NAT창선 NETWORKS  
네트워크 설계 eem, SNMP 가이드

네트워크 설계 및 사용자 설명서

# 개요

더본코리아의 나마을식당은 대규모 식당 사업을 위해 네트워크 인프라를 새롭게 구축하는 프로젝트입니다. 이 프로젝트는 네트워크 운영의 효율성과 안정성을 극대화하고, 네트워크 이벤트 처리를 자동화하기 위해 EEM (Embedded Event Manager) 기술을 활용하고 지속적인 네트워크 모니터링을 위해 SNMP (Simple Network Management Protocol) 기술을 활용할 계획입니다.

이 가이드는 해당 프로젝트에서 EEM및 SNMP을 사용하는 방법과 기대 효과에 대해 설명합니다.

## 요구사항

더본코리아/나마을식당 측에서 네트워크 설계시 요구한 요구사항에 대한 목록입니다.

* <요구 사항 1: 네트워크 장비 상태 모니터링>
* <요구 사항 2: 네트워크 장애 대응>
* <요구 사항 3: 네트워크 장비에 대한 주기적인 관리>

## 솔루션

EEM 기술을 활용해 위 3개의 요구사항에 대한 설계를 추가합니다.

* <솔루션 1: SNMP기술을 활용해 주기적인 네트워크 장비 상대에 대한 상태 모니터링>
* <솔루션 2: SNMP기술을 활용해 네트워크 장비 부하시 알림기능 >
* <솔루션 3: EEM기술을 활용해 네트워크 장비 시스템 정보를 주기적으로 백업>
* <솔루션 4: EEM기술을 활용해 네트워크 장비 장애시 자동 백업 시스템 구축
* <솔루션 5: 네트워크 장비에 관리자만 SSH를 통해 접근 가능하도록 ACL 및 ssh 설정 >

# 설계

더본코리아/나마을식당의 인프라 구축에 있어 사용된 EEM기술에 대한 적용범위 및 적용방법에 대한 기술을 명세합니다.

## EEM기술 소개

EEM의 개념 및 목적

EEM은 시스코 라우터 및 스위치에서 이벤트 기반 자동화 스크립트를 생성하고 실행하기 위한 펌웨어 기술입니다. 이 기술은 특정 이벤트가 발생할 때 자동으로 액션을 수행하도록 프로그래밍할 수 있으며, 이를 통해 네트워크 관리의 자동화와 유연성을 극대화할 수 있습니다. EEM은 네트워크 운영 효율을 높이고, 인력과 자원을 절약하는 데 큰 도움이 됩니다.

주요 기능과 기대 효과

EEM은 다양한 기능을 제공하여 네트워크 관리를 강화합니다. 이벤트 감지, 상태 변화 알림, 자동 장비 재부팅, 에러 처리 등 다양한 시나리오에서 유연하고 효과적인 대응이 가능합니다. 이로 인해 장애 대응 시간을 단축하고, 서비스 품질을 향상시키는 데에도 기여합니다. 또한, EEM은 장애 예방과 성능 최적화를 위한 자동화된 스크립트를 작성하여 안정적이고 신뢰성 있는 네트워크 운영을 도모합니다.

## SSH 기술 소개

SSH 의 개념 및 목적

SSH는 네트워크 프로토콜로 라우터, 스위치 등 원격으로 컴퓨터나 네트워크 장비에 접속하고 관리하기 위해 사용하는 보안 프로토콜입니다. SSH는 인터넷을 통해 데이터를 암호화하여 안전한 통신을 제공하고, 기밀성과 무결성을 보장합니다.

