Deep Security 9.0 사용자 / 관리자 가이드

목차

제품 개요

용어설명

매뉴얼에서 반복 사용 되는 용어를 설명 합니다.

- DSM : Deep Security Manager의 약어로, 중앙관리 Web Console
- DSA : Deep Security Agent의 약어로, 각 서버에 agent 설치되어 Deep Security의 기능을 수행
- 컴퓨터 : DSA가 설치 되는 각각의 서버를 컴퓨터라고 함

제품소개

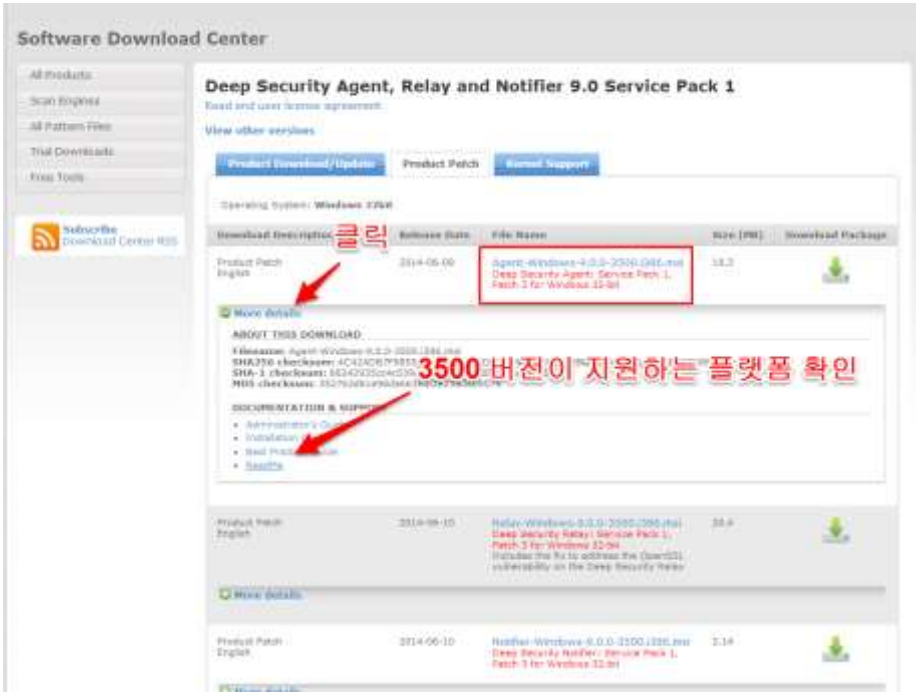
Deep Security는 통합 클라우드 보안 서비스 이며, 클라우드 환경에서 보다 편리 하게 적용 할 수 있도록 하였습니다. 기능은 아래와 같이 총 6가지 구성 됩니다.

1. Anti-Malware : 서버 백신 업계 세계 1위의 Trend Micro의 인정받은 Anti-Malware 엔진을 사용하여, 악성코드로부터 서버를 보호 합니다.
2. Web Reputation : 굉장히 효과적이고 간단한 또 하나의 보안 툴 입니다. 기본적인 배경은 시스템의 보안은 도메인 레벨에서의 컴퓨터간의 커뮤니케이션을 컨트롤 함으로 증대 될 수 있다는 점에서 출발 하였습니다. 전 세계로부터 수집되는 Trend Micro의 웹사이트 정보를 바탕으로 악성 도메인을 차단하며, 관리자는 간단히 화이트 리스트를 생성하여 도메인간의 통신을 허가 할 수도 있습니다.
3. Firewall : 각각의 서버에 필요한 포트와 프로토콜만 허용 합니다. 예를 들면, 같은 보안 설정 그룹 내에서 한 서버만 LDAP(389)를 열어야 하고 다른 서버들은 아니라면, 오직 그 필요한 서버만 389포트를 열어 줍니다. IP 프로토콜 자체의 취약점인 spoofing 공격에 대비한 Stateful Firewall기능도 제공합니다.
4. Intrusion Prevention : 새로운 단계의 서버 보안 입니다. Firewall로부터 허가된 inbound와 outbound 트래픽을 검사를 하여, 아직 패치가 되지 않은 OS나 어플리케이션으로 부터의 취약점을 타겟으로 하는 의심스러운 활동이나 공격을 차단합니다.
5. Integrity Monitoring : 관리자에게 허가된 그리고 허가 되지 않은 시스템의 변화를 추적할 수 있게 합니다. 공격자의 허가되지 않은 시스템의 변경을 적시에 발견하는 것은 보안 향상에 아주 효과적입니다.
6. Log Inspection : 관리자가 중요 시스템 로그를 적시에 확인 할 수 있도록 합니다. 각 시스템 들의 중요 로그가 통합 관리되며, 관리자의 설정에 따라 이벤트를 설정하여 적시에 이상 징후를 찾아 냅니다.

Deep Security 호환성

Deep Security Agent 호환성

- 아래의 Installer를 다운로드 받는 웹페이지에서, 다운 받고자 하는 Deep Security Agent 버전의 Installer의 Readme 파일 참고
  http://downloadcenter.trendmicro.com/index.php?regs=NABU&clk=latest&clkval=4367&lang_loc=1
- 예를 들면, DSA 3500 버전이 지원하는 플랫폼을 확인하고자 한다면 위의 링크로 들어가, 3500 버전의 DSA의 "More details"를 클릭하고, ReadMe 파일을 다운 받아 확인



Deep Security 를 Agent-less방식으로 구동 시 VMware와 호환성

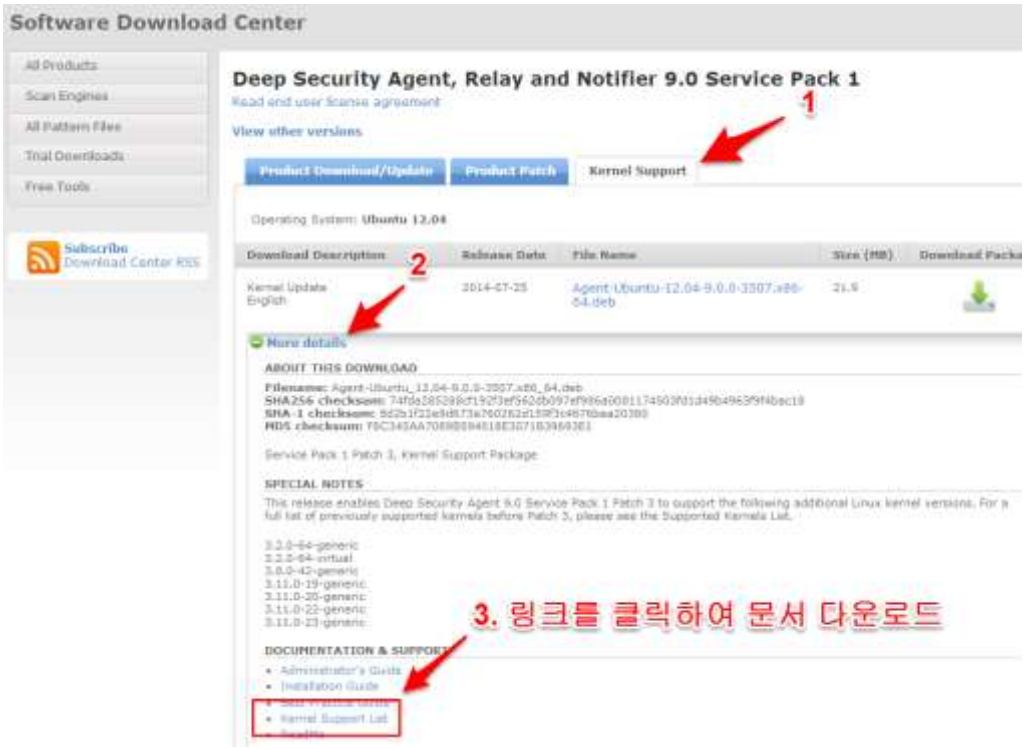
- 위와 같은 방법으로, 설치하고자 하는 버전의 Installer의 Readme 파일 확인
- Deep Security and VMware compatibility matrix 링크
  http://esupport.trendmicro.com/solution/en-US/1060499.aspx

Deep Security Manager 호환성

- 위와 같은 방법으로, 설치하고자 하는 버전의 Installer의 Readme파일 확인

Linux Kernel 호환성

- Kernel support 문서확인. 문서 다운 방법은 아래의 링크로 이동
  http://downloadcenter.trendmicro.com/index.php?regs=NABU&clk=latest&clkval=4367&lang_loc=1
- 상단의 "Kernel Support" 탭 > "More details" 클릭 > "Kerner support list" 클릭하여 문서 다운로드



KT ucloud 사용자 **필독** 사항

- 라이선스는 기본형(Anti-malware)에서 보급형(Anti-malware + Intrusion Prevention), 보급형에서 확장형(All modules)으로는 변경 가능하지만, 확장형에서 보급형, 보급형에서 기본형으로의 변경은 불가능 합니다.
- DSM의 default 호스트 명을 변경 하지 마세요. DSM 운영에 장애가 생깁니다.
- 상품 신청 이후, 수령하신 default 패스워드를 꼭 변경 하여 사용하여 주세요. 변경 방법은 본 매뉴얼의 "자주하는 질문 > 비밀번호 변경 방법" 을 참고 하세요.
- DSM의 서버 스펙(2vCore 4G memory)은 DSA 최대 20개 까지만 설치 가능한 스펙입니다. 그 이상 설치 하고자 하시면 한국 트렌드 마이크로 서포트로 연락 주세요.
  (ds_support@trendmicro.co.kr)
- DSM의 HDD는 총 20G입니다. DSM의 스토리지 관리를 하시어, HDD가 꽉 차지 않게 주의 하여 주세요. 본 매뉴얼의 "자주하는 질문 > DSM 스토리지 관리 방법" 을 참고 하세요.
- 기본 SMTP서버 설정은, Trend Micro로만 e-메일을 보낼 수 있는 설정(DSA abusing 방지용) 입니다. DSM의 e-메일 전송 기능을 사용하고자 하시면, SMTP 서버 설정을 사용자의 SMTP서버로 다시 설정하여 주세요.
- DSM서버 리부팅 시에는, 항상 DSM 서비스를 먼저 내려 주셔야 합니다. 본 매뉴얼의 "자주하는 질문 > DSM 리부팅 하는 방법" 을 참고 하세요.

참고 매뉴얼 및 사이트

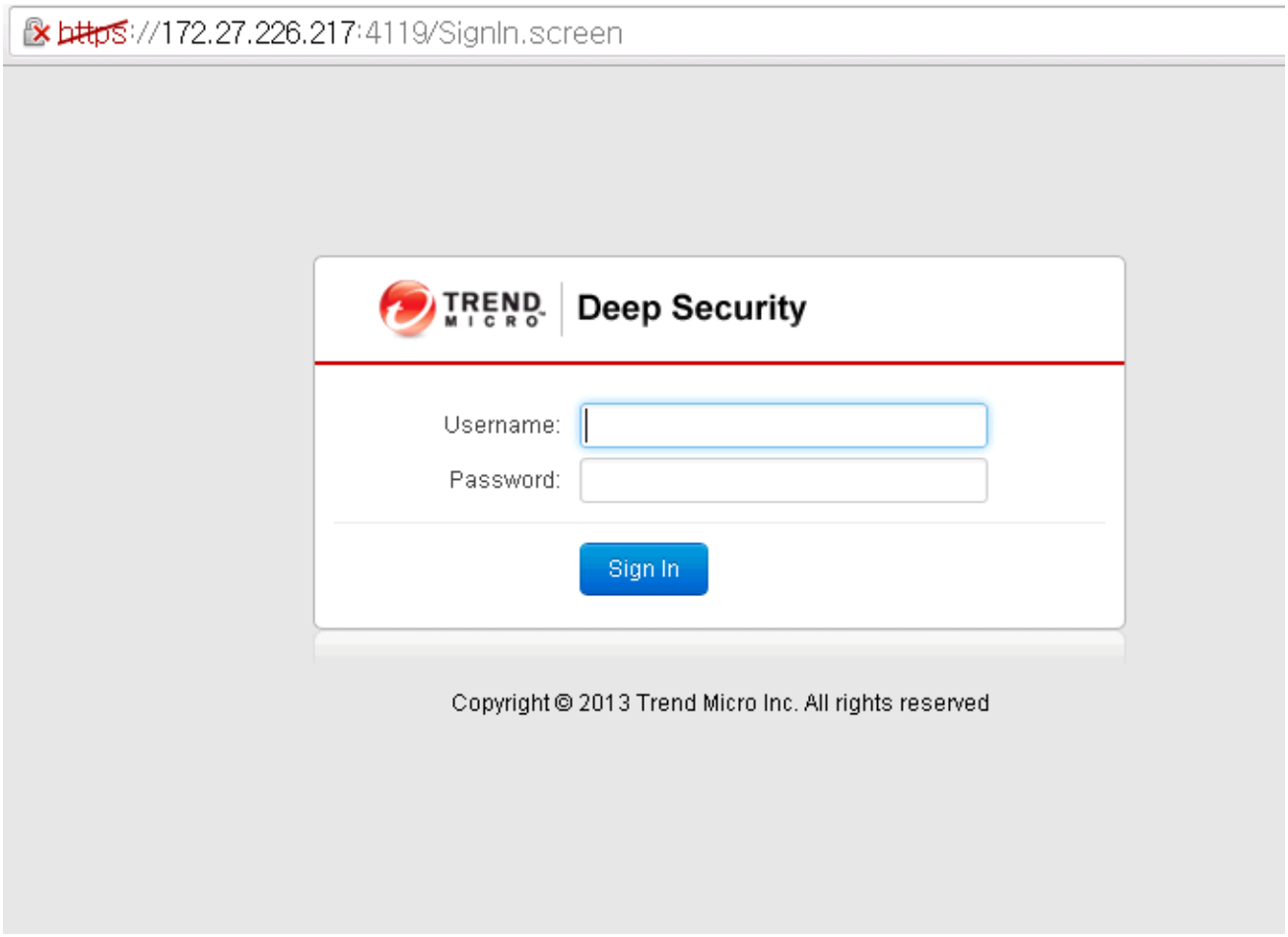
- 트렌드 마이크로 esupport
  - 주소 : http://esupport.trendmicro.com/en-us/business/pages/technical-support/deep-security-9-0-support.aspx
  - 관련 매뉴얼, System requirement 확인가능
  - 설치, 설정, 이슈 해결 그리고 업그레이드 4가지 파트로 구성하여 각종 사례
- Deep Security Online Help
  - DSM 웹 콘솔 우측 상단 클릭을 통해 접속
  - DSM의 각 화면 및 컬럼 들에 대한 설명과 설정 방법이 상당히 잘 나와 있음.
- 매뉴얼 종류 및 설명
  - Installation Guide : 설치, 삭제, System requirement
  - Administrator's Guide : DS 개념 설명 및 운영 방법
  - Best Practice Guide : Sizing, 설치, 설정, 운영 등에 대한 개념설명 보단, 구체적인 행동 위주의 설명

Deep Security Agent 설치

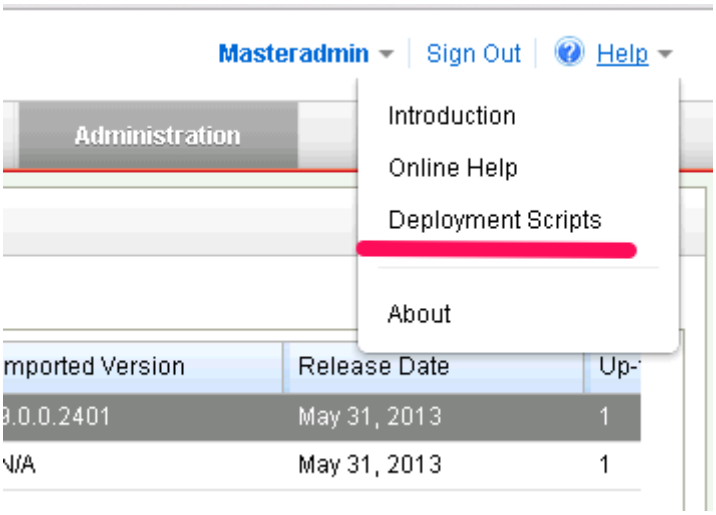
Windows 시스템에 DSA(Deep Security Agent) 설치

Deep Security Manager에 접속하여 installation 스크립트 생성

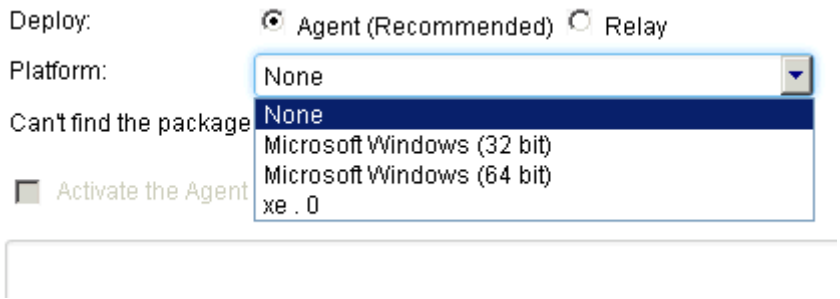
- 포탈로부터 수령한 DSM(Deep Security Manager)의 정보를 활용 하여 DSM 접속(https://ipaddress:4119) 및 로그인.



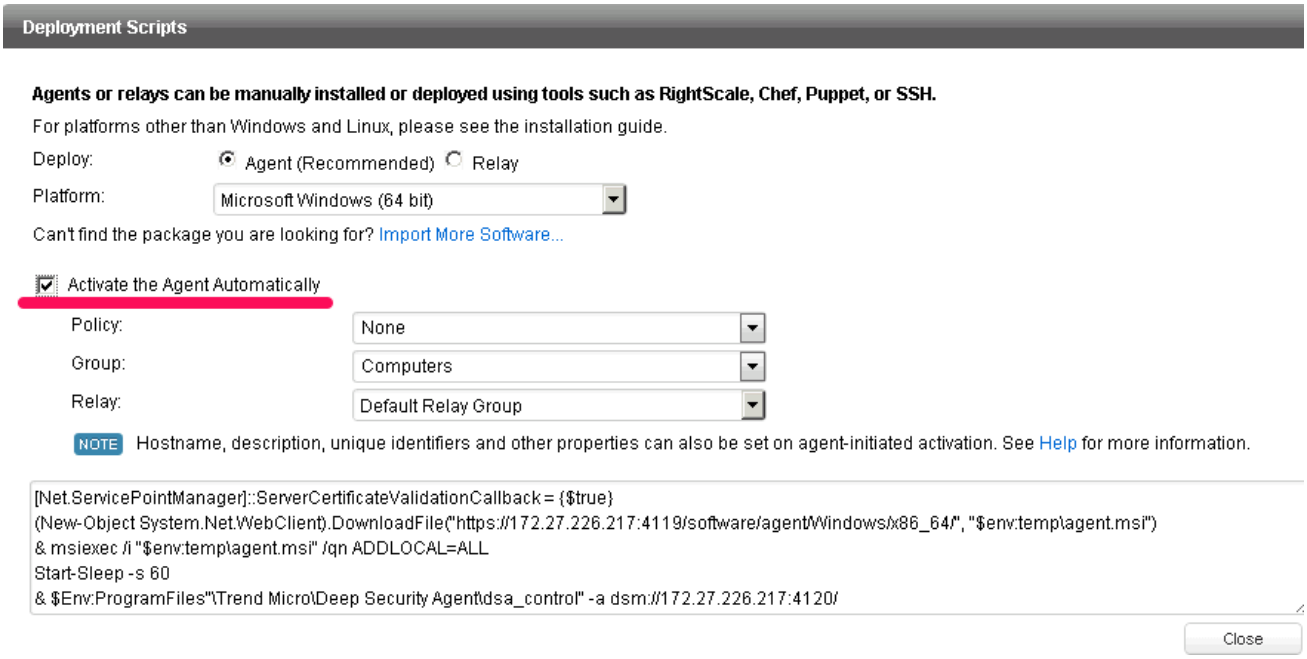
- 우측상단의 "help" > "Deployment Scripts" 클릭



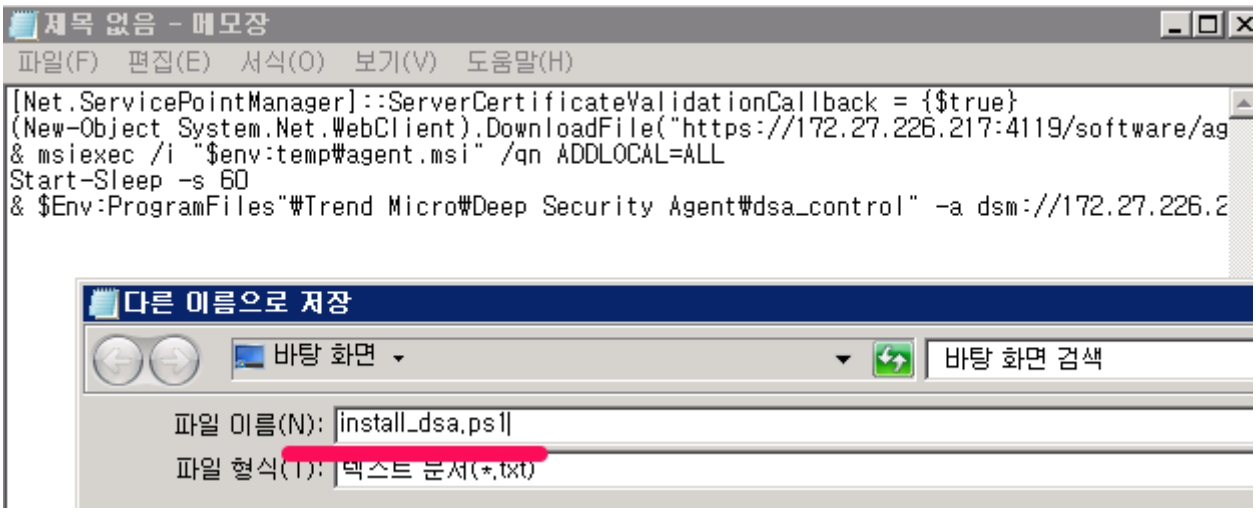
- Platform에서 DSA(Deep Security Agent)를 설치할 Windows의 bit에 맞게 선택



- "Activate the Agent Automatically" 선택



- 선택 후 나오는 박스 안의 powershell 코드를 복사하여, 작업자 PC의 임의의 공간에 "install_dsa.ps1" 이름으로 저장



- 스크립트는 한번만 생성하면 되며, 여러대의 시스템에 반복 사용 가능.

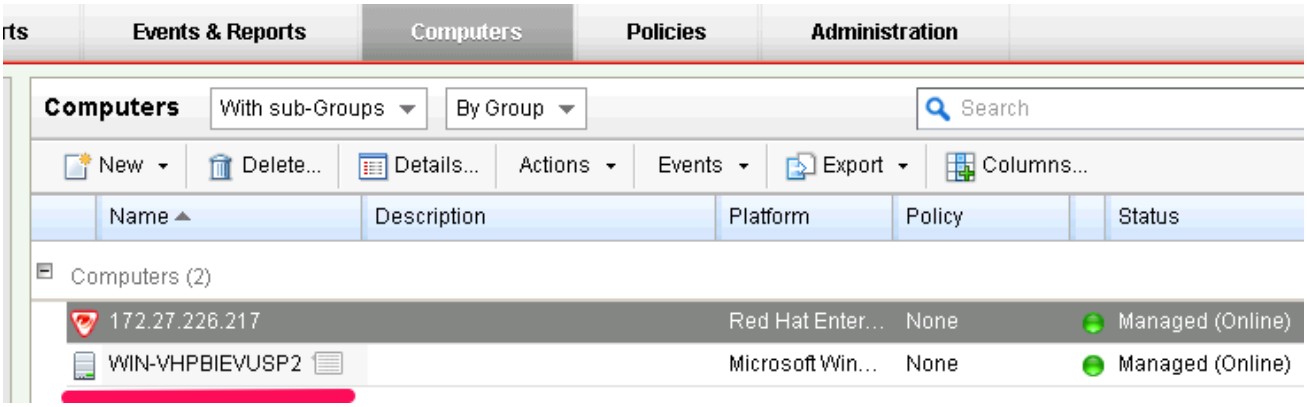
위의 installation 스크립트를 이용하여 DSA 설치

- DSA를 설치하고자 하는 Windows 시스템에 위의 스크립트 복사 후, CMD 실행
- 아래의 명령어를 이용하여 power script 실행 후 2에서 10분간 대기.
  - powershell -noprofile -executionpolicy bypass -file [파일경로와 파일명]

```
C:\>powershell -noprofile -executionpolicy bypass -file c:\install_dsa.ps1
Set-ExecutionPolicy : Windows PowerShell updated your execution policy successf
ully, but the setting is overridden by a policy defined at a more specific scop
e.  Due to the override, your shell will retain its current effective execution
 policy of "Bypass". Type "Get-ExecutionPolicy -List" to view your execution po
licy settings. For more information, please see "Get-Help Set-ExecutionPolicy."
At C:\install_dsa.ps1:1 char:20
+ set-executionpolicy <<<<  remotesigned
    + CategoryInfo          : PermissionDenied: (:) [Set-ExecutionPolicy], Sec
   urityException
    + FullyQualifiedErrorId : ExecutionPolicyOverride,Microsoft.PowerShell.Com
   mands.SetExecutionPolicyCommand
Sending the command to the agent on the local machine...

Attempting to connect to https://172.27.226.217:4120/
```

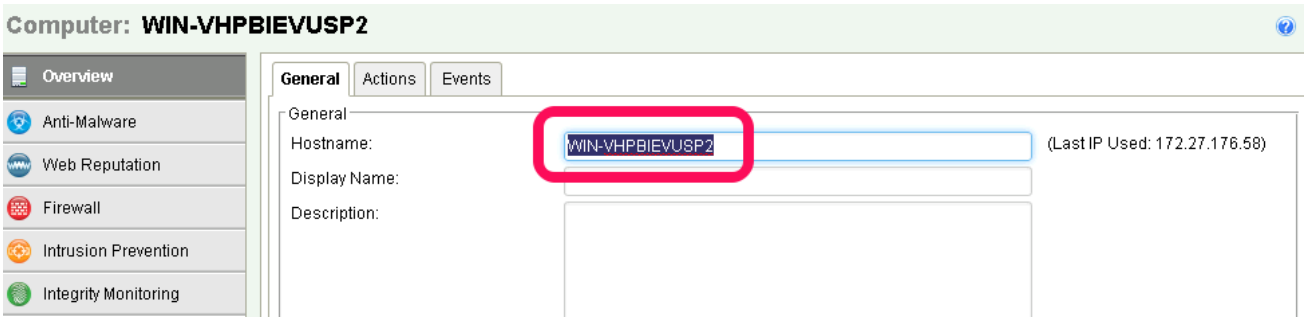
Deep Security Manager에 접속하여 호스트명 확인 및 필요 시 변경

- DSM web console(https://ipaddress:4119)로 로그인
- "Computer" 탭 선택 후, 등록된 컴퓨터 더블 클릭



- 필요 시, "Hostname" 컬럼의 값 변경.

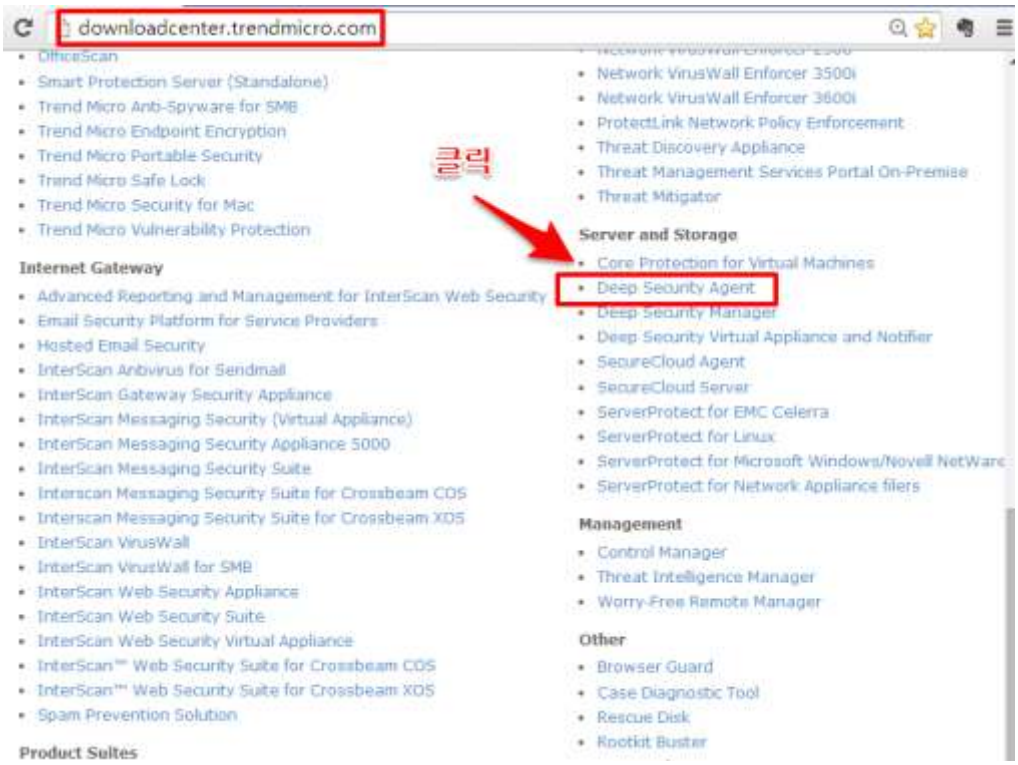
  "Hostname" 컬럼의 값이 기본으로 컴퓨터의 hostname으로 세팅되어 있는 상태 입니다. DSM에서 DSA로 통신 시, "Hostname"컬럼의 값을 이용하여 통신을 하기에, DNS가 설정 되어 있는 상태가 아니시라면, 왼편의 "Last IP Used" 의 Ip address 값을 참고하여, "Hostname"의 컬럼 값을 IP address로 변경 하여 주시기 바랍니다.



