APPENDIX A

RBAC Configuration

This chapter includes information about RBAC configurations in relation to FCoE operations and it includes the following sections:

Global Administrator Actions

The Global administrator role is unrestricted and all commands are available.

LAN Administrator Actions

This section lists the commands that the LAN administrator may not perform. Commands that are not listed are implicitly permitted.

Global Level Deny Actions

```
switch(config)# feature lacp
switch(config)# feature tacacs+
switch(config)# feature udld
switch(config)# feature fcoe
switch(config)# aaa *
switch(config)# boot *
switch(config)# cfs *
switch(config)# class-map *
switch(config)# device-alias *
switch(config)# diagnostic *
switch(config)# fex *
switch(config)# hw-module logging onboard *
switch(config)# license *
switch(config)# line *
switch(config)# lldp *
switch(config)# monitor session *
switch(config)# ntp *
switch(config)# policy-map *
switch(config)# privilege *
switch(config)# radius-server *
```

```
switch(config)# role *
switch(config)# snmp-server *
switch(config)# spanning-tree
    bridge assurance *
    loopguard *
    mode *
    mst *
    pathcost *
    port type *
    vlan <fcoe-vlan>
switch(config)# ssh *
switch(config)# system
    core *
    default switchport *
    jumbomtu *
    qos *
switch(config)# tacacs+ *
switch(config)# telnet server enable
switch(config)# trunk protocol enable
switch(config)# username *
switch(config)# vrf  *
switch(config)# xml server *
```

This section includes the following topics:

VLAN-Level Deny Actions

Deny Actions for All VLANs

```
switch(config)# vlan vlan
switch(config-vlan)# fcoe
```

Deny Actions for Pre-determined FCoE VLANs

```
switch(config)# no vlan fcoe-vlan
switch(config)# vlan fcoe-vlan *
switch(config)# spanning-tree vlan fcoe-vlan *
switch(config-mst)# instance n vlan fcoe-vlan
switch(config)# mac-address-table aging-time t vlan fcoe-vlan
switch(config)# mac-address-table static aaaa.bbbb.cccc vlan fcoe-vlan
switch(config-monitor)# source vlan fcoe-vlan
switch(config)# vlan fcoe-vlan
switch(config-vlan)# ip igmp snooping *
```

Interface-Level Deny Actions

Interface-Level Deny Actions

Note Access to the management interface is limited to the unified administrator.

```
switch(config)# interface mgmt *
```

Deny Actions for Pre-determined Ethernet Interfaces Designated to Carry FCoE Traffic

```
switch(config-if)# bandwidth *
switch(config-if)# fcoe *
switch(config-if)# flowcontrol *
switch(config-if)# link debounce *
switch(config-if)# lldp *
switch(config-if)# priority-flow-control *
switch(config-if)# service-policy *
switch(config-if)# shutdown
switch(config-if)# shutdown force
switch(config-if)# spanning-tree bpdufilter
switch(config-if)# spanning-tree bpduguard
switch(config-if)# spanning-tree cost *
switch(config-if)# spanning-tree guard *
switch(config-if)# spanning-tree link-type *
switch(config-if)# spanning-tree mst *
switch(config-if)# spanning-tree port type *
switch(config-if)# spanning-tree port-priority *
switch(config-if)# speed *
switch(config-if)# switchport host
switch(config-if)# switchport mode *
switch(config-if)# switchport monitor
switch(config-if)# switchport trunk native vlan <fcoe-vlan>
switch(config-if)# switchport trunk allowed vlan <range>
switch(config-if)# switchport trunk allowed vlan add <fcoe-vlan>
switch(config-if)# switchport trunk allowed vlan all
switch(config-if)# switchport trunk allowed vlan except *
switch(config-if)# switchport trunk allowed vlan none
switch(config-if)# switchport trunk allowed vlan remove <fcoe-vlan>
```

