目 录

1 用户身份识别和管理

1.1 用户身份识别和管理命令

1.1.1 account-update-interval

account-update-interval 命令用来配置自动导入身份识别用户账户的周期。

undo account-update-interval 命令用来恢复缺省情况。

【命令】

account-update-interval *interval*

undo account-update-interval

【缺省情况】

自动导入身份识别用户账户的周期为 24 小时。

【视图】

身份识别用户导入策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

interval：表示导入身份识别用户账户的周期，取值范围为 1～65536，单位为小时。

【使用指导】

身份识别用户导入策略处于开启状态时，设备将以本命令指定的周期从服务器上导入所有身份识别用户账户，使得设备与服务器上的账户信息定期保持一致。

【举例】

在身份识别用户导入策略 policy1 中，配置自动导入身份识别用户账户的周期为 12 小时。

```
<Sysname> system-view
[Sysname] user-identity user-import-policy policy1
[Sysname-identity-user-impt-policy-policy1] account-update-interval 12
```

【相关命令】

- **user-identity user-account auto-import policy**

1.1.2 connection-detect

connection-detect 命令用来配置对 RESTful 服务器的探测参数。

undo connection-detect 命令用来恢复缺省情况。

【命令】

connection-detect { **interval** *interval* | **maximum** *max-times* }

undo connection-detect { **interval** | **maximum** }

【缺省情况】

对 RESTful 服务器的探测周期为 5 分钟，每周期内的最大探测次数为 3。

【视图】

RESTful 服务器视图

【缺省用户角色】

network-admin

context-admin

【参数】

interval *interval*：探测周期，取值范围为 1～10，单位为分钟。

maximum *max-times*：每个探测周期内的最大探测次数，取值范围为 1～5。

【使用指导】

如果对设备与 RESTful 服务器的连接状态要求比较高，建议设置较小的探测周期，以及较大的探测次数。

配置的探测周期不建议太小，因为探测周期过小会增加设备与 RESTful 服务器交互的频率，增加 RESTful 服务器负担，具体配置请结合 RESTful 服务器的性能参数综合考虑。

【举例】

配置对 RESTful 服务器 rest1 的探测周期为 2 分钟，每周期内的最大探测次数为 3。

```
<Sysname> system-view
[Sysname] user-identity restful-server rest1
[Sysname-restfulserver-rest1] connection-detect interval 2
[Sysname-restfulserver-rest1] connection-detect maximum 3
```

【相关命令】

- **connection-detect enable**
- **display user-identity restful-server**
- **login-name**
- **uri**
- **user-identity restful-server**

1.1.3 connection-detect enable

connection-detect enable 命令用来开启对 RESTful 服务器的探测功能。

undo connection-detect enable 命令用来关闭对 RESTful 服务器的探测功能。

【命令】

connection-detect enable

undo connection-detect enable

【缺省情况】

对 RESTful 服务器的探测功能处于关闭状态。

【视图】

RESTful 服务器视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

开启本探测功能后，设备将立即与该 RESTful 服务器进行交互，探测与 RESTful 服务器的连接状态（可达或者不可达）。此连接状态可被安全业务模块作为用户接入控制策略的参考信息。

开启本探测功能前，必须要配置 RESTful 视图下的 **login-name** 以及 **uri** 命令。

设备在一个探测周期内（时长由 **connection-detect interval** *interval* 命令设置），会尝试发起多次探测（次数由 **connection-detect maximum** *max-times* 命令设置）来决定服务器是否可达，具体如下：

- 只要设备收到服务器回应，即认为服务器可达，并停止探测。
- 若设备在最大尝试次数达到之后，仍然未收到服务器回应，则认为服务器不可达。

上一轮探测周期结束后，设备自动进入下一轮探测，过程同上。

关闭本探测功能后，设备将停止与 RESTful 服务器进行探测交互。

【举例】

开启对 RESTful 服务器 rest1 的探测功能。

```
<Sysname> system-view
[Sysname] user-identity restful-server rest1
[Sysname-restfulserver-rest1] connection-detect enable
```

【相关命令】

- **connection-detect**
- **display user-identity restful-server**
- **login-name**
- **uri**
- **user-identity restful-server**

1.1.4 display user-identity

display user-identity 命令用来显示指定的身份识别用户或身份识别用户组。

【命令】

display user-identity { **domain** *domain-name* | **null-domain** } { **user** [*user-name* [**group**]] | **user-group** [*group-name* [**member** { **group** | **user** }]] }

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

domain *domain-name*：表示身份识别域的名称，为 1～255 个字符的字符串，不区分大小写。

null-domain：表示未加入任何身份识别域的身份识别用户或身份识别用户组。

user：显示身份识别用户信息。

user-name：身份识别用户名，为 1～55 个字符的字符串，区分大小写。若不指定该参数，则表示显示所有身份识别用户的信息。

group：显示用户所属用户组。若不指定该参数，则不显示用户组信息。

user-group：显示身份识别用户组信息。

group-name：用户组名，为 1～32 个字符的字符串，不区分大小写。若不指定该参数，则表示显示所有身份识别用户组的配置信息。

member：显示身份识别的成员信息。若不指定该参数，则不显示成员信息。

group：用户组成员。

user：用户成员。

【使用指导】

本命令显示的身份识别用户或身份识别用户组信息，包括从本地用户数据库学习的和从 CSV 文件、服务器导入的身份识别用户账户以及身份识别用户组的信息。

【举例】

显示 system 域下所有身份识别用户组的信息。

```
<Sysname> display user-identity domain system user-group
Identity domain: system
  Group ID      Group name
  0x888         abc
  0x123         gp1

Total 2 records matched.
```

