# match r – me

# match regex

要标识正则表达式类映射中的正则表达式，请在 class-map type regex 配置模式下使用 **matchregex** 命令。要从类映射中删除正则表达式，请使用此命令的 **no** 形式。

**matchregex**名称
**nomatchregex***name*

## Syntax Description

| | |
|---|---|
| *name* | 通过 **regex** 命令添加的正则表达式的名称。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 类映射类型正则表达式配置 | • 是 | • 支持 | • 支持 | — | • 是 |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(2) | 添加了此命令。 |

## 使用指南

**regex** 命令可用于需要文本匹配的各种功能。您可以使用 **class-maptyperegex** 命令，然后使用多个 **matchregex** 命令，对正则表达式类映射中的正则表达式进行分组。

例如，您可以使用检查策略图配置应用程序检查的特殊操作（参见**policymaptypeinspect**命令）。在检测策略映射中，您可以创建包含一个或多个 **match** 命令的检测类映射，标识要对其执行操作的流量，也可以直接在检测策略映射中使用 **match** 命令。某些 **match** 命令可使用正则表达式标识数据包中的文本，请参阅；例如，可以匹配 HTTP 数据包内的 URL 字符串。

## CR_Examples

以下是 HTTP 检测策略映射和相关类映射的示例。此策略映射由第 3/4 层策略映射激活，而第 3/4 层策略映射由服务策略启用。

```
ciscoasa(config)# regex url_example example\.com
ciscoasa(config)# regex url_example2 example2\.com
ciscoasa(config)# class-map type regex match-any URLs
ciscoasa(config-cmap)# match regex url_example
ciscoasa(config-cmap)# match regex url_example2
ciscoasa(config-cmap)# class-map type inspect http match-all http-traffic
ciscoasa(config-cmap)# match req-resp content-type mismatch
```

```
ciscoasa(config-cmap)# match request body length gt 1000
ciscoasa(config-cmap)# match not request uri regex class URLs
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# drop-connection log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# protocol-violation action log
ciscoasa(config-pmap-p)# policy-map test
ciscoasa(config-pmap)# class test
 [a Layer 3/4 class map not shown]
ciscoasa(config-pmap-c)# inspect http http-map1
ciscoasa(config-pmap-c)# service-policy test interface outside
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **class-maptyperegex** | 创建正则表达式类映射。 |
| **regex** | 添加正则表达式。 |
| **testregex** | 测试正则表达式。 |

# match req-resp

要为 HTTP 请求和响应配置匹配条件，请在策略映射配置模式下使用 **matchreq-resp** 命令。要禁用此功能，请使用此**no**命令的形式。

**match** [**not**] **req-respcontent-typemismatch**
**nomatch** [**not**] **req-respcontent-typemismatch**

## Syntax Description

| | |
|---|---|
| 内容类型不匹配 | 将 HTTP 响应中的 content-type 字段与相应 HTTP 请求消息中的 accept 字段不匹配的流量进行匹配。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 策略映射配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.2(1) | 添加了此命令。 |

## 使用指南

此命令可启用以下检查：

- 验证报头 content-type 的值是否在受支持内容类型的内部列表中，
- 验证报头内容类型是否与消息的数据或实体正文部分中的实际内容匹配。
- 验证 HTTP 响应中的内容类型字段是否与相应 HTTP 请求消息中的 **accept** 字段匹配。

如果该消息未通过上述任一检查，则 ASA 将执行已配置的操作。

以下是受支持的内容类型列表。

| | | |
|---|---|---|
| 音频/* \| | 音频/基本 \| | 视频/x-msvideo |
| 音频/mpeg \| 转换 | x-adpcm \| 音频/x-adpcm | 音频/midi |
| 音频/x-ogg \| 音频 | x-wav \| 音频/x-wav | \| 音频/x-aiff \| 音频 |
| application/octet-stream | application/pdf | application/msword |

| | | |
|---|---|---|
| application/vnd.ms-excel | application/vnd.ms-powerpoint | application/postscript |
| application/x-java-arming | application/x-msn-messenger | application/x-gzip |
| 图片 \| | application/x-java-xm | application/zip |
| image/jpeg \| | image/cgf \| | image/gif \| |
| image/x-3ds \| | image/png \| | image/tiff \| |
| image/x-portable-bitmap \| | image/x-bitmap \| | x-niff \| image/x-niff |
| text/* \| | image/x-portable-greymap \| image/x-portable-greymap | image/x-xpm \| 映像 |
| text/plain \| | text/css | text/html \| |
| text/xmcd | text/richtext \| | text/sgml |
| video/-flc | text/xml | video/* |
| 视频/Sgi | 视频/mpeg | 视频/quicktime |
| 视频/x-mng | 视频/x-avi | 视频/x-fli |

此列表中的某些内容类型可能没有相应的正则表达式（幻数），因此无法在邮件的正文部分中对其进行验证。当发生这种情况时，将允许 HTTP 消息。

## CR_Examples

以下示例显示如何根据 HTTP 策略映射中 HTTP 消息的内容类型来限制 HTTP 流量：

```
ciscoasa
(config)#
 policy-map type inspect http http_map
ciscoasa
(config-pmap)#
 match req-resp content-type mismatch
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **class-map** | 创建第 3/4 层类映射。 |
| **clearconfigureclass-map** | 删除所有类映射。 |
| **showrunning-configclass-map** | 显示有关类映射配置的信息。 |

# match request-command

要限制特定 FTP 命令，请在 class-map 或 policy-map 配置模式下使用 **matchrequest-command** 命令。要删除匹配条件，请使用此 **no**命令的形式。

**match** [**not**] **request-command***ftp_command* [*ftp_command* . . . ]
**no match** [**not**] **request-command***ftp_command* [*ftp_command* . . . ]

## Syntax Description

| | |
|---|---|
| *ftp_*命令 | 指定要限制的一个或多个FTP命令。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 类映射或策略映射配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.2(1) | 添加了此命令。 |

## 使用指南

可以在 FTP 类映射或策略映射中配置此命令。一个 FTP 类映射中只能输入一个条目。

## CR_Examples

以下示例显示如何在 FTP 检测策略映射中为特定 FTP 命令配置匹配条件：

```
ciscoasa(config)# policy-map type inspect ftp ftp_map1
ciscoasa(config-pmap)# match request-command stou
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **class-map** | 创建第 3/4 层类映射。 |
| **clearconfigureclass-map** | 删除所有类映射。 |
| **matchany** | 包括类映射中的所有流量。 |
| **matchport** | 标识类映射中的特定端口号。 |

| 命令 | 说明 |
| --- | --- |
| **showrunning-configclass-map** | 显示有关类映射配置的信息。 |

# match request-method

要配置 SIP 方法类型的匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchrequest-method** 命令。要删除匹配条件，请使用此 **no**命令的形式。

**match** [**not**] **request-method***method_type*
**no match** [**not**] **request-method***method_type*

## Syntax Description

| | |
|---|---|
| *method_type* | 根据 RFC 3261 和支持的扩展指定方法类型。支持的方法类型包括：ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 类映射或策略映射配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.2(1) | 添加了此命令。 |

## 使用指南

可以在 SIP 类映射或策略映射中配置此命令。一个 SIP 类映射中只能输入一个条目。

## CR_Examples

以下示例展示如何为 SIP 检测类映射中的 SIP 消息配置匹配条件：

```
ciscoasa(config-cmap)# match request-method ack
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **class-map** | 创建第 3/4 层类映射。 |
| **clearconfigureclass-map** | 删除所有类映射。 |
| **matchany** | 包括类映射中的所有流量。 |
| **matchport** | 标识类映射中的特定端口号。 |

| 命令 | 说明 |
| --- | --- |
| **showrunning-configclass-map** | 显示有关类映射配置的信息。 |

# match request method

要配置 HTTP 请求的匹配条件，请在 policy-map 配置模式下使用 **matchrequestmethod** 命令。要禁用此功能，请使用此**no**命令的形式。

**match** [**not**] **request** {*built-in-regex* | **regex** {**regex_name** | **class***class_map_name*}}
**no match** [**not**] **request** {*built-in-regex* | **regex** {**regex_name** | **class***class_map_name*}}

## Syntax Description

| | |
|---|---|
| *built-in-regex* | 指定内容类型、方法或传输编码的内置正则表达式。 |
| **class***class_map name* | 指定正则表达式类型的类映射的名称。 |
| **regex***regex_name* | 指定使用 **regex** 命令配置的正则表达式的名称。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 策略映射配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.2(1) | 添加了此命令。 |

## 使用指南

表 *1:* 内置 ***Regex*** 值

| | | | |
|---|---|---|---|
| bcopy | bdelete | bmove | bpropfind |
| bproppatch | connect | copy | delete |
| edit | get | getattribute | getattributenames |
| getproperties | head | index | 锁定 |
| mkcol | mkdir | 迁移 | notify |
| 选项 | poll | 岗位 | propfind |
| proppatch | put | revadd | revlabel |

| | | | |
|---|---|---|---|
| revlog | revnum | 保存 | 搜索 |
| 设置属性 | 开始/旋转 | stoprev | 订阅 |
| trace | unedit | 解锁 | unsubscribe |

## CR_Examples

以下示例显示如何定义 HTTP 检查策略映射，该策略映射将允许并记录任何尝试使用方法“GET”或“PUT”访问“www\.example.com/.*\.asp”或“www\example[0-9][0-9]\.com”的 HTTP 连接。所有其他 URL/方法组合将被默许：

```
ciscoasa(config)# regex url1 "www\.example.com/.*\.asp
ciscoasa(config)# regex url2 "www\.example[0-9][0-9]\.com"
ciscoasa(config)# regex get "GET"
ciscoasa(config)# regex put "PUT"
ciscoasa(config)# class-map type regex match-any url_to_log
ciscoasa(config-cmap)# match regex url1
ciscoasa(config-cmap)# match regex url2
ciscoasa(config-cmap)# exit
ciscoasa(config)# class-map type regex match-any methods_to_log
ciscoasa(config-cmap)# match regex get
ciscoasa(config-cmap)# match regex put
ciscoasa(config-cmap)# exit
ciscoasa(config)# class-map type inspect http http_url_policy
ciscoasa(config-cmap)# match request uri regex class url_to_log
ciscoasa(config-cmap)# match request method regex class methods_to_log
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map type inspect http http_policy
ciscoasa(config-pmap)# class http_url_policy
ciscoasa(config-pmap-c)# log
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **class-map** | 创建第 3/4 层类映射。 |
| **clearconfigureclass-map** | 删除所有类映射。 |
| **showrunning-configclass-map** | 显示有关类映射配置的信息。 |

# match route-type

要重新分发指定类型的路由，请在 route-map 配置模式下使用 **matchroute-type** 命令。要删除路由类型条目，请使用此命 **no**令的形式。

**matchroute-type** {**local** | **internal** | {**external** [**type-1** | **type-2**] } | {**nssa-external** [**type-1** | **type-2**] } }
**no matchroute-type** {**local** | **internal** | {**external** [**type-1** | **type-2**] } | {**nssa-external** [**type-1** | **type-2**] } }

## Syntax Description

| | |
|---|---|
| **external** | OSPF 外部路由或 EIGRP 外部路由。 |
| **internal** | OSPF区域内和区域间路由或EIGRP内部路由。 |
| **local** | 本地生成的 BGP 路由。 |
| **nssa-external** | 指定外部 NSSA。 |
| **type-1** | （可选）指定路由类型 1。 |
| **type-2** | （可选）指定路由类型 2。 |

## Command Default

此命令默认禁用。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 路由映射配置 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |
| 9.0(1) | 增加了多情景模式支持。 |

## 使用指南

通过**route-map**使用 全局配置命令以及 **match** 和 **set**配置命令，您可以定义将路由从一个路由协议重新分发到另一个路由协议的条件。每个 **route-map** 命令都有 **match** 和 **set** 命令与其关联。 **match** 命令指定匹配条件 - 当前 **route-map** 命令允许重新分发的条件。 **set** 命令指定 set 操作 - 当满足 **match** 命令执行的条件时要执行的特定重新分发操作。 **noroute-map** 命令可删除路由映射。

**match**route-map 配置命令具有多种格式。您可以按任何顺序输入 **match** 命令。所有 **match** 命令都必须“通过”，才能根据 **set** 命令给定的 set 操作重新分发路由。命令的 **nomatch** 形式可删除指定的匹配条件。

路由映射可包含多个部分。任何与 **route-map** 命令相关的至少一个 match 子句不匹配的路由都将被忽略。要仅修改部分数据，您必须配置第二个路由映射部分并指定显式匹配。

对于 OSPF， **externaltype-1** 关键字仅匹配 1 类外部路由， **externaltype-2** 关键字仅匹配 2 类外部路由。

## CR_Examples

以下示例显示如何重新分配内部路由：

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match route-type internal
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **matchinterface** | 分发任何下一跳位于指定接口之一的路由， |
| **matchipnext-hop** | 分配任何具有由指定的访问列表之一传递的下一跳路由器地址的路由。 |
| **matchmetric** | 根据指定的度量重新分配路由。 |
| **route-map** | 定义将路由从一个路由协议重新分发到另一个路由协议的条件。 |
| **setmetric** | 为路由映射指定目标路由协议中的指标值。 |

# match rtp

如要在类映射中指定偶数端口的 UDP 端口范围，请在 class-map 配置模式下使用 **matchrtp**命令。要删除此规范，请使用此 **no**命令的形式。

**matchrtp***starting_port*范围
**nomatchrtp***starting_port*范围

## Syntax Description

| | |
|---|---|
| 起始端口 | 指定偶数UDP目标端口的下限。范围为2000-65535 |
| *range* | 指定 RTP 端口范围。范围是 0-16383。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 类映射配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |

## 使用指南

**match** 命令用于标识类映射的流量类中包含的流量。它们包括用于定义类映射中包含的流量的不同条件。在使用模块化策略框架配置安全功能的过程中，使用 **class-map** 全局配置命令定义流量类。在 class-map 配置模式下，可以使用 **match** 命令定义要包含在类中的流量。

流量类应用于接口之后，会将该接口上接收的数据包与类映射中的**match**语句定义的条件进行比较。如果数据包符合指定的条件，则会包含在该流量类中，并且会承担与该流量类关联的所有操作。不匹配任何流量类别中的任何条件的数据包被分配到默认流量类别。

使用 **matchrtp** 命令匹配 RTP 端口（偶数 UDP 端口号介于 *starting_port* 与 *starting_port* 加上 范围）。

## CR_Examples

以下示例显示如何使用类映射和 **matchrtp**命令定义流量类：

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# matchrtp 20000 100
ciscoasa(config-cmap)#
```