FC Deny Actions

FC Deny Actions

Note The LAN administrator may not execute SAN-related commands.

```
switch(config)# fabric-binding *
switch(config)# fcalias *
switch(config)# fcdomain *
switch(config)# fcdroplatency *
switch(config)# fcflow *
switch(config)# fcid-allocation *
switch(config)# fcinterop *
switch(config)# fcns *
switch(config)# fcroute *
switch(config)# fcs *
switch(config)# fcsp *
switch(config)# fctimer *
switch(config)# fdmi *
switch(config)# fspf *
switch(config)# in-order-guarantee
switch(config)# interface fc *
switch(config)# interface san-port-channel *
switch(config)# interface vfc *
switch(config)# npiv *
switch(config)# npv *
switch(config)# port-security enable
switch(config)# port-track enable
switch(config)# rib *
```

```
switch(config)# rlir *
switch(config)# rscn *
switch(config)# scsi-target *
switch(config)# system default zone *
switch(config)# vsan database  *
switch(config)# wwn *
switch(config)# zone *
switch(config)# zoneset *
```

SAN Administrator Actions

This section lists the commands that the SAN administrator may not perform. Commands that are not listed are implicitly permitted.

Global Level Deny Actions

```
switch(config)# feature * (except feature fcoe)
switch(config)# aaa *
switch(config)# boot *
switch(config)# cfs *
switch(config)# class-map *
switch(config)# device-alias *
switch(config)# diagnostic *
switch(config)# fex *
switch(config)# hw-module logging onboard *
switch(config)# ip *
switch(config)# ipv6 *
switch(config)# license *
switch(config)# line *
switch(config)# lldp *
switch(config)# mac-address-table *
switch(config)# monitor session *
switch(config)# ntp *
switch(config)# policy-map *
switch(config)# privilege *
switch(config)# radius-server *
switch(config)# role *
switch(config)# snmp-server *
switch(config)# spanning-tree
    bridge assurance *
    loopguard *
    mode *
    mst *
    pathcost *
    port type *
    vlan <non-fcoe-vlan>
switch(config)# ssh *
switch(config)# system
    core *
    default switchport *
    jumbomtu *
    qos *
switch(config)# tacacs+ *
switch(config)# telnet server enable
switch(config)# trunk protocol enable
switch(config)# username *
switch(config)# vrf  *
switch(config)# xml server *
```

This section includes the following topics:

VLAN Level Deny Actions

Deny Actions for Pre-determined Non-FCoE VLANs

```
switch(config)# no vlan <non-fcoe-vlan>
switch(config)# vlan <non-fcoe-vlan>*
switch(config)# spanning-tree vlan <non-fcoe-vlan>*
switch(config-mst)# instance n vlan <non-fcoe-vlan>
switch(config)# mac-address-table aging-time t vlan <non-fcoe-vlan>
switch(config)# mac-address-table static aaaa.bbbb.cccc vlan <non-fcoe-vlan>
switch(config-monitor)# source vlan <non-fcoe-vlan>
switch(config)# vlan <non-fcoe-vlan>
switch(config-vlan)# ip igmp snooping *
switch(config-if)# spanning-tree vlan <non-fcoe-vlan>
```

Interface Level Deny Actions

Interface Level Deny Actions

Note Access to the management interface is limited to the unified administrator.

```
switch (config)# interface mgmt *
```

Deny Actions for Pre-determined Ethernet Interfaces Designated to not Carry FCoE Traffic

The SAN administrator may execute **no** commands on these interfaces.

Deny Actions for Pre-determined Ethernet Interfaces Designated to Carry FCoE Traffic

This deny-list applies to Ethernet, port-channel, and vEthernet interfaces that are designated to carry FCoE traffic.

```
switch(config-if)# bandwidth *
switch(config-if)# fcoe *
switch(config-if)# flowcontrol *
switch(config-if)# link debounce *
switch(config-if)# lldp *
switch(config-if)# priority-flow-control *
switch(config-if)# service-policy *
switch(config-if)# shutdown
switch(config-if)# shutdown force
switch(config-if)# shutdown lan // TBD. This is a new command to shut stop LAN VLANs
switch(config-if)# spanning-tree bpdufilter
switch(config-if)# spanning-tree bpduguard
switch(config-if)# spanning-tree cost *
switch(config-if)# spanning-tree guard *
switch(config-if)# spanning-tree link-type *
switch(config-if)# spanning-tree mst *
switch(config-if)# spanning-tree port type *
switch(config-if)# spanning-tree port-priority *
switch(config-if)# speed *
switch(config-if)# switchport host
```

```
switch(config-if)# switchport mode *
switch(config-if)# switchport monitor
switch(config-if)# switchport trunk native *
switch(config-if)# switchport trunk allowed vlan <range>
switch(config-if)# switchport trunk allowed vlan add <non-fcoe-vlan>
switch(config-if)# switchport trunk allowed vlan all
switch(config-if)# switchport trunk allowed vlan except *
switch(config-if)# switchport trunk allowed vlan none
switch(config-if)# switchport trunk allowed vlan remove <non-fcoe-vlan>
```