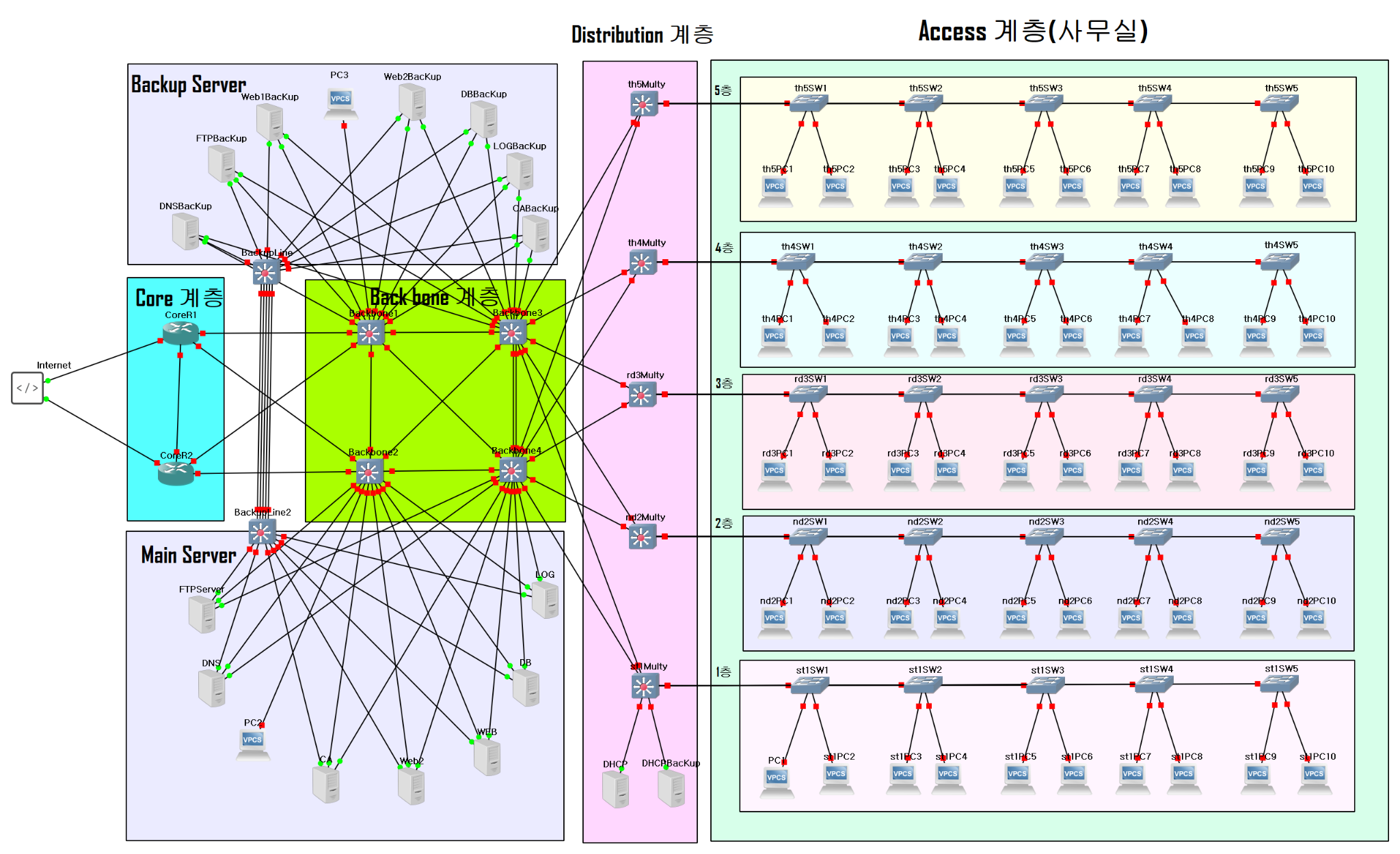
주요 기능과 기대 효과

SSH는 트래픽을 암호화하여 타인이 데이터를 엿보는 것을 방지합니다. 데이터를 암호화하여 전송하기 때문에 민감한 정보가 노출되는 것을 막습니다. SSH를 사용하면 네트워크 장비와 물리적으로 맞닿아 있지 않아도 해당 장비로 접근이 가능함으로 장비를 효율적으로 관리할 수 있습니다.

