osquery

Osquery Version: 4.5.1

Show only Tables compatible with:

Restore Default View

account_policy_data

Additional OS X user account data from the AccountPolicy section of OpenDirectory.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
uid	BIGINT	User ID
creation_time	DOUBLE	When the account was first created
failed_login_count	BIGINT	The number of failed login attempts using an incorrect password. Count resets after a correct password is entered.
failed_login_timestamp	DOUBLE	The time of the last failed login attempt. Resets after a correct password is entered
password_last_set_time	DOUBLE	The time the password was last changed

acpi_tables

Firmware ACPI functional table common metadata and content.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	ACPI table name
size	INTEGER	Size of compiled table data
md5	TEXT	MD5 hash of table content

ad_config

OS X Active Directory configuration.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	The OS X-specific configuration name
domain	TEXT	Active Directory trust domain
option	TEXT	Canonical name of option
value	TEXT	Variable typed option value

alf

OS X application layer firewall (ALF) service details.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
allow_signed_enabled	INTEGER	1 If allow signed mode is enabled else 0
firewall_unload	INTEGER	1 If firewall unloading enabled else 0
global_state	INTEGER	1 If the firewall is enabled with exceptions, 2 if the firewall is configured to block all incoming connections, else 0
logging_enabled	INTEGER	1 If logging mode is enabled else 0
logging_option	INTEGER	Firewall logging option
stealth_enabled	INTEGER	1 If stealth mode is enabled else 0
version	TEXT	Application Layer Firewall version

alf_exceptions

OS X application layer firewall (ALF) service exceptions.

Improve this Description on Github

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
path	TEXT	Path to the executable that is excepted
state	INTEGER	Firewall exception state

alf_explicit_auths

ALF services explicitly allowed to perform networking.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
process	TEXT	Process name explicitly allowed

app_schemes

OS X application schemes and handlers (e.g., http, file, mailto).

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
scheme	TEXT	Name of the scheme/protocol
handler	TEXT	Application label for the handler
enabled	INTEGER	1 if this handler is the OS default, else 0
external	INTEGER	1 if this handler does NOT exist on OS X by default, else 0
protected	INTEGER	1 if this handler is protected (reserved) by OS X, else 0

apparmor_events (EVENTED TABLE)

Track AppArmor events.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
type	TEXT	Event type
message	TEXT	Raw audit message
time	BIGINT	Time of execution in UNIX time
uptime	BIGINT	Time of execution in system uptime
eid	TEXT	Event ID
apparmor	TEXT	Apparmor Status like ALLOWED, DENIED etc.
operation	TEXT	Permission requested by the process
parent	UNSIGNED_BIGINT	Parent process PID
profile	TEXT	Apparmor profile name
name	TEXT	Process name
pid	UNSIGNED_BIGINT	Process ID
comm	TEXT	Command-line name of the command that was used to invoke the analyzed process
denied_mask	TEXT	Denied permissions for the process
capname	TEXT	Capability requested by the process
fsuid	UNSIGNED_BIGINT	Filesystem user ID
ouid	UNSIGNED_BIGINT	Object owner's user ID
capability	BIGINT	Capability number
requested_mask	TEXT	Requested access mask

COLUMN	TYPE	DESCRIPTION
info	TEXT	Additional information
error	TEXT	Error information
namespace	TEXT	AppArmor namespace
label	TEXT	AppArmor label

apparmor_profiles

Track active AppArmor profiles.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
path	TEXT	Unique, aa-status compatible, policy identifier.
name	TEXT	Policy name.
attach	TEXT	Which executable(s) a profile will attach to.
mode	TEXT	How the policy is applied.
sha1	TEXT	A unique hash that identifies this policy.

appcompat_shims

Application Compatibility shims are a way to persist malware. This table presents the AppCompat Shim information from the registry in a nice format. See http://files.brucon.org/2015/Tomczak_and_Ballenthin_Shims_for_the_Win.pdf for more details.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
executable	TEXT	Name of the executable that is being shimmed. This is pulled from the registry.
path	TEXT	This is the path to the SDB database.

COLUMN	TYPE	DESCRIPTION
description	TEXT	Description of the SDB.
install_time	INTEGER	Install time of the SDB
type	TEXT	Type of the SDB database.
sdb_id	TEXT	Unique GUID of the SDB.

apps

OS X applications installed in known search paths (e.g., /Applications).

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Name of the Name.app folder
path	TEXT	Absolute and full Name.app path
bundle_executable	TEXT	Info properties CFBundleExecutable label
bundle_identifier	TEXT	Info properties CFBundleIdentifier label
bundle_name	TEXT	Info properties CFBundleName label
bundle_short_version	TEXT	Info properties CFBundleShortVersionString label
bundle_version	TEXT	Info properties CFBundleVersion label
bundle_package_type	TEXT	Info properties CFBundlePackageType label
environment	TEXT	Application-set environment variables
element	TEXT	Does the app identify as a background agent
compiler	TEXT	Info properties DTCompiler label

development_region COLUMN	TEXT TYPE	Info properties CFBundleDevelopmentRegion label DESCRIPTION
display_name	TEXT	Info properties CFBundleDisplayName label
info_string	TEXT	Info properties CFBundleGetInfoString label
minimum_system_version	TEXT	Minimum version of OS X required for the app to run
category	TEXT	The UTI that categorizes the app for the App Store
applescript_enabled	TEXT	Info properties NSAppleScriptEnabled label
copyright	TEXT	Info properties NSHumanReadableCopyright label
last_opened_time	DOUBLE	The time that the app was last used

apt_sources

Current list of APT repositories or software channels.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Repository name
source	TEXT	Source file
base_uri	TEXT	Repository base URI
release	TEXT	Release name
version	TEXT	Repository source version
maintainer	TEXT	Repository maintainer
components	TEXT	Repository components

COLUMN	TYPE	DESCRIPTION
architectures	TEXT	Repository architectures

arp_cache

Address resolution cache, both static and dynamic (from ARP, NDP).

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
address	TEXT	IPv4 address target
mac	TEXT	MAC address of broadcasted address
interface	TEXT	Interface of the network for the MAC
permanent	TEXT	1 for true, 0 for false

asl

Queries the Apple System Log data structure for system events.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
time	INTEGER	Unix timestamp. Set automatically
time_nano_sec	INTEGER	Nanosecond time.
host	TEXT	Sender's address (set by the server).
sender	TEXT	Sender's identification string. Default is process name.
facility	TEXT	Sender's facility. Default is 'user'.
pid	INTEGER	Sending process ID encoded as a string. Set automatically.
gid	BIGINT	GID that sent the log message (set by the server).
uid	BIGINT	UID that sent the log message (set by the server).

COLUMN	TYPE	DESCRIPTION
level	INTEGER	Log level number. See levels in asl.h.
message	TEXT	Message text.
ref_pid	INTEGER	Reference PID for messages proxied by launchd
ref_proc	TEXT	Reference process for messages proxied by launchd
extra	TEXT	Extra columns, in JSON format. Queries against this column are performed entirely in SQLite, so do not benefit from efficient querying via asl.h.

atom_packages

Lists all atom packages in a directory or globally installed in a system.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Package display name
version	TEXT	Package supplied version
description	TEXT	Package supplied description
path	TEXT	Package's package.json path
license	TEXT	License for package
homepage	TEXT	Package supplied homepage
uid	BIGINT	The local user that owns the plugin

augeas

Configuration files parsed by augeas.

Improve this Description on Github

COLUMN COLUMN	TYPE TYPE	DESCRIPTION DESCRIPTION
node	TEXT	The node path of the configuration item
value	TEXT	The value of the configuration item
label	TEXT	The label of the configuration item
path	TEXT	The path to the configuration file

authenticode

File (executable, bundle, installer, disk) code signing status.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
path	TEXT	Must provide a path or directory
original_program_name	TEXT	The original program name that the publisher has signed
serial_number	TEXT	The certificate serial number
issuer_name	TEXT	The certificate issuer name
subject_name	TEXT	The certificate subject name
result	TEXT	The signature check result

authorization_mechanisms

OS X Authorization mechanisms database.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
label	TEXT	Label of the authorization right

COLUMN	TYPE	DESCRIPTION
plugin	TEXT	Authorization plugin name
mechanism	TEXT	Name of the mechanism that will be called
privileged	TEXT	If privileged it will run as root, else as an anonymous user
entry	TEXT	The whole string entry

authorizations

OS X Authorization rights database.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
label	TEXT	Item name, usually in reverse domain format
modified	TEXT	Label top-level key
allow_root	TEXT	Label top-level key
timeout	TEXT	Label top-level key
version	TEXT	Label top-level key
tries	TEXT	Label top-level key
authenticate_user	TEXT	Label top-level key
shared	TEXT	Label top-level key
comment	TEXT	Label top-level key
created	TEXT	Label top-level key
class	TEXT	Label top-level key

session_owner COLUMN	TEXT TYPE	Label top-level key DESCRIPTION

authorized_keys

A line-delimited authorized_keys table.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
uid	BIGINT	The local owner of authorized_keys file
algorithm	TEXT	algorithm of key
key	TEXT	parsed authorized keys line
key_file	TEXT	Path to the authorized_keys file

autoexec

Aggregate of executables that will automatically execute on the target machine. This is an amalgamation of other tables like services, scheduled_tasks, startup_items and more.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
path	TEXT	Path to the executable
name	TEXT	Name of the program
source	TEXT	Source table of the autoexec item

azure_instance_metadata

Azure instance metadata.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
location	TEXT	Azure Region the VM is running in

name COLUMN	TEXT TYPE	Name of the VM DESCRIPTION
offer	TEXT	Offer information for the VM image (Azure image gallery VMs only)
publisher	TEXT	Publisher of the VM image
sku	TEXT	SKU for the VM image
version	TEXT	Version of the VM image
os_type	TEXT	Linux or Windows
platform_update_domain	TEXT	Update domain the VM is running in
platform_fault_domain	TEXT	Fault domain the VM is running in
vm_id	TEXT	Unique identifier for the VM
vm_size	TEXT	VM size
subscription_id	TEXT	Azure subscription for the VM
resource_group_name	TEXT	Resource group for the VM
placement_group_id	TEXT	Placement group for the VM scale set
vm_scale_set_name	TEXT	VM scale set name
zone	TEXT	Availability zone of the VM

azure_instance_tags

Azure instance tags.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION

vm_id COLUMN	TEXT TYPE	Unique identifier for the VM DESCRIPTION

key	TEXT	The tag key
value	TEXT	The tag value

background_activities_moderator

Background Activities Moderator (BAM) tracks application execution.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
path	TEXT	Application file path.
last_execution_time	INTEGER	Most recent time application was executed.
sid	TEXT	User SID.

battery

Provides information about the internal battery of a Macbook.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
manufacturer	TEXT	The battery manufacturer's name
manufacture_date	INTEGER	The date the battery was manufactured UNIX Epoch
model	TEXT	The battery's model number
serial_number	TEXT	The battery's unique serial number
cycle_count	INTEGER	The number of charge/discharge cycles
		One of the following: "Good" describes a well-performing battery,

COLUMN	TYPE	DESCRIPTION
health	TEXT	"Fair" describes a functional battery with limited capacity, or "Poor" describes a battery that's not capable of providing power
condition	TEXT	One of the following: "Normal" indicates the condition of the battery is within normal tolerances, "Service Needed" indicates that the battery should be checked out by a licensed Mac repair service, "Permanent Failure" indicates the battery needs replacement
state	TEXT	One of the following: "AC Power" indicates the battery is connected to an external power source, "Battery Power" indicates that the battery is drawing internal power, "Off Line" indicates the battery is off-line or no longer connected
charging	INTEGER	1 if the battery is currently being charged by a power source. 0 otherwise
charged	INTEGER	1 if the battery is currently completely charged. 0 otherwise
designed_capacity	INTEGER	The battery's designed capacity in mAh
max_capacity	INTEGER	The battery's actual capacity when it is fully charged in mAh
current_capacity	INTEGER	The battery's current charged capacity in mAh
percent_remaining	INTEGER	The percentage of battery remaining before it is drained
amperage	INTEGER	The battery's current amperage in mA
voltage	INTEGER	The battery's current voltage in mV
minutes_until_empty	INTEGER	The number of minutes until the battery is fully depleted. This value is -1 if this time is still being calculated
minutes_to_full_charge	INTEGER	The number of minutes until the battery is fully charged. This value is -1 if this time is still being calculated

bitlocker_info

Retrieve bitlocker status of the machine.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
device_id	TEXT	ID of the encrypted drive.
drive_letter	TEXT	Drive letter of the encrypted drive.
persistent_volume_id	TEXT	Persistent ID of the drive.
conversion_status	INTEGER	The bitlocker conversion status of the drive.
protection_status	INTEGER	The bitlocker protection status of the drive.
encryption_method	TEXT	The encryption type of the device.
version	INTEGER	The FVE metadata version of the drive.
percentage_encrypted	INTEGER	The percentage of the drive that is encrypted.
lock_status	INTEGER	The accessibility status of the drive from Windows.

block_devices

Block (buffered access) device file nodes: disks, ramdisks, and DMG containers.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Block device name
parent	TEXT	Block device parent name
vendor	TEXT	Block device vendor string
model	TEXT	Block device model string identifier
size	BIGINT	Block device size in blocks

block_size COLUMN	INTEGER TYPE	Block size in bytes DESCRIPTION
uuid	TEXT	Block device Universally Unique Identifier
type	TEXT	Block device type string
label	TEXT	Block device label string

browser_plugins

All C/NPAPI browser plugin details for all users.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
uid	BIGINT	The local user that owns the plugin
name	TEXT	Plugin display name
identifier	TEXT	Plugin identifier
version	TEXT	Plugin short version
sdk	TEXT	Build SDK used to compile plugin
description	TEXT	Plugin description text
development_region	TEXT	Plugin language-localization
native	INTEGER	Plugin requires native execution
path	TEXT	Path to plugin bundle
disabled	INTEGER	Is the plugin disabled. 1 = Disabled

carbon_black_info

Returns info about a Carbon Black sensor install.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
sensor_id	INTEGER	Sensor ID of the Carbon Black sensor
config_name	TEXT	Sensor group
collect_store_files	INTEGER	If the sensor is configured to send back binaries to the Carbon Black server
collect_module_loads	INTEGER	If the sensor is configured to capture module loads
collect_module_info	INTEGER	If the sensor is configured to collect metadata of binaries
collect_file_mods	INTEGER	If the sensor is configured to collect file modification events
collect_reg_mods	INTEGER	If the sensor is configured to collect registry modification events
collect_net_conns	INTEGER	If the sensor is configured to collect network connections
collect_processes	INTEGER	If the sensor is configured to process events
collect_cross_processes	INTEGER	If the sensor is configured to cross process events
collect_emet_events	INTEGER	If the sensor is configured to EMET events
collect_data_file_writes	INTEGER	If the sensor is configured to collect non binary file writes
collect_process_user_context	INTEGER	If the sensor is configured to collect the user running a process
collect_sensor_operations	INTEGER	Unknown
log_file_disk_quota_mb	INTEGER	Event file disk quota in MB
log_file_disk_quota_percentage	INTEGER	Event file disk quota in a percentage
protection_disabled	INTEGER	If the sensor is configured to report tamper events

COLUMN	TYPE	DESCRIPTION
sensor_ip_addr	TEXT	IP address of the sensor
sensor_backend_server	TEXT	Carbon Black server
event_queue	INTEGER	Size in bytes of Carbon Black event files on disk
binary_queue	INTEGER	Size in bytes of binaries waiting to be sent to Carbon Black server

carves

List the set of completed and in-progress carves. If carve=1 then the query is treated as a new carve request.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
time	BIGINT	Time at which the carve was kicked off
sha256	TEXT	A SHA256 sum of the carved archive
size	INTEGER	Size of the carved archive
path	TEXT	The path of the requested carve
status	TEXT	Status of the carve, can be STARTING, PENDING, SUCCESS, or FAILED
carve_guid	TEXT	Identifying value of the carve session
carve	INTEGER	Set this value to '1' to start a file carve

certificates

Certificate Authorities installed in Keychains/ca-bundles.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION

COLUMN	TYPE	DESCRIPTION
common_name	TEXT	Certificate CommonName
subject	TEXT	Certificate distinguished name
issuer	TEXT	Certificate issuer distinguished name
ca	INTEGER	1 if CA: true (certificate is an authority) else 0
self_signed	INTEGER	1 if self-signed, else 0
not_valid_before	TEXT	Lower bound of valid date
not_valid_after	TEXT	Certificate expiration data
signing_algorithm	TEXT	Signing algorithm used
key_algorithm	TEXT	Key algorithm used
key_strength	TEXT	Key size used for RSA/DSA, or curve name
key_usage	TEXT	Certificate key usage and extended key usage
subject_key_id	TEXT	SKID an optionally included SHA1
authority_key_id	TEXT	AKID an optionally included SHA1
sha1	TEXT	SHA1 hash of the raw certificate contents
path	TEXT	Path to Keychain or PEM bundle
serial	TEXT	Certificate serial number
sid	TEXT	SID
store_location	TEXT	Certificate system store location
store	TEXT	Certificate system store

COLUMN	TYPE	DESCRIPTION
username	TEXT	Username
store_id	TEXT	Exists for service/user stores. Contains raw store id provided by WinAPI.

chassis_info

Display information pertaining to the chassis and its security status.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
audible_alarm	TEXT	If TRUE, the frame is equipped with an audible alarm.
breach_description	TEXT	If provided, gives a more detailed description of a detected security breach.
chassis_types	TEXT	A comma-separated list of chassis types, such as Desktop or Laptop.
description	TEXT	An extended description of the chassis if available.
lock	TEXT	If TRUE, the frame is equipped with a lock.
manufacturer	TEXT	The manufacturer of the chassis.
model	TEXT	The model of the chassis.
security_breach	TEXT	The physical status of the chassis such as Breach Successful, Breach Attempted, etc.
serial	TEXT	The serial number of the chassis.
smbios_tag	TEXT	The assigned asset tag number of the chassis.
sku	TEXT	The Stock Keeping Unit number if available.
status	TEXT	If available, gives various operational or nonoperational statuses such as OK, Degraded, and Pred Fail.
visible_alarm	TEXT	If TRUE, the frame is equipped with a visual alarm.

