Docker Engine / Security / Seccomp security profiles

Seccomp security profiles for Docker

Secure computing mode (seccomp) is a Linux kernel feature. You can use it to restrict the actions available within the container. The seccomp() system call operates on the seccomp state of the calling process. You can use this feature to restrict your application's access.

This feature is available only if Docker has been built with secomp and the kernel is configured with CONFIG_SECCOMP enabled. To check if your kernel supports | seccomp :

```
$ grep CONFIG_SECCOMP= /boot/config-$(uname -r)
CONFIG_SECCOMP=y
```

Pass a profile for a container

The default secomp profile provides a sane default for running containers with seccomp and disables around 44 system calls out of 300+. It is moderately protective while providing wide application compatibility. The default Docker profile can be found here .

In effect, the profile is an allowlist which denies access to system calls by default, then allowlists specific system calls. The profile works by defining a defaultAction of SCMP_ACT_ERRNO and overriding that action only for specific system calls. The effect of SCMP_ACT_ERRNO is to cause a Permission Denied error. Next, the profile defines a specific list of system calls which are fully allowed, because their action is overridden to be SCMP_ACT_ALLOW. Finally, some specific rules are for individual system calls such as personality, and others, to allow variants of those system calls with specific arguments.

seccomp is instrumental for running Docker containers with least privilege. It is not recommended to change the default seccomp profile.

When you run a container, it uses the default profile unless you override it with the --security-opt option. For example, the following explicitly specifies a policy:

```
$ docker run --rm \
             --security-opt seccomp=/path/to/seccomp/profile.json \
             hello-world
```

Significant syscalls blocked by the default profile

Docker's default seccomp profile is an allowlist which specifies the calls that are allowed. The table below lists the significant (but not all) syscalls that are effectively blocked because they are not on the Allowlist. The table includes the reason each syscall is blocked rather than white-listed.

Syscall	Description		
acct	Accounting syscall which could let containers disable their own resource limits or process accounting. Also gated by CAP_SYS_PACCT.		
add_key	Prevent containers from using the kernel keyring, which is not namespaced.		
bpf	Deny loading potentially persistent bpf programs into kernel, already gated by CAP_SYS_ADMIN.		
clock_adjtime	Time/date is not namespaced. Also gated by CAP_SYS_TIME.		
ock_settime	Time/date is not namespaced. Also gated by CAP_SYS_TIME.		

