



GENIAN NAC 범용OS 매뉴얼

2021-09-17 / 네트워크보안기술부



목차

제품 설치

1. 범용 OS 기본 구성
2. 장비 접속 방법
3. CLI 명령어
4. 초기 설정
5. 구성 별 설정방법
6. OS 업그레이드

유지보수

1. 장비 점검
 2. Backup 및 Restore
 3. 장비 초기화 및 종료
 4. 시간 동기화
-

제품 설치



* 범용OS 변경사항

범용 OS 버전 구성

지원 OS

범용 OS인 Ubuntu에서 동작하는 NAC 제품으로 다음 버전에서 구동 지원

〈참고사항〉

- OS : Ubuntu 18.04.5 LTS
Kernel: Linux 4.15.0
Architecture: x86-64
- DB : Mysql 8.0.18-9
- Web : Apache 2.4.29, Apache Tomcat 8.5.39
- LOG : Elasticsearch 6.8.6

지원 장비 모델

아래 해당되는 모델만 범용 OS 버전 NAC 설치 지원

구분	모델
센터	C10_R1, C20_R1, C30_R1, C40_R1, C50_R1, C50_R2 ES30, ES30_R1, ES50, ES50_R1
센서	S10_R2, S20_R2, S30H_R1, S40H_R1, S50H_R1

* 범용OS 변경사항

범용 OS 제품 이미지

- NAC 제품 정책 서버 이미지, 센서 이미지 등 이미지 종류 및 릴리즈 과정에 대해 설명
- 범용 OS 버전 제품 이미지 파일은 기존 img -> deb 파일로 변경

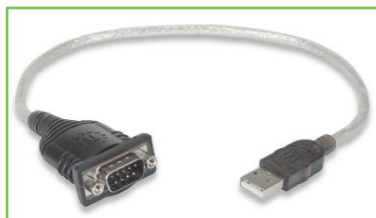
릴리즈 명	용도
CURRENT	<p>현재 개발버전으로 개발자 간의 소스 공유를 목적으로 하는 버전 버전에 따라 미완성 기능이 포함되므로 실제 서비스용으로 사용 불가</p> <p>센터 : NAC-UBUNTU-C-xxxxx-x.x.x.xxxx.deb 센서 : NAC-UBUNTUNS-C-xxxxx-x.x.x.xxxx.deb</p>
BETA	<p>기능의 수정이 완료되면 적용하는 버전 동작은 정상적이나 반복되는 기능 갱신이 발생</p> <p>센터 : NAC-UBUNTU-B-xxxxx-x.x.x.xxxx.deb 센서 : NAC-UBUNTUNS-B-xxxxx-x.x.x.xxxx.deb</p>
RELEASE (CANDIDATE, RELEASE)	<p>실제 고객제품에 사용될 것을 목적으로 만들어진 버전 일정기간 수정되거나 추가된 기능을 모아서 주기적으로 릴리즈 CANDIDATE는 RELEASE보다 한단계 높은 버전을 가지고 있으며 신규 기능이 필요하면 CANDIDATE이미지를 사용하고 안정성이 요구되면 RELEASE를 사용하면 된다</p> <p>센터 : NAC-UBUNTU-R-xxxxx-x.x.x.xxxx.deb 센서 : NAC-UBUNTUNS-R-xxxxx-x.x.x.xxxx.deb</p>

장비 접속 방법

- Console 직접 연결 방식으로 접속 하는 방법을 설명

Console 접속 준비물

USBtoSerial converter, Serial consol(Rj45 type, DB9 type)



〈USB to Serial〉



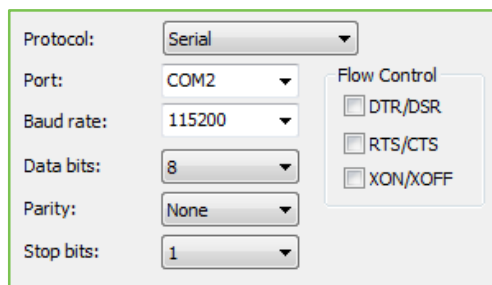
〈RJ45 type Serial〉



〈DB9 type Serial〉

Console 접속 방법

터미널프로그램 실행 : SecureCRT, X-shell, Putty 등



〈연결 설정〉

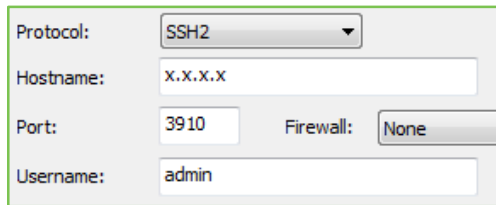
- 1) Protocol : Serial
- 2) Port : USBtoSerial 케이블을 연결한 PC의 포트
- 장치관리자 > 포트 > 연결된 COM포트 확인
- 3) Baud rate : 연결 속도(115200)
- 4) Data bits : 8bit
- 5) Parity : None
- 6) Stop bit : 1

장비 접속 방법

- SSH 방식으로 장비 접속하는 방법

SSH 접속 방법

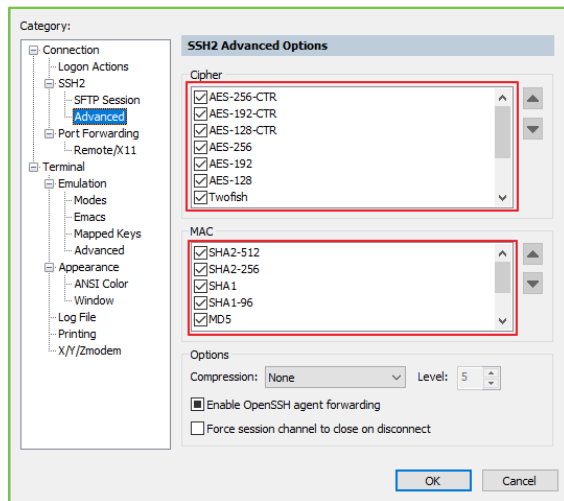
터미널프로그램 실행 : SecureCRT, X-shell, Putty등



Protocol: SSH2
Hostname: x.x.x.x
Port: 3910 Firewall: None
Username: admin

- 1) Protocol : SSH2
- 2) Hostname : 접속장비 IP
- 3) Port : 3910

〈연결 설정〉



Category: SSH2

SSH2 Advanced Options

Cipher

- ☒ AES-256-CTR
- ☒ AES-192-CTR
- ☒ AES-128-CTR
- ☒ AES-256
- ☒ AES-192
- ☒ AES-128
- ☒ Twofish

MAC

- ☒ SHA2-512
- ☒ SHA2-256
- ☒ SHA1
- ☒ SHA1-96
- ☒ MD5

Options

Compression: None Level: 5

☒ Enable OpenSSH agent forwarding

☐ Force session channel to close on disconnect

OK Cancel

- AES-256, SHA2-512를 지원하지 않는 터미널프로그램은 최신 버전으로 업데이트를 권장한다.

