availability in Splunk's data model and/or "Search Processing Language" (SPL)
- Related settings in the [configuration file](#)

## Threat Detection Metrics

November 25, 2024

### Process Tagging

uberAgent processes a rule set and applies tags accordingly.

#### Notes:

- Field: [AppVersion](#) - uberAgent has an internal filter to minimize data volume by suppressing version information for system processes and system services. As a result, the [AppVersion](#) field is typically empty for most system processes and services.

#### Details

- Source type: [uberAgentESA:ActivityMonitoring:ProcessTagging](#)
- Used in dashboards: *Threat Detection Events*
- Enabled through configuration setting: [ActivityMonitoring](#)
- Related configuration settings: [[ActivityMonitoringRule](#)]
- Supported platform: *Windows*

#### List of Fields in the Raw Agent Data

| Field          | Description                                                                                                                                                  | Data type | Unit | Example                                                                                                        |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|----------------------------------------------------------------------------------------------------------------|
| EventType      | Event type. Can be 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25 or 26. See also <a href="#">EventTypeName</a> . | Number    |      | 4                                                                                                              |
| ProcName       | Process name.                                                                                                                                                | String    |      | svchost.exe                                                                                                    |
| ProcParentName | Parent process name.                                                                                                                                         | String    |      | services.exe                                                                                                   |
| ProcUser       | Process user.                                                                                                                                                | String    |      | domain\JohnDoe                                                                                                 |
| ProcLifetimeMs | Process lifetime.                                                                                                                                            | Number    | ms   | 500                                                                                                            |
| Procid         | Process ID.                                                                                                                                                  | Number    |      | 12345                                                                                                          |
| ProcParentId   | Parent process ID.                                                                                                                                           | Number    |      | 67890                                                                                                          |
| ProcGUID       | Process GUID.                                                                                                                                                | String    |      | 4b3e3686-7854-4d98-0023-1e0e617bf2e4                                                                           |
| ProcParentGUID | Parent process GUID.                                                                                                                                         | String    |      | d72ceb7e-7851-02ec-005d-139741c4afd6                                                                           |
| ProcPath       | Process path                                                                                                                                                 | String    |      | C:\WINDOWS\System32\svcho                                                                                      |
| ProcCmdline    | Process commandline.                                                                                                                                         | String    |      | C:\WINDOWS\System32\svcho<br>-k<br>LocalSystemNet-<br>workRestricted<br>net-connect-<br>suspicious-<br>sources |
| ProcTag1       | Rule tag: the tag assigned to events originating from the matching rule.                                                                                     | String    |      | net-connect-<br>suspicious-<br>sources                                                                         |

| Field          | Description                                                                            | Data type | Unit | Example                                  |
|----------------|----------------------------------------------------------------------------------------|-----------|------|------------------------------------------|
| ProcRiskScore1 | Rule risk score: the risk score assigned to events originating from the matching rule. | Number    |      | 75                                       |
| IsElevated     | Indicates if the process was started elevated (admin rights).                          | String    |      | 1                                        |
| SessionId      | Session ID.                                                                            | Number    |      | 2                                        |
| SessionGUID    | Session GUID.                                                                          | String    |      | 00000000-b242-d759-7a63-d686b0ffd501     |
| AppId          | Application ID.                                                                        | String    |      | Svc:WdiSystemHost                        |
| AppVersion     | Application version.                                                                   | String    |      | 1.0                                      |
| IsProtected    | Indicates if the process was started protected.                                        | String    |      | 1                                        |
| EventCount     | The number of identical events that occurred during the interval period.               | Number    |      | 42                                       |
| RuleAnnotation | JSON of rule annotations like security frameworks.                                     | String    |      | {“mitre_attack”: [“T1086”, “T1059.001”]} |

Additionally, one can enhance the information sent to the back-end by defining a number of [generic properties](#) that will be sent along with the fields above. Any field listed under [Common Event Properties](#), [Network Event Properties](#), [Image Load Event Properties](#), or [Registry Event Properties](#) can be used as a generic property.

## **List of Calculated Fields**



| Field         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Data type | Unit | Example       | Where available                  |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|---------------|----------------------------------|
| EventTypeName | Names for event types based on the lookup<br>lookup_process_tagging_eventtype<br>. Can be<br>Process.<br>Start,<br>Process.<br>Stop,<br>Image.Load<br>,<br>Net.<br>Connect,<br>Net.<br>Receive,<br>Net.<br>Reconnect,<br>Net.<br>Retransmit<br>,Net.Send,<br>Reg.Key.<br>Create,<br>Reg.Value.<br>Write,<br>Reg.Delete<br>,<br>Reg.Key.<br>Delete,<br>Reg.Value.<br>Delete,<br>Reg.Key.<br>SecurityChange<br>,<br>Reg.Key.<br>Rename,Reg<br>.Key.<br>SetInformation<br>,<br>Reg.Key.<br>Load, | String    |      | Process.Start | Splunk data model,<br>Splunk SPL |

| Field                                 | Description                                                                                                    | Data type | Unit | Example            | Where available                  |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------|-----------|------|--------------------|----------------------------------|
| ProcUser                              | <code>coalesce ( ProcUserExpanded , ProcUser )</code> .                                                        | String    |      | Domain\JohnDoe     | Splunk data model                |
| User                                  | <code>ProcUser</code> .                                                                                        | String    |      | Domain\JohnDoe     | Splunk data model                |
| TimestampMs                           | <code>_time * 1000</code> .                                                                                    | Number    | ms   | 1585913547467      | Splunk data model                |
| RuleAnnotation. <del>One attack</del> | <code>One attack</code> MITRE ATT&CK® IDs for the event. The source is the field <code>RuleAnnotation</code> . | String    |      | T1086<br>T1059.001 | Splunk data model,<br>Splunk SPL |

## Generic Properties

July 30, 2024

Sometimes, when a Threat Detection rule matches an event, one would like to have more information than what the fields of the source type `uberAgentESA:ActivityMonitoring:ProcessTagging` provide. In such a case, one can define up to 10 generic properties per rule that can access the event information the query has access to. Any event property listed under [Common Event Properties](#), [Network Event Properties](#), [Image Load Event Properties](#), or [Registry Event Properties](#) can be used as a generic property. Note that certain properties are only defined for specific event types. For instance, `Net.Target.Port` and `Reg.Key.Path` are only available for `network` and `registry` event types, respectively. Please refer to [Event Types](#) for a list of available event types, as well as the individual event properties documentation pages mentioned above.

Generic properties can be defined using one of the two syntaxes, long form:

```
1 GenericProperty1Name = ProcHash
2 GenericProperty1Data = Process.Hash.MD5
```

or short form:

```
1 GenericProperty1 = Process.Hash.MD5
```

in which case, the fields `GenericProperty1Name` and `GenericProperty1Data`, containing `Process.Hash.MD5` and the process's MD5 hash respectively, will be sent to `uberAgentESA:ActivityMonitoring:ProcessTagging`.

## DNS Query Monitoring Metrics

July 9, 2024

### DNS Query Monitoring

uberAgent collects [detailed information about DNS queries](#): the request, all responses, and the process from which the query originated.

#### Details

- Source type: `uberAgentESA:Process:DnsQuery`
- Used in dashboards: *Process DNS*
- Enabled through configuration setting: `DnsMonitoring`
- Related configuration settings: *n/a*
- Supported platform: *all*

#### List of Fields in the Raw Agent Data

---

| Field                    | Description         | Data type | Unit | Example                                           |
|--------------------------|---------------------|-----------|------|---------------------------------------------------|
| <code>ProcName</code>    | Process name.       | String    |      | <code>svchost.exe</code>                          |
| <code>ProcGUID</code>    | Process GUID.       | String    |      | <code>4b3e3686-7854-4d98-0023-1e0e617bf2e4</code> |
| <code>DnsRequest</code>  | DNS query name.     | String    |      | <code>www.example.com</code>                      |
| <code>DnsResponse</code> | DNS query response. | String    |      | <code>10.1.3.12</code>                            |



| Field           | Description                                     | Data type | Unit | Example |
|-----------------|-------------------------------------------------|-----------|------|---------|
| DnsResponseType | DNS query response type (e.g.: A, AAAA, CNAME). | String    |      | A       |
| DnsEventCount   | Number of requests in the last interval.        | Number    |      | 1       |

The fields [DnsRequest](#), [DnsResponse](#), and [DnsResponseType](#) may contain multiple values, separated by a semicolon ;.

### List of Calculated Fields

| Field       | Description                | Data type | Unit | Example       | Where available   |
|-------------|----------------------------|-----------|------|---------------|-------------------|
| TimestampMs | <code>_time</code> * 1000. | Number    | ms   | 1585913547467 | Splunk data model |

## Process Stop Metrics

November 25, 2024

### Process Stop

uberAgent collects detailed process stop information like the process name, the process lifetime as well as the parent process.

#### Notes:

- Field: [AppVersion](#) - uberAgent has an internal filter to minimize data volume by suppressing version information for system processes and system services. As a result, the [AppVersion](#) field is typically empty for most system processes and services.

**Details**

- Source type: [uberAgentESA:Process:ProcessStop](#)
- Used in dashboards: *Process Tree*
- Enabled through configuration setting: [ProcessStop](#)
- Related configuration settings: *n/a*
- Supported platform: *Windows*

**List of Fields in the Raw Agent Data**

---

| Field          | Description                                                   | Data type | Unit | Example                                                              |
|----------------|---------------------------------------------------------------|-----------|------|----------------------------------------------------------------------|
| ProcName       | Process name.                                                 | String    |      | svchost.exe                                                          |
| ProcUser       | Process user.                                                 | String    |      | domain\JohnDoe                                                       |
| ProcLifetimeMs | Process lifetime.                                             | Number    | Ms   | 500                                                                  |
| AppId          | Application ID.                                               | String    |      | Svc:WdiSystemHost                                                    |
| ProcId         | Process ID.                                                   | Number    |      | 12345                                                                |
| ProcParentId   | Parent process ID.                                            | Number    |      | 67890                                                                |
| SessionId      | Session ID.                                                   | Number    |      | 2                                                                    |
| ProcGUID       | Process GUID.                                                 | String    |      | 4b3e3686-7854-4d98-0023-1e0e617bf2e4                                 |
| SessionGUID    | Session GUID.                                                 | String    |      | 00000000-b242-d759-7a63-d686b0ffd501                                 |
| ProcParentName | Parent process name.                                          | String    |      | services.exe                                                         |
| ProcPath       | Process path.                                                 | String    |      | C:\WINDOWS\System32\svcho                                            |
| ProcCmdline    | Process commandline.                                          | String    |      | C:\WINDOWS\System32\svcho<br>-k<br>LocalSystemNet-<br>workRestricted |
| IsElevated     | Indicates if the process was started elevated (admin rights). | String    |      | 1                                                                    |

| Field          | Description                                     | Data type | Unit | Example                              |
|----------------|-------------------------------------------------|-----------|------|--------------------------------------|
| AppVersion     | Application version.                            | String    |      | 1.0                                  |
| ProcParentGUID | Parent process GUID.                            | String    |      | d72ceb7e-7851-02ec-005d-139741c4afd6 |
| IsProtected    | Indicates if the process was started protected. | String    |      | 1                                    |
| HashMD5        | Process hash value in MD5.                      | String    |      | 7FFE122B109F1B586DEA2ED0             |
| HashSHA1       | Process hash value in SHA1.                     | String    |      | 26DBC241A37881072689CD05             |
| HashSHA256     | Process hash value in SHA256.                   | String    |      | 95F0FBBAEF28999238598550D            |
| HashIMP        | Import-table hash.                              | String    |      | 188392D5FBCC485811BB54211            |

### List of Calculated Fields

| Field       | Description                                             | Data type | Unit | Example        | Where available   |
|-------------|---------------------------------------------------------|-----------|------|----------------|-------------------|
| ProcUser    | <code>coalesce ( ProcUserExpanded , ProcUser )</code> . | String    |      | Domain\JohnDoe | Splunk data model |
| User        | <code>ProcUser</code> .                                 | String    |      | Domain\JohnDoe | Splunk data model |
| TimestampMs | <code>_time * 1000</code> .                             | Number    | Ms   | 1585913547467  | Splunk data model |

### Scheduled Task Metrics

July 9, 2024

## Scheduled Tasks

uberAgent collects detailed scheduled task information like the task name, the author as well as if it has actions.

### Details

- Source type: [uberAgentESA:System:ScheduledTasks](#)
- Used in dashboards: *Scheduled Tasks*
- Enabled through configuration setting: [ScheduledTaskMonitoring](#)
- Related configuration settings: *n/a*
- Supported platform: *Windows*

### List of Fields in the Raw Agent Data

---

| Field         | Description                                                                                                | Data type | Unit | Example                       |
|---------------|------------------------------------------------------------------------------------------------------------|-----------|------|-------------------------------|
| TaskEventType | Scheduled task event type.<br>Possible values:<br>0, 1, 2. See also <a href="#">TaskEventDisplayName</a> . | Number    |      | 2                             |
| TaskFolder    | Folder where the scheduled task is stored.                                                                 | String    |      | \Microsoft\Windows\Flighting\ |
| TaskName      | Scheduled task name.                                                                                       | String    |      | RefreshCache                  |

---

| Field         | Description                                                                                                                                                                                                                                                                                                        | Data type | Unit | Example    |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------|
| TaskUserName  | Account that created, changed, or deleted the task. Possible values: <code>sys</code> , <code>lvc</code> , <code>nvc</code> or any other user. The first three will be expanded in the field <code>TaskPrincipalExpanded</code> through the lookup [ <code>systemusers</code> ] from the uberAgent UXM Splunk app. | String    |      | AD\JohnDoe |
| TaskPrincipal | Account that is used when running the task. Possible values: <code>sys</code> , <code>lvc</code> , <code>nvc</code> or any other user. The first three will be expanded in the field <code>UserNameExpanded</code> through the lookup [ <code>systemusers</code> ] from the uberAgent UXM Splunk app.              | String    |      | sys        |

---

| Field      | Description                                                                                                                                                            | Data type | Unit | Example               |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-----------------------|
| LogonType  | The logon type for the account configured in the field <code>TaskPrincipal</code> . Possible values: 0, 1, 2, 3, 4, 5, 6. See also <code>LogonTypeDisplayName</code> . | Number    |      | 5                     |
| Elevated   | Indicates whether the task is running elevated or not. Possible values: 0, 1.                                                                                          | Number    |      | 0                     |
| TaskAuthor | Author that created the task. Can be any string and will often be empty.                                                                                               | String    |      | Microsoft Corporation |
| TaskHidden | Indicates if the task is hidden in the UI or not. Possible values: 0, 1.                                                                                               | String    |      | 0                     |
| WakeToRun  | Indicates if the Task Scheduler will wake the computer when it is time to run the task. Possible values: 0, 1.                                                         | String    |      | 0                     |

| Field      | Description                                                                                                                                                                                                 | Data type | Unit | Example |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|---------|
| HasActions | Indicates if the task has actions. Actions are send separately in the source type<br><code>uberAgentESA</code><br><code>:System:</code><br><code>ScheduledTaskActions</code><br>. Possible values:<br>0, 1. | String    |      | 1       |

**List of Calculated Fields**

| Field            | Description                                            | Data type | Unit | Example                                              | Where available   |
|------------------|--------------------------------------------------------|-----------|------|------------------------------------------------------|-------------------|
| TaskPath         | <code>TaskFolder</code><br>+ <code>TaskName</code> .   | String    |      | <code>\Microsoft\Windows\Sysprep\OneSettings\</code> | Splunk data model |
| time             | <code>_time</code> .                                   | Number    |      | 2020-04-06T14:48:01.394+02:00                        | Splunk data model |
| UserNameExpanded | <code>coalesce(UserNameExpanded,TaskUserName)</code> . | String    |      | SYSTEM                                               | Splunk data model |

| Field                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Data type | Unit | Example        | Where available               |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|----------------|-------------------------------|
| LogonTypeDisplayName | <p>Field Name for the field</p> <p><a href="#">LogonType</a> based on the lookup <a href="#">scheduledtasks_logontypes</a>.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li><a href="#">Unspecified</a>: used for non-NT credentials.</li> <li><a href="#">UsePassword</a>: use a password for logging on the user.</li> <li><a href="#">ServiceForUser</a>: the service will log the user on using Service For User (S4U), and the task will run in a non-interactive desktop.</li> <li><a href="#">LogonInteractive</a>: user must already be logged on. The task will be run only in an existing interactive session.</li> <li><a href="#">LogonGroup</a>: group activation.</li> </ul> | String    |      | ServiceAccount | Splunk data model, Splunk SPL |



| Field                | Description                                                                                                                                                                                           | Data type | Unit | Example | Where available               |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|---------|-------------------------------|
| TaskEventDisplayName | Expansion for the field <code>TaskEventType</code> based on the lookup <code>scheduledtasks_eventtypes</code> . Possible values: <code>Created</code> , <code>Updated</code> , <code>Deleted</code> . | String    |      | Updated | Splunk data model, Splunk SPL |

## Scheduled Task Actions

uberAgent collects details about configured actions of scheduled tasks like the action type, the path to the exe as well as mail settings.

### Details

- Source type: `uberAgentESA:System:ScheduledTaskActions`
- Used in dashboards: *Scheduled Tasks*
- Enabled through configuration setting: `ScheduledTaskMonitoring`
- Related configuration settings: *n/a*
- Supported platform: *Windows*

## List of Fields in the Raw Agent Data

| Field        | Description                                                        | Data type | Unit | Example                         |
|--------------|--------------------------------------------------------------------|-----------|------|---------------------------------|
| TaskPath     | Task path.                                                         | String    |      | \Microsoft\Windows\WindowsStart |
| IsDeprecated | Indicates if the task is deprecated or not. Possible values: 0, 1. | String    |      | 0                               |

---

| Field           | Description                                                                                                                                                | Data type | Unit | Example                    |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|----------------------------|
| ActionType      | The configured action. Possible values: 0, 1, 2, 3. See also <a href="#">ActionTypeDisplayName</a> .                                                       | Number    |      | 2                          |
| ActionListIndex | Represents the position in the list of configured actions. 1 means that the action is at the top of the list, 2 represents the second position, and so on. | Number    |      | 1                          |
| ExePath         | Path to the executable which is run. Only filled if <a href="#">ActionTypeDisplayName</a> is <a href="#">ExecutableAction</a> .                            | String    |      | C:\WINDOWS\system32\sc.exe |
| ExeArguments    | Arguments of the executable which is run. Only filled if <a href="#">ActionTypeDisplayName</a> is <a href="#">ExecutableAction</a> .                       | String    |      | start wuau serv            |

| Field                 | Description                                                                                                                      | Data type | Unit | Example                              |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------|-----------|------|--------------------------------------|
| ExeWorkingDir         | Working dir of the executable which is run. Only filled if <code>ActionTypeDisplayName</code> is <code>ExecutableAction</code> . | String    |      | C:\WINDOWS\system32                  |
| ComClsid              | COM action ID. Only filled if <code>ActionTypeDisplayName</code> is <code>ComAction</code> .                                     | String    |      | b1aebb5d-ead9-4476-b375-9c3ed9f32afc |
| ComData               | COM action data. Only filled if <code>ActionTypeDisplayName</code> is <code>ComAction</code> .                                   | String    |      | timer                                |
| ComBinary             | COM action binary. Only filled if <code>ActionTypeDisplayName</code> is <code>ComAction</code> .                                 | String    |      | %SystemRoot%\System32\sp             |
| ComHandlerDescription | COM action handler description. Only filled if <code>ActionTypeDisplayName</code> is <code>ComAction</code> .                    | String    |      | SppSvcRestartTaskHandler Class>      |
| ComRemoteComputer     | COM action remote computer. Only filled if <code>ActionTypeDisplayName</code> is <code>ComAction</code> .                        | String    |      |                                      |

| Field          | Description                                                                                                                                                         | Data type | Unit | Example              |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|----------------------|
| ComServiceName | COM action service name.<br>Only filled if <a href="#">ActionTypeDisplayName</a> is <a href="#">ComAction</a> .                                                     | String    |      | wuuser               |
| AutoElevated   | Indicates if the COM action runs auto-elevated.<br>Only filled if <a href="#">ActionTypeDisplayName</a> is <a href="#">ComAction</a> .<br>Possible values:<br>0, 1. | String    |      | 0                    |
| EmailBcc       | Email Bcc value.<br>Only filled if <a href="#">ActionTypeDisplayName</a> is <a href="#">EmailAction</a> .                                                           | String    |      | johndoe@company.com  |
| EmailCc        | Email Cc value.<br>Only filled if <a href="#">ActionTypeDisplayName</a> is <a href="#">EmailAction</a> .                                                            | String    |      | johndoe@company.com  |
| EmailFrom      | Email sender.<br>Only filled if <a href="#">ActionTypeDisplayName</a> is <a href="#">EmailAction</a> .                                                              | String    |      | Alerting@company.com |
| EmailServer    | Email server.<br>Only filled if <a href="#">ActionTypeDisplayName</a> is <a href="#">EmailAction</a> .                                                              | String    |      | mail.company.com     |
| EmailSubject   | Email subject.<br>Only filled if <a href="#">ActionTypeDisplayName</a> is <a href="#">EmailAction</a> .                                                             | String    |      | Very urgent alert    |

---

| Field      | Description                                                                                                       | Data type | Unit | Example            |
|------------|-------------------------------------------------------------------------------------------------------------------|-----------|------|--------------------|
| EmailTo    | Email recipient.<br>Only filled if<br><code>ActionTypeDisplayName</code><br>is<br><code>EmailAction</code> .      | String    |      | alerts@company.com |
| MsgTitle   | Message title.<br>Only filled if<br><code>ActionTypeDisplayName</code><br>is<br><code>MessageAction</code><br>.   | String    |      | Some title         |
| MsgContent | Message content.<br>Only filled if<br><code>ActionTypeDisplayName</code><br>is<br><code>MessageAction</code><br>. | String    |      | Some content       |

---

### List of Calculated Fields

| Field                  | Description                                                                                                                                                                                                                                    | Data type | Unit | Example                       | Where available               |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-------------------------------|-------------------------------|
| ActionTypeDisplayNames | Expansion of the field <code>ActionType</code> based on the lookup <code>scheduledtasks_actiontypes</code> . Possible values: <code>ExecutableAction</code> , <code>ComAction</code> , <code>EmailAction</code> , <code>MessageAction</code> . | String    |      | ExecutableAction              | Splunk data model, Splunk SPL |
| time                   | <code>_time.</code>                                                                                                                                                                                                                            | Number    |      | 2020-04-06T14:48:01.394+02:00 | Splunk data model             |

## Scheduled Task Triggers

uberAgent collects details about configured triggers of scheduled tasks like the trigger type as well as the repetition.

### Details

- Source type: `uberAgentESA:System:ScheduledTaskTriggers`
- Used in dashboards: *Scheduled Tasks*
- Enabled through configuration setting: `ScheduledTaskMonitoring`
- Related configuration settings: *n/a*
- Supported platform: *Windows*

### List of Fields in the Raw Agent Data

| Field                    | Description                                                                                                                               | Data type | Unit | Example                                                                                       |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-----------------------------------------------------------------------------------------------|
| TaskPath                 | Task path.                                                                                                                                | String    |      | \Microsoft\Windows\Device Information\Device                                                  |
| TriggerId                | Identifier for the trigger. Is often empty.                                                                                               | String    |      | NightlyTrigger                                                                                |
| TriggerType              | Trigger type.<br>Possible values:<br>0, 1, 2, 3, 4, 5, 6,<br>7, 8, 9, 10, 11,<br>12. See also<br><a href="#">TriggerTypeDisplayName</a> . | Number    |      | 1                                                                                             |
| EventTriggerSubscription | A query string that identifies the event that fires the trigger.                                                                          | String    |      | <query id='1'<br>><select<br>path='System'<br>>*[System/<br>Level=2]</<br>select></<br>query> |
| EventTriggerNumValue     | The number of queries specified on the matching event.                                                                                    | Number    |      | 2                                                                                             |
| TriggerUserId            | The ID of the user that fires the trigger (only in State-change trigger and logon trigger).                                               | String    |      | AD\JohnDoe                                                                                    |

| Field                     | Description                                                                                                                                         | Data type | Unit | Example                             |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-------------------------------------|
| LogonTriggerPossiblyGroup | The ID displayed in the field <a href="#">TriggerUserId</a> is possibly the ID of user-group, instead of an individual user. Possible values: 0, 1. | String    |      | 1                                   |
| TriggerEnabled            | Indicates if the trigger is enabled or not. Possible values: 0, 1.                                                                                  | String    |      | 1                                   |
| TriggerStartBoundary      | The start date when the trigger is active.                                                                                                          | String    |      | 2020-04-09<br>15:41:27.000<br>+0200 |
| TriggerEndBoundary        | The end date after which the trigger is not active anymore.                                                                                         | String    |      | 2020-04-11<br>15:41:27.000<br>+0200 |
| TriggerRepetitionDuration | For how long the repetition pattern (repetition interval) is repeated, see <a href="#">ISO8601 Durations</a> .                                      | String    |      | PT23H59M                            |
| TriggerRepetitionInterval | The repetition pattern (e.g. daily, monthly, etc.), see <a href="#">ISO8601 Durations</a> .                                                         | String    |      | PT2H                                |



| Field                                | Description                                                                                                                                                  | Data type | Unit | Example                       |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|-------------------------------|
| TriggerRepetitionStopAtDateWhenEnter | Indicates whether a running task is stopped when the repetition pattern duration expires. Possible values: 0, 1.                                             | String    |      | 0                             |
| TriggerListIndex                     | Represents the position in the list of configured triggers. 1 means that the trigger is at the top of the list, 2 represents the second position, and so on. | Number    |      | 1                             |
| DayDisplayName                       | Indicates on which days the trigger runs.                                                                                                                    | String    |      | Sunday                        |
| WeekDisplayName                      | Indicates on which weeks the trigger runs.                                                                                                                   | String    |      | First;Second;Third;Fourth     |
| MonthDisplayName                     | Indicates in which months the trigger runs.                                                                                                                  | String    |      | Jan;Feb;Mar;Apr;May;Jun;Jul;A |
| DayOfMonthDisplayName                | Indicates on which days of a month the trigger runs.                                                                                                         | String    |      | 1;15;30                       |
| DailyTriggerDaysInterval             | The number of days between the subsequent firing of the daily trigger.                                                                                       | Number    |      | 2                             |

| Field                                    | Description                                                                                                                                                                                                                      | Data type | Unit | Example          |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------------|
| WeeklyTriggerWeeksInterval               | Number of weeks between the subsequent firing of the weekly trigger.                                                                                                                                                             | Number    |      | 3                |
| MonthlyTriggerRunOnLastDayOfTheMonth     | monthly trigger is fired on the last day of the month.<br>Possible values:<br>0, 1.                                                                                                                                              | String    |      | 1                |
| MonthlyDowTriggerRunOnLastWeekOfTheMonth | monthly day-of-week trigger is fired on the last week of the month.<br>Possible values:<br>0, 1.                                                                                                                                 | String    |      | 1                |
| StateChangeId                            | User session state change ID. Only filled if <a href="#">TriggerTypeDisplayName</a> is <a href="#">SessionStateChangeTrigger</a> . Possible values:<br>0, 1, 2, 3, 4, 7, 8.<br>See also <a href="#">StateChangeDisplayName</a> . | String    |      | 1                |
| WnfTriggerStateName                      | Windows Notification Facility (WNF) state name. Also see <a href="#">WnfIdDisplayName</a> .                                                                                                                                      | String    |      | 1192063AA3BC0875 |

**List of Calculated Fields**

| Field              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Data type | Unit | Example        | Where available               |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|----------------|-------------------------------|
| StateChangeDisplay | Expansion of the field <code>StateChange</code> based on the lookup <code>scheduledtasks_sessionstatechanges</code> . Possible values:<br><code>UndefinedStateChange0</code><br><code>,</code><br><code>ConsoleConnect</code><br><code>,</code><br><code>ConsoleDisconnect</code><br><code>,</code><br><code>RemoteConnect</code><br><code>,</code><br><code>RemoteDisconnect</code><br><code>,</code><br><code>UndefinedStateChange1</code><br><code>,</code><br><code>UndefinedStateChange2</code><br><code>,</code><br><code>SessionLock</code><br><code>,</code><br><code>SessionUnlock</code><br><code>.</code> | String    |      | ConsoleConnect | Splunk data model, Splunk SPL |

| Field              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Data type | Unit | Example                   | Where available               |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|---------------------------|-------------------------------|
| TriggerTypeDisplay | <p>Expansion of the field <code>TriggerType</code> based on the lookup <code>scheduledtasks_triggertypes</code>. Possible values:</p> <ul style="list-style-type: none"> <li>EventTrigger</li> <li>,</li> <li>TimeTrigger</li> <li>,</li> <li>DailyTrigger</li> <li>,</li> <li>WeeklyTrigger</li> <li>,</li> <li>MonthlyTrigger</li> <li>,</li> <li>MonthlyDowTrigger</li> <li>,</li> <li>IdleTrigger</li> <li>,</li> <li>RegistrationTrigger</li> <li>,</li> <li>BootTrigger</li> <li>,</li> <li>LogonTrigger</li> <li>,</li> <li>UndefinedTrigger</li> <li>,</li> <li>SessionStateChangeTrigger</li> <li>,</li> <li>CustomTrigger01</li> </ul> <p>. Further explanations on these triggers are available in the lookup</p> | String    |      | SessionStateChangeTrigger | Splunk data model, Splunk SPL |

| Field            | Description                                                                                                                                                                                         | Data type | Unit | Example                                      | Where available   |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|----------------------------------------------|-------------------|
| time             | <code>_time.</code>                                                                                                                                                                                 | Number    |      | 2020-04-06T14:48:01.394+0200                 | Splunk data model |
| WnfIdDisplayName | Expansion of the field <code>WnfTriggerStateName</code> based on the lookup <code>wnf_ids</code> . Further explanations on the collected WNF IDs are available in the lookup <code>wnf_ids</code> . | String    |      | WNF_RTDS_NAME_SPLUNK_RELATION_TRIGGER_CHANGE | Splunk SPL        |

## Advanced Topics

July 9, 2024

This section contains information about advanced topics like multi-tenancy or data volume optimization.

### Multi-Tenancy With Splunk

July 9, 2024

If you are a service provider, it is not necessary to set up a dedicated Splunk server for every customer. Splunk fully supports multi-tenancy and uberAgent does, too. This article describes how to configure it.

## Concepts

Splunk stores data in indexes. Regarding multi-tenancy, the important thing is that you can set permissions per index.

Setting up a multi-tenant Splunk & uberAgent installation is simple. We are going to follow the concept outlined in the [Splunk blog](#).

## Implementation

Actually, all you have to do is described very well in the [Splunk blog article](#) mentioned earlier. Here is a summary:

- Create a unique index per customer. Please note that all uberAgent indexes should start with a common prefix (e.g. `uberagent`) so that they can be searched with a single wildcard statement (e.g. `uberagent*`). Valid names would be `uberagent-customer1` and `uberagent-customer2`.
- To set up custom index names follow the instructions in [this article](#).
- Configure users according to the [Splunk blogs article](#).

## Result

If you have configured this, you have a setup where Splunk administrators can search everything while individual customer admins can only search their own data.

## Reducing the Data Volume

September 2, 2024

Since Splunk is licensed by daily indexed data volume, it is in every customer's interest to keep the data volume generated by uberAgent as small as possible. uberAgent comes prepared for that by offering two default configurations and many ways for fine-tuning.

### Choose Between Detail and Data Volume

Start by choosing either the default configuration, which provides **full detail** and high resolution or the configuration optimized for data volume, which differs from the default in the following ways:

- Process & application performance: information is collected only on the 10-15 **most active processes** in terms of CPU, RAM, disk, and network utilization. The processes included in the data collection are determined dynamically for every collection interval. One could say uberAgent "follows" the active processes.
- **Collection interval** of 120 s instead of 30 s.

See [this document](#) for instructions on how to switch between the two configurations.

## Take Stock

Before modifying the configuration, find out how much data is generated per endpoint by the default settings. The easiest way to do that is to have uberAgent tell you in the [Data Volume dashboard](#).

## Reduce the Data Volume per Endpoint

Once you know the currently generated data volume, you should have an idea by how much it needs to be reduced. Start with the endpoint configuration.

Through [uberAgent's configuration](#) you can do three things to reduce the data volume:

### Reduce the Frequency

By default, uberAgent collects performance data every 30 seconds. You can cut the volume nearly in half by changing the frequency to one minute (any other value is possible, too, of course).

You can fine-tune the data collection by adding additional timers. The data collection frequency can be set per timer. Move each metric to the timer with the desired frequency to optimally balance accuracy and data volume. While optimizing, focus on those metrics that generate the highest data volume (the *Data Volume* dashboard shows you which those are).

### Remove Metrics

By default, all metrics are enabled. If you do not need the information collected by some of them, turn them off by removing them from the configuration.

### Special Treatment for ProcessDetail

As you can see in the *Data Volume* dashboard, the ProcessDetail metric generates by far the highest data volume. Consider replacing `ProcessDetailFull` with `ProcessDetailTop5`. Once you do that, uberAgent only collects performance data for processes with the highest activity. This may lead to a dramatic reduction in data volume.

**ProcessDetailTop5** By configuring `ProcessDetailTop5`, only the top 5 ProcessDetail metrics are collected based on each of the following criteria:

- Process CPU usage
- Count of process I/O read/write operations
- Amount of process I/O read/write operations data volume
- Process consumed RAM
- Process generated network traffic

**Process Allowlist and Denylist** Alternatively, you can filter the processes for which detailed performance data is collected. The [configuration](#) section `ProcessDetailFull_Filter` makes it possible to put processes on an allowlist or denylist. The allowlist takes precedence over the denylist. If you are only interested in specific processes, put them on the allowlist. On the other hand, if you want to see everything except data from certain processes, put them on the denylist.

## Reduce the Number of Endpoints

If the data volume is still too high after optimizing the configuration as recommended above you need to reduce the number of endpoints that send data to Splunk. You can simply do that by stopping and disabling the `uberAgent` system service on select endpoints.

## Demoing uberAgent With the Event Generator for Splunk

July 25, 2024

Demonstrating uberAgent can be a bit difficult if you do not have a few dozen machines with live users available. To simplify demos, we offer an event generator that simulates an RDSH site with 5 active servers and 10 user sessions each.

### Architecture

Starting with uberAgent version 6, the Splunk event generator dependency was removed and uberAgent event generator is a single Splunk app. When Splunk is started, a .NET Core program generates sample data. By default sample data for two hours is generated. If you want to generate additional sample data, you can either restart the Splunk service after 2 hours, or modify the `uAEventGen.conf` file (see section "Advanced configuration").



The Splunk app can be used on Windows, Linux, and on macOS-based Splunk installations. Single server setups and distributed deployments are fully supported. The standard installation sends the data to a local Splunk instance using the TCP port 19500.

## Installation

### .NET Core

As of uberAgent version 6, .NET Core is a prerequisite that must be installed on the same server where Splunk is installed. In the case of a distributed environment, .NET Core must be installed on the same Splunk indexers where you want to install the uberAgent event generator Splunk app.

You can download .NET Core [here](#).

### uberAgent Event Generator

Install the uberAgent event generator on one of the indexers. If you have a single Splunk server, install the event generator on that server.

- Download the [uberAgent event generator](#) (find out what's new in the [changelog](#))
- On the Splunk server navigate to **Manage apps**
- Click **Install app from file**
- Select the archive you downloaded earlier and click **Upload**
- Restart Splunk

That's it. The event generator starts generating events right after Splunk has been restarted. It will continue to do so for approx. 2 hours and then stop on its own. Just what you need for a demo. To re-enable restart Splunk again.

## Configuration

### Enabling or Disabling the Event Generator

To enable or disable the uberAgent event generator:

1. On the Splunk server where the uberAgent event generator app is installed navigate to **Manage apps**
2. Locate the *uberAgent event generator* app and click on **enable** or **disable**
3. Restart Splunk

## Advanced Configuration

The default configuration should work for a single instance Splunk environment. If you have a distributed Splunk environment or you want to generate different generated sample data, you can modify the configuration file `uAEventGen.conf` which is located `%Splunkhome%/etc/apps/uberAgent_eventgenerator/bin/uAEventGenBinaries/your platform`. The file contains full documentation of all possible configuration options.

## Recommendations for Custom Dashboards (Splunk)

July 9, 2024

### Why Create Custom Dashboards

uberAgent ships with more than 60 dashboards that visualize every metric uberAgent collects. So why create custom dashboards?

uberAgent's dashboards need to work for all customers. They must be generic and cannot have dependencies on other apps.

The needs of our customers are as diverse as their networks. Custom dashboards meet the most specific requirements. They provide KPIs and views tailored to a customer's needs. And custom dashboards can bring data from multiple sources together: uberAgent + X + Y. That is what Splunk calls operational intelligence.

### Where to Create Custom Dashboards

Dashboards need to "live" somewhere. In Splunk, a dashboard's natural habitat is an app. Apps are containers for dashboards and files. Apps allow you to:

- Keep related items in one place
- Add a corporate logo
- Assign permissions
- Publish to Splunkbase

## Dashboard Authoring Recommendations

### Create Your Own App

At first, people are often tempted to store their custom dashboard files in the uberAgent app directory. That seems to be the easiest way, but it breaks easily when the uberAgent Splunk apps are updated.

**We recommend hosting custom dashboards in your own app**, independent of uberAgent.

### Do Not Hard-Code Things

Networks are dynamic, as is uberAgent. New versions may bring new sourcetypes, data models, and fields.

uberAgent provides macros to simplify future upgrades. uberAgent's macros can be used globally (e.g., in other apps, too). The use of the following macros is highly recommended:

- `uberAgent_index`: stores the name of the uberAgent Splunk index
- `uA_DM_dataset`: stores the name of the data model that contains a given dataset

All macros are defined in the file `macros.conf` of the uberAgent Splunk dashboard app.

### Copy From Us

The best way to get to know the data collected and visualized by uberAgent is to look at the source code of the dashboards that ship with the product. We understand that practical examples can be very helpful and we explicitly recommend to reuse parts of the product's default dashboards in your custom dashboards.

### Professional Services

Help and support services for custom dashboard creation are available through our network of [solution partners and consultants](#). Our partners are competent both with uberAgent and with Splunk. They are able to assist you with PoCs, architecture, customizations as well as quotes and pricing.

### Custom Scripts

July 9, 2024

uberAgent can collect data for arbitrary custom metrics through a generic script execution engine. It runs any type of script at any desired interval, either per machine or per user session.

## How to Configure Custom Script Execution

The execution of custom scripts is handled by uberAgent's endpoint agent. Scripts are configured as part of `Timer` stanzas in [uberAgent's configuration](#). The following lists the relevant configuration options:

```
1 # Setting name: Name
2 # Description: Arbitrary name for the timer.
3 # Valid values: any string
4 # Default: empty
5 # Required: yes
6 #
7 # Setting name: Interval
8 # Description: How long to wait before collecting data again. Unit:
 milliseconds.
9 # Valid values: any number
10 # Default: [none]
11 # Required: yes
12 #
13 # Setting name: Script
14 # Description: Run a script once or periodically, depending on the
 configured Interval (0 = run only once). The script's output to
 stdout is sent to Splunk, each line as a new event. Can be specified
 more than once per timer.
15 # Valid values: Any valid command line, optionally including command
 line parameters.
16 # Default: empty
17 # Required: no
18 #
19 # Setting name: ScriptContext
20 # Description: The user context to run a script in.
21 # Valid values: Session0AsSystem | UserSessionAsSystem |
 UserSessionAsUser
22 # Default: Session0AsSystem
23 # Required: no
```

Please note that the uberAgent service on the endpoint is running in the context of `LocalSystem`, so the referenced script must be accessible by the `LocalSystem` account. This is particularly relevant when running scripts stored on a network file share.

### Script

You can use any script written in your preferred scripting language, e.g., PowerShell, Python, VB-Script... Our agent will capture all script output sent to standard output (`stdout`), i.e., printed to the console. Every line of output is sent to the backend as one event. Script output must be formatted as **key-value** pairs (e.g., `key1=value1 key2=value2`).

The key name may contain characters that are invalid for field names on some backends. Such characters are automatically replaced with underscores (`_`). If field names do not start with a letter, they are

prepended with `uA_`. This is done for every type of receiver to ensure that field names are identical on every backend.

Please keep in mind that any data collected in addition to our default dataset has an impact on the generated data volume. Running custom scripts generates additional load on the endpoint the amount of which depends on the executed process (e.g., `powershell.exe` or `cscript.exe`) and the underlying data source. Especially Windows Management Instrumentation (WMI) can cause a significant load.

Additionally, please choose an appropriate timer interval for your script. Data that does not change often, like inventory information, probably only need to be collected once a day whereas volatile metrics like network throughput might have to be collected once per minute.

**Deployment** uberAgent does not manage the deployment process of custom scripts to the endpoints. Please feel free to use either your existing software distribution system or Splunk's Deployment Server.