create would. Deep coloning new namespaces. Also gated by CAP_SYS_AMPIN for CLONE_* figg, except CLONE_NEWBER, in create would. Deep manipulation and functions on kernel modules. Also gated by CAP_SYS_MIGURE. Final_residate Deep manipulation and functions on kernel modules. Also gated by CAP_SYS_MIGURE. Final_residate Deep manipulation and functions on kernel modules. Also gated by CAP_SYS_MIGURE. Deep manipulation and functions on kernel modules. Also gated by CAP_SYS_MIGURE. Tritt_module Deep manipulation and functions on kernel modules. Also gated by CAP_SYS_MIGURE. Tritt_module Deep manipulation and functions on kernel modules. Also gated by CAP_SYS_MIGURE. Tritt_module Deep manipulation and functions on kernel modules. Also gated by CAP_SYS_MIGURE. Tritt_module Deep manipulation and functions on kernel modules. Also gated by CAP_SYS_MIGURE. Tritt_module Deep manipulation and functions on kernel modules. Also gated by CAP_SYS_MIGURE. Tritt_module Deep manipulation and functions on kernel modules. Also gated by CAP_SYS_MIGURE. Tritt_module Deep modules from modifying kernel I/O privilege levels. Already gated by CAP_SYS_MIGURE. Tritt_module Stated process inspection capabilities, shready blocked by dropping CAP_SYS_MIGURE. Tritt_module Deep loading a new kernel for later execution. Also gated by CAP_SYS_MIGURE. Tritt_module Deep loading a new kernel for later execution. Also gated by CAP_SYS_MIGURE. Tritt_module Deep moduling already gated by CAP_SYS_MIGURE. Tritt_moduling already gated by CAP_SYS_MIGURE. Tritt_moduling already gated by CAP_SYS_MIGURE. Deep moduling already gated by CAP_SYS_MIGURE. Process via ready Resided process inspection capabilities, already blocked by dropping CAP_SYS_PYS_MIGURE. Deep moduling already gated by CAP_SYS_MIGURE. Dee	Syscall	Description
delive_webuild Deny manipulation and functions on kernel modules. Also gated by CAP_SYS_MOULE. finit_nebuile Deny manipulation and functions on kernel modules. Also gated by CAP_SYS_MOULE. get_kernel_syms Deny retrieval of exported kernel and module symbols. Obsolete. got_nempolity Syscall that modules kernel memory and NIAMA settings. Already gated by CAP_SYS_MOULE. Intit nebule Deny manipulation and functions on kernel modules. Also gated by CAP_SYS_MOULE. Prevent containings from modifying kernel I/O privilege levels. Already gated by CAP_SYS_MANIO. Total Prevent containings from modifying kernel I/O privilege levels. Already gated by CAP_SYS_MANIO. Retrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. Respective of the symbol of the same thing, slightly different arguments. Also gated by CAP_SYS_MANIO. Respective of the same thing, slightly different arguments. Also gated by CAP_SYS_MODI. Respective or containing from using the kernel keyring, which is not namespaced. Dowkup_secolial Tracing/profiling syscall, which could leak a lot of information on the host. Also gated by CAP_SYS_ARKEN. Build Syscall that modifies kernel memory and NUMA settings. Already gated by CAP_SYS_ARKEN. Build Deny mounting, already gated by CAP_SYS_ARKEN. Deny interaction with the kernel risk deemon. Obsolete since Linux 3.1. perior by hankle_sis. Cause of an old container breakout. Also gated by CAP_DCR_CAP_SYARCE. Prevent_ceen. Tracing/profiling syscall, which could leak a lot of information on the host. Prevent container from enabling BSD candiation. Not inhorently dangerous, but proofly tested, potential for a lot of kernel wints. Prevent container from enabling BSD candiation. Not inhorently dangerous, but proofly tested, potential for a lot of kernel wints. Prevent posters inspection capabilities, already blocked by dropping CAP_SYS_PIRACE. Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PIRACE. Prevent containers reboot the host. Al	clone	Deny cloning new namespaces. Also gated by CAP_SYS_ADMIN for CLONE_* flags, except CLONE_NEWUSER.
first_module Deny manipulation and functions on kernel modules. Also gated by [CAP_SYS_MODU F] get_kernel_systs. Deny retrieval of exported kernel and module symbols. Obsolete. get_mempolasy Syscall that modifies kernel memory and NUMA settings. Already gated by _CAP_SYS_NICC. Litat module Deny manipulation and functions on kernel modules. Also gated by _CAP_SYS_NICC. Loveris. Prevent containers from modifying kernel I/O privilege levels. Already gated by _CAP_SYS_RAND. Total Prevent containers from modifying kernel I/O privilege levels. Already gated by _CAP_SYS_RAND. Keeper Restrict process inspection capabilities, already blocked by dropping _CAP_SYS_RAND. Keeper Lital_load Stater syscall of _kexsc_loads that does the same thing, slightly different arguments. Also gated by _CAP_SYS_ROOT _ Keeper Lital_load Deny loading a new kernel for later execution. Also gated by _CAP_SYS_ROOT _ Keeper Lital_load Deny loading a new kernel for later execution. Also gated by _CAP_SYS_ROOT _ Keeper Lital_load Deny loading a new kernel for later execution. Also gated by _CAP_SYS_ROOT _ Keeper Lital_load Deny loading a new kernel for later execution. Also gated by _CAP_SYS_ROOT _ Keeper Lital_load Deny loading a new kernel for later execution. Also gated by _CAP_SYS_ROOT _ Keeper Lital_load Deny loading a new kernel for later execution. Also gated by _CAP_SYS_ROOT _ Keeper Lital_load Deny loading a new kernel for later execution. Also gated by _CAP_SYS_ROOT _ Bootal_ Syscall that modifies kernel memory and NUMA settings. Record	create_module	Deny manipulation and functions on kernel modules. Obsolete. Also gated by CAP_SYS_MODULE.