LAN Deny Actions

LAN Deny Actions

The SAN administrator can not execute LAN-related commands.

```
switch(config)# cdp *
switch(config)# ip igmp snooping *
switch(config)# port-channel load-balance ethernet
switch(config)# rmon
switch(config)# track
```

Sample Configurations

The following configurations are used to create both LAN and SAN administrative roles. These configurations follow the outline listed above concerning the commands that are assigned to or withheld from each role. Configuration is not needed for the Global Administrator who automatically has access to all configuration commands.

Note This configuration assumes that vFC 1 is mapped to Ethernet 1/1 and that VLAN 100 has been designated the FCoE VLAN. This configuration is based on the specific environment and which Ethernet ports and VLANs have been pre-determined to carry FCoE traffic.

LAN-Admin Configuration

role name LAN-admin

description assume vlan 100 is fcoe enabled and eth1/1 is an vfc bound (fcoe) interface

rule 97 deny command config t ; feature lacp

rule 96 deny command config t ; feature tacacs+

rule 95 deny command config t ; feature udld

rule 94 deny command config t ; feature fcoe

rule 93 deny command config t ; aaa *

rule 92 deny command config t ; boot *

rule 91 deny command config t ; cfs *

rule 90 deny command config t ; class-map *

rule 89 deny command config t ; device-alias *

rule 88 deny command config t ; diagnostic *

rule 87 deny command config t ; fex *

rule 86 deny command config t ; hw-module logging onboard *
rule 85 deny command config t ; license *
rule 84 deny command config t ; line *
rule 83 deny command config t ; lldp *
rule 82 deny command config t ; monitor session *
rule 81 deny command config t ; ntp *
rule 80 deny command config t ; policy-map *
rule 79 deny command config t ; privilege *
rule 78 deny command config t ; radius-server *
rule 77 deny command config t ; role *
rule 76 deny command config t ; snmp-server *
rule 75 deny command config t ; ssh *
rule 74 deny command config t ; system *
rule 73 deny command config t ; no system *
rule 72 deny command config t ; tacacs+ *
rule 71 deny command config t ; telnet server enable
rule 70 deny command config t ; trunk protocol enable
rule 69 deny command config t ; username *
rule 68 deny command config t ; vrf *
rule 67 deny command config t ; xml server *
rule 66 deny command config t ; fabric-binding *
rule 65 deny command config t ; fcalias *
rule 64 deny command config t ; fcdomain *
rule 63 deny command config t ; fcdroplatency *
rule 62 deny command config t ; fcflow *
rule 61 deny command config t ; fcid-allocation *
rule 60 deny command config t ; fcinterop *
rule 59 deny command config t ; fcns *
rule 58 deny command config t ; fcroute *
rule 57 deny command config t ; fcs *
rule 56 deny command config t ; fcsp *
rule 55 deny command config t ; fctimer *
rule 54 deny command config t ; fdmi *
rule 53 deny command config t ; fspf *
rule 52 deny command config t ; in-order-guarantee
rule 51 deny command config t ; npiv *
rule 50 deny command config t ; npv *
rule 49 deny command config t ; port-security enable

