Deep Security 9.0 사용자 / 관리자 가이드

목차

제품 개요	3
용어설명	3
제품소개	3
Deep Security 호환성	4
KT ucloud 사용자 필독 사항	5
참고 매뉴얼 및 사이트	6
Deep Security Agent 설치	6
Windows 시스템에 DSA(Deep Security Agent) 설치	6
Linux 시스템에 DSA 설치	10
Amazon 환경에서 자동 배포 구성하여 설치	16
Deep Security Agent 삭제	20
Linux 에서 Deep Security Agent 삭제	20
Windows에서 Deep Security Agent 삭제	21
Deep Security Manager 운영	23
DSM 접속	24
Dashboard	24
Alert	26
Events&Reports	26
Computers	28
Policies	

Administration	32
Deep Security 운영 따라하기	34
정책 설정 및 적용(Recommendation Scan)	34
Anti-malware 설정하고 운영 하기(예외처리)	41
각종 Scheduled task 만들기	46
Security와 System event 전송 설정(syslog로 전송)	48
자주하는 질문(FAQ)	50
패스워드 변경하는 방법은?	50
DSM 스토리지 관리 방법은?	51
DSM 서버 리부팅 하는 방법은?	52
Amazon 환경에서 리부팅 후, 서버 IP 변경으로 인한 DSM offline 발생시 조치 방법	52
Agent offline시 조치 방법 1 (리셋 후 다시 Activation)	54
Agent offline시 조치 방법 2 (Agent 삭제 후, 재설치)	55
DSA가 설치 되며 네트웍이 단절 되는 현상	55
IP기능 중 Illegal Characters in URI로 생성된 이벤트 인데 URI 정보가 모두 안 나오는 증상	57
Intrusion Prevention 룰에 대한 자세한 설명이 있는 문서가 있나요?	57
Log Inspection Rules Require Log File 상태 해결 방법	59
Anti-malware 예외처리 방법은?	63
Diagnostic Package 생성 방법은?	63

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 하였습니 다. 기능은 아래와 같이 총 6가지 구성 됩니다.

- 1. Anti-Malware : 서버 백신 업계 세계 1위의 Trend Micro의 인정받은 Anti-Malware 엔진을 사용하여, 악성코 드로부터 서버를 보호 합니다.
- 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 간단 히 화이트 리스트를 생성하여 도메인간의 통신을 허가 할 수도 있습니다.
- 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.
- Intrusion Prevention : 새로운 단계의 서버 보안 입니다. Firewall로부터 허가된 inbound와 outbound 트래픽 을 검사를 하여, 아직 패치가 되지 않은 OS나 어플리케이션으로 부터의 취약점을 타겟으로 하는 의심스러운 활동이나 공격을 차단합니다.
- 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.
- Log Inspection : 관리자가 중요 시스템 로그를 적시에 확인 할 수 있도록 합니다. 각 시스템 들의 중요 로그 가 통합 관리되며, 관리자의 설정에 따라 이벤트를 설정하여 적시에 이상 징후를 찾아 냅니다.

3

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 DSA
 의 "More details"를 클릭하고, ReadMe 파일을 다운 받아 확인

Al: 10 Likets	Deen Security Acent	Relay an	d Notifier 8 6 Cervice Re	ele 1	
Scan Engines	Find and unit terms arranged	Relay an	u notilier 3.0 Service Pa	CR 4	
All Putters Files	View other versions				
That Downleads from Tools	Second Construction Statestics	Product Perch	Record Scorpett		
	Spending System: Windows 2264				
Subscribe Dosinkant Center Hus	Benerhaat Benerhaten 🗃 🛃	Reference Date:	fife Baren	nen (1981)	Stonets ad Package
	Product Patch	2014-05-00	Agent - Windows - 4.0.0-2000 (2016-mill Orea Security Agent: Service Pech 1, Pech 3 for Windows 15-bill	34.2	*.
	 Hore Behalli ABOUT THIS SCHMILOAD Elisame April Wolfsey 8.20 SIR270 elisekseen ACAUCHY SIR-1 checkseen ACAUCHY SIR-1 checkseen SCHOLOGIUM 	3500	버전이 지원하는	플랫	몸 확인
	About databili Adout Tutus SodenLoAD Historen Agent Workberg 3.25 Historen Agent Workberg 3.25 Historen Agent Workberg Historen Agent Historen Agent Adout Agent Adout Agent Market Agent Ma	3500	버전이 지원하는	플랫	볼 확인
	Nove definition Addorf Table	3500	버전이 지원하는 employed at a 200 200 Point Serie Margin (Margin Point) Point Strain (Margin Point) Point Strain (Margin Point) Point Strain (Margin Point)	"플랫	볼 확인 호
	Noor datable Addorf Television Addorf Television Addorf Television March Marcale Marcale	3500	바라고 아이지 원하는 해외 아니는 100 100 100 100 100 100 100 100 100 100	·플랫	볼 확인 호

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 "자
 주하는 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 : <u>http://esupport.trendmicro.com/en-us/business/pages/technical-support/deep-security-9-0-</u> <u>support.aspx</u>
 - ◆ 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

<u>Deep Security Agent 설치</u>

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(<u>https://ipaddress:4119)</u> 및 로그인.

TREND. Deep Security
Username: Password:
Sign In
Copyright © 2013 Trend Micro Inc. All rights reserved

● 우측상단의 "help" > "Deployment Scripts" 클릭

Maste	eradmi	n 👻 Sign Out 🧕) <u>Help</u> –		
Administration		Introduction			
	-	Online Help			
		Deployment Scri	pts		
		About			
mported Version	Relea	ase Date	Up-		
9.0.0.2401	May 3	1,2013	1		
۹/A	May 3	1,2013	1		

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

Deploy:	Agent (Recommended) C Relay
Platform:	None
Can't find the package	None
e antennie nie paenage	Microsoft Windows (32 bit)
Activate the Accept	Microsoft Windows (64 bit)
Activate the Agent	xe.0

• "Activate the Agent Automatically" 선택

Deploy:	⊙ Agent (Recommended) ○ Relay
Platform:	Microsoft Windows (64 bit)
Can't find the pac	kage you are looking for? Import More Software
Activate the A	Agent Automatically
Policy:	None
Group:	Computers
Relay:	Default Relay Group
NOTE HOST	tname, description, unique identifiers and other properties can also be set on agent-initiated activation. See Help for more information.
Vet.ServicePoint New-Object Syst msiexec /i "\$en itart-Sleep -s 60	tManager]::ServerCertificateValidationCallback = {\$true} tem.Net.WebClient).DownloadFile("https://172.27.226.217:4119/software/agentWindows/x86_64/", "\$env.temp\agent.msi") w.temp\agent.msi" /qn ADDLOCAL=ALL

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

川 和	록 없음 - 메5	2장						
파일(F) 편집(E)	서식(0)	보기(V)	도움말(H)				
[Net. (New- & msi Start	ServicePoin Object Syst exec /i "\$e -Sleep -s 6	tManager em.Net.₩ nv∶temp₩ Ю]::Serve ebClient agent.ms	erCertifica 2).Download 31°/qn ADD	teValidatio File("http: LOCAL=ALL	onCallback s://172.27.	= {\$true} 226.217:41	19/software/ag
& \$En	v:ProgramFi	les"#Tre	nd Micro	ı₩Deep Secu	rity Agentt	#dsa_contro	l" —a dsm∶	//172.27.226.2
	다른 이름	으로 저짐	;					
	00	📃 바탕 호	ŀ면 ▾			▼ [🔊 🛛 바탕 화	면 검색
	파일	이름(N): [i	nstall_dsa	a,ps1				
	파일	형식(T): [텍스트 문/	५(★,txt)				

• 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

rts	Events & Reports	Computers	Policies	Administ	ration		
	Computers With sub-Group	es 🔻 🛛 By Group 👻			🔍 Search		
	📑 New 👻 🟦 Delete	Details Action	is 🔹 Events 🔹	🔄 Export 🕤	- 🔛 Column	S	
	Name 🔺	Description	Pla	tform	Policy		Status
	E Computers (2)						
	🦁 172.27.226.217		Red	i Hat Enter	None	θ	Managed (Online)
			Mic	rosoft Win	None	Θ	Managed (Online)

● 필요 시, "Hostname" 컬럼의 값 변경.

"Hostname" 컬럼의 값이 기본으로 컴퓨터의 hostname으로 세팅되어 있는 상태 입니다. DSM에서 DSA로 통 신 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 바랍 니다.

Computer: WIN-VH	PBIEVUSP2		0
Overview	General Actions Eve	nts	
📀 Anti-Malware	General		
💿 Web Reputation	Display Name:	WIN-VHPBIEVUSP2	(Last IP Used: 172.27.176.58)
🛞 Firewall	Description:		
Intrusion Prevention			
Integrity Monitoring			

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

STOL Inninoconcercion				and the second sec
TREND	Securing Your Journey to the Cloud		Where to Buy 👘 🛓	Doonloads Partnera
For Home	For Business	Security Intellige	nce	Why Trend Micro
oftware Downlo	oad Center			
d Products	Deen Security Ageni	· All Version	ne	
ican Engines	Deep Security Agen	. : All version	15	
l Pattern Files	Platform		Version	
ital Downloads	ADE	-		-
too Tools	Abt SL Version 5.3 and n.1 Powe	uPC	9.0 Service Park	4
	Amagon Linux			
	Amazon Latur		9,0 Service Park	8
Subscribe	Amizon Linux		9.0	
	CentOS 5		9.0 Service Pack	i
	CentOS 6.0		9.0 Service Pack	(41)
	Cloud Linux 3		9.5	
	Cloud Linux 5		9.0 Service Pack	(1)
	Cloud Linux 6		9.5	
	Cloud Linux 6		9.0 Service Pack	(b)
	HP-UX 11/ v3 IA-04		9.0 Service Pack	3
	LEADY STORATE AND		II II Sanaca Park	10

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

All Products	Deen Security Ana	nt Belay an	d Notifier 9 0 Service Pa	ck 1
Scan Engines	Read and user license agreemo	c Relay an		Ch I
All Pattern Files	View other versions			
Trial Downloads	Martin and Andrewson and Antonio	The state of the state	Commission and the second second	
Pree Tools	Present Commondy Optimi	Product Patch	- Renne Soffort	
	Operating Bustern: Windows 3	26-8		
Subscribe Download Center RSS	Download Description	Release Date	File Name	Size (MR
	Product Peter English	2014-06-09	Agent-Windows-9.6.0-3300.086.mm Desp Security Agent: Service Feck 1, Patch 3 for Windows 33-bit	18.5
	O More details			
	Product Patish. Koglash	2014-06-18	Relay Western 9.0.0 3300.000 mm	25.4

• DSA를 설치하고자 하는 OS에 맞게 최신 DSA installer 다운로드

🗋 downloadcente	r.trendmicro.com/index.php?	regs=NABU&c	:lk=latest&clkval=4367⟨_loc=1		\$
	O More details				
	Product Patch English	2013-09-19	Agent-RedHat-EL6-9.0.0-2401.x86- 64.rpm 64-bit	9.21	
	© More details	를 설치	이하고자 하는 OS	버전	선택
	Operating System: CentOS 5	Deleses Del			Demeland Deduces
	Download Description	Release Date	File Name	SIZE (MB)	Download Package
	Product Patch English	2013-12-17	<u>Agent-RedHat-EL5-9.0.0-</u> <u>3044.i386.rpm</u> 32-bit	5.49	
	O More details				
	Product Patch English	2013-12-17	Agent-RedHat-EL5-9.0.0-3044.x86- 64.rpm 64-bit	11.9	*

- DSM web console(<u>https://ipaddress:4119</u>) 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

Maste	eradmii	n - -	Sign Out	?	Help -	
Administration		Intr	oduction			
	_	On	line Help			
		De	ployment S	Script	ts	
		Abo	out			
mported Version	Relea	ise Da	ate		Up-	
9.0.0.2401	Мау З	1, 201	3		1	
N/A	May 3	1,201	3		1	

● "Platform" 컬럼에서 DSA를 설치하고자 하는 OS 플랫폼 선택

Agents or relays can be	e manually installed or deployed using tools such	as RightScale, Chef, Puppet, or SSH.
For platforms other thar	n Windows and Linux, please see the installation g	uide.
Deploy:	• Agent (Recommended)	
Platform:	None 💌	
Can't find the package	None Microsoft Windows (32 bit)	
Activate the Agent	Microsoft Windows (64 bit) Red Hat Enterprise 5 (32 bit)	
[]	xe.U	

• "Activate the Agent Automatically" 선택

eploy:	🖲 Agent (Recommended) 💭 Relay		
latform:	Red Hat Enterprise 5 (32 bit)	-	
an't find the pac	kage you are looking for? Import More Soft	are	
Activate the A	gent Automatically		
Policy:	None	-	
Group:	Computers	*	
Relay:	Default Relay Grou	-	
NOTE HOST	tname, description, unique identifiers and	ther properties can also be set on age	ent-initiated activation. See Help for more information

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



- 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-a98	b-lee9eb7e07	9b ~] # . /ir	nstall_dsa.s	h
Preparing	############	*********	*############	######## [1
]				
package ds_agent-9.0	0.0-2402.i386	(which is	newer than	ds_agent-9.0
2008.i386) is already instal	lled			
file /opt/ds_agent/2	.6.18-164.9.	1.el5PAE-i6	586/dsa_filt	er.ko from i

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

	Events & Reports	Computers	Policies	Adminis	tration		
Co	mputers With sub-Grou	ps 👻 🛛 By Group 👻]		🔍 Sear	rch	
	rrnew → 👔 Delete	📰 Details Actions	s 🗸 🛛 Events 🗸	🛐 Export	🗸 🔛 Columns	3	
	Name 🔺	Description	Pla	atform	Policy		Status
E (Computers (3)						
5	🞅 172.27.226.217		Re	ed Hat Enter	None	0	Managed (Online)
	 71b32395-7853-4324		Re	ed Hat Enter	None	θ	Managed (Online)

● 필요 시, "Hostname" 컬럼의 값 변경.