## 적용 범위

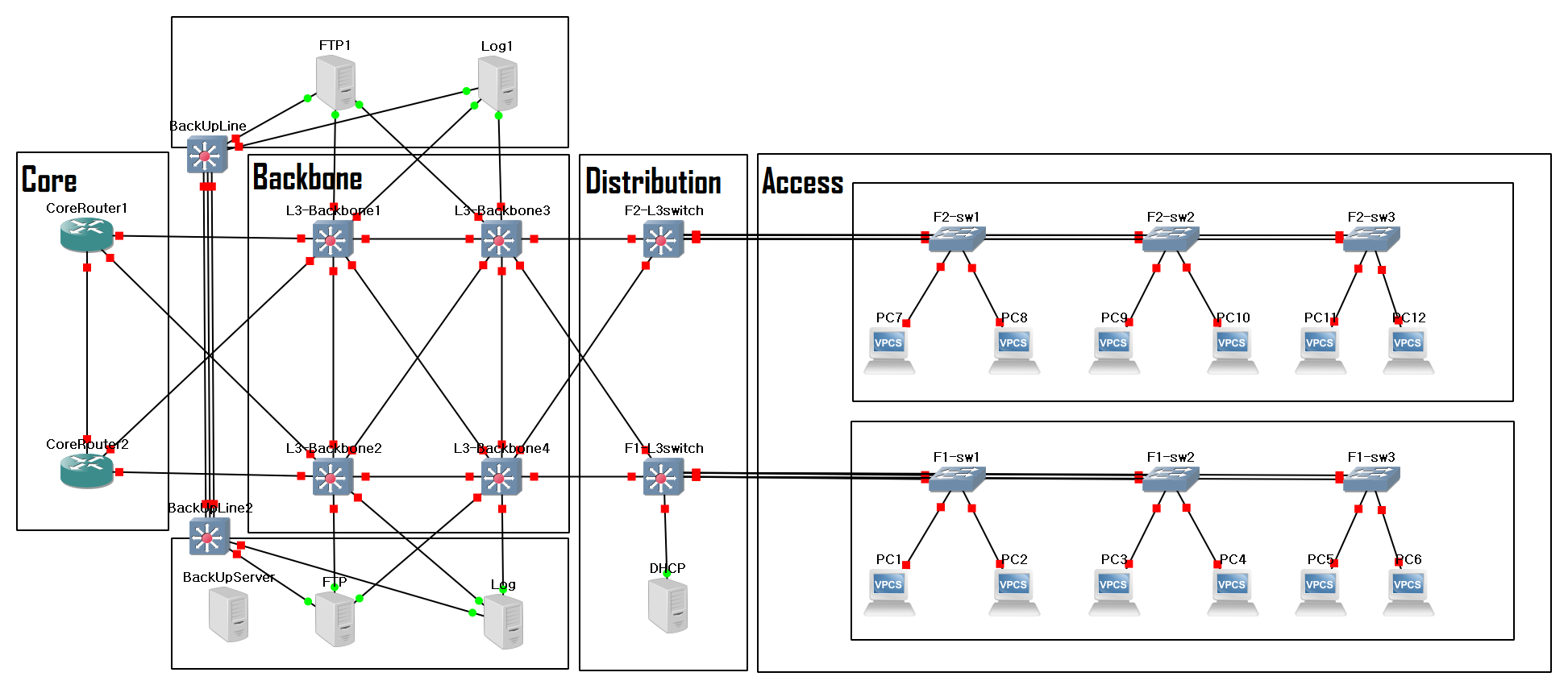
더본코리아/나마을식당의 본사, 경기지사, 서울지사에 네트워크 인프라 구축시 해당 기술이 적용된 범위에 대한 명세입니다.

