Name of the OSQuery Table	Description
account_policy_data	Displays information about user account policies such as password expiration and lockout policies.
acpi_tables	Shows information from the system's ACPI (Advanced Configuration and Power Interface) tables for hardware management.
ad_config	Provides the configuration settings for Active Directory integration on the system.
alf	Displays the status and configuration of the Application Layer Firewall (ALF) on macOS.
alf_exceptions	Lists applications and services that are allowed to bypass the macOS firewall.
alf_explicit_auths	Shows explicitly allowed or denied applications in the macOS firewall.
app_schemes	Lists custom URL schemes that are registered by installed applications.
apparmor_events	Displays events logged by AppArmor, a Linux security module.
apparmor_profiles	Shows active AppArmor security profiles that restrict what certain applications can do.
appcompat_shims	Lists compatibility fixes (shims) applied to applications in Windows for better functionality.
apps	Displays a list of installed applications on the system, including versions and installation paths.
apt_sources	Lists the repositories configured for the Advanced Package Tool (APT) on Linux systems.
arp_cache	Displays the system's ARP (Address Resolution Protocol) cache, showing mappings between IP and MAC addresses.
asl	Shows Apple System Logger (ASL) messages logged on macOS systems.
atom_packages	Lists installed packages for the Atom text editor.
augeas	Provides configuration data parsed from system files using the Augeas tool.

authenticode	Displays information about Windows Authenticode signatures for executables.
authorization_mechanisms	Lists available macOS authorization mechanisms, which manage user authentication.
authorizations	Displays macOS system authorizations, detailing what users are allowed to perform certain actions.
authorized_keys	Shows SSH public keys that are authorized for user login.
autoexec	Displays the contents of the Windows autoexec.bat file, which configures environment variables at boot.
azure_instance_metadata	Provides metadata for instances running in Microsoft Azure, such as instance IDs and region information.
azure_instance_tags	Lists tags associated with an Azure instance for easy identification and management.
background_activities_moderator	Displays information about background tasks managed by the Background Activities Moderator (BAM) on Windows.
battery	Displays information about the system's battery, such as charge level and status.
bitlocker_info	Provides details about BitLocker encryption status and configuration on Windows systems.
block_devices	Lists all block storage devices connected to the system, including hard drives and USB drives.
bpf_process_events	Logs events related to processes monitored using BPF (Berkeley Packet Filter) on Linux systems.
bpf_socket_events	Shows socket events monitored using BPF, such as network connection activity.
browser_plugins	Displays a list of installed browser plugins across different browsers.
carbon_black_info	Provides information from the Carbon Black endpoint security agent, such as version and configuration details.
carves	Lists files carved from the system using osquery's file carving capabilities.
certificates	Displays information about installed security certificates, including their validity and issuer.

chassis_info	Provides details about the system's physical chassis, such as type and manufacturer.
chocolatey_packages	Lists software packages installed using the Chocolatey package manager on Windows.
chrome_extension_content_scripts	Displays content scripts registered by Chrome extensions, which have access to modify websites.
chrome_extensions	Lists all installed extensions in the Chrome browser.
connectivity	Displays the system's network connectivity status, including DNS and internet access checks.
cpu_info	Provides detailed information about the CPU, including model, speed, and the number of cores.
cpu_time	Shows how much CPU time has been used by different tasks on the system.
cpuid	Displays raw CPUID (CPU identification) information to gather detailed hardware details.
crashes	Logs application or system crashes, providing details on what caused the crash.
crontab	Lists scheduled tasks (cron jobs) set to run at specific times on Unix-based systems.
cups_destinations	Lists the available printers configured through the CUPS (Common UNIX Printing System) print server.
cups_jobs	Displays print jobs sent to printers managed by CUPS, including job status and user information.
curl	Displays recent HTTP requests made using the curl command, useful for tracking network activity.
curl_certificate	Shows details about SSL/TLS certificates used in curl HTTP requests.
deb_packages	Lists installed DEB packages on Debian-based systems, including version and installation source.
default_environment	Displays default environment variables set for users when they log in.
device_file	Provides information about device files, which are interfaces to hardware devices.

