Description of Windows 10 Features

Service profile: Processor activity			
ID	**Feature**	**Type**	**Description**
1	ts	Number	Timestamp of connection captured by Bro for network data
2	Processor_DPC_Rate	Number	The time rate that is a single processor spent receiving and servicing deferred procedure calls (DPCs)
3	Processor_pct_ Idle_Time	Number	The idle time of the processor that is not being used by any program
4	Processor_pct_ C3_Time	Number	The time rate of processor deep sleep state, where the clock generator and the processor does not need to keep its cache coheren
5	Processor_pct_ Interrupt_Time	Number	the time rate that is the processor spends receiving and servicing hardware interrupts during sample intervals
6	Processor_pct_ C2_Time	Number	The time rate of processor stop clock state, where the core and bus clocks are off and the processor maintains all software-visible state, but may take longer to wake up
7	Processor_pct_ User_Time	Number	The percentage of elapsed time the processor spends in the user mode. User mode is a restricted processing mode designed for applications, environment subsystems, and integral subsystems. This counter displays the average busy time as a percentage of the sample time.
8	Processor_pct_ C1_Time	Number	The percentage of time the processor spends in the C1 low-power idle state. % C1 Time is a subset of the total processor idle time.
9	Processor_pct_ Processor_Time	Number	The percentage of elapsed time that the processor spends to execute a non-Idle thread. It is calculated by measuring the percentage of time that the processor spends executing the idle thread and then subtracting that value from 100%. This counter is the primary indicator of processor activity, and displays the average percentage of busy time observed during the sample interval.
10	Processor_C1_ransitions_sec	Number	The rate that the CPU enters the C1 low-power idle state. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval.
11	Processor_pct_ DPC_Time	Number	The percentage of time that the processor spent receiving and servicing deferred procedure calls (DPCs) during the sample interval. DPCs are interrupts that run at a lower priority than standard interrupts. This counter displays the average busy time as a percentage of the sample time.
12	Processor_C2_ransitions_sec	Number	The rate that the CPU enters the C2 low-power idle state. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval.
13	Processor_pct_ Privileged_Time	Number	The percentage of elapsed time that the process threads spent executing code in privileged mode.

14	Processor_C3_ransitions_sec	Number	The rate that the CPU enters the C3 low-power idle state. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval.
15	Processor_DPCs_Queued_sec	Number	The average rate, in incidents per second, at which deferred procedure calls (DPCs) were added to the processor's DPC queue. DPCs are interrupts that run at a lower priority than standard interrupts. This counter measures the rate that DPCs are added to the queue, not the number of DPCs in the queue. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval.
16	Processor_Interrupts_sec	Number	The average rate, in incidents per second, at which the processor received and serviced hardware interrupts. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval.

Service profile: Process activity			
ID	**Feature**	**Type**	**Description**
17	Process_Pool_Paged Bytes	Number	The size, in bytes, of the paged pool, an area of the system virtual memory that is used for objects that can be written to disk when they are not being used. Memory/Pool Paged Bytes is calculated differently than Process/Pool Paged Bytes, so it might not equal Process(_Total)/Pool Paged Bytes. This counter displays the last observed value only; it is not an average.
18	Process_IO Read_Operations_sec	Number	The process is issuing read I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/Os.
19	Process_Working_Set_ Private	Number	The size of the working set, in bytes, that is use for this process only and not shared nor sharable by other processes.
20	Process_Working_Set_Peak	Number	The maximum size, in bytes, of the Working Set of this process at any point in time. The Working Set is the set of memory pages touched recently by the threads in the process.
21	Process_IO_Write Operations_sec	Number	The process is issuing write I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/Os.
22	Process_Page_File Bytes	Number	The current amount of virtual memory, in bytes, that this process has reserved for use in the paging file(s). Paging files are used to store pages of memory used by the process that are not contained in other files.
23	Process_pct_ User_Time	Number	The percentage of elapsed time that the process threads spent executing code in user mode. Applications, environment subsystems, and integral subsystems execute in user mode.