COLUMN	TYPE	DESCRIPTION

chocolatey_packages

Chocolatey packages installed in a system.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Package display name
version	TEXT	Package-supplied version
summary	TEXT	Package-supplied summary
author	TEXT	Optional package author
license	TEXT	License under which package is launched
path	TEXT	Path at which this package resides

chrome_extension_content_scripts

Chrome browser extension content scripts.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
uid	BIGINT	The local user that owns the extension
identifier	TEXT	Extension identifier
version	TEXT	Extension-supplied version
script	TEXT	The content script used by the extension
match	TEXT	The pattern that the script is matched against

chrome_extensions

Chrome browser extensions.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
uid	BIGINT	The local user that owns the extension
name	TEXT	Extension display name
profile	TEXT	The Chrome profile that contains this extension
identifier	TEXT	Extension identifier
version	TEXT	Extension-supplied version
description	TEXT	Extension-optional description
locale	TEXT	Default locale supported by extension
update_url	TEXT	Extension-supplied update URI
author	TEXT	Optional extension author
persistent	INTEGER	1 If extension is persistent across all tabs else 0
path	TEXT	Path to extension folder
permissions	TEXT	The permissions required by the extension
optional_permissions	TEXT	The permissions optionally required by the extensions

connectivity

Provides the overall system's network state.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
disconnected	INTEGER	True if the all interfaces are not connected to any network

COLUMN	TYPE	DESCRIPTION
ipv4_no_traffic	INTEGER	True if any interface is connected via IPv4, but has seen no traffic
ipv6_no_traffic	INTEGER	True if any interface is connected via IPv6, but has seen no traffic
ipv4_subnet	INTEGER	True if any interface is connected to the local subnet via IPv4
ipv4_local_network	INTEGER	True if any interface is connected to a routed network via IPv4
ipv4_internet	INTEGER	True if any interface is connected to the Internet via IPv4
ipv6_subnet	INTEGER	True if any interface is connected to the local subnet via IPv6
ipv6_local_network	INTEGER	True if any interface is connected to a routed network via IPv6
ipv6_internet	INTEGER	True if any interface is connected to the Internet via IPv6

cpu_info

Retrieve cpu hardware info of the machine.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
device_id	TEXT	The DeviceID of the CPU.
model	TEXT	The model of the CPU.
manufacturer	TEXT	The manufacturer of the CPU.
processor_type	TEXT	The processor type, such as Central, Math, or Video.
availability	TEXT	The availability and status of the CPU.
cpu_status	INTEGER	The current operating status of the CPU.
number_of_cores	TEXT	The number of cores of the CPU.

COLUMN	TYPE	DESCRIPTION
logical_processors	INTEGER	The number of logical processors of the CPU.
address_width	TEXT	The width of the CPU address bus.
current_clock_speed	INTEGER	The current frequency of the CPU.
max_clock_speed	INTEGER	The maximum possible frequency of the CPU.
socket_designation	TEXT	The assigned socket on the board for the given CPU.

cpu_time

Displays information from /proc/stat file about the time the cpu cores spent in different parts of the system.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
core	INTEGER	Name of the cpu (core)
user	BIGINT	Time spent in user mode
nice	BIGINT	Time spent in user mode with low priority (nice)
system	BIGINT	Time spent in system mode
idle	BIGINT	Time spent in the idle task
iowait	BIGINT	Time spent waiting for I/O to complete
irq	BIGINT	Time spent servicing interrupts
softirq	BIGINT	Time spent servicing softirqs
steal	BIGINT	Time spent in other operating systems when running in a virtualized environment
	BIGINT	Time spent running a virtual CPU for a guest OS under the control of the Linux

COLUMN	TYPE	DESCRIPTION
guest	BIGINT	kernel
guest_nice	BIGINT	Time spent running a niced guest

cpuid

Useful CPU features from the cpuid ASM call.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
feature	TEXT	Present feature flags
value	TEXT	Bit value or string
output_register	TEXT	Register used to for feature value
output_bit	INTEGER	Bit in register value for feature value
input_eax	TEXT	Value of EAX used

crashes

Application, System, and Mobile App crash logs.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
type	TEXT	Type of crash log
pid	BIGINT	Process (or thread) ID of the crashed process
path	TEXT	Path to the crashed process
crash_path	TEXT	Location of log file
identifier	TEXT	Identifier of the crashed process

COLUMN	TYPE	DESCRIPTION
version	TEXT	Version info of the crashed process
parent	BIGINT	Parent PID of the crashed process
responsible	TEXT	Process responsible for the crashed process
uid	INTEGER	User ID of the crashed process
datetime	TEXT	Date/Time at which the crash occurred
crashed_thread	BIGINT	Thread ID which crashed
stack_trace	TEXT	Most recent frame from the stack trace
exception_type	TEXT	Exception type of the crash
exception_codes	TEXT	Exception codes from the crash
exception_notes	TEXT	Exception notes from the crash
registers	TEXT	The value of the system registers

crontab

Line parsed values from system and user cron/tab.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
event	TEXT	The job @event name (rare)
minute	TEXT	The exact minute for the job
hour	TEXT	The hour of the day for the job
day_of_month	TEXT	The day of the month for the job

month COLUMN	TEXT TYPE	The month of the year for the job DESCRIPTION
day_of_week	TEXT	The day of the week for the job
command	TEXT	Raw command string
path	TEXT	File parsed

cups_destinations

Returns all configured printers.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Name of the printer
option_name	TEXT	Option name
option_value	TEXT	Option value

cups_jobs

Returns all completed print jobs from cups.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
title	TEXT	Title of the printed job
destination	TEXT	The printer the job was sent to
user	TEXT	The user who printed the job
format	TEXT	The format of the print job
size	INTEGER	The size of the print job

COLUMN	TYPE	DESCRIPTION
completed_time	INTEGER	When the job completed printing
processing_time	INTEGER	How long the job took to process
creation_time	INTEGER	When the print request was initiated

curl

Perform an http request and return stats about it.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
url	TEXT	The url for the request
method	TEXT	The HTTP method for the request
user_agent	TEXT	The user-agent string to use for the request
response_code	INTEGER	The HTTP status code for the response
round_trip_time	BIGINT	Time taken to complete the request
bytes	BIGINT	Number of bytes in the response
result	TEXT	The HTTP response body

curl_certificate

Inspect TLS certificates by connecting to input hostnames.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
hostname	TEXT	Hostname (domain[:port]) to CURL
common_name	TEXT	Common name of company issued to

COLUMN	TYPE	DESCRIPTION
organization	TEXT	Organization issued to
organization_unit	TEXT	Organization unit issued to
serial_number	TEXT	Certificate serial number
issuer_common_name	TEXT	Issuer common name
issuer_organization	TEXT	Issuer organization
issuer_organization_unit	TEXT	Issuer organization unit
valid_from	TEXT	Period of validity start date
valid_to	TEXT	Period of validity end date
sha256_fingerprint	TEXT	SHA-256 fingerprint
sha1_fingerprint	TEXT	SHA1 fingerprint
version	INTEGER	Version Number
signature_algorithm	TEXT	Signature Algorithm
signature	TEXT	Signature
subject_key_identifier	TEXT	Subject Key Identifier
authority_key_identifier	TEXT	Authority Key Identifier
key_usage	TEXT	Usage of key in certificate
extended_key_usage	TEXT	Extended usage of key in certificate
policies	TEXT	Certificate Policies
subject_alternative_names	TEXT	Subject Alternative Name

COLUMN	TYPE	DESCRIPTION
issuer_alternative_names	TEXT	Issuer Alternative Name
info_access	TEXT	Authority Information Access
subject_info_access	TEXT	Subject Information Access
policy_mappings	TEXT	Policy Mappings
has_expired	INTEGER	1 if the certificate has expired, 0 otherwise
basic_constraint	TEXT	Basic Constraints
name_constraints	TEXT	Name Constraints
policy_constraints	TEXT	Policy Constraints
dump_certificate	INTEGER	Set this value to '1' to dump certificate
timeout	INTEGER	Set this value to the timeout in seconds to complete the TLS handshake (default 4s, use 0 for no timeout)
pem	TEXT	Certificate PEM format

deb_packages

The installed DEB package database.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Package name
version	TEXT	Package version
source	TEXT	Package source
size	BIGINT	Package size in bytes

COLUMN	TYPE	DESCRIPTION
arch	TEXT	Package architecture
revision	TEXT	Package revision
status	TEXT	Package status
maintainer	TEXT	Package maintainer
section	TEXT	Package section
priority	TEXT	Package priority
pid_with_namespace	INTEGER	Pids that contain a namespace
mount_namespace_id	TEXT	Mount namespace id

default_environment

Default environment variables and values.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
variable	TEXT	Name of the environment variable
value	TEXT	Value of the environment variable
expand	INTEGER	1 if the variable needs expanding, 0 otherwise

device_file

Similar to the file table, but use TSK and allow block address access.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
device	TEXT	Absolute file path to device node

COLUMN	TYPE	DESCRIPTION
partition	TEXT	A partition number
path	TEXT	A logical path within the device node
filename	TEXT	Name portion of file path
inode	BIGINT	Filesystem inode number
uid	BIGINT	Owning user ID
gid	BIGINT	Owning group ID
mode	TEXT	Permission bits
size	BIGINT	Size of file in bytes
block_size	INTEGER	Block size of filesystem
atime	BIGINT	Last access time
mtime	BIGINT	Last modification time
ctime	BIGINT	Creation time
hard_links	INTEGER	Number of hard links
type	TEXT	File status

device_firmware

A best-effort list of discovered firmware versions.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
type	TEXT	Type of device

device COLUMN	TEXT TYPE	The device name DESCRIPTION
version	TEXT	Firmware version

device_hash

Similar to the hash table, but use TSK and allow block address access.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
device	TEXT	Absolute file path to device node
partition	TEXT	A partition number
inode	BIGINT	Filesystem inode number
md5	TEXT	MD5 hash of provided inode data
sha1	TEXT	SHA1 hash of provided inode data
sha256	TEXT	SHA256 hash of provided inode data

device_partitions

Use TSK to enumerate details about partitions on a disk device.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
device	TEXT	Absolute file path to device node
partition	INTEGER	A partition number or description
label	TEXT	
type	TEXT	

COLUMN	TYPE	DESCRIPTION
offset	BIGINT	
blocks_size	BIGINT	Byte size of each block
blocks	BIGINT	Number of blocks
inodes	BIGINT	Number of meta nodes
flags	INTEGER	

disk_encryption

Disk encryption status and information.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Disk name
uuid	TEXT	Disk Universally Unique Identifier
encrypted	INTEGER	1 If encrypted: true (disk is encrypted), else 0
type	TEXT	Description of cipher type and mode if available
uid	TEXT	Currently authenticated user if available (Apple)
user_uuid	TEXT	UUID of authenticated user if available (Apple)
encryption_status	TEXT	Disk encryption status with one of following values: encrypted | not encrypted | undefined

disk_events (EVENTED TABLE)

Track DMG disk image events (appearance/disappearance) when opened.

Improve this Description on Github

COLUMN COLUMN	TYPE TYPE	DESCRIPTION DESCRIPTION
action	TEXT	Appear or disappear
path	TEXT	Path of the DMG file accessed
name	TEXT	Disk event name
device	TEXT	Disk event BSD name
uuid	TEXT	UUID of the volume inside DMG if available
size	BIGINT	Size of partition in bytes
ejectable	INTEGER	1 if ejectable, 0 if not
mountable	INTEGER	1 if mountable, 0 if not
writable	INTEGER	1 if writable, 0 if not
content	TEXT	Disk event content
media_name	TEXT	Disk event media name string
vendor	TEXT	Disk event vendor string
filesystem	TEXT	Filesystem if available
checksum	TEXT	UDIF Master checksum if available (CRC32)
time	BIGINT	Time of appearance/disappearance in UNIX time
eid	TEXT	Event ID

disk_info

Retrieve basic information about the physical disks of a system.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
partitions	INTEGER	Number of detected partitions on disk.
disk_index	INTEGER	Physical drive number of the disk.
type	TEXT	The interface type of the disk.
id	TEXT	The unique identifier of the drive on the system.
pnp_device_id	TEXT	The unique identifier of the drive on the system.
disk_size	BIGINT	Size of the disk.
manufacturer	TEXT	The manufacturer of the disk.
hardware_model	TEXT	Hard drive model.
name	TEXT	The label of the disk object.
serial	TEXT	The serial number of the disk.
description	TEXT	The OS's description of the disk.

dns_cache

Enumerate the DNS cache using the undocumented DnsGetCacheDataTable function in dnsapi.dll.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	DNS record name
type	TEXT	DNS record type
flags	INTEGER	DNS record flags

dns_resolvers

Resolvers used by this host.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
id	INTEGER	Address type index or order
type	TEXT	Address type: sortlist, nameserver, search
address	TEXT	Resolver IP/IPv6 address
netmask	TEXT	Address (sortlist) netmask length
options	BIGINT	Resolver options

docker_container_fs_changes

Changes to files or directories on container's filesystem.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
id	TEXT	Container ID
path	TEXT	FIle or directory path relative to rootfs
change_type	TEXT	Type of change: C:Modified, A:Added, D:Deleted

docker_container_labels

Docker container labels.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
id	TEXT	Container ID

COLUMN	TYPE	DESCRIPTION
key	TEXT	Label key
value	TEXT	Optional label value

docker_container_mounts

Docker container mounts.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
id	TEXT	Container ID
type	TEXT	Type of mount (bind, volume)
name	TEXT	Optional mount name
source	TEXT	Source path on host
destination	TEXT	Destination path inside container
driver	TEXT	Driver providing the mount
mode	TEXT	Mount options (rw, ro)
rw	INTEGER	1 if read/write. 0 otherwise
propagation	TEXT	Mount propagation

docker_container_networks

Docker container networks.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
id	TEXT	Container ID

COLUMN	TYPE	DESCRIPTION
name	TEXT	Network name
network_id	TEXT	Network ID
endpoint_id	TEXT	Endpoint ID
gateway	TEXT	Gateway
ip_address	TEXT	IP address
ip_prefix_len	INTEGER	IP subnet prefix length
ipv6_gateway	TEXT	IPv6 gateway
ipv6_address	TEXT	IPv6 address
ipv6_prefix_len	INTEGER	IPv6 subnet prefix length
mac_address	TEXT	MAC address

docker_container_ports

Docker container ports.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
id	TEXT	Container ID
type	TEXT	Protocol (tcp, udp)
port	INTEGER	Port inside the container
host_ip	TEXT	Host IP address on which public port is listening
host_port	INTEGER	Host port

docker_container_processes

Docker container processes.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
id	TEXT	Container ID
pid	BIGINT	Process ID
name	TEXT	The process path or shorthand argv[0]
cmdline	TEXT	Complete argv
state	TEXT	Process state
uid	BIGINT	User ID
gid	BIGINT	Group ID
euid	BIGINT	Effective user ID
egid	BIGINT	Effective group ID
suid	BIGINT	Saved user ID
sgid	BIGINT	Saved group ID
wired_size	BIGINT	Bytes of unpagable memory used by process
resident_size	BIGINT	Bytes of private memory used by process
total_size	BIGINT	Total virtual memory size
start_time	BIGINT	Process start in seconds since boot (non-sleeping)
parent	BIGINT	Process parent's PID
pgroup	BIGINT	Process group

COLUMN	TYPE	DESCRIPTION
threads	INTEGER	Number of threads used by process
nice	INTEGER	Process nice level (-20 to 20, default 0)
user	TEXT	User name
time	TEXT	Cumulative CPU time. [DD-]HH:MM:SS format
cpu	DOUBLE	CPU utilization as percentage
mem	DOUBLE	Memory utilization as percentage

docker_container_stats

Docker container statistics. Queries on this table take at least one second.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
id	TEXT	Container ID
name	TEXT	Container name
pids	INTEGER	Number of processes
read	BIGINT	UNIX time when stats were read
preread	BIGINT	UNIX time when stats were last read
interval	BIGINT	Difference between read and preread in nano-seconds
disk_read	BIGINT	Total disk read bytes
disk_write	BIGINT	Total disk write bytes
num_procs	INTEGER	Number of processors

cpu_total_usage COLUMN	BIGINT TYPE	Total CPU usage DESCRIPTION
cpu_kernelmode_usage	BIGINT	CPU kernel mode usage
cpu_usermode_usage	BIGINT	CPU user mode usage
system_cpu_usage	BIGINT	CPU system usage
online_cpus	INTEGER	Online CPUs
pre_cpu_total_usage	BIGINT	Last read total CPU usage
pre_cpu_kernelmode_usage	BIGINT	Last read CPU kernel mode usage
pre_cpu_usermode_usage	BIGINT	Last read CPU user mode usage
pre_system_cpu_usage	BIGINT	Last read CPU system usage
pre_online_cpus	INTEGER	Last read online CPUs
memory_usage	BIGINT	Memory usage
memory_max_usage	BIGINT	Memory maximum usage
memory_limit	BIGINT	Memory limit
network_rx_bytes	BIGINT	Total network bytes read
network_tx_bytes	BIGINT	Total network bytes transmitted

docker_containers

Docker containers information.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION

id COLUMN	TEXT TYPE	Container ID DESCRIPTION
name	TEXT	Container name
image	TEXT	Docker image (name) used to launch this container
image_id	TEXT	Docker image ID
command	TEXT	Command with arguments
created	BIGINT	Time of creation as UNIX time
state	TEXT	Container state (created, restarting, running, removing, paused, exited, dead)
status	TEXT	Container status information
pid	BIGINT	Identifier of the initial process
path	TEXT	Container path
config_entrypoint	TEXT	Container entrypoint(s)
started_at	TEXT	Container start time as string
finished_at	TEXT	Container finish time as string
privileged	INTEGER	Is the container privileged
security_options	TEXT	List of container security options
env_variables	TEXT	Container environmental variables
readonly_rootfs	INTEGER	Is the root filesystem mounted as read only
cgroup_namespace	TEXT	cgroup namespace
ipc_namespace	TEXT	IPC namespace

