目 录

1 RBAC

1.1 RBAC配置命令

1.1.1 description

description 命令用来配置用户角色的描述信息，用来方便管理员对用户角色进行管理。

undo description 命令用来恢复缺省情况。

【命令】

description *text*

undo description

【缺省情况】

未定义用户角色描述信息。

【视图】

用户角色视图

【缺省用户角色】

network-admin

context-admin

【参数】

text：用户角色描述信息，为 1～128 个字符的字符串，区分大小写。

【举例】

为用户角色 role1 配置描述信息为“labVIP”。

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] description labVIP
```

【相关命令】

- **display role**
- **role**

1.1.2 display role

display role 命令用来显示用户角色信息。

【命令】

display role [**name** *role-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

name *role-name*：用户角色名称，为 1～63 个字符的字符串，区分大小写。如果不指定用户角色名称，则表示显示所有用户角色的信息，包括系统缺省存在的用户角色的信息。

【举例】

显示用户角色 123 的信息。

```
<Sysname> display role name 123
Role: 123
  Description: new role
  VLAN policy: Deny
  Permitted VLANs: 1 to 5, 7 to 8
  Interface policy: Deny
  Permitted interfaces: GigabitEthernet1/0/1 to GigabitEthernet1/0/3, Vlan-interface1 to
Vlan-interface20
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
```

显示所有用户角色的信息。

```
<Sysname> display role
Role: network-admin
  Description: Predefined network admin role has access to all commands on the device
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ----------------------------------------------------------------------
  Rule    Perm    Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       *
  sys-2   permit RWX   web-menu      -
  sys-3   permit RWX   xml-element   -
  sys-4   deny         command       display security-logfile summary
  sys-5   deny         command       system-view ; info-center securi
                                     ty-logfile directory *
  sys-6   deny         command       security-logfile save
  sys-7   permit RW-   oid           1
  R:Read W:Write X:Execute

Role: network-operator
  Description: Predefined network operator role has access to all read commands on the device
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
```

```
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       display *
  sys-2   permit       command       xml
  sys-3   deny         command       display history-command all
  sys-4   deny         command       display exception *
  sys-5   deny         command       display cpu-usage configuration
                                     *
  sys-6   deny         command       display kernel exception *
  sys-7   deny         command       display kernel deadloop *
  sys-8   deny         command       display kernel starvation *
  sys-9   deny         command       display kernel reboot *
  sys-12  permit       command       system-view ; local-user *
  sys-13  permit       command       system-view ; switchto *
  sys-14  permit R--   web-menu      -
  sys-15  permit RW-   web-menu      m_device/m_maintenance/m_changep
                                     assword
  sys-16  permit R--   xml-element   -
  sys-17  deny         command       display security-logfile summary
  sys-18  deny         command       system-view ; info-center securi
                                     ty-logfile directory *
  sys-19  deny         command       security-logfile save
  sys-20  deny         command       system-view ; local-user-import
                                     *
  sys-21  deny         command       system-view ; local-user-export
                                     *
  sys-22  permit R--   oid           1
  R:Read W:Write X:Execute

Role: context-admin
  Description: Predefined context admin role has access to all commands within a context
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       *
  sys-2   permit RWX   web-menu      -
  sys-3   permit RWX   xml-element   -
  sys-4   deny   RWX   feature       context
  sys-5   permit       command       display context *
  sys-6   deny         command       display security-logfile summary
  sys-7   deny         command       system-view ; info-center securi
```

```
                                    ty-logfile directory *
  sys-8   deny         command       security-logfile save
  sys-9   permit RW-   oid           1
  R:Read W:Write X:Execute

Role: context-operator
  Description: Predefined context operator role has access to all read commands within a
context
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ------------------------------------------------------------------
  sys-1   permit       command       display *
  sys-2   permit       command       xml
  sys-3   deny         command       display history-command all
  sys-4   deny         command       display exception *
  sys-5   deny         command       display cpu-usage configuration
                                     *
  sys-6   deny         command       display kernel exception *
  sys-7   deny         command       display kernel deadloop *
  sys-8   deny         command       display kernel starvation *
  sys-9   deny         command       display kernel reboot *
  sys-12  permit       command       system-view ; local-user *
  sys-13  permit R--   web-menu      -
  sys-14  permit RW-   web-menu      m_device/m_maintenance/m_changep
                                     assword
  sys-15  permit R--   xml-element   -
  sys-16  deny         command       display security-logfile summary
  sys-17  deny         command       system-view ; info-center securi
                                     ty-logfile directory *
  sys-18  deny         command       security-logfile save
  sys-19  permit R--   oid           1
  R:Read W:Write X:Execute

Role: level-0
  Description: Predefined level-0 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ------------------------------------------------------------------
  sys-1   permit       command       tracert *
  sys-2   permit       command       telnet *
  sys-3   permit       command       ping *
```

```
  sys-4   permit       command       ssh2 *
  sys-5   permit       command       super *
  R:Read W:Write X:Execute

Role: level-1
  Description: Predefined level-1 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       tracert *
  sys-2   permit       command       telnet *
  sys-3   permit       command       ping *
  sys-4   permit       command       ssh2 *
  sys-5   permit       command       display *
  sys-6   permit       command       super *
  sys-7   deny         command       display history-command all
  R:Read W:Write X:Execute

Role: level-2
  Description: Predefined level-2 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)

Role: level-3
  Description: Predefined level-3 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)

Role: level-4
  Description: Predefined level-4 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)

Role: level-5
  Description: Predefined level-5 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
```

```
  Security zone policy: Permit (default)

Role: level-6
  Description: Predefined level-6 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)

Role: level-7
  Description: Predefined level-7 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)

Role: level-8
  Description: Predefined level-8 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)

Role: level-9
  Description: Predefined level-9 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ------------------------------------------------------------------
  sys-1   permit RWX   feature       -
  sys-2   deny   RWX   feature       device
  sys-3   deny   RWX   feature       filesystem
  sys-4   permit       command       display *
  sys-5   deny         command       display history-command all
  R:Read W:Write X:Execute

Role: level-10
  Description: Predefined level-10 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)

Role: level-11
  Description: Predefined level-11 role
```

```
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)

Role: level-12
  Description: Predefined level-12 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)

Role: level-13
  Description: Predefined level-13 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)

Role: level-14
  Description: Predefined level-14 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)

Role: level-15
  Description: Predefined level-15 role
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ------------------------------------------------------------------
  sys-1   permit       command       *
  sys-2   permit RWX   web-menu      -
  sys-3   permit RWX   xml-element   -
  sys-4   deny         command       display security-logfile summary
  sys-5   deny         command       system-view ; info-center securi
                                     ty-logfile directory *
  sys-6   deny         command       security-logfile save
  sys-7   permit RW-   oid           1
  R:Read W:Write X:Execute

Role: security-audit
  Description: Predefined security audit role only has access to commands for the security
log administrator
  VLAN policy: Permit (default)
```

```
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   deny         command       *
  sys-2   permit       command       display security-logfile summary
  sys-3   permit       command       system-view ; info-center securi
                                     ty-logfile directory *
  sys-4   permit       command       security-logfile save
  sys-5   permit       command       cd *
  sys-6   permit       command       copy *
  sys-7   permit       command       delete *
  sys-8   permit       command       dir *
  sys-9   permit       command       mkdir *
  sys-10  permit       command       more *
  sys-11  permit       command       move *
  sys-12  permit       command       rmdir *
  sys-13  permit       command       pwd
  sys-14  permit       command       rename *
  sys-15  permit       command       undelete *
  sys-16  permit       command       ftp *
  sys-17  permit       command       sftp *
  R:Read W:Write X:Execute

Role: guest-manager
  Description: Predefined guest manager role can't access to commands
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit RWX   xml-element   useraccounts/approveguest/
  sys-2   permit RWX   xml-element   useraccounts/exportguestaccount/
  sys-3   permit RWX   xml-element   useraccounts/generateguestaccoun
                                     t/
  sys-4   permit RWX   xml-element   useraccounts/guest/
  sys-5   permit RWX   xml-element   useraccounts/guestconfigure/
  sys-6   permit RWX   xml-element   useraccounts/importguestaccount/
  sys-7   permit RWX   xml-element   useraccounts/exportguesttemplet/
  sys-8   permit RWX   xml-element   rpc/
  sys-9   permit RWX   web-menu      m_global/m_networksecurity/m_gue
                                     stmanage/m_guestlist/
  sys-10  permit RWX   web-menu      m_global/m_networksecurity/m_gue
                                     stmanage/m_importguest/
```

```
  sys-11  permit RWX   web-menu      m_global/m_networksecurity/m_gue
                                     stmanage/m_generateguest/
  sys-12  permit RWX   web-menu      m_global/m_networksecurity/m_gue
                                     stmanage/m_approveguest/
  sys-13  deny         command       *
  R:Read W:Write X:Execute