显示 system 域下身份识别用户组 abc 的信息。

```
<Sysname> display user-identity domain system user-group abc
Identity domain: system
  Group ID      Group name
  0x888         abc

Total 1 records matched.
```

显示 system 域下身份识别用户组 abc 中的用户成员信息。

```
<Sysname> display user-identity domain system user-group abc member user
Identity domain: system
  User ID      Username
  0x234        user1
  0xffffffff   user2
```

```
Total 2 records matched.
```

显示 system 域下身份识别用户组 abc 中的用户组成员信息。

```
<Sysname> display user-identity domain system user-group abc member group
Identity domain: system
  Group ID      Group name
  0x567         group1
  0x111         group2

Total 2 records matched.
```

显示 system 域下所有身份识别用户的信息。

```
<Sysname> display user-identity domain system user
Identity domain: system
  User ID       Username
  0x234         user1
  0xffffffff    user2

Total 2 records matched.
```

显示 system 域下身份识别用户 user1 的信息。

```
<Sysname> display user-identity domain system user user1
Identity domain: system
  User ID       Username
  0x234         user1

Total 1 records matched.
```

显示 system 域下身份识别用户 user1 的用户组信息。

```
<Sysname> display user-identity domain system user user1 group
Identity domain: system
  Group ID      Group name
  0x888         abc
  0x123         gp1

Total 2 records matched.
```

显示未加入任何身份识别域的身份识别用户信息。

```
<Sysname> display user-identity null-domain user
  User ID     Username
  0x1         test
  0x3         jj
  0x2         abc

Total 3 records matched.
```

表1-1 display user-identity 命令显示信息描述表

字段	描述
Identity domain	身份识别用户或身份识别用户组所属身份识别域的名称 若用户或用户组不属于任何身份识别域，则不显示该字段
Username	用户名

字段	描述
User ID	用户ID
Group name	用户组名
Group ID	用户组ID
Total *n* records matched	匹配的用户或用户组数目

【相关命令】

- **reset user-identity user-account**
- **reset user-identity user-group**

1.1.5 display user-identity active-user-group

display user-identity active-user-group 命令用来显示激活的身份识别用户组。

【命令】

display user-identity active-user-group { **all** | **domain** *domain-name* | **null-domain** }

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

all：显示所有身份识别域下的激活用户组。

domain *domain-name*：显示指定身份识别域下的激活用户组。*domain-name* 表示身份识别域的名称，为 1～255 个字符的字符串，不区分大小写。

null-domain：显示未加入任何身份识别域的激活用户组。

【使用指导】

当身份识别用户组被域间策略等安全特性引用之后，若该引用配置生效，则该用户组将处于激活状态。只有身份识别用户组处于激活状态时，该用户组才能在基于用户身份的访问控制过程中生效。

【举例】

显示身份识别域 system 下的激活的身份识别用户组信息。

```
<Sysname> display user-identity active-user-group domain system
Identity domain: system
  Group ID      Group name
  0x888         abc
  0x123         gp1
```

```
Total 2 records matched.
```

表1-2 display user-identity active-user-group 命令显示信息描述表

字段	描述
Identity domain	身份识别用户组所属的身份识别域名 若用户不属于任何身份识别域，则不显示该字段
Group ID	身份识别用户组的ID
Group name	身份识别用户组名
Total *n* records matched	匹配的用户组数目

【相关命令】

- **reset user-identity user-group**

1.1.6 display user-identity all

display user-identity all 命令用来显示所有身份识别用户或身份识别用户组。

【命令】

display user-identity all { **user** | **user-group** }

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

user：显示身份识别用户信息。

user-group：显示身份识别用户组信息。

【使用指导】

本命令显示的身份识别用户或身份识别用户组信息，包括从本地用户数据库学习的和从 CSV 文件以及第三方服务器导入的身份识别用户账户及身份识别用户组的信息。

【举例】

显示所有身份识别用户信息。

```
<Sysname> display user-identity all user
Identity domain: system
  User ID       Username
  0x121         test1
  0x123         test2
```

```
Identity domain: 11
  User ID       Username
  0x888         test3
  0x899         test4

Total 4 records matched.
```

表1-3 display user-identity all user 命令显示信息描述表

字段	描述
Identity domain	身份识别用户所属身份识别域的名称 若用户不属于任何身份识别域，则不显示该字段
User ID	用户ID
Username	用户名
Total *n* records matched	匹配的用户数目

显示所有身份识别用户组。

```
<Sysname> display user-identity all user-group
Identity domain: system
  Group ID      Group name
  0x888         abc
  0x123         gp1
Identity domain: 11
  Group ID      Group name
  0x255         001
  0x256         002

Total 4 records matched.
```

表1-4 display user-identity all user-group 命令显示信息描述表

字段	描述
Identity domain	身份识别用户组所属身份识别域的名称 若用户组不属于任何身份识别域，则不显示该字段
Group ID	用户组ID
Group name	用户组
Total *n* records matched	匹配的用户组数目

【相关命令】

- **reset user-identity user-account**
- **reset user-identity user-group**

1.1.7 display user-identity online-user

display user-identity online-user 命令用来显示在线身份识别用户。

【命令】

display user-identity online-user { **domain** *domain-name* | **null-domain** } **name** *user-name*