**Related Commands**

| 命令 | 说明 |
| --- | --- |
| **class-map** | 将流量类应用于接口。 |
| **clearconfigureclass-map** | 删除所有流量映射定义。 |
| **matchaccess-list** | 识别类映射中的访问列表流量。 |
| **matchany** | 包括类映射中的所有流量。 |
| **showrunning-configclass-map** | 显示有关类映射配置的信息。 |

# match selection-mode

要为创建 PDP 情景请求中的选择模式信息元素配置匹配，请在策略映射配置模式下使用 **matchselection-mode**命令。要删除匹配条件，请使用此 **no**命令的形式。

**match** [**not**] **selection-mode**模式值
**nomatch** [**not**] **selection-mode**模式值

## Syntax Description

| | |
|---|---|
| 模式值 | 创建PDP上下文请求中的选择模式信息元素。选择模式指定消息中的无线接入点名称(APN)来源，可以是以下项目之一。<br>• 0 - 已验证。由移动站点或网络提供 APN，并且已验证订用。<br>• 1 - 移动站点。由移动站点提供 APN，并且已验证订用。<br>• 2 - 网络。由网络提供 APN，并且已验证订用。<br>• 3 - 保留，未使用。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 策略映射配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.10(1) | 引入了此命令。 |

## 使用指南

可以在 GTP 策略映射中配置此命令。

您可以根据创建 PDP 上下文请求中的选择模式信息元素进行过滤。选择模式指定消息中接入点名称（APN）的来源。您可以根据这些模式丢弃和选择记录消息。选择模式过滤仅支持 GTPv1 和 GTPv2。

## CR_Examples

以下示例显示如何匹配选择模式 1 和 2，以及如何丢弃和记录采用这两种模式的创建 PDP 情景消息。

```
ciscoasa(config)# policy-map type inspect gtp gtp-map
```

```
ciscoasa(config-pmap)# match selection-mode 1
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap)# match selection-mode 2
ciscoasa(config-pmap-c)# drop log
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **drop** | 丢弃符合条件的数据包。 |
| **log** | 记录匹配条件的数据包。 |
| **inspectgtp** | 启用 GTP 应用检查。 |
| **policy-maptypeinspectgtp** | 创建或编辑 GTP 检查策略图。 |

# match sender-address

要配置 ESMTP 发件人邮件地址的匹配条件，请在策略映射配置模式下使用 **matchsender-address** 命令。要禁用此功能，请使用此**no**命令的形式。

**match** [**not**] **sender-address** [**lengthgt***bytes* | **regex***regex*]
**nomatch** [**not**] **sender-address** [**lengthgt***bytes* | **regex***regex*]

## Syntax Description

| | |
|---|---|
| **lengthgt***bytes* | 指定要匹配发件人邮件地址的长度。 |
| **regex***regex* | 指定匹配正则表达式。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 策略映射配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.2(1) | 添加了此命令。 |

## CR_Examples

以下示例显示如何在 ESMTP 检测策略映射中为长度超过 320 个字符的发件人邮件地址配置匹配条件：

```
ciscoasa(config-pmap)# match sender-address length gt 320
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **class-map** | 创建第 3/4 层类映射。 |
| **clearconfigureclass-map** | 删除所有类映射。 |
| **matchany** | 包括类映射中的所有流量。 |
| **matchport** | 标识类映射中的特定端口号。 |
| **showrunning-configclass-map** | 显示有关类映射配置的信息。 |

# match server

要配置 FTP 服务器的匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchserver** 命令。要删除匹配条件，请使用此 **no**命令的形式。

**match** [**not**] **serverregex** [*regex_name* | **class***regex_class_name*]
**no match** [**not**] **serverregex** [*regex_name* | **class***regex_class_name*]

## Syntax Description

| | |
|---|---|
| *regex_name* | 指定正则表达式。 |
| **class** *regex_class_name* | 指定正则表达式类映射。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 类映射或策略映射配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.2(1) | 添加了此命令。 |

## 使用指南

可以在 FTP 类映射或策略映射中配置此命令。一个 FTP 类映射中只能输入一个条目。

ASA 使用连接到 FTP 服务器时登录提示上方显示的初始 220 服务器消息来匹配服务器名称。220 服务器消息可能包含多行。服务器匹配不基于通过 DNS 解析的服务器名称的 FQDN。

## CR_Examples

以下示例显示如何在 FTP 检测策略映射中配置 FTP 服务器的匹配条件：

```
ciscoasa(config-pmap)# match server class regex ftp-server
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **class-map** | 创建第 3/4 层类映射。 |
| **clearconfigureclass-map** | 删除所有类映射。 |

| 命令 | 说明 |
| --- | --- |
| **matchany** | 包括类映射中的所有流量。 |
| **matchport** | 标识类映射中的特定端口号。 |
| **showrunning-configclass-map** | 显示有关类映射配置的信息。 |

# match service

要为特定即时消息服务配置匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchservice** 命令。要删除匹配条件，请使用此 **no**命令的形式。

**match** [**not**] {**service** {**chat** | **file-transfer** | **games** | **voice-chat** | **webcam** | **conference**}
**no match** [**not**] {**service** {**chat** | **file-transfer** | **games** | **voice-chat** | **webcam** | **conference**}

## Syntax Description

| | |
|---|---|
| chat | 指定 来匹配即时消息聊天服务。 |
| file-transfer | 指定 来匹配即时消息文件传输服务。 |
| 游戏 | 指定 以匹配即时消息游戏服务。 |
| 语音聊天 | 指定 以匹配即时消息通话聊天服务。 |
| 网络摄像头 | 指定 以匹配即时消息网络摄像头服务。 |
| 会议 | 指定以匹配即时消息会议服务。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 类映射或策略映射配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.2(1) | 添加了此命令。 |

## 使用指南

可以在 IM 类映射或策略映射中配置此命令。一个 IM 类映射中只能输入一个条目。

## CR_Examples

以下示例显示如何在即时消息类映射中配置聊天服务的匹配条件：

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match service chat
```

**Related Commands**

| 命令 | 说明 |
|---|---|
| **class-map** | 创建第 3/4 层类映射。 |
| **clearconfigureclass-map** | 删除所有类映射。 |
| **matchany** | 包括类映射中的所有流量。 |
| **showrunning-configclass-map** | 显示有关类映射配置的信息。 |

# match service-indicator

要配置 M3UA 消息的服务指示符的匹配条件，请在策略映射配置模式下使用 **matchservice-indicator** 命令。要删除匹配条件，请使用此 **no**命令的形式。

**match** [ **not** ] **service-indicator***number*
**no match** [ **not** ] **service-indicator***number*

## Syntax Description

| | |
|---|---|
| *number* | 服务指示器编号，0-15。有关受支持的服务指示符列表，请参阅用量部分。 |

## Command Default

M3UA 检测允许所有服务指示符。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 策略映射配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.6(2) | 添加了此命令。 |

## 使用指南

您可以在 M3UA 检测策略映射中配置此命令。可以根据服务指标丢弃数据包。下面是可用的服务指示符。有关这些服务指示符的详细信息，请参阅 M3UA RFC 和文档。

- 0 - 信令网络管理消息
- 1 - 信令网络测试和维护消息
- 2 - 信令网络测试和维护特殊消息
- 3 - SCCP
- 4 - 电话用户部分
- 5 - ISDN 用户部分
- 6 - 数据用户部分（呼叫和电路相关消息）
- 7 - 数据用户部分（设备注册和取消消息）
- 8 - 预留用于 MTP 测试用户部分
- 9 - 宽带 ISDN 用户部分

- 10 - 卫星 ISDN 用户设备
- 11 - 预留
- 12 - AAL 第 2 类信令
- 13 - 承载独立呼叫控制
- 14 - 网关控制协议
- 15 - 预留

## CR_Examples

以下示例显示如何配置 M3UA 服务指示符的匹配条件。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# match service-indicator 15
ciscoasa(config-pmap-c)# drop
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **inspectm3ua** | 启用 M3UA 检测。 |
| **policy-maptypeinspect** | 创建检查策略映射。 |

# match third-party-registration

要为第三方注册请求者配置匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchthird-party-registration** 命令。要删除匹配条件，请使用此 **no**命令的形式。

**match** [**not**] **third-party-registrationregex** [*regex_name* | **class***regex_class_name*]
**no match** [**not**] **third-party-registrationregex** [*regex_name* | **class***regex_class_name*]

## Syntax Description

| | |
|---|---|
| *regex_name* | 指定正则表达式。 |
| **class** *regex_class_name* | 指定正则表达式类映射。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 类映射或策略映射配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.2(1) | 添加了此命令。 |

## 使用指南

可以在 SIP 类映射或策略映射中配置此命令。一个 SIP 类映射中只能输入一个条目。

third-party registration match 命令用于识别可使用 SIP 注册器或 SIP 代理注册其他用户的用户。在 From 和 To 值不匹配的情况下，可通过 REGISTER 消息中的 From 报头字段进行标识。

## CR_Examples

以下示例显示如何在 SIP 检测类映射中配置第三方注册的匹配条件：

```
ciscoasa(config-cmap)# match third-party-registration regex class sip_regist
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **class-map** | 创建第 3/4 层类映射。 |
| **clearconfigureclass-map** | 删除所有类映射。 |

| 命令 | 说明 |
| --- | --- |
| **matchany** | 包括类映射中的所有流量。 |
| **matchport** | 标识类映射中的特定端口号。 |
| **showrunning-configclass-map** | 显示有关类映射配置的信息。 |

# match tunnel-group

要匹配属于之前定义的隧道组的类映射中的流量，请在class-map配置模式下使用**matchtunnel-group**命令。要删除此规范，请使用此 **no**命令的形式。

**matchtunnel-group***name*
**nomatchtunnel-group***name*

## Syntax Description

*name* 隧道组名称的文本。

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 类映射配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |

## 使用指南

**match** 命令用于标识类映射的流量类中包含的流量。它们包括用于定义类映射中包含的流量的不同条件。在使用模块化策略框架配置安全功能的过程中，使用 **class-map** 全局配置命令定义流量类。在 class-map 配置模式下，可以使用 **match** 命令定义要包含在类中的流量。

流量类应用于接口之后，会将该接口上接收的数据包与类映射中的**match**语句定义的条件进行比较。如果数据包符合指定的条件，则会包含在该流量类中，并且会承担与该流量类关联的所有操作。不匹配任何流量类别中的任何条件的数据包被分配到默认流量类别。

要启用基于流的策略操作，请将 **matchflowipdestination-address** 和 **matchtunnel-group** 命令配合使用 **class-map**、 **policy-map**和 **service-policy** 命令。定义流的条件是目的 IP 地址。所有流向某唯一 IP 目标地址的流量都被视为流。策略操作应用于每个数据流，而不是整个流量类。QoS 操作策略使用 **police** 命令应用。使用**matchtunnel-group** 和 **matchflowipdestination-address** 会将隧道组中的每个隧道策略为指定的速率。

## CR_Examples

以下示例展示如何在隧道组内启用基于流的策略管制，并将每个隧道限制为指定的速率：

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# matchtunnel-group
```

```
ciscoasa(config-cmap)# match flow ip destination-address
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# police 56000
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy pmap global
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **class-map** | 将流量类应用于接口。 |
| **clearconfigureclass-map** | 删除所有流量映射定义。 |
| **matchaccess-list** | 识别类映射中的访问列表流量。 |
| **showrunning-configclass-map** | 显示有关类映射配置的信息。 |
| **tunnel-group** | 创建和管理 IPsec 和 L2TP 连接特定记录数据库，|

# match uri

要配置 SIP 报头中 URI 的匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchuri** 命令。要删除匹配条件，请使用此 **no**命令的形式。

**match** [**not**] **uri** {**sip** | **tel**} **lengthgt***gt_bytes*
**no match** [**not**] **uri** {**sip** | **tel**} **lengthgt***gt_bytes*

## Syntax Description

| | |
|---|---|
| **sip** | 指定 SIP URI。 |
| **tel** | 指定 TEL URI。 |
| **lengthgt***gt_bytes* | 指定 URI 的最大长度。值介于 0 和 65536 之间。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 类映射或策略映射配置 | • 是 | • 支持 | • 支持 | • 支持 | — • 是 |

## Command History

| 版本 | 修改 |
|---|---|
| 7.2(1) | 添加了此命令。 |

## 使用指南

可以在 SIP 类映射或策略映射中配置此命令。一个 SIP 类映射中只能输入一个条目。

## CR_Examples

以下示例展示如何为 SIP 消息中的 URI 配置匹配条件：

```
ciscoasa(config-cmap)# match uri sip length gt
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **class-map** | 创建第 3/4 层类映射。 |
| **clearconfigureclass-map** | 删除所有类映射。 |

| 命令 | 说明 |
| --- | --- |
| **matchany** | 包括类映射中的所有流量。 |
| **matchport** | 标识类映射中的特定端口号。 |
| **showrunning-configclass-map** | 显示有关类映射配置的信息。 |

# match url-filter

要配置 RTSP 消息中 URL 过滤的匹配条件，请在 class-map 或 policy-map 配置模式下使用 **matchurl-filter** 命令。要删除匹配条件，请使用此 **no**命令的形式。

**match** [**not**] **url-filterregex** [*regex_name* | **class***regex_class_name*]
**no match** [**not**] **url-filterregex** [*regex_name* | **class***regex_class_name*]

## Syntax Description

| | |
|---|---|
| *regex_name* | 指定正则表达式。 |
| **class** *regex_class_name* | 指定正则表达式类映射。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 类映射或策略映射配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 8.0(2) | 添加了此命令。 |