24	Process_Virtual_Bytes Peak	Number	The maximum size, in bytes, of virtual address space the process has used at any one time. Use of virtual address space does not necessarily imply corresponding use of either disk or main memory pages. However, virtual space is finite, and the process might limit its ability to load libraries.
25	Process_Page_File Bytes Peak	Number	The maximum amount of virtual memory, in bytes, that this process has reserved for use in the paging file(s). Paging files are used to store pages of memory used by the process that are not contained in other files.
26	Process_IO_Other_Bytes_sec	Number	The process is issuing bytes to I/O operations that do not involve data such as control operations. This counter counts all I/O activity generated by the process to include file, network and device I/Os.
27	Process_Private_Bytes	Number	The current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.
28	Process_IO_Write_Bytes_sec	Number	The process is writing bytes to I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/Os.
29	Process_Elapsed_Time	Number	The total elapsed time, in seconds, that this process has been running.
30	Process_Virtual_Bytes	Number	The current size, in bytes, of the virtual address space the process is using. Use of virtual address space does not necessarily imply corresponding use of either disk or main memory pages.
31	Process_pct_ Processor_Time	Number	The percentage of elapsed time that all of process threads used the processor to execution instructions. An instruction is the basic unit of execution in a computer, a thread is the object that executes instructions, and a process is the object created when a program is run.
32	Process_Creating Process ID	Number	The Process ID of the process that created the process. The creating process may have terminated, so this value may no longer identify a running process.
33	Process_Pool Nonpaged Bytes	Number	The size, in bytes, of the nonpaged pool, an area of the system virtual memory that is used for objects that cannot be written to disk, but must remain in physical memory as long as they are allocated. Memory/Pool Nonpaged Bytes is calculated differently than Process/Pool Nonpaged Bytes, so it might not equal Process(_Total)/Pool Nonpaged Bytes. This counter displays the last observed value only; it is not an average.
34	Process_Working Set	Number	The current size, in bytes, of the Working Set of this process. The Working Set is the set of memory pages touched recently by the threads in the process.

35	Process_Page Faults_sec	Number	The rate at which page faults by the threads executing in this process are occurring. A page fault occurs when a thread refers to a virtual memory page that is not in its working set in main memory.
36	Process_ID Process	Number	The unique identifier of this process. ID Process numbers are reused, so they only identify a process for the lifetime of that process.
37	Process_IO Other Operations_sec	Number	The rate at which the process is issuing I/O operations that are neither read nor write operations (for example, a control function). This counter counts all I/O activity generated by the process to include file, network and device I/Os.
38	Process_IO Data Operations_sec	Number	The rate at which the process is issuing read and write I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/Os.
39	Process_Thread Count	Number	The number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.
40	Process_pct_ Privileged_Time	Number	The percentage of elapsed time that the process threads spent executing code in privileged mode. When a Windows system service is called, the service will often run in privileged mode to gain access to system-private data. Such data is protected from access by threads executing in user mode.
41	Process_IO Data Bytes_sec	Number	The rate at which the process is reading and writing bytes in I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/Os.
42	Process_IO Read Bytes_sec	Number	The rate at which the process is reading bytes from I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/Os.
43	Process_Priority Base	Number	The current base priority of this process. Threads within a process can raise and lower their own base priority relative to the process' base priority.
44	Process_Handle Count	Number	The total number of handles currently open by this process. This number is equal to the sum of the handles currently open by each thread in this process.

