firewallctl

Client en ligne de commande pour firewalld

Il y a des options qui peuvent être spécifiées plusieurs fois. Le code de sortie est 0 s'il y a au moins un élément qui réussit. les erreurs ALREADY_ENABLED, NOT_ENABLED et ZONE_ALREADY_SET sont traité comme réussis.

Options générales

-v, –verbose mode verbeux

-q, –quiet N'affiche pas de messages de status

Option de status

state Vérifie si le service firewalld est actif

Option de rechargement

reload [-c | –complete] Recharge les règle firemall et conserve les informations d'état. La configuration permanente devient la configuration courante. -c recharge complètement le firewall, incluant les modules netfilter.

Option runtime-to-permanent

runtime-to-permanent Sauve la configuration active en tant que configuration permanente.

Options de liste

list zones [-a | –active | -p | –permanent] Affiche la liste des zones prédéfinies. -a n'affiche que les zones actives, -p n'affiche que les zones dans l'environnement permanent

list services [-p | –permanent] Affiche la liste des services prédéfinis.

list ipsets [-p | –permanent] Affiche la liste des ipsets prédéfinis

list helpers [-p | –permanent] Affiche la liste des helpers

list icmptypes [-p | –permanent] Affiche la liste des types icmp prédéfinis

Options d'informations

info zone <zone> [-p | –permanent] Affiche des informations sur la zone

info zones [-a | –active | -p | –permanent] Affiche des informations sur les zones

info service service [-p | –permanent] Affiche des informations sur le service spécifié

info services [-p | –permanent] Affiche des informations sur les services

info ipset ipset [-p | –permanent] Affiche des informations sur l'ipset spécifié

info ipsets [-p | –permanent] Affiche des informations sur les ipsets

info helper helper [-p | –permanent] Affiche des informations sur l'helper spécifié

info helpers [-p | –permanent] Affiche des informations sur les helper

info icmptype icmptype [-p | –permanent] Affiche des informations sur le type icmp spécifié

info icmptypes [-p | –permanent] Affiche des informations sur les types icmp

Options de zone

zone zone [-p | –permanent] add element.. [–timeout=timeval] Ajoute un élément ou de nombreux éléments de même type à une zone avec un timeout optionnel. Si la zone est une chaîne vide, la zone par défaut est utilisée. -p ajoute les éléments dans l'environnement permanent.

zone zone [-p | –permanent] remove element ... Supprime un ou plusieurs éléments d'une zone.

zone zone [-p | –permanent] query element ... Affiche si le ou les éléments sont activés dans la zone

zone zone [-p | –permanent] get { short | description } Affiche une description de la zone

zone zone [-p | –permanent] set { short | description } text Définis un description pour une zone

zone zone [-p | –permanent] list { interfaces | sources | services | ports | protocols | source-ports | rich-rules | forward-ports | icmp-bl Retourne la liste des éléments ajoutés pour la zone

zone zone { -p | –permanent } load-defaults Charge les paramètres de la zone par défaut ou affiche l'erreur NO_DEFAULTS

Éléments de zone

interface <interface> Nom d'une interface. Si l'interface est sous le contrôle de NetworkManager, elle doit d'abord être connectée.

source { address[/mask] | MAC | ipset :ipset } Une adresse ou plage d'adresse source ou une adresse MAC ou un ipset.

service <service> Nom d'un service

port portid[-portid]/protocol Port, plage de port ou nom de protocole

source-port portid[-portid]/protocol Port source

rich-rule 'rule' Règle en langage rich

masquerade Masquerading IPv4

forward-port port=portid[-portid] :proto=protocol[:toport=portid[-portid]][:toaddr=address[/mask]] Port forward ipv4

icmp-block icmptype block de type ICMP

icmp-block-inversion Inverse les blocks de type icmp

Options de service

service service [-p | –permanent] add element... Ajoute un ou plusiuers éléments à un service

service service [-p | –permanent] remove element... Supprime un ou plusieurs éléments d'un service

service service [-p | –permanent] query element... Affiche si un ou plusieurs éléments sont activés dans le service

service service [-p | –permanent] get { short | description } Affiche la description du service

service service [-p | –permanent] set { short | description } text Définis la description pour un service

service service [-p | –permanent] list { ports | protocols | source-ports | modules | destinations } Retourne la liste des éléments ajoutés pour un service

service service { -p | –permanent } load-defaults Charge les paramètres par défaut du service ou affiche NO_DEFAULTS

Éléments de service

port portid [-portid] /protocol Port ou plage de port / tcp|udp

protocol protocol Protocole supporté par le système

source-port portid [-portid] /protocol Port ou plage de port source / tcp|udp

module module Module netfilter

destination ipv :address [/mask] Adresse de destination. ipv=ipv4 ou ipv6

Options ipset

ipset ipset [-p | –permanent] add { entry entry | entries-from-file filename }... Ajoute une ou plusieurs entrées dans l'ipset

ipset ipset [-p | –permanent] remove { entry entry | entries-from-file filename | all }... Supprime une ou plusieurs entrées dans l'ipset

ipset ipset [-p | –permanent] query { entry entry | entries-from-file filename }... Affiche si la ou les entrées sont dans l'ipset

ipset ipset [-p | –permanent] get { short | description } Retourne la description de l'ipset

ipset ipset [-p | –permanent] set { short | description } text Définis la description de l'ipset

ipset ipset [-p | –permanent] list entries Liste les entrées ajoutées dans l'ipset

ipset ipset { -p | –permanent } load-defaults Charge les paramètres par défaut pour l'ipset ou retourne NO_DEFAULTS