"Hostname" 컬럼의 값이 기본으로 컴퓨터의 hostname으로 세팅되어 있는 상태 입니다. DSM에서 DSA로 통 신 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 바랍 니다. Computer: 71b32395-7853-4324-a98b-1ee9eb7e079b.cs389dcloud.internal

E Overview	General Actions Events		
📀 Anti-Malware	General		
🥯 Web Reputation	Display Name:	71b32395-7853-4324-a98b-1ee9eb7e079b.cs389dcloud.interr	LastiP Osed: 172.27.194.8)
🛞 Firewall	Description:		
Intrusion Prevention			
Integrity Monitoring			

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

O Hure details.				
Product Parch English	2013-09-20	Agent Uburku 10,04-9,0 0 0401 x88-64,048 64-54	5.62	*
Q Hare details				
Operating Systems Amaze	on Linux			
Downland Description	Release Date	File Name	Size (MB)	Downhad Package
Brodust Patch English	2013-12-17	Agenth amart1-9.0,01 3044-4585 rpm	6.63	
Store datails				
Product Patch English	2013-12-17	Againt amin1/9.0.0-3044.x88- 64.pm	12.9	٠.
O Hore distuits				
Product Patch English	2013-09-19	Agenti amon 1-8.0.0- 04016581.rpm 32-bit	5.93	٠.
O More distails				10
Deaduret Rateria	2012-09-19	Agent empril 1 2.0 2412 vill	17.1	

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

Dashboard	Alerts	Events & Reports	Computers	Policies	Administration
Dashboard System Settings Scheduled Tasks Event-Based Tasks Manager Nodes Licenses Licenses User Management Subsers Contacts System Information Updates	Alerts	Events & Reports	Computers Updates Relays Download Ce 9.0.0.2014 x) 9.0.0.2008 (9.x) 9.0.0.2008 9.0.5370	Policies	Administration 1 nported Version 0.0.2404 0.0.2008 0.0.2401 /A
		Open Download Center.		Import Software	4

DSM에서 자동 배포를 위해 사용할 스크립트 가져오기

• Help > Deployment Scripts 클릭

Dashboard Alerts	Ev	enta & Repo	eta Compu	ters Policies	Administration			_	Online H	elp.
🔁 System Settings	Update	1							Deploym	etti Scopti
 Scheduled Tasks Event-Based Tasks 	Secur	ty Updates	Software Updates	Relays					About	
Manager Nodes	Packs	ge Name		Download Center Version	Imported Version	Release Date	Up-to-date	Qui	-of-date	Percent Up
Tenants.	Agent	- Windows (d96_64) (9 x)	9 0 0 3044	9 8 8 3044	December 6, 2013	3	1		
P Licenses	Relay	- Windows ()	(86_64) (9 x)	9 0 0 3044	9 0 0 3044	December 6, 2013	1	0		
User Management	Agent	- RedHat_EL	.6 (x85_64) (9 x)	9.0.0.3044	9.0.0.3044	December 6. 2013	2	Ű		
L Users	Filter	Driver - ESX	5 0 (x86_64) (9 x)	9 0 0 2636	9 0 0 2636	December 6, 2013	3	0		
Roles	Maria;	ger - Window	a (x64) (9.x)	9.0.6019	N4A	December 6, 2013	01	0		

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

Deployment Scrip	ts	
Agents or relays	can be manually installed or deployed us	sing tools such as RightScale, Chef, Puppet, or SSH.
Deploy:	 Agent (Recommended) Relay 	stanation guide.
Platform:	s or relays can be manually installed or deployed using tools so tforms other than Windows and Linux, please see the installation gui ∴ ● Agent (Recommended) ● Relay m: Amazon Linux AMI (64 bit) • nd the package you are looking for? Import More Software tivate the Agent Automatically plicy: Base Policy ▶ Linux Server roup: Computers elay: Default Relay Group OTE Hostname, description, unique identifiers and other properties pin/env bash	τ
Can't find the pack	age you are looking for? Import More Softwar	re
Activate the A	gent Automatically	
Policy:	Base Policy ► Linux	Server 🗸
Group:	Computers	▼
Relay:	Default Relay Group	
NOTE Hostr	name, description, unique identifiers and othe	er properties can also be set on agent-initiated activation. See Help for more information.
#!/usr/bin/env bash wget https://221.1: rpm -ihv /tmp/agen sleep 5 /opt/ds_agent/dsa	n 32.91.214:4119/software/agent/amzn1/x86_6 it.rpm _control -a dsm://221.132.91.214:4120/ "polic	i4/ -O /tmp/agent.rpmno-check-certificatequiet

• 아래의 텍스트창에 설정한 내용으로 스크립트가 생성됨을 확인

or platforms oth	her than Windows and Linux, please see the in	stallation guide.			
)eploy:	Agent (Recommended)				
Platform:	Amazon Linux AMI (64 bit)	•			
an't find the pa	ckage you are looking for? Import More Softwa	ire			
Activate the	Agent Automatically				
Policy:	Base Policy ► Linux	Server	•		
Group:	Computers		•		
Relay:	Default Relay Group		•		
NOTE Hos	stname, description, unique identifiers and oth	er properties can also b	e set on agent-initiated act	ivation. See Help for more information.	
/usr/bin/env ba get https://221	ish 132.91.214 ⁻ 4119/software/agent/amzn1/x86	64/ -O /tmp/agent rpm -	-no-check-certificatequie		
	ent rom				

EC2에서 Instance 생성 부분에, 설치 스크립트 추가

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

equest Inst	ances Wizard			Canc
HOOSE AN AMI	INSTANCE DETAILS CREATE KEY P	Ain CONFIGURE FIREWALL	REVIEW	
Number of In:	stances: 1	Availability Zo	one: No Preference	
Advanced I	nstance Options			
You can choose	to enable CloudWatch Detailed Mo	nitoring or enter data that will I	be available from your inst	ances once they launch.
Monitoring:	Enable CloudWatch detailed moni (additional charges will apply)	toring for this instance		
User Data:	kpowershell> [Net.ServicePointManager]::Server (New-Object System.Net.WebClien ("https://iserve.com/comm.com/11	CertificateValidationCallback = {\$1 t).DownloadFile	true}	
	Use shift enter to insert a newline)	1	
	base64 encoded			
Fermination Protection:	Prevention against accidental terr	nination. Shutdown Behavior:	Stop	
IAM Role: 🎯	None 🔻			

<u>Deep Security Agent 삭제</u>

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@sta	atic d	sa]# ls /pr	coc/drive	r/dsa	
configs	info	interfaces	stats	trace	trace_ctl
[root@st	atic d	sal#			

Lsmod를 수행 했을 때, kernel module dsa_filter이 없어야 함.

🗬 root@static:~		
[root@static ~] # rpr	n -ivh Age	nt-RedHat EL6-9.0.0-3500.x86 64.rpm
Preparing	#	######################################
1:ds_agent	#	######################################
Loaded dsa_filter mo	dule vers	ion 2.6.32-431.el6.x86_64 [OK]
Starting ds_agent:	[OK]	
[root@static ~]# lsr	nod grep	dsa
dsa_filter	923469	12
[root@static ~]# lsr	nod	
Module	Size	us d by
dsa_filter	923469	12
autofs4	26513	3
oosid	20010	
garp	7152	1 8021q
stp	2218	1 garp Ξ
11c	5546	2 garp, stp
ipt_REJECT	2351	0
nf_conntrack_ipv4	9506	0
nf_defrag_ipv4	1483	1 nf_conntrack_ipv4
iptable_filter	2793	0
ip_tables	17831	1 iptable_filter
ip6t_REJECT	4628	2
nf_conntrack_ipv6	8748	2
nf dofnog inve	11100	1 nf conntrack inu6

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

Quénieu	Computer Network Engine Scanning SIEM		
Att-Malware	Communication Direction	1. Walder and 1. Walder	1997
Web Reputation	Direction of Deep Security Manager to AgentiAppliance communication	E Interfed (Bidrectional)	
7 result	Heatbeat		
Intrusion Prevention	Heartbeat (Werval (In minutes):	Intertied (10 binutes)	•
Integrity Montoring	Number of Headbears that can be missed before an alert is name.	Inhertied (2)	
Looperation	computer between heartseats before an alert is raised:	HINGTON (UNITABLE)	
- cogniticoni	 Make Office Errors For Inactive Virtual Machines. 	interited (Na)	(*)
Interfaces	Bend Paticy Changes Immediately		
a francisco de la companya de	Automatically send Policy changes to computers:	Interted (Yes)	··•}
Updateo	Training to the second		
Overnites	Looping Level	Inhediat (for hot friends)	7743
	Agent Set Protection	Terr I	100
	modiling the Agent	File Instantion (Mark)	
	Local overside requires paperword	Yes.	
	Present	Ris	
	Patawar Patawar Samu Patawar		
	Environment variable overnides:		
	And Designed and the second seco		

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

	Computers with suf-	Aires v Britma v				
	The	Bitters. Attent	- Sen - Star	tix: [[Ceures]		
	August -	finantalise .	Pattern	Pote	date:	Last Sociacold Lipitan
	W formation 111					
	1 11117.7.91		Red Vel Steel	Linux Server Exerpte	Constant Control	177 FAILURE - Name
	T 42410000.036 wate	10.	April Had Briter	Sure .	Conception Contract	20 Annual Page
	B merffell men men	*	Barrow William	Wessian Deves Jack Se	ALCO DALLARS	Continues Apr.
1	2					
	0					

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 나 옴.

💽 관리자: 명령 프롬프트	
C:#>"#Program Files#Trend Micro#Deep Security Agent#dsa_control.exe" Sending the command to the agent on the local machine	harden=0
Config harden agent option successfully. C:#>_	

DSA 삭제

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

프로그램 제거 또는 변경

프로그램을 제거하려면 목록에서 선택한 후 [제거], [변경] 또는 [복구]를 클릭하십시오.

