

Windows Server 2003 EOS를 대비한 "How to migrate" 고객 세미나

2015년 7월 14일,
Windows Server 2003 지원 종료!

- 날짜: 2014년 5월 28일 수요일
- 시간: 13:30 ~ 17:15
- 장소: 한국마이크로소프트 광화문 사무실 11층





보안 관점에서 살펴본

Windows Server 2003 vs. Windows Server 2012

Seung Joo Baek

Sr. Technical Evangelist

Microsoft Korea

Windows Server 2003 EOS를 대비한

"How to migrate" 고객 세미나



Windows Server 2003, How to migrate

Security

Windows Server 2003 EOS를 대비한

"How to migrate" 고객 세미나





오늘의 게스트 스피커

INDEX

PRODUCT

PRESS

ABOUT

CONTACT



Services with SEcurity.

SEWORKS IS WORLD'S BEST MOBILE SECURITY COMPANY CONSISTING OF HACKERS WHO HAVE HIGH LEVEL OF PROFICIENCY IN SECURITY FIELD OF EXPERTISE.

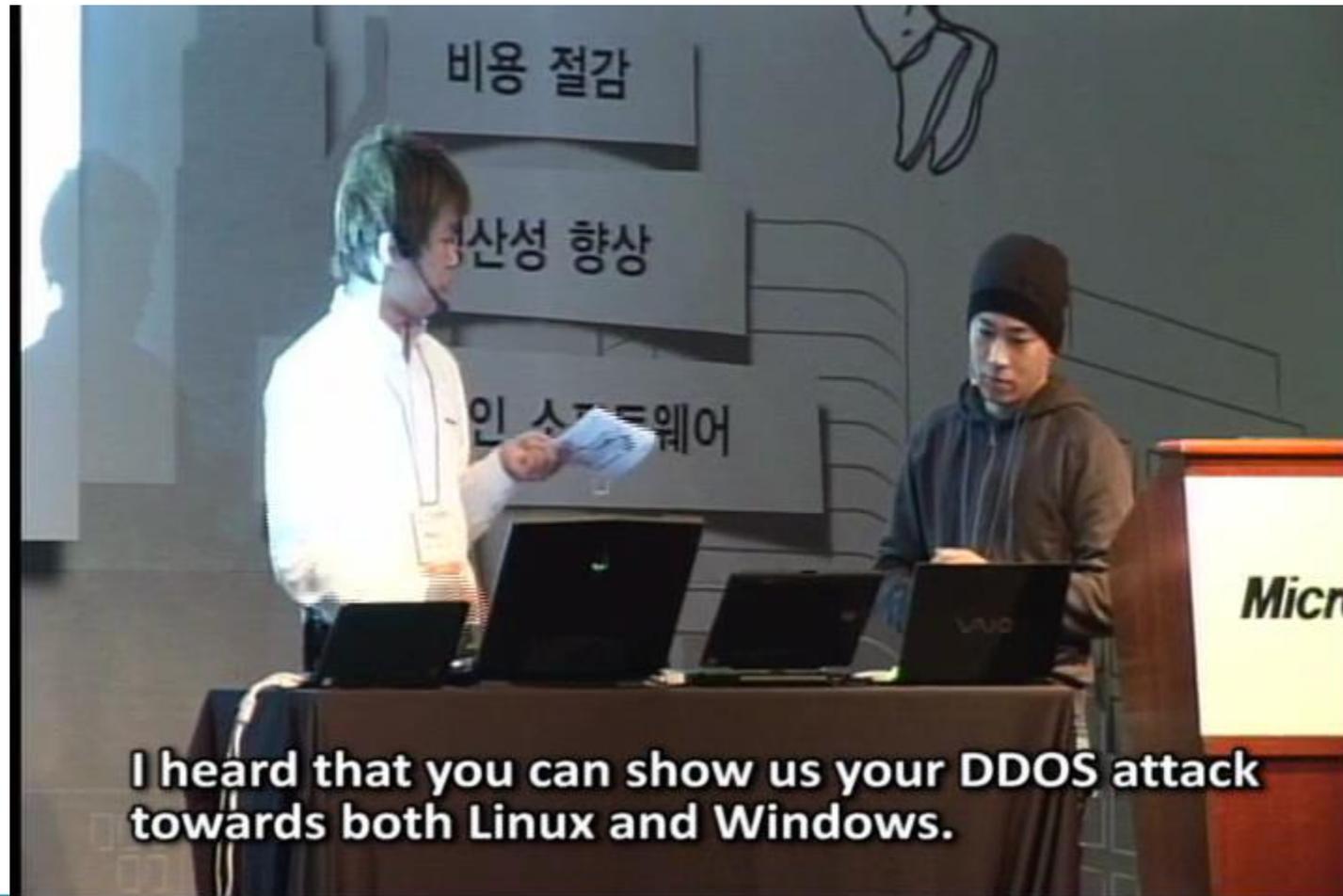


홍민표 (Min Pyo Hong) 기업인

경력사항	학력사항	수상내역
2012.12 ~		에스이웍스 대표이사
2008.07 ~ 2012.12		쉬프트웍스 대표이사
1999.08 ~		와우해커 대표



2009.11.02 @ Windows Server 2008 R2 Launch



1st Point

Patch

Windows Server 2003 EOS를 대비한
"How to migrate" 고객 세미나





매월 2주차 수요일이면...

2014년 5월 Microsoft 보안 업데이트

Microsoft의 정기적인 월례 보안 업데이트 계획에 따라 2014년 5월 14일 신규 보안 업데이트 8건이 발표되었습니다.

세부 정보 받기

IT 전문가 및 시스템 관리자

해당 업데이트에 관한 자세한 정보는 [Microsoft TechNet](#) 을 참조하시기 바랍니다.

최신 업데이트 다운로드를 위해

해당 업데이트에 관한 자세한 정보는 [Microsoft 업데이트](#) 를 참조하시기 바랍니다.

최신 보안 업데이트

공지 번호	공지 제목	공지 KB
MS14-021	Internet Explorer 보안 업데이트	2965111
MS14-022	Microsoft SharePoint Server의 취약점으로 인한 원격 코드 실행 문제점	2952166
MS14-023	Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점	2961037
MS14-024	Microsoft 공용 컨트롤의 취약점으로 인한 보안 기능 우회	2950145
MS14-025	그룹 정책 기본 설정 취약점으로 인한 권한 상승 문제점	2962486
MS14-026	.NET Framework의 취약점으로 인한 권한 상승 문제점	2958732
MS14-027	Windows 셸 처리기의 취약점으로 인한 권한 상승 문제점	2962488



2015년 7월

Seoul, KOR



Today 26°C/16°C



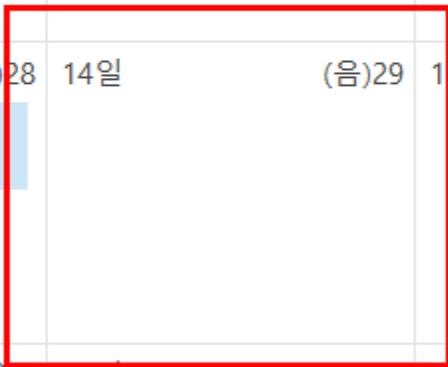
Tomorrow 29°C/14°C



목요일 30°C/14°C

Search 일정 (Ctrl+E)

일요일	월요일	화요일	수요일	목요일	금요일	토요일
6월 28일 (음)13	29일 (음)14 13:00 Eva's Weekly meeting; 16F Andes Room; Han Hong Choi	30일	보름 7월 1일 (음)16	2일 (음)17	3일 (음)18	4일 (음)19
5일 (음)20	6일 (음)21 13:00 Eva's Weekly meeting; 16F Andes Room; Han Hong Choi	7일 (음)22	8일 (음)23	9일 (음)24	10일 (음)25	11일 (음)26
12일 (음)27	13일 (음)28 13:00 Eva's Weekly meeting; 16F Andes Room; Han Hong Choi	14일 (음)29	15일 (음)30	그믐 16일 (음)1	유월 17일 (음)2	18일 (음)3
19일 (음)10	20일 (음)11	21일 (음)12	22일 (음)13	23일 (음)14	24일 (음)15	25일 (음)16





업데이트를 안하게 되면 어떤 결과가...

