

Search A : Quick Start 가이드



㈜에이원네트웍스

서울특별시 구로구 구로동 디지털로 32길 30, 코오롱디지털타워빌란드 1차 1003호 Tel: 02-853-8700 | Email: sale@nidc.kr Customer Support: 1544-6191 www.SearchA.kr

Copyright © 2017 AONE NETWORKS INC. All Rights Reserved.



목차

| I. 모니터링 동작 프로세스 개요 | 3 |
|------------------------------------|---|
| II. 사전 준비사항 | 3 |
| 1. 방화벽 허용정책 설정하기 | 3 |
| 1) 방화벽에서 허용정책 설정하기 | 3 |
| 2) Windows 에서 방화벽 허용정책 설정하기 | 3 |
| 3) Linux 에서 방화벽(iptable) 허용정책 설정하기 | 4 |
| 2. SNMP 설치하기 | 5 |
| 1) Windows 에서 SNMP 설치하기 | 5 |
| 2) Linux 에서 SNMP 설치하기 | 5 |
| 3. SNMP 설정하기 | 6 |
| 1) Windows 에서 SNMP 설정하기 | 6 |
| 2) Linux 에서 SNMP 설정하기 | 7 |
| III. 모니터링 등록하기 | 8 |
| 1. 웹모니터링(웹페이지) 등록하기 | 8 |
| 2. 웹모니터링(도메인) 등록하기 | 8 |
| 3. 서버 모니터링 등록하기 | 9 |
| 4. 네트워크 모니터링 등록하기 | 9 |



I. 모니터링 동작 프로세스 개요

Search A는 에이전트 프로그램의 설치 없이 손쉬운 회원가입(www.searcha.kr) 및 등록으로 웹, 서버, 네트워크에 대해 통합 모니터링을 제공하는 클라우드 기반의 가입형 모니터링 서비스입 니다.



II. 사전 준비사항

1. 방화벽 허용정책 설정하기

방화벽 또는 Windows/Linux의 자체 OS 방화벽을 운영중인 사용자의 경우, 사전에 모니터링 서버 에 대한 허용정책을 생성해야 합니다.

1) 방화벽에서 허용정책 설정하기

| ▼ 발신지 | ▼ 목적지 | ▼ 스케쥴 | ▼ 서비스 |
|------------------|--------------------|----------|------------------|
| 12.122.42.157 | • <u>ali</u> | always 💡 | ICMP_ANY SNMP |
| • 발신지(출발지): 2 | 222.122.42.157 | | |
| • 수신지(목적지): | 모니터링 대상서버 | | |
| ┃ • 서비스: ICMP(AN | IY), SNMP(UDP 161) | | |

2) Windows에서 방화벽 허용정책 설정하기

『제어판 > 관리도구 > 고급보안이 포함된 Windows 방화벽』을 클릭하여 허용정책을 생성합니다.

발신지(출발지): 222.122.42.157
수신지(목적지): 모니터링 대상서버
서비스: ICMP(ANY), SNMP(UDP 161)



🎡 Windows 방화벽 설정 × 일반 예외 고급 | Windows 방화벽을 통한 프로그램의 통신 방법을 제어합니다. 방화벽을 통한 통신을 허용할 예외 프로그램 또는 포트를 추가하십시오. Windows 방화벽에서 현재 공용 네트워크 위치에 대한 설정을 사용하고 있습니다. 프로그램 차단 해제의 위험 요소 예외를 허용하려면 해당 확인란을 선택하십시오(T), 프로그램 또는 포트 □ BITS 피어 캐싱 □ COM+ 네트워크 액세스 DTC(Distributed Transaction Coordinator) □ iSCSI 서비스 □Netlogon 서비스 SNMP Service SNMP Trap SSTP(Secure Socket Tunneling Protocol) \mathbb{R} □ Windows 방화벽 원격 관리 □ Windows 보안 구성 마법사 □ Windows 원격 관리 WMI(Windows Management Instrumentation) • 프로그램 추가(R)... 포트 추가(O)... 속성(1) □ Windows 방화벽이 새 프로그램을 차단할 때 알림(B) 적용(A) 확인 취소