Genian Shell Command

* 범용OS 변경사항

Login step

Ubuntu 로그인	1. ID/PW 입력 - user/admin123! (Default)
Exec mode	2. Root 권한 획득 - 명령어 : sudo su 3. Genian Shell 로그인 - 명령어 : gnlogin - PW 입력 : admin123! (Default)
privileged mode	4. Privileged mode 전환 - 명령어 : enable - PW 입력 : admin123! (Default)
configuration mode	5. configuration mode 전환 - 명령어 : configure terminal - PW 입력 : admin123! (Default)

Genian Shell Command

STEP 1 : exec mode

genian> ?

exit	Exit from current mode
help	Show available commands
history	Show a list of previously run commands
quit	Exit from the console
clear	Clear Operation
enable	Turn on privileged command.
ping	Send ICMP echo request
show	Show system information
tracert	Trace route information to destination

STEP 2 : privileged mode

genian# ?

exit	Exit from current mode
help	Show available commands
history	Show a list of previously run commands
quit	Exit from the console
configure	Enter configuration mode
clear	Clear Operation
clock	Manage system clock
disable	Turn off privileged command.
do	Do system command
halt	Prepare to Power Shutdown mode
kill	Kill
ping	Send ICMP echo request
reboot	Halt and perform a cold restart
restart	Restart service
show	Show system information
shutdown	Shutdown
tracert	Trace route information to destination

Genian Shell Command

STEP3 : configuration mode

genian(config)# ?

exit	Exit from current mode
help	Show available commands
history	Show a list of previously run commands
quit	Exit from the console
no	Negate a command
clear	Clear all configuration
add	Add data
admin-acl	Change Administrator ACL
bonding	Interface bonding parameters
consoleadmin	Create Console Administrator
device-id	Manual setup Device ID
data-server	Modify DataBase Server parameter
delete	Delete data
dist-server	Modify Distribute-Server parameter
enable	Modify enable Administrator.
force-passive	always run passive mode

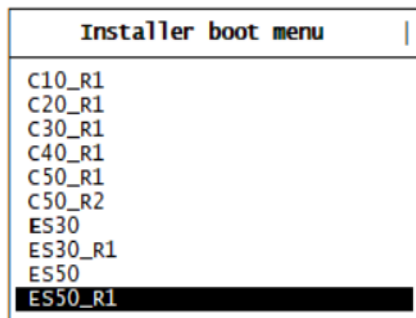
healthcheck	HealthCheck Options
hostname	Device HostName
interface	Network interface parameters
ip	IP networking parameters
log-server	Modify Log Server parameter
management-server	Modify Management-Server parameter
node-server	Modify Node-Server parameter
ntp	Configure NTP
sensor	Sensor configuration
show	Show system information
ssh	SSH configuration
superadmin	Create Super Administrator
system-locale	Modify System Default Locale
syslog	Syslog configuration
procmond	Procmond configuration
sysfault	System fault check parameters

* 범용OS 변경사항

초기 설정

- CLI 기본 설정에 대한 설명

최초 설치(참고)



Press ENTER to boot or TAB to edit a menu entry

- USB로 부팅 시, 설치할 장비의 모델을 선택
- 모델 선택 후, 랜 케이블이 연결된 상태에서 자동설치 진행

※ 참고사항

- 자동설치 시, 장비 모델 별 랜 케이블 연결할 인터페이스 고정

eth0	센터 : C20_R1, C30_R1, C40_R1, C50_R1, C50_R2 센서 : S10_R2, S20_R2, S50H_R1
eth2	센터 : C10_R1 센서 : S30H_R1, S40H_R1

해당 Step 은 양산 과정에서 처리 후 출고되기 때문에 엔지니어에 의한 작업 X

STEP 1 : Ubuntu 및 Gnlogin 접속

```
genians login: user
Password :
user@genians:~# sudo su
root@genians:~# gnlogin
Password :
```

```
sudo su : root 권한 획득
gnlogin : Genian Shell 진입
```

초기 설정

- CLI 기본 설정에 대한 설명

STEP 2 : 인터페이스 설정

```
genian> enable
Password :
genian# configure terminal
genian(config)# interface eth0 address [IP]
[Subnetmask]
genian(config)# interface eth0 gateway [IP]
genian(config)# ip default-gateway [IP]
genian(config)# ip name-server [IP]
genian(config)#ntp server [IP]
```

enable : exec모드로 진입
configure terminal : 설정 모드로 진입
인터페이스의 아이피와 서브넷 마스크 설정
인터페이스의 게이트 웨이 설정
장비 기본 게이트 웨이 설정
장비 DNS 서버 설정
장비 NTP 서버 설정

STEP 3 : DB 설정

```
genian(config)# data-server username [DB계정]
Genian(config)# data-server enable
Genian(config)# data-server password [DB 패스워드]
Genian(config)# data-server access-list all
```

DB 계정 설정
DB 서버 구동 명령
DB서버 접속 계정 패스워드 설정
DB 접근 권한 설정

STEP 4 : 로그서버 설정

```
genian(config)# log-server enable
```

LOG서버 구동 명령

초기 설정

- CLI 기본 설정에 대한 설명

STEP 5 : 관리WebUI, SoapServer 설정

```
genian(config)# interface eth0 management-server  
enable  
genian(config)# interface eth0 node-server enable
```

관리 Web UI 구동 명령
Soap 서버 구동 명령

STEP 6 : 관리자 계정 생성 (최초1회 가능)

```
genian(config)# superadmin [관리자 계정] [관리자 패스워드]  
[관리자 이메일]
```

관리 WebUI 계정 생성 명령

STEP 7 : Debug 설정

```
genian(config)# debug sensord all  
genian(config)# debug centerd all
```