## 使用指南

可以在 RTSP 类映射或策略映射中配置此命令。

## CR_Examples

以下示例显示如何在 RTSP 检查策略映射中配置 URL 过滤的匹配条件：

```
ciscoasa(config)# regex badurl www.example.com/rtsp.avi
ciscoasa(config)# policy-map type inspect rtsp rtsp-map
ciscoasa(config-pmap)# match url-filter regex badurl
ciscoasa(config-pmap-p)# drop-connection
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **class-map** | 创建第 3/4 层类映射。 |
| **clearconfigureclass-map** | 删除所有类映射。 |

| 命令 | 说明 |
| --- | --- |
| **matchany** | 包括类映射中的所有流量。 |
| **matchport** | 标识类映射中的特定端口号。 |
| **showrunning-configclass-map** | 显示有关类映射配置的信息。 |

# match user group

如要指定云网络安全白名单中的用户或组，请在 class-map 配置模式下使用 **matchusergroup** 命令。要删除匹配，请使用此命 **no**令的形式。

用户名**match**[**not**]{[**user**][**group**组名]}
用户名**no match**[**not**]{[**user**][**group**组名]}

## Syntax Description

| | |
|---|---|
| **not** | （可选）指定应使用 Web 云安全过滤用户和/或组。例如，如果您将组“cisco”列入白名单，但想要扫描用户“johncrichton”和“aerynsun”的流量，则可以 **matchnot** 为这些用户指定。 |
| **user***username* | 将用户指定到白名单。 |
| **group***groupname* | 指定要白名单的组。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 类映射配置模式 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.0(1) | 添加了此命令。 |

## 使用指南

如果您使用 AAA 规则或 IDFW，则可以配置 ASA，以便来自特定用户或组的、与服务策略规则匹配的 Web 流量不会重定向到云 Web 安全代理服务器进行扫描。当绕过云网络安全扫描时，ASA 会直接从最初请求的 Web 服务器检索内容，而不联系代理服务器。当它收到 Web 服务器的响应时，它会将数据发送至客户端。此过程被称作将流量“列入白名单”。

虽然当您使用ACL配置发送到云网络安全的流量类别时，您可以实现基于用户或组豁免流量的相同结果，但您可能会发现使用白名单更为直接。请注意，白名单功能仅基于用户和组，而不基于 IP 地址。

在检测策略映射 (**policy-maptypeinspectscansafe**) 中创建白名单后，当您使用 **inspectscansafe**命令指定云网络安全操作时，可以使用此映射。

## CR_Examples

以下示例将 HTTP 及 HTTPS 检测策略映射的相同用户和组加入白名单：

```
ciscoasa(config)# class-map type inspect scansafe match-any whitelist1
ciscoasa(config-cmap)# match user user1 group cisco
ciscoasa(config-cmap)# match user user2
ciscoasa(config-cmap)# match group group1
ciscoasa(config-cmap)# match user user3 group group3
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default group default_group
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap2
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# https
ciscoasa(config-pmap-p)# default group2 default_group2
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **class-maptypeinspectscansafe** | 为加入白名单的用户和组创建检查类映射。 |
| **inspectscansafe** | 对类中的流量启用云网络安全检查。 |
| **matchusergroup** | 匹配白名单的用户或组。 |
| **policy-maptypeinspectscansafe** | 创建检查策略映射，以便配置重要的规则参数并选择性地标识白名单。 |
| **whitelist** | 对流量类执行白名单操作。 |

# match username

要配置FTP用户名的匹配条件，请在class-map或policy-map配置模式下使用 **matchusername** 命令。要删除匹配条件，请使用此**no**命令的形式。

**match** [**not**] **usernameregex** [*regex_name* | **class***regex_class_name*]
**no match** [**not**] **usernameregex** [*regex_name* | **class***regex_class_name*]

## Syntax Description

| | |
|---|---|
| *regex_name* | 指定正则表达式。 |
| **class** *regex_class_name* | 指定正则表达式类映射。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 类映射或策略映射配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.2(1) | 添加了此命令。 |

## 使用指南

可以在 FTP 类映射或策略映射中配置此命令。一个 FTP 类映射中只能输入一个条目。

## CR_Examples

以下示例显示如何在 FTP 检测类映射中配置 FTP 用户名的匹配条件：

```
ciscoasa(config)# class-map type inspect ftp match-all ftp_class1
ciscoasa(config-cmap)# match username regex class ftp_regex_user
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **class-map** | 创建第 3/4 层类映射。 |
| **clearconfigureclass-map** | 删除所有类映射。 |
| **matchany** | 包括类映射中的所有流量。 |

| 命令 | 说明 |
| --- | --- |
| **matchport** | 标识类映射中的特定端口号。 |
| **showrunning-configclass-map** | 显示有关类映射配置的信息。 |

# match uuid

要配置 DCERPC 消息的通用唯一标识符 (UUID) 的匹配条件，请在类映射或策略映射配置模式下使用 **matchuuid** 命令。要删除匹配条件，请使用此 **no**命令的形式。

**match** [**not**] **uuid***type*
**nomatch** [**not**] **uuid***type*

## Syntax Description

*type* 要匹配的 UUID 类型。以下项之一：

- **ms-rpc-epm**- 匹配 Microsoft RPC EPM 消息。
- **ms-rpc-isystemactivator**- 匹配 ISystemMapper 消息。
- **ms-rpc-oxidresolver**- 匹配 OxidResolver 消息。

## Command Default

DCERPC 检测允许所有消息类型。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 类映射或策略映射配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.5(2) | 添加了此命令。 |

## 使用指南

可以在 DCERPC 检测类映射或策略映射中配置此命令。使用它可根据 DCERPC UUID 过滤流量。然后，可以重置或记录匹配的流量。

## CR_Examples

以下示例显示如何为 DCERPC 消息中的 ms-rpc-isiustemactivator UUID 配置匹配条件：

```
ciscoasa(config)# class-map type inspect dcerpc dcerpc-cmap

ciscoasa(config-cmap)# match uuid ms-rpc-isystemactivator
```

**Related Commands**

| 命令 | 说明 |
| --- | --- |
| **class-maptypeinspect** | 创建检查类别图。 |
| **policy-maptypeinspect** | 创建检查策略映射。 |

# match version

要在 GTP 检测中配置 GTP 版本的匹配条件，请在策略映射配置模式下使用 **matchversion**命令。要删除匹配条件，请使用此 **no**命令的形式。

**match** [**not**] **version** [*version_idlower_rangeupper_range* | **range**]
**no match** [**not**] **version** [*version_idlower_rangeupper_range* | **range**]

## Syntax Description

| | |
|---|---|
| *version_id* | 指定介于 0 和 255 之间的版本。 |
| **range***lower_range upper_range* | 指定版本的下限和上限范围。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 策略映射配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.2(1) | 添加了此命令。 |

## 使用指南

可以在 GTP 策略映射中配置此命令。

## CR_Examples

以下示例显示如何为 GTP 检测策略映射中的消息版本配置匹配条件：

```
ciscoasa(config-pmap)# match version 1
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **inspectgtp** | 配置 GTP 流量检测。 |

# max-area-addresses

要为 IS-IS 区域配置其他手动地址，请在路由器 isis 配置模式下使用 **max-area-addresses** 命令。要禁用手动地址，请使用此命 **no**令的形式。

**max-area-addresses** 编号
**no max-area-addresses** *number*

## Syntax Description

| | |
|---|---|
| *number* | 要添加的手动地址数量。范围是 3 到 234。 |

## Command Default

没有为 IS-IS 区域配置手动地址。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 路由器配置 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.6(1) | 添加了此命令。 |

## 使用指南

此命令使您可以通过配置其他手动地址来最大化 IS-IS 区域的大小。您指定要添加的地址数，并分配一个 NET 地址来创建每个手动地址。

## CR_Examples

以下示例配置三个地址：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# max-are-addreses 3
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **advertise passive-only** | 配置 ASA 以通告被动接口。 |
| **area-password** | 配置 IS-IS 区域身份验证密码。 |
| **authentication key** | 全局启用 IS-IS 身份验证。 |
| **authentication mode** | 指定IS-IS实例全局使用的IS-IS报文认证方式。 |

| 命令 | 说明 |
| --- | --- |
| **authentication send-only** | 全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。 |
| **clear isis** | 清除 IS-IS 数据结构。 |
| default-information originate | 在 IS-IS 路由域中生成默认路由。 |
| **distance** | 定义分配给 IS-IS 协议发现的路由的管理距离。 |
| **domain-password** | 配置 IS-IS 域身份验证密码。 |
| **fast-flood** | 将 IS-IS LSP 配置为完整的。 |
| **hello padding** | 将 IS-IS hello 配置为完整 MTU 大小。 |
| **hostname dynamic** | 启用 IS-IS 动态主机名功能。 |
| **ignore-lsp-errors** | 配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。 |
| **isis adjacency-filter** | 过滤 IS-IS 邻接关系的建立。 |
| **isis advertise-prefix** | 在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。 |
| **isis authentication key** | 启用接口的身份验证。 |
| **isis authentication mode** | 指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型 |
| **isis authentication send-only** | 配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。 |
| **isis circuit-type** | 配置用于 IS-IS 的邻接类型。 |
| **isis csnp-interval** | 配置在广播接口上发送周期性 CSNP 数据包的间隔。 |
| **isis hello-interval** | 指定 IS-IS 发送的连续 hello 数据包之间的时间长度。 |
| **isis hello-multiplier** | 指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。 |
| **isis hello padding** | 将 IS-IS hello 配置为每个接口的完整 MTU 大小。 |
| **isis lsp-interval** | 配置每个接口连续 IS-IS LSP 传输之间的时间延迟。 |
| **isis metric** | 配置 IS-IS 度量的值。 |
| **isis password** | 配置接口的认证密码。EXTEN |
| **isis priority** | 配置接口上指定 ASA 的优先级。 |

| 命令 | 说明 |
| --- | --- |
| **isis protocol shutdown** | 禁用每个接口的 IS-IS 协议。 |
| **isis retransmit-interval** | 配置接口上每个 IS-IS LSP 重新传输之间的时间量。 |
| **isis retransmit-throttle-interval** | 配置接口上每个 IS-IS LSP 重新传输之间的时间量。 |
| **isis tag** | 当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。 |
| **is-type** | 为 IS-IS 路由进程分配路由级别。 |
| **log-adjacency-changes** | 使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。 |
| **lsp-full suppress** | 配置当 PDU 已满时哪些路由会被抑制。 |
| **lsp-gen-interval** | 定制 IS-IS 对 LSP 生成的限制。 |
| **lsp-refresh-interval** | 设置LSP刷新间隔。 |
| **max-area-addresses** | 为 IS-IS 区域配置额外的手动地址。 |
| **max-lsp-lifetime** | 设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。 |
| **maximum-paths** | 为 IS-IS 配置多路径负载共享。 |
| **metric** | 全局更改所有 IS-IS 接口的度量值。 |
| **metric-style** | 配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。 |
| **net** | 指定路由过程的NET。 |
| **passive-interface** | 配置被动接口。 |
| **prc-interval** | 定制 PRC 的 IS-IS 限制。 |
| **protocol shutdown** | 全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。 |
| **redistribute isis** | 将 IS-IS 路由从第 1 级重新分配到第 2 级或从第 2 级重新分配到第 1 级。 |
| **route priority high** | 为 IS-IS IP 前缀分配高优先级。 |
| **router isis** | 启用 IS-IS 路由。 |
| **set-attached-bit** | 指定第 1 级至第 2 级路由器应设置其附加位的约束。 |
| **set-overload-bit** | 配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。 |

| 命令 | 说明 |
| --- | --- |
| **show clns** | 显示 CLNS 特定信息。 |
| **show isis** | 显示 IS-IS 信息。 |
| **show route isis** | 显示 IS-IS 路由。 |
| **spf-interval** | 自定义 IS-IS 对 SPF 计算的限制。 |
| **summary-address** | 为 IS-IS 创建聚合地址。 |

# max-failed-attempts

要指定服务器组中的任何给定服务器在停用之前允许该服务器执行的失败AAA事务数，请在aaa-server组配置模式下使用 **max-failed-attempts** 命令。要删除此规范并恢复为默认值，请使用此命令的 **no**形式。

**max-failed-attempts**编号
**nomax-failed-attempts**

## Syntax Description

| | |
|---|---|
| *number* | 1-5 范围内的整数，用于指定之前 **aaa-server** 命令中指定的服务器组中的任何给定服务器允许的失败 AAA 事务数。 |

## Command Default

*number* 的默认值为 3。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| aaa-server group 配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |

## 使用指南

必须已配置 AAA 服务器或组，才能发出此命令。

## CR_Examples

```
ciscoasa
(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa
(config-aaa-server-group)# max-failed-attempts 4
ciscoasa
(config-aaa-server-group)#
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **aaa-server***server-tag***protocol***protocol* | 进入 aaa 服务器组配置模式，以便您可以配置特定于组且对组内所有主机通用的 AAA 服务器参数。 |
| **clearconfigureaaa-server** | 删除所有 AAA 服务器配置。 |

| 命令 | 说明 |
| --- | --- |
| **showrunning-configaaa** | 显示所有 AAA 服务器、特定服务器组、特定组中的特定服务器或特定协议的 AAA 服务器统计信息。 |

# max-forwards-validation

要启用对 Max-forwards 报头字段是否为 0 的检查，请在参数配置模式下使用 **max-forwards-validation** 命令。参数配置模式可从策略映射配置模式访问。要禁用此功能，请使用此**no** 命令的形式。

**max-forwards-validation action** {**drop** | **drop-connection** | **reset** | **log**} [**log**]
**no max-forwards-validation action** {**drop** | **drop-connection** | **reset** | **log**} [**log**]

## Syntax Description

| | |
|---|---|
| **drop** | 如果进行验证，则丢弃数据包。 |
| **drop-connection** | 发生违规时丢弃连接。 |
| **reset** | 发生违规时重置连接。 |
| **log** | 指定违规情况下的独立或附加日志。可将其与任何 操作相关联。 |

## Command Default

此命令默认禁用。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 参数配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.2(1) | 添加了此命令。 |

## 使用指南

此命令计算到目标的跳数，在到达目标之前目标不能为 0。

## CR_Examples

以下示例显示如何在 SIP 检查策略映射中启用最大转发验证：

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# max-forwards-validation action log
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **class** | 在策略映射中标识类映射名称。 |

| 命令 | 说明 |
| --- | --- |
| **class-maptypeinspect** | 创建检查类映射以匹配特定于应用的流量。 |
| **policy-map** | 创建第 3/4 层策略映射。 |
| **showrunning-configpolicy-map** | 显示所有当前的策略映射配置。 |

# max-header-length

要根据 HTTP 标头长度限制 HTTP 流量，请在 **max-header-length**HTTP 映射配置模式下使用该命令，可以使用该 **http-map**命令访问。要删除此命令，请使用此命 **no**令的形式。

**max-header-length**{**request**字节数 字节[**response**数]|**response**字节数}**action**{**allow**|**reset**|**drop**}[**log**]
**no max-header-length**{**request**字节数 字节[**response**数]|**response**字节数}**action**{**allow**|**reset**|**drop**}[**log**]

## Syntax Description

| | |
|---|---|
| **action** | 当邮件未通过此命令检查时采取的操作。 |
| **allow** | 允许消息。 |
| **drop** | 关闭连接。 |
| **bytes** | 字节数，范围为 1 到 65535。 |
| **log** | （可选）生成系统日志。 |
| **request** | 请求消息。 |
| **reset** | 向客户端和服务器发送 TCP 重置消息。 |
| **response** | （可选）响应消息。 |

## Command Default

此命令默认禁用。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| HTTP 映射配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |

## 使用指南

启用 max-header-length 命令后，ASA 仅允许 HTTP 报头在配置的限制范围内的消息，否则采取指定的操作。使用 **action** 关键字导致 ASA 重置 TCP 连接和创建系统日志条目（可选）。

## CR_Examples

以下示例将 HTTP 请求限制为 HTTP 报头长度不超过 100 个字节的请求。如果报头太大，ASA 将重置 TCP 连接并创建一个系统日志条目。

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# max-header-length request bytes 100 action log reset
ciscoasa(config-http-map)#
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **class-map** | 定义要应用的安全操作的流量类。 |
| **debugappfw** | 显示与增强型 HTTP 检查关联的流量详细信息。 |
| **http-map** | 为配置的增强型 HTTP 检查定义 HTTP 映射。 |
| **inspecthttp** | 应用要用于应用检查的特定 HTTP 映射。 |
| **policy-map** | 将类映射与特定的安全操作相关联。 |

# max-lsp-lifetime

如要设置 LSP 可在不刷新的情况下保留在 ASA 数据库中的最长时间，请在路由器配置模式下使用 **max-lsp-lifetime** 命令。要恢复默认生存期，请使用此命 **no**令的形式。

**max-lsp-lifetime**秒
**nomax-lsp-lifetime**

## Syntax Description

| |
|---|
| 秒LSP 的生命周期（以秒为单位）。范围为 1 到 65535。 |

## Command Default

默认值为 1200 秒（20 分钟）。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 路由器配置 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.6(1) | 添加了此命令。 |

## 使用指南

如果在新 LSP 到达前超出有效期，该 LSP 将从数据库中删除。

如果使用 **lsp-refresh-interval** 命令更改了 LSP 刷新间隔，则可能需要调整最大 LSP 有效期。在 LSP 的有效期到期前，必须定期刷新 LSP。为 **lsp-refresh-interval** 命令设置的值应小于为 **max-lsp-lifetime** 命令设置的值；否则 LSP 将在刷新前超时。如果您错误地将 LSP 生存时间配置得与 LSP 刷新间隔相比太低，则软件会减少 LSP 刷新间隔以防止 LSP 超时。

您可能更愿意为每个 命令使用更高的值以减少控制流量，但这样做的代价是使来自崩溃或无法访问的路由器的过时 LSP 在数据库中保留的时间更长（从而浪费内存），或增加未检测到的不良 LSP 保持活动状态的风险（非常罕见）。

## CR_Examples

以下示例将 LSP 生存期配置为 40 分钟：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# max-lsp-lifetime 2400
```

**Related Commands**

| 命令 | 说明 |
|---|---|
| **advertisepassive-only** | 配置 ASA 以通告被动接口。 |
| **area-password** | 配置 IS-IS 区域身份验证密码。 |
| **authenticationkey** | 全局启用 IS-IS 身份验证。 |
| **authenticationmode** | 指定IS-IS实例全局使用的IS-IS报文认证方式。 |
| **authenticationsend-only** | 全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。 |
| **clearisis** | 清除 IS-IS 数据结构。 |
| default-information originate | 在 IS-IS 路由域中生成默认路由。 |
| **distance** | 定义分配给 IS-IS 协议发现的路由的管理距离。 |
| **domain-password** | 配置 IS-IS 域身份验证密码。 |
| **fast-flood** | 将 IS-IS LSP 配置为完整的。 |
| **hellopadding** | 将 IS-IS hello 配置为完整 MTU 大小。 |
| **hostnamedynamic** | 启用 IS-IS 动态主机名功能。 |
| **ignore-lsp-errors** | 配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。 |
| **isisadjacency-filter** | 过滤 IS-IS 邻接关系的建立。 |
| **isisadvertise-prefix** | 在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。 |
| **isisauthenticationkey** | 启用接口的身份验证。 |
| **isisauthenticationmode** | 指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型 |
| **isisauthenticationsend-only** | 配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。 |
| **isiscircuit-type** | 配置用于 IS-IS 的邻接类型。 |
| **isiscsnp-interval** | 配置在广播接口上发送周期性 CSNP 数据包的间隔。 |
| **isishello-interval** | 指定 IS-IS 发送的连续 hello 数据包之间的时间长度。 |
| **isishello-multiplier** | 指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。 |
| **isishellopadding** | 将 IS-IS hello 配置为每个接口的完整 MTU 大小。 |

| 命令 | 说明 |
| --- | --- |
| **isislsp-interval** | 配置每个接口连续 IS-IS LSP 传输之间的时间延迟。 |
| **isismetric** | 配置 IS-IS 度量的值。 |
| **isispassword** | 配置接口的认证密码。EXTEN |
| **isispriority** | 配置接口上指定 ASA 的优先级。 |
| **isisprotocolshutdown** | 禁用每个接口的 IS-IS 协议。 |
| **isisretransmit-interval** | 配置接口上每个 IS-IS LSP 重新传输之间的时间量。 |
| **isisretransmit-throttle-interval** | 配置接口上每个 IS-IS LSP 重新传输之间的时间量。 |
| **isistag** | 当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。 |
| **is-type** | 为 IS-IS 路由进程分配路由级别。 |
| **log-adjacency-changes** | 使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。 |
| **lsp-fullsuppress** | 配置当 PDU 已满时哪些路由会被抑制。 |
| **lsp-gen-interval** | 定制 IS-IS 对 LSP 生成的限制。 |
| **lsp-refresh-interval** | 设置LSP刷新间隔。 |
| **max-area-addresses** | 为 IS-IS 区域配置额外的手动地址。 |
| **max-lsp-lifetime** | 设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。 |
| **maximum-paths** | 为 IS-IS 配置多路径负载共享。 |
| **metric** | 全局更改所有 IS-IS 接口的度量值。 |
| **metric-style** | 配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。 |
| **net** | 指定路由过程的NET。 |
| **passive-interface** | 配置被动接口。 |
| **prc-interval** | 定制 PRC 的 IS-IS 限制。 |
| **protocolshutdown** | 全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。 |
| **redistributeisis** | 将 IS-IS 路由从第 1 级重新分配到第 2 级或从第 2 级重新分配到第 1 级。 |
| **routepriorityhigh** | 为 IS-IS IP 前缀分配高优先级。 |

| 命令 | 说明 |
| --- | --- |
| **routerisis** | 启用 IS-IS 路由。 |
| **set-attached-bit** | 指定第 1 级至第 2 级路由器应设置其附加位的约束。 |
| **set-overload-bit** | 配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。 |
| **showclns** | 显示 CLNS 特定信息。 |
| **showisis** | 显示 IS-IS 信息。 |
| **showrouteisis** | 显示 IS-IS 路由。 |
| **spf-interval** | 自定义 IS-IS 对 SPF 计算的限制。 |
| **summary-address** | 为 IS-IS 创建聚合地址。 |

# maximum-paths (BGP)

要控制可安装在路由表中的并行 BGP 路由的最大数量，请在 address-family 配置模式下使用 maximum-paths 命令。要恢复默认值，请使用此命令的 no 形式。

**maximum-paths** [**ibgp**] *number-of-paths*
**nomaximum-paths** [**ibgp**] *number-of-paths*

## Syntax Description

| | |
|---|---|
| **ibgp** | （可选）这将使您能够控制可以安装到路由表的内部 BGP 路由的最大数量。 |
| **number-of-paths** | 安装到路由表中的路由数。 |

## Command Default

默认情况下，BGP 仅在路由表中安装一个最佳路径。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| Address-family 配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |

## 使用指南

maximum-paths 命令用于为 BGP 对等会话配置等价或不等价多路径负载共享。要将路由安装为 BGP 路由表中的多路径，路由的下一跳不能与已安装的另一个路由相同。配置 BGP 多路径负载共享时，BGP 路由进程仍会通告到 BGP 对等成员的最佳路径。对于等价路由，来自路由器 ID 最小的相邻设备的路径被通告为最佳路径。

要配置 BGP 等价多路径负载共享，所有路径属性必须相同。路径属性包括权重、本地优先级、自治系统路径（整个属性，而不只是长度）、源代码，多出口标识符 (MED) 和内部网关协议 (IGP) 距离。

## CR_Examples

以下示例配置安装两个并行 iBGP 路径：

```
ciscoasa(config)# router bgp 3
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

**Related Commands**

| 命令 | 说明 |
| --- | --- |
| **showbgp** | 显示BGP路由表中的条目。 |

# maximum-paths (IS-IS)

要为 IS-IS 协议配置多路径负载共享，请在路由器 isis 配置模式下使用 **maximum-paths** 命令。要为 ISIS 路由禁用多路径负载共享，请使用此命令的 **no** 形式。

**maximum-paths***number-of-paths*
**nomaximum-paths***number-of-paths*

## Syntax Description

| | |
|---|---|
| *number-of-paths* | 要安装到路由表中的路由数。范围为 1 到 8。 |

## Command Default

默认情况下，IS-IS 仅在路由表中安装一个最佳路径。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 路由器配置 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.6(1) | 添加了此命令。 |

## 使用指南

当 ASA 中 **maximum-paths**配置了 ECMP 时，此命令用于配置 ISIS 多路径负载共享。

## CR_Examples

以下示例将路由表中的最大路径数配置为 8：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# maximum-paths 8
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **advertisepassive-only** | 配置 ASA 以通告被动接口。 |
| **area-password** | 配置 IS-IS 区域身份验证密码。 |
| **authenticationkey** | 全局启用 IS-IS 身份验证。 |
| **authenticationmode** | 指定IS-IS实例全局使用的IS-IS报文认证方式。 |

| 命令 | 说明 |
| --- | --- |
| **authenticationsend-only** | 全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。 |
| **clearisis** | 清除 IS-IS 数据结构。 |
| default-information originate | 在 IS-IS 路由域中生成默认路由。 |
| **distance** | 定义分配给 IS-IS 协议发现的路由的管理距离。 |
| **domain-password** | 配置 IS-IS 域身份验证密码。 |
| **fast-flood** | 将 IS-IS LSP 配置为完整的。 |
| **hellopadding** | 将 IS-IS hello 配置为完整 MTU 大小。 |
| **hostnamedynamic** | 启用 IS-IS 动态主机名功能。 |
| **ignore-lsp-errors** | 配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。 |
| **isisadjacency-filter** | 过滤 IS-IS 邻接关系的建立。 |
| **isisadvertise-prefix** | 在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。 |
| **isisauthenticationkey** | 启用接口的身份验证。 |
| **isisauthenticationmode** | 指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型 |
| **isisauthenticationsend-only** | 配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。 |
| **isiscircuit-type** | 配置用于 IS-IS 的邻接类型。 |
| **isiscsnp-interval** | 配置在广播接口上发送周期性 CSNP 数据包的间隔。 |
| **isishello-interval** | 指定 IS-IS 发送的连续 hello 数据包之间的时间长度。 |
| **isishello-multiplier** | 指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。 |
| **isishellopadding** | 将 IS-IS hello 配置为每个接口的完整 MTU 大小。 |
| **isislsp-interval** | 配置每个接口连续 IS-IS LSP 传输之间的时间延迟。 |
| **isismetric** | 配置 IS-IS 度量的值。 |
| **isispassword** | 配置接口的认证密码。EXTEN |
| **isispriority** | 配置接口上指定 ASA 的优先级。 |

| 命令 | 说明 |
| --- | --- |
| **isisprotocolshutdown** | 禁用每个接口的 IS-IS 协议。 |
| **isisretransmit-interval** | 配置接口上每个 IS-IS LSP 重新传输之间的时间量。 |
| **isisretransmit-throttle-interval** | 配置接口上每个 IS-IS LSP 重新传输之间的时间量。 |
| **isistag** | 当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。 |
| **is-type** | 为 IS-IS 路由进程分配路由级别。 |
| **log-adjacency-changes** | 使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。 |
| **lsp-fullsuppress** | 配置当 PDU 已满时哪些路由会被抑制。 |
| **lsp-gen-interval** | 定制 IS-IS 对 LSP 生成的限制。 |
| **lsp-refresh-interval** | 设置LSP刷新间隔。 |
| **max-area-addresses** | 为 IS-IS 区域配置额外的手动地址。 |
| **max-lsp-lifetime** | 设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。 |
| **maximum-paths** | 为 IS-IS 配置多路径负载共享。 |
| **metric** | 全局更改所有 IS-IS 接口的度量值。 |
| **metric-style** | 配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。 |
| **net** | 指定路由过程的NET。 |
| **passive-interface** | 配置被动接口。 |
| **prc-interval** | 定制 PRC 的 IS-IS 限制。 |
| **protocolshutdown** | 全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。 |
| **redistributeisis** | 将 IS-IS 路由从第 1 级重新分配到第 2 级或从第 2 级重新分配到第 1 级。 |
| **routepriorityhigh** | 为 IS-IS IP 前缀分配高优先级。 |
| **routerisis** | 启用 IS-IS 路由。 |
| **set-attached-bit** | 指定第 1 级至第 2 级路由器应设置其附加位的约束。 |
| **set-overload-bit** | 配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。 |

| 命令 | 说明 |
| --- | --- |
| **showclns** | 显示 CLNS 特定信息。 |
| **showisis** | 显示 IS-IS 信息。 |
| **showrouteisis** | 显示 IS-IS 路由。 |
| **spf-interval** | 自定义 IS-IS 对 SPF 计算的限制。 |
| **summary-address** | 为 IS-IS 创建聚合地址。 |

# max-object-size

要设置 ASA 可为 WebVPN 会话缓存的最大对象大小，请在缓存模式下使用 max-object-size 命令。要更改大小，请再次使用 命令。

**max-object-size**整数范围

## Syntax Description

| | |
|---|---|
| 整数范围 | 0 - 10000 KB |

## Command Default

1000 KB

## Command Modes

下表显示了输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| Cache mode | • 是 | — | • 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.1(1) | 添加了此命令。 |

## 使用指南

最大对象尺寸必须大于最小对象尺寸。如果已启用缓存压缩，ASA 会在压缩对象后计算大小。

## CR_Examples

以下示例显示如何将最大对象大小设置为 4000 KB：

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 cache
ciscoasa(config-webvpn-cache)# max-object-size4000
ciscoasa(config-webvpn-cache)#
```