COLUMN	TYPE	DESCRIPTION
mnt_namespace	TEXT	Mount namespace
net_namespace	TEXT	Network namespace
pid_namespace	TEXT	PID namespace
user_namespace	TEXT	User namespace
uts_namespace	TEXT	UTS namespace

docker_image_labels

Docker image labels.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
id	TEXT	Image ID
key	TEXT	Label key
value	TEXT	Optional label value

docker_image_layers

Docker image layers information.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
id	TEXT	Image ID
layer_id	TEXT	Layer ID
layer_order	INTEGER	Layer Order (1 = base layer)

docker_images

Docker images information.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
id	TEXT	Image ID
created	BIGINT	Time of creation as UNIX time
size_bytes	BIGINT	Size of image in bytes
tags	TEXT	Comma-separated list of repository tags

docker_info

Docker system information.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
id	TEXT	Docker system ID
containers	INTEGER	Total number of containers
containers_running	INTEGER	Number of containers currently running
containers_paused	INTEGER	Number of containers in paused state
containers_stopped	INTEGER	Number of containers in stopped state
images	INTEGER	Number of images
storage_driver	TEXT	Storage driver
memory_limit	INTEGER	1 if memory limit support is enabled. 0 otherwise
swap_limit	INTEGER	1 if swap limit support is enabled. 0 otherwise
kernel_memory	INTEGER	1 if kernel memory limit support is enabled. 0 otherwise

COLUMN	TYPE	DESCRIPTION
cpu_cfs_period	INTEGER	1 if CPU Completely Fair Scheduler (CFS) period support is enabled. 0 otherwise
cpu_cfs_quota	INTEGER	1 if CPU Completely Fair Scheduler (CFS) quota support is enabled. 0 otherwise
cpu_shares	INTEGER	1 if CPU share weighting support is enabled. 0 otherwise
cpu_set	INTEGER	1 if CPU set selection support is enabled. 0 otherwise
ipv4_forwarding	INTEGER	1 if IPv4 forwarding is enabled. 0 otherwise
bridge_nf_iptables	INTEGER	1 if bridge netfilter iptables is enabled. 0 otherwise
bridge_nf_ip6tables	INTEGER	1 if bridge netfilter ip6tables is enabled. 0 otherwise
oom_kill_disable	INTEGER	1 if Out-of-memory kill is disabled. 0 otherwise
logging_driver	TEXT	Logging driver
cgroup_driver	TEXT	Control groups driver
kernel_version	TEXT	Kernel version
os	TEXT	Operating system
os_type	TEXT	Operating system type
architecture	TEXT	Hardware architecture
cpus	INTEGER	Number of CPUs
memory	BIGINT	Total memory
http_proxy	TEXT	HTTP proxy

COLUMN	TYPE	DESCRIPTION
https_proxy	TEXT	HTTPS proxy
no_proxy	TEXT	Comma-separated list of domain extensions proxy should not be used for
name	TEXT	Name of the docker host
server_version	TEXT	Server version
root_dir	TEXT	Docker root directory

docker_network_labels

Docker network labels.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
id	TEXT	Network ID
key	TEXT	Label key
value	TEXT	Optional label value

docker_networks

Docker networks information.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
id	TEXT	Network ID
name	TEXT	Network name
driver	TEXT	Network driver

created COLUMN	BIGINT TYPE	Time of creation as UNIX time DESCRIPTION
enable_ipv6	INTEGER	1 if IPv6 is enabled on this network. 0 otherwise
subnet	TEXT	Network subnet
gateway	TEXT	Network gateway

docker_version

Docker version information.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
version	TEXT	Docker version
api_version	TEXT	API version
min_api_version	TEXT	Minimum API version supported
git_commit	TEXT	Docker build git commit
go_version	TEXT	Go version
os	TEXT	Operating system
arch	TEXT	Hardware architecture
kernel_version	TEXT	Kernel version
build_time	TEXT	Build time

docker_volume_labels

Docker volume labels.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Volume name
key	TEXT	Label key
value	TEXT	Optional label value

docker_volumes

Docker volumes information.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Volume name
driver	TEXT	Volume driver
mount_point	TEXT	Mount point
type	TEXT	Volume type

drivers

Details for in-use Windows device drivers. This does not display installed but unused drivers.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
device_id	TEXT	Device ID
device_name	TEXT	Device name
image	TEXT	Path to driver image file
description	TEXT	Driver description

COLUMN	TYPE	DESCRIPTION
service	TEXT	Driver service name, if one exists
service_key	TEXT	Driver service registry key
version	TEXT	Driver version
inf	TEXT	Associated inf file
class	TEXT	Device/driver class name
provider	TEXT	Driver provider
manufacturer	TEXT	Device manufacturer
driver_key	TEXT	Driver key
date	BIGINT	Driver date
signed	INTEGER	Whether the driver is signed or not

ec2_instance_metadata

EC2 instance metadata.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
instance_id	TEXT	EC2 instance ID
instance_type	TEXT	EC2 instance type
architecture	TEXT	Hardware architecture of this EC2 instance
region	TEXT	AWS region in which this instance launched
availability_zone	TEXT	Availability zone in which this instance launched

COLUMN	TYPE	DESCRIPTION
local_hostname	TEXT	Private IPv4 DNS hostname of the first interface of this instance
local_ipv4	TEXT	Private IPv4 address of the first interface of this instance
mac	TEXT	MAC address for the first network interface of this EC2 instance
security_groups	TEXT	Comma separated list of security group names
iam_arn	TEXT	If there is an IAM role associated with the instance, contains instance profile ARN
ami_id	TEXT	AMI ID used to launch this EC2 instance
reservation_id	TEXT	ID of the reservation
account_id	TEXT	AWS account ID which owns this EC2 instance
ssh_public_key	TEXT	SSH public key. Only available if supplied at instance launch time

ec2_instance_tags

EC2 instance tag key value pairs.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
instance_id	TEXT	EC2 instance ID
key	TEXT	Tag key
value	TEXT	Tag value

elf_dynamic

ELF dynamic section information.

Improve this Description on Github

COLUMN COLUMN	TYPE TYPE	DESCRIPTION DESCRIPTION
tag	INTEGER	Tag ID
value	INTEGER	Tag value
class	INTEGER	Class (32 or 64)
path	TEXT	Path to ELF file

elf_info

ELF file information.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
class	TEXT	Class type, 32 or 64bit
abi	TEXT	Section type
abi_version	INTEGER	Section virtual address in memory
type	TEXT	Offset of section in file
machine	INTEGER	Machine type
version	INTEGER	Object file version
entry	BIGINT	Entry point address
flags	INTEGER	ELF header flags
path	TEXT	Path to ELF file

elf_sections

ELF section information.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Section name
type	INTEGER	Section type
vaddr	INTEGER	Section virtual address in memory
offset	INTEGER	Offset of section in file
size	INTEGER	Size of section
flags	TEXT	Section attributes
link	TEXT	Link to other section
align	INTEGER	Segment alignment
path	TEXT	Path to ELF file

elf_segments

ELF segment information.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Segment type/name
offset	INTEGER	Segment offset in file
vaddr	INTEGER	Segment virtual address in memory
psize	INTEGER	Size of segment in file
msize	INTEGER	Segment offset in memory

flags COLUMN	TEXT TYPE	Segment attributes DESCRIPTION
align	INTEGER	Segment alignment
path	TEXT	Path to ELF file

elf_symbols

ELF symbol list.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Symbol name
addr	INTEGER	Symbol address (value)
size	INTEGER	Size of object
type	TEXT	Symbol type
binding	TEXT	Binding type
offset	INTEGER	Section table index
table	TEXT	Table name containing symbol
path	TEXT	Path to ELF file

etc_hosts

Line-parsed /etc/hosts.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
address	TEXT	IP address mapping

COLUMN	TYPE	DESCRIPTION
hostnames	TEXT	Raw hosts mapping

etc_protocols

Line-parsed /etc/protocols.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Protocol name
number	INTEGER	Protocol number
alias	TEXT	Protocol alias
comment	TEXT	Comment with protocol description

etc_services

Line-parsed /etc/services.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Service name
port	INTEGER	Service port number
protocol	TEXT	Transport protocol (TCP/UDP)
aliases	TEXT	Optional space separated list of other names for a service
comment	TEXT	Optional comment for a service.

event_taps

Returns information about installed event taps.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
COLUMN	TYPE	DESCRIPTION
enabled	INTEGER	Is the Event Tap enabled
event_tap_id	INTEGER	Unique ID for the Tap
event_tapped	TEXT	The mask that identifies the set of events to be observed.
process_being_tapped	INTEGER	The process ID of the target application
tapping_process	INTEGER	The process ID of the application that created the event tap.

example (EVENTED TABLE)

This is an example table spec.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Description for name column
points	INTEGER	This is a signed SQLite int column
size	BIGINT	This is a signed SQLite bigint column
action	TEXT	Action performed in generation
id	INTEGER	An index of some sort
path	TEXT	Path of example

extended_attributes

Returns the extended attributes for files (similar to Windows ADS).

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION

COLUMN	TYPE	DESCRIPTION
path	TEXT	Absolute file path
directory	TEXT	Directory of file(s)
key	TEXT	Name of the value generated from the extended attribute
value	TEXT	The parsed information from the attribute
base64	INTEGER	1 if the value is base64 encoded else 0

fan_speed_sensors

Fan speeds.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
fan	TEXT	Fan number
name	TEXT	Fan name
actual	INTEGER	Actual speed
min	INTEGER	Minimum speed
max	INTEGER	Maximum speed
target	INTEGER	Target speed

fbsd_kmods

Loaded FreeBSD kernel modules.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Module name

COLUMN	TYPE	DESCRIPTION
size	INTEGER	Size of module content
refs	INTEGER	Module reverse dependencies
address	TEXT	Kernel module address

file

Interactive filesystem attributes and metadata.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
path	TEXT	Absolute file path
directory	TEXT	Directory of file(s)
filename	TEXT	Name portion of file path
inode	BIGINT	Filesystem inode number
uid	BIGINT	Owning user ID
gid	BIGINT	Owning group ID
mode	TEXT	Permission bits
device	BIGINT	Device ID (optional)
size	BIGINT	Size of file in bytes
block_size	INTEGER	Block size of filesystem
atime	BIGINT	Last access time
mtime	BIGINT	Last modification time

COLUMN	TYPE	DESCRIPTION
ctime	BIGINT	Last status change time
btime	BIGINT	(B)irth or (cr)eate time
hard_links	INTEGER	Number of hard links
symlink	INTEGER	1 if the path is a symlink, otherwise 0
type	TEXT	File status
attributes	TEXT	File attrib string. See: https://ss64.com/nt/attrib.html
volume_serial	TEXT	Volume serial number
file_id	TEXT	file ID
file_version	TEXT	File version
product_version	TEXT	File product version
bsd_flags	TEXT	The BSD file flags (chflags). Possible values: NODUMP, UF_IMMUTABLE, UF_APPEND, OPAQUE, HIDDEN, ARCHIVED, SF_IMMUTABLE, SF_APPEND
pid_with_namespace	INTEGER	Pids that contain a namespace
mount_namespace_id	TEXT	Mount namespace id

file_events (EVENTED TABLE)

Track time/action changes to files specified in configuration data.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
target_path	TEXT	The path associated with the event
category	TEXT	The category of the file defined in the config

COLUMN	TYPE	DESCRIPTION
action	TEXT	Change action (UPDATE, REMOVE, etc)
transaction_id	BIGINT	ID used during bulk update
inode	BIGINT	Filesystem inode number
uid	BIGINT	Owning user ID
gid	BIGINT	Owning group ID
mode	TEXT	Permission bits
size	BIGINT	Size of file in bytes
atime	BIGINT	Last access time
mtime	BIGINT	Last modification time
ctime	BIGINT	Last status change time
md5	TEXT	The MD5 of the file after change
sha1	TEXT	The SHA1 of the file after change
sha256	TEXT	The SHA256 of the file after change
hashed	INTEGER	1 if the file was hashed, 0 if not, -1 if hashing failed
time	BIGINT	Time of file event
eid	TEXT	Event ID

firefox_addons

Firefox browser extensions, webapps, and addons.

Improve this Description on Github

COLUMN COLUMN	TYPE TYPE	DESCRIPTION DESCRIPTION
uid	BIGINT	The local user that owns the addon
name	TEXT	Addon display name
identifier	TEXT	Addon identifier
creator	TEXT	Addon-supported creator string
type	TEXT	Extension, addon, webapp
version	TEXT	Addon-supplied version string
description	TEXT	Addon-supplied description string
source_url	TEXT	URL that installed the addon
visible	INTEGER	1 If the addon is shown in browser else 0
active	INTEGER	1 If the addon is active else 0
disabled	INTEGER	1 If the addon is application-disabled else 0
autoupdate	INTEGER	1 If the addon applies background updates else 0
native	INTEGER	1 If the addon includes binary components else 0
location	TEXT	Global, profile location
path	TEXT	Path to plugin bundle

gatekeeper

OS X Gatekeeper Details.

Improve this Description on Github

COLUMN COLUMN	TYPE TYPE	DESCRIPTION DESCRIPTION
assessments_enabled	INTEGER	1 If a Gatekeeper is enabled else 0
dev_id_enabled	INTEGER	1 If a Gatekeeper allows execution from identified developers else 0
version	TEXT	Version of Gatekeeper's gke.bundle
opaque_version	TEXT	Version of Gatekeeper's gkopaque.bundle

gatekeeper_approved_apps

Gatekeeper apps a user has allowed to run.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
path	TEXT	Path of executable allowed to run
requirement	TEXT	Code signing requirement language
ctime	DOUBLE	Last change time
mtime	DOUBLE	Last modification time

groups

Local system groups.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
gid	BIGINT	Unsigned int64 group ID
gid_signed	BIGINT	A signed int64 version of gid
groupname	TEXT	Canonical local group name

COLUMN	TYPE	DESCRIPTION
group_sid	TEXT	Unique group ID
comment	TEXT	Remarks or comments associated with the group
is_hidden	INTEGER	IsHidden attribute set in OpenDirectory

hardware_events (EVENTED TABLE)

Hardware (PCI/USB/HID) events from UDEV or IOKit.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
action	TEXT	Remove, insert, change properties, etc
path	TEXT	Local device path assigned (optional)
type	TEXT	Type of hardware and hardware event
driver	TEXT	Driver claiming the device
vendor	TEXT	Hardware device vendor
vendor_id	TEXT	Hex encoded Hardware vendor identifier
model	TEXT	Hardware device model
model_id	TEXT	Hex encoded Hardware model identifier
serial	TEXT	Device serial (optional)
revision	TEXT	Device revision (optional)
time	BIGINT	Time of hardware event
eid	TEXT	Event ID

hash

Filesystem hash data.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
path	TEXT	Must provide a path or directory
directory	TEXT	Must provide a path or directory
md5	TEXT	MD5 hash of provided filesystem data
sha1	TEXT	SHA1 hash of provided filesystem data
sha256	TEXT	SHA256 hash of provided filesystem data
ssdeep	TEXT	ssdeep hash of provided filesystem data
pid_with_namespace	INTEGER	Pids that contain a namespace
mount_namespace_id	TEXT	Mount namespace id

homebrew_packages

The installed homebrew package database.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Package name
path	TEXT	Package install path
version	TEXT	Current 'linked' version

hvci_status

Retrieve HVCI info of the machine.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
version	TEXT	The version number of the Device Guard build.
instance_identifier	TEXT	The instance ID of Device Guard.
vbs_status	TEXT	The status of the virtualization based security settings. Returns UNKNOWN if an error is encountered.
code_integrity_policy_enforcement_status	TEXT	The status of the code integrity policy enforcement settings. Returns UNKNOWN if an error is encountered.
umci_policy_status	TEXT	The status of the User Mode Code Integrity security settings. Returns UNKNOWN if an error is encountered.

ibridge_info

Information about the Apple iBridge hardware controller.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
boot_uuid	TEXT	Boot UUID of the iBridge controller
coprocessor_version	TEXT	The manufacturer and chip version
firmware_version	TEXT	The build version of the firmware
unique_chip_id	TEXT	Unique id of the iBridge controller

ie_extensions

Internet Explorer browser extensions.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION

COLUMN	TYPE	DESCRIPTION
name	TEXT	Extension display name
registry_path	TEXT	Extension identifier
version	TEXT	Version of the executable
path	TEXT	Path to executable

intel_me_info

Intel ME/CSE Info.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
version	TEXT	Intel ME version

interface_addresses

Network interfaces and relevant metadata.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
interface	TEXT	Interface name
address	TEXT	Specific address for interface
mask	TEXT	Interface netmask
broadcast	TEXT	Broadcast address for the interface
point_to_point	TEXT	PtP address for the interface
type	TEXT	Type of address. One of dhcp, manual, auto, other, unknown

COLUMN	TYPE	DESCRIPTION
friendly_name	TEXT	The friendly display name of the interface.