Entrées ipset

ip [/cidr] Ajoute un ip ou une plage d'ip.

ip [/cidr] | fromaddr-toaddr idem en spécifiant les ip source et de destination

mac L'entrée est une adresse MAC

Options helper

helper helper -p | –permanent { add | remove } port portid [-portid] /protocol Ajoute ou supprime le port au helper.

helper helper [-p | –permanent] query port portid [-portid] /protocol Affiche si le port est mis dans le helper

helper helper [-p | –permanent] get { short | description } Affiche la description du helper

helper helper [-p | –permanent] get family Affiche la famille du helper

helper helper [-p | –permanent] get module Affiche le module netfilter du helper

helper helper -p | –permanent set { short | description } text Définis la description du helper

helper helper -p | –permanent set family Définis la famille du helper

helper helper -p | –permanent set module Définis le module helper netfilter pour le helper

helper helper [-p | –permanent] list ports Retourne la liste des ports ajoutés au helper

helper helper { -p | –permanent } load-defaults Charge les paramètres par défaut du helper ou retourne NO_DEFAULTS

Options icmptype

icmptype icmptype [-p | –permanent] { add | remove } destination { ipv4 | ipv6 } Ajoute ou supprime la destination au icmptype.

icmptype icmptype [-p | –permanent] query destination { ipv4 | ipv6 } Affiche si la destination est dans le icmptype

icmptype icmptype [-p | –permanent] get { short | description } Affiche la description du icmptype

icmptype icmptype [-p | –permanent] set { short | description } text Définis la description du icmptype

icmptype icmptype [-p | –permanent] list destinations Affiche la liste des destinations ajoutées pour l'icmptype

icmptype icmptype { -p | –permanent } load-defaults Charge le paramètres par défaut du icmptype ou affiche NO_DEFAULTS

Options new

new { -p | –permanent } zone { { -n | –name } name | { -f | –filename} filename [{ -n | –name } name }] } Ajoute une zone permanente.

new { -p | –permanent } service { { -n | –name } name | { -f | –filename} filename [{ -n | –name } name }] } Ajoute un service permanent

new { -p | –permanent } ipset { { -n | –name } name { -t | –type } ipsettype [{ -o | –option } option [=value]] | { -f | –filename} filenam Ajoute un ipset permanent

new { -p | –permanent } icmptype { { -n | –name } name | { -f | –filename} filename [{ -n | –name } name }] } Ajoute un icmptype permanent

Options delete

delete { -p | –permanent } zone zone Supprime une zone permanente

delete { -p | –permanent } service service Supprime un service permanent

delete { -p | –permanent } ipset ipset Supprime un ipset permanent

delete { -p | –permanent } icmptype icmptype Supprime un ipset permanent

Options direct

direct [-p | –permanent] { add | remove } chain { ipv4 | ipv6 | eb } table chain Ajoute une nouvelle chaîne nommé à la table spécifiée.

direct [-p | –permanent] query chain { ipv4 | ipv6 | eb } table chain Affiche si un chaîne existe dans la table spécifiée

direct [-p | –permanent] get chains { ipv4 | ipv6 | eb } table Affiche les chaînes ajoutées à la table spécifiée

direct [-p | –permanent] get all-chains Récupère toutes les chaînes ajoutées à toutes les tables

direct [-p | –permanent] { add | remove } rule { ipv4 | ipv6 | eb } table chain priority args Ajoute ou supprime une règle à la chaîne spécifiée. La priorité est utilisée pour l'ordre des règles (0 étant la première)

direct [-p | –permanent] query rule { ipv4 | ipv6 | eb } table chain priority args Affiche si une règle avec la priorité et les arguments existe dans la chaîne dans la table spécifiés. Retourne 0 si vrai, 1 sinon.

direct [-p | –permanent] get all-rules Affiche toutes les règles ajoutées à toutes les chaînes d-ans toutes les tables

direct [-p | –permanent] get rules { ipv4 | ipv6 | eb } table chain Affiche les règles ajoutées à la chaîne dans la table spécifiées.

direct [-p | –permanent] { add | remove } passthrough { ipv4 | ipv6 | eb } args Ajoute une règle passthrough

direct [-p | –permanent] query passthrough { ipv4 | ipv6 | eb } args Affiche une règle passthrough

direct [-p | –permanent] get all-passthroughs Affiche toutes les règles passthrough

direct [-p | –permanent] get passthroughs { ipv4 | ipv6 | eb } Affiche les règles passthrough pour une valeur ipv

direct passthrough { ipv4 | ipv6 | eb } args Passe une commande au firewall args peut être iptables, ip6tables et ebtables.