* **본사**



<본사 인프라 네트워크 구성도>

* BackBone 계층의 Router 4개
  + 적용 솔루션
    - 솔루션 1 ,2: 서버실 관리자 PC로 전송
    - 솔루션 3, 4 : FTP server에 상태파일 전송
    - 솔루션 5 : SSH 를 통해 접근이 가능, ACL 을 통해 ser제한
* Core 계층의 Router 2개
  + 적용 솔루션
    - 솔루션 1 ,2: 서버실 관리자 PC로 전송
    - 솔루션 3, 4 : FTP server에 상태파일 전송
    - 솔루션 5 : SSH 를 통해 접근이 가능, ACL 을 통해 ser제한
* Disrtibution 계층의 Router 5 개
  + 적용 솔루션
    - 솔루션 1 ,2: 서버실 관리자 PC로 전송
    - 솔루션 3, 4 : FTP server에 상태파일 전송
    - 솔루션 5 : SSH 를 통해 접근이 가능, ACL 을 통해 ser제한
* **경기지사 & 서울지사**



<경기지사 & 서울지사 인프라 네트워크 구성도>

* BackBone 계층의 Router 4개
  + 적용 솔루션
    - 솔루션 1 ,2: 서버실 관리자 PC로 전송
    - 솔루션 3, 4 : FTP server에 상태파일 전송
    - 솔루션 5 : SSH 를 통해 접근이 가능, ACL 을 통해 ser제한
* Core 계층의 Router 2개
  + 적용 솔루션
    - 솔루션 1 ,2: 서버실 관리자 PC로 전송
    - 솔루션 3, 4 : FTP server에 상태파일 전송
    - 솔루션 5 : SSH 를 통해 접근이 가능, ACL 을 통해 ser제한
* Disrtibution 계층의 Router 2 개
  + 적용 솔루션
    - 솔루션 1 ,2: 서버실 관리자 PC로 전송
    - 솔루션 3, 4 : FTP server에 상태파일 전송
    - 솔루션 5 : SSH 를 통해 접근이 가능, ACL 을 통해 ser제한

## 기술 설계

각 솔루션에 해당하는 실제 설계에 명세합니다.

* 솔루션 0 : SNMP , SNMP TRAP SERVER 설치

## 서버 설정

|  |
| --- |
| sudo apt-get install snmpd snmptrapd  sudo vi /etc/snmp/snmpd.conf  agentaddress udp:161,udp6:161  rocommunity [커뮤니티이름] [에이전트 ip] -V systemonly  sudo vi /etc/snmp/snmptrapd.conf  authCommunity log,execute,net public  authCommunity log,execute,net [에이전트 ip] [커뮤니티이름] |

* 네트워크 장비의 모니터링을 위해SNMP 및 SNMP-trap을 관리자 PC에 설치해 사용
* sudo vi /etc/snmp/snmpd.conf 는 일반적 SNMP 설정을 위한 파일입니다.
  + **agentaddress udp:161,udp6:16**  
    해당 PC에 161번 포트로 접속을 대기
  + rocommunity [커뮤니티이름] [에이전트 ip] -V systemonly  
    **rocommunity** : Read-Only 커뮤니티 설정  
    **[커뮤니티이름]:** 사용자가 정의하는 커뮤니티 이름을 입력합니다. SNMP 에이전트로부터 해당 커뮤니티 이름으로 전송되는 요청을 수락합니다.  
    **[에이전트 ip]:** 해당 커뮤니티 이름이 허용되는 SNMP 에이전트의 IP 주소를 지정합니다. 이 주소로부터 오는 요청을 수락합니다.
* sudo vi /etc/snmp/snmptrapd.conf 는 일반적 SNMP-trap 설정을 위한 파일입니다
* **authCommunity log,execute,net [에이전트 ip] [커뮤니티이름]**
  + **authCommunity**   
    옵션은 해당 커뮤니티로 들어오는 SNMP 요청에 대해 권한을 부여하고 로깅 설정을 지정
  + **log**   
    해당 커뮤니티로 들어오는 요청을 로깅합니다.
  + **Execute**  
    해당 커뮤니티로 들어오는 요청을 실행합니다.
  + **net**  
    해당 커뮤니티로 들어오는 요청에 대해 네트워크 접근을 허용합니다.
  + **[에이전트 ip]**  
    SNMP 요청을 수신하는 에이전트(네트워크 장치 또는 서버)의 IP 주소를 지정합니다.
  + **[커뮤니티이름]**  
    SNMP 커뮤니티 이름을 지정합니다. 이 커뮤니티 이름은 SNMP 요청을 수신하는데 사용됩니다.