Service profile: Network activity			
ID	**Feature**	**Type**	**Description**

45	Network_I(Intel[R]_82574L_GNC)TCP_APS	Number	The average size in bytes of received packets across all TCP connections on this network interface.
46	Network_I(Intel[R]_82574L_GNC)/Packets Received Unknown	Number	The number of packets received through the interface that were discarded because of an unknown or unsupported protocol.
47	Network_I(Intel[R]_82574L_GNC)/Bytes Received/sec	Number	The rate at which bytes are received over each network adapter, including framing characters. Network Interface\Bytes Received/sec is a subset of Network Interface\Bytes Total/sec.
48	Network_I(Intel[R]_82574L_GNC)/Bytes Sent/sec	Number	The rate at which bytes are sent over each network adapter, including framing characters. Network Interface\Bytes Sent/sec is a subset of Network Interface\Bytes Total/sec.
49	Network_I(Intel[R]_82574L_GNC)/Packets Outbound Errors	Number	The number of outbound packets that could not be transmitted because of errors.
50	Network_I(Intel[R]_82574L_GNC)/Packets Received Discarded	Number	The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their delivery to a higher-layer protocol. One possible reason for discarding packets could be to free up buffer space.
51	Network_I(Intel[R]_82574L_GNC)/Bytes Total/sec	Number	The rate at which bytes are sent and received over each network adapter, including framing characters. Network Interface\Bytes Total/sec is a sum of Network Interface\Bytes Received/sec and Network Interface\Bytes Sent/sec.
52	Network_I(Intel[R]_82574L_GNC)/Packets Outbound Discarded	Number	The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent transmission. One possible reason for discarding packets could be to free up buffer space.
53	Network_I(Intel[R]_82574L_GNC)/TCP RSC Exceptions/sec	Number	The RSC exception rate for receive packets across all TCP connections on this network interface.
54	Network_I(Intel[R]_82574L_GNC)/Packets Sent Unicast/sec	Number	The rate at which packets are requested to be transmitted to subnet-unicast addresses by higher-level protocols. The rate includes the packets that were discarded or not sent.
55	Network_I(Intel[R]_82574L_GNC)/Output Queue Length	Number	The length of the output packet queue (in packets). If this is longer than two, there are delays and the bottleneck should be found and eliminated, if possible. Since the requests are queued by the Network Driver Interface Specification (NDIS) in this implementation, this will always be 0.
56	Network_I(Intel[R]_82574L_GNC)/Packets Received/sec	Number	The rate at which packets are received on the network interface.
57	Network_I(Intel[R]_82574L_GNC)/Current Bandwidth	Number	The current bandwidth of the network interface in bits per second (BPS). For interfaces that do not vary in bandwidth or for those where no accurate estimation can be made, this value is the nominal bandwidth.

58	Network_I(Intel[R]_82574L_GNC)/Packets/sec	Number	The rate at which packets are sent and received on the network interface.
59	Network_I(Intel[R]_82574L_GNC)/TCP Active RSC Connections	Number	The number of TCP connections (over both IPv4 and IPv6) that are currently receiving large packets from the RSC capable network adapter on this network interface.
60	Network_I(Intel[R]_82574L_GNC)/Packets Sent/sec	Number	The rate at which packets are sent on the network interface.
61	Network_I(Intel[R]_82574L_GNC)/Packets Received Unicast/sec	Number	The rate at which (subnet) unicast packets are delivered to a higher-layer protocol.
62	Network_I(Intel[R]_82574L_GNC)/Packets Sent Non-Unicast/sec	Number	The rate at which packets are requested to be transmitted to non-unicast (subnet broadcast or subnet multicast) addresses by higher-level protocols. The rate includes the packets that were discarded or not sent.
63	Network_I(Intel[R]_82574L_GNC)/Packets Received Non-Unicast/sec	Number	The rate at which non-unicast (subnet broadcast or subnet multicast) packets are delivered to a higher-layer protocol.
64	Network_I(Intel[R]_82574L_GNC)/TCP RSC Coalesced Packets/sec	Number	The large packet receive rate across all TCP connections on this network interface.
65	Network_I(Intel[R]_82574L_GNC)/Offloaded Connections	Number	The number of TCP connections (over both IPv4 and IPv6) that are currently handled by the TCP chimney offload capable network adapter.
66	Network_I(Intel[R]_82574L_GNC)/Packets Received Errors	Number	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