Derry retrieval of exported kernel and module symbols. Obsolete. get_nampolisy Syscall that modifies kernel memory and NUMA settings. Already gated by CAP_SYS_NOBILIF. Dery manipulation and functions on kernel modules. Also gated by CAP_SYS_NOBILIF. Prevent containers from modifying kernel I/O privilege levels. Already gated by CAP_SYS_RANZO. Dery loading a new kernel from privilege levels. Already gated by CAP_SYS_RANZO. Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PERACE. Responsible of kexec_load that does the same thing, slightly different arguments. Also gated by CAP_SYS_RANZO. Deny loading a new kernel for later execution. Also gated by CAP_SYS_BOOT. Responsible of the same thing, slightly different arguments. Also gated by CAP_SYS_RANZO. Prevent containers from using the kernel keyring, which is not namespaced. Tracing/profiling syscall, which could leak a lot of information on the host. Also gated by CAP_SYS_RANZO. Deny mounting, already gated by CAP_SYS_RANZO. Deny mounting, already gated by CAP_SYS_RANZO. Syscall that modifies kernel memory and NUMA settings. Tracing/profiling already gated by CAP_SYS_RANZO. Deny interaction with the kernel field domain. Obsolete since Linux 3.1. Deny interaction with the kernel field domain. Obsolete since Linux 3.1. Deny interaction with the kernel field domain. Not inherently dangerous, but poorly tested, potential for a lot of kernel value. process_valu_residy Prevent container from enabling ISD emulation. Not inherently dangerous, but poorly tested, potential for a lot of kernel value. process_valu_residy Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. process_valu_residy Tracing/profiling syscall, which could leak a lot of information on the host. Process_valu_residy Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. Tracing/profiling syscall, which could leak a lot of information on the host. Process_valu_residy Restrict process	delete_module	Deny manipulation and functions on kernel modules. Also gated by CAP_SYS_MODULE.
pet_memobility Syscall that modifies komel memory and NUMA settings. Already gated by CAP_SYS_NICE. Initi_modules Deny manipulation and functions on kernel modules. Also gated by CAP_SYS_POULE. Loperin Prevent containers from modifying kernel I/O privilege levels. Already gated by CAP_SYS_RANTO. 1001 Prevent containers from modifying kernel I/O privilege levels. Already gated by CAP_SYS_RANTO. Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PIRACE. Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PIRACE. Deny loading a new kernel for later execution. Also gated by CAP_SYS_BOOT. Revert1 Prevent containers from using the kernel keyring, which is not namespaced. Tracing/profiling syscall, which could leak a lot of information on the host. Also gated by CAP_SYS_ADMIN. Insure Deny mounting, already gated by CAP_SYS_ADMIN. Deny mounting, already gated by CAP_SYS_ADMIN. Deny interaction with the kernel infa deemon Obsolete since Linux 3.1. Deny interaction with the kernel infa deemon Obsolete since Linux 3.1. Cause of an old container breakout. Also gated by CAP_SYS_ADMIN. per_Levent_open Tracing/profiling syscall, which could leak a lot of information on the host. personality Prevent container from enabling BSD enulation. Not inherently dangerous, but poorly tested, potential for a lot of kernel vulns. process_we_ready Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. Praces Tracing/profiling syscall blocked in Linux kernel versions before 4.8 to avoid second paysas. Tracing/profiling arbitrary processes is already blocked by dropping CAP_SYS_PTRACE. Deny payst_read_ Book blocked by dropping CAP_SYS_PTRACE. Deny spocal which could let containers disable their own resource limits or process accounting. Also gated by CAP_SYS_RONT. Quota syscall which could let containers disable their own resource limits or process accounting. Also gated by CAP_SYS_RONT. Prevent containers from using the kemel ke	finit_module	Deny manipulation and functions on kernel modules. Also gated by CAP_SYS_MODULE.
init_module	get_kernel_syms	Deny retrieval of exported kernel and module symbols. Obsolete.
Prevent containers from modifying kernel I/O privilege levels. Already gated by CAP_SYS_RANTO. Prevent containers from modifying kernel I/O privilege levels. Already gated by CAP_SYS_RANTO. Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PARCE. Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PARCE. Reves_Insul Deny loading a new kernel for later execution. Also gated by CAP_SYS_ROOT. Revest 1 Prevent containers from using the kernel keyring, which is not namespaced. Tracing/profiling syscall, which could leak a lot of information on the host. Also gated by CAP_SYS_NTCF. Bunust 1 Deny mounting, already gated by CAP_SYS_ADRITY. Deny mounting, already gated by CAP_SYS_ADRITY. Deny mounting, already gated by CAP_SYS_ADRITY. Deny interaction with the kernel infs daemon. Obsolete since Linux 3.1. Open_by_handle_a1 Cause of an old container breakout. Also gated by CAP_CALREAQ_SEARCH . Perf_event_open 1 Tracing/profiling syscall, which could leak a lot of information on the host. Personality Prevent container from enabling BSD emulation. Not inherently dangerous, but poorly tested, potential for a lot of kernel vulns. Process_Vm_ready 1 Deny [pivot_root] should be privileged aperation. Process_Vm_ready 1 Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. Prace 1 Tracing/profiling syscall. Blocked in Linux kernel versions before 4.8 to avoid seccomp bypass. Tracing/profiling arbitrary processes is already blocked by dropping CAP_SYS_PTRACE. Prace 1 Tracing/profiling syscall. Blocked in Linux kernel versions before 4.8 to avoid seccomp bypass. Tracing/profiling arbitrary processes is already blocked by dropping CAP_SYS_PTRACE. Prace 1 Tracing/profiling syscall which could let containers disable their own resource limits or process accounting. Also gated by CAP_SYS_ADMT I. Process 2 Tracing/profiling arbitrary processes is already blocked by United Sys_Second I. Provent containers from using the ker	get_mempolicy	Syscall that modifies kernel memory and NUMA settings. Already gated by CAP_SYS_NICE.