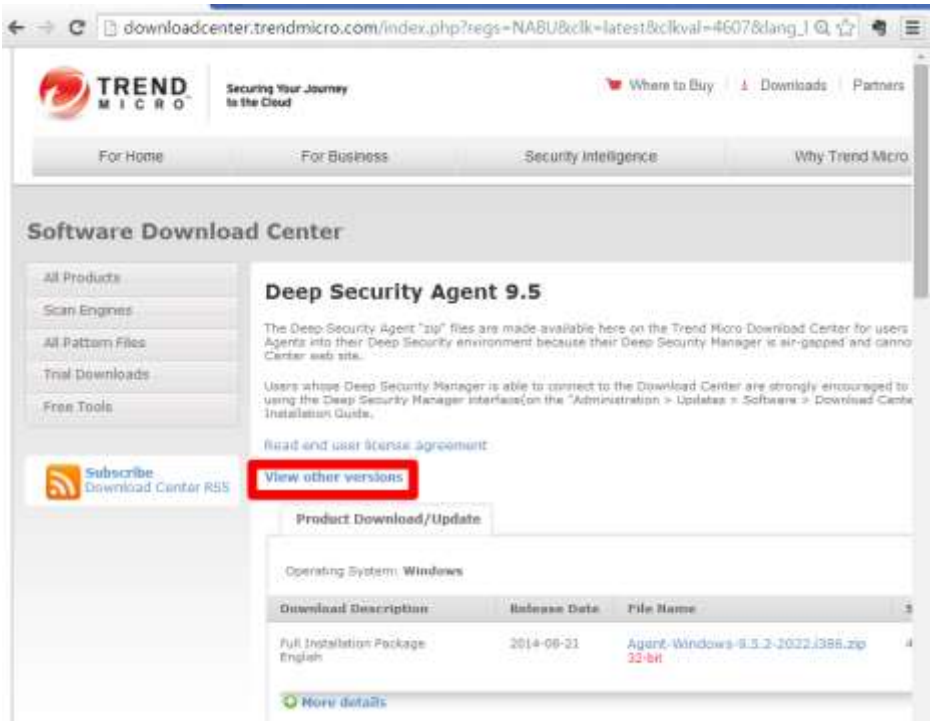
Linux 시스템에 DSA 설치

트렌드 마이트로의 다운로드 센터에서 DSA installer 다운로드 및 DSM에 import

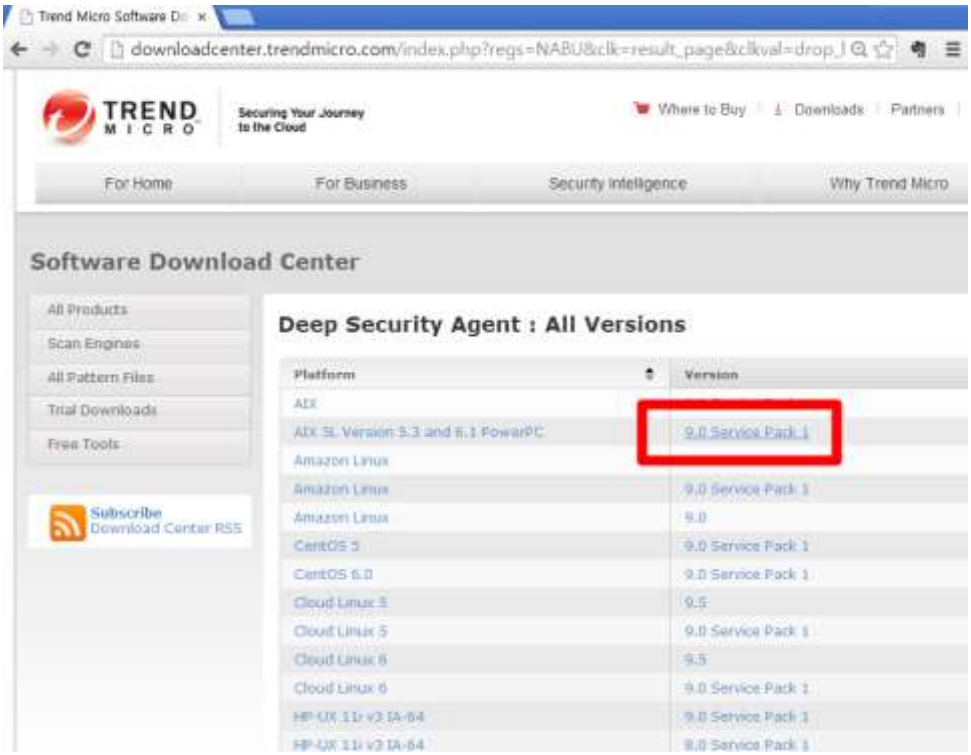
- 트렌드 마이크로 다운로드 센터 접속하여 "Deep Security Agent" 클릭



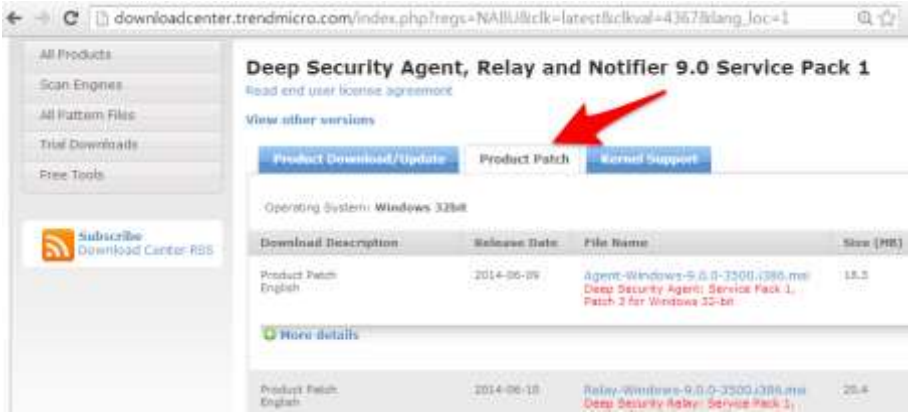
- 현재 9.0 버전을 다운 받기 위해 view other versions 클릭



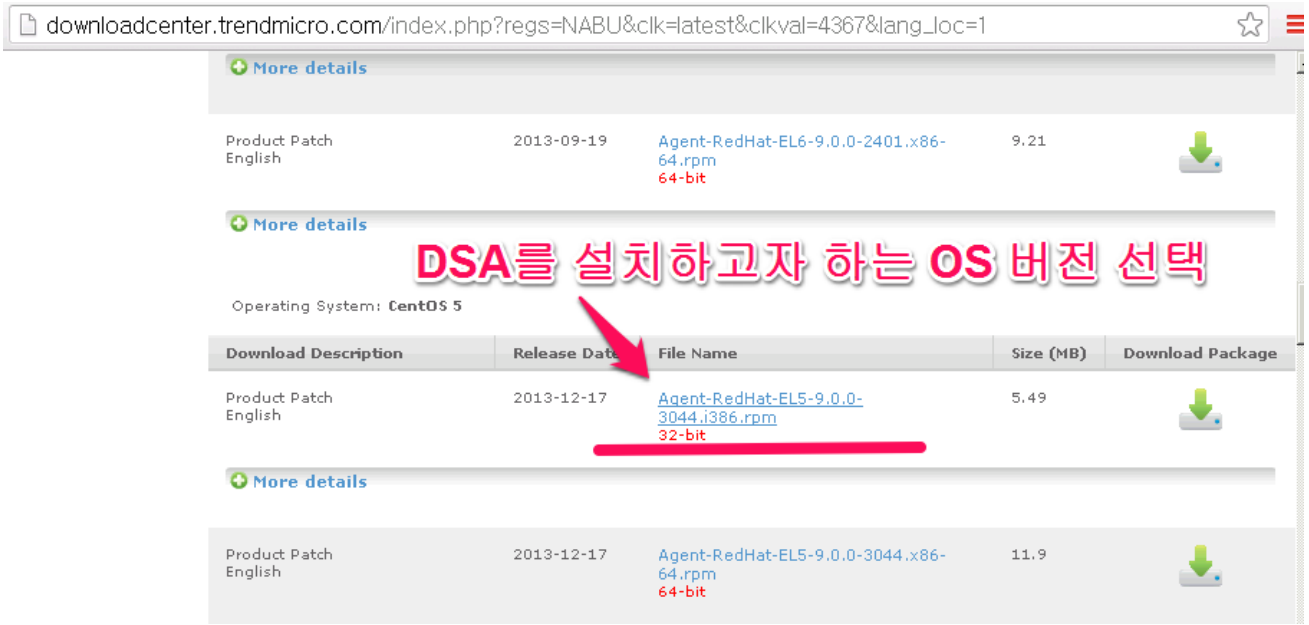
- 9.0 Service Pack 1 클릭



- "Product Patch" 탭을 클릭. 최신 버전이 Product Patch 탭에 있음. Product Patch 탭이 없다면, 초기에 보여지는 Product Download/Update 탭에서 다운 로드.

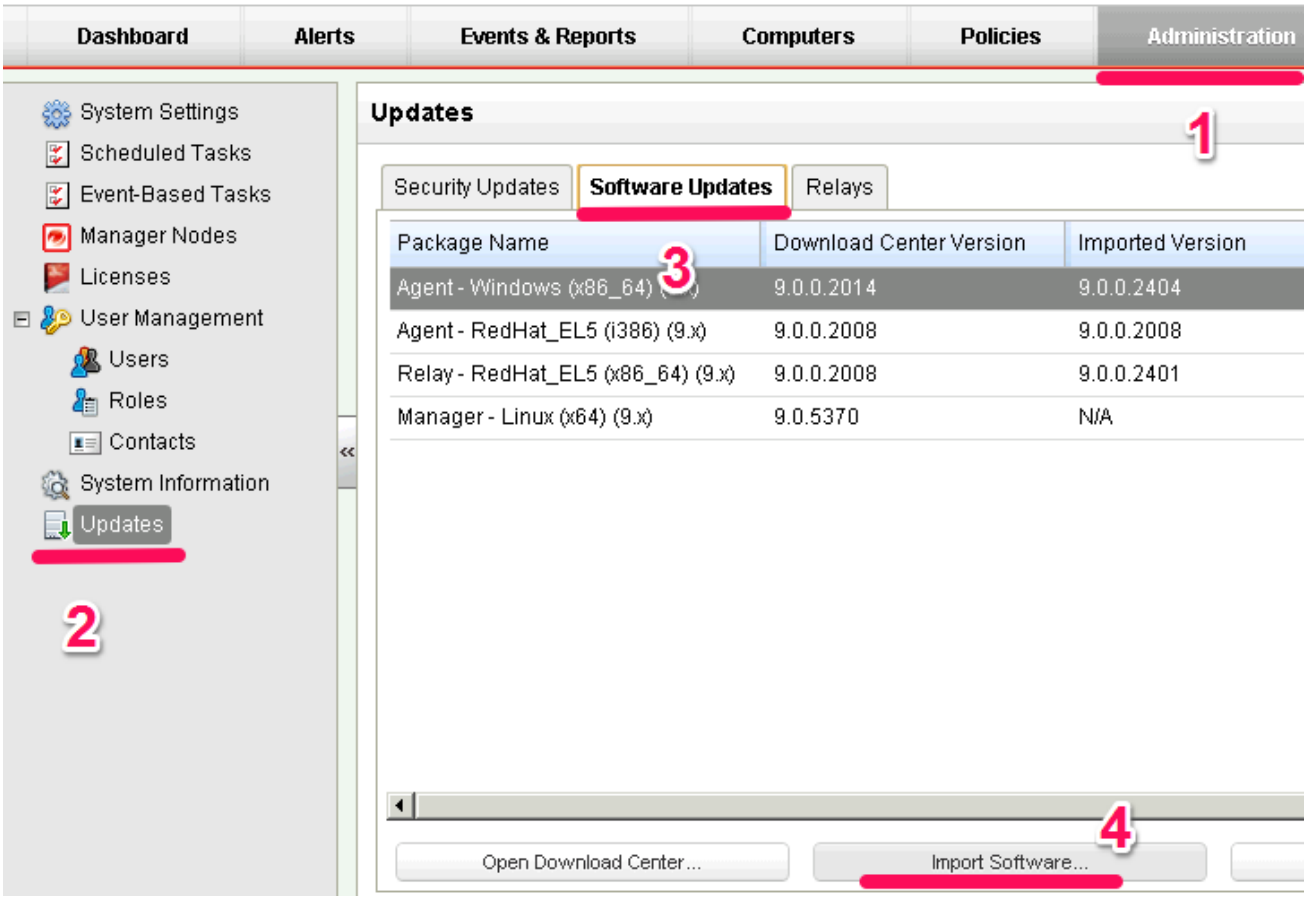


- DSA를 설치하고자 하는 OS에 맞게 최신 DSA installer 다운로드

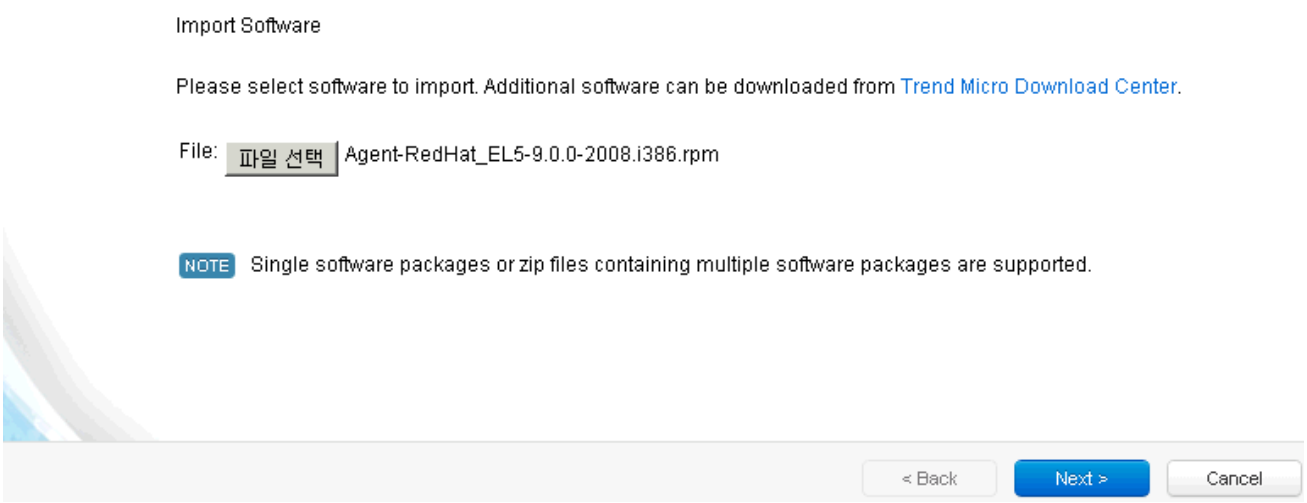


- DSM web console(https://ipaddress:4119) 접속

- "Administration" > "Update" > "Software Updates" > "Import Software" 클릭

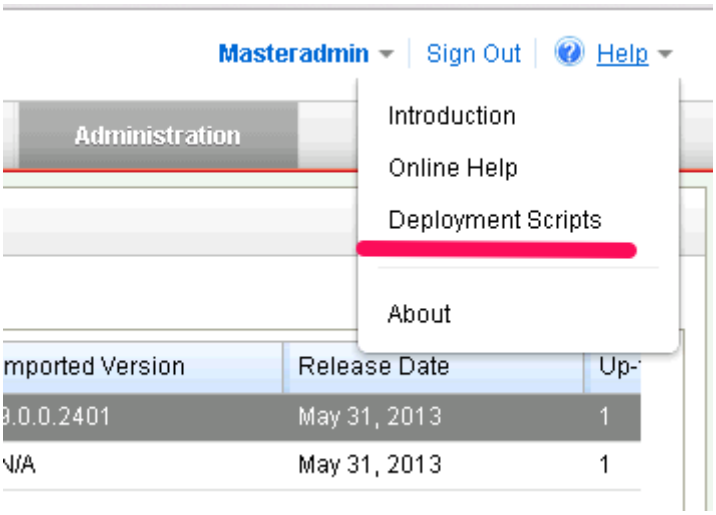


- "파일 선택" 을 클릭하여, 위에서 다운로드한 DSA installer 선택 후 "next" 클릭. 후에 "finish" 클릭

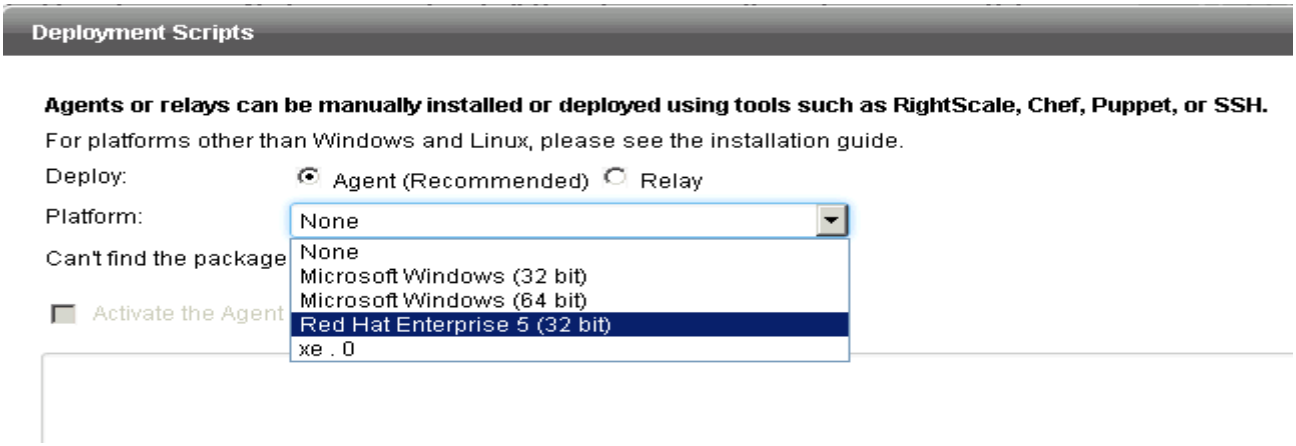


Installation 스크립트 생성

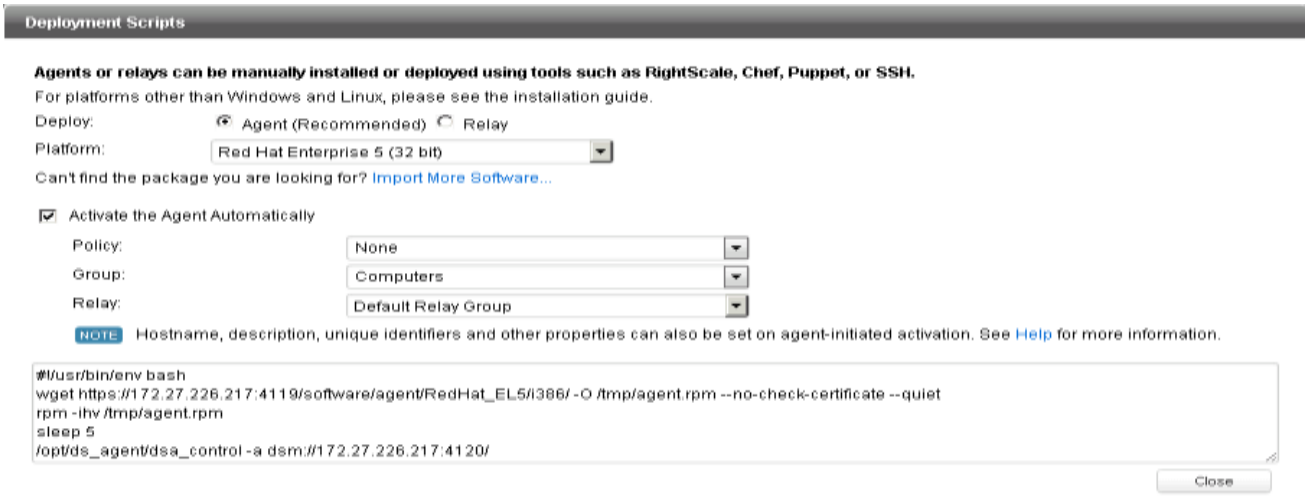
- "Help" > "Deployment Scripts" 클릭



- "Platform" 컬럼에서 DSA를 설치하고자 하는 OS 플랫폼 선택



- "Activate the Agent Automatically" 선택



- 위의 박스 안의 bash 스크립트를 vi 편집기를 이용하여 install_dsa.sh 로 저장.

```
#!/usr/bin/env bash
wget https://172.27.226.217:4119/software/agent/RedHat_EL5/i386/ -O /tmp/agen
t.rpm --no-check-certificate --quiet
rpm -ihv /tmp/agent.rpm
sleep 5
/opt/ds_agent/dsa_control -a dsm://172.27.226.217:4120/
~
~
~
~
~
~
~
:wq
```

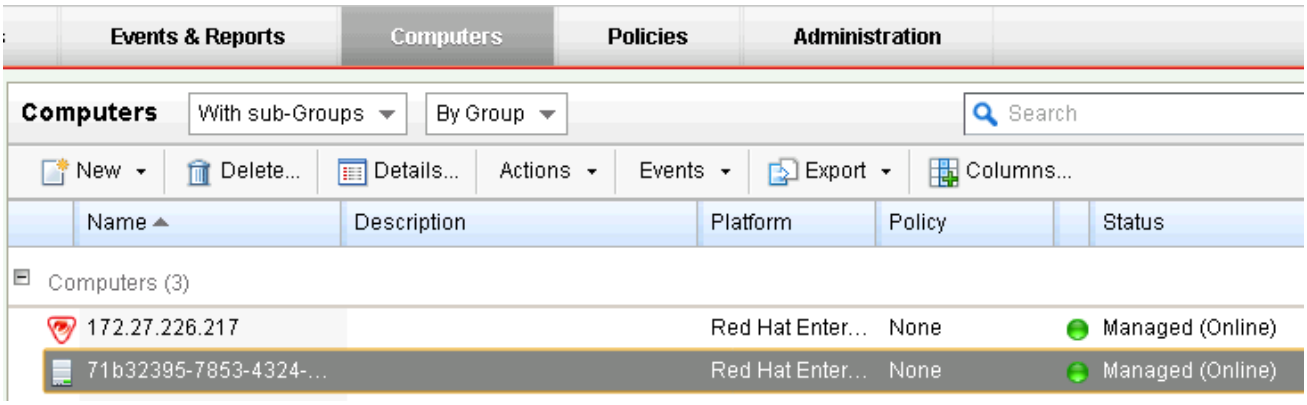
- 아래의 커맨드를 이용하여 스크립트에 실행 권한 부여.
  - Chmod 755 install_dsa.sh
- 스크립트는 한번만 생성하면 되며, 여러 대의 시스템에 반복 사용 가능.

위의 생성한 스크립트를 이용하여 Linux 시스템에 설치

- 위에서 생성한 "install_dsa.sh" 스크립트를 DSA를 설치하고자 하는 컴퓨터에 복사 및 실행.

```
[root@71b32395-7853-4324-a98b-1ee9eb7e079b ~]# ./install_dsa.sh
Preparing...                ########################################### [1
]
        package ds_agent-9.0.0-2402.i386 (which is newer than ds_agent-9.0
2008.i386) is already installed
        file /opt/ds_agent/2.6.18-164.9.1.el5PAE-i686/dsa_filter.ko from i
```

- DSM web console(https://ipaddress:4119)에 접속하여, "Computers" 탭 클릭 후, 등록된 컴퓨터 더블클릭



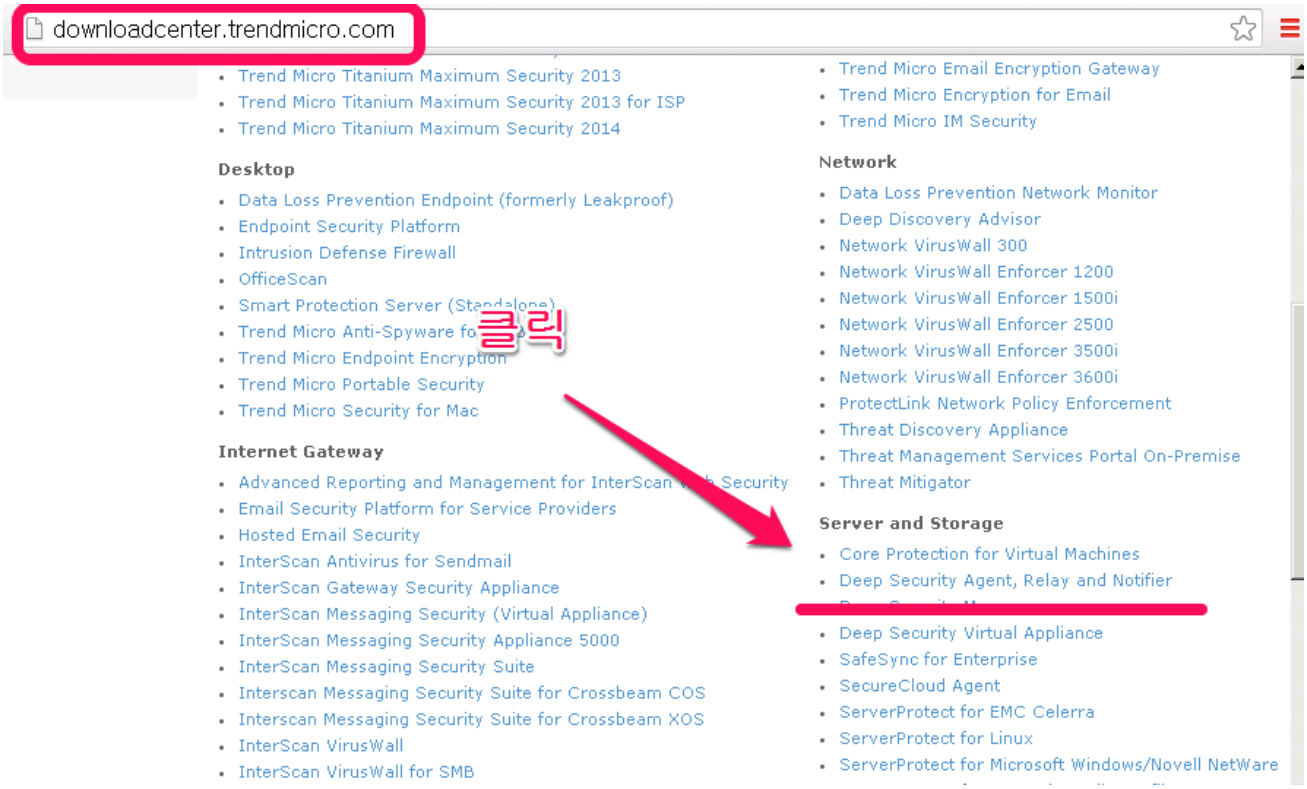
- 필요 시, "Hostname" 컬럼의 값 변경.

"Hostname" 컬럼의 값이 기본으로 컴퓨터의 hostname으로 세팅되어 있는 상태 입니다. DSM에서 DSA로 통신 시, "Hostname"컬럼의 값을 이용하여 통신을 하기에, DNS가 설정 되어 있는 상태가 아니시라면, 왼편의 "Last IP Used" 의 Ip address 값을 참고하여, "Hostname"의 컬럼 값을 IP address로 변경 하여 주시기 바랍니다.

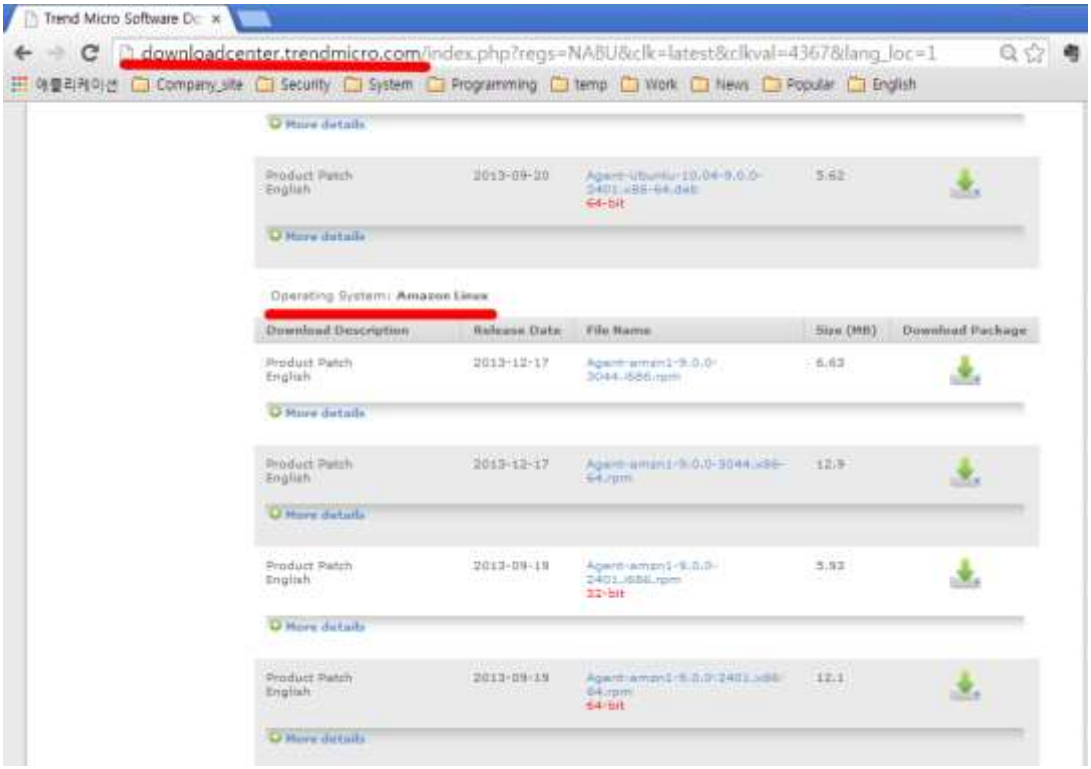
Amazon 환경에서 자동 배포 구성하여 설치

Amazon 커널버전에 해당하는 Installer를 다운 받아, DSM import

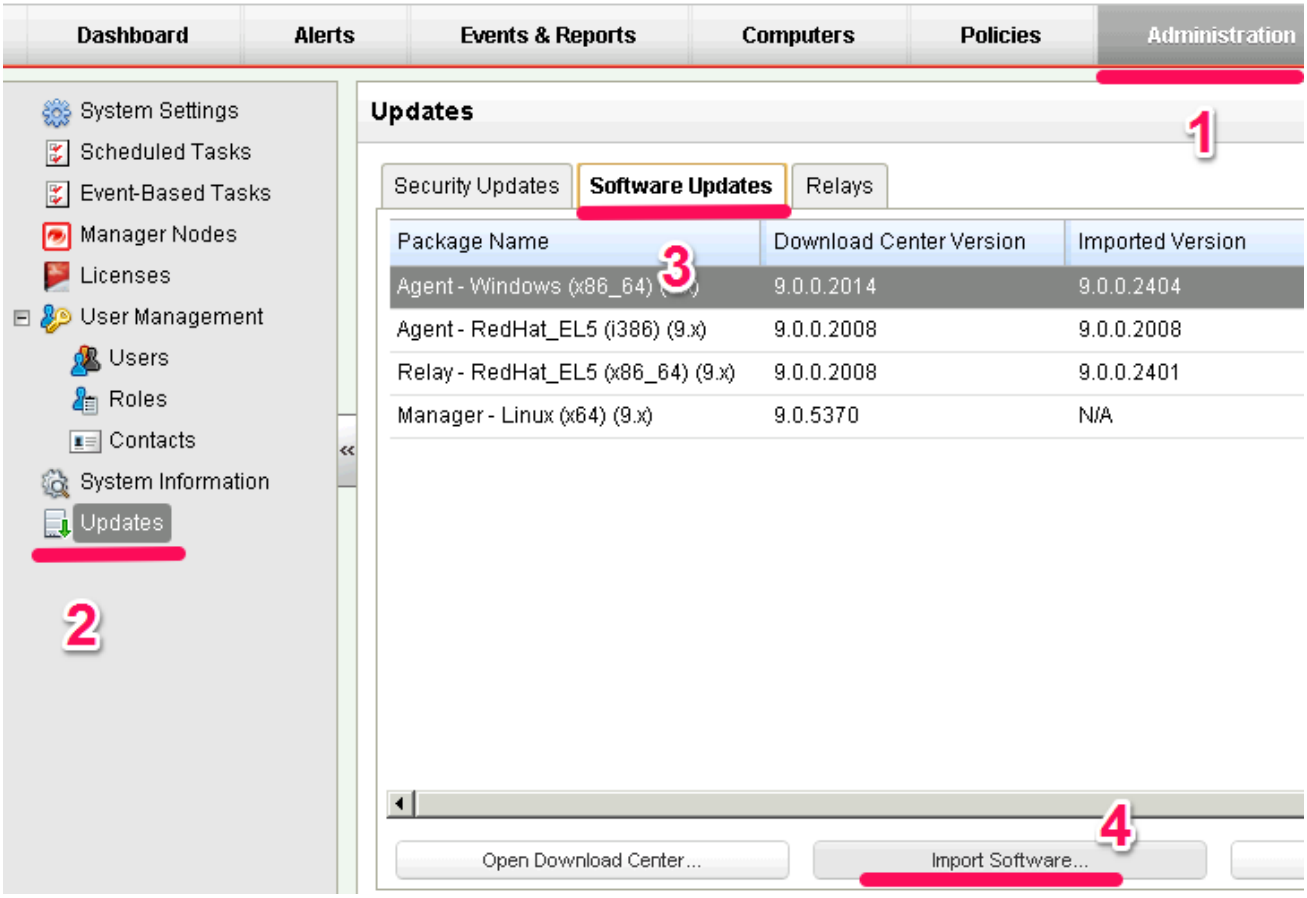
- 트렌드 마이크로 download center로 접속하여, "Deep Security Agent, Relay and Notifier"링크 클릭



- Amazon에 해당하는 installer 다운로드

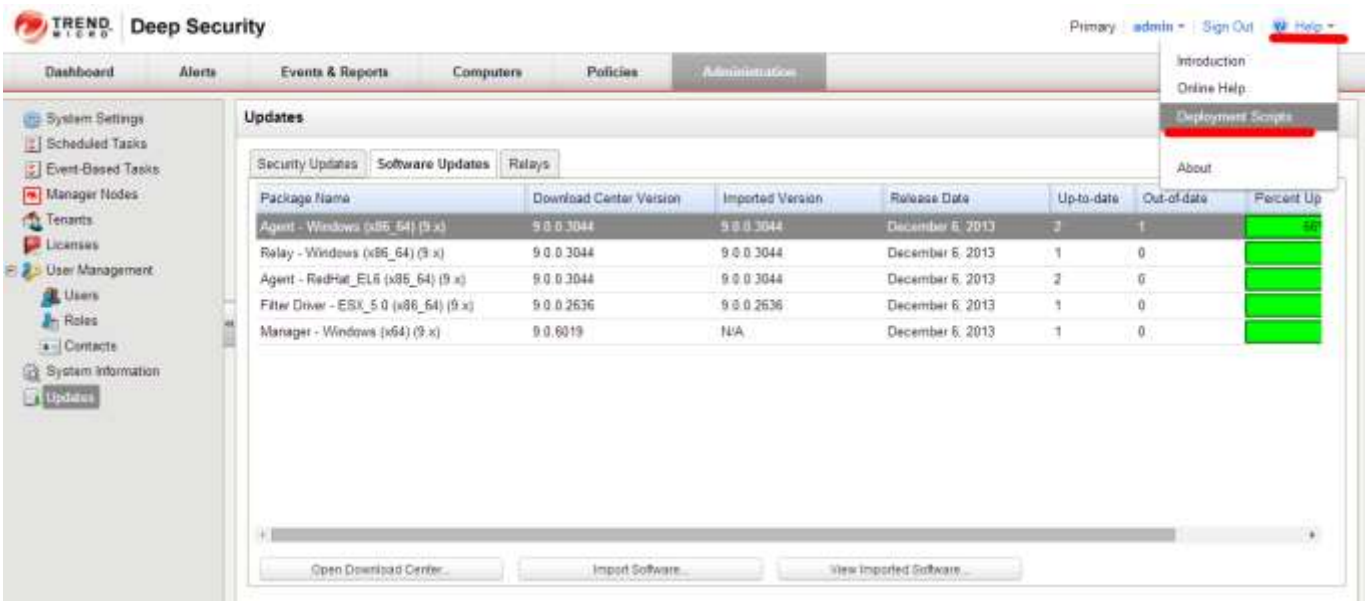


- Administration > Updates > Software Updates > Import Software 로 이동하여 다운받은 파일 업로드