	구성 🔻		:== 👻 🔞
	이름 🔺	◄ 게시자	▼ 설치 날짜 ▼
	🛛 Citrix Xen Windows x64 PV Drivers	Citrix	2013-09-09
	🐼 Citrix XenServer Tools Installer	Citrix	2013-09-09
	🐼 Citrix XenServer VSS Provider	Citrix	2013-09-09
	🐼 Citrix XenServer Windows Guest Agent	Citrix	2013-09-09
	💼 Cloud, com VM Instance Manager	Cloud,com, Inc,	2013-09-09
	🌄 Microsoft ,NET Framework 4 Client Profile	Microsoft Corporation	2013-09-09
	- 😡 Microsoft ,NET Framework 4 Client Profile 한국어,,	, Microsoft Corporation	2013-09-09
	😡 Microsoft ,NET Framework 4 Extended	Microsoft Corporation	2013-09-09
ſ		. Microsoft Corporation	2013-09-09
	🖲 Trend Micro Deep Security Agent	Trend Micro Inc,	2014-08-19
	colocal coming connect	КТ	2014-08-19
	- 🕿 Windows 드라이버 패키지 - Citrix Systems Inc. (. Citrix Systems Inc.	2013-09-09
	🕿 Windows 드라이버 패키지 - Citrix Systems Inc. (. Citrix Systems Inc.	2013-09-09
	🕿 Windows 드라이버 패키지 - Citrix Systems Inc. (. Citrix Systems Inc.	2013-09-09
	: 🕿 Windows 드라이버 패키지 - Citrix Systems, Inc. (,,	., Citrix Systems, Inc,	2013-09-09
	🛭 📚 Windows 도라이버 패키지 - Citrix Systems, Inc. (., Citrix Systems, Inc.	2013-09-09

● 리부팅

<u>Deep Security Manager 운영</u>

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

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

Deep Security Manager 9.0 Service Pack 1

View other versions

Product Pat	ch		
bit			
Release Date	File Name	Size (MB)	Download Package
2013-06-06	Manager-Windows-9.0.5370.x64.zip	178	
9.0.5370.x64.zip 1ed648d4e87be81d 19583c0dd59529a3	62c0a 17483c92006e		
	Product Pat	Product Patch it File Name 2013-06-06 Manager-Windows-9.0.5370.x64.zip 0.0.5370.x64.zip ed648d4e87be81d62c0a 9583c0dd59529a317483c92006e 9583c0dd59529a317483c92006e	Product Patch it Size (MB) 2013-06-06 Manager-Windows-9.0.5370.x64.zip 178 .0.5370.x64.zip 178 e6488d4e87be81d62c0a 9583c0dd59529a317483c92006e

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)

Deep Security
Username: Password: Sign In
Copyright © 2013 Trend Micro Inc. All rights reserved

Dashboard

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

TREND. Deep Security

Desidorat Alerta Ever	its & Reports Computers	Policies Ad	munistration		
Default 41 All + 24 Hour View + All Computers	•				
Abert Status × Critical D S Warreng D There are currently no alerte to report	Computer Status Computer Status Consuler Status Contrail Contrail Contrail Contrail Contrail Contrail Contrail Contrail Contrailer Status Contrailer Status Contrailer Status Contrailer Status Contrailer Status Contrailer Status Contrailer Status Contrailer Status Contrailer Status	 My Account Usemane Rolo Last Sign-In Previous Sign Total Sign-Ine 	Status 32 admit Full Access July 4, 2013 19:02 -In: July 4, 2013 17:48 3	My Sign-in History Last 4 Sign-in Alberryts July 4 2013 18:02 July 4 2013 17:02 July 3 2013 17:23 July 3 2013 15:23 July 3 2013 16:22	Buccess Buccess Buccess Buccess Fature

● Dashboard 추가

TREND Deep Security				
Auto Exe	nts & Reports Computers	Policies Administration	0e	
Senanti () Al -) (24 triair West -) Ad Correction	15 ¢			
Almost Annotae	Company Inser	 By Account in Account of Accoun	I New Deshiboard Name <mark>See Continued</mark> New Deshiboard Name <mark>See Continued</mark>	Cano

Dashboard Page를 추가하여 여러 관제 포인트를 가져가실 수 있습니다.

● Widget 추가/제거

Monitoring	<u>^</u>	
Activity Overview	=	
Alert History [2x1]		
Alert Status		
Computer Status		
Manager Node Status [3x1]		
Security Update Status		
System	 	
My Sign-in History		
Software Packages [2x1]		
System Event History [2x1]		
	-	
Anti-Malware		

• 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.

	eep Securit	ty .			
Dashboard	Alerts	Events & Reports	Computers	Policies	Administration
Alerts Summary View	w 👻 🛛 By Time	Ŧ			
Computers: All Comput	ters	•			
There are currently no ale	erts to report.				

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 있 습니다.

	ep Securi	ty			
Dashboard	Alerts	Events & Repor	ts Comp	uters Po	licies Administration
🗉 🛅 Events	Sys	tem Events All	No Grouping	1 🔻	
限 Generate Reports	Per	iod: Last Hour		•	
	Co	mputers: All Compu	ters	•	
		View 🔄 Export	- 省 Auto-Tago	jing 🏭 Colun	nns
	1	Fime 🔻	Level	Event ID	Event
		luly 4, 2013 18:02:17	Info	600	User Signed In
		July 4, 2013 18:01:38	Info	601	User Signed Out
		July 4, 2013 17:48:41	Info	600	User Signed In

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

Period:	Last Hour	•	
Computers:	All Computers	•	
📰 View	Export 👻 省 Auto-Tagging	Columns	_
Time 👻	Export to CSV		Event
📄 July 4, 201	😰 Export Selected to CSV	'n	System Settings Sa
Duly 4, 201	Export to CSV (With Full Description	/ ons)	events Retrieved
Duly 4, 201	Export Selected to CSV (With Full I	Descriptions)	Security Update Su
Duly 4, 201	5 15.11.10 min	001	Relay Group Update

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

Events	Generate Reports	
🔣 Generate Reports	Single Report Recurring Reports	
	Report: Select Report	
	Viser and Contact Report	
	Tag Filter Anti-Maiware Report Attack Report	
	All: Computer Report Summary Report	
	O Untagged: System Event Report	
	Tag(s): System Report 日子 学	

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.

Deshboard	Alert	n Events & Reports	Germanitern	Policies Administ	ration		
Competient		Computers With sub-G	roups + By Group +				
		🔄 New • 😭 Delete.	Details. Actions -	Events - DEvent	- Colum	ni	
		Name +	Description	Flatham	Palicy	Status	Last Successful Update
		E Computers (4)					
		E 10203.4		Red that Enher_	Tâxene	Manuped (Centre)	7 kimules Aga
		₩ 10.20.3.5		Red Hat Enter	None	Managed (Online)	7 Minutes Ago
		10.20.5.6		Red Hat Enter	None	Managed (Online)	7 Minufex Ago
		10.20.3.7		Red Hat Enter	None	Managed (Online)	5 Minutes Ago

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

Events & Reports	Computers	@ 10.20 1.4 - Chrome		
and the second sec		(* 1107/14.49.26.11 4119/Com	L=Clinut/Teetse antidation	
Computers With sub-G	roups - By Group -	Computer: 10.20.3.4		
Tiew - 👔 Delete	Details. Action		La statement i manage	
Name +	Description	Ovisiview	General Actions Events	
E Compiders (4)		Anti-Malware	General	THEFT
10.203.4		S Web Reputation	Display Name	Not State
· 10.20.3.5		O Firewall	Description	
10.20.3.6		🌝 Intrusion Prevention		
10.20.3.7	_	🔵 Integrity Monituring		
		() LogInspection	Platform	Red Hat Enterprise 5 (64 bit) (2.6.18-308 el5x
		📟 Interfaces	Group	Computers
		🍏 Settings	Policy	None
		Updates	Asset Importance.	None
		-ff Overndes	Download Security Opdates From	Default Relay Group
			Status	
			🛞 Agent	
			Status: e Manage	d (Online)
			Anti-Matware: Cft, no c	onfiguration
			Web Reputation I'm Off	

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

dtabus Last Buccessful Update Managed (Online) S Minutes Ago
Managed (Online) 7 Minuheskos Managed (Online) 7 Minuhes Ago Managed (Online) 7 Minuhes Ago Managed (Online) 6 Minuhes Ago Managed (Online) 6 Minuhes Ago
I Policy Isoad Security Update back Security Update Ivents I Warnings/Errors ade Agent Software Tor Recommendatione Scan for Malware for Open Ports
THE REAL PROPERTY AND INCOME.

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.

TREND. Deep Security



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



• 각 정책 템플릿에서 각 보안기능에 대한 상세 설정이 가능합니다.

Overview	Gene	ral Advanced	Events						
O Anti-Malware	- Intru	sion Prevention -							_
Web Reputation	intru intru	sion Prevention St	ate On		 Not Licensed 				
🕘 Firewall		Prevent							
intrusion Provention	0	Detect							
Integrity Monitoring	Assi	gned Intrusion Pre	vention Rules						_
C Log Inspection	A	ll 🕶							
🚥 Intertace Types	1	ssign/Unassign	Propertie	s 🗊 Export 🔹	Application Types	Column	h.,		
Callines		Name 🔺		Application Type	Priority	Severity	Mode	Туре	C
dia permita	° 😩	1000128 - HETP P	holocol Decod	Web Server Commo	n: 1-Low/	🗰 High	Prevent	Smart	W
Svenides	8	1000505 - Buffer o	verflow in get	Database MySQL	2 - Norma	l colow	Prevent	Vuinerab	N
	0	1000530 - Apache	htgrep Heade	Web Server Apache	2 - Norma	l 💼 Medium	Prevent	Exploit	N
	0	1000834 - SMTP D	ecoding	Mail Server Common	i 4 - Highe	t 🚥 Critical	Prevent	Smart	N
	0	1001028 - Apache	mod_cache	Web Server Apache	2 - Norma	e Medium	Prevent	Vuinerab.	N
	0	1001332 - Web Se	ever Apache '	Web Server Apache	2 - Norma	i 🐑 Medium	Prevent	Exploit	N

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

Policy: Base Policy	inux Server	
🙀 Overview	General Smart Protection Advanced Quarantined Files Events	
😵 Anti-Malware	Anti-Malware	
web Reputation	Anti-Maiware State. On	
🛞 Firewall	Real-Time Scan	
Intrusion Prevention	Configuration: No Configuration	Edit
Integrity Monitoring	Schedule: Select Schedule	Edit
S Log Inspection	- Manual Scan	
🎟 Interface Types		
ô Settings	Configuration: Default Manual Scan Configuration	Edit
Gverrides	Scheduled Scan	
	Inherited	
	Configuration: Default Scheduled Scan Configuration	Edit

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

Policy: Base Policy :	> Linux Server						-
Dverview	General Advanced Events						
O Anti-Matware	Intrusion Prevention	-					
C Web Reputation	Intrusion Prevention State On	Not Lic	ensed				
Firewall	Prevent						
Intrasion Prevention	C Detect						
Integrity Monitoring	Assigned Intrusion Prevention Rules						
C Log Inspection	All 🐨						
Interface Types	Assign/Unassign E Propertie	es 🔂 Export 🔹 💽 Application	Types_	Columns	-		
R. Defines	Name =	Application Type	Priority	Severity	Mode	Type	C.
(gr senings	1000128 - HTTP Protocol Decod	Web Server Common	T-Low	en High	Prevent.	Smart	W
-F Overrides	1000505 - Buffer overflow in get_	Database MySQL	2 - Normal	Low.	Prevent	Vuinerab	14
	🙁 1000630 - Apache htgrep Heade	Web Server Apache	2 - Normai	💼 Medium	Prevent	Exploit	N
	S 1000834 - SMTP Decoding	Mail Server Common	4 - Highest	con Critical	Prevent	Smart	N
	1001028 - Apache mod_cache	Web Server Apache	2-Normal	C Medium	Prevent	Vulnerab.	N
	1001332 - Web Server Apache '	Web Server Apache	2 - Normal	C) Nedium	Prevent	Exploit	14 -

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.