device_firmware	Shows firmware version information for hardware devices on the system.
device_hash	Displays cryptographic hash information for storage devices, useful for verifying integrity.
device_partitions	Lists partitions on the system’s storage devices, showing how storage is divided and formatted.
disk_encryption	Shows details about disk encryption, such as which drives are encrypted and the encryption methods used.
disk_events	Logs events related to storage devices, such as mounting or unmounting a disk.
disk_info	Provides detailed information about the system’s storage devices, including capacity and health status.
dns_cache	Displays cached DNS records on the system, including resolved domain names.
dns_resolvers	Lists DNS servers the system uses to resolve domain names.
docker_container_envs	Shows environment variables for running Docker containers.
docker_container_fs_changes	Lists changes made to the filesystem of running Docker containers.
docker_container_labels	Displays labels applied to Docker containers for organization and management.
docker_container_mounts	Shows file system mounts in Docker containers, including volumes and bind mounts.
docker_container_networks	Displays network information for Docker containers, such as connected networks and IP addresses.
docker_container_ports	Lists the ports Docker containers expose and forward to the host.
docker_container_processes	Displays running processes within Docker containers, showing their PID and command.
docker_container_stats	Provides resource usage statistics for Docker containers, including CPU and memory usage.
docker_containers	Lists all running and stopped Docker containers, including their state and configuration.
docker_image_history	Displays the history of changes made to Docker images, including layers and commands.

docker_image_labels	Shows labels applied to Docker images for categorization and management.
docker_image_layers	Displays the layers that make up a Docker image, showing changes made to the image over time.
docker_images	Lists Docker images present on the system, including image IDs and sizes.
docker_info	Provides detailed information about the Docker installation, such as version, storage drivers, and containers.
docker_network_labels	Displays labels applied to Docker networks for management purposes.
docker_networks	Lists Docker networks, showing connected containers and network settings.
docker_version	Displays the version of Docker running on the system, including API version and build details.
docker_volume_labels	Shows labels applied to Docker volumes for better organization.
docker_volumes	Lists Docker volumes, showing where they are mounted and their size.
drivers	Lists all installed drivers on the system, including device drivers and their version information.
ec2_instance_metadata	Provides metadata for instances running in AWS EC2, such as instance IDs, region, and instance type.
ec2_instance_tags	Lists tags associated with AWS EC2 instances, which help in managing and identifying resources.
es_process_events	Logs process creation and termination events on macOS systems with Endpoint Security (ES) enabled.
es_process_file_events	Displays file operations (create, read, write) tied to processes on macOS with Endpoint Security enabled.
etc_hosts	Shows entries from the /etc/hosts file, which maps IP addresses to hostnames.
etc_protocols	Displays protocols defined in the /etc/protocols file, listing network protocol numbers and names.
etc_services	Lists services defined in the /etc/services file, showing common ports and services.
event_taps	Provides information about macOS Event Taps, which allow applications to capture and modify input events.

extended_attributes	Displays extended file attributes, which store metadata such as tags and security labels on macOS.
fan_speed_sensors	Lists the current speed of the system's fans, helping monitor hardware temperature.
file	Provides detailed information about files, such as size, path, and permissions.
file_events	Logs changes to files, such as creation, modification, or deletion.
firefox_addons	Lists installed Firefox browser extensions (addons) and their details.
gatekeeper	Displays the configuration of macOS Gatekeeper, which controls which apps can be installed and run.
gatekeeper_approved_apps	Lists apps that are approved to run by macOS Gatekeeper.
groups	Displays all user groups on the system, showing which users belong to each group.
hardware_events	Logs hardware-related events, such as hardware failures or status changes.
hash	Calculates file hashes (MD5, SHA1, SHA256) to verify file integrity.
homebrew_packages	Lists installed software packages using the Homebrew package manager on macOS.
hvci_status	Shows the status of Hypervisor-Enforced Code Integrity (HVCI) on Windows systems for added security.
ibridge_info	Displays information about the iBridge chip on macOS, which helps manage security features.
ie_extensions	Lists installed Internet Explorer extensions on Windows.
intel_me_info	Provides details about the Intel Management Engine (ME), which allows for remote management of the system.
interface_addresses	Displays the IP addresses assigned to each network interface on the system.
interface_details	Shows detailed information about each network interface, such as status and speed.
interface_ipv6	Lists IPv6 addresses assigned to network interfaces.

