Setting method_①Disable management access from the Internet to a NetScaler interface (SNIP)

Setting method via GUI

Setting method in case of logging in to NetScaler via http or https is as follows.

Confirm SNIP subject of working

Click System>Network>IPs, and confirm IP addresses registered to NetScaler.

Make sure there is IP address necessary to change settings out of several IP addresses which types are SNIPs.

Example below shows 172.16.10.14 and 172.16.20.12 are SNIPs.

172.16.20.12 is subject of working in the following procedure.

Open Edit screen of SNIP

Select SNIP customers want to change setting, and click [Edit].

Confirm Detail settings of SNIP

Scroll down the edit screen, "Application Access Controls" is displayed.

Example Below shows four boxes of Enable Management Access, SSH, GUI and SNMP are checked(Enabled).

Disable management access of SNIP

Uncheck all boxes enabled option.

Example below shows boxes of SSH, GUI, SNMP and "Enable Management Access" are unchecked.

⚠ To disable option without fail, unchecking box in order from except for "Enable Management Access" is recommended.

When box of "Enable Management Access" is unchecked, pop up box is displayed and click [Yes].

"Application Access Controls" is displayed as follows, and click [OK] after confirming box is unchecked.

⚠ Logging in is not available if above action is taken to SNIP which customers access to change settings.

Settings are not saved yet, customers can restore the state before by rebooting NetScaler via ECL2.0 Customer Portal etc.

Confirm settings are disabled 1

Select SNIP which customers change settings, and click [Edit].

Reduced screen of "Application Access Controls" is displayed as follows.

Settings are disabled if box is unchecked.

Confirm settings are disabled 2

To confirm settings are disabled, login to SNIP which setting is disabled from outside of NetScaler via ssh and gui(http,https), and acquire value via snmp. Confirm there is no response.

Examples are not shown because it depends on customers' environment.

Save settings

Click Floppy disk mark which is shown at upper right of screen.

Pop up box is displayed, click [Yes].

⚠ If above procedure is not followed, restoration to its former state occurs in case of rebooting NetScaler with some reason.

Please make sure to save setting.

Setting method via CLI

Setting method in case of logging in to NetScaler via ssh is as follows.

Confirm SNIP subject of working

```
show ns ip
```

Execute above command, and confirm IP address registered to NetScaler.

Make sure there is IP address necessary to change settings out of several IP addresses which types are SNIPs.

Example below shows 172.16.10.14 and 172.16.20.12 are SNIPs.

172.16.20.12 is subject of working in the following procedure.

```
> show ns ip
  Ipaddress       Traffic Domain  Type          Mode     Arp     Icmp    Vserver  State
  ---------       --------------  ----          ----     ---     ----    -------  ------
1) 172.16.10.14     10            SNIP          Active   Enabled  Enabled  NA      Enabled
2) 172.16.20.12     10            SNIP          Active   Enabled  Enabled  NA      Enabled
3) 172.16.10.100    10             VIP          Active   Enabled  Enabled  Enabled  Enabled
 Done
```

Confirm Detail settings of SNIP

```
show ns ip "Target IP address" -td 10
```

Execute above command, and confirm option status of management access and ssh and so on.

Example below shows management access, ssh, gui and snmp are Enabled.

```
> show ns ip 172.16.20.12 -td 10
 IP: 172.16.20.12
 （Omitted）
 management access: Enabled
   telnet: Disabled
   ftp: Disabled
   ssh: Enabled
   gui: Enabled
   snmp: Enabled
 （Omitted）
 Done
```

Disable management access of SNIP

Disable management access and ssh options enabled on IP address subject of working by executing command below.

```
set ns ip "Target IP address" -td 10 -ssh Disabled -gui Disabled -snmp Disabled -mgmtAccess Disabled
```

Example below shows management access, ssh, gui, snmp are disabled on 172.16.20.12.

```
> set ns ip 172.16.20.12 -td 10 -ssh Disabled -gui Disabled -snmp Disabled -mgmtAccess Disabled
 Done
```

⚠ Logging in is not available again if above command is executed to SNIP which they access to change settings.

Settings are not saved yet, customers can restore its former state by rebooting NetScaler via ECL2.0 Customer Portal etc.

Confirm settings are disabled 1

```
show ns ip "Target IP address" -td 10
```

Execute above command, and confirm option status of management access and ssh and so on.

Example below shows management access, ssh, gui and snmp are all disabled.

```
> show ns ip 172.16.20.12 -td 10
 IP: 172.16.20.12
 （Omitted）
 management access: Disabled
   telnet: Disabled
   ftp: Disabled
   ssh: Disabled
   gui: Disabled
   snmp: Disabled
 （Omitted）
 Done
```

Confirm settings are disabled 2

To confirm settings are disabled, login to SNIP which setting is disabled from outside of NetScaler via ssh and gui(http,https), and acquire value via snmp. Confirm there is no response.

Examples are not shown because it depends on customers' environment.

Save settings

```
save ns config
```

Execute above command, and save settings changed.

⚠ To confirm settings are disabled, login to SNIP which setting is disabled from outside of NetScaler via ssh and gui(http,https), and acquire value via snmp. Confirm there is no response.

Examples are not shown because it depends on customers' environment.

Revision history

Date	Version	Detail
2017/9/27	1.0.0	First edition