Role: system-admin
  Description: Predefined system admin role only has access to commands for the system
administrator
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ---------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ---------------------------------------------------------------------
  sys-1   permit RWX   web-menu      dashboard/
  sys-2   permit RWX   web-menu      m_monitor/m_monitorlog/m_syslog
  sys-3   permit RWX   web-menu      m_device/m_virtualdevice/m_clust
                                     er
  sys-4   permit RWX   web-menu      m_device/m_virtualdevice/m_conte
                                     xt/
  sys-5   permit RWX   web-menu      m_device/m_highavailability/m_ho
                                     tbackup
  sys-6   permit RWX   web-menu      m_device/m_highavailability/m_vr
                                     rp
  sys-7   permit RWX   web-menu      m_device/m_highavailability/m_vr
                                     rpinterface
  sys-8   permit RWX   web-menu      m_device/m_logconf/m_basiclog
  sys-9   permit RWX   web-menu      m_device/m_logconf/m_natlog
  sys-10  permit RWX   web-menu      m_device/m_logconf/m_sessionlog
  sys-11  permit RWX   web-menu      m_device/m_logconf/m_atkadvancel
                                     og
  sys-12  permit RWX   web-menu      m_device/m_logconf/m_threatenlog
  sys-13  permit RWX   web-menu      m_device/m_logconf/m_urlfilterlo
                                     g
  sys-14  permit RWX   web-menu      m_device/m_logconf/m_auditlog
  sys-15  permit RWX   web-menu      m_device/m_logconf/m_cfgadvancel
                                     og
  sys-16  permit RWX   web-menu      m_device/m_reportconf/m_reportsu
                                     bscription
  sys-17  permit RWX   web-menu      m_device/m_reportconf/m_mailserv
                                     erconfig
  sys-18  permit RWX   web-menu      m_device/m_persistdisk
  sys-19  permit RWX   web-menu      m_device/m_sessionagingtimeset/m
                                     _protocolstatesessionagingtime
  sys-20  permit RWX   web-menu      m_device/m_sessionagingtimeset/m
                                     _appagingtime
```

```
  sys-21  permit RWX   web-menu      m_device/m_sessionagingtimeset/m
                                     _sessionsettings
  sys-22  permit RWX   web-menu      m_device/m_signatureupgrade/m_up
                                     gradecenter
  sys-23  permit RWX   web-menu      m_device/m_signatureupgrade/m_up
                                     grade
  sys-24  permit RWX   web-menu      m_device/m_license
  sys-25  permit RWX   web-menu      m_device/m_maintenance/m_devices
                                     ettings/
  sys-26  permit RWX   web-menu      m_device/m_maintenance/m_config
  sys-27  permit RWX   web-menu      m_device/m_maintenance/m_diagnos
                                     tic
  sys-28  permit RWX   web-menu      m_device/m_maintenance/m_pcapwar
                                     e
  sys-29  permit RWX   web-menu      m_device/m_maintenance/m_reboot
  sys-30  permit RWX   web-menu      m_device/m_maintenance/m_about/
  sys-31  permit RWX   web-menu      m_device/m_maintenance/m_changep
                                     assword
  sys-32  permit RWX   web-menu      m_device/m_adminuser/m_admin
  sys-33  permit RWX   web-menu      m_device/m_adminuser/m_rbacrole
  sys-34  permit       command       tracert *
  sys-35  permit       command       ping *
  R:Read W:Write X:Execute

Role: security-admin
  Description: Predefined security admin role only has access to commands for the security
administrator
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit RWX   web-menu      m_monitor/m_atklog/m_blacklistlo
                                     g
  sys-2   permit RWX   web-menu      m_monitor/m_atklog/m_singleatk
  sys-3   permit RWX   web-menu      m_monitor/m_atklog/m_scanatk
  sys-4   permit RWX   web-menu      m_monitor/m_atklog/m_floodatk
  sys-5   permit RWX   web-menu      m_monitor/m_atklog/m_threatlog
  sys-6   permit RWX   web-menu      m_monitor/m_atklog/m_urllog
  sys-7   permit RWX   web-menu      m_monitor/m_atklog/m_filefilterl
                                     og
  sys-8   permit RWX   web-menu      m_monitor/m_atklog/m_zonepairlog
  sys-9   permit RWX   web-menu      m_monitor/m_auditlogs/m_auditimc
                                     hatlog
  sys-10  permit RWX   web-menu      m_monitor/m_auditlogs/m_auditcom
                                     munitylog
  sys-11  permit RWX   web-menu      m_monitor/m_auditlogs/m_auditsea
```

```
                                    rchenginelog
sys-12  permit RWX   web-menu       m_monitor/m_auditlogs/m_auditmai
                                    llog
sys-13  permit RWX   web-menu       m_monitor/m_auditlogs/m_auditfil
                                    etransferlog
sys-14  permit RWX   web-menu       m_monitor/m_auditlogs/m_auditrel
                                    axstocklog
sys-15  permit RWX   web-menu       m_monitor/m_auditlogs/m_auditoth
                                    erapplog
sys-16  permit RWX   web-menu       m_monitor/m_monitorlog/m_traffic
                                    log
sys-17  permit RWX   web-menu       m_monitor/m_rank/m_trafficrank/
sys-18  permit RWX   web-menu       m_monitor/m_rank/m_threadrank/
sys-19  permit RWX   web-menu       m_monitor/m_rank/m_urlfilterrank
                                    /
sys-20  permit RWX   web-menu       m_monitor/m_rank/m_ffilterrank/
sys-21  permit RWX   web-menu       m_monitor/m_rank/m_securityaudit
                                    /
sys-22  permit RWX   web-menu       m_monitor/m_rank/m_lb_serverrepo
                                    rt/
sys-23  permit RWX   web-menu       m_monitor/m_rank/m_lb_linkreport
                                    /
sys-24  permit RWX   web-menu       m_monitor/m_rank/m_lb_dnsproxyre
                                    port/
sys-25  permit RWX   web-menu       m_monitor/m_rank/m_dropstats
sys-26  permit RWX   web-menu       m_monitor/m_trend/m_traffictrend
                                    /
sys-27  permit RWX   web-menu       m_monitor/m_trend/m_threadtrend/
sys-28  permit RWX   web-menu       m_monitor/m_trend/m_urlfiltertre
                                    nd/
sys-29  permit RWX   web-menu       m_monitor/m_trend/m_ffiltertrend
                                    /
sys-30  permit RWX   web-menu       m_monitor/m_trend/m_lb_urltrend
sys-31  permit RWX   web-menu       m_monitor/m_report
sys-32  permit RWX   web-menu       m_monitor/m_session
sys-33  permit RWX   web-menu       m_monitor/m_userinfocenter
sys-34  permit RWX   web-menu       m_monitor/m_lb_dnscaches
sys-35  permit RWX   web-menu       m_policy/m_firewall/m_secpolicy
sys-36  permit RWX   web-menu       m_policy/m_firewall/m_targetpoli
                                    cy
sys-37  permit RWX   web-menu       m_policy/m_firewall/m_redundancy
                                    rules
sys-38  permit RWX   web-menu       m_policy/m_attackdefense/m_atkpo
                                    licy
sys-39  permit RWX   web-menu       m_policy/m_attackdefense/m_clien
                                    tverifyprotectip
sys-40  permit RWX   web-menu       m_policy/m_attackdefense/m_black
                                    listmanual
```

```
sys-41  permit RWX   web-menu      m_policy/m_attackdefense/m_white
                                   listmanual
sys-42  permit RWX   web-menu      m_policy/m_attackdefense/m_clien
                                   tverifyzone
sys-43  permit RWX   web-menu      m_policy/m_attackdefense/m_connl
                                   imitpolicies
sys-44  permit RWX   web-menu      m_policy/m_attackdefense/m_urpf/
sys-45  permit RWX   web-menu      m_policy/m_nat/m_natbasicchange
sys-46  permit RWX   web-menu      m_policy/m_nat/m_natoutboundconf
                                   ig/
sys-47  permit RWX   web-menu      m_policy/m_nat/m_natserverconfig
                                   /
sys-48  permit RWX   web-menu      m_policy/m_nat/m_natstaticchange
                                   /
sys-49  permit RWX   web-menu      m_policy/m_nat/m_natoutbound444c
                                   onfig/
sys-50  permit RWX   web-menu      m_policy/m_nat/m_natoutboundstat
                                   ic444config/
sys-51  permit RWX   web-menu      m_policy/m_nat/m_natsettings/
sys-52  permit RWX   web-menu      m_policy/m_appaudit/m_auditpolic
                                   y
sys-53  permit RWX   web-menu      m_policy/m_appaudit/m_keywordgro
                                   ups
sys-54  permit RWX   web-menu      m_policy/m_bandwidthmanagement/m
                                   _bandwidthpolicy
sys-55  permit RWX   web-menu      m_policy/m_bandwidthmanagement/m
                                   _bandwidthchannel
sys-56  permit RWX   web-menu      m_policy/m_bandwidthmanagement/m
                                   _interfacebandwidth
sys-57  permit RWX   web-menu      m_policy/m_loadbalance/m_lb_glob
                                   alconfig/
sys-58  permit RWX   web-menu      m_policy/m_loadbalance/m_lb_serv
                                   er/
sys-59  permit RWX   web-menu      m_policy/m_loadbalance/m_lb_link
                                   /
sys-60  permit RWX   web-menu      m_resource/m_healthmonitor
sys-61  permit RWX   web-menu      m_policy/m_netshare/m_netsharepo
                                   licy
sys-62  permit RWX   web-menu      m_policy/m_netshare/m_netsharest
                                   atus
sys-63  permit RWX   web-menu      m_resource/m_user/m_usercontrol/
sys-64  permit RWX   web-menu      m_resource/m_user/m_authenticati
                                   on/
sys-65  permit RWX   web-menu      m_resource/m_user/m_access/
sys-66  permit RWX   web-menu      m_resource/m_dpi/m_ipscfg/
sys-67  permit RWX   web-menu      m_resource/m_dpi/m_antiviruscfg/
sys-68  permit RWX   web-menu      m_resource/m_dpi/m_dfltcfg/
sys-69  permit RWX   web-menu      m_resource/m_dpi/m_ufltcfg/
```