Options Lockdown Whitelist

Les applications locales ou services sont capable de changer la configuration firewall s'ils tournent en root (par exemple libvirt) ou sont authentifiés via PolKit. Avec cette fonctionnalité, les administrateurs peuvent bloquer la configuration du firewall pour que seuls les applications dans la lockdown whitelist soient capable de changer le firewall.

lockdown-whitelist [-p | –permanent] { add | remove } element... Ajoute ou supprime un ou plusieurs éléments à la liste

lockdown-whitelist [-p | –permanent] query element... Affiche si le ou les éléments sont membres de la liste

lockdown-whitelist [-p | –permanent] list { commands | contexts | uids | users } Affiche la liste des membres de la liste

Options de configuration

config set { default-zone zone | lockdown { on | off } | log-denied value | panic { on | off } } Définis une option de configuration firewalld. Les valeurs possibles sont :

default-zone zone Définis la zone par défaut pour les connexions et les interfaces

lockdown Active/désactive le lockdown. Noter que par défaut firewall-cmd n'est pas dans la liste.

log-denied Si activé, les règles de logging sont ajoutées avant les règles de rejet/suppression dans les chaînes INPUT, FORWARD, et OUTPUT pour les règles par défaut. Les valeurs possibles sont all, unicast, broadcast, multicast, et off. Défaut : off.

panic Active le mode panic. Si activé, tous les paquets entrant et sortant sont supprimés. À activer uniquement en cas de problème sérieux dans le réseau.

config list Liste les options de configuration de firewalld

config get { default-zone | lockdown | log-denied | panic } Afficher les options de configuration de firewalld

Options de paramètrage

settings list Liste les paramètres de firewalld comme BRIDGE, CleanupOnExit, IPSet, IPSetTypes, IPv4, IPv6, IPv6_rpfilter, IndividualCalls et MinimalMark

settings get { BRIDGE | CleanupOnExit | IPSet | IPSetTypes | IPv4 | IPv6 | IPv6_rpfilter | IndividualCalls | MinimalMark } AFficher les paramètres de firewalld :

BRIDGE Affiche si la commutation est disponible

CleanupOnExit Affiche si CleanupOnExit est activé

IPSet Affiche si le support ipset est disponible

IPSetTypes Affiche les types ipsets supportés

IPv4 Affiche si le support IPv4 est disponible

IPv6 Affiche si le support IPv6 est disponible

IPv6_rpfilter Affiche si rpfilter IPv6 est activé

IndividualCalls Retourne les paramètres d'appel individuels

MinimalMark Retourne le paramètre de marque minimum

Codes de sortie

0 succès
11 ALREADY_ENABLED
12 NOT_ENABLED
13 COMMAND_FAILED
14 NO_IPV6_NAT
15 PANIC_MODE
16 ZONE_ALREADY_SET
17 UNKNOWN_INTERFACE
18 ZONE_CONFLICT
19 BUILTIN_CHAIN
20 EBTABLES_NO_REJECT
21 NOT_OVERLOADABLE
22 NO_DEFAULTS
23 BUILTIN_ZONE
24 BUILTIN_SERVICE
25 BUILTIN_ICMPTYPE
26 NAME_CONFLICT
27 NAME_MISMATCH
28 PARSE_ERROR
29 ACCESS_DENIED
30 UNKNOWN_SOURCE
31 RT_TO_PERM_FAILED
32 IPSET_WITH_TIMEOUT
33 BUILTIN_IPSET
34 ALREADY_SET
35 MISSING_IMPORT
36 DBUS_ERROR
37 BUILTIN_HELPER
100 INVALID_ACTION
101 INVALID_SERVICE
102 INVALID_PORT
103 INVALID_PROTOCOL
104 INVALID_INTERFACE
105 INVALID_ADDR
106 INVALID_FORWARD
107 INVALID_ICMPTYPE
108 INVALID_TABLE
109 INVALID_CHAIN
110 INVALID_TARGET
111 INVALID_IPV
112 INVALID_ZONE
113 INVALID_PROPERTY
114 INVALID_VALUE
115 INVALID_OBJECT

116 INVALID_NAME
117 INVALID_FILENAME
118 INVALID_DIRECTORY
119 INVALID_TYPE
120 INVALID_SETTING
121 INVALID_DESTINATION
122 INVALID_RULE
123 INVALID_LIMIT
124 INVALID_FAMILY
125 INVALID_LOG_LEVEL
126 INVALID_AUDIT_TYPE
127 INVALID_MARK
128 INVALID_CONTEXT
129 INVALID_COMMAND
130 INVALID_USER
131 INVALID_UID
132 INVALID_MODULE
133 INVALID_PASSTHROUGH
134 INVALID_MAC
135 INVALID_IPSET
136 INVALID_ENTRY
137 INVALID_OPTION
138 INVALID_HELPER
200 MISSING_TABLE
201 MISSING_CHAIN
202 MISSING_PORT
203 MISSING_PROTOCOL
204 MISSING_ADDR
205 MISSING_NAME
206 MISSING_SETTING
207 MISSING_FAMILY
252 NOT_RUNNING
253 NOT_AUTHORIZED
254 UNKNOWN_ERROR