2nd Point

Basic Security

Windows Server 2003 EOS를 대비한

"How to migrate" 고객 세미나



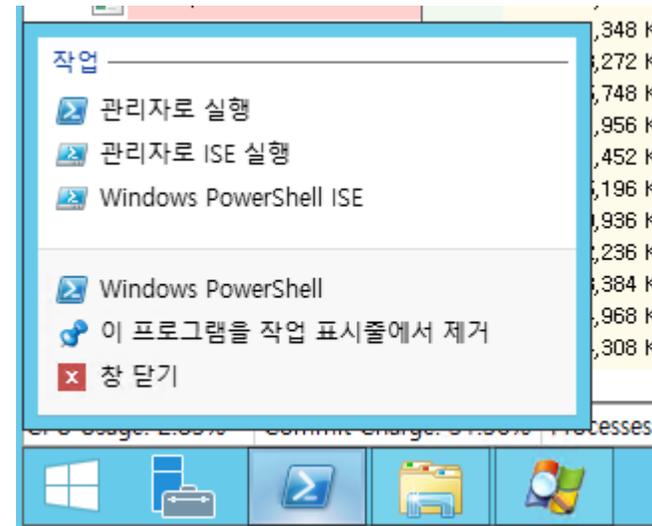
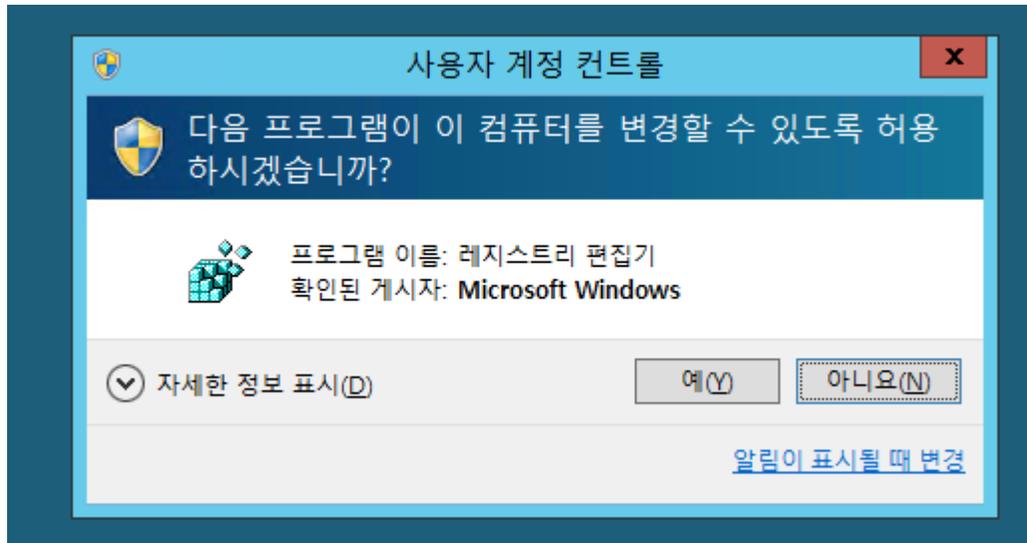


가장 기본적인 차이, 커널

- Windows Server 2003
 - NT Kernel v5.2
- Windows Server 2012 R2
 - NT Kernel v6.3
- SDL(Security Development Lifecycle)이 초기 시점부터 반영되었는지
- 보안에 대한 기본 골격이 갖춰져 있는지

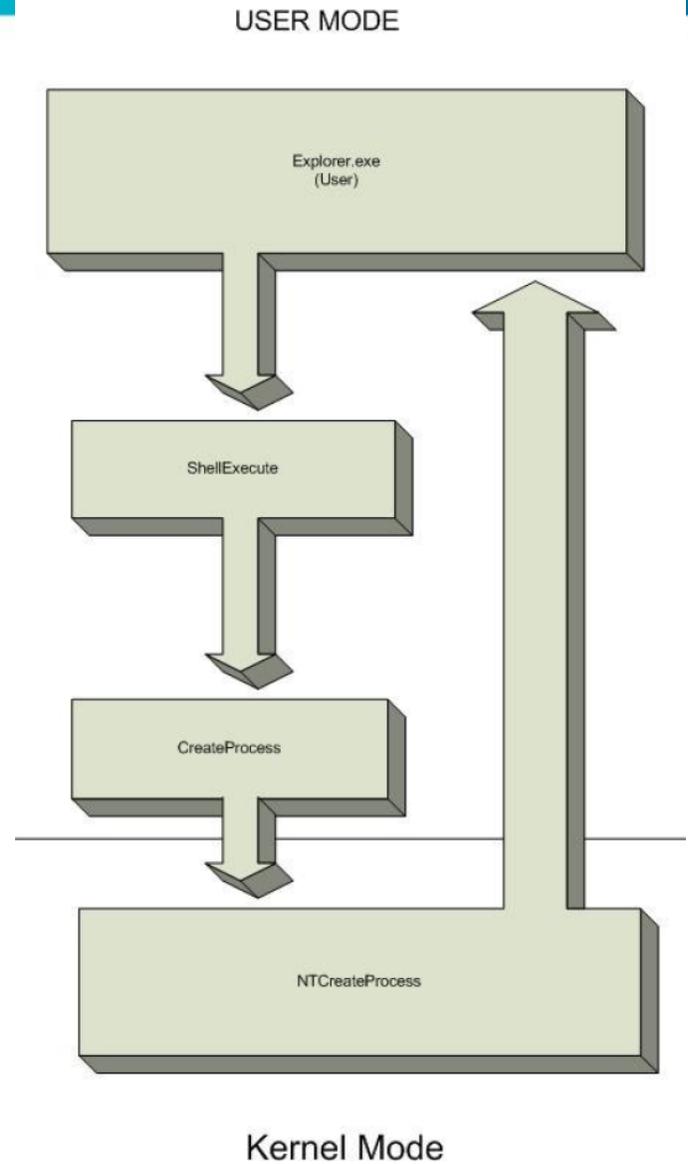
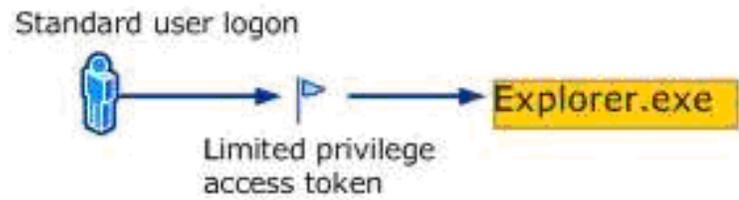
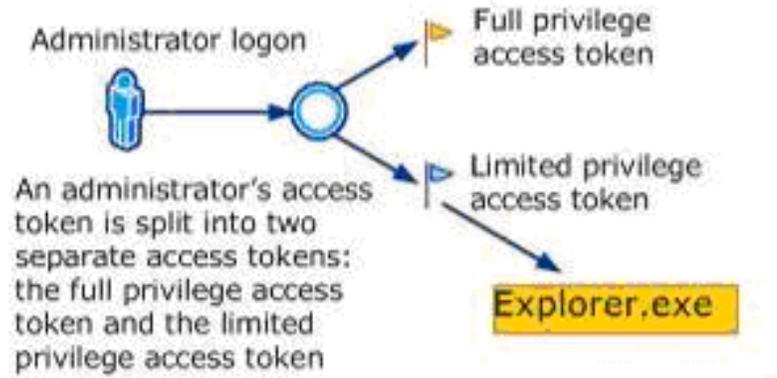


사용자 계정 컨트롤 (UAC)





Windows Legacy Process Creation





보안의 기본, Permission, 그리고 Windows 리소스 보호

ntoskrnl.exe 등록 정보

그룹 또는 사용자 이름(G):

- Administrators (MP2003\Administrators)
- Power Users (MP2003\Power Users)
- SYSTEM
- Users (MP2003\Users)

Administrators의 사용 권한(P)

	허용	거부
모든 권한	<input checked="" type="checkbox"/>	<input type="checkbox"/>
수정	<input checked="" type="checkbox"/>	<input type="checkbox"/>
읽기 및 실행	<input checked="" type="checkbox"/>	<input type="checkbox"/>
읽기	<input checked="" type="checkbox"/>	<input type="checkbox"/>
쓰기	<input checked="" type="checkbox"/>	<input type="checkbox"/>
특정 권한	<input type="checkbox"/>	<input type="checkbox"/>

특정 권한 및 고급 설정을 보려면 [고급]을 클릭하십시오.

ntoskrnl 속성

개체 이름: C:\Windows\System32\ntoskrnl.exe

그룹 또는 사용자 이름(G):

- ALL APPLICATION PACKAGES
- SYSTEM
- Administrators (MP2012R2\Administrators)
- Users (MP2012R2\Users)
- TrustedInstaller

사용 권한을 변경하려면 [편집]을 클릭하십시오.