센서데몬 디버그 설정
센터데몬 디버그 설정
- vrrpd, kernel, storage 도 설정 가능

NAC 구성 방식

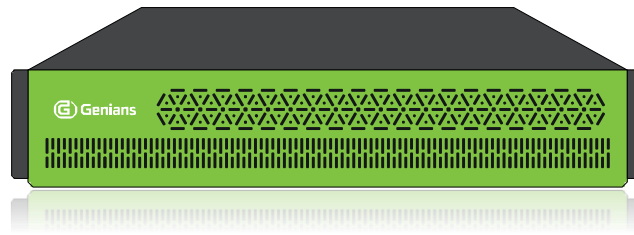
1. 정책서버 구성

- 모듈 형태로 일부 기능을 H/W 단위로 분리하여 구성 가능
- Policy, DB, LOG, RADIUS 4가지 모듈로 분리 가능
- 각 모듈들은 역할별로 Active/Active 구성, Active/Standby 구성이 가능
- Bonding 설정 지원 가능

2. 센서 구성

- 멀티 센서와 싱글 센서로 구분하며 VLAN 사용/미사용으로 구별
- Bonding 설정이 가능하며 VRRP를 이용한 H/W 이중화도 가능

단일 구성 (Policy + Database + Radius + LOG)



(WEB+DB+LOG+RADIUS)

* 범용OS 변경사항

단일 구성 (Policy + Database + Radius + LOG)

- Policy와 Database, Radius, Log서버를 단일 장비에 구성할 때 config

```
genian(config)#debug sensord all
genian(config)#debug centerd all
```

```
genian(config)#interface eth0 address [IP] [Subnetmask]
genian(config)#interface eth0 gateway [IP]
genian(config)#ip default-gateway [IP]
genian(config)#ip name-server [IP]
genian(config)#ntp server [IP]
```

```
genian(config)#data-server username [string]
genian(config)#data-server enable
genian(config)#data-server password [string]
genian(config)#data-server access-list [IP/CIDR]
```

```
genian(config)#log-server=enable
log-server_cluster-name=GENIAN (자동생성)
log-server access-password [암호화 값] (자동생성)
log-server access-user elastic (자동생성)
```

```
genian(config)#interface eth0 management-server enable
genian(config)#interface eth0 node-server enable
genian(config)#Interface eth0 radius-server enable
```

```
genian(config)#device-id 6029b2d8-b21e-1001-8001-009 (자동생성)
```

SENSORD 데몬 디버그 설정
CENTERD 데몬 디버그 설정

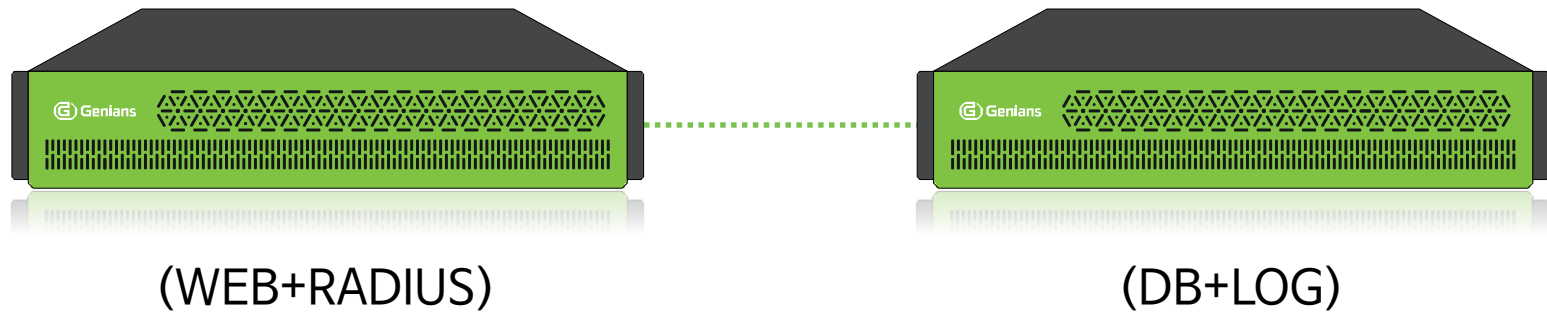
인터페이스 아이피, 서브넷 마스크
인터페이스 게이트웨이
장비 기본 게이트웨이
장비 도메인네임서버

DB 계정 설정
DB 서버 구동 명령
DB서버 접속 계정 패스워드 설정
DB 접근 권한 설정

로그서버 설정

관리UI 구동 설정
SOAP서버 구동 설정
RADIUS서버 구동 설정

분리 구성 (Database + LOG / WEB + RADIUS)



* 범용OS 변경사항

분리 구성 (Database + LOG)

- Database 서버와 Log 서버를 단일 장비에 구성할 때 config

```
genian(config)#debug sensord all
```

```
genian(config)#interface eth0 address [IP] [Subnetmask]  
genian(config)#interface eth0 gateway [IP]
```

```
genian(config)#ip default-gateway [IP]  
genian(config)#ip name-server [IP]
```

```
genian(config)#data-server username [string]  
genian(config)#data-server enable  
genian(config)#data-server password [string]  
genian(config)#data-server access-list [IP/CIDR]
```

```
genian(config)#log-server=enable  
genian(config)#log-server_cluster-name=GENIAN (자동생성)  
log-server access-password [암호화 값] (자동생성)  
log-server access-user elastic (자동생성)
```

```
genian(config)#node-server ip [IP]
```

디버그 설정

인터페이스 아이피, 서브넷 마스크
인터페이스 게이트웨이
장비 기본 게이트웨이
장비 도메인네임서버

DB 계정 설정
DB 서버 구동 명령
DB서버 접속 계정 패스워드
DB 접근 권한 설정

로그서버 구동

정책서버 지정

* 범용OS 변경사항

분리 구성 (Policy + Radius)

- Policy 서버와 Radius 서버를 단일 장비에 구성할 때 config

```
genian(config)#debug sensord all  
genian(config)#debug centerd all
```

```
interface eth0 address [IP] [Subnetmask]  
interface eth0 gateway [IP]  
ip default-gateway [IP]  
ip name-server [IP]  
ntp server [IP]
```

```
data-server ip [IP]  
data-server username [string]  
data-server password [string]
```

```
log-server ip [IP]  
log-server access-password [암호화 값]  
log-server access-user elastic
```

```
interface eth0 management-server enable  
interface eth0 node-server enable  
Interface eth0 radius-server enable
```

