Object Group Configuration Mode Commands

Object groups allow you to simplify the creation of multiple access control list (ACL) entries in an ACL. By grouping like objects together, you can use an object group in an ACL entry instead of having to enter an ACL entry for each object separately.

To create an object group and access object group configuration mode, use the **object-group** command. The CLI prompt changes to (config-objgrp-netw or config-objgrp-serv) depending upon whether you create a network or service object group. Use the **no** form of this command to delete an existing object group.

object-group [**network** | **service**] *name*

no object-group [**network** | **service**] *name*

Syntax Description

network	Specifies a group of hosts or subnet IP addresses.
service	Specifies a group of TCP or UDP port specifications or ICMP types.
name	Unique identifier of the object group. Enter the object group name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Action list modify configuration mode

Admin and user contexts

Command History

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

You can create either network or service object groups. After you create these groups, you can use a single ACL entry to allow trusted hosts to make specific service requests to a group of public servers.

If you add new members to an existing object group that is already in use by an entry in a large ACL, recommitting the ACL can take a long time, depending on the size of the ACL and the object group. In some cases, making this change can cause the ACE to devote over an hour to committing the ACL, during which time you cannot access the terminal. We recommend that you first remove the ACL entry that refers to the object group, make your change, and then add the ACL entry back into the ACL.

Examples

To create a network object group, enter:

```
host1/Admin(config)# object-group network NET_OBJ_GROUP1
host1/Admin(config-objgrp-netw)#
```

To create a service object group, enter:

```
host1/Admin(config)# object-group service SERV_OBJ_GROUP1
host1/Admin(config-objgrp-serv)#
```

Related Commands

(config-objgrp-netw) description
(config-objgrp-netw) host
(config-objgrp-netw) ip_address

(config-objgrp-netw) description

To add an optional description to a network object group, use the **description** command. Use the **no** form of this command to remove a description from a network object group.

description *text*

no description *text*

Syntax Description

text	(Optional) Description of the network object group. Enter the description as an unquoted, alphanumeric, text string from 1 to 240 characters.

Command Modes

Network object group configuration mode

Admin and user contexts

Command History

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description to the network object group, enter:

```
host1/Admin(config-objgrp-netw)# description intranet network object group
```

To remove a description from the network object group, enter:

```
host1/Admin(config-objgrp-netw)# no description intranet network object group
```

Related Commands

(config) object-group
(config-objgrp-netw) host
(config-objgrp-netw) ip_address

(config-objgrp-netw) host

To associate a host IPv6 or IPv4 address with a network object group, use the **host** command. Use the **no** form of this command to remove a host from the network object group.

host *ip_address*

no host *ip_address*

Syntax Description

ip_address	Host IP address associated with the network object group. Enter an IP address in dotted-decimal notation (for example, 192.168.12.15).

Command Modes

Network object group configuration mode

Admin and user contexts

Command History

ACE Module Release	Modification
A2(1.0)	This command was introduced.
A5(1.0)	Added IPv6 support.

ACE Appliance Release	Modification
A3(1.0)	This command was introduced.
A5(1.0)	Added IPv6 support.

Usage Guidelines

You cannot mix an IPv6 address and an IPv4 address in the same network object group.

Examples

IPv6 Example

To create a network object group that includes three IPv6 host addresses, enter:

```
host1/Admin(config)# object-group network NET_OBJ_GROUP1
host1/Admin(config-objgrp-netw)# description Administrator Addresses
host1/Admin(config-objgrp-netw)# host 2001:DB8:1::/64
host1/Admin(config-objgrp-netw)# host 2001:DB8:2::/64
host1/Admin(config-objgrp-netw)# host 2001:DB8:3::/64
```

To remove host IPv6 address 2001:DB8:1::/64 from the network object group, enter:

```
host1/Admin(config-objgrp-netw)# no host 2001:DB8:1::/64
```

IPv4 Example

To create a network object group that includes three IPv4 host addresses, enter:

```
host1/Admin(config)# object-group network NET_OBJ_GROUP1
host1/Admin(config-objgrp-netw)# description Administrator Addresses
host1/Admin(config-objgrp-netw)# host 192.168.12.15
host1/Admin(config-objgrp-netw)# host 192.168.12.21
host1/Admin(config-objgrp-netw)# host 192.168.12.27
```