SNMP-trap 확인 : **sudo smptrapd -m -all -Le -f -d**

* 장비정보 받기(서버측 명령어)  
  **snmpwalk -v2c -c [커뮤니티이름] [IP] [option : oid]**  
  해당 IP장비에 해당 커뮤니티로 장비 정보로 요청해 받음

## 장비 설정

|  |
| --- |
| [SNMP Manager 설정]  enable  configure terminal  snmp-server community [커뮤니티이름] RO  snmp-server enable traps  snmp-server trap-source [인터페이스]  [SNMP Trap 설정]  snmp-server host [SNMP-SERVER] version 2c [커뮤니티이름] |

* SNMP 사용을 위해 네트워크 장비 설절을 추가합니다.
* 솔루션 1 : SNMP기술을 활용해 주기적인 네트워크 장비 상대에 대한 상태 모니터링

|  |
| --- |
| event manager applet Router\_Check  event timer watchdog time 60  action 0.01 info type routername  action 2.0 cli command "sh processes cpu"  action 3.0 snmp-trap strdata "$\_info\_routername : $\_cli\_result" |

* 60초 주기로 해당 네트워크 장비의 CPU상태를 SNMP-trap으로 전송합니다

.

* 솔루션 2: EEM기술을 활용해 네트워크 장비 부하시 알림기능
  + 장비 OID 참조 : <https://oidref.com/1.3.6.1.4.1.9.9.109.1.1.1.1>

## 메일서버가 있는 경우 해당 정보를 메일로 전송

|  |
| --- |
| event manager applet CPU\_Utilization\_mail  event snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.3.1 get-type exact entry-op gt entry-val 60 exit-op lt exit-val 60 poll-interval 15  action 0.01 info type routername  action 1.0 cli command "enable"  action 2.0 cli command "sh processes cpu"  action 3.0 syslog msg "The CPU applet has ran (CPU is at $\_cli\_result %)"  action 4.0 mail server "x.x.x.x" to "xxx@xxx.com" from "xxxx@xxx.com" subject "$\_info\_routername$\_CPU\_Utilization" body "$\_cli\_result" |

* Network에 Mail server가 존재할 경우 해당 네트워크 장비의 CPU사용량이 60을 넘어갈 경우 해당 정보를 메일로 전송합니디.

## 메일서버가 없는 경우 해당 정보를 SNMP로 전송

|  |
| --- |
| event manager applet CPU\_Utilization\_snmp  event snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.3.1 get-type exact entry-op gt entry-val 60 exit-op lt exit-val 60 poll-interval 15  action 0.01 info type routername  action 4.0 snmp-trap strdata "$\_info\_routername Check CPU The CPU applet has ran (CPU is at $\_snmp\_oid\_val %)" |