Restrict process inspection capabilities, already blocked by dropping CAP SYS_SANTO. Restrict process inspection capabilities, already blocked by dropping CAP SYS_PTRACE. Revec_fize_load Sister syscall of kexec_load that does the same thing, slightly different arguments. Also gated by CAP_SYS_BOOT. Revect_1 Prevent containers from using the kernel keyring, which is not namespaced. 3ookup doookie	init_module	Deny manipulation and functions on kernel modules. Also gated by CAP_SYS_MODULE.
Restrict process inspection capabilities, already blocked by dropping. CAP_SYS_PTRACE. kexec_file_load. Sister syscall of kexec_load that does the same thing, slightly different arguments. Also gated by CAP_SYS_BOOT. kexec_load. Deny loading a new kernel for later execution. Also gated by CAP_SYS_BOOT. keyot1	ioperm	Prevent containers from modifying kernel I/O privilege levels. Already gated by CAP_SYS_RAWIO.
kexec_file_load Sister syscall of kexec_load that does the same thing, slightly different arguments. Also gated by CAP_SYS_BOOT kexec_load Deny loading a new kernel for later execution. Also gated by CAP_SYS_BOOT keyct Prevent containers from using the kernel keyring, which is not namespaced. Tracing/profiling syscall, which could leak a lot of information on the host. Also gated by CAP_SYS_ADMIN move_pages Syscall that modifies kernel memory and NUMA settings. Already gated by CAP_SYS_NICE mount Deny mounting, already gated by CAP_SYS_ADMIN move_pages Syscall that modifies kernel memory and NUMA settings. Infaservet1 Deny interaction with the kernel fis daemon. Obsolete since Linux 3.1. upon_by_handle_st Cause of an old container breakout. Also gated by CAP_DAC_READ_SEARCH perf_event_open Tracing/profiling syscall, which could leak a lot of information on the host. personality Prevent container from enabling BSD emulation. Not inherently dangerous, but poorly tested, potential for a lot of kernel vulns. pivot_root Deny pivot_root should be privileged operation. process_ven_readv Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE praces Tracing/profiling syscall. Blocked in Linux kernel versions before 4.8 to avoid seccomp bypass. Tracing/profiling arbitrary processes is already blocked by dropping CAP_SYS_PTRACE prace Tracing/profiling syscall. Blocked in Linux kernel versions before 4.8 to avoid seccomp bypass. Tracing/profiling arbitrary processes is already blocked by dropping CAP_SYS_PTRACE because it could leak a lot of information on the host. query_module Deny manipulation and functions on kernel modules. Obsolete. quotact1 Quota syscall which could let containers disable their own resource limits or process accounting. Also gated by CAP_SYS_BOOT. request_key Prevent containers from using the kernel keyring, which is not namespaced. set_mempolicy Syscall that modifies kernel memory and NUMA settings.	iopl	Prevent containers from modifying kernel I/O privilege levels. Already gated by CAP_SYS_RAWIO.
keyec1 Deny loading a new kernel for later execution. Also gated by CAP_SYS_BOOT . keyec1 Prevent containers from using the kernel keyring, which is not namespaced. Tracing/profiling syscall, which could leak a lot of information on the host. Also gated by CAP_SYS_ADMIN . Beny mounting, already gated by CAP_SYS_ADMIN . Beny interaction with the kernel nis daemon. Obsolete since Linux 3.1. Deny interaction with the kernel nis daemon. Obsolete since Linux 3.1. Deny interaction with the kernel nis daemon. Obsolete since Linux 3.1. Deny processor and obsolete since Linux 3.1. Tracing/profiling syscall, which could leak a lot of information on the host. Personality Prevent container from enabling BSD emulation. Not inherently dangerous, but poorly tested, potential for a lot of kernel vulns. Deny plvot_root ; should be privileged operation. Process_val_ready Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE . Prace Tracing/profiling syscall. Blocked in Linux kernel versions before 4.8 to avoid seccomp bypass. Tracing/profiling arbitrary processes is already blocked by dropping CAP_SYS_PTRACE . Personality Quota syscall which could let containers disable their own resource limits or process accounting. Also gated by CAP_SYS_PSACE . Prevent Containers reboot the host. Also gated by CAP_SYS_BOOT . Prequest_key Prevent containers from using the kernel keyring, which is not namespaced. Bettimeofday Time/date is not namespaced. Also gated by CAP_SYS_TIME . Time/date is not namespaced. Also gated by CAP_SYS_TIME .	kcmp	Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE.
Prevent containers from using the kernel keyring, which is not namespaced. Tracing/profiling syscall, which could leak a lot of information on the host. Also gated by CAP_SYS_ADMIN. mind Syscall that modifies kernel memory and NUMA settings. Already gated by CAP_SYS_NICE: meunt Deny mounting, already gated by CAP_SYS_ADMIN. move_pages Syscall that modifies kernel memory and NUMA settings. Inf servet1 Deny interaction with the kernel nfs daemon. Obsolete since Linux 3.1. open_by_handle_st Cause of an old container breakout. Also gated by CAP_DAC_BEAD_SEARCH. perf_event_open Tracing/profiling syscall, which could leak a lot of information on the host. personality Prevent container from enabling BSD emulation. Not inherently dangerous, but poorly tested, potential for a lot of kernel vulns. privot_root Deny pivot_root; should be privileged operation. process_vm_readv Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. pracess_vm_writev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. pracess_vm_writev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. prace Tracing/profiling syscall. Blocked in Linux kernel versions before 4.8 to avoid seccomp bypass. Tracing/profiling arbitrary processes is already blocked by dropping CAP_SYS_PTRACE, because it could leak a lot of information on the host. query_module Deny manipulation and functions on kernel modules. Obsolete. quotuct1 Quota syscall which could let containers disable their own resource limits or process accounting. Also gated by CAP_SYS_NONTN. repost Don't let containers from using the kernel keyring, which is not namespaced. set_mempolicy Syscall that modifies kernel memory and NUMA settings. Already gated by CAP_SYS_NITE. Time/date is not namespaced. Also gated by CAP_SYS_TIME.	kexec_file_load	Sister syscall of kexec_load that does the same thing, slightly different arguments. Also gated by CAP_SYS_BOOT.