```
sys-70  permit RWX   web-menu      m_resource/m_dpi/m_ffltcfg/
sys-71  permit RWX   web-menu      m_resource/m_dpi/m_apprecognitio
                                   n/
sys-72  permit RWX   web-menu      m_resource/m_dpi/m_securityactio
                                   n/
sys-73  permit RWX   web-menu      m_resource/m_dpi/m_dpicfg
sys-74  permit RWX   web-menu      m_resource/m_objectgroup/m_ipv4o
                                   bjectgroup
sys-75  permit RWX   web-menu      m_resource/m_objectgroup/m_ipv6o
                                   bjectgroup
sys-76  permit RWX   web-menu      m_resource/m_objectgroup/m_macob
                                   jectgroup
sys-77  permit RWX   web-menu      m_resource/m_objectgroup/m_servi
                                   ceobjectgroup
sys-78  permit RWX   web-menu      m_resource/m_objectgroup/m_timer
                                   ange
sys-79  permit RWX   web-menu      m_resource/m_acl/m_ipv4acl
sys-80  permit RWX   web-menu      m_resource/m_acl/m_ipv6acl
sys-81  permit RWX   web-menu      m_resource/m_acl/m_macacl
sys-82  permit RWX   web-menu      m_resource/m_ssl/m_sslserver
sys-83  permit RWX   web-menu      m_resource/m_ssl/m_sslclient
sys-84  permit RWX   web-menu      m_resource/m_ssl/m_ssladvanceset
                                   tiing
sys-85  permit RWX   web-menu      m_resource/m_publickey/m_publick
                                   eylocal
sys-86  permit RWX   web-menu      m_resource/m_publickey/m_publick
                                   eypeer
sys-87  permit RWX   web-menu      m_resource/m_pki_cert/m_pki
sys-88  permit RWX   web-menu      m_resource/m_pki_cert/m_certific
                                   atepolicy
sys-89  permit RWX   web-menu      m_resource/m_pki_cert/m_certific
                                   atesubject
sys-90  permit RWX   web-menu      m_network/m_vrf
sys-91  permit RWX   web-menu      m_network/m_if/m_interface
sys-92  permit RWX   web-menu      m_network/m_if/m_inline
sys-93  permit RWX   web-menu      m_network/m_if/m_collaborations
sys-94  permit RWX   web-menu      m_network/m_if/m_lagg
sys-95  permit RWX   web-menu      m_network/m_seczone
sys-96  permit RWX   web-menu      m_network/m_link/m_vlan
sys-97  permit RWX   web-menu      m_network/m_link/m_mac
sys-98  permit RWX   web-menu      m_network/m_dns_sum/m_dnshosts
sys-99  permit RWX   web-menu      m_network/m_dns_sum/m_dns
sys-100 permit RWX   web-menu      m_network/m_dns_sum/m_ddns
sys-101 permit RWX   web-menu      m_network/m_dns_sum/m_dnsadvance
sys-102 permit RWX   web-menu      m_network/m_ip_net/m_ip
sys-103 permit RWX   web-menu      m_network/m_ip_net/m_arp
sys-104 permit RWX   web-menu      m_network/m_ipv6_net/m_ipv6
sys-105 permit RWX   web-menu      m_network/m_ipv6_net/m_nd
```

```
  sys-106 permit RWX   web-menu      m_network/m_vpn/m_gre
  sys-107 permit RWX   web-menu      m_network/m_vpn/m_ipsec/
  sys-108 permit RWX   web-menu      m_network/m_vpn/m_advpn/
  sys-109 permit RWX   web-menu      m_network/m_vpn/m_l2tp/
  sys-110 permit RWX   web-menu      m_network/m_sslvpn/m_sslvpn_cont
                                     ext
  sys-111 permit RWX   web-menu      m_network/m_sslvpn/m_sslvpn_gate
                                     way
  sys-112 permit RWX   web-menu      m_network/m_sslvpn/m_sslvpn_ipv4
                                     addrpool
  sys-113 permit RWX   web-menu      m_network/m_sslvpn/m_sslvpn_acif
  sys-114 permit RWX   web-menu      m_network/m_sslvpn/m_sslvpn_stat
                                     istics
  sys-115 permit RWX   web-menu      m_network/m_routing/m_routingtab
                                     le
  sys-116 permit RWX   web-menu      m_network/m_routing/m_staticrout
                                     ing
  sys-117 permit RWX   web-menu      m_network/m_routing/m_policyrout
                                     ing/
  sys-118 permit RWX   web-menu      m_network/m_routing/m_ospf
  sys-119 permit RWX   web-menu      m_network/m_routing/m_bgp
  sys-120 permit RWX   web-menu      m_network/m_routing/m_rip
  sys-121 permit RWX   web-menu      m_network/m_multicast/m_multicas
                                     trouting
  sys-122 permit RWX   web-menu      m_network/m_multicast/m_pim
  sys-123 permit RWX   web-menu      m_network/m_multicast/m_igmp
  sys-124 permit RWX   web-menu      m_network/m_dhcp/m_dhcpservice
  sys-125 permit RWX   web-menu      m_network/m_dhcp/m_dhcppool
  sys-126 permit RWX   web-menu      m_network/m_ipservice/m_http
  sys-127 permit RWX   web-menu      m_network/m_ipservice/m_ssh
  sys-128 permit RWX   web-menu      m_network/m_ipservice/m_ntp
  sys-129 permit RWX   web-menu      m_network/m_ipservice/m_ftp
  sys-130 permit RWX   web-menu      m_network/m_ipservice/m_telnet
  sys-131 permit RWX   web-menu      m_network/m_probe/m_ping
  sys-132 permit RWX   web-menu      m_network/m_probe/m_tracert
  sys-133 permit RWX   web-menu      m_device/m_maintenance/m_changep
                                     assword
  sys-134 permit       command       tracert *
  sys-135 permit       command       ping *
  R:Read W:Write X:Execute

Role: audit-admin
  Description: Predefined audit admin role only has access to commands for the audit
administrator
  VLAN policy: Permit (default)
  Interface policy: Permit (default)
  VPN instance policy: Permit (default)
  Security zone policy: Permit (default)
  ------------------------------------------------------------------
```

```
Rule    Perm   Type  Scope         Entity
------------------------------------------------------------------
sys-1   permit RWX   web-menu      m_monitor/m_monitorlog/m_operati
                                   onlog
sys-2   permit RWX   web-menu      m_device/m_maintenance/m_changep
                                   assword
sys-3   permit       command       tracert *
sys-4   permit       command       ping *
R:Read W:Write X:Execute
```

表1-1 display role 命令显示信息描述表

字段	描述
Role	用户角色名称，其中系统预定义的用户角色名称分别为network-admin、network-operator、context-admin、context-operator、level-*n*（*n*为0～15）、security-audit、guest-manager、system-admin、security-admin、audit-admin
Description	用户角色描述信息
VLAN policy	配置的VLAN策略： • Deny：表示除允许操作指定的 VLAN 外，其它 VLAN 均不能被用户操作 • Permit (default)：表示系统缺省允许用户操作任何 VLAN
Permitted VLANs	允许用户操作的VLAN
Interface policy	配置的接口策略： • Deny：表示除允许操作指定的接口外，其它接口均不能被用户操作 • Permit (default)：表示系统缺省允许用户操作任何接口
Permitted interfaces	允许用户操作的接口
VPN-instance policy	配置的VPN策略： • Deny：表示除允许操作指定的 VPN 实例外，其它 VPN 实例均不能被用户操作 • Permit (default)：表示系统缺省允许用户操作任何 VPN 实例
Permitted VPN instances	允许用户操作的VPN实例
Security zone policy	配置的安全域策略： • Deny：表示除允许操作指定的安全域外，其它安全域均不能被用户操作 • Permit (default)：表示系统缺省允许用户操作任何安全域
Permitted security zones	允许用户操作的安全域
Rule	用户角色规则编号（系统预定义的权限规则通过sys-n标识）
Perm	对命令行的操作许可： • Permit：允许操作 • Deny：禁止操作

字段	描述
Type	命令行类型： • R：读类型 • W：写类型 • X：执行类型
Scope	用户角色规则的类型： • command：基于命令行的规则 • feature：基于特性的规则 • feature-group：基于特性组规则 • web-menu：基于 Web 菜单的规则 • xml-element：基于 XML 元素的规则 • oid：基于 OID 元素的规则
Entity	用户角色规则中定义的具体内容（命令特征字符串、特性名称、特性组名称、Web菜单、XML元素或OID） • “-”表示所有特性 • “*”为通配符，表示 0 个或多个任意字符

【相关命令】

- **role**

1.1.3 display role feature

display role feature 命令用来显示特性相关信息。

【命令】

display role feature [**name** *feature-name* | **verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

name *feature-name*：显示指定特性的详细信息，*feature-name* 表示系统中的特性名称，且所有特性名称中的字母均为小写。

verbose：显示所有特性的详细信息，即显示特性内包含的所有命令行列表。

【使用指导】

如果不指定任何关键字，则显示系统中所有特性的名称列表。

【举例】

显示系统中所有特性的名称列表。