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

domain *domain-name*：指定在线身份识别用户所属的身份识别域。*domain-name* 表示身份识别域名，为 1～255 个字符的字符串，不区分大小写。

null-domain：表示未加入任何身份识别域的在线身份识别用户。

name *user-name*：指定在线身份识别用户的用户名。*user-name* 表示用户名，为 1～55 个字符的字符串，区分大小写，不能携带域名。

【使用指导】

在线身份识别用户包括两类：由静态配置生成的静态在线身份识别用户，以及由设备动态生成的动态在线身份识别用户。

【举例】

显示 system 域下名称为 user1 的在线身份识别用户信息。

```
<Sysname> display user-identity online-user domain system name user1
User name: user1
  Identity domain: system
  IP  : 199.199.0.15
  MAC : 0001-0002-0003
  Type: Static

Total 1 records matched.
```

表1-5 display user-identity online-user 命令显示信息描述表

字段	描述
User name	身份识别用户的名称
Identity domain	身份识别用户所属的身份识别域 若用户不属于任何身份识别域，则不显示该字段
IP	身份识别用户的IP地址
MAC	身份识别用户的MAC地址 若没有获取到MAC地址信息，则不显示该字段
Type	身份识别用户的类型，包括以下取值：

字段	描述
	• Static：静态在线身份识别用户 • Dynamic：动态在线身份识别用户
Total *n* records matched	匹配的用户数目

【相关命令】

- **reset user-identity dynamic-online-user**
- **user-identity static-user**

1.1.8 display user-identity restful-server

display user-identity restful-server 命令用来显示 RESTful 服务器配置。

【命令】

display user-identity restful-server [*server-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

server-name：表示 RESTful 服务器的名称，为 1～31 个字符的字符串，不区分大小写。如果不指定本参数，则表示显示所有 RESTful 服务器的配置信息。

【举例】

显示 RESTful 服务器 rest1 的配置。

```
<Sysname> display user-identity restful-server rest1
RESTful server name: rest1
  Login name: u1
  Vpn Instance: v1
  Get User URI: http://1.1.1.1:8080/imcrs/ssm/imcuser/accessUser
  Get User Group URI: http://1.1.1.1:8080/imcrs/ssm/imcuser/accessUserGroup
  Get Online User URI: http://1.1.1.1:8080/imcrs/ssm/imcuser/onlineUser
  Put Online User URI: http://1.1.1.1:8080/imcrs/ssm/imcuser/uploadOnlineUser
  Put Offline User URI: http://1.1.1.1:8080/imcrs/ssm/imcuser/uploadOfflineUser
  Connectivity detection:  Enabled
    Detection interval: 1 minutes
    Maximum times: 1
  Connectivity status: Reachable
```

表1-6 display user-identity restful-server 命令显示信息描述表

字段	描述
Login name	连接到RESTful服务器所需的用户名
Vpn Instance	RESTful服务器所属VPN实例名称 若属于公网，则不显示本字段
Get User URI	请求用户账户信息的URI
Get User Group URI	请求用户组信息的URI
Get Online User URI	请求在线用户信息的URI
Put Online User URI	上传在线用户信息的URI
Put Offline User URI	上传下线用户信息的URI
Connectivity detection	RESTful服务器探测功能的开启状态 • Enabled：开启 • Disabled：关闭
Detection interval	设备对RESTful服务器的探测周期，单位为分钟
Maximum times	设备对RESTful服务器的最大探测次数
Connectivity status	设备对RESTful服务器的探测结果 • Reachable：可达 • Unreachable：不可达 若未开启RESTful服务器探测功能，则不显示本字段

【相关命令】

- **connection-detect**
- **connection-detect enable**
- **login-name**
- **uri**
- **user-identity restful-server**
- **vpn-instance**

1.1.9 display user-identity user-import-policy

display user-identity user-import-policy 命令用来显示身份识别用户导入策略。

【命令】

display user-identity user-import-policy [*policy-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

policy-name：表示身份识别用户导入策略名，为 1～31 个字符的字符串，不区分大小写。若不指定该参数，则显示所有的身份识别用户导入策略。

【举例】

显示身份识别用户导入策略 policy1 的配置信息。

```
<Sysname> display user-identity user-import-policy policy1
Policy name: policy1
  Interval time: 24 hours
  RESTful server name:
    ser1
  LDAP import type: All
  LDAP scheme name:
    ldap-scheme

 Total 1 records matched.
```

表1-7 display user-identity user-import-policy 命令显示信息描述表

字段	描述
Policy name	身份识别用户导入策略名称
Interval time	自动导入身份识别用户账户的周期，单位为小时
RESTful server name	RESTful服务器名称
LDAP import type	从LDAP服务器上导入的用户信息类型，包括以下取值： • All：表示导入用户和用户组信息 • User：表示导入用户信息 • Group：表示导入用户组信息
LDAP scheme name	LDAP方案名称
Total *n* records matched	匹配的策略数目

【相关命令】

- **import-type**
- **user-identity user-import-policy**

1.1.10 import-type

import-type 命令用来配置从 LDAP 服务器上导入的用户信息类型。

undo import-type 命令用来恢复缺省情况。

【命令】

import-type { **all** | **group** | **user** }

undo import-type

【缺省情况】

未配置从 LDAP 服务器上导入的用户信息类型，允许导入用户和用户组信息。

【视图】

身份识别用户导入策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

all：表示导入用户和用户组信息。

group：表示导入用户组信息。

user：表示导入用户信息。

【使用指导】

根据实际导入需求选择一个对应的类型进行配置，导入时会根据配置的导入类型从 LDAP 服务器将该类型信息导入到设备上。

多次配置本命令，仅最后一次执行的命令生效。

【举例】

配置从 LDAP 服务器上导入的用户类型为所有类型，即包括用户和用户组信息。

```
<Sysname> system-view
[Sysname] user-identity user-import-policy policy
[Sysname-identity-user-impt-policy-policy] import-type all
```