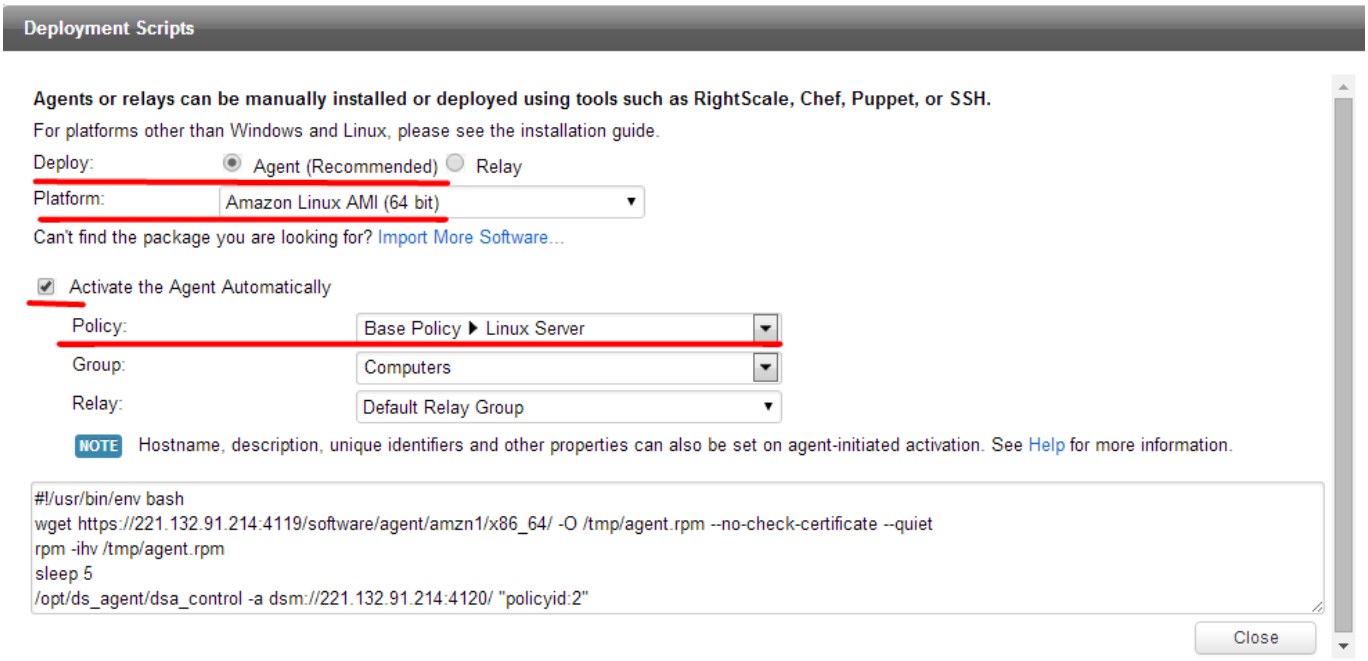


DSM에서 자동 배포를 위해 사용할 스크립트 가져오기

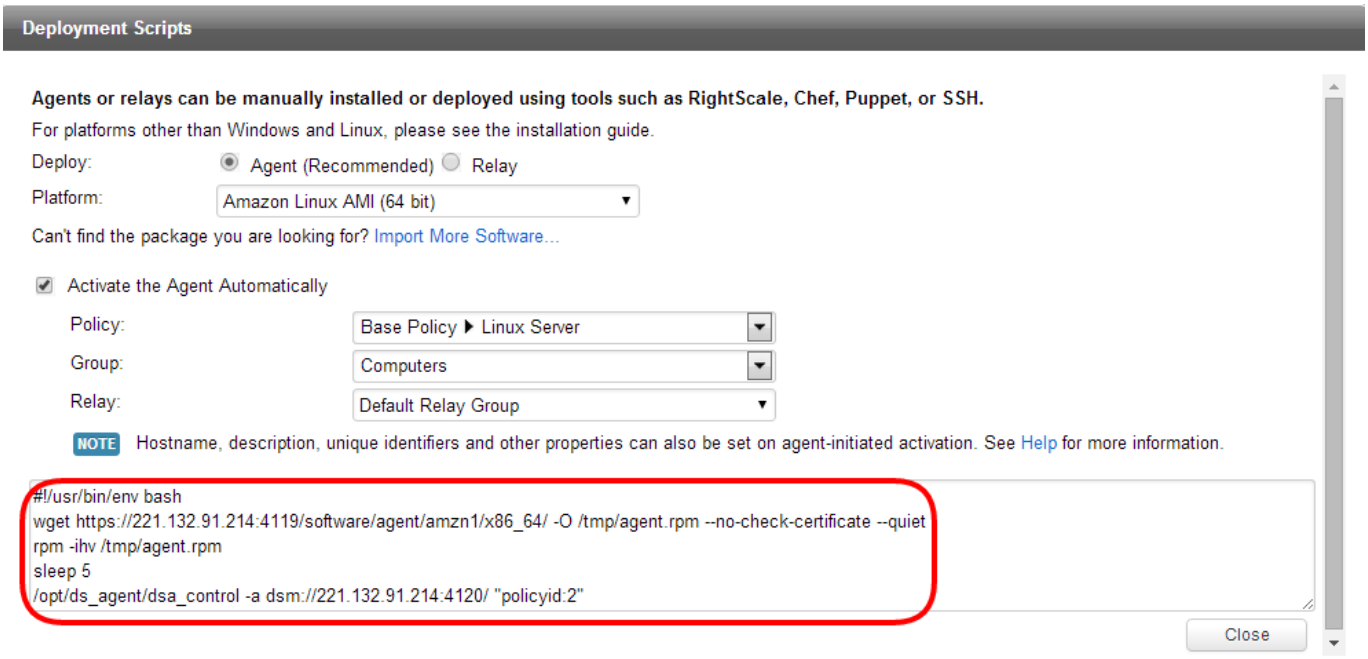
- Help > Deployment Scripts 클릭



- 위를 클릭하여 생성된 팝업 창에서, Agent, Platform, 체크박스, 그리고 적용할 policy를 설정

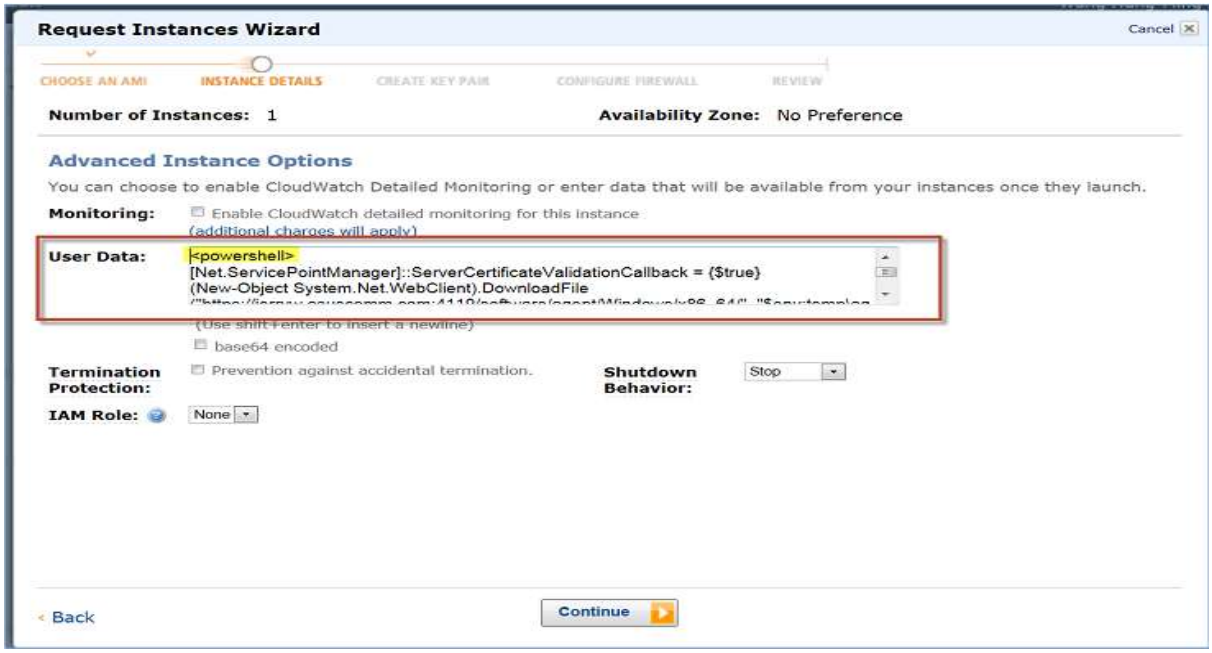


- 아래의 텍스트창에 설정한 내용으로 스크립트가 생성됨을 확인



EC2에서 Instance 생성 부분에, 설치 스크립트 추가

- 설치 진행과정에서, 아래의 User Data란에 위에서 복사한 설치 스크립트를 추가. 이후 Instance 생성 과정은 동일



Deep Security Agent 삭제

Linux 에서 Deep Security Agent 삭제

DSA 서비스 Stop(서비스가 돌고 있지 않으면서, Failed 뜨는 것은 무시하고 진행)

- Service ds_agent stop
- Service ds_am stop

루트 권한으로 로그인 후 아래의 커맨드 입력

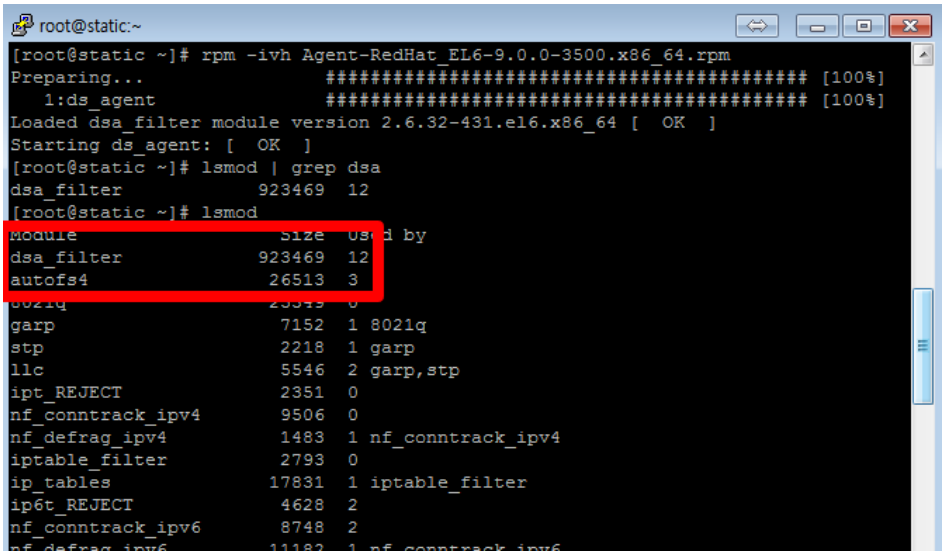
- Rpm –ev ds_agent

삭제 잘 되었는지 확인

- 아래의 /proc/driver/dsa 폴더와 그 예하의 파일이 없어야 함

```
[root@static dsa]# ls /proc/driver/dsa
configs  info  interfaces  stats  trace  trace_ctl
```

- Lsmod를 수행 했을 때, kernel module dsa_filter이 없어야 함.



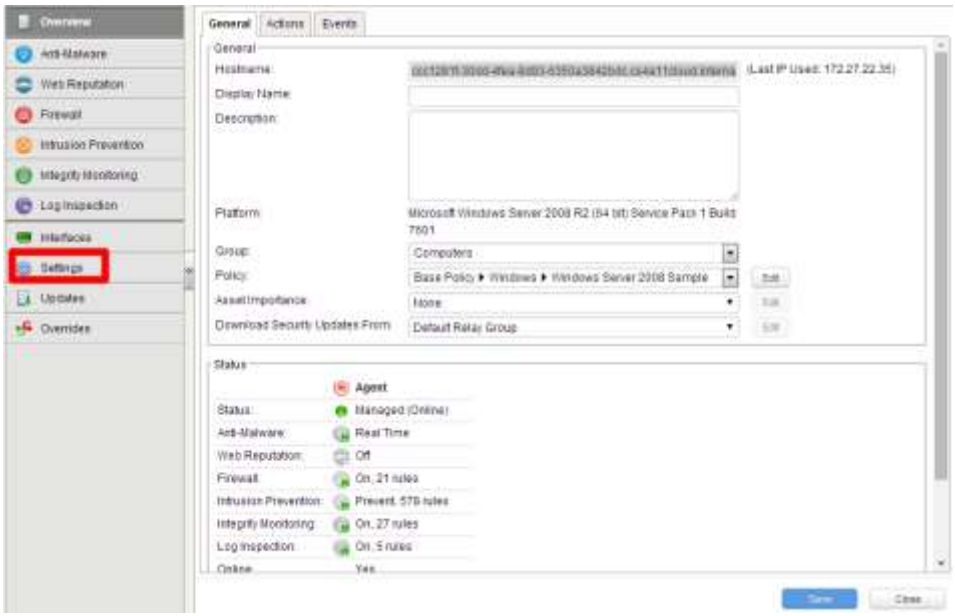
DSA 관련 폴더에 남은 파일 제거

- Rm –rf /opt/ds_agent
- Rm –rf /var/opt/ds_agent

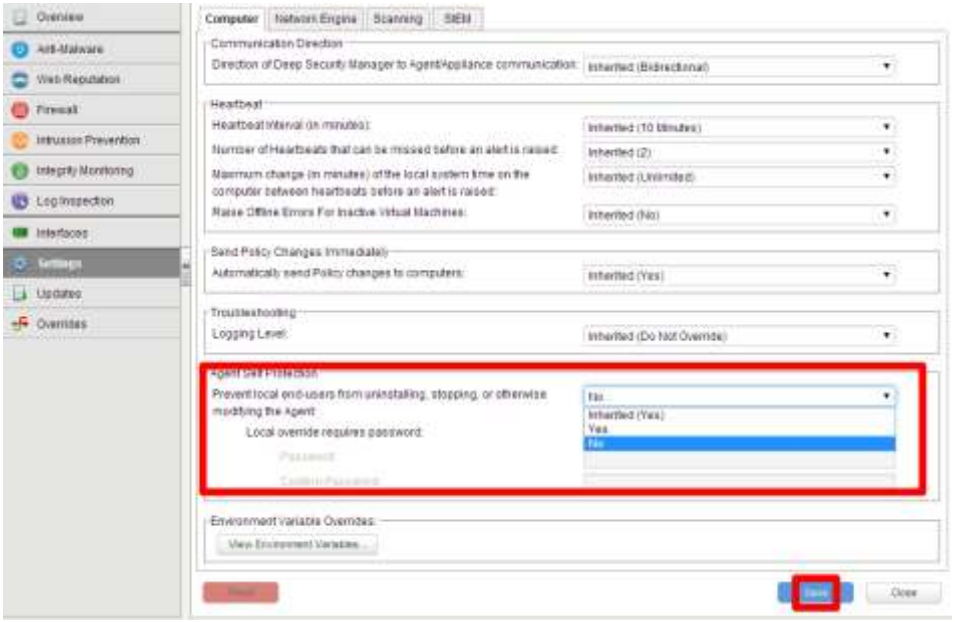
Windows에서 Deep Security Agent 삭제

DSM에서 지우고자 하는 DSA의 Self-protection 해제

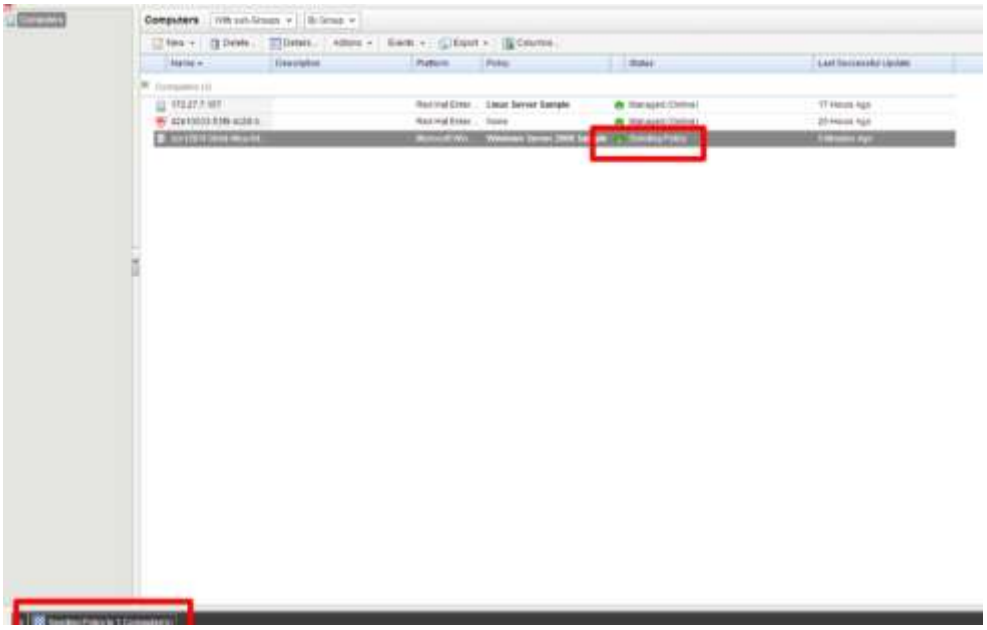
- DSA를 지우고자 하는 Computer의 상세 페이지로 이동 > 왼쪽의 "Setting" 클릭



- 하단의 "Agent Self Protection"에서 "No"로 설정 및 "Save" 클릭

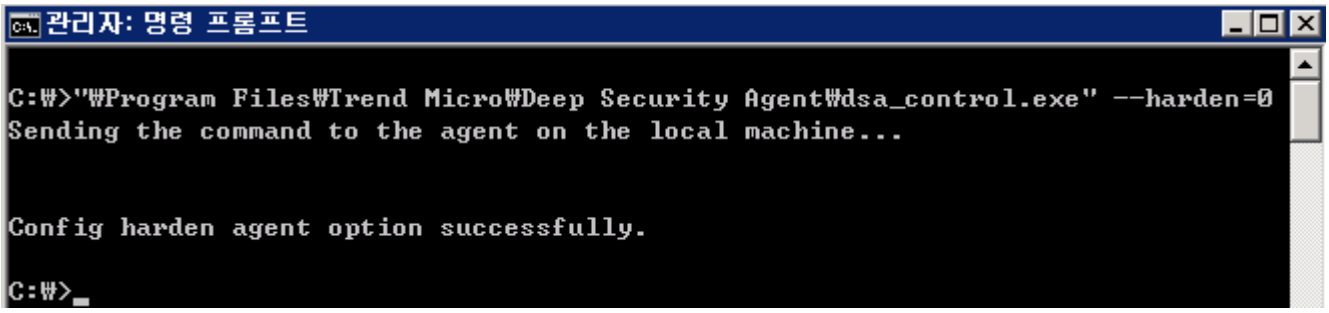


- 해당 컴퓨터로 정책이 잘 전달 되는지 확인. 아래의 Sending Policy 상태가 Managed(Online) 상태로 되면 정상.



DSM에서 DSA의 Self-protection 해제가 되지 않는 다면, DSA가 설치 되어있는 윈도우 서버로 직접 접속하여 해제

- 서버 접속 및 CMD 창 생성하여 아래의 커맨드 2~3회 수행 하며 성공하면 아래와 같이 성공 메시지가 나옴.



DSA 삭제

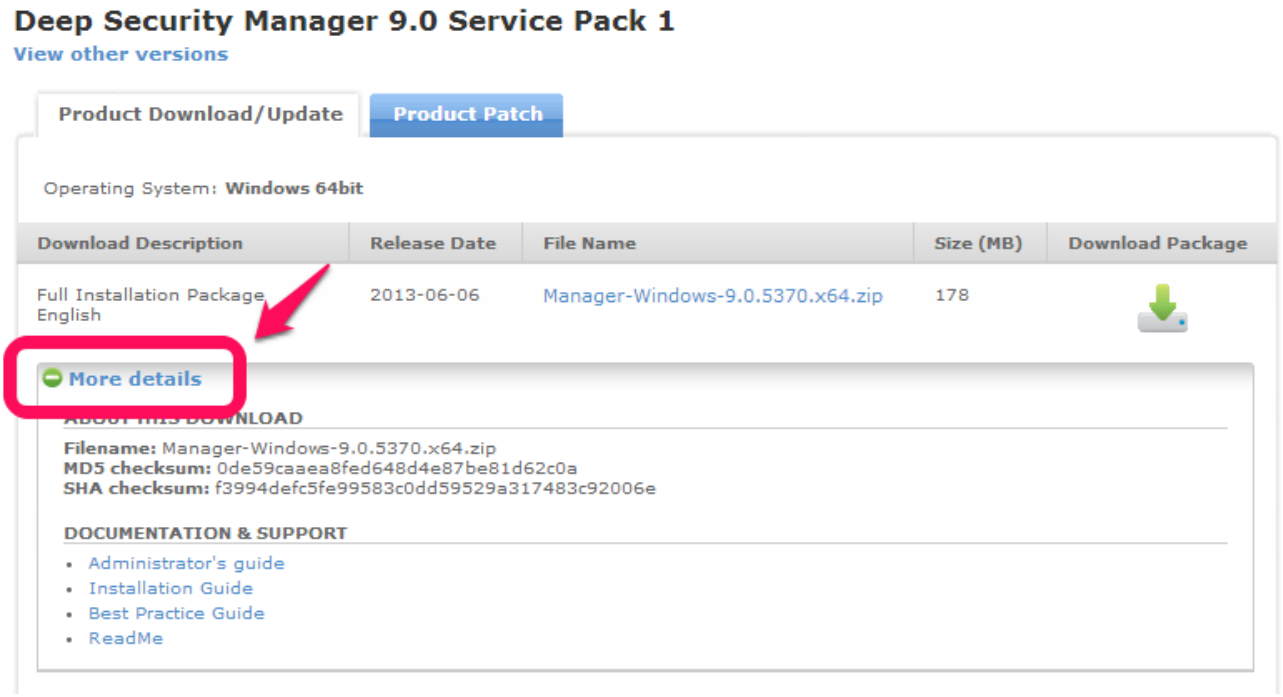
- 제어판으로 이동, 프로그램 메뉴에서 Trend Micro Deep Security Agent 찾아 제거

- 리부팅

Deep Security Manager 운영

본 매뉴얼은 간단한 Deep Security의 기본 개념을 익힐 수 있게 함이 목적 입니다. 더 자세한 매뉴얼은 다음의 링크에서 "More details"을 클릭 하시어 다운로드 가능합니다.

http://downloadcenter.trendmicro.com/index.php?regs=NABU&clk=latest&clkval=4370&lang_loc=1

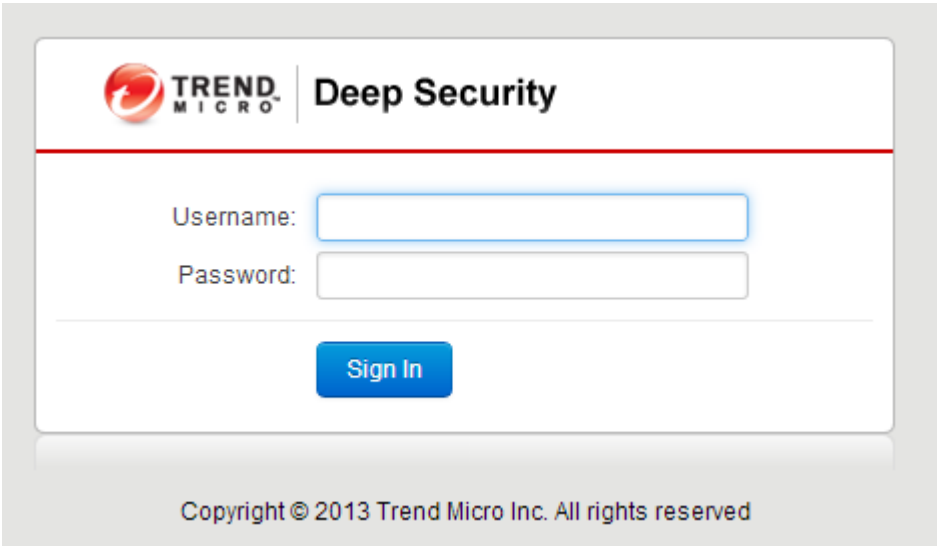


DSM 접속

웹을 통한 중앙관리 서버 콘솔 접속

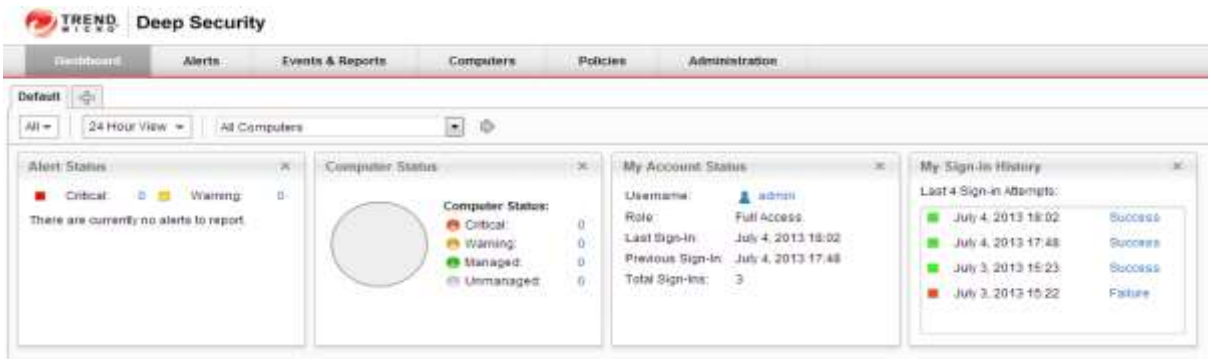
https://DSM IP address:4119/

(username/password: DSM VM이 Deploy 될 때 전송되는 KT ucloud 공지 메일에 Default ID / PW 포함)

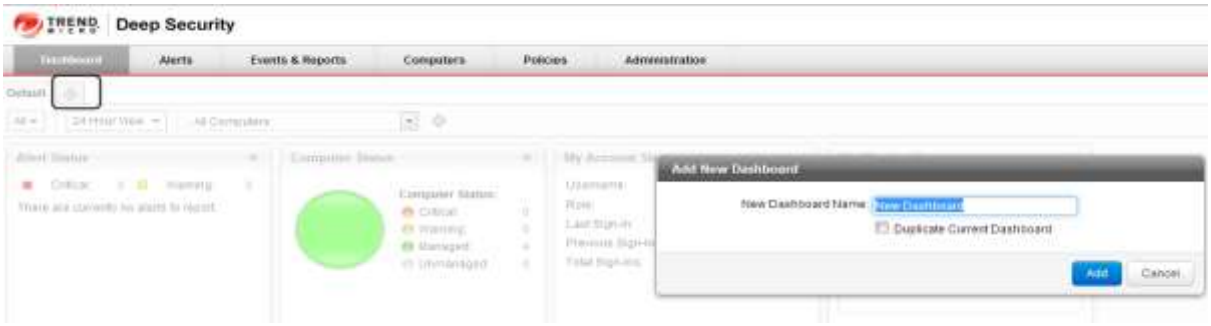


Dashboard

Dashboard에서는 Agent가 설치된 시스템들의 상태와 보안 이벤트 현황을 보실 수 있습니다.

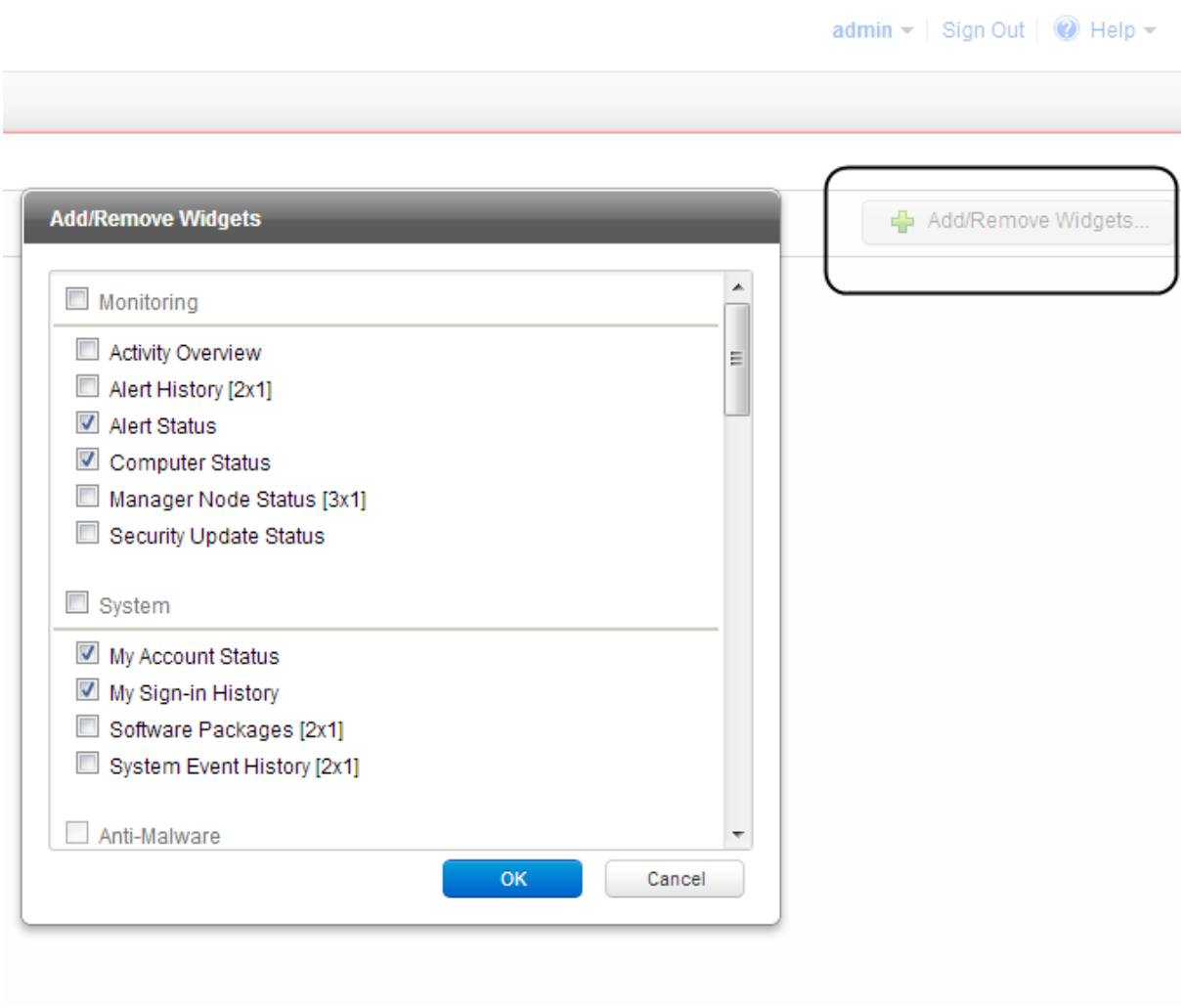


- Dashboard 추가



Dashboard Page를 추가하여 여러 관제 포인트를 가져가실 수 있습니다.

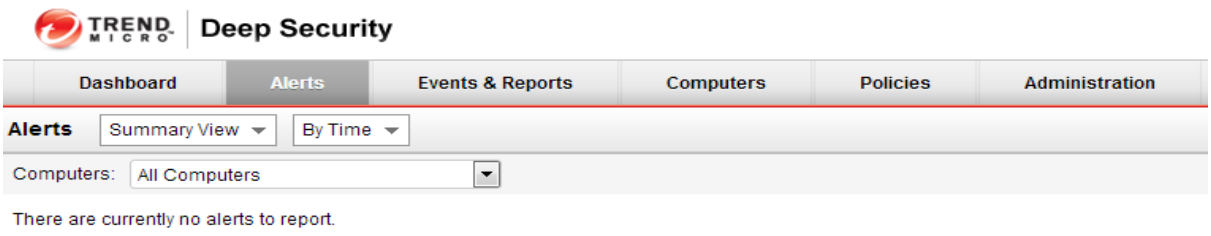
- Widget 추가/제거



- Dashboard 화면에 모니터링 원하는 Widget을 추가 또는 제거하실 수 있습니다.

Alert

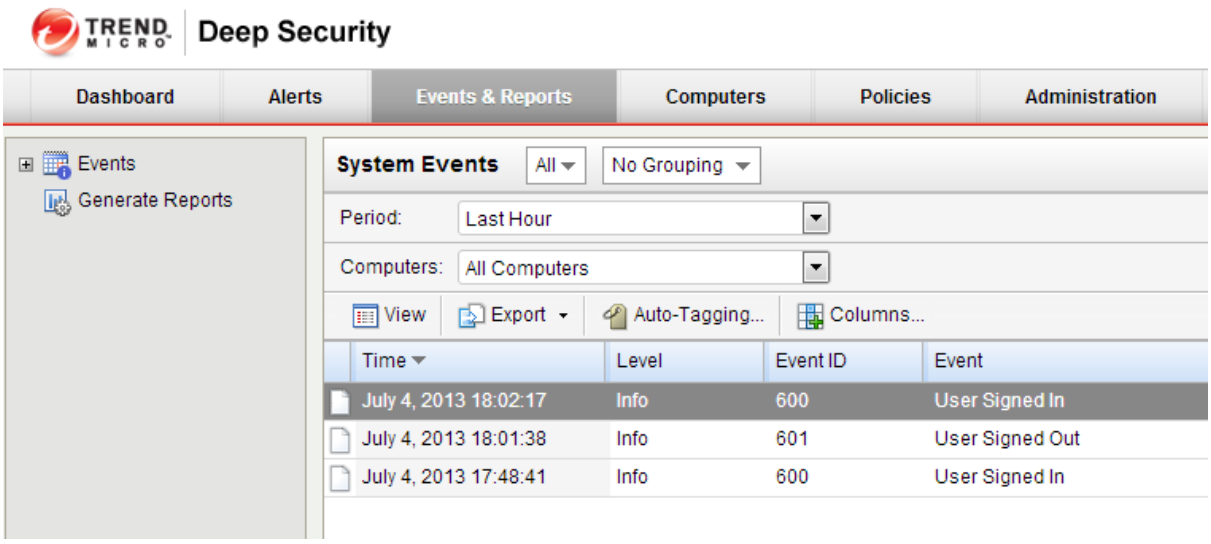
Alert 에서는 Agent가 설치된 시스템에서 Agent의 상태(서비스, 드라이버, 정책설정등)나 보안 이벤트(악성코드 탐지, 취약점 공격(Zero-day), 패턴 업데이트등)가 발생할 경우, 경고(Warning), 심각(Critical)으로 알려줍니다.