iokit_devicetree	Displays the I/O Kit device tree on macOS, which lists hardware devices connected to the system.
iokit_registry	Shows a detailed registry of hardware devices and drivers using macOS's I/O Kit.
iptables	Lists the firewall rules configured using iptables on Linux systems.
kernel_extensions	Displays kernel extensions (drivers) loaded on the system.
kernel_info	Provides detailed information about the system’s kernel, such as version and architecture.
kernel_modules	Lists kernel modules (drivers) loaded into the system kernel on Linux.
kernel_panics	Displays information about kernel panics (system crashes) on macOS.
keychain_acls	Shows access control lists (ACLs) for macOS Keychain items, determining which users and apps can access them.
keychain_items	Lists items stored in the macOS Keychain, such as passwords and certificates.
known_hosts	Displays known SSH hosts from the ~/.ssh/known_hosts file.
kva_speculative_info	Provides information about Kernel Virtual Address (KVA) speculative execution mitigation on the system.
last	Displays the login history of users, showing when users last logged in and logged out.
launchd	Lists services and tasks managed by launchd on macOS, which handles system startup and task scheduling.
launchd_overrides	Shows any user overrides for launchd services, such as enabling or disabling services.
listening_ports	Displays the network ports currently open and listening for connections.
load_average	Shows the system’s average CPU load over the past 1, 5, and 15 minutes.
location_services	Displays the status of macOS location services and which apps have access.
logged_in_users	Lists users currently logged into the system, along with their login methods and times.

logical_drives	Displays logical drives (virtualized storage devices) on Windows systems.
logon_sessions	Provides details about user logon sessions on Windows, including session IDs and times.
lxd_certificates	Lists the certificates used by LXD containers for secure communication.
lxd_cluster	Shows details of the LXD cluster, if the system is part of one, including the cluster name and nodes.
lxd_cluster_members	Lists the members of the LXD cluster, including their roles and statuses.
lxd_images	Displays the available LXD images on the system, including their IDs and descriptions.
lxd_instance_config	Shows the configuration of LXD container instances on the system.
lxd_instance_devices	Lists the devices attached to LXD container instances.
lxd_instances	Displays information about LXD containers, including status and resource usage.
lxd_networks	Shows details of the networks used by LXD containers.
lxd_storage_pools	Lists storage pools available to LXD containers, including their configurations and statuses.
magic	Displays the MIME type and content type of a file using libmagic to identify file types.
managed_policies	Displays the policies applied to the system, such as security or configuration management policies.
md_devices	Lists the software RAID (Redundant Array of Independent Disks) devices managed by mdadm on Linux.
md_drives	Shows the drives that are part of a RAID array managed by mdadm on Linux.
md_personalities	Displays the available RAID configurations (personalities) supported by mdadm on Linux systems.
mdfind	Uses macOS's mdfind command to search for files indexed by Spotlight.
mdls	Displays metadata for files as indexed by macOS's Spotlight.

memory_array_mapped_addresses	Shows the mapped memory addresses for physical memory arrays.
memory_arrays	Provides information about the physical memory arrays on the system.
memory_device_mapped_addresses	Displays the memory addresses mapped to individual memory devices (RAM).
memory_devices	Lists details about the memory devices (RAM), such as capacity and manufacturer.
memory_error_info	Provides information about memory errors detected on the system.
memory_info	Displays the total and available memory (RAM) on the system.
memory_map	Shows a map of the memory layout, including reserved areas and available space.
mounts	Lists all mounted file systems and their mount points on the system.
msr	Provides access to Model-Specific Registers (MSRs), which contain low-level CPU information.
nfs_shares	Lists the NFS (Network File System) shares that are configured on the system.
npm_packages	Displays Node.js packages installed via the npm package manager.
ntdomains	Shows information about Windows NT domains that the system is part of.
ntfs_acl_permissions	Lists the Access Control List (ACL) permissions for files on NTFS file systems.
ntfs_journal_events	Logs file events recorded by the NTFS journal, such as file creation and modification.
nvram	Displays Non-Volatile Random Access Memory (NVRAM) settings on macOS, which store persistent system settings.
oem_strings	Provides OEM (Original Equipment Manufacturer) specific information from the system BIOS.