* 해당 네트워크 장비의 CPU사용량이 60을 넘어갈 경우 해당 정보를 SNMP-trar을 관리자에게 전송합니디.
* 솔루션 3: EEM기술을 활용해 네트워크 장비 시스템 정보를 주기적으로 백업

|  |
| --- |
| event manager applet Router\_Backup  event timer cron cron-entry "0 18 \* \* \*"  action 0.01 info type routername  action 1.01 cli command "enable"  action 1.02 cli command "show clock"  action 1.03 regexp "(2[0-3]|[01][0-9]):([0-6][0-9]):([0-6][0-9])" "$\_cli\_result" time hour minute second  action 1.04 puts "$time"  action 1.05 puts "$hour"  action 1.06 puts "$minute"  action 1.07 puts "$second"  action 1.11 cli command "show clock"  action 1.12 regexp "(Jan|Feb|Mar|Apr|May|Jun|Jul|Aug|Sep|Oct|Nov|Dec) ([1-9]|0[1-9]|[1-2][0-9]|3[0-1]) (20[1-9][0-9])" "$\_cli\_result" time2 month day year  action 1.13 puts "$time2"  action 1.14 puts "$month"  action 1.15 puts "$day"  action 1.16 puts "$year"  action 1.17 puts "$\_info\_routername-$year$month$day-$hour$minute$second"  action 2.01 cli command "configure terminal"  action 2.02 cli command "file prompt quiet"  action 2.03 cli command "do copy run ftp://server:admin@10.0.0.10/$\_info\_routername-$year$month$day-$hour$minute$second.config"  action 3.0 syslog msg "FTP backup successful" |

* 매일 18시에 해당 네트워크 장비의 설정파일을 백업서버에 저장합니다.  
  (라우터 버전 15이상에서 사용)
* FTP서버에 “장치이름-년월일-시분초.config” 으로 저장됩니다.

1. Version 12

|  |
| --- |
| event manager applet Router\_Backup  event timer cron cron-entry "0 18 \* \* \*"  action 0.01 info type routername  action 1.01 cli command "enable"  action 2.01 cli command "configure terminal"  action 2.02 cli command "file prompt quiet"  action 2.03 cli command "do copy run ftp://server:admin@10.0.0.10/$\_info\_routername.config"  action 3.0 syslog msg " FTP backup successful" |

* 매일 18시에 해당 네트워크 장비의 설정파일을 백업서버에 저장합니다.  
  (라우터 버전 14이하에서 사용)
* FTP서버에 “장치이름.config” 으로 저장됩니다.
* 솔루션 4: EEM기술을 활용해 네트워크 장비 장애시 자동 백업 시스템 구축

1. Version 15

|  |
| --- |
| event manager applet Router\_Error\_Backup\_InterfaceName  event syslog pattern "%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down"  action 0.01 info type routername  action 1.01 cli command "enable"  action 1.02 cli command "show clock"  action 1.03 regexp "(2[0-3]|[01][0-9]):([0-6][0-9]):([0-6][0-9])" "$\_cli\_result" time hour minute second  action 1.04 puts "$time"  action 1.05 puts "$hour"  action 1.06 puts "$minute"  action 1.07 puts "$second"  action 1.11 cli command "show clock"  action 1.12 regexp "(Jan|Feb|Mar|Apr|May|Jun|Jul|Aug|Sep|Oct|Nov|Dec) ([1-9]|0[1-9]|[1-2][0-9]|3[0-1]) (20[1-9][0-9])" "$\_cli\_result" time2 month day year  action 1.13 puts "$time2"  action 1.14 puts "$month"  action 1.15 puts "$day"  action 1.16 puts "$year"  action 1.17 puts "$\_info\_routername-$year$month$day-$hour$minute$second"  action 2.01 cli command "configure terminal"  action 2.02 cli command "file prompt quiet"  action 2.03 cli command "do copy run ftp://server:admin@10.0.0.10/$\_info\_routername-$year$month$day-$hour$minute$second-error-backup.config"  action 3.0 syslog msg " Interface Error FTP backup successful" |

* 해당 장비에 인터페이스 장애가 발생시 해당 장치의 설정파일을 백업하는 기능을 수행합니다. (라우터 버전 15이상에서 사용)
* FTP서버에 “장치이름-년월일-시분초.config” 으로 저장됩니다.