interface_details

Detailed information and stats of network interfaces.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
interface	TEXT	Interface name
mac	TEXT	MAC of interface (optional)
type	INTEGER	Interface type (includes virtual)
mtu	INTEGER	Network MTU
metric	INTEGER	Metric based on the speed of the interface
flags	INTEGER	Flags (netdevice) for the device
ipackets	BIGINT	Input packets
opackets	BIGINT	Output packets
ibytes	BIGINT	Input bytes
obytes	BIGINT	Output bytes
ierrors	BIGINT	Input errors
oerrors	BIGINT	Output errors
idrops	BIGINT	Input drops
odrops	BIGINT	Output drops
collisions	BIGINT	Packet Collisions detected
last_change	BIGINT	Time of last device modification (optional)

COLUMN	TYPE	DESCRIPTION
link_speed	BIGINT	Interface speed in Mb/s
pci_slot	TEXT	PCI slot number
friendly_name	TEXT	The friendly display name of the interface.
description	TEXT	Short description of the object a one-line string.
manufacturer	TEXT	Name of the network adapter's manufacturer.
connection_id	TEXT	Name of the network connection as it appears in the Network Connections Control Panel program.
connection_status	TEXT	State of the network adapter connection to the network.
enabled	INTEGER	Indicates whether the adapter is enabled or not.
physical_adapter	INTEGER	Indicates whether the adapter is a physical or a logical adapter.
speed	INTEGER	Estimate of the current bandwidth in bits per second.
service	TEXT	The name of the service the network adapter uses.
dhcp_enabled	INTEGER	If TRUE, the dynamic host configuration protocol (DHCP) server automatically assigns an IP address to the computer system when establishing a network connection.
dhcp_lease_expires	TEXT	Expiration date and time for a leased IP address that was assigned to the computer by the dynamic host configuration protocol (DHCP) server.
dhcp_lease_obtained	TEXT	Date and time the lease was obtained for the IP address assigned to the computer by the dynamic host configuration protocol (DHCP) server.
dhcp_server	TEXT	IP address of the dynamic host configuration protocol (DHCP) server.
		Organization name followed by a period and an extension

COLUMN	TYPE	DESCRIPTION
dns_domain	TEXT	Organization name followed by a period and an extension that indicates the type of organization, such as 'microsoft.com'.
dns_domain_suffix_search_order	TEXT	Array of DNS domain suffixes to be appended to the end of host names during name resolution.
dns_host_name	TEXT	Host name used to identify the local computer for authentication by some utilities.
dns_server_search_order	TEXT	Array of server IP addresses to be used in querying for DNS servers.

interface_ipv6

IPv6 configuration and stats of network interfaces.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
interface	TEXT	Interface name
hop_limit	INTEGER	Current Hop Limit
forwarding_enabled	INTEGER	Enable IP forwarding
redirect_accept	INTEGER	Accept ICMP redirect messages
rtadv_accept	INTEGER	Accept ICMP Router Advertisement

iokit_devicetree

The IOKit registry matching the DeviceTree plane.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Device node name
class	TEXT	Best matching device class (most-specific category)

COLUMN	TYPE	DESCRIPTION
id	BIGINT	IOKit internal registry ID
parent	BIGINT	Parent device registry ID
device_path	TEXT	Device tree path
service	INTEGER	1 if the device conforms to IOService else 0
busy_state	INTEGER	1 if the device is in a busy state else 0
retain_count	INTEGER	The device reference count
depth	INTEGER	Device nested depth

iokit_registry

The full IOKit registry without selecting a plane.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Default name of the node
class	TEXT	Best matching device class (most-specific category)
id	BIGINT	IOKit internal registry ID
parent	BIGINT	Parent registry ID
busy_state	INTEGER	1 if the node is in a busy state else 0
retain_count	INTEGER	The node reference count
depth	INTEGER	Node nested depth

iptables

Linux IP packet filtering and NAT tool.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
filter_name	TEXT	Packet matching filter table name.
chain	TEXT	Size of module content.
policy	TEXT	Policy that applies for this rule.
target	TEXT	Target that applies for this rule.
protocol	INTEGER	Protocol number identification.
src_port	TEXT	Protocol source port(s).
dst_port	TEXT	Protocol destination port(s).
src_ip	TEXT	Source IP address.
src_mask	TEXT	Source IP address mask.
iniface	TEXT	Input interface for the rule.
iniface_mask	TEXT	Input interface mask for the rule.
dst_ip	TEXT	Destination IP address.
dst_mask	TEXT	Destination IP address mask.
outiface	TEXT	Output interface for the rule.
outiface_mask	TEXT	Output interface mask for the rule.
match	TEXT	Matching rule that applies.
packets	INTEGER	Number of matching packets for this rule.
bytes	INTEGER	Number of matching bytes for this rule.

kernel_extensions

OS X's kernel extensions, both loaded and within the load search path.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
idx	INTEGER	Extension load tag or index
refs	INTEGER	Reference count
size	BIGINT	Bytes of wired memory used by extension
name	TEXT	Extension label
version	TEXT	Extension version
linked_against	TEXT	Indexes of extensions this extension is linked against
path	TEXT	Optional path to extension bundle

kernel_info

Basic active kernel information.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
version	TEXT	Kernel version
arguments	TEXT	Kernel arguments
path	TEXT	Kernel path
device	TEXT	Kernel device identifier

kernel_modules

Linux kernel modules both loaded and within the load search path.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Module name
size	TEXT	Size of module content
used_by	TEXT	Module reverse dependencies
status	TEXT	Kernel module status
address	TEXT	Kernel module address

kernel_panics

System kernel panic logs.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
path	TEXT	Location of log file
time	TEXT	Formatted time of the event
registers	TEXT	A space delimited line of register:value pairs
frame_backtrace	TEXT	Backtrace of the crashed module
module_backtrace	TEXT	Modules appearing in the crashed module's backtrace
dependencies	TEXT	Module dependencies existing in crashed module's backtrace
name	TEXT	Process name corresponding to crashed thread
os_version	TEXT	Version of the operating system
kernel_version	TEXT	Version of the system kernel

COLUMN	TYPE	DESCRIPTION
system_model	TEXT	Physical system model, for example 'MacBookPro12,1 (Mac-E43C1C25D4880AD6)'
uptime	BIGINT	System uptime at kernel panic in nanoseconds
last_loaded	TEXT	Last loaded module before panic
last_unloaded	TEXT	Last unloaded module before panic

keychain_acls

Applications that have ACL entries in the keychain.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
keychain_path	TEXT	The path of the keychain
authorizations	TEXT	A space delimited set of authorization attributes
path	TEXT	The path of the authorized application
description	TEXT	The description included with the ACL entry
label	TEXT	An optional label tag that may be included with the keychain entry

keychain_items

Generic details about keychain items.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
label	TEXT	Generic item name
description	TEXT	Optional item description
comment	TEXT	Optional keychain comment

COLUMN	TYPE	DESCRIPTION
created	TEXT	Data item was created
modified	TEXT	Date of last modification
type	TEXT	Keychain item type (class)
path	TEXT	Path to keychain containing item

known_hosts

A line-delimited known_hosts table.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
uid	BIGINT	The local user that owns the known_hosts file
key	TEXT	parsed authorized keys line
key_file	TEXT	Path to known_hosts file

kva_speculative_info

Display kernel virtual address and speculative execution information for the system.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
kva_shadow_enabled	INTEGER	Kernel Virtual Address shadowing is enabled.
kva_shadow_user_global	INTEGER	User pages are marked as global.
kva_shadow_pcid	INTEGER	Kernel VA PCID flushing optimization is enabled.
kva_shadow_inv_pcid	INTEGER	Kernel VA INVPCID is enabled.
bp_mitigations	INTEGER	Branch Prediction mitigations are enabled.

COLUMN	TYPE	DESCRIPTION
bp_system_pol_disabled	INTEGER	Branch Predictions are disabled via system policy.
bp_microcode_disabled	INTEGER	Branch Predictions are disabled due to lack of microcode update.
cpu_spec_ctrl_supported	INTEGER	SPEC_CTRL MSR supported by CPU Microcode.
ibrs_support_enabled	INTEGER	Windows uses IBRS.
stibp_support_enabled	INTEGER	Windows uses STIBP.
cpu_pred_cmd_supported	INTEGER	PRED_CMD MSR supported by CPU Microcode.

last

System logins and logouts.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
username	TEXT	Entry username
tty	TEXT	Entry terminal
pid	INTEGER	Process (or thread) ID
type	INTEGER	Entry type, according to ut_type types (utmp.h)
time	INTEGER	Entry timestamp
host	TEXT	Entry hostname

launchd

LaunchAgents and LaunchDaemons from default search paths.

Improve this Description on Github

COLUMN COLUMN	TYPE TYPE	DESCRIPTION DESCRIPTION
path	TEXT	Path to daemon or agent plist
name	TEXT	File name of plist (used by launchd)
label	TEXT	Daemon or agent service name
program	TEXT	Path to target program
run_at_load	TEXT	Should the program run on launch load
keep_alive	TEXT	Should the process be restarted if killed
on_demand	TEXT	Deprecated key, replaced by keep_alive
disabled	TEXT	Skip loading this daemon or agent on boot
username	TEXT	Run this daemon or agent as this username
groupname	TEXT	Run this daemon or agent as this group
stdout_path	TEXT	Pipe stdout to a target path
stderr_path	TEXT	Pipe stderr to a target path
start_interval	TEXT	Frequency to run in seconds
program_arguments	TEXT	Command line arguments passed to program
watch_paths	TEXT	Key that launches daemon or agent if path is modified
queue_directories	TEXT	Similar to watch_paths but only with non-empty directories
inetd_compatibility	TEXT	Run this daemon or agent as it was launched from inetd
start_on_mount	TEXT	Run daemon or agent every time a filesystem is mounted

COLUMN	TYPE	DESCRIPTION
root_directory	TEXT	Key used to specify a directory to chroot to before launch
working_directory	TEXT	Key used to specify a directory to chdir to before launch
process_type	TEXT	Key describes the intended purpose of the job

launchd_overrides

Override keys, per user, for LaunchDaemons and Agents.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
label	TEXT	Daemon or agent service name
key	TEXT	Name of the override key
value	TEXT	Overridden value
uid	BIGINT	User ID applied to the override, 0 applies to all
path	TEXT	Path to daemon or agent plist

listening_ports

Processes with listening (bound) network sockets/ports.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
pid	INTEGER	Process (or thread) ID
port	INTEGER	Transport layer port
protocol	INTEGER	Transport protocol (TCP/UDP)
family	INTEGER	Network protocol (IPv4, IPv6)

COLUMN	TYPE	DESCRIPTION
address	TEXT	Specific address for bind
fd	BIGINT	Socket file descriptor number
socket	BIGINT	Socket handle or inode number
path	TEXT	Path for UNIX domain sockets
net_namespace	TEXT	The inode number of the network namespace

lldp_neighbors

LLDP neighbors of interfaces.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
interface	TEXT	Interface name
rid	INTEGER	Neighbor chassis index
chassis_id_type	TEXT	Neighbor chassis ID type
chassis_id	TEXT	Neighbor chassis ID value
chassis_sysname	TEXT	CPU brand string, contains vendor and model
chassis_sys_description	INTEGER	Max number of CPU physical cores
chassis_bridge_capability_available	INTEGER	Chassis bridge capability availability
chassis_bridge_capability_enabled	INTEGER	Is chassis bridge capability enabled.
chassis_router_capability_available	INTEGER	Chassis router capability availability
chassis_router_capability_enabled	INTEGER	Chassis router capability enabled

chassis_repeater_capability_available COLUMN	INTEGER TYPE	Chassis repeater capability availability DESCRIPTION
chassis_repeater_capability_enabled	INTEGER	Chassis repeater capability enabled
chassis_wlan_capability_available	INTEGER	Chassis wlan capability availability
chassis_wlan_capability_enabled	INTEGER	Chassis wlan capability enabled
chassis_tel_capability_available	INTEGER	Chassis telephone capability availability
chassis_tel_capability_enabled	INTEGER	Chassis telephone capability enabled
chassis_docsis_capability_available	INTEGER	Chassis DOCSIS capability availability
chassis_docsis_capability_enabled	INTEGER	Chassis DOCSIS capability enabled
chassis_station_capability_available	INTEGER	Chassis station capability availability
chassis_station_capability_enabled	INTEGER	Chassis station capability enabled
chassis_other_capability_available	INTEGER	Chassis other capability availability
chassis_other_capability_enabled	INTEGER	Chassis other capability enabled
chassis_mgmt_ips	TEXT	Comma delimited list of chassis management IPS
port_id_type	TEXT	Port ID type
port_id	TEXT	Port ID value
port_description	TEXT	Port description
port_ttl	BIGINT	Age of neighbor port
port_mfs	BIGINT	Port max frame size
port_aggregation_id	TEXT	Port aggregation ID

COLUMN	TYPE	DESCRIPTION
port_autoneg_supported	INTEGER	Auto negotiation supported
port_autoneg_enabled	INTEGER	Is auto negotiation enabled
port_mau_type	TEXT	MAU type
port_autoneg_10baset_hd_enabled	INTEGER	10Base-T HD auto negotiation enabled
port_autoneg_10baset_fd_enabled	INTEGER	10Base-T FD auto negotiation enabled
port_autoneg_100basetx_hd_enabled	INTEGER	100Base-TX HD auto negotiation enabled
port_autoneg_100basetx_fd_enabled	INTEGER	100Base-TX FD auto negotiation enabled
port_autoneg_100baset2_hd_enabled	INTEGER	100Base-T2 HD auto negotiation enabled
port_autoneg_100baset2_fd_enabled	INTEGER	100Base-T2 FD auto negotiation enabled
port_autoneg_100baset4_hd_enabled	INTEGER	100Base-T4 HD auto negotiation enabled
port_autoneg_100baset4_fd_enabled	INTEGER	100Base-T4 FD auto negotiation enabled
port_autoneg_1000basex_hd_enabled	INTEGER	1000Base-X HD auto negotiation enabled
port_autoneg_1000basex_fd_enabled	INTEGER	1000Base-X FD auto negotiation enabled
port_autoneg_1000baset_hd_enabled	INTEGER	1000Base-T HD auto negotiation enabled
port_autoneg_1000baset_fd_enabled	INTEGER	1000Base-T FD auto negotiation enabled
power_device_type	TEXT	Dot3 power device type
power_mdi_supported	INTEGER	MDI power supported
power_mdi_enabled	INTEGER	Is MDI power enabled
power_paircontrol_enabled	INTEGER	Is power pair control enabled

COLUMN	TYPE	DESCRIPTION
power_pairs	TEXT	802.3 power pairs
power_class	TEXT	Power class
power_8023at_enabled	INTEGER	Is 802.3at enabled
power_8023at_power_type	TEXT	802.3at power type
power_8023at_power_source	TEXT	802.3at power source
power_8023at_power_priority	TEXT	802.3at power priority
power_8023at_power_allocated	TEXT	802.3at power allocated
power_8023at_power_requested	TEXT	802.3at power requested
med_device_type	TEXT	Chassis MED type
med_capability_capabilities	INTEGER	Is MED capabilities enabled
med_capability_policy	INTEGER	Is MED policy capability enabled
med_capability_location	INTEGER	Is MED location capability enabled
med_capability_mdi_pse	INTEGER	Is MED MDI PSE capability enabled
med_capability_mdi_pd	INTEGER	Is MED MDI PD capability enabled
med_capability_inventory	INTEGER	Is MED inventory capability enabled
med_policies	TEXT	Comma delimited list of MED policies
vlans	TEXT	Comma delimited list of vlan ids
pvid	TEXT	Primary VLAN id
ppvids_supported	TEXT	Comma delimited list of supported PPVIDs

COLUMN	TYPE	DESCRIPTION
ppvids_enabled	TEXT	Comma delimited list of enabled PPVIDs
pids	TEXT	Comma delimited list of PIDs

load_average

Displays information about the system wide load averages.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
period	TEXT	Period over which the average is calculated.
average	TEXT	Load average over the specified period.

logged_in_users

Users with an active shell on the system.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
type	TEXT	Login type
user	TEXT	User login name
tty	TEXT	Device name
host	TEXT	Remote hostname
time	INTEGER	Time entry was made
pid	INTEGER	Process (or thread) ID
sid	TEXT	The user's unique security identifier
registry_hive	TEXT	HKEY_USERS registry hive

COLUMN	TYPE	DESCRIPTION

logical_drives

Details for logical drives on the system. A logical drive generally represents a single partition.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
device_id	TEXT	The drive id, usually the drive name, e.g., 'C:'.
type	TEXT	Deprecated (always 'Unknown').
description	TEXT	The canonical description of the drive, e.g. 'Logical Fixed Disk', 'CD-ROM Disk'.
free_space	BIGINT	The amount of free space, in bytes, of the drive (-1 on failure).
size	BIGINT	The total amount of space, in bytes, of the drive (-1 on failure).
file_system	TEXT	The file system of the drive.
boot_partition	INTEGER	True if Windows booted from this drive.

logon_sessions

Windows Logon Session.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
logon_id	INTEGER	A locally unique identifier (LUID) that identifies a logon session.
user	TEXT	The account name of the security principal that owns the logon session.
logon_domain	TEXT	The name of the domain used to authenticate the owner of the logon session.
authentication_package	TEXT	The authentication package used to authenticate the owner of the logon session.