```
<Sysname> display role feature
Feature: device          (Device configuration related commands)
Feature: interface       (Interface related commands)
Feature: syslog          (Syslog related commands)
……（略）
```

显示所有特性的详细信息。

```
<Sysname> display role feature verbose
Feature: device          (Device configuration related commands)
  display clock    (R)
  debugging dev    (W)
  display debugging dev    (R)
  display device *    (R)
  display diagnostic-information    (R)
  display environment *    (R)
  display fan *    (R)
  display alarm *    (R)
  display power *    (R)
  display current-configuration *    (R)
  display saved-configuration *    (R)
  display default-configuration *    (R)
  display startup    (R)
  display this *    (R)
……（略）
```

显示特性 aaa 的详细信息。

```
<Sysname> display role feature name aaa
Feature: aaa             (AAA related commands)
  system-view ; domain *    (W)
  system-view ; header *    (W)
  system-view ; aaa *    (W)
  display domain *    (R)
  system-view ; user-group *    (W)
  system-view ; local-user *    (W)
  display local-user *    (R)
  display user-group *    (R)
  display debugging local-server    (R)
  debugging local-server *    (W)
  super *    (X)
  display password-control *    (R)
  reset password-control *    (W)
  system-view ; password-control *    (W)
……（略）
```

表1-2 display role feature 命令显示信息描述表（以 display role feature name aaa 的显示字段为例）

字段	描述
Feature	特性名称以及功能简介

字段	描述
system-view ; domain *	系统视图下以**domain**开头的所有命令，以及ISP域视图下的所有命令
system-view ; header *	系统视图下以**header**开头的所有命令
system-view ; aaa *	系统视图下以**aaa**开头的所有命令
display domain *	用户视图下以**display domain**开头的所有命令
system-view ; user-group *	系统视图下以**user-group**开头的所有命令，以及用户组视图下的所有命令
system-view ; local-user *	系统视图下以**local-user**开头的所有命令，以及本地用户视图下的所有命令
display local-user *	用户视图下以**display local-user**开头的所有命令
display user-group *	用户视图下以**display user-group**开头的所有命令
display debugging local-server	用户视图下以命令**display debugging local-server**开头的所有命令
debugging local-server *	用户视图下以**debugging local-server**开头的所有命令
super *	用户视图下以**super**开头的所有命令
display password-control *	用户视图下以**display password-control**开头的所有命令
reset password-control *	用户视图下以**reset password-control**开头的所有命令
system-view ; password-control *	系统视图下以**password-control**开头的所有命令
(W)	命令行的类型为写命令，本类型的命令用于对系统进行配置
(R)	命令行的类型为读命令，本类型的命令仅能显示系统配置信息和维护信息
(X)	命令行的类型为执行命令，本类型的命令用于执行特定的功能

【相关命令】

- **feature**

1.1.4 display role feature-group

display role feature-group 命令用来显示特性组信息。

【命令】

display role feature-group [**name** *feature-group-name*] [**verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

name *feature-group-name*：显示指定特性组包含的特性名称列表。*feature-group-name* 表示特性组名称，为 1～31 个字符的字符串，区分大小写。如果不指定本参数，则表示显示所有特性组的相关信息。

verbose：显示特性组的详细信息，即显示特性组内的特性所包含的命令行列表。如果不指定本参数，则表示显示特性组中的特性名称列表。

【使用指导】

特性组 L2 和 L3 为系统预定义的两个特性组。

【举例】

显示所有特性组内的特性名称列表。

```
<Sysname> display role feature-group
Feature group: L2
Feature: igmp-snooping   (IGMP-Snooping related commands)
Feature: mld-snooping    (MLD-Snooping related commands)
Feature: lacp            (LACP related commands)
Feature: stp             (STP related commands)
Feature: lldp            (LLDP related commands)
Feature: dldp            (DLDP related commands)
Feature: smart-link      (Smart-link related commands)
Feature: monitor-link    (Monitor-link related commands)
Feature: loopbk-detect   (Loopback-detection related commands)
Feature: vlan            (Virtual LAN related commands)
Feature: evb             (EVB related commands)
Feature: ofp             (OFP related commands)
Feature group: L3
Feature: route           (Route management related commands)
Feature: usr             (Unicast static route related commands)
Feature: ospf            (Open Shortest Path First protocol related commands)
Feature: rip             (Routing Information Protocol related commands)
Feature: isis            (ISIS protocol related commands)
Feature: lisp            (LISP protocol related commands)
Feature: bgp             (Border Gateway Protocol related commands)
Feature: l3vpn           (Layer 3 Virtual Private Network related commands)
Feature: route-policy    (Routing Policy related commands)
Feature: multicast       (Multicast related commands)
Feature: pim             (Protocol Independent Multicast related commands)
Feature: igmp            (Internet Group Management Protocol related commands)
Feature: mld             (Multicast Listener Discovery related commands)
```

显示所有特性组的详细信息。

```
<Sysname> display role feature-group verbose
Feature group: L2
Feature: igmp-snooping   (IGMP-Snooping related commands)
  display l2-multicast *    (R)
  system-view ; probe ; display system internal l2-multicast *    (R)
```

```
  reset l2-multicast *    (W)
Feature: mld-snooping    (MLD-Snooping related commands)
  display ipv6 l2-multicast *    (R)
  system-view ; probe ; display system internal ipv6 l2-multicast *    (R)
  reset ipv6 l2-multicast *    (W)
Feature: lacp            (LACP related commands)
  display link-aggregation *    (R)
  display lacp *    (R)
  system-view ; interface Bridge-Aggregation *    (W)
  system-view ; interface Route-Aggregation *    (W)
  system-view ; link-aggregation *    (W)
  system-view ; lacp *    (W)
  system-view ; interface * ; link-aggregation *    (W)
  system-view ; interface * ; port link-aggregation *    (W)
  system-view ; interface * ; lacp *    (W)
  system-view ; probe ; display system internal link-aggregation *    (R)
  system-view ; probe ; debugging system internal link-aggregation *    (W)
  reset lacp *    (W)
  debugging link-aggregation *    (W)
```

……（略）

显示特性组 L3 的特性名称列表。

```
<Sysname> display role feature-group name L3
Feature group: L3
Feature: route           (Route management related commands)
Feature: usr             (Unicast static route related commands)
Feature: ospf            (Open Shortest Path First protocol related commands)
Feature: rip             (Routing Information Protocol related commands)
Feature: isis            (ISIS protocol related commands)
Feature: lisp            (LISP protocol related commands)
Feature: bgp             (Border Gateway Protocol related commands)
Feature: l3vpn           (Layer 3 Virtual Private Network related commands)
Feature: route-policy    (Routing Policy related commands)
Feature: multicast       (Multicast related commands)
Feature: pim             (Protocol Independent Multicast related commands)
Feature: igmp            (Internet Group Management Protocol related commands)
Feature: mld             (Multicast Listener Discovery related commands)
```

表1-3 display role feature-group 命令显示信息描述表

字段	描述
Feature group	特性组名称，其中L2和L3为系统预定义的两个特性组
Feature	特性名称以及功能简介 关于特性内具体命令的详细介绍请参考表1-2

【相关命令】

- **feature**
- **role feature-group**

1.1.5 feature

feature 命令用来向特性组中添加一个特性。

undo feature 命令用来删除特性组中的指定特性。

【命令】

feature *feature-name*

undo feature *feature-name*

【缺省情况】

自定义特性组中不包括任何特性。

【视图】

特性组视图

【缺省用户角色】

network-admin

context-admin

【参数】

feature-name：系统支持的特性名称，所有特性名称中的字母均为小写。

【使用指导】

可通过多次执行本命令，向特性组中添加多个特性。

【举例】

向特性组 security-features 中添加特性 AAA 和 ACL。

```
<Sysname> system-view
[Sysname] role feature-group name security-features
[Sysname-featuregrp-security-features] feature aaa
[Sysname-featuregrp-security-features] feature acl
```

【相关命令】

- **display role feature**
- **display role feature-group**
- **role feature-group**

1.1.6 interface policy deny

interface policy deny 命令用来进入接口策略视图。

undo interface policy deny 命令用来恢复缺省情况。

【命令】

interface policy deny

undo interface policy deny

【缺省情况】

用户具有操作任何接口的权限。

【视图】

用户角色视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

进入接口策略视图后，如果不配置允许操作的接口列表，则用户将没有操作任何接口的权限；如果需要限制或区分用户对接口资源的使用权限，则还应该通过 **permit interface** 命令配置允许用户操作的接口列表。若接口策略视图中未配置允许操作的接口列表，则表示不允许用户操作所有的接口。对接口的操作指的是创建接口并进入接口视图、删除和应用接口。其中，创建和删除接口，仅针对逻辑接口。

允许修改用户角色的接口策略，但修改后的策略只在被授权该角色的用户重新登录时才会生效。

【举例】

在用户角色 role1 中，进入接口策略视图，并禁止角色为 role1 的用户操作任何接口。

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] interface policy deny
[Sysname-role-role1-ifpolicy] quit
```

在用户角色 role1 中，进入接口策略视图，允许角色为 role1 的用户操作接口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/4。