디버그 설정

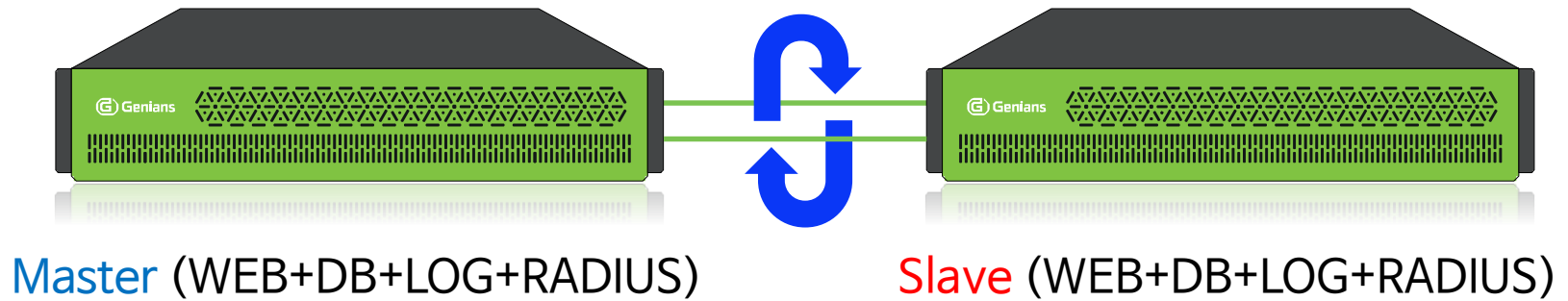
인터페이스 아이피, 서브넷 마스크
인터페이스 게이트웨이
장비 기본 게이트웨이
장비 도메인네임서버
시간동기화 서버

DB 서버 IP 지정
DB 서버 구동 명령
DB서버 접속 계정 패스워드

로그서버 IP 지정
log-server access-password 값과 log-server access-user elastic 값은 분리구성 된 log 서버의 값과 동일하게 변경해야 한다. (변경 방법 P.23 참고)

정책서버 관리UI 구동
SOAP서버 구동
RADIUS서버 구동

이중화 설정



* 범용OS 변경사항

이중화 설정

1. Policy, DB, LOG 구성의 장비 이중화 구성 설정

- 이중화 구성은 장비 설정 순서가 중요
- 이중화 구성 설정 중, 순서의 실수나 오류가 발생하면 장비 초기화를 수행하여 처음부터 다시 설정
- 장비 2대는 간이스위치나 HUB로 연결한 상태에서 Config 설정

2. 장비 이중화 설정 순서

Master Device

- 1) Debug 설정
- 2) 장비 인터페이스 설정 (IP, Subnet, Gateway, DNS, Default GW)
- 3) Data-server 설정
- 4) Log-server 설정
- 5) Policy center 설정
- 6) 인터페이스 HA 설정

Slave Device

- 1) Debug 설정
- 2) Device ID 설정 (Master device id)
- 3) 장비 인터페이스 설정
- 4) Data-server 설정
- 5) Log-server 설정
- 6) 인터페이스 HA 설정
- 7) Policy center 설정

3. 설정 완료 후, 확인사항

- VRRP Master / Slave 체크
- DB Replication 체크
- Elasticsearch clustering 체크
- log-server access-user, log-server access-password 값 일치 여부 확인
- 기본 서비스 체크

* 범용OS 변경사항

이중화 설정

- 이중화 구성을 하는 장비의 설정 명령어 순서 - Master

Master

```
debug sensord all
debug centerd all
debug vrrpd all
```

```
interface eth0 address [IP] [SubnetMask]
interface eth0 gateway [Gateway IP]
ip default-gateway [Gateway IP]
ip name-server [DNS IP]
ntp server [NTP server IP]
```

```
data-server username [ID]
data-server enable
data-server password [password]
data-server access-list [IP/CIDR]
data-server replica serverid [1]
data-server replica enable
```

```
log-server=enable
log-server access-password [암호화 값] (자동생성)
log-server access-user elastic (자동생성)
log-server_cluster-name=GENIAN (자동생성)
log-server cluster-peers [Slave log server ip]
```

```
interface eth0 management-server enable
interface eth0 node-server enable
```

```
superadmin [ID] [PASSWORD] [EMAIL]
```

```
interface eth0 ha group [Number]
interface eth0 ha priority 200
interface eth0 ha virtual-ip [IP]
```

※ 주의

위 설정 순서를 꼭 지켜서 입력해주세요.
설정 순서 변경으로 예상치 못한 동작이 발생 할 수 있습니다.
HA설정 중 devid관련 error가 발생할 시, console session을 종료 후 다시 접속하여 설정해보시기 바랍니다.

- DB replication을 위해서는 data-server access-list에 Slave server의 IP가 포함되어야 합니다.

* 범용OS 변경사항

이중화 설정

- 이중화 구성을 하는 장비의 설정 명령어 순서 - **Slave**

Slave

```
debug sensord all
debug centerd all
debug vrrpd all
```

```
device-id [ Primary Device id]
```

```
Interface eth0 address [IP] [SubnetMask]
```

```
Interface eth0 gateway [Gateway IP]
```

```
ip default-gateway [Gateway IP]
```

```
Ip name-server [DNS IP]
```

```
ntp server [NTP server IP]
```

```
data-server username [ID]
```

```
data-server enable
```

```
data-server password [password]
```

```
data-server access-list [IP/CIDR]
```

```
data-server replica serverid [2]
```

```
data-server replica masterhost [Master DB IP]
```

```
data-server replica enable
```

```
log-server=enable
```

```
log-server access-password [암호화 값] (자동생성)
```

```
log-server access-user elastic (자동생성)
```

```
log-server_cluster-name=GENIAN (자동생성)
```

```
log-server cluster-peers [Master log server ip]
```

```
superadmin [ID] [PASSWORD] [EMAIL]
```

```
interface eth0 ha group [Number]
```

```
interface eth0 ha priority 100
```

```
interface eth0 ha virtual-ip [IP]
```

```
interface eth0 management-server enable
```

```
interface eth0 node-server enable
```

※ 주의

위 설정 순서를 꼭 지켜서 입력해주세요.

설정 순서 변경으로 예상치 못한 동작이 발생 할 수 있습니다.

HA설정 중 devid관련 error가 발생할 시, console session을 종료 후 다시 접속하여 설정해보시기 바랍니다.

HA설정 중 nopreempt, linkupdelay, timeout 옵션은 필요에 따라 적용해야 합니다.