## Related Commands

| 命令 | 说明 |
|---|---|
| cache | 进入 WebVPN 缓存模式。 |
| **cache-compressed** | 配置 WebVPN 缓存压缩。 |

| 命令 | 说明 |
| --- | --- |
| disable | 禁用缓存。 |
| **expiry-time** | 配置缓存对象的到期时间而不重新验证它们。 |
| **lmfactor** | 为仅具有最后修改时间戳的缓存对象设置重新验证策略。 |
| **min-object-size** | 定义要缓存的最小对象大小。 |

# 最大重试次数（已弃用）

注释 支持此命令的最后一个版本是版本 9.5(1)。

要配置ASA在让请求超时之前重试失败的SSO身份验证的次数，请在特定SSO服务器类型的webvpn配置模式下使用 **max-retry-attempts**命令。

要返回默认值，请使用此**no**命令形式。

**max-retry-attempts***retries*
**nomax-retry-attempts**

**Syntax Description**

| | |
|---|---|
| *retries* | ASA 重试失败的 SSO 身份验证的次数。重试次数范围为 1 到 5。 |

**Command Default**

此命令的默认值为 3。

**Command Modes**

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 类映射类型正则表达式配置 | • 是 | — | • 是 | — | — |
| config-webvpn-sso-siteminder | • 是 | — | • 是 | — | — |

**Command History**

| 版本 | 修改 |
|---|---|
| 7.1(1) | 添加了此命令。 |
| 9.5(2) | 为了支持 SAML 2.0，此命令已弃用。 |

使用指南

单点登录支持，仅供 WebVPN 使用，可让用户能够访问不同服务器不同安全服务，无需多次输入用户名和密码。ASA 目前支持 SiteMinder 类型的 SSO 服务器和 SAML POST 类型的 SSO 服务器。

此命令适用于这两种类型的 SSO 服务器。

将 ASA 配置为支持 SSO 身份验证后，您可以选择调整以下两个超时参数：

- ASA 重试 SSO 身份验证尝试失败的次数。 **max-retry-attemptscommand.**
- SSO 身份验证尝试失败之前的超时秒数（参见 **request-timeout** 命令）。

## CR_Examples

以下示例在 webvpn-sso-siteminder 配置模式下为名为 my-sso-server 的 SiteMinder SSO 服务器配置四次身份验证重试：

```
ciscoasa(config-webvpn)# sso-server my-sso-server type siteminder
ciscoasa(config-webvpn-sso-siteminder)#max-retry-attempts 4
ciscoasa(config-webvpn-sso-siteminder)#
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **policy-server-secret** | 创建密钥用于加密身份验证请求到 SiteMinder SSO 服务器。 |
| **request-timeout** | 指定失败的 SSO 身份验证尝试超时之前的秒数。 |
| **showwebvpnsso-server** | 显示在安全设备上配置的所有 SSO 服务器的运行统计信息。 |
| **sso-server** | 创建单点登录服务器。 |
| **web-agent-url** | 指定 ASA 向其发出 SiteMinder SSO 身份验证请求的 SSO 服务器 URL。 |

# max-uri-length

要根据 HTTP 请求消息中 URI 的长度限制 HTTP 流量，请在 HTTP 映射配置模式下使用 **max-uri-length** 命令。此模式可使用 **http-map** 命令访问。要删除此命令，请使用此命 **no**令的形式。

**max-uri-length***bytes***action** { **allow** | **reset** | **drop** } [ **log** ]
**no max-uri-length***bytes***action** { **allow** | **reset** | **drop** } [ **log** ]

## Syntax Description

| | |
|---|---|
| **action** | 当邮件未通过此命令检查时采取的操作。 |
| **allow** | 允许消息。 |
| **drop** | 关闭连接。 |
| **bytes** | 字节数，范围为 1 到 65535。 |
| **log** | （可选）生成系统日志。 |
| **reset** | 向客户端和服务器发送 TCP 重置消息。 |

## Command Default

此命令默认禁用。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| HTTP 映射配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |

## 使用指南

启用 max-uri-length 命令后，ASA 仅允许 URI 在配置的限制范围内的消息，否则执行指定的操作。使用 **action** 关键字导致 ASA 重置 TCP 连接并创建系统日志条目。

允许使用长度小于或等于配置值的 URI。否则，将执行指定的操作。

## CR_Examples

以下示例将 HTTP 请求限制为 URI 不超过 100 个字节的请求。如果 URI 太大，ASA 将重置 TCP 连接并创建一个系统日志条目。

```
ciscoasa(config)# http-map inbound_http
```

```
ciscoasa(config-http-map)# max-uri-length 100 action reset log
ciscoasa(config-http-map)#
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **class-map** | 定义要应用的安全操作的流量类。 |
| **debugappfw** | 显示与增强型 HTTP 检查关联的流量详细信息。 |
| **http-map** | 为配置的增强型 HTTP 检查定义 HTTP 映射。 |
| **inspecthttp** | 应用要用于应用检查的特定 HTTP 映射。 |
| **policy-map** | 将类映射与特定的安全操作相关联。 |

# mcast-group

要为 VXLAN VNI 接口指定组播组，请在接口配置模式下使用 **mcast-group** 命令。要删除该组，请使用此命 **no**令的形式。

**mcast-group***mcast_ip*
**nomcast-group**

## Syntax Description

| | |
|---|---|
| *mcast_ip* | 设置多播组IP地址，IPv4 或IPv6。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 接口配置 | • 是 | • 支持 | • 支持 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.4(1) | 添加了此命令。 |
| 9.20(1) | 此命令现在支持 IPv6。 |

## 使用指南

ASA 向对等体 VTEP 后的设备发送数据包时，ASA 需要两条重要信息：

- 远程设备的目标 MAC 地址
- 对等体 VTEP 的目标 IP 地址

ASA 可以通过两种方式找到这些信息：

- 单个对等体 VTEP IP 地址可以在 ASA 上静态配置。

无法手动定义多个对等体。

然后，ASA 将向 VTEP 发送一条 VXLAN 封装的 ARP 广播，以了解结束节点 MAC 地址。

- 可以使用该命令在每个 VNI 接口上（或在**mcast-group**整个 VTEP 上）配置多播组。

ASA 将通过 VTEP 源接口在 IP 组播数据包内发送一个 VXLAN 封装的 ARP 广播数据包。对此 ARP 请求的响应使 ASA 可以获悉远程 VTEP IP 地址以及远程结束节点的目标 MAC 地址。

ASA 维护目标 MAC 地址到 VNI 接口的远程 VTEP IP 地址的映射。

如果没有为 VNI 接口设置多播组，则使用 VTEP 源接口配置中的默认组（如果可用）（**default-mcast-group**命令）。如果使用该命令为 VTEP 源接口手动设置 VTEP 对 **peerip**等 IP，则无法为 VNI 接口指定多播组。多情景模式下不支持组播。

## CR_Examples

以下示例配置 VNI 1 接口并指定组播组 236.0.0.100：

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **debugvxlan** | 调试 VXLAN 流量。 |
| **default-mcast-group** | 为与 VTEP 源接口关联的所有 VNI 接口指定默认组播组。 |
| **encapsulationvxlan** | 将 NVE 实例设置为 VXLAN 封装。 |
| **inspectvxlan** | 强制遵守标准 VXLAN 报头格式。 |
| **interfacevni** | 创建用于 VXLAN 标记的 VNI 接口。 |
| **mcast-group** | 为 VNI 接口设置组播组地址。 |
| **nve** | 指定网络虚拟化终端实例。 |
| nve-only | 将 VXLAN 源接口指定为仅限 NVE。 |
| **peerip** | 手动指定对等 VTEP IP 地址。 |
| **segment-id** | 指定 VNI 接口的 VXLAN 网段 ID。 |
| **showarpvtep-mapping** | 显示 VNI 接口上缓存的与远程网段域中的 IP 地址和远程 VTEP IP 地址对应的 MAC 地址。 |
| **showinterfacevni** | 显示 VNI 接口的参数、状态和统计信息，其桥接接口（如果已配置）的状态，以及与其关联的 NVE 接口。 |
| **showmac-address-tablevtep-mapping** | 使用远程 VTEP IP 地址在 VNI 接口上显示第 2 层转发表（MAC 地址表）。 |

| 命令 | 说明 |
| --- | --- |
| **shownve** | 显示 NVE 接口的参数、状态和统计信息，其载频接口（源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。 |
| **showvnivlan-mapping** | 显示透明模式下的 VNI 网段 ID 与 VLAN 接口或物理接口之间的映射。 |
| **source-interface** | 指定 VTEP 源接口。 |
| **vtep-nve** | 将 VNI 接口与 VTEP 源接口相关联。 |
| **vxlanport** | 设置 VXLAN UDP 端口。默认情况下，VTEP 源接口接收发往 UDP 端口 4789 的 VXLAN 流量。 |

# mcc

要在 GTP 检测中标识用于 IMSI 前缀过滤的移动国家/地区代码和移动网络代码，请在策略映射参数配置模式下使用 **mcc** 命令。要删除配置，请使用此命令的 no 形式。

［**drop**］ **mcc***country_code***mnc***network_code*
**no** ［**drop**］ **mcc***country_code***mnc***network_code*

## Syntax Description

| | |
|---|---|
| **drop** | 指定应丢弃与前缀组合匹配的连接。因此，组合将指示不需要的前缀。<br>如果没有此关键字，连接必须与允许的前缀组合匹配。<br>给定映射中的所有前缀过滤都必须一致，要么全部丢弃，要么全部允许。 |
| *country_code* | 非零的三位数值，用于标识移动国家/地区。一位数或两位数条目将添加0前缀以创建三位数值。 |
| *network_code* | 标识网络代码的两位或三位数值。 |

## Command Default

默认情况下，GTP 检查不会检查有效的 MCC/MNC 组合。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 参数配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |
| 9.16（1） | 添加了 **drop** 关键字。 |

## 使用指南

您可以根据需要多次输入命令，以指定所有目标 MCC/MNC 对，但策略映射中的所有命令都必须是 **mcc** 或 **drop mcc**。这些命令不能组合使用。

默认情况下，GTP 检测不检查移动国家/地区代码 (MCC)/移动网络代码 (MNC) 组合的有效性。如果配置 IMSI 前缀过滤，接收到的数据包 IMSI 中的 MCC 和 MNC 将会与配置的 MCC/MNC 组合进行比较。然后，系统会根据命令采取以下行动之一：

- **mcc** 命令 - 如果数据包不匹配，则丢弃该数据包。
- **drop mcc** 命令 - 如果数据包匹配，则将其丢弃。

移动设备国家/地区代码是非零的三位数值；应在一位或两位数值前添加零作为前缀。移动网络代码是两位或三位数值。

添加您希望允许或放弃的所有 MCC 和 MNC 组合。默认情况下，ASA 不会检查 MNC 和 MCC 组合的有效性，所以您必须验证配置组合的有效性。有关 MCC 和 MNC 代码的详细信息，请参阅 ITU E.212 建议《*Identification Plan for Land Mobile Stations*》（陆地移动站识别计划）。

## CR_Examples

以下示例标识需要 MCC 为 111 且 MNC 为 222 的 IMSI 前缀过滤的流量：

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mcc 111 mnc 222
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **clearservice-policyinspectgtp** | 将清除全局 GTP 统计数据。 |
| **inspectgtp** | 适用于特定的GTP映射，以用于应用检查。 |
| **showservice-policyinspectgtp** | 显示 GTP 配置。 |

# media-termination (已弃用)

要指定用于至电话代理功能的媒体连接的媒体终止实例，请在电话代理配置模式下使用**media-termination**命令。

要从电话代理配置中删除媒体终止地址，请使用此命令的 **no**形式。

*media-terminationinstance_name*
**nomedia-termination***instance_name*

## Syntax Description

*instance_name* 指定使用介质终端地址的接口名称。每个接口只能配置一个媒体终止地址。

## Command Default

此命令没有默认设置。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 电话代理配置 | • 是 | — | • 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 8.0(4) | 命令已添加。 |
| 8.2(1) | 此命令已更新，以允许使用具有媒体终止地址的 NAT。**rtp-min-port** 和 **rtp-max-ports** 关键字已从命令语法中删除，并作为单独的命令包含在内。 |
| 9.4(1) | 此命令与所 **phone-proxy**有模式命令一起已被弃用。 |

## 使用指南

ASA 必须具有符合以下条件的媒体终端 IP 地址：

对于媒体终止实例，您可以为所有接口配置全局媒体终止地址，或为不同接口配置媒体终止地址。但是，不能同时使用全局媒体终止地址和为每个接口配置的媒体终止地址。

如果为多个接口配置媒体终端地址，则必须在 ASA 与 IP 电话通信时使用的每个接口上配置地址。

IP 地址是公开的可路由地址，并且是该接口上的地址范围内未使用的 IP 地址。

请参阅《CLI 配置指南》，查看在创建介质终止实例和配置介质终止地址时必须遵循的完整前提条件列表。

## CR_Examples

以下示例显示使用 media-termination address 命令来指定用于媒体连接的 IP 地址：

```
ciscoasa(config-phone-proxy)# media-termination mta_instance1
```

**Related Commands**

| 命令 | 说明 |
| --- | --- |
| **phone-proxy** | 配置电话代理实例。 |

# media-type

要将介质类型设置为铜缆或千兆光纤以太网，请在接口配置模式下使用 **media-type** 命令。光纤 SFP 连接器在 ASA 5500 系列自适应安全设备的 4GE SSM 上可用。要将媒体类型设置恢复为默认值，请使用此命令的 **no**形式。

**media-type** { **rj45** | **sfp** }
**nomedia-type** [ **rj45** | **sfp** ]

## Syntax Description

| | |
|---|---|
| **rj45** | （默认）将介质类型设置为铜RJ-45连接器。 |
| **sfp** | 将介质类型设置为光纤 SFP 连接器。 |