An alternative for PowerShell scripts is to encode the script in Base64 and reference the result as parameter.

```
1 # Place the script content in the variable MyScript
2 $MyScript = '@'
3 script content goes here
4 '@
5
6 # Convert to base64 and output to a file to avoid word wrapping on the
 commandline.
7 [Convert]::ToBase64String([Text.Encoding]::Unicode.GetBytes($MyScript))
 > C:\base64_output.txt
```

Add the result as parameter to PowerShell in a timer:

```
1 [Timer]
2 Name = Some name
3 Interval = 30000
4 Script = powershell.exe -executionpolicy bypass -
 EncodedCommand "JABFAHIAcgB ... vAGkAbgAgACcAIAAnACkA"
5 ScriptContext = UserSessionAsUser
```

## Script Context

Custom scripts can be executed in three different contexts:

- **Session0AsSystem:** the script runs in session 0 as LocalSystem
- **UserSessionAsSystem:** the script runs in every interactive user session as LocalSystem

- **UserSessionAsUser:** the script runs in every interactive user session as the user logged on to the session

The script context is configured per timer. Of course, you can configure multiple timers for independent execution of different scripts.

### Session GUIDs

To uniquely identify RDS sessions, uberAgent creates its own session GUIDs. These GUIDs are part of all sourcetypes containing data related to user sessions (e.g., logon and logoff).

If the data from a custom script needs to be associated with a specific session, the script should make use of the session's GUID.

Scripts can read session GUIDs from the registry key `HKLM\SOFTWARE\vast limits\uberAgent\SessionGuids`. Each value *name* is the ID of a Windows session. The associated value *data* contains uberAgent's session GUID.

The **sourcetype** used for the script's output is a concatenation of `uberAgent:Script:` and the timer name specified in uberAgent's configuration.

### Examples

For examples that make use of the custom script functionality please see the [practice guide](#) section. Another example can be found [here](#).

## Data Distribution and Separation (Routing to Multiple Backends)

July 9, 2024

In some scenarios, it is necessary to distribute the data collected by uberAgent to different backend systems. Do you need to build an even more complex backend infrastructure for that? No, this can be achieved in an easy and straightforward way just by modifying the [agent's configuration](#).

### Concept

uberAgent supports multiple data receivers per endpoint by default. Every timer and metric can be bound to one or multiple receivers. That architectural option gives you amazing flexibility out of the box.

The index name can be configured per receiver stanza as well. This makes it possible to configure the data retention per uberAgent metric based on the resulting index in the backend infrastructure.

## Implementation

You can make use of this configuration as follows:

- Create a second (, third, ...) [Receiver] stanza.
- Bind all [Timer] stanzas to the correct receiver based on your requirements.
- Restart the uberAgent service.

## Configuration Example

In this example, we are separating uberAgent's inventory data by routing it to an additional Splunk environment.

Configure two [Receiver] stanzas like this:

```
1 [Receiver]
2 Name = uberAgent
3 Type = Splunk
4 Protocol = TCP
5 Index = uberAgent
6 Servers = Server_A:19500
7
8 [Receiver]
9 Name = uberAgent_Inventory
10 Type = Splunk
11 Protocol = TCP
12 Index = uberAgent_Inventory
13 Servers = Server_B:19500
```

Bind all [Timer] stanzas and the [OnDemand] stanza to the default receiver **uberAgent** like this:

```
1 #####
2 # On-demand metrics
3 #####
4 [OnDemand]
5 Receivers = uberAgent
6 UA metric = LogonDetail
7 UA metric = LogonProcesses
8 UA metric = BootDetail
9 UA metric = ShutdownDetail
10 UA metric = StandbyDetail
11 UA metric = ProcessStartup
12 UA metric = OutlookPerformanceEvents
13 UA metric = ApplicationErrors
14 UA metric = ApplicationUIDelay
15 #####
```

```

16 # Timer 1
17 #####
18 [Timer]
19 Receivers = uberAgent
20 Name = Default timer
21 Comment = Metrics are placed here unless there is a reason to
 have them run at different frequencies or to isolate them
22 Interval = 30000
23 UA metric = ProcessDetailFull
24 UA metric = ApplicationUsage
25 UA metric = SessionCount
26 UA metric = SessionDetail
27 UA metric = SystemPerformanceSummary
28 UA metric = SMBClientSharePerformance

```

Configure only the inventory [Timer] stanza (default: Timer6) to use the `uberAgent_Inventory` receiver:

```

1 #####
2 # Timer 6
3 #####
4 [Timer]
5 Receivers = uberAgent_Inventory
6 Name = Inventory
7 Comment = Perform an inventory at a very low frequency
8 Interval = 86400000
9 Start delay = 6000
10 Persist interval = true
11 Thread priority = background
12 UA metric = ApplicationInventory
13 UA metric = SoftwareUpdateInventory
14 UA metric = MachineInventory
15 UA metric = CitrixADCInventory

```

## Result

As described in this example, you have the ability to granularly route uberAgent's data on a per-metric level to different backend systems. That can be very handy to separate and distribute a subset of data to a specific group or to implement a per-metric data retention policy.

## User & Host Tags

July 25, 2024

uberAgent collects an extensive [list of metrics](#). Pre-built Splunk dashboards allow you to filter the data by computer name, hardware manufacturer, IP address, or user, to name just a few of the available



filtering options.

Businesses often store data about a machine's build in the device's registry. User information, on the other hand, is typically managed in Active Directory (e.g., the user's department).

uberAgent's user & host tags feature allows you to integrate custom identifiers in such a way that dashboards can be filtered by their values.

Here is an **example**: your organization stores the version of a machine's OS image in a registry value on each machine. If you configure uberAgent to pick up that image build version through a host tag, you can filter the uberAgent dashboards by the version of your OS images. This allows you to determine if a new issue you are analyzing was introduced with a recent OS image, for example.

## Tag Sources

Supported sources for tags are:

- Active Directory attributes
- Environment variables
- Registry values

These sources can be queried either per user or per computer.

## Requirements

- uberAgent version 5.3 or later
- Host tags are determined with the *HostTags* metric.
- User tags are determined with the *UserTags* metric.

## Configuration

*To configure the tags feature you can either use the configuration file or group policy. In this article, we are using the configuration file.*

The stanza of interest in the configuration file is [[UserHostTagging](#)]. You can have multiple of these, one for each tag you want to set. The configurable settings are:

Tag name

- A user-defined unique name of the tag. Spaces are permitted.
- This is the tag you can search for later in the dashboards.
- Example: [Department](#)

Tag type

- Defines if the tag is a host or a user tag
- Valid values: `Host`, `User`
- Example: `User`

#### Tag source

- Defines the source where the tag data is read from. Registry values of type `REG_EXPAND_SZ` are automatically expanded.
- Valid values: `Registry`, `Environment`, `Ad`
- Example: `Registry`

#### Tag value

- The source element/path to read the tag's data from.
- Registry format: any registry path, e.g., `HKCU\Software\vast limits\Department` (supported hives: `HKLM` and `HKCU`)
- Environment variable format: the variable name enclosed in percent signs, e.g., `%DEPARTMENT%`
- AD format: just the attribute name, e.g., `Department`

Additionally, the metric `UserTags` and/or `HostTags` need to be configured in at least one timer.

With the examples from above, you would get the following stanza:

```
1 [Timer]
2 Name = User tags
3 Comment = Collect configured user tags
4 Interval = 60000
5 UA metric = UserTags
6
7 [UserHostTagging]
8 Tag name = Department
9 Tag type = User
10 Tag source = Registry
11 Tag value = HKCU\Software\vast limits\Department
```

Additionally, an [event trigger](#) can be defined to collect the user tag for a single user after logon.

```
1 [Timer]
2 Name = User tags
3 Comment = Collect configured user tags
4 Interval = 60000
5 UA metric = UserTags
6 EventTrigger = TriggerUserTags
7
8 [EventTrigger platform=Windows]
9 Name = TriggerUserTags
10 Type = UserLogon
11
12 [UserHostTagging]
```

```

13 Tag name = Department
14 Tag type = User
15 Tag source = Registry
16 Tag value = HKCU\Software\vast limits\Department

```

Another example: group machines by roles like notebook, graphics workstation, desktop PC, virtual machine, or executive machine with an environment variable.

```

1 [Timer]
2 Name = Host tags
3 Comment = Collect configured host tags
4 Interval = 600000
5 UA metric = HostTags
6
7 [UserHostTagging]
8 Tag name = Machine role
9 Tag type = Host
10 Tag source = Environment
11 Tag value = %MACHINEROLE%

```

You can find more examples in our [practice guide](#) on the subject.

## Usage in Splunk

The capability to filter for tags is built into the dashboards since version 5.3. To filter for host tags choose the `Host tags` filter field and to filter for user tags choose the `User tags` filter field.

When using our user tag `Department` from above a search for all users from human resources would look like this:

| Filter field: | Filter operator: | Filter expression:          |        |
|---------------|------------------|-----------------------------|--------|
| User tags     | in               | Department=Human Ressources | Submit |

You can also search for users from two or more departments by listing them comma-separated.

| Filter field: | Filter operator: | Filter expression:           |        |
|---------------|------------------|------------------------------|--------|
| User tags     | in               | Department=IT,Department=Hur | Submit |

Interested in all users where `Department` has a value (is not `null`)?

| Filter field: | Filter operator: | Filter expression: |        |
|---------------|------------------|--------------------|--------|
| User tags     | in               | *Department*       | Submit |

**Note** the asterisks around the tag's name. This is needed by design when searching for the tag's name only.

## uAQL - uberAgent Query Language

July 30, 2024

### Overview

The **uberAgent Query Language (uAQL)** is the language for uberAgent's powerful [Threat Detection](#) and [Event Data Filtering](#) queries. Take a look at [this blog post](#) for an quick **introduction**.

uAQL query strings evaluate to either **true** or **false**. A simple example: the query `Process.Name == "explorer.exe"` tests if the current process name is equal to `explorer.exe`.

1. If yes, the query yields **true**
2. If no, the query yields **false**

### Data Types

uAQL is a type-safe language supporting the following data types:

- Integer (a number)
- Boolean (**true** or **false**)
- String (a UTF-8 string literal, in other words: text)

#### Integer

A uAQL integer is a 64-bit signed number. Valid values are in the range between `-9223372036854775808` and `9223372036854775807`.

#### Boolean

A uAQL boolean is either **true** or **false**. Strings are implicitly converted to **false**. Integers with the value 1 are implicitly converted to **true**. All other integers are implicitly converted to **false**.

#### String

A uAQL string represents a sequence of characters that are wrapped in double quotes (`"`) or single quotes (`'`), e.g., `"string 1"` or `'string 2'`. Mixing different types of quotes (e.g., `"uberAgent'`) is not allowed and results in a syntax error.

**Character Escaping** Special characters can be specified by escaping them with a prepended backslash (\). This makes it possible to use newlines (\n), tabs (\t), and many other special characters in queries.

As a result, backslashes in paths, etc. need to be escaped, too. A Windows path such as C:\Windows is written in uAQL as "C:\\Windows".

**Important:** Regular expressions require a second round of escaping. To use the path C:\Windows in a regex, specify it as "C:\\\\\\Windows".

**Raw Strings** To avoid having to write so many backslashes, consider using raw string literals, in other words, strings with character escaping disabled. Raw string literals start with a leading r before the opening quote. The path C:\Windows would be specified as a raw string like this: r"C:\Windows".

**Important:** regular expressions and the operators like as well as glob still require escaping, even with raw strings. To use the path C:\Windows in a regex or with like or glob, specify it as a raw string literal as r"C:\\Windows".

**Character Escaping Examples** The following uAQL queries demonstrate different ways of matching files in uberAgent's Config cache directory.

Using the `icontains` operator and a regular string:

```
1 Query = icontains(File.Path, "\\vast limits\\uberAgent\\Config cache\\")
```

Using the `like` operator and a raw string:

```
1 Query = File.Path like r"%\\vast limits\\uberAgent\\Config cache\\%"
```

Using the `like` operator and a regular string:

```
1 Query = File.Path like "%\\\\vast limits\\\\uberAgent\\\\Config cache\\\\%"
```

## Array

Arrays are special datatypes in uAQL that can hold one or multiple integers, booleans, and strings. An array is defined through square brackets: [Element 1, Element 2, Element n].

Arrays can be used in queries with the `in` operator. The following example tests if the current process name is equal to one of the elements in the array:

```
1 Process.Name in ["uberAgent.exe", "explorer.exe", "cmd.exe"]
```

## Operators

uAQL comes with operators for all sorts of logical and binary comparisons.

---

| Operator                | Description                                                                                                                                                                                              |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>and, AND</code>   | Logical AND                                                                                                                                                                                              |
| <code>or, OR</code>     | Logical OR                                                                                                                                                                                               |
| <code>not, NOT</code>   | Logical NOT                                                                                                                                                                                              |
| <code>==</code>         | Equality. Case-insensitive for strings.                                                                                                                                                                  |
| <code>===</code>        | Equality. Case-sensitive for strings.                                                                                                                                                                    |
| <code>!=</code>         | Inequality. Case-insensitive for strings.                                                                                                                                                                |
| <code>!==</code>        | Inequality. Case-sensitive for strings.                                                                                                                                                                  |
| <code>&lt;</code>       | Less than.                                                                                                                                                                                               |
| <code>&lt;=</code>      | Less than or equal.                                                                                                                                                                                      |
| <code>&gt;</code>       | Greater than.                                                                                                                                                                                            |
| <code>&gt;=</code>      | Greater than or equal.                                                                                                                                                                                   |
| <code>in, IN</code>     | Tests if the value on the left-hand side is equal to any element of the array on the right-hand side. Case-sensitive for strings.                                                                        |
| <code>like, LIKE</code> | Pattern matching comparison as in SQL. The following wildcards can be used: The percent sign (%) matches zero, one, or many characters, including spaces. The underscore (_) matches a single character. |
| <code>glob, GLOB</code> | Uses the Unix file globbing syntax for wildcards. Case-sensitive.                                                                                                                                        |

---

## Functions

The following functions can be used in uAQL queries:

---

| Function                    | Description                                                 |
|-----------------------------|-------------------------------------------------------------|
| <code>strlen(string)</code> | Returns the length of a string in characters as an integer. |

---

| Function                                            | Description                                                                                                                                                                                                                    |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>concat(string, string)</code>                 | Concatenates two strings and returns the result.                                                                                                                                                                               |
| <code>lower(string)</code>                          | Transforms a string to lowercase and returns the result.                                                                                                                                                                       |
| <code>upper(string)</code>                          | Transforms a string to uppercase and returns the result.                                                                                                                                                                       |
| <code>startswith(string, string)</code>             | Returns <b>true</b> if the first string starts with the second string, otherwise <b>false</b> . Case-sensitive.                                                                                                                |
| <code>istartswith(string, string)</code>            | Returns <b>true</b> if the first string starts with the second string, otherwise <b>false</b> .<br>Case-insensitive.                                                                                                           |
| <code>endswith(string, string)</code>               | Returns <b>true</b> if the first string ends with the second string, otherwise <b>false</b> . Case-sensitive.                                                                                                                  |
| <code>iendswith(string, string)</code>              | Returns <b>true</b> if the first string ends with the second string, otherwise <b>false</b> .<br>Case-insensitive.                                                                                                             |
| <code>contains(string, string)</code>               | Returns <b>true</b> if the first string contains the second string, otherwise <b>false</b> . Case-sensitive.                                                                                                                   |
| <code>icontains(string, string)</code>              | Returns <b>true</b> if the first string contains the second string, otherwise <b>false</b> .<br>Case-insensitive.                                                                                                              |
| <code>join(string array, seperator)</code>          | Returns a concatenated list of all elements from the string array. The seperator can contain 0 to n characters. This function is useful when querying results returned by the <code>registry_read_stringmulti</code> function. |
| <code>regex_match(string, string)</code>            | Returns <b>true</b> if the first string is matchable against the regular expression in the second string, otherwise <b>false</b> . Case-insensitive.                                                                           |
| <code>regex_match_path(string, string)</code>       | Unlike the default <code>regex_match</code> this version evaluates paths first. See <a href="#">PATH_REGEX</a> for more details. Case-insensitive.                                                                             |
| <code>registry_read_binary(hive, key, value)</code> | Reads a binary value from the registry and returns the data as a hexadecimal string (e.g. 0102FCFF). The hive, key and value parameters are strings.                                                                           |
| <code>registry_read_number(hive, key, value)</code> | Reads a number from the registry. The hive, key and value parameters are strings.                                                                                                                                              |

| Function                                                 | Description                                                                                              |
|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| <code>registry_read_string(hive, key, value)</code>      | Reads a string from the registry. The hive, key and value parameters are strings.                        |
| <code>registry_read_stringmulti(hive, key, value)</code> | Reads a multi line string from the registry. The hive, key and value parameters are strings.             |
| <code>get_env(environment variable name)</code>          | Reads and returns the string value of a given environment variable name.                                 |
| <code>set(variable name, value)</code>                   | Changes the string value of a given variable. Returns true on success, otherwise false.                  |
| <code>seti(variable name, value)</code>                  | Changes the integer value of a given variable. Returns true on success, otherwise false.                 |
| <code>setb(variable name, value)</code>                  | Changes the boolean value of a given variable. Returns true on success, otherwise false.                 |
| <code>isnull(variable name)</code>                       | Returns <b>true</b> if the given variable name has a null (undefined) value.                             |
| <code>isnull_or_empty(variable name)</code>              | Returns <b>true</b> if the given variable name has a null (undefined) value or if it is an empty string. |
| <code>r"string"</code>                                   | Evaluates a string as raw string, i.e., with character escaping turned off (see above).                  |

## Reserved Keywords

All [event property names](#) are reserved. Also, operator names including the following keywords are reserved:

| Keyword                     | Description                                                                                                                                              |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>true</b> , TRUE, True    | Boolean <b>true</b> constant.                                                                                                                            |
| <b>false</b> , FALSE, False | Boolean <b>false</b> constant.                                                                                                                           |
| <b>null</b> , NULL, Null    | Null (undefined) value. E.g. returned by any <code>registry_read_</code> function which reads data that does not match the expected registry value type. |



## Persistent Output Queue With Intelligent Disk Buffering

July 9, 2024

Persistent Output Queue with Intelligent Disk Buffering is uberAgent's sophisticated technology that ensures no outgoing events are lost while maintaining a minimal footprint and generating no disk IO at all during normal (online) operations.

### How Does the Persistent Output Queue Work

#### Case A: Backend is Reachable

uberAgent constantly monitors network connectivity to its backend. As long as the backend is reachable and processes new events correctly, the endpoint agent does not store events on disk but sends them to the backend directly, thus avoiding any disk IO on the endpoint.

#### Case B: Backend is Unreachable

If the backend becomes unreachable, either because network connectivity is lost or because the backend has issues accepting data, the agent writes new events to the Persistent Output Queue's local database. uberAgent periodically checks if connectivity is back up. Once that is the case, it sends all events that were buffered to disk and reverts to the efficient direct sending (see case A).

### Persistent Output Queue and Splunk Universal Forwarder

On mobile devices, uberAgent was traditionally coupled with Splunk's Universal Forwarder (UF) due to the UF's persistent queue functionality. With uberAgent's built-in POQ, it's not necessary anymore to deploy the UF just for its disk buffering feature.

### Disk Space Requirements

The maximum disk space to be used by the POQ can be limited in uberAgent's configuration (see below). The following table is intended as a rough indicator of disk space requirements (PC with average usage, 10 hours uptime, default uberAgent configuration):

---

| Backend | Disk space per day |
|---------|--------------------|
| Elastic | 200 MB             |

---

---

| Backend         | Disk space per day |
|-----------------|--------------------|
| Kafka           | 410 MB             |
| Microsoft OMS   | 220 MB             |
| Splunk via HTTP | 120 MB             |
| Splunk via TCP  | 70 MB              |

---

## Configuration Settings

Persistent Output Queue is configured per receiver. Please note that receivers with a POQ must have a unique name.

### Enabling or Disabling the POQ

**PersistentOutputQueue** Enables or disables the Persistent Output Queue for the current receiver.

If the Persistent Output Queue is disabled, uberAgent reverts to simple memory buffering (see the configuration setting [MaxQueueSizeRamMb](#)).

- Setting name: [PersistentOutputQueue](#)
- Valid values: [Off](#), [SQLite](#)
- Default: [SQLite](#)
- Required: no

### Limiting POQ Disk Space Usage

**PersistentOutputQueueMaxAgeDays** Configures the maximum retention time for POQ entries. Entries older than the specified number of days are removed.

- Setting name: [PersistentOutputQueueMaxAgeDays](#)
- Valid values: positive numbers (0 = unlimited)
- Default: 120
- Required: no

**PersistentOutputQueueMaxSizeMb** Configures the maximum disk space in MB for the Persistent Output Queue. The file size is checked after events are stored. It is therefore possible that the configured limit is slightly exceeded.

- Setting name: `PersistentOutputQueueMaxSizeMb`
- Valid values: positive numbers (0 = unlimited)
- Default: 500
- Required: no

POQ events are stored in the format expected by the receiver's backend. Some backends expect the data in a JSON format, while others accept raw data. Especially the JSON format bloats events considerably, which means that the required disk space can be much larger than the raw event data as indexed by Splunk.

### POQ Location on Disk

**PersistentOutputQueuePathWindows** Specifies the POQ storage location on Windows machines. Environment variables are supported.

- Setting name: `PersistentOutputQueuePathWindows`
- Valid values: any valid path
- Default: `%PROGRAMDATA%\vast limits\uberAgent\Output Queue`
- Required: no

When the default path is used, uberAgent sets the permissions on the directory so that only members of the local group `Administrators` and the local system have read/write access. When a custom path is specified, uberAgent does not set permissions on the POQ directory. We highly recommend securing the directory.

**PersistentOutputQueuePathMacOS** The setting `PersistentOutputQueuePathMacOS` specifies the POQ storage location on Windows machines. Environment variables are *not* supported.

- Setting name: `PersistentOutputQueuePathMacOS`
- Valid values: any valid path
- Default: `/Library/Application Support/uberAgent/Output Queue`
- Required: no

When the default path is used, uberAgent sets the permissions on the directory so that only the root user has read/write access. When a custom path is specified, uberAgent does not set permissions on the POQ directory. We highly recommend securing the directory.

### Miscellaneous Settings

**PersistentOutputQueueErrorHandling** Configures how errors during POQ event processing are handled.

- Setting name: `PersistentOutputQueueErrorHandling`
- Valid values: `IgnoreFile`, `StopReceiver`, `Shutdown`
- Default: `IgnoreFile`
- Required: no

In case of an error (e.g., out of disk space), uberAgent may either stop the current receiver (`StopReceiver`), shut down the agent entirely (`Shutdown`), or ignore the current POQ file (`IgnoreFile`). In case all receivers have stopped, uberAgent shuts itself down.

## Advanced Settings

**PersistentOutputQueueNextSendAttemptSeconds** Configures when to perform a next send attempt in case the backend is not reachable.

- Setting name: `PersistentOutputQueueNextSendAttemptSeconds`
- Valid values: positive numbers (0 = no wait delay)
- Default: 25
- Required: no

**PersistentOutputQueueMaxInMemoryBulkOperations** Configures how many bulk send operations are kept in memory before storing them in the Persistent Output Queue. A single bulk send operation consists of all events within a run that are generated for an uberAgent metric (e.g., process detail).

A value of 0 (zero) disables the in-memory cache. In this case, all events are stored in the Persistent Output Queue before sending them to the backend. This provides maximum preservation of data at the expense of I/O.

- Setting name: `PersistentOutputQueueMaxInMemoryBulkOperations`
- Valid values: positive numbers (0 = disables in-memory cache)
- Default: 10
- Required: no

## Advanced Topics

### Data Collection Without Network Connectivity

Receivers with a POQ can be used without a configured backed. In other words: the `Servers` setting can be left empty. This is useful to collect data on a machine without network connectivity, such as in a DMZ. The collected data can then be transferred to a machine with network connectivity simply by copying the POQ files.

### **Recommendations** DMZ machine:

- Configure the receiver's settings **Name**, **Type**, and **Protocol** to match the settings on the machine you later plan to transfer the POQ files to.
- Once sufficient data has been collected, stop uberAgent and copy the POQ files off the machine.

### Machine with network connectivity:

- Stop uberAgent.
- Copy the POQ files from the DMZ machine to the local POQ path.
- Start uberAgent. The agent sends the DMZ machine's data off to its backend.

### **POQ File Data Format**

The internal format of the Persistent Output Queue is an SQLite database that is not protected and can be read by SQLite browsers like [DB Browser for SQLite](#).

## **Event Triggers for Timers**

July 9, 2024

uberAgent timers are configuration items that specify when and how often metrics are collected. Classic uberAgent timers operate on a fixed schedule, collecting data at static time intervals. Event triggers extend classic timers by enabling uberAgent to collect data when a specified event occurs on the endpoint, independent of the time.

Classic timers and event triggers are compatible and can be used together. You can, for example, configure a timer to run a script once when a user has logged on to a new session and continue to run the script periodically for every session on the endpoint. This ensures that information about new sessions is collected quickly after the logon and that information about older sessions is refreshed regularly. This is but one use case for event triggers. Please see below for full-featured examples.

### **Configuration**

#### **Event Trigger Stanza**

The stanza [[EventTrigger](#)] starts a new event trigger configuration block. Please note that every event trigger must be linked to a [[Timer](#)] stanza (see the examples below).

Event triggers are configured using the following configuration settings:

| Setting | Description                                                                                                                                                                                              | Valid Values                                                                   | Required |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|----------|
| Name    | Specifies the name of an event trigger. This name must be linked in the <a href="#">[Timer]</a> configuration.                                                                                           | Any                                                                            | Yes      |
| Type    | The type of event that triggers the timer. This configuration option may be used more than once per <a href="#">[EventTrigger]</a> stanza if the timer should be triggered by multiple different events. | Any event type from the list below.<br>Example:<br><a href="#">UserLogon</a> . | Yes      |
| Query   | The query rule to limit trigger evaluation using uAQL.                                                                                                                                                   | Please refer to the <a href="#">uAQL documentation</a> .                       | No       |

## Event Types

The following table lists the event types that can be used with the [Type](#) field of the [\[EventTrigger\]](#) stanza:

| Event Type                   | Description                                                                                                                                                          | Platform |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| UserLogon                    | This event type is triggered shortly after a user logs on to the endpoint (on average, after half the duration of the <a href="#">SessionDetail</a> timer interval). | Windows  |
| SessionConnectionStateChange | This event type is triggered each time a user's session state changes.                                                                                               | Windows  |

| Event Type     | Description                                                                     | Platform |
|----------------|---------------------------------------------------------------------------------|----------|
| SessionRoaming | This event type is triggered each time a session is roamed to another endpoint. | Windows  |

## Supported Metrics

Event Triggers for timers support the following metrics:

- UserTags
- CitrixSessionConfig
- Script

## Examples

### Example 1: Configuration With Metric UserTags

In this example, the metric `UserTags` is collected through a standard timer run at a specific interval. Using the standard timer configuration, uberAgent collects the metric `UserTags` for all users logged on to the endpoint at the execution time. Since this metric supports the usage of event triggers, uberAgent can collect this metric upon the occurrence of a specified event for a single user instead of all logged-in users. This example shows that the metric `UserTags` is collected every 10000 ms and when a `UserLogon` event occurs.

```

1 [Timer platform=Windows]
2 Name = Determine user tags
3 Comment = Determine user tags
4 Interval = 10000
5 UA metric = UserTags
6 EventTrigger = TriggerUserTags
7
8 [EventTrigger platform=Windows]
9 Name = TriggerUserTags
10 Type = UserLogon

```

Please find more examples of configuring User & Host Tags [here](#).

### Example 2: Configuration With Metric CitrixSessionConfig

This example shows a standard timer to collect the metric `CitrixSessionConfig`. To collect data for a single user that logs on, disconnects, or continues the session on another endpoint, all event

types need to be configured within the [EventTrigger] stanza. The event trigger in this example is limited to Citrix sessions only by using the uAQL query `BrokerType == "Citrix"`. Using this limitation ensures that the data collection is only started for Citrix remoting sessions.

```

1 [Timer platform=Windows]
2 Name = Citrix session configuration details
3 Comment = Collect Citrix HDX metrics
4 Interval = 900000
5 UA metric = CitrixSessionConfig
6 EventTrigger = TriggerCitrixSessionConfig
7
8 [EventTrigger platform=Windows]
9 Name = TriggerCitrixSessionConfig
10 Type = UserLogon
11 Type = SessionConnectionStateChange
12 Type = SessionRoaming
13 Query = BrokerType == "Citrix"

```

### Example 3: Configuration With a Custom Script

This example describes a standard timer that executes a custom script at a defined interval. This timer can also be enriched with an event trigger so that the script is started on the occurrence of a particular event. In this configuration example, the script is executed in the script context `UserSessionAsUser`. Therefore, uberAgent executes this script additionally for a user that logs on and collects data only for this user.

```

1 [Timer platform=Windows]
2 Name = CustomScriptTrigger
3 Comment = Executes a custom script
4 Interval = 10000
5 Script = powershell.exe -executionpolicy bypass -file "C:\
 Program Files\vast limits\uberAgent\scripts\test-script.ps1"
6 ScriptContext = UserSessionAsUser
7 EventTrigger = TriggerCustomScript
8
9 [EventTrigger platform=Windows]
10 Name = TriggerCustomScript
11 Type = UserLogon

```

### uAQL Properties for Event Triggers

Event Triggers can be limited in evaluation using uAQL. The following table shows the options that are available for a query.



## UserLogon, SessionConnectionStateChange and SessionRoaming

The following properties are available if one of the listed events is triggered.

---

| Property name                           | uAQL Data Type | Description                                                                                                                                                                           |
|-----------------------------------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>SessionId</code>                  | Integer        | The session id of the associated user.                                                                                                                                                |
| <code>BrokerType</code>                 | String         | The broker type. ( <a href="#">Citrix</a> or <a href="#">Microsoft</a> or <a href="#">VMware</a> or <a href="#">NutanixFrame</a> or <a href="#">Unknown</a> or <a href="#">None</a> ) |
| <code>Current.ConnectionStateId</code>  | Integer        | The system's connection state id. This value is from <a href="#">WTS_CONNECTSTATE_CLASS</a> .                                                                                         |
| <code>Current.ClientName</code>         | String         | Computername of the remoting client.                                                                                                                                                  |
| <code>Current.ClientIp</code>           | String         | IP address of the remoting client.                                                                                                                                                    |
| <code>Previous.ConnectionStateId</code> | Integer        | Previous system's connection state id. This value is from <a href="#">WTS_CONNECTSTATE_CLASS</a> .                                                                                    |
| <code>Previous.ClientName</code>        | String         | Previous computer name of the remoting client.                                                                                                                                        |
| <code>Previous.ClientIp</code>          | String         | Previous IP address of the remoting client.                                                                                                                                           |

---

## Troubleshooting

July 9, 2024

The information in this section helps you troubleshoot uberAgent deployments.

## Creating an uberAgent Support Bundle

August 1, 2024

It may happen that the uberAgent support team asks you to create an uberAgent support bundle. A support bundle is a collection of log files and registry items which helps the support team troubleshoot your case. For Windows there is a PowerShell module available which does the work for you. On macOS we provide a convenient shell script. Learn below how to use it.

## Requirements

### Windows

- At least Windows 7 or Windows Server 2008 R2
- PowerShell version 5 or above
- Administrative permissions
  - Needed to collect process owners of all running uberAgent processes
- The script execution policy must be set to either `RemoteSigned` or `Unrestricted`. Check the script execution policy setting by executing `Get-ExecutionPolicy`. If the policy is not set to one of the two required values, run PowerShell as an administrator and execute `Set-ExecutionPolicy RemoteSigned -Scope CurrentUser -Confirm`

### macOS

- At least macOS Catalina
- Z shell (Zsh)
- Administrative permissions

## Download & Installation

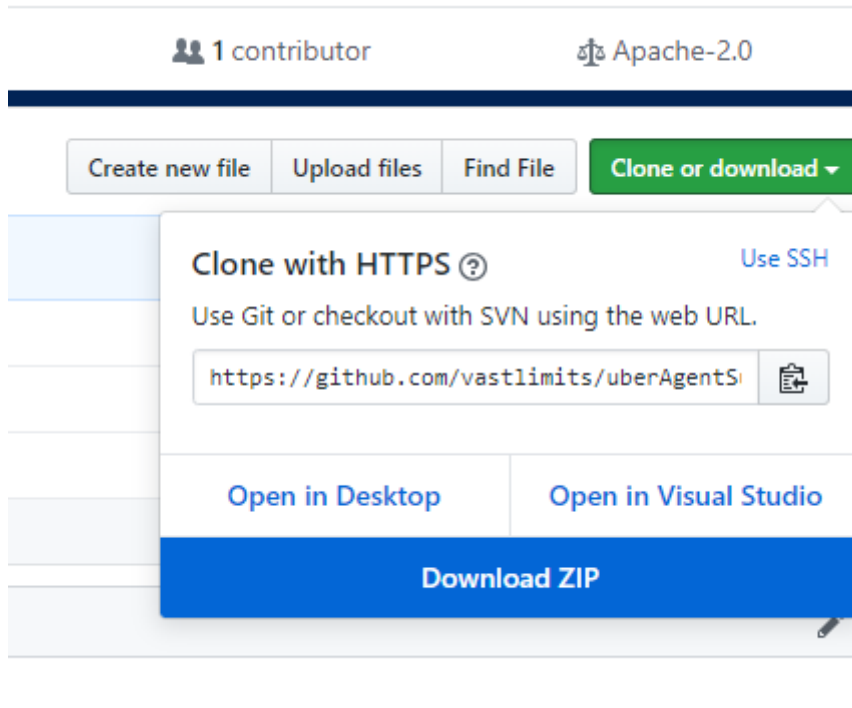
### Windows

**Via PowerShellGet** The uberAgent support module is available on the [PowerShell Gallery](#) and can be installed using the PowerShellGet module.

- Open PowerShell and run `Install-Module uberAgentSupport`
- If you see an error like “*The term ‘Install-Module’ is not recognized as the name...*” install [PowerShellGet](#) or update to at least PowerShell version 5.0.
- To update to the latest module version use `Update-Module uberAgentSupport`

## Manually

- Download the module from [GitHub](#) as a zip file and unzip it somewhere



- Run `Import-Module path-to-module\uberAgentSupport.psd1`
- To update to the latest module version use `Import-Module path-to-module\uberAgentSupport.psd1 -Force` when importing

## macOS

- Download the bundle from [GitHub](#) as a zip file and unzip it somewhere
- Grant execute permissions for the script.
  - `chmod +x path-to-folder/uberAgentSupport-macOS/uberAgentSupport.zsh`

## Usage

### Windows

Open an elevated PowerShell and run `New-uASupportBundle`. No parameters required. A zip file will be placed on your desktop.

## macOS

Open a Terminal and run `sudo path-to-folder/uberAgentSupport-macOS/uberAgentSupport.zsh`. No parameters required. A zip file will be placed on your desktop.

## Deinstallation

### Windows

To completely remove the module from your system run

```
1 $Module = Get-Module uberAgentSupport
2 Remove-Module $Module.Name
3 Remove-Item $Module.ModuleBase -Recurse -Force
```

## macOS

Just delete the downloaded zip file, extracted folders, and files created on your desktop.

## Log Files

July 9, 2024

Things do not always work the way they should. When that happens, uberAgent does not keep you in the dark. Its log files show you exactly what is going on.

### Agent Log

#### Explanation

This is the log file of uberAgent's main component, the system service/daemon.

#### Location

**Windows** The agent log file `uberAgent.log` is stored in the SYSTEM account's `Temp` directory, which typically resolves to `C:\Windows\Temp`.

**macOS** The default location for the `uberAgent.log` file is `/Library/Logs/uberAgent`.

**Note:** Starting with uberAgent version 6.2 this directory will be owned by root with permissions 700. As a consequence Console.app won't be able to access the log files if it runs as a normal user. If you need to use Console.app to view uberAgent logs in this directory you can either change the permissions or start the app as root from terminal with this command: `sudo /System/Applications/Utilities/Console.app/Contents/MacOS/Console`.

## Agent Configuration Log

### Explanation

This is the log file of the system service/daemon's configuration.

### Location

**Windows** The configuration log file `uberAgentConfiguration.log` is stored in the SYSTEM account's `Temp` directory, which typically resolves to `C:\Windows\Temp`.

**macOS** The default location for the `uberAgentConfiguration.log` file is `/Library/Logs/uberAgent`.

## In-Session Helper Log

### Explanation

This is the log file of uberAgent's in-session helper component which is used for collecting information from within user sessions.

### Location

**Windows** The in-session helper log file `uAInSessionHelper.log` is stored in the SYSTEM account's `Temp` directory, which typically resolves to `C:\Windows\Temp`.

**macOS** The default location for the `uAInSessionHelper.log` file is `~/Library/Logs/uberAgent`.

## Chrome/Edge/Firefox Browser Extension In-Session Helper Log

### Explanation

This is the log file of uberAgent's in-session helper instances that are acting as communication gateways between the agent and the Chrome and Firefox browser extensions.

### Location

**Windows** The Chrome/Firefox extension in-session helper log file `uAInSessionHelper.log` is stored in the user account's `Temp` directory, which typically resolves to `C:\Users\USERNAME\AppData\Local\Temp`.

**macOS** The default location for the `uAInSessionHelper.log` file is `~/Library/Logs/uberAgent`.

## IE Browser Add-on Log

### Explanation

This is the log file of uberAgent's Internet Explorer add-on.

### Location

The IE add-on's log file `uberAgentIEExtension.log` is stored in the user account's low-integrity `Temp` directory, which typically resolves to `C:\Users\USERNAME\AppData\Local\Temp\Low`.

If Enhanced Protection Mode is enabled and OS is Windows 8 (or newer), the IE add-on's log file is stored in `C:\Users\USERNAME\AppData\Local\Packages\windows_ie_ac_001\AC\Temp`. For Windows 7 the log files' location is the same as described in the previous paragraph.

## Sandbox Log

### Explanation

This is the log file of uberAgent's XPC Service that wraps potentially unsafe API calls.

## Location

**macOS** The default location for the `uberAgentSandbox.log` file is `/Library/Logs/uberAgent`.

## More Information

### Enabling Debug Mode

Unless debug mode is enabled uberAgent logs only important events like errors. To enable debug mode make sure the following settings are present in the [configuration](#):

```
1 [Miscellaneous]
2 debugMode = true
```

### Activating Trace Logging

Trace logging is a very detailed log level that can be enabled to facilitate troubleshooting of specific agent components. We recommend only enabling trace logging temporarily.

To enable trace logging for an agent component, add the component's name to the `TraceLogFilterExpression` regex of the `ConfigFlags` setting, e.g.:

```
1 ConfigFlags = TraceLogFilterExpression:REGEX
```

The following table lists examples for `REGEX`:

---

| TraceLogFilterExpression regex                | Description                                                                                              |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------|
| <code>.Dns.</code>                            | Logs additional information for DNS queries.                                                             |
| <code>.POQ create new file.</code>            | Logs additional information if a new persistent output queue file was created.                           |
| <code>.Event POQ/queue send.</code>           | Logs additional information if data was sent to the backend.                                             |
| <code>.Event POQ increase error count.</code> | Logs additional information if illformed data was sent to the backend and the error count was increased. |
| <code>.Event POQ remove.</code>               | Logs additional information if events were removed from the persistent output queue.                     |
| <code>.Event POQ store.</code>                | Logs additional information if events were stored in the persistent output queue.                        |

| TraceLogFilterExpression regex | Description                                                                                                                      |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <i>.Event queue store.</i>     | Logs additional information if events were stored in an in-memory queue.                                                         |
| <i>.Event POQ read.</i>        | Logs additional information if events were read from the persistent output queue.                                                |
| <i>.Performance counter.</i>   | Logs additional information for mapping performance counter names (english to localized and vice versa) and determination times. |
| <i>.Locking.</i>               | Logs additional information if internal locking mechanism for lists took too long.                                               |

### File Size and Log Rotation

When the size of the log file grows to 10 MB uberAgent archives it. This is done by appending the current timestamp to the filename and starting a new empty log file. uberAgent keeps the four newest archive files. When four archive files are present and a fifth file is archived the oldest archive file is deleted. This log rotation mechanism guarantees that the total log file size never exceeds 50 MB.

The number of log files to keep around can be changed via the [configuration](#) parameter `LogFileCount`.

### Log Format

Log file entries always have the same structure, explained in the following table:

| Timestamp                            | Severity                                   | Domain                                 | Thread Owner                                                                                  | Thread ID                                    | Source                                                          | Message                     |
|--------------------------------------|--------------------------------------------|----------------------------------------|-----------------------------------------------------------------------------------------------|----------------------------------------------|-----------------------------------------------------------------|-----------------------------|
| Timestamp in the machine's time zone | Possible entries: DEBUG, INFO, WARN, ERROR | The computer's Active Directory domain | <b>Windows:</b> the <i>name</i> of the computer account<br><b>macOS:</b> the <i>user root</i> | The ID of the thread that logged the message | Message source. For example LicenseCheck or Receiver-Statistics | Actual message to be logged |

Here is an example:



```
1 2018-10-04 11:19:51.076 +0100,INFO ,VASTLIMITS,PC1$,4432,
 ReceiverStatistics,Splunk; localhost:19500 - Events in queue: 11961,
 queue size: 3073.1 KB, sent: 0, added to queue: 361, rejected from
 queue: 0
2
3 Timestamp = 2018-10-04 11:19:51.076 +0100
4 Severity = INFO
5 Domain = VASTLIMITS
6 Machine = PC1
7 Thread ID = 4432
8 Source = ReceiverStatistics
9 Message = Splunk; localhost:19500 - Events in queue: 11961, queue
 size: 3073.1 KB, sent: 0, added to queue: 361, rejected from queue:
 0
```

### Notepad++ Syntax Highlighter

Even though we take great care to optimize the log for readability it is sometimes hard to find the needle in the haystack. That is why we created an [uberAgent log syntax highlighter for Notepad++](#). It highlights the key information, making it easier to find what you are searching for.