3) Linux에서 방화벽(iptable) 허용정책 설정하기

Linux 서버의 iptable 방화벽을 사용하고 있는 경우, 아래 SNMP 포트의 접근허용정책을 설정합니다.

```
# iptables -I INPUT -p udp -m udp --dport 161 -j ACCEPT
# iptables -I INPUT -p udp -m udp --dport 162 -j ACCEPT
# iptables-save > /etc/sysconfig/iptables
```



2. SNMP 설치하기

1) Windows에서 SNMP 설치하기

『제어판 > 관리도구 > 서버관리자』에서 기능 추가를 통해 SNMP 서비스를 설치합니다.



2) Linux에서 SNMP 설치하기

아래 설치 명령어를 통해 SNMP를 설치합니다.

yum install net-snmp -y

| CLOOCEUDIO_DGCKUP 1# |
|---|
| [root@holo_backup ~]• |
| [root@holo_backup ~]• |
| [root@holo_backup "] |
| [root@holo_backup ~]• |
| [root@holo_backup "] |
| [root@holo_backup "]• yum -y install net-snmp* |
| Setting up Install Process |
| Setting up repositories |
| update 100% =================================== |
| base 100% =================================== |
| addons 100% =================================== |
| extras 100% =================================== |
| Reading repository metadata in from local files |
| Parsing package install arguments |
| Resolving Dependencies |
| > Populating transaction set with selected packages. Please wait. |
| > Downloading header for net-snmp-utils to pack into transaction set. |



3. SNMP 설정하기

1) Windows에서 SNMP 설정하기

『제어판 > 관리도구 > 서비스 > SNMP Service > 속성 > 보안』탭에서 읽기전용 선택 후,

아래와 같이 임의의 커뮤니티 이름 및 호스트(222.122.42.157)를 추가한다.

| Q, 서비스 | | | | | | | |
|---|--|--|---|--|---|---|-------------|
| 파일(F) 동작(A) | 보기(V) 도움말(H) | | | | | | |
| (+ +) III | a 📑 🔽 📷 👂 🗰 11 10 | | | | | | |
| 🖓 서비스(로컬) | Q, 시비스(로컬) SNMP Service | 이름수 | | 설명 | 상태 | 시작 유형 | 다음 사용자로 로그온 |
| SNMP Service 1 서비스 즐지 서비스 <u>다시 시작</u> 실명: 이 컴퓨터에서 SNMP(Simple Network Management Protocol) 요 청을 처리할 수 있도록 합니다. 이 서 비스를 장지하면 이 컴퓨터에서 SNMP 요청을 처리할 수 없습니다. 이 서비스를 사용하지 않도록 설정하 면 관련된 모든 서비스는 사용할 수 없습니다. | Remote Pr Remote Pr Remote Pr Resultant Routing ar Secondary Secure Sc Secure Sc Secur | rocedu rocedu egistry Set of d Re y Logon icket T kccoun ware ficatio d Rem | 불점 RPC 요청 로컬 대체 VPN 이 지동 소프 검퓨 | 시작될 시작될 시작될 시작될 시작될 시작될 | 자수동동 안 할 한 사동동동동 안 할 한 사자 수동동동동동동동동동동동동동동동동동동동동동동동동동동동동동동 | Network Service Network Service Local Service Local System Local System Local System Local Service Local System Local System Local System Local Service Local Service Local Service | |
| | SNMP Software Software Software Special SSDP D Superfet System Task Sc C TCP/IP | 사작(S) 중지(O) 일사 중 계속(M 다시 사 모든 작 새로 고려 속성(B | 지(U) 작(E) 업(K) · 철(F) ; | 시작됨 시작됨 시작됨 시작됨 시작팀 | 자동 수동 자동 안함 함 사용 안함 사용 안함 자동 자동 자동 주동 | Local System Local Service Network Service Local System Local System Local System Local System Local System Local Service Network Service | |
| | 확장/표준/ | and an and a | CROW | H) | 1 | 0.0 | |
| 현재 선택 내용에 대형 | 한 속성 대화 상자를 엽니다. | | 工品 5() | | | | 📎 A 漌 😡 |