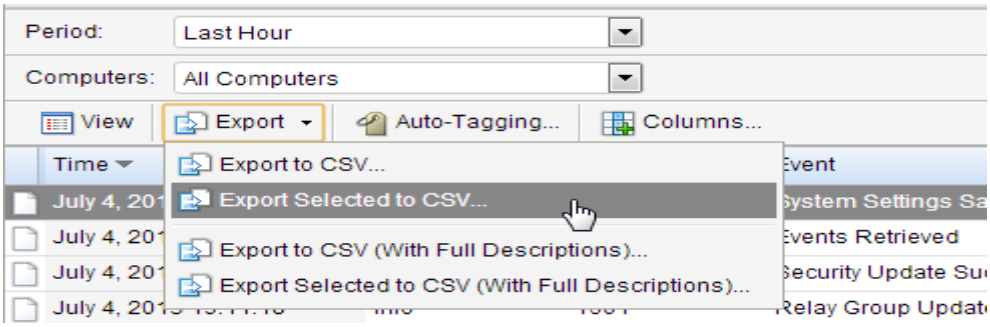
Events&Reports

Deep Security Agent 또는 Deep Security Manager에서 발생하는 시스템 로그 및 보안 이벤트 로그의 RAW Data 를 조회 / 모니터링 할 수 있습니다.

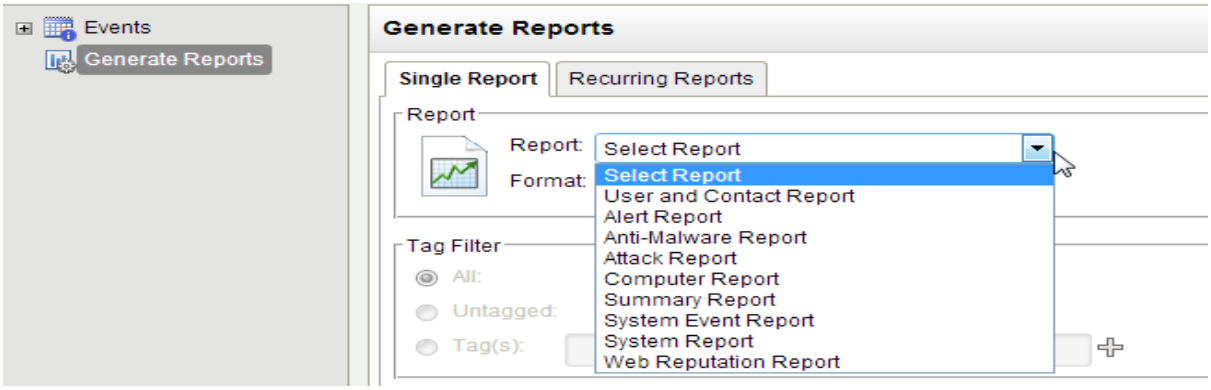
- Deep Security Manager에서 제공하는 다양한 리포트 템플릿을 통해 통계/리포트를 추출하여 받으실 수 있습니다.



- 기간, 대상 옵션을 설정하여 검색할 수 있으며 파일로 추출할 수 있습니다.



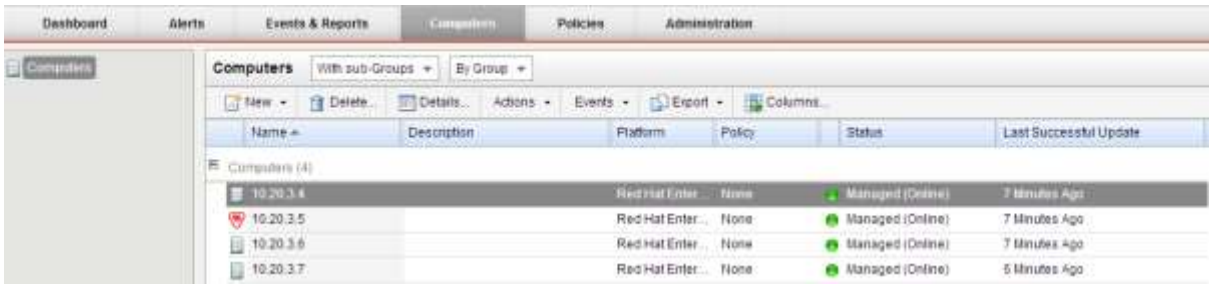
- 원하는 리포트 양식을 선택하고 다양한 필터 옵션을 선택하여 파일로 리포트를 추출할 수 있습니다.



Computers

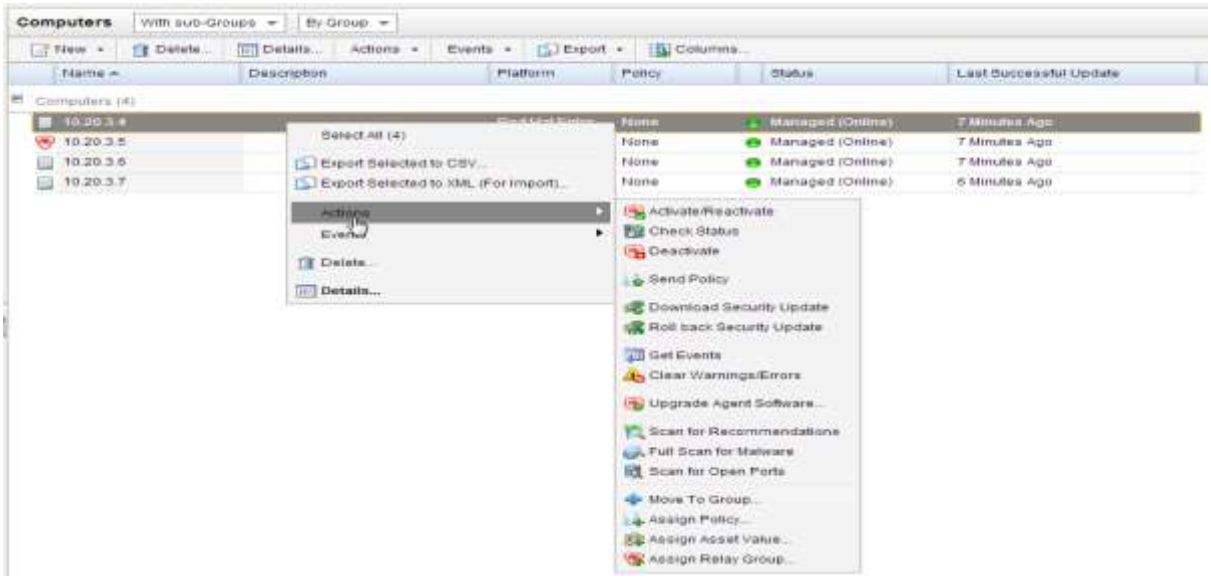
등록 된 총 컴퓨터를 확인 하며, 각각의 컴퓨터 별로 설정이나 이벤트 등을 종합 적으로 확인 및 설정 합니다.

- Agent가 설치되고 Manager로 등록된 리스트 정보를 볼 수 있습니다.

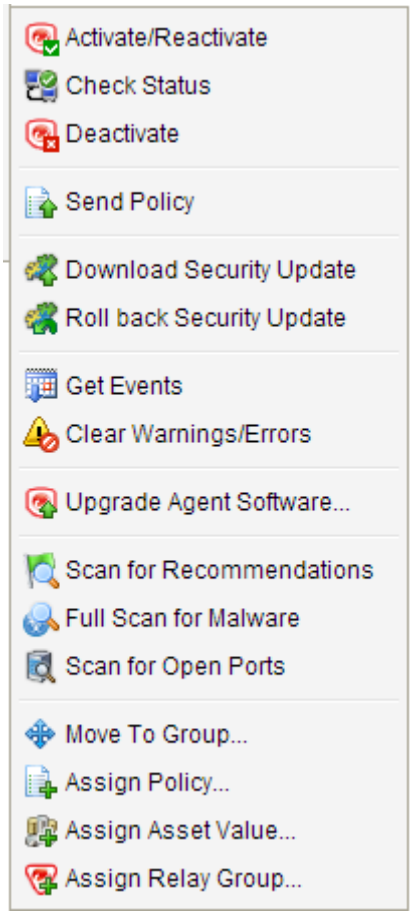


- 특정 Agent를 더블 클릭하면 해당 시스템 창을 띄우고 관리할 수 있습니다.

- 또한 특정 Agent에서 마우스 오른쪽 버튼 클릭하면 적용할 수 있는 Command 메뉴를 보실 수 있습니다.



- Command 설명

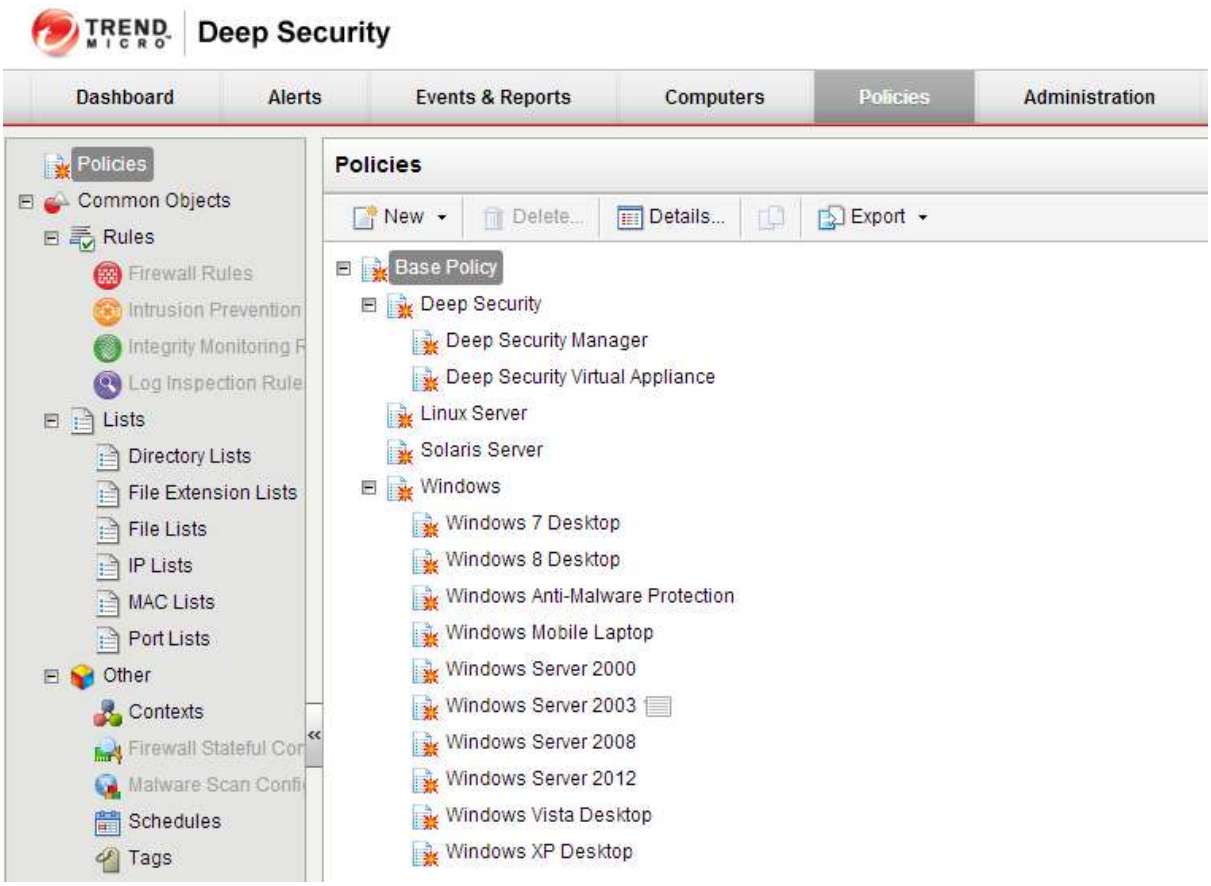


- Activate/Reactivate : Agent 등록/재등록 명령
- Check Status : 통신 상태 체크
- Deactivate : Agent 등록 해제 명령
- Send Policy : 정책 배포 명령
- Download Security Update : 패턴 / 룰 업데이트
- Roll back Security Update : 이전 패턴/룰로 롤백
- Get Events : Agent의 보안 이벤트 쿼리
- Clear Warnings/Errors : 경고/에러 메시지 지움
- Upgrade Agent Software : 새 Agent 버전 업그레이드
- Scan for Recommendations : 시스템의 필요 룰 검사
- Full Scan for Malware : 악성코드 검사(디스크 전체)
- Scan for Open Ports : 시스템의 오픈 포트 검사
- Move To Group : 특정 그룹으로 Agent 이동
- Assign Policy : 정책 적용
- Assign Asset Value : Agent의 중요도 분류
- Assign Relay Group : 패턴/룰 업데이트 서버 선택

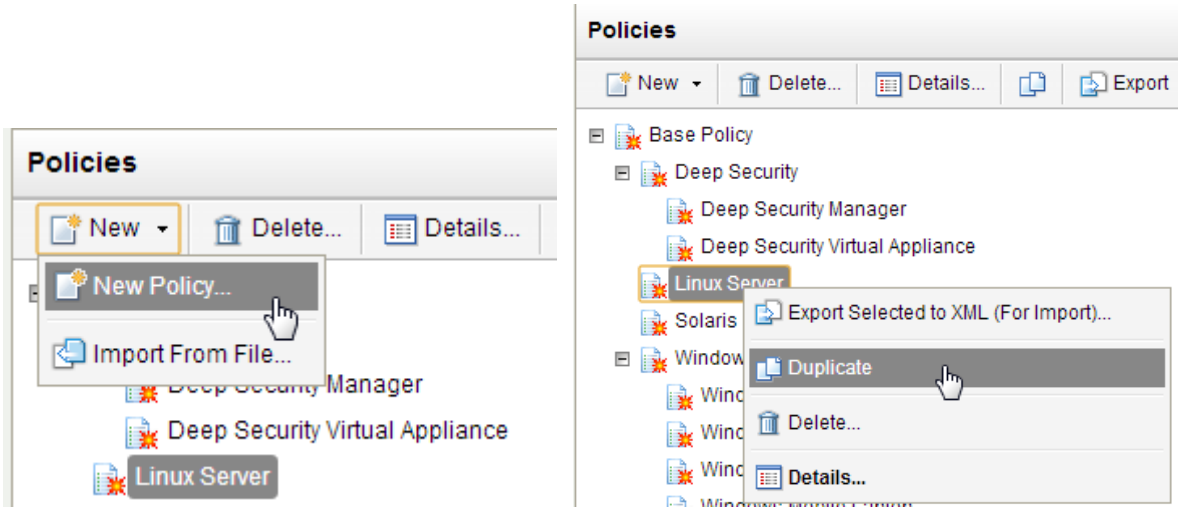
Policies

정책 템플릿을 만들고 각 보안 기능의 룰 적용 및 조회할 수 있습니다.

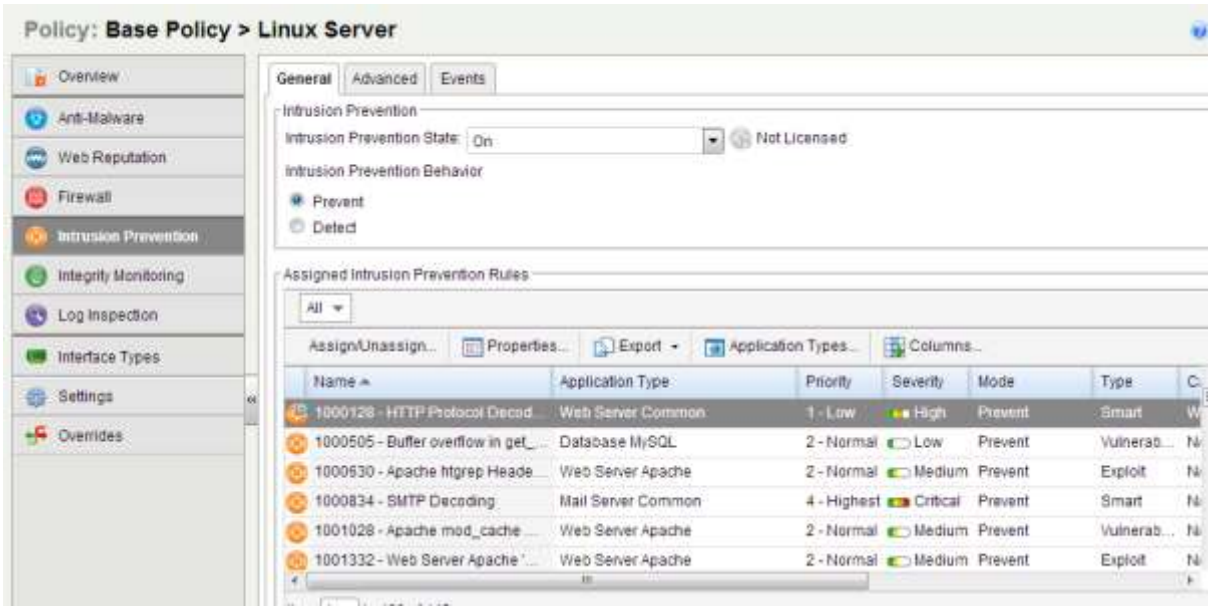
- 정책 조회 화면 입니다.



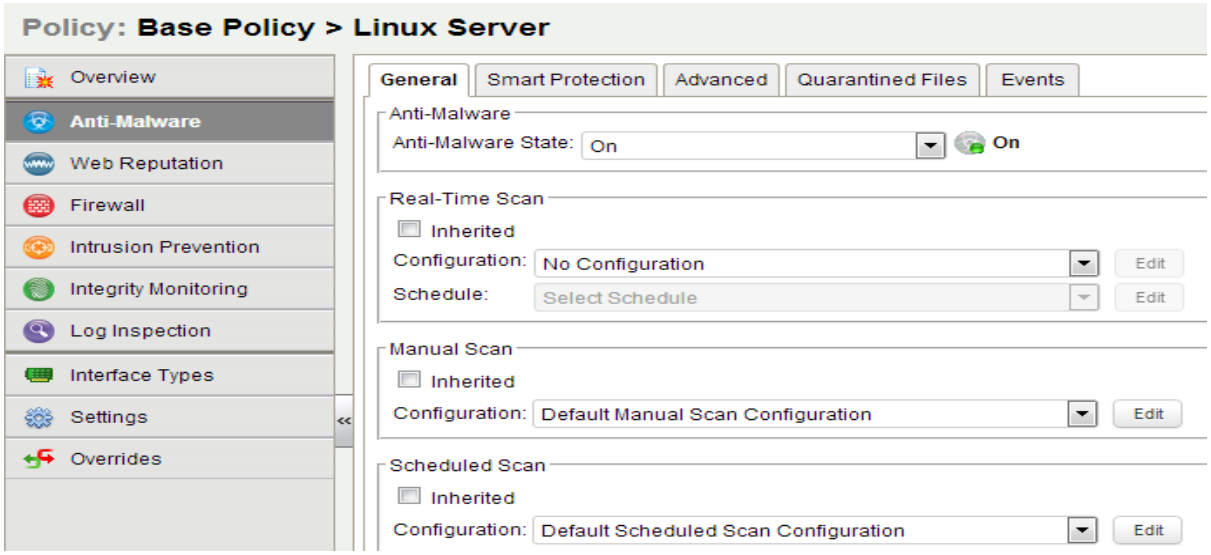
- 기본적으로 OS별 정책 템플릿을 제공하고 있으며 추가 생성/변경 가능 합니다.



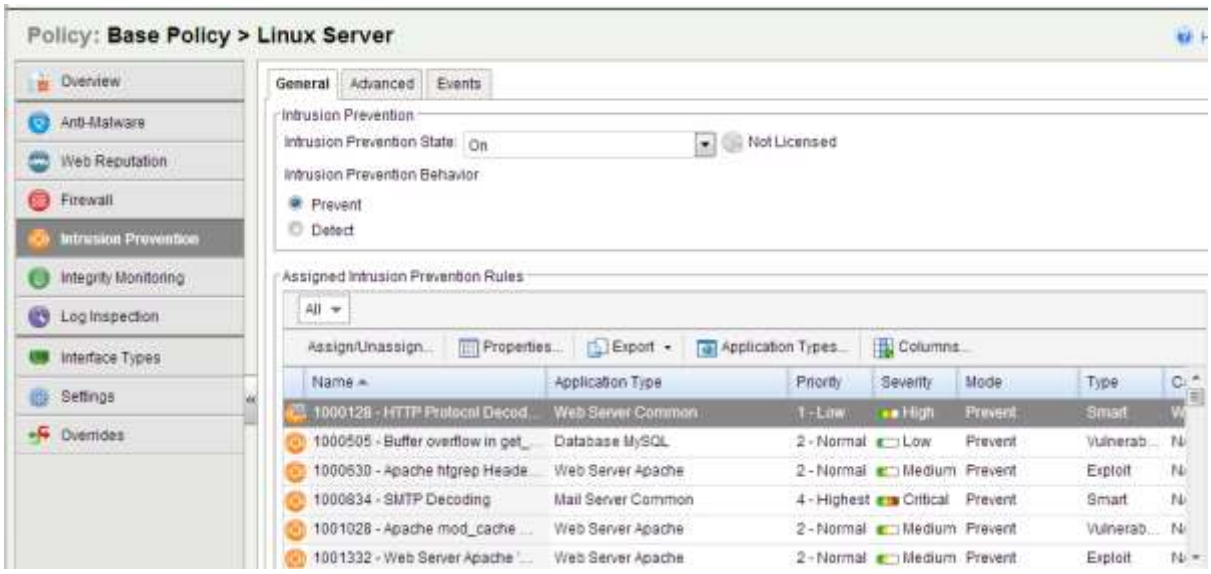
- 각 정책 템플릿에서 각 보안기능에 대한 상세 설정이 가능합니다.



- Anti-Malware 기능 설정 화면이며, "ON / OFF", "실시간 / 수동 / 예약 검사 설정", "검사 예외 처리", "격리 파일 처리" 등이 가능 합니다.



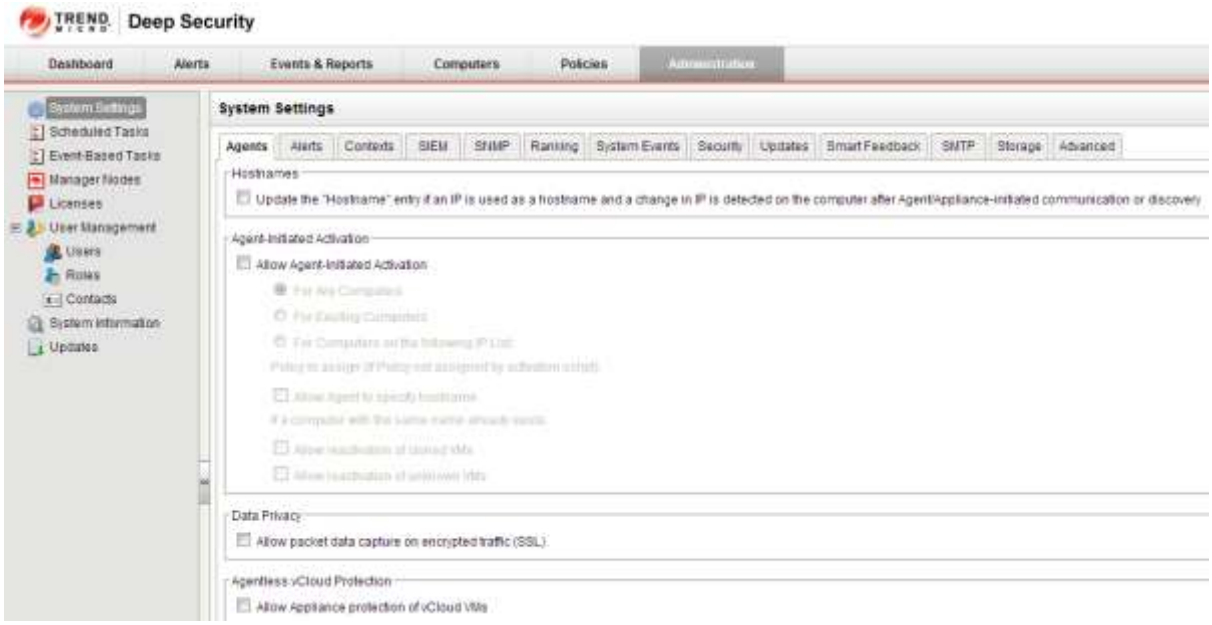
- DPI 기능 설정 화면이며, "차단 / 탐지 모드 설정", "ON / OFF", "룰 선택 / 제외 처리 설정", "새 룰 작성" 등이 가능합니다.



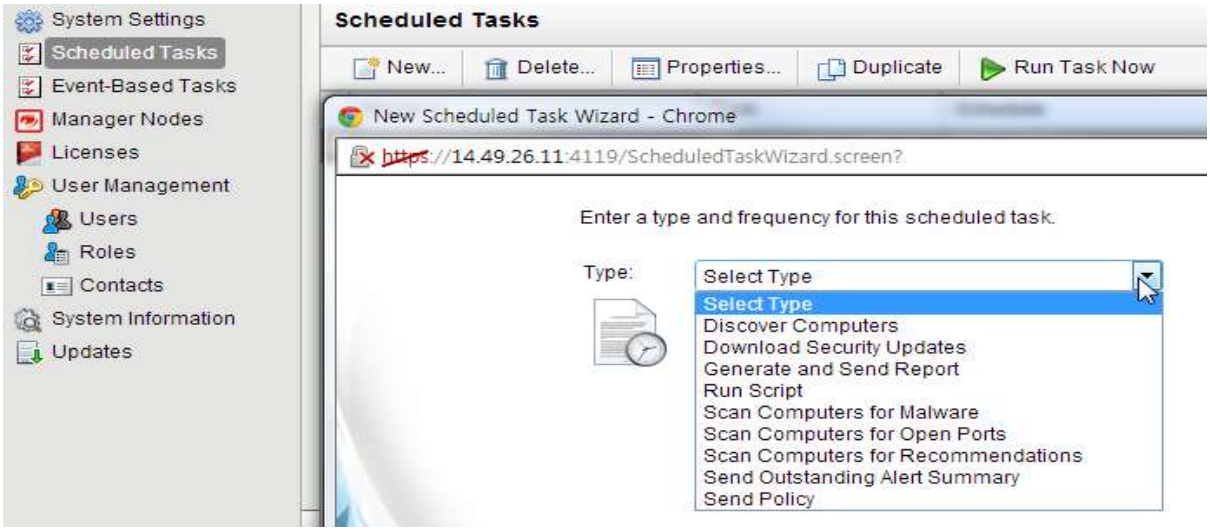
Administration

보안 정책 설정외 운영/관리에 필요한 다양한 설정을 하실 수 있습니다.

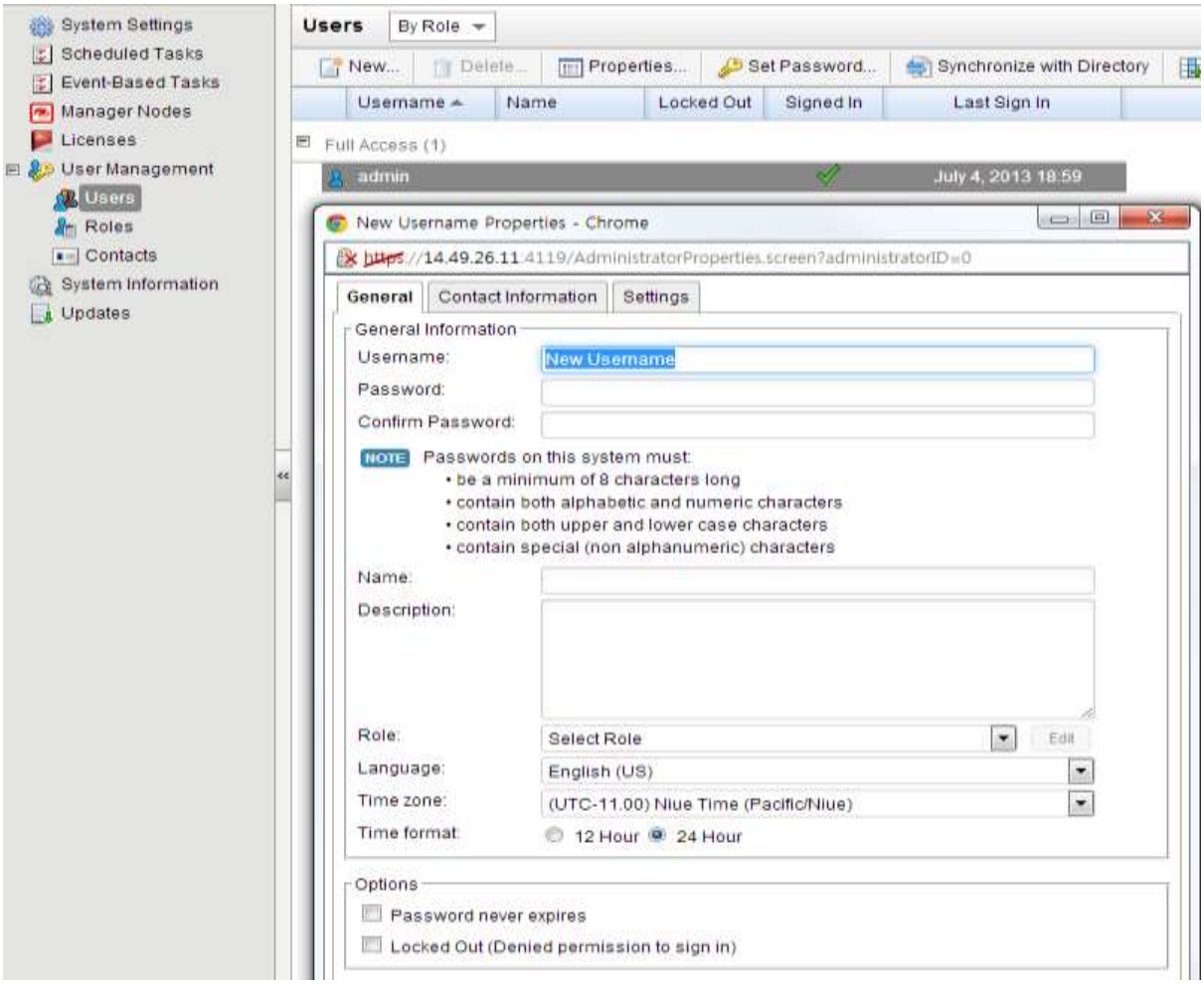
- System Settings에서는 Deep Security Agent / Manager에 대한 다양한 운영 설정을 하실 수 있습니다. SIEM(관제 포탈) 연동 설정, Agent와의 통신 설정, SNMP 설정, 패턴/룰 업데이트 설정, SMTP 설정, Log Maintenance 설정 등이 가능합니다.



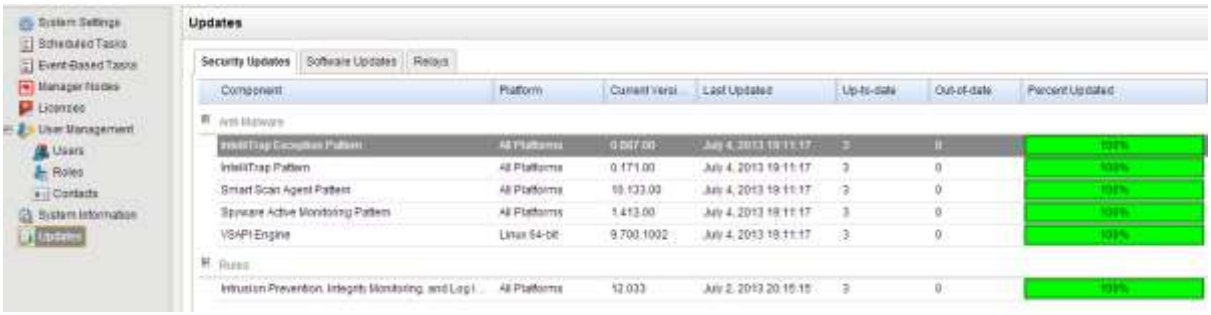
- Scheduled Tasks에서 여러가지 작업들을 예약 설정을 하여 자동화 할 수 있습니다.



- User Management에서 Deep Security Manager 콘솔에 접속하는 계정을 추가로 생성할 수 있습니다. 각 계정에는 권한을 다양하게 분류하여 운영을 분산 관리 하실 수 있습니다.



- Update 메뉴에서는 각 보안 기능이 제공하는 패턴/룰에 대한 최신 업데이트 상태와 수동으로 업데이트 수행할 수 있도록 합니다.