【相关命令】

- **display user-identity user-import-policy**

1.1.11 ldap-scheme

ldap-scheme 命令用来指定 LDAP 方案。

undo ldap-scheme 命令用来删除 LDAP 方案。

【命令】

ldap-scheme *ldap-scheme-name*

undo ldap-scheme *ldap-scheme-name*

【缺省情况】

未指定 LDAP 方案。

【视图】

身份识别用户导入策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

ldap-scheme-name：LDAP 方案名，为 1～32 个字符的字符串，不区分大小写。

【使用指导】

指定的 LDAP 方案中定义了 LDAP 服务器的相关参数，用户可以通过执行 **user-identity user-account import policy** 命令从该方案定义的 LDAP 服务器上导入身份识别用户账户信息。但是，系统不支持从 LDAP 服务器上导入在线身份识别用户信息。

最多可以指定 16 个 LDAP 方案，使得可以同时从多个 LDAP 服务器上导入身份识别用户账户信息。

【举例】

在身份识别用户导入策略 policy1 中，指定名称为 ser2 的 LDAP 方案。

```
<Sysname> system-view
[Sysname] user-identity user-import-policy policy1
[Sysname-identity-user-impt-policy-policy1] ldap-scheme ser2
```

【相关命令】

- **display user-identity user-import-policy**
- **ldap scheme**（安全命令参考/AAA）

1.1.12 login-name

login-name 命令用来配置登录到 RESTful 服务器所需的用户名和密码。

undo login-name 命令用来恢复缺省情况。

【命令】

login-name *user-name* **password** { **cipher** | **simple** } *string*

undo login-name

【缺省情况】

未配置登录到 RESTful 服务器所需的用户名和密码。

【视图】

RESTful 服务器视图

【缺省用户角色】

network-admin

context-admin

【参数】

user-name：表示用户名，为 1～55 字符的字符串，区分大小写。

password：表示密码。

cipher：表示以密文方式设置密码。

simple：表示以明文方式设置密码，该密码将以密文形式存储。

string：密码字符串，区分大小写。明文密码为 1～63 个字符的字符串，密文密码为 1～117 个字符的字符串。

【使用指导】

设备与 RESTful 服务器建立连接时，服务器首先需要验证连接请求发起方的合法性。本命令配置的用户名和密码，即为设备向 RESTful 服务器提供的身份信息。RESTful 服务器验证该用户名和密码成功后，才允许连接请求发起方与之建立连接，以及获取相应的服务器资源。

本命令指定的用户名和密码，必须在 RESTful 服务器上已经存在。

【举例】

配置与 RESTful 服务器 rest1 建立连接时使用的登录用户名为 abc，密码为明文 123。

```
<Sysname> system-view
[Sysname] user-identity restful-server rest1
[Sysname-restfulserver-rest1] login-name abc password simple 123
```

【相关命令】

- **display user-identity restful-server**
- **user-identity restful-server**

1.1.13 reset user-identity dynamic-online-user

reset user-identity dynamic-online-user 命令用来删除动态的在线身份识别用户。

【命令】

reset user-identity dynamic-online-user { **all** | { **domain** *domain-name* | **null-domain** } [**name** *user-name*] | { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**mac** *mac-address*] }

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

all：所有动态的在线身份识别用户信息。

domain *domain-name*：身份识别用户所属的身份识别域。*domain-name* 表示域名，为 1～255 个字符的字符串，不区分大小写。

null-domain：未加入任何身份识别域的身份识别用户信息。

name *user-name*：表示用户名，为 1～55 个字符的字符串，区分大小写。如果不指定该参数，则表示指定身份识别域或者未加入任何身份识别域的所有在线身份识别用户。

ip *ipv4-address*：身份识别用户的 IPv4 地址。

ipv6 *ipv6-address*：身份识别用户的 IPv6 地址。

mac *mac-address*：身份识别用户的 MAC 地址，格式为 H-H-H。若不指定该参数，则表示同一用户名，不同 MAC 地址的所有在线身份识别用户。

【使用指导】

动态的在线身份识别用户信息是指，设备从远程服务器上动态学习到的在线身份识别用户信息。静态的在线身份识别用户信息是由静态配置产生的，不能通过本命令删除，可以通过执行 **undo user-identity static-user** 命令删除。

【举例】

删除全部动态在线身份识别用户信息。

```
<Sysname> reset user-identity dynamic-online-user all
```

删除身份识别域 abc 下的所有动态在线身份识别用户信息。

```
<Sysname> reset user-identity dynamic-online-user domain abc
```

删除身份识别域 dom1 下名称为 user1 的动态在线身份识别用户信息。

```
<Sysname> reset user-identity dynamic-online-user domain dom1 name user1
```

删除用户名为 user2 且未加入任何身份识别域的动态在线身份识别用户信息。

```
<Sysname> reset user-identity dynamic-online-user null-domain name user2
```

删除 IP 地址为 1.2.3.4 的动态在线身份识别用户信息。

```
<Sysname> reset user-identity dynamic-online-user ip 1.2.3.4
```

删除 IP 地址为 1.2.3.4、MAC 地址为 2222-3333-4444 的动态在线身份识别用户信息。

```
<Sysname> reset user-identity dynamic-online-user ip 1.2.3.4 mac 2222-3333-4444
```