Tracing/profiling syscall, which could leak a lot of information on the host. Also gated by CAP_SYS_ADMIN. mount Derry mounting, already gated by CAP_SYS_ADMIN. move_pages Syscall that modifies kernel memory and NUMA settings. nfsservct1 Deny interaction with the kernel nfs daemon. Obsolete since Linux 3.1. Cause of an old container breakout. Also gated by CAP_DAC_READ_SEARCH. perf_event_open Tracing/profiling syscall, which could leak a lot of information on the host. Prevent container from enabling BSD emulation. Not inherently dangerous, but poorly tested, potential for a lot of kernel vulns. pivot_root Deny pivot_root, should be privileged operation. Process_vm_ready Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. Prace Tracing/profiling syscall. Blocked in Linux kernel versions before 4.8 to avoid seccomp bypass. Tracing/profiling arbitrary processes is already blocked by dropping CAP_SYS_PTRACE. Query_module Deny manipulation and functions on kernel modules. Obsolete. Quotact1 Quate syscall which could let containers disable their own resource limits or process accounting. Also gated by CAP_SYS_ADMIN. reboot Don't let containers reboot the host. Also gated by CAP_SYS_BOOT. request_key Prevent containers from using the kernel keyring, which is not namespaced. set_mempolicy Syscall that modifies kernel memory and NUMA settings. Already gated by CAP_SYS_ADMIN. Time/date is not namespaced. Also gated by CAP_SYS_TIME. Time/date is not namespaced. Also gated by CAP_SYS_TIME.	kexec_load	Deny loading a new kernel for later execution. Also gated by CAP_SYS_BOOT.
mount Syscall that modifies kernel memory and NUMA settings. Already gated by CAP_SYS_NICE. mount Deny mounting, already gated by CAP_SYS_ABMIN. move_pages Syscall that modifies kernel memory and NUMA settings. nfsservet1 Deny interaction with the kernel nfs daemon. Obsolete since Linux 3.1. open_by_handle_st Cause of an old container breakout. Also gated by CAP_DAC_READ_SEARCH. perf_event_open Tracing/profiling syscall, which could leak a lot of information on the host. personality Prevent container from enabling BSD emulation. Not inherently dangerous, but poorly tested, potential for a lot of kernel vulns. pivot_root Deny pivot_root, should be privileged operation. process_vm_readv Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. process_vm_writev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. process_vm_writev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. process_vm_writev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. process_vm_writev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. process_vm_writev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. process_vm_writev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. process_vm_writev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. process_vm_writev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. process_vm_writev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_BODICE. Quota syscall which could let containers disable their own resource limits or process accounting. Also gated by CAP_SYS_BODICE. Quota syscall which could let containers disable their own resource limits or process accounting. Also gated by CAP_SYS_BODICE. Quota syscall which could let containers disable their	keyctl	Prevent containers from using the kernel keyring, which is not namespaced.
mount Deny mounting, already gated by CAP_SYS_ADMIN . move_pages Syscall that modifies kernel memory and NUMA settings. nfsservct1 Deny interaction with the kernel nfs daemon. Obsolete since Linux 3.1. open_by_handle_at Cause of an old container breakout. Also gated by CAP_DAC_READ_SEARCH . perf_event_open Tracing/profiling syscall, which could leak a lot of information on the host. personality Prevent container from enabling BSD emulation. Not inherently dangerous, but poorly tested, potential for a lot of kernel vulns. pivot_root Deny psvot_root , should be privileged operation. pracess_vm_readv Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE . pracess_vm_writev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE . pracess_vm_exritev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE . pracess_vm_exritev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE . pracess_vm_exritev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE . pracess_vm_exritev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE . pracess_vm_exritev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE . pracess_vm_exritev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE . pracess_vm_exritev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE . pracess_vm_exritev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE . pracess_vm_exritev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE . pracess_vm_exritev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE . pracess_vm_exritev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE . pracess_vm_exritev Restrict process inspection capabilities, al	lookup_dcookie	Tracing/profiling syscall, which could leak a lot of information on the host. Also gated by CAP_SYS_ADMIN.