| SNMP Service 속성(로컬 컴퓨터) | × |
|--|-------|
| 일반 로그온 복구 에이전트 트랩 보안 중속성 | |
| ☞ 인증 트럼 보내기(U) | |
| 받아들인 커뮤니티 이름(N) | |
| public 밝기 전용 | |
| 1 추가(D) 편집(E) 제거(R) | |
| ○ 모든 호스트로부터 SNMP 패킷 받아들이기(C) ○ 다음 호스트로부터 SNMP 패킷 받아들이기(T) | |
| localhost | |
| (2) 추가 편집(I) 제거(M) | |
| SNMP에 대해 자세히 알아봅니다. | |
| 확인 취소 | 적용(A) |



2) Linux에서 SNMP 설정하기

net-snmp가 설치되어 있을 경우, snmpd.conf 파일의 편집을 통해 허용정책을 설정합니다.

/etc/snmp/snmpd.conf

snmpd.conf 파일을 편집하여 SNMP 커뮤니티 이름, 서버 IP, SNMP 버전 등을 추가합니다.

| <pre># Here is a commented out example configuration that allows less # restrictive access.</pre> | | | |
|---|--|--|--|
| # YOU SHOULD CHANGE THE "COMMUNITY" TOKEN BEL # KNOWN AT YOUR SITE, YOU "MUST" CHNAGE THE NE # SOME THING REFLECTIVE YOUR LOCAL NETWORK ADD | OW TO A NEW KEYWOD ONLY TWORK TOKEN BELOW TO RESS SPACE, | | |
| ## sec.nme source commu | nity | | |
| #com2sec local localhost COMMU | NITY | | |
| #com2sec mynetwork NETWORK/24 COMMU | NITY | | |
| com2sec network_1 222, 122, 42, 157 search | ha> (1) 허용 호스트 및 커뮤니티 생성 | | |
| ## group.name sec.model sec.name | | | |
| #group NykWGroup any local | | | |
| +group wykUGroup any mynetwork | | | |
| group MyROCroup 1 v1 petwork 1 | | | |
| group MyROGroup 1 v2c network 1 | > (2) 접근 그룹 및 버전 생성 | | |
| group symbologp_r voc metsors_r | | | |
| # | | | |
| #group MyRWGroup any otherv3user | | | |
| # | | | |
| | | | |
| ## incl/excl subtree m | ask | | |
| #view all included ,1 8 | 0 | | |
| view all-mibs included .1 8 | 0> (3) 접근 MIB 생성 | | |
| | | | |
| ## -or just the mib2 tree- | | | |
| # · · · · · · · · · · · · · · · · · · · | | | |
| #view mib2 included .iso.org.dod.internet.m | gmt.miD-2 IC | | |
| II context sec model coc l | evel prefix read write potif | | |
| faccess MyROGroup "" any noa | uth 0 all none none | | |
| #access MyROGroup "" any noa | uth 0 all all all | | |
| any noa | | | |
| access MyROGroup_1 "" v1 noa | uth exact all-mibs none none | | |
| access MyROGroup_2 "" v2c noar | uth exact all-mibs none none | | |
| | > (4) 접근권한 설정 | | |

SNMP 시작, 중지 및 재시작 명령은 아래와 같습니다.

| /etc/rc.d/init.d/snmpd start | (시작) |
|--------------------------------|-------|
| /etc/rc.d/init.d/snmpd stop | (중지) |
| /etc/rc.d/init.d/snmpd restart | (재시작) |