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] interface policy deny
[Sysname-role-role1-ifpolicy] permit interface gigabitethernet 1/0/1 to gigabitethernet
1/0/4
```

【相关命令】

- **display role**
- **permit interface**
- **role**

1.1.7 permit interface

permit interface 命令用来配置允许用户操作的接口列表。

undo permit interface 命令用来禁止用户操作指定的或所有的接口。

【命令】

permit interface *interface-list*

undo permit interface [*interface-list*]

【缺省情况】

接口策略视图下未定义允许操作的接口列表，用户没有操作任何接口的权限。

【视图】

接口策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

interface *interface-list*：允许用户操作的接口列表，表示多个接口，表示方式为 *interface-list* = { *interface-type interface-number* [to *interface-type interface-number*] }&<1-10>。其中，*interface-type* 为接口类型，*interface-number* 为接口编号。&<1-10>表示前面的参数最多可以输入 10 次。起始接口类型必须和终止接口类型一致，并且终止接口编号必须大于起始接口编号。

【使用指导】

通过 **interface policy deny** 命令进入接口策略视图后，必须要通过本命令配置允许操作的接口列表，用户才能具有操作相应接口的权限。

对接口的操作指的是创建并进入接口视图、删除和应用接口。其中，创建和删除接口，只针对逻辑接口。

可通过多次执行此命令向接口列表中添加允许用户操作的接口。

undo permit interface 命令如果不指定 *interface-list* 参数，则表示禁止用户操作所有接口。

修改后的接口资源控制策略对于当前已经在线的用户不生效，对于之后使用该角色登录设备的用户生效。

【举例】

创建用户角色 role1 并进入其视图。

```
<Sysname> system-view
[Sysname] role name role1
```

配置用户角色规则 1，允许用户执行进入接口视图以及接口视图下的相关命令。

```
[Sysname-role-role1] rule 1 permit command system-view ; interface *
```

配置用户角色规则 2，允许用户执行创建 VLAN 以及进入 VLAN 视图后的相关命令。

```
[Sysname-role-role1] rule 2 permit command system-view ; vlan *
```

配置用户角色 role1 仅可以对接口 GigabitEthernet1/0/1 以及 GigabitEthernet1/0/3～GigabitEthernet1/0/5 进行操作。

```
[Sysname-role-role1] interface policy deny
[Sysname-role-role1-ifpolicy] permit interface gigabitethernet 1/0/1 gigabitethernet 1/0/3
to gigabitethernet 1/0/5
```

当拥有用户角色 role1 的用户登录设备后，可以操作接口 GigabitEthernet1/0/1 以及 GigabitEthernet1/0/3～GigabitEthernet1/0/5，但不能操作其它接口。

配置结果验证如下：

- 进入接口 GigabitEthernet1/0/1 视图。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1]
```

- 将接口 GigabitEthernet1/0/5 加入到 VLAN 10。

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] port gigabitethernet 1/0/5
```

- 无法进入接口 GigabitEthernet1/0/2 视图。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
Permission denied.
```

【相关命令】

- **display role**
- **interface policy deny**
- **role**

1.1.8 permit security-zone

permit security-zone 命令用来配置允许用户操作的安全域列表。

undo permit security-zone 命令用来禁止用户操作指定的或所有的安全域实例。

【命令】

permit security-zone *security-zone-name*&<1-10>

undo permit security-zone [*security-zone-name*&<1-10>]

【缺省情况】

安全域策略视图下未定义允许操作的安全域列表，用户没有操作任何安全域的权限。

【视图】

安全域策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

security-zone-name&<1-10>：表示允许用户操作的安全域的名称，为1～31个字符的字符串，区分大小写。&<1-10>表示前面的参数最多可以输入 10 次。

【使用指导】

通过 **security-zone policy deny** 命令进入安全域策略视图后，必须要通过本命令配置允许操作的安全域列表，用户才能具有操作相应安全域的权限。

对安全域的“操作”指的是创建安全域并进入其视图、删除和应用安全域。

可通过多次执行此本命令向安全域列表中添加允许用户操作的安全域。

undo permit security-zone 命令如果不指定 *security-zone-name* 参数，则表示禁止用户操作所有安全域。

修改后的安全域资源控制策略对于当前已经在线的用户不生效，对于之后使用该角色登录设备的用户生效。

【举例】

创建用户角色 role1 并进入其视图。

```
<Sysname> system-view
[Sysname] role name role1
```

配置用户角色规则 1，允许用户执行系统视图下的所有命令以及所有子视图下的命令。

```
[Sysname-role-role1] rule 1 permit command system-view ; *
```

配置用户角色 role1 仅可以对安全域 trust 和 abc 进行操作。

```
[Sysname-role-role1] security-zone policy deny
[Sysname-role-role1-zonepolicy] permit security-zone trust abc
```

拥有用户角色 role1 的用户登录设备后，可以操作安全域 abc，但不能操作其它安全域。

配置结果验证如下：

- 创建并进入名称为 abc 的安全域视图。

```
<Sysname> system-view
[Sysname] security-zone name abc
[Sysname-security-zone-abc]
```

- 创建源安全域 trust 到目的安全域 abc 的域间实例。

```
<Sysname> system-view
[Sysname] zone-pair security source trust destination abc
[Sysname-zone-pair-security-Trust-abc]
```

- 无法创建名称为 local 的安全域或进入其视图。

```
<Sysname> system-view
[Sysname] security-zone name local
Permission denied.
```

【相关命令】

- **display role**
- **role**
- **security-zone policy deny**

1.1.9 permit vlan

permit vlan 命令用来配置允许用户操作的 VLAN 列表。

undo permit vlan 命令用来禁止用户操作指定的或所有的 VLAN。

【命令】

permit vlan *vlan-id-list*

undo permit vlan [*vlan-id-list*]

【缺省情况】

VLAN 接口视图下未定义允许操作的 VLAN 列表，用户没有操作任何 VLAN 的权限。

【视图】

VLAN 策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

vlan-id-list：允许用户操作的 VLAN 列表，表示方式为 *vlan-id-list* = { *vlan-id1* [to *vlan-id2*] }&<1-10>，*vlan-id* 取值范围为 1～4094，&<1-10>表示前面的参数最多可以重复输入 10 次。终止 VLAN 编号必须大于起始 VLAN 编号。

【使用指导】

通过 **vlan policy deny** 命令进入 VLAN 策略视图后，必须要通过本命令配置允许操作的 VLAN 列表，用户才能具有操作相应 VLAN 的权限。

对 VLAN 的操作指的是创建 VLAN 并进入 VLAN 视图、删除和应用 VLAN。

可通过多次执行此命令向 VLAN 列表中添加多个允许用户操作的 VLAN。

undo permit vlan 命令如果不指定 *vlan-id-list* 参数，则表示禁止用户操作所有 VLAN。

修改后的 VLAN 资源控制策略对于当前已经在线的用户不生效，对于之后使用该角色登录设备的用户生效。

缺省情况下，设备上所有的 access 端口都属于 VLAN 1。使用 **port access vlan** 命令将 access 端口加入到其它指定VLAN中时，该角色必须同时具备VLAN 1的操作权限（通过命令**permit vlan** 1 配置）。

【举例】

创建用户角色 role1 并进入其视图。

```
<Sysname> system-view
[Sysname] role name role1
```

配置用户角色规则 1，允许用户执行进入接口视图以及接口视图下的相关命令。

```
[Sysname-role-role1] rule 1 permit command system-view ; interface *
```

配置用户角色规则 2，允许用户执行创建 VLAN 以及进入 VLAN 视图后的相关命令。

```
[Sysname-role-role1] rule 2 permit command system-view ; vlan *
```

配置用户角色 role1 仅可以操作 VLAN 1、VLAN 2、VLAN 4、VLAN 50～VLAN 100。

```
[Sysname-role-role1] vlan policy deny
[Sysname-role-role1-vlanpolicy] permit vlan 1 2 4 50 to 100
```

当拥有用户角色 role1 的用户登录设备后，可以操作 VLAN 1、VLAN 2、VLAN 4、VLAN 50～VLAN 100，但不能操作其它 VLAN。

配置结果验证如下：

- 创建并进入 VLAN 100 视图。

```
<Sysname> system-view
[Sysname] vlan 100
[Sysname-vlan100]
```

- 向 VLAN 100 中添加 Access 类型的端口 GigabitEthernet1/0/1。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port access vlan 100
```

- 无法创建 VLAN 101 或进入其视图。

```
<Sysname> system-view
[Sysname] vlan 101
Permission denied.
```

【相关命令】

- **display role**
- **role**
- **vlan policy deny**

1.1.10 permit vpn-instance

permit vpn-instance 命令用来配置允许用户操作的 VPN 实例列表。

undo permit vpn-instance 命令用来禁止用户操作指定的或所有的 VPN 实例。

【命令】

permit vpn-instance *vpn-instance-name*&<1-10>

undo permit vpn-instance [*vpn-instance-name*&<1-10>]

【缺省情况】

VPN 策略视图下未定义允许操作的 VPN 实例列表，用户没有操作任何 VPN 实例的权限。

【视图】

VPN 策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

vpn-instance-name&<1-10>：表示允许用户操作的 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。&<1-10>表示前面的参数最多可以输入 10 次。

【使用指导】

通过 **vpn-instance policy deny** 命令进入 VPN 策略视图后，必须要通过本命令配置允许操作的 VPN 实例列表，用户才能具有操作相应 VPN 实例的权限。

对 VPN 实例的“操作”指的是创建 MPLS L3VPN 实例并进入其视图、删除和应用 VPN 实例。

可通过多次执行此命令向接口列表中添加多个允许用户操作的 VPN 实例。

undo permit vpn-instance 命令如果不指定 *vpn-instance-name* 参数，则表示禁止用户操作所有 VPN 实例。

修改后的 VPN 资源控制策略对于当前已经在线的用户不生效，对于之后使用该角色登录设备的用户生效。

【举例】

创建用户角色 role1 并进入其视图。