COLUMN	TYPE	DESCRIPTION
logon_type	TEXT	The logon method.
session_id	INTEGER	The Terminal Services session identifier.
logon_sid	TEXT	The user's security identifier (SID).
logon_time	BIGINT	The time the session owner logged on.
logon_server	TEXT	The name of the server used to authenticate the owner of the logon session.
dns_domain_name	TEXT	The DNS name for the owner of the logon session.
upn	TEXT	The user principal name (UPN) for the owner of the logon session.
logon_script	TEXT	The script used for logging on.
profile_path	TEXT	The home directory for the logon session.
home_directory	TEXT	The home directory for the logon session.
home_directory_drive	TEXT	The drive location of the home directory of the logon session.

lxd_certificates

LXD certificates information.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Name of the certificate
type	TEXT	Type of the certificate
fingerprint	TEXT	SHA256 hash of the certificate
certificate	TEXT	Certificate content

lxd_cluster

LXD cluster information.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
server_name	TEXT	Name of the LXD server node
enabled	INTEGER	Whether clustering enabled (1) or not (0) on this node
member_config_entity	TEXT	Type of configuration parameter for this node
member_config_name	TEXT	Name of configuration parameter
member_config_key	TEXT	Config key
member_config_value	TEXT	Config value
member_config_description	TEXT	Config description

lxd_cluster_members

LXD cluster members information.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
server_name	TEXT	Name of the LXD server node
url	TEXT	URL of the node
database	INTEGER	Whether the server is a database node (1) or not (0)
status	TEXT	Status of the node (Online/Offline)
message	TEXT	Message from the node (Online/Offline)

lxd_images

lxd_images

LXD images information.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
id	TEXT	Image ID
architecture	TEXT	Target architecture for the image
os	TEXT	OS on which image is based
release	TEXT	OS release version on which the image is based
description	TEXT	Image description
aliases	TEXT	Comma-separated list of image aliases
filename	TEXT	Filename of the image file
size	BIGINT	Size of image in bytes
auto_update	INTEGER	Whether the image auto-updates (1) or not (0)
cached	INTEGER	Whether image is cached (1) or not (0)
public	INTEGER	Whether image is public (1) or not (0)
created_at	TEXT	ISO time of image creation
expires_at	TEXT	ISO time of image expiration
uploaded_at	TEXT	ISO time of image upload
last_used_at	TEXT	ISO time for the most recent use of this image in terms of container spawn
update_source_server	TEXT	Server for image update
update_source_protocol	TEXT	Protocol used for image information update and image import from source server

COLUMN	TYPE	DESCRIPTION
update_source_certificate	TEXT	Certificate for update source server
update_source_alias	TEXT	Alias of image at update source server

lxd_instance_config

LXD instance configuration information.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Instance name
key	TEXT	Configuration parameter name
value	TEXT	Configuration parameter value

lxd_instance_devices

LXD instance devices information.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Instance name
device	TEXT	Name of the device
device_type	TEXT	Device type
key	TEXT	Device info param name
value	TEXT	Device info param value

lxd_instances

LXD instances information

LXD instances information.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Instance name
status	TEXT	Instance state (running, stopped, etc.)
stateful	INTEGER	Whether the instance is stateful(1) or not(0)
ephemeral	INTEGER	Whether the instance is ephemeral(1) or not(0)
created_at	TEXT	ISO time of creation
base_image	TEXT	ID of image used to launch this instance
architecture	TEXT	Instance architecture
os	TEXT	The OS of this instance
description	TEXT	Instance description
pid	INTEGER	Instance's process ID
processes	INTEGER	Number of processes running inside this instance

lxd_networks

LXD network information.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Name of the network
type	TEXT	Type of network
managed	INTEGER	1 if network created by LXD, 0 otherwise

ipv4_address COLUMN	TEXT TYPE	IPv4 address DESCRIPTION

ipv6_address	TEXT	IPv6 address
used_by	TEXT	URLs for containers using this network
bytes_received	BIGINT	Number of bytes received on this network
bytes_sent	BIGINT	Number of bytes sent on this network
packets_received	BIGINT	Number of packets received on this network
packets_sent	BIGINT	Number of packets sent on this network
hwaddr	TEXT	Hardware address for this network
state	TEXT	Network status
mtu	INTEGER	MTU size

lxd_storage_pools

LXD storage pool information.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Name of the storage pool
driver	TEXT	Storage driver
source	TEXT	Storage pool source
size	TEXT	Size of the storage pool
space_used	BIGINT	Storgae space used in bytes

COLUMN	TYPE	DESCRIPTION
space_total	BIGINT	Total available storage space in bytes for this storage pool
inodes_used	BIGINT	Number of inodes used
inodes_total	BIGINT	Total number of inodes available in this storage pool

magic

Magic number recognition library table.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
path	TEXT	Absolute path to target file
magic_db_files	TEXT	Colon(:) separated list of files where the magic db file can be found. By default one of the following is used: /usr/share/file/magic/magic, /usr/share/misc/magic or /usr/share/misc/magic.mgc
data	TEXT	Magic number data from libmagic
mime_type	TEXT	MIME type data from libmagic
mime_encoding	TEXT	MIME encoding data from libmagic

managed_policies

The managed configuration policies from AD, MDM, MCX, etc.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
domain	TEXT	System or manager-chosen domain key
uuid	TEXT	Optional UUID assigned to policy set
name	TEXT	Policy key name

COLUMN	TYPE	DESCRIPTION
value	TEXT	Policy value
username	TEXT	Policy applies only this user
manual	INTEGER	1 if policy was loaded manually, otherwise 0

md_devices

Software RAID array settings.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
device_name	TEXT	md device name
status	TEXT	Current state of the array
raid_level	INTEGER	Current raid level of the array
size	BIGINT	size of the array in blocks
chunk_size	BIGINT	chunk size in bytes
raid_disks	INTEGER	Number of configured RAID disks in array
nr_raid_disks	INTEGER	Number of partitions or disk devices to comprise the array
working_disks	INTEGER	Number of working disks in array
active_disks	INTEGER	Number of active disks in array
failed_disks	INTEGER	Number of failed disks in array
spare_disks	INTEGER	Number of idle disks in array
superblock_state	TEXT	State of the superblock

superblock_version COLUMN	TEXT TYPE	Version of the superblock DESCRIPTION
superblock_update_time	BIGINT	Unix timestamp of last update
bitmap_on_mem	TEXT	Pages allocated in in-memory bitmap, if enabled
bitmap_chunk_size	TEXT	Bitmap chunk size
bitmap_external_file	TEXT	External referenced bitmap file
recovery_progress	TEXT	Progress of the recovery activity
recovery_finish	TEXT	Estimated duration of recovery activity
recovery_speed	TEXT	Speed of recovery activity
resync_progress	TEXT	Progress of the resync activity
resync_finish	TEXT	Estimated duration of resync activity
resync_speed	TEXT	Speed of resync activity
reshape_progress	TEXT	Progress of the reshape activity
reshape_finish	TEXT	Estimated duration of reshape activity
reshape_speed	TEXT	Speed of reshape activity
check_array_progress	TEXT	Progress of the check array activity
check_array_finish	TEXT	Estimated duration of the check array activity
check_array_speed	TEXT	Speed of the check array activity
unused_devices	TEXT	Unused devices
other	TEXT	Other information associated with array from /proc/mdstat

md_drives

Drive devices used for Software RAID.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
md_device_name	TEXT	md device name
drive_name	TEXT	Drive device name
slot	INTEGER	Slot position of disk
state	TEXT	State of the drive

md_personalities

Software RAID setting supported by the kernel.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Name of personality supported by kernel

mdfind

Run searches against the spotlight database.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
path	TEXT	Path of the file returned from spotlight
query	TEXT	The query that was run to find the file

mdls

Query file metadata in the Spotlight database.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
path	TEXT	Path of the file
key	TEXT	Name of the metadata key
value	TEXT	Value stored in the metadata key
valuetype	TEXT	CoreFoundation type of data stored in value

memory_array_mapped_addresses

Data associated for address mapping of physical memory arrays.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
handle	TEXT	Handle, or instance number, associated with the structure
memory_array_handle	TEXT	Handle of the memory array associated with this structure
starting_address	TEXT	Physical stating address, in kilobytes, of a range of memory mapped to physical memory array
ending_address	TEXT	Physical ending address of last kilobyte of a range of memory mapped to physical memory array
partition_width	INTEGER	Number of memory devices that form a single row of memory for the address partition of this structure

memory_arrays

Data associated with collection of memory devices that operate to form a memory address.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
handle	TEXT	Handle, or instance number, associated with the array

COLUMN	TYPE	DESCRIPTION
location	TEXT	Physical location of the memory array
use	TEXT	Function for which the array is used
memory_error_correction	TEXT	Primary hardware error correction or detection method supported
max_capacity	INTEGER	Maximum capacity of array in gigabytes
memory_error_info_handle	TEXT	Handle, or instance number, associated with any error that was detected for the array
number_memory_devices	INTEGER	Number of memory devices on array

memory_device_mapped_addresses

Data associated for address mapping of physical memory devices.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
handle	TEXT	Handle, or instance number, associated with the structure
memory_device_handle	TEXT	Handle of the memory device structure associated with this structure
memory_array_mapped_address_handle	TEXT	Handle of the memory array mapped address to which this device range is mapped to
starting_address	TEXT	Physical stating address, in kilobytes, of a range of memory mapped to physical memory array
ending_address	TEXT	Physical ending address of last kilobyte of a range of memory mapped to physical memory array
partition_row_position	INTEGER	Identifies the position of the referenced memory device in a row of the address partition

COLUMN	TYPE	DESCRIPTION
interleave_position	INTEGER	The position of the device in a interleave, i.e. 0 indicates non-interleave, 1 indicates 1st interleave, 2 indicates 2nd interleave, etc.
interleave_data_depth	INTEGER	The max number of consecutive rows from memory device that are accessed in a single interleave transfer; 0 indicates device is non-interleave

memory_devices

Physical memory device (type 17) information retrieved from SMBIOS.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
handle	TEXT	Handle, or instance number, associated with the structure in SMBIOS
array_handle	TEXT	The memory array that the device is attached to
form_factor	TEXT	Implementation form factor for this memory device
total_width	INTEGER	Total width, in bits, of this memory device, including any check or error-correction bits
data_width	INTEGER	Data width, in bits, of this memory device
size	INTEGER	Size of memory device in Megabyte
set	INTEGER	Identifies if memory device is one of a set of devices. A value of 0 indicates no set affiliation.
device_locator	TEXT	String number of the string that identifies the physically-labeled socket or board position where the memory device is located
bank_locator	TEXT	String number of the string that identifies the physically-labeled bank where the memory device is located
memory_type	TEXT	Type of memory used
memory_type_details	TEXT	Additional details for memory device

COLUMN	TYPE	DESCRIPTION
memory_type_details	TEXT	Additional details for memory device
max_speed	INTEGER	Max speed of memory device in megatransfers per second (MT/s)
configured_clock_speed	INTEGER	Configured speed of memory device in megatransfers per second (MT/s)
manufacturer	TEXT	Manufacturer ID string
serial_number	TEXT	Serial number of memory device
asset_tag	TEXT	Manufacturer specific asset tag of memory device
part_number	TEXT	Manufacturer specific serial number of memory device
min_voltage	INTEGER	Minimum operating voltage of device in millivolts
max_voltage	INTEGER	Maximum operating voltage of device in millivolts
configured_voltage	INTEGER	Configured operating voltage of device in millivolts

memory_error_info

Data associated with errors of a physical memory array.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
handle	TEXT	Handle, or instance number, associated with the structure
error_type	TEXT	type of error associated with current error status for array or device
error_granularity	TEXT	Granularity to which the error can be resolved
error_operation	TEXT	Memory access operation that caused the error
vendor_syndrome	TEXT	Vendor specific ECC syndrome or CRC data associated with the

COLUMN	TYPE	DESCRIPTION
vendor_syndrome	TEXT	erroneous access
memory_array_error_address	TEXT	32 bit physical address of the error based on the addressing of the bus to which the memory array is connected
device_error_address	TEXT	32 bit physical address of the error relative to the start of the failing memory address, in bytes
error_resolution	TEXT	Range, in bytes, within which this error can be determined, when an error address is given

memory_info

Main memory information in bytes.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
memory_total	BIGINT	Total amount of physical RAM, in bytes
memory_free	BIGINT	The amount of physical RAM, in bytes, left unused by the system
buffers	BIGINT	The amount of physical RAM, in bytes, used for file buffers
cached	BIGINT	The amount of physical RAM, in bytes, used as cache memory
swap_cached	BIGINT	The amount of swap, in bytes, used as cache memory
active	BIGINT	The total amount of buffer or page cache memory, in bytes, that is in active use
inactive	BIGINT	The total amount of buffer or page cache memory, in bytes, that are free and available
swap_total	BIGINT	The total amount of swap available, in bytes
swap_free	BIGINT	The total amount of swap free, in bytes

memory_map

OS memory region map.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Region name
start	TEXT	Start address of memory region
end	TEXT	End address of memory region

mounts

System mounted devices and filesystems (not process specific).

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
device	TEXT	Mounted device
device_alias	TEXT	Mounted device alias
path	TEXT	Mounted device path
type	TEXT	Mounted device type
blocks_size	BIGINT	Block size in bytes
blocks	BIGINT	Mounted device used blocks
blocks_free	BIGINT	Mounted device free blocks
blocks_available	BIGINT	Mounted device available blocks
inodes	BIGINT	Mounted device used inodes
inodes_free	BIGINT	Mounted device free inodes
flags	TEXT	Mounted device flags

COLUMN	TYPE	DESCRIPTION

msr

Various pieces of data stored in the model specific register per processor. NOTE: the msr kernel module must be enabled, and osquery must be run as root.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
processor_number	BIGINT	The processor number as reported in /proc/cpuinfo
turbo_disabled	BIGINT	Whether the turbo feature is disabled.
turbo_ratio_limit	BIGINT	The turbo feature ratio limit.
platform_info	BIGINT	Platform information.
perf_ctl	BIGINT	Performance setting for the processor.
perf_status	BIGINT	Performance status for the processor.
feature_control	BIGINT	Bitfield controlling enabled features.
rapl_power_limit	BIGINT	Run Time Average Power Limiting power limit.
rapl_energy_status	BIGINT	Run Time Average Power Limiting energy status.
rapl_power_units	BIGINT	Run Time Average Power Limiting power units.

nfs_shares

NFS shares exported by the host.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
share	TEXT	Filesystem path to the share
options	TEXT	Options string set on the export share

readonly COLUMN	INTEGER TYPE	1 if the share is exported readonly else 0 DESCRIPTION

npm_packages

Lists all npm packages in a directory or globally installed in a system.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Package display name
version	TEXT	Package supplied version
description	TEXT	Package supplied description
author	TEXT	Package author name
license	TEXT	License for package
path	TEXT	Module's package.json path
directory	TEXT	Node module's directory where this package is located
pid_with_namespace	INTEGER	Pids that contain a namespace
mount_namespace_id	TEXT	Mount namespace id

ntdomains

Display basic NT domain information of a Windows machine.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	The label by which the object is known.
client_site_name	TEXT	The name of the site where the domain controller is configured.
dc_site_name	TEXT	The name of the site where the domain controller is located.

COLUMN	TYPE	DESCRIPTION
dns_forest_name	TEXT	The name of the root of the DNS tree.
domain_controller_address	TEXT	The IP Address of the discovered domain controller..
domain_controller_name	TEXT	The name of the discovered domain controller.
domain_name	TEXT	The name of the domain.
status	TEXT	The current status of the domain object.

ntfs_acl_permissions

Retrieve NTFS ACL permission information for files and directories.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
path	TEXT	Path to the file or directory.
type	TEXT	Type of access mode for the access control entry.
principal	TEXT	User or group to which the ACE applies.
access	TEXT	Specific permissions that indicate the rights described by the ACE.
inherited_from	TEXT	The inheritance policy of the ACE.

ntfs_journal_events (EVENTED TABLE)

Track time/action changes to files specified in configuration data.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
action	TEXT	Change action (Write, Delete, etc)
category	TEXT	The category that the event originated from

COLUMN	TYPE	DESCRIPTION
old_path	TEXT	Old path (renames only)
path	TEXT	Path
record_timestamp	TEXT	Journal record timestamp
record_usn	TEXT	The update sequence number that identifies the journal record
node_ref_number	TEXT	The ordinal that associates a journal record with a filename
parent_ref_number	TEXT	The ordinal that associates a journal record with a filename's parent directory
drive_letter	TEXT	The drive letter identifying the source journal
file_attributes	TEXT	File attributes
partial	BIGINT	Set to 1 if either path or old_path only contains the file or folder name
time	BIGINT	Time of file event
eid	TEXT	Event ID

nvram

Apple NVRAM variable listing.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Variable name
type	TEXT	Data type (CFData, CFString, etc)
value	TEXT	Raw variable data

oem_strings

OEM defined strings retrieved from SMBIOS.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
handle	TEXT	Handle, or instance number, associated with the Type 11 structure
number	INTEGER	The string index of the structure
value	TEXT	The value of the OEM string

office_mru NEW

View recently opened Office documents.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
application	TEXT	Associated Office application
version	TEXT	Office application version number
path	TEXT	File path
last_opened_time	INTEGER	Most recent opened time file was opened
sid	TEXT	User SID

opera_extensions

Opera browser extensions.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
uid	BIGINT	The local user that owns the extension
name	TEXT	Extension display name

identifier COLUMN	TEXT TYPE	Extension identifier DESCRIPTION
version	TEXT	Extension-supplied version
description	TEXT	Extension-optional description
locale	TEXT	Default locale supported by extension
update_url	TEXT	Extension-supplied update URI
author	TEXT	Optional extension author
persistent	INTEGER	1 If extension is persistent across all tabs else 0
path	TEXT	Path to extension folder

os_version

A single row containing the operating system name and version.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Distribution or product name
version	TEXT	Pretty, suitable for presentation, OS version
major	INTEGER	Major release version
minor	INTEGER	Minor release version
patch	INTEGER	Optional patch release
build	TEXT	Optional build-specific or variant string
platform	TEXT	OS Platform or ID

platform_like COLUMN	TEXT TYPE	Closely related platforms DESCRIPTION
codename	TEXT	OS version codename
arch	TEXT	OS Architecture
install_date	BIGINT	The install date of the OS.
pid_with_namespace	INTEGER	Pids that contain a namespace
mount_namespace_id	TEXT	Mount namespace id

osquery_events

Information about the event publishers and subscribers.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Event publisher or subscriber name
publisher	TEXT	Name of the associated publisher
type	TEXT	Either publisher or subscriber
subscriptions	INTEGER	Number of subscriptions the publisher received or subscriber used
events	INTEGER	Number of events emitted or received since osquery started
refreshes	INTEGER	Publisher only: number of runloop restarts
active	INTEGER	1 if the publisher or subscriber is active else 0

osquery_extensions

List of active osquery extensions.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
uuid	BIGINT	The transient ID assigned for communication
name	TEXT	Extension's name
version	TEXT	Extension's version
sdk_version	TEXT	osquery SDK version used to build the extension
path	TEXT	Path of the extenion's domain socket or library path
type	TEXT	SDK extension type: extension or module

osquery_flags

Configurable flags that modify osquery's behavior.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Flag name
type	TEXT	Flag type
description	TEXT	Flag description
default_value	TEXT	Flag default value
value	TEXT	Flag value
shell_only	INTEGER	Is the flag shell only?