### Splunk It

As text-based log files, uberAgent's logs are ideal candidates for processing by Splunk. We have built the [uberAgent Log Collector](#) specifically for that purpose.

## uberAgent Log Collector Splunk App

July 9, 2024

The [endpoint agent's log files](#) are the primary source for agent health and status information. The log files are kept locally on the endpoint, but they can easily be forwarded to the backend with the uberAgent Log Collector Splunk App.

Please refer to the [log collector's documentation for details](#).

## uberAgent Browser Extensions

July 25, 2024

uberAgent's browser web app performance functionality requires a browser extension to be installed. This article lists possible troubleshooting steps.

## Dashboards That Do Not Require Browser Extensions

uberAgent monitors Chrome and Internet Explorer performance on a process level. The collected data is available in the dashboards *Browser Performance: Chrome* and *Browser Performance: Internet Explorer*, respectively. You do not need any extensions for this to work.

However, if you want data about websites, like page load time, extensions are needed. Website data is visualized in the dashboards *Browser Web App Performance* and *Browser Web App Usage* for all supported browsers. Grouping and filtering by browser type or browser version are possible, of course.

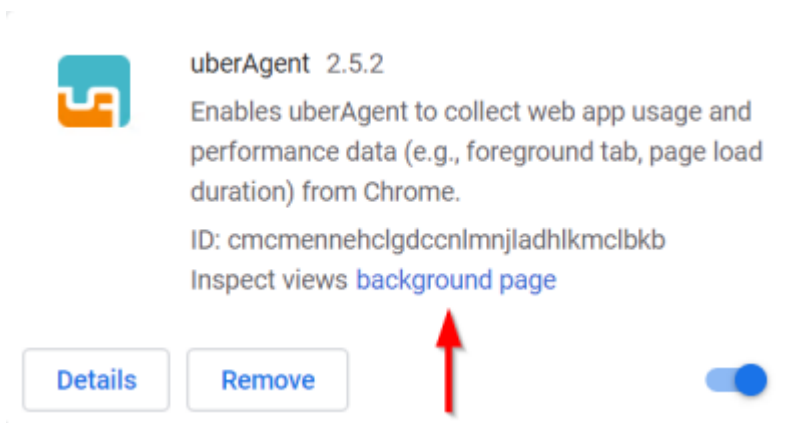
## Troubleshooting the Chrome Extension

1. Reread the [Chrome extension installation guide](#) carefully. Take notice of the [relevant configuration settings](#) section.
2. Check the [uberAgent service log](#) as well as the [Chrome extension logs](#) for any errors.
3. uberAgent is using native messaging for communication with the extension. Make sure that the extension is not on the [native messaging denylist](#).
  - a) If the denylist is enforced in the company, adding `com.vastlimits.uainsessionhelper` to the [allowlist](#) overrides the denylist.
4. Check if the native messaging host is configured correctly:
  - a) On an x86 machine running Windows, the following registry item is created by the uberAgent service and must be present.  
Key: `HKEY_LOCAL_MACHINE\SOFTWARE\Google\Chrome\NativeMessagingHosts\com.vastlimits.uainsessionhelper`  
Value: (Default)  
Data: `C:\Program Files\vast limits\uberAgent\uAInSessionHelperChrome.json`
  - b) On an x64 machine running Windows, the following registry item is created by the uberAgent service and must be present.  
Key: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Google\Chrome\NativeMessagingHosts\com.vastlimits.uainsessionhelper`  
Value: (Default)  
Data: `C:\Program Files\vast limits\uberAgent\uAInSessionHelperChrome.json`

- c) On macOS, a file called `com.vastlimits.uainsessionhelper.json` is created and must be present in the directory `/Library/Google/Chrome/NativeMessagingHosts/`.

5. Enable console logging

- a) Navigate to: `chrome://extensions/`
- b) Enable developer mode
- c) Click the extension's background page link



- a) The developer tools appear
- b) In the dev tools console enter:

```
1 logSeverity = LogSeverities.Info
2 logContext = LogContexts.All
```

6. The extension now logs events to the dev tools console

### Troubleshooting the Firefox Extension

- 1. Reread the [Firefox extension installation guide](#) carefully.
- 2. Check the [uberAgent service log](#) as well as the [Firefox extension logs](#) for any errors.
- 3. Check if the native messaging host is configured correctly:
  - a) On an x86 machine running Windows, the following registry item is created by the uberAgent service and must be present.  
Key: `HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\NativeMessagingHosts\com.vastlimits.uainsessionhelper`  
Value: (Default)  
Data: `C:\Program Files\vast limits\uberAgent\uAInSessionHelperFirefox.json`

- b) On an x64 machine running Windows, the following registry items are created by the uberAgent service and must be present.
  - c) Key: `HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\NativeMessagingHosts\com.vastlimits.uainsessionhelper`  
Value: (Default)  
Data: `C:\Program Files\vast limits\uberAgent\uAInSessionHelperFirefox.json`
  - d) Key: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Mozilla\NativeMessagingHosts\com.vastlimits.uainsessionhelper`  
Value: (Default)  
Data: `C:\Program Files\vast limits\uberAgent\uAInSessionHelperFirefox.json`
  - e) On macOS, a file called `com.vastlimits.uainsessionhelper.json` is created and must be present in the directory `/Library/Application Support/Mozilla/NativeMessagingHosts/`.
4. Enable console logging
- a) Navigate to: `about:debugging#/runtime/this-firefox`
  - b) Identify the uberAgent extension and click **Inspect**
  - c) The developer tools appear
  - d) In the dev tools console enter:

```
1 logSeverity = LogSeverities.Info
2 logContext = LogContexts.All
```

5. The extension now logs events to the dev tools console

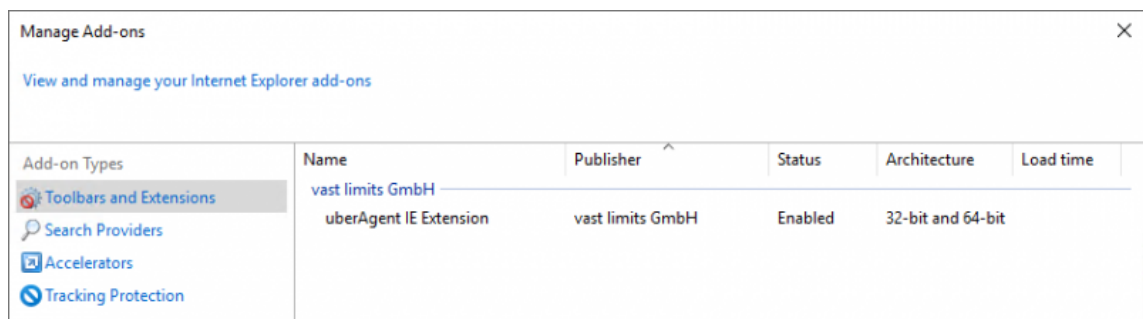
## Troubleshooting the Internet Explorer Extension

1. Reread the [Internet Explorer installation](#) guide carefully. Take notice of the [relevant configuration settings](#) section.
2. Check the [uberAgent service log](#) as well as the [IE add-on logs](#) for any errors.
3. Check if the IE add-on is registered correctly
  - a) On an x86 machine, the following registry items must be present.
  - b) Key: `HKEY_CLASSES_ROOT\CLSID\{ 82004312-5B53-46F1-B179-4FCE28048E6F } \InProcServer32`  
Value: (Default)

Data: C:\Program Files\vast limits\uberAgent\uaIEExtension32.dll

- c) Key: HKEY\_CLASSES\_ROOT\CLSID\{ 82004312-5B53-46F1-B179-4FCE28048E6F } \InProcServer32  
Value: ThreadingModel  
Data: Apartment
- d) On an x64 machine, the following registry items must be present.
- e) Key: HKEY\_CLASSES\_ROOT\CLSID\{ 82004312-5B53-46F1-B179-4FCE28048E6F } \InProcServer32  
Value: (Default)  
Data: C:\Program Files\vast limits\uberAgent\uaIEExtension64.dll
- f) Key: HKEY\_CLASSES\_ROOT\CLSID\{ 82004312-5B53-46F1-B179-4FCE28048E6F } \InProcServer32  
Value: ThreadingModel  
Data: Apartment
- g) Key: HKEY\_CLASSES\_ROOT\WOW6432Node\CLSID\{ 82004312-5B53-46F1-B179-4FCE28048E6F } \InProcServer32  
Value: (Default)  
Data: C:\Program Files\vast limits\uberAgent\uaIEExtension32.dll
- h) Key: HKEY\_CLASSES\_ROOT\WOW6432Node\CLSID\{ 82004312-5B53-46F1-B179-4FCE28048E6F } \InProcServer32  
Value: ThreadingModel  
Data: Apartment

4. Check if the IE add-on is enabled in *Settings > Manage add-ons*



5. uberAgent identifies IE processes by the full path to the EXE file. For this, the path must correspond to one of the following paths entered in the registry.

- a) Key: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\IEXPLORE.EXE`  
Value: (Default)  
Data (example): `C:\Program Files\Internet Explorer\IEXPLORE.EXE`
- b) Key: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main`  
Value: `x86AppPath`  
Data (example for a x86 machine): `C:\Program Files\Internet Explorer\IEXPLORE.EXE`  
Data (example for a x64 machine): `C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE`

## Troubleshooting Specific Fields

Please see the following articles for additional information on specific fields:

- [Reasons For Empty SessionFgBrowserActiveTabHost Field](#)

## Creating an uberAgent Performance Recording

July 25, 2024

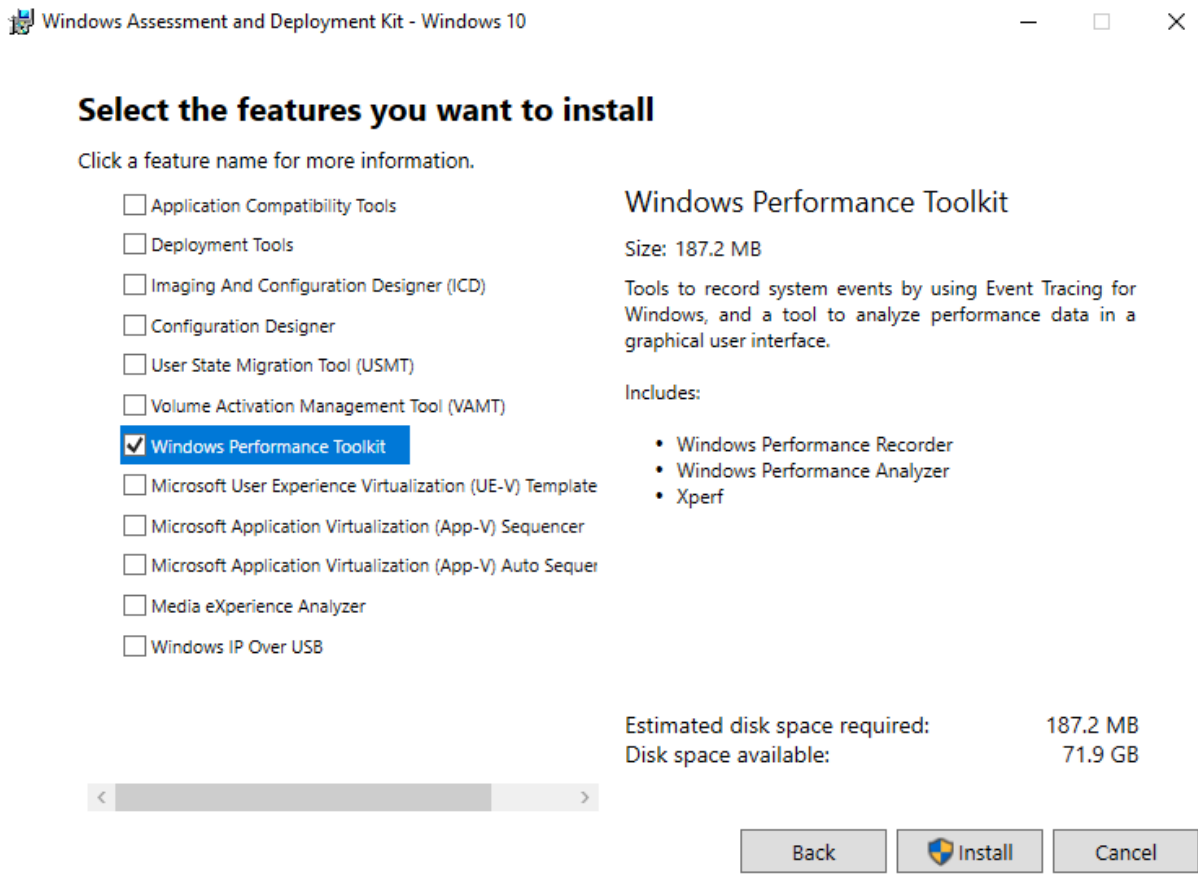
It may happen that the uberAgent support team asks you to create an uberAgent performance recording. A performance recording is a detailed analysis of the processes running on a machine. The recording is created with the Windows Performance Recorder.

### Downloading and Installing the Windows Performance Recorder

The Windows Performance Recorder is part of the Windows Assessment and Deployment Kit (Windows ADK).

Download the appropriate version of the ADK for your Windows operating system from [Microsoft](#).

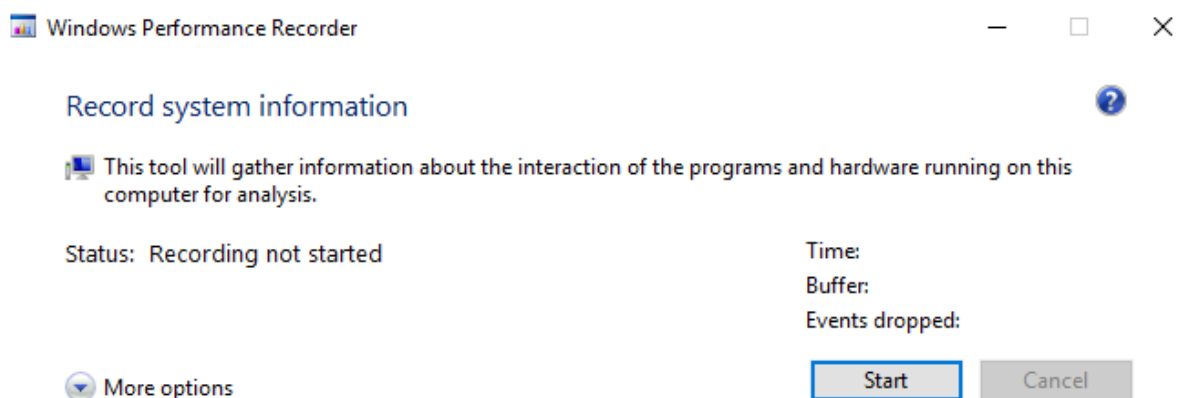
Run the setup. When asked for features to install, select **Windows Performance Toolkit**. The other features may be deselected.



## Creating The Recording

After the installation has finished, start the **Windows Performance Recorder** from the start menu.

Click on **Start** to start the recording and let the recording run for five minutes, if not told otherwise by uberAgent support.



When the recording has finished, save the recording on disk and send the generated ETL file to the

uberAgent support.

## uberAgent's Driver Safety Net Feature

July 9, 2024

To collect high-quality network and process metrics, uberAgent relies on kernel-mode drivers that are started when the computer boots. While we invested a lot of time and energy to make our drivers as reliable as humanly possible, a driver is just a piece of software, and even software developed to the highest standards cannot be tested in all of the millions of possible combinations of hardware and software. One of the worst possible situations is a driver that crashes during the machine startup phase, more specifically during *every* machine startup. In such a bluescreen loop situation it can be difficult to restore the operating system to working order.

uberAgent's drivers come with **Driver Safety Net**, a unique feature that prevents bluescreen loops: in the unlikely event of a crash in one of uberAgent's drivers, the driver disables itself.

### How Driver Safety Net Detects Crashes

In a nutshell, Driver Safety Net works as follows: uberAgent's drivers write their current states to a location in the registry. The information from these registry values is used during the driver initialization phase. When a driver determines that its last start was unsuccessful it increments a failure count value. Once that count reaches a threshold of 3 (three), the driver disables itself.

### False Positives

There are events that "look and feel" like a blue screen but have very different root causes, for example, power outages or hardware failures. If multiple such events occur in a short timeframe, uberAgent's Driver Safety Net may be triggered, even though no driver crashed.

### How to Re-Enable uberAgent's Drivers After Driver Safety Net Triggered

Once Driver Safety Net triggers, uberAgent's drivers remain disabled until re-enabled with the simple procedure outlined below. This is to ensure maximum system stability and reliability.

To re-enable uberAgent's drivers remove the following registry values and restart the [uberAgent](#) service:

- `DrvFailureCount`



- `DrvStartupFinished`
- `DrvShutdownFinished`
- `DrvLastStart`

Depending on the driver that triggered Driver Safety Net, the above registry values are located in one of the following two registry paths:

- **Process** driver: `HKLM\SYSTEM\CurrentControlSet\Services\UberAgentDrv`
- **Network** driver: `HKLM\SYSTEM\CurrentControlSet\Services\uberAgentNetMon`

## Knowledge Base

July 9, 2024

Welcome to the uberAgent knowledge base. Here you'll find best practices, explanations as well as tips & tricks.

## Architecture

July 9, 2024

This section contains knowledge base articles about the architecture.

## Description of the `uAInSessionHelper/uberAgentHelper` Process

July 9, 2024

Some information is only available to processes running in a user's session, not to services running in session 0 respectively in the context of the system. In order to be able to collect such data, too, uberAgent makes use of the helper process `uAInSessionHelper.exe` on Windows and `uberAgentHelper` on macOS.

The helper is a lightweight process that collects specific data and sends it to the main service.

## The Helper Process

### Windows

There is one `uAgentHelper.exe` process running permanently for every user session in the local SYSTEM context, e.g. to collect GPU usage information. When collecting web app metrics from Chrome, Edge, or Firefox, a dedicated `uAgentHelper.exe` instance is started (with user privileges) by each browser that has uberAgent's extension installed.

### macOS

There is one `uberAgentHelper` process running permanently for every user session with user privileges. When collecting web app metrics from Chrome, Edge, or Firefox, a dedicated `uberAgentHelper` instance is started (with user privileges) by each browser that has uberAgent's extension installed.

## Helper Metrics

The helper process is utilized to collect the following metrics:

### Windows

- Information about a **UWP app**
- **Internet Explorer performance** data  
Metric: `BrowserPerformanceIE`
- UX metrics for SaaS and web apps in **Internet Explorer**  
Metric: `BrowserPerformanceIE`
- UX metrics for SaaS and web apps in **Chrome**  
Metric: `BrowserPerformanceChrome`
- UX metrics for SaaS and web apps in **Firefox**  
Metric: `BrowserPerformanceFirefox`
- UX metrics for SaaS and web apps in **Edge**  
Metric: `BrowserPerformanceEdge`
- **GPU performance** data  
Metric: `GpuUsage`

## macOS

- **Session Detail** data  
Metric: `SessionDetail`
- UX metrics for SaaS and web apps in **Chrome**  
Metric: `BrowserPerformanceChrome`
- UX metrics for SaaS and web apps in **Firefox**  
Metric: `BrowserPerformanceFirefox`
- UX metrics for SaaS and web apps in **Edge**  
Metric: `BrowserPerformanceEdge`

## Troubleshooting the Helper

Helper log locations are documented [here](#).

Please review the contents of these log files when you suspect things are not working correctly.

## Common Errors

### Class Not Registered (Windows)

You may see messages like the following in uAlnSessionHelper's log file:

```
1 2015-09-04 22:16:48.140 +0200, ERROR, HK, XA1$, 1856, IE Performance,
 Action 2 failed with: -2147221164
2 2015-09-04 22:16:48.142 +0200, ERROR, HK, XA1$, 1856,
 GetBrowserPerformanceIE, Failed (2) with: Class not registered
```

The root cause for these errors is that uberAgent can only determine IE performance per website if IE is run in desktop mode, i.e. not as a Citrix XenApp published application. If IE is run as a published application certain classes required by uAlnSessionHelper are not available, thus the messages.

## Name or Version may be Inconsistent Between App Inventory & Usage

July 9, 2024

uberAgent collects information about applications on multiple levels:

- Which applications are installed (app **inventory**)
- Which applications are running (app **usage**)

- Which applications are being worked with (**foreground** app)

Not all of that information is available in one data source. In fact, uberAgent has to query quite disparate sources to collect its extensive application information. That can lead to inconsistencies, specifically between the app inventory and all the other application source types.

## Root Cause

The root of the problem is that Windows has no generic concept of applications. Windows knows and cares about processes, threads and a good number of other things, but APIs for applications? Nonexistent.

As a consequence, there are no application naming and versioning standards for software vendors. This may lead to the situation that vendors use one name/version in one place and a different name/version in another - for the same application.

## uberAgent

uberAgent has sophisticated algorithms to deal with the situation and determine the best possible application names and versions. However, there may be inconsistencies between the source types `ApplicationInventory` and other application source types, e.g., `ApplicationUsage` or `ProcessDetail`.

The reason for these inconsistencies lies in the fact that the data for the `ApplicationInventory` sourcetype is based on the `Uninstall` registry key so that it matches what Windows displays in *Apps & features*.

All other source types' application info, on the other hand, is based on an algorithm that determines application properties depending on the application type (Win32, UWP, App-V, Java, ...). Naturally, this algorithm cannot use the `Uninstall` registry key.

For that reason, inconsistencies may exist and mapping between the `ApplicationInventory` and other application source types is not recommended.

## Using uberAgent With a Proxy

July 9, 2024

uberAgent uses libcurl to send data when using HTTP or HTTPS as protocol. libcurl ignores common per-system or per-user proxy settings. Customers who want to use uberAgent with a proxy, must configure the following two system environment variables:

- [http\\_proxy](#)
- [https\\_proxy](#)

Customers who have a proxy configured but don't want to route the traffic from uberAgent to Splunk through it, must set the environment variable `no_proxy` to the Splunk server name.

More information is available in the [libcurl documentation](#).

## uberAgent vs. Splunk Template for XenDesktop 7

July 9, 2024

Both uberAgent and the Splunk Template for XenDesktop 7 can be used to monitor a Citrix XenDesktop/XenApp environment. This article highlights the key differences between both products.

### Scope

The Splunk Template for XenDesktop 7 monitors part of the XenDesktop infrastructure (e.g. license server) and collects performance data per session and per machine on the XenApp session hosts.

uberAgent monitors user experience and application performance of Windows machines.

### Support and Maintenance

Splunk does not provide support for its App for Citrix XenDesktop. New versions with bugfixes and additional features are rare.

uberAgent is fully supported. New versions are being released every 2-3 months. Fixes for critical bugs are made available immediately.

### Footprint

The Splunk Template for XenDesktop 7 collects data via PowerShell scripts and WMI.

uberAgent, on the other hand, is written in C++ and accesses native APIs (no WMI). Therefore uberAgent has a much smaller footprint and consumes fewer resources on the monitored system.

### Data volume

The Splunk Template for XenDesktop 7 generates a higher data volume per XenApp server than uberAgent.

## Data collection

The Splunk Template for XenDesktop 7 collects the following data:

- High-level overviews supporting multiple farms
- Alerting
- ICA latency reporting
- User experience investigation
- User logon time details
- Performance visualization and monitoring
- Application usage
- Critical service monitoring

uberAgent collects the data about the following:

- Logon duration
- Computer startup duration
- Machine performance
- Session performance
- Process performance
- Application performance
- Application usage
- Application versions
- Process startup duration
- GPU usage
- Browser performance per website

Here is the full [list of metrics collected by uberAgent](#).

## Configuration

July 29, 2024

This section contains knowledge base articles about the configuration.

## Metric Dependencies

October 18, 2024

### Use one process detail metric only

You can either use `ProcessDetailFull` OR `ProcessDetailTop5`, not both. If you have accidentally configured both, uberAgent uses `ProcessDetailTop5`.

There is no entry in the log for this case.

### Use a process detail metric in one timer only

`ProcessDetailTop5` or `ProcessDetailFull` can be configured in one timer only.

If you have it configured in two or more timers, you get the following warning in the `uberAgentConfiguration.log`:

```
1 CheckForUnconfiguredMetrics,Metric(s) ProcessDetailFull can only be
 configured once.
```

### Use session and process detail metrics in the same timer only

`SessionDetail` and `ProcessDetailTop5` OR `ProcessDetailFull` must be configured in the same timer. If you have accidentally configured these metrics in different timers, you get the following warning in the `uberAgentConfiguration.log`:

```
1 CheckSessionAndProcessInSameTimer,Metric(s) SessionDetail and (
 ProcessDetailFull or ProcessDetailTop5) should only be configured in
 the same timer.
```

### Session details require logon details

If you enable `SessionDetail`, you must also enable the metric `LogonDetail`.

## Custom Queries

July 9, 2024

This section contains knowledge base articles about custom queries.

## Walkthrough: Building a Splunk Search

July 25, 2024

The following walkthroughs illustrate how to build a Splunk search from scratch.

**Scenario:** we want to identify users who launch a specific executable more often than *n* times in a given time range.

### Splunk SPL Search

Let's build the Splunk SPL search step by step.

#### Step 1

We start with all events from uberAgent's index.

**Note:** to facilitate changing the index name used by uberAgent, all our dashboards make use of the `uberAgent_index` macro which contains the actual index name. The macro is defined in `macros.conf` of the uberAgent searchhead app.

```
1 index=`uberAgent_index`
```

#### Step 2

We filter for the process startup sourcetype which contains one event per started process.

**Note:** The documentation of uberAgent's sourcetypes and fields can be found [here](#).

```
1 index=`uberAgent_index` sourcetype=uberAgent:Process:ProcessStartup
```

#### Step 3

We ignore processes started by SYSTEM, LOCAL SERVICE and NETWORK SERVICE.

**Note:** The pseudo-users `sys`, `lvc` and `nvc` are defined in the lookup table `systemusers.csv` of the uberAgent searchhead app. They are auto-expanded to the proper user names SYSTEM, LOCAL SERVICE and NETWORK SERVICE in uberAgent's data model.

```
1 index=`uberAgent_index` sourcetype=uberAgent:Process:ProcessStartup
 ProcUser!=sys ProcUser!=lvc ProcUser!=nvc
```



**Step 4**

We add a filter for the name of the process we are interested in, `Winword.exe` in this example.

```
1 index=`uberAgent_index` sourcetype=uberAgent:Process:ProcessStartup
 ProcUser!=sys ProcUser!=lvc ProcUser!=nvc ProcName=Winword.exe
```

**Step 5**

We count the number of (start) events per user.

**Note:** The only purpose of adding the field `ProcName` to the `stats` command is to make it part of the results table, too.

```
1 index=`uberAgent_index` sourcetype=uberAgent:Process:ProcessStartup
 ProcUser!=sys ProcUser!=lvc ProcUser!=nvc ProcName=Winword.exe
2 | stats count as Starts by ProcName ProcUser
```

**Step 6**

We only keep users with more than five starts in the results list.

```
1 index=`uberAgent_index` sourcetype=uberAgent:Process:ProcessStartup
 ProcUser!=sys ProcUser!=lvc ProcUser!=nvc ProcName=Winword.exe
2 | stats count as Starts by ProcName ProcUser
3 | where Starts > 5
```

**Step 7**

We rename fields to make them look nicer.

```
1 index=`uberAgent_index` sourcetype=uberAgent:Process:ProcessStartup
 ProcUser!=sys ProcUser!=lvc ProcUser!=nvc ProcName=Winword.exe
2 | stats count as Starts by ProcName ProcUser
3 | where Starts > 5
4 | rename ProcUser as User ProcName as Process
```

**Step 8**

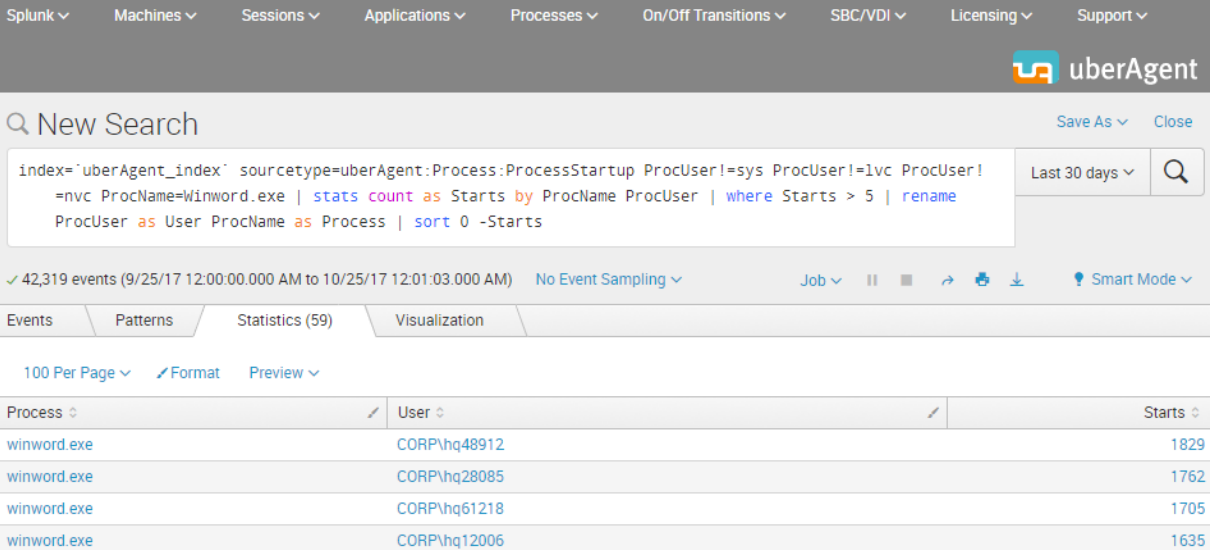
We sort the results so that the user with the highest number of starts is listed first. The `0` in the `sort` command ensures that the output is not truncated after the 10,000th result.

```
1 index=`uberAgent_index` sourcetype=uberAgent:Process:ProcessStartup
 ProcUser!=sys ProcUser!=lvc ProcUser!=nvc ProcName=Winword.exe
```

```
2 | stats count as Starts by ProcName ProcUser
3 | where Starts > 5
4 | rename ProcUser as User ProcName as Process
5 | sort 0 -Starts
```

## The Result

This is what the final Splunk SPL search for users with more than five starts of `Winword.exe` looks like. The screenshot below shows the search being run over the past 30 days. In practice, you would adjust the time range to any relevant time interval.



The screenshot shows the Splunk Search interface with the following search query:

```
index='uberAgent_index' sourcetype=uberAgent:Process:ProcessStartup ProcUser!=sys ProcUser!=lvc ProcUser!
-nvc ProcName=Winword.exe | stats count as Starts by ProcName ProcUser | where Starts > 5 | rename
ProcUser as User ProcName as Process | sort 0 -Starts
```

The search results are displayed in a table with the following columns: Process, User, and Starts.

| Process     | User         | Starts |
|-------------|--------------|--------|
| winword.exe | CORP\hq48912 | 1829   |
| winword.exe | CORP\hq28085 | 1762   |
| winword.exe | CORP\hq61218 | 1705   |
| winword.exe | CORP\hq12006 | 1635   |

## Accelerated Data Model Search

uberAgent comes with an accelerated data model. Searching an accelerated data model is a lot faster than searching the underlying index (by "a lot" we mean at least 50x), but requires a different search syntax based on the `pivot` or `tstats` commands. We are using `pivot` because of the easier syntax compared to `tstats`.

In this second example, we demonstrate how to search for starts of a "modern" UWP app, specifically the weather app that is part of Windows. Most UWP apps cannot be identified by process name - which is simply `backgroundTaskHost.exe`. Luckily uberAgent determines the real app name automatically.

### Step 1

We start with a count of all process starts.

**Note:** The documentation for the Splunk pivot command can be found [here](#).

**Note:** the macro `uA_DM_Process_ProcessStartup` resolves to the name of the data model containing the `Process_ProcessStartup` dataset. We use this technique to facilitate moving datasets between data models.

```
1 | pivot `uA_DM_Process_ProcessStartup` Process_ProcessStartup count(
 Process_ProcessStartup) as Starts
```

## Step 2

We filter for the weather app.

**Note:** An easy way to identify the name of the weather app is to dig around with a search like the following: `index=`uberAgent_index` sourcetype=uberAgent:Process:ProcessStartup AppName=*Weather*`

```
1 | pivot `uA_DM_Process_ProcessStartup` Process_ProcessStartup count(
 Process_ProcessStartup) as Starts
2 filter AppName is "Microsoft.BingWeather"
```

## Step 3

We split by user so that we get a count of process starts per user (renaming the `ProcUser` field to `User` in the process).

```
1 | pivot `uA_DM_Process_ProcessStartup` Process_ProcessStartup count(
 Process_ProcessStartup) as Starts
2 filter AppName is "Microsoft.BingWeather"
3 splitrow ProcUser as User
```

## Step 4

We only keep users with more than five starts in the results list. We also sort the results so that the user with the highest number of starts is listed first. The `0` in the `sort` command ensures that the output is not truncated after the 10,000th result.

```
1 | pivot `uA_DM_Process_ProcessStartup` Process_ProcessStartup count(
 Process_ProcessStartup) as Starts
2 filter AppName is "Microsoft.BingWeather"
3 splitrow ProcUser as User
4 | where Starts > 5
5 | sort 0 -Starts
```

## Step 5

We add the application name as a row to the results table.

```
1 | pivot `uA_DM_Process_ProcessStartup` Process_ProcessStartup count(
2 | Process_ProcessStartup) as Starts latest(AppName) as Application
3 | filter AppName is "Microsoft.BingWeather"
4 | splitrow ProcUser as User
4 | where Starts > 5
5 | sort 0 -Starts
6 | table Application User Starts
```

## The Result

The resulting output is very similar to the first example above: a table with the application, the users and the number of starts that can easily be exported to CSV or otherwise be processed further.

## How to Implement Drilldowns on Custom Dashboards

July 24, 2024

When you create a custom dashboard, Splunk automatically adds a drilldown to the search page. In many cases, that is not what you want. This article describes an easy way to implement custom drill-downs.

### How It Works

1. Add a JavaScript file to your dashboard
2. Implement click event handlers in JavaScript, in which you set the new URL and optionally pass values to the drilldown page
3. Use the passed values in the drilldown page

Let's explain these steps in more detail.

### Add a JavaScript File

To add one or more JavaScript files to your Simple XML dashboard specify the names of the `.js` files in the `form` tag like this:

JavaScript files reside in the `appserver\static` directory of your app.

## Click Event Handlers

In your JavaScript file add click event handlers to those dashboard elements (charts, tables, ...) you want to implement a custom drilldown behavior for.

Please note that the dashboard elements need to have unique IDs in Simple XML for this to work, e.g.:

```
1 <table id="Table_Panel41"></table>
```

The JavaScript could look like this:

```
1 // RequireJS dependency handling
2 require (["splunkjs/mvc",
3 "splunkjs/mvc/simplexml/ready!"], function (mvc)
4 {
5
6 // Set click event handlers
7 var chart21 = mvc.Components.getInstance ("Chart_Panel21");
8 chart21.on ("click", drilldown);
9 var table41 = mvc.Components.getInstance ("Table_Panel41");
10 table41.on ("click:row", drilldown);
11
12 // Define a drilldown function that can be used by multiple click
13 // event handlers
14 function drilldown (event)
15 {
16 // Don't do any further event processing
17 event.preventDefault ();
18
19 // Get token values
20 var earliest = GetToken (mvc, "earliest");
21 var latest = GetToken (mvc, "latest");
22
23 // Build the new URL
24 var drilldownUrl = "single_machine_detail";
25 drilldownUrl += "?earliest=" + encodeURIComponent (earliest);
26 drilldownUrl += "&latest=" + encodeURIComponent (latest);
27 drilldownUrl += "&FilterHostName=" + encodeURIComponent (event.
28 data["click.value"]);
29
30 // Go to the new URL
31 window.location = drilldownUrl;
32 }
33 }
34);
```

## Use the Passed Values on the Drilldown Page

In the example above we are passing the search time range (earliest and latest) to the drilldown page, where it is used automatically.

In addition to time, we pass the variable `FilterHostName`. This variable can be used in the Simple XML drilldown page searches by enclosing it in dollar signs, e.g. `$FilterHostName$`.

If you want to pass a value to an input field instead, prepend the field token's name with "form.". Example: your input field on the drilldown page is defined like this:

Specify the field's value as follows in JavaScript:

```
drilldownUrl += "&form.FilterField="+ encodeURIComponent ("Some field value");
```

## Examples

The technique described here is used extensively on uberAgent's dashboards. Poke around our search head app and you will find many real-world examples.

## How to Report on CPU Seconds & RAM GB Hours per User

July 9, 2024

uberAgent determines all the required data for charging based on usage. If you want to bill your customers depending on how much CPU or RAM their users' sessions consume you basically need the metrics *CPU seconds per user* and *RAM GB hours per user*. The latter can be explained as the number of gigabytes of RAM multiplied by the number of hours.

### Example: RAM GB Hours per User

User A runs one session with an average RAM footprint of 2 GB for 3 hours. User B runs 2 sessions for 5 hours, one with an average RAM footprint of 1 GB and the other with an average RAM footprint of 2 GB. *GB hours* would be:

- **User A:** 2 GB \* 3 hours = 6 GB hours
- **User B:** 1 GB \* 5 hours + 2 GB \* 5 hours = 15 GB hours

## Splunk Search

The following Splunk search will return the total CPU seconds and RAM GB hours per Active Directory user account. It can be run over any time range (= billing period). Please note that due to the nature of the calculation every started hour counts in full, i.e. the resolution is one hour.

```
1 | pivot uberAgent Session_SessionDetail_Users
2 first(SessionUserLower) as User
3 avg(SessionWorkingSetMB) as AvgHourSessionWorkingSetMB
4 sum(SessionCPUTimeS) as SumHourSessionCPUTimeS
5 splitrow
6 _time
7 period hour
8 splitrow
9 SessionGUID
10 | eval AvgHourSessionWorkingSetGB=AvgHourSessionWorkingSetMB/1024
11 | stats
12 count as SessionHours
13 sum(AvgHourSessionWorkingSetGB) as GBHours
14 sum(SumHourSessionCPUTimeS) as CPUSeconds
15 avg(AvgHourSessionWorkingSetGB) as AvgSessionGB
16 by
17 User
18 | eval GBHoursRounded=round(GBHours, 2)
19 | eval CPUSecondsRounded=round(CPUSeconds, 2)
20 | eval AvgSessionGBRounded=round(AvgSessionGB, 2)
21 | fields
22 User
23 SessionHours
24 GBHoursRounded
25 CPUSecondsRounded
26 AvgSessionGBRounded
```

Above search returns these fields per user:

- RAM GB hours
- CPU seconds
- Session hours (sessions \* hours run per session)
- Average memory usage per session

## How it Works

We are searching uberAgent's accelerated data model. That is why we use the `pivot` command.

The search consists of two main parts. First, we determine the average RAM usage per session and hour. Then we summarize the session hours per user.

CPU usage is even easier to calculate because uberAgent already reports it as CPU seconds so that we already have the length of time. We only need to summarize; we do that in two steps because the

search needs to be constructed that way to determine RAM usage.

## Data Collection

July 9, 2024

This section contains knowledge base articles about the data collection.

## Citrix Applications Are Still Displayed with Old Name After Renaming

July 24, 2024

After renaming published applications in Citrix Studio, they still show up with the old name in uberAgent's dashboards.

uberAgent reads information for user's published applications from the registry from the path `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\Session\`.

---

| Registry value | uberAgent field         |
|----------------|-------------------------|
| PublishedName  | SessionPublishedName    |
| AppNames       | SessionPublishedAppsCtx |

---

When you look at a published application with `Get-BrokerApplication` via PowerShell you can identify multiple application name fields.

- ApplicationName
- BrowserName
- Name
- PublishedName

Citrix writes the application's BrowserName to the registry. But, this property does not get altered when changing the application's name through Studio. You can change the BrowserName property with PowerShell: `Get-BrokerApplication -Name SomeName | Set-BrokerApplication -BrowserName NewBrowserName`

After setting the BrowserName correctly, published applications will show up with the new name in uberAgent's dashboards.



## Dashboards Have No Data

July 9, 2024

If you do not see any data on a dashboard please check all of the following.

### uberAgent indexer app

Check the following in *Apps > Manage Apps*:

- Do you have a Splunk app with the name *uberAgent indexer* installed?

### Index uberagent

Check the following in *Settings > Indexes*:

- Do you have an index with the name *uberagent*?
- What is the index's event count?
- How long ago was the latest event recorded?

### Data flow

There are multiple options for sending the data uberAgent collects on the endpoints to the Splunk backend. Make sure one of the following is configured correctly:

- **uberAgent** on endpoint > **TCP port 19500** on Splunk **indexer**
- **uberAgent** on endpoint > Splunk **HTTP Event Collector** on Splunk **indexer**
- **uberAgent** on endpoint > TCP port 19500 on **Universal Forwarder** on endpoint > receiver port 9997 on Splunk **indexer**

The port numbers above are default values that can be changed.

### Index contents

Run the following Splunk search: `index=uberagent*`

- Do you see results from all hosts with uberAgent installed?
- Do you see results from many different source types?