Administrators의 사용 권한(P)

	허용	거부
모든 권한		
수정		
읽기 및 실행	<input checked="" type="checkbox"/>	
읽기	<input checked="" type="checkbox"/>	
쓰기		
특정 권한		



Windows Integrity Mechanism

- 개별 프로세스의 보안 토큰에 IL이 부여
- IL의 예
 - Low – 보호 모드의 Internet Explorer(IE)와 해당 IE에서 실행된 프로세스
 - Medium – Standard User 프로세스
 - High – 권한이 상승된 Administrator 프로세스
 - System – System 서비스
- IL 역시 상속
- IL을 확인할 방법 – Whoami, Process Explorer, AccessChk, Icacls

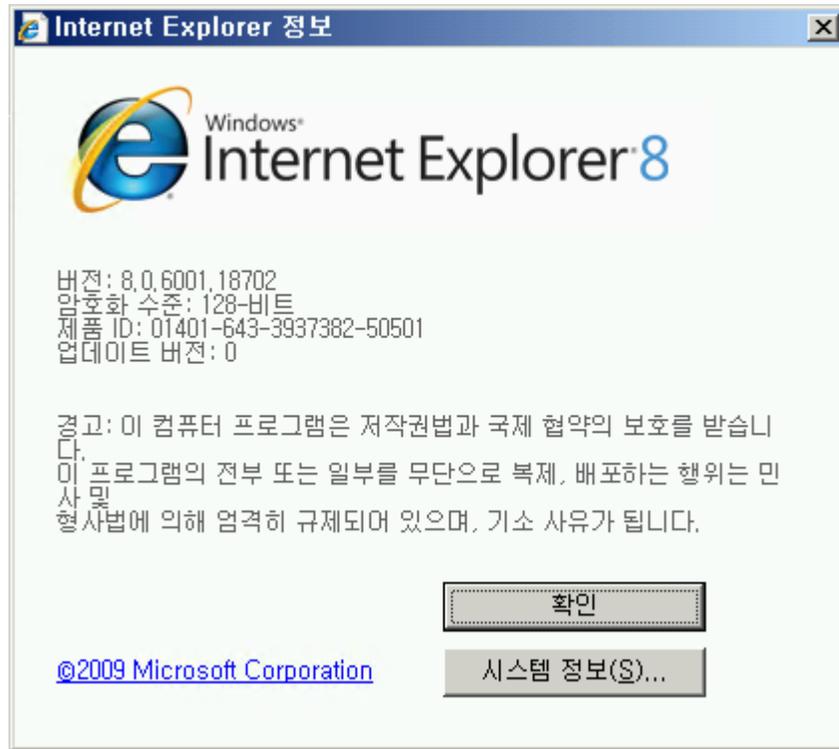


Windows Integrity Mechanism

explorer.exe	0,04	40,604 K	98,780 K	860 Windows 탐색기	Microsoft Corporation	Medium
procexp.exe		2,236 K	7,456 K	1140 Sysinternals Process E...	Sysinternals - www,s...	High
procexp64.exe	1,87	13,408 K	29,988 K	3508 Sysinternals Process E...	Sysinternals - www,s...	High
powershell.exe		64,824 K	65,704 K	3024 Windows PowerShell	Microsoft Corporation	Medium
conhost.exe	< 0,01	4,308 K	11,324 K	2168 콘솔 창 호스트	Microsoft Corporation	Medium
mmc.exe		12,540 K	34,040 K	3572 Microsoft Management ...	Microsoft Corporation	High
ieexplore.exe	0,01	5,416 K	21,564 K	2432 Internet Explorer	Microsoft Corporation	Medium
ieexplore.exe	< 0,01	9,404 K	40,692 K	2356 Internet Explorer	Microsoft Corporation	Low



Internet Explorer, 그리고 보호 모드





세션 0 고립

- Windows Server 2003
 - 모든 Windows 관련 서비스가 로그인한 사용자와 같은 세션으로 동작
- Windows Server 2008 이후
 - 서비스를 Session 0에 고립시킴
 - 첫번째 로그인한 사용자를 Session 1에 배정
 - Session 0와 Session 1간에 상호 작용 금지



부트 영역에 대한 보호, 보안 부팅

시스템 요약

- 하드웨어 리소스
- 구성 요소
- 소프트웨어 환경

항목	값
OS 이름	Microsoft Windows Server 2012 R2 Datacenter
버전	6.3.9600 빌드 9600
기타 OS 설명	사용할 수 없음
OS 제조업체	Microsoft Corporation

KOALRAHV-01의 KOALRA-SECURITY-2012에 대한 설정

KOALRA-SECURITY-2012

- 하드웨어
 - 하드웨어 추가
 - 펌웨어
 - 파일에서 부팅
 - 메모리
 - 4096MB
 - 프로세서
 - BIOS 보드
 - BaseBoard 제조업체: Microsoft Corporation
 - BaseBoard 모델: 사용할 수 없음
 - BaseBoard 이름: 기관
 - 클래픽 연산: 데스크톱
 - 보안 부팅 상태: **설정**
 - PCR7 구성: 사용할 수 없음

펌웨어

보안 부팅

보안 부팅은 부팅 시 권한 없는 코드가 실행되지 않도록 하는 기능입니다. 이 설정을 사용하는 것이 좋습니다.

보안 부팅 사용(E)



보안 구조 개선, 그 나머지

- 커널 패치 보호
 - 코드 무결성
 - DEP/NX (Data Execution Protection)
 - ASLR (Address Space Layout Randomization)
 - 액티브 디렉터리의 커베로스 v5 이후 지원
-
- [http://technet.microsoft.com/en-us/library/cc771361\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc771361(v=ws.10).aspx)

3rd Point

Service Security

Windows Server 2003 EOS를 대비한

"How to migrate" 고객 세미나





Windows Server의 시스템 계정

- Local System
 - 가장 권한이 높은 내장 계정
 - NT AUTHORITY\SYSTEM
- Local Service
 - Users 그룹과 같은 권한
 - 네트워크 접근시 계정 정보를 가지지 않은 Null 세션
 - NT AUTHORITY\LOCAL SERVICE
- Network Service
 - Users 그룹과 같은 권한
 - 네트워크 접근시 컴퓨터 계정으로 인증
 - NT AUTHORITY\NETWORK SERVICE



서비스

파일(F) 동작(A) 보기(V) 도움말(H)

서비스(로컬)

서비스(로컬)

설명이 필요한 항목을 선택하십시오.

이름	설명	상태	시작 유형	다음 사용자 로그인
Alerter	선택...		사용 안 함	Local Service
Application Experience Lookup Service	응용...	시작됨	자동	Local System
Application Layer Gateway Service	인터...		수동	Local Service
Application Management	Acti...		수동	Local System
Automatic Updates	Win...	시작됨	자동	Local System
Background Intelligent Transfer Service	다른...	시작됨	자동	Local System
ClipBook	정보...		사용 안 함	Local System
COM+ Event System	SEN...	시작됨	자동	Local System
COM+ System Application	CO...		수동	Local System
Computer Browser	네트...	시작됨	자동	Local System
Cryptographic Services	Win...	시작됨	자동	Local System
DCOM Server Process Launcher	DC...	시작됨	자동	Local System
DHCP Client	컴퓨...	시작됨	자동	Network Service
Distributed File System	서로...		수동	Local System
Distributed Link Tracking Client	클라...	시작됨	자동	Local System
Distributed Link Tracking Server	도메...		사용 안 함	Local System
Distributed Transaction Coordinator	데이...	시작됨	자동	Network Service
DNS Client	이 ...	시작됨	자동	Network Service
Error Reporting Service	예상...	시작됨	자동	Local System
Event Log	이벤...	시작됨	자동	Local System
File Replication	여러...		수동	Local System
Help and Support	이 ...	시작됨	자동	Local System
HTTP SSL	HTT...		수동	Local System
Human Interface Device Access	키보...		사용 안 함	Local System
Hyper-V Data Exchange Service	물리...	시작됨	자동	Local System
Hyper-V Guest Shutdown Service	물리...	시작됨	자동	Local System
Hyper-V Heartbeat Service	정기...	시작됨	자동	Local System
Hyper-V Time Synchronization Service	이 ...	시작됨	자동	Local System
Hyper-V Volume Shadow Copy Requestor	볼륨...	시작됨	자동	Local System
IAS Jet Database Access	인터...		수동	Local System
IMAPI CD-Burning COM Service	IMA...		사용 안 함	Local System
Indexing Service	로컬...		사용 안 함	Local System
Intersite Messaging	Win...		사용 안 함	Local System
IPSEC Services	TCP...	시작됨	자동	Local System

확장 표준



서비스

파일(F) 동작(A) 보기(V) 도움말(H)

← → [Icons] [Icons] [Icons] [Icons] [Icons] [Icons]

서비스(로컬)

서비스(로컬)

설명이 필요한 항목을 선택하십시오.