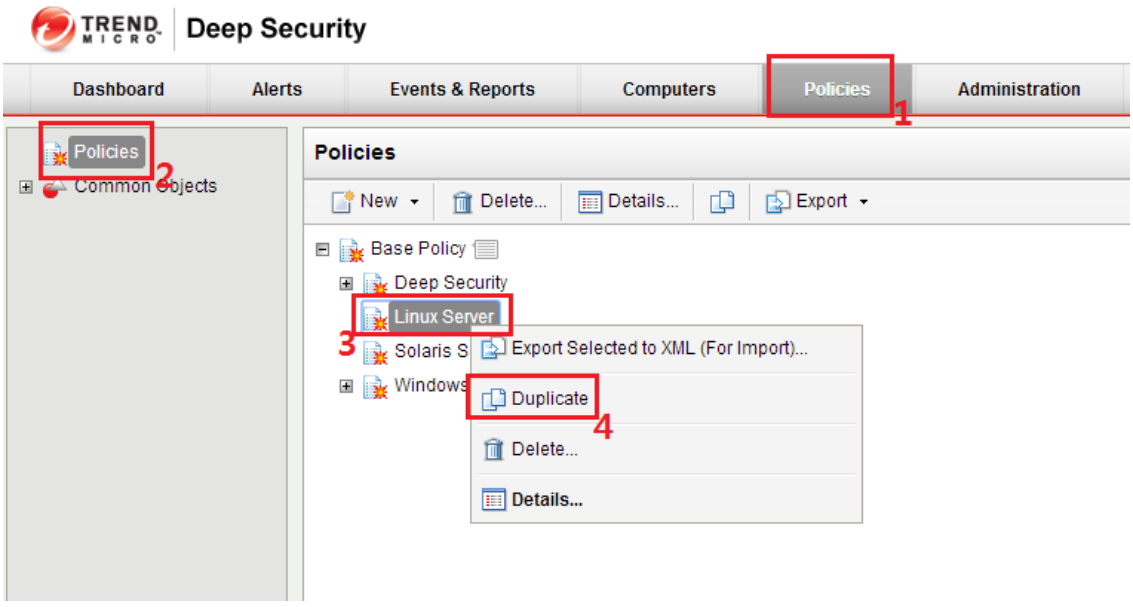
Deep Security 운영 따라하기

정책 설정 및 적용(Recommendation Scan)

: DSA가 설치되어 있고, Activation 까지 된 CentOS 6에 정책을 설정하는 하나의 예 입니다. 다른 OS도 이와 같은 방식으로 하시면 됩니다.

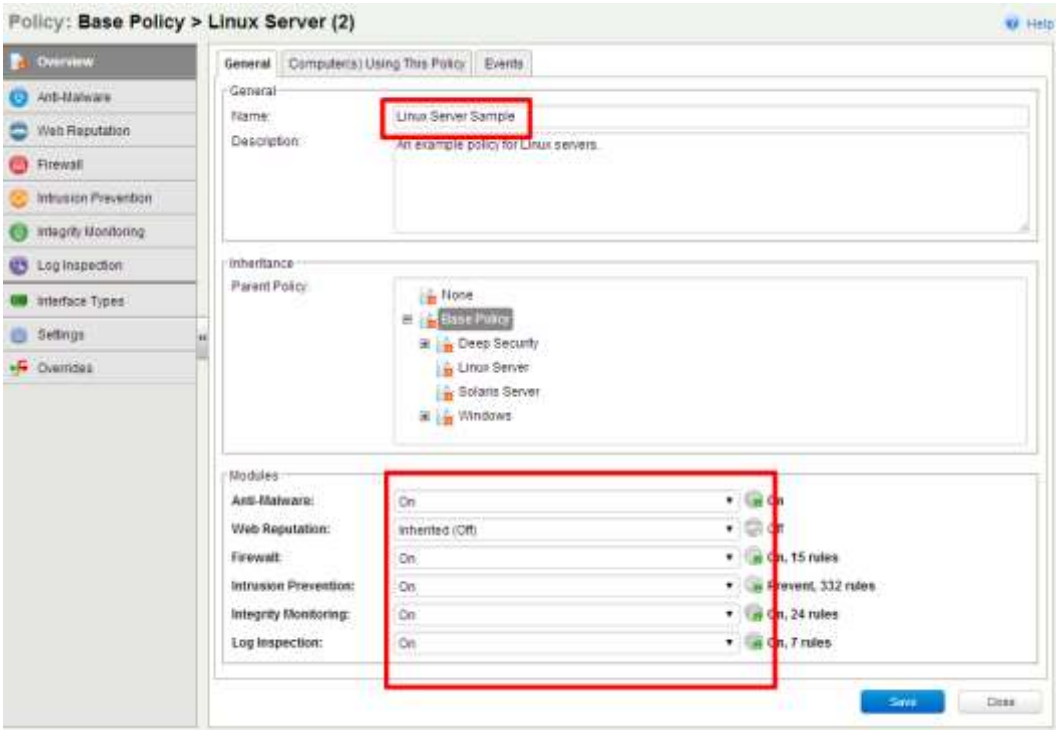
새로운 정책 만들기

- 정책을 수정하여 적용할 때, Default 정책을 바로 수정 하기보다, 이를 복사하여 새로운 정책을 만든 후 적용할 것을 추천 드리며, 이와 같은 방식으로 정책 설정하는 예를 보여 드릴 것입니다.
- "Policies" > "Policies" > "Linux Server"에서 오른쪽 마우스 클릭 > "Duplicate" 클릭



- 복사된 정책 확인. "Linux Server (2)"로 생성 되었음

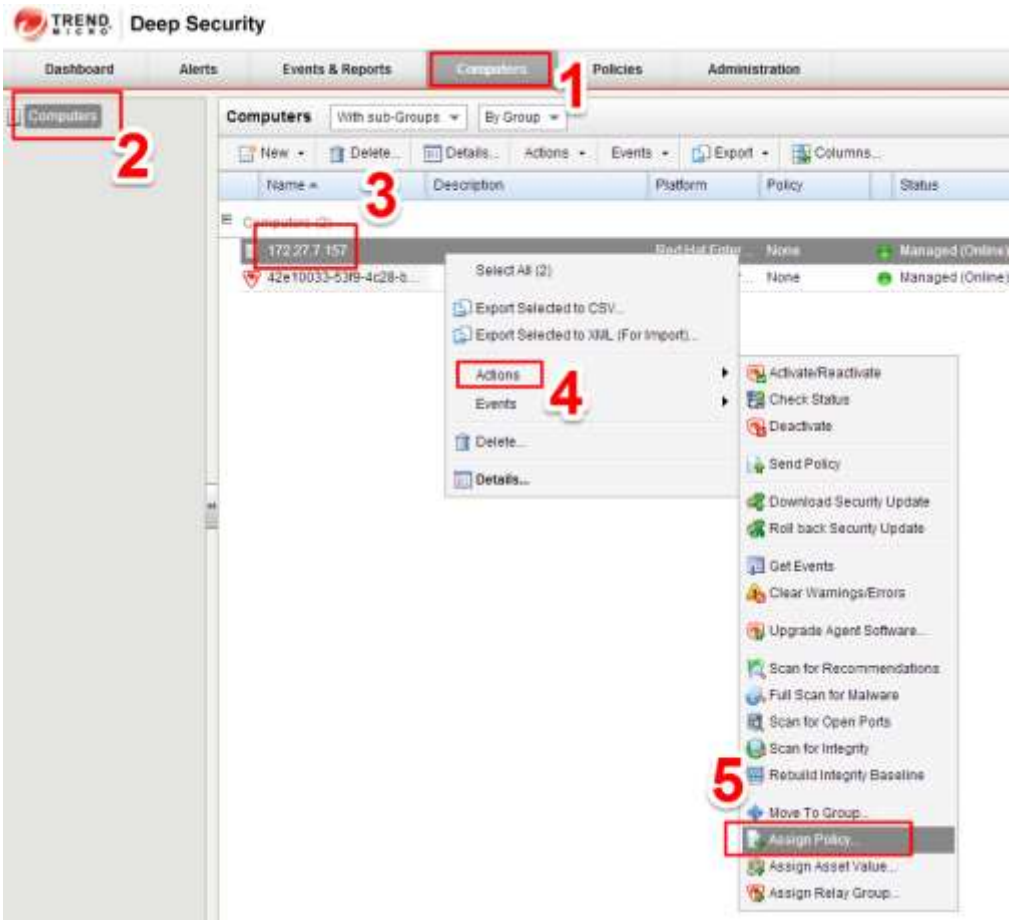
- 더블 클릭하여 팝업된 창에서, 정책 이름 설정 및 DS 의 6가지 기능 중 사용하고자 하는 기능 On 또는 Off 설정. 여기서는 Linux의 경우 지원하지 않는 Web Reputation 기능을 제외한 모든 기능을 On으로 설정



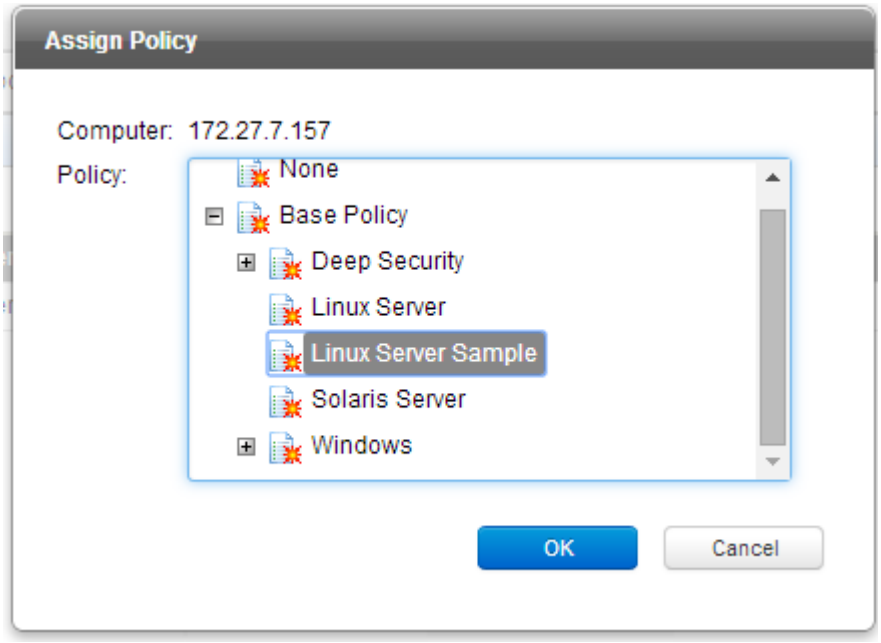
- "Save" 클릭

정책을 컴퓨터에 적용 하기

- 1:"Computers" > 2:"Computers" > 3:정책을 적용하고자 하는 Computer에 오른쪽 마우스 클릭 > 4:Actions > 5:Assign Policy 클릭



- 팝업된 메뉴에서, 위에서 새로 생성한 정책을 선택 후 "OK" 클릭

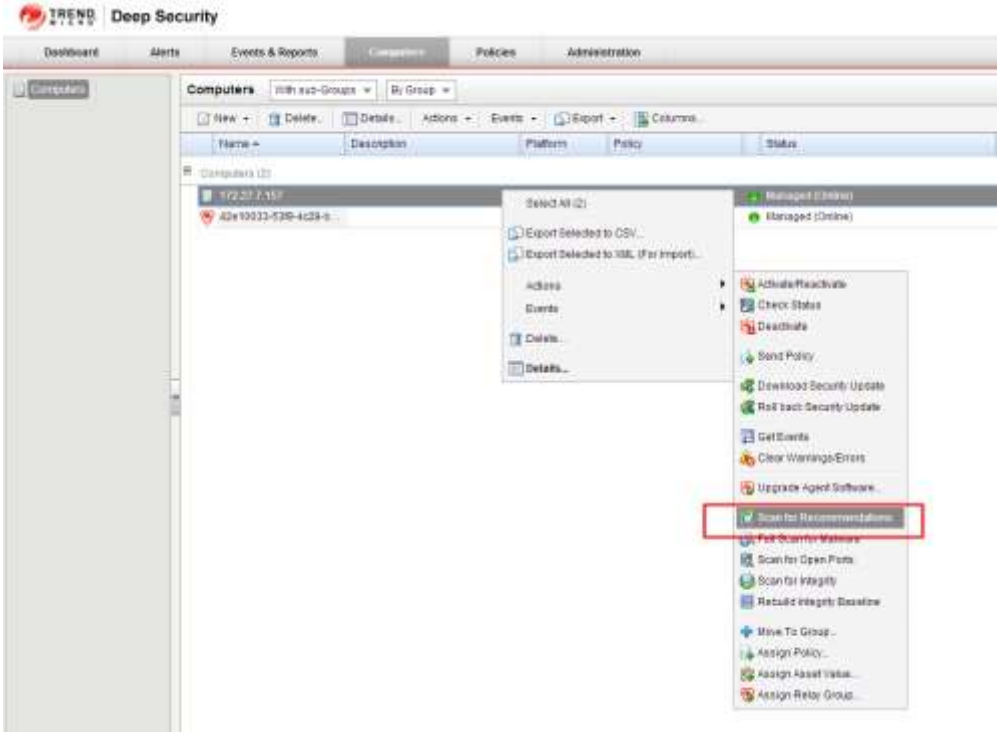


- Status 창을 확인하여 상태 변화 되는 것을 확인 후, "Managed (Online)" 상태가 되는지 확인. "Log Inspection Rules Require Log files" 상태가 된다면, 아래 자주하는 질문에서 "Log Inspection Rules Require Log File" 해결 방법 확인 하세요.

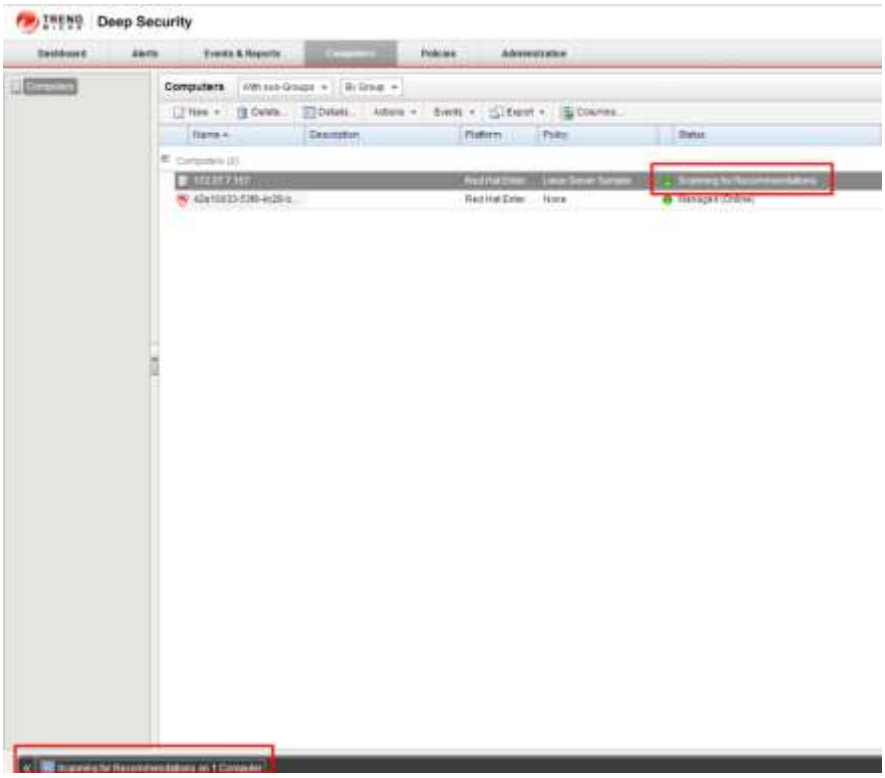
Recommendation Scan 설정 및 적용 하기

- Intrusion Prevention, Integrity monitoring, Log inspection 기능은, Recommendation Scan을 통해 룰 설정이 가능하며 적용하는 예를 아래와 같이 진행할 하겠습니다.

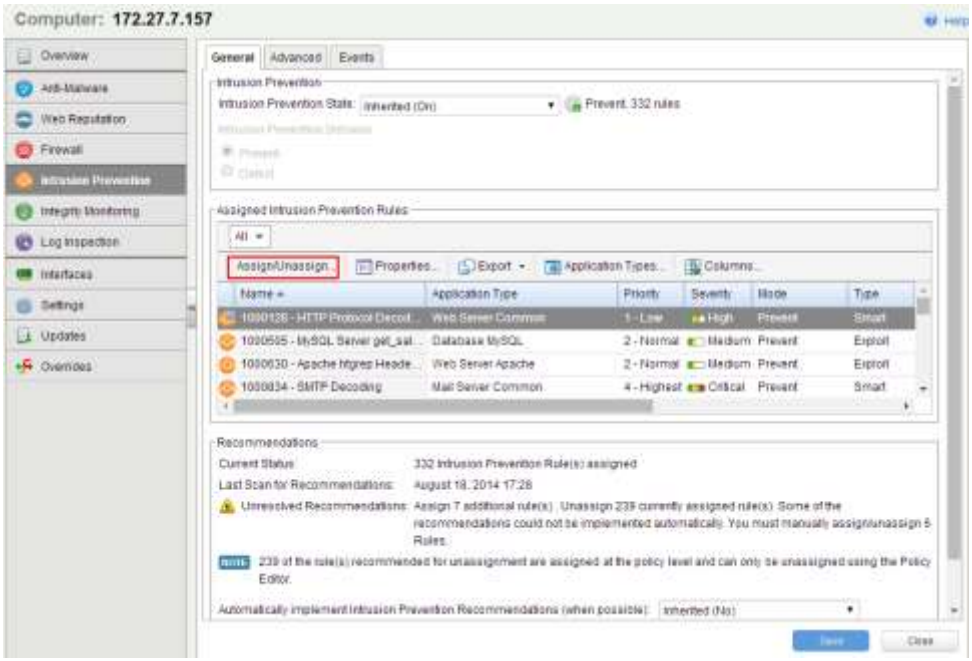
- "Computers" 탭에서 Recommendation Scan을 하고자 하는 Computer에 오른쪽 마우스 클릭하여 Recommendation Scan 실시



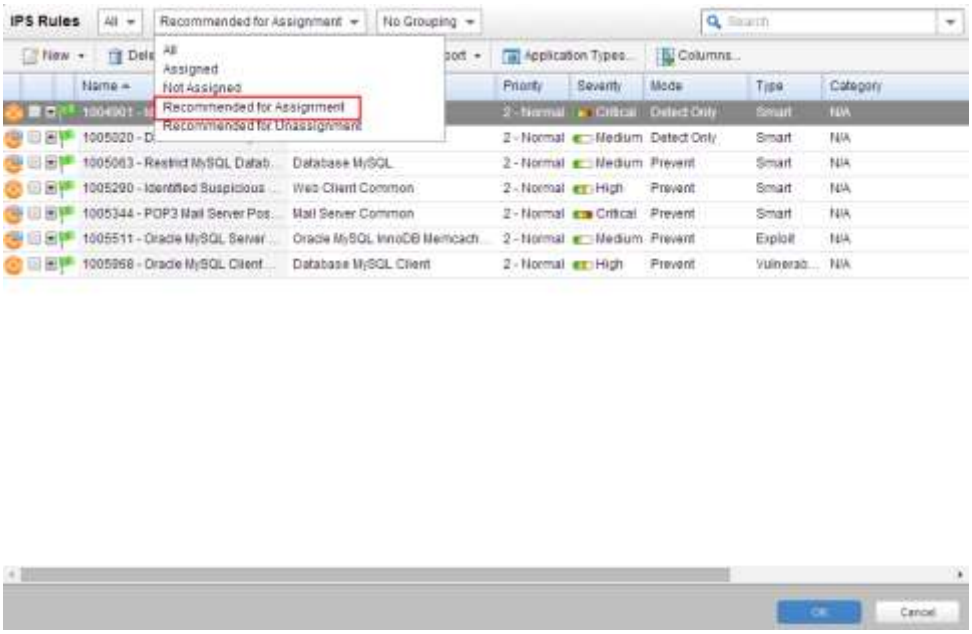
- 상태 창을 확인하여 진행 상태 확인.



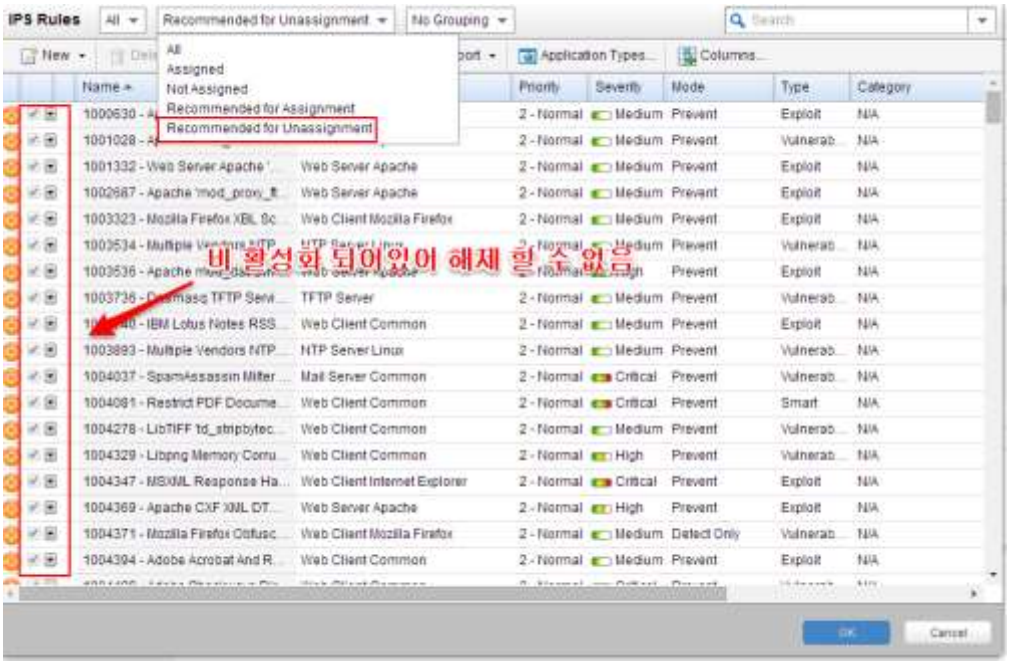
- 종료가 되면 상태가 "Managed (Online)"로 돌아오면, Computer를 더블 클릭 하여 상세 화면으로 이동 > 왼쪽 패널에서 "Intrusion Prevention" 클릭 > "Assign/Unassign" 클릭



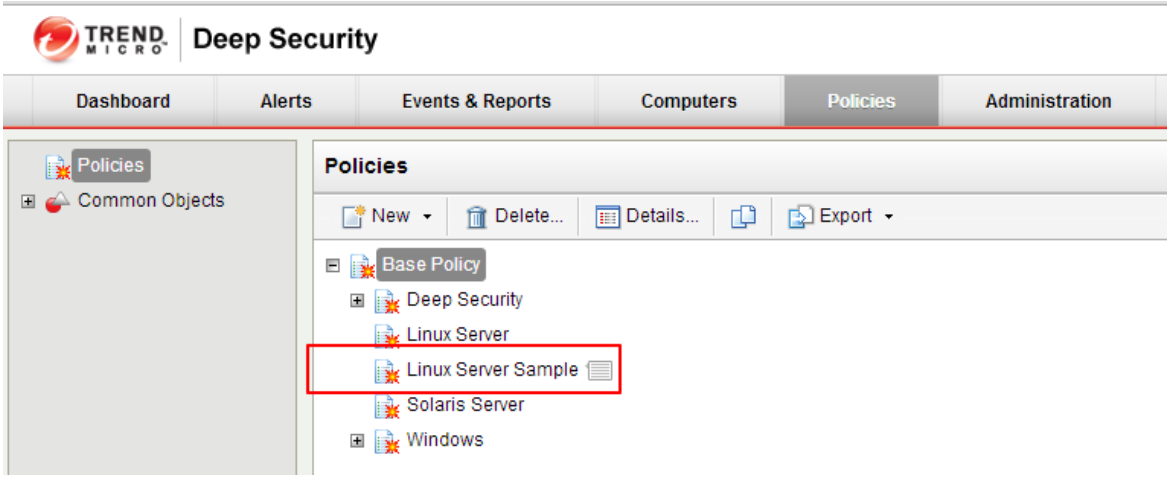
- 상단의 Recommened for Assignment 클릭하여 Assign 할 것으로 추천된 룰을 확인 후, 체크박스를 클릭후, OK버튼을 클릭하여 룰 설정.



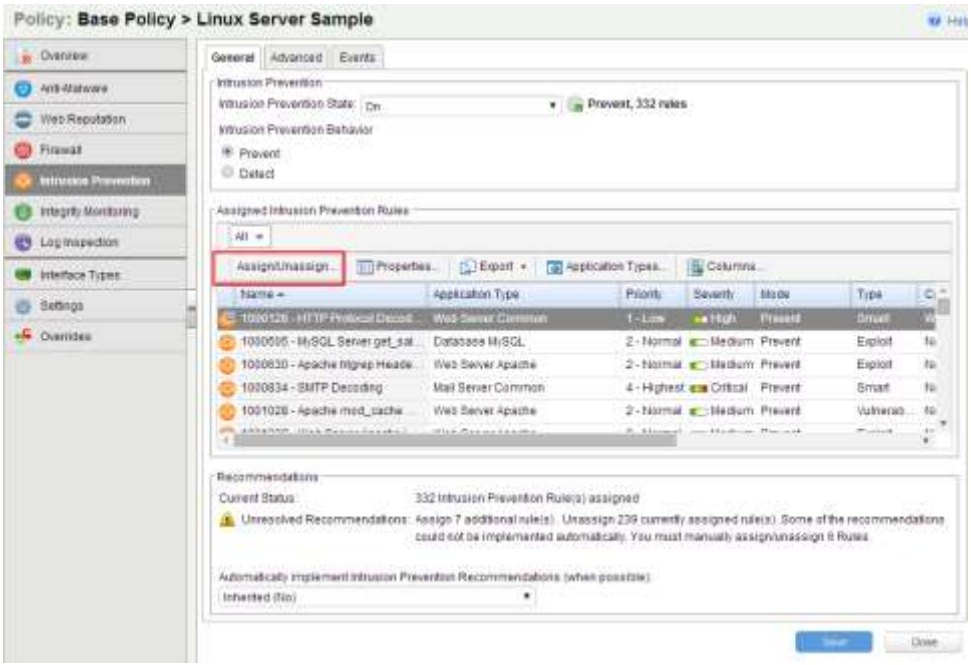
- 다시 "Assign/Unassign" 클릭 후, 나오는 팝업 창에서 이번에는 상단의 리스트 박스에서 "Recommended for Unassignment" 클릭. 룰의 가장 앞의 체크 박스를 클릭하여 룰 선택을 해제 해야 하는 데 비활성화 되어 있어서 해제 할 수 없다. 정책 레벨에서 적용된 룰을 컴퓨터 레벨에서 해제할 수 없기 때문이다.



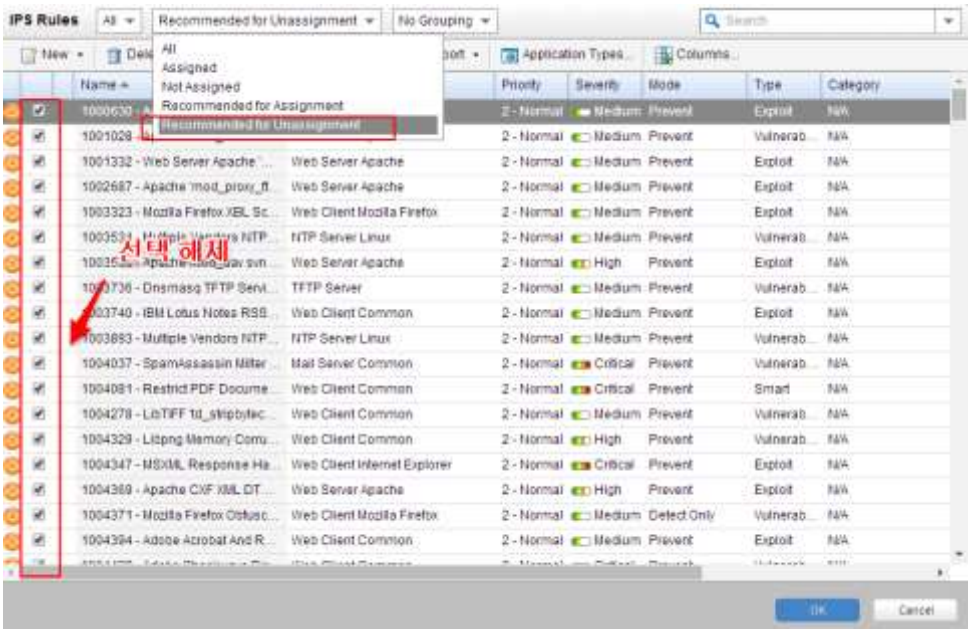
- Unassignment 추천된 룰을 해제하기 위해, 해당 컴퓨터에 적용된 Policy 더블 클릭



- 팝업된 상세 화면에서 왼쪽 패널의 "Intrusion Prevention" 클릭 > "Assign/Unassign" 클릭



- 상단의 리스트 박스에서 "Recommended for Unassignment" 클릭하여 나오는 룰들의 체크박스 해제 및 "OK" 버튼 을 클릭하여 Unassignment 작업 완료. 참고 사항으로, 지금의 정책 레벨에서 룰을 변경하면, 이 정책이 적용된 모든 컴퓨터에 변화 사항이 적용 됨.



Anti-malware 설정하고 운영 하기(예외처리)

Exclusion 설정을 제외한 다른 설정들은 default 설정을 사용 하셔도 됩니다. 직접 튜닝을 하고 싶으시면, 위의 "제품 개요 > 참고 매뉴얼 및 사이트" 를 참고하세요.

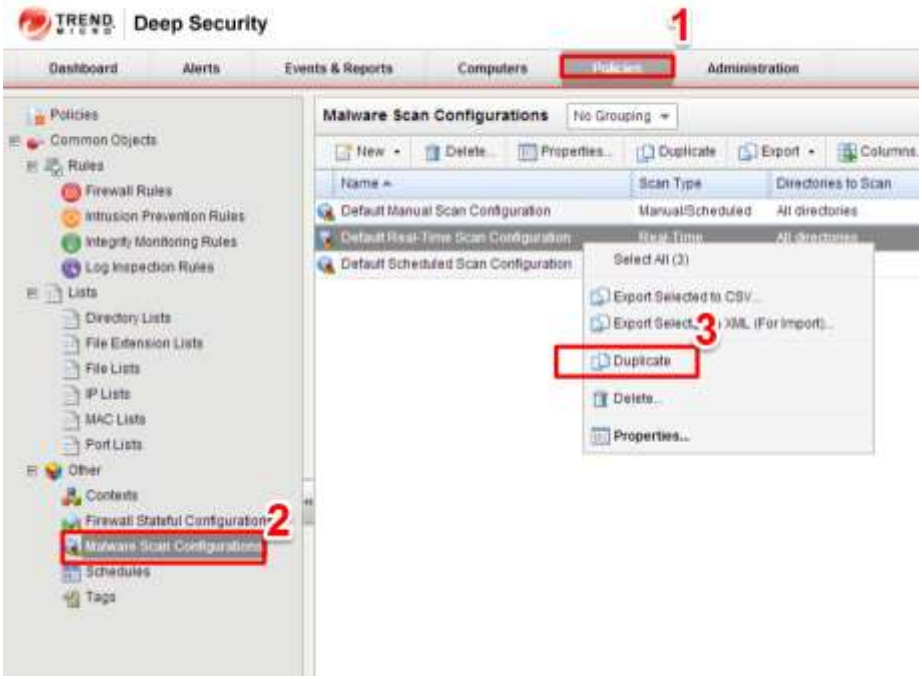
서버에서 Exclusion 설정은 서비스의 특성에 맞게 꼭 해주셔야 합니다. 변화가 많은 로그 파일이나 디비파일을 Anti-malware 모듈이 스캔을 하다 서비스에 영향을 미치는 경우가 있기 때문 입니다. 서비스 별로 Exclusion해야할 리스트는 아래의 사이트를 참고하세요. 아래의 링크에 정보가 없다면, 해당 솔루션 회사에 Anti-malware 솔루션 대비하여 예외 처리해야 하는 부분이 어디인지 문의 하세요.

http://esupport.trendmicro.com/solution/en-us/1059770.aspx?referral=1059795

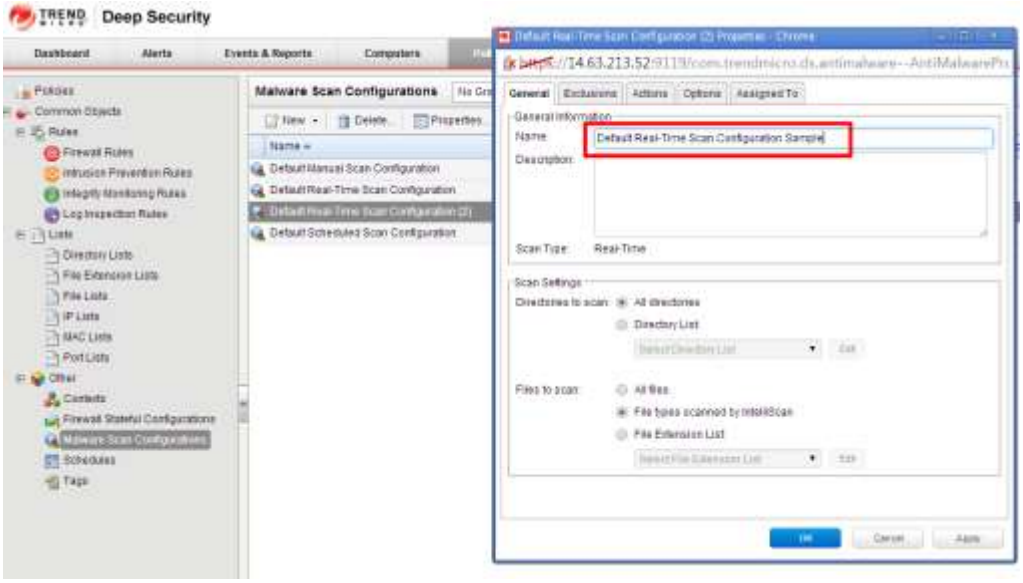
그래서 여기서는 Exclusion 설정을 하는 하나의 예를 보여 드리겠습니다.