## Command Default

默认值为 **rj45**。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 接口配置 | • 是 | • 支持 | • 支持 | — | • 是 |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(4) | 添加了此命令。 |

## 使用指南

**sfp** 设置使用固定速度 (1000 Mbps)，因此 **speed** 命令允许您设置接口是否协商链路参数。不支持该 **duplex**命令。 **sfp**

## CR_Examples

以下示例将介质类型设置为 SFP：

```
ciscoasa(config)# interface gigabitethernet1/1
ciscoasa(config-if)# media-type sfp
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **interface** | 配置接口并进入接口配置模式。 |

| 命令 | 说明 |
| --- | --- |
| **showinterface** | 显示接口的运行时间状态和统计信息。 |
| **showrunning-configinterface** | 显示接口配置。 |
| **speed** | 设置接口速度。 |

# member

要将情景分配给资源类，请在情景配置模式下使用 **member** 命令。要从类中删除上下文，请使用此命 **no**令的形式。

**member***class_name*
**nomember***class_name*

## Syntax Description

| | |
|---|---|
| *class_name* | 指定使用 **class** 命令创建的类名称。 |

## Command Default

默认情况下，系统会将情景分配给默认类。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 上下文配置 | • 是 | • 支持 | — | — | • 是 |

## Command History

| 版本 | 修改 |
|---|---|
| 7.2(1) | 添加了此命令。 |

## 使用指南

默认情况下，所有安全上下文都可以无限制地访问ASA的资源，除非强制执行每个上下文的最大限制。但是，如果您发现一个或多个上下文使用了太多资源，并且导致其他上下文被拒绝连接，那么您可以配置资源管理来限制每个上下文的资源使用。ASA 通过向资源类分配情景来管理资源。每个情景使用由类设置的资源限制。

## CR_Examples

以下示例将情景 test 分配到 gold 类：

```
ciscoasa(config-ctx)# contexttest
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-urlftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold
```

## Related Commands

| 命令 | 说明 |
|---|---|
| class | 创建资源类。 |

| 命令 | 说明 |
| --- | --- |
| context | 配置安全上下文。 |
| limit-resource | 设置资源的限制。 |
| 显示资源分配 | 显示如何跨类分配资源。 |
| show resource types | 显示您可以设置限制的资源类型。 |

# member-interface

要将物理接口分配给冗余接口，请在接口配置模式下使用 **member-interface**命令。此命令仅适用于冗余接口类型。您可以向冗余接口分配两个成员接口。要删除成员接口，请使用此命 **no**令的形式。您不能从冗余接口中同时删除两个成员接口；冗余接口至少需要一个成员接口。

**member-interface***physical_interface*
**nomember-interface***physical_interface*

## Syntax Description

| | |
|---|---|
| *physical_interface* | 标识接口ID，例如。 **gigabitethernet0/1** 有关接受的值，请参阅 **interface** 命令。两个成员接口均必须为相同的物理类型。 |

## Command Default

没有默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 接口配置 | • 是 | • 支持 | • 支持 | — | • 是 |

## Command History

| 版本 | 修改 |
|---|---|
| 8.0(2) | 添加了此命令。 |

## 使用指南

两个成员接口均必须为相同的物理类型。例如，二者都必须是以太网接口。

如果已为物理接口配置了名称，则不能将该物理接口添加到冗余接口。您必须先使用 **nonameif** 命令删除名称。

⚠

**注意** 如果使用的是配置中已有的物理接口，则删除名称将会清除引用该接口的任何配置。

对于属于冗余接口对的物理接口，唯一可用的配置是物理参数，例如 **speed** 和 **duplex** 命令、 **description** 命令和 **shutdown** 命令。还可以输入 **default** 和 **help**等运行时命令。

如果关闭主用接口，则备用接口变为主用接口。

要更改活动接口，请输入**redundant-interface** 命令。

冗余接口使用您添加的第一个物理接口的 MAC 地址。如果在配置中更改成员接口的顺序，则 MAC 地址会发生更改，以与当前最先列出的接口的 MAC 地址相匹配。或者，您可以为冗余接口分配一

个 MAC 地址，无论成员接口 MAC 地址如何，都会使用该 **mac-address** 地址（请参阅命令或命 **mac-addressauto** 令）。当活动接口故障转移到备用接口时，将保持相同的 MAC 地址，因此流量不会中断。

## CR_Examples

以下示例创建两个冗余接口：

```
ciscoasa(config)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# interface redundant 2
ciscoasa(config-if)# member-interface gigabitethernet 0/2
ciscoasa(config-if)# member-interface gigabitethernet 0/3
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **clearinterface** | 清除命令的计数 **showinterface**器。 |
| **debugredundant-interface** | 显示与冗余接口事件或错误相关的调试消息。 |
| **interfaceredundant** | 创建冗余接口。 |
| **redundant-interface** | 更改活动成员接口。 |
| **showinterface** | 显示接口的运行时间状态和统计信息。 |

# memberof

要指定此用户所属的组名列表，请在用户名属性配置模式下使用**memberof**命令。要从配置中删除此属性，请使用此命 **no**令的形式。

**memberof***group_1*[,*group_2*,...*group_n*]
**no memberof***group_1*[,*group_2*,...*group_n*]

## Syntax Description

| | |
|---|---|
| *group_1*至*group_n* | 指定此用户所属的组。 |

## Command Default

没有默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 用户名属性配置 | • 是 | — | • 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 8.0(2) | 添加了此命令。 |

## 使用指南

输入此用户所属组的名称的逗号分隔列表。

## CR_Examples

以下示例是在全局配置模式下输入的，创建名为 newuser 的用户名，然后指定 newuser 是 DevTest 组和管理组的成员：

```
ciscoasa(config)# username newuser nopassword
ciscoasa(config)# username newuser attributes
ciscoasa(config-username)# memberof DevTest,management
ciscoasa(config-username)#
```

## Related Commands

| 命令 | 说明 |
|---|---|
| 清除配置用户名 | 清除整个用户名数据库或仅清除指定的用户名。 |
| show running-config username | 显示指定用户或所有用户当前运行的用户名配置。 |

| 命令 | 说明 |
| --- | --- |
| username | 创建和管理用户名数据库。 |

# memory appcache-threshold enable

要启用内存应用缓存阈值，请在配置模式下使用 **memoryappcache-thresholdenable**命令。要禁用，请使 **memoryappcache-threshold,** 用此命 **no**令的形式。

**memoryappcache-thresholdenable**
**nomemoryappcache-thresholdenable**

## Syntax Description

此命令没有任何参数或关键字。

## Command Default

在 ASA 5585-X FirePOWER SSP-60 (5585-60) 上，默认启用此 **memoryappcache-thresholdenable**命令。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 配置 | • 是 | • 支持 | • 支持 | — | • 是 |

## Command History

| 版本 | 修改 |
|---|---|
| 9.10(1) | 引入了此命令。 |

## 使用指南

启用内存 appcache-threshold 会在达到特定内存阈值后限制应用程序缓存分配，以便保留内存来维持设备的稳定性和可管理性。

在 ASA 9.10.1 版本中，在 5585-60 上实施内存应用缓存阈值功能，以将应用缓存分配限制为仅通过设备的连接。

此命令将应用缓存分配阈值配置为系统内存的 85%。当内存使用率达到阈值级别时，系统会丢弃新的通过设备的连接。

命令的**no** 形式会导致所有内存分配限制被释放以供使用，而无需验证。当前统计计数器将被保留，以维护故障排除历史记录，直到 **clearmemoryappcache-threshold** 命令被执行。

对于 9.10.1 版本，仅管理 SNP Conn Core 00 应用缓存类型。此名称与“show mem app-cache”的输出一致。

## CR_Examples

以下示例启用 appcache-memory 阈值：

```
ciscoasa(config)# memory appcache-threshold enable
```

**Related Commands**

| 命令 | 说明 |
| --- | --- |
| show memory appcache-threshold | 显示内存 appcache-threshold 的状态和命中计数 |
| **clearmemoryappcache-threshold** | 清除内存应用缓存阈值的命中计数 |

# memory delayed-free-poisoner enable

要启用延迟释放内存毒化工具，请在 **memorydelayed-free-poisonerenable**特权 EXEC 模式下使用该命令。要禁用 delayed free-memory poisoner 工具，请使用此命令的 **no** 形式。delayed free-memory poisoner 工具可用于监视可用的内存在被应用释放后有何变化。

**memorydelayed-free-poisonerenable**
**nomemorydelayed-free-poisonerenable**

## Syntax Description

此命令没有任何参数或关键字。

## Command Default

该命令默认为禁用。 **memorydelayed-free-poisonerenable**

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 特权 EXEC | • 是 | • 支持 | • 支持 | — | • 是 |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |

## 使用指南

启用 delayed free-memory poisoner 工具对内存使用和系统性能有重大影响。该命令只能在 Cisco TAC 的监督下使用。在大量使用系统的生产环境下不应该运行此工具。

启用此工具后，ASA 上运行的应用程序释放内存的请求将被写入 FIFO 队列。当每个请求写入队列时，低级内存管理不需要的每个相关内存字节都会被写入值 0xcc，从而受到“污染”。

释放的内存请求将保留在队列中，直到应用程序所需的内存多于可用内存池中的内存为止。当需要内存时，系统会从队列中提取第一个释放的内存请求，并验证中毒的内存。

如果内存未被修改，则将其返回到较低级别的内存池，并且该工具从发出初始请求的应用程序重新发出内存请求。该过程持续进行，直到为请求的应用程序释放足够的内存。

如果中毒内存已被修改，则系统会强制崩溃并产生诊断输出以确定崩溃的原因。

delayed free-memory poisoner 工具自动定期验证队列的所有元素。也可以使用命令手动启动验**memorydelayed-free-poisonervalidate**证。

若使用此命令的**no**形式，则队列中请求引用的所有内存不经过验证即返回到可用内存池，同时清除所有统计数据计数器。

## CR_Examples

以下示例启用 delayed free-memory poisoner 工具：

```
ciscoasa# memory delayed-free-poisoner enable
```

下面是 delayed free-memory poisoner 工具检测到非法内存重用时的示例输出：

```
delayed-free-poisoner validate failed because a
        data signature is invalid at delayfree.c:328.
    heap region:    0x025b1cac-0x025b1d63 (184 bytes)
    memory address: 0x025b1cb4
    byte offset:    8
    allocated by:   0x0060b812
    freed by:       0x0060ae15
Dumping 80 bytes of memory from 0x025b1c88 to 0x025b1cd7
025b1c80:                         ef cd 1c a1 e1 00 00 00  |           ........
025b1c90: 23 01 1c a1 b8 00 00 00 15 ae 60 00 68 ba 5e 02  |  #.........`.h.^.
025b1ca0: 88 1f 5b 02 12 b8 60 00 00 00 00 00 6c 26 5b 02  |  ..[...`.....l&[.
025b1cb0: 8e a5 ea 10 ff ff ff ff cc cc cc cc cc cc cc cc  |  ................
025b1cc0: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  |  ................
025b1cd0: cc cc cc cc cc cc cc cc                         |  ........
An internal error occurred.  Specifically, a programming assertion was
violated.  Copy the error message exactly as it appears, and get the
output of the show version command and the contents of the configuration
file.  Then call your technical support representative.
assertion "0" failed: file "delayfree.c", line 191
```

<xref> 描述输出的重要部分。

**表 *2*: 非法内存使用输出说明**

| 字段 | 说明 |
|---|---|
| heap region | 可供请求的应用使用的地址区域以及内存区域大小。这与请求的大小不同，根据发出内存请求时系统分配内存的方式，它可能小于请求的大小。 |
| memory address | 内存中检测到故障的位置。 |
| byte offset | 字节偏移与堆区域的开头有关，可在结果用于保存以此地址开头的数据结构时用于查找修改的字段。0 或大于堆区域字节计数的值可能表示问题是低层堆数据包中的值异常。 |
| allocated by/freed by | 指示最近发出的、涉及此特定内存区域的 malloc/calloc/realloc 和释放调用的地址。 |
| Dumping... | 一个或两个内存区域的转储，具体取决于检测到的故障相距堆内存区域开头的距离。任何系统堆信头后的八个字节是此工具用来保存各系统报头散列值以及队列链路的内存。区域中在遇到任何系统堆尾部之前的所有其他字节应设置为 0xcc。 |

## Related Commands

| 命令 | 说明 |
|---|---|
| **clearmemorydelayed-free-poisoner** | 清除 delayed free-memory poisoner 工具队列和统计信息。 |

| 命令 | 说明 |
| --- | --- |
| **memorydelayed-free-poisonervalidate** | 强制验证延迟释放内存毒化工具队列中的元素。 |
| **showmemorydelayed-free-poisoner** | 显示 delayed free-memory poisoner 工具队列使用摘要。 |

# memory delayed-free-poisoner validate

要强制验证 **memorydelayed-free-poisoner**队列中的所有元素，请在特权 EXEC 模式下使用 **memorydelayed-free-poisonervalidate**命令。

**memorydelayed-free-poisonervalidate**

## Syntax Description

此命令没有任何参数或关键字。

## Command Default

没有默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 特权 EXEC | • 是 | • 支持 | • 支持 | — | • 是 |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |

## 使用指南

在发出 **memorydelayed-free-poisonervalidate** 命令之前，您必须使用 **memorydelayed-free-poisonerenable**命令启用 delayed free-memory poisoner 工具。

**memorydelayed-free-poisonervalidate** 命令导致 **memorydelayed-free-poisoner**队列的每个元素被验证。如果有元素包含非预期的值，则系统发生故障并产生诊断输出来确定故障的原因。如果没有遇到意外值，元素将保留在队列中并由工具正常处理；该**memorydelayed-free-poisonervalidate**命令不会导致队列中的内存返回到系统内存池。