osquery_info

Top level information about the running version of osquery.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
pid	INTEGER	Process (or thread/handle) ID
uuid	TEXT	Unique ID provided by the system
instance_id	TEXT	Unique, long-lived ID per instance of osquery
version	TEXT	osquery toolkit version
config_hash	TEXT	Hash of the working configuration state
config_valid	INTEGER	1 if the config was loaded and considered valid, else 0
extensions	TEXT	osquery extensions status
build_platform	TEXT	osquery toolkit build platform
build_distro	TEXT	osquery toolkit platform distribution name (os version)
start_time	INTEGER	UNIX time in seconds when the process started
watcher	INTEGER	Process (or thread/handle) ID of optional watcher process
platform_mask	INTEGER	The osquery platform bitmask

osquery_packs

Information about the current query packs that are loaded in osquery.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	The given name for this query pack
platform	TEXT	Platforms this query is supported on

version COLUMN	TEXT TYPE	Minimum osquery version that this query will run on DESCRIPTION
shard	INTEGER	Shard restriction limit, 1-100, 0 meaning no restriction
discovery_cache_hits	INTEGER	The number of times that the discovery query used cached values since the last time the config was reloaded
discovery_executions	INTEGER	The number of times that the discovery queries have been executed since the last time the config was reloaded
active	INTEGER	Whether this pack is active (the version, platform and discovery queries match) yes=1, no=0.

osquery_registry

List the osquery registry plugins.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
registry	TEXT	Name of the osquery registry
name	TEXT	Name of the plugin item
owner_uuid	INTEGER	Extension route UUID (0 for core)
internal	INTEGER	1 If the plugin is internal else 0
active	INTEGER	1 If this plugin is active else 0

osquery_schedule

Information about the current queries that are scheduled in osquery.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	The given name for this query

COLUMN	TYPE	DESCRIPTION
query	TEXT	The exact query to run
interval	INTEGER	The interval in seconds to run this query, not an exact interval
executions	BIGINT	Number of times the query was executed
last_executed	BIGINT	UNIX time stamp in seconds of the last completed execution
denylisted	INTEGER	1 if the query is denylisted else 0
output_size	BIGINT	Total number of bytes generated by the query
wall_time	BIGINT	Total wall time spent executing
user_time	BIGINT	Total user time spent executing
system_time	BIGINT	Total system time spent executing
average_memory	BIGINT	Average private memory left after executing

package_bom

OS X package bill of materials (BOM) file list.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
filepath	TEXT	Package file or directory
uid	INTEGER	Expected user of file or directory
gid	INTEGER	Expected group of file or directory
mode	INTEGER	Expected permissions
size	BIGINT	Expected file size

COLUMN	TYPE	DESCRIPTION
modified_time	INTEGER	Timestamp the file was installed
path	TEXT	Path of package bom

package_install_history

OS X package install history.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
package_id	TEXT	Label packageIdentifiers
time	INTEGER	Label date as UNIX timestamp
name	TEXT	Package display name
version	TEXT	Package display version
source	TEXT	Install source: usually the installer process name
content_type	TEXT	Package content_type (optional)

package_receipts

OS X package receipt details.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
package_id	TEXT	Package domain identifier
package_filename	TEXT	Filename of original .pkg file
version	TEXT	Installed package version
location	TEXT	Optional relative install path on volume

COLUMN	TYPE	DESCRIPTION
install_time	DOUBLE	Timestamp of install time
installer_name	TEXT	Name of installer process
path	TEXT	Path of receipt plist

patches

Lists all the patches applied. Note: This does not include patches applied via MSI or downloaded from Windows Update (e.g. Service Packs).

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
csname	TEXT	The name of the host the patch is installed on.
hotfix_id	TEXT	The KB ID of the patch.
caption	TEXT	Short description of the patch.
description	TEXT	Fuller description of the patch.
fix_comments	TEXT	Additional comments about the patch.
installed_by	TEXT	The system context in which the patch as installed.
install_date	TEXT	Indicates when the patch was installed. Lack of a value does not indicate that the patch was not installed.
installed_on	TEXT	The date when the patch was installed.

pci_devices

PCI devices active on the host system.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION

COLUMN	TYPE	DESCRIPTION
pci_slot	TEXT	PCI Device used slot
pci_class	TEXT	PCI Device class
driver	TEXT	PCI Device used driver
vendor	TEXT	PCI Device vendor
vendor_id	TEXT	Hex encoded PCI Device vendor identifier
model	TEXT	PCI Device model
model_id	TEXT	Hex encoded PCI Device model identifier
pci_class_id	TEXT	PCI Device class ID in hex format
pci_subclass_id	TEXT	PCI Device subclass in hex format
pci_subclass	TEXT	PCI Device subclass
subsystem_vendor_id	TEXT	Vendor ID of PCI device subsystem
subsystem_vendor	TEXT	Vendor of PCI device subsystem
subsystem_model_id	TEXT	Model ID of PCI device subsystem
subsystem_model	TEXT	Device description of PCI device subsystem

physical_disk_performance

Provides provides raw data from performance counters that monitor hard or fixed disk drives on the system.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Name of the physical disk

COLUMN	TYPE	DESCRIPTION
avg_disk_bytes_per_read	BIGINT	Average number of bytes transferred from the disk during read operations
avg_disk_bytes_per_write	BIGINT	Average number of bytes transferred to the disk during write operations
avg_disk_read_queue_length	BIGINT	Average number of read requests that were queued for the selected disk during the sample interval
avg_disk_write_queue_length	BIGINT	Average number of write requests that were queued for the selected disk during the sample interval
avg_disk_sec_per_read	INTEGER	Average time, in seconds, of a read operation of data from the disk
avg_disk_sec_per_write	INTEGER	Average time, in seconds, of a write operation of data to the disk
current_disk_queue_length	INTEGER	Number of requests outstanding on the disk at the time the performance data is collected
percent_disk_read_time	BIGINT	Percentage of elapsed time that the selected disk drive is busy servicing read requests
percent_disk_write_time	BIGINT	Percentage of elapsed time that the selected disk drive is busy servicing write requests
percent_disk_time	BIGINT	Percentage of elapsed time that the selected disk drive is busy servicing read or write requests
percent_idle_time	BIGINT	Percentage of time during the sample interval that the disk was idle

pipes

Named and Anonymous pipes.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
pid	BIGINT	Process ID of the process to which the pipe belongs

COLUMN	TYPE	DESCRIPTION
name	TEXT	Name of the pipe
instances	INTEGER	Number of instances of the named pipe
max_instances	INTEGER	The maximum number of instances creatable for this pipe
flags	TEXT	The flags indicating whether this pipe connection is a server or client end, and if the pipe for sending messages or bytes

pkg_packages

pkgng packages that are currently installed on the host system.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Package name
version	TEXT	Package version
flatsize	BIGINT	Package size in bytes
arch	TEXT	Architecture(s) supported

platform_info

Information about EFI/UEFI/ROM and platform/boot.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
vendor	TEXT	Platform code vendor
version	TEXT	Platform code version
date	TEXT	Self-reported platform code update date

revision COLUMN	TEXT TYPE	BIOS major and minor revision DESCRIPTION
address	TEXT	Relative address of firmware mapping
size	TEXT	Size in bytes of firmware
volume_size	INTEGER	(Optional) size of firmware volume
extra	TEXT	Platform-specific additional information

plist

Read and parse a plist file.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
key	TEXT	Preference top-level key
subkey	TEXT	Intermediate key path, includes lists/dicts
value	TEXT	String value of most CF types
path	TEXT	(required) read preferences from a plist

portage_keywords

A summary about portage configurations like keywords, mask and unmask.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
package	TEXT	Package name
version	TEXT	The version which are affected by the use flags, empty means all
keyword	TEXT	The keyword applied to the package

COLUMN	TYPE	DESCRIPTION
mask	INTEGER	If the package is masked
unmask	INTEGER	If the package is unmasked

portage_packages

List of currently installed packages.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
package	TEXT	Package name
version	TEXT	The version which are affected by the use flags, empty means all
slot	TEXT	The slot used by package
build_time	BIGINT	Unix time when package was built
repository	TEXT	From which repository the ebuild was used
eapi	BIGINT	The eapi for the ebuild
size	BIGINT	The size of the package
world	INTEGER	If package is in the world file

portage_use

List of enabled portage USE values for specific package.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
package	TEXT	Package name
version	TEXT	The version of the installed package

COLUMN	TYPE	DESCRIPTION
use	TEXT	USE flag which has been enabled for package

power_sensors

Machine power (currents, voltages, wattages, etc) sensors.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
key	TEXT	The SMC key on OS X
category	TEXT	The sensor category: currents, voltage, wattage
name	TEXT	Name of power source
value	TEXT	Power in Watts

powershell_events (EVENTED TABLE)

Powershell script blocks reconstructed to their full script content, this table requires script block logging to be enabled.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
time	BIGINT	Timestamp the event was received by the osquery event publisher
datetime	TEXT	System time at which the Powershell script event occurred
script_block_id	TEXT	The unique GUID of the powershell script to which this block belongs
script_block_count	INTEGER	The total number of script blocks for this script
script_text	TEXT	The text content of the Powershell script
script_name	TEXT	The name of the Powershell script
script_path	TEXT	The path for the Powershell script
cosine_similarity	DOUBLE	How similar the Powershell script is to a provided 'normal' character

COLUMN	TYPE	frequency DESCRIPTION

preferences

OS X defaults and managed preferences.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
domain	TEXT	Application ID usually in com.name.product format
key	TEXT	Preference top-level key
subkey	TEXT	Intemediate key path, includes lists/dicts
value	TEXT	String value of most CF types
forced	INTEGER	1 if the value is forced/managed, else 0
username	TEXT	(optional) read preferences for a specific user
host	TEXT	'current' or 'any' host, where 'current' takes precedence

process_envs

A key/value table of environment variables for each process.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
pid	INTEGER	Process (or thread) ID
key	TEXT	Environment variable name
value	TEXT	Environment variable value

process_events (EVENTED TABLE)

Track time/action process executions.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
pid	BIGINT	Process (or thread) ID
path	TEXT	Path of executed file
mode	TEXT	File mode permissions
cmdline	TEXT	Command line arguments (argv)
cmdline_size	BIGINT	Actual size (bytes) of command line arguments
env	TEXT	Environment variables delimited by spaces
env_count	BIGINT	Number of environment variables
env_size	BIGINT	Actual size (bytes) of environment list
cwd	TEXT	The process current working directory
auid	BIGINT	Audit User ID at process start
uid	BIGINT	User ID at process start
euid	BIGINT	Effective user ID at process start
gid	BIGINT	Group ID at process start
egid	BIGINT	Effective group ID at process start
owner_uid	BIGINT	File owner user ID
owner_gid	BIGINT	File owner group ID
atime	BIGINT	File last access in UNIX time
mtime	BIGINT	File modification in UNIX time

COLUMN	TYPE	DESCRIPTION
ctime	BIGINT	File last metadata change in UNIX time
btime	BIGINT	File creation in UNIX time
overflows	TEXT	List of structures that overflowed
parent	BIGINT	Process parent's PID, or -1 if cannot be determined.
time	BIGINT	Time of execution in UNIX time
uptime	BIGINT	Time of execution in system uptime
eid	TEXT	Event ID
status	BIGINT	OpenBSM Attribute: Status of the process
fsuid	BIGINT	Filesystem user ID at process start
suid	BIGINT	Saved user ID at process start
fsgid	BIGINT	Filesystem group ID at process start
sgid	BIGINT	Saved group ID at process start
syscall	TEXT	Syscall name: fork, vfork, clone, execve, execveat

process_file_events (EVENTED TABLE)

A File Integrity Monitor implementation using the audit service.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
operation	TEXT	Operation type
pid	BIGINT	Process ID

ppid COLUMN	BIGINT TYPE	Parent process ID DESCRIPTION

time	BIGINT	Time of execution in UNIX time
executable	TEXT	The executable path
partial	TEXT	True if this is a partial event (i.e.: this process existed before we started osquery)
cwd	TEXT	The current working directory of the process
path	TEXT	The path associated with the event
dest_path	TEXT	The canonical path associated with the event
uid	TEXT	The uid of the process performing the action
gid	TEXT	The gid of the process performing the action
auid	TEXT	Audit user ID of the process using the file
euid	TEXT	Effective user ID of the process using the file
egid	TEXT	Effective group ID of the process using the file
fsuid	TEXT	Filesystem user ID of the process using the file
fsgid	TEXT	Filesystem group ID of the process using the file
suid	TEXT	Saved user ID of the process using the file
sgid	TEXT	Saved group ID of the process using the file
uptime	BIGINT	Time of execution in system uptime
eid	TEXT	Event ID

process_memory_map

Process memory mapped files and pseudo device/regions.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
pid	INTEGER	Process (or thread) ID
start	TEXT	Virtual start address (hex)
end	TEXT	Virtual end address (hex)
permissions	TEXT	r=read, w=write, x=execute, p=private (cow)
offset	BIGINT	Offset into mapped path
device	TEXT	MA:MI Major/minor device ID
inode	INTEGER	Mapped path inode, 0 means uninitialized (BSS)
path	TEXT	Path to mapped file or mapped type
pseudo	INTEGER	1 If path is a pseudo path, else 0

process_namespaces

Linux namespaces for processes running on the host system.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
pid	INTEGER	Process (or thread) ID
cgroup_namespace	TEXT	cgroup namespace inode
ipc_namespace	TEXT	ipc namespace inode
mnt_namespace	TEXT	mnt namespace inode
net_namespace	TEXT	net namespace inode

COLUMN	TYPE	DESCRIPTION
pid_namespace	TEXT	pid namespace inode
user_namespace	TEXT	user namespace inode
uts_namespace	TEXT	uts namespace inode

process_open_files

File descriptors for each process.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
pid	BIGINT	Process (or thread) ID
fd	BIGINT	Process-specific file descriptor number
path	TEXT	Filesystem path of descriptor

process_open_pipes

Pipes and partner processes for each process.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
pid	BIGINT	Process ID
fd	BIGINT	File descriptor
mode	TEXT	Pipe open mode (r/w)
inode	BIGINT	Pipe inode number
type	TEXT	Pipe Type: named vs unnamed/anonymous
partner_pid	BIGINT	Process ID of partner process sharing a particular pipe

COLUMN	TYPE	DESCRIPTION
partner_fd	BIGINT	File descriptor of shared pipe at partner's end
partner_mode	TEXT	Mode of shared pipe at partner's end

process_open_sockets

Processes which have open network sockets on the system.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
pid	INTEGER	Process (or thread) ID
fd	BIGINT	Socket file descriptor number
socket	BIGINT	Socket handle or inode number
family	INTEGER	Network protocol (IPv4, IPv6)
protocol	INTEGER	Transport protocol (TCP/UDP)
local_address	TEXT	Socket local address
remote_address	TEXT	Socket remote address
local_port	INTEGER	Socket local port
remote_port	INTEGER	Socket remote port
path	TEXT	For UNIX sockets (family=AF_UNIX), the domain path
state	TEXT	TCP socket state
net_namespace	TEXT	The inode number of the network namespace

processes

All running processes on the host system.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
pid	BIGINT	Process (or thread) ID
name	TEXT	The process path or shorthand argv[0]
path	TEXT	Path to executed binary
cmdline	TEXT	Complete argv
state	TEXT	Process state
cwd	TEXT	Process current working directory
root	TEXT	Process virtual root directory
uid	BIGINT	Unsigned user ID
gid	BIGINT	Unsigned group ID
euid	BIGINT	Unsigned effective user ID
egid	BIGINT	Unsigned effective group ID
suid	BIGINT	Unsigned saved user ID
sgid	BIGINT	Unsigned saved group ID
on_disk	INTEGER	The process path exists yes=1, no=0, unknown=-1
wired_size	BIGINT	Bytes of unpagable memory used by process
resident_size	BIGINT	Bytes of private memory used by process
total_size	BIGINT	Total virtual memory size
user_time	BIGINT	CPU time in milliseconds spent in user space

COLUMN	TYPE	DESCRIPTION
system_time	BIGINT	CPU time in milliseconds spent in kernel space
disk_bytes_read	BIGINT	Bytes read from disk
disk_bytes_written	BIGINT	Bytes written to disk
start_time	BIGINT	Process start time in seconds since Epoch, in case of error -1
parent	BIGINT	Process parent's PID
pgroup	BIGINT	Process group
threads	INTEGER	Number of threads used by process
nice	INTEGER	Process nice level (-20 to 20, default 0)
is_elevated_token	INTEGER	Process uses elevated token yes=1, no=0
elapsed_time	BIGINT	Elapsed time in seconds this process has been running.
handle_count	BIGINT	Total number of handles that the process has open. This number is the sum of the handles currently opened by each thread in the process.
percent_processor_time	BIGINT	Returns elapsed time that all of the threads of this process used the processor to execute instructions in 100 nanoseconds ticks.
upid	BIGINT	A 64bit pid that is never reused. Returns -1 if we couldn't gather them from the system.
uppid	BIGINT	The 64bit parent pid that is never reused. Returns -1 if we couldn't gather them from the system.
cpu_type	INTEGER	Indicates the specific processor designed for installation.
cpu_subtype	INTEGER	Indicates the specific processor on which an entry may be used.