## Endpoints

If data from a specific endpoint is missing check the following on the endpoint:

- Make sure the service [uberAgent](#) is running.
- Check uberAgent's [log file](#) for issues.

## Index permissions

The account you are accessing the uberAgent app with needs read permissions on the uberAgent index(es) or else no data will be returned by the searches. For details please see the article about [multi-tenancy](#).

## Time range

The dashboards display data from the selected time range only. Please make sure the time range selector is set to a period from which you expect events.

## Differences between `SessionPublishedAppsCtx` and `SessionPublishedName`

July 9, 2024

The source type `uberAgent:Session:SessionDetail` contains two fields that appear to have the same purpose: `SessionPublishedAppsCtx` and `SessionPublishedName`.

One might assume, that both contain information about Citrix published applications run by a user. But, there are differences.

- `SessionPublishedAppsCtx`: all published applications run by a user. Applies to Citrix sessions.
- `SessionPublishedName`: name of the published application which was used to create the session. Applies to Citrix and VMware sessions.

## How Application Startup Duration is Measured

July 9, 2024

uberAgent measures the startup duration of every process. This happens fully automatically whenever an application is launched and does not require configuration per application. A high-level overview of this feature can be found [here](#).

### **How Not to Do it**

uberAgent does not monitor application startup duration by waiting for specific windows to show up on the screen. Such an approach would be difficult to implement reliably because applications often display splash screens or other helper windows while starting up in order to reduce perceived launch times. A reliable mechanism would have to ignore those and wait for the main application window.

Additionally, even when the main window is shown, it may not be fully populated, the content might be missing.

Summing up, this would be hard to get right and would most likely require configuration per application, something we are trying very hard to avoid.

### **How Instead**

Windows processes need to load DLLs in order to access operating system APIs or call functions from their own libraries. When a new process is created, it loads many DLLs in quick succession during its initialization phase. Once the process is ready, the DLL loading stops.

uberAgent monitors the DLL loading phase of new processes closely. The end of that phase is determined by looking for the first 30 second time window in which no DLLs are loaded.

Additionally, if there are IO operations during the DLL loading phase, uberAgent calculates the average IOPS during that phase and waits until IOPS drop to less than 20% for at least 10 seconds after the end of the DLL loading phase.

When those conditions are met uberAgent considers the process to be fully started up. Both of these timeout values can be adjusted globally. The DLL loading timeout is also available on a per-process level. Take look at the section [ProcessStartupDurationWaitIntervalOverride](#) of the configuration file.

### **DLL Loading and Disk IO**

DLLs are only loaded from disk the first time around. When a process is started a second time most or all DLLs will already be in the operating system's file system cache. This optimization often effectively reduces the number of disk IOs incurred by a process start to zero.

uberAgent's startup duration algorithm works correctly regardless of whether DLLs are loaded from disk or from RAM (the file system cache).

Because uberAgent reports the number of disk IOs per process startup the data it collects can be used to easily determine how efficient the caching mechanism is.

## ”Visual” Startup Duration

uberAgent’s algorithm for determining process and application startup durations is reliable and produces consistent results. However, it may not always correlate 100% with the duration as perceived by the end-user. The reason for this potential discrepancy is that uberAgent does not monitor what happens on the screen.

## How to Configure the Data Collection Frequency

July 9, 2024

By default, uberAgent collects performance data every 30 seconds. That can be changed through the [configuration file](#). uberAgent can run an unlimited number of independent *timers*. Each timer wakes up at regular intervals and collects the metrics assigned to it. As stated before, this happens every 30 seconds for all metrics by default.

To change this to 10 seconds edit the file `uberAgent.conf` so that the lines where the intervals are configured read like this:

```
1 # interval unit: milliseconds
2 interval = 10000
```

If, on the other hand, you want only specific metrics at a higher resolution (say 5 seconds), create a new timer section like this:

```
1 [Timer]
2 name = High-frequency app usage
3 comment = This field is optional
4 # interval unit: milliseconds
5 interval = 5000
6 UA metric = ApplicationUsage
```

This makes uberAgent collect application usage data every 5 seconds. Be sure to remove the *ApplicationUsage* metric from any other timers or it will be collected there, too.

**Note:** In addition to timers that collect data at fixed intervals uberAgent also has on-demand metrics that gather data when certain events occur, for example, user logons.

## Incomplete Boot Duration Metrics

July 9, 2024

uberAgent collects detailed information about each machine boot process. This is governed by the on-demand metric *BootDetail* which is enabled by default and can be adjusted through uberAgent's [configuration](#).

### Symptoms

Sometimes the collected *BootDetail* metrics are incomplete and not all data is visualized in the *Boot Duration* dashboard. After reviewing uberAgent's [logfile](#) you may find entries like this:

```
OnOffTransition,Data from boot trace file missing! The following analysis may be incomplete. Lost events: 1000000, lost buffers: 0. Typical cause: insufficient disk bandwidth
```

### Resolution

uberAgent does not add any load to the boot processes. It uses logs that are created by Windows anyway. Depending on the complexity of the boot process (e.g. installed drivers, applications) the pre-defined number of buffers, as well as the buffer size, are insufficient. You can adjust the number of buffers and the buffer size within the endpoint's registry:

```
1 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Diagnostics\
 Performance\BootCKCLSettings
2 "BufferSize"
3 "MaximumBuffers"
4 "MinimumBuffers"
```

Increase all three values until the *lost events* message disappears in uberAgent's logfile. Doubling the default values is a good starting point.

## No Data in Splunk Even Though uberAgent Sends Successfully

July 9, 2024

## Scenario 1: uberAgent is sending data directly to Splunk

### Symptoms

According to uberAgent's log file, there are no events in its in-memory send queue, indicating a successful data transfer to the Splunk server(s):

```
ReceiverStatistics,Splunk; SPLUNKSERVER:19500 - Events in queue: 0,
queue size: 0.0 KB, sent: 1597, added to queue: 1597, rejected from
queue: 0
```

When searching in Splunk's internal logs for errors using the following search:`index=_internal error` you see messages like the following:

```
ERROR TcpInputProc - Message rejected. Received unexpected 707406419
byte message! from src=IPADDRESS:PORT. Maximum message allowed:
67108864
```

### Cause

The port uberAgent sends data to (default: 19500) is configured to receive data from Universal Forwarders.

Splunk Universal Forwarders do not send raw event data, they use a specific protocol. uberAgent, on the other hand, sends raw event data. If the formats sent by the source and expected on the target do not match the above error message may be logged and the incoming data is ignored on the Splunk server.

### Resolution

If uberAgent is sending data directly to Splunk do **not** open port 19500 via *Forwarding and receiving* on the Splunk server. Install the `uberAgent_indexer` app instead which opens port 19500 as a raw TCP port.

## Scenario 2: uberAgent is sending data to a locally installed Splunk Universal Forwarder

### Symptoms

According to uberAgent's log file, there are no events in its in-memory send queue, indicating a successful data transfer to the locally installed Universal Forwarder:



## Extension Not Installed or Enabled

The `SessionFgBrowserActiveTabHost` field is determined with the help of uberAgent's browser extension. If the extension is not installed or enabled in the browser window that is in the foreground, the field cannot be populated.

## Private Mode

The uberAgent extension is not active in private mode unless the browser has specifically been configured to run the extension in private windows, too.

## Denylist/Allowlist

If a tab's site URL is excluded by the `BrowserWebAppURL_Filter` configuration setting uberAgent leaves the `SessionFgBrowserActiveTabHost` field empty.

## Save As or Similar Dialog

While a browser dialog such as *Save As* or *Authentication Required* is being displayed, the foreground window is not a tab, but that modal dialog. Therefore, uberAgent leaves the foreground tab field `SessionFgBrowserActiveTabHost` empty. When that happens, the `SessionFgWindowTitle` field contains the title of the modal dialog, not the title of the previously active tab.

## Developer Tools

While a browser's developer tools window is in the foreground, uberAgent leaves the foreground tab field `SessionFgBrowserActiveTabHost` empty. When that happens, the `SessionFgWindowTitle` field contains the title of the developer tools window.

## Reported GPU Memory Usage per Process is Too High

July 9, 2024

uberAgent determines and reports the GPU memory usage. This happens if the `GpuUsage configuration option` is enabled (default: yes). GPU memory and compute usage are determined for every process that is using the GPU as part of the `ProcessDetail` source type.



## Symptoms

On rare occasions, we have observed that the reported GPU memory usage is far too high. In those cases, the *ProcGpuMemMB* field would reach values as high as 17592178311168.

## Cause

In the observed cases, the cause of the high values was a broken Citrix XenDesktop graphics driver that would cause display issues, too. The issue could be fixed by uninstalling and reinstalling the Citrix XenDesktop VDA (including a reboot after uninstall and reinstall).

## Event Data Filtering Examples

July 9, 2024

### Article Purpose

This article is a pool of Event Data Filtering rules and gets extended continually. Sources could be support tickets or community posts.

The rules serve as a suggestion of what is possible with Event Data Filtering and must be tested before use in your own company.

First, read the [official documentation on Event Data Filtering](#). A few examples are listed there. Then, browse through the rules below.

### List of Rules

#### Logons

```
1 # Do not send data about logons of the service user "LogonTest" in
 # domain "AD" and of local as well as domain admins
2 # Last rule update: 2021-12-22
3
4 [EventDataFilter]
5 Action = deny
6 Sourcetype = Logon:LogonDetail
7 Sourcetype = Logon:GroupPolicyCSEDetail2
8 Query = User == "AD\\LogonTest" OR User LIKE r"%\\administrator"
9
10 [EventDataFilter]
```

```
11 Action = deny
12 Sourcetype = Process:LogonProcesses
13 Query = ProcUser == "AD\\LogonTest" OR ProcUser LIKE r"%\\administrator"
```

## Miscellaneous

```
1 # Do not send any data about the user "JohnDoe" in domain "AD"
2 # You need to list every source type with one of the following fields:
 User, ProcUser, or SessionUser
3 # A list of source types is available in the metrics documentation on /
 en-us/uberagent/
4 # Last rule update: 2021-12-22
5
6 [EventDataFilter]
7 Action = deny
8 Sourcetype = Application:BrowserPerformanceChrome
9 Sourcetype = Application:BrowserWebRequests2
10 Sourcetype = Application:Errors
11 Sourcetype = Process:LogoffProcesses
12 Sourcetype = Process:LogonProcesses
13 Sourcetype = Process:NetworkTargetPerformance
14 Sourcetype = Process:ProcessDetail
15 Sourcetype = Process:ProcessStartup
16 Sourcetype = Process:ProcessStop
17 Sourcetype = ActivityMonitoring:ProcessTagging
18 Query = ProcUser == "AD\\JohnDoe"
19
20 [EventDataFilter]
21 Action = deny
22 Sourcetype = Application:NetworkConnectFailure
23 Sourcetype = Application:UIDelay
24 Sourcetype = Logoff:LogoffDetail
25 Sourcetype = Logon:GroupPolicyCSEDetail2
26 Sourcetype = Logon:LogonDetail
27 Sourcetype = Tags:UserHost
28 Query = User == "AD\\JohnDoe"
29
30 [EventDataFilter]
31 Action = deny
32 Sourcetype = Session:SessionDetail
33 Query = SessionUser == "AD\\JohnDoe"
```

## PowerShell Constrained Language mode

July 9, 2024

This document explains how to use uberAgent with PowerShell's Constrained Language mode enabled.

## Understanding Constrained Language Mode

PowerShell Constrained Language mode is a security feature that restricts access to sensitive language elements that can be used to invoke arbitrary Windows APIs. These features are often required to perform sophisticated cyber attacks. For a detailed description, see this [Microsoft blog post](#).

### Impact on uberAgent

uberAgent relies on PowerShell for collecting various metrics, such as details related to [Citrix](#) or [Custom Scripts](#). The required data is accumulated via multiple APIs, most of which need full access to PowerShell's capabilities.

### Identifying Potential Issues

If you encounter problems in this context, you will notice the following keywords near `powershell.exe` in [uberAgent's log files](#):

- `PermissionDenied`
- `PSNotSupportedException`

The above keywords indicate issues that may have arisen due to the limitations imposed by Constrained Language mode in PowerShell.

## How to use Constrained Language Mode With uberAgent

Constrained Language mode is often implemented by system-wide application control tools, such as AppLocker or Windows Defender Application Control. These tools can also remove the restrictions for files and folders you trust, allowing full command functionality for those particular files.

### AppLocker

If AppLocker is used for application control, you can allow-list uberAgent's PowerShell scripts with the following steps:

1. Open the Group Policy editor.
2. Navigate to **Computer Configuration > Windows Settings > Security Settings > Application Control Policies > AppLocker > Script Rules**.

3. Create a new rule
  - a) Action: **Allow**
  - b) You can choose between Publisher (4) and Path (5)
4. Did you choose Publisher?
  - a) Select an uberAgent script, e.g., `C:\ProgramData\vast limits\uberAgent\Configuration\Security inventory\Windows\Antivirus\Antivirus.ps1`
  - b) Set the slider to **Publisher**
5. Did you choose Path?
  - a) Select **Browse Folders**
  - b) Select a folder e.g., `%OSDRIVE%\ProgramData\vast limits\uberAgent\Configuration\Security inventory\*`
6. If you want to exclude files from the allowlist, you can do that on the Exceptions page.
7. Finally, enter a name for the rule and a description.
8. Click **Create** to add the new rule.

Once the policies are synchronized at the endpoint, uberAgent's scripts should run in `FullLanguage` mode.

Ensure that allow-listed folders and scripts are read-only for regular users. This prevents privilege escalation and ensures PowerShell can execute scripts without modifications.

## Saving uberAgent Data to Disk on the Endpoint

July 25, 2024

Occasionally, you may find yourself in a situation where you need to look at uberAgent's collected data before it is sent to the configured backend(s). This knowledgebase article shows you how to do that by guiding you through the following steps:

- Make the required **adjustments** to your **uberAgent configuration**.
- Set up a **local TCP listener** on the endpoint, which ultimately saves the data to a text file on the local disk.
- **Compare** local with backend data.

## uberAgent Configuration

Add an additional [Receiver] stanza to your [active uberAgent configuration](#) (uberAgent.conf) as follows:

```
1 [Receiver]
2 Name = Local TCP Receiver
3 Type = Splunk
4 Protocol = TCP
5 Servers = localhost:19501
```

This instructs uberAgent to send the data to a local TCP listener on port 19501 - in addition to any other backends you already had configured.

## TCP Listener

Download the latest version of the TCP listener script from the [uberAgent Support Scripts GitHub repository](#) and save it to a location of your choice on the endpoint. We use `C:\Temp\UA-StartTcpReceiver.ps1` here. Start the TCP listener script by running one of the following examples in an elevated PowerShell console.

### Example 1

```
1 C:\Temp\UA-StartTcpReceiver.ps1 -Port 19501 -TimeoutMinutes 10 -
 EnableLogging
```

This starts the TCP listener on port **19501** and saves the received data to `C:\Temp\UA-Data.txt`. The script automatically **stops after 10 minutes**. Logging is enabled, and the log file is saved to `C:\Temp\UA-StartTcpReceiver.ps1.log`.

### Example 2

```
1 C:\Temp\UA-StartTcpReceiver.ps1 -Port 19501 -TimeoutMinutes 0 -
 SearchString "sourcetype=uberAgent:Application:Errors" -
 EnableLogging
```

This starts the TCP listener on port **19501** and saves the received data to `C:\Temp\UA-Data.txt`. The script does not stop after a fixed timeout. It **stops when the string sourcetype=uberAgent:Application:Errors is found** in the received data, meaning an application crash occurred. Logging is enabled, and the log file is saved to `C:\Temp\UA-StartTcpReceiver.ps1.log`.

## Comparing Local With Backend Data

After the TCP listener stops, you can now open the file `C:\Temp\uA-Data.txt` with your text editor of choice and compare the raw data before it leaves the endpoint with the data that is available in your backend(s). For the sake of this article, we compare the formatting and values of a particular event from the `uberAgent:System:SystemPerformanceSummary2` sourcetype.

### Local Data

The raw data, as saved locally by the script, looks as follows:

```
1 ***SPLUNK*** host=VM-WINDOWS11ARM index=uberagent source=uberAgent
 sourcetype=uberAgent:System:SystemPerformanceSummary2
2 1694008385925,0.4,32,2.57,0,1,0,29,0,0.3,,0.6,0.1,0,266,124.5,51369,1213,99,100,0
```

Please note that this data format uses two lines per event: one line of metadata (which does **not** count towards the Splunk data volume) and one line of actual event data.

### Backend Data

We use the below Splunk search to retrieve the same data as saved locally:

```
1 index=uberagent host=VM-WINDOWS11ARM sourcetype=uberAgent:System:
 SystemPerformanceSummary2 Timestamp=1694008385925
```

The search gives us an event that is identical to the locally saved data (the metadata has, of course, been processed by Splunk).

| i | Time                     | Event                                                                                                                                                                                                |
|---|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| > | 9/6/23<br>3:53:05.925 PM | 1694008385925,0.4,32,2.57,0,1,0,29,0,0.3,,0.6,0.1,0,266,124.5,51369,1213,99,100,0.5,7.3,0,0<br>host = VM-WINDOWS11ARM   source = uberAgent   sourcetype = uberAgent:System:SystemPerformanceSummary2 |

So, in this case, everything works as it should.

## Data Storage

July 9, 2024

This section contains knowledge base articles about data storage.

## How to Configure Data Retention

July 9, 2024

Splunk is very flexible with regards to data retention. You can configure when data is old enough to be deleted (after optionally being archived elsewhere). The place to do this is the file `indexes.conf` in uberAgent's app directory.

uberAgent stores its data in its own index called `uberagent`. The default configuration for the uberagent index comes from the file `[uberagent app directory]\default\indexes.conf`:

```
1 [uberagent]
2 homePath = $SPLUNK_DB/uberagent/db
3 coldPath = $SPLUNK_DB/uberagent/colddb
4 thawedPath = $SPLUNK_DB/uberagent/thaweddb
5 maxMemMB = 20
6 maxConcurrentOptimizes = 6
7 maxHotIdleSecs = 86400
8 maxHotBuckets = 10
9 maxDataSize = auto_high_volume
```

**Important:** Do not change this file! If you do, your changes will be lost when the application is updated. Instead, create a new `indexes.conf` in the app's `local` subdirectory. Settings from `local/indexes.conf` overwrite settings from `default/indexes.conf`.

The Splunk documentation page [Configure index storage](#) lists the relevant settings from `indexes.conf`. The most important settings for controlling index storage and data retention are:

- `frozenTimePeriodInSecs`: Absolute time in seconds after which data is deleted (default) or archived (if configured). The default is approximately 6 years.
- `maxTotalDataSizeMB`: Maximum total size of the index in MB. The default is 500,000 MB. When the index reaches this size, the oldest buckets (data directories) are "rolled to frozen", a process that triggers archival (if configured) and subsequent deletion.

By the way, Splunk will never completely fill your disks. By default, it stops accepting new data when the free disk space reaches 2,000 MB.

## Data Volume

July 9, 2024

This section contains knowledge base articles about the data volume.

## The Data Volume Dashboard Does Not Display Values For All Metrics

July 25, 2024

### Symptom

The data volume dashboard only displays "N/A" for the volume of some or all metrics.

### Possible Cause: Splunk Configuration

The data volume dashboard queries Splunk's `_internal` index which in turn reads that data from Splunk's log file `license_usage.log`. By default, every Splunk indexer periodically reports to the license manager stats of the data indexed: broken down by source, source type, host, and index. If the number of distinct (source, source type, host, index) tuples grows over the `squash_threshold`, Splunk squashes the {host, source} values and only reports a breakdown by {sourcetype, index}. This is to prevent high memory usage and an unwieldy number of `license_usage.log` lines.

### Resolution

Increase the `squash_threshold` by adding the following to `$SPLUNK_HOME/etc/system/local/server.conf`:

```
1 [license]
2 squash_threshold = 10000
```

You will find more information [here](#).

### Possible Cause: Permissions

Your user account might not have permissions for the index `_internal`. To check first go to *Settings -> Access controls -> Users -> Your user name* and note the roles assigned to you. Then go to *Settings -> Access controls -> Roles* and check if any of your roles has either `_internal` or *All internal indexes* in the box *Selected search indexes*, i.e. one of these:



| Index Name <input type="text" value="filter"/> | Included <a href="#">?</a>          | Default <a href="#">?</a>           | All <span>▼</span> |
|------------------------------------------------|-------------------------------------|-------------------------------------|--------------------|
| All non-internal indexes                       | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |                    |
| All internal indexes                           | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |                    |
| _audit                                         | <input type="checkbox"/>            | <input type="checkbox"/>            |                    |
| _internal                                      | <input type="checkbox"/>            | <input type="checkbox"/>            |                    |
| _introspection                                 | <input type="checkbox"/>            | <input type="checkbox"/>            |                    |
| _metrics                                       | <input type="checkbox"/>            | <input type="checkbox"/>            |                    |
| _telemetry                                     | <input type="checkbox"/>            | <input type="checkbox"/>            |                    |
| _thefishbucket                                 | <input type="checkbox"/>            | <input type="checkbox"/>            |                    |
| cim_modactions                                 | <input type="checkbox"/>            | <input type="checkbox"/>            |                    |
| history                                        | <input type="checkbox"/>            | <input type="checkbox"/>            |                    |
| main                                           | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |                    |
| summary                                        | <input type="checkbox"/>            | <input type="checkbox"/>            |                    |
| uberagent                                      | <input type="checkbox"/>            | <input type="checkbox"/>            |                    |

### Resolution

Assign either [\\_internal](#) or *All internal indexes* to *Selected search indexes* of one of your roles.

### Footprint & Performance

July 9, 2024

This section contains knowledge base articles about footprint and performance.

## Changing the Accelerated Time Range

July 25, 2024

uberAgent's dashboards make use of a Splunk technology called *accelerated data model*. In a nutshell, an accelerated data model relies on an additional index that speeds up searches by 50x to 100x. As a caveat, an accelerated data model creates a slightly higher CPU load during index time and takes up more disk space on the indexers.

### When Dashboards Might Load Slowly

You may notice that dashboards load slowly if the selected time range goes further back than seven days. This is due to the fact that uberAgent's default accelerated time range is exactly seven days. Older events will be included in searches and dashboards, too, of course, given an appropriate time range was selected, but will be a lot slower to come up.

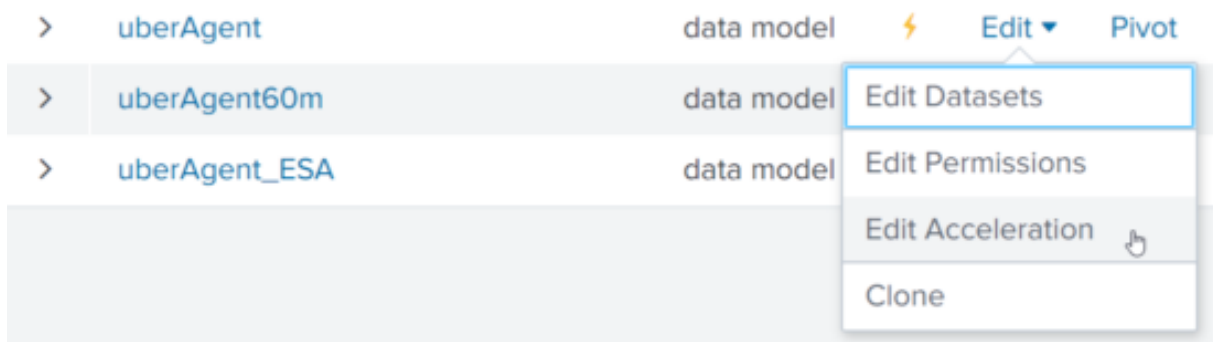
### What To Do About It

To speed up searches that go further back than seven days you can increase the summary range, i.e. the number of days the accelerated data goes back in time. This can be done via the UI or via configuration files. In both cases, the actually changed setting is stored in `[uberagent app directory]\local\datamodels.conf` on the search heads.

**Important:** After updating the uberAgent search head (dashboard) app, make sure your changed file(s) in the `local` subdirectory are still there.

### User Interface

To change the accelerated summary range via the UI navigate to *Settings > Data models* and click *Edit > Edit Acceleration* for any of the uberAgent data models:



Select the desired summary range in the dialog that comes up:

**Edit Acceleration** ✕

Data Model **uberAgent**

Accelerate

Acceleration may increase storage and processing costs.

Summary Range <sup>?</sup> **7 Days** ▾

> Advanced Settings

- 1 Day
- ✓ 7 Days
- 1 Month
- 3 Months
- 1 Year
- All Time
- Custom

**Save**

### Configuration File

To change the accelerated summary range via the configuration files:

- Create a new directory `$SPLUNK_HOME\etc\apps\uberAgent\local` (if it does not already exist)
- Copy `$SPLUNK_HOME\etc\apps\uberAgent\default\datamodels.conf` to `$SPLUNK_HOME\etc\apps\uberAgent\local\datamodels.conf`
- Edit the setting `acceleration.earliest_time` in `$SPLUNK_HOME\etc\apps\uberAgent\local\datamodels.conf`
- Restart Splunk

## Estimating Disk Space Requirements

Before you change the accelerated summary range you should make sure that sufficient disk space is available. To determine the disk space currently occupied by the high-performance analytics store (the special index used by data model acceleration) navigate to *Settings > Data models* in the Splunk UI and click the arrow next to uberAgent. You should see information similar to the following:

### uberAgent

Enables data analytics and reporting for uberAgent.

#### MODEL

Datasets ..... 46 Events, 2 Transactions [Edit](#)

Permissions ..... Shared Globally. Owned by nobody. [Edit](#)

#### ACCELERATION

[Rebuild](#)   [Update](#)   [Edit](#)

Status ..... 100.00% Completed

Access Count ..... 1114. Last Access: 12/2/19 11:56:21.000 AM

Size on Disk ..... 21.09 MB

Summary Range ..... 604800 second(s)

Buckets ..... 2

Updated ..... 11/27/19 10:56:15.000 AM

This shows the summary range (the default is 604800 seconds which is equivalent to 7 days) and the *Size on Disk*. If you plan to extend the summary range to a month expect an approximate increase by 4x.

## Reuse of Open HTTP Connections

July 9, 2024

This article explains how the uberAgent endpoint agent handles open HTTP connections.

## Where HTTP is Used

uberAgent makes use of HTTP(S) to send the collected data from the endpoint to some types of backends, for example, Splunk HEC, Elasticsearch, or Apache Kafka (via Confluent REST Proxy).

## HTTP Connection Reuse

All HTTP(S) communication initiated by uberAgent is performed through [libcurl](#) (a variant of curl), which is probably the highest-quality networking library available today.

Libcurl automatically caches and reuses HTTP(S) connections. As the [documentation](#) states:

Reusing a connection instead of creating a new one offers significant benefits in speed and required resources.

## Requirements for HTTP Connection Reuse

For an HTTP connection to be reused, both server and client must support and enable **HTTP/1.1**.

## Splunk HTTP Event Collector (HEC)

In its default configuration, Splunk's HTTP Event Collector (HEC) only enables HTTP/1.1 if the client sends a user agent string. uberAgent does that starting with version 6.0 beta 2.

We recommend configuring Splunk to always enable HTTP/1.1 for all versions of uberAgent by setting the following in the HEC's [inputs.conf](#) file, located in `$SPLUNK_HOME/etc/apps/splunk_httpinput/local`:

```
1 [http]
2 forceHttp10 = never
```

## Server Failover and Load-Balancing

uberAgent can be [configured](#) with multiple servers per receiver. When there is more than one server per receiver, uberAgent randomly switches between servers every 100 seconds. If a server does not respond, uberAgent fails over to the next server in the list. This algorithm ensures that the load is distributed evenly between backend servers.

## Installation & Upgrade

July 9, 2024

This section contains knowledge base articles about the installation and upgrades.

## Directories and Registry Key Created by uberAgent's Installer

July 9, 2024

uberAgent is not only lightweight and unobtrusive, but it also creates only a minimal set of files and registry keys during installation that can be removed easily.

### Uninstalling uberAgent

#### Windows

If you want to remove uberAgent from a Windows machine please use the installer's uninstall functionality from *Programs and Features*. The following list is intended as a reference.

#### macOS

Use the `uninstall.command` file to remove uberAgent. It can only be executed with elevated privileges. Only use this script if you want to completely remove uberAgent and its configuration from the computer. Its default location is `/Library/Application Support/uberAgent/uninstall.command`.

### File System Changes

#### Windows

All files required by uberAgent go into the installation directory selected during setup (typically `c:\Program Files\vast limits\uberAgent`). During operation, the following additional files/folders are created:

- `uberAgent's log file`
- `%ProgramData%\vast limits\uberAgent`
- `%SystemRoot%\System32\drivers\UberAgentDrv.sys`
- `%SystemRoot%\System32\drivers\uberAgentNetMon.sys`

## macOS

- [uberAgent's log file](#)
- [uberAgent's configuration file](#)
- Application bundle `/Library/uberAgent/uberAgent.app`
- Daemon configuration file `/Library/LaunchDaemons/com.vastlimits.uberAgent.plist`

## Registry Changes

uberAgent stores installation and runtime state information to the key `HKEY_LOCAL_MACHINE\SOFTWARE\vast limits`.

## uberAgent macOS Installation Fails When Executed From a Network Drive

July 9, 2024

### Problem

uberAgent installation on macOS might fail when executed from a network drive, with a similar error. `PackageKit: Install Failed: Error Domain=PKInstallErrorDomain Code =106 "The package "uberAgent.pkg" is missing or invalid."`

### Workaround

If you are facing a problem like the one described above, copy the `uberAgent.pkg` file to a local directory on the endpoint first and repeat the installation from there.

## uberAgent With Splunk Cloud: Differences to On-Premises Splunk Enterprise

July 30, 2024

If you are running **uberAgent** in combination with **Splunk Cloud**, there are several things to be aware of. Due to the [certification policies](#) for Splunk Cloud apps, the uberAgent indexer app and uberAgent dashboard apps (UXM & ESA) slightly differ from the ones available for download on our website. Hence you need to perform the following tasks by hand after the [uberAgent apps](#) have been installed in your Splunk Cloud environment.

## uberAgent Indexer App

### Index Creation

Manually create the uberAgent index. This can be achieved by using Splunk Web and the steps provided [here](#). Use the following settings.

### uberAgent Events

- **Index Name:** uberagent
- **Index Data Type:** Events
- **App:** uberAgent\_indexer

### uberAgent Scores

- **Index Name:** score\_uberagent\_uxm
- **Index Data Type:** Events
- **App:** uberAgent\_indexer

Further index settings depend on your individual requirements. Feel free to [download](#) uberAgent from our website and have a closer look at the settings we ship with the [indexes.conf](#) for non-cloud deployments.

## Configure Data Input

Splunk Cloud only accepts data via encrypted protocols. This means that you have the following options for sending uberAgent data to Splunk Cloud:

- via [uberAgent's native functionality](#) to send to Splunk's HTTP Event Collector (HEC). A guide on how to create an HEC token in Splunk Cloud is available [here](#)
- via a Universal Forwarder installed on the endpoint and configured to communicate with Splunk Cloud

Read [here](#) if you run into problems with self-signed certificates and how that affects your uberAgent deployment.



Alternatively, heavy forwarders can be used. More information on how to configure forwarders to send data to Splunk Cloud can be found [here](#) and [here](#).

## uberAgent Dashboard App

### Data Model Acceleration

Enable acceleration for all uberAgent data models. Please follow the Splunk [documentation](#) for guidance.

### Data Model Configuration

To avoid skipped searches, we recommend allowing the Splunk search scheduler to randomly distribute scheduled searches more evenly over their periods. To enable this setting, you need `acceleration.allow_skew = 100%` to be set within **every uberAgent's app datamodels.conf** file for **each uberAgent data model** ([documentation](#)).

The customization may be applied in one of these two places:

- Directly modify the `datamodels.conf` file shipped with the uberAgent apps in `$SPLUNK_HOME/etc/apps/[uberAgent|uberAgent_ESA]/default/`
- Create a new `datamodels.conf` file containing the `acceleration.allow_skew` setting in `$SPLUNK_HOME/etc/apps/[uberAgent|uberAgent_ESA]/local/`

For reference, please [download](#) uberAgent from our website to inspect the settings we ship with the `datamodels.conf` for non-cloud deployments. As direct modifications to configuration files are not possible when using Splunk Cloud, you need the assistance of Splunk support to change this setting.

## uberAgent HTTP Event Collector (HEC) Receiver Configuration

Carefully read [Splunk's documentation](#) on how to send data to a HEC on Splunk Cloud Platform.

**Important:** Do not add the `<endpoint>` option, e.g. `/services/collector/event`, to your receiver configuration, as uberAgent does this automatically.

## Using uberAgent With Self-Signed Certificates

July 9, 2024

uberAgent natively supports secure data transport for multiple backends, like Splunk, Elasticsearch, or Apache Kafka (via Confluent REST Proxy). For such communication via HTTPS uberAgent uses libcurl (a variant of curl), which is probably the highest-quality networking library available today.

## Why Using Self-Signed Certificates

One might come to a point, during a PoC or evaluation phase, when using a certificate issued by an external or internal CA is not possible or a very complex process. Backends like Splunk or Elasticsearch offer the creation of self-signed certificates, which, by default, are not trusted by libcurl when presented to the client during the communication process. Therefore communication between uberAgent and the desired backend will fail. However, there are ways to change the configuration to make such a test scenario work.

## Working With Self-Signed Certificates on macOS

uberAgent on macOS uses the operating systems implementation of libcurl. And libcurl itself utilizes *LibreSSL* as its library.

This can be easily verified by typing `curl --version` in the Terminal. The following output is an excerpt from a system running macOS 11.1 (Big Sur).

```
1 curl 7.64.1 (x86_64-apple-darwin20.0) libcurl/7.64.1 (SecureTransport)
 LibreSSL/2.8.3 zlib/1.2.11 nghttp2/1.41.0
```

In order to establish a successful connection, the following tasks need to be accomplished:

- Import the self-signed certificate into the macOS system keychain (aka *Keychain.app*), e.g. by double-clicking it
- Set the trust level for the just imported certificate to *Always Trust*, by using the *Keychain.app*

## Working With Self-Signed Certificates on Windows

uberAgent supports a variety of [different versions of Microsoft Windows](#). Since not every operating system release comes with its own implementation of libcurl, uberAgent takes care of that.

Libcurl for Windows relies on [Schannel](#) as its library. Since Schannel acts differently, compared to LibreSSL on macOS when dealing with self-signed certificates, the following steps are required:

- Import the self-signed CA certificate into the Windows certificate store (Trusted Root Certification Authorities)
- Depending on your requirement, add either *TLSRevocationChecksDisabled* or *TLSRevocationChecksBestEffort* ([curl documentation](#)) as an additional `ConfigFlag` to your [uberAgent configuration](#)

An example configuration stanza looks like this:

```
1 [Miscellaneous]
2 DebugMode = true
3 ConfigFlags = TLSRevocationChecksBestEffort
```

## Licensing

July 9, 2024

This section contains knowledge base articles about the licensing.

### How to Enable uberAgent on a Subset of Machines Only

July 9, 2024

With technologies like Citrix Provisioning Services (PVS) a single operating system image can be used for many machines. Typically all relevant applications are installed in that image.

Some customers may want to install uberAgent in such an image but not use it on all machines that run the image. To only enable uberAgent on a subset of machines do the following:

- Install uberAgent in the image
- Change the start type of the system service `uberAgent` from `automatic` to `manual`
- Use a computer startup script to determine whether uberAgent should be enabled on a machine. If so, start the service `uberAgent`

### Supported License File Names & Multiple License Files

July 9, 2024

When you receive a license file for uberAgent it will most likely be named `uberAgent.lic`. That name can be changed, but when doing so please follow these guidelines:

- License file names must follow the pattern: `uberAgent*.lic`
- Multiple license files are supported. uberAgent will use the first license file that is valid.
- On Windows the license file(s) need to reside in the same directory as the main executable `uberAgent.exe`. On macOS the license file needs to be copied to `/Library/Application Support/uberAgent`.

- Alternatively, license file(s) can be hosted on a central file share ([details](#)).

These are examples for valid license file names:

- `uberAgent.lic`
- `uberAgent-clients.lic`
- `uberAgent license 2019-05-08.lic`

## Storing uberAgent's License in Azure Files

July 23, 2024

### Prerequisites

#### Note

This article describes how to use an Azure storage account key to access a file share hosted on Azure Files. Storage account keys are administrative keys for a storage account that grant full read and write permissions for all files, folders, and file shares within the storage account. The permissions are also applied to other storage resources, such as blobs, queues, and tables, contained within the storage account.

Please review [Microsoft's documentation](#) and make sure you understand the potential security concerns and whether this concept of storing uberAgent data in Azure Files meets your requirements.

If you want to store your uberAgent license file(s) in Azure Files, you need to meet the following prerequisites:

- TCP port 445 is not blocked (firewall/ISP)
- For mounting an SMB Azure file share on a Windows machine, SMB 3.1.1 is used. This means that Windows 10, version 1507, or Windows Server 2016 or above is needed. Microsoft provides a [detailed list](#) of supported OS versions.
- For mounting an SMB Azure file share on a macOS machine, SMB 3 is used. This means that macOS High Sierra 10.13 or above is needed. Further details on the requirements for macOS can be found [here](#).

This KB article assumes that a file share within the Azure Storage account already exists. The uberAgent license file(s) can be stored in the file share directly.

## uberAgent Configuration

To configure a central license directory, the `LicenseFilePath` option must be configured in the [uberAgent configuration](#); the value of that option must contain the UNC path to the Azure files directory.

### Using Azure Files With Your On-Premises Client

By default, Azure Files SMB shares can be accessed with a storage key that must be provided when mounting the directory, e.g.:

```
net use
```

When mapping the drive with the command shown above, it is mapped in the *USER* context. Therefore, uberAgent cannot interact with the file share because the agent runs in the *SYSTEM* context.

uberAgent accesses its central license file path via integrated authentication. The login data must be stored for the *SYSTEM* account by adding the credentials to the credential store. To store credentials as *SYSTEM*, one could use `PsExec` by running the following command:

```
.\psexec.exe -s -i cmd.exe cmdkey /add:"
```

After adding the credentials to the credential store for the *SYSTEM* account, uberAgent should be able to access the license file(s) stored in Azure Files.

### Setting Up an Azure File Share With On-Premises AD-Authentication

There is a possibility to integrate a storage account into the local Active Directory and set permissions for your on-premises groups or users. Based on our research, it is not possible to set permissions for computer objects, though. Hence, this can't be used for uberAgent's license validation.

## Logon

July 9, 2024

This section contains knowledge base articles about the logon.

### ”GP logon script” is longer than ”Total duration”

July 25, 2024

## Symptoms

Looking at uberAgent's **User Logon Duration** dashboard, you notice that for some logons, the value for **GP logon script** is larger than the value for **Total duration**.

Data table

| User ↕    | Host ↕  | Logon time ↕        | Total duration ↕ | User profile ↕ | Group policy ↕ | AD logon script ↕ | GP logon script ↕ | Shell start ↕ |
|-----------|---------|---------------------|------------------|----------------|----------------|-------------------|-------------------|---------------|
| AD\dbtest | CTX-DC1 | 2024-06-19 10:03:12 | 7.26             | 0.04           | 1.64           |                   | 336.79            | 0.88          |

## Cause

Most likely, your group policy logon scripts are not configured to [run synchronously](#). By default, Explorer is started before logon scripts have finished. Thus, the desktop appears earlier, and the logon seems to be faster. Many administrators do not want this—they want to make sure all customizations are in place when the desktop is displayed. That is why synchronous script execution is often enabled.

In any case, with uberAgent, the **total logon duration is defined as the time from the actual logon until the shell is fully initialized**. If logon scripts are still running (potentially invisibly) when the second point is reached, then the script execution duration can be longer than the total logon duration.

See also [Logon Data Arrives Late or Never in the Backend](#) for more information how uberAgent calculates the **GP logon script** phase.

## Not all CSEs Used are Listed on the Dashboard "User Logon Duration - Group Policy"

July 25, 2024

The dashboard **Session > User Logon Duration - Group Policy** lists all Group Policy Client-Side Extensions (CSEs) that were applied during each of the logons listed. However, sometimes CSEs that are used in Group Policy are not shown on the dashboard. The display may look like this:

Data table

| User ↕     | Host ↕         | Logon time ↕        | Total policy duration ↕ | DC discovery ↕ | Citrix Group Policy ↕ |
|------------|----------------|---------------------|-------------------------|----------------|-----------------------|
| AD\dominik | LAPTOP-DOMINIK | 2020-05-26 07:58:25 | 0.13                    |                |                       |
| AD\dominik | LAPTOP-DOMINIK | 2020-05-25 13:24:56 | 0.06                    |                |                       |
| AD\dominik | LAPTOP-DOMINIK | 2020-05-19 16:15:23 | 0.11                    |                |                       |

The dashboard only lists CSEs whose settings are *applied* during a logon. When a user has an existing user profile and a Group Policy Object (GPO) has not changed since the last logon the GPO normally is not applied again - this improves logon performance. Since the CSE's settings are not applied, it does not slow down the logon and consequently, it does not show up on the dashboard.

## What is the Definition of the Metric "Pre Logon Init"

July 9, 2024

The *pre login init* metric, displayed on the dashboard *Single Logon*, measures the time from session creation until user logon. High values may or may not indicate a problem, depending on the situation.