【相关命令】

- **display user-identity online-user**

1.1.14 reset user-identity user-account

reset user-identity user-account 命令用来删除身份识别用户账户。

【命令】

reset user-identity user-account { **all** | { **domain** *domain-name* | **null-domain** } [**name** *user-name*] }

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

all：所有身份识别用户账户信息。

domain *domain-name*：表示身份识别域的名称，为 1～255 个字符的字符串，不区分大小写。

null-domain：未加入任何身份识别域的身份识别用户账户信息。

name *user-name*：表示身份识别用户的账户名，为 1～55 个字符的字符串，区分大小写。若不指定该参数，则表示删除所有指定身份识别域的或未加入任何身份识别域的身份识别用户账户。

【使用指导】

此命令用来删除从服务器导入或者从 CSV 文件导入的身份识别用户账户信息。

从本地用户数据库中学习到的身份识别用户账户不能通过该命令删除。

【举例】

删除所有身份识别用户账户信息。

```
<Sysname> reset user-identity user-account all
```

删除身份识别域 dom1 下名称为 test 的身份识别用户账户信息。

```
<Sysname> reset user-identity user-account domain dom1 name test
```

【相关命令】

- **display user-identity all user**

1.1.15 reset user-identity user-group

reset user-identity user-group 命令用来删除身份识别用户组。

【命令】

reset user-identity user-group { **all** | { **domain** *domain-name* | **null-domain** } [**name** *group-name*] }

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

all：所有身份识别用户组信息。

domain *domain-name*：表示身份识别域的名称，为 1～255 个字符的字符串，不区分大小写。

null-domain：未加入任何身份识别域的身份识别用户组。

name *group-name*：身份识别用户组名，为 1～32 个字符的字符串，不区分大小写。若不指定该参数，则表示删除所有指定身份识别域的或未加入任何身份识别域的身份识别用户组。

【使用指导】

本命令用来删除从远程服务器和 CVS 文件导入的身份识别用户组，而从本地用户数据库学习到的身份识别用户组不能通过该命令删除。

【举例】

删除全部身份识别用户组信息。

```
<Sysname> reset user-identity user-group all
```

删除身份识别域 dom1 下名称为 g1 的身份识别用户组信息。

```
<Sysname> reset user-identity user-group domain dom1 name g1
```

【相关命令】

- **display user-identity all user-group**

1.1.16 restful-server

restful-server 命令用来指定 RESTful 服务器。

undo restful-server 命令用来恢复缺省情况。

【命令】

restful-server *server-name*

undo restful-server *server-name*

【缺省情况】

未指定 RESTful 服务器。

【视图】

身份识别用户导入策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

server-name：RESTful 服务器名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

指定的 RESTful 服务器中定义了 RESTful 服务器的相关参数,用户可以通过执行 **user-identity user-account import policy** 命令从该服务器上导入身份识别用户账户，通过执行 **user-identity online-user import policy** 命令从该服务器上导入在线身份识别用户。

最多只能指定一个 RESTful 服务器。如需指定其它的 RESTful 服务器，请先通过 **undo restful-server** 命令删除已经指定的 RESTful 服务器。

【举例】

在身份识别用户导入策略 policy1 中，指定名称为 ser1 的 RESTful 服务器。

```
<Sysname> system-view
[Sysname] user-identity user-import-policy policy1
[Sysname-identity-user-impt-policy-policy1] restful-server ser1
```

【相关命令】

- **display user-identity restful-server**
- **display user-identity user-import-policy**
- **user-identity restful-server**

1.1.17 uri

uri 命令用来指定 RESTful 服务器的 URI。

undo uri 命令用来删除指定的 RESTful 服务器 URI。

【命令】

uri { **get-online-user** | **get-user-database** | **get-user-group-database** | **put-offline-user** | **put-online-user** } *uri-string*

undo uri { **get-online-user** | **get-user-database** | **get-user-group-database** | **put-offline-user** | **put-online-user** }

【缺省情况】

未指定 RESTful 服务器的 URI。

【视图】

RESTful 服务器视图

【缺省用户角色】

network-admin

context-admin

【参数】

get-online-user：表示请求网络接入类在线用户信息的 URI。

get-user-database：表示请求网络接入类用户账户信息的 URI。

get-user-group-database：表示请求用户组信息的 URI。

put-offline-user：表示上传下线用户信息的 URI。

put-online-user：表示上传在线用户信息的 URI。

uri-string：URI 名称，为 1～255 字符的字符串，不区分大小写。

【使用指导】

本命令指定的 URI 必须与 RESTful 服务器上提供各类用户资源服务的 URI 保持一致，否则将会导致用户信息交互失败。

新增或删除一个在线身份识别用户时，若该用户来源不是指定的 RESTful 服务器，则设备会将这些上线/下线用户信息上传给 RESTful 服务器。

可通过多次执行本命令，指定的不同服务类型的 RESTful 服务器 URI。

【举例】

指定向 RESTful 服务器 rest1 请求网络接入类在线用户信息的 URI 为 http://1.1.1.1:8080/imcrs/ssm/imcuser/onlineUser。

```
<Sysname> system-view
[Sysname] user-identity restful-server rest1
[Sysname-restfulserver-rest1] uri get-online-user
http://1.1.1.1:8080/imcrs/ssm/imcuser/onlineUser
```

指定向 RESTful 服务器 rest1 请求网络接入类用户账户信息的 URI 为 http://1.1.1.1:8080/imcrs/ssm/imcuser/accessUser。

```
<Sysname> system-view
[Sysname] user-identity restful-server rest1
[Sysname-restfulserver-rest1] uri get-user-database
http://1.1.1.1:8080/imcrs/ssm/imcuser/accessUser
```