programs

Represents products as they are installed by Windows Installer. A product generally correlates to one installation package on Windows. Some fields may be blank as Windows installation details are left to the discretion of the product author.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Commonly used product name.
version	TEXT	Product version information.
install_location	TEXT	The installation location directory of the product.
install_source	TEXT	The installation source of the product.
language	TEXT	The language of the product.
publisher	TEXT	Name of the product supplier.
uninstall_string	TEXT	Path and filename of the uninstaller.
install_date	TEXT	Date that this product was installed on the system.
identifying_number	TEXT	Product identification such as a serial number on software, or a die number on a hardware chip.

prometheus_metrics

Retrieve metrics from a Prometheus server.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
target_name	TEXT	Address of prometheus target
metric_name	TEXT	Name of collected Prometheus metric
metric_value	DOUBLE	Value of collected Prometheus metric
timestamp_ms	BIGINT	Unix timestamp of collected data in MS

python_packages

Python packages installed in a system.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Package display name
version	TEXT	Package-supplied version
summary	TEXT	Package-supplied summary
author	TEXT	Optional package author
license	TEXT	License under which package is launched
path	TEXT	Path at which this module resides
directory	TEXT	Directory where Python modules are located

quicklook_cache

Files and thumbnails within OS X's Quicklook Cache.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
path	TEXT	Path of file
rowid	INTEGER	Quicklook file rowid key
fs_id	TEXT	Quicklook file fs_id key
volume_id	INTEGER	Parsed volume ID from fs_id
inode	INTEGER	Parsed file ID (inode) from fs_id
mtime	INTEGER	Parsed version date field

COLUMN	TYPE	DESCRIPTION
size	BIGINT	Parsed version size field
label	TEXT	Parsed version 'gen' field
last_hit_date	INTEGER	Apple date format for last thumbnail cache hit
hit_count	TEXT	Number of cache hits on thumbnail
icon_mode	BIGINT	Thumbnail icon mode
cache_path	TEXT	Path to cache data

registry

All of the Windows registry hives.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
key	TEXT	Name of the key to search for
path	TEXT	Full path to the value
name	TEXT	Name of the registry value entry
type	TEXT	Type of the registry value, or 'subkey' if item is a subkey
data	TEXT	Data content of registry value
mtime	BIGINT	timestamp of the most recent registry write

routes

The active route table for the host system.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION

COLUMN	TYPE	DESCRIPTION
destination	TEXT	Destination IP address
netmask	INTEGER	Netmask length
gateway	TEXT	Route gateway
source	TEXT	Route source
flags	INTEGER	Flags to describe route
interface	TEXT	Route local interface
mtu	INTEGER	Maximum Transmission Unit for the route
metric	INTEGER	Cost of route. Lowest is preferred
type	TEXT	Type of route
hopcount	INTEGER	Max hops expected

rpm_package_files

RPM packages that are currently installed on the host system.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
package	TEXT	RPM package name
path	TEXT	File path within the package
username	TEXT	File default username from info DB
groupname	TEXT	File default groupname from info DB
mode	TEXT	File permissions mode from info DB

size COLUMN	BIGINT TYPE	Expected file size in bytes from RPM info DB DESCRIPTION
sha256	TEXT	SHA256 file digest from RPM info DB

rpm_packages

RPM packages that are currently installed on the host system.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	RPM package name
version	TEXT	Package version
release	TEXT	Package release
source	TEXT	Source RPM package name (optional)
size	BIGINT	Package size in bytes
sha1	TEXT	SHA1 hash of the package contents
arch	TEXT	Architecture(s) supported
epoch	INTEGER	Package epoch value
install_time	INTEGER	When the package was installed
vendor	TEXT	Package vendor
package_group	TEXT	Package group
pid_with_namespace	INTEGER	Pids that contain a namespace
mount_namespace_id	TEXT	Mount namespace id

running_apps

macOS applications currently running on the host system.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
pid	INTEGER	The pid of the application
bundle_identifier	TEXT	The bundle identifier of the application
is_active	INTEGER	1 if the application is in focus, 0 otherwise

safari_extensions

Safari browser extension details for all users.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
uid	BIGINT	The local user that owns the extension
name	TEXT	Extension display name
identifier	TEXT	Extension identifier
version	TEXT	Extension long version
sdk	TEXT	Bundle SDK used to compile extension
update_url	TEXT	Extension-supplied update URI
author	TEXT	Optional extension author
developer_id	TEXT	Optional developer identifier
description	TEXT	Optional extension description text
path	TEXT	Path to extension XAR bundle

sandboxes

OS X application sandboxes container details.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
label	TEXT	UTI-format bundle or label ID
user	TEXT	Sandbox owner
enabled	INTEGER	Application sandboxings enabled on container
build_id	TEXT	Sandbox-specific identifier
bundle_path	TEXT	Application bundle used by the sandbox
path	TEXT	Path to sandbox container directory

scheduled_tasks

Lists all of the tasks in the Windows task scheduler.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Name of the scheduled task
action	TEXT	Actions executed by the scheduled task
path	TEXT	Path to the executable to be run
enabled	INTEGER	Whether or not the scheduled task is enabled
state	TEXT	State of the scheduled task
hidden	INTEGER	Whether or not the task is visible in the UI
last_run_time	INTEGER	Timestamp the task last ran

COLUMN	TYPE	DESCRIPTION
next_run_time	INTEGER	Timestamp the task is scheduled to run next
last_run_message	TEXT	Exit status message of the last task run
last_run_code	TEXT	Exit status code of the last task run

screenlock

macOS screenlock status for the current logged in user context.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
enabled	INTEGER	1 If a password is required after sleep or the screensaver begins; else 0
grace_period	INTEGER	The amount of time in seconds the screen must be asleep or the screensaver on before a password is required on-wake. 0 = immediately; -1 = no password is required on-wake

selinux_events (EVENTED TABLE)

Track SELinux events.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
type	TEXT	Event type
message	TEXT	Message
time	BIGINT	Time of execution in UNIX time
uptime	BIGINT	Time of execution in system uptime
eid	TEXT	Event ID

selinux_settings

Track active SELinux settings.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
scope	TEXT	Where the key is located inside the SELinuxFS mount point.
key	TEXT	Key or class name.
value	TEXT	Active value.

services

Lists all installed Windows services and their relevant data.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Service name
service_type	TEXT	Service Type: OWN_PROCESS, SHARE_PROCESS and maybe Interactive (can interact with the desktop)
display_name	TEXT	Service Display name
status	TEXT	Service Current status: STOPPED, START_PENDING, STOP_PENDING, RUNNING, CONTINUE_PENDING, PAUSE_PENDING, PAUSED
pid	INTEGER	the Process ID of the service
start_type	TEXT	Service start type: BOOT_START, SYSTEM_START, AUTO_START, DEMAND_START, DISABLED
win32_exit_code	INTEGER	The error code that the service uses to report an error that occurs when it is starting or stopping
service_exit_code	INTEGER	The service-specific error code that the service returns when an error occurs while the service is starting or stopping
path	TEXT	Path to Service Executable

COLUMN	TYPE	DESCRIPTION
module_path	TEXT	Path to ServiceDll
description	TEXT	Service Description
user_account	TEXT	The name of the account that the service process will be logged on as when it runs. This name can be of the form Domain\UserName. If the account belongs to the built-in domain, the name can be of the form .\UserName.

shadow

Local system users encrypted passwords and related information. Please note, that you usually need superuser rights to access `/etc/shadow`.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
password_status	TEXT	Password status
hash_alg	TEXT	Password hashing algorithm
last_change	BIGINT	Date of last password change (starting from UNIX epoch date)
min	BIGINT	Minimal number of days between password changes
max	BIGINT	Maximum number of days between password changes
warning	BIGINT	Number of days before password expires to warn user about it
inactive	BIGINT	Number of days after password expires until account is blocked
expire	BIGINT	Number of days since UNIX epoch date until account is disabled
flag	BIGINT	Reserved
username	TEXT	Username

shared_folders

Folders available to others via SMB or AFP.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	The shared name of the folder as it appears to other users
path	TEXT	Absolute path of shared folder on the local system

shared_memory

OS shared memory regions.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
shmid	INTEGER	Shared memory segment ID
owner_uid	BIGINT	User ID of owning process
creator_uid	BIGINT	User ID of creator process
pid	BIGINT	Process ID to last use the segment
creator_pid	BIGINT	Process ID that created the segment
atime	BIGINT	Attached time
dtime	BIGINT	Detached time
ctime	BIGINT	Changed time
permissions	TEXT	Memory segment permissions
size	BIGINT	Size in bytes
attached	INTEGER	Number of attached processes
status	TEXT	Destination/attach status

COLUMN	TYPE	DESCRIPTION
locked	INTEGER	1 if segment is locked else 0

shared_resources

Displays shared resources on a computer system running Windows. This may be a disk drive, printer, interprocess communication, or other sharable device.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
description	TEXT	A textual description of the object
install_date	TEXT	Indicates when the object was installed. Lack of a value does not indicate that the object is not installed.
status	TEXT	String that indicates the current status of the object.
allow_maximum	INTEGER	Number of concurrent users for this resource has been limited. If True, the value in the MaximumAllowed property is ignored.
maximum_allowed	INTEGER	Limit on the maximum number of users allowed to use this resource concurrently. The value is only valid if the AllowMaximum property is set to FALSE.
name	TEXT	Alias given to a path set up as a share on a computer system running Windows.
path	TEXT	Local path of the Windows share.
type	INTEGER	Type of resource being shared. Types include: disk drives, print queues, interprocess communications (IPC), and general devices.

sharing_preferences

OS X Sharing preferences.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
screen_sharing	INTEGER	1 If screen sharing is enabled else 0
file_sharing	INTEGER	1 If file sharing is enabled else 0

COLUMN	TYPE	DESCRIPTION
printer_sharing	INTEGER	1 If printer sharing is enabled else 0
remote_login	INTEGER	1 If remote login is enabled else 0
remote_management	INTEGER	1 If remote management is enabled else 0
remote_apple_events	INTEGER	1 If remote apple events are enabled else 0
internet_sharing	INTEGER	1 If internet sharing is enabled else 0
bluetooth_sharing	INTEGER	1 If bluetooth sharing is enabled for any user else 0
disc_sharing	INTEGER	1 If CD or DVD sharing is enabled else 0
content_caching	INTEGER	1 If content caching is enabled else 0

shell_history

A line-delimited (command) table of per-user .*_history data.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
uid	BIGINT	Shell history owner
time	INTEGER	Entry timestamp. It could be absent, default value is 0.
command	TEXT	Unparsed date/line/command history line
history_file	TEXT	Path to the .*_history for this user

shimcache

Application Compatibility Cache, contains artifacts of execution.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION

COLUMN	TYPE	DESCRIPTION
entry	INTEGER	Execution order.
path	TEXT	This is the path to the executed file.
modified_time	INTEGER	File Modified time.
execution_flag	INTEGER	Boolean Execution flag, 1 for execution, 0 for no execution, -1 for missing (this flag does not exist on Windows 10 and higher).

signature

File (executable, bundle, installer, disk) code signing status.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
path	TEXT	Must provide a path or directory
hash_resources	INTEGER	Set to 1 to also hash resources, or 0 otherwise. Default is 1
arch	TEXT	If applicable, the arch of the signed code
signed	INTEGER	1 If the file is signed else 0
identifier	TEXT	The signing identifier sealed into the signature
cdhash	TEXT	Hash of the application Code Directory
team_identifier	TEXT	The team signing identifier sealed into the signature
authority	TEXT	Certificate Common Name

sip_config

Apple's System Integrity Protection (rootless) status.

Improve this Description on Github

COLUMN COLUMN	TYPE TYPE	DESCRIPTION DESCRIPTION
config_flag	TEXT	The System Integrity Protection config flag
enabled	INTEGER	1 if this configuration is enabled, otherwise 0
enabled_nvram	INTEGER	1 if this configuration is enabled, otherwise 0

smart_drive_info

Drive information read by SMART controller utilizing autodetect.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
device_name	TEXT	Name of block device
disk_id	INTEGER	Physical slot number of device, only exists when hardware storage controller exists
driver_type	TEXT	The explicit device type used to retrieve the SMART information
model_family	TEXT	Drive model family
device_model	TEXT	Device Model
serial_number	TEXT	Device serial number
lu_wwn_device_id	TEXT	Device Identifier
additional_product_id	TEXT	An additional drive identifier if any
firmware_version	TEXT	Drive firmware version
user_capacity	TEXT	Bytes of drive capacity
sector_sizes	TEXT	Bytes of drive sector sizes

COLUMN	TYPE	DESCRIPTION
rotation_rate	TEXT	Drive RPM
form_factor	TEXT	Form factor if reported
in_smartctl_db	INTEGER	Boolean value for if drive is recognized
ata_version	TEXT	ATA version of drive
transport_type	TEXT	Drive transport type
sata_version	TEXT	SATA version, if any
read_device_identity_failure	TEXT	Error string for device id read, if any
smart_supported	TEXT	SMART support status
smart_enabled	TEXT	SMART enabled status
packet_device_type	TEXT	Packet device type
power_mode	TEXT	Device power mode
warnings	TEXT	Warning messages from SMART controller

smbios_tables

BIOS (DMI) structure common details and content.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
number	INTEGER	Table entry number
type	INTEGER	Table entry type
description	TEXT	Table entry description

handle COLUMN	INTEGER TYPE	Table entry handle DESCRIPTION
header_size	INTEGER	Header size in bytes
size	INTEGER	Table entry size in bytes
md5	TEXT	MD5 hash of table entry

smc_keys

Apple's system management controller keys.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
key	TEXT	4-character key
type	TEXT	SMC-reported type literal type
size	INTEGER	Reported size of data in bytes
value	TEXT	A type-encoded representation of the key value
hidden	INTEGER	1 if this key is normally hidden, otherwise 0

socket_events (EVENTED TABLE)

Track network socket opens and closes.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
action	TEXT	The socket action (bind, listen, close)
pid	BIGINT	Process (or thread) ID
path	TEXT	Path of executed file

COLUMN	TYPE	DESCRIPTION
fd	TEXT	The file description for the process socket
auid	BIGINT	Audit User ID
success	INTEGER	The socket open attempt status
family	INTEGER	The Internet protocol family ID
protocol	INTEGER	The network protocol ID
local_address	TEXT	Local address associated with socket
remote_address	TEXT	Remote address associated with socket
local_port	INTEGER	Local network protocol port number
remote_port	INTEGER	Remote network protocol port number
socket	TEXT	The local path (UNIX domain socket only)
time	BIGINT	Time of execution in UNIX time
uptime	BIGINT	Time of execution in system uptime
eid	TEXT	Event ID

ssh_configs

A table of parsed ssh_configs.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
uid	BIGINT	The local owner of the ssh_config file
block	TEXT	The host or match block

option COLUMN	TEXT TYPE	The option and value DESCRIPTION
ssh_config_file	TEXT	Path to the ssh_config file

startup_items

Applications and binaries set as user/login startup items.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Name of startup item
path	TEXT	Path of startup item
args	TEXT	Arguments provided to startup executable
type	TEXT	Startup Item or Login Item
source	TEXT	Directory or plist containing startup item
status	TEXT	Startup status; either enabled or disabled
username	TEXT	The user associated with the startup item

sudoers

Rules for running commands as other users via sudo.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
source	TEXT	Source file containing the given rule
header	TEXT	Symbol for given rule
rule_details	TEXT	Rule definition

COLUMN	TYPE	DESCRIPTION

suid_bin

suid binaries in common locations.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
path	TEXT	Binary path
username	TEXT	Binary owner username
groupname	TEXT	Binary owner group
permissions	TEXT	Binary permissions

syslog_events (EVENTED TABLE)

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
time	BIGINT	Current unix epoch time
datetime	TEXT	Time known to syslog
host	TEXT	Hostname configured for syslog
severity	INTEGER	Syslog severity
facility	TEXT	Syslog facility
tag	TEXT	The syslog tag
message	TEXT	The syslog message
eid	TEXT	Event ID

system_controls

system_controls

sysctl names, values, and settings information.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Full sysctl MIB name
oid	TEXT	Control MIB
subsystem	TEXT	Subsystem ID, control type
current_value	TEXT	Value of setting
config_value	TEXT	The MIB value set in /etc/sysctl.conf
type	TEXT	Data type
field_name	TEXT	Specific attribute of opaque type

system_info

System information for identification.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
hostname	TEXT	Network hostname including domain
uuid	TEXT	Unique ID provided by the system
cpu_type	TEXT	CPU type
cpu_subtype	TEXT	CPU subtype
cpu_brand	TEXT	CPU brand string, contains vendor and model
cpu_physical_cores	INTEGER	Number of physical CPU cores in to the system
cpu_logical_cores	INTEGER	Number of logical CPU cores available to the system