※ log-server access 설정 변경

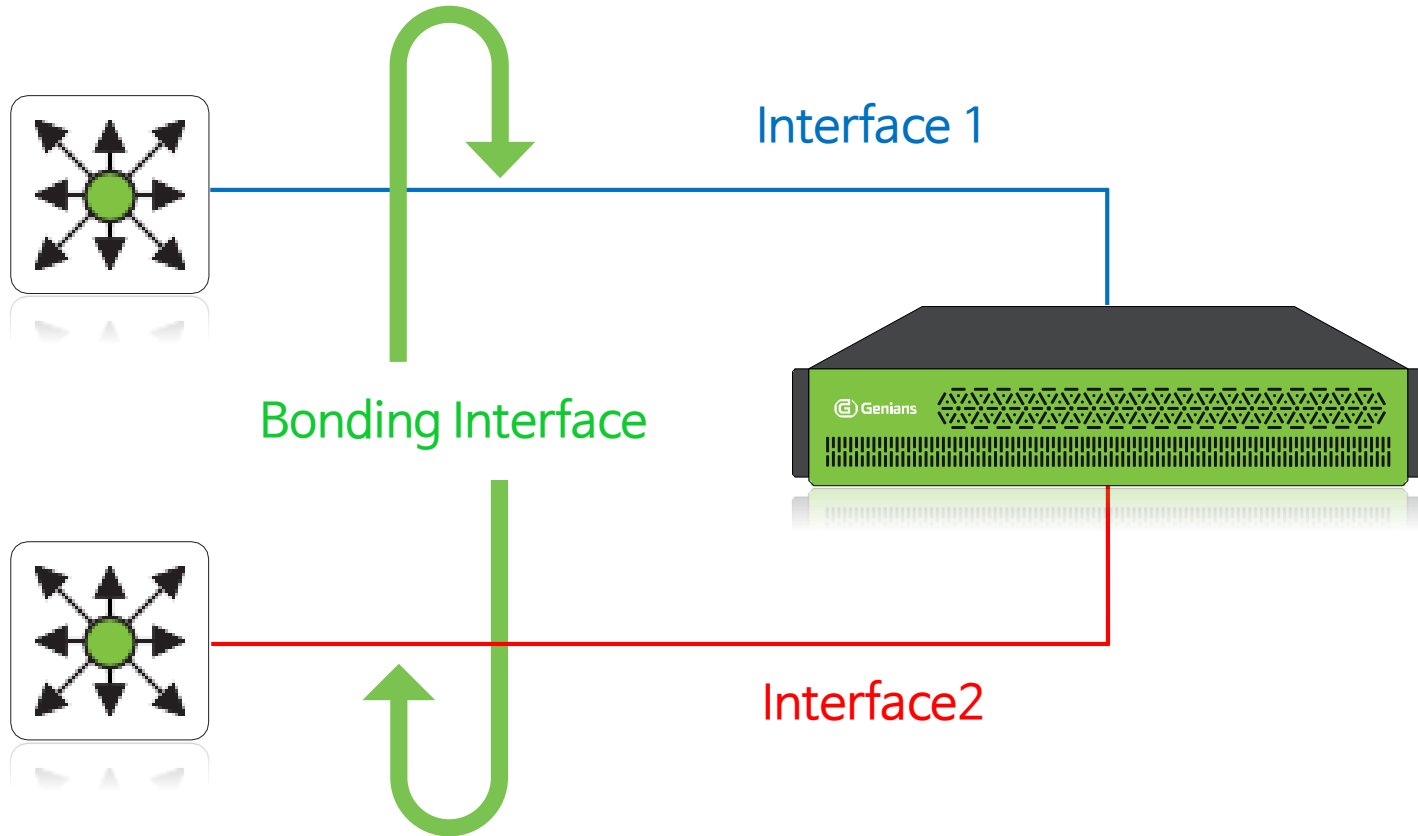
- log-server access-password 값과 log-server access-user elastic 값은 Master 서버의 값과 동일하게 변경해야 한다.

- gnlogin에서 변경 불가능

- /disk/sys/conf/local.conf 파일을 vi편집기를 사용하여 Master 서버의 값과 동일하게 변경 한다.

- /disk/data/elasticsearch 폴더, disk/data/ssdev/elasticsearch 폴더 삭제 후, 서버 재 기동

Bonding 설정 - 정책 서버



Bonding 설정

- Bonding 구성을 하는 장비의 설정 명령어 순서

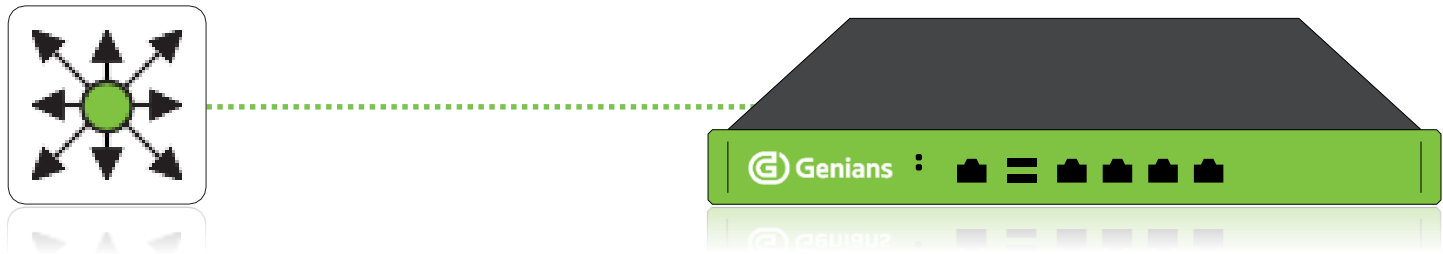
```
bonding parameters "mode=1 primary=eth0"
```

```
interface bond0 address [IP] [Subnetmask]  
interface bond0 gateway [IP]  
interface bond0 management-server enable  
interface bond0 node-server enable  
interface bond0 slave eth0,eth1
```

- primary 인터페이스 저장 이유로는 재 구동 시, 해당 인터페이스가 eth0으로 구동되고 인터페이스 Fault 시, eth1로 전환하기 위함

- Bond0으로 그룹(eth0, eth1)을 지정하여 IP, GW, Web Service enable

Single sensor 구성 설정



Single sensor 구성 설정

- 단일 네트워크 대역을 관리하는 싱글 센서 설정

```
genian(config)#debug sensord all
```

```
interface eth0 address [IP] [Subnetmask]  
interface eth0 gateway [IP]  
ip default-gateway [IP]  
ip name-server [IP]
```

```
node-server ip [IP]
```

디버그 설정

(Diskless h/w는 정책서버 sensord로 debug 전송)

(Disk h/w는 로컬디스크에 debug 저장)