이름	설명	상태	시작 유형	다음 사용자로 로그인
Active Directory Certificate Services	S/MI...	실행 ...	자동	Local System
ADFS(Active Directory Federation Services)	ADF...	실행 ...	자동(지연...	BLUE#ADFSservice
App Readiness	사용...		수동	Local System
Application Experience	응용 ...		수동(트리...	Local System
Application Host Helper Service	IIS에...	실행 ...	자동	Local System
Application Identity	응용 ...		수동(트리...	Local Service
Application Information	추가...	실행 ...	수동(트리...	Local System
Application Layer Gateway Service	인터...	실행 ...	수동	Local Service
Application Management	그룹 ...		수동	Local System
AppX Deployment Service (AppXSVC)	저장...		수동	Local System
Background Intelligent Transfer Service	유휴 ...		수동	Local System
Background Tasks Infrastructure Service	시스...	실행 ...	자동	Local System
Base Filtering Engine	BFE(...	실행 ...	자동	Local Service
Certificate Propagation	스마...	실행 ...	수동	Local System
CNG Key Isolation	CNG...	실행 ...	수동(트리...	Local System
COM+ Event System	SEN...	실행 ...	자동	Local Service
COM+ System Application	COM...		수동	Local System
Computer Browser	네트...		사용 안 함	Local System
Credential Manager	사용...		수동	Local System
Cryptographic Services	다음 ...	실행 ...	자동	Network Service
DCOM Server Process Launcher	DCO...	실행 ...	자동	Local System
Device Association Service	시스...		수동(트리...	Local System
Device Install Service	사용...		수동(트리...	Local System
Device Registration Service	Devi...		사용 안 함	BLUE#ADFSservice
Device Setup Manager	장치 ...		수동(트리...	Local System
DHCP Client	이 컴...	실행 ...	자동	Local Service
DHCP Server	IP 주...	실행 ...	자동	Network Service
Diagnostic Policy Service	진단 ...	실행 ...	자동(지연...	Local Service
Diagnostic Service Host	진단 ...		수동	Local Service
Diagnostic System Host	진단 ...		수동	Local System

< [Icons] > 확장 표준



서버 코어

The screenshot displays two overlapping Windows PowerShell windows within a virtual machine environment. The top window, titled "KOALRAHV-01의 KOALRA-SECURITY-2012 - 가상 컴퓨터 연결", shows the following command and output:

```
PS C:\Users\Administrator> <Get-Service>.count
133
```

The bottom window, titled "KOALRAHV-01의 KOALRA-SECURITY-CORE - 가상 컴퓨터 연결", shows the following command and output:

```
PS C:\Users\Administrator> <Get-Service>.Count
97
```

Scanning

Windows Server 2003 EOS를 대비한

"How to migrate" 고객 세미나





옛날에는

랜 케이블을 연결하지 않고 운영 체제를 설치한 적이 있었습니다. 😊



Windows Server 2003 SP2에서

Windows Server 설치 후 보안 업데이트

서버를 보호하기 위해 정책 설정 및 설치하는 동안 열린 포트는 제외하고 다른 모든 인바운드 연결이 차단되었습니다. 지금 다음 단계를 완료하십시오.

단계 1: 중요 보안 업데이트 설치 [자세한 정보\(M\)](#)

Microsoft는 바이러스 및 다른 보안 위협이 발견되는 즉시 Windows를 계속적으로 업데이트하며 사용자의 서버를 보호합니다. Windows Update에서 제공하는 모든 최신 보안 업데이트를 다운로드하고 설치하기를 권장합니다.

일부의 업데이트를 설치하면 Windows를 다시 시작해야 할 수도 있습니다. 업데이트 과정 중 Windows가 다시 시작되면 다음 순서로 진행하기 전, Windows Update를 다시 방문하여 모든 중요 업데이트가 올바르게 설치되었는지 확인해야 합니다.

[서버를 업데이트\(U\)](#)

단계 2: 자동 업데이트를 구성 [자세한 정보\(O\)](#)

자동 업데이트 기능을 사용하면 사용자가 지정한 일정에 따라 최신 보안 업데이트를 자동으로 다운로드할 수 있습니다. 이 서버는 이미 자동 업데이트를 사용하도록 구성되었습니다.

이 페이지를 닫고 서버에서 인바운드 연결을 허용하도록 하려면 [마침]을 클릭하십시오. 인바운드 연결 차단에 대한 자세한 정보는 [보안 구성 마법사 도움말을 참조하십시오.](#)

[마침\(F\)](#)



지금은

고급 보안이 포함된 Windows 방화벽

파일(F) 동작(A) 보기(V) 도움말(H)

로컬 컴퓨터의 고급 보안이 포함된 인바운드 규칙

이름	그룹	프로필	사용	작업	다시 정의	프로그램	로컬 주소	원격 주소	작업
AD FS HTTP 서비스(TCP-In)	AD FS	모두	예	허용	아니오	System	모두	모두	T
AD FS HTTPS 서비스(TCP-In)	AD FS	모두	예	허용	아니오	System	모두	모두	T
AD FS 스마트카드 인증 서비스(TCP-In)	AD FS	모두	예	허용	아니오	System	모두	모두	T
경계 게이트웨이 프로토콜(BGP-In)	BGP(경계 게이트웨이 프로...	모두	아니오	허용	아니오	%System...	모두	모두	T
BranchCache 콘텐츠 검색(HTTP-In)	BranchCache - 콘텐츠 검색...	모두	아니오	허용	아니오	SYSTEM	모두	모두	T
BranchCache 피어 검색(WSD-In)	BranchCache - 피어 검색(...	모두	아니오	허용	아니오	%systemr...	모두	로컬 서브넷	T
BranchCache 호스트 캐시 서버(HTTP-In)	BranchCache - 호스트 캐시...	모두	아니오	허용	아니오	SYSTEM	모두	모두	T
COM+ 네트워크 액세스(DCOM-In)	COM+ 네트워크 액세스	모두	아니오	허용	아니오	%systemr...	모두	모두	T
COM+ 원격 관리(DCOM-In)	COM+ 원격 관리	모두	아니오	허용	아니오	%systemr...	모두	모두	T
Device Registration Service(HTTPS-TCP-...	Device Registration Service	모두	아니오	허용	아니오	%WINDIR...	모두	모두	T
Device Registration Service(HTTP-TCP-In)	Device Registration Service	모두	아니오	허용	아니오	%WINDIR...	모두	모두	T
DHCPv4 릴레이 에이전트 [클라이언트](...	DHCP 릴레이 에이전트	모두	예	허용	아니오	%systemr...	모두	모두	U
DHCP 서버 v4(UDP-In)	DHCP 서버	모두	예	허용	아니오	%systemr...	모두	모두	U
DHCP 서버 v4(UDP-In)	DHCP 서버	모두	예	허용	아니오	%systemr...	모두	모두	U
DHCP 서버 v6(UDP-In)	DHCP 서버	모두	예	허용	아니오	%systemr...	모두	모두	U
DHCP 서버 v6(UDP-In)	DHCP 서버	모두	예	허용	아니오	%systemr...	모두	모두	U
DHCP 서버 - SCM을 사용한 원격 서비...	DHCP 서버 관리	모두	예	허용	아니오	%systemr...	모두	모두	U
DHCP 서버 장애 조치(failover)(TCP-In)	DHCP 서버 관리	모두	예	허용	아니오	%systemr...	모두	모두	T
DHCP 서버(RPC-In)	DHCP 서버 관리	모두	예	허용	아니오	%systemr...	모두	모두	T
DHCP 서버(RPCSS-In)	DHCP 서버 관리	모두	예	허용	아니오	%systemr...	모두	모두	T
DHCP 서버(SMB-In)	DHCP 서버 관리	모두	예	허용	아니오	System	모두	모두	T
DHCPv6 릴레이 에이전트[서버](UDP-In)	DHCPv6 릴레이 에이전트	모두	예	허용	아니오	%systemr...	모두	모두	U
DTC(Distributed Transaction Coordinato...	DTC(Distributed Transactio...	모두	아니오	허용	아니오	%System...	모두	모두	T
DTC(Distributed Transaction Coordinato...	DTC(Distributed Transactio...	모두	아니오	허용	아니오	%System...	모두	모두	T
DTC(Distributed Transaction Coordinato...	DTC(Distributed Transactio...	모두	아니오	허용	아니오	%System...	모두	모두	T
iSCSI 서비스(TCP-In)	iSCSI 서비스	모두	아니오	허용	아니오	%System...	모두	모두	T
Netlogon 서비스 인증(RPC)	Netlogon 서비스	모두	아니오	허용	아니오	%System...	모두	모두	T
Netlogon 서비스(NP-In)	Netlogon 서비스	모두	아니오	허용	아니오	System	모두	모두	T
Routing Information Protocol(RIP-In)	RIP(Routing Information Pr...	모두	아니오	허용	아니오	%System...	모두	모두	U
SMBDirect(iWARP-In)를 통한 파일 및 프...	SMBDirect를 통한 파일 및 프...	모두	아니오	허용	아니오	System	모두	모두	T

작업

- 인바운드 규칙
 - 새 규칙...
 - 프로필별 필터링
 - 상태로 필터링
 - 그룹으로 필터링
 - 보기
 - 새로 고침
 - 목록 내보내기...
 - 도움말



포트가 열렸다는 것은

단순하게 무엇을 하고 있다는 것만 의미하지 않습니다. 😊



5th Point

Web Server

Windows Server 2003 EOS를 대비한

"How to migrate" 고객 세미나





모듈 기반의 설치

Windows 구성 요소 마법사

Windows 구성 요소
 Windows 구성 요소를 추가 또는 제거할 수 있습니다.