To remove host IPv4 address 192.168.12.15 from the network object group, enter:

```
host1/Admin(config-objgrp-netw)# no host 192.168.12.15
```

Related Commands

(config) object-group
(config-objgrp-netw) description
(config-objgrp-netw) ip_address

(config-objgrp-netw) *ip_address*

To associate a network IP address with a network object group, use the *ip_address* command. Use the **no** form of this command to remove an IP address or host from the network object group.

ip_address{*/prefix_length* | *netmask*}

no *ip_address*{*/prefix_length* | *netmask*}

Syntax Description

ip_address	IP address assigned to the network object group.
/prefix_length	For an IPv6 address, the length of the network prefix. Enter a "/" (forward slash) followed by an integer from 1 to 128.
netmask	Network mask applied to the IP address. Enter a network mask in dotted decimal notation (for example, 255.255.255.0).

Command Modes

Network object group configuration mode

Admin and user contexts

Command History

ACE Module Release	Modification
A2(1.0)	This command was introduced.
A5(1.0)	Added IPv6 support.

ACE Appliance Release	Modification
A3(1.0)	This command was introduced.
A5(1.0)	Added IPv6 support.

Usage Guidelines

You cannot mix an IPv6 address and an IPv4 address in the same network object group.

Examples

IPv6 Example

To add the IPv6 address and prefix length 2001:DB8:1::1/64 to a network object group, enter:

```
host1/Admin(config-objgrp-netw)# 2001:DB8:1::1/64
```

Enter additional object-group IP addresses as required.

To remove an IP address from the network object group, enter:

```
host1/Admin(config-objgrp-netw)# no 2001:DB8:1::1/64
```

IPv4 Example

To add the IP address 192.168.12.15 and network mask 255.255.255.0 to a network object group, enter:

```
host1/Admin(config-objgrp-netw)# 192.168.12.15 255.255.255.0
```

To remove an IP address from the network object group, enter:

```
host1/Admin(config-objgrp-netw)# no 192.168.12.15 255.255.255.0
```

Related Commands

(config) object-group
(config-objgrp-netw) description
(config-objgrp-netw) host

(config-objgrp-serv) description

To add an optional description to a service object group, use the **description** command. Use the **no** form of this command to remove a description from a service object group.

description *text*

no description *text*

Syntax Description

text	(Optional) Description of the service object group. Enter the description as an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Service object group configuration mode

Admin and user contexts

Command History

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description to the service object group, enter:

```
host1/Admin(config-objgrp-serv)# description intranet service object group
```

To remove a description from the service object group, enter:

```
host1/Admin(config-objgrp-serv)# no description intranet service object group
```

Related Commands

(config) object-group
(config-objgrp-serv) protocol

(config-objgrp-serv) *protocol*

To associate a protocol and port designation with a service object group, use the *protocol* command. Use the **no** form of this command to remove the protocol and port designation from a service object group.

protocol [**source** *operator port1* [*port2*]] [*operator port3* [*port4*]] [**icmp-type** *type* **code** *operator code1 code2*]

no *protocol* [**source** *operator port1* [*port2*]] [*operator port3* [*port4*]] [**icmp-type** *type* **code** *operator code1 code2*]

Syntax Description

protocol	Name or number of an IP protocol. Enter a protocol name or an integer from 1 to 255 that represents an IP protocol number. See Table 2-12.
source	Specifies a source port for TCP, TCP-UDP, or UDP. To specify a destination port, use the *operator* argument with no keyword.
operator	(Optional) Operand used to compare source and destination port numbers for TCP and UDP protocols, and message codes for ICMP. To specify a destination port, use the *operator* argument with no keyword.The operators are as follows: • **lt**—Less than. • **gt**—Greater than. • **eq**—Equal to. • **neq**—Not equal to. • **range**—An inclusive range of port values or ICMP message codes. If you enter this operator, enter a second port number value or second ICMP message code to define the upper limit of the range.
port1 [*port2*]	TCP or UDP source name or port number from which you permit or deny services access. Enter a port name or an integer from 0 to 65535. To enter an inclusive range of ports, enter two port numbers. *Port2* must be greater than or equal to *port1*. See Table 2-13 for a list of well-known TCP keywords and port numbers and Table 2-14 for a list of well-known UDP key words and port numbers.
port3 [*port4*]	TCP or UDP destination name or port number to which you permit or deny services access. To enter an optional inclusive range of ports, enter two port numbers. *port4* must be greater than or equal to *port3*. See Table 2-13 for a list of well-known TCP keywords and port numbers and Table 2-14 for a list of well-known UDP keywords and port numbers.
icmp-type *type*	(Optional) If you entered ICMP as the protocol, specifies the type of ICMP messaging. Enter either an integer corresponding to the ICMP code number or one of the ICMP types listed in Table 2-15 (ICMPv4) or Table 2-16 (ICMPv6).
code	(Optional) Specifies that a numeric operator and ICMP code follows.
code1 [*code2*]	ICMP code number that corresponds to an ICMP type. See Table 2-15 (ICMPv4) or Table 2-16 (ICMPv6). If you entered the **range** operator, enter a second ICMP code value to define the upper limit of the range.