신규 Malware Scan Configuration objects 생성

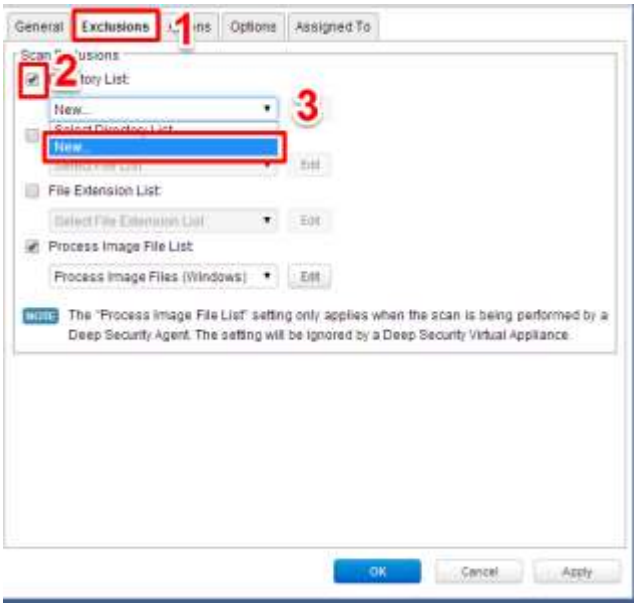
- 1:"Policies" > 2:"Malware Scan" > 3:"Default Real-Time Scan Configuration"에서 오른쪽 마우스 클릭 하여 "Duplicate" 클릭



- 새로 생성된 object인 "Default Real-Time Scan Configuration (2)"을 클릭하여 상세 페이지 팝업 시킨 후 이름 변경.

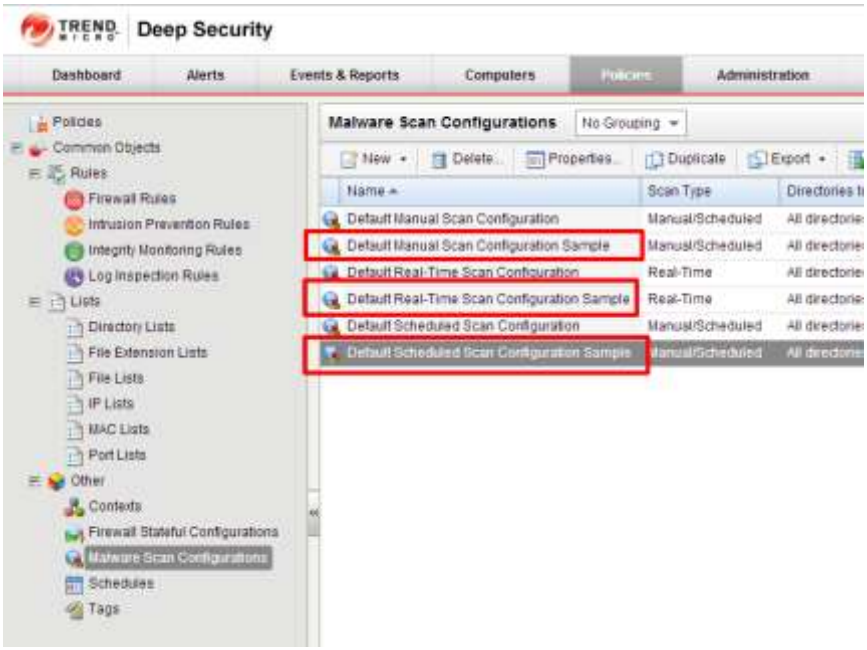


- Exclusions 탭을 클릭 하고, Directory를 예외 처리 하기 위해, 체크박스 체크. 리스트 박스를 클릭하여 "New" 선택.



- Directory 리스트 이름을 입력 하고, 아래의 "Supported Formats"를 참고 하여 예외처리 할 디렉토리 추가. "OK" 클릭하여 저장.(File 과 File Extention도 위와 같이 수행)

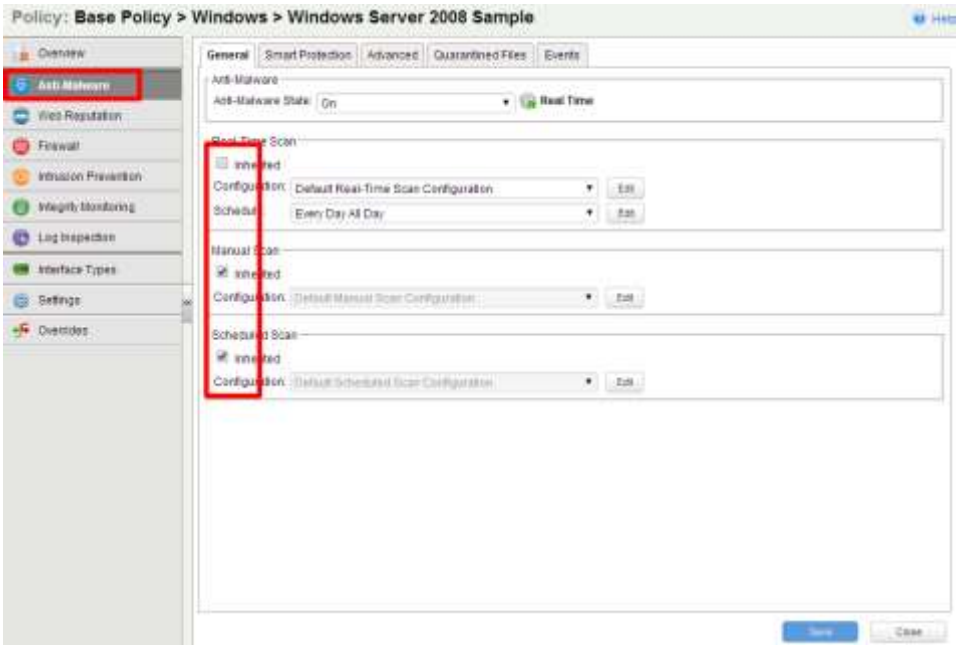
- 위와 같은 방법으로, "Default Manual Scan Configuration" 과 "Default Scheduled Scan Configuration"에 대해서도 수행



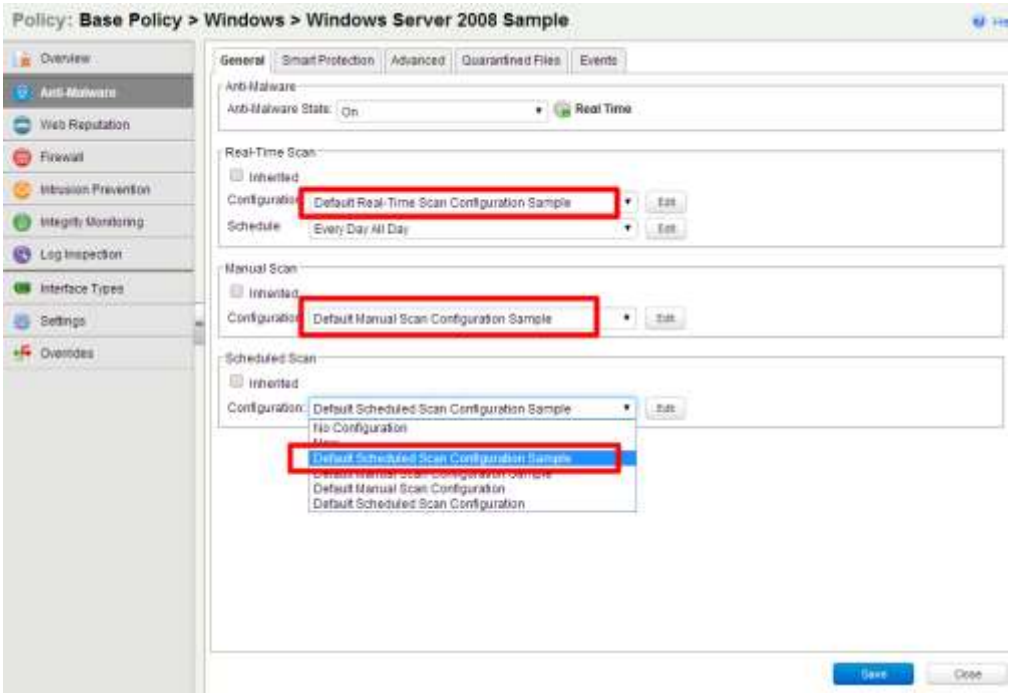
신규 생성된 Objects를, 예외처리를 하고자 하는 Computer에 할당 되어 있는 정책에 적용

- "Policies" > "Policies" > 예외처리를 해야할 Computer에 해당하는 Policy 더블 클릭

- 팝업된 상세페이지에서 왼쪽 패널의 Anti-malware 클릭 > "Inherited" 해제



- Real-time, Manual, Scheduled 각각의 Scan 설정에, 위에서 생성한 Object 적용 및 Save 클릭



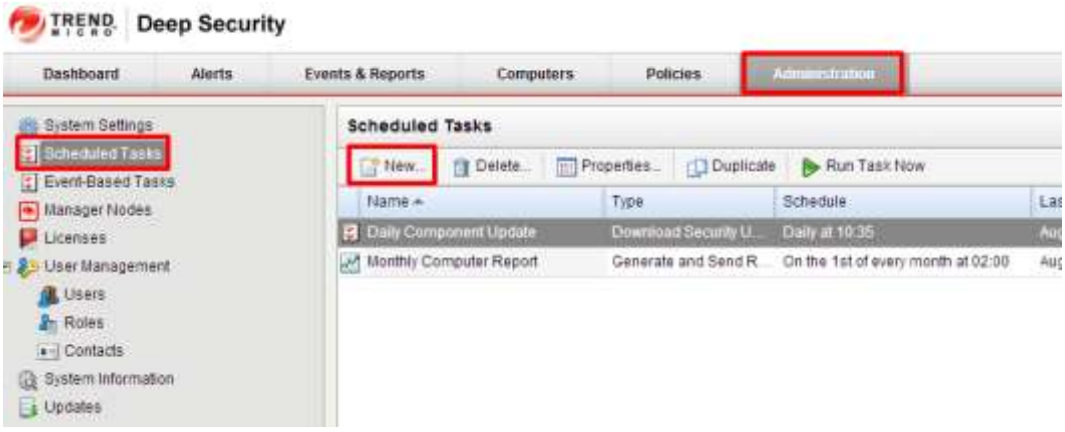
- 정책이 잘 전달 되는지 확인. 아래의 Sending Policy 가 끝난 후 Managed (Online) 상태가 되면 작업 완료

각종 Scheduled task 만들기

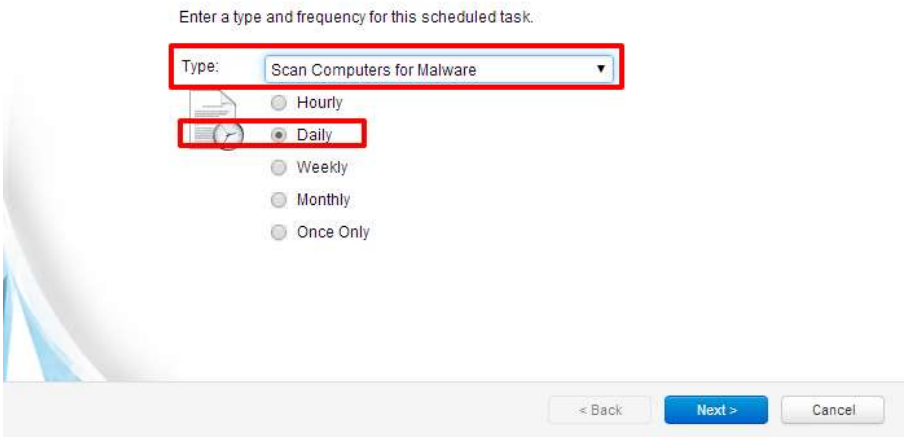
DSM에서 Anti-malware 스캔, 보안 업데이트, 리포트 발송 등의 작업을 정기적으로 할 수 있도록 지원 하고 있습니다. 몇가지 자주 사용 하는 것들을 해보겠습니다.

정기 Anti-malware 스캔 설정

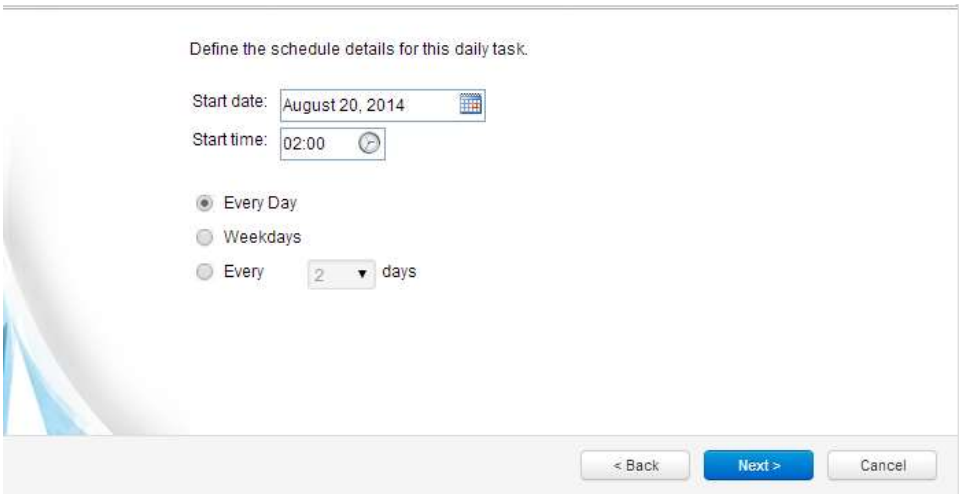
- "Administration" 탭 > "Scheduled Tasks" > "New" 버튼 클릭



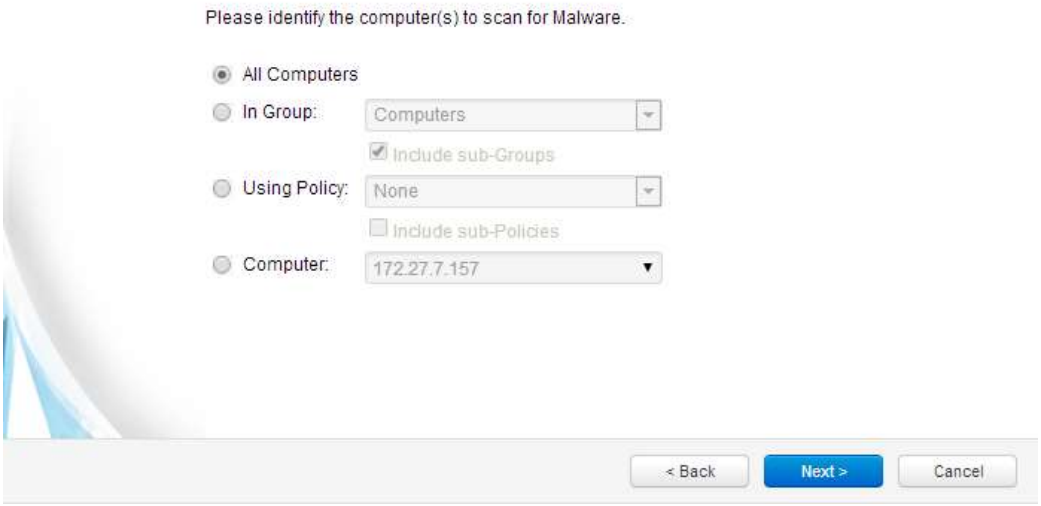
- Type과 스캔 주기 선택 후 Next



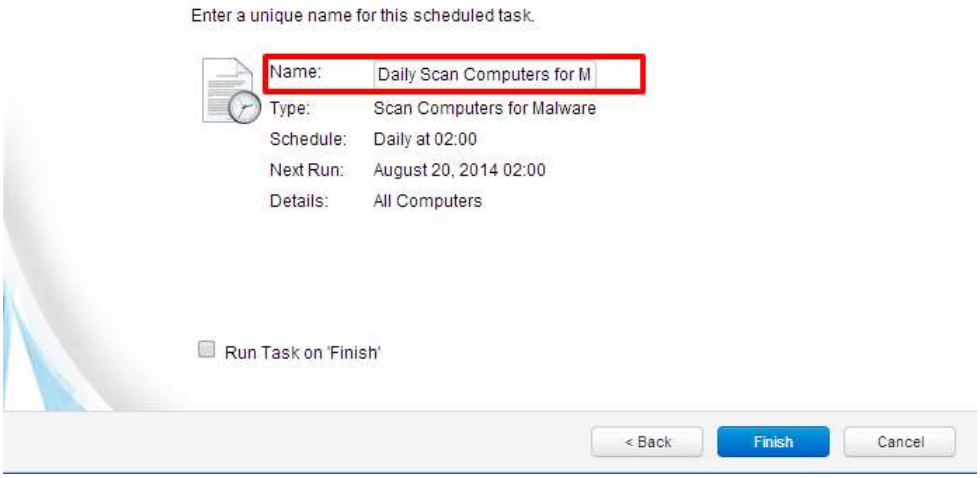
- 최초 시작 일시 및 스캔 주기 선택 후 Next. 아래의 경우 8월 20일 새벽 2시부터 시작 되며, 매일 새벽 2시에 스캔 하게 됨



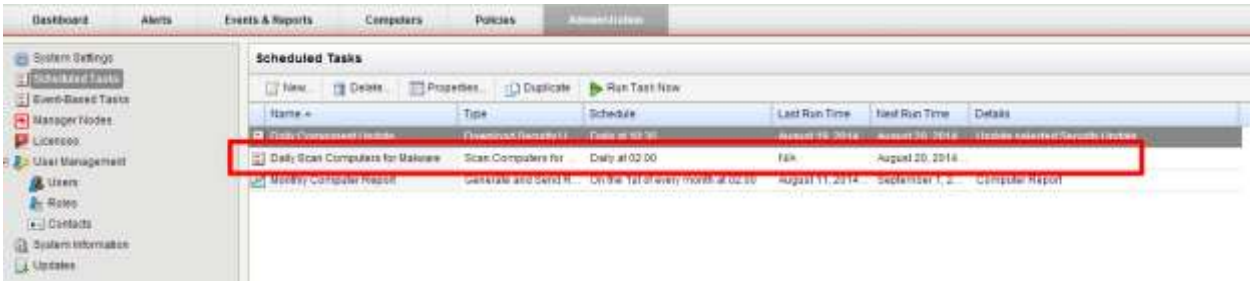
- 스캔 대상 선택 후 Next. 그룹 별, 각 컴퓨터에 할당된 정책 별, 각 컴퓨터 별로 선택 가능



- 이름 지정 및 "Finish" 클릭

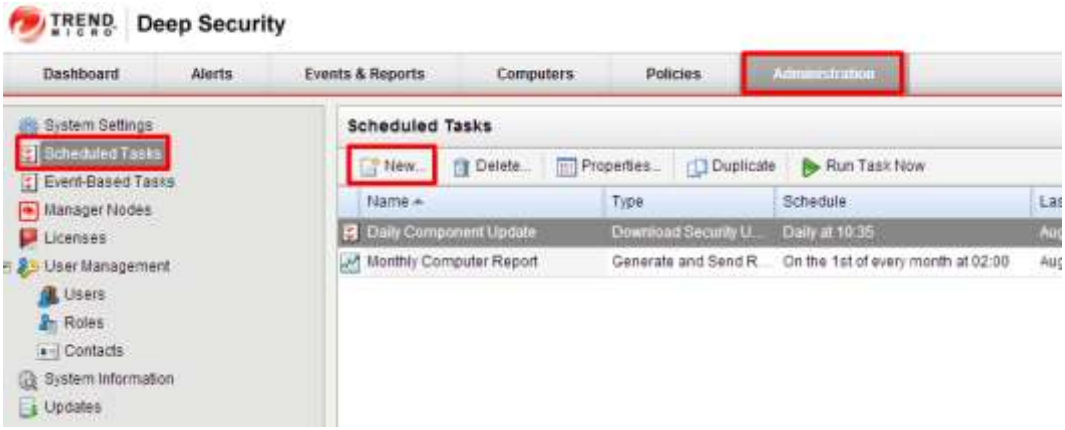


- 아래와 같이 매일 새벽 2시에 정기적으로 Malware Scan이 설정 되었음을 확인

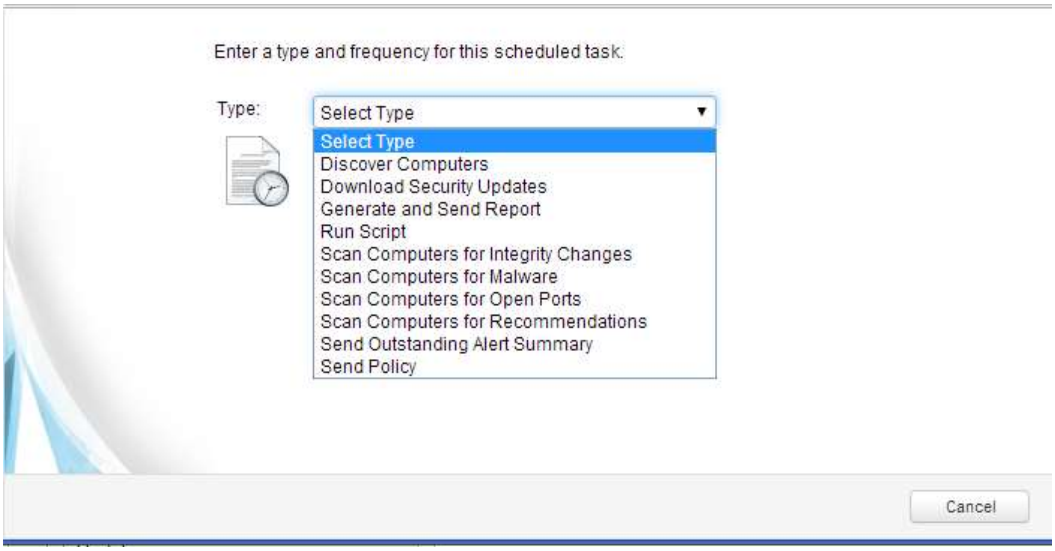


그 외의 Scheduled Task 설정

- "Administration" 탭 > "Scheduled Tasks" > "New" 버튼 클릭



- 아래와 같이 다양한 Scheduled Task 설정 가능하며, 위와 같이 직관적으로 설정할 수 있도록 쉽게 UI가 되어 있음.

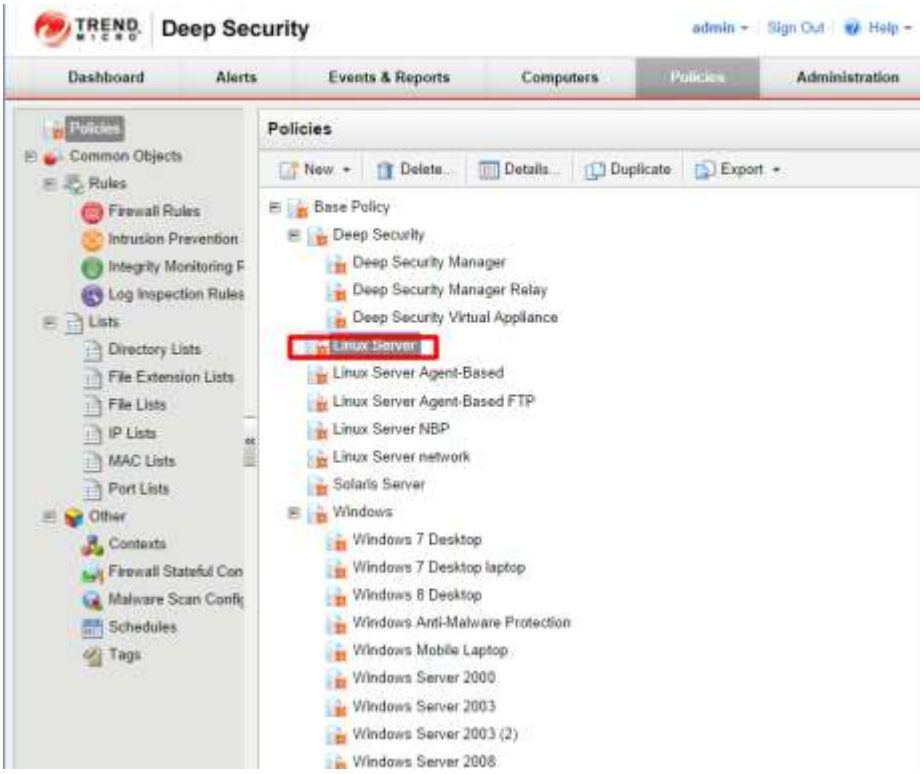


Security와 System event 전송 설정(syslog로 전송)

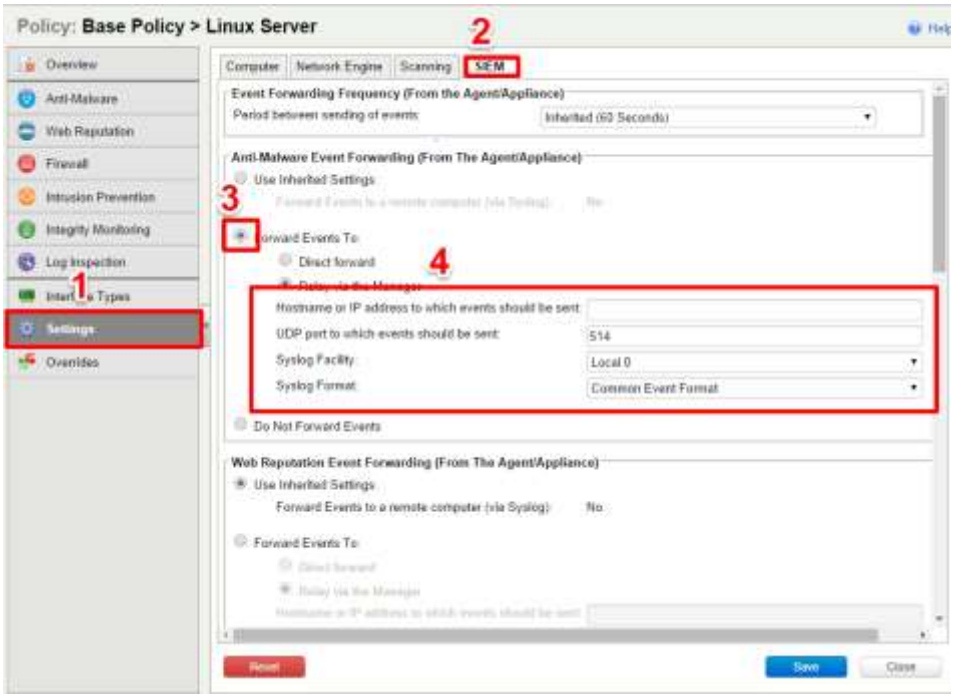
Deep Security의 Security와 System event를 syslog 타입으로 리모트에 있는 서버에 전송을 할 수 있습니다. Security Event는 Deep Security 의 6가지 기능(Anti-malware, Firewall, Web Reputation, Intrusion prevention, Integrity Monitoring, Log Inspection)에 해당하는 event를 말하며, System Event는 Deep Security를 운영 자체에 대한 정보를 말합니다. 각각의 설정을 해보겠습니다.

Security Event의 syslog로 전송 설정

- Security Event를 syslog로 전송 시키고 싶은 Computer에 적용되어 있는 정책 더블 클릭



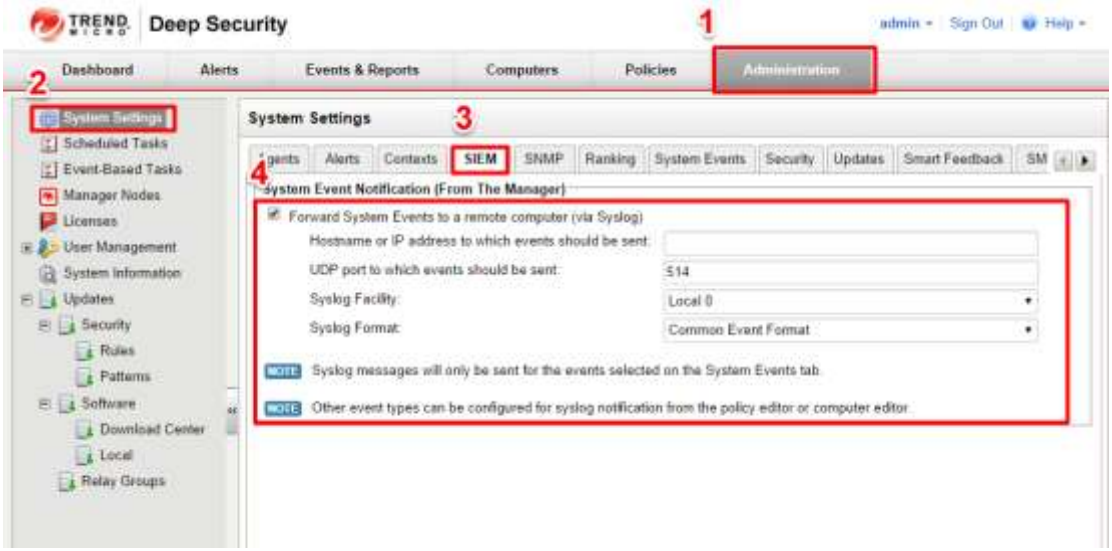
- 아래의 번호 순서로 클릭 후에, 4번에 syslog를 전송 받는 서버 정보 입력 후 "save" 클릭



- 위의 설정은 Anti-Malware Event 에 대해서만 설정이 되었음. 아래로 스크롤을 하면 Web Reputation, Firewall 등 다른 Security Event에 대해서도 위와 동일한 방법으로 설정

System Event의 syslog로 전송 설정

- 아래의 순서대로 클릭 후에, 4번 박스의 체크박스 클릭 후, syslog를 전송 받을 서버 정보 입력 후 "save"버튼 클릭

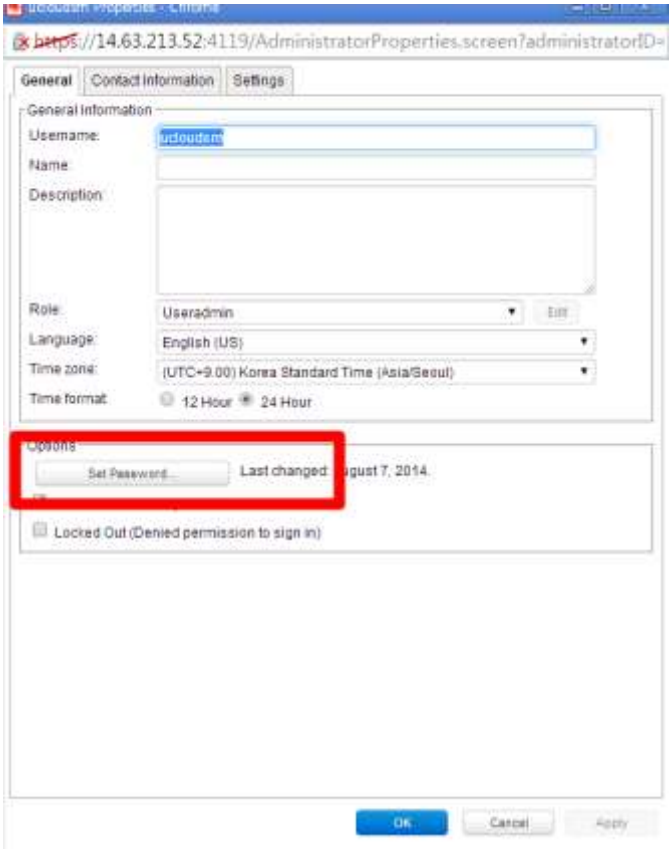


자주하는 질문(FAQ)

패스워드 변경하는 방법은?

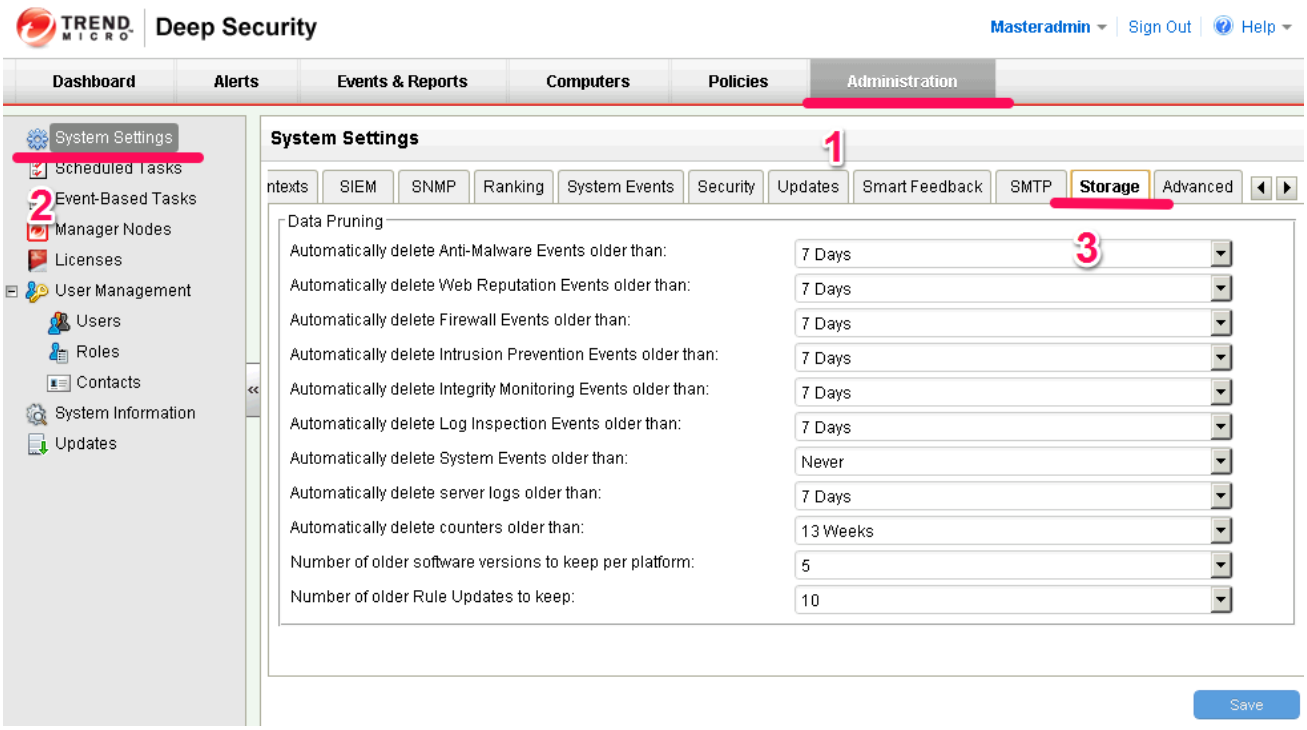
- 로그인
- "Administration" > "User management" > "Users" > 변경하고자하는 아이디 더블 클릭

- 클릭하여 나오는 팝업 창의, 하단에 "Set Password" 버튼을 클릭하여 비밀번호 변경



DSM 스토리지 관리 방법은?