指定向 RESTful 服务器 rest1 请求用户组信息的 URI 为 http://1.1.1.1:8080/imcrs/ssm/imcuser/accessUserGroup。

```
<Sysname> system-view
[Sysname] user-identity restful-server rest1
```

```
[Sysname-restfulserver-rest1] uri get-user-group-database
http://1.1.1.1:8080/imcrs/ssm/imcuser/accessUserGroup
```

指定向 RESTful 服务器 rest1 上传下线用户信息的 URI 为 http://1.1.1.1:8080/imcrs/ssm/imcuser/uploadOfflineUser。

```
<Sysname> system-view
[Sysname] user-identity restful-server rest1
[Sysname-restfulserver-rest1] uri put-offline-user
http://1.1.1.1:8080/imcrs/ssm/imcuser/uploadOfflineUser
```

指定向 RESTful 服务器 rest1 上传在线用户信息的 URI 为 http://1.1.1.1:8080/imcrs/ssm/imcuser/uploadOnlineUser。

```
<Sysname> system-view
[Sysname] user-identity restful-server rest1
[Sysname-restfulserver-rest1] uri put-online-user
http://1.1.1.1:8080/imcrs/ssm/imcuser/uploadOnlineUser
```

【相关命令】

- **display user-identity restful-server**
- **user-identity restful-server**

1.1.18 user-identity enable

user-identity enable 命令用来开启用户身份识别功能。

undo user-identity enable 命令用来关闭用户身份识别功能。

【命令】

user-identity enable

undo user-identity enable

【缺省情况】

用户身份识别功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

开启用户身份识别功能后，用户身份识别模块才会与接入模块以及应用模块一起联动实现基于用户身份的访问控制。

【举例】

开启用户身份识别功能。

```
<Sysname> system-view
[Sysname] user-identity enable
```

1.1.19 user-identity online-user import policy

user-identity online-user import policy 命令用来导入服务器上的在线身份识别用户。

【命令】

user-identity online-user import policy *policy-name*

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name：身份识别用户导入策略名，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

执行该命令后，系统将向身份识别用户导入策略中指定的服务器发起一次连接请求，之后导入服务器上的网络接入类在线用户信息（用户名、身份识别域名、用户组名、IP 地址、MAC 地址）。

只有用户身份识别功处于开启状态，才能成功执行本命令。

【举例】

从名称为 policy1 的身份识别用户导入策略指定的服务器上导入在线身份识别用户。

```
<Sysname> system-view
[Sysname] user-identity online-user import policy policy1
Loading...Done.
```

【相关命令】

- **user-identity user-account auto-import policy**
- **user-identity user-import-policy**

1.1.20 user-identity online-user-name-match

user-identity online-user-name-match 命令用来配置在线用户身份识别的用户名匹配模式。

undo user-identity online-user-name-match 命令用来恢复缺省情况。

【命令】

user-identity online-user-name-match { **keep-original** | **with-domain** | **without-domain** }

undo user-identity online-user-name-match

【缺省情况】

在线用户身份识别的用户名匹配模式为 **keep-original**。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

keep-original：使用用户输入的用户名进行身份识别用户账户匹配。例如，用户的认证域为 abc，用户输入的用户名为 test@123，则使用用户名 test@123 进行身份识别用户账户匹配。

with-domain：使用用户的认证域进行身份识别用户账户匹配，即将采用“用户的纯用户名@认证域名”格式进行用户账户匹配。例如，用户的认证域为 abc，用户输入的用户名为 test@123，则使用用户名 test@abc 进行身份识别用户账户匹配。

without-domain：不对用户账户的域名进行匹配，即使用用户输入的纯用户名与设备上未加入任何身份识别域的身份识别用户账户进行匹配。例如，用户的认证域为 abc，用户输入的用户名为 test@123，则使用用户名 test 与未加入身份识别域的用户账户进行匹配。

【使用指导】

设备创建一条在线身份识别用户表项之前，首先检查该用户是否能够匹配上本地的身份识别用户账户，如果能够匹配上，才会生成对应的在线身份识别用户表项。本命令用来配置设备采用哪种用户名格式去匹配身份识别用户账户。

【举例】

配置在线用户身份识别的用户名匹配模式 with-domain。

```
<Sysname> system-view
[Sysname] user-identity online-user-name-match with-domain
```

1.1.21 user-identity restful-server

user-identity restful-server 命令用来创建 RESTful 服务器，并进入 RESTful 服务器视图。如果指定的 RESTful 服务器已经存在，则直接进入 RESTful 服务器视图。

undo user-identity restful-server 命令用来删除指定的 RESTful 服务器。

【命令】

user-identity restful-server *server-name*

undo user-identity restful-server *server-name*

【缺省情况】

不存在 RESTful 服务器。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

server-name：RESTful 服务器的名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

RESTful 服务器视图用于配置 RESTful 服务器的相关参数，包括服务器 URI 和登录用户。

系统中仅能存在一个 RESTful 服务器。

【举例】

创建名称为 rest1 的 RESTful 服务器，并进入该服务器视图。

```
<Sysname> system-view
[Sysname] user-identity restful-server rest1
[Sysname-restfulserver-rest1]
```

【相关命令】

- **display user-identity restful-server**
- **login-name**
- **uri**
- **user-identity user-import-policy**