인터페이스 아이피, 서브넷 마스크

인터페이스 게이트웨이

장비 기본 게이트웨이

장비 도메인네임서버

정책서버 지정

Multi sensor 구성 설정



Multi sensor 구성 설정

- 여러 VLAN 네트워크대역을 관리하는 멀티센서 설정

```
genian(config)#debug sensord all
```

```
genian(config)# interface eth0 vlan [60,86,87,135]
genian(config)# interface eth0.[135] address [IP]
[Subnetmask]
genian(config)# interface eth0.[135] gateway [IP]
genian(config)# interface eth0.[60] address [IP]
[Subnetmask]
genian(config)# interface eth0.[60] gateway [IP]
genian(config)# interface eth0.[86] address [IP]
[Subnetmask]
genian(config)# interface eth0.[86] gateway [IP]
genian(config)# interface eth0.[87] address [IP]
[Subnetmask]
genian(config)# interface eth0.[87] gateway [IP]
```

```
genian(config)# ip default-gateway [IP]
genian(config)# ip name-server [IP]
```

```
genian(config)# node-server ip [IP]
```

디버그 설정

(Diskless h/w는 정책서버 sensord로 debug 전송)
(Disk h/w는 로컬디스크에 debug 저장)

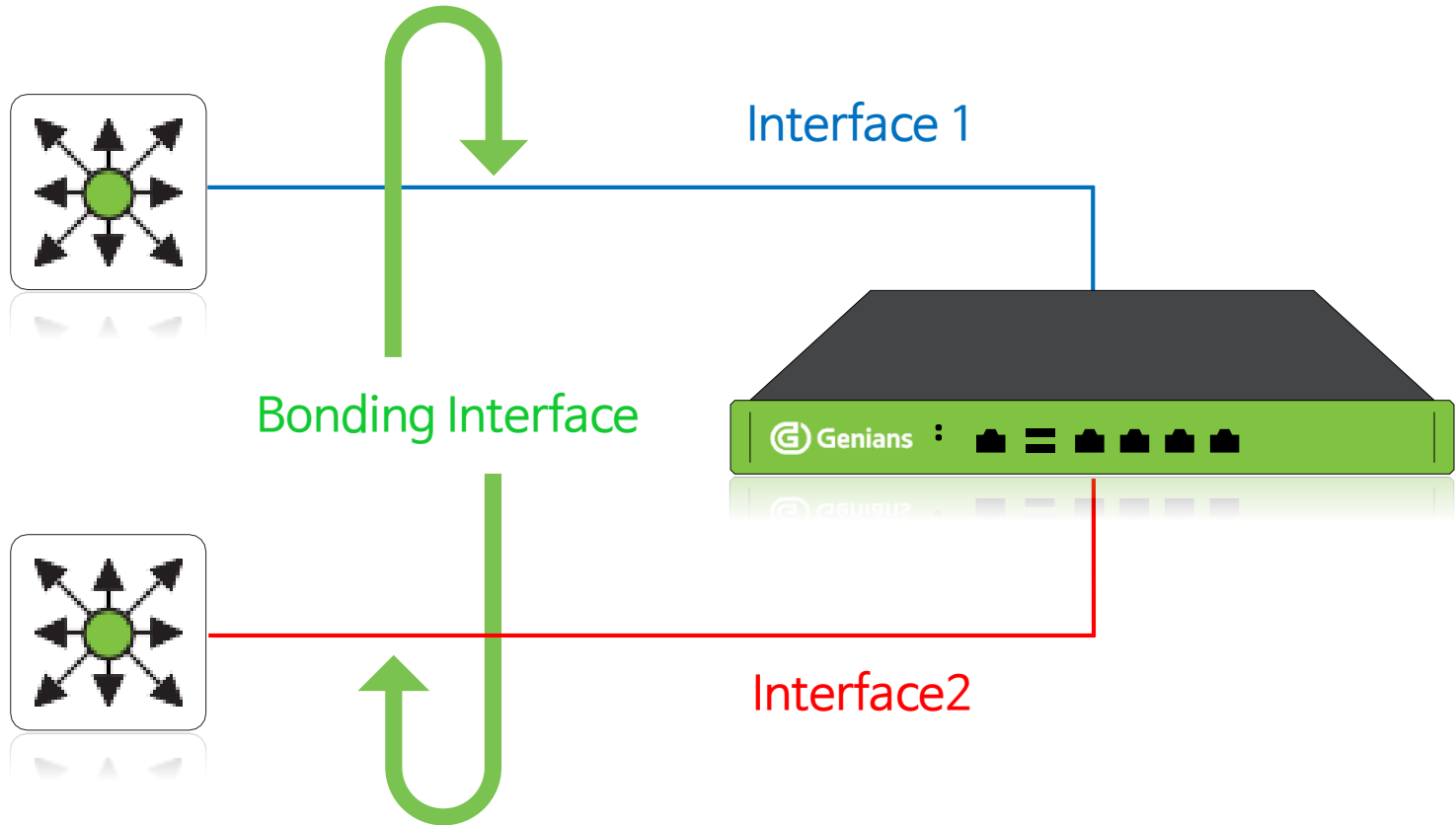
인터페이스에 VLAN 정의

VLAN 인터페이스별로 아이피, 서브넷 마스크
VLAN 인터페이스별로 게이트웨이

장비 기본 게이트웨이
장비 도메인네임서버

정책서버 지정

Bonding 설정 - 센서



Sensor Bonding 설정

- Sensor의 Bonding 구성을 하는 장비의 설정 명령어 순서

Bonding parameters “mode=1 primary=eth0”

Interface bond0 address [IP] [Subnetmask]
Interface bond0 gateway [IP]
interface bond0 slave eth0,eth1

- primary 인터페이스 저장 이유로는 재구동시 해당 인터페이스가 eth0으로 구동되고 인터페이스 Fault시 eth1로 전환하기 위함
- Bond0으로 그룹(eth0, eth1)을 지정하여 IP, GW 설정

* 범용OS 변경사항

이미지 업그레이드

- 초기 제품에 설치되어 있는 이미지의 종류를 변경하거나 상위버전으로 업그레이드 하는 방법

STEP 1 : SSH 접속

```
Username: ID  
Password: PASSWORD
```

※ geniup 명령 옵션

- h : help
- f [image filename] : 업데이트 파일 지정
- u [URL] : 업데이트파일 URL지정
- d : 다운그레이드 수행 시 옵션
- c : 이미지 종류 체크 하지 않는 옵션

STEP 2 : 이미지 업로드

```
user@genians:# sudo su  
  
root@genians:# cd /tmp  
root@genians:# rz
```

※ rz : zmodem을 통하여 PC의 파일을 현재 디렉토리로 저장

※ sz [파일명] : 지정된 파일을 zmodem을 통해 PC로 저장
(zmodem을 지원하는 터미널 프로그램을 사용)

STEP 3 : 이미지 업그레이드

```
root@genians:# geniup -f NAC-UBUNTU-R-95402-5.0.42.0628.deb
```

※ 업그레이드 명령 수행 후 물어보는 사항

Do you want to upgrade this target version? --> 해당 버전으로 업그레이드 수행할 것인지 확인

Do you want to upgrade this target version? --> DB를 백업할지 확인

Do you want to restart system after upgrade ? --> 업그레이드 후 자동 재부팅 할지 확인

* 범용OS 변경사항

이미지 업그레이드

STEP 4 : 이미지 업그레이드 확인

```
Checking Signature ..... done
Splitting image file ..... done
Checking disk space ..... done
Deleting current image ..... done
Updating kernel ..... done
Updating product ..... done
Updating checksum ..... done
Syncing ..... done
```

System software upgrade finished. You must restart system.