System Settings	System Settings
Scheduled Tasks Event-Based Tasks Nanaper Nodes Licenses User Management	Agents Alerts Contexts SIEM SHMP Ranking System Events Security Upstates Smart Feedback SMTP Storage Advanced Hostnames Update the "Hostname" entry if an IP is used as a hostname and a change in IP is detected on the computer after AgentiAppliance-initiated communication or di
Users Roses Contacts System intermation Updates	Algorithmater Advances Marken Agent-Initiated Advances Print And Companys Or Her Aventing Companys Or Her Aventing Companys Print Barryon Print Barryong Print Print Barryon Print Barryon Print
	El Allona Aguert fu rápicol, textificares # a compañía estil: Par Lance como encodo seculo El Apper constitución el allona d MAA El Afren (Autoriadante el anticione) (Max
	Data Privacy

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



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

El Event-Based Tasks		🚰 New 🏼 🏫 🗅	elete Prop	erties 🦉 🌽 Se	et Password	🗐 Synchronize	with Directory
Manager Nodes		Usemame 🝝	Name	Locked Out	Signed In	Last Sign	In
📕 Licenses	E	Full Access (1)					
User Management		🔏 admin			4	July 4, 2013	18:59
Se Roles	ſ	S New Usernam	e Properties - Chro	пе			
Contacts		A https://14.49	.26.11 4119/Admin	IstratorProperties.	screen?adminis	tratorID = 0	
A System Information		General Con	tact Information	Settings			
📑 Updates		- General Inform	nation				
		Username:	New User	name			
		Password:					
		Confirm Pass	word:				
		NOTE Passy	words on this system	m must:			
	**	• be	e a minimum of 8 ct ontain both alphabe	haracters long tic and numeric c	haracters		
		• cc	ontain both upper ar	nd lower case cha	aracters		
		0.000					
		• cd	ontain special (non	alphanumeric) ch	aracters		
		• co Name:	ontain special (non	alphanumeric) ch	aracters		
		• co Name: Description:	ontain special (non	alphanumeric) ch	aracters		
		• co Name: Description:	ontain special (non	alphanumeric) ch	aracters		
		• co Name: Description:	ontain special (non	alphanumeric) ch	aracters		
		• co Name: Description: Role:	Select Ro	alphanumeric) ch	aracters		Edil
		• co Name: Description: Role: Language:	Select Ro English (L	alphanumeric) ch le JS)	aracters		Edit
		• co Name: Description: Role: Language: Time zone:	Select Ro English (UTC-11.0	alphanumeric) ch le JS) 00) Niue Time (Pa	acific/Niue)		Edit
		• co Name: Description: Role: Language: Time zone: Time format:	Select Ro English (U UTC-11.0 © 12 Hou	le JS) J0) Niue Time (Pa J24 Hour	acific/Niue)		Edit
		• co Name: Description: Role: Language: Time zone: Time format.	Select Ro English (((UTC-11.) © 12 Hot	alphanumeric) ch le JS) JO) Niue Time (P: JI @ 24 Hour	acific/Niue)		Edit
		• co Name: Description: Role: Language: Time zone: Time format: Options	Select Ro English (UTC-11.) © 12 Hou	alphanumeric) ch le JS) JO) Niue Time (Pa JO) Niue Time (Pa	acific/Niue)		Edit

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

lam Seltinga wituked Tasko ne Based Tasko nagar Nacika pinteo wi Wanagémeni Usans	Up	dates							
ent-Based Tasks	5	ecurity Updates	Softwale Updates Relays						
anaper filoces		Component		Piatorm	Carrent Versi	Last Updated	Up-ts-date	Out-of-date	Percent Updated
oonsee ker Varagement Users Roles Contacts		Arth Histware							
		ministraji Ceceginan Pullanti		481754820111	0 867 80	Aug 4, 2013 10 11 17	3	11	1975
		IntelliTrap Patte	m	All Ptallorms	0.171.00	July 4, 2013 19-11-17	3	0	1085
		Smiant Scart Age	ent Pathets	All Ptationna	10.133.00	July 4, 2013 19 11:17	3	0	101%
stare intornation		Spream Active	Vonitoiry Patters	All Flatforms	1,413.00	July 4, 2013 19 11 17	3	0	- ANN-
DEPENDING IN CONTRACTOR		VSAPI Englise		Linux 64-bit	9.700.1002	July 4, 2013 10,11.17	3	0	1014
	H	Russ							(
		Intrustion Preven	Figs.1 bre. printmini Higher I and	All Ptatkiems	12.033	July 2, 2013 20 16 15	3	0	101%

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 적 용할 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

CVerverw.	General Computerts) U	Ising This Policy Events	
Ant-Malware	General		
Web Reputation	Description	Linux Server Sample	
Preval		An example panel of clinic servers.	
notnever? notautni 📀			
🕤 integrity Wondoring			4
Log inspection	inheritance	11	
interface Types	Parent Policy	1 None	
Settings	**	a Deep Security	
	Distance of the second s		
• Overrides		Eine Server	
P Overrides	Nadules	i Linux Server Solans Server R i Vindows	
P Overrides	Nodules Anti-Matware: Web Resulation:	Linux Server	• @ a. • @ a
Cverrdes	Nodules Anti-Matware: Web Reputation: Firewalt:	Dn Solaris Server Con Solaris Server Solaris Server Solar	• @ on • © or • @ or. 15 rules
Cverrides	Nodules Anti-Mahvare: Web Reputation: Firewalt Intrusion Prevention:	Linus Server Solaris Server R Windows Cn Inherited (Off) Dn On	• @ On • @ Ot • @ Ch. 15 rules • @ Drevent, 332 rules
- Overridea	Nodules Anti-Mateuare: Web Reputation: Firewalt: Intrusion Prevention: Integrity Monitoring:	Linux Server	• 🕞 Cn • 💬 Cr • 🕞 Cr. 15 rules • 🕞 Gravent, 332 rules • 😭 Cn, 24 rules

● "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

Assign Polic	у
Computer:	172.27.7.157
Policy:	None 🔺
	🖻 🙀 Base Policy
	🗉 🙀 Deep Security
	🙀 Linux Server
	🙀 Linux Server Sample
	🙀 Solaris Server
	🗉 🙀 Windows 🗸 🗸
	OK Cancel

 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.

Dashboard	Alerts	Events	& Reports	Computers	Policies	Adminis	tration		
Computera	c	omputers	With sub-Gr	oups 👻 🛛 By Grou	p +				
		Thew -	1 Delete	Details_ A	dions + Events	• 🔂 Export	- 🛄 Column	S	
		Name +	5	Description	1	Platform	Policy		Status
	an a	Computers (2	0						
		172217	157		3	Red Hat Enter	Linux Server S.	-	Managed (Omine)
		@ 42e1003	3-53/9-4c28-6			Red Hat Enter	None		Managed (Online)

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

Doolsboard	Alerte	Events & Reports	CONTRACTOR NO.	Policies /	dministration		
CITE AND	00	mputers (mm sus-6	kouta + RyGroep +				
	1	3 New + 12 Delete.	Details_ Action	a + Evena + 🕼	Export + 🔛 Celurare		
		Name +	Description	Plafern	Prince		394/1
		Contegularia (27					
		102.22.5.457		2610/2748	izi-		- In Reliagent stimines
		9 42+10033-539-4c39-		CD Export Se	lected to CSV lected to XML. (For Import	4	() Harrages (Dmine)
	-			Actions Counts Counts Colors Delation		;	Ng Athene Reactivitie Check States Description Send Policy
							Download Security Update Rist tact: Security Update Get Elimits Clear Warrings Enters Upgrade Apent Software
							🐨 Scan fai Recentriestations
							 Boan for Open Ports Boan for Wagath Recurd crispit: Desailore
							Move To Group . Assign Policy. Assign Absel Total.

• 상태 창을 확인하여 진행 상태 확인.

Desidenced	24m	Trends	& Reports	Concession in which	Policies	Advers	and the second second		
Recolute		Computers	1785 MA-Q1	Not + Rilling +	1				
		12 100 -	Color.	Detetti. Autor	a dienti	Siter	+ Downey		
		figme -		Description	11	Suffirm (Pally	Datas	
		E Crissies I	10						
		CONTRACTOR OF	187/1		10	and plat to over	and Seventian	nen 1 (
		W 40x1083	5.5340-4126-1		1	Ad Hat Enter	Nore	· manager (Critise)	-
	1								
	_								

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

Overview	General	Advanced	Events						
Ard-Malware	tritrusion	Prevention	Contraction of the second	0.0354	0352030				
Web Regulation	intrusion	Prevention S	talls: inherited (Ont 🕴 🍙 Pre	vent. 332 n.ies				
Frewall	8.00	and.							
intrusion Provention	(P CH								
nisgin Nontoring	Assigne	d Intrusion Pro	wention Rules -						
Log hapedian	All -								
Infertaces	Appl	gnUnaasign	Properti	es. 🗊 Ekport • 📺 Applica	san Types	Columna 🙀			
Settings	hiar	ne -		Application Type	Priority	Sewith	Histe	T)@#	1
Lindatas	101	0128 - HETPI	Protocol Decol	web Sever Commun	1-1.00	##High	Frenhl	Entat	
t opones	S 100	0505 - MysqL	Server get_sel	Distabase W/SQL	2-Normal	C Hadum	Prevent	Export	
Overvices	0 100	0030 - Apache	e htyres Heade	Web Server Apache	2+1401703	E Meidlom	Prevent	Exprov	
	9 100	0034 - SMTP	Decoding	Mail Server Common	4-Highes	Criscal	Prevant	Smart	. "
	Record	nesdations							
	Current	Stature		132 Intrusion Prevention Rule(s) as	igned.				
	Last Sci	an for Record	netdations a	ugust 18.2014 17:28					
	🏦 Um	eaclived Reco	mmesdalishs A F F	kesign 7 additional rule(k) ; Unassig atommendations could not be impl fullet.	in 239 currently emerited autor	vesigned nä natically: You	e(s) Some of must manual	the Ir assign/una:	asign 8
		239 of the rule Editor.	(a) recommend	ed for unassignment are assigned	at the policy law	el and can or	it) be unassig	net using the	Patic
	Citation in	the second second	of internation Designation	and the first strategies of the second strategies and	and the little				

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

IPS Rules	41 =	Recommended for As	signment + N	o Grouping 📼			9	ikarin.		
Haw -	Dela	AB		+ those	Applica	son Types	Columns	9		
1	iome =	Not Assigned	12		Priority	Seventy	Mode	Tipe	Category	
2 B C 1	004001-1	Recommended for As	säignment		2-tiernal	an Critical	Delet Only	Smart	16A	
() D E 1	005020 - D	Hecommended for U	nassignment		Z~Normal	<_Nedum	Detect Only	Smart	NA	
B	005063-R	estrict MySQL Datab	Database M/SQL		2 - Normal	E Nedum	Prevent	Smart	NIA	
C	005290 - 10	tentified Buspicious	Web Client Comm	non	2 - Normal	CT: High	Prevent	Smart	N/A	
C	005344 - P	OP3 Mail Server Pos	Mail Sever Comm	non	2 - Normal	Critical	Prevent	Smart	NA	
S 0 2 P 1	005511-0	rade NySQL Server	Oracle MySQL Inn	NOCE Nemicach	2-Normal	E Nedum	Prevent	Exploit	144	
S	005968 - D	racie MySQL Cilent	Database MySQL	Client	2 - Normal	ex: High	Prevent	Vuinerab	NA	

1			
		-	

 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.