1.1.22 user-identity static-user

user-identity static-user 命令用来配置静态类型的身份识别用户。

undo user-identity static-user 命令用来删除指定的静态类型的身份识别用户。

【命令】

user-identity static-user *user-name* [**domain** *domain-name*] **bind** { **ipv4** *ipv4-address* | **ipv6** *ipv6-address* } [**mac** *mac-address*]

undo user-identity static-user *user-name* [**domain** *domain-name*] [**bind** { **ipv4** *ipv4-address* | **ipv6** *ipv6-address* } [**mac** *mac-address*]]

【缺省情况】

不存在静态类型的身份识别用户。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

user-name：静态类型的身份识别用户名，为 1～55 个字符的字符串，区分大小写。

domain *domain-name*：指定用户所属的身份识别域。*domain-name* 表示身份识别域的名称，为 1～255 个字符的字符串，不区分大小写。若不指定该参数，则表示用户不属于任何身份识别域。

bind：指定与该用户名绑定的 IP 地址属性。

ipv4 *ipv4-address*：指定用户的 IPv4 地址。*ipv4-address* 不能为全 0 地址、全 1 地址以及组播 IP 地址。

ipv6 *ipv6-address*：指定用户的 IPv6 地址。*ipv6-address* 不能为全 0 地址、组播地址、环回地址以及链路本地地址。

mac *mac-address*：指定用户的 MAC 地址，格式为 H-H-H。若不指定该参数，则表示不限制该 IP 地址用户的 MAC 地址。

【使用指导】

当管理员允许某些用户不需要通过认证，也能够在相关安全特性的管理下访问网络时，就可以通过本命令将这类用户手工添加为身份识别用户。

若 **undo** 命令中不指定 **bind** 参数，则表示删除使用指定用户名的所有静态类型的身份识别用户。

可以通过多次执行本命令添加多个静态类型的身份识别用户。

一个用户名可以绑定多个 IP 地址或者多个 IP 地址和 MAC 地址的组合，但同一个 IP 地址或者 IP 地址和 MAC 地址的组合不能被多个用户名绑定。

配置的静态类型的身份识别用户，只有在用户身份识别功能处于开启状态，且能够匹配上本地身份识别用户账户的情况下，才能生成对应的静态在线身份识别用户。

【举例】

配置一个静态类型的身份识别用户：用户名为 test，身份识别域为 dom1，绑定的 IP 地址为 109.15.0.15。

```
<Sysname> system-view
[Sysname] user-identity static-user test domain dom1 bind ipv4 109.15.0.15
```

【相关配置】

- **display user-identity online-user**
- **user-identity enable**

1.1.23 user-identity user-account auto-import policy

user-identity user-account auto-import policy 命令用来开启身份识别用户账户自动导入功能。

undo user-identity user-account auto-import policy 命令用来关闭身份识别用户账户自动导入功能。

【命令】

user-identity user-account auto-import policy *policy-name*

undo user-identity user-account auto-import policy *policy-name*

【缺省情况】

身份识别用户自动账户导入功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name：身份识别用户导入策略名，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

开启指定策略的身份识别用户账户自动导入功能后，身份识别模块首先会从该策略指定的服务器上导入所有身份识别用户账户信息和所有在线身份识别用户信息，然后定期从该服务器上自动导入身份识别用户账户信息（导入周期由 **account-update-interval** 命令配置）。

需要注意的是，成功导入在线身份识别用户信息的前提是，用户身份识别功能处于开启状态（通过 **user-identity enable** 命令配置）。

【举例】

开启策略 policy1 的身份识别用户账户自动导入功能。

```
<Sysname> system-view
[Sysname] user-identity user-account auto-import policy policy1
```

【相关命令】

- **account-update-interval**
- **user-identity user-import-policy**

1.1.24 user-identity user-account export url

user-identity user-account export url 命令用来将身份识别用户账户导出到 CSV 文件。

【命令】

user-identity user-account export url *url-string* [{ **domain** *domain-name* | **null-domain** } [**user** *user-name*] | **template**] [**vpn-instance** *vpn-instance-name*]

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

url-string：URL，为 1～255 字符的字符串，不区分大小写。

domain *domain-name*：身份识别域的名称，为 1～255 个字符的字符串，不区分大小写。

null-domain：表示导出未加入身份识别域的所有身份识别用户账户信息。

user *user-name*：身份识别用户账户名，为 1～55 个字符的字符串，区分大小写。若不指定该参数，则表示指定条件下的所有身份识别用户账户。

template：表示导出一个标准的 CSV 文件模板。用户可根据此模板编辑符合设备要求的 CSV 文件用于导入身份识别用户。

vpn-instance *vpn-instance-name*：表示 CSV 文件保存路径所属 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。若未指定该参数，则表示 CSV 文件保存路径位于公网。

【使用指导】

身份识别用户账户信息导出时必须以 CSV 格式保存，即保存的文件扩展名为 csv。

若不指定任何参数，则表示将设备上的所有身份识别用户账户信息导出到一个 CSV 文件。

本命令支持 TFTP 和 FTP 两种文件上传方式，具体的 URL 格式要求如下：

- TFTP 协议 URL 格式：tftp://server/path/filename，server 为 TFTP 服务器 IP 地址或主机名，例如 tftp://1.1.1.1/user/user.csv。
- FTP 协议 URL 格式：
  - 携带用户名和密码的格式为 ftp://username:password@server/path/filename。其中，username 为 FTP 用户名，password 为 FTP 认证密码，server 为 FTP 服务器 IP 地址或主机名，例如 ftp://1:1@1.1.1.1/user/user.csv。如果 FTP 用户名中携带域名，则该域名会被设备忽略，例如 ftp://1@abc:1@1.1.1.1/user/user.csv 将被当作 ftp://1:1@1.1.11/user/user.csv 处理。
  - 不需要携带用户名和密码的格式为 ftp://server/path/filename，例如 ftp://1.1.1.1/user/user.csv。
  - FTP 协议 URL 字符串中的用户名或密码携带表 1-8 中的特殊字符时，需要按照对应的输入格式输入才能正常执行操作。