위 메시지가 나타나면 업그레이드가 정상적으로 수행

※ 참고사항

- 이미지 업로드 시, 완료 후 파일의 용량을 확인한다.
- 센터 장비에 **UBUNTU 이미지**만 사용 가능
- 센서 장비에 **UBUNTUNS 이미지**만 사용 가능

유지보수



* 범용OS 변경사항

SYSTEM 점검

- 제품의 시스템 점검을 위한 항목과 방법 설명
- sysinspect로 기본적인 시스템의 상태를 체크
- sysinspect의 기본 항목 설명

sysinspect.sh

```
root@genians:# cd /usr/geni/tools
root@genians:/usr/geni/tools# ./sysinspect.sh
```

=====Regualr Inspection=====

- 1) Check Server/Service infomation
- 2) Check Service status
- 3) Check Disk & Memory information
- 4) Check Smartctl
- 5) Check Slow Query
- 6) Check Total Inspection
- 9) Check Setup Config

=====

Enter Select Number :

- /usr/geni/tools 경로로 이동
- shell 모드에서 해당 경로의 sysinspect.sh 실행

sysinspect 점검 가능 항목

1) 서버 정보 출력

> Uptime, LoadAverage, platform, version, MAC, HA, OpenSSL version, mysql version, apache version, JAVA version, ElasticSearch Version, LOG,DB Backup Check

2) 서비스 상태 체크

> mysqld, java, centerd, sensor, vrrpd, apache2, procmond, sshd, syslog-ng, radius

3) 디스크, 메모리 상태 체크

> Disk, mount, 디스크사용률, 메모리 사용률, 실제 메모리 사용률

4) HDD 상태 체크

> smartctl 을 사용한 디스크 검사

5) mysql slowquery 검사

> slowquery 발생 현황

6) 1~5항목 전체 출력

※ httpd 데몬은 범용 OS에서 존재하지 않고 apache 로 대체

* 범용OS 변경사항

SYSTEM 점검

- DB 이중화 구성에서 Replication이 정상으로 동작하는지 확인하는 방법

Replication 상태 확인

```
user@genians:~$ sudo su
root@genians:/home/user# gnlogin
genian> show dataserver replicastatus
Replication health is good.
===== Primary Replication Status =====
Host           : 127.0.0.1
File           : mysqld.000002
Position       : 60027
===== Secondary Replication Status =====
Host           : 172.29.126.102
Slave_IO_Running : Yes
Slave_IO_State   : Waiting for master to send event
Slave_SQL_Running : Yes
Slave_SQL_Running_State : Slave has read all relay log; waiting
for the slave I/O thread to update it
Master_Log_File   : mysqld.000002
Read_Master_Log_Pos : 60027
Relay_Master_Log_File : mysqld.000002
Exec_Master_Log_Pos : 60027
Last_Errno       : 0
Last_Error       :
Last_IO_Errno    : 0
Last_IO_Error    :
Last_SQL_Errno   : 0
Last_SQL_Error   :
Relay_Log_File   : mysqld-relay-bin.000006
Relay_Log_Pos    : 14022
```

- Genian Shell 접근
- replication 체크 명령어 수행
- replication 상태 표시
- Primary replication 상태 표시
- Secondary replication status 상태 표시
- Slave 서버의 In/out put 동작상태 (YES가 정상)
- Slave 서버의 SQL 동작상태 (YES가 정상)

데이터베이스 백업 및 복구

* 범용OS 변경사항

- 명령어를 수행하여 데이터베이스 백업하는 방법을 설명
- Database와 감사 로그는 함께 백업되지만 저장되는 디렉토리가 다르며 백업도 별도로 수행

DB 백업

```
user@genians:~$ sudo su
root@genians:/home/user# gnlogin
genian> enable
Password:

genian# do backup all

Are you sure to backup database (y/N): y
Start backup...Finished.

genian# show backup
Backup lists
-----
ALDER-95375-20210713-140910
ALDER-95962-20210714-040000
ALDER-95962-20210714-111936
```

- Genian Shell 접근
- Privileged mode 접근
- 백업 명령 수행
- 백업 파일 확인

데이터베이스 백업 및 복구

* 범용OS 변경사항

- 백업파일의 실제 위치를 확인

백업파일 위치 확인

```
user@genians:~$ sudo su
root@genians:/home/user#

root@genians:/disk/data/DBBACKUP# ls -la

-rw-r--r-- 1 root root 397014490 Jul 13 14:09 ALDER-95375-20210713-140910.tar.gz
-rw-r--r-- 1 root root 397014730 Jul 14 04:00 ALDER-95962-20210714-040000.tar.gz
-rw-r--r-- 1 root root 397016680 Jul 14 11:19 ALDER-95962-20210714-111936.tar.gz

root@genians:/disk/data/LOGBACKUP# ls -la

-rw-r--r-- 1 elastic elastic 318 Jun 24 15:53 snap-wSTue7a0SyOn-AGAgILOGQ.dat
-rw-r--r-- 1 elastic elastic 318 Jun 17 04:00 snap-ypZI4gepSeuMW3SbQaf0xg.dat
-rw-r--r-- 1 elastic elastic 318 Jun 25 04:00 snap-zQ9Pz0eyQomjW8tsU3VIOA.dat
```

- DB 백업파일위치 : /disk/data/DBBACKUP/
- LOG 백업파일위치 : /disk/data/LOGBACKUP/

* 범용OS 변경사항

데이터베이스 백업 및 복구

- 백업파일을 이용하여 데이터베이스 복구하는 방법을 설명 (CENTER/DB/LOG 단일 구성)