1. Version 12

|  |
| --- |
| event manager applet Router\_Error\_Backup\_InterfaceName  event syslog pattern "%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down"  action 0.01 info type routername  action 1.01 cli command "enable"  action 2.01 cli command "configure terminal"  action 2.02 cli command "file prompt quiet"  action 2.03 cli command "do copy run ftp://server:admin@10.0.0.10/$\_info\_routername.config"  action 3.0 syslog msg " Interface Error FTP backup successful" |

* 해당 장비에 인터페이스 장애가 발생시 해당 장치의 설정파일을 백업하는 기능을 수행합니다. (라우터 버전 14이하에서 사용)
* FTP서버에 “장치이름.config” 으로 저장됩니다.
* 솔루션 5 : 네트워크 장비에 관리자만 SSH를 통해 접근 가능하도록 ACL 및 ssh 설정

1. SSH 설정

|  |
| --- |
| ip domain-name coreR1.com  crypto key generate rsa 1024  username coreR1 secret coreR1  line vty 0 4  login local  transport input ssh  ip ssh version 2  ip ssh time-out 120  ip ssh authentication-retries 5 |

* Ip domain-name : 라우터의 도메인 이름을 생성합니다. 생성한 도메인 이름을 활용하여 SSH key를 생성합니다.
* crypto key generate rsa 1024 : SSH 통신에 사용되는 암호화 키를 1024비트로 생성합니다.
* username coreR1 secret coreR1 : Username과 암호화된 패스워드를 설정합니다.(md-5)
* line vty 0 4 : 0~4까지의 범위의 VTY라인을 설정합니다(최대 5개를 연속적으로 연결 가능합니다.)
* login local : 로컬에서 생성한 user를 사용하여 로그인합니다.
* Transport input ssh : Telnet등을 제외한 SSH를 통한 접근만 허용합니다.
* Ip ssh version2 : SSH버전 2를 사용하도록 설정합니다.(보안성이 version 1보다 높습니다)
* Ip ssh time-out : 특정 초 동안 세션의 응답이 없면 자동으로 종료합니다.
* Ip ssh authentication-retries 5 : SSH의 인증 횟수를 최대 5번으로 지정합니다. 해당 login 횟수를 초과하면 세션이 종료됩니다.

1. 관리자만 SSH를 통해 접근이 가능하도록 ACL설정

|  |
| --- |
| access-list 10 permit 172.20.1.10 0.0.0.0  access-list 10 permit 172.20.2.10 0.0.0.0  access-list 10 deny any  line vty 0 4  access-class 10 in |

* Access-list 10 permit : 새 Access-list를 생성하여 관리용 IP대역대(메인, 보조 서버실)를 허용한다.
* access-class 10 in: 생성한 Access-list를 vty 0 4에 적용시킨다(ssh로 접속을 할 때에만 해당 Access-list를 lookup한다)

# 결과

위 솔루션을 적용한 네트워크의 테스트 결과에 대한 내용입니다.

## 솔루션 1

|  |  |
| --- | --- |
| **SNMP 모니터링** | |
|  | |
| **설명** | 네트워크 관지자가 네트워크 장비에 대한 상태를 위한시 다음과 같은 형식을 Snmp reuest를 헤당 장비에 보내면 장비는 해당 번호에 해당하는 정보를 응답하게 된다. |

## 솔루션 2

|  |  |
| --- | --- |
| **SNMP Trap** | |
|  | |
| **설명** | 네트워크 장비에 설정된 EEM을 통해서 네트워크 장비의 CPU가 측정 임계치를 넘어갈 경우 사용자가 설정한 내용을 네트워크 관리자에게 전송합니다.  해당 테스트 시나리오는 CPU 5%일 경우 네크워크 장비 명과 현재 CPU정보를 전송합니다. |