表1-8 特殊字符输入对照表

特殊字符	输入格式
\	\\
"	\"
/	%2F
:	%3A
@	%40

成功执行该命令后，将会在目标服务器上生成一个指定名称的 CSV 文件。若相同配置条件下重复导出，新的文件将会覆盖已有文件。

【举例】

将身份识别域 dom1 中的所有身份识别用户账户信息导出到 CSV 文件中，文件保存路径为 tftp://1.1.1.1/user.csv。

```
<Sysname> system-view
[Sysname] user-identity user-account export url tftp://1.1.1.1/user.csv domain dom1
```

【相关命令】

- **user-identity user-account import url**

1.1.25 user-identity user-account import policy

user-identity user-account import policy 命令用来导入服务器上的身份识别用户账户。

【命令】

user-identity user-account import policy *policy-name*

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name：身份识别用户导入策略名，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

执行该命令后，系统将立即向身份识别用户导入策略中指定的服务器发起请求，并导入服务器上的所有身份识别用户账户信息。

【举例】

从名称为 policy1 的身份识别用户导入策略指定的服务器上导入身份识别用户账户。

```
<Sysname> system-view
[Sysname] user-identity user-account import policy policy1
```

【相关命令】

- **user-identity user-import-policy**

1.1.26 user-identity user-account import url

user-identity user-account import url 命令用来从 CSV 文件中导入身份识别用户账户。

【命令】

user-identity user-account import url *url-string* [**vpn-instance** *vpn-instance-name*] [**auto-create-group** | **override** | **start-line** *line-number*] *

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

url-string：要导入的 CSV 文件的 URL，为 1～255 个字符的字符串，不区分大小写。

vpn-instance *vpn-instance-name*：表示待导入 CSV 文件所属 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。若未指定该参数，则表示 CSV 文件保存路径位于公网。

auto-create-group：表示当设备上不存在身份识别用户账户所属的身份识别用户组时，系统会自动创建该身份识别用户组。若不指定该参数，则表示当设备上不存在该身份识别用户组时，系统不会创建该身份识别用户组。

override：表示当导入的身份识别用户账户已经存在于设备上时，系统使用导入的身份识别用户账户覆盖掉已有的同名身份识别用户账户。若不指定该参数，则表示不导入文件中的同名身份识别用户账户信息，即保留设备上原有的同名身份识别用户账户信息。

start-line *line-number*：表示从 CSV 文件的指定行开始导入身份识别用户账户。*line-number* 为文件内容的行编号，取值范围为 1～1048576。若不指定该参数，则表示从文件中第一行开始导入。

【使用指导】

导入文件必须是 CSV 格式，即文件扩展名为 csv。

可以通过 **user-identity user-account export url** 命令导出符合导入要求的 CSV 文件模板。

【举例】

从 ftp://1.1.1.1/newpath 路径的 user.csv 文件中导入身份识别用户账户信息，且从该文件的第二行开始导入。

```
<Sysname> system-view
[Sysname] user-identity user-account import url ftp://1.1.1.1/newpath/user.csv start-line
2
```

【相关命令】

- **user-identity user-account export url**

1.1.27 user-identity user-import-policy

user-identity user-import-policy 命令用来创建身份识别用户导入策略，并进入身份识别用户导入策略视图。如果指定的身份识别用户导入策略已经存在，则直接进入身份识别用户导入策略视图。

undo user-identity user-import-policy 命令用来删除指定的身份识别用户导入策略。

【命令】

user-identity user-import-policy *policy-name*

undo user-identity user-import-policy *policy-name*

【缺省情况】

不存在身份识别用户导入策略。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name：策略名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

身份识别用户导入策略用于配置用户身份识别模块从服务器上导入身份识别用户信息的策略，可导入的用户信息包括身份识别用户账户信息和在线身份识别用户信息。目前，系统支持的服务器为H3C iMC 服务器和 LDAP 服务器。

系统中仅能存在一个身份识别用户导入策略。如需配置其它身份识别用户导入策略，请先通过 **undo user-identity user-import-policy** 命令删除已有的身份识别用户导入策略。

【举例】

创建名称为 policy1 的身份识别用户导入策略，并进入该策略视图。

```
<Sysname> system-view
[Sysname] user-identity user-import-policy policy1
[Sysname-identity-user-impt-policy-policy1]
```

【相关命令】

- **display user-identity user-import-policy**

1.1.28 vpn-instance

vpn-instance 命令用来配置 RESTful 服务器所属的 VPN。

undo vpn-instance 命令用来恢复缺省情况。

【命令】

vpn-instance *vpn-instance-name*

undo vpn-instance

【缺省情况】

未配置 RESTful 服务器的 VPN，表示 RESTful 服务器位于公网。

【视图】

RESTful 服务器视图

【缺省用户角色】

network-admin

context-admin

【参数】

vpn-instance-name：MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。

【使用指导】

本命令指定的 VPN 为设备与 RESTful 服务器通信的接口所属的 VPN。

【举例】

配置 RESTful 服务器的所属的 VPN 为 v1。

```
<Sysname> system-view
[Sysname] user-identity restful-server r1
[Sysname-restfulserver-r1] vpn-instance v1
```

【相关命令】

- **display user-identity restful-server**
- **user-identity restful-server**