office_mru	Lists the most recently used (MRU) documents in Microsoft Office applications.
os_version	Displays the operating system version and related details like build number and platform type.
osquery_events	Logs events generated by osquery, such as file access, process activity, and network connections.
osquery_extensions	Shows the extensions currently loaded in osquery, which add new functionality.
osquery_flags	Lists the configuration flags that control how osquery operates.
osquery_info	Displays basic information about the osquery instance, including its version and PID.
osquery_packs	Lists the query packs loaded in osquery, which group sets of queries for specific purposes.
osquery_registry	Displays registry information for osquery, such as registered extensions and packs.
osquery_schedule	Shows the scheduled queries configured in osquery, along with their intervals and statuses.
package_bom	Lists the bill of materials (BOM) for installed packages, detailing their contents.
package_install_history	Displays the history of installed packages on the system, including installation dates and sources.
package_receipts	Shows installed package receipts on macOS, detailing the files installed by each package.
password_policy	Lists the password policies applied on the system, including password strength and expiration rules.
patches	Displays information about patches applied to the system.
pci_devices	Lists PCI (Peripheral Component Interconnect) devices connected to the system, such as network and graphics cards.
physical_disk_performance	Provides performance statistics for physical disks, such as read/write speeds.
pipes	Lists the named pipes (a method for inter-process communication) on Windows systems.

platform_info	Displays platform-specific details about the system, such as architecture and vendor.
plist	Reads values from macOS property list (plist) files, which store settings and configurations.
portage_keywords	Shows package keywords used by the Portage package management system on Gentoo-based systems.
portage_packages	Lists installed packages managed by Portage on Gentoo-based Linux systems.
portage_use	Displays USE flags for packages installed via Portage, which determine optional features in Gentoo systems.
power_sensors	Shows power sensor readings, such as voltage and wattage, from various system components.
powershell_events	Logs events generated by PowerShell scripts on Windows systems.
preferences	Lists user and system preferences, such as settings for applications and system services.
prefetch	Displays information about files and applications recently accessed by Windows Prefetch, helping with performance optimization.
process_envs	Displays the environment variables associated with running processes.
process_events	Logs process creation and termination events on the system.
process_file_events	Monitors file access events tied to specific processes.
process_memory_map	Shows the memory map of running processes, detailing how memory is allocated.
process_namespaces	Lists the Linux namespaces used by running processes.
process_open_files	Displays the files that are currently opened by running processes.
process_open_pipes	Lists the pipes (for inter-process communication) opened by processes.
process_open_sockets	Shows network sockets currently opened by running processes.

processes	Provides details of all running processes, including their CPU and memory usage.
programs	Lists installed programs on Windows, similar to what you see in "Add/Remove Programs".
prometheus_metrics	Displays metrics exposed by Prometheus endpoints for system monitoring.
python_packages	Shows Python packages installed on the system via pip.
quicklook_cache	Displays cached files used by macOS QuickLook to generate previews.
registry	Shows key-value pairs from the Windows registry, which stores configuration settings.
routes	Lists the system's network routing table, which shows how data is routed between networks.
rpm_package_files	Displays the files installed as part of RPM packages on the system.
rpm_packages	Lists installed RPM packages on systems using the RPM package manager (like Fedora, CentOS).
running_apps	Shows currently running applications on macOS.
safari_extensions	Lists installed Safari browser extensions.
sandboxes	Displays details of sandboxed applications and their restrictions.
scheduled_tasks	Lists tasks set to run at scheduled times on Windows systems.
screenlock	Displays the configuration of the screen lock settings on macOS.
seccomp_events	Logs security-related events using Seccomp (Secure Computing Mode) on Linux.
secureboot	Shows the system's Secure Boot configuration, used to ensure boot-time security.
selinux_events	Logs events generated by SELinux, a security module for Linux.
selinux_settings	Displays the active SELinux policies and settings.

services	Lists system services, showing which are enabled or running.
shadow	Displays user password hashes and expiration details on Unix-based systems.
shared_folders	Shows folders that are shared over the network, such as on Windows or macOS.
shared_memory	Displays information about shared memory segments used for inter-process communication.
shared_resources	Lists network resources (e.g., printers, folders) that are shared on the system.
sharing_preferences	Displays macOS sharing preferences, such as file or screen sharing settings.
shell_history	Shows the shell command history for users, such as commands executed in bash or zsh.
shellbags	Displays information from Windows ShellBags, which track folder views and preferences.
shimcache	Shows entries from the Application Compatibility Shim Cache, which logs executed applications on Windows.
signature	Displays details of digital signatures for files and software on the system.
sip_config	Shows the System Integrity Protection (SIP) configuration on macOS, which restricts root-level modifications.
smbios_tables	Provides hardware information from the system's SMBIOS (System Management BIOS) tables.
smc_keys	Displays macOS System Management Controller (SMC) key values, which manage low-level system functions.
socket_events	Logs network socket activity, such as connections and disconnections.
ssh_configs	Shows the configuration details of SSH clients on the system.
startup_items	Lists applications and services set to start automatically when the system boots.
sudoers	Displays the users and their privileges for running commands as root via sudo.
suid_bin	Lists files that have the setuid bit set, allowing users to run them with elevated privileges.