구성 요소를 추가하거나 제거하려면 확인란을 클릭하십시오. 회색 상자는 일부 구성 요소만 설치됨을 나타내며, 포함된 항목을 보려면 [자세히]를 클릭하십시오.

구성 요소(C):

- 원격 저장소 5.3MB
- 응용 프로그램 서버 15.5MB
- 인덱스 서비스 0.0MB
- 인증서 서비스 1.4MB

설명: 인터넷 정보 서비스(IIS) 및 응용 프로그램 서버 콘솔을 포함합니다.

필요한 총 디스크 공간: 11.4MB
 사용 가능한 디스크 공간: 124950.4MB

[자세히(D)...]

응용 프로그램 서버

구성 요소를 추가 또는 제거하려면 확인란을 클릭하십시오. 확인란이 회색으로 표시된 항목에서는 구성 요소 중 일부만이 설치됩니다. 구성 요소에 포함된 항목을 보려면 [자세히]를 클릭하십시오.

응용 프로그램 서버의 하위 구성 요소(C):

- 네트워크 COM+ 액세스 사용 0.0MB
- 네트워크 DTC 액세스 사용 0.0MB
- 메시지 큐 7.0MB
- 응용 프로그램 서버 콘솔 0.0MB
- 인터넷 정보 서비스(IIS) 8.5MB

설명: FrontPage Server Extension, Active Server Pages(ASP)와 함께 웹, FTP, SMTP, NNTP 지원을 포함합니다.

필요한 총 디스크 공간: 11.4MB
 사용 가능한 디스크 공간: 124950.4MB

[자세히(D)...]

[확인] [취소]

역할 및 기능 추가 마법사

서버 역할 선택

시작하기 전
 설치 유형
 서버 선택
서버 역할
 기능
 확인
 결과

선택한 서버에 설치할 역할을 하나 이상 선택하십시오.

역할

- 웹 서버(IIS)(설치됨)
 - 보안(설치됨)
 - 요청 필터링(설치됨)
 - IIS 클라이언트 인증서 매핑 인증(설치됨)
 - IP 및 도메인 제한(설치됨)
 - URL 권한 부여(설치됨)
 - Windows 인증(설치됨)
 - 기본 인증(설치됨)
 - 다이제스트 인증(설치됨)
 - 중앙 SSL 인증서 지원(설치됨)
 - 클라이언트 인증서 매핑 인증(설치됨)
 - 상태 및 진단(설치됨)
 - HTTP 로깅(설치됨)
 - ODBC 로깅(설치됨)
 - 로깅 도구(설치됨)
 - 사용자 지정 로깅(설치됨)
 - 요청 모니터(설치됨)
 - 추적(설치됨)
 - 성능(설치됨)
 - 정적 콘텐츠 압축(설치됨)
 - 동적 콘텐츠 압축(설치됨)
 - 일반적인 HTTP 기능(설치됨)

설명

보안은 사용자 및 요청으로부터 웹 서버를 보호하기 위한 인프라를 제공합니다. IIS는 여러 인증 방법을 지원합니다. 서버의 역할에 따라 적절한 인증 체계를 선택합니다. 들어오는 모든 요청을 필터링하여 사용자 정의 값과 일치하는 요청을 처리하지 않고 거부하거나 시작 주소 공간에 따라 요청을 제한합니다.

< 이전(P) 다음(N) > 설치(O) 취소



기본 보안 기술

- IIS 관리자 인증 및 위임
- IP 주소 및 도메인 제한
- 권한 부여 규칙
- 요청 필터링(URLSCAN)

- 그리고 보안은 아니지만 이기종에 대한 지원



IIS 6 vs. IIS 8

Secunia Stay Secure About Secunia | Careers | Latest News | Blog | Login

Search

[PRODUCTS](#) [SOLUTIONS](#) [CUSTOMERS](#) [PARTNER](#) [RESOURCES](#) [COMPANY](#) [COMMUNITY](#)

Complete Patch Management

The Secunia CSI 7.0 gives you the when, the where, the what and the how. **It works the way you do.**

Try it now!

» Home » Community » Advisories » Advisories by Product

[Advisories](#) | [Research](#) | [Forums](#) | [Create Profile](#) | [Our Commitment](#)

[Database](#) | [Search](#) | [Advisories by Product](#) | [Advisories by Vendor](#) | [Terminology](#) | [Report Vulnerability](#) | [Insecure Library Loading](#)

Vulnerability Report: Microsoft Internet Information Services (IIS) 8.x

This vulnerability report for **Microsoft Internet Information Services (IIS) 8.x** contains a complete overview of all Secunia advisories affecting it. You can use this vulnerability report to ensure that you are aware of all vulnerabilities, both patched and unpatched, affecting this product allowing you to take the necessary precautions.

If you have information about a new or an existing vulnerability in **Microsoft Internet Information Services (IIS) 8.x** then you are more than welcome to [contact us](#).

<p>Table of Contents</p> <ol style="list-style-type: none"> 1. Product Summary Only 2. Secunia Advisory Statistics (All time) <ul style="list-style-type: none"> 2.1. Statistics for 2014 2.2. Statistics for 2013 2.3. Statistics for 2012 2.4. Statistics for 2011 2.5. Statistics for 2010 2.6. Statistics for 2009 2.7. Statistics for 2008 2.8. Statistics for 2007 2.9. Statistics for 2006 2.10. Statistics for 2005 2.11. Statistics for 2004 2.12. Statistics for 2003 	<p>Vendor, Links, and Unpatched Vulnerabilities</p> <table border="0" style="width: 100%;"> <tr> <td style="width: 20%;">Vendor</td> <td>Microsoft</td> </tr> <tr> <td>Product Link</td> <td>View Here (Link to external site)</td> </tr> <tr> <td>Affected By</td> <td>0 Secunia advisories 0 Vulnerabilities</td> </tr> <tr> <td>Monitor Product</td> <td>Receive alerts for this product</td> </tr> <tr> <td>Unpatched</td> <td>0% (0 of 0 Secunia advisories)</td> </tr> <tr> <td colspan="2">Most Critical Unpatched</td> </tr> <tr> <td colspan="2">There are no unpatched Secunia advisories affecting this product, when all vendor patches are applied.</td> </tr> </table>	Vendor	Microsoft	Product Link	View Here (Link to external site)	Affected By	0 Secunia advisories 0 Vulnerabilities	Monitor Product	Receive alerts for this product	Unpatched	0% (0 of 0 Secunia advisories)	Most Critical Unpatched		There are no unpatched Secunia advisories affecting this product, when all vendor patches are applied.	
Vendor	Microsoft														
Product Link	View Here (Link to external site)														
Affected By	0 Secunia advisories 0 Vulnerabilities														
Monitor Product	Receive alerts for this product														
Unpatched	0% (0 of 0 Secunia advisories)														
Most Critical Unpatched															
There are no unpatched Secunia advisories affecting this product, when all vendor patches are applied.															

Secunia Stay Secure About Secunia | Careers | Latest News | Blog | Login

Search

[PRODUCTS](#) [SOLUTIONS](#) [CUSTOMERS](#) [PARTNER](#) [RESOURCES](#) [COMPANY](#) [COMMUNITY](#)

Complete Patch Management

The Secunia CSI 7.0 gives you the when, the where, the what and the how. **It works the way you do.**

Try it now!