- 3 Hule	5	AI *	Recommended for Un	tassignment +	No Grouping +	1		1	Permits		
C New	•	TT Del	AB		- hog	AppReat	ton Types	Colur	nns		
	N	ame e	Not Assigned			Priority	Severity:	Node	Type	Callegory	
28	10	000530 - A	Recommended for As	ssignment		Z - Normal	C Medium	Prevent	Exploit	NH.	
10.00	10	01028 - A	Hecommended for D	nassignment		2 - Normal	C Hedum	Prevent	Vulnerab	NIA	
秋田.	10	01332-V	veis Server Apache 1	Web Server Apar	she	2 - Normal	muibell つ	Prevent	Exploit	NA	
100	10	02687 - A	pache mod_prov_t	Web Server Apar	che	2 - Normal	C lledum	Prevent	Exploit	NA	
16.8	10	N- 55560	Iopila Firefox XBL Sc	Web Client Mozil	la Firefox	2 - Normal	E llecium	Prevent	Exploit	NA	
28	11	000534-1	Whiple Venture LITP	HTP Parenting		2 Normal	S Hedum	Prevent	Vulnerab.	NA	
×.	10	003536 - A	pache mus das un	워니고민이	인에세	S No.mar	14 Elin	Prevent	Explore	NIA	
18	10	003736 - 0	masg TFTP Serv	TFTP Server		2 - Normal	C Medum	Prevent	Vulnerab	N9A	
28	75	40-18	M Lotus Notes RSS	Web Client Com	mon	2 - Normal	E Medum	Prevent	Exploit	NA	
20	10	103893 - N	White Vendors MTP	NTP Server Linu	R	2 - Normal	m Medum	Prevent	Vulnerab	NIA	
23	30	084037-5	pamAssassin Milter	Mail Server Com	mon	2 - Normal	ca Critical	Prevent	Vulnerab	NISA	
10.00	10	04091-R	lestrict PDF Docume	Web Client Com	man	2 - Normal	co Critical	Prevent	Smart	NA	
18	10	04278 - L	ibTIFF td_stripbytec	Web Client Com	moti	2 - Normal	e Hedum	Prevent	Vulnerab	9414	
米田	11	04329 · L	ibpng Memory Contu	Web Client Com	man	Z - Normal	en High	Prevent	Vulnerab	N/A	
28	10	04347 - N	SINL Response Ha	Web Client Intern	set Explorer	2 - Normal	Critical	Prevent	Exploit	NIA	
10	10	04369 - A	pache CXF XVL DT	Web Server Apar	the	2 - Normal	et: High	Prevent	Exploit	N9A	
28	10	04371-1	tozila Firefox Otifuec	Web Client Mozi	la Firator	2 - Normal	C Nedum	Detect Onl	y Vulnerab	N/A	
*3	10	004394 - A	dobe Acrobat And R	Web Client Com	mon	2 - Normal	C Medium	Prevent	Exploit	NA	
14.75		- 2011	**** **********	the office of	500 cm	a	- 0.0	Return	14.4	6177	-

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



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

B Overview	General Advance	d Exents								
Anti-Matware	Initruston Preventio	n								
Web Reputation	Intrusion Preventio	in State: Dw		 Prevent, 	332 rules	5				
Emeral	Worusion Prevented	in Bahavior								
Print and a second second	Prevent									
Intraston Prevention	- L00953									
entegrity Monitoring	- Assigned Intrusion	Prevention Rules -								
Loginapedias	All =									
Interface Types	AssignUnassi	ph_ Property	iii. (DEmail +	Application T	ipes.	Columns				
Colleges	hanse -		Application Type	P	tion	Seventy	110.04	Tipe	0	
ceange	1000520 - HF	W Protocol Decold	Web Server Correct	n t	Lun	en High	Presenta	Smuel	12	
Overrides	3000005 - Mrt	OL Server get_sal	Database M/SGL	2	- Normal	E Medium	Prevent	Exploit	10	
	🙂 1000830 - Api	scheitigrep Heade	Web Server Apache	2	- Normal	C Hathem	Prevent	Explore	-10	
	C 1020834 - SM	TP Decoding	Mail Server Commo	- Highest	Critical	Frevent	Smart	10		
	🈗 1001028 - Api	when_bom whe	Web Derver Apache	- biormail	C Hedium	Prevent	Vulnerati	- 14		
	7	1 F	2016.2010.00111.001		\$11.00m		H			
	Recommendations									
	Current Status	3	32 Intrusion Preventio	n Rule(s) assigne	σ					
	Lunreactived R	ecommendations A c	asigo 7 additional rule cuid sót be implemen	els). Unassign 23 lad automatically. 1	9 currently You must	sesigned rul manually ass	e(s). Some of Igniunassign	the recommend 8 Rulai	ations	
	Autometically impl	ement intruston Pre-	entran Recommendat	ions (when possib	ziw).					
	Inherted (film)									

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 정책
 이 적용된 모든 컴퓨터에 변화 사항이 적용 됨.

s reu	95	A8 -	Recommended for U	nassignment +	No Grouping 👻	-		9	Sketh-		
14	w. +	1 De	All		+ 10d	Applicat	tion Types.	Colum	hs		
	N	ame +	NotAssigned			Priority	Sevents	Mode	Type	Category	
		000630	Recommended for A	ssignment		Z-Normal	👝 Nedum	If revent	Exploit	144	
1	1	001028	Hecommunities for C	itini ingrittate		2 - Normai	C Nedium	Prevent	Vulnerab	NAV.	
8	2	001332-1	Neb Server Apache	Web Server Apa	the	2 - Normal	C: Netturn	Prevent	Exploit	144	
8	5	002687-4	pache mod_prox_ft	Web Server Apa	che	2 - Normal	C Medium	Prevent	Exploit	NEA.	
¥.	3	003323 - 1	footilia Finefox XBL Sc.	Web Client Nozi	la Firefox	2 - Normal	C: Nedium	Prevent	Exploit	NIN.	
2	1	003531	A diple Vacators NTP	NTP Server Linu	¢	2-Normal	C Nedum	Prevent	Vulnerab	MA.	
1	1	D036	patherson way sun	Web Server Apa	che .	2 - Normal	etti High	Prevent	Exploit	14%	
R	1	0/0736-0	Insmasq TFTP Servi	TFTP Server		2 - Normal	E Medium	Prevent	Vulnerab	144	
₫.		003740 - 1	BM Lotus Notes RSB	Vieb Client Com	mon	2 - Normai	C Nedium	Prevent	Exploit	844	
2	P	003853-1	Autiple Vendors NTP	NTP Server Linu	0	2 - Normal	C: Nedum	Prevent	Vulnerab	144	
2	\$	004037 - 5	spamAssassin Nilter .	Mail Server Com	nion	2 - Normal	con Critical	Prevent	Vutnerab	NPA.	
H.	3	004081-F	Restrict PDF Docume	Web Citerit Com	men	2 - Normal	Critical	Prevent	Smart	N/A	
2	1	004278-1	INTIFF to_stipbylac .	Web Client Com	man	2 - Normal	C Nédum	Prevent	Vulnerab	M/A	
H)	1	004329 - 1	Itang Memory Comu	Vieb Client Com	mon	2 - Normal	er: High	Prevent	Vulnerab	144	
×.	1	004347-1	ISXML Response Ha	Web Client Inten	net Explorer	2 - Normal	Em Critical	Prevent	Exptoit	144	
1	- 1	004369 - /	pache CXF XML DT	Web Server Apa	the	2 - Normai	ett) High	Prevent	Exploit	P4/4	
2	3	004371-1	Indita Firefox Obtuec	Web Client Modil	la Fireftx	2 - Normal	C: Nedum	Detect Only	Vulnerab	144	
2	5	004394-4	dobe Acrobal And R	Web Client Com	nion	2 - Normal	C Nedum	Prevent	Exploit	NPA.	
14			d					Toronto.	the base state		

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 Antimalware 모듈이 스캔을 하다 서비스에 영향을 미치는 경우가 있기 때문 입니다. 서비스 별로 Exclusion해야할 리스 트는 아래의 사이트를 참고하세요. 아래의 링크에 정보가 없다면, 해당 솔루션 회사에 Anti-malware 솔루션 대비하 여 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

Dashboard Alerts	Events & Reports Comp	uters.	Admin	istration
Policies	Malware Scan Configu	rations No G	rouping +	
🖕 Common Objects	Thew • 👔 Detete	Properties.	. (D Outlicate)	Export • 👔 Colum
Firewall Rules	Name +		Scan Type	Directories to Scan
intrusion Prevention Rules	Q Default Manual Scan Cor	dguration .	Manual/Scheduled	Alt directories
👩 Integrity Monitoring Rules	Sefault Real-Time Scan (Configuration	Red Time.	All directories
C Log Inspection Rules	Default Scheduled Scan	Configuration	Select AII (3)	
et 📋 Lists		15	Export Selected to CSV	t _{me} -
Directory Lists		15	Export Select. 3 NML	(For import)
File Estension Lists		10	Dupicate	
D P Lists			Delate	
Pt MAC Lists			Daima-a	
PortLists		0.0	Properties	
E 😪 Other				
🗸 Contexts				
Firewall Stateful Configuration	2			
Malware Scat Colligurations				
Schedules				

 새로 생성된 object인 "Default Real-Time Scan Configuration (2)"을 클릭하여 상세 페이지 팝업 시킨 후 이 로 버거



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

New_	•	3
New_		28
File Extension List		
Calect File Extension Col.		EOR
Process Image File List Process Image Files (Windows	•	Ent
Process image File List Frocess image Files (Windows The 'Process image File Lis Deep Security Agent. The set	t) •	EM confy applies when the scan is being performed by a be ignored by a Deep Security Virtual Appliance
Process image File List Process image Files (Windows The 'Process image File Lie Deep Securit/ Agent. The set	ij • T setting ting will t	Effi conly applies when the scan is being performed by a be ignored by a Deep Security Virtual Appliance
Process image File List Process image Files (Windows The "Process image File Lie Deep Security Agent. The set	i) • f setting ting will t	Eff only applies when the scan is being performed by a be ignored by a Deep Security Virtual Appliance
1 Process Image File List Process Image Files (Windows The "Process Image File Lie Deep Security Agent. The set	r) • T setting ting will t	Efft only applies when the scan is being performed by a be ignored by a Deep Security Virtual Appliance
Process Image File List Process Image Files (Windows The "Process Image File Lie Deep Security Agent. The set	r setting ting will t	Efft confy applies when the scan is being performed by a be ignored by a Deep Security Virtual Appliance

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)

ieneral Assigned	To
General Information	
Name:	reday List Sample
Description:	
Directory(s): (One di	rectory per line)
Citamai	And References
C.sempt	
o.sempt	
Caemp	
C.sempi	
Claempi	
Claemp	
Chemp	
<u>이라의</u>	양식을 참고하여 입력
	양식을 참고하여 입력
O C atempy	양식을 참고하여 입력
O Calenty O Calenty Supported Formats Directory: DIRECTORY	양 <u>식을 참고하여 입력</u> Example ciProgram Filesi
O Calentry O C Calentry Supported Formats Directory: DIRECTORY Directory with Wild	양식을 참고하여 입력 Example: c:(Program Files). Card (*):
Orectory: Directory: Directory: Directory: Directory: Directory:	양식을 참고하여 입력 Example: c:Program Files\ CiProgram Files*\
Original Supported Formats Directory: DIRECTORY Directory with Wild DIRECTORY DIRECTORY DIRECTORY	양식을 참고하여 입력 Example: c:Program Files\ Card (*): C:Program Files*\ C:Program Files\SubDirName*\
Orectory: Directory: Directory: Directory with Wild Directory with	양식을 참고하여 입력 Example: c:Program Files\ Card (*): C:Program Files*\ C:Program Files\SubDirName*\
Orectory: Directory: Directory: Directory: Directory with Wild Directory with Wild	양식을 참고하여 입력 Example: c:Program Files\ Card (*): C:Program Files*\ C:Program Files\SubDirName*\ We: Example: S(windir)
Orectory: Directory: Directory: Directory with Wild Directory with	양식을 참고하여 입력 Example: c:Program Files\ Card (*): C:Program Files*\ C:Program Files\SubDirName*\ We: Example: S(windir)
Caterings Contractions Directory: Direc	양식을 참고하여 입력 Example: c:Program Files\ Card (*): C:Program Files\SubDirName*\ Ve: Example: S(windir)
Calentity Supported Formats Directory: DIRECTORY DIRECTORY* DIRECTORY* Environment Variat S(ENV VAR) Contractory DIRECTORY DIRECTORY BLOW TORY	양소식 을 참고하여 입력 Example: c:(Program Files) C:(Program Files)*) C:(Program Files)*SubDirfName*) Ne: Example: C(temp #Exclude the temp directory

 위와 같은 방법으로, "Default Manual Scan Configuration" 과 "Default Scheduled Scan Configuration"에 대 해서도 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

Policy: Base Policy	> windows > windows Server 2008 Sample	W He
E Oversew	General Smart Postedios Advanced Quarantined Files Events	
Astr Materia	Arth Malware	1
Web Reputation	Act-Manware State On • Un Name Tarter	
🕽 Firewall	Real Time Scan	
ethusion Prevention	Configuration Securit Real Time Price Configuration	
hitegrity biorutoring	Schedul Every Day Al Day + Est	
Logbospection		
Atterface Types	R meted	
🔋 Setinge	Configuration: The International Science Configuration: • 128	
F Dvertides	Bichetunet Stan	
	R metted	
	Configuration - Turbur Schedung Dark Configuration • 208	
		Case

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

Drethew .	General Smart Protection Advanced Quarantined Files Events	
😳 Anti-Malwata	And Halware	
C Web Reputation	Anto-Malware State: On • 🕞 Real Time	
💮 Firewall	Real-Time Scan	
C Intrusion Prevention	Contracting Cost a Day Cost Cost Cost Cost	
🕐 Integrity Monitoring	Schedule Even Day All Day • Ent	
Cog Impection		
interface Types	Interter	
👩 Settings	Configuration Default Manual Scan Configuration Sample	
P Overdes	Scheduled Scan The Configuration Default Scheduled Scan Configuration Sample The Configuration The Configuration The Configuration Default Scheduled Scan Configuration Default Scheduled Scan Configuration	