move_pages Syscall that modifies kernel memory and NUMA settings. nfsservct1 Deny interaction with the kernel nfs daemon. Obsolete since Linux 3.1. qpen_by_handle_at Cause of an old container breakout. Also gated by CAP_DAC_READ_SEARCH. perf_event_open Tracing/profiling syscall, which could leak a lot of information on the host. personality Prevent container from enabling BSD emulation. Not inherently dangerous, but poorly tested, potential for a lot of kernel vulns. process_vm_readv Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. process_vm_writev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. process_vm_writev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. process_vm_writev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. process_vm_writev	mbind	Syscall that modifies kernel memory and NUMA settings. Already gated by CAP_SYS_NICE.
Deny interaction with the kernel nfs daemon. Obsolete since Linux 3.1. open_by_handle_at	mount	Deny mounting, already gated by CAP_SYS_ADMIN.
open_by_handle_at	move_pages	Syscall that modifies kernel memory and NUMA settings.
Prevent container from enabling BSD emulation. Not inherently dangerous, but poorly tested, potential for a lot of kernel vulns. Prevent container from enabling BSD emulation. Not inherently dangerous, but poorly tested, potential for a lot of kernel vulns. Pivot_root Deny pivot_root , should be privileged operation. Process_vm_readv Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE . Process_vm_writev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE . Ptrace Tracing/profiling syscall. Blocked in Linux kernel versions before 4.8 to avoid seccomp bypass. Tracing/profiling arbitrary processes is already blocked by dropping CAP_SYS_PTRACE , because it could leak a lot of information on the host. query_module Deny manipulation and functions on kernel modules. Obsolete. quotact1 Quota syscall which could let containers disable their own resource limits or process accounting. Also gated by CAP_SYS_ADMIN . reboot Don't let containers reboot the host. Also gated by CAP_SYS_BOOT . request_key Prevent containers from using the kernel keyring, which is not namespaced. set_mempolicy Syscall that modifies kernel memory and NUMA settings. Already gated by CAP_SYS_NICE . Beny associating a thread with a namespace. Also gated by CAP_SYS_ADMIN . settime Time/date is not namespaced. Also gated by CAP_SYS_TIME . Time/date is not namespaced. Also gated by CAP_SYS_TIME .	nfsservctl	Deny interaction with the kernel nfs daemon. Obsolete since Linux 3.1.
Prevent container from enabling BSD emulation. Not inherently dangerous, but poorly tested, potential for a lot of kernel vulns. process_vm_readv Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. Process_vm_writev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. Ptrace Tracing/profiling syscall. Blocked in Linux kernel versions before 4.8 to avoid seccomp bypass. Tracing/profiling arbitrary processes is already blocked by dropping CAP_SYS_PTRACE. Query_module Deny manipulation and functions on kernel modules. Obsolete. Quota syscall which could let containers disable their own resource limits or process accounting. Also gated by CAP_SYS_ADMIN. reduction Don't let containers reboot the host. Also gated by CAP_SYS_BOOT. request_key Prevent containers from using the kernel keyring, which is not namespaced. set_mempolicy Syscall that modifies kernel memory and NUMA settings. Already gated by CAP_SYS_NICE. Deny associating a thread with a namespace. Also gated by CAP_SYS_ADMIN. settime Time/date is not namespaced. Also gated by CAP_SYS_TIME. Time/date is not namespaced. Also gated by CAP_SYS_TIME.	open_by_handle_at	Cause of an old container breakout. Also gated by CAP_DAC_READ_SEARCH.
vulns. Deny pivot_root Deny pivot_root, should be privileged operation. Process_vm_readv Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. Process_vm_writev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. Ptrace Tracing/profiling syscall. Blocked in Linux kernel versions before 4.8 to avoid seccomp bypass. Tracing/profiling arbitrary processes is already blocked by dropping CAP_SYS_PTRACE, because it could leak a lot of information on the host. Query_module Deny manipulation and functions on kernel modules. Obsolete. Quota syscall which could let containers disable their own resource limits or process accounting. Also gated by CAP_SYS_ADMIN. reboot Don't let containers reboot the host. Also gated by CAP_SYS_BOOT. request_key Prevent containers from using the kernel keyring, which is not namespaced. set_mempolicy Syscall that modifies kernel memory and NUMA settings. Already gated by CAP_SYS_NICE. beny associating a thread with a namespace. Also gated by CAP_SYS_ADMIN. Time/date is not namespaced. Also gated by CAP_SYS_TIME. Time/date is not namespaced. Also gated by CAP_SYS_TIME.	perf_event_open	Tracing/profiling syscall, which could leak a lot of information on the host.
Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. Process_vm_writev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. Ptrace Tracing/profiling syscall. Blocked in Linux kernel versions before 4.8 to avoid seccomp bypass. Tracing/profiling arbitrary processes is already blocked by dropping CAP_SYS_PTRACE, because it could leak a lot of information on the host. Query_module Deny manipulation and functions on kernel modules. Obsolete. Quota syscall which could let containers disable their own resource limits or process accounting. Also gated by CAP_SYS_ADMIN. reboot Don't let containers reboot the host. Also gated by CAP_SYS_BOOT. request_key Prevent containers from using the kernel keyring, which is not namespaced. Set_mempolicy Syscall that modifies kernel memory and NUMA settings. Already gated by CAP_SYS_NICE. setns Deny associating a thread with a namespace. Also gated by CAP_SYS_ADMIN. Time/date is not namespaced. Also gated by CAP_SYS_TIME. Time/date is not namespaced. Also gated by CAP_SYS_TIME.	personality	