» Home » Community » Advisories » Advisories by Product

[Advisories](#) | [Research](#) | [Forums](#) | [Create Profile](#) | [Our Commitment](#)

[Database](#) | [Search](#) | [Advisories by Product](#) | [Advisories by Vendor](#) | [Terminology](#) | [Report Vulnerability](#) | [Insecure Library Loading](#)

Vulnerability Report: Microsoft Internet Information Services (IIS) 6

This vulnerability report for **Microsoft Internet Information Services (IIS) 6** contains a complete overview of all Secunia advisories affecting it. You can use this vulnerability report to ensure that you are aware of all vulnerabilities, both patched and unpatched, affecting this product allowing you to take the necessary precautions.

If you have information about a new or an existing vulnerability in **Microsoft Internet Information Services (IIS) 6** then you are more than welcome to [contact us](#).

<p>Table of Contents</p> <ol style="list-style-type: none"> 1. Product Summary Only 2. Secunia Advisory Statistics (All time) <ul style="list-style-type: none"> 2.1. Statistics for 2014 2.2. Statistics for 2013 2.3. Statistics for 2012 2.4. Statistics for 2011 2.5. Statistics for 2010 2.6. Statistics for 2009 2.7. Statistics for 2008 2.8. Statistics for 2007 2.9. Statistics for 2006 2.10. Statistics for 2005 2.11. Statistics for 2004 2.12. Statistics for 2003 	<p>Vendor, Links, and Unpatched Vulnerabilities</p> <table border="0" style="width: 100%;"> <tr> <td style="width: 20%;">Vendor</td> <td>Microsoft</td> </tr> <tr> <td>Product Link</td> <td>N/A</td> </tr> <tr> <td>Affected By</td> <td>11 Secunia advisories 11 Vulnerabilities</td> </tr> <tr> <td>Monitor Product</td> <td>Receive alerts for this product</td> </tr> <tr> <td>Unpatched</td> <td>9% (1 of 11 Secunia advisories)</td> </tr> <tr> <td colspan="2">Most Critical Unpatched</td> </tr> <tr> <td colspan="2">The most severe unpatched Secunia advisory affecting Microsoft Internet Information Services (IIS) 6, with all vendor patches applied, is rated Less critical ■■■■</td> </tr> </table>	Vendor	Microsoft	Product Link	N/A	Affected By	11 Secunia advisories 11 Vulnerabilities	Monitor Product	Receive alerts for this product	Unpatched	9% (1 of 11 Secunia advisories)	Most Critical Unpatched		The most severe unpatched Secunia advisory affecting Microsoft Internet Information Services (IIS) 6, with all vendor patches applied, is rated Less critical ■ ■ ■ ■	
Vendor	Microsoft														
Product Link	N/A														
Affected By	11 Secunia advisories 11 Vulnerabilities														
Monitor Product	Receive alerts for this product														
Unpatched	9% (1 of 11 Secunia advisories)														
Most Critical Unpatched															
The most severe unpatched Secunia advisory affecting Microsoft Internet Information Services (IIS) 6, with all vendor patches applied, is rated Less critical ■ ■ ■ ■															



IIS 6 vs. Apache Tomcat 7.x



Complete Patch Management

The Secunia CSI 7.0 gives you the when, the where, the what and the how. **It works the way you do.**

Try it now!

Home > Community > Advisories > Advisories by Product

Advisories | Research | Forums | Create Profile | Our Commitment

Database Search **Advisories by Product** Advisories by Vendor Terminology Report Vulnerability Insecure Library Loading

Vulnerability Report: Microsoft Internet Information Services (IIS) 6

This vulnerability report for Microsoft Internet Information Services (IIS) 6 contains a complete overview of all Secunia advisories affecting it. You can use this vulnerability report to ensure that you are aware of all vulnerabilities, both patched and unpatched, affecting this product allowing you to take the necessary precautions.

If you have information about a new or an existing vulnerability in Microsoft Internet Information Services (IIS) 6 then you are more than welcome to [contact us](#).

Table of Contents

- 1. Product Summary Only
- 2. Secunia Advisory Statistics (All time)
 - 2.1. Statistics for 2014
 - 2.2. Statistics for 2013
 - 2.3. Statistics for 2012
 - 2.4. Statistics for 2011
 - 2.5. Statistics for 2010
 - 2.6. Statistics for 2009
 - 2.7. Statistics for 2008
 - 2.8. Statistics for 2007
 - 2.9. Statistics for 2006
 - 2.10. Statistics for 2005
 - 2.11. Statistics for 2004
 - 2.12. Statistics for 2003

Vendor, Links, and Unpatched Vulnerabilities

Vendor	Microsoft
Product Link	N/A
Affected By	11 Secunia advisories 11 Vulnerabilities
Monitor Product	Receive alerts for this product
Unpatched	9% (1 of 11 Secunia advisories)
Most Critical Unpatched	The most severe unpatched Secunia advisory affecting Microsoft Internet Information Services (IIS) 6, with all vendor patches applied, is rated Less critical ■ ■ ■ ■



Complete Patch Management

The Secunia CSI 7.0 gives you the when, the where, the what and the how. **It works the way you do.**

Try it now!

Home > Community > Advisories > Advisories by Product

Advisories | Research | Forums | Create Profile | Our Commitment

Database Search **Advisories by Product** Advisories by Vendor Terminology Report Vulnerability Insecure Library Loading

Vulnerability Report: Apache Tomcat 7.x

This vulnerability report for Apache Tomcat 7.x contains a complete overview of all Secunia advisories affecting it. You can use this vulnerability report to ensure that you are aware of all vulnerabilities, both patched and unpatched, affecting this product allowing you to take the necessary precautions.

If you have information about a new or an existing vulnerability in Apache Tomcat 7.x then you are more than welcome to [contact us](#).

Table of Contents

- 1. Product Summary Only
- 2. Secunia Advisory Statistics (All time)
 - 2.1. Statistics for 2014
 - 2.2. Statistics for 2013
 - 2.3. Statistics for 2012
 - 2.4. Statistics for 2011
 - 2.5. Statistics for 2010
 - 2.6. Statistics for 2009
 - 2.7. Statistics for 2008
 - 2.8. Statistics for 2007
 - 2.9. Statistics for 2006
 - 2.10. Statistics for 2005
 - 2.11. Statistics for 2004
 - 2.12. Statistics for 2003

Vendor, Links, and Unpatched Vulnerabilities

Vendor	Apache Software Foundation
Product Link	View Here (Link to external site)
Affected By	15 Secunia advisories 33 Vulnerabilities
Monitor Product	Receive alerts for this product
Unpatched	0% (0 of 15 Secunia advisories)
Most Critical Unpatched	There are no unpatched Secunia advisories affecting this product, when all vendor patches are applied..



오늘의 게스트 스피커

- INDEX
- PRODUCT
- PRESS
- ABOUT
- CONTACT



Services with Security.

SEWORKS IS WORLD'S BEST MOBILE SECURITY COMPANY CONSISTING OF HACKERS WHO HAVE HIGH LEVEL OF PROFICIENCY IN SECURITY FIELD OF EXPERTISE.



홍민표 (Min Pyo Hong) 기업인

37세 (만 36세) | 남성 | 쌍둥이자리 | 말뚝

출생 1978년 5월 27일 (대전광역시)

소속 [에스이웍스](#) (대표이사)

사이트 [공식사이트](#), [미투데이](#), [트위터](#)

경력사항	학력사항	수상내역
2012.12 ~		에스이웍스 대표이사
2008.07 ~ 2012.12		쉬프트웍스 대표이사
1999.08 ~		와우해커 대표