```
<Sysname> system-view
[Sysname] role name role1
```

配置用户角色规则 1，允许用户执行系统视图下的所有命令以及所有子视图下的命令。

```
[Sysname-role-role1] rule 1 permit command system-view ; *
```

配置用户角色 role1 仅可以对 VPN 实例 vpn1 进行操作。

```
[Sysname-role-role1] vpn policy deny
```

```
[Sysname-role-role1-vpnpolicy] permit vpn-instance vpn1
```

拥有用户角色 role1 的用户登录设备后，可以操作 VPN 实例 vpn1，但不能操作其它 VPN 实例。

配置结果验证如下：

- 进入名称为 vpn1 的 VPN 实例视图。

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1]
```

- 设置 RADIUS 方案 radius1 的主计费服务器的 IP 地址为 10.110.1.2，且属于 VPN 实例 vpn1。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary accounting 10.110.1.2 vpn-instance vpn1
```

- 无法创建名称为 vpn2 的 VPN 实例或进入其视图。

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn2
Permission denied.
```

【相关命令】

- **display role**
- **role**
- **vpn-instance policy deny**

1.1.11 role

role 命令用来创建用户角色，并进入用户角色视图。如果指定的用户角色已经存在，则直接进入用户角色视图。

undo role 命令用来删除指定的用户角色。

【命令】

role name *role-name*

undo role name *role-name*

【缺省情况】

存在系统预定义的用户角色：network-admin、network-operator、context-admin、context-operator、level-*n*（*n* 为 0～15 的整数）、security-audit、guest-manager、system-admin、security-admin、audit-admin。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

name *role-name*：用户角色名称，*role-name* 为 1～63 个字符的字符串，区分大小写。

【使用指导】

除系统预定义的缺省用户角色之外，系统中最多允许创建 64 个用户角色。

缺省的用户角色不能被删除，而且其中的 network-admin、network-operator、context-admin、context-operator、level-15、security-audit、guest-manager、system-admin、security-admin、audit-admin 这些用户角色内定义的所有权限均不能被修改；用户角色 level-0～level-14 可以通过自定义规则和资源控制策略调整自身的权限，但这种修改对于 **display history-command all** 命令不生效，即不能通过添加对应的规则来更改它的缺省执行权限。

非 AAA 认证用户不能被授予安全日志管理员角色。

【举例】

创建用户角色 role1，并进入用户角色视图。

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1]
```

【相关命令】

- **display role**
- **interface policy deny**
- **rule**
- **vlan policy deny**
- **vpn-instance policy deny**

1.1.12 role default-role enable

role default-role enable 命令用来使能缺省用户角色授权功能。

undo role default-role enable 命令用来恢复缺省情况。

【命令】

role default-role enable [*role-name*]

undo role default-role enable

【缺省情况】

缺省用户角色授权功能处于关闭状态，没有被 AAA 授权用户角色的用户不能登录设备。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

role-name：缺省用户角色名称，为 1～63 个字符的字符串，区分大小写，可以是系统中已存在的任意用户角色。

【使用指导】

对于通过 AAA 认证登录设备的用户，由服务器（远程认证服务器或本地认证服务器）为其授权对应的用户角色。如果用户没有被授权任何用户角色，将无法成功登录设备。若未通过 **authorization-attribute** 命令配置本地用户或用户组的授权属性，则必须使能缺省用户角色授权功能。使能该功能后，用户将在没有被服务器授权任何用户角色的情况下，具有一个缺省的用户角色。

若用户通过 AAA 认证且被授予了具体的用户角色，则用户不具有缺省的用户角色。

若不指定 *role-name* 参数，如果用户登录于缺省 Context，则缺省用户角色为 network-operator；如果用户登录于非缺省 Context，则缺省用户角色为 context-operator。

【举例】

使能缺省用户角色授权功能。

```
<Sysname> system-view
[Sysname] role default-role enable
```

【相关命令】

- **role**

1.1.13 role feature-group

role feature-group 命令用来创建特性组，并进入特性组视图。如果指定的特性组已经存在，则直接进入特性组视图。

undo role feature-group 命令用来删除指定的特性组。

【命令】

role feature-group name *feature-group-name*

undo role feature-group name *feature-group-name*

【缺省情况】

存在两个特性组，名称分别为 L2 和 L3。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

name *feature-group-name*：特性组名称，*feature-group-name* 为 1～31 个字符的字符串，区分大小写。

【使用指导】

除系统预定义的特性组 L2 和 L3 之外，系统中最多允许创建 64 个特性组。

不能修改和删除系统预定义的特性组 L2 和 L3。L2 中包含了所有的二层协议相关功能的命令，L3 中包含了所有三层协议相关功能的命令。

【举例】

创建特性组 security-features，并进入特性组视图。