정책이 잘 전달 되는지 확인. 아래의 Sending Policy 가 끝난 후 Managed (Online) 상태가 되면 작업 완료
 전 1519 Deep Security

Çenfésarit	Alerts	Events & Reports	Constitute	Policies Add	mentation			
Geografien		Computers	With auto-Groups. +	B) Group =				
		CTREW.+	Deute. Deu	sta. Adona + Eve	ns + (Ditiger	+ Deturne		
		Martin -	Deac	19801	Platform.	Policy	304us	
		E Compatera (1)						
		MINISTER IN	11 ¹		Red Hol Erder	Times Server Earspie	A Renaged (Centre)	
		# 42x10033	63%-4:25.0		Rad Hat Eider	Titlet.	Alamaded (Crime)	
		ii met2844-3	Dod-affea-Bid		iterment with	Withdows Dever 2008 Sample	Banding Patito	

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

Dashboard Alerts	Events & Reports	Compute	ers Poli	cies 🦷	Manunestration	
System Settings	Scheduled T	asks				
Scheduled Tasks	Triew	Delete	Properties_	Duplicate	Run Task Now	
Manager Nodes	Name +		Type		Schedule	La
Licenses	🛃 Daily Compo	nent Update	Downioa	d Security U	Daily at 10:35	ha
🐉 User Management	Monthly Com	puter Report	Generate	and Send R	On the 1st of every month at 02:00	Au
🧥 Users						
🌆 Roles						
Contacts						
(2 System Information						
📑 Updates						

• Type과 스캔 주기 선택 후 Next

Type:	Scan Computers for Malware	•	
	O Hourly		
(r)	Daily		
	Weekly		
	Monthly		
	Once Only		

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

Start date: August 20,	2014		
Start time: 02:00 (Ð		
Every Day			
Weekdays			
Every 2	days		

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

Please identify the	computer(s) to scan	for Malware.
---------------------	---------------------	--------------

All Computer	S			
In Group:	Computers	~		
	🗹 Include sub-Groups			
Using Policy:	None	*		
	Include sub-Policies			
Computer:	172.27.7.157	•		
		< Back	Next >	Cancel

● 이름 지정 및 "Finish" 클릭

Name:	Daily Scan Computers for M		
Type:	Scan Computers for Malware		
Schedule:	Daily at 02:00		
Next Run:	August 20, 2014 02:00		
Details:	All Computers		
🖉 Run Task on 'Fini	sh'		

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

C Sestern Datlings	Scheduled Tasks					
E Sant Tract	🔄 New, 📑 Delate, 📰 Prope	etien. Duplicate	📴 Run Tant Now			
Nanacer Tipdes	ftarte e	Tipe	Rchedule	Last Run Time	Next Run Time	Detaks
	and R. Collectores and Collide	Destinat Beauty 11	Della M TE	Autorit 15 2014	watert 20 2014	Index selecter Security (2010)
2 Uber Managemeitt	E Dally Scat Computers for Makerere	Stat.Computers for	Dialty at 02 00	Faix.	August 20, 2014	
A Users	22 Monthly Contractor Reader	Generals and Send H	On the fail of every month at 02.00	August 11, 2014	Depletitier 1,2	Compose Napon
A Roles						
💽 Cardada						
(2 Systemation						
La Undales						

그 외의 Scheduled Task 설정

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

Dashboard Alerts	Events & Reports	Compu	ters Pol	cies	Administration	
System Settings	Scheduled	Tasks				
Scheduled Tasks	Triew	Delete	Properties_	Duplicate	Run Task Now	
Manager Nodes	Name +		Type		Schedule	La
Licenses	🛃 Daily Comp	onent Update	Downioa	d Security U	Daily at 10:35	ha
5 🐌 User Management	Monthly Con	nputer Report	Generate	and Send R	On the 1st of every month at 02:00	Au
A Users						
🌆 Roles						
Contacts						
System Information						
Updates						

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

Type:	Select Type 🔹	
	Select Type Discover Computers Download Security Updates Generate and Send Report Run Script Scan Computers for Integrity Changes Scan Computers for Malware Scan Computers for Open Ports Scan Computers for Recommendations Send Outstanding Alert Summary Send Policy	

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

Policy: Base Policy :	> Linux Server 2		@ 194
Dverview	Corruster Network Engine Scanning	EM	
O Anti-Matuare	Event Forwarding Frequency (From the Age	int/Appliance)	1
C Web Reputation	Period between sending of events	Inherited (69: Seconds)	
😑 Fireval	Anti-Malware Event Forwarding (From The	Agent/Appliance)	
Intrusion Prevention	3 Use inherited Settings	Ma Territorial	
Integrity Monitoring	Provand Events Te		
Cog hispection	Direct forward		
an Intert Types	The Party of the Harragen		1
O Settings-	UDP part to which events should be se	ns stoyes se sent	
ovenides	Syslog Pacety	Local 0	
	Syslog Format	Common Event Format	•
	Do Not Forward Events		
	Web Reputation Event Forwarding (From Th	he Agent/Appliance)	
	Use Inherited Settings		
	Forward Events to a remote computer	(via Sysiog) No	
	Forward Events To:		
	() Distance		
	· Harring Vola Man Mannenger		
	Manual of Pathens to Mid-ever	is should be been []	
	1.1	1.7	
	The second se		Class

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"버

Dashboard Ale	rts Events & Reports Computers	Policies	
(C) System Sections	System Settings 3		
Scheduled Tasks	gents Alarts Contaxts SIEM SNMP R	anking System Events Security Updates Smart Feedb	ack SM +)
Manager Nodes	System Event Notification (From The Manager)		and an and a second
Licenses	Forward System Events to a remote computer (via	Syslog)	
User Management	Hostname or IP address to which events should	be sent.	
System information	UDP port to which events should be sent.	514	
Updates	Syslog Fincility:	Local 0	
E 📑 Security	Syslog Format:	Common Event Format	
Roles	Systog messages will only be sent for the event	s selected on the System Events tab.	-
Download Center	W Other event types can be configured for syslog	notification from the policy editor or computer editor.	

<u>자주하는 질문(FAQ)</u>

패스워드 변경하는 방법은?

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

Dashboard	Alerts	Events & F	Reports	Computers	s	Policies	Administration
🍪 System Settings	Us	By Role	•				
Scheduled Tasks		🛉 New 🛛 🏦 🛙	Delete	Properties	🔑 Se	t Password	Synchronize with Direct
Manager Nodes	5	Username 🔺	Name	Lock	ed Out	Signed In	Last Sign In
E 🐉 User Managemen	t 🗉	APladmin (1)					
🔏 Users		🤱 dsmapi					N/A
Contacts	n	Full Access (1)	l	더블클릭			
Updates		& Masteradmin	1				August 14, 2014 11:15
	E	Useradmin (1)					
		& ucloudsm				1	August 14, 2014 11:16

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

	Contact Information Settings	
General	Information	
Usema	ne: Distolation	
Name		
Descrip	lon	
Role	Useradmin 💌	Eur
Langua	98 English (US)	•
Time zo	14: (UTC+9.00) Korea Standard Time (Asia/Secul)	
Time for	mat 0 12 Hour 🖲 24 Hour	
D Loc	red Out (Denied permission to sign in)	

DSM 스토리지 관리 방법은?

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

)ashboard	Alerts		Events	& Reports	: (Computers	Policies		Administration	_		
System Settings		Syste	m Settir	igs				- 1				
Scrieduled Tasks Event-Based Tasks Manager Nodes Licenses User Management Users Tontacts System Information Updates	~	Auto Auto Auto Auto Auto Auto Auto Auto	SIEM a Pruning - prnatically operationally operationally operatically operatically operationally operationall	SNMP delete Anti delete Wel delete Fire delete Inter delete Inter delete Log delete Sys delete Sys delete ser delete sou delete cou	Ranking -Malware Ev b Reputation wall Events usion Preven grity Monitor Inspection term Events ver logs older ners older 1 e versions t pdates to ke	System Events vents older than: n Events older than older than: ntion Events older than Events older than Events older than: older than: er than: than: o keep per platform eep:	Security : than: n: n:	Updates 7 Days 7 Days 7 Days 7 Days 7 Days 7 Days 13 We 5 10	Smart Feedback	SMTP	torage Advand	