DB 복구

```
user@genians:~$  
user@genians:~$ sudo su  
root@genians:/home/user# gnlogin  
genian> enable  
Password:  
  
genian#  
genian# show backup  
Backup lists  
-----  
ALDER-95962-20210714-111936  
ALDER-95962-20210714-113149  
ALDER-95962-20210714-124217  
  
genian# do restore ALDER-95962-20210714-124217  
Are you sure to restore configuration files (y/N): n  
Are you sure to restore agent files (y/N): n  
Are you sure to restore custom files (y/N): n  
Are you sure to restore database (y/N): y  
Do you want to start service after restore? (Y/n): y  
Do you want to restart system after restore? (Y/n): y  
Stopping Service...  
Restoring policy database...  
Stopping Service...done  
Shutdown System .....
```

- Genian Shell 접근
- 백업 파일 확인
- 백업 파일로 restore 수행
- CLI 설정 파일 복구 선택
:(정책서버에서 restore 수행 시, 정책 서버의 config)
- 에이전트 파일 복구 선택
- 커스텀 파일 복구 선택
- 데이터베이스 복구 선택
- 복구 후 서비스 재 구동 선택
- 복구 후 시스템 재 시작 선택

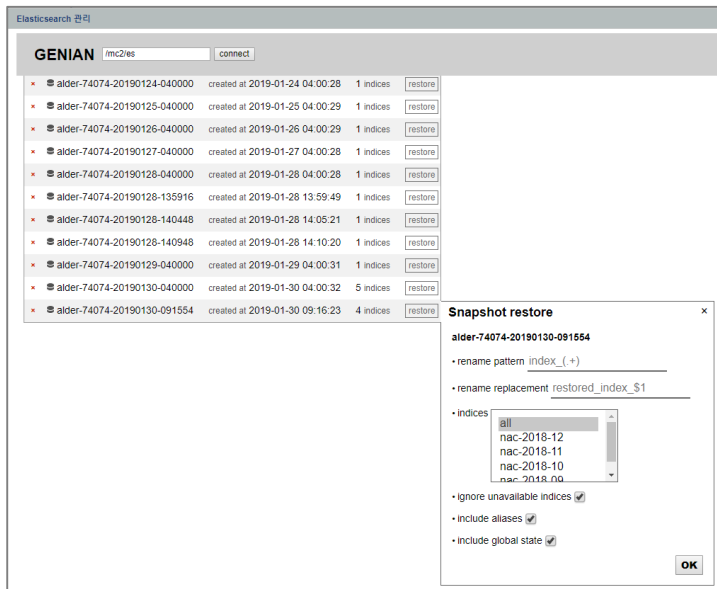
* 범용OS 변경사항

LOG 백업 및 복구

- 감사로그 복구 방법을 설명 (CENTER/DB/LOG 단일 구성)

LOG 백업

- 1) Web콘솔 접속
- 2) ADV 페이지 접속
- 3) Elasticsearch 관리
- 4) Overview tab에서 확인되는 Index 전체 Close
- 5) Snapshot tab에서 백업한 시점의 Snapshot으로 restore



- 관리UI에서 설정한 주기적 백업 시각에 자동 백업이 수행됨
- 기본적인 백업방법은 Database 백업 방법과 동일
- ‘show backup’ 명령을 수행했을 때 LOG백업 파일의 존재 유무는 확인이 되지 않으며 ADV페이지내 Elasticsearch 관리 메뉴에서 확인
- 백업한 Snapshot으로 restore 수행할 경우 기존 인덱스들의 데이터는 모두 사라지고 snapshot 기준으로 복원
- 향후 기능개선으로 Index close하는 과정을 제거될 예정

장비 초기화

* 범용OS 변경사항

- Database를 초기화 하는 방법 설명

reset-database.sh

```
user@genians:~$ sudo su
root@genians:/home/user#
root@genians:/home/user# cd /usr/geni/tools/
root@genians:/usr/geni/tools# . reset-database.sh
Are you sure to reset database (with reboot) (y/N) ? y
Please type 'database reset' for process: database reset
Shutdown System .....
```

- Genian Shell 접근
- 셸 스크립트 위치 : /usr/geni/tools/
- database reset을 정상적으로 입력했을 때 수행하는 항목
 - : /etc/init.d/alder stop
 - : rm -rf /disk/data/elasticsearch
 - : rm -rf /disk/data/mysql
 - : rm -f /disk/sys/conf/custom.sql
 - : rm -f /disk/sys/conf/customview.sql
 - : /etc/init.d/alder start
- 위와 같이 제품 데몬을 모두 중지하고 해당 디렉토리에 있는 데이터를 모두 삭제
- 완료 후 재부팅

장비 초기화

* 범용OS 변경사항

- 장비 공장 초기화 하는 방법 설명

reset-factory.sh

```
user@genians:~$ sudo su
root@genians:/home/user#
root@genians:/home/user# cd /usr/geni/tools/
root@genians:/usr/geni/tools# . reset-factory.sh
!!! WARNNIGN WARNING WARNING WARNING
WARNING WARNING !!!

ALL DATA WILL BE ERASED (DATABASE, CONFIG, BACKUP)

Are you sure to reset factory default (with reboot) (y/N) ? y
Please type 'factory reset' for process: factory reset
Shutdown System ..... plymouth-reboot.service
[ OK ] Stopped System Logger Daemon.
[ **] A stop job is running for Session 860 of user user (29s
/ 40s)
```

- Genian Shell 접근
- 셸 스크립트 위치
: /usr/geni/tools/reset-factory.sh
- Factory reset을 정상적으로 입력했을 때 수행하는 항목
: /etc/init.d/alder stop
: rm -rf /disk/sys/conf/*
: rm -rf /disk/data/*
- 위와 같이 제품 데몬을 모두 중지하고 해당 디렉토리에 있는 데이터를 모두 삭제
- 완료 후 재부팅

시간 동기화

* 범용OS 변경사항

- 장비 관리 중 시스템 시각이 맞지 않는 Center장비의 경우 수동으로 설정 하는 방법

Time sync

1. genian shell 에서 타임 서버를 지정하는 명령어

```
> genian(config)# ntp server [x.x.x.x]
```

2. 인터넷이 연결된 환경에서 내부에 time서버가 별도로 구성되어 있지 않은 경우 외부의 타임서버시간으로 장비 시간을 싱크

```
> root@genians:/# ntpdate time.bora.net  
14 Jul 13:47:19 ntpdate[10826]: adjust time server 203.248.240.140 offset -0.018528 sec
```

3. 수동으로 원하는 시각으로 변경하는 명령

```
> root@genians:/# date 031310252018  
Tue Mar 13 10:25:00 KST 2018
```

03 - 월
13 - 일
10 - 시
25 - 분
2018 - 년