Table 2-12 Supported Protocol Keywords and Numbers

Protocol Name	Protocol Number	Description
ah	**51**	Authentication Header
eigrp	**88**	Enhanced IGRP
esp	**50**	Encapsulated Security Payload
gre	**47**	Generic Routing Encapsulation
icmp	**1**	Internet Control Message Protocol v4
icmpv6	**58**	Internet Control Message Protocol v6
igmp	**2**	Internet Group Management Protocol
ip	**any**	Internet Protocol
ip-in-ip	**4**	IP-in-IP Layer 3 Tunneling Protocol
ospf	**89**	Open Shortest Path First
pim	**103**	Protocol Independent Multicast
tcp	**6**	Transmission Control Protocol
tcp-udp	**6 and 17**	TCP and UDP
udp	**17**	User Datagram Protocol

Table 2-13 Well-Known TCP Port Numbers and Keywords

Keyword	Port Number	Description
aol	**5190**	America-Online
bgp	**179**	Border Gateway Protocol
chargen	**19**	Character Generator
citrix-ica	**1494**	Citrix Independent Computing Architecture Protocol
cmd	**514**	Same as exec, with automatic authentication
ctiqbe	**2748**	Computer Telephony Interface Quick Buffer Encoding
daytime	**13**	Daytime
discard	**9**	Discard
domain	**53**	Domain Name System
echo	**7**	Echo
exec	**512**	Exec (RSH)
finger	**79**	Finger
ftp	**21**	File Transfer Protocol
ftp-data	**20**	FTP data connections
gopher	**70**	Gopher
h323	**1720**	H.323 call signaling

Table 2-13 Well-Known TCP Port Numbers and Keywords (continued)

Keyword	Port Number	Description
hostname	**101**	NIC hostname server
http	**80**	Hypertext Transfer Protocol
https	**443**	HTTP over TLS/SSL
ident	**113**	Ident Protocol
imap4	**143**	Internet Message Access Protocol, version 4
irc	**194**	Internet Relay Chat
kerberos	**88**	Kerberos
klogin	**543**	Kerberos Login
kshell	**544**	Kerberos Shell
ldap	**389**	Lightweight Directory Access Protocol
ldaps	**636**	LDAP over TLS/SSL
login	**513**	Login (rlogin)
lotusnotes	**1352**	IBM Lotus Notes
lpd	**515**	Printer Service
matip-a	**350**	Mapping of Airline Traffic over Internet Protocol Type A
netbios-ssn	**139**	NetBIOS Session Service
nntp	**119**	Network News Transport Protocol
pcanywhere-data	**5631**	PC Anywhere data
pim-auto-rp	**496**	PIM Auto-RP
pop2	**109**	Post Office Protocol v2
pop3	**110**	Post Office Protocol v3
pptp	**1723**	Point-to-Point Tunneling Protocol, RFC 2637
rtsp	**554**	Real-Time Streaming Protocol
sip	**5060**	Session Initiation Protocol
skinny	**2000**	Cisco Skinny Client Control Protocol (SCCP)
smtp	**25**	Simple Mail Transfer Protocol
sqlnet	**1521**	Structured Query Language Network
ssh	**22**	Secure Shell
sunrpc	**111**	Sun Remote Procedure Call
tacacs	**49**	Terminal Access Controller Access Control System
talk	**517**	Talk
telnet	**23**	Telnet