6th Point

Security with Client

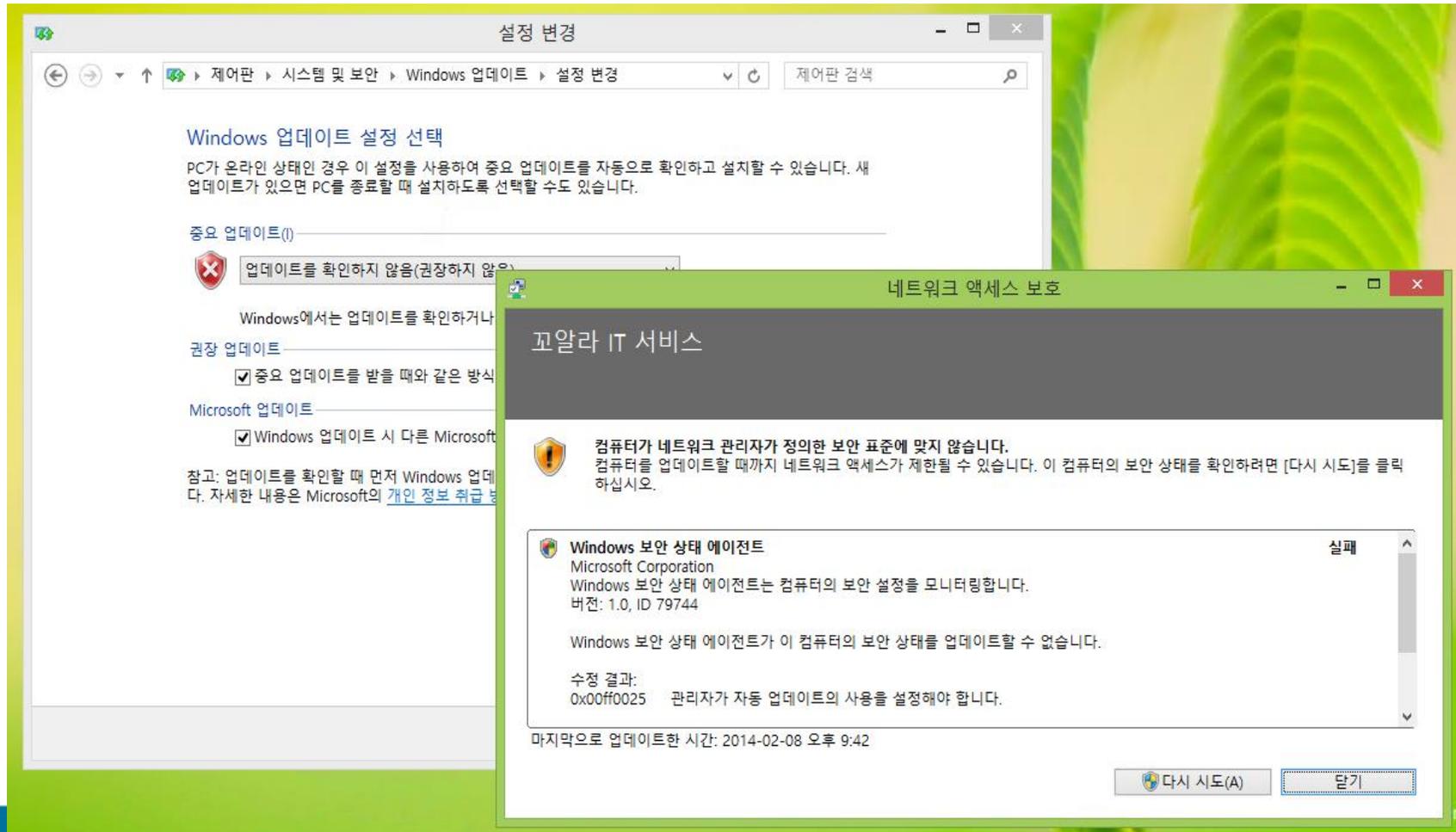
Windows Server 2003 EOS를 대비한

"How to migrate" 고객 세미나





End-Point Security



The image shows a Windows Update settings window in Korean. The window title is "설정 변경" (Change Settings). The breadcrumb path is "제어판 > 시스템 및 보안 > Windows 업데이트 > 설정 변경". The main heading is "Windows 업데이트 설정 선택" (Choose Windows Update settings). Below this, there are sections for "중요 업데이트" (Important updates), "권장 업데이트" (Recommended updates), and "Microsoft 업데이트" (Microsoft updates). A red shield icon with a white 'X' is visible, indicating a security warning. A dialog box titled "네트워크 액세스 보호" (Network Protection) is overlaid on the settings window. The dialog box has a title bar with "네트워크 액세스 보호" and a red 'X' icon. The main text in the dialog box reads: "꼬알라 IT 서비스" (Kkoalra IT Service) and "컴퓨터가 네트워크 관리자가 정의한 보안 표준에 맞지 않습니다. 컴퓨터를 업데이트할 때까지 네트워크 액세스가 제한될 수 있습니다. 이 컴퓨터의 보안 상태를 확인하려면 [다시 시도]를 클릭하십시오." (The computer does not meet the security standards defined by the network administrator. Network access may be limited until the computer is updated. To check the security status of this computer, click [Try again]). Below this text is a section for "Windows 보안 상태 에이전트" (Windows Security State Agent) with a status of "실패" (Failed). The text in this section says: "Microsoft Corporation Windows 보안 상태 에이전트는 컴퓨터의 보안 설정을 모니터링합니다. 버전: 1.0, ID 79744. Windows 보안 상태 에이전트가 이 컴퓨터의 보안 상태를 업데이트할 수 없습니다." (Microsoft Corporation Windows Security State Agent monitors the security settings of the computer. Version: 1.0, ID 79744. Windows Security State Agent cannot update the security status of this computer.). At the bottom of the dialog box, there are two buttons: "다시 시도(A)" (Try again) and "닫기" (Close). The bottom of the dialog box also shows the text "마지막으로 업데이트한 시간: 2014-02-08 오후 9:42" (Last updated time: 2014-02-08 PM 9:42).



End-Point Connectivity with Secure

원격 액세스 관리 콘솔

원격 액세스 설정
 DirectAccess 및 VPN을 포함한 원격 액세스를 구성하십시오.

구성

- DirectAccess 및 VPN
- 대시보드
- 작동 상태
- 원격 클라이언트 상태
- 보고

BLUE-DASVR

단계 1
 원격 클라이언트(R)
 DirectAccess를 허용할 클라이언트 컴퓨터를 식별합니다.
 편집...

단계 2
 원격 액세스 서버(E)
 원격 액세스 서버의 구성 및 네트워크 설정을 정의합니다.
 편집...

인터넷

내부 네트워크

작업

일반

- 구성 설정 제거
- 응용 프로그램 서버 추가
- 구성 요약 보기
- 관리 서버 복구
- 구성 다시 로드

VPN

- RRAS 관리 열기
- VPN 사용
- 사이트 간 VPN 사용

멀티 사이트 배포

- 멀티 사이트 사용

부하가 분산된 클러스터

- 부하 분산 사용

DirectAccess 내부 리: 에 액세스: 를 식별

DirectAccess 종단 간: 용 프: 랍니다.

마침(F)...