注释 delayed free-memory poisoner 工具自动定期验证队列的所有元素。

## CR_Examples

以下示例导致验证 **memorydelayed-free-poisoner**队列中的所有元素：

```
ciscoasa# memory delayed-free-poisoner validate
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **clearmemorydelayed-free-poisoner** | 清除延迟的空闲内存毒化工具队列和统计信息。 |

| 命令 | 说明 |
| --- | --- |
| **memorydelayed-free-poisonerenable** | 启用延迟释放内存毒化工具。 |
| **showmemorydelayed-free-poisoner** | 显示 delayed free-memory poisoner 工具队列使用摘要。 |

# memory caller-address

要为调用跟踪或调用方PC配置特定范围的程序内存以帮助隔离内存问题，请在**memorycaller-address**特权 EXEC 模式下使用该命令。调用方 PC 是调用内存分配基元的程序的地址。要删除地址范围，请使用此命 **no**令的形式。

**memorycaller-address***startPCendPC*
**nomemorycaller-address**

## Syntax Description

| | |
|---|---|
| *endPC* | 指定内存块的结束地址范围。 |
| *startPC* | 指定内存块的开始地址范围。 |

## Command Default

实际调用方 PC 会被记录以用于内存跟踪。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 特权 EXEC | • 是 | • 支持 | — | • 是 | • 支持 |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0 | 添加了此命令。 |

## 使用指南

使用该 **memorycaller-address**命令将内存问题隔离到特定的内存块。

在某些情况下，内存分配基元的实际调用方 PC 是程序中许多位置使用的已知库功能。要隔离程序中的个别位置，请配置库功能的开始和结束程序地址，从而记录库功能调用方的程序地址。

注释 启用呼叫者地址跟踪时，ASA 的性能可能会暂时下降。

## CR_Examples

以下示例显示了使用命令配置的 **memorycaller-address** 地址范围以及命令的 **showmemory-calleraddress**结果显示：

```
ciscoasa# memory caller-address 0x00109d5c 0x00109e08

ciscoasa# memory caller-address 0x009b0ef0 0x009b0f14
```

```
ciscoasa# memory caller-address 0x00cf211c 0x00cf4464

ciscoasa# show memory-caller address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **memoryprofileenable** | 启用对内存使用（内存分析）的监控。 |
| **memoryprofiletext** | 配置要分析的内存的文本范围。 |
| **showmemory** | 显示可供操作系统使用的最大物理内存量和当前可用内存量的摘要。 |
| **showmemorybinsize** | 显示为特定存储空间分配的数据块的摘要信息。 |
| **showmemoryprofile** | 显示有关 ASA 内存使用情况（分析）的信息。 |
| **showmemory-calleraddress** | 显示在 ASA 上配置的地址范围。 |

# memory logging

要启用内存日志记录，请在**memorylogging**全局配置模式下使用该命令。要禁用内存日志记录功能，请使用此命令的 **no** 形式。

**memory logging**[**1024-4194304**][**wrap**][**size**[**1-2147483647**]][**process**进程名称、][**context**情景名称]
**nomemorylogging**

## Syntax Description

| | |
|---|---|
| 1024-4194304 | 指定内存日志记录缓冲区中的日志记录条目数。这是唯一需要指定的参数。 |
| **context** *context-name* | 指定要监控的虚拟情景和情景名称。 |
| **process***process-name* | 指定要监视的进程和进程名称。<br>注释<br>Checkheaps 进程被当作一个进程完全忽略，因为它以非标准方式使用内存分配器。 |
| 1**size**-2147483647 | 指定要监控的条目的大小和数量。 |
| **wrap** | 回绕时保存缓冲区。缓冲区只能保存一次。如果它 wrap 多次，会被覆写。当缓冲区 wrap 时，系统会将触发器发送到事件管理器，以启用数据保存。 |

## Command Default

没有默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 全局配置 | • 是 | • 支持 | — | • 是 | • 支持 |

## Command History

| 版本 | 修改 |
|---|---|
| 9.4(1) | 添加了此命令。 |

## 使用指南

要更改内存日志记录参数，必须将其禁用，然后重新启用。

## CR_Examples

以下示例启用内存日志记录：

```
ciscoasa
(config)#
memory logging 202980
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **eventmemory-logging-wrap** | 启用响应内存日志记录包装事件。 |
| **showmemorylogging** | 显示内存日志记录结果。 |

# memory profile enable

要启用内存使用情况监控（内存分析），请在 **memoryprofileenable** 特权 EXEC 模式下使用该命令。要禁用内存分析功能，请使用此命令的 **no** 形式。

**memoryprofileenablepeak***peak_value*
**nomemoryprofileenablepeak***peak_value*

## Syntax Description

| | |
|---|---|
| *peak_value* | 指定内存使用阈值，达到此阈值就会在峰值使用缓冲区中保存内存使用率快照。此缓冲区的内容以后可用来分析以确定系统的峰值内存需求。 |

## Command Default

内存分析默认禁用。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 特权 EXEC | • 是 | • 支持 | — | • 是 | • 支持 |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0 | 添加了此命令。 |

## 使用指南

在启用内存分析之前，您必须首先使用该命令配置要分析的 **memoryprofiletext** 内存文本范围。

在您输入命令之前，分析系统会保留一些内 **clearmemoryprofile** 存。查看命令的 **showmemorystatus** 输出。

**注释** 启用内存分析时，ASA 的性能可能会暂时下降。

以下示例启用内存分析：

```
ciscoasa# memory profile enable
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **memoryprofiletext** | 配置要分析的内存的文本范围。 |

| 命令 | 说明 |
| --- | --- |
| **showmemoryprofile** | 显示有关ASA内存使用情况（分析）的信息。 |

# memory profile text

要配置要分析的程序文本内存范围，请在 **memoryprofiletext** 特权 EXEC 模式下使用该命令。要禁用此功能，请使用此命令的 **no** 形式。

**memoryprofiletext** {*startPCendPC* | **all***resolution*}
**nomemoryprofiletext** {*startPCendPC* | **all***resolution*}

## Syntax Description

| | |
|---|---|
| **all** | 指定内存块的整个文本范围。 |
| *endPC* | 指定内存块的整个文本范围。 |
| *resolution* | 指定源文本区域的跟踪分辨率。 |
| *startPC* | 指定内存块的开始文本范围。 |

## Command Default

没有默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 特权 EXEC | • 是 | • 支持 | — | • 是 | • 支持 |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0 | 添加了此命令。 |

## 使用指南

如果文本范围小，分辨率“4”通常便可跟踪对指令的调用。如果文本范围较大，低分辨率对第一遍可能够了，但在下一遍时范围可能需要缩小到一组更小的区域。

使用命令输入文本范围 **memoryprofiletext**后，您必须输入命令来开始内 **memoryprofileenable**存分析。内存分析默认禁用。

注释 启用内存分析时，ASA 的性能可能会暂时下降。

## CR_Examples

以下示例显示如何配置要分析的文本范围的内存，分辨率为 4：

```
ciscoasa# memory profile text 0x004018b4 0x004169d0 4
```

以下示例显示文本范围的配置和内存分析的状态 (OFF)：

```
ciscoasa# show memory profile
InUse profiling: OFF Peak profiling: OFF Profile: 0x004018b4-0x004169d0(00000004)
```

注释 要开始内存分析，您必须输入 **memoryprofileenable**命令。内存分析默认禁用。

## Related Commands

| 命令 | 说明 |
|---|---|
| **clearmemoryprofile** | 清除内存分析功能保留的缓冲区。 |
| **memoryprofileenable** | 启用对内存使用（内存分析）的监控。 |
| **showmemoryprofile** | 显示有关ASA 内存使用情况（分析）的信息。 |
| **showmemory-calleraddress** | 显示在 ASA 上配置的地址范围。 |

# memory-size

要配置 WebVPN 的各种组件可访问的 ASA 上的内存量，请在 webvpn 模式下使用 **memory-size**命令。您可以将内存量配置为设定的内存量（以 KB 为单位）或总内存的百分比。要删除已配置的内存大小，请使用此命令的 **no** 形式。

注释 需要重新启动才能使新的内存大小设置生效。

**memory-size** { **percent** | **kb** } *size*
**nomemory-size** [ { **percent** | **kb** } *size* ]

## Syntax Description

| | |
|---|---|
| **kb** | 指定内存量（以千字节为单位）。 |
| **percent** | 在 ASA 上指定内存量占总内存的百分比。 |
| *size* | 以KB为单位或以总内存的百分比的形式指定内存量。 |

## Command Default

没有默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| Webvpn 模式 | • 是 | — | • 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.1(1) | 添加了此命令。 |

## 使用指南

将立即分配配置的内存量。在配置此命令之前，请使用 show memory 检查可用内存量。如果使用总内存的一定百分比进行配置，请确保配置的值低于可用百分比。如果使用千字节值进行配置，请确保配置的值小于可用内存量（以千字节为单位）。

## CR_Examples

以下示例显示如何将 WebVPN 内存大小配置为 30%：

```
ciscoasa
(config)#
 webvpn
```

```
ciscoasa
(config-webvpn)#
 memory-size percent 30
ciscoasa(config-webvpn)#
ciscoasa(config-webvpn)# reload
```

## Related Commands

| 命令 | 说明 |
| --- | --- |
| **showmemorywebvpn** | 显示 WebVPN 内存使用统计信息。 |

# memory tracking enable

要启用堆内存请求的跟踪，请在**memorytrackingenable**特权 EXEC 模式下使用该命令。要禁用内存日志跟踪功能，请使用此命令的 **no** 形式。

**memorytrackingenable**
**nomemorytrackingenable**

## Syntax Description

此命令没有任何参数或关键字。

## Command Default

没有默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 特权 EXEC | • 是 | • 支持 | — | • 是 | • 支持 |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(8) | 添加了此命令。 |

## 使用指南

使用 **memorytrackingenable**命令跟踪堆内存请求。要禁用内存日志跟踪功能，请使用此命令的 **no** 形式。

在启用内存跟踪之前，请确保将 app-agent heartbeat 命令中的默认间隔和计数值更改为以下值：

**app-agent heartbeat interval 6000 retry-count 6**

## CR_Examples

以下示例启用跟踪堆内存请求：

```
ciscoasa# memory tracking enable
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **clearmemorytracking** | 清除所有当前收集的信息。 |
| **showmemorytracking** | 显示当前分配的内存。 |
| **showmemorytrackingaddress** | 列出工具跟踪的每个当前分配的内存块的大小、位置和最顶层调用函数。 |

| 命令 | 说明 |
| --- | --- |
| **showmemorytrackingdump** | 此命令显示给定内存地址的大小、位置、部分调用堆栈和内存转储。 |
| **showmemorytrackingdetail** | 显示用于深入了解工具内部行为的各种内部细节。 |

# memory-utilization

使用 memory usage 命令将 ASA 配置为在系统内存用尽量达到预定义级别后自动重新启动或使 ASA 崩溃。一旦内存使用率达到配置的阈值限制，系统就会自动重新加载。阈值的范围可能为 90-99%。

**memory-utilizationreload-threshold**<**%**>
**memory-utilizationreload-threshold**<**%**>[**crashinfo**]

## Syntax Description

| | |
|---|---|
| **reload-threshold** | 指定系统内存限制阈值。 |
| **crashinfo** | （可选）指定使用崩溃信息后，系统会在系统重新加载之前保存崩溃信息。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 全局配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.7(1) | 添加了此命令。 |

## 使用指南

建议您不要在已知处于高内存使用率环境中的系统上配置此功能。使用可选的 crashinfo 参数在系统重新加载之前生成崩溃信息文件。

## CR_Examples

以下示例显示了如何在 ASA 上配置内存利用率功能：

```
ciscoasa# memory-utilization reload-threshold 95
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **memoryprofiletext** | 配置要分析的内存的文本范围。 |
| **memoryprofileenable** | 启用对内存使用（内存分析）的监控。 |
| **clearmemoryprofile** | 清除内存分析功能保留的缓冲区。 |
| **showmemoryprofile** | 显示有关ASA内存使用情况（分析）的信息。 |

# merge-dacl

要将可下载的 ACL 与从 RADIUS 数据包的 Cisco AV 对中接收的 ACL 合并，请在 **merge-dacl**aaa-server group 配置模式下使用该命令。要禁用可下载 ACL 与从 RADIUS 数据包的 Cisco AV 对中接收的 ACL 的合并，请使用此命令的 **no**形式。

**mergedacl** {**before_avpair** | **after_avpair**}
**nomergedacl**

## Syntax Description

| | |
|---|---|
| **after_avpair** | 指定可下载的 ACL 条目应放置在 Cisco AV 对条目之后。此选项仅适用于 VPN 连接。对于 VPN 用户，ACL 的形式可以是思科 AV 对 ACL、可下载 ACL 和在 ASA 上配置的 ACL。此选项确定可下载 ACL 和 AV 对 ACL 是否会合并，并且不适用于在 ASA 上配置的任何 ACL。 |
| **before_avpair** | 指定可下载的 ACL 条目应放置在 Cisco AV 对条目之前。 |

## Command Default

默认设置为 **nomergedacl**，指定可下载的 ACL 不会与 Cisco AV 对 ACL 合并。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| AAA-server group 配置 | • 是 | • 支持 | • 支持 | • 支持 | • 支持 |