III. 모니터링 등록하기

1. 웹모니터링(웹페이지) 등록하기

Search A 로그인 > 모니터링 설정 > 웹모니터링(웹페이지) > 등록

| 🔅 웹모니터링 웹페이기 | 시 - 등록하기 | |
|--|---|----------------------------|
| 사이트명 | ex) 써치에이 ☞ 웹사이트 명칭 지정 | |
| 위변조 체크 페이지 | ex) www.searcha.kr | ⊘ 위변조 여부를 체크할 웹사이트의 URL 기입 |
| 모니터링 페이지 문자열 | ex) SearchA | |
| 모니터링 페이지 이미지 | http:// | ❷ 모니터링 페이지에서 감시할 이미지 경로 지정 |
| 접속속도 임계치 | 알림없음 ✔ 초 ❷ 웹사이트 응답속도에 따른 알림임계치 설정(권장설정: | 3초) |
| | 등록 취소 | |
| ♥ 웹사이트 등록 후 적용 간 최대 1 ♥ 웹사이트 정보 등록 시 웹사이트 | 10분의 시간이 소요됩니다. 의 위변조, 장애 여부, 응답속도를 모니터링 할 수 있습니다. | |

2. 웹모니터링(도메인) 등록하기

Search A 로그인 > 모니터링 설정 > 웹모니터링(도메인) > 등록

| 🌣 웹모니터링 도메인 | 년 - <mark>등록하기</mark> | | |
|---|--|------------------------------|-----------|
| 도메인 | ex) search.kr | Whois검색 ❷도메인 입력 후 경 | 검색버튼 클릭 |
| 도메인 등록일 | | ☞ 도메인 등록일 | |
| 도메인 만료일 | | 龠 ⊘ 도메인 만료일 | |
| 도메인 대행기관 | | ◎ 도메인 대행기관 | |
| 1차 네임서버 | 호스트명: | IP Address: | ❷ 1차 네임서버 |
| 2차 네임서버 | 호스트명: | IP Address: | ❷ 2차 네임서버 |
| | | 등록 | 취소 |
| ♥ www 등의 호스트네임을 제3 ♥ .com, .net 등 .kr 이외의 도미 ♥ 도메인 등록 시 도메인만료 7 | 익한 도메인 입력. www.sea 베인은 수동입력 필요 일 전에 알림이 발생합니다. | rcha.kr (X), searcha.kr (O). | |



3. 서버 모니터링 등록하기

Search A 로그인 > 모니터링 설정 > 서버 모니터링 > 등록

| 🔅 서버 모니터링 - 등 | 록하기 | |
|---|------------------|----------------------------|
| ※ <mark>서</mark> 버 정보 등록 시 서버의 자원 | l, 트래픽, 장애여부에 대해 | 모니터링 할 수 있습니다. |
| ₽주소 | ex) 1.1.1.2 | ❷ 모니터링대상 서버의 IP정보 기입 |
| SNMP 포트 | 161 | ⊗ SNMP포트 |
| SNMP 커뮤니티 | ex) test | ❷ 서버에 등록되어 있는 SNMP커뮤니티값 등록 |
| ♥ 잠깐! 사전 준비사항은 확인하 ♥ 서버 모니터링 등록 절차 안내 ♥ SNIAP에 대해 약아보기! | ·셨나요? (클릭 시 사전준비 | SNMP 조회 취소 페이지로 이동합니다. |

4. 네트워크 모니터링 등록하기

Search A 로그인 > 모니터링 설정 > 네트워크 모니터링 > 등록

| ※ 장비 정보 등록 시 서버의 자원 | , 트래픽, 장애여부에 대해 | 모니터링 할 수 있습니다. |
|---|-----------------|----------------------------|
| IP 주소 | ex) 1.1.1.2 | ❷ 모니터링내상 장비의 IP정보 기업 |
| SNMP 포트 | 161 | ❷ Default 값으로 UDP 161 지정 |
| SNMP 커뮤니티 | ex) test | ⊘ 장비에 등록되어 있는 SNMP커뮤니티값 등록 |
| | | SNMP 조희 취소 |
| 4 잠깐! 사전 준비사항은 확인하 4 네트워크 장비 모니터링 등록 4 이마 바이 티하 아이니고! | 셨나요? 절차 안내 | |

모든 설정이 완료된 이후에는 해당 서버에 대한 모니터링이 시작되며, 알람수신 설정을 통해 이 메일, SMS 및 일일보고서가 발송됩니다.