rule 48 deny command config t ; port-track enable
rule 47 deny command config t ; rib *
rule 46 deny command config t ; rlir *
rule 45 deny command config t ; rscn *
rule 44 deny command config t ; scsi-target *
rule 43 deny command config t ; vsan database *
rule 42 deny command config t ; wwn *
rule 41 deny command config t ; zone *
rule 40 deny command config t ; zoneset *
rule 39 deny command config t ; vlan * ; fcoe *
rule 38 deny command config t ; vlan * ; no fcoe *
rule 37 deny command config t ; spanning-tree vlan 100
rule 36 permit command config t ; spanning-tree vlan *
rule 35 deny command config t ; spanning-tree *
rule 34 deny command config t ; mac-address-table aging-time * vlan 100
rule 33 deny command config t ; mac-address-table static * vlan 100 *
rule 32 deny command config t ; monitor session * ; source vlan 100
rule 31 deny command config t ; vlan 100 *
rule 30 deny command config t ; no vlan 100 *
rule 29 deny command config t ; interface Ethernet1/1 ; bandwidth *
rule 28 deny command config t ; interface Ethernet1/1 ; fcoe *
rule 27 deny command config t ; interface Ethernet1/1 ; flowcontrol *
rule 26 deny command config t ; interface Ethernet1/1 ; link debounce *
rule 25 deny command config t ; interface Ethernet1/1 ; lldp *
rule 24 deny command config t ; interface Ethernet1/1 ; priority-flow-control *
rule 23 deny command config t ; interface Ethernet1/1 ; service-policy *
rule 22 deny command config t ; interface Ethernet1/1 ; shutdown
rule 21 deny command config t ; interface Ethernet1/1 ; shutdown force
rule 20 deny command config t ; interface Ethernet1/1 ; spanning-tree bpdufilter *
rule 19 deny command config t ; interface Ethernet1/1 ; spanning-tree bpduguard *
rule 18 deny command config t ; interface Ethernet1/1 ; spanning-tree cost *
rule 17 deny command config t ; interface Ethernet1/1 ; spanning-tree guard *
rule 16 deny command config t ; interface Ethernet1/1 ; spanning-tree link-type *
rule 15 deny command config t ; interface Ethernet1/1 ; spanning-tree mst *
rule 14 deny command config t ; interface Ethernet1/1 ; spanning-tree port type *
rule 13 deny command config t ; interface Ethernet1/1 ; spanning-tree port-priority *
rule 12 deny command config t ; interface Ethernet1/1 ; speed *
rule 11 deny command config t ; interface Ethernet1/1 ; switchport host

```
  rule 10 deny command config t ; interface Ethernet1/1 ; switchport mode *
  rule 9 deny command config t ; interface Ethernet1/1 ; switchport monitor
  rule 8 deny command config t ; interface Ethernet1/1 ; switchport trunk native vlan 100
  rule 7 deny command config t ; interface Ethernet1/1 ; switchport trunk allowed vlan *
  rule 6 deny command config t ; interface Ethernet1/1 ; switchport trunk allowed vlan add 100
  rule 5 deny command config t ; interface Ethernet1/1 ; switchport trunk allowed vlan all
  rule 4 deny command config t ; interface Ethernet1/1 ; switchport trunk allowed vlan except *
  rule 3 deny command config t ; interface Ethernet1/1 ; switchport trunk allowed vlan none
  rule 2 deny command config t ; interface Ethernet1/1 ; switchport trunk allowed vlan remove 100
  rule 1 permit read-write
  interface policy deny
    permit interface eth1/1-40
  vlan policy deny
    permit vlan 100-200
  vsan policy deny
```

SAN-Admin Configuration

```
role name SAN-admin
  description assuming vlan 100 is fcoe enabled and vfc1 has been bound to eth1/1
  rule 83 permit command config t ; vlan * ; fcoe *
  rule 82 deny command config t ; vlan * ; *
  rule 81 deny command config t ; ip igmp snooping *
  rule 80 deny command config t ; cdp *
  rule 79 deny command config t ; port-channel load-balance ethernet *
  rule 78 deny command config t ; rmon *
  rule 77 deny command config t ; track *
  rule 76 deny command config t ; no ip igmp *
  rule 75 deny command config t ; no cdp *
  rule 74 deny command config t ; no port-channel load-balance *
  rule 73 deny command config t ; no rmon *
  rule 72 deny command config t ; no track *
  rule 71 deny command config t ; interface * ; switchport trunk native *
  rule 70 deny command config t ; interface * ; switchport trunk allowed vlan *
  rule 69 deny command config t ; interface * ; switchport trunk allowed vlan add 100
  rule 68 deny command config t ; interface * ; switchport trunk allowed vlan all
  rule 67 deny command config t ; interface * ; switchport trunk allowed vlan except *
  rule 66 deny command config t ; interface * ; switchport trunk allowed vlan none
  rule 65 deny command config t ; interface * ; switchport trunk allowed vlan remove 100
```