Table 2-13 Well-Known TCP Port Numbers and Keywords (continued)

Keyword	Port Number	Description
time	**37**	Time
uucp	**540**	Unix-to-Unix Copy Program
whois	**43**	Nicname
www	**80**	World Wide Web (HTTP)

Table 2-14 Well-Known UDP Keywords and Port Numbers

Keyword	Port Number	Description
biff	**512**	Mail notification
bootpc	**68**	Bootstrap Protocol client
bootps	**67**	Bootstrap Protocol server
discard	**9**	Discard
dnsix	**195**	DNSIX Security protocol auditing (dn6-nlm-aud)
domain	**53**	Domain Name System
echo	**7**	Echo
isakmp	**500**	Internet Security Association Key Management Protocol
kerberos	**88**	Kerberos
mobile-ip	**434**	Mobile IP registration
nameserver	**42**	Host Name Server
netbios-dgm	**138**	NetBIOS datagram service
netbios-ns	**137**	NetBIOS name service
netbios-ssn	**139**	NetBIOS Session Service
ntp	**123**	Network Time Protocol
pcanywhere-status	**5632**	PC Anywhere status
radius-auth	**1812**	(ACE module only) Remote Authentication Dial-in User Service
radius	**1812**	(ACE appliance only) Remote Authentication Dial-in User Service
radius-acct	**1813**	RADIUS Accounting
rip	**520**	Routing Information Protocol
snmp	**161**	Simple Network Management Protocol
snmptrap	**162**	SNMP Traps
sunrpc	**111**	Sun Remote Procedure Call
syslog	**514**	System Logger

Table 2-14 Well-Known UDP Keywords and Port Numbers (continued)

Keyword	Port Number	Description
tacacs	**49**	Terminal Access Controller Access Control System
talk	**517**	Talk
tftp	**69**	Trivial File Transfer Protocol
time	**37**	Time
who	**513**	Who service (rwho)
wsp	**9200**	Connectionless Wireless Session Protocol
wsp-wtls	**9202**	Secure Connectionless WSP
wsp-wtp	**9201**	Connection-based WSP
wsp-wtp-wtls	**9203**	Secure Connection-based WSP
xdmcp	**177**	X Display Manager Control Protocol

Table 2-15 ICMPv4 Types

ICMP Code Number	ICMP Type
0	**echo-reply**
3	**unreachable**
4	**source-quench**
5	**redirect**
6	**alternate-address**
8	**echo**
9	**router-advertisement**
10	**router-solicitation**
11	**time-exceeded**
12	**parameter-problem**
13	**timestamp-request**
14	**timestamp-reply**
15	**information-request**
16	**information-reply**
17	**mask-request**
18	**mask-reply**
30	**traceroute**
31	**conversion-error**
32	**mobile-redirect**

Table 2-16 ICMPv6 Types

ICMPv6 Code Number	ICMPv6 Type
1	**unreachable**
3	**time-exceeded**
4	**parameter-problem**
30	**traceroute**
128	**echo**
129	**echo-reply**
137	**redirect**
139	**information-request**
140	**information-reply**

Command Modes

Service object group configuration mode

Admin and user contexts

Command History

ACE Module Release	Modification
A2(1.0)	This command was introduced.
A2(2.1)	The **radius** keyword is deprecated and is now the **radius-auth** keyword.
A5(1.0)	Added IPv6 support.

ACE Appliance Release	Modification
A3(1.0)	This command was introduced.
A5(1.0)	Added IPv6 support.

Usage Guidelines

This command has no usage guidelines.

Examples

To create a service object group for TCP (source port only), UDP (source and destination ports), and ICMPv6, enter:

```
ISM/Admin(config)# object-group service TCP_UDP_ICMP
ISM/Admin(config-objgrp-serv)# tcp source eq domain
ISM/Admin(config-objgrp-serv)# udp source eq radius eq radius-acct
ISM/Admin(config-objgrp-serv)# icmpv6 echo code eq 128
```

To remove the ICMP protocol from the above service object group, enter:

```
host1/Admin(config-objgrp-prot)# no icmpv6 echo code eq 128
```

Related Commands (config) object-group
(config-objgrp-serv) description