Service profile: Memory activity

ID	Feature	Type	Description
67	Memory/Pool Paged Bytes	Number	The size, in bytes, of the paged pool, an area of the system virtual memory that is used for objects that can be written to disk when they are not being used. Memory/Pool Paged Bytes is calculated differently than Process/Pool Paged Bytes, so it might not equal Process(_Total)/Pool Paged Bytes. This counter displays the last observed value only; it is not an average.
68	Memory/Free & Zero Page List Bytes	Number	The amount of physical memory, in bytes, that is assigned to the free and zero page lists. This memory does not contain cached data. It is immediately available for allocation to a process or for system use.
69	Memory/Cache Bytes Peak	Number	The maximum number of bytes used by the system file cache since the system was last restarted. This might be larger than the current size of the cache. This counter displays the last observed value only; it is not an average.
70	Memory/System Code Resident Bytes	Number	The size, in bytes, of the pageable operating system code that is currently resident and active in physical memory. This value is a component of Memory/System Code Total Bytes. This counter displays the last observed value only; it is not an average.
71	Memory/Available Bytes	Number	The amount of physical memory, in bytes, immediately available for allocation to a process or for system use. It is equal to the sum of memory assigned to the standby (cached), free and zero page lists.
72	Memory/Commit Limit	Number	The amount of virtual memory that can be committed without having to extend the paging file(s). It is measured in bytes. This counter displays the last observed value only; it is not an average.
73	Memory/Transition Pages RePurposed/sec	Number	The rate at which the number of transition cache pages were reused for a different purpose. These pages would have otherwise remained in the page cache to provide a (fast) soft fault (instead of retrieving it from backing store) in the event the page was accessed in the future. Note these pages can contain private or sharable memory.
74	Memory/Pages Output/sec	Number	The rate at which pages are written to disk to free up space in physical memory. A high rate of pages output might indicate a memory shortage. This counter shows the number of pages, and can be compared to other counts of pages, without conversion.

75	Memory/Page Reads/sec	Number	The rate at which the disk was read to resolve hard page faults. It shows the number of reads operations, without regard to the number of pages retrieved in each operation. This counter is a primary indicator of the kinds of faults that cause system-wide delays. Compare the value of Memory/Pages Reads/sec to the value of Memory/Pages Input/sec to determine the average number of pages read during each operation.
76	Memory/Demand Zero Faults/sec	Number	The rate at which a zeroed page is required to satisfy the fault. Zeroed pages, pages emptied of previously stored data and filled with zeros, are a security feature of Windows that prevent processes from seeing data stored by earlier processes that used the memory space. This counter shows the number of faults, without regard to the number of pages retrieved to satisfy the fault. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval.
77	Memory/Available KBytes	Number	The amount of physical memory, in Kilobytes, immediately available for allocation to a process or for system use. It is equal to the sum of memory assigned to the standby (cached), free and zero page lists.
78	Memory/Pages/sec	Number	The rate at which pages are read from or written to disk to resolve hard page faults. It is the sum of Memory/Pages Input/sec and Memory/Pages Output/sec. It is counted in numbers of pages, so it can be compared to other counts of pages, such as Memory/Page Faults/sec, without conversion. It includes pages retrieved to satisfy faults in the file system cache (usually requested by applications) non-cached mapped memory files.
79	Memory/Cache Bytes	Number	The size, in bytes, of the portion of the system file cache which is currently resident and active in physical memory. This counter displays the last observed value only; it is not an average.
80	Memory/Pool Nonpaged Bytes	Number	The size, in bytes, of the nonpaged pool, an area of the system virtual memory that is used for objects that cannot be written to disk, but must remain in physical memory as long as they are allocated. Memory/Pool Nonpaged Bytes is calculated differently than Process/Pool Nonpaged Bytes. This counter displays the last observed value only; it is not an average.
81	Memory/Page Faults/sec	Number	The average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory).
82	Memory/Transition Faults/sec	Number	The rate at which page faults are resolved by recovering pages that were being used by another process sharing the page, or were on the modified page list or the standby list, or were being written to disk at the time of the page fault. Transition faults are counted in numbers of faults; because only one page is faulted in each operation, it is also equal to the number of pages faulted.