- 로그인
- "Administration" > "System Settings" > "Storage" 클릭



- 각 이벤트 별로, 보유 기간을 아래의 메뉴에서 설정 가능 합니다. Firewall event 또는 사용자의 환경에 따라

로그가 많이 생기는 것들은 보유기간을 짧게 설정 하여 주세요.

DSM 서버 리부팅 하는 방법은?

DSM 서버 리부팅 시, 서버에서 DSM service를 먼저 내려 주어야 합니다. Database가 먼저 내려가면, DSM이 수령한 이벤트를 DB에 저장하지 못해, 시스템에 이슈가 생길 수 있기 때문입니다.

- SSH 로 DSM 서버에 접속 하여, 아래의 커맨드 실행
  - # service dsm_s stop

```
[root@dsm-trendmicro temp]# cd
[root@dsm-trendmicro ~]# service dsm_s status
The daemon is running.
[root@dsm-trendmicro ~]# service dsm_s stop
```

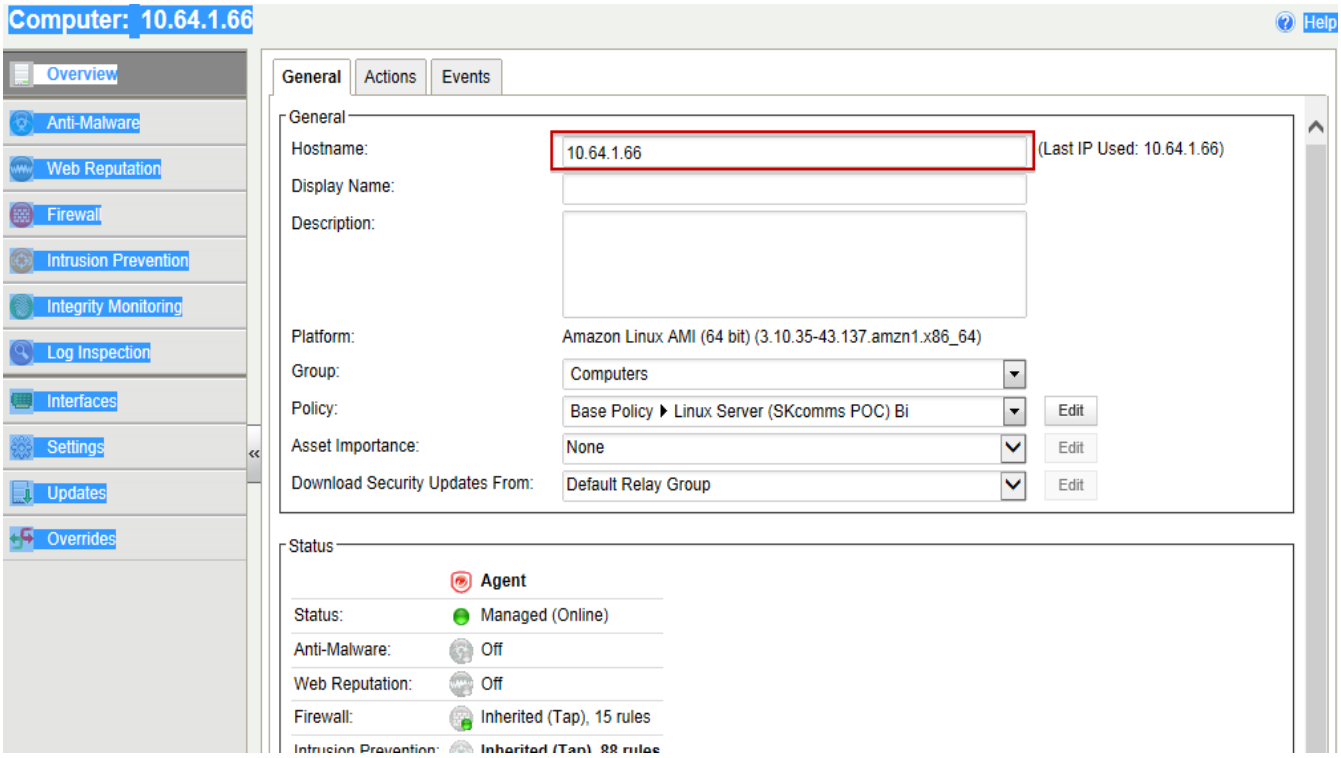
- 아래의 커맨드를 이용하여 리부팅
  - # Init 6

Amazon 환경에서 리부팅 후, 서버 IP 변경으로 인한 DSM offline 발생시 조치 방법

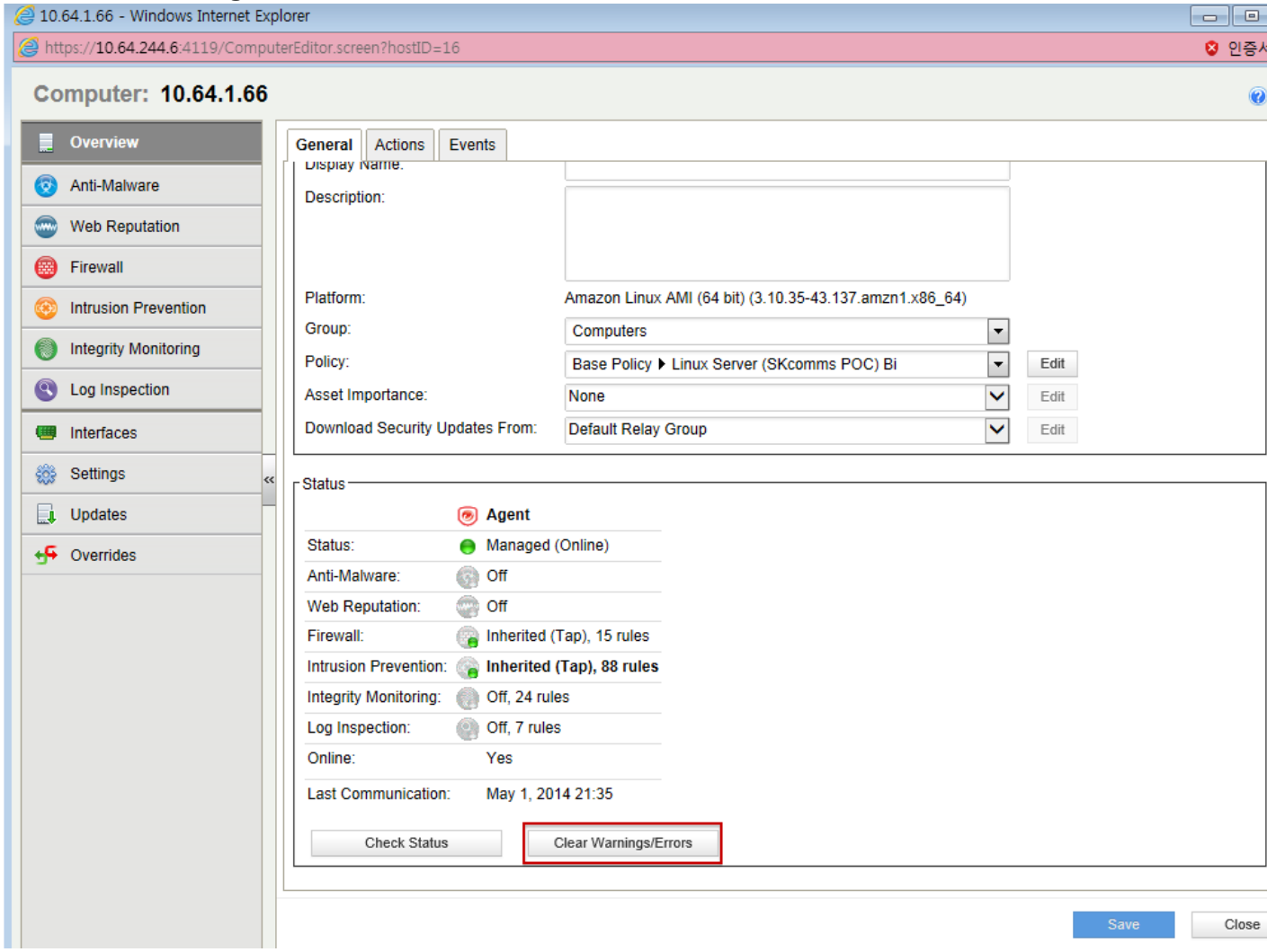
- DSA 가 설치된 서버 관련 작업
  - offline 이 발생한 해당 서버에 접속 후 루트권한 로그인
  - 아래의 커맨드를 1~2 회 실행 : Deep Security Agent 가 DSM 으로 heartbeat 하는 구문
    - #/opt/ds_agent/dsa_control –m
  - 아래와 같은 메세지가 나오면 잘 수행된 것

```
[root@static ~]# /opt/ds_agent/dsa_control -m
Sending the command to the agent on the local machine...

Manager contact has been scheduled to occur in the next few seconds.
[root@static ~]#
```

- Deep Security Manager 관련 작업
  - Deep Security Manager 로그인
  - Computer 탭에서 offline 이된 computer 더블 클릭
  - 아래의 hostname 필드의 값을 신규 IP 로 입력후, 우측 하단의 “save”버튼 클릭



- Clear Warning/Errors 클릭



- 해당 컴퓨터의 상태가 “Managed(online)”상태로 돌아오면 작업 완료

Agent offline시 조치 방법 1 (리셋 후 다시 Activation)

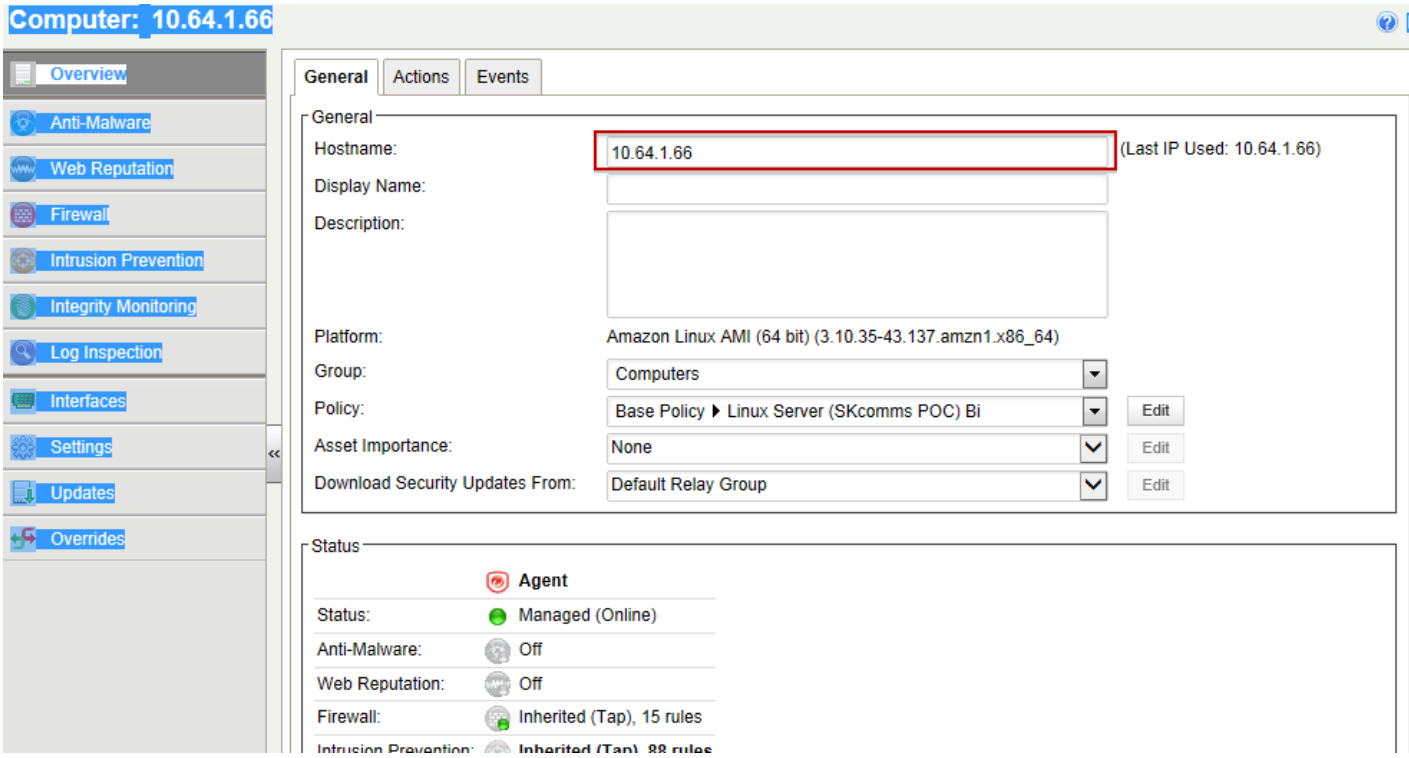
- DSA 가 설치된 서버 관련 작업
  - Offline 이 발생한 해당 서버에 접속 후 루트 권한 로그인
  - 아래의 커멘드로 DSA 리셋 실행
    - #/opt/ds_agent/dsa_control –r
  - 아래와 같은 메시지가 나오면 잘 수행 된 것

```
[root@static ~]# /opt/ds_agent/dsa_control -r
Sending the command to the agent on the local machine...

Agent reset successfully.
[root@static ~]#
```

  - 아래의 커맨드로 Deep Security Agent Activation
    - #/opt/ds_agent/dsa_control –a dsm://10.64.244.6:4120/
  - 아래와 같은 메시지가 나오면 잘 수행 된 것

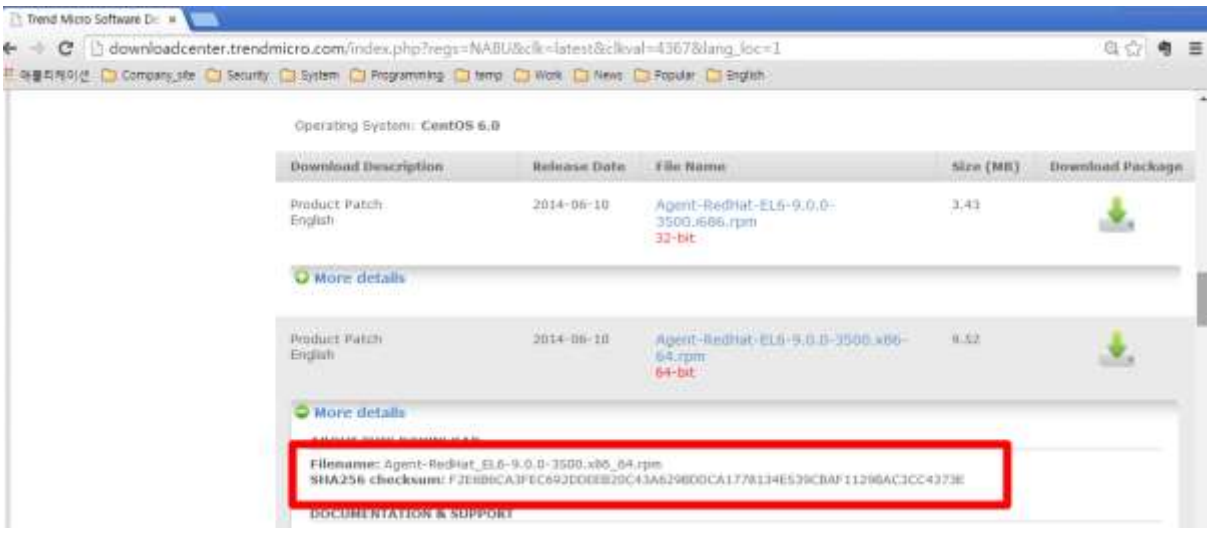
```
[root@static ~]# /opt/ds_agent/dsa_control -a dsm://22. . . . ':4:4120/
Sending the command to the agent on the local machine...

Attempting to connect to https://[redacted]:4120/
Connected successfully - attempting SSL handshake.
SSL handshake completed successfully - initiating command session.
Connected with AES256-SHA to peer at [redacted]
Received a 'GetHostInfo' command from the manager.
Received a 'GetHostInfo' command from the manager.
Received a 'SetDSMCert' command from the manager.
Received a 'SetAgentCredentials' command from the manager.
[LCA] OnActivation()
Received a 'GetAgentEvents' command from the manager.
Received a 'GetInterfaces' command from the manager.
Received a 'GetAgentEvents' command from the manager.
Received a 'GetAgentStatus' command from the manager.
Received a 'GetAgentEvents' command from the manager.
Received a 'GetComponentInfo' command from the manager.
Received a 'SetSecurityConfiguration' command from the manager.
[Log] CLogReaderThread::OnSecurityConfigurationChanged()
[LCA] CLogInspectionThread()
Received a 'GetAgentEvents' command from the manager.
Received a 'GetAgentStatus' command from the manager.
Command session completed.
[root@static ~]#
```

- Deep Security Manager 관련 작업
  - Deep Security Manager 로그인
  - Computer 탭에서 신규 생성된 computer 더블 클릭
  - 아래의 hostname 필드의 값을 신규 IP 로 입력후, 우측 하단의 “save”버튼 클릭



Agent offline시 조치 방법 2 (Agent 삭제 후, 재설치)

- 매뉴얼의 Agent 삭제방법 참고하여 삭제
- Trend Micro에서 Agent installer의 checksum 값을 확인하여 이상이 있다면 다시 설치 파일 다운로드

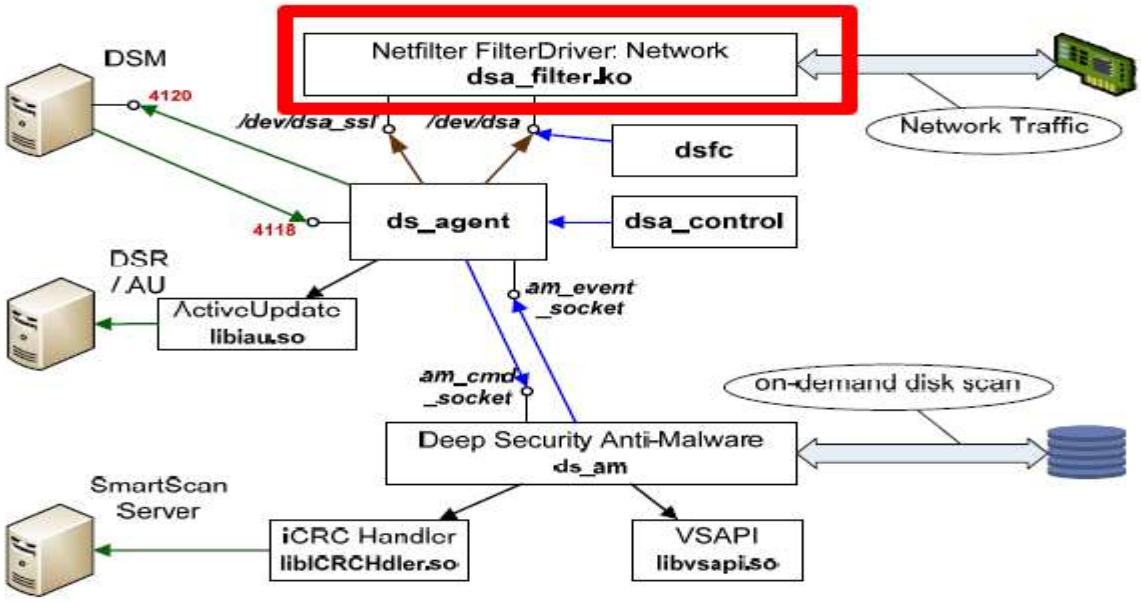


- 매뉴얼의 Agent 설치방법 참고하여 설치

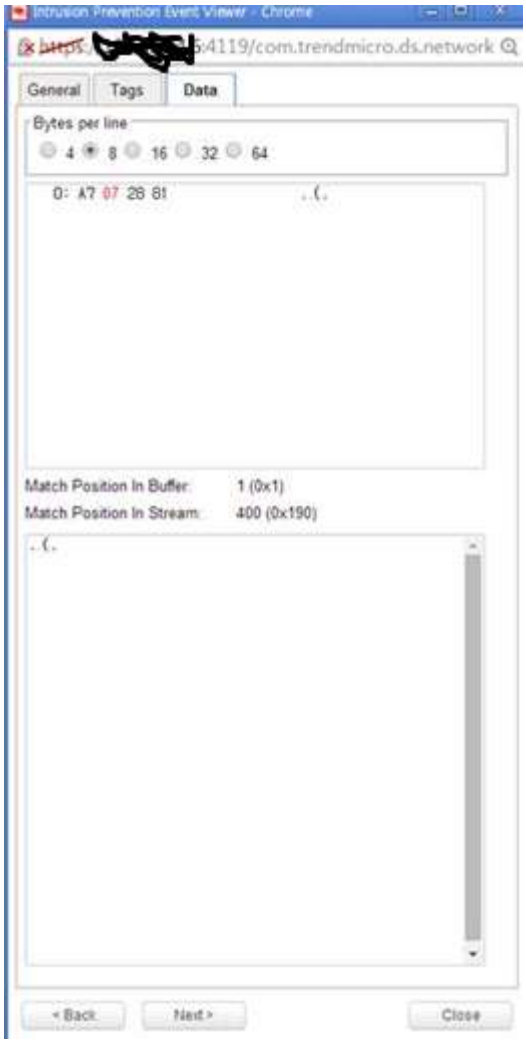
DSA가 설치 되며 네트웍이 단절 되는 현상

DSA가 설치가 되며 아래 와 같이 dsa_filter.ko 커널 모듈이 생성 되고 이 커널 모듈을 통하여 OS는 네트웍 드라이버와 통신을 하게 됩니다. 이렇게 커널 모듈이 올라오는 과정에서, 연결되어 있는 모든 커넥션이 끊어지는 순단 현

상이 발생 합니다. 리눅스의 경우 순단 현상이 1초 이내로 발생 합니다.



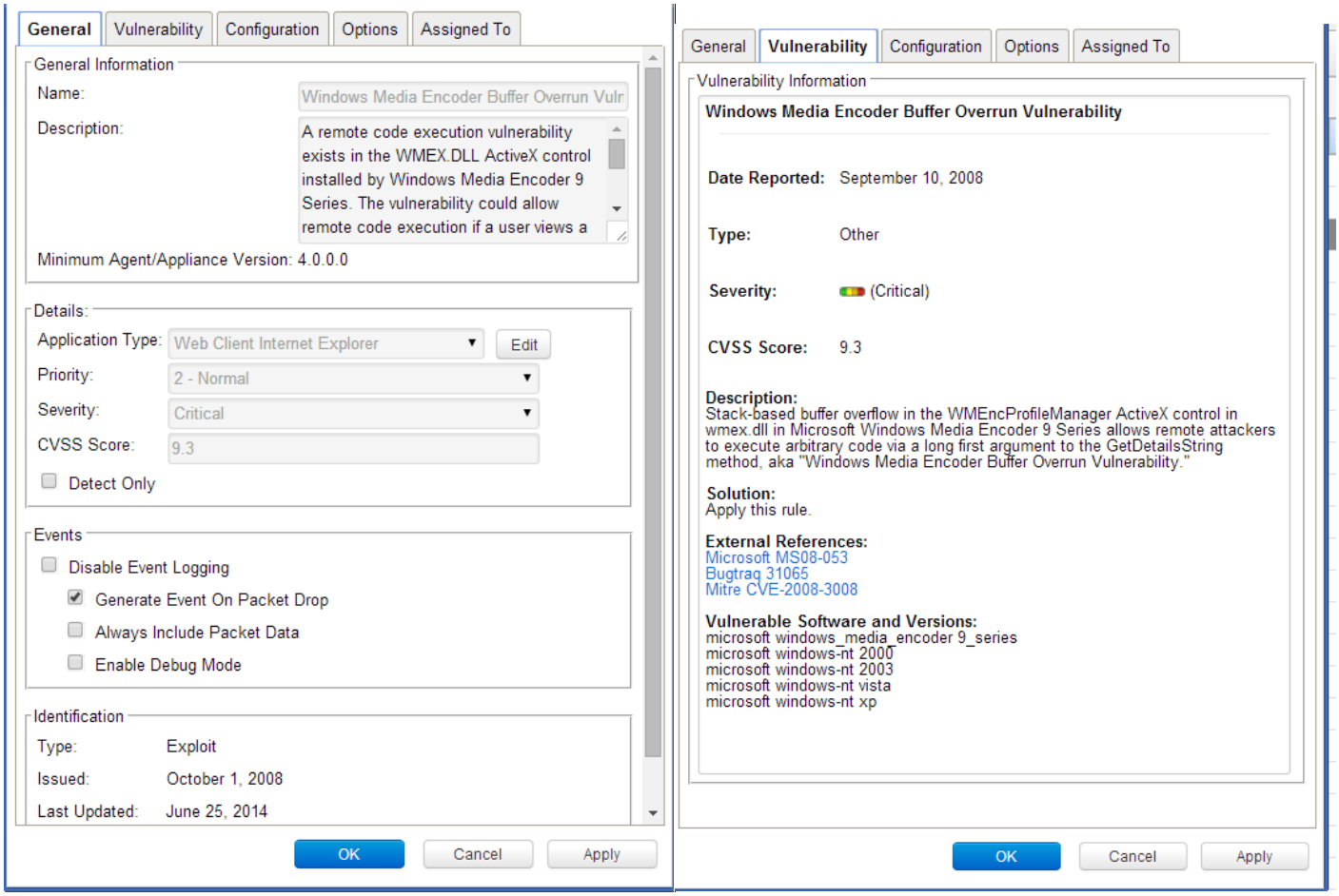
IP기능 중 Illegal Characters in URI로 생성된 이벤트 인데 URI 정보가 모두 안 나오는 증상



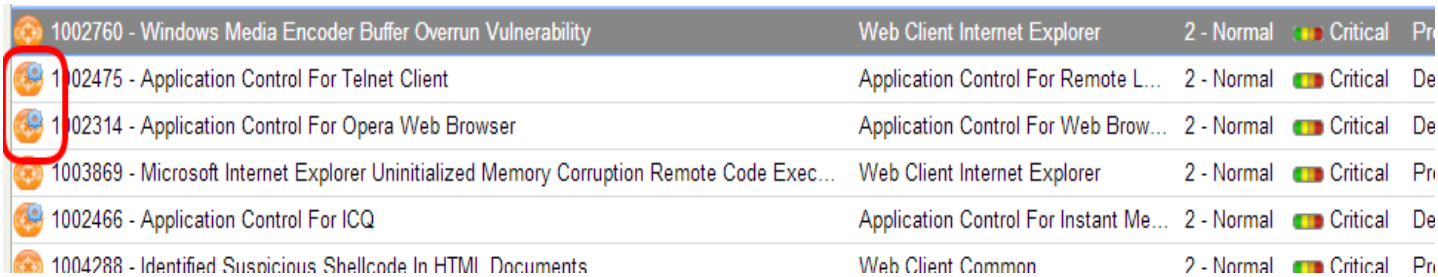
URI값은 HTTP 프로토콜의 헤더 값입니다. DS는 Application 계층이 아닌 트랜스포트 계층에서 트래픽을 캡쳐 합니다. 위의 이벤트는 Application 계층에서 보낸 데이터의 stream 중 일부 가 캡쳐되어 보여진 것입니다.
위의 또한 post 방식일 경우 데이터 영역까지 URI가 포함되기에, 위의 데이터도 URI로 보아야 합니다.

Intrusion Prevention 룰에 대한 자세한 설명이 있는 문서가 있나요?

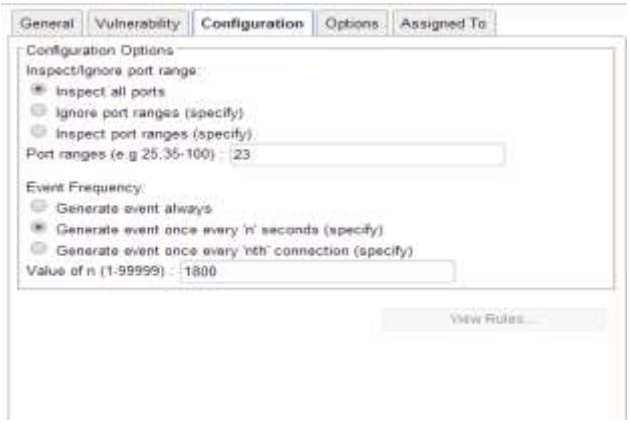
각 룰을 더블 클릭 하시면, 아래와 같이 General 탭에서 기본적인 설명을 보실 수 있고, Vulnerability 탭에서는 이룰이 방어하는 취약점에 대한 정보를 보실 수 가 있습니다.



룰 중에서는 추가로 설정을 해주어야 하는 룰이 있습니다. 이런 룰의 경우 아래와 같이 룰 앞에 톱니바퀴 모양이 있



으며, Configuration 탭을 확인하시어 어떤 설정이 있는지 확인 하심으로 룰을 이해 하실 수 있습니다.

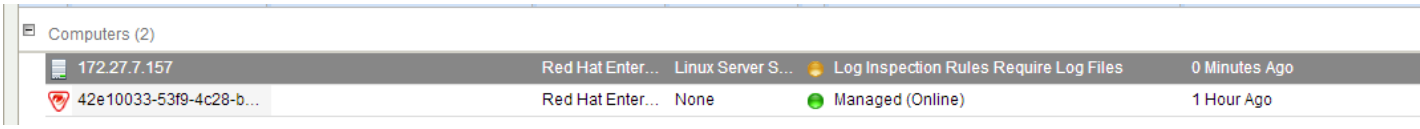


Log Inspection Rules Require Log File 상태 해결 방법

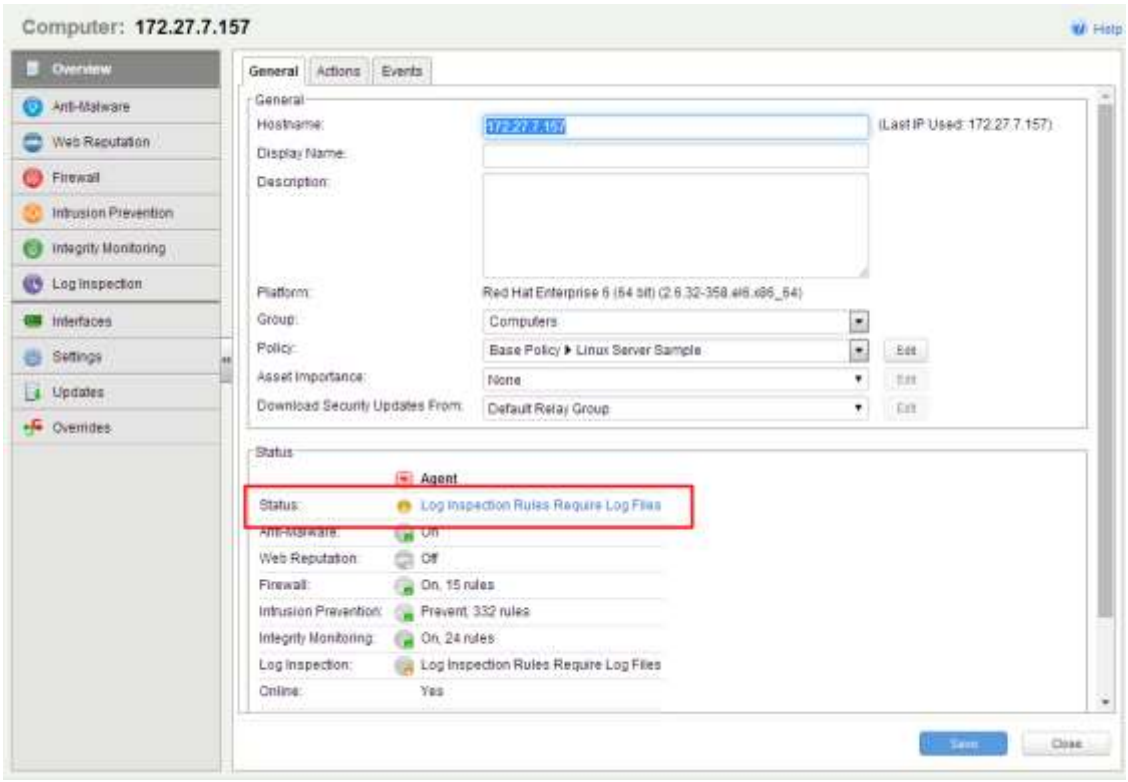
위의 경고 메시지의 내용은 Log Inspection 룰이 모니터링 할 로그를 지정해 주라는 내용 입니다. 모니터링할 로그를 지정하는 방법을 아래와 같이 진행 하겠습니다.