● 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<mark>.</mark>
```

- 아래의 커맨드를 이용하여 리부팅
 - # Init 6

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

치 방법

- DSA 가 설치된 서버 관련 작업
 - o 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
 - o 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.

● Deep Security Manager 관련 작업

root@static ~]#

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

erview	Gene	eral Action	s Events						
	Gen	eral							
I-Maiware	Hos	tname:		10	0.64.1.66		(Last IP Used	1: 10.64.1.66)	
b Reputation	Disc	olav Name:							
ewall	Des	cription:		-					
usion Prevention									
arity Monitoring									
gnty Montoning	Plat	form:		An	nazon Linux AMI (64 bit) (3.10.35-43.137.amzn1.x86.6	54)			
Inspection	Gro	up:		C	computers	•			
erfaces	Poli	cy:		в	ase Policy Linux Server (SKcomms POC) Bi	•	Edit		
tinas "	Ass	et Importance	e:	N	one	V	Edit		
	Dow	vnload Securi	ity Updates F	From: D	efault Relay Group	\sim	Edit		
lates				-					
errides	Stat	us ———							
			🖲 Ag	gent					
	Sta	tus:	😑 Ma	anaged (On	line)				
	Ant	i-Malware:	of 💿	ff					
	We	b Reputation:	: 🧼 Of	ff					
	Fire	ewall:	ini 🌍 ini	herited (Tap), 15 rules				
	I Intri	ileinn Prai/an	tion: 2525 Ini	horitori (Tai	n) 88 milde				
Clear Warning	g/Err	·ors 클i	릭						
64.1.66 - Windows Interne	et Explo	orer							
rps:// 10.64.244.6 :4119/Co	ompute	rEditor scree	en?hostID=1	16					
				10					
mputer: 10.64.1.	.66			10					
mputer: 10.64.1. Overview	.66	General	Actions	Events					
mputer: 10.64.1. Overview Anti-Malware	.66	General	Actions anne.	Events					
mputer: 10.64.1. Overview Anti-Malware	.66	General Display N Descriptio	Actions hame.	Events					
mputer: 10.64.1. Overview Anti-Malware Web Reputation	.66	General Display N Descriptio	Actions arme.	Events					
mputer: 10.64.1. Overview Anti-Malware Web Reputation Firewall	.66	General Display N Descriptio	Actions arms. on:	Events					
mputer: 10.64.1. Overview Anti-Malware Web Reputation Firewall Intrusion Prevention	.66	General Display N Descriptio	Actions arme.	Events	Amazon Linux AMI (64 bit) (3.10.35-43.137.a	amzn1.x8	3_64)		
mputer: 10.64.1. Overview Anti-Malware Web Reputation Firewall Intrusion Prevention Integrity Monitoring	.66	General Display N Description Platform: Group:	Actions arme. on:	Events	Amazon Linux AMI (64 bit) (3.10.35-43.137.a	amzn1.x8	3_64) ▼		
mputer: 10.64.1. Overview Anti-Malware Web Reputation Firewall Intrusion Prevention Integrity Monitoring	.66	General Display N Description Platform: Group: Policy:	Actions rame. on:	Events	Amazon Linux AMI (64 bit) (3.10.35-43.137.a Computers Base Policy ▶ Linux Server (SKcomms PO0	amzn1.x84 C) Bi	5_64) v	Edit	
mputer: 10.64.1. Overview Anti-Malware Web Reputation Firewall Intrusion Prevention Integrity Monitoring Log Inspection	.66	General Display N Description Platform: Group: Policy: Asset Imp	Actions arme. on:	Events	Amazon Linux AMI (64 bit) (3.10.35-43.137.ε Computers Base Policy ► Linux Server (SKcomms POC None	amzn1.x84 C) Bi	3_64) • •	Edit Edit	
mputer: 10.64.1. Overview Anti-Malware Web Reputation Firewall Intrusion Prevention Integrity Monitoring Log Inspection Interfaces	.66	General Display N Description Platform: Group: Policy: Asset Imp Download	Actions arme. on: portance: d Security U	Events Jpdates Fro	Amazon Linux AMI (64 bit) (3.10.35-43.137.a Computers Base Policy ▶ Linux Server (SKcomms POO None m: Default Relay Group	amzn1.x84 C) Bi	6_64) ▼ ▼ ▼	Edit Edit Edit	
mputer: 10.64.1. Overview Anti-Malware Web Reputation Firewall Intrusion Prevention Integrity Monitoring Log Inspection Interfaces Settings	.66	General Display N Description Platform: Group: Policy: Asset Imp Download	Actions arme. on: portance: d Security U	Events Jpdates Fro	Amazon Linux AMI (64 bit) (3.10.35-43.137.∉ Computers Base Policy ▶ Linux Server (SKcomms POO None m: Default Relay Group	amzn1.x84 C) Bi	3_64) • • •	Edit Edit Edit	
mputer: 10.64.1. Overview Anti-Malware Web Reputation Firewall Intrusion Prevention Integrity Monitoring Log Inspection Interfaces Settings Updates	.66	General Display N Description Platform: Group: Policy: Asset Imp Download	Actions arme. on: portance: d Security U	Events	Amazon Linux AMI (64 bit) (3.10.35-43.137.a Computers Base Policy ➤ Linux Server (SKcomms POO None m: Default Relay Group	amzn1.x8/ C) Bi	3_64) ▼ ▼ ▼	Edit Edit Edit	
mputer: 10.64.1. Overview Anti-Malware Web Reputation Firewall Intrusion Prevention Integrity Monitoring Log Inspection Interfaces Settings Updates	.66	General Display N Description Platform: Group: Policy: Asset Imp Download	Actions arme. on: portance: d Security U	Events Updates Fro Agen Mana	Amazon Linux AMI (64 bit) (3.10.35-43.137.a Computers Base Policy ➤ Linux Server (SKcomms POO None m: Default Relay Group	amzn1.x8/ C) Bi	5_64) • • •	Edit Edit Edit	
mputer: 10.64.1. Overview Anti-Malware Web Reputation Firewall Intrusion Prevention Integrity Monitoring Log Inspection Interfaces Settings Updates Overrides	.66	General Display N Description Platform: Group: Policy: Asset Imp Download Status Status Anti-Malv	Actions arme. on: portance: d Security U ware:	Events Updates Fro Agen Mana G Off	Amazon Linux AMI (64 bit) (3.10.35-43.137.∉ Computers Base Policy ▶ Linux Server (SKcomms POO None m: Default Relay Group	amzn1.x84 C) Bi	3_64) ▼ ▼ ▼	Edit Edit Edit	
mputer: 10.64.1. Overview Anti-Malware Web Reputation Firewall Intrusion Prevention Integrity Monitoring Log Inspection Interfaces Settings Updates Overrides	.66	General Display N Description Platform: Group: Policy: Asset Imp Download Status Status Anti-Malw Web Rep	Actions arme. on: portance: d Security U ware: putation:	Events Updates Fro Mana Mana Off	Amazon Linux AMI (64 bit) (3.10.35-43.137.ε Computers Base Policy ▶ Linux Server (SKcomms POO None m: Default Relay Group	amzn1.x8i C) Bi	5_64) ▼ ▼ ▼	Edit Edit Edit	
mputer: 10.64.1. Overview Anti-Malware Web Reputation Firewall Intrusion Prevention Integrity Monitoring Log Inspection Interfaces Settings Updates Overrides	.66	General Display N Description Platform: Group: Policy: Asset Imp Download Status Status Status: Anti-Malv Web Rep Firewall:	Actions tarme. on: portance: d Security U ware: putation:	Events Updates Fro Agen Mana Off G Off G Inher	Amazon Linux AMI (64 bit) (3.10.35-43.137.a Computers Base Policy > Linux Server (SKcomms POO None m: Default Relay Group	amzn1.x8/ C) Bi	6_64) ▼ ▼	Edit Edit Edit	
Overview Anti-Malware Web Reputation Firewall Intrusion Prevention Integrity Monitoring Log Inspection Interfaces Settings Updates Overrides	.66	General Display N Description Platform: Group: Policy: Asset Imp Download Status Status Status Status Firewall: Intrusion	Actions arme. on: portance: d Security U ware: putation: Prevention:	Events Events Updates Fro Regen Mana Geno Off Geno Inher Ceno Inher	Amazon Linux AMI (64 bit) (3.10.35-43.137.a Computers Base Policy ▶ Linux Server (SKcomms POU None m: Default Relay Group nt aged (Online) ited (Tap), 15 rules rited (Tap), 88 rules	amzn1.x80 C) Bi	5_64)	Edit Edit Edit	
mputer: 10.64.1. Overview Anti-Malware Web Reputation Firewall Intrusion Prevention Integrity Monitoring Log Inspection Interfaces Settings Updates Overrides	.66	General Display N Description Platform: Group: Policy: Asset Imp Download Status Status Status Anti-Malv Web Rep Firewall: Intrusion Integrity I	Actions arme. on: portance: d Security U ware: putation: Prevention: Monitoring:	Events Events Updates From Reg Agen Mana Reg Off Reg Inher Reg Off Reg Inher Reg Off, 2	Amazon Linux AMI (64 bit) (3.10.35-43.137.ε Computers Base Policy ▶ Linux Server (SKcomms POO None m: Default Relay Group tt aged (Online) ited (Tap), 15 rules rited (Tap), 88 rules 24 rules	amzn1.x8i C) Bi	3_64) ▼ ▼ ▼	Edit Edit Edit	
mputer: 10.64.1. Overview Anti-Malware Web Reputation Firewall Intrusion Prevention Integrity Monitoring Log Inspection Interfaces Settings Updates Overrides	.66	General Display N Description Platform: Group: Policy: Asset Imp Download Status Status Status Status: Anti-Malv Web Rep Firewall: Intrusion Integrity I Log Inspe	Actions arme. on: portance: d Security U ware: putation: Prevention: Monitoring: ection:	Events Events Updates Fro Agen Mana G Off C Inher C Inher Off, 2 Off, 2 Off, 7	Amazon Linux AMI (64 bit) (3.10.35-43.137.a Computers Base Policy > Linux Server (SKcomms POU None m: Default Relay Group at aged (Online) ited (Tap), 15 rules rited (Tap), 88 rules Particl	amzn1.x8/ C) Bi	5_64)	Edit Edit Edit	
mputer: 10.64.1. Overview Anti-Malware Web Reputation Firewall Intrusion Prevention Integrity Monitoring Log Inspection Interfaces Settings Updates Overrides	.66	General Display N Description Platform: Group: Policy: Asset Imp Download Status Status Status Status: Anti-Malw Web Repp Firewall: Intrusion Integrity I Log Inspe Online:	Actions hame. on: on: portance: d Security U ware: putation: Prevention: Monitoring: ection:	Events Events Updates Fro Contemporate Service Cont	Amazon Linux AMI (64 bit) (3.10.35-43.137.a Computers Base Policy > Linux Server (SKcomms POO None m: Default Relay Group tt aged (Online) ited (Tap), 15 rules rited (Tap), 88 rules 24 rules 24 rules	amzn1.x80 C) Bi	5_64)	Edit Edit Edit	
mputer: 10.64.1. Overview Anti-Malware Web Reputation Firewall Intrusion Prevention Integrity Monitoring Log Inspection Interfaces Settings Updates Overrides	.66	General Display N Description Platform: Group: Policy: Asset Imp Download Status: Status: Anti-Malv Web Rep Firewall: Intrusion Integrity I Log Inspe Online: Last Corr	Actions rame. on: portance: d Security U ware: outation: Prevention: Monitoring: ection: nmunication	Events Events Updates From Mana Off Mana Off Off Off Off Off, 2 Off, 2 Off, 7 Yes May	Amazon Linux AMI (64 bit) (3.10.35-43.137.a Computers Base Policy ► Linux Server (SKcomms POU None m: Default Relay Group tt aged (Online) ited (Tap), 15 rules rited (Tap), 88 rules 24 rules 1, 2014 21:35	amzn1.x8 C) Bi	3_64) ▼ ▼ ▼	Edit Edit Edit	
mputer: 10.64.1. Overview Anti-Malware Web Reputation Firewall Intrusion Prevention Integrity Monitoring Log Inspection Interfaces Settings Updates Overrides	.66	General Display N Description Platform: Group: Policy: Asset Imp Download Status Status Status Status: Anti-Malw Web Rep Firewall: Intrusion Integrity I Log Inspi Online: Last Com	Actions arme. on: portance: d Security U ware: putation: Prevention: Monitoring: ection: nmunication Check Status	Events Events Updates Fro Agen Mana Off Off Off Off Off Off Yes May s	Amazon Linux AMI (64 bit) (3.10.35-43.137.a Computers Base Policy ► Linux Server (SKcomms POO None m: Default Relay Group tt aged (Online) ited (Tap), 15 rules rited (Tap), 88 rules 1, 2014 21:35 Clear Warnings/Errors	amzn1.x8i	3_64) ▼ ▼ ▼	Edit Edit Edit	

o 해당 컴퓨터의 상태가 "Managed(online)"상태로 돌아오면 작업 완료

Agent offline시 조치 방법 1 (리셋 후 다시 Activation)

```
• DSA가 설치된 서버 관련 작업
        o Offline 이 발생한 해당 서버에 접속 후 루트 권한 로그인
        o 아래의 커멘드로 DSA 리셋 실행

    #/opt/ds_agent/dsa_control -r

           아래와 같은 메시지가 나오면 잘 수행 된 것
        0
[root@static ~]# /opt/ds agent/dsa control -r
Sending the command to the agent on the local machine...
Agent reset successfully.
[root@static ~]#
        o 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
 Sending the command to the agent on the local machine...
Attempting to connect to https://
                                            :4120/
Connected successfully - attempting SSL handshake.
SSL handshake completed successfully - initiating command session.
Connected with AES256-SHA to peer at
Connected with AES256-SHA to peer at
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
 - o Deep Security Manager 로그인
 - o Computer 탭에서 신규 생성된 computer 더블 클릭
 - 아래의 hostname 필드의 값을 신규 IP로 입력후, 우측 하단의 "save"버튼 클릭

Computer: 10.64.1.6	6						Q
		General Actions Events					
Anti-Malware		General	-				
Web Reputation		Display Name:	L	10.64.1.66			(Last IP Used: 10.64.1.66)
Firewall		Description:					
Intrusion Prevention							
Integrity Monitoring		Diatform		Amerop Linux	AMI /64 bit) /2 10 25 42 127 amont v06	64)	
C Log Inspection		Group:		Computers	Amii (04 bit) (5.10.35-45.137.am2n1.x80_	•4)	
Interfaces		Policy:		Base Policy	Linux Server (SKcomms POC) Bi	-	Edit
Settings	~~	Asset Importance:		None		\checkmark	Edit
Updates		Download Security Updates From	m:	Default Relay	Group	~	Edit
Overrides		_ Status					
		Agen	t				
		Status: 😝 Mana	iged (Online)			
		Anti-Malware: 💮 Off					
		Web Reputation: Off					
		Firewall:	ited (T	Гар), 15 rules			
		Intrusion Prevention: 🧥 Inheri	itod (Tan) 88 rulee			

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

Operating System: CentOS 6	.0			
Download Description	Release Date	file Nome	Size (MB)	Download Package
Product Patch English	2014-0fr-10	Apent-RedHat-EL6-9.0.0- 3500.686.rpm 32-bit	3,43	<u>الج</u>
O More details				
Product Patzn English	2014-06-10	Agent-Andhat 616-9.0.0-3500 x86- 64.rpm 64-bit	0.52	٠.
O More details				

• 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 드라이 버와 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

Bytes per line 4 * 8 16 32 64 0: A7 07 28 81 . (. latch Position In Buffer 1 (0x1) latch Position In Stream 400 (0x190) (.	Seneral Tags Data		
4 * 8 16 32 64 0: A7 07 28 81 . (, atch Position In Buffer 1 (0x1) atch Position In Stream 400 (0x190) (,	Bytes per line		
0: 47 97 28 81 (. latch Position In Buffer: 1 (0x1) latch Position In Stream: 400 (0x190) . (.	© 4 ⊕ 8 © 16 © 33	2 🗇 64	
Aatch Position In Buffer 1 (0x1) Aatch Position In Stream 400 (0x190) . (.	0: x7 07 28 81		
· (.	Aatch Position In Buffer Aatch Position In Stream	1 (0×1) 400 (0×190)	
			Î

URI값은 HTTP 프로토콜의 헤더 값입니다. DS는 Application 계층이 아닌 트랜스포트 계층에서 트래픽을 캡쳐 합니 다. 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 이룰 이 방어하는 취약점에 대한 정보를 보실 수 가 있습니다.