```
<Sysname> system-view
[Sysname] role feature-group name security-features
[Sysname-featuregrp-security-features]
```

【相关命令】

- **display role feature**
- **display role feature-group**
- **feature**

1.1.14 rule

rule 命令用来为用户角色创建一条规则。

undo rule 命令用来为用户角色删除规则。

【命令】

rule *number* { **deny** | **permit** } { **command** *command-string* | { **execute** | **read** | **write** } * { **feature** [*feature-name*] | **feature-group** *feature-group-name* | **oid** *oid-string* | **web-menu** [*web-string*] | **xml-element** [*xml-string*] } }

undo rule { *number* | **all** }

【缺省情况】

新创建的用户角色中未定义规则，即当前用户角色无任何权限。

【视图】

用户角色视图

【缺省用户角色】

network-admin

context-admin

【参数】

number：权限规则编号，取值范围为 1～256。

deny：禁止执行指定的命令、Web 菜单、XML 元素或 MIB 节点 OID。

permit：允许执行指定的命令、Web 菜单、XML 元素或 MIB 节点 OID。

command *command-string*：配置基于命令的规则。*command-string* 表示命令特征字符串，为 1～128 个字符的字符串，区分大小写，可以是特定的一条命令行，也可以是用星号（*）通配符表示的一批命令，可包含空格、Tab（它们用于分隔关键字、参数以及输入的字符），以及所有可打印字符。

execute：表示执行类型的命令、Web 菜单、XML 元素或 MIB 节点 OID。用于执行特定的程序或功能，执行类型的命令如 **ping** 命令。

read：表示读类型的命令、Web 菜单、XML 元素或 MIB 节点 OID，用于显示系统配置和维护信息。读类型的命如 **display**、**dir**、**more** 和 **pwd** 命令。

write：表示写类型的命令、Web 菜单、XML 元素或 MIB 节点 OID，用于对系统进行配置。写类型的命如 **ssh server enable** 命令。

feature [*feature-name*]：配置基于特性的规则。*feature-name* 表示系统预定义的特性名称，区分大小写。若不指定特性名称，则表示所有特性。

feature-group *feature-group-name*：配置基于特性组的规则。*feature-group-name* 表示特性组名称，为 1～31 个字符的字符串，区分大小写。只有特性组创建后，基于特性组的规则才能生效。使用 **display role feature-group** 命令可以查看已创建的特性组信息。

oid *oid-string*：配置基于 MIB 节点 OID（Object Identifier，对象标识符）的规则。*oid-string* 表示允许操作的 OID，为 1～255 个字符的字符串，不区分大小写。OID 是由一系列的整数组成，标明节点在 MIB 树中的位置，它能唯一地标识一个 MIB 库中的对象。例如：1.3.6.1.4.1.25506.8.35.14.19.1.1。

web-menu [*web-string*]：配置基于 Web 菜单的规则。*web-string* 表示允许操作的 Web 菜单选项的 ID 路径，为 1～255 个字符的字符串，不区分大小写，以“/”为分隔符来分隔不同级别的菜单。合法的 *web-string* 为通过 **display web menu** 命令显示的 ID 路径,例如：M_DEVICE/l_BASIC_INFO/l_reboot；若不指定 *web-string* 参数，则表示对所有菜单选项生效。

xml-element [*xml-string*]：配置基于 XML 元素的规则。*xml-string* 表示允许操作的 XML 元素的 XPath，为 1～255 个字符的字符串，不区分大小写，以“/”为分隔符来分隔不同级别的菜单，例如：Interfaces/Index/Name；若不指定 *xml-string* 参数，则表示对所有 XML 元素生效。

all：指定所有权限规则。

【使用指导】

可为一个用户角色定义以下几种类型的规则：

- 禁止或允许执行特定的命令行。
- 禁止或允许执行指定或所有特性的某一类或某几类命令。
- 禁止或允许执行某个特性组中所有特性的某一类或某几类命令。
- 禁止或允许执行指定所有或指定的 MIB 节点 OID。
- 禁止或允许执行 Web 页面中所有菜单选项或某几类菜单选项。
- 禁止或允许执行所有 XML 元素或某几类 XML 元素。

每个用户角色中最多可以配置 256 条规则，系统中可以配置的用户角色规则总数不能超过 1024。

访问文件系统的命令，受基于文件系统特性规则以及具体命令规则的双重控制。

对于需要将输出信息重定向到文件中保存的命令，只有在用户角色被授权了文件系统写权限后才允许执行。

为用户角色定义规则时，需要注意的是：

- 如果指定编号的规则不存在，则表示创建一条新的规则；如果指定编号的规则已存在，则表示对已有的规则进行修改。修改后的规则对于当前已经在线的用户不生效，对于之后使用该角色登录设备的用户生效。
- 一个用户角色中允许创建多条规则，各规则以创建时指定的编号为唯一标识，被授权该角色的用户可以执行的命令为这些规则定义的可执行命令的并集。若这些规则定义的权限内容有冲突，则规则编号大的有效。例如，规则 1 允许执行命令 A，规则 2 允许执行命令 B，规则 3 禁止执行命令 A，则最终规则 2 和规则 3 生效，即禁止执行命令 A，允许执行命令 B。
- 在同时存在系统预定义规则（以 sys-x 为权限规则编号，x 为整数值）和自定义规则的用户角色中，若预定义规则定义的权限内容与自定义规则定义的权限内容有冲突，则以自定义规则为准。

输入命令特征字符串时，需要遵循以下规则：

(1) 段（segment）的划分

- 若要描述多级视图下的命令，则需要使用分号（;）将命令特征字符串分成多个段，每一个段代表一个或一系列命令，后一个段中的命令是执行前一个段中命令所进入视图下的命令。一个段中可以包含多个星号（*），每个星号（*）代表了 0 个或多个任意字符。例如：命令特征字符串“system ; interface * ; ip * ;”代表从系统视图进入到任意接口视图后，以 **ip** 开头的所有命令。
- 除最后一个段外，其余段中的命令应为描述如何进入子视图的命令特征字符串。
- 一个段中必须至少出现一个可打印字符，不能全部为空格或 Tab。

(2) 分号的使用

- 在输入命令特征字符串时必须指定该命令所在的视图，进入各视图的命令特征字符串由分号分隔。但是，对于能在任意视图下执行的命令（例如 **display** 命令）以及用户视图下的命令（例如 **dir** 命令），在配置包含此类命令的规则时，不需要在规则的命令匹配字符串中指定其所在的视图。
- 当最后一个段中的最后一个可见字符为分号时，表示所指的命令范围不再扩展，否则将向子视图中的命令扩展。例如：命令特征字符串“system ; radius scheme * ;”代表系统视图下以 **radius scheme** 开头的所有命令；命令特征字符串“system ; radius scheme * ”代表系统视图下以 **radius scheme** 开头的所有命令，以及进入子视图（RADIUS 方案视图）下的所有命令。

(3) 星号的使用

- 当星号（*）出现在一个段的首部时，其后面不能再出现其它可打印字符，且该段必须是命令特征字符串的最后一个段。例如：命令特征字符串“system ; *”就代表了系统视图下的所有命令，以及所有子视图下的命令。
- 当星号（*）出现在一个段的中间时，该段必须是命令特征字符串的最后一个段。例如：命令特征字符串“debugging * event”就代表了用户视图下所有模块的事件调试信息开关命令。

(4) 前缀匹配

- 命令关键字与命令特征字符串是采用前缀匹配算法进行匹配的，即只要命令行中关键字的首部若干连续字符或全部字符与规则中定义的关键字相匹配，就认为该命令行与此规则匹配。因此，命令特征字符串中可以包括完整的或部分的命令关键字。例如，若规则“**rule 1 deny command display arp source**”生效，则命令 **display arp source-mac interface** 和命令 **display arp source-suppression** 都会被禁止执行。

对于基于命令的规则，有以下使用注意事项：

- 基于命令的规则只对指定视图下的命令生效。若用户输入的命令在当前视图下不存在而在其父视图下被查找到时，用于控制当前视图下的命令的规则不会对其父视图下的命令执行权限进行控制。例如，定义一条规则“rule 1 deny command system ; interface * ; *”禁止用户执行接口视图下的任何命令。当用户在接口视图下输入命令 **acl advanced** 3000 时，该命令仍然可以成功执行，因为系统在接口视图下搜索不到指定的 **acl** 命令时，会回溯到系统视图（父视图）下执行，此时该规则对此命令不生效。
- **display** 命令中的重定向符（“|”、“>”、“>>”）及其后面的关键字不被作为命令行关键字参与规则的匹配。例如，若规则“rule 1 permit command display debugging”生效，则命令 **display debugging > log** 是被允许执行的，其中的关键字**> log** 将被忽略，RBAC 只

对重定向符前面的命令行 **display debugging** 进行匹配。但是，如果在规则中配置了重定向符，则 RBAC 会将其作为普通字符处理。例如，若规则“rule 1 permit command display debugging > log”生效，则命令 **display debugging > log** 将会匹配失败，因为其中的关键字**> log** 被 RBAC 忽略了，最终是命令 **display debugging** 与规则进行匹配。因此，配置规则时不要使用重定向符。

进行基于 OID 的规则的匹配时，遵循以下规则：

- 与用户访问的 OID 形成最长匹配的规则生效。例如用户访问的 OID 为 1.3.6.1.4.1.25506.141.3.0.1，角色中存在“rule 1 permit read write oid 1.3.6”，“rule 2 deny read write oid 1.3.6.1.4.1”和“rule 3 permit read write oid 1.3.6.1.4”，其中 rule 2 与用户访问的 OID 形成最长匹配，则认为 rule 2 与 OID 匹配，匹配的结果为用户的此访问请求被拒绝。
- 对于定义的 OID 长度相同的规则，规则编号大的生效。例如用户访问的 OID 为 1.3.6.1.4.1.25506.141.3.0.1，角色中存在“rule 1 permit read write oid 1.3.6”，“rule 2 deny read write oid 1.3.6.1.4.1”和“rule 3 permit read write oid 1.3.6.1.4.1”，其中 rule 2 和 rule 3 与访问的 OID 形成最长匹配，则 rule 3 生效，匹配的结果为用户的访问请求被允许。

【举例】

为用户角色 role1 创建一条规则，允许用户执行命令 **display acl**。

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] rule 1 permit command display acl
```

为用户角色 role1 添加一条权限规则，允许用户执行所有以 **display** 开头的命令。

```
[Sysname-role-role1] rule 2 permit command display *
```

为用户角色 role1 添加一条权限规则，允许用户执行系统视图下的 **radius scheme aaa** 命令，以及使用该命令进入子视图后的所有命令。

```
[Sysname-role-role1] rule 3 permit command system ; radius scheme aaa
```

为用户角色 role1 添加一条权限规则，禁止用户执行所有特性中读类型和写类型的命令。

```
[Sysname-role-role1] rule 4 deny read write feature
```

为用户角色 role1 添加一条权限规则，禁止用户执行特性 aaa 中所有读类型的命令。

```
[Sysname-role-role1] rule 5 deny read feature aaa
```

为用户角色 role1 添加一条权限规则，允许执行特性组 security-features 中所有特性的读类型、写类型以及执行类型的命令。

```
[Sysname-role-role1] rule 6 permit read write execute feature-group security-features
```

为用户角色 role1 添加一条基于 OID 的规则，允许对 OID 为 1.1.2 的 MIB 节点进行读、写操作。

```
[Sysname-role-role1] rule 7 permit read write oid 1.1.2
```

【相关命令】

- **display role**
- **display role feature**
- **display role feature-group**
- **display web menu**（基础配置命令参考/登录设备）
- **role**

1.1.15 security-zone policy deny

security-zone policy deny 命令用来进入安全域策略视图。

undo security-zone policy deny 命令用来恢复缺省情况。

【命令】

security-zone policy deny

undo security-zone policy deny

【缺省情况】

用户具有操作任何安全域的权限。

【视图】

用户角色视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

进入安全域策略视图后，如果不配置允许操作的安全域列表，则用户将没有操作任何安全域的权限；如果需要限制或区分用户对安全域资源的使用权限，则还应该通过 **permit security-zone** 命令配置允许用户操作的安全域列表。若安全域策略视图中未配置允许操作的安全域列表，则表示不允许用户操作所有的安全域。对安全域的“操作”指的是创建并进入安全域视图、删除和应用安全域。

允许修改用户角色的安全域策略，但修改后的策略只对被授权该角色的用户重新登录时才会生效。

【举例】

在用户角色 role1 中，进入安全域策略视图，禁止角色为 role1 的用户操作任意安全域。

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] security-zone policy deny
[Sysname-role-role1-zonepolicy] quit
```

在用户角色 role1 中，进入安全域策略视图，允许角色为 role1 的用户操作安全域 trust 和 abc。

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] security-zone policy deny
[Sysname-role-role1-zonepolicy] permit security-zone trust abc
```

【相关命令】

- **display role**
- **permit security-zone**
- **role**

1.1.16 super

super 命令用来使用户从当前角色切换到指定的用户角色。

【命令】

super [*role-name*]

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

role-name：待切换的用户角色名称，为 1～63 个字符的字符串，区分大小写，可以是系统中已存在的除 security-audit、guest-manager 之外的任意用户角色。若不指定本参数，则切换到当前缺省的目的用户角色。缺省的目的用户角色由 **super default role** 命令指定。

【使用指导】

切换后的用户角色只对当前登录生效，用户重新登录后，又会恢复到原有角色。

为了保证操作的安全性，通常用户进行用户角色切换时，均需要输入用户角色切换密码。切换到不同的用户角色时，需要输入相应切换密码。如果服务器没有响应或者没有配置用户角色切换密码，则切换操作失败，若还有备份认证方案，则转而进行备份认证。因此，在进行切换操作前，请先保证配置了正确的用户角色切换密码。