### Example 1: Citrix Virtual Apps and Desktops (CVAD)

During a logon to a Citrix XenApp terminal server typically a new session is created. In this case, the *pre login init* metric is important: it shows how long it takes to prepare the new session and connect to it from the client.

### Example 2: Physical PC

On a PC, on the other hand, the situation is often different. When a machine is booted, it presents its logon screen, waiting for the user to enter credentials. That, however, may take a very long time. The user might not even be near the machine when it is started. Therefore the *pre login init* value can be very high without indicating a problem.

## Logon Data Arrives Late or Never in the Backend

July 9, 2024

### Symptoms

- Logon data for a user session is not available in Splunk immediately. Instead, it arrives after the user logged off.
- Logon data for a user session is not available in Splunk at all.

## Cause

The cause is similar to "[GP logon script](#)" is longer than "[Total duration](#)" and how uberAgent determines the **GP logon script** phase.

For uberAgent, the phase starts with the process start `gpscript.exe /logon`. The phase ends when all recursive children of that process are stopped. So, if you have a main logon script that starts other scripts or processes and these continue to run, uberAgent waits for these to stop.

Two situations make uberAgent stop monitoring the logon:

1. **Logoff**: the user logs off, which effectively stops all processes in the session, including the ones from your logon script. uberAgent stops the logon monitoring and sends the data to the back-end. This typically results in high values for the phase **GP logon script**.
2. **Logon timeout expires**: after 30 minutes, uberAgent stops monitoring the logon. No data about the logon is sent.

## Splunk

July 9, 2024

This section contains knowledge base articles about Splunk.

## Configuring Alerts

July 25, 2024

Splunk has a powerful alerting system that can be used to send emails or run arbitrary commands whenever a specific condition is met, as defined in a Splunk search.

In this walkthrough, we demonstrate how to alert when the duration of user logons exceeds a certain threshold.

### Defining the Condition

An easy way to find the right Splunk search for defining the alert condition is to use an element already present on one of uberAgent's dashboards. In this example, we are interested in logon duration which is displayed on the **User Logon Duration** dashboard.




Navigate to the table near the bottom and click the button with the little lens symbol on it:



Data table

| User ↕       | Host ↕      | Logon time ↕           | Total duration ↕ | User profile ↕ | Group policy ↕ | AD logon script ↕ | GP logon script ↕ | Shell start ↕ |
|--------------|-------------|------------------------|------------------|----------------|----------------|-------------------|-------------------|---------------|
| CORP\hq31590 | UA-<br>TS-5 | 2020-05-20<br>15:23:37 | 38.90            | 5.24           | 29.51          | 1.74              | 1.72              | 0.22          |
| CORP\hq99981 | UA-<br>TS-1 | 2020-05-20<br>15:23:37 | 27.34            | 9.72           | 11.54          | 1.28              | 2.98              | 0.42          |

[Explanation of the data in the table](#)

[Open in Search](#)    1m ago

This opens the search in another window. At this stage you can add a condition (highlighted below) to filter for specific events:

**New Search**
Save As ▾ Close

```

| pivot `uA_DM_Logon_All_Transaction` Logon_All_Transaction
 latest(User) as User
 latest(host) as Host
 values(SessionLogonTimeFiltered) as SessionLogonTimeFiltered
 sum(TotalLogonTimeMs) as TotalLogonTimeMs
 sum(ProfileLoadTimeMs) as ProfileLoadTimeMs
 sum(GroupPolicyTotalProcessingTimeMs) as GroupPolicyTotalProcessingTimeMs
 sum(ADLogonScriptTimeMs) as ADLogonScriptTimeMs
 sum(GroupPolicyLogonScriptTimeMs) as GroupPolicyLogonScriptTimeMs
 sum(ShellStartupTimeMs) as ShellStartupTimeMs
 splitrow
 SessionGUID
 filter SessionLogonTimeFiltered is "*"
| eval "Logon time"=strftime(strptime(SessionLogonTimeFiltered,"%Y-%m-%d %H:%M:%S.%Q %z"),
"%Y-%m-%d %H:%M:%S")
| eval "Total duration"=round(TotalLogonTimeMs/1000,2)
| eval "User profile"=round(ProfileLoadTimeMs/1000,2)
| eval "Group policy"=round(GroupPolicyTotalProcessingTimeMs/1000,2)
| eval "AD logon script"=round(ADLogonScriptTimeMs/1000,2)
| eval "GP logon script"=round(GroupPolicyLogonScriptTimeMs/1000,2)
| eval "Shell start"=round(ShellStartupTimeMs/1000,2)
| eval sortfield=lower('Logon time')
| sort limit=0 -sortfield
| table
 SessionGUID
 User
 Host
 "Logon time"
 "Total duration"
 "User profile"
 "Group policy"
 "AD logon script"
 "GP logon script"
 "Shell start"
| where 'Total duration' > 10

```

✓ 90 events (5/20/20 1:36:31.000 PM to 5/20/20 2:36:31.000 PM) No Event Sampling ▾
Job ▾ || ■ → 🖨️ ⬇️ ⚡ Fast Mode ▾

Events Patterns **Statistics (90)** Visualization

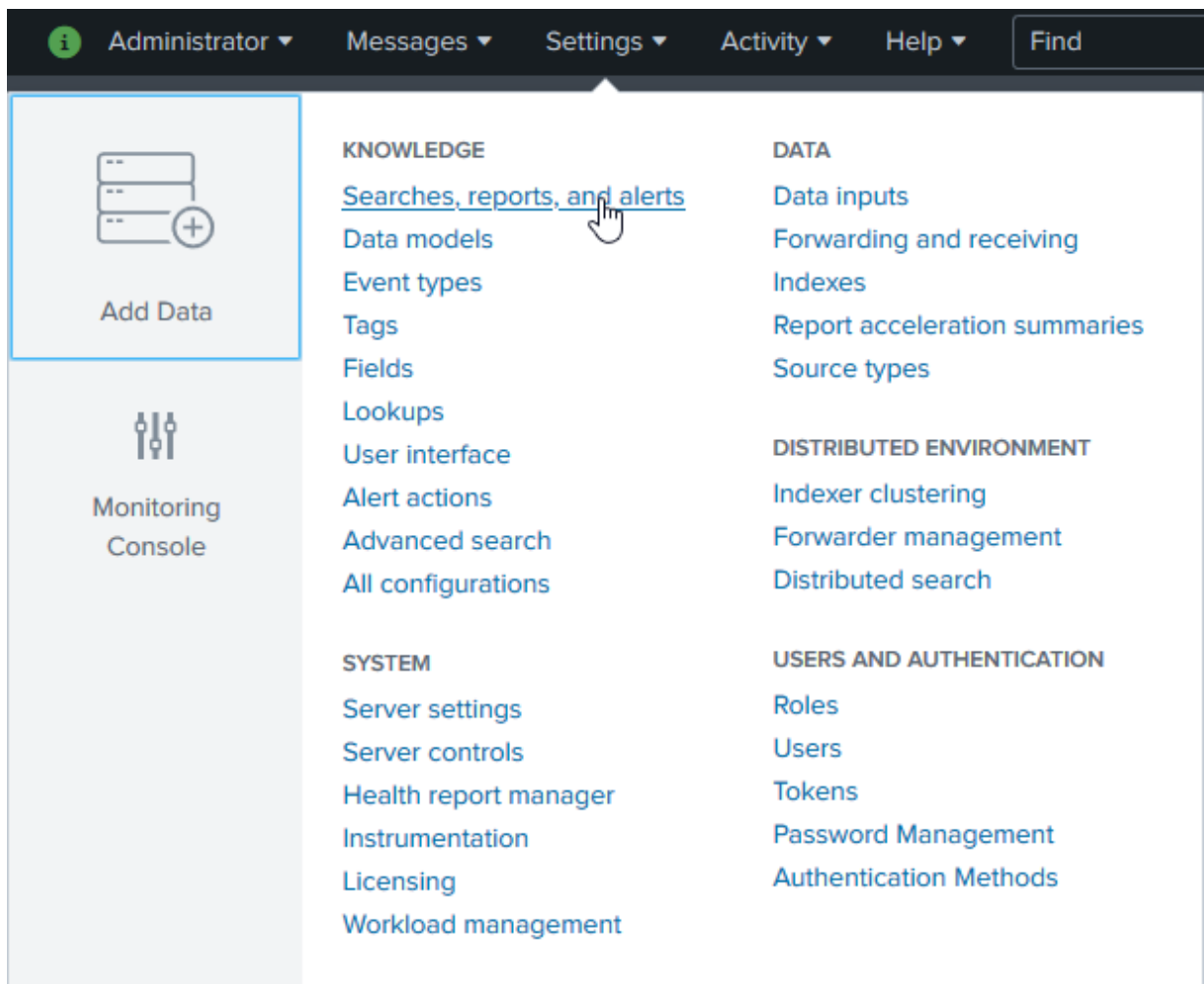
20 Per Page ▾ / Format Preview ▾
< Prev 1 2 3 4 5 Next >

| SessionGUID                          | User         | Host    | Logon time          | Total duration | User profile | Group policy | AD logon script | GP logon script | Shell start |
|--------------------------------------|--------------|---------|---------------------|----------------|--------------|--------------|-----------------|-----------------|-------------|
| 1121a9c3-fc6b-4f5c-9ed8-de3c272f7107 | CORP\hq67623 | UA-TS-1 | 2020-05-20 15:36:19 | 22.95          | 2.64         | 11.16        | 5.88            | 2.31            | 0.28        |
| dd153f81-0152-4ba6-8610-a5071ce03805 | CORP\hq96524 | UA-TS-5 | 2020-05-20 15:33:59 | 40.57          | 7.40         | 28.09        | 1.74            | 2.21            | 0.40        |

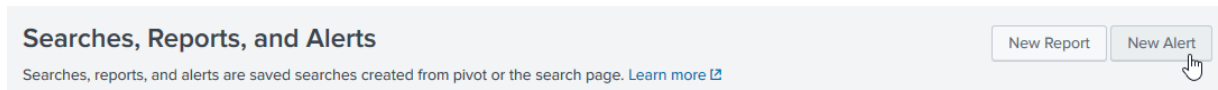
## Setting up the Alert

Once you are happy with the results returned from your conditional search, copy the search string.

Click **Settings > Searches, reports and alerts:**



Click **New Alert**:



Configure the alert as shown in the following very large screenshot:

Create Alert X

**Settings**

Title: Logon duration > 10s

Description: Optional

Search: 

```
| pivot `ua_DM_Logon_All_Transaction` Logon_All_Transaction
 latest(User) as User
 latest(host) as Host
 values(SessionLogonTimeFiltered) as
 SessionLogonTimeFiltered
 sum(TotalLogonTimeMs) as TotalLogonTimeMs
 sum(ProfileLoadTimeMs) as ProfileLoadTimeMs
 sum(GroupPolicyTotalProcessingTimeMs) as
 GroupPolicyTotalProcessingTimeMs
 sum(ADLogonScriptTimeMs) as ADLogonScriptTimeMs
 sum(GroupPolicyLogonScriptTimeMs) as
 GroupPolicyLogonScriptTimeMs
 sum(ShellStartupTimeMs) as ShellStartupTimeMs
 splitrow
 SessionGUID
 filter SessionLogonTimeFiltered is "*"
 | eval "Logon time"=sprintf(%s,
 (SessionLogonTimeFiltered,"%Y-%m-%d %H:%M:%S.%3q %z"),
 "%Y-%m-%d %H:%M:%S")
 | eval "Total duration"=round(TotalLogonTimeMs/1000,2)
 | eval "User profile"=round(ProfileLoadTimeMs/1000,2)
 | eval "Group policy"=round(GroupPolicyTotalProcessingTimeMs
 /1000,2)
 | eval "AD logon script"=round(ADLogonScriptTimeMs/1000,2)
 | eval "GP logon script"=round(GroupPolicyLogonScriptTimeMs
 /1000,2)
 | eval "Shell start"=round(ShellStartupTimeMs/1000,2)
 | eval sortfield=lower("Logon time")
 | sort limit=0 -sortfield
 | table
 SessionGUID
 User
 Host
 "Logon time"
 "Total duration"
 "User profile"
 "Group policy"
 "AD logon script"
 "GP logon script"
 "Shell start"
 | where "Total duration" > 10
```

App: uberAgent LUXM (uberAgent)

Permissions: Private / Shared in App

Alert type: Scheduled / Real-time

Run every hour

At: 0 minutes past the hour

Expires: 24 hours

Trigger Conditions: Number of Results is greater than 0

Trigger: Once / For each result

Throttle:

**Trigger Actions**

+ Add Actions

When triggered:

- Add to Triggered Alerts (Severity: Medium)
- Send email (To: info@uberagent.com, Priority: Normal, Subject: Splunk Alert: \$name\$, Message: The alert condition for '\$name\$' was triggered. Include:  Link to Alert,  Link to Results,  Search String,  Inline Table,  Trigger,  Attach CSV,  Condition,  Trigger Time,  Attach PDF. Type: HTML & Plain Text / Plain Text)

Cancel Save

Specify email addresses for the email trigger action. It might also be a good idea to check **Inline** so that you get the actual data causing the alert right in the email.

## Configure Email Alerting

To configure alerting via Email go to **Settings > Server settings > Email settings**.

The following mail server settings apply to Google Apps:

### Mail Server Settings

Mail host   
Set the host that sends mail for this Splunk instance.

Email security  none  Enable SSL  Enable TLS  
Check with SMTP server admin. When SSL is enabled, mail host should include the port. IE: smtp.splunk.com:465

Username   
Username to use when authenticating with the SMTP server. Leave empty for no authentication.

Password   
Password to use when authenticating with the SMTP server.

Confirm password

## The Resulting Alerts

With that, you are all done. With the sample configuration you will receive an email like the following whenever a user logon takes more than 10 seconds:

The alert condition for 'Logon duration > 10s' was triggered.

Alert: [Logon duration > 10s](#)

[View results in Splunk](#)

| SessionGUID                          | User         | Host    | Logon time          | Total duration | User profile | Group policy | AD logon script | GP logon script | Shell start |
|--------------------------------------|--------------|---------|---------------------|----------------|--------------|--------------|-----------------|-----------------|-------------|
| 3a95ec74-782d-47ba-ba8a-d7703f3f7a21 | CORP\hq28885 | UA-TS-2 | 2020-05-25 10:09:51 | 36.89          | 22.32        | 10.88        | 1.48            | 1.46            | 0.29        |
| 2b89341f-b45c-415a-aafd-70f1f46d671e | CORP\hq53750 | UA-TS-4 | 2020-05-25 10:09:03 | 39.18          | 5.24         | 28.64        | 0.79            | 2.21            | 0.24        |

You can also see all alerts in **Activity > Triggered Alerts**:

|                          | Time ↕                                              | Fired alerts ↕          | App       | Type ↕    | Severity ↕  | Mode ↕ | Actions                                                                                |
|--------------------------|-----------------------------------------------------|-------------------------|-----------|-----------|-------------|--------|----------------------------------------------------------------------------------------|
| <input type="checkbox"/> | 2020-05-25 08:10:02<br>Mitteleuropäische Sommerzeit | Logon<br>duration > 10s | uberAgent | Scheduled | ●<br>Medium | Digest | <a href="#">View results</a>  <br><a href="#">Edit search</a>   <a href="#">Delete</a> |
| <input type="checkbox"/> | 2020-05-25 08:05:03<br>Mitteleuropäische Sommerzeit | Logon<br>duration > 10s | uberAgent | Scheduled | ●<br>Medium | Digest | <a href="#">View results</a>  <br><a href="#">Edit search</a>   <a href="#">Delete</a> |

## How to Change uberAgent's Splunk Index Name

July 9, 2024

By default, uberAgent sends the data it collects to the Splunk index *uberagent*.

### How is the index created

The index *uberagent* is created in the indexer app *uberAgent\_indexer*. The file `default\indexes.conf` contains the relevant definitions.

### How to change the index name

If you want to change the index name, you need to do so in the following places:

- `indexes.conf` (see above)
- uberAgent configuration (see below)
- `macros.conf` (see below)
- `eventtypes.conf` (see below)

### uberAgent configuration

The index uberAgent sends the collected data to can be configured in uberAgent's [configuration](#) with the setting *Index*.

### Macros.conf

The index searched in the dashboards can be configured through the *uberAgent\_index* stanza in the file `macros.conf` of the dashboard (search head) app. The default is as follows:

```
1 [uberAgent_index]
2 definition = uberagent*
```

## Eventtypes.conf

The index searched for the event type `uberAgent_index_query` can be configured through the `uberAgent_index_query` stanza in the file `eventtypes.conf` of the dashboard (search head) apps. The default is as follows:

```
1 [uberAgent_index_query]
2 search = index=uberagent*
```

## Splunk Product Editions (SKUs) Supported by uberAgent

July 9, 2024

Splunk comes in multiple product editions:

- Splunk Enterprise
- Splunk Cloud
- Splunk Free
- Splunk Light (discontinued as of 2020-05-01)

Splunk Enterprise, Splunk Free, and Splunk Light are hosted on-premises while Splunk Cloud is hosted by Splunk.

Out of these SKUs, **Splunk Enterprise and Splunk Cloud are fully supported by uberAgent.**

### Splunk Enterprise

After installation, Splunk operates in Enterprise mode for 60 days after the installation. After that, it reverts to Free mode if no license is added.

During the 60-day trial period, Splunk is restricted to a daily data volume of 500 MB per day.

### Splunk Cloud

uberAgent apps can be installed using the self-service app installation method. More information is available in Splunk's [documentation](#).

The following apps are available in Splunk Cloud:

- [uberAgent indexer app](#)
- [uberAgent UXM dashboard app](#)
- [uberAgent ESA dashboard app](#)

After the uberAgent apps have been installed in your Splunk Cloud environment, some manual actions need to be taken. This [knowledgebase article](#) contains all the necessary details.

## Splunk Free

uberAgent generally works well with Splunk Free except for one thing: Splunk bug [SPL-40332](#) breaks not the initial creation but the update of CSV lookup tables. To workaround that we had to replace the `outputlookup` command with `action.populate_lookup` in a saved search. That, however, is a feature not enabled with Splunk Free.

As a result, uberAgent does not work correctly on Splunk Free until [SPL-40332](#) has been fixed in a future version of Splunk.

However, using [this workaround](#) the lookup table can be generated manually.

Please see [this document](#) for more information on Splunk Free. There is also a [feature comparison table](#) between Splunk Free, Splunk Enterprise and Splunk Cloud available.

## Splunk Light (Discontinued)

Splunk Light has a very limited feature set that does not even include the installation of apps (see [Splunk Light vs. Splunk Enterprise](#)). Due to these limitations, uberAgent cannot work with Splunk Light.

## What to Do When You Get Splunk License Errors

July 9, 2024

### What Are Splunk License Warnings and Violations

The Splunk [documentation](#) explains license warnings and violations as follows:

*Warnings and violations occur when you exceed the maximum indexing volume allowed for your license.*

*If you exceed your licensed daily volume on any one calendar day, you will get a violation warning. The message persists for 14 days. If you have 5 or more warnings on an Enterprise license or 3 warnings on a Free license in a rolling 30-day period, you are in violation of your license, and search will be disabled for the offending pool (but indexing continues). Search capabilities return when you have fewer than 5 (Enterprise) or 3 (Free) warnings in the previous 30 days, or when you apply a temporary reset license (available for Enterprise only).*



## Symptoms of Splunk License Violations

When a license violation occurs you typically get this message:

Error in 'litsearch' command: Your Splunk license expired or you have exceeded your license limit too many times. Renew your Splunk license by visiting [www.splunk.com/store](http://www.splunk.com/store) or calling 866.GET.SPLUNK.

## What You Can Do

You can do either one of the following things to get back search functionality:

- Send fewer data to Splunk for indexing and then wait until there are no more than three (Splunk Free) / five (Splunk Enterprise) violations in the past 30 days
- Uninstall and then reinstall Splunk
- If you are on Splunk Enterprise contact Splunk to get a temporary reset license
- If you are trying the product out contact Splunk to get an evaluation license *and* a temporary reset license

## Workaround for Lookup Errors with Splunk Free

July 9, 2024

On Splunk Free, uberAgent cannot automatically generate needed lookup tables. Because of the missing lookup tables, the following or similar error messages are displayed on many dashboards:

- No results found
- The lookup table `lookup_appnameidmapping` does not exist. It is referenced by configuration `uberAgent:Process:NetworkTargetPerformance`.
- The lookup table `lookup_appnameidmapping` does not exist. It is referenced by configuration `uberAgent:Process:ProcessDetail`.
- The lookup table `lookup_appnameidmapping` does not exist. It is referenced by configuration `uberAgent:Process:ProcessStartup`.

See [this article](#) for details and for information on officially supported versions.

## Workaround

As a workaround, the lookup tables can be generated manually. To do that run slightly modified searches from uberAgent's `savedsearches.conf`.

One of the original searches:

```
index=`uberAgent_index` sourcetype=uberAgent:Application:AppNameIdMapping
 AppId=* AppName=* | stats latest(_time)as _time mode(AppName)as
 AppName by AppId | inputlookup append=t lookup_appnameidmapping |
 stats latest(_time)as _time latest(AppName)as AppName by AppId | eval
 TimeDelta=now()-_time | search TimeDelta<31536000 | fields AppName
 AppId _time
```

We simply append the `outputlookup` command to have Splunk create the lookup tables. The full searches look like this:

```
index=`uberAgent_index` sourcetype=uberAgent:Application:AppNameIdMapping
 AppId=* AppName=* | stats latest(_time)as _time mode(AppName)as
 AppName by AppId | inputlookup append=t lookup_appnameidmapping |
 stats latest(_time)as _time latest(AppName)as AppName by AppId | eval
 TimeDelta=now()-_time | search TimeDelta<31536000 | fields AppName
 AppId _time | outputlookup lookup_appnameidmapping
```

```
index=`uberAgent_index` (sourcetype=uberAgent:System:MachineInventory
 OR sourcetype=uberAgent:System:NetworkConfigInformation)OsVersion=*
 | stats latest(_time)as _time latest(OsVersion)as OsVersion latest
 (OsBuild)as OsBuild latest(OsType)as OsType latest(AdDomainDns)as
 AdDomainDns latest(AdSite)as AdSite latest(AdOu)as AdOu latest(
 CtxFarmName)as CtxFarmName latest(CtxMachineCatalogName)as CtxMachineCatalogName
 latest(CtxDeliveryGroupName)as CtxDeliveryGroupName latest(HwManufacturer
)as HwManufacturer latest(HwModel)as HwModel values(NetworkConfigIPv4
)as NetworkConfigIPv4 by host | inputlookup append=t lookup_hostinfo
 | fields - Ipv4Address | stats latest(_time)as _time latest(OsVersion
)as OsVersion latest(OsBuild)as OsBuild latest(OsType)as OsType
 latest(AdDomainDns)as AdDomainDns latest(AdSite)as AdSite latest(AdOu
)as AdOu latest(CtxFarmName)as CtxFarmName latest(CtxMachineCatalogName
)as CtxMachineCatalogName latest(CtxDeliveryGroupName)as CtxDeliveryGroupName
 latest(HwManufacturer)as HwManufacturer latest(HwModel)as HwModel
 values(NetworkConfigIPv4)as Ipv4Address by host | eval TimeDelta=now
 ()-_time | search TimeDelta<31536000 | fields host OsVersion OsBuild
 OsType AdDomainDns AdSite AdOu CtxFarmName CtxMachineCatalogName
 CtxDeliveryGroupName HwManufacturer HwModel Ipv4Address _time |
 outputlookup lookup_hostinfo
```

```
index=`uberAgent_index` sourcetype=uberAgent:System:MachineInventory
 RAMSizeGB=* | stats latest(_time)as _time latest(RAMSizeGB)as
 RAMSizeGB latest(IsBatteryPresent)as IsBatteryPresent latest(CPUName
```

```
)as CPUName latest(CPUSockets)as CPUSockets latest(CPUCoresPhysical)
as CPUCoresPhysical latest(CPUCoresLogical)as CPUCoresLogical latest(
CPUMaxMhz)as CPUMaxMhz latest(HwIsVirtualMachine)as HwIsVirtualMachine
 latest(OsUpdateBuildRevision)as OsUpdateBuildRevision by host |
 inputlookup append=t lookup_hostinfo2 | stats latest(_time)as
_time latest(RAMSizeGB)as RAMSizeGB latest(IsBatteryPresent)as
IsBatteryPresent latest(CPUName)as CPUName latest(CPUSockets)as
 CPUSockets latest(CPUCoresPhysical)as CPUCoresPhysical latest(
CPUCoresLogical)as CPUCoresLogical latest(CPUMaxMhz)as CPUMaxMhz
latest(HwIsVirtualMachine)as HwIsVirtualMachine latest(OsUpdateBuildRevision
)as OsUpdateBuildRevision by host | eval TimeDelta=now()-_time |
search TimeDelta<31536000 | fields host RAMSizeGB IsBatteryPresent
 CPUName CPUSockets CPUCoresPhysical CPUCoresLogical CPUMaxMhz
HwIsVirtualMachine OsUpdateBuildRevision _time | outputlookup lookup_hostinfo2

| pivot uberAgent Process_ProcessStartup latest(_time)as LastSeen
splitrow ProcName | eval ProcName = lower (ProcName)| inputlookup
append=t lookup_processstartup_processlist | stats first(LastSeen)
as LastSeen by ProcName | eval LastSeen = round (strptime (LastSeen
, "%Y-%m-%dT%H:%M:%S.%Q%z"), 0)| eval TimeDelta=now()-LastSeen |
search TimeDelta<31536000 | fields ProcName LastSeen | outputlookup
lookup_processstartup_processlist

| pivot uberAgent Process_NetworkTargetPerformance latest(_time)as
LastSeen splitrow NetTargetRemoteNameAddress | eval ProcName = lower
(NetTargetRemoteNameAddress)| inputlookup append=t lookup_networktargetperform
 | stats first(LastSeen)as LastSeen by NetTargetRemoteNameAddress |
eval LastSeen = round (strptime (LastSeen, "%Y-%m-%dT%H:%M:%S.%Q%z"
), 0)| eval TimeDelta=now()-LastSeen | search TimeDelta<31536000 |
fields NetTargetRemoteNameAddress LastSeen | outputlookup lookup_networktarget
```

Run these searches over a longer time range (e.g. last seven days) to capture among other things mappings for applications that are run only infrequently, too.

After running one of the full searches Splunk might display error messages like `"Could not write to file 'lookup_appnameidmapping': Failed to move file to final destination."` However, we found that it still creates all output files successfully.

## User Interface

July 9, 2024

This section contains knowledge base articles about the user interface.

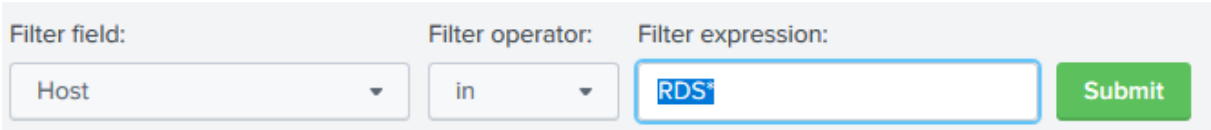
## How to Separate Data from Different Types of Machines

July 25, 2024

If you are monitoring different types of machines with uberAgent, say XenDesktop/VDI clients and XenApp/RDS servers, you may want to separate the data in the dashboards so that you only see data from one group of machines or the other.

### Temporary Separation

To temporarily view only data from a group of machines enter that part of the computer names that uniquely define machines in the desired group in the *Filter expression* input box on the dashboard. E.g. to filter for machines whose names start with the string *RDS*:



The screenshot shows a filter configuration interface with three main sections: 'Filter field:', 'Filter operator:', and 'Filter expression:'. Below 'Filter field:' is a dropdown menu with 'Host' selected. Below 'Filter operator:' is a dropdown menu with 'in' selected. Below 'Filter expression:' is a text input box containing 'RDS\*'. To the right of the input boxes is a green 'Submit' button.

### Permanent Separation

To permanently separate data from a group of machines utilize [uberAgent's multi-tenancy capabilities](#).

Splunk stores data in containers called indexes. By default uberAgent stores all its data in the index *uberagent*. But you can easily configure one group of machines to store data in an index called *uberagent-clients* and another to store in *uberagent-servers*. The only requirement is that all index names should start with a common prefix, otherwise the dashboards will not work.

By default uberAgent's dashboards search all indexes whose names start with *uberagent*. But you can configure individual Splunk user accounts so that they only have permissions to search in the index of one machine group, not the other. Depending on the user account you log on to Splunk with you see data from different machine groups.

For details on how to implement this please see [this article](#).

## Alternative for Permanent Separation

As an alternative to separating data into multiple indexes, you can always create custom dashboards that use some other means of differentiating between different types of machines. You could, for example, use a lookup table that stores a mapping between machine groups and computer name regexes.

## Remoting Protocol is Console Instead of ICA or RDP

July 9, 2024

It may happen the dashboard *User Sessions* displays the remoting protocol as *Console* even though you know that the users were connecting over ICA or RDP.

### Explanation

The Windows API used to query for the connection type does not always return ICA/RDP for an ICA/RDP session. During the logon and logoff phases, the connection type returned by the API is *Console*.

uberAgent determines the connection type every 30 seconds by default. Since the connection type may change during the lifetime of a session uberAgent needs to choose somehow which of the potentially multiple values to display. It does so by displaying the last reported value for that session.

For that reason sessions that take long to log on and/or off and/or are short-lived may be displayed with a connection type of *Console* instead of the expected *ICA* or *RDP*.

## The Dashboards Do Not Work Correctly in Internet Explorer

July 9, 2024

Unfortunately part of the dashboard functionality does not work correctly in Internet Explorer 8. This also affects newer versions of IE in compatibility mode. If you have IE9 or newer, disable compatibility mode.

As of Splunk 6.1 support for Internet Explorer 7 and 8 has officially been removed by Splunk. The [release notes](#) state:

*Internet Explorer versions 7 and 8: Browser support has been removed because they have either been marked as end-of-life by Microsoft or are no longer widely used. Support for these browsers might be removed entirely in a future release. For Internet Explorer support, use versions 9, 10, or 11.*

## Practice Guides

July 9, 2024

This section contains practical examples of how to use uberAgent for specific tasks.

### Detecting Network Connectivity Problems

July 25, 2024

Network connectivity issues severely impact application functionality and performance, yet are often difficult to diagnose. This practice guide demonstrates how uberAgent helps.

Network issues come in two flavors: permanent and intermittent. The following sections explain both in detail.

#### Permanent Network Connectivity Issues

Permanent issues are often caused by configuration errors. Examples:

- A server service was migrated to a new machine but the application configuration is still pointing to the old machine.
- Firewall rules are missing so application connectivity is blocked.

#### Intermittent Network Connectivity Issues

Intermittent issues only occur from time to time and may cause seemingly random application slowness or occasional application errors. Examples:

- Bad WiFi signal reception
- Packet loss
- Saturated internet connection

#### Diagnosing Network Connectivity Issues

uberAgent monitors all network traffic and enriches it with metadata like the originating application, the user account, the machine type, Active Directory OU, Citrix site, and much more. Network traffic is categorized as successful or failed connection, regular transmission or retransmit, and so on.

When suspecting network problems the dashboard to consult is *Application Network Issues*, located in the *Applications* menu.

### Network Availability Indicator

The first thing to check is the *Network availability* metric:

#### Overview

Network availability:

98.80 %

It is the ratio of successful connections and transmissions to the total number of connection and transmission attempts and should be at 100%.

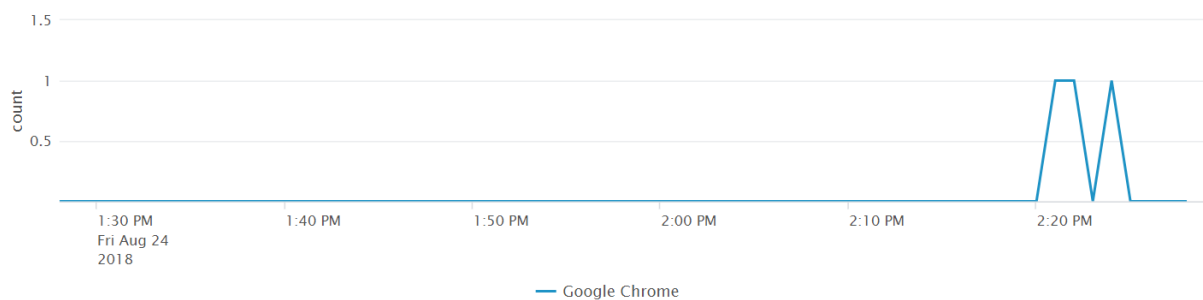
### Network Issues Over Time

The next thing to check are the timecharts in the section *Issues grouped over time*:

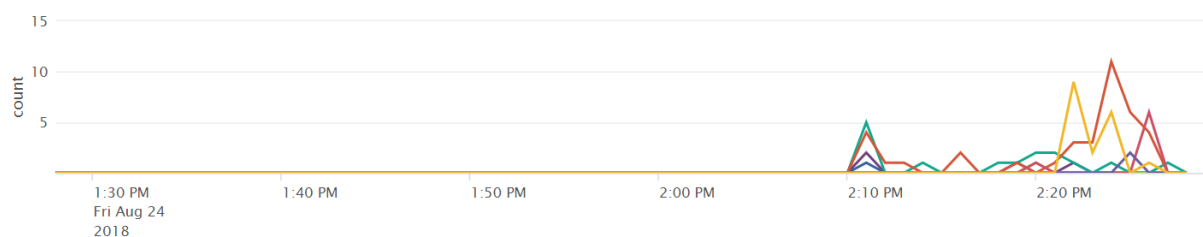
Issues grouped over time

Group by:  Target host:  Target port:

#### Connection failures



#### Reconnects & retransmits



The two graphs show connection failures and reconnects & retransmits over the selected time range. By default both graphs group errors per application, but you can switch to errors per process, per

source or target host, per target port or even per user.

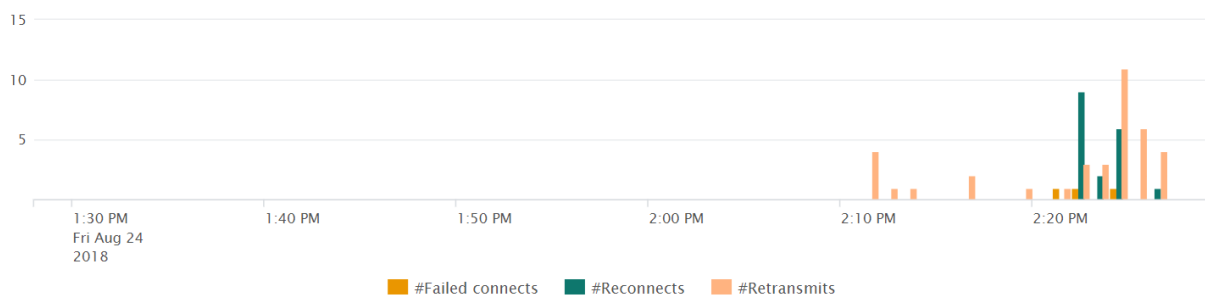
### Network Issues per Application

To further analyze the errors for a specific application (or host, user, etc.) click on the respective row of the table *Issues grouped (top 100)*. This performs an in-page drilldown, bringing up an additional table and chart with details on the selected item:

Targets with issues: Application = Google Chrome

| Target host                  | Target port | #Failed connects | #Successful connects | #Reconnects | #Retransmits | #Sends | #Receives |
|------------------------------|-------------|------------------|----------------------|-------------|--------------|--------|-----------|
| 34.196.163.159               | 443         | 1                | 0                    | 0           | 0            | 0      | 0         |
| 52.45.125.18                 | 443         | 1                | 0                    | 0           | 0            | 0      | 0         |
| 54.174.70.29                 | 443         | 1                | 1                    | 2           | 0            | 5      | 3         |
| 104.197.19.184               | 443         | 0                | 3                    | 0           | 4            | 17     | 28        |
| 104.244.42.196               | 443         | 0                | 4                    | 3           | 0            | 59     | 24        |
| api.twitter.com              | 443         | 0                | 21                   | 10          | 16           | 378    | 189       |
| app2.frontapp.com            | 443         | 0                | 14                   | 0           | 5            | 250    | 406       |
| capi.grammarly.com           | 443         | 0                | 5                    | 2           | 6            | 275    | 566       |
| f-log-extension.grammarly.io | 443         | 0                | 2                    | 0           | 2            | 10     | 11        |
| mail.google.com              | 443         | 0                | 1                    | 0           | 1            | 86     | 1579      |

« prev 1 2 next »



In the screenshot above we can see that reconnection and retransmission errors started at around 2:10 PM for the selected application (Google Chrome). The errors are not limited to specific target hosts. This indicates intermittent problems, most likely related to unstable internet connectivity.

## Citrix ADC Monitoring & Alerting

July 9, 2024

uberAgent 5.2 introduced Citrix ADC monitoring (formerly NetScaler ADC). This functionality lets you check the appliance health, gateway data volume, and service availability of your ADCs. While it is great to have all this information in dashboards, it sometimes makes sense to get notified when things are not working the way they should. This article demonstrates how to use Splunk’s alerting capabilities to configure just that.



## Splunk Alerting

If you are not familiar with Splunk alerting here is the explanation in a nutshell: you create a search; every time it produces a result you will get notified. Several notification methods are available (email, webhooks and so on). More on this topic is available in [Splunk's documentation](#).

### Example Searches for Citrix ADC Alerts

We created some example searches showing what is possible with uberAgent's data and Splunk's alerting capabilities. Feel free to customize them to your needs or use them as a starting point for your own creations.

#### Max Bandwidth per Appliance

The purchased license determines the maximum amount of data the ADC will process - it is a software limitation. Hence it is important to keep an eye on the bandwidth usage to react in a timely manner and buy a bigger license to not slow down the users. Here is an example where you will be notified when the bandwidth usage exceeded 900 megabytes.

```
1 | pivot `uA_DM_CitrixADC_AppliancePerformance`
 CitrixADC_AppliancePerformance
2 max(ApplianceMBReceived) as "max(ApplianceMBReceived)"
3 max(ApplianceMBSent) as "max(ApplianceMBSent)"
4 splitrow
5 HostName
6 | eval "Max. network data volume (MB)" = round('max(ApplianceMBReceived
)' + 'max(ApplianceMBSent)',1)
7 | where 'Max. network data volume (MB)' > 900
```

#### Too Many HA Status Changes

A Citrix ADC high-availability (HA) pair consists of a primary and a secondary node. If the primary fails the secondary takes over. Too many status changes indicate that there is something wrong. Maybe your hypervisor does live migration of VMs? It should not for Citrix ADC VPX machines!

```
1 | pivot `uA_DM_CitrixADC_ApplianceInventory`
 CitrixADC_ApplianceInventory
2 dc>LastHAStatusChange as "#Status changes"
3 splitrow
4 HostName
5 | where '#Status changes' > 5
```

The current status is collected once per day by default consequently let that search run for at least a few days.

### Get Notified When SSL Cards Are Down

In a hardware Citrix ADC appliance, SSL cards handle the encryption and decryption of SSL traffic. If an SSL card is down the encryption/decryption rate drops which possibly affects user experience.

```

1 | pivot `uA_DM_CitrixADC_ApplianceInventory`
 CitrixADC_ApplianceInventory
2 | latest(SSLCards) as "#SSL cards"
3 | latest(SSLCardsUp) as "#SSL cards up"
4 | splitrow
 HostName
6 | eval "#SSL cards down" = '#SSL cards' - '#SSL cards up'
7 | where '#SSL cards down' != 0

```

### Get Notified When the Configuration Was Not Saved Within 24 Hours After a Change

Citrix ADC configuration changes are active immediately, even if they have not been specifically saved. However, unsaved changes are lost when the appliance is rebooted. With this search, you will be notified after 24 hours if someone forgot to save the configuration.

```

1 | pivot `uA_DM_CitrixADC_ApplianceInventory`
 CitrixADC_ApplianceInventory
2 | latest>LastConfigSaveTime) as LastConfigSaveTime
3 | latest>LastConfigChangedTime) as LastConfigChangedTime
4 | splitrow
 HostName
6 | eval LastConfigSaveTime_epoch = strptime>LastConfigSaveTime, "%Y-%m-%d %H:%S:%M")
7 | eval LastConfigChangedTime_epoch = strptime>LastConfigChangedTime, "%Y-%m-%d %H:%S:%M")
8 | eval Offset = LastConfigChangedTime_epoch - LastConfigSaveTime_epoch
9 | where Offset > 86400

```

### Get Notified When a Certificate Expires Within Four Weeks

The all-time favorite. A certificate is installed but the team managing it forgot to update it. Never let that happen again with this search!

```

1 | pivot `uA_DM_CitrixADC_Certificate` CitrixADC_Certificate
2 | latest(CertExpirationDate) as CertExpirationDate
3 | splitrow
 CertName as "Certificate name"
5 | eval CertExpirationDate_epoch = strptime(CertExpirationDate, "%Y-%m-%d %H:%S:%M")
6 | eval CurrentTime_epoch = now()
7 | convert ctime(now)
8 | eval thirty_days_from_now = CurrentTime_epoch + 2592000

```

```
9 | eval Expires_within_next_30_days = if(CertExpirationDate_epoch >=
 CurrentTime_epoch AND CertExpirationDate_epoch <=
 thirty_days_from_now, "yes", "no")
10 | where Expires_within_next_30_days = "yes"
11 | table
12 "Certificate name"
13 CertExpirationDate
14 Expires_within_next_30_days
```

### List All IPs Where Management Access Is Enabled but It Is Not an NSIP

It is a common best practice to enable management only on the NetScaler IP (NSIP). Anyway, managing it through the Subnet IP (SNIP) is much more easy, right? Just don't! Keep safe with this search:

```
1 | pivot `uA_DM_CitrixADC_Ip` CitrixADC_Ip
2 latest(IpNetmask) as Netmask
3 latest(IpType) as Type
4 latest(IpvServer) as "Bound to vServer"
5 latest(IpMgmtAccess) as "Mgmt. access"
6 splitrow
7 IPAddress as "IP address"
8 filter HostName is "ns1"
9 | eval "Mgmt. access" = if('Mgmt. access'=1,"Yes","No")
10 | where Type != "NSIP" and 'Mgmt. access' = "Yes"
11 | table
12 "IP address"
13 Netmask
14 Type
15 "Bound to vServer"
16 "Mgmt. access"
```

## Generating Driver Version Inventory Reports

July 25, 2024

When users report hardware problems, it is often not the hardware itself that is malfunctioning, but the installed driver. In these situations, it can be invaluable to have an overview of all drivers on your endpoints. Here is how to create driver reports that list names and versions of some or all installed drivers.