로그를 지정해 줘야 할 룰 확인 하기

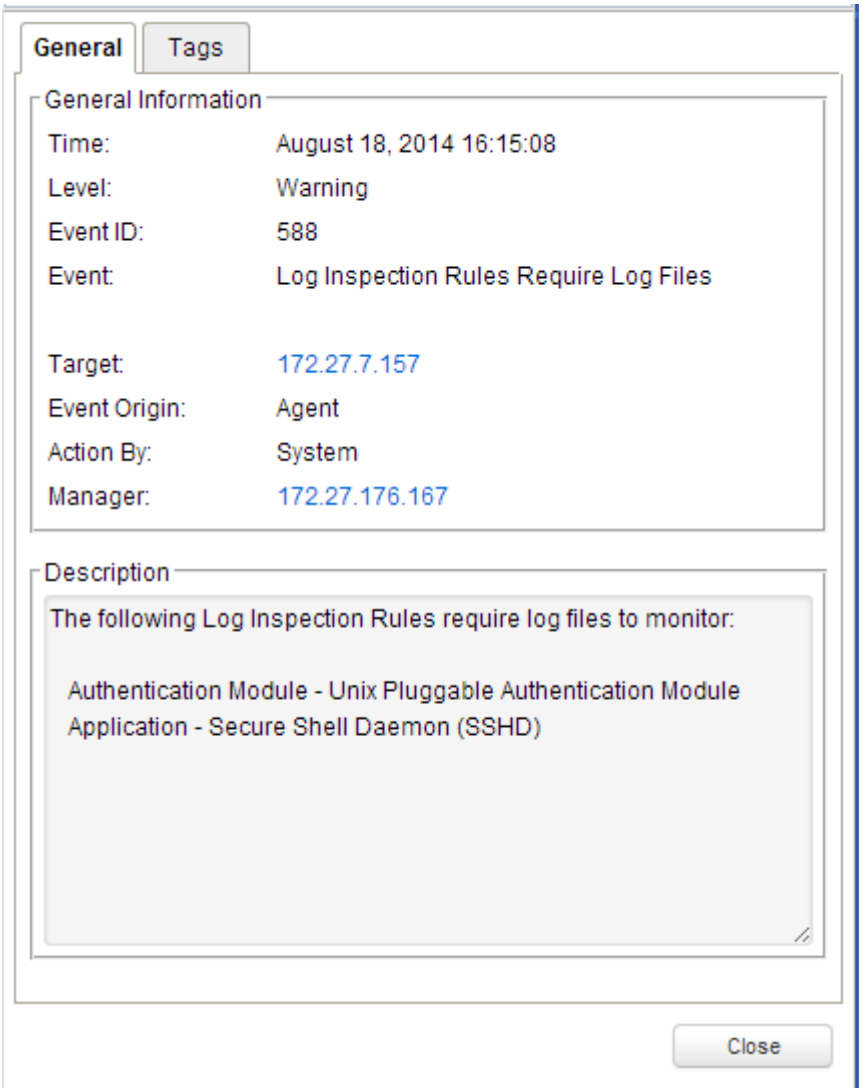
- "Computer" 탭에서 "Log Inspection Rules Require Log Files" 상태 확인



- 해당 Computer를 더블 클릭하여 상세화면 출력 및 상태 클릭

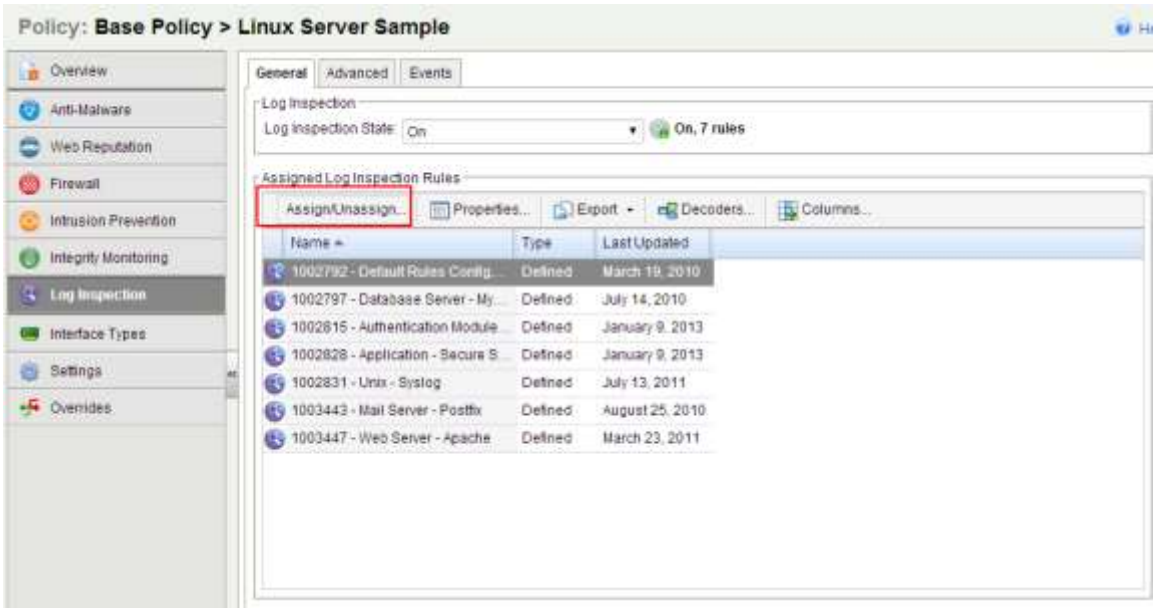


- 팝업된 화면에서 로그파일을 지정해 줘야 하는 룰을 확인. 아래의 경우는 "Authenticatin Module – Unix Pluggable Authentication Module", "Application – Secure Shell Daemon(SSH)" 두개의 룰에 로그 지정이 필요.

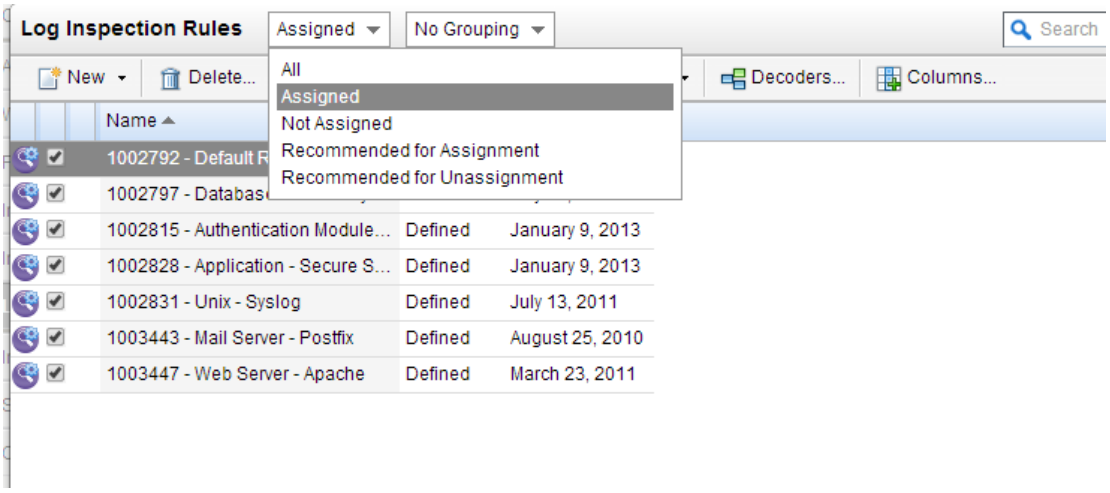


룰에 로그 지정

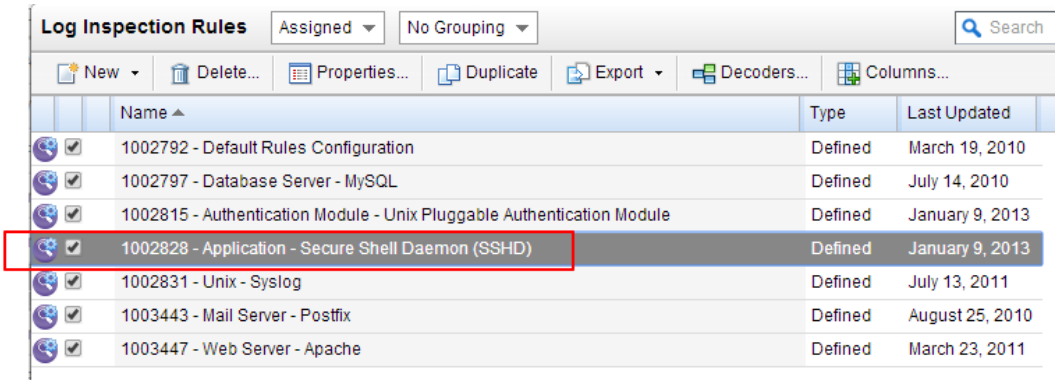
- "Policies" 탭 > 왼쪽의 패널에서 "Policies" 선택 > "Linux Server Sample" 더블 클릭 하여 상세화면 출력
- 왼쪽의 패널에서 "Log Instpection" 클릭 > "Assign/Unassign" 클릭



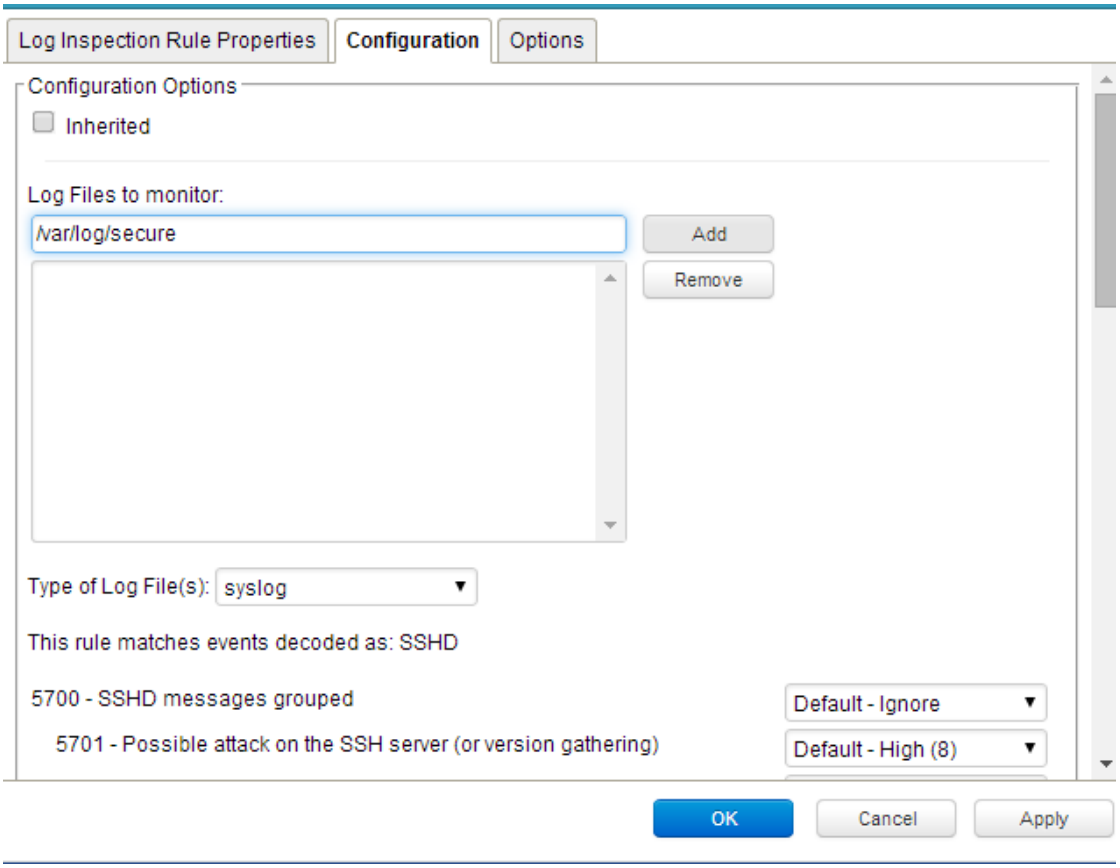
- 상단에서 Assigned 만 보도록 설정



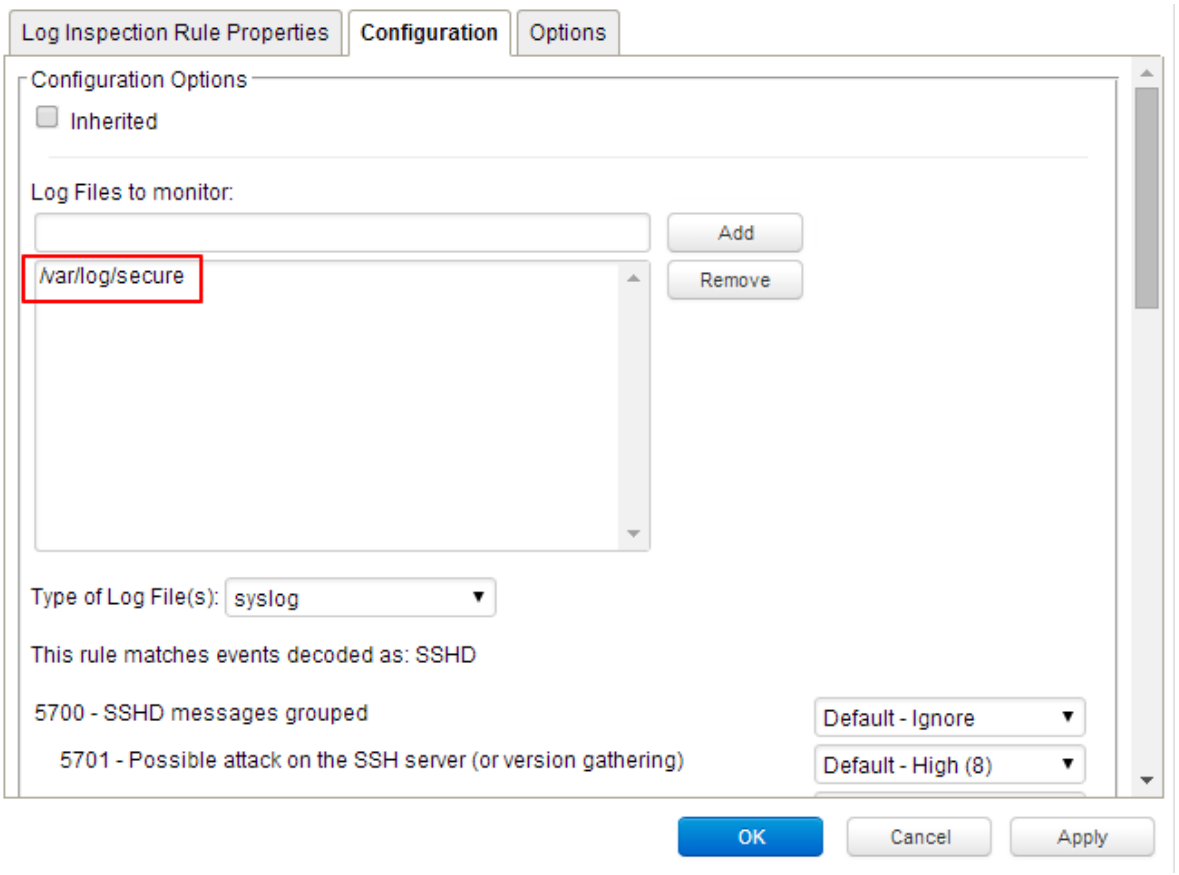
- 로그를 넣어 줘야 하는 룰 클릭.



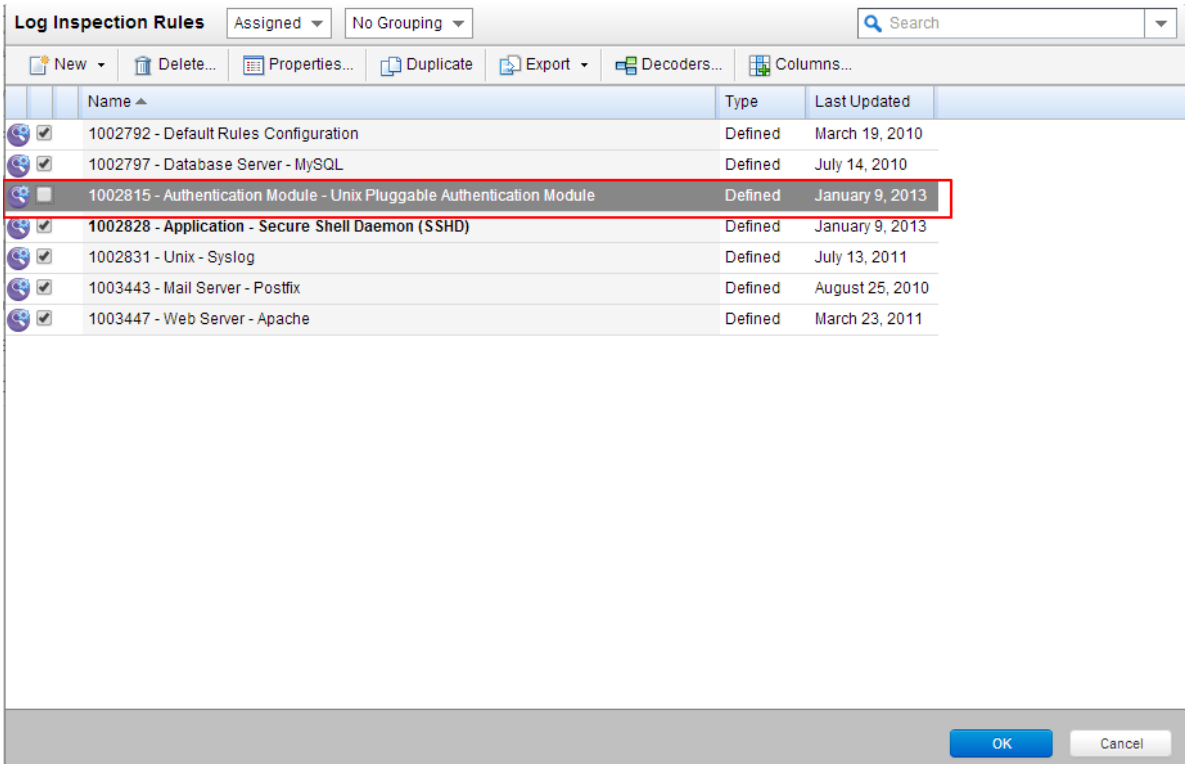
- 해당 룰이 관찰할 로그 파일의 경로를 넣어 준 후, "Add" 버튼 클릭



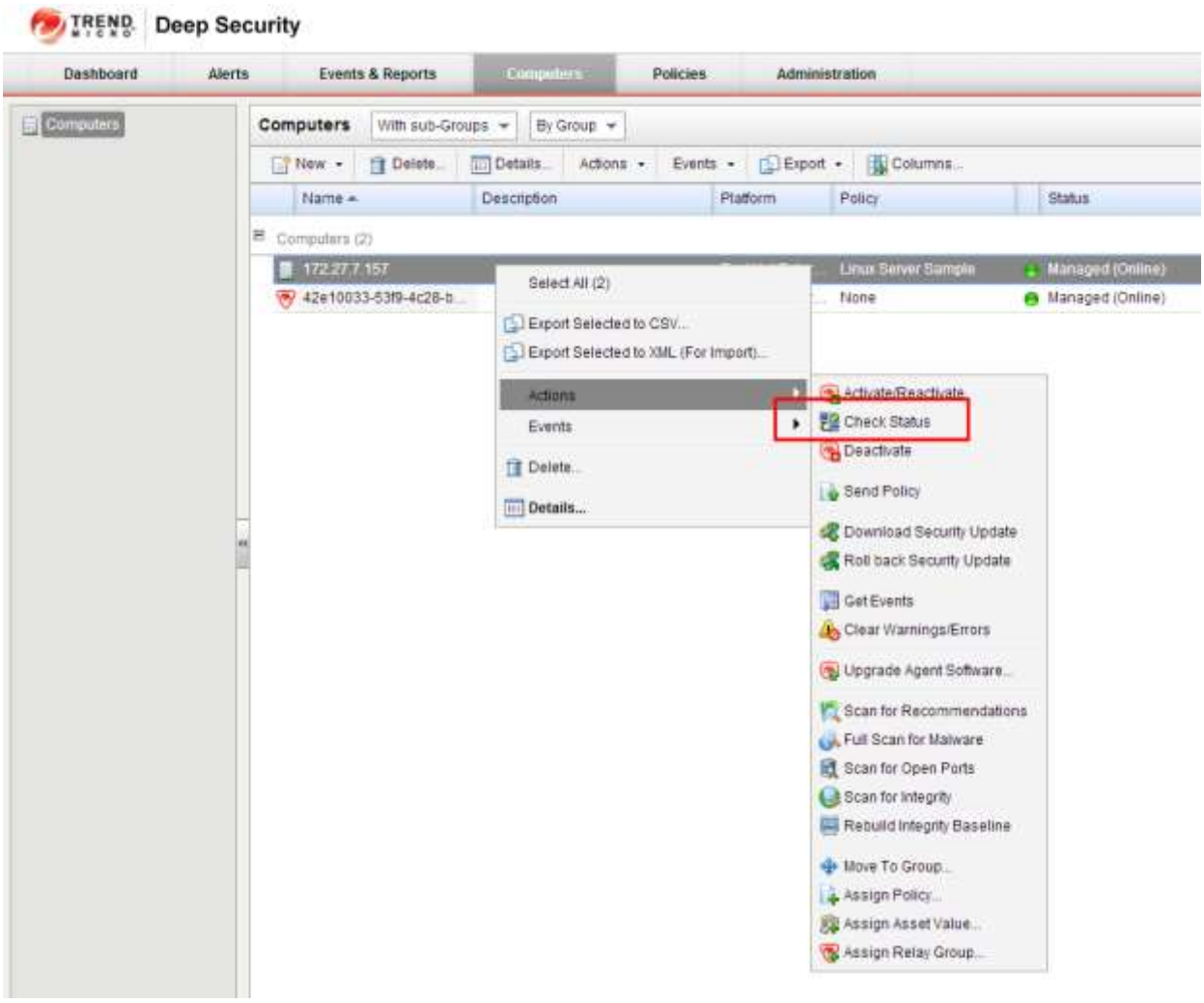
- 하단의 창으로 이동하는 것 확인 후 "OK" 버튼 클릭



- 위와 같이 룰에 해당하는 로그 파일의 위치를 지정해 주거나 또는, 룰 자체를 가장 앞의 체크 박스를 해제하여 Unassigned 후 "OK" 버튼 클릭



- 다시 "Computer" 탭의 해당 Computer의 오른쪽 마우스를 클릭하여, "Check Status" 수행. 상태가 "Managed(Online) 상태가 된다면 작업 완료



Anti-malware 예외처리 방법은?

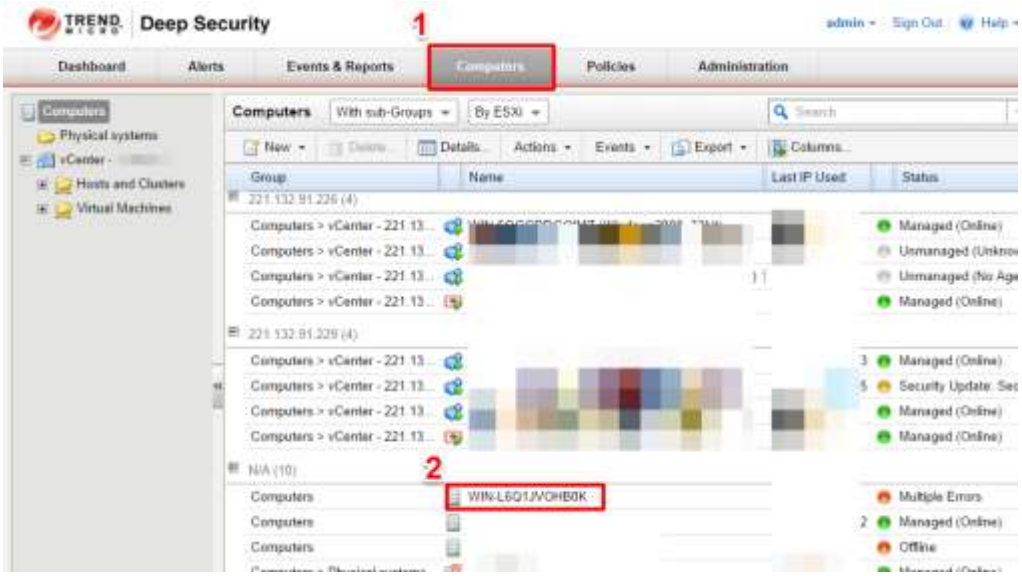
위의 "Deep Security 운영 따라하기 > Anti-malware 설정하고 운영 하기" 를 참고

Diagnostic Package 생성 방법은?

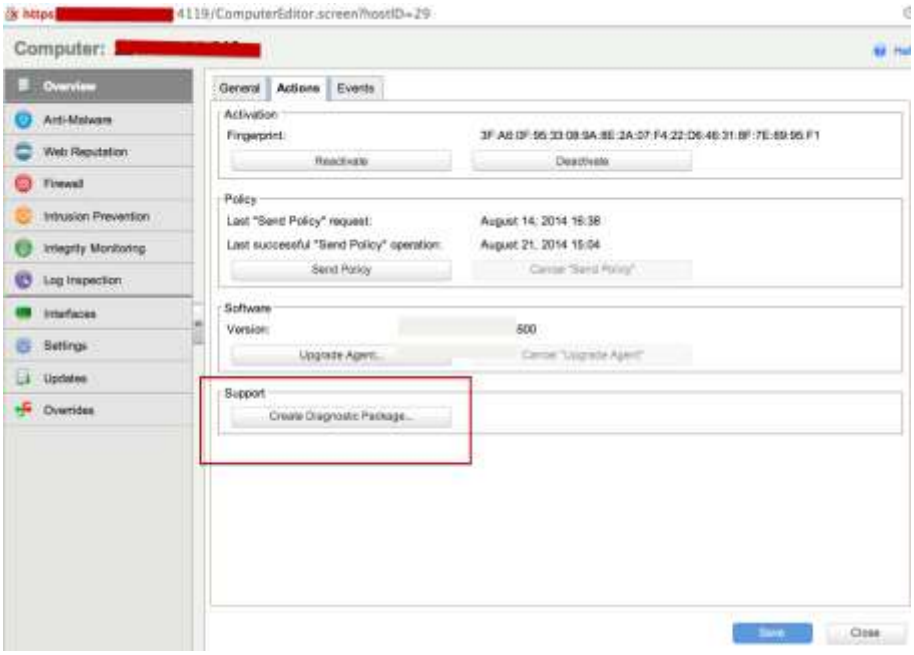
Deep Security Agent, Deep Security Relay, Deep Security Manager 에서 Diagnostic Package를 생성 하실 수 있습니다.

DSA Diagnostic Package 생성

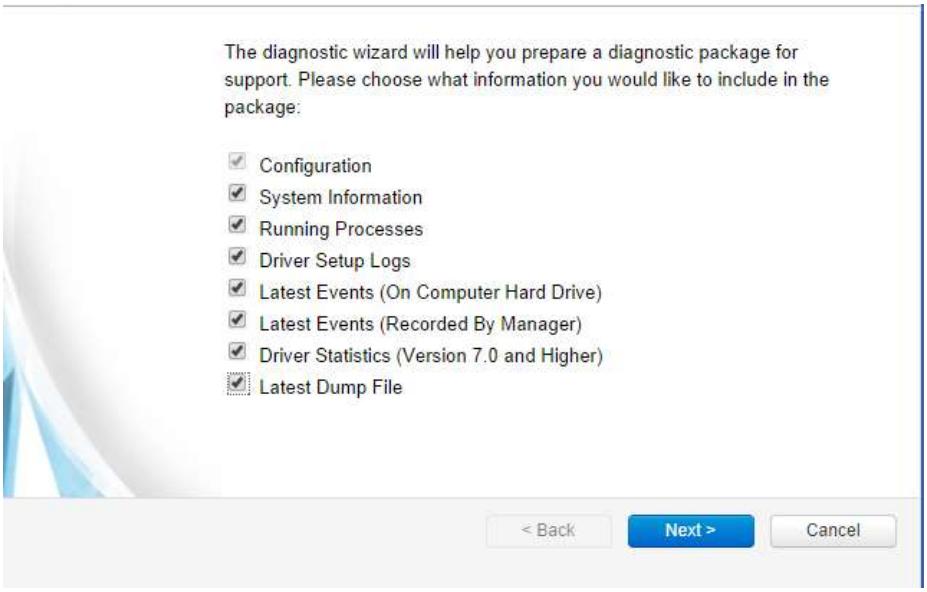
- Diagnostic Package를 생성하고자 하는 컴퓨터의 상세화면 출력(1번 컴퓨터 탭을 클릭 후, 상세화면을 보고자 하는 컴퓨터 더블클릭



- 왼쪽의 Overview 클릭, 우측의 Action 탭 클릭 후, "Create Diagnostic Package"를 클릭



- 생성된 팝업 창에서 아래와 같이 모든 옵션 체크 한 후 "Next"

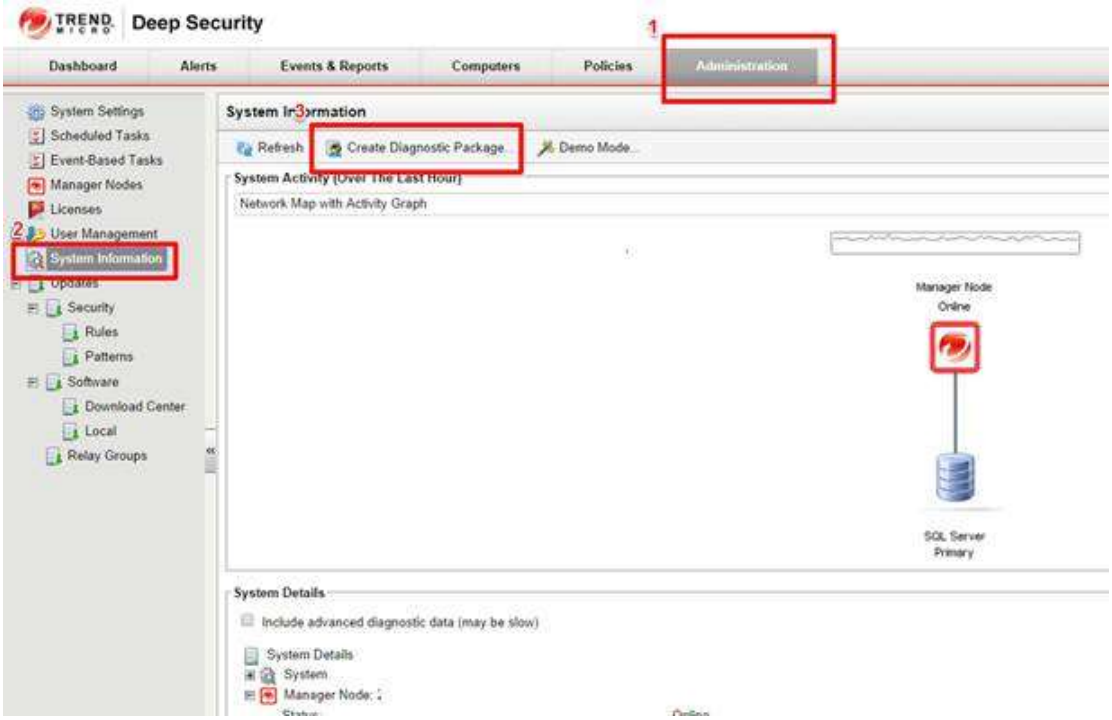


DSR Diagnostic package 생성

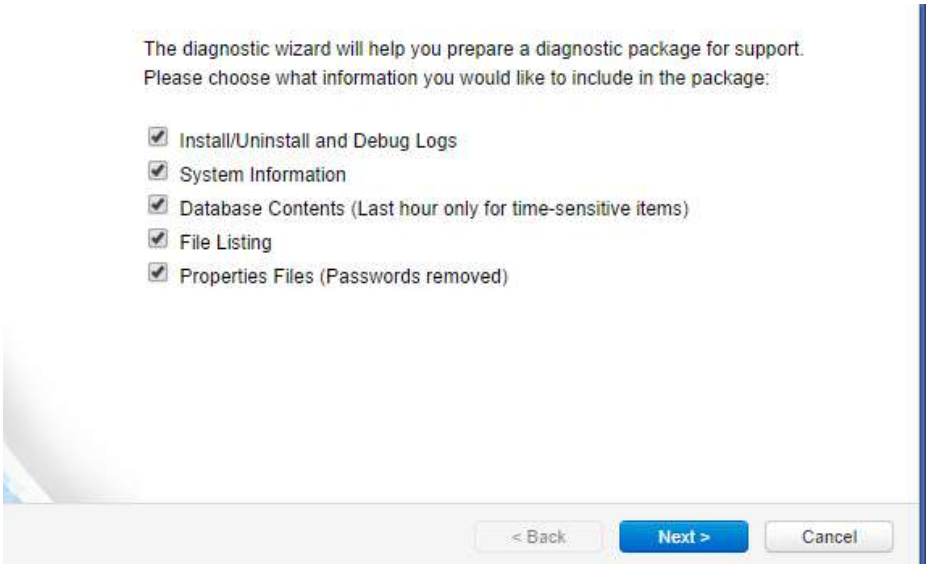
- DSA에서 생성하는 방법과 동일 합니다. Computer 탭에서 아래의 DSR 표시가 있는 컴퓨터의 상세 페이지를 출력 후에 DSA와 동일한 방법으로 생성 하시면 됩니다.

DSM Diagnostic package 생성

- 아래의 순서로 클릭



- 모든 옵션 클릭 "Next" 버튼 클릭하여 Diagnostic Package 생성



Revision History

날짜	작성자	내용
2014.5.20	전철민 과장	문서 생성
2014.7.2	전철민 과장	문의 및 알아두어야 할 사항에 내용 추가
2014.7.8	전철민 과장	Linux 에서 Agent 삭제 방법 보완
2014.8.14	전철민 과장	KT ucloud 매뉴얼에 반영