process_vm_writev Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE. ptrace Tracing/profiling syscall. Blocked in Linux kernel versions before 4.8 to avoid seccomp bypass. Tracing/profiling arbitrary processes is already blocked by dropping CAP_SYS_PTRACE, because it could leak a lot of information on the host. Query_module Deny manipulation and functions on kernel modules. Obsolete. Quota syscall which could let containers disable their own resource limits or process accounting. Also gated by CAP_SYS_ADMIN. reboot Don't let containers reboot the host. Also gated by CAP_SYS_BOOT. request_key Prevent containers from using the kernel keyring, which is not namespaced. set_mempolicy Syscall that modifies kernel memory and NUMA settings. Already gated by CAP_SYS_NICE. setns Deny associating a thread with a namespace. Also gated by CAP_SYS_ADMIN. Time/date is not namespaced. Also gated by CAP_SYS_TIME. Time/date is not namespaced. Also gated by CAP_SYS_TIME.	pivot_root	Deny pivot_root, should be privileged operation.
Tracing/profiling syscall. Blocked in Linux kernel versions before 4.8 to avoid seccomp bypass. Tracing/profiling arbitrary processes is already blocked by dropping CAP_SYS_PTRACE, because it could leak a lot of information on the host. Deny manipulation and functions on kernel modules. Obsolete. Quota syscall which could let containers disable their own resource limits or process accounting. Also gated by CAP_SYS_ADMIN. reboot Don't let containers reboot the host. Also gated by CAP_SYS_BOOT. request_key Prevent containers from using the kernel keyring, which is not namespaced. set_mempolicy Syscall that modifies kernel memory and NUMA settings. Already gated by CAP_SYS_NICE. setns Deny associating a thread with a namespace. Also gated by CAP_SYS_ADMIN. Time/date is not namespaced. Also gated by CAP_SYS_TIME. Time/date is not namespaced. Also gated by CAP_SYS_TIME.	process_vm_readv	Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE.
processes is already blocked by dropping CAP_SYS_PTRACE, because it could leak a lot of information on the host. query_module Deny manipulation and functions on kernel modules. Obsolete. quotact1 Quota syscall which could let containers disable their own resource limits or process accounting. Also gated by CAP_SYS_ADMIN. reboot Don't let containers reboot the host. Also gated by CAP_SYS_BOOT. request_key Prevent containers from using the kernel keyring, which is not namespaced. set_mempolicy Syscall that modifies kernel memory and NUMA settings. Already gated by CAP_SYS_NICE. setns Deny associating a thread with a namespace. Also gated by CAP_SYS_ADMIN. settimeofday Time/date is not namespaced. Also gated by CAP_SYS_TIME. Time/date is not namespaced. Also gated by CAP_SYS_TIME.	process_vm_writev	Restrict process inspection capabilities, already blocked by dropping CAP_SYS_PTRACE.
Quota syscall which could let containers disable their own resource limits or process accounting. Also gated by CAP_SYS_ADMIN. reboot Don't let containers reboot the host. Also gated by CAP_SYS_BOOT. request_key Prevent containers from using the kernel keyring, which is not namespaced. set_mempolicy Syscall that modifies kernel memory and NUMA settings. Already gated by CAP_SYS_NICE. setns Deny associating a thread with a namespace. Also gated by CAP_SYS_ADMIN. settimeofday Time/date is not namespaced. Also gated by CAP_SYS_TIME.	ptrace	Tracing/profiling syscall. Blocked in Linux kernel versions before 4.8 to avoid seccomp bypass. Tracing/profiling arbitrary processes is already blocked by dropping CAP_SYS_PTRACE, because it could leak a lot of information on the host.
CAP_SYS_ADMIN. reboot Don't let containers reboot the host. Also gated by CAP_SYS_BOOT. request_key Prevent containers from using the kernel keyring, which is not namespaced. set_mempolicy Syscall that modifies kernel memory and NUMA settings. Already gated by CAP_SYS_NICE. setns Deny associating a thread with a namespace. Also gated by CAP_SYS_ADMIN. settimeofday Time/date is not namespaced. Also gated by CAP_SYS_TIME. Stime Time/date is not namespaced. Also gated by CAP_SYS_TIME.	query_module	Deny manipulation and functions on kernel modules. Obsolete.
request_key Prevent containers from using the kernel keyring, which is not namespaced. Syscall that modifies kernel memory and NUMA settings. Already gated by CAP_SYS_NICE. Deny associating a thread with a namespace. Also gated by CAP_SYS_ADMIN. Time/date is not namespaced. Also gated by CAP_SYS_TIME. Time/date is not namespaced. Also gated by CAP_SYS_TIME.	quotactl	
Syscall that modifies kernel memory and NUMA settings. Already gated by CAP_SYS_NICE. Deny associating a thread with a namespace. Also gated by CAP_SYS_ADMIN. Settimeofday Time/date is not namespaced. Also gated by CAP_SYS_TIME. Time/date is not namespaced. Also gated by CAP_SYS_TIME.	reboot	Don't let containers reboot the host. Also gated by CAP_SYS_BOOT.
Deny associating a thread with a namespace. Also gated by CAP_SYS_ADMIN. Settimeofday Time/date is not namespaced. Also gated by CAP_SYS_TIME. Stime Time/date is not namespaced. Also gated by CAP_SYS_TIME.	request_key	Prevent containers from using the kernel keyring, which is not namespaced.
settimeofday Time/date is not namespaced. Also gated by CAP_SYS_TIME. Stime Time/date is not namespaced. Also gated by CAP_SYS_TIME.	set_mempolicy	Syscall that modifies kernel memory and NUMA settings. Already gated by CAP_SYS_NICE.
stime Time/date is not namespaced. Also gated by CAP_SYS_TIME.	setns	Deny associating a thread with a namespace. Also gated by CAP_SYS_ADMIN.
	settimeofday	Time/date is not namespaced. Also gated by CAP_SYS_TIME.
Deny start/stop swapping to file/device. Also gated by CAP_SYS_ADMIN.	stime	Time/date is not namespaced. Also gated by CAP_SYS_TIME.
	wapon	Deny start/stop swapping to file/device. Also gated by CAP_SYS_ADMIN.