General Vulner	ability Config	uration Opti	ons Assigned To		General Vulnerability Configuration Options Assigned To				
General Informatio	on			^					
Name:		Windows	Media Encoder Buffe	r Overrun Vuln	Windows Modia Encoder Buffer Overrun Vulnerability				
Description:		A remote exists in t installed I Series. Th remote co	code execution vulne the WMEX.DLL Active by Windows Media E the vulnerability could ade execution if a use	er views a	Date Reported: September 10, 2008 Type: Other				
Minimum Agent/A	Appliance Versi	on: 4.0.0.0			Severity: (Critical)				
Application Type:	Web Client In	ternet Explore	r T	dit	CVSS Score: 9.3				
Priority:	2 - Normal			•	Description				
Severity:	Critical			•	Stack-based buffer overflow in the WMEncProfileManager ActiveX control in				
CVSS Score:	9.3				to execute arbitrary code via a long first argument to the GetDetailSString				
Detect Only					Solution: Apply this rule.				
Events					External References:				
Disable Even	t Logging				Microsoft MS08-053 Bugtrag 31065				
Generate	Event On Pack	ket Drop			Mittre CVE-2008-3008				
 Always In Enable D 	nclude Packet [ebug Mode	Data			microsoft windows-nt 2003 microsoft windows-nt 2000 microsoft windows-nt 2003 microsoft windows-nt vista				
Identification —					microson windows-nt xp				
Туре:	Exploit								
Issued:	October 1, 200)8							
Last Updated:	June 25, 2014			-					
		ОК	Cancel	Apply	OK Cancel Apply				

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

🚳 1002760 - Windows Media Encoder Buffer Overrun Vulnerability	Web Client Internet Explorer	2 - Normal	🚥 Critical	Pr
1 02475 - Application Control For Telnet Client	Application Control For Remote L	2 - Normal	🚥 Critical	De
I 02314 - Application Control For Opera Web Browser	Application Control For Web Brow	2 - Normal	🚥 Critical	De
003869 - Microsoft Internet Explorer Uninitialized Memory Corruption Remote Code Exec	Web Client Internet Explorer	2 - Normal	🚥 Critical	Pr
4 1002466 - Application Control For ICQ	Application Control For Instant Me	2 - Normal	🚥 Critical	De
🙆 1004288 - Identified Suspicious Shellcode In HTMI Documents 으며, Configuration 탭을 확인하시어 어떤 설정이 있는지 확인 하심.	Web Client Common 으로 룰을 이해 하실 수 있	<mark>2 - Normal</mark> 습니다.	ritical	Pri

Configur	abon Options -			
inspect/	ignore port range	a::,		
🛎 insp	ect all ports			
C Igno	re port ranges (specify)		
C insp	ect port ranges	(specify)		
Port ran	ges (e.g.25,35-1	00) 23		
Event Fr	equency			
Gen	erate event alw	6/5		
· Gen	erate event onc	e every 'n' second:	(specify)	
Gen	erate event onc	e every 'nth' conne	ction (spec	(fy)
Value of	n (1-99999) : 1	800		
				View Rules

Log Inspection Rules Require Log File 상태 해결 방법

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

로그를 지정해 줘야 할 룰 확인 하기

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

Computers (2)			
172.27.7.157	Red Hat Enter Linux Server S	🎒 Log Inspection Rules Require Log Files	0 Minutes Ago
🦁 42e10033-53f9-4c28-b	Red Hat Enter None	😝 Managed (Online)	1 Hour Ago

● 해당 Computer를 더블 클릭하여 상세화면 출력 및 상태 클릭

Overslaw	General Actions E	vents			
 Anti-Idatware Web Reputation Firewall 	- General Hostname Display Name Description		DIFFORMUT		(Last IP Used: 172.27.7.157)
3 Intrusion Prevention					
C Log Inspection	Platform:		Red Hat Enterprise 6 (54 bit) (2.6.32-358 4/6 x86_54)		
interfaces	Group		Computers		
Settings	Policy		Base Policy + Linux Server Sample		Eet
j Updates	Asset Importance		None	•	. Tint
Gvemides	Download Security Up	dates From.	Default Relay Group		£A.
	Status	Agent	ection Rules Require Log Files		
	Anti-Marware.	CH UN			
	Web Reputation	C of			
	Firewall:	🕞 On, 15 n	des		
	Intrusion Prevention:	Prevent	332 rules		
	Integrity Manitoring	G Und land	action Dulan Demote Lon Ellan		
	Coline.	Yes	Same rans Aspare Log rass		
		1022			

 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.

Time:	August 18, 2014 16:15:08
Level:	Warning
Event ID:	588
Event:	Log Inspection Rules Require Log Files
Target:	172.27.7.157
Event Origin:	Agent
Action By:	System
Manager:	172.27.176.167
Description The following Lo	g Inspection Rules require log files to monitor:
Description The following Lo Authentication Application - Si	g Inspection Rules require log files to monitor: Module - Unix Pluggable Authentication Module ecure Shell Daemon (SSHD)

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

Anti-Malware	r i on inspection			
Web Reputation	Log inspection state: On	• 🖬 0	on, 7 rules	
Sirewall	Assigned Log Inspection Rules			
S Intrusion Prevention	Assign/Unassign Propertie	s 🖸 Export • 🚭	Decoders SColumns	
Integrity Monitoring	Name +	Type Last Update	d	
S Log Impection	1002797 - Database Server - My	Defined July 14, 2010	0	
Interface Types	1002815 - Authentication Module	Defined January 9, 20	013	
🝵 Settings 🛛 🚽	1002828 - Application - Secure S 1002831 - Unix - System	Defined January 9, 20 Defined July 13, 2011	013	
👎 Oversides	1003443 - Mail Server - Postfix	Defined August 25. 2	010	
	🚯 1003447 - Web Server - Apache	Defined March 23, 20	911	

• 상단에서 Assigned 만 보도록 설정

Log Inspection Rules	Assigned 👻	No Group	ing 🔻		Q Search
Image: New Image:	All Assigned Not Assigned Recommende Recommende	d for Assign	ment	• 🖶 Decoders 🏭 Col	lumns
Image: Second	ation Module	Defined Defined	January 9, 2013 January 9, 2013		
1002831 - Unix - Sy	slog	Defined	July 13, 2011		
Image: Service of the servi	ver - Postfix ver - Apache	Defined Defined	August 25, 2010 March 23, 2011		
c					

• 로그를 넣어 줘야 하는 룰 클릭.

Log	j Insp	Assigned Vo Grouping Vo Groupi		Q Search
	hew	▼ 1 Delete Properties □ Duplicate Structure Content version	📑 Colu	umns
		Name 🔺	Туре	Last Updated
()		1002792 - Default Rules Configuration	Defined	March 19, 2010
()		1002797 - Database Server - MySQL	Defined	July 14, 2010
()		1002815 - Authentication Module - Unix Pluggable Authentication Module	Defined	January 9, 2013
۷ 🏵	/	1002828 - Application - Secure Shell Daemon (SSHD)	Defined	January 9, 2013
۲ 🌮		1002831 - Unix - Syslog	Defined	July 13, 2011
()		1003443 - Mail Server - Postfix	Defined	August 25, 2010
(/	1003447 - Web Server - Apache	Defined	March 23, 2011

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

Log Inspection Rule Properties	Configuration	Options			
Configuration Options					
Inherited					
Log Files to monitor:					
/var/log/secure			Add)	
		*	Remove)	
		-			
Turne of Lee File (a)					
Type of Log Flie(s): syslog	•				
This rule matches events decor	ded as: SSHD				
5700 - SSHD messages group	ed			Default - Ignore	T
5701 - Possible attack on the	e SSH server (or v	ersion gatheri	ng)	Default - High (8)	T

● 하단의 창으로 이동하는 것 확인 후 "OK" 버튼 클릭

Log Inspection Rule Properties Configu	uration Options				
Configuration Options				A	
Inherited				- 11	
Log Files to monitor:					
harllagisacura		Add			
Walnog/secure		Remove			
		*			
Type of Log File(s): syslog	•				
This rule matches events decoded as: S	SHD				
5700 - SSHD messages grouped			Default - Ignore	_	
5701 - Possible attack on the SSH se	rver (or version gatl	nering)	Default - High (8)	.	
		ОК	Cancel	Apply	

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

Log Ins	pection Rules Assigned 💌 No Grouping 💌		Q Search	 -
📑 Nev	v 🔹 👔 Delete 📰 Properties [] Duplicate 🔂 Export 🔹 🖷 Decoders.	📑 Col	umns	
	Name 🔺	Туре	Last Updated	
S	1002792 - Default Rules Configuration	Defined	March 19, 2010	
ی 🧐	1002797 - Database Server - MySQL	Defined	July 14, 2010	
S	1002815 - Authentication Module - Unix Pluggable Authentication Module	Defined	January 9, 2013	
(4)	1002828 - Application - Secure Shell Daemon (SSHD)	Defined	January 9, 2013	
ی 🧐	1002831 - Unix - Syslog	Defined	July 13, 2011	
ی 🧐	1003443 - Mail Server - Postfix	Defined	August 25, 2010	
ی 🧐	1003447 - Web Server - Apache	Defined	March 23, 2011	

아< Cancel
 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 있습니 다.

DSA Diagnostic Package 생성

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



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

Dvarview	General Actions Events	
Anti-Malware Web Reputation	Activition Fingepost	3F A5 (2 ⁶ 55 (2) (2) (3A 3E (2A 37 F4 22 (2) (46 31 (3 ⁶ 7E (6) 16 F1 Deartheas
Tinewal	Poley	
 Integrity Monitoring 	Last "Sent Policy" request: Last successful "Send Policy" operation	August 14: 2014 19:38 m. August 21: 2014 19:04
Log Inspection	Software	variat sets to d
5 Betlings	Upgrade Agent.	500 Carrow "Suggrade Agent"
J Updates Overrides	Support Create Diagnostic Package	

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

The diagnostic wizard will help you prepare a diagnostic package for support. Please choose what information you would like to include in the package:

- Configuration
- System Information
- Running Processes
- Driver Setup Logs
- Latest Events (On Computer Hard Drive)
- Latest Events (Recorded By Manager)
- Driver Statistics (Version 7.0 and Higher)

Latest Dump File			
	< Back	Next >	Cancel

DSR Diagnostic package 생성

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

Dashboard	Alerts Events &	Reports	Comp	ultera.	Policies	Administrati	on			
Computere	Computers V	With sub-Groups	s + By	Group +				Q Seath		10
	📑 New 🔸 🍵	Delete	Detaits	Actions +	Events +	Export +	Columns.			
	Name +	1	Descrip	Platform			Policy			Status
	8 Computers (3)									
	100dad2c-a	206-4110-9		Red Hat Enter	prise 6 (64 bit)		Linux Serve	121		Update of C
	🕎 44 38/23-et	E1-4245-st		Red Hall Enter	prise li (64 bit)	S	None		Ð	Managed (
	CC 12811-30	dd-tfea-8d		Microsoft Wind	dows Server 20	08 R2 (64 bit)	Windows Se	river 2008 (2)		Lipdate of C

DSM Diagnostic package 생성

•

아래의 순서로 클릭 TREND. Deep Security Dashboard Alerts Events & Reports Computers Policies System In 3 mation System Settings Scheduled Tasks Refresh 🛛 🛃 Create Diagnostic Package. > Demo Mode. Event-Based Tasks System Activity (Over The Last Hour) Manager Nodes Network Map with Activity Graph Elcenses Licenses 🐌 User Managemen System Information 1 updates Manager Node E Security Online Rules P.99 Patterns 🖹 📴 Software Download Center Local 🚺 Relay Groups SQL Server Primary System Details Include advanced diagnostic data (may be slow) System Details a 🔄 System E 🗑 Manager Node: 1 College 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