在切换用户角色时，需要注意的是：

- 若级别切换认证方式为 **local**，在设备上未配置切换密码的情况下，对于 Console 用户，设备不关心用户是否输入切换密码以及输入切换密码的内容，可允许用户成功切换用户角色。
- 若级别切换认证方式为 **local scheme**，在设备上未配置切换密码的情况下，对于 Console 或 VTY 用户，则转为远程 AAA 认证。

【举例】

将用户角色切换到 network-operator。（假设用户当前的角色为 network-admin，切换认证方式为 local，切换密码已经设置）

```
<Sysname> super network-operator
Password:
User privilege role is network-operator, and only those commands that authorized to the role can be used.
```

【相关命令】

- **authentication super**（安全命令参考/AAA）
- **super authentication-mode**
- **super password**

1.1.17 super authentication-mode

super authentication-mode 命令用来设置切换用户角色时使用的认证方式。

undo super authentication-mode 命令用来恢复缺省情况。

【命令】

super authentication-mode { **local** | **scheme** } *

undo super authentication-mode

【缺省情况】

采用 **local** 认证方式。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

local：使用本地配置的用户角色切换密码进行认证。

scheme：使用 AAA 配置进行认证。

【使用指导】

使用本地密码认证时，需要通过 **super password** 命令在设备上配置用户角色切换的密码。

使用远程 AAA 认证时，需要在 RADIUS 或 HWTACACS 服务器上配置用户名和用户角色切换密码。

用户可以选择使用 **local** 或者 **scheme** 方式认证，也可以同时选择 **local** 和 **scheme** 方式，多选时根据配置顺序依次认证。

- **local scheme** 方式：先进行本地密码认证，若设备上未设置本地用户角色切换密码，使用 Console 或 VTY 用户线登录的用户则转为远程 AAA 认证。
- **scheme local** 方式：先进行远程 AAA 认证，远程 HWTACACS/RADIUS 服务器无响应或设备上的 AAA 远程认证配置无效时，转为本地密码认证。

scheme 认证方式需要与 AAA 的认证方案相配合，具体请参考“安全配置指导”中的“AAA”。

【举例】

配置切换用户角色时采用 **local** 认证方式。

```
<Sysname> system-view
[Sysname] super authentication-mode local
```

配置切换用户角色时采用先 **scheme** 后 **local** 的认证方式。

```
<Sysname> system-view
[Sysname] super authentication-mode scheme local
```

【相关命令】

- **authentication super**（安全命令参考/AAA）
- **super password**

1.1.18 super default role

super default role 命令用来配置用户角色切换的缺省目的角色。

undo super default role 命令用来恢复缺省情况。

【命令】

super default role *role-name*

undo super default role

【缺省情况】

对于登录缺省 Context 的用户，用户角色切换的缺省目的角色为 network-admin；对于登录非缺省 Context 的用户，用户角色切换的缺省目的角色为 context-admin。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

role-name：待切换的用户角色名称，为 1～63 个字符的字符串，区分大小写，可以是系统中已存在的除 security-audit、guest-manager 之外的任意用户角色。

【使用指导】

当执行 **super** 命令切换用户角色时，或配置用户角色切换的密码时，如不指定目的切换的角色名称，则表示使用 **super default role** 命令配置的缺省用户角色。

【举例】

配置用户切换角色的缺省目的角色为 network-operator。

```
<Sysname> system-view
[Sysname] super default role network-operator
```

【相关命令】

- **super**
- **super password**

1.1.19 super password

super password 命令用来设置用户角色切换的密码。

undo super password 命令用来删除用户角色切换密码。

【命令】

super password [**role** *role-name*] [{ **hash** | **simple** } *string*]

undo super password [**role** *role-name*]

【缺省情况】

未设置用户角色切换密码。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

role *role-name*：待切换的用户角色的名称，为 1～63 个字符的字符串，区分大小写，可以为系统中已存在的除 security-audit、guest-manager 之外的任意用户角色。如果不指定角色名称，则表示设置的是切换到当前缺省目的用户角色的密码。缺省的目的用户角色由 **super default role** 命令指定。

hash：以哈希方式设置密码。

simple：以明文方式设置密码，该密码将以哈希计算后的密文形式存储。

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；哈希密码为 1～110 个字符的字符串。

【使用指导】

如果不指定 **hash** 或 **simple** 参数，**super password** [**role** *role-name*]命令将以交互式方式设置本地用户密码，涵义与指定 **simple** 关键字相同。

当用户切换认证方式为 **local** 或包含 **local**（**local scheme**、**scheme local**）时，才需要本命令指定的用户角色切换密码。

为保证权限控制更加安全，推荐给不同的用户角色指定不同的切换密码。

【举例】

配置将用户角色切换到 network-operator 时使用的密码为明文密码 123456TESTplat&!。

```
<Sysname> system-view
[Sysname] super password role network-operator simple 123456TESTplat&!
```

以交互式方式设置将用户角色切换到 network-operator 时使用的密码为明文密码 123456TESTplat&!。

```
<Sysname> system-view
[Sysname] super password role network-operator
Password:
Confirm :
Updating user information. Please wait......
```

【相关命令】

- **super authentication-mode**
- **super default role**

1.1.20 super use-login-username

super use-login-username 命令用来配置用户角色切换认证时使用用户登录的用户名进行认证。

undo super use-login-username 命令用来恢复缺省情况。

【命令】

super use-login-username

undo super use-login-username

【缺省情况】

用户角色切换认证时系统提示用户输入用户名进行认证。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

通过开启本功能，在设备采用远程 AAA 认证方案进行用户角色切换认证，且用户采用用户名和密码方式登录设备的情况下，用户切换用户角色时，设备会自动获取用户登录使用的用户名作为角色切换认证的用户名，不再提示用户输入用户名。

开启本功能后，若设备采用远程 AAA 认证方案进行用户角色切换认证，但用户未采用用户名和密码方式登录设备，则用户角色切换失败。

若设备未采用远程 AAA 认证方案进行用户角色切换认证，则本功能配置无效。

【举例】

配置用户角色切换认证时使用用户登录的用户名进行认证。

```
<Sysname> system-view
[Sysname] super use-login-username
```

【相关命令】

- **authentication super**（安全命令参考/AAA）
- **super authentication-mode**
- **super password**

1.1.21 vlan policy deny

vlan policy deny 命令用来进入 VLAN 策略视图。

undo vlan policy deny 命令用来恢复缺省情况。

【命令】

vlan policy deny

undo vlan policy deny

【缺省情况】

用户具有操作任何 VLAN 的权限。

【视图】

用户角色视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

进入 VLAN 策略视图后，如果不配置允许操作的 VLAN 列表，则用户将没有操作任何 VLAN 的权限；如果需要限制或区分用户对 VLAN 资源的使用权限，则还应该通过 **permit vlan** 命令配置允许用

户操作的 VLAN 列表。若 VLAN 策略视图中未配置允许操作的 VLAN 列表，则表示不允许用户操作所有的 VLAN。对 VLAN 的“操作”指的是创建并进入 VLAN 视图、删除和应用 VLAN。

允许修改用户角色的 VLAN 策略，但修改后的策略只对被授权该角色的用户重新登录时才会生效。

【举例】

在用户角色 role1 中，进入 VLAN 策略视图，禁止角色为 role1 的用户操作任意 VLAN。

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] vlan policy deny
[Sysname-role-role1-vlanpolicy] quit
```

在用户角色 role1 中，进入 VLAN 策略视图，允许角色为 role1 的用户操作 VLAN 50～VLAN 100。

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] vlan policy deny
[Sysname-role-role1-vlanpolicy] permit vlan 50 to 100
```

【相关命令】

- **display role**
- **permit vlan**
- **role**

1.1.22 vpn-instance policy deny

vpn-instance policy deny 命令用来进入 VPN 策略视图。

undo vpn-instance policy deny 命令用来恢复缺省情况。

【命令】

vpn-instance policy deny

undo vpn-instance policy deny

【缺省情况】

用户具有操作任何 VPN 实例的权限。

【视图】

用户角色视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

进入 VPN 策略视图后，如果不配置允许操作的 VPN 实例列表，则用户将没有操作任何 VPN 实例的权限；如果需要限制或区分用户对 VPN 资源的使用权限，则还应该通过 **permit vpn-instance** 命令配置允许用户操作的 VPN 实例列表。若 VPN 策略视图中未配置允许操作的 VPN 实例列表，则表示不允许用户操作所有的 VPN 实例。对 VPN 实例的“操作”指的是创建 MPLS L3VPN 实例并进入其视图、删除和应用 VPN 实例。

允许修改用户角色的 VPN 策略，但修改后的策略只对被授权该角色的用户重新登录时才会生效。

【举例】

在用户角色 role1 中，创建并进入一个 VPN 策略视图，并禁止角色为 role1 的用户操作任意 VPN 实例。

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] vpn-instance policy deny
[Sysname-role-role1-vpnpolicy] quit
```

在用户角色 role1 中，创建并进入一个 VPN 策略视图，允许角色为 role1 的用户操作 VPN 实例 vpn2。

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] vpn-instance policy deny
[Sysname-role-role1-vpnpolicy] permit vpn-instance vpn2
```

【相关命令】

- **display role**
- **permit vpn-instance**
- **role**