83	Memory/System Cache Resident Bytes	Number	The size, in bytes, of the portion of the system file cache which is currently resident and active in physical memory. The System Cache Resident Bytes and Memory/Cache Bytes counters are equivalent. This counter displays the last observed value only; it is not an average.
84	Memory/Long-Term Average Standby Cache Lifetime (s)	Number	The average lifetime of data in the standby cache over a long interval is measured.
85	Memory/Standby Cache Reserve Bytes	Number	The amount of physical memory, in bytes, that is assigned to the reserve standby cache page lists. It is immediately available for allocation to a process or for system use.
86	Memory/Page Writes/sec	Number	The rate at which pages are written to disk to free up space in physical memory. This counter shows write operations, without regard to the number of pages written in each operation. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval.
87	Memory/System Code Total Bytes	Number	The size, in bytes, of the pageable operating system code currently mapped into the system virtual address space. This value is calculated by summing the bytes in Ntoskrnl.exe, Hal.dll, the boot drivers, and file systems loaded by Ntldr/osloader. This counter displays the last observed value only; it is not an average.
88	Memory/Standby Cache Core Bytes	Number	The amount of physical memory, in bytes, that is assigned to the core standby cache page lists. This memory contains cached data and code that is not actively in use by processes, the system and the system cache.
89	Memory/System Driver Resident Bytes	Number	The size, in bytes, of the pageable physical memory being used by device drivers. It is the working set (physical memory area) of the drivers. This value is a component of Memory/System Driver Total Bytes, which also includes driver memory that has been written to disk.
90	Memory/Standby Cache Normal Priority Bytes	Number	The amount of physical memory, in bytes, that is assigned to the normal priority standby cache page lists. This memory contains cached data and code that is not actively in use by processes, the system and the system cache. It is immediately available for allocation to a process or for system use.
91	Memory/Pool Paged Allocs	Number	The number of calls to allocate space in the paged pool. It is measured in numbers of calls to allocate space, regardless of the amount of space allocated in each call. This counter displays the last observed value only; it is not an average.
92	Memory/Pool Nonpaged Allocs	Number	The number of calls to allocate space in the nonpaged pool. It is measured in numbers of calls to allocate space, regardless of the amount of space allocated in each call. This counter displays the last observed value only; it is not an average.
93	Memory/pct_ Committed Bytes In Use	Number	The ratio of Memory/Committed Bytes to the Memory/Commit Limit. This counter displays the current percentage value only; it is not an average.

94	Memory/Free System Page Table Entries	Number	The number of page table entries not currently in used by the system. This counter displays the last observed value only; it is not an average.
95	Memory/Available MBytes	Number	The amount of physical memory, in Megabytes, immediately available for allocation to a process or for system use. It is equal to the sum of memory assigned to the standby (cached), free and zero page lists.
96	Memory/Modified Page List Bytes	Number	The amount of physical memory, in bytes, that is assigned to the modified page list. This memory contains cached data and code that is not actively in use by processes, the system and the system cache.
97	Memory/Cache Faults/sec	Number	The rate at which faults occur when a page sought in the file system cache is not found and must be retrieved from elsewhere in memory (a soft fault) or from disk (a hard fault). This counter shows the number of faults, without regard for the number of pages faulted in each operation.
98	Memory/Committed Bytes	Number	The amount of committed virtual memory, in bytes. This counter displays the last observed value only; it is not an average.
99	Memory/System Driver Total Bytes	Number	The size, in bytes, of the pageable virtual memory currently being used by device drivers. This counter displays the last observed value only; it is not an average.
100	Memory/Pages Input/sec	Number	The rate at which pages are read from disk to resolve hard page faults. Hard page faults occur when a process refers to a page in virtual memory that is not in its working set or elsewhere in physical memory, and must be retrieved from disk.
101	Memory/Pool Paged Resident Bytes	Number	The size, in bytes, of the portion of the paged pool that is currently resident and active in physical memory. The paged pool is an area of the system virtual memory that is used for objects that can be written to disk when they are not being used. This counter displays the last observed value only; it is not an average.
102	Memory/Write Copies/sec	Number	The rate at which page faults are caused by attempts to write that have been satisfied by coping of the page from elsewhere in physical memory. This counter shows the number of copies, without regard for the number of pages copied in each operation.