## Command History

| 版本 | 修改 |
|---|---|
| 8.0(2) | 添加了此命令。 |

## 使用指南

如果同时收到 AV 对和可下载 ACL，则优先使用 AV 对。

## CR_Examples

以下示例指定可下载的 ACL 条目应放置在 Cisco AV 对条目之前：

```
ciscoasa(config)# aaa-server servergroup1 protocol radius
ciscoasa(config-aaa-server-group)# merge-dacl before-avpair
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **aaa-serverhost** | 标识服务器及其所属的 AAA 服务器组。 |

| 命令 | 说明 |
| --- | --- |
| **aaa-serverprotocol** | 确定服务器组名称和协议。 |
| **max-failed-attempts** | 指定在尝试下一个服务器之前向组中的AAA服务器发送的最大请求数。 |

# message-authenticator-required

要指定 Message-Authenticator 属性必须存在于 RADIUS 请求和响应中，请在 **message-authenticator-required**aaa-server 主机配置模式下使用该命令。要禁用消息身份验证器要求，请使用此命令的 **no** 形式。

**message-authenticator-required**
**no message-authenticator-required**

## Syntax Description

此命令没有任何参数或关键字。

## Command Default

不需要消息身份验证器 (Message-Authenticator) 属性。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| AAA服务器主机配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.23(1) | 添加了此命令。 |

## 使用指南

Message-Authenticator 属性用于防御 Blast-RADIUS 攻击。如果已升级 RADIUS 服务器使其支持消息身份验证器，则可以启用此选项来帮助防御这些攻击。启用后，所有请求和响应都必须有消息身份验证器，否则身份验证将失败。

### 示例

以下示例启用该功能

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa(config-aaa-host)# message-authenticator-required
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **aaa-server host** | 标识 AAA 服务器组的 AAA 服务器。 |

# message-length

要过滤不符合配置的最大长度的 DNS 数据包，请在参数配置模式下使用 message-length 命令。使用 **no**表单删除该命令。

**message-lengthmaximum**{长度 | **client**{长度 | **auto**} | **server**{长度 | **auto**}}
**no message-lengthmaximum**{长度 | **client**{长度 | **auto**} | **server**{长度 | **auto**}}

## Syntax Description

| | |
|---|---|
| *length* | DNS 消息中允许的最大字节数，从 512 到 65535。 |
| **client** {*length* \| **auto**} | 客户端 DNS 消息中允许的最大字节数，从 512 到 65535，或 **auto** 将最大长度设置为资源记录中的值。 |
| **server** {*length* \| **auto**} | 服务器 DNS 消息中允许的最大字节数，范围为 512 到 65535，或使用 **auto** 将最大长度设置为资源记录中的值。 |

## Command Default

默认检测将 DNS 最大消息长度设置为 512，并将客户端长度设置为 **auto**。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 参数配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 8.2(2) | 添加了此命令。 |

## 使用指南

您可以将最大 DNS 消息长度配置为 DNS 检测映射中的参数。

## CR_Examples

以下示例显示如何在 DNS 检查策略映射中配置最大 DNS 消息长度：

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-length 512
ciscoasa(config-pmap-p)# message-length client auto
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **parameter** | 在策略图配置模式下进入参数配置模式。 |

| 命令 | 说明 |
| --- | --- |
| **policy-maptypeinspectdns** | 创建 DNS 检测策略映射。 |

# message-tag-validation

要验证M3UA消息中某些字段的内容，请在参数配置模式下使用 **message-tag-validation** 命令。首先输入命令即可进入参数配置 **policy-maptypeinspectm3ua**模式。使用此命 **no**令的形式来删除设置。

**message-tag-validation** { **dupu** | **error** | **notify** }
**no message-tag-validation** { **dupu** | **error** | **notify** }

## Syntax Description

| | |
|---|---|
| **dupu** | 启用对目的用户部分不可用 (DUPU) 消息的验证。用户/原因字段必须存在，并且必须仅包含有效的原因和用户代码。 |
| **error** | 为错误消息启用验证。所有必填字段必须存在并且仅包含允许的值。每个错误消息都必须包含该错误代码的必填字段。 |
| **notify** | 为通知消息启用验证。状态类型和状态信息字段必须仅包含允许的值。 |

## Command Default

该命令的默认设置是禁用的。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 参数配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.7(1) | 添加了此命令。 |

## 使用指南

使用此命令确保针对指定的 M3UA 消息类型检查并验证某些字段的内容。验证失败的消息将被丢弃。

## CR_Examples

以下示例在 M3UA 检测中启用对 DUPU、错误和通知消息的消息验证。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-tag-validation dupu
ciscoasa(config-pmap-p)# message-tag-validation error
ciscoasa(config-pmap-p)# message-tag-validation notify
```

**Related Commands**

| 命令 | 说明 |
| --- | --- |
| **inspectm3ua** | 启用 M3UA 检测。 |
| **policy-maptypeinspect** | 创建检查策略映射。 |
| **showservice-policyinspectm3ua** | 显示M3UA统计信息。 |

# metric

要全局更改所有 IS-IS 接口的指标值，请在路由器 isis 配置模式下使用 **metric** 命令。要禁用指标值并恢复默认指标值 10，请使用此命令的 **no** 形式。

**metric***default-value* [**level-1** | **level-2**]
**nometric***default-value* [**level-1** | **level-2**]

## Syntax Description

| | |
|---|---|
| 默认值 | 分配给链路并用于计算通过链路到目的地的路径成本的度量值。范围为 1 到 63。 |
| **level-1** | （可选）设置 IS-IS 第 1 级 IPv4 或 IPv6 度量。 |
| **level-2** | （可选）设置 IS-IS 第 2 级 IPv4 或 IPv6 度量。 |

## Command Default

默认值为 10。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 路由器配置 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.6(1) | 添加了此命令。 |

## 使用指南

当需要更改所有 IS-IS 接口的默认度量值时，建议您使用 in 命令对 **metric**所有接口进行全局配置。以全局方式配置指标值可以防止出现用户错误，如从某一接口意外删除已设置的指标，而又没有配置新值，并且意外允许该接口恢复为默认指标 10，从而成为网络中的高度优先接口。

输入 命令 **metric** 更改默认 IS-IS 接口指标值后，已启用的接口将使用新值而不是默认值 10。被动接口继续使用指标值 0。

## CR_Examples

以下示例将 IS-IS 接口配置为全局度量为 111：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# metric 111
```

**Related Commands**

| 命令 | 说明 |
|---|---|
| **advertisepassive-only** | 配置 ASA 以通告被动接口。 |
| **area-password** | 配置 IS-IS 区域身份验证密码。 |
| **authenticationkey** | 全局启用 IS-IS 身份验证。 |
| **authenticationmode** | 指定IS-IS实例全局使用的IS-IS报文认证方式。 |
| **authenticationsend-only** | 全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。 |
| **clearisis** | 清除 IS-IS 数据结构。 |
| default-information originate | 在 IS-IS 路由域中生成默认路由。 |
| **distance** | 定义分配给 IS-IS 协议发现的路由的管理距离。 |
| **domain-password** | 配置 IS-IS 域身份验证密码。 |
| **fast-flood** | 将 IS-IS LSP 配置为完整的。 |
| **hellopadding** | 将 IS-IS hello 配置为完整 MTU 大小。 |
| **hostnamedynamic** | 启用 IS-IS 动态主机名功能。 |
| **ignore-lsp-errors** | 配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。 |
| **isisadjacency-filter** | 过滤 IS-IS 邻接关系的建立。 |
| **isisadvertise-prefix** | 在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。 |
| **isisauthenticationkey** | 启用接口的身份验证。 |
| **isisauthenticationmode** | 指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型 |
| **isisauthenticationsend-only** | 配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。 |
| **isiscircuit-type** | 配置用于 IS-IS 的邻接类型。 |
| **isiscsnp-interval** | 配置在广播接口上发送周期性 CSNP 数据包的间隔。 |
| **isishello-interval** | 指定 IS-IS 发送的连续 hello 数据包之间的时间长度。 |
| **isishello-multiplier** | 指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。 |
| **isishellopadding** | 将 IS-IS hello 配置为每个接口的完整 MTU 大小。 |

| 命令 | 说明 |
| --- | --- |
| **isislsp-interval** | 配置每个接口连续 IS-IS LSP 传输之间的时间延迟。 |
| **isismetric** | 配置 IS-IS 度量的值。 |
| **isispassword** | 配置接口的认证密码。EXTEN |
| **isispriority** | 配置接口上指定 ASA 的优先级。 |
| **isisprotocolshutdown** | 禁用每个接口的 IS-IS 协议。 |
| **isisretransmit-interval** | 配置接口上每个 IS-IS LSP 重新传输之间的时间量。 |
| **isisretransmit-throttle-interval** | 配置接口上每个 IS-IS LSP 重新传输之间的时间量。 |
| **isistag** | 当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。 |
| **is-type** | 为 IS-IS 路由进程分配路由级别。 |
| **log-adjacency-changes** | 使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。 |
| **lsp-fullsuppress** | 配置当 PDU 已满时哪些路由会被抑制。 |
| **lsp-gen-interval** | 定制 IS-IS 对 LSP 生成的限制。 |
| **lsp-refresh-interval** | 设置LSP刷新间隔。 |
| **max-area-addresses** | 为 IS-IS 区域配置额外的手动地址。 |
| **max-lsp-lifetime** | 设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。 |
| **maximum-paths** | 为 IS-IS 配置多路径负载共享。 |
| **metric** | 全局更改所有 IS-IS 接口的度量值。 |
| **metric-style** | 配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。 |
| **net** | 指定路由过程的NET。 |
| **passive-interface** | 配置被动接口。 |
| **prc-interval** | 定制 PRC 的 IS-IS 限制。 |
| **protocolshutdown** | 全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。 |
| **redistributeisis** | 将 IS-IS 路由从第 1 级重新分配到第 2 级或从第 2 级重新分配到第 1 级。 |
| **routepriorityhigh** | 为 IS-IS IP 前缀分配高优先级。 |

| 命令 | 说明 |
| --- | --- |
| **routerisis** | 启用 IS-IS 路由。 |
| **set-attached-bit** | 指定第 1 级至第 2 级路由器应设置其附加位的约束。 |
| **set-overload-bit** | 配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。 |
| **showclns** | 显示 CLNS 特定信息。 |
| **showisis** | 显示 IS-IS 信息。 |
| **showrouteisis** | 显示 IS-IS 路由。 |
| **spf-interval** | 自定义 IS-IS 对 SPF 计算的限制。 |
| **summary-address** | 为 IS-IS 创建聚合地址。 |

# metric-style

要配置运行 IS-IS 的路由器，使其仅生成和接受新式类型、长度、值对象 (TLV)，请在路由器 isis 配置模式下使用 **metric-style** 命令。要禁用该功能，请使用此命令的 **no** 形式。

**metric-style** [**narrow** | **transition** | **wide**] [**level-1** | **level-2** | **level-1-2**]
**nometric** [**level-1** | **level-2** | **level-1-2**]

## Syntax Description

| | |
|---|---|
| **narrow** | 指示 ASA 使用具有窄度量的旧式 TLV。 |
| **transition** | （可选）指示 ASA 在过渡期间接受旧式和新式 TLV。 |
| **wide** | 指示 ASA 使用新样式的 TLV 来承载更广泛的度量。 |
| **level-1** | （可选）在路由级别 1 上启用此命令。 |
| **level-2** | （可选）在路由级别 2 上启用此命令。 |
| level-1-2 | （可选）指示路由器接受旧式和新式 TLV。 |

## Command Default

默认值为 10。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 路由器配置 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.6(1) | 添加了此命令。 |

## 使用指南

如果输入 metric-space宽命令，则 ASA 仅生成和接受新式 TLV。因此，与同时生成旧式和新式 TLV 时相比，ASA 使用的内存和其他资源更少。

此样式适用于跨整个网络启用 MPLS 流量工程。

## CR_Examples

以下示例将 ASA 配置为在第 1 级生成和接受新式 TLV：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# metric-style wide level-1
```

**Related Commands**

| 命令 | 说明 |
|---|---|
| **advertisepassive-only** | 配置 ASA 以通告被动接口。 |
| **area-password** | 配置 IS-IS 区域身份验证密码。 |
| **authenticationkey** | 全局启用 IS-IS 身份验证。 |
| **authenticationmode** | 指定IS-IS实例全局使用的IS-IS报文认证方式。 |
| **authenticationsend-only** | 全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。 |
| **clearisis** | 清除 IS-IS 数据结构。 |
| default-information originate | 在 IS-IS 路由域中生成默认路由。 |
| **distance** | 定义分配给 IS-IS 协议发现的路由的管理距离。 |
| **domain-password** | 配置 IS-IS 域身份验证密码。 |
| **fast-flood** | 将 IS-IS LSP 配置为完整的。 |
| **hellopadding** | 将 IS-IS hello 配置为完整 MTU 大小。 |
| **hostnamedynamic** | 启用 IS-IS 动态主机名功能。 |
| **ignore-lsp-errors** | 配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。 |
| **isisadjacency-filter** | 过滤 IS-IS 邻接关系的建立。 |
| **isisadvertise-prefix** | 在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。 |
| **isisauthenticationkey** | 启用接口的身份验证。 |
| **isisauthenticationmode** | 指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型 |
| **isisauthenticationsend-only** | 配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。 |
| **isiscircuit-type** | 配置用于 IS-IS 的邻接类型。 |
| **isiscsnp-interval** | 配置在广播接口上发送周期性 CSNP 数据包的间隔。 |
| **isishello-interval** | 指定 IS-IS 发送的连续 hello 数据包之间的时间长度。 |
| **isishello-multiplier** | 指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。 |
| **isishellopadding** | 将 IS-IS hello 配置为每个接口的完整 MTU 大小。 |

| 命令 | 说明 |
| --- | --- |
| **isislsp-interval** | 配置每个接口连续 IS-IS LSP 传输之间的时间延迟。 |
| **isismetric** | 配置 IS-IS 度量的值。 |
| **isispassword** | 配置接口的认证密码。EXTEN |
| **isispriority** | 配置接口上指定 ASA 的优先级。 |
| **isisprotocolshutdown** | 禁用每个接口的 IS-IS 协议。 |
| **isisretransmit-interval** | 配置接口上每个 IS-IS LSP 重新传输之间的时间量。 |
| **isisretransmit-throttle-interval** | 配置接口上每个 IS-IS LSP 重新传输之间的时间量。 |
| **isistag** | 当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。 |
| **is-type** | 为 IS-IS 路由进程分配路由级别。 |
| **log-adjacency-changes** | 使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。 |
| **lsp-fullsuppress** | 配置当 PDU 已满时哪些路由会被抑制。 |
| **lsp-gen-interval** | 定制 IS-IS 对 LSP 生成的限制。 |
| **lsp-refresh-interval** | 设置LSP刷新间隔。 |
| **max-area-addresses** | 为 IS-IS 区域配置额外的手动地址。 |
| **max-lsp-lifetime** | 设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。 |
| **maximum-paths** | 为 IS-IS 配置多路径负载共享。 |
| **metric** | 全局更改所有 IS-IS 接口的度量值。 |
| **metric-style** | 配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。 |
| **net** | 指定路由过程的NET。 |
| **passive-interface** | 配置被动接口。 |
| **prc-interval** | 定制 PRC 的 IS-IS 限制。 |
| **protocolshutdown** | 全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。 |
| **redistributeisis** | 将 IS-IS 路由从第 1 级重新分配到第 2 级或从第 2 级重新分配到第 1 级。 |
| **routepriorityhigh** | 为 IS-IS IP 前缀分配高优先级。 |

| 命令 | 说明 |
| --- | --- |
| **routerisis** | 启用 IS-IS 路由。 |
| **set-attached-bit** | 指定第 1 级至第 2 级路由器应设置其附加位的约束。 |
| **set-overload-bit** | 配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。 |
| **showclns** | 显示 CLNS 特定信息。 |
| **showisis** | 显示 IS-IS 信息。 |
| **showrouteisis** | 显示 IS-IS 路由。 |
| **spf-interval** | 自定义 IS-IS 对 SPF 计算的限制。 |
| **summary-address** | 为 IS-IS 创建聚合地址。 |

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。