## 솔루션 3

|  |  |
| --- | --- |
| **시스템 정보 주기적 백업** | |
|  | |
| **설명** | 정기적 스케줄링 EEM 작성  설정한 네트워크 장비에서 특정 시간이 지나면 현재 기기가 가지고있는 Running-config 파일을 FTP Server로 전송합니다. FTP Server의 IP를 domain으로 설정하여 특정 서버에 장애가 발생할 시 다른 서버를 사용할 수 있도록 설정할 수 있습니다.  다음 명령어는 매일 18시에 Cron작업을 실행하여 라우터의 이름을 읽어 온 후, enable명령어를 실행하여 관리자 모드로 접속합니다. 전역설정 모드로 진입, 파일 복사를 진행할 시 부가적인 기능을 묻는 프롬프트를 무시하도록 설정합니다. 현재 running-config파일을 저장하고 본사 FTP 서비인 hq.restaurant.com에 네트워크를 자동으로 전송하도록 설정하였습니다. |
| **결과 (1)** |  |
| **설명** | 사전에 정의된 FTP(Router Config)저장 폴더에서, 각 파일들이 정상적으로 저장되어 있는 것을 확인하였습니다. 이를 통해, 네트워크 장비별 Running-config 파일의 안정적인 저장이 이루어지고 있음을 확인할 수 있습니다. |

## 솔루션 4

|  |  |
| --- | --- |
| **장애 발생 시 시스템 정보 주기적 백업** | |
|  | |
| **설명** | 인터페이스 장애 스케줄링 EEM 작성  주기적인 스케줄 이외에도 특정 상황에서 발생하는 이벤트 또한 이벤트를 설정할 수 있습니다.  다음 명령어는 특정 Interface에 장애가 발생 시 라우터의 이름을 읽어 온 후,, enable명령어를 실행하여 관리자 모드로 접속합니다. 전역설정 모드로 진입, 파일 복사를 진행할 시 부가적인 기능을 묻는 프롬프트를 무시하도록 설정합니다. 현재 running-config파일을 본사 FTP 서비인 hq.restaurant.com에 네트워크를 자동으로 전송하도록 설정하였습니다. |
| **결과 (1)** |  |
| **설명** | 사전에 정의된 FTP(Router Config)저장 폴더에서, 각 파일들이 정상적으로 저장되어 있는 것을 확인하였습니다. 이를 통해, 네트워크 장비별 Running-config 파일의 안정적인 저장이 이루어지고 있음을 확인할 수 있습니다. |

## 솔루션 5

|  |  |
| --- | --- |
| **관리자 SSSH 접근** | |
|  | |
| **설명** | Access-list(ACL)를 사용하여 특정 IP에 대한 접근을 차단, 허용할 수 있습니다.  해당 명령어는 관리용 PC가 존재하는 172.20.1.0/24, 172.20.2.0/24의 네트워크 대역만 SSH접속을 허용하는 Access-list 로 그 밖에 interface, nat 등 다양한 분야에 ACL을 사용할 수 있습니다.  Access-list 0~99, 1300~1999 까지는 출발지의 IP만 필더가 가능한 Standard, 100~199, 2000~2699까지는 출발지와 목적지, 프로토콜, 포트별로 필터가 가능한Extended 모드로 사용할 수 있습니다. |
|  | |
| **설명** | 관리용 네트워크 대역이 아닌 CoreR1에서 Backbone3로 ssh접속 시 Deny되는걸 확인할 수 있습니다. |
|  | |
| **설명** | 간혹 Server에서 Router 및 Switch에 접속할 때 다음곽 타은 에러가 발생할 수 있습니다. 이는 ssh의 키 매칭방식의 오류가 발생했기 떄문입니다.  ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -c aes128-cbc 명령어를 통해 키 교환방식을 맞춰주면 정상적으로 접근이 가능합니다. |

감사합니다