COLUMN	TYPE	DESCRIPTION
cpu_microcode	TEXT	Microcode version
physical_memory	BIGINT	Total physical memory in bytes
hardware_vendor	TEXT	Hardware vendor
hardware_model	TEXT	Hardware model
hardware_version	TEXT	Hardware version
hardware_serial	TEXT	Device serial number
board_vendor	TEXT	Board vendor
board_model	TEXT	Board model
board_version	TEXT	Board version
board_serial	TEXT	Board serial number
computer_name	TEXT	Friendly computer name (optional)
local_hostname	TEXT	Local hostname (optional)

temperature_sensors

Machine's temperature sensors.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
key	TEXT	The SMC key on OS X
name	TEXT	Name of temperature source
celsius	DOUBLE	Temperature in Celsius

fahrenheit COLUMN	DOUBLE TYPE	Temperature in Fahrenheit DESCRIPTION

time

Track current date and time in the system.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
weekday	TEXT	Current weekday in the system
year	INTEGER	Current year in the system
month	INTEGER	Current month in the system
day	INTEGER	Current day in the system
hour	INTEGER	Current hour in the system
minutes	INTEGER	Current minutes in the system
seconds	INTEGER	Current seconds in the system
timezone	TEXT	Current timezone in the system
local_time	INTEGER	Current local UNIX time in the system
local_timezone	TEXT	Current local timezone in the system
unix_time	INTEGER	Current UNIX time in the system, converted to UTC if --utc enabled
timestamp	TEXT	Current timestamp (log format) in the system
datetime	TEXT	Current date and time (ISO format) in the system
iso_8601	TEXT	Current time (ISO format) in the system
win_timestamp	BIGINT	Timestamp value in 100 nanosecond units.

time_machine_backups

Backups to drives using TimeMachine.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
destination_id	TEXT	Time Machine destination ID
backup_date	INTEGER	Backup Date

time_machine_destinations

Locations backed up to using Time Machine.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
alias	TEXT	Human readable name of drive
destination_id	TEXT	Time Machine destination ID
consistency_scan_date	INTEGER	Consistency scan date
root_volume_uuid	TEXT	Root UUID of backup volume
bytes_available	INTEGER	Bytes available on volume
bytes_used	INTEGER	Bytes used on volume
encryption	TEXT	Last known encrypted state

ulimit_info

System resource usage limits.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
type	TEXT	System resource to be limited

COLUMN	TYPE	DESCRIPTION
soft_limit	TEXT	Current limit value
hard_limit	TEXT	Maximum limit value

uptime

Track time passed since last boot.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
days	INTEGER	Days of uptime
hours	INTEGER	Hours of uptime
minutes	INTEGER	Minutes of uptime
seconds	INTEGER	Seconds of uptime
total_seconds	BIGINT	Total uptime seconds

usb_devices

USB devices that are actively plugged into the host system.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
usb_address	INTEGER	USB Device used address
usb_port	INTEGER	USB Device used port
vendor	TEXT	USB Device vendor string
vendor_id	TEXT	Hex encoded USB Device vendor identifier
version	TEXT	USB Device version number

COLUMN	TYPE	DESCRIPTION
model	TEXT	USB Device model string
model_id	TEXT	Hex encoded USB Device model identifier
serial	TEXT	USB Device serial connection
class	TEXT	USB Device class
subclass	TEXT	USB Device subclass
protocol	TEXT	USB Device protocol
removable	INTEGER	1 If USB device is removable else 0

user_events (EVENTED TABLE)

Track user events from the audit framework.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
uid	BIGINT	User ID
auid	BIGINT	Audit User ID
pid	BIGINT	Process (or thread) ID
message	TEXT	Message from the event
type	INTEGER	The file description for the process socket
path	TEXT	Supplied path from event
address	TEXT	The Internet protocol address or family ID
terminal	TEXT	The network protocol ID

COLUMN	TYPE	DESCRIPTION
time	BIGINT	Time of execution in UNIX time
uptime	BIGINT	Time of execution in system uptime
eid	TEXT	Event ID

user_groups

Local system user group relationships.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
uid	BIGINT	User ID
gid	BIGINT	Group ID

user_interaction_events (EVENTED TABLE)

Track user interaction events from macOS' event tapping framework.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
time	BIGINT	Time

user_ssh_keys

Returns the private keys in the users ~/.ssh directory and whether or not they are encrypted.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
uid	BIGINT	The local user that owns the key file
path	TEXT	Path to key file

COLUMN	TYPE	DESCRIPTION
encrypted	INTEGER	1 if key is encrypted, 0 otherwise

userassist

UserAssist Registry Key tracks when a user executes an application from Windows Explorer.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
path	TEXT	Application file path.
last_execution_time	INTEGER	Most recent time application was executed.
count	INTEGER	Number of times the application has been executed.
sid	TEXT	User SID.

users

Local user accounts (including domain accounts that have logged on locally (Windows)).

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
uid	BIGINT	User ID
gid	BIGINT	Group ID (unsigned)
uid_signed	BIGINT	User ID as int64 signed (Apple)
gid_signed	BIGINT	Default group ID as int64 signed (Apple)
username	TEXT	Username
description	TEXT	Optional user description
directory	TEXT	User's home directory
shell	TEXT	User's configured default shell

COLUMN	TYPE	DESCRIPTION
uuid	TEXT	User's UUID (Apple) or SID (Windows)
type	TEXT	Whether the account is roaming (domain), local, or a system profile
is_hidden	INTEGER	IsHidden attribute set in OpenDirectory

video_info

Retrieve video card information of the machine.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
color_depth	INTEGER	The amount of bits per pixel to represent color.
driver	TEXT	The driver of the device.
driver_date	BIGINT	The date listed on the installed driver.
driver_version	TEXT	The version of the installed driver.
manufacturer	TEXT	The manufaturer of the gpu.
model	TEXT	The model of the gpu.
series	TEXT	The series of the gpu.
video_mode	TEXT	The current resolution of the display.

virtual_memory_info

Darwin Virtual Memory statistics.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
free	BIGINT	Total number of free pages.

COLUMN	TYPE	DESCRIPTION
active	BIGINT	Total number of active pages.
inactive	BIGINT	Total number of inactive pages.
speculative	BIGINT	Total number of speculative pages.
throttled	BIGINT	Total number of throttled pages.
wired	BIGINT	Total number of wired down pages.
purgeable	BIGINT	Total number of purgeable pages.
faults	BIGINT	Total number of calls to vm_faults.
copy	BIGINT	Total number of copy-on-write pages.
zero_fill	BIGINT	Total number of zero filled pages.
reactivated	BIGINT	Total number of reactivated pages.
purged	BIGINT	Total number of purged pages.
file_backed	BIGINT	Total number of file backed pages.
anonymous	BIGINT	Total number of anonymous pages.
uncompressed	BIGINT	Total number of uncompressed pages.
compressor	BIGINT	The number of pages used to store compressed VM pages.
decompressed	BIGINT	The total number of pages that have been decompressed by the VM compressor.
compressed	BIGINT	The total number of pages that have been compressed by the VM compressor.
page_ins	BIGINT	The total number of requests for pages from a pager.

page_outs COLUMN	BIGINT TYPE	Total number of pages paged out. DESCRIPTION
swap_ins	BIGINT	The total number of compressed pages that have been swapped out to disk.
swap_outs	BIGINT	The total number of compressed pages that have been swapped back in from disk.

wifi_networks

OS X known/remembered Wi-Fi networks list.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
ssid	TEXT	SSID octets of the network
network_name	TEXT	Name of the network
security_type	TEXT	Type of security on this network
last_connected	INTEGER	Last time this network was connected to as a unix_time
passpoint	INTEGER	1 if Passpoint is supported, 0 otherwise
possibly_hidden	INTEGER	1 if network is possibly a hidden network, 0 otherwise
roaming	INTEGER	1 if roaming is supported, 0 otherwise
roaming_profile	TEXT	Describe the roaming profile, usually one of Single, Dual or Multi
captive_portal	INTEGER	1 if this network has a captive portal, 0 otherwise
auto_login	INTEGER	1 if auto login is enabled, 0 otherwise
temporarily_disabled	INTEGER	1 if this network is temporarily disabled, 0 otherwise
disabled	INTEGER	1 if this network is disabled, 0 otherwise

wifi_status

OS X current WiFi status.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
interface	TEXT	Name of the interface
ssid	TEXT	SSID octets of the network
bssid	TEXT	The current basic service set identifier
network_name	TEXT	Name of the network
country_code	TEXT	The country code (ISO/IEC 3166-1:1997) for the network
security_type	TEXT	Type of security on this network
rssi	INTEGER	The current received signal strength indication (dbm)
noise	INTEGER	The current noise measurement (dBm)
channel	INTEGER	Channel number
channel_width	INTEGER	Channel width
channel_band	INTEGER	Channel band
transmit_rate	TEXT	The current transmit rate
mode	TEXT	The current operating mode for the Wi-Fi interface

wifi_survey

Scan for nearby WiFi networks.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION

COLUMN	TYPE	DESCRIPTION
interface	TEXT	Name of the interface
ssid	TEXT	SSID octets of the network
bssid	TEXT	The current basic service set identifier
network_name	TEXT	Name of the network
country_code	TEXT	The country code (ISO/IEC 3166-1:1997) for the network
rssi	INTEGER	The current received signal strength indication (dbm)
noise	INTEGER	The current noise measurement (dBm)
channel	INTEGER	Channel number
channel_width	INTEGER	Channel width
channel_band	INTEGER	Channel band

winbaseobj

Lists named Windows objects in the default object directories, across all terminal services sessions. Example Windows ojbect types include Mutexes, Events, Jobs and Semaphors.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
session_id	INTEGER	Terminal Services Session Id
object_name	TEXT	Object Name
object_type	TEXT	Object Type

windows_crashes

Extracted information from Windows crash logs (Minidumps).

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
datetime	TEXT	Timestamp (log format) of the crash
module	TEXT	Path of the crashed module within the process
path	TEXT	Path of the executable file for the crashed process
pid	BIGINT	Process ID of the crashed process
tid	BIGINT	Thread ID of the crashed thread
version	TEXT	File version info of the crashed process
process_uptime	BIGINT	Uptime of the process in seconds
stack_trace	TEXT	Multiple stack frames from the stack trace
exception_code	TEXT	The Windows exception code
exception_message	TEXT	The NTSTATUS error message associated with the exception code
exception_address	TEXT	Address (in hex) where the exception occurred
registers	TEXT	The values of the system registers
command_line	TEXT	Command-line string passed to the crashed process
current_directory	TEXT	Current working directory of the crashed process
username	TEXT	Username of the user who ran the crashed process
machine_name	TEXT	Name of the machine where the crash happened
major_version	INTEGER	Windows major version of the machine
minor_version	INTEGER	Windows minor version of the machine

COLUMN	TYPE	DESCRIPTION
build_number	INTEGER	Windows build number of the crashing machine
type	TEXT	Type of crash log
crash_path	TEXT	Path of the log file

windows_eventlog

Table for querying all recorded Windows event logs.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
channel	TEXT	Source or channel of the event
datetime	TEXT	System time at which the event occurred
task	INTEGER	Task value associated with the event
level	INTEGER	Severity level associated with the event
provider_name	TEXT	Provider name of the event
provider_guid	TEXT	Provider guid of the event
eventid	INTEGER	Event ID of the event
keywords	TEXT	A bitmask of the keywords defined in the event
data	TEXT	Data associated with the event
pid	INTEGER	Process ID which emitted the event record
tid	INTEGER	Thread ID which emitted the event record
time_range	TEXT	System time to selectively filter the events

timestamp COLUMN	TEXT TYPE	Timestamp to selectively filter the events DESCRIPTION
xpath	TEXT	The custom query to filter events

windows_events (EVENTED TABLE)

Windows Event logs.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
time	BIGINT	Timestamp the event was received
datetime	TEXT	System time at which the event occurred
source	TEXT	Source or channel of the event
provider_name	TEXT	Provider name of the event
provider_guid	TEXT	Provider guid of the event
eventid	INTEGER	Event ID of the event
task	INTEGER	Task value associated with the event
level	INTEGER	The severity level associated with the event
keywords	TEXT	A bitmask of the keywords defined in the event
data	TEXT	Data associated with the event
eid	TEXT	Event ID

windows_optional_features

Lists names and installation states of windows features. Maps to Win32_OptionalFeature WMI class.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Name of the feature
caption	TEXT	Caption of feature in settings UI
state	INTEGER	Installation state value. 1 == Enabled, 2 == Disabled, 3 == Absent
statename	TEXT	Installation state name. 'Enabled','Disabled','Absent'

windows_security_center

The health status of Window Security features. Health values can be "Good", "Poor". "Snoozed", "Not Monitored", and "Error".

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
firewall	TEXT	The health of the monitored Firewall (see windows_security_products)
autoupdate	TEXT	The health of the Windows Autoupdate feature
antivirus	TEXT	The health of the monitored Antivirus solution (see windows_security_products)
antispyware	TEXT	The health of the monitored Antispyware solution (see windows_security_products)
internet_settings	TEXT	The health of the Internet Settings
windows_security_center_service	TEXT	The health of the Windows Security Center Service
user_account_control	TEXT	The health of the User Account Control (UAC) capability in Windows

windows_security_products

Enumeration of registered Windows security products.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
type	TEXT	Type of security product
name	TEXT	Name of product
state	TEXT	State of protection
state_timestamp	TEXT	Timestamp for the product state
remediation_path	TEXT	Remediation path
signatures_up_to_date	INTEGER	1 if product signatures are up to date, else 0

wmi_bios_info

Lists important information from the system bios.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Name of the Bios setting
value	TEXT	Value of the Bios setting

wmi_cli_event_consumers

WMI CommandLineEventConsumer, which can be used for persistence on Windows. See https://www.blackhat.com/docs/us-15/materials/us-15-Graeber-Abusing-Windows-Management-Instrumentation-WMI-To-Build-A-Persistent%20Asynchronous-And-Fileless-Backdoor-wp.pdf for more details.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Unique name of a consumer.
		Standard string template that specifies the process to be started. This

COLUMN	TYPE	DESCRIPTION
command_line_template	TEXT	Standard string template that specifies the process to be started. This property can be NULL, and the ExecutablePath property is used as the command line.
executable_path	TEXT	Module to execute. The string can specify the full path and file name of the module to execute, or it can specify a partial name. If a partial name is specified, the current drive and current directory are assumed.
class	TEXT	The name of the class.
relative_path	TEXT	Relative path to the class or instance.

wmi_event_filters

Lists WMI event filters.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Unique identifier of an event filter.
query	TEXT	Windows Management Instrumentation Query Language (WQL) event query that specifies the set of events for consumer notification, and the specific conditions for notification.
query_language	TEXT	Query language that the query is written in.
class	TEXT	The name of the class.
relative_path	TEXT	Relative path to the class or instance.

wmi_filter_consumer_binding

Lists the relationship between event consumers and filters.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
consumer	TEXT	Reference to an instance of __EventConsumer that represents the object path to a logical consumer, the recipient of an event

a logical consumer, the recipient of an event.

COLUMN	TYPE	DESCRIPTION
filter	TEXT	Reference to an instance of __EventFilter that represents the object path to an event filter which is a query that specifies the type of event to be received.
class	TEXT	The name of the class.
relative_path	TEXT	Relative path to the class or instance.

wmi_script_event_consumers

WMI ActiveScriptEventConsumer, which can be used for persistence on Windows. See https://www.blackhat.com/docs/us-15/materials/us-15-Graeber-Abusing-Windows-Management-Instrumentation-WMI-To-Build-A-Persistent%20Asynchronous-And-Fileless-Backdoor-wp.pdf for more details.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Unique identifier for the event consumer.
scripting_engine	TEXT	Name of the scripting engine to use, for example, 'VBScript'. This property cannot be NULL.
script_file_name	TEXT	Name of the file from which the script text is read, intended as an alternative to specifying the text of the script in the ScriptText property.
script_text	TEXT	Text of the script that is expressed in a language known to the scripting engine. This property must be NULL if the ScriptFileName property is not NULL.
class	TEXT	The name of the class.
relative_path	TEXT	Relative path to the class or instance.

xprotect_entries

Database of the machine's XProtect signatures.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Description of XProtected malware
launch_type	TEXT	Launch services content type
identity	TEXT	XProtect identity (SHA1) of content
filename	TEXT	Use this file name to match
filetype	TEXT	Use this file type to match
optional	INTEGER	Match any of the identities/patterns for this XProtect name
uses_pattern	INTEGER	Uses a match pattern instead of identity

xprotect_meta

Database of the machine's XProtect browser-related signatures.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
identifier	TEXT	Browser plugin or extension identifier
type	TEXT	Either plugin or extension
developer_id	TEXT	Developer identity (SHA1) of extension
min_version	TEXT	The minimum allowed plugin version.

xprotect_reports

Database of XProtect matches (if user generated/sent an XProtect report).

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION

COLUMN	TYPE	DESCRIPTION
name	TEXT	Description of XProtected malware
user_action	TEXT	Action taken by user after prompted
time	TEXT	Quarantine alert time

yara

Track YARA matches for files or PIDs.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
path	TEXT	The path scanned
matches	TEXT	List of YARA matches
count	INTEGER	Number of YARA matches
sig_group	TEXT	Signature group used
sigfile	TEXT	Signature file used
sigrule	TEXT	Signature strings used
strings	TEXT	Matching strings
tags	TEXT	Matching tags
sigurl	TEXT	Signature url

yara_events (EVENTED TABLE)

Track YARA matches for files specified in configuration data.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION

COLUMN	TYPE	DESCRIPTION
target_path	TEXT	The path scanned
category	TEXT	The category of the file
action	TEXT	Change action (UPDATE, REMOVE, etc)
transaction_id	BIGINT	ID used during bulk update
matches	TEXT	List of YARA matches
count	INTEGER	Number of YARA matches
strings	TEXT	Matching strings
tags	TEXT	Matching tags
time	BIGINT	Time of the scan
eid	TEXT	Event ID

yum_sources

Current list of Yum repositories or software channels.

Improve this Description on Github

COLUMN	TYPE	DESCRIPTION
name	TEXT	Repository name
baseurl	TEXT	Repository base URL
enabled	TEXT	Whether the repository is used
gpgcheck	TEXT	Whether packages are GPG checked
gpgkey	TEXT	URL to GPG key

Open Source

View the code on GitHub

Resources

Blog

Schema

Docs

Downloads

THE LINUX FOUNDATION PROJECTS

Site made with ♥ by Kolide