The scripts listed in this guide are managed in vast limits'public [GitHub repository](#).

## Listing Drivers With uberAgent's Built-In Functionality

uberAgent collects version numbers for all installed applications, including driver packages. The following search, for example, gives you an overview of all installed Nvidia and Intel graphics software:

```
1 | pivot `uberAgent_index` Application_ApplicationInventory
2 dc(host) as "#Installations"
3 splitrow
4 DisplayName as Name
5 splitrow
6 DisplayVersion as Version
7 filter DisplayName in ("Nvidia Graphics Driver*", "Intel(R)
8 Processor Graphics")
8 | table
9 Name
10 Version
11 "#Installations"
```

## Listing Even More Drivers With Custom Scripts

Anyway, not all drivers are installed via software packages. Some are e.g. installed via Microsoft updates. uberAgent's [custom script functionality](#) to the rescue! In a nutshell, it executes any script you like and sends the output to Splunk.

Use this PowerShell script to list all installed drivers:

```
1 $Output = @{}
2 }
3
4 $DriverPackages = $null
5
6 $DriverPackages = Get-WmiObject Win32_PnPSignedDriver | select
7 devicename, driverversion, driverprovidername | where-object {
8 $PSItem.driverprovidername -notlike "" -and $PSItem.driverprovidername
9 -notlike "*Microsoft*" }
10
11
12
13 # Do some formatting for Intel drivers as the vendor name is not
14 consistent
15 If ($DriverPackage.driverprovidername -like "*Intel*")
16 {
17 $DriverPackage.driverprovidername = "Intel"
18 }
19
20 $Output = @{}
21
```

```

22 'DeviceName' = "`"`${$DriverPackage.devicename}`""
23 'DriverVersion' = $DriverPackage.driverversion
24 'DriverVendor' = "`"`${$DriverPackage.driverprovidername}`""
25 }
26
27 Write-Output $($Output.Keys.ForEach({
28 "$_=${$Output.$_}" })
29) -join ' '
30 }

```

I denylisted everything Microsoft related reducing the list to third-party drivers only. Another way would be to just include specific vendors:

```

1 $Output = @{}
2 }
3
4 $DriverPackages = $null
5
6 $DriverPackages = Get-WmiObject Win32_PnPSignedDriver | select
7 devicename, driverversion, driverprovidername | where-object {
8 $PSItem.driverprovidername -like "*Intel*" -or $PSItem.
9 driverprovidername -like "*Lenovo*" }
10
11 Foreach ($DriverPackage in $DriverPackages)
12 {
13 # Do some formatting for Intel drivers as the vendor name is not
14 # consistent
15 If ($DriverPackage.driverprovidername -like "*Intel*")
16 {
17 $DriverPackage.driverprovidername = "Intel"
18 }
19
20 $Output = @{}
21
22 'DeviceName' = "`"`${$DriverPackage.devicename}`""
23 'DriverVersion' = $DriverPackage.driverversion
24 'DriverVendor' = "`"`${$DriverPackage.driverprovidername}`""
25 }
26
27 Write-Output $($Output.Keys.ForEach({
28 "$_=${$Output.$_}" })
29) -join ' '
30 }

```

In any case, filtering is recommended to sort out unneeded drivers and keep the indexed data volume as small as possible.

Let us stick to the first example script and have a look at the output:

```

1 DriverVendor="Lenovo" DeviceName="System Interface Foundation V2 Device

```

```
" DriverVersion=1.1.17.2
2 DriverVendor="Synaptics" DeviceName="Synaptics HID-Compliant Touch pad
 Device" DriverVersion=19.3.4.219
3 DriverVendor="Intel" DeviceName="Intel(R) Software Guard Extensions
 Platform Software Component" DriverVersion=2.1.100.46245
4 DriverVendor="Intel" DeviceName="Intel(R) Software Guard Extensions
 Device" DriverVersion=1.9.103.38781
5 DriverVendor="Intel" DeviceName="Intel(R) Ethernet Connection (4) I219-
 V" DriverVersion=12.15.24.1
6 DriverVendor="Synaptics" DeviceName="Synaptics SMBus Driver"
 DriverVersion=19.3.4.219
7 DriverVendor="Intel" DeviceName="Intel(R) Display-Audio" DriverVersion
 =10.22.1.97
8 DriverVendor="Realtek Semiconductor Corp." DeviceName="Realtek High
 Definition Audio" DriverVersion=6.0.1.8551
9 DriverVendor="Intel" DeviceName="Mobile 6th/7th Generation Intel(R)
 Processor Family I/O PMC - 9D21" DriverVersion=10.1.1.38
10 DriverVendor="Synaptics" DeviceName="Synaptics Pointing Device"
 DriverVersion=19.3.4.219
11 DriverVendor="Lenovo" DeviceName="Lenovo Power Manager" DriverVersion
 =10.0.56.0
12 DriverVendor="Lenovo" DeviceName="Lenovo PM Device" DriverVersion
 =1.67.12.23
13 DriverVendor="Intel" DeviceName="Mobile 7th Generation Intel(R)
 Processor Family I/O LPC Controller (U Premium) - 9D58"
 DriverVersion=10.1.1.38
14 DriverVendor="Intel" DeviceName="Mobile 6th/7th Generation Intel(R)
 Processor Family I/O PCI Express Root Port #9 - 9D18" DriverVersion
 =10.1.1.38
15 DriverVendor="Intel" DeviceName="Intel(R) Dual Band Wireless-AC 8265"
 DriverVersion=20.70.3.3
16 DriverVendor="Intel" DeviceName="Mobile 6th/7th Generation Intel(R)
 Processor Family I/O PCI Express Root Port #3 - 9D12" DriverVersion
 =10.1.1.38
17 DriverVendor="Intel" DeviceName="Mobile 6th/7th Generation Intel(R)
 Processor Family I/O PCI Express Root Port #1 - 9D10" DriverVersion
 =10.1.1.38
18 DriverVendor="Intel" DeviceName="Intel(R) Management Engine Interface "
 DriverVersion=11.7.0.1040
19 DriverVendor="Intel" DeviceName="Mobile 6th/7th Generation Intel(R)
 Processor Family I/O Thermal subsystem - 9D31" DriverVersion
 =10.1.1.38
20 DriverVendor="SunplusIT" DeviceName="Integrated Camera" DriverVersion
 =3.5.7.4802
21 DriverVendor="Intel" DeviceName="Intel(R) Wireless Bluetooth(R)"
 DriverVersion=19.30.1648.920
22 DriverVendor="Sierra Wireless Inc." DeviceName="Sierra Wireless EM7455
 Qualcomm Snapdragon swmbbnode device 01" DriverVersion=17.3.2.9
23 DriverVendor="AlcorMicro" DeviceName="Alcor Micro USB Smart Card Reader
 " DriverVersion=1.7.45.15
24 DriverVendor="Logitech" DeviceName="Logitech USB Input Device"
 DriverVersion=1.10.78.0
25 DriverVendor="Realtek Semiconductor Corp." DeviceName="Realtek USB 3.0
```

```

 Card Reader" DriverVersion=10.0.14393.31228
26 DriverVendor="Lenovo" DeviceName="Wide viewing angle & High density
 FlexView Display 2560x1440" DriverVersion=6.3.0.0
27 DriverVendor="Intel" DeviceName="Intel(R) HD Graphics 620"
 DriverVersion=21.20.16.4590
28 DriverVendor="Intel" DeviceName="Intel(R) Xeon(R) E3 - 1200 v6/7th Gen
 Intel(R) Core(TM) Host Bridge/DRAM Registers - 5904" DriverVersion
 =10.1.1.38
29 DriverVendor="Sierra Wireless Incorporated" DeviceName="Sierra Wireless
 Location Sensor" DriverVersion=17.8.1030.33

```

## Start Collecting Data

Save the script to disk and create a new timer in uberAgent's configuration. After a service restart, uberAgent starts collecting data.

```

1 [Timer]
2 Name = PowerShell Driver Versions
3 Interval = 86400000
4 Start delay = 600000
5 Persist interval = true
6 Thread priority = background
7 Script = powershell.exe -executionpolicy bypass -file "C:\
 Program Files\vast limits\uberAgent\Scripts\Get-DriverVersions.ps1"
8 ScriptContext = Session0AsSystem

```

## Splunk it

Once the data is in Splunk you can use it to help you troubleshooting these nasty driver issues. Run the following search to list all driver versions per device:

```

1 index = `uberAgent_index` sourcetype = "\"uberAgent:Script:PowerShell
 Driver Versions\""
2 | stats
3 values(DriverVersion) as "Driver versions"
4 dc(DriverVersion) as "#Driver versions"
5 latest(DriverVendor) as Vendor
6 by DeviceName
7 | sort limit=0 Vendor
8 | table
9 Vendor
10 DeviceName
11 "Driver versions"
12 "#Driver versions"

```

| Vendor ↕   | DeviceName ↕                            | Driver versions ↕ | #Driver versions ↕ |
|------------|-----------------------------------------|-------------------|--------------------|
| AlcorMicro | Alcor Micro USB Smart Card Reader       | 1.7.45.15         | 1                  |
| Intel      | Intel(R) Display-Audio                  | 10.22.1.97        | 1                  |
| Intel      | Intel(R) Dual Band Wireless-AC 8265     | 20.70.3.3         | 1                  |
| Intel      | Intel(R) Ethernet Connection (4) I219-V | 12.15.24.1        | 1                  |
| Intel      | Intel(R) HD Graphics 620                | 21.20.16.4590     | 1                  |
| Intel      | Intel(R) Management Engine Interface    | 11.7.0.1040       | 1                  |

Note that the number of driver versions is always one as I ran this only on my laptop. The number will likely change when running the script in a corporate environment on multiple machines.

## Querying Windows Performance Counters

July 9, 2024

In addition to its built-in metrics, uberAgent can collect data from Windows performance counters.

### Configuration

As with all other uberAgent metrics, performance counters need to be associated with a timer that defines how often data is collected. Performance counter metrics can be added to an existing timer or placed in a new timer section. See the [configuration docs](#) and the [performance counter metrics documentation](#) for details.

### Example

In the following example, we configured a new timer that collects data every 60 seconds. We added two performance counters to the timer that collect .NET information for the entire machine and for a specific process (PowerShell). We also added a performance counter that collects the system's uptime. Finally, we added a performance counter that collects the handle count for every running process. The result looks like this:

```
1 [Timer]
2 Name = Performance counter timer
3 Interval = 60000
4 Perf counter = \.NET CLR Memory(_Global_)\# Gen 0 Collections
5 Perf counter = \.NET CLR Memory(powershell)\# Gen 0 Collections
6 Perf counter = \System\System Up Time
7 Perf counter = \Process(*)\Handle Count
```



## Counter Paths

Most performance counter paths have one of the following two formats:

- 1 \object(instance)\counter
- 2 \object\counter

As you can see, some counter paths have instance names (`powershell` in one of the examples above) while others do not.

See [Microsoft Docs](#) for more information.

## Wildcards

uberAgent can use the wildcard characters `*` and `?` in the instance section of performance counter paths.

## Finding Counter Paths

To find the paths for your counters you can use the following method.

Add the desired counters to Performance Monitor. Then right-click the graph section of Perfmon's window, select *Save settings as...*, save as web page (`*.html`) and locate the counter path in the HTML code. Perfmon saves the counter path in language-neutral format, which is what is uberAgent needs.

## Language-Neutral or Localized

Some tools require localized performance counter paths. This becomes a problem if you configure paths for machines with different language versions of Windows.

With uberAgent, you can configure localized or language-neutral performance counter paths. The performance counter path is always sent to the backend in English.

## Documenting Applied Computer GPOs

July 25, 2024

Managing thousands of machines is a tough job for which many organizations are using Group Policy. If you are familiar with uberAgent you may know that it lists GPOs that are applied during user logon. Computer policies, on the other hand, are not part of uberAgent's regular feature set. However, that

can easily be remedied with the help of [uberAgent's custom script functionality](#). This article shows how.

The scripts listed in this guide are managed in vast limits' public [GitHub repository](#).

## Listing Applied Machine Policies

In a nutshell, the uberAgent custom scripts feature executes any script you like and sends the output to Splunk. This works with any scripting engine, of course. In this case, we used PowerShell.

The following script lists all applied machine policies.

```
1 # We need a temporary XML file to store the data
2 $OutputFile = "C:\Windows\Temp\TempGPOExport.xml"
3
4 # If the file exists delete it
5 If (Test-Path $OutputFile)
6 {
7
8 Remove-Item $OutputFile -Force
9 }
10
11
12 # Run gpresult and store the result in the temporary xml file
13 gpresult.exe /Scope Computer /X $OutputFile /F
14
15 # Read the xml file
16 [xml]$XML = Get-Content $OutputFile
17
18 # Get the names of all GPOs
19 $GPOs = ($XML.Rsop.ComputerResults.GPO).Name | Sort-Object
20
21 # Remove the temporary file
22 Remove-Item $OutputFile -Force
23
24 # Join all GPOs to a long string
25 $GPOs = $GPOs -join ';'
26
27 # Write the output. uberAgent will pick this up.
28 Write-Output "MachineGPOs=`"$GPOs`""
```

Save the script somewhere. For this example, we save the script as C:\Program Files\vast limits\uberAgent\Scripts\Get-MachineGPOs.ps1.

## Configure uberAgent to Run the Script

Create a new timer in uberAgent's configuration. With the settings shown below, the script will be executed once per day.

```
1 [Timer]
2 Name = Get-MachineGPOs
3 Interval = 86400000
4 Start delay = 600000
5 Persist interval = true
6 Thread priority = background
7 Script = powershell.exe -executionpolicy bypass -file "C:\Program Files
 \vast limits\uberAgent\Scripts\Get-MachineGPOs.ps1"
8 ScriptContext = Session0AsSystem
```

## Splunk it

Once the data is in Splunk it can be used to document the applied computer GPOs. Run the following search to list all group policy objects per machine.

```
1 index = `uberAgent_index` sourcetype = "\"uberAgent:Script:Get-
 MachineGPOs\""
2 | stats
3 latest(MachineGPOs) as MachineGPOs
4 by host
5 | eval MachineGPOs = split(MachineGPOs,";")
6 | table
7 host
8 MachineGPOs
```

The results from the above search look like this:

| host ↕   | MachineGPOs ↕                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CTX-VDI8 | {1F8F2BE6-1307-47AC-9241-B0A12E64950E}<br>{86E5B8DF-6279-49D6-89BE-1BE5E9E34B29}<br>{E668B1EA-87E3-4E2D-83D8-FFC603DA6F7B}<br>Default Domain Policy<br>Firefox<br>IE enterprise mode<br>Stratégie de groupe locale<br>Timm_StartupDelay<br>v1 BGInfo<br>v1 Domain<br>v1 LAPS<br>v1 RDP access<br>v1 Splunk UF Config<br>v1 uberAgent - Copy custom Scripts<br>v1 uberAgent - Copy license file<br>v1 uberAgent - ns.int.vastlimits.com - http<br>v1 Update Apps<br>v1 Windows Update |

## Identifying Applications That Use 100% of a CPU Core

July 25, 2024

Some applications fully use one or multiple CPU cores, either because they are badly written or because they simply make such complex calculations. Back in the days of single-core CPUs, this was easy to detect: the machine's CPU usage would spike to 100%. Today, even lightweight laptops have at least four physical cores, workstations many more. Looking at a machine's or a process' CPU usage percentage is not enough. You need to factor in the number of CPU cores in order to determine whether one or multiple cores are fully utilized. This article explains how to do that.

uberAgent determines the number of physical and logical CPU cores as part of its [machine inventory metric](#). The resulting data is then added to all sourcetypes as additional fields during search time via automatic lookups. This means that you can use (nearly) all machine inventory fields in (nearly) all searches! The main exceptions are sourcetypes where the data does not apply to a specific endpoint, e.g., Citrix site or ADC metrics.

With that knowledge, we can build a simple search that lists processes that utilized at least a given number of CPU cores for the duration of a data collection interval (30 seconds by default):

```

1 index=`uberAgent_index` sourcetype=uberAgent:Process:ProcessDetail
 ProcCPUPercent>0
2 | eval CoresUsed = ProcCPUPercent * CPUCoresLogical / 100
3 | where CoresUsed > 0.8
4 | table _time, host, AppName, AppVersion, ProcName, CoresUsed,
 CPUCoresPhysical, CPUCoresLogical

```

In the example above, I filtered for events where one process used at least 80% of a CPU core (`where CoresUsed > 0.8`). The actual calculation of the number of cores used is simple: `CoresUsed = ProcCPUPercent * CPUCoresLogical / 100`. The last command, `table`, selects the fields to be displayed: application name, application version, process name, number of cores used, total number of physical and logical cores.

The result looks like this:

| <code>_time</code>         | <code>host</code> | <code>AppName</code> | <code>AppVersion</code> | <code>ProcName</code> | <code>Cores used</code> | <code>Physical cores</code> | <code>Logical cores</code> |
|----------------------------|-------------------|----------------------|-------------------------|-----------------------|-------------------------|-----------------------------|----------------------------|
| 2019-05-08<br>23:04:50.376 | HK87K             | Cinebench            | 20.0.4.0                | Cinebench.exe         | 1.00                    | 6                           | 12                         |
| 2019-05-08<br>23:04:20.357 | HK87K             | Cinebench            | 20.0.4.0                | Cinebench.exe         | 1.00                    | 6                           | 12                         |
| 2019-05-08<br>23:03:50.342 | HK87K             | Cinebench            | 20.0.4.0                | Cinebench.exe         | 1.10                    | 6                           | 12                         |
| 2019-05-08<br>23:02:50.307 | HK87K             | Cinebench            | 20.0.4.0                | Cinebench.exe         | 9.37                    | 6                           | 12                         |
| 2019-05-08<br>23:02:20.287 | HK87K             | Cinebench            | 20.0.4.0                | Cinebench.exe         | 11.10                   | 6                           | 12                         |

You may notice that I ran a CPU benchmark, Cinebench, to generate a high enough load. First I ran the multi-core, then the single-core benchmark. Please note that I renamed some fields to optimize formatting.

## Collecting the Processor Temperature With uberAgent

July 25, 2024

The other day a customer asked if uberAgent collects the CPU temperature. By default, it doesn't, but you can easily add the CPU temperature as a metric via uberAgent's custom script functionality. Here is how.

In a nutshell, uberAgent's custom script functionality allows you to execute arbitrary scripts whose output is sent to the backend (e.g., Splunk). [Go here](#) to get more details on the configuration.

The scripts listed in this guide are managed in vast limits' public [GitHub repository](#).

## Choose Your Preferred Data Source

The processor temperature is stored in one of these WMI objects, or both:

1. `MSAcpi_ThermalZoneTemperature`
2. `Win32_PerfFormattedData_Counters_ThermalZoneInformation`

On some test machines, the values differed between the two objects. We compared them with the values from other tools like HWInfo and found that `Win32_PerfFormattedData_Counters_ThermalZoneInformation` is the better option for our machines. That could be different for yours, though.

Either way, your machines have to support at least one of these WMI classes. If your PCs are equipped with Intel processors, they will likely do. If not, you will get the error `Get-WMIObject : Not supported` when querying WMI.

The PowerShell script gives you the temperature in Celsius, Fahrenheit, and Kelvin. Choose your preferred unit by commenting out the other unnecessary rows.

```
1 <#
2 .SYNOPSIS
3 uberAgent script to determine the current CPU temperature.
4
5 .DESCRIPTION
6 Reads the current CPU temperature from WMI and converts the resulting
7 output to the KV format required by uberAgent custom scripts.
8
9 If the default WMI class does not yield satisfactory resulty, try
10 switching to the alternative data source by commenting out the
11 relevant lines.
12
13 Most machines have multiple thermal zones. Test with your PCs and
14 enter the name of the appropriate thermal zone in the variable
15 $thermalZone.
16 To retrieve a list of all thermal zones run either of the following:
17 - Get-CimInstance -ClassName
18 Win32_PerfFormattedData_Counters_ThermalZoneInformation
19 - Get-CimInstance -ClassName MSAcpi_ThermalZoneTemperature -Namespace
20 "root/wmi"
21 #>
22
23 # Thermal zone (wildcard string)
24 $thermalZone = "*tz00*"
25
26 # Default: get the CPU temperature from the WMI class
27 Win32_PerfFormattedData_Counters_ThermalZoneInformation
28 $temp = Get-CimInstance -ClassName
29 Win32_PerfFormattedData_Counters_ThermalZoneInformation | Where-
30 Object -Property Name -like $thermalZone
31 $TempKelvin = $temp.Temperature
32
33 # Alternative: get the CPU temperature from the WMI class
34 MSAcpi_ThermalZoneTemperature
```

```
24 # Note: requires elevation (admin rights)
25 # $temp = Get-CimInstance -ClassName MSAcpi_ThermalZoneTemperature -
 Namespace "root/wmi" | Where-Object -Property InstanceName -like
 $thermalZone
26 # $TempKelvin = $temp.Temperature / 10
27
28 $TempKelvin = $temp.Temperature
29 $TempCelsius = $TempKelvin - 273.15
30 $TempFahrenheit = (9/5) * $TempCelsius + 32
31
32 $Output = @{
33
34 # delete rows which are not needed
35 'TempCelsius' = [math]::Round($TempCelsius)
36 'TempFahrenheit' = [math]::Round($TempFahrenheit)
37 'TempKelvin' = [math]::Round($TempKelvin)
38 }
39
40 Write-Output $($Output.Keys.ForEach({
41 "$_=${$Output.$_}" })
42) -join ' '
```

The output of the script looks like this: TempCelsius=65 TempFahrenheit=149 TempKelvin=338

## Configure uberAgent to Start Querying

Store your preferred script somewhere on the target machines. We went with `C:\Program Files\vast limits\uberAgent\Scripts\Get-ProcessorTemperature.ps1`.

Next step is to create a new timer in uberAgent's configuration, like this:

```
1 #####
2 # Timer 12
3 #####
4 [Timer]
5 Name = Processor temperature
6 Comment = Collect processor temperature with a custom script
7 # Run every 5 minutes
8 Interval = 300000
9 # Run the first time 10 minutes after boot to give the machine time to
 get into a normal working state
10 Start delay = 600000
11 Script = powershell.exe -executionpolicy bypass -file "C:\Program Files
 \vast limits\uberAgent\Scripts\Get-ProcessorTemperature.ps1"
12 # Run this script with system permissions
13 ScriptContext = Session0AsSystem
```

## Splunk it

Now you have the processor's temperature in Splunk and can relate it to the machine's performance.

| i               | Time                                             | Event                                                                |         |
|-----------------|--------------------------------------------------|----------------------------------------------------------------------|---------|
| ▼               | 9/3/19<br>1:21:14.206 PM                         | 1567509674206 TempCelsius="65" TempFahrenheit="149" TempKelvin="338" |         |
| Event Actions ▼ |                                                  |                                                                      |         |
| Type            | Field                                            | Value                                                                | Actions |
| Selected        | <input checked="" type="checkbox"/> host ▼       | LAPTOP-DOMINIK                                                       | ▼       |
|                 | <input checked="" type="checkbox"/> source ▼     | uberAgent                                                            | ▼       |
|                 | <input checked="" type="checkbox"/> sourcetype ▼ | "uberAgent:Script:Processor temperature"                             | ▼       |
| Event           | <input type="checkbox"/> TempCelsius ▼           | 65                                                                   | ▼       |
|                 | <input type="checkbox"/> TempFahrenheit ▼        | 149                                                                  | ▼       |
|                 | <input type="checkbox"/> TempKelvin ▼            | 338                                                                  | ▼       |
| Time            | <input type="checkbox"/> _time ▼                 | 2019-09-03T13:21:14.206+02:00                                        |         |
| Default         | <input type="checkbox"/> index ▼                 | uberagent                                                            | ▼       |
|                 | <input type="checkbox"/> linecount ▼             | 1                                                                    | ▼       |
|                 | <input type="checkbox"/> punct ▼                 | _"_="_"_="_"                                                         | ▼       |

Please note that there are more advanced technologies to get the processor temperature, like Intel DTS. But using these with PowerShell would go beyond the scope of a practice guide.

## User & Host Tagging Examples

July 9, 2024

With uberAgent 5.3 comes a very powerful and flexible tagging feature which lets you enrich uberAgent's dataset with your own custom data. While there is a [feature description](#) in the advanced topics section, we wanted to share a comprehensive list of tags you may find useful which you can copy and paste without further ado. Please read the feature description first to get the most out of the following list.

### Operating System Language

```
1 # The language the operating system was installed with
2 [UserHostTagging]
3 Tag name = Host install language
4 Tag type = Host
```



```
5 Tag source = Registry
6 Tag value = HKLM\SYSTEM\CurrentControlSet\Control\Nls\Language\
 InstallLanguage
7
8 # The default language for the operating system
9 [UserHostTagging]
10 Tag name = Host default language
11 Tag type = Host
12 Tag source = Registry
13 Tag value = HKLM\SYSTEM\CurrentControlSet\Control\Nls\Language\Default
14
15 # The user's preferred language
16 [UserHostTagging]
17 Tag name = User preferred language
18 Tag type = User
19 Tag source = Registry
20 Tag value = HKCU\Software\Microsoft\CTF\SortOrder\Language\00000000
```

### Windows 10 Version

```
1 # Windows 10 version like 1709 or 1909. More information: https://docs.microsoft.com/en-us/windows/release-information/
2 [UserHostTagging]
3 Tag name = WindowsVersion
4 Tag type = Host
5 Tag source = Registry
6 Tag value = HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ReleaseId
```

### User Name

```
1 # uberAgent collects the user name in the format domain\username. This
 tag gives you the user name without the domain.
2 [UserHostTagging]
3 Tag name = Username
4 Tag type = User
5 Tag source = Environment
6 Tag value = USERNAME
```

### User Domain

```
1 # uberAgent collects the user name in the format domain\username. This
 tag gives you the user's domain without the user name.
2 [UserHostTagging]
3 Tag name = Userdomain
4 Tag type = User
5 Tag source = Environment
6 Tag value = USERDOMAIN
```

### User Principal Name

```
1 # The user's principal name (UPN). Example: johndoe@company.com
2 [UserHostTagging]
3 Tag name = UPN
4 Tag type = User
5 Tag source = Ad
6 Tag value = userPrincipalName
```

### User Company

```
1 # The user's company. The AD attribute company has to be set for this
 to work.
2 [UserHostTagging]
3 Tag name = User company
4 Tag type = User
5 Tag source = Ad
6 Tag value = company
```

### User Department

```
1 # The user's department. The AD attribute department has to be set for
 this to work.
2 [UserHostTagging]
3 Tag name = User department
4 Tag type = User
5 Tag source = Ad
6 Tag value = department
```

### User AD Organizational Unit

```
1 [UserHostTagging]
2 Tag name = User OU
3 Tag type = User
4 Tag source = Ad
5 Tag value = distinguishedName
```

### User DNS Domain

```
1 # This gives you the user's full qualified DNS domain name
2 [UserHostTagging]
3 Tag name = User DNS domain
4 Tag type = User
5 Tag source = Environment
```

```
6 Tag value = USERDNSDOMAIN
```

## User Account Control

```
1 # Account options. 512 = activated, 514 = deactivated, 66048 = password
 never expires. More information: https://support.microsoft.com/en-
 us/help/305144/how-to-use-useraccountcontrol-to-manipulate-user-
 account-properties
2 [UserHostTagging]
3 Tag name = User account control
4 Tag type = User
5 Tag source = Ad
6 Tag value = userAccountControl
```

## Querying Windows Event Log

July 25, 2024

A question we get asked quite often is whether uberAgent is able to query Windows Event Log for specific events IDs. This functionality is not in the product, as Splunk, uberAgent's primary backend, has this [built-in](#). Hence we generally recommend making use of Splunk's capabilities.

However, not all of our customers have Universal Forwarder, Splunk's client software, deployed to their endpoints, mostly for performance reasons. If that is the case for you, too, then this practice guide should be of interest. If you do have Splunk's Universal Forwarder deployed, please use its functionality instead. UF is more efficient than the script-based solution presented in this article.

The scripts listed in this guide are managed in vast limits'public [GitHub repository](#).

### Collect Event IDs With a Custom Script

As Windows Event Log data is not part of uberAgent's default data set, we are using the agent's [custom script functionality](#).

In a nutshell, the uberAgent custom scripts feature executes any script you like and sends the output to Splunk. This works with any scripting engine, of course. In this case, we are using PowerShell.

The following script queries Event Log for a given event ID in a specific event log (Application, System, etc.). It also needs an interval in which it should search. Due to the parameters, you can use that script to query arbitrary events and don't need a new script for each. The required parameters are passed to the script through an uberAgent timer.

```
1 PARAM
2 (
3 [Parameter(Mandatory = $true)]
4 [System.Int32]$EventID,
5
6 [Parameter(Mandatory = $true)]
7 [System.String]$EventLog,
8
9 [Parameter(Mandatory = $true)]
10 [System.Int32]$IntervalMS
11)
12
13 $IntervalMS = -$IntervalMS
14
15 $StartTime=$(get-date).AddMilliseconds($IntervalMS)
16
17 $Filter= @{
18
19 LogName="$EventLog"
20 StartTime=$StartTime
21 Id=$EventID
22 }
23
24
25 $Events = Get-WinEvent -FilterHashtable $Filter -ErrorAction
26 SilentlyContinue
27
28 if (@($Events).Count -gt 0)
29 {
30 foreach ($Event in $Events)
31 {
32
33 [Hashtable]$Output = @{
34
35 'ProviderName' = "`"$($Event.ProviderName)`""
36 'Id' = $Event.id
37 'LevelDisplayName' = $Event.LevelDisplayName
38 'LogName' = $Event.LogName
39 'Message' = "`"$($Event.Message)`""
40 'TimeCreated' = "`"$($Event.TimeCreated)`""
41 'TaskDisplayName' = "`"$($Event.TaskDisplayName)`""
42 }
43
44 Write-Output $($Output.keys.foreach({
45 "$_=$($Output.$_)" })
46) -join ' '
47 }
48 }
49
50 }
```

Save the script somewhere. For this example, we save the script as `C:\Program Files\vast`

limits\uberAgent\Scripts\Get-WinEvent.ps1.

## Configure uberAgent to Run the Script

Create a new timer in uberAgent's configuration. With the settings shown below, the script will be executed every five minutes.

```

1 [Timer]
2 Name = Get-WinEvent
3 Interval = 300000
4 Script = powershell.exe -executionpolicy bypass -file "C:\
 Program Files\vast limits\uberAgent\Scripts\Get-WinEvent.ps1" -
 EventID 1000 -EventLog "Application" -IntervalMS 300000
5 ScriptContext = Session0AsSystem

```

Note that you define the parameters in the `Script` setting. The parameter `IntervalMS` should be the same number of milliseconds as the setting `Interval`.

## Splunk it

Once the data is in Splunk it can be used to search for Windows Events.

The screenshot shows the Splunk Search interface. At the top, the search bar contains the query: `index=uberagent sourcetype="uberAgent:Script:Get-WinEvent"`. Below the search bar, it indicates that 2 events were found for the time range 5/27/20 12:55:20.000 PM to 5/27/20 1:10:20.000 PM. The interface is set to 'List' view with 50 items per page. Two event results are displayed in a table format.

| i | Time                      | Event                                                                                                                                                                                                                                                                            |
|---|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| > | 5/27/20<br>1:09:48.908 PM | 1590577788908 Id=1000 Message="Faulting module: unknown" LevelDisplayName=Informationen TimeCreated="05/27/2020 13:09:47" ProviderName=Custom LogName=Application TaskDisplayName=<br>host = LAPTOP-DOMINIK   source = uberAgent  <br>sourcetype = uberAgent:Script:Get-WinEvent |
| > | 5/27/20<br>1:09:48.907 PM | 1590577788907 Id=1000 Message="Faulting module: unknown" LevelDisplayName=Informationen TimeCreated="05/27/2020 13:09:48" ProviderName=Custom LogName=Application TaskDisplayName=<br>host = LAPTOP-DOMINIK   source = uberAgent  <br>sourcetype = uberAgent:Script:Get-WinEvent |

## Collecting More WiFi Details From WFH Employees

July 25, 2024

Normally, laptop workers enjoy good quality WiFi or even a LAN network, connected through a docking station, in their company offices. Well, that changed during the Corona pandemic. The majority of employees are now working from home - connected through their personal WiFi and internet connection. That can be challenging for administrators when they have to troubleshoot a problem, as they have no insight into the quality of the employee's network.

uberAgent supports administrators already to identify if a bad network is the cause of an issue. Head over to [this blog post](#) to learn how!

One cannot have enough information when it comes to solving problems, though. Custom scripts to the rescue! This practice guide helps you with collecting even more information about WiFi connections.

The scripts listed in this guide are managed in vast limits' public [GitHub repository](#).

### Collecting WiFi Information With PowerShell

#### Data Source: Netsh Command-Line Tool

Of course, using PowerShell is the standard these days when it comes to scripting. Sadly, there is no native PowerShell cmdlet for the information we're interested in. We have to use the good old `netsh` command: `netsh wlan show interface`.

The output looks similar to the following:

```
1 There is 1 interface on the system:
2
3 Name : WLAN
4 Description : Intel(R) Dual Band Wireless-AC 8265
5 GUID : 1796b603-2174-45f7-8001-c05c4a011617
6 Physical address : ac:ed:5c:02:f0:30
7 State : connected
8 SSID : G12
9 BSSID : cc:ce:1e:2d:b0:86
10 Network type : Infrastructure
11 Radio type : 802.11n
12 Authentication : WPA2-Personal
13 Cipher : CCMP
14 Connection mode : Profile
15 Channel : 1
16 Receive rate (Mbps) : 144.4
17 Transmit rate (Mbps) : 144.4
18 Signal : 86%
```

```
19 Profile : Dominiks-WiFi
20
21 Hosted network status : Not available
```

The most interesting bits are the **signal strength**, the **receive/transmit rates**, the **radio type**, and the **authentication type**. With a little work, we can refactor that old-style text output to some useful PowerShell objects we can actually work with.

### Converting Netsh Output to PowerShell Objects (EN)

```
1 $interface = @(netsh wlan show interface)
2 $hash = $null
3
4 # We only support machines with one interface for now. The following
 line also makes sure that the scripts only proceed if a WiFi
 interface is found at all.
5 If ($interface -match 'There is 1 interface on the system')
6 {
7
8 # The following builds a hash table from the netsh output
9 foreach($item in $interface)
10 {
11
12 if($item.Contains(':'))
13 {
14
15 $hash += @{
16
17 $item.Replace(" ", "").split('{
18 : }
19 ')[0] = $item.Replace(" ", "").split('{
20 : }
21 ')[1]
22 }
23
24 }
25
26 }
27
28
29 # Only connected interfaces are interesting
30 If ($hash.State -eq 'connected')
31 {
32
33 # Get the WiFi band by looking at the used channel
34 If ([int]$hash.Channel -gt 33)
35 {
36
37 $Band = '5'
38 }
39
```

```
40 Else
41 {
42
43 $Band = '2.4'
44 }
45
46
47 # Build the output hash
48 $Output = @{
49
50 'Signal' = $hash.Signal -replace '%',''
51 'Type' = $hash.Radiotype
52 'Receiverate' = $hash.'Receiverate(Mbps)''
53 'Transmitrate' = $hash.'Transmitrate(Mbps)''
54 'Band' = $Band
55 'SSID' = "`"`${$hash.SSID}`""
56 'Authentication' = $hash.Authentication
57 'Cipher' = $hash.Cipher
58 }
59
60
61 # Finally, write the hash to stdout. The output will be picked
62 # up by uberAgent.
63 Write-Output $($Output.Keys.ForEach({
64 "$_=${$Output.$_}" })
65) -join ' '
66 }
67
68 Else
69 {
70
71 Throw "Interface `${$hash.Name}` not connected. Exiting..."
72 }
73
74 }
75
76 Else
77 {
78
79 Throw 'Zero or more than one interface on machine. Exiting...'
80 }
```

Running that script outputs the following:

```
Authentication=WPA2-Personal Transmitrate=144.4 Signal=86 Type=802.11
n SSID="Dominiks-WiFi"Cipher=CCMP Receiverate=144.4 Band=2.4
```



## Converting Netsh Output to PowerShell Objects (DE)

Unfortunately, the `netsh` output is language-specific. Hence the above script only works on **English** Windows operating systems. Below is a version for a **German** Windows, too. If you have other languages, please check the script and replace localized words according to your requirements.

```
1 $interface = @(netsh wlan show interface)
2 $hash = $null
3
4 # We only support machines with one interface for now. The following
 line also makes sure that the scripts only proceed if a WiFi
 interface is found at all.
5 If ($interface -match 'Es ist 1 Schnittstelle auf dem System vorhanden'
)
6 {
7
8 # The following builds a hash table from the netsh output
9 foreach($item in $interface)
10 {
11
12 if($item.Contains(':'))
13 {
14
15 $hash += @{
16
17 $item.Replace(" ", "").split('{
18 : }
19 ')[0] = $item.Replace(" ", "").split('{
20 : }
21 ')[1]
22 }
23
24 }
25
26 }
27
28
29 # Only connected interfaces are interesting
30 If ($hash.Status -eq 'Verbunden')
31 {
32
33 # Get the WiFi band by looking at the used channel
34 If ([int]$hash.Kanal -gt 33)
35 {
36
37 $Band = '5'
38 }
39
40 Else
41 {
42
43 $Band = '2.4'
```

```
44 }
45
46
47 # Build the output hash
48 $Output = @{
49
50 'Signal' = $hash.Signal -replace '%',''
51 'Type' = $hash.Funktyp
52 'Receiverate' = $hash.'Empfangsrate(MBit/s)'
53 'Transmitrate' = $hash.'Übertragungsrate(MBit/s)'
54 'Band' = $Band
55 'SSID' = "`"`${($hash.SSID)}`""
56 'Authentication' = $hash.Authentifizierung
57 'Cipher' = $hash.Verschlüsselung
58 }
59
60
61 # Finally, write the hash to stdout. The output will be picked
62 # up by uberAgent.
63 Write-Output $($Output.Keys.ForEach({
64 "$_=${($Output.$_)}" })
65) -join ' '
66 }
67
68 Else
69 {
70
71 Throw "Interface $($hash.Name) not connected. Exiting..."
72 }
73
74 }
75
76 Else
77 {
78
79 Throw 'Zero or more than one interface on machine. Exiting...'
80 }
```

## Start Collecting Data

Save the script to disk and create a new timer in uberAgent's configuration. After a service restart, uberAgent starts collecting data.

```
1 [Timer]
2 Name = Get-WifiInfo
3 Interval = 60000
4 Script = powershell.exe -executionpolicy bypass -file "C:\
 Program Files\vast limits\uberAgent\Scripts\Get-WifiInfo.ps1"
5 ScriptContext = Session0AsSystem
```

The interval at which the script is run in the timer configuration above is 60 seconds; adjust it to your needs as required. Just remember that the value is specified in milliseconds.

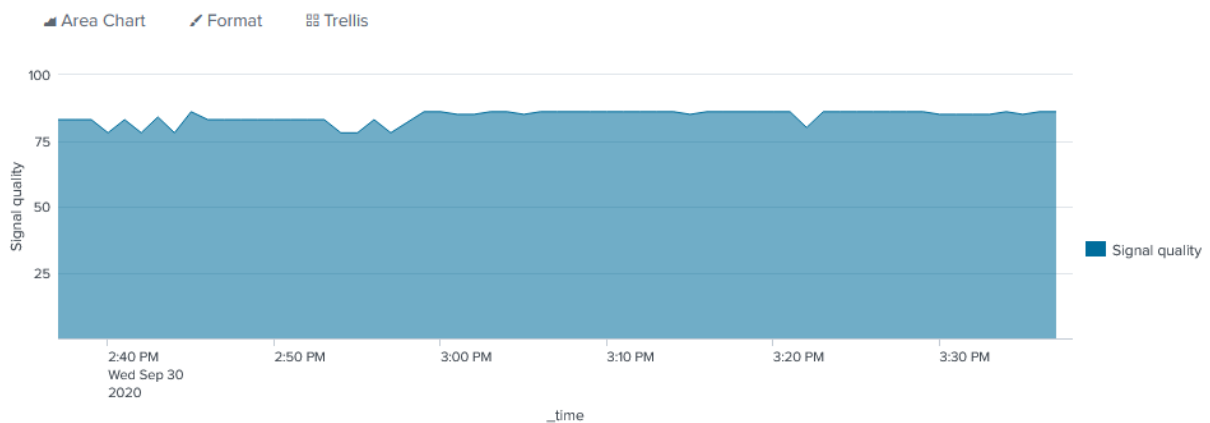
## Splunk it

Once the data is in Splunk you can use it to help you troubleshoot issues in WFH scenarios even easier.