7th Point

IDentity with Security

Windows Server 2003 EOS를 대비한

"How to migrate" 고객 세미나



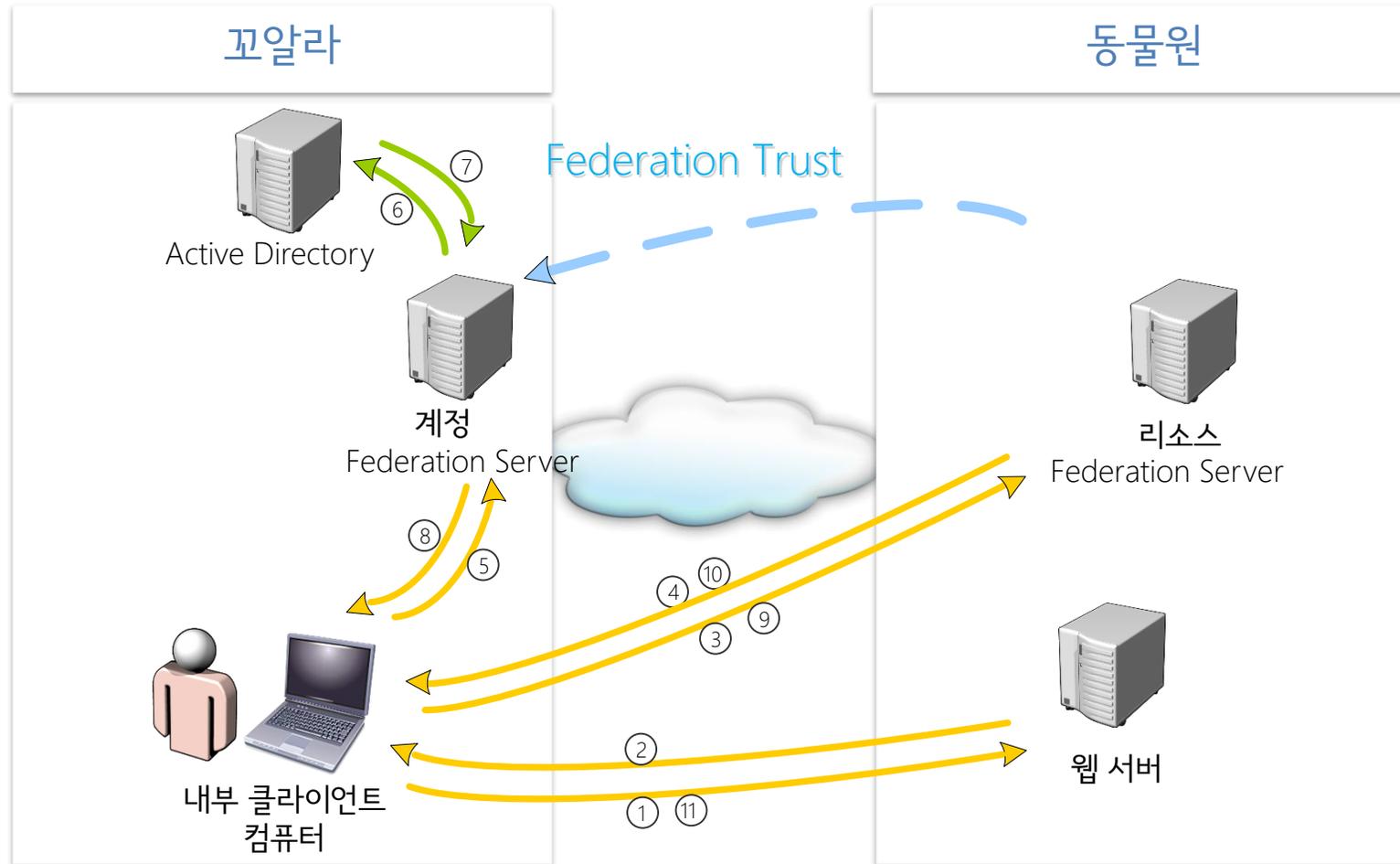


Enterprise IDentity

- Windows Server의 액티브 디렉터리
 - 인증 : Kerberos
 - 관리 : 그룹 정책
- 그러나, 액티브 디렉터리의 범위를 외부로 안전하게 넓히는 방법에 대한 고민



D+S 시대에 적절한 IDentity





사용 권한 관리에 대한 편의성 - 그룹

Active Directory 사용자 및 컴퓨터 [KOALRA-DC-02.KC]

- ▶ 저장된 쿼리
- ▶ KOALRA.COM
 - ▶ Builtin
 - ▶ Computers
 - ▶ Domain Controllers
 - ▶ ForeignSecurityPrincipals
 - ▶ KOALRA CLOUD
 - ▶ KOALRA IT
 - ▶ LostAndFound
 - ▶ Managed Service Accounts
 - ▶ Microsoft Exchange Security Groups
 - ▶ OpsMgrLatencyMonitors
 - ▶ Program Data
 - ▶ System
 - ▶ Users
 - ▶ Microsoft Exchange System Objects
 - ▶ NTDS Quotas
 - ▶ RegisteredDevices
 - ▶ TPM Devices

이름	종류	설명
Administrator	사용자	컴퓨터/도메인을 관리하도록 기본 제공된 계정
Allowed RODC Password Replicatio...	보안 그룹 - 도메인 로컬	이 그룹의 구성원은 도메인에 있는 모든 읽기 전용 도메인 컨트롤러에 암호를 복제할 수 있습니다.
Cert Publishers	보안 그룹 - 도메인 로컬	이 그룹의 구성원은 디렉터리로의 인증서 게시가 허용됩니다.
Cloneable Domain Controllers	보안 그룹 - 글로벌	도메인 컨트롤러가 아닌 이 그룹의 구성원이 복제될 수 있습니다.
CSAdministrator	보안 그룹 - 유니버설	이 그룹의 구성원은 Lync Server 2013에서 모든 관리 작업을 수행할 수 있습니다.
CSArchivingAdministrator	보안 그룹 - 유니버설	이 그룹의 구성원은 Lync Server 2013의 보관 관련 설정과 정책을 만들고 구성하며 관리할 수 있습니다.
CSHelpDesk	보안 그룹 - 유니버설	이 그룹의 구성원은 사용자 속성 및 정책을 비롯한 배포를 보고 Lync Server 2013에서 특정 문제 해결 작업을 수행할 수 있습니다.
CSLocationAdministrator	보안 그룹 - 유니버설	이 그룹의 구성원은 E911 관리에 대한 최하위 수준의 권한을 갖습니다. E911 위치 및 네트워크 식별자를 만들 수 있습니다.
CsPersistentChatAdministrator	보안 그룹 - 유니버설	이 그룹의 구성원은 범주/방/추가 기능에 대해 영구 채팅 관리 cmdlet을 실행할 수 있습니다.
CSResponseGroupAdministrator	보안 그룹 - 유니버설	이 그룹의 구성원은 Lync Server 2013의 응답 그룹 응용 프로그램 구성을 관리할 수 있습니다.
CSResponseGroupManager	보안 그룹 - 유니버설	이 그룹의 구성원은 Lync Server 2013에서 할당된 응답 그룹의 구성을 제한적으로 관리할 수 있습니다.
CSServerAdministrator	보안 그룹 - 유니버설	이 그룹의 구성원은 Lync Server 2013 및 서비스를 관리 및 모니터링하고 관련 문제를 해결할 수 있습니다.
CSUserAdministrator	보안 그룹 - 유니버설	이 그룹의 구성원은 Lync Server 2013의 사용자를 설정 및 해제하고, 사용자를 이동하며, 기존 정책을 사용자 지정할 수 있습니다.
CSViewOnlyAdministrator	보안 그룹 - 유니버설	이 그룹의 구성원은 배포 상태를 모니터링하기 위해 서버 정보를 비롯한 Lync Server 2013 배포를 볼 수 있습니다.
CSVoiceAdministrator	보안 그룹 - 유니버설	이 그룹의 구성원은 Lync Server 2013에서 음성 관련 설정과 정책을 만들고 구성하며 관리할 수 있습니다.
Dell Connections License Administr...	보안 그룹 - 글로벌	Dell Group
Dell Connections License Operators	보안 그룹 - 글로벌	Dell Group
Dell Connections License Users	보안 그룹 - 글로벌	Dell Group
Denied RODC Password Replication...	보안 그룹 - 도메인 로컬	이 그룹의 구성원은 도메인에 있는 어느 읽기 전용 도메인 컨트롤러에도 암호를 복제할 수 없습니다.
DiscoverySearchMailbox {D919BA0...	사용자	



정적인 그룹 관리에 대한 한계

- 비즈니스 변화에 따른 반복적인 변화 필요
- 실수 및 미파악으로 인한 보안 문제 발생 가능성

- HR(인사) 데이터베이스와의 연계적 측면 한계



동적 액세스 제어(DAC)

Active Directory 관리 센터

Active Directory 관리 센터 > 동적 액세스 제어 >

Active Directory... < 동적 액세스 제어 (5)

필터

이름	종류	설명
Central Access Policies	msAuthz-CentralAccessPolicies	
Central Access Rules	msAuthz-CentralAccessRules	
Claim Types	msDS-ClaimTypes	
Resource Properties	msDS-ResourceProperties	
Resource Property Lists	컨테이너	

개요
 BLUE(로컬)
 동적 액세스 제어
 Central Access Policies
 Central Access Rules
 Resource Property Lists
 인증
 전체 검색

Blue.Com

파일 홈 공유 보기

내 PC > 로컬 디스크 (C:) > Data > Blue.Com

Blue.Com 검색

이름	수정된 날짜	유형	크기
대한민국	2014-02-07 오후...	파일 폴더	
미국	2014-02-07 오후...	파일 폴더	
일본	2014-02-07 오후...	파일 폴더	

내 PC
 네트워크

3개 항목 | 1개 항목 선택함 | 상태: 공유됨

대한민국 속성

일반 공유 보안 이전 버전 사용자 지정 분류

이름	값
근무국가	대한민국
부서	(없음)
직급	(없음)
호스트 이름	(없음)
회사	Blue.Com

속성: 근무국가
 값:

값	설명
(없음)	속성을 지우려면 이 값을 선택
대한민국	
미국	
일본	

1st Point

Patch

Windows Server 2003 EOS를 대비한
"How to migrate" 고객 세미나



2nd Point

Basic Security

Windows Server 2003 EOS를 대비한

"How to migrate" 고객 세미나



3rd Point

Service Security

Windows Server 2003 EOS를 대비한

"How to migrate" 고객 세미나



Scanning

Windows Server 2003 EOS를 대비한

"How to migrate" 고객 세미나





5th Point

Web Server

Windows Server 2003 EOS를 대비한

"How to migrate" 고객 세미나



6th Point

Security with Client

Windows Server 2003 EOS를 대비한

"How to migrate" 고객 세미나



7th Point

IDentity with Security

Windows Server 2003 EOS를 대비한

"How to migrate" 고객 세미나





Windows Server 2003 EOS를 대비한

"How to migrate" 고객 세미나