Syscall	Description
swapoff	Deny start/stop swapping to file/device. Also gated by CAP_SYS_ADMIN.
sysfs	Obsolete syscall.
_sysctl	Obsolete, replaced by /proc/sys.
umount	Should be a privileged operation. Also gated by CAP_SYS_ADMIN.
umount2	Should be a privileged operation. Also gated by CAP_SYS_ADMIN.
unshare	Deny cloning new namespaces for processes. Also gated by CAP_SYS_ADMIN, with the exception of unshareuser.
uselib	Older syscall related to shared libraries, unused for a long time.
userfaultfd	Userspace page fault handling, largely needed for process migration.
ustat	Obsolete syscall.
vm86	In kernel x86 real mode virtual machine. Also gated by CAP_SYS_ADMIN.
vm86old	In kernel x86 real mode virtual machine. Also gated by CAP_SYS_ADMIN.

Run without the default seccomp profile

You can pass unconfined to run a container without the default seccomp profile.

```
$ docker run --rm -it --security-opt seccomp=unconfined debian:jessie \
    unshare --map-root-user --user sh -c whoami
```

About us	Developers	Features	Product offerings
Careers	Block	Container Runtime	Docker Business
Contact us	Community	Developer Tools	Docker Personal
Customers	Get started	Docker Desktop	Docker Pro
Newsletter	Open Source	Docker Hub	Docker Team
Newsroom	Preview Program	Docker Product	Docker Verified
Swag store	Use cases	Roadmap	Publisher
Virtual events		Secure Software	Partners
N/I at the second at the O		Supply Chain	Pricing FAQs
What is a container?		Trusted Content	3 4
Why Docker?			

Terms of Service Status Legal

Copyright © 2013-2023 Docker Inc. All rights reserved.

Twitter Youtube GitHub Linkedin Facebook Reddit



Cookies Settings