Service profile: Disk activity

ID	Feature	Type	Description
103	LogicalDisk(_Total)/Avg. Disk Bytes/Write	Number	The average number of bytes transferred to the disk during write operations.
104	LogicalDisk(_Total)/pct_ Idle Time	Number	The percentage of time during the sample interval that the disk was idle.
105	LogicalDisk(_Total)/Disk Reads/sec	Number	The rate of read operations on the disk.
106	LogicalDisk(_Total)/pct_ Free Space	Number	The percentage of total usable space on the selected logical disk drive that was free.
107	LogicalDisk(_Total)/Disk Read Bytes/sec	Number	The rate at which bytes are transferred from the disk during read operations.
108	LogicalDisk(_Total)/Avg. Disk sec/Read	Number	The average time, in seconds, of a read of data from the disk.

109	LogicalDisk(_Total)/Disk Writes/sec	Number	The rate of write operations on the disk.
110	LogicalDisk(_Total)/Current Disk Queue Length	Number	The number of requests outstanding on the disk at the time the performance data is collected. It also includes requests in service at the time of the collection. This is a instantaneous snapshot, not an average over the time interval. Requests experience delays proportional to the length of this queue minus the number of spindles on the disks. For good performance, this difference should average less than two.
111	LogicalDisk(_Total)/Split IO/Sec	Number	The rate at which I/Os to the disk were split into multiple I/Os. A split I/O may result from requesting data of a size that is too large to fit into a single I/O or that the disk is fragmented.
112	LogicalDisk(_Total)/Free Megabytes	Number	The unallocated space, in megabytes, on the disk drive in megabytes. One megabyte is equal to 1,048,576 bytes.
113	LogicalDisk(_Total)/Avg. Disk sec/Write	Number	The average time, in seconds, of a write of data to the disk.
114	LogicalDisk(_Total)/Disk Bytes/sec	Number	The rate bytes are transferred to or from the disk during write or read operations.
115	LogicalDisk(_Total)/Avg. Disk Read Queue Length	Number	The average number of read requests that were queued for the selected disk during the sample interval.
116	LogicalDisk(_Total)/pct_ Disk Time	Number	The percentage of elapsed time that the selected disk drive was busy servicing read or write requests.

117	LogicalDisk(_Total)/Avg. Disk Bytes/Read	Number	The average number of bytes transferred from the disk during read operations.
118	LogicalDisk(_Total)/Avg. Disk Write Queue Length	Number	The average number of write requests that were queued for the selected disk during the sample interval.
119	LogicalDisk(_Total)/Avg. Disk Queue Length	Number	The average number of both read and write requests that were queued for the selected disk during the sample interval.
120	LogicalDisk(_Total)/pct_ Disk Read Time	Number	The percentage of elapsed time that the selected disk drive was busy servicing read requests.
121	LogicalDisk(_Total)/Disk Write Bytes/sec	Number	The rate at which bytes are transferred to the disk during write operations.
122	LogicalDisk(_Total)/Disk Transfers/sec	Number	The rate of read and write operations on the disk.
123	LogicalDisk(_Total)/Avg. Disk Bytes/Transfer	Number	The average number of bytes transferred to or from the disk during write or read operations.
124	LogicalDisk(_Total)/pct_ Disk Write Time	Number	The percentage of elapsed time that the selected disk drive was busy servicing write requests.
125	LogicalDisk(_Total)/Avg. Disk sec/Transfer	Number	The time, in seconds, of the average disk transfer.

Service profile: Data labelling			
ID	**Feature**	**Type**	**Description**
126	label	Number	Tag normal and attack records, where 0 indicates normal and 1 indicates attacks
127	type	String	Tag attack categories, such as normal, DoS, DDoS and backdoor attacks, and normal records