Let's assume you get a call by a WFH user who complains about a slow application. With the following search, you can quickly check if the user's WiFi signal strength is low, causing the slowness of the application.

```
index=uberagent sourcetype="uberAgent:Script:Get-WifiInfo"host="LAPTOP-DOMINIK" | timechart latest(Signal)as "Signal quality (%)"
```

In the author's case, the signal quality looks okay, but could be better:



Signal quality is only one of the metrics we collected. Go and try one of the others for yourself!

## Monitoring Windows Update Performance

July 25, 2024

Use the Splunk search below to list the duration of Windows Update activities that are part of the machine boot process. In addition to the Windows Update processing time, the search returns the disk IO incurred by the update process.

## Why Measuring Windows Update Performance Is Crucial

A fundamental component of good endpoint management is Windows Update management. All devices must be kept up to date in order to provide as few opportunities as possible for malware to attack.

However, applying Windows updates also means stopping work for users, because typically the computer has to be restarted for this purpose. This is because Windows updates are installed during the computer startup.

Administrators are therefore keen to ensure that everything runs smoothly during the installation of updates in order to minimize the waiting time for users. So they need a way to monitor the performance of the update installation.

## How uberAgent Can Help

uberAgent provides a deep insight into the computer startup performance of Windows endpoints in the dashboard *Boot Duration*. Every computer startup is divided into phases based on the Microsoft document [Windows On/Off Transitions Solutions Guide](#). The installation of Windows updates is not a separate phase, but only a sub-phase.

Nevertheless, the installation of Windows Updates can be monitored with uberAgent, because uberAgent determines the runtime, command line and performance for each process that ran during boot.

Windows updates are installed by the *Windows Update* service. This is an instance of the `svchost.exe` process and can be identified by the following command line: `svchost.exe -k netsvcs -p -s wuauerv.`

The performance of processes at boot is best measured by the number of disk accesses (IOs). Many IOs means that the application or service has a negative impact on boot performance.

## Splunk Search

The search below returns the following results for each *Windows Update* service startup:

- The computer name
- The unique ID generated by uberAgent to analyze the complete computer startup
- The start time of the computer startup
- The duration of the *Windows Update* phase
- The percentage of the total boot time that is taken up by the *Windows Update* phase
- The total duration of the computer startup
- The number of IOs of the *Windows Update* phase

- The percentage of the *Windows Update* phase in the total IOs of the computer startup
- The total number of IOs of the computer startup

```

1 | pivot `uA_DM_OnOffTransition_BootProcesses`
 OnOffTransition_BootProcesses
2 latest(ProcLifetimeMs) as ProcLifetimeMs
3 latest(TotalBootDurationMs) as TotalBootDurationMs
4 sum(ProcIOReadCount) as SumProcIOReadCount
5 sum(ProcIOWriteCount) as SumProcIOWriteCount
6 splitrow BootUID
7 splitrow host
8 splitrow ProcCmdline
9 filter ProcCmdline is "*svchost.exe -k netsvcs -p -s wuauclt"
10 | join type=left BootUID
11 [
12 | pivot `uA_DM_OnOffTransition_BootProcesses`
 OnOffTransition_BootProcesses
13 sum(ProcIOReadCount) as SumTotalBootProcIOReadCount
14 sum(ProcIOWriteCount) as SumTotalBootProcIOWriteCount
15 splitrow BootUID
16 | fields + BootUID SumTotalBootProcIOReadCount
 SumTotalBootProcIOWriteCount
17]
18 | join type=left BootUID
19 [
20 | pivot `uA_DM_OnOffTransition_BootDetail`
 OnOffTransition_BootDetail
21 latest(_time) as BootStartTime
22 splitrow BootUID
23 | eval "Boot start time"=strfTime(strftime(BootStartTime, "%Y-%m-%dT
 %H:%M:%S.%Q%z"), "%Y-%m-%d %H:%M:%S")
24 | fields + BootUID "Boot start time"
25]
26 | eval "Applying Windows Updates duration (s)" = round(ProcLifetimeMs /
 1000,1)
27 | eval "Total boot duration (s)" = round(TotalBootDurationMs / 1000,1)
28 | eval "Windows Updates duration of total (%)" = round(ProcLifetimeMs /
 TotalBootDurationMs * 100,1)
29
30 | eval "Applying Windows Updates IO count" = SumProcIOReadCount +
 SumProcIOWriteCount
31 | eval "Total boot IOs" = SumTotalBootProcIOReadCount +
 SumTotalBootProcIOWriteCount
32 | eval "Windows Updates IOs of total (%)" = round('Applying Windows
 Updates IO count' / 'Total boot IOs',1)
33
34 | sort - "Applying Windows Updates duration (s)"
35 | table
36 host
37 "Boot start time"
38 BootUID
39 "Applying Windows Updates duration (s)"
40 "Total boot duration (s)"

```

```

41 "Windows Updates duration of total (%)"
42 "Applying Windows Updates IO count"
43 "Total boot IOs"
44 "Windows Updates IOs of total (%)"

```

## Splunk Search Result

This is what the result looks like in Splunk's UI:

| host         | Boot start time     | BootUID                              | Applying Windows Updates duration (s) | Total boot duration (s) | Windows Updates duration of total (%) | Applying Windows Updates IO count | Total boot IOs | Windows Updates IOs of total (%) |
|--------------|---------------------|--------------------------------------|---------------------------------------|-------------------------|---------------------------------------|-----------------------------------|----------------|----------------------------------|
| T145-DOMINIK | 2021-01-13 02:44:04 | 00000344-0049-004b-a3c5-f6924de9d601 | 145.3                                 | 171.2                   | 84.9                                  | 1667                              | 289953         | 0.0                              |
| HK87K        | 2021-01-13 15:31:11 | 0000014d-0037-004b-b598-41bdb8e9d601 | 134.0                                 | 150.9                   | 88.8                                  | 191                               | 363129         | 0.0                              |
| CJ580DS      | 2021-01-20 13:45:46 | 000001c1-0044-0053-55e9-3e2c2aefd601 | 118.6                                 | 138.5                   | 85.6                                  | 183                               | 236700         | 0.0                              |
| T145-DOMINIK | 2021-01-20 10:15:58 | 00000344-0049-004b-7285-0add0cef601  | 117.1                                 | 152.1                   | 77.0                                  | 0                                 | 202613         | 0.0                              |

Example result for above search

## Customize Using Filters

Above's search gives you probably a long list back. By extending the search with the following line, the output can be filtered to computer startups where the Windows Update phase exceeds a certain value in seconds.

```
| where 'Applying Windows Updates duration (s)' > 60
```

## Creating a TPM Status Inventory Report

July 25, 2024

This article shows how to collect detailed status and inventory information about each endpoint's trusted platform module (TPM). The output includes the TPM's state and version and can easily be used in Splunk reports and dashboards.

There are multiple ways to get TPM information. We chose the command-line tool `tpmtool.exe` as our data source because its output is more complete than PowerShell's `Get-Tpm` cmdlet (which lacks the TPM version).

The scripts listed in this guide are managed in vast limits' public [GitHub repository](#).

## Collecting TPM Information With PowerShell From Tpmtool

### Data Source: Tpmtool.exe

When run with the parameter `getdeviceinformation`, Tpmtool's output looks as follows

```
1 -TPM Present: True
2 -TPM Version: 2.0
3 -TPM Manufacturer ID: INTC
4 -TPM Manufacturer Full Name: Intel
5 -TPM Manufacturer Version: 302.12.0.0
6 -PPI Version: 1.3
7 -Is Initialized: True
8 -Ready For Storage: True
9 -Ready For Attestation: True
10 -Is Capable For Attestation: True
11 -Clear Needed To Recover: False
12 -Clear Possible: True
13 -TPM Has Vulnerable Firmware: False
14 -PCR7 Binding State: 0
15 -Maintenance Task Complete: True
16 -TPM Spec Version: 1.16
17 -TPM Errata Date: Wednesday, September 21, 2016
18 -PC Client Version: 1.00
19 -Is Locked Out: False
```

### Converting Tpmtool's Output to a Key Value String

We'll use the following PowerShell script to execute `tpmtool` and convert its output to the KV string format required by uberAgent custom scripts:

```
1 <#
2 .SYNOPSIS
3 uberAgent script to collect TPM status information.
4
5 .DESCRIPTION
6 Runs the command "tpmtool.exe getdeviceinformation" and converts the
7 output to the KV format required by uberAgent custom scripts.
8
9 #>
10 # Run tpmtool
11 $tpmtoolOutput = @(tpmtool getdeviceinformation)
12
13 # We'll store the output fields here
14 $output = @{
15 }
16
17 foreach ($line in $tpmtoolOutput)
18 {
```

```
19
20 # Ignore empty lines
21 if (!$line) {
22 continue }
23
24
25 # Remove the leading dash
26 $line = $line -replace "^-", ""
27
28 # Split at the colon
29 $kv = $line.Split(":")
30
31 if ($kv.Count -ne 2) {
32 continue }
33
34
35 # Remove the leading space in the value
36 $kv[1] = $kv[1] -replace "^\s+", ""
37
38 # Ignore certain fields
39 if ($kv[0] -like "*spec version*" -or $kv[0] -like "*errata date*")
40 {
41 continue }
42
43 # Remove spaces in the key name
44 $kv[0] = $kv[0] -replace "\s+", ""
45
46 # Add the field to the output hashtable
47 $output.Add($kv[0], "`"$($kv[1])`"")
48 }
49
50
51 # Write the KV output to the console so uberAgent can pick it up
52 Write-Output $($output.Keys.Each({
53 "$_=$($output[$_]" })
54) -join ' ')
```

The script's output looks like this:

```
1 ReadyForAttestation="True" ClearNeededToRecover="False" TPMVersion="2.0
 TPMManufacturerVersion="302.12.0.0" IsInitialized="True"
 ReadyForStorage="True" PPIVersion="1.3" PCR7BindingState="0"
 TPMManufacturerFullName="Intel" TPMManufacturerID="INTC" IsLockedOut
 ="False" PCClientVersion="1.00" ClearPossible="True" TPMPresent="
 True" MaintenanceTaskComplete="True" IsCapableForAttestation="True"
 TPMHasVulnerableFirmware="False"
```



## Configuring uberAgent to Run the Script

Deploy the script to any directory on your endpoints. In this example, we're storing it in `C:\Program Files\vast limits\uberAgent\scripts` as `Get-TpmtoolAsKv.ps1`.

Create a new timer in uberAgent's [configuration](#). With the settings shown below, the script is executed five minutes after uberAgent is started and then once every 24 hours.

```
1 [Timer]
2 Name = TPMStatusInventory
3 Interval = 86400000
4 Start delay = 300000
5 Persist interval = true
6 Script = powershell.exe -executionpolicy bypass -file "C:\
 Program Files\vast limits\uberAgent\Scripts\Get-TpmtoolAsKv.ps1"
7 ScriptContext = Session0AsSystem
```

Restart the agent to start collecting data.

## Splunk It

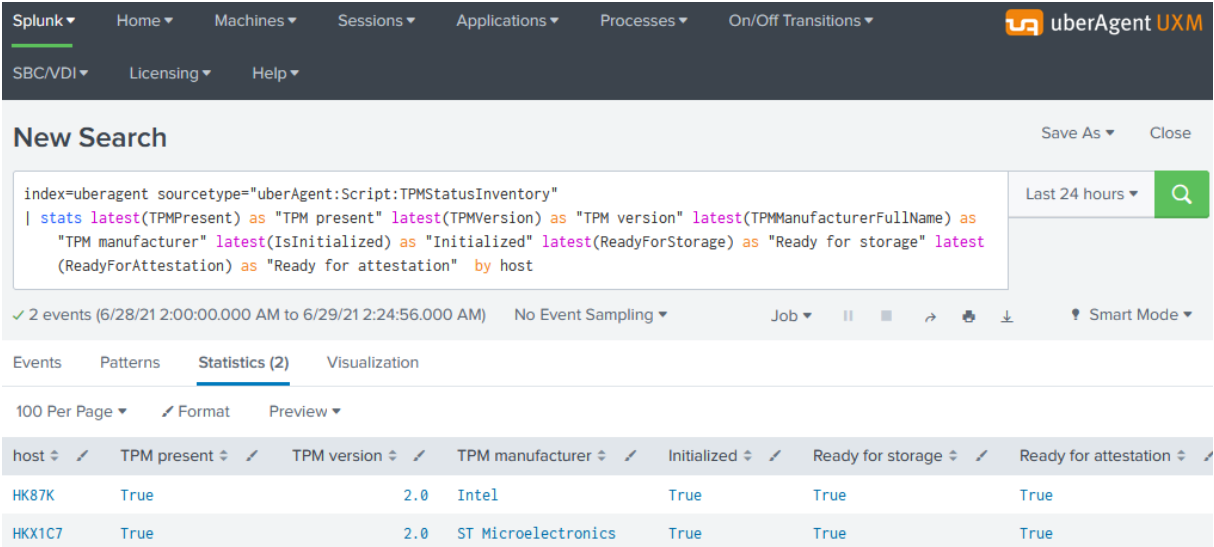
Once the data is in Splunk, you can list the incoming event data as follows

```
1 index=uberagent sourcetype="uberAgent:Script:TPMStatusInventory"
```

To generate a report, use a Splunk search like the following:

```
1 index=uberagent sourcetype="uberAgent:Script:TPMStatusInventory"
2 | stats latest(TPMPresent) as "TPM present" latest(TPMVersion) as "TPM
 version" latest(TPMManufacturerFullName) as "TPM manufacturer"
 latest(IsInitialized) as "Initialized" latest(ReadyForStorage) as "
 Ready for storage" latest(ReadyForAttestation) as "Ready for
 attestation" by host
```

The above Splunk search creates a table with the latest TPM status per endpoint (host in Splunk terminology):



The screenshot shows the Splunk interface for a search titled "New Search". The search query is: `index=uberagent sourcetype="uberAgent:Script:TPMStatusInventory" | stats latest(TPMPresent) as "TPM present" latest(TPMVersion) as "TPM version" latest(TPMManufacturerFullName) as "TPM manufacturer" latest(IsInitialized) as "Initialized" latest(ReadyForStorage) as "Ready for storage" latest(ReadyForAttestation) as "Ready for attestation" by host`. The search results show 2 events from 6/28/21 2:00:00.000 AM to 6/29/21 2:24:56.000 AM. The results table is as follows:

| host   | TPM present | TPM version | TPM manufacturer    | Initialized | Ready for storage | Ready for attestation |
|--------|-------------|-------------|---------------------|-------------|-------------------|-----------------------|
| HK87K  | True        | 2.0         | Intel               | True        | True              | True                  |
| HKX1C7 | True        | 2.0         | ST Microelectronics | True        | True              | True                  |

## Building a Browser Extension Inventory Report (Chrome/Edge/Firefox)

July 30, 2024

This article shows how to collect detailed inventory information about all installed browser extensions. The solution presented includes a Splunk dashboard that visualizes the collected data.

The scripts listed in this guide are managed in vast limits' public [GitHub repository](#).

### Solution Brief: Browser Extension Inventory

1. Extensions and metadata are stored in **browser profiles**.
2. A **PowerShell script** extracts extension info from browser profiles. The script inspects all browser profiles in the current user's Windows user profile.
3. The script is executed by **uberAgent** for each user logged on to the endpoint. The script's output is captured by uberAgent and forwarded to the (Splunk) backend.
4. A **Splunk dashboard** visualizes the collected data.

### Background Information

#### Listing Chrome Profiles

#### Getting the Location of the User Data Directory

- Default location on Windows: `%LocalAppData%\Google\Chrome\User Data`
- [Documentation](#)

### Parsing the JSON file 'Local State'to Find Profile Directories

1. Profile objects are children of the following: `profile > info_cache`
2. Profile properties related to the user:
  - `gaia_given_name`
  - `gaia_id`
  - `gaia_name`
  - `name`
  - `shortcut_name`
  - `user_name`
3. Profile names
  - Default profile: `Default`
  - Additional profiles: `Profile`
4. Locating profile directories
  - Profile directories are subdirectories of the user data directory
  - Names of profile directories are identical to profile names

### Listing Edge Profiles

#### Getting the Location of the User Data Directory

- Default location on Windows: `%LocalAppData%\Microsoft\Edge\User Data`
- Everything else is identical to Chrome

#### Collecting Chrome Extension Inventory Data

**'Preferences'vs. 'Secure Preferences'** Extensions are listed in one of two possible JSON files located in the profile directory: `Preferences` or `Secure Preferences`. The script checks both.

*Note:* `Secure Preferences` is typically used instead of the `Preferences` file.

**Extension Settings** Extension settings are children of the following: `extensions > settings > <extension ID>`.

Relevant settings for inventory purposes include:

- `from_webstore`: was the extension installed from the Chrome Web Store?
- `install_time`: timestamp of the last update (format: FILETIME / 10 [= microseconds since Jan 1st 1601])

- **path**: extension path, either absolute or relative to the profile subdirectory `Extensions`
- **location**: 1 = user data subdirectory `Extensions`, 5 = Chrome installation directory
- **state**: 1 = enabled
- **was\_installed\_by\_default**: [part of Chrome, not removable?]
- **version**: extension version

## Collecting Firefox Extension Inventory Data

### Getting the Location of the Profile Directory

- Default location on Windows: `%AppData%\Mozilla\Firefox\Profiles`

**Extension Settings** The configuration of Firefox extensions is stored in each profile's `extensions.json` file. Within that file, extension settings are children of: `addons`.

Relevant settings for inventory purposes include:

- **sourceURI**: installation source (Firefox Addons or a different site?)
- **updateDate**: timestamp of the last update (format: Unix epoch in ms)
- **location**: `app-profile` = browser profile
- **active**: **true** = enabled
- **version**: extension version

## Configuring uberAgent to Run the Inventory Script

Note: you can find the latest version of the script in vast limits' public [GitHub repository](#).

1. Store the script file in `C:\Program Files\vast limits\uberAgent\scripts` as `Get-BrowserExtensionInfo.ps1`.
2. Create a new timer in uberAgent's [configuration](#). With the settings shown below, the script is executed in each user session five minutes after uberAgent is started. The script execution is repeated every 24 hours.

```
1 [Timer]
2 Name = BrowserExtensionInventory
3 Interval = 86400000
4 Start delay = 300000
5 Persist interval = true
6 Script = powershell.exe -executionpolicy bypass -file "C:\
 Program Files\vast limits\uberAgent\Scripts\Get-BrowserExtensionInfo
 .ps1"
7 ScriptContext = UserSessionAsUser
```

Restart the agent to start collecting data.

## Script Output

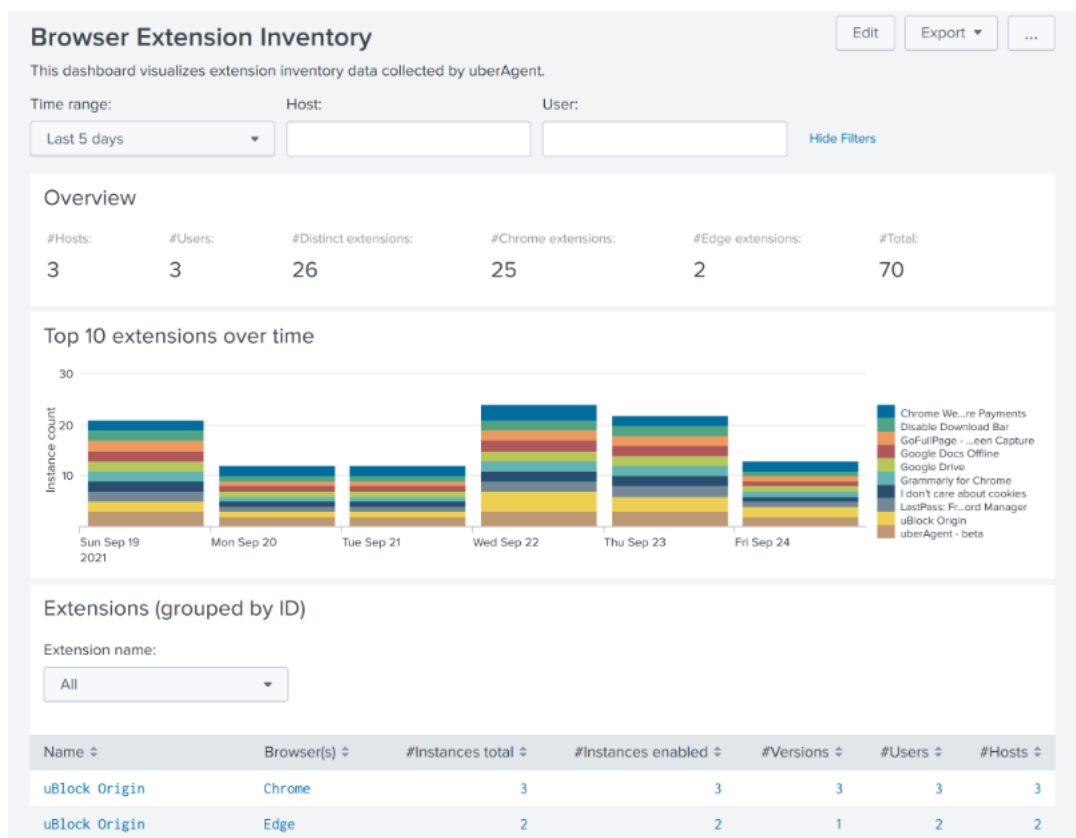
The output from the inventory script looks like this:

```
1 OsUser="helge" Browser="Chrome" ProfileDir="Default" ProfileName="
 Person 1" ProfileGaiaName="Helge Klein" ProfileUserName="
 email@domain.com" ExtensionId="cmcmenehclgdcclmnladhikmclbkb"
 ExtensionName="uberAgent" ExtensionVersion="3.0.6"
 ExtensionFromWebstore="True" ExtensionState="1" ExtensionInstallTime
 ="1606912508508" ExtensionInstalledByDefault="False"
```

## Splunk Dashboard

Once inventory data is sent from endpoints with uberAgent to Splunk, install the Splunk app that is part of this practice guide. You can find it in this guide’s [GitHub repository](#) or in [Splunkbase](#).

The dashboard provides a timeline of the top 10 extensions along with a data table listing all browser extensions. Selecting an extension’s row in the table brings up additional charts and tables that list all extension instances in full detail.



## Internet Explorer: Distinguish Standalone and Edge IE Mode Starts

July 25, 2024

Internet Explorer has been with us for many years as the ever-present browser. Most people will agree that the relationship is quite ambivalent. Especially in the corporate world, Internet Explorer was and still is deeply rooted. Many companies have applications in use that were not only developed on the basis of Internet Explorer but would not work at all without it.

### Background Information

#### End-of-Life for Internet Explorer Announced

As you may have noticed, Microsoft has [announced](#) that the Internet Explorer 11 desktop application will be retired and go out of support on June 15, 2022. The challenge is to identify the dependencies of existing web applications on Internet Explorer and, perhaps more importantly, which of these applications are actually still being used.

#### Capture Internet Explorer Starts: Standalone & Edge IE Mode

Typically, two scenarios are of interest. Either the user launches Internet Explorer, `iexplore.exe`, directly, or a website is launched within Microsoft Edge in *Internet Explorer mode*. We would like to be able to capture both and distinguish between them.

To do so, the command line of the process contains the necessary information. To get a better understanding, let us compare a direct Internet Explorer startup vs. one coming from Edge IE mode.

**Standalone Internet Explorer Start** When Internet Explorer is launched as a standalone application, the command line looks as follows:

```
"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE"SCODEF:6456
CREDAT:9730 /prefetch:2
```

**Internet Explorer Started in Edge IE Mode** In Edge IE mode, the command line of the embedded Internet Explorer executable looks as follows:

```
"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE"SCODEF:11244
CREDAT:75266 APPID:MSEdge /prefetch:2
```

As you can see, the additional parameter `APPID:MSEdge` can be used to distinguish between standalone IE and Edge IE mode.

## Configuration Instructions

### Activate uberAgent Feature: EnableExtendedInfo

uberAgent does not send the command line to the backend by default. The reason behind this is that we want to keep the generated data volume as low as possible (more information about managing the data volume can be found [here](#)). However, for this scenario, the command line is required. Activate `EnableExtendedInfo` via `uberAgent.conf` as shown below.

```
1 # Setting name: EnableExtendedInfo
2 # Description: Send detailed information about each started process
 to the backend, e.g. path, command line, process ID, parent ID. This
 also enables the population of the ProcGUID field in other
 sourcetypes, which can be used for detailed process instance
 tracking.
3 # Valid values: true | false
4 # Default: false
5 # Required: no
6
7 [ProcessStartupSettings]
8 EnableExtendedInfo = true
```

### Configure uberAgent Feature: Event Data Filtering

uberAgent provides a feature called Event Data Filtering. It is a powerful filtering mechanism for the collected data that operates right on the endpoint. Please learn more about it in our [documentation](#).

For this use scenario, Event Data Filtering allows us to reduce the additional data volume generated by activating by `EnableExtendedInfo` to an absolute minimum. Specifically, we only need the command line for the process `iexplore.exe` in the sourcetypes `uberAgent:Process:ProcessDetail` and `uberAgent:Process:ProcessStartup`.

Since the only extra fields of interest are `ProcID`, `ProcGUID` and `ProcCmdLine`, everything else that is not needed can be removed. Please find the example configuration below. Save the content as `uberAgent-eventdata-filter-vastlimits-Internet-Explorer.conf` and place that file in the same directory as `uberagent.conf`.

```
1 [EventDataFilter]
2 # Unnecessary for this use case.
3 Action = clear
4 Sourcetype = Process:ProcessDetail
5 Field = ProcGUID
6 Query = true
7
8 [EventDataFilter]
9 # Unnecessary for any other process than iexplore.exe.
```

```
10 Action = clear
11 Sourcetype = Process:ProcessStartup
12 Field = ProcID
13 Field = ProcParentID
14 Field = SessionID
15 Field = ProcGUID
16 Field = SessionGUID
17 Field = ProcParentName
18 Field = ProcPath
19 Field = ProcCmdline
20 Field = ProcParentGUID
21 Query = ProcName != "iexplore.exe"
22
23 [EventDataFilter]
24 # Remove unnecessary fields for iexplore.exe itself.
25 Action = clear
26 Sourcetype = Process:ProcessStartup
27 Field = ProcParentID
28 Field = SessionID
29 Field = SessionGUID
30 Field = ProcParentName
31 Field = ProcPath
32 Field = ProcParentGUID
33 Query = ProcName == "iexplore.exe"
```

Include the new configuration file by using the `@ConfigInclude` directive below. A good place for the include directive is in `uberAgent-eventdata-filter.conf` which also resides in the same directory as `uberAgent.conf`. Find out more about configuration file locations [here](#).

```
1 # Additional fields for Internet Explorer analysis (requires
 EnableExtendedInfo to be enabled)
2 @ConfigInclude uberAgent-eventdata-filter-vastlimits-Internet-Explorer.
 conf platform=Windows
```

Finally, restart uberAgent with the new configuration in place and head over to Splunk.


## Verify Configuration

To prove our newly configured event data filtering works as expected, run the search below which highlights two raw events in Splunk. One for `iexplore.exe` and another one for `chrome.exe`. You can clearly see the difference in populated fields.



**New Search** Save As ▾ Create Table View Close

```
index='uberAgent_index' sourcetype="uberAgent:Process:ProcessStartup" ProcName=iexplore.exe OR ProcName=chrome.exe
| stats latest(_raw) by ProcName
| rename ProcName as "Process Name" latest(_raw) as "Raw event"
```

Last 15 minutes ▾ 

✓ 37 events (28/09/2021 10:49:01.000 to 28/09/2021 11:04:01.000) No Event Sampling ▾ Job ▾ || ▢ → 🗑️ ⬇️ 🔊 Verbose Mode ▾

Events (37) Patterns **Statistics (2)** Visualization

100 Per Page ▾ Format Preview ▾

| Process Name ↕ | Raw event ↕                                                                                                                                                                                                                            |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| iexplore.exe   | 1632819172370,iexplore.exe,"MK-WIN10\\martin",3744,0.8,IntrntExplrr,548,,9b3158b4-78c1-0224-0009-354437c80f04,,,"C:\\Program Files\\Internet Explorer\\iexplore.exe\" SCODEF:4872 CREDAT:9474 /prefetch:2",0,11.789.19041.0,,,,,0,,,,, |
| chrome.exe     | 1632819305447,chrome.exe,"MK-WIN10\\martin",72,0,GglChrm,,,,,,,,,0,93.0.4577.82,,,,,0,,,,,                                                                                                                                             |

## Splunk it

Once the data is available in Splunk, it can be used to search for every direct or indirect Internet Explorer start, for every user on every host. In order to get the information about the actual web applications being used, the uberAgent browser add-on for Internet Explorer is required ([documentation](#)). This information is only available for direct Internet Explorer starts though, because of Microsoft Edge/Chromium API limitations.

## The Search

```
1 | pivot `uA_DM_Process_ProcessStartup` Process_ProcessStartup
2 latest(AppName) as "App name"
3 latest(AppVersion) as "App version"
4 latest(_time) as StartTime
5 latest(ProcCmdline) as "Process Commandline"
6 latest(ProcID) as ProcID
7 filter host in ("*")
8 filter ProcName is "iexplore.exe"
9 splitrow ProcGUID
10 splitrow host as Host
11 splitrow ProcUser as "User name"
12 | join type=left Host, ProcID
13 [
14 | pivot `uA_DM_Application_BrowserPerformanceIE`
15 Application_BrowserPerformanceIE
16 values(URL)
17 splitrow host as Host
18 splitrow ProcID
19 | fields + *
20]
21 | eval "Start time" = strftime (strftime (StartTime, "%Y-%m-%dT%H:%M:%S.%Q%z"), "%Y-%m-%d %H:%M:%S")
```

```

21 | eval "Started via Microsoft Edge"=if(like('Process Commandline', "%
 APPID:MSEdge%"), "Yes", "No")
22 | eval "Web App (direct Internet Explorer starts only)"=nullif('values(
 URL)', "none")
23 | sort - "Start time"
24 | table "Start time", Host, "User name", "App name", "App version", "
 Started via Microsoft Edge", "Web App (direct Internet Explorer
 starts only)"

```

## The Results

The resulting table shows for each instance of `iexplore.exe` whether it was launched standalone or via Edge IE mode (column "Started via Microsoft Edge"). For standalone IE processes that are used to rendering a web page, the URL is displayed, too.

| Start time          | Host     | User name       | App name          | App version    | Started via Microsoft Edge | Web App (direct Internet Explorer starts only) |
|---------------------|----------|-----------------|-------------------|----------------|----------------------------|------------------------------------------------|
| 2021-09-28 11:28:55 | MK-WIN10 | MK-WIN10\martin | Internet Explorer | 11.789.19041.0 | No                         |                                                |
| 2021-09-28 11:28:55 | MK-WIN10 | MK-WIN10\martin | Internet Explorer | 11.789.19041.0 | No                         | https://helgeklein.com/                        |
| 2021-09-28 11:26:09 | MK-WIN10 | MK-WIN10\martin | Internet Explorer | 11.789.19041.0 | No                         |                                                |
| 2021-09-28 11:26:09 | MK-WIN10 | MK-WIN10\martin | Internet Explorer | 11.789.19041.0 | No                         | https://vastlimits.com/                        |
| 2021-09-28 11:25:14 | MK-WIN10 | MK-WIN10\martin | Internet Explorer | 11.789.19041.0 | Yes                        |                                                |
| 2021-09-28 11:25:13 | MK-WIN10 | MK-WIN10\martin | Internet Explorer | 11.789.19041.0 | Yes                        |                                                |

## Testing the Azure AD (Entra ID) Join Status

July 25, 2024

This article shows how to test each endpoint's Azure AD (aka Entra ID) join status. The output can easily be used in Splunk reports and dashboards.

Machines do not always register smoothly with Azure AD. This is especially true for customers with non-persistent virtual desktops, as these types of machines must re-register with Azure AD each time they start. The script presented in this guide helps with troubleshooting by making the registration state available in Splunk.

**Note:** The script(s) listed in this guide are managed in vast limits' public [GitHub repository](#).

### Collecting AAD Join Status With PowerShell From Dsregcmd

#### Data Source: Dsregcmd.exe

When run with the parameter `Status`, `Dsregcmd`'s outputs a lot of information. Below is the output cropped to the data we are interested in:

```
1 +-----+
2 | Device State
3 +-----+
4
5 AzureAdJoined : YES
6 EnterpriseJoined : NO
7 DomainJoined : NO
8 Virtual Desktop : NOT SET
9 Device Name : MACHINE1
10 ...
```

### Converting Dsregcmd's Output to a Key-Value String

We'll use the following PowerShell script to execute `Dsregcmd` and convert its output to the KV string format required by uberAgent custom scripts:

```
1 function Test-AzureAdJoined {
2
3 $output = & dsregcmd /status
4
5 # Check if the output contains "AzureAdJoined : YES"
6 return $output -match "AzureAdJoined\s+:\s+YES"
7 }
8
9
10 $AzureAdJoined = 0
11
12 $joinedToAzureAd = Test-AzureAdJoined
13
14 if ($joinedToAzureAd) {
15 $AzureAdJoined = 1
16 }
17
18
19
20 # Build the output hash
21 $Output = @{
22
23 'AzureAdJoined' = $AzureAdJoined
24 }
25
26
27 # Finally, write the hash to stdout. The output will be picked up by
28 uberAgent.
29 Write-Output $($Output.Keys.ForEach({
30 "$_=${$Output.$_}" })
31) -join ' '
```

The script's output looks like this:

```
1 AzureAdJoined=1
```

## Configuring uberAgent to Run the Script

Deploy the script to a directory on your endpoints. In this example, we're storing it in `C:\Program Files\vast limits\uberAgent\scripts` as `Get-AzureAdJoinStatus.ps1`.

Create a new timer in uberAgent's [configuration](#). With the settings shown below, the script is executed one hour after uberAgent is started to give the registration process enough time, and then once every 24 hours.

```
1 [Timer]
2 Name = AzureAdJoinStatus
3 Interval = 86400000
4 Start delay = 3600000
5 Persist interval = true
6 Script = powershell.exe -executionpolicy bypass -file "C:\
 Program Files\vast limits\uberAgent\Scripts\Get-AzureAdJoinStatus.
 ps1"
7 ScriptContext = Session0AsSystem
```

Restart the agent to start collecting data.

## Splunk It

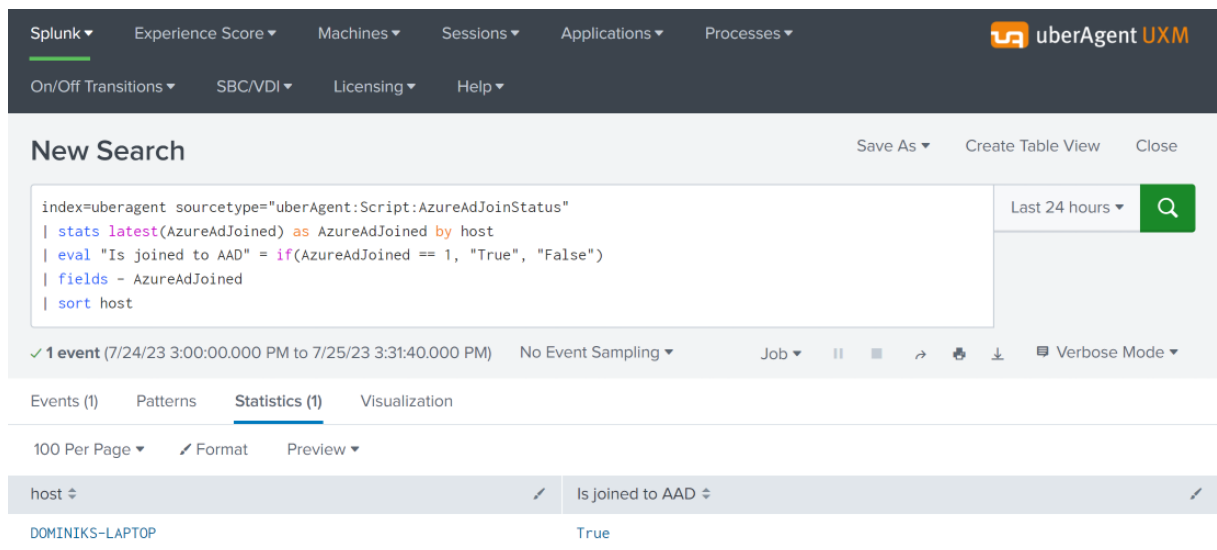
Once the data is in Splunk, you can list the incoming event data as follows:

```
1 index=uberagent sourcetype="uberAgent:Script:AzureAdJoinStatus"
```

To generate a report, use a Splunk search like the following:

```
1 index=uberagent sourcetype="uberAgent:Script:AzureAdJoinStatus"
2 | stats latest(AzureAdJoined) as AzureAdJoined by host
3 | eval "Is joined to AAD" = if(AzureAdJoined == 1, "True", "False")
4 | fields - AzureAdJoined
5 | sort host
```

The above Splunk search creates a table with the latest AAD join status per endpoint (host in Splunk terminology):



## Addons and Tools

July 25, 2024

### uberAgent Helpdesk Splunk App

[uberAgent Helpdesk](#) is a Splunk app for IT professionals who support virtual or physical desktops and who need to resolve issues quickly. This app provides a different view of the existing uberAgent dataset that is streamlined for helpdesk use.

### uberAgent Event Generator

The [event generator](#) is the perfect tool for uberAgent product demonstrations. It simulates a large number of endpoints and generates data for all dashboards.

### uberAgent Log Collector Splunk App

[uberAgent Log Collector](#) helps you monitor the health of your uberAgent deployment by collecting the data logged by uberAgent and sending it to Splunk for indexing. Dashboards provide easy access.

### uberAgent Logfile Syntax Highlighter for Notepad++

This [syntax highlighter](#) makes uberAgent log files easier to read in Notepad++.

## uberAgent Event Generator for Splunk

July 25, 2024

The uberAgent Event Generator is a powerful tool designed for product demonstrations of uberAgent. It simulates a large number of endpoints and generates data for all dashboards, allowing you to showcase the full capabilities of uberAgent without the need for a complex setup.

### Features

- Simulates multiple endpoints
- Generates data for all uberAgent dashboards
- Perfect for product demonstrations and testing

### Quick Links

- [Changelog and Release Notes](#)
- [Quickstart Guide](#)

### Getting Started

To get started with the uberAgent Event Generator:

1. Download the Event Generator from the [uberAgent website](#)
2. Install the Event Generator on your Splunk instance
3. Access your uberAgent Splunk dashboards to see the simulated data

For more detailed instructions, please refer to our [Quickstart Guide](#).

### Related Tools

- [uberAgent Helpdesk Splunk App](#)
- [uberAgent Log Collector Splunk App](#)

For a complete list of uberAgent addons and tools, visit our [Addons and Tools](#) page.

## Changelog and Release Notes

July 25, 2024

## Version 7.1

### Release notes

- Increased .NET version to 7.
- Changed configuration file format to JSON.

### Improvements

- Log messages are written to stdout and a log file located in the %TEMP% (Windows) or /tmp (Linux) directory.
- The fields `SessionFgBrowserType`, `SessionFgBrowserType` and `SessionFgBrowserActiveT` of sourcetype `uberAgent:Session:SessionDetail` are now available on macOS, too.

### New Sourcetypes

- New sourcetype `uberAgentESA:System:SecurityInventory` with fields: `SecurityInventoryC`, `SecurityInventoryName`, `SecurityInventoryScore`, `SecurityInventoryRiskScore`, `SecurityInventoryResultData`, `SecurityInventoryErrorCode`, `SecurityInventoryEr`, `SecurityInventoryScope`, `SecurityInventoryScopeEntity`.

### Updated Sourcetypes

- **Sourcetype [B287]:** `uberAgent:Process:ProcessStatistics` has new field(s): `ProcInputDelayMaxMs`, `ProcInputDelaySumMs` and `ProcInputDelayCount`.
- **Sourcetype [B287]:** `uberAgent:Session:SessionDetail` has new field(s): `SessionInputDelay`, `SessionInputDelaySumMs` and `SessionInputDelayCount`.
- **Sourcetype [B751]:** `uberAgent:OnOffTransition:BootDetail2` has new field(s): `UserLogonWaitDurationMs`.
- **Sourcetype [B766]:** `uberAgentESA:Process:DnsQuery` has new field(s): `DnsRisk52Chars`, `DnsRisk27UniqueChars`, `DnsRiskEmptyResponse`, `DnsRiskTXTRecord`, `DnsRiskHighEntropy`, `DnsResponseStatus`.

## Version 7.0

### Release notes

- macOS client machines are now supported.

## Improvements

- Machines get their IP addresses once and they do not change.
- Machines get their disk volumes only once and they do not change during their lifetime.
- A random in-session process needs a long time to start.
- Application UI delay events can now only be generated by processes started during a session.
- WiFi data is now sent only for WiFi adapters.
- BSODs are now sent less frequently.