syslog_events	Shows system log events from the syslog service, including errors and warnings.
system_controls	Lists system control parameters (sysctl) used to configure kernel behavior.
system_extensions	Displays the loaded system extensions on macOS, which extend the system's functionality.
system_info	Provides basic system information, such as hardware model, hostname, and operating system.
systemd_units	Lists services and units managed by systemd on Linux systems.
temperature_sensors	Displays temperature readings from various hardware components like CPU and GPU.
time	Displays the current system time and related time zone information.
time_machine_backups	Shows details about macOS Time Machine backups, such as the backup date and size.
time_machine_destinations	Lists the backup destinations used by Time Machine on macOS.
tpm_info	Provides details about the Trusted Platform Module (TPM) used for hardware-based security.
ulimit_info	Displays user limit settings (ulimit), which restrict resource usage for processes.
unified_log	Shows logs from Apple's Unified Logging system on macOS.
uptime	Displays how long the system has been running since the last boot.
usb_devices	Lists USB devices connected to the system, including details like manufacturer and product IDs.
user_events	Logs user account activity such as logins and logouts.
user_groups	Shows which users belong to which groups on the system.
user_interaction_events	Logs user interactions like mouse clicks and key presses (macOS).
user_ssh_keys	Lists the SSH keys associated with user accounts on the system.

userassist	Displays Windows UserAssist entries, which track user activity and recently accessed files.
users	Lists all user accounts on the system, including user IDs and home directories.
video_info	Provides details about the video devices (e.g., GPUs) on the system, such as model and memory.
virtual_memory_info	Shows information about the system's virtual memory, including swap usage and paging activity.
wifi_networks	Lists nearby Wi-Fi networks, displaying information such as SSID, signal strength, and security type.
wifi_status	Displays the current status of the system's Wi-Fi connection, including SSID and signal strength.
wifi_survey	Provides detailed information about nearby Wi-Fi networks, including signal quality and noise levels.
winbaseobj	Lists base objects in Windows, such as named pipes and events.
windows_crashes	Displays details about application or system crashes on Windows.
windows_eventlog	Shows events from the Windows Event Log, which records system, security, and application events.
windows_events	Provides logs of significant events on Windows, including security and operational events.
windows_firewall_rules	Lists the firewall rules configured in the Windows Firewall, including allowed and blocked connections.
windows_optional_features	Displays optional features installed or available for installation on Windows systems.
windows_security_center	Shows the security status of the system as reported by Windows Security Center.
windows_security_products	Lists security products like antivirus and firewall software installed on Windows.
windows_update_history	Displays the history of Windows updates installed on the system.
wmi_bios_info	Provides information about the system's BIOS through Windows Management Instrumentation (WMI).
wmi_cli_event_consumers	Lists WMI (Windows Management Instrumentation) CLI event consumers, which are triggered by event filters.

wmi_event_filters	Displays WMI event filters that define the events monitored in Windows.
wmi_filter_consumer_binding	Shows the bindings between WMI filters and consumers, linking event filters to the actions they trigger.
wmi_script_event_consumers	Lists WMI script event consumers that execute scripts when specific events occur.
xprotect_entries	Displays the rules enforced by macOS XProtect, Apple's built-in anti-malware system.
xprotect_meta	Shows metadata related to XProtect definitions and updates.
xprotect_reports	Lists reports generated by macOS XProtect when malware is detected.
yara	Runs YARA rules on the system to detect files based on pattern matching for security purposes.
yara_events	Logs events triggered by YARA rule matches on the system.
ycloud_instance_metadata	Displays metadata for instances running in Yandex Cloud, similar to AWS and Azure instance metadata.
yum_sources	Lists repository sources for the YUM package manager on Linux systems.