rule 64 deny command config t ; interface * ; bandwidth *
rule 63 deny command config t ; interface * ; fcoe *
rule 62 deny command config t ; interface * ; flowcontrol *
rule 61 deny command config t ; interface * ; link debounce *
rule 60 deny command config t ; interface * ; lldp *
rule 59 deny command config t ; interface * ; priority-flow-control *
rule 58 deny command config t ; interface * ; service-policy *
rule 57 deny command config t ; interface * ; shutdown
rule 56 deny command config t ; interface * ; shutdown force
rule 55 deny command config t ; interface * ; shutdown lan
rule 54 deny command config t ; interface * ; spanning-tree bpdufilter
rule 53 deny command config t ; interface * ; spanning-tree bpduguard
rule 52 deny command config t ; interface * ; spanning-tree cost *
rule 51 deny command config t ; interface * ; spanning-tree guard *
rule 50 deny command config t ; interface * ; spanning-tree link-type *
rule 49 deny command config t ; interface * ; spanning-tree mst *
rule 48 deny command config t ; interface * ; spanning-tree port type *
rule 47 deny command config t ; interface * ; spanning-tree port-priority *
rule 46 deny command config t ; interface * ; speed *
rule 45 deny command config t ; interface * ; switchport host
rule 44 deny command config t ; interface * ; switchport mode *
rule 43 deny command config t ; interface * ; switchport monitor
rule 42 deny command config t ; no vlan 100 *
rule 41 permit command config t ; feature fcoe
rule 40 deny command config t ; feature *
rule 39 deny command config t ; aaa *
rule 38 deny command config t ; boot *
rule 37 deny command config t ; cfs *
rule 36 deny command config t ; class-map *
rule 35 deny command config t ; device-alias *
rule 34 deny command config t ; diagnostic *
rule 33 deny command config t ; fex *
rule 32 deny command config t ; hw-module logging onboard *
rule 31 deny command config t ; ip *
rule 30 deny command config t ; ipv6 *
rule 29 deny command config t ; license *
rule 28 deny command config t ; line *
rule 27 deny command config t ; lldp *

```
rule 26 deny command config t ; mac-address-table *
rule 25 deny command config t ; monitor session *
rule 24 deny command config t ; ntp *
rule 23 deny command config t ; policy-map *
rule 22 deny command config t ; privilege *
rule 21 deny command config t ; radius-server *
rule 20 deny command config t ; role *
rule 19 deny command config t ; snmp-server *
rule 18 deny command config t ; spanning-tree bridge assurance *
rule 17 deny command config t ; spanning-tree loopguard *
rule 16 deny command config t ; spanning-tree mode *
rule 15 deny command config t ; spanning-tree mst *
rule 14 deny command config t ; spanning-tree pathcost *
rule 13 deny command config t ; spanning-tree port type *
rule 12 deny command config t ; ssh *
rule 11 deny command config t ; system core *
rule 10 deny command config t ; system default switchport *
rule 9 deny command config t ; system jumbomtu *
rule 8 deny command config t ; system qos *
rule 7 deny command config t ; tacacs+ *
rule 6 deny command config t ; telnet server enable
rule 5 deny command config t ; trunk protocol enable
rule 4 deny command config t ; username *
rule 3 deny command config t ; vrf  *
rule 2 deny command config t ; xml server *
rule 1 permit read-write
vlan policy deny
  permit vlan 100-100
interface policy deny
  permit interface fc3/1-4
  permit interface Ethernet1/1
  permit interface vfc1
```