## New Sourcetypes

- **Sourcetype:** new sourcetype `uberAgent:CitrixSession:VirtualChannelDetail` with fields: `SessionGUID`, `SessionUser`, `VirtualChannelVendorName`, `VirtualChannelData`, `VirtualChannelDataVolumeOutputMB`.
- **Sourcetype:** new sourcetype `uberAgent:CitrixSession:SessionConfig` with fields: `SessionGUID`, `SessionUser`, `AudioActualPriority`, `AudioPolicyAllowMicrophoneRedirection`, `AudioPolicyAllowRedirection`, `AudioPolicyPriority`, `AudioPolicySoundQuality`, `CdmActualPriority`, `CdmVolumes`, `CdmPolicyAllowDriveRedirection`, `CdmPolicyPriority`, `CdmPolicyReadOnly`, `DisplayMode`, `ThinwireActualPriority`, `ThinwireColorDepth`, `ThinwireComponentEncoder`, `ThinwireHardwareEncodeInUse`, `ThinwireVideoCodecType`, `ThinwireColorspace`, `ThinwireVideoCodecUse`, `ThinwirePolicyFps`, `ThinwirePolicyPriority`, `ThinwirePolicyUseHardwareEncoding`, `ThinwirePolicyUseVideoCodec`, `ThinwirePolicyVisualQuality`, `FramehawkActualPriority`, `FramehawkPolicyPriority`, `D3DActualPriority`, `D3DPolicyAeroRedirection`, `D3DPolicyGraphicsQuality`, `D3DPolicyPriority`, `GraphicsActualPriority`, `GraphicsPolicyDisplayDegradeNotifyUser`, `GraphicsPolicyDisplayDegradePolicy`, `GraphicsPolicyPriority`, `NetworkConnectedVia`, `NetworkEdtMtu`, `NetworkPolicyAcceptance`, `NetworkPolicyICAListenerPortNumber`, `NetworkPolicySessionReliabilityPort`, `NetworkPolicySessionReliabilityTimeout`, `PrinterActualPriority`, `PrinterSessionPrinter`, `PrinterPolicyAllowRedirection`, `PrinterPolicyAutoCreate`, `PrinterPolicyPriority`, `USBActualPriority`, `USBPolicyAllowPNPRedirection`, `USBPolicyAllowUSBSupport`, `USBPolicyPriority`.
- **Sourcetype:** new sourcetype `uberAgent:Process:ProcessStatistics` with fields: `ProcHandleCount`, `ProcThreadCount`, `ProcPriority`, `ProcPrivateMB`, `ProcVirtualSizeMB`, `ProcPageFaultsPS`, `ProcPageFileMB`, `ProcName`, `ProcID`, `ProcGUID`, `ProcUser` and `AppId`.
- **Sourcetype:** new sourcetype `uberAgent:System:PerformanceCounter` with fields: `PerformanceCounterObject`, `PerformanceCounterInstance`, `PerformanceCounterName`, `PerformanceCounterValue`.



### Updated Sourcetypes

- **Sourcetype:** `uberAgent:Application:NetworkConnectFailure` has new field(s): `NetTargetSourcePort`.
- **Sourcetype:** `uberAgent:System:MachineInventory` has new field(s): `HwHypervisorVendor`.
- **Sourcetype:** `uberAgent:Session:SessionDetail` has new field(s): `SessionRoundTripTimeMs`, `SessionFps`, `SessionTransportProtocols`.
- **Sourcetype:** `uberAgent:Citrix:Applications` has new field(s): `CustomerId`.
- **Sourcetype:** `uberAgent:Citrix:Catalogs` has new field(s): `CustomerId`.
- **Sourcetype:** `uberAgent:Citrix:DesktopGroups` has new field(s): `CustomerId`.
- **Sourcetype:** `uberAgent:Citrix:Machines` has new field(s): `CustomerId`.
- **Sourcetype:** `uberAgent:Citrix:PublishedDesktops` has new field(s): `CustomerId`.
- **Sourcetype:** replaced KV sourcetype `uberAgent:PerformanceCounter:<TimerName>` with CSV sourcetype `uberAgent:System:PerformanceCounter`.
- **Sourcetype:** `uberAgent:Application:ApplicationUsage` has been removed (it was marked as deprecated as of version 6.1.1).

### Version 6.2.0

#### Updated Sourcetypes

- **Sourcetype:** `uberAgent:Application:NetworkConnectFailure` has new field(s): `NetTargetSourcePort`.
- **Sourcetype:** `uberAgent:Process:NetworkTargetPerformance` has new field(s): `NetTargetSourcePort`.

### Version 6.1.1.4416

#### Improvements

- Improved number of sent events during session lifetime.
- Improved values in *Application Performance* dashboard.

#### Bugfixes

- Added `chmod` call to “`StartEventgen.cmd`”.

## Version 6.1.1

### Improvements

- Added some more hardware models.
- Added `ModuleName` and `ExceptionCode` to the sourcetype `uberAgent:Application:Errors` (applications crashes).
- Generated outliers for Process DNS.

### Updated Sourcetypes

- **Sourcetype:** `uberAgent:Process:ProcessStartup` has new field(s): `HashMD5`, `HashSHA1`, `HashSHA256`, `HashIMP`, `SignatureStatus`, `IsSignedByOSVendor`, `SignerName`.
- **Sourcetype:** `uberAgent:Process:ProcessStartup`: fields `ProcHash` and `HashType` have been removed.
- **Sourcetype:** `uberAgent:Process:ProcessStop` has new field(s): `HashMD5`, `HashSHA1`, `HashSHA256`, `HashIMP`.
- **Sourcetype:** `uberAgent:Process:ProcessStop`: fields `ProcHash` and `HashType` have been removed.
- **Sourcetype:** `uberAgent:Process:ProcessDetail` has new field(s): `SessionID`.
- **Sourcetype:** `uberAgent:CitrixADC:AppliancePerformance` has new field(s): `CpuFan0Speed`, `CpuFan1Speed`, `SystemFanSpeed`, `Cpu0Temp`, `Cpu2Temp`, `InternalTemp`, `PowerSupply1Status`, `PowerSupply2Status`, `PowerSupply3Status`, `PowerSupply4Status`, `VoltageV33Main`, `ICAOnlySessions`, `ICAOnlyConnections`, `SmartAccessSessions`, `SmartAccessICAConnections`, `SSLSessions`.
- **Sourcetype:** `uberAgent:CitrixADC:Gateway` has new field(s): `HSTS`, `HSTSMAXAGE`, `HSTSIInclSubdom`, `TLS13`.
- **Sourcetype:** `uberAgent:CitrixADC:vServer` has new field(s): `HSTS`, `HSTSMAXAGE`, `HSTSIInclSubdom`, `TLS13`.
- **Sourcetype:** `uberAgent:System:NetworkConfigInformation` has new field(s): `NetworkConfigWiFiSignalQuality`, `NetworkConfigWiFiType`, `NetworkConfigWiFiAuth`.

### New Sourcetypes

- **Sourcetype:** new sourcetype `uberAgent:ESA:Process:DnsQuery` with fields: `ProcName`, `ProcGUID`, `DnsRequest`, `DnsResponse`, `DnsResponseType` and `DnsEventCount`.

## Bugfixes

- SMB paths had only one backslash.

## Demoing uberAgent With the Event Generator for Splunk

July 25, 2024

Demonstrating uberAgent can be a bit difficult if you do not have a few dozen machines with live users available. To simplify demos, we offer an event generator that simulates an RDSH site with 5 active servers and 10 user sessions each.

### Architecture

Starting with uberAgent version 6, the Splunk event generator dependency was removed and uberAgent event generator is a single Splunk app. When Splunk is started, a .NET Core program generates sample data. By default sample data for two hours is generated. If you want to generate additional sample data, you can either restart the Splunk service after 2 hours, or modify the `uAEventGen.conf` file (see section "Advanced configuration").

The Splunk app can be used on Windows, Linux, and on macOS-based Splunk installations. Single server setups and distributed deployments are fully supported. The standard installation sends the data to a local Splunk instance using the TCP port 19500.

### Installation

#### .NET Core

As of uberAgent version 6, .NET Core is a prerequisite that must be installed on the same server where Splunk is installed. In the case of a distributed environment, .NET Core must be installed on the same Splunk indexers where you want to install the uberAgent event generator Splunk app.

You can download .NET Core [here](#).

#### uberAgent Event Generator

Install the uberAgent event generator on one of the indexers. If you have a single Splunk server, install the event generator on that server.

- Download the [uberAgent event generator](#) (find out what's new in the [changelog](#))
- On the Splunk server navigate to **Manage apps**
- Click **Install app from file**
- Select the archive you downloaded earlier and click **Upload**
- Restart Splunk

That's it. The event generator starts generating events right after Splunk has been restarted. It will continue to do so for approx. 2 hours and then stop on its own. Just what you need for a demo. To re-enable restart Splunk again.

## Configuration

### Enabling or Disabling the Event Generator

To enable or disable the uberAgent event generator:

1. On the Splunk server where the uberAgent event generator app is installed navigate to **Manage apps**
2. Locate the *uberAgent event generator* app and click on **enable** or **disable**
3. Restart Splunk

### Advanced Configuration

The default configuration should work for a single instance Splunk environment. If you have a distributed Splunk environment or you want to generate different generated sample data, you can modify the configuration file `uAEventGen.conf` which is located `%Splunkhome%/etc/apps/uberAgent_eventgenerator/bin/uAEventGenBinaries/your platform`.

The file contains full documentation of all possible configuration options.

## uberAgent Helpdesk Splunk App

August 1, 2024

The uberAgent Helpdesk Splunk App is a specialized tool designed for IT professionals who support virtual or physical desktops and need to resolve issues quickly. This app provides a streamlined view of the existing uberAgent dataset, optimized for helpdesk use.

## Features

- Simplified view of uberAgent data tailored for helpdesk professionals
- Quick access to key metrics and information for troubleshooting
- Intuitive interface for faster issue resolution
- Customized dashboards for common helpdesk scenarios

## Quick Links

- [Changelog and Release Notes](#)
- [Quickstart Guide](#)

## Getting Started

To get started with the uberAgent Helpdesk Splunk App:

1. Ensure you have uberAgent and Splunk installed and configured
2. Download the Helpdesk Splunk App from the [Citrix downloads page](#)
3. Install the app on your Splunk instance
4. Start using the specialized dashboards for efficient issue resolution

For more detailed instructions, please refer to our [Quickstart Guide](#).

## Related Tools

- [uberAgent Event Generator for Splunk](#)
- [uberAgent Log Collector Splunk App](#)

For a complete list of uberAgent addons and tools, visit our [Addons and Tools](#) page.

## Changelog and Release Notes

July 25, 2024

### Version 1.4.0

#### Improvements

- **Dashboards:** added user input delay metrics that were introduced in uberAgent 7.1.

## Release notes

- **Dashboards:** replaced the chart *Disk latency (ms)* with *Input delay (ms)*.

## Version 1.3.0

### Improvements

- **Dashboards:** added Citrix metrics that were introduced in uberAgent 7.0.
- **Dashboards:** the WiFi signal quality chart is inserted into the *Network details* section dynamically. In older versions, it was always there, even for non-WiFi connections.
- **Dashboards:** all charts are now column charts for better visibility.

### Bug fixes

- **Dashboards:** fixed wrong timeframe evaluation in the *Machine details* chart. It now loads much faster.

## Release notes

- **Dashboards:** removed the chart *Session activity* in favor of session connection change annotations.

## Version 1.2.3

### Improvements

- **Splunk:** added `sc_admin` permissions to meet Splunk Cloud requirements.

## Version 1.2.2

### Improvements

- **Dashboards:** upgraded dashboards to version 1.1. This is a requirement for Splunk Cloud requirements.

## Version 1.2.1

### Bug fixes

- **Dashboards:** rounded Wifi signal quality
- **Dashboards:** fixed timeframe issues for the machines and network details charts

## Version 1.2.0

### Improvements

- **Dashboards:** added WiFi metrics
- **Dashboards:** added network latency metric selector

## Version 1.1

- Support for uberAgent 6.0.

## Version 1.0

- Initial release

## uberAgent Helpdesk Splunk App

October 2, 2024

The uberAgent Helpdesk Splunk App is designed for helpdesk heroes who support virtual or physical desktops and who need quick answers to typical questions like the following:

- Why is my login so slow? It was fast yesterday.
- Why is my app constantly crashing?
- Citrix is slow!
- The website is not loading fast enough!

### What Does the App Look Like

The app has just one dashboard, nice and easy. You start by searching either for a user or a machine. After selecting a session of interest detailed information will be provided.

### Helpdesk Center

Search for users and machines, get all the details you need and narrow down the problem - uberAgent's helpdesk center to the rescue

Time range: Last 1 hour Search for: User  Submit Hide Filters

Dashboard controls Clear charts

#### Sessions for User = \*dbtest\*

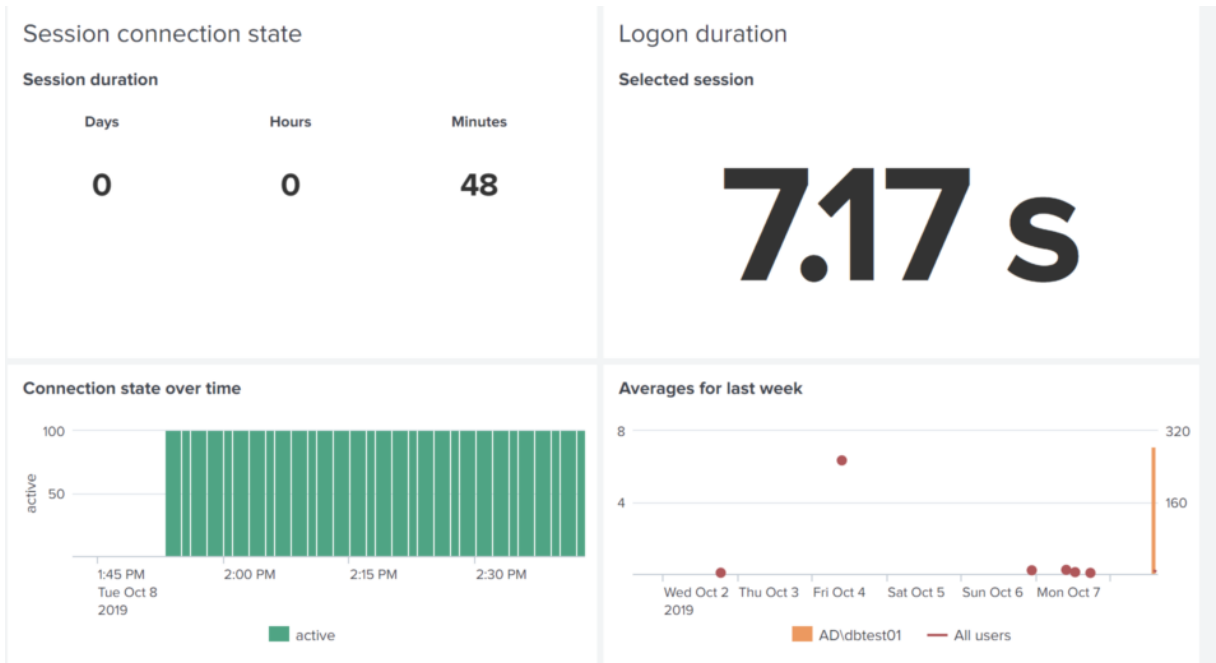
| Machine | User        | Session ID | Logon time             | Last seen              | Last state | Protocol | Used apps                     | Used web apps                              | Remoting client |
|---------|-------------|------------|------------------------|------------------------|------------|----------|-------------------------------|--------------------------------------------|-----------------|
| CTX-SH1 | AD\dbtest01 | 8          | 2019-10-08<br>13:53:19 | 2019-10-08<br>14:41:46 | active     | ICA      | Google<br>Chrome<br>Notepad++ | conf.splunk.com<br>newtab<br>uberagent.com | LAPTOP-DOMINIK  |
| CTX-SH1 | AD\dbtest01 | 5          | 2019-09-20<br>13:44:13 | 2019-10-08<br>13:52:41 | active     | ICA      | Internet<br>Explorer          |                                            | LAPTOP-DOMINIK  |

The dashboard gives you an overview of the user's session with helpful content like user and machine information, connection state over time as well as logon time compared to the previous week.

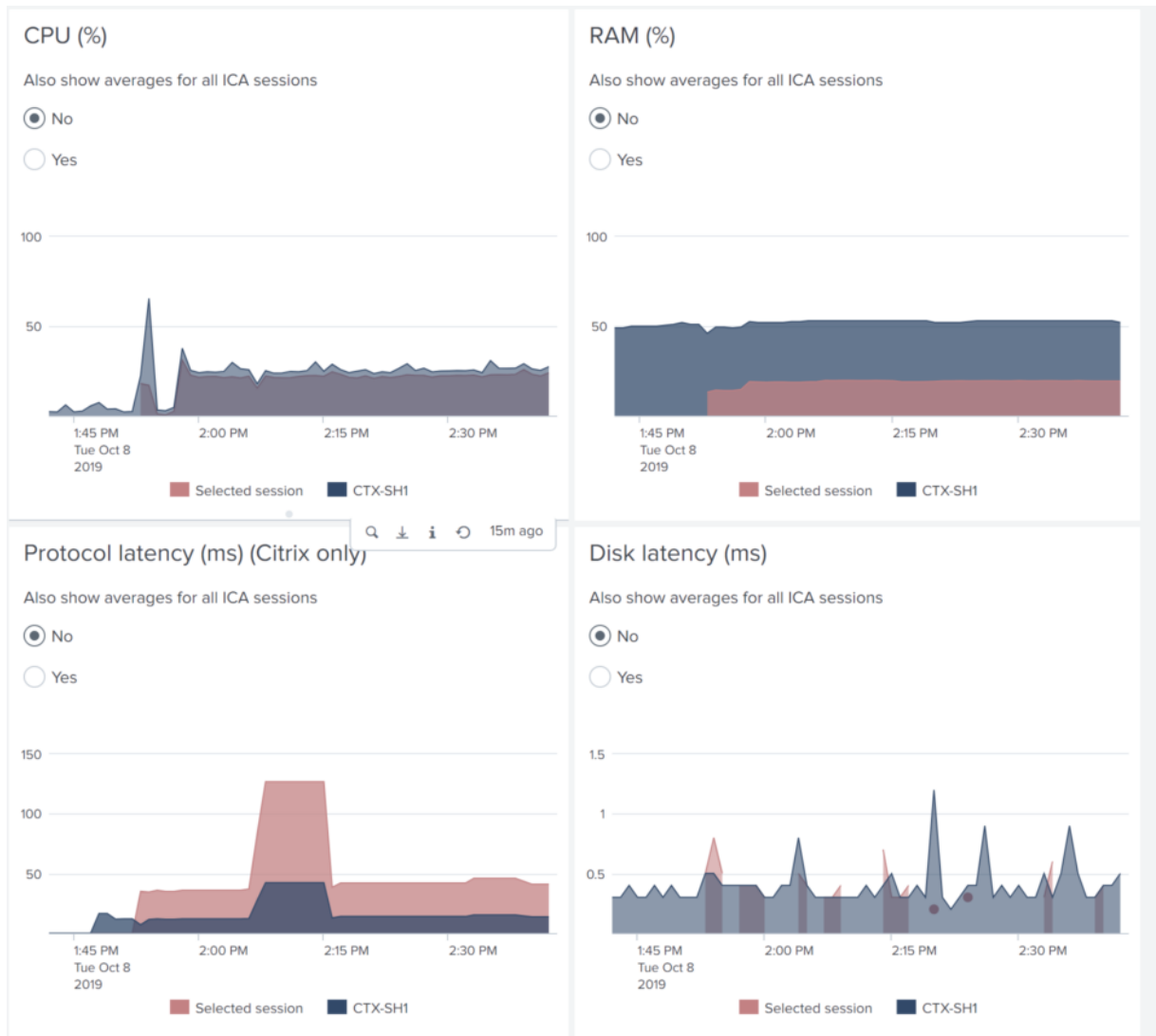
| Remoting details                                  |                               | Machine details               |                                       |
|---------------------------------------------------|-------------------------------|-------------------------------|---------------------------------------|
| Latest info about RDP, Citrix and VMware sessions |                               | Latest info about the machine |                                       |
| Property                                          | Data                          | Property                      | Data                                  |
| Client IP                                         | 10.1.1.171                    | AD OU                         | vast limits/Computers/DominikTest     |
| Client OS                                         | Windows                       | AD domain DNS                 | ad.int.vastlimits.com                 |
| Client name                                       | LAPTOP-DOMINIK                | AD domain NetBIOS             | AD                                    |
| Client type                                       | WI                            | AD site                       | Default-First-Site-Name               |
| Encryption                                        | basic                         | CPU name                      | Intel(R) Xeon(R) W-2145 CPU @ 3.70GHz |
| Initial published ressource                       | Desktop - SessionHost \$S13-4 | Citrix delivery group         | VDA - SessionHost                     |
| Remoting client version                           | 19.7.0.15                     | Citrix machine catalog        | VDA-SessionHost                       |
| Remoting technology                               | Citrix                        | Citrix site                   | CTX-XD715LTSR                         |
| Resolution                                        | 1502x1162x24                  | Hardware                      | Microsoft Corporation Virtual Machine |
|                                                   |                               | Hardware: has battery?        | 0                                     |

< Prev 1 2 Next >

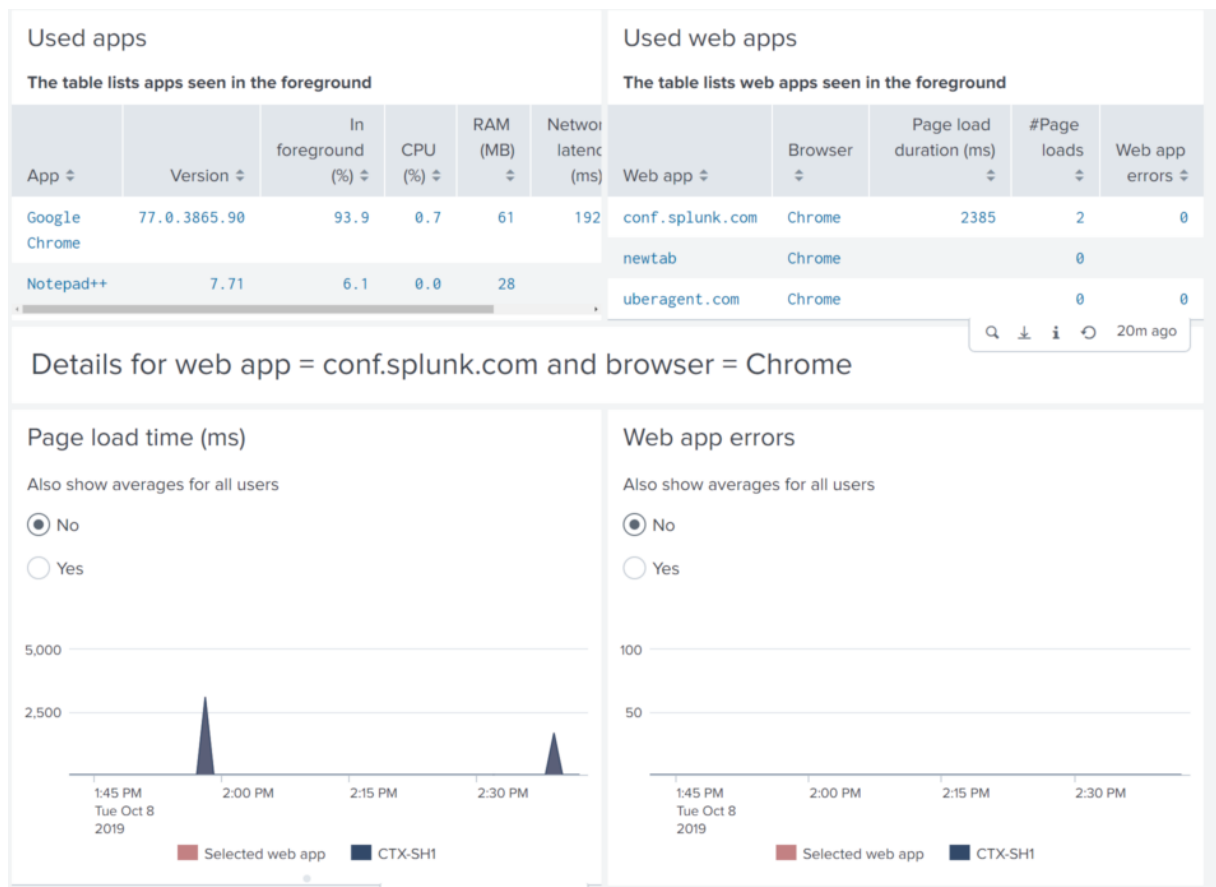




Now dive into the session's performance and compare it to the entire machine or even to other sessions in the organization.



The user is reporting issues with a specific native application or SaaS app? Click on an item in the list and you will get details to solve the user’s problem immediately!



## Download

The app is available **for free** and can be downloaded from [Splunkbase](#).

## Requirements

The helpdesk app provides a different view of the regular dataset collected by uberAgent. As such it requires a working uberAgent infrastructure on Splunk. General [uberAgent requirements](#) apply.

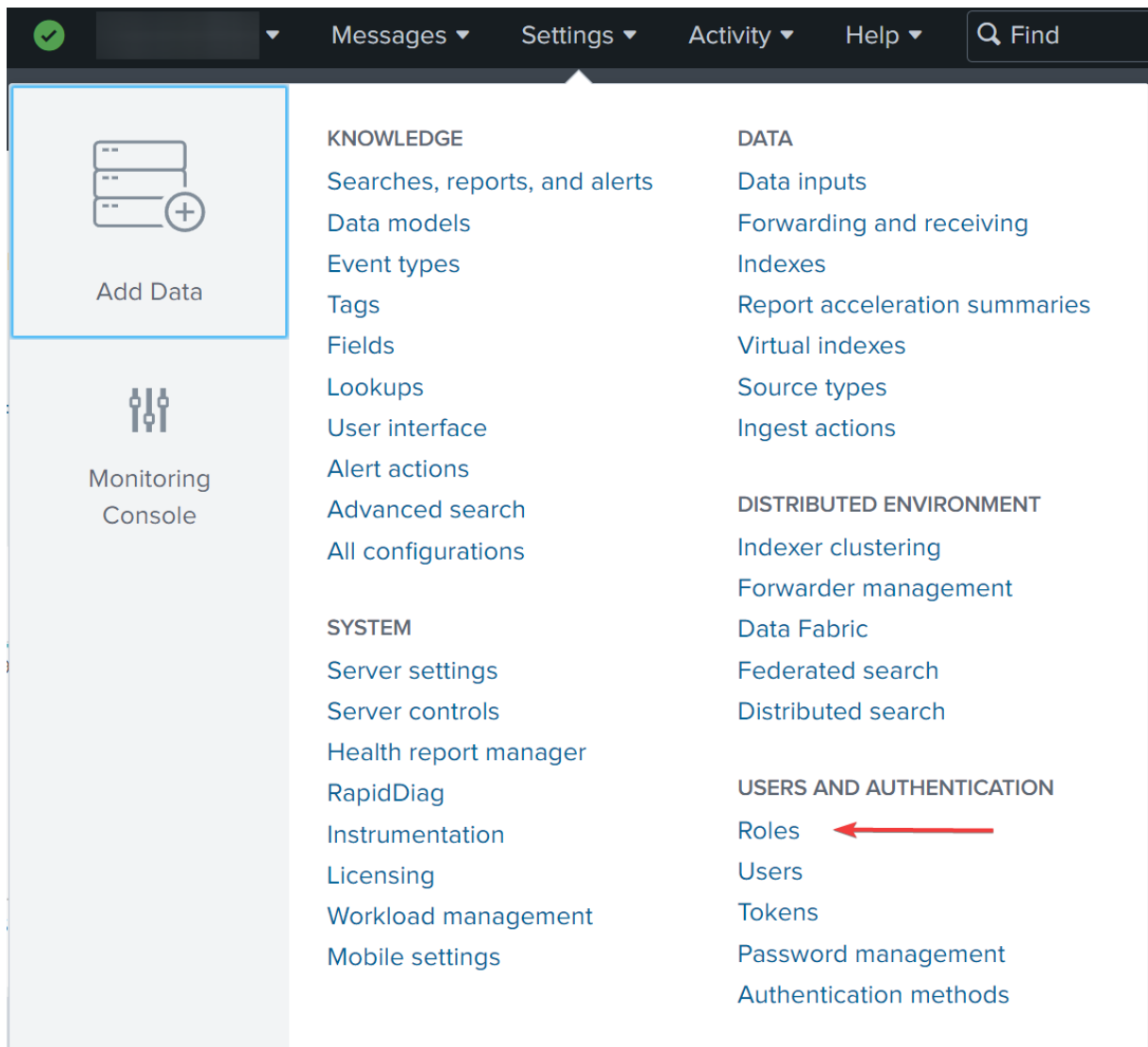
## uberAgent Version

- uberAgent UXM 6.0 or greater

## Limit Helpdesk Employees to the Helpdesk App

With role based access in Splunk, you can configure that helpdesk employees only see the helpdesk app and are automatically forwarded to the app after logging on to Splunk.

Navigate to **Settings -> Users and Authentication -> Roles**.



Create a new **user** role with a meaningful name like **uberagent-helpdesk-users**. More information on roles are available in [Splunk's documentation](#).

In the last step, select the **uberAgent\_helpdesk** app as default.

## New Role

Name \* 

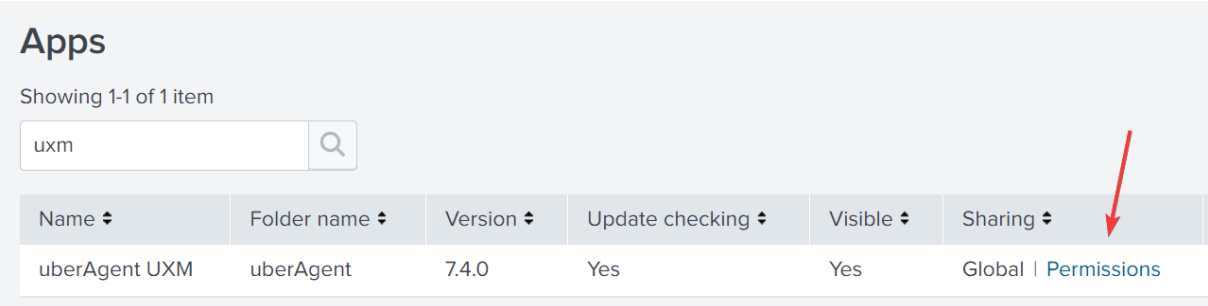
- 1. Inheritance
- 2. Capabilities
- 3. Indexes
- 4. Restrictions
- 5. Resources**

### This role

Default app

Put your helpdesk users in the new **uberagent-helpdesk-users** role.

Go to **Apps -> Manage Apps**, find the uberAgent UXM app, click on **Permissions**, and remove **Read** access for **Everyone**. Give **Read** access to admins only.



The screenshot shows the 'Apps' management interface. At the top, it says 'Showing 1-1 of 1 item' and has a search bar containing 'uxm'. Below is a table with columns: Name, Folder name, Version, Update checking, Visible, and Sharing. The row for 'uberAgent UXM' shows 'uberAgent' as the folder name, version '7.4.0', update checking 'Yes', visible 'Yes', and sharing 'Global | [Permissions](#)'. A red arrow points to the 'Permissions' link.

| Name          | Folder name | Version | Update checking | Visible | Sharing                              |
|---------------|-------------|---------|-----------------|---------|--------------------------------------|
| uberAgent UXM | uberAgent   | 7.4.0   | Yes             | Yes     | Global   <a href="#">Permissions</a> |

Note that the group **uberagent-helpdesk-users** does not have read access anymore.

# Permissions

Apps » uberAgent » Permissions

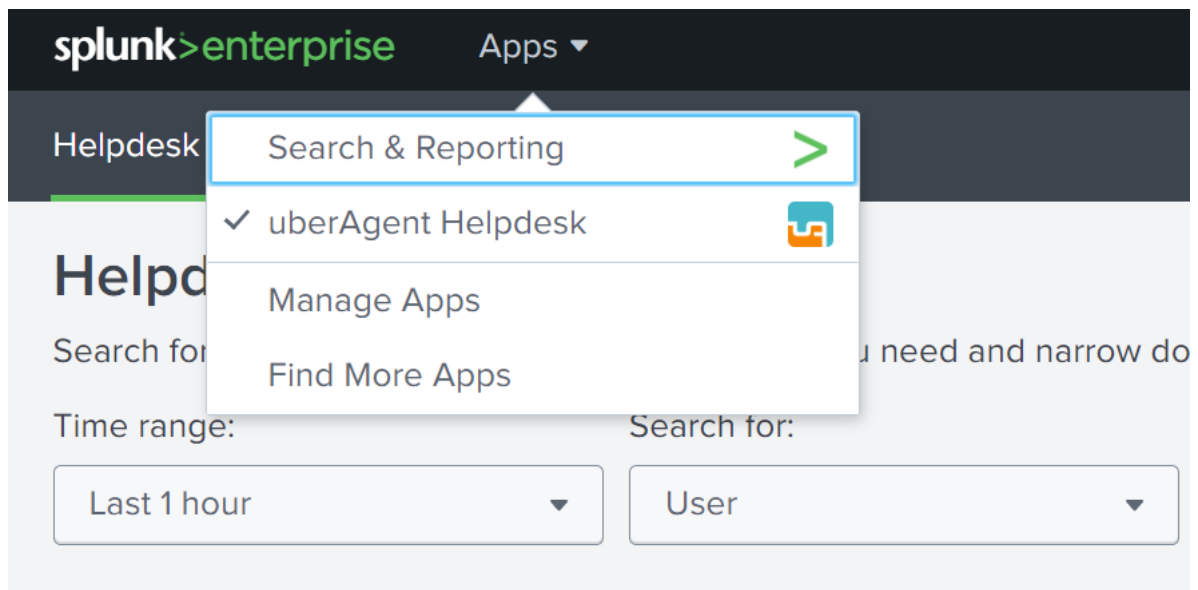
## App permissions

Users with read access can only save objects for themselves, and

| Roles                    | Read                                | Write                               |
|--------------------------|-------------------------------------|-------------------------------------|
| <b>Everyone</b>          | <input type="checkbox"/>            | <input type="checkbox"/>            |
| admin                    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| can_delete               | <input type="checkbox"/>            | <input type="checkbox"/>            |
| power                    | <input type="checkbox"/>            | <input type="checkbox"/>            |
| splunk-system-role       | <input type="checkbox"/>            | <input type="checkbox"/>            |
| uberagent-helpdesk-users | <input type="checkbox"/>            | <input type="checkbox"/>            |
| user                     | <input type="checkbox"/>            | <input type="checkbox"/>            |

Repeat the process for the uberAgent ESA app.

Now helpdesk employees only see the helpdesk app when logging on to Splunk.



*This chapter was contributed by Antoin Carroll.*

## uberAgent Log Collector Splunk App

July 26, 2024

The uberAgent Log Collector Splunk App is a powerful tool designed to help you monitor the health of your uberAgent deployment. It collects the data logged by uberAgent and sends it to Splunk, providing easy access through pre-build dashboards.

### Features

- Automated collection of uberAgent log data
- Centralized logging and monitoring of uberAgent deployments
- Custom dashboards for quick health checks and troubleshooting
- Easy integration with existing Splunk environments

### Quick Links

- [Changelog and Release Notes](#)
- [Quickstart Guide](#)

## Getting Started

To get started with the uberAgent Log Collector App, please refer to our [Quickstart Guide](#).

## Related Tools

- [uberAgent Event Generator for Splunk](#)
- [uberAgent Helpdesk Splunk App](#)

For a complete list of uberAgent addons and tools, visit our [Addons and Tools](#) page.

## Changelog and Release Notes

August 1, 2024

### Version 1.2.3

- Compatibility with the latest Splunk app packaging rules
- No new features were added in this release

### Version 1.2.2

- Upgraded dashboards to version 1.1
- Added sc\_admin permissions to meet Splunk Cloud requirements.
- Disabled index creation to meet Splunk Cloud requirements.
- Disabled data model acceleration to meet Splunk Cloud requirements.

### Version 1.2.1

- Disabled the truncation of lines greater than 10,000 bytes.

### Version 1.2

- Complete dashboard redesign including various filtering capabilities
- Changed all dashboard searches from raw to pivot
- Added support for macOS log files
- Added Splunk data model [uberAgentMeta](#)

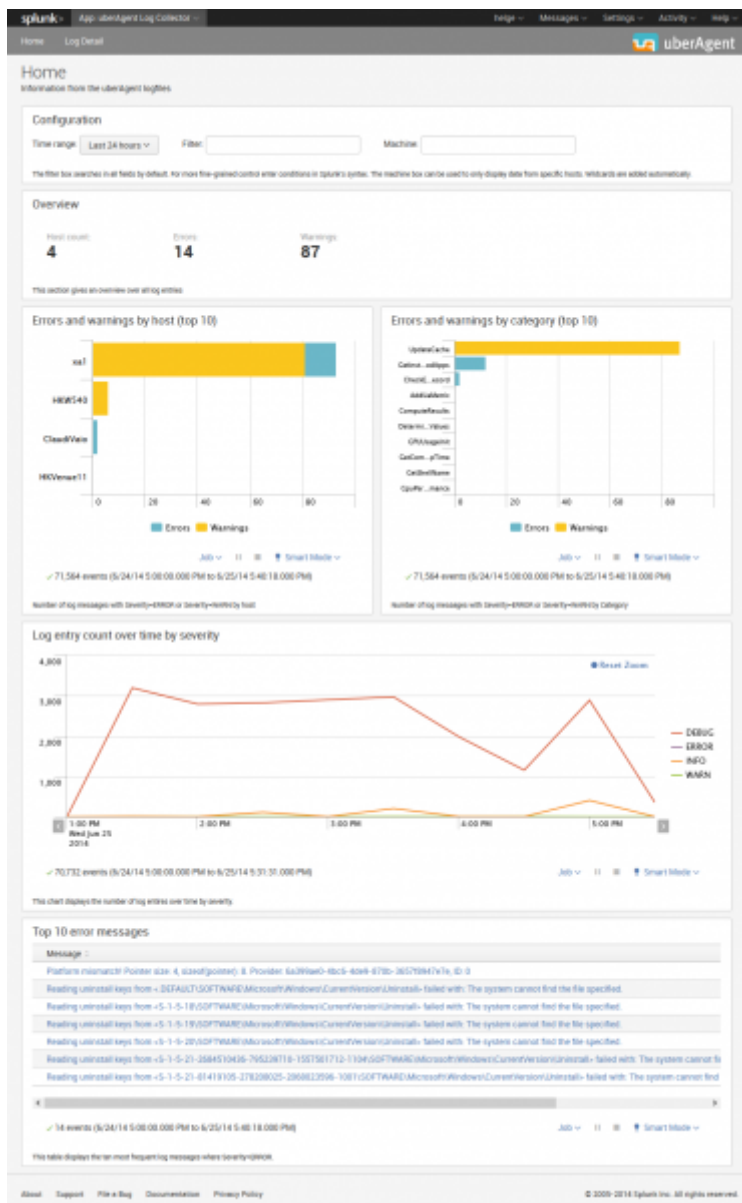


- Added additional logfile `uAInSessionHelper.log`
- Added new sourcetype `uberAgent:Meta:uAInSessionHelperLog`
- Added additional logfile `uberAgentIEExtension.log`
- Added new sourcetype `uberAgent:Meta:uAIEExtensionLog`
- Added additional logfile `uberAgentSandbox.log`
- Added new sourcetype `uberAgent:Meta:uASandboxLog`
- Changed the default index name from `uberagent_log` to `ua_meta_log`
- Added `macros.conf` to centrally rename the index
- Changed the sourcetype name from `uberAgent:log` to `uberAgent:Meta:uberAgentLog`

## uberAgent Log Collector Splunk App

November 25, 2024

uberAgent maintains a very detailed and informative [log file](#) that can tell you a lot not only about uberAgent's health but also about the machine uberAgent is running on. Naturally, the log file is stored locally on the computer uberAgent is running on which makes analysis and troubleshooting a bit difficult in large environments. But luckily it is very easy to solve that problem with Splunk!



## What is it

*uberAgent Log Collector* is a set of associated Splunk apps that collect the data logged by uberAgent, send it to Splunk for indexing and provide dashboards for easy access.

## Installation

*uberAgent Log Collector* consists of the Splunk app containing the dashboards and a technology add-on (TA) for collecting the data with Splunk’s Universal Forwarder. These two components need to be installed on the following systems:

- **App:** search head(s)
- **TA:** endpoints where uberAgent and the Splunk Universal Forwarder are deployed

## Splunk Index

You need to create the Splunk index `ua_meta_log` that stores the logs.

To add the new index `ua_meta_log` with the CLI run `splunk add index ua_meta_log`. The full documentation on creating Splunk indexes is available in the [Splunk docs](#).

## System Requirements

The TA requires Splunk's Universal Forwarder to be installed on the same machine.

## Download

The *uberAgent Log Collector* apps are available in the Splunk App Directory:

- Download [uberAgent Log Collector app](#)
- Download [uberAgent Log Collector TA](#)



© 2024 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at <https://www.cloud.com/legal>. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (<https://www.cloud.com/legal>) for more information.