

Welcome to
the modern
datacenter.



Windows Server 2012

Windows Server 2003 EOS(End of Service)에 따른 Windows Server 2012로의 업그레이드를 제안합니다.

- 01 Microsoft Window Server 기술 지원 주기
- 03 Windows Server 2003 EOS가 귀사에 미치는 영향
- 04 Windows Server 2012로 업그레이드 해야 하는 가장 중요한이유
- 05 Windows Server 2012를 통한 서버 플랫폼의 현대화
- 07 Windows Server 2012로 경쟁에서 앞서가십시오
- 09 Windows Server 버전별 기능 비교



Microsoft Window Server 기술 지원 주기

Microsoft가 주요 제품들에 대한 지원 정책을 수립하고, 이를 명시적으로 알린 것은 2002년 10월 15일 이후입니다. Microsoft는 비즈니스 및 개발 제품에 대해 최소 10년의 지원, 다시 말해, 일반 지원의 경우에는 5년 혹은 다음 제품 (N+1)이 출시된 이후 2년 중 긴 기간으로, 일반 지원 이후 5년간 혹은 두번째 후속 제품(N+2)이 출시된 이후 2년 중에 긴 기간에 대해서 연장 지원을 제공하고 있습니다.

최소 10년이 보장되는 이유는 일반 지원 5년, 연장 지원 5년을 합한 기간에 대한 부분이며, 최소라는 단어가 붙어 있는 이유는 후속 제품이 출시된 후 2년과 5년 가운데 긴 기간으로 결정되기 때문입니다. 서비스팩이 출시된 경우, 서비스팩 이전 버전에 대해서는 최대 2년동안 기술 지원이 제공됩니다.


제공되는 지원	일반지원	연장지원
유료 문제 해결 지원	●	●
보안 업데이트 지원	●	●
보안과는 관련 없는 핫픽스 지원	●	핫픽스 지원 계약 체결이 요구됨
무료 문제 해결 지원	●	—
하자보증(Warranty) 주장	●	—
디자인 변경과 새 기능 요청	●	—
온라인 기술 자료(KB)에서 이용 가능한 제품 상세 정보	●	●
기술 질문에 대한 답변을 위한 Microsoft 고객 지원 사이트에서 이용 가능한 제품 상세 정보	●	●

2015년 7월 14일. Windows Server 2003 확장 지원 종료

Windows Server 2003 및 2003 R2의 경우에는 2006년 3월 5일에 지원을 시작하여, 이미 일반 기술 지원을 2010년에 공식적으로 종료하였고 2015년 7월 14일에는 연장 기술 지원마저도 종료하게 됩니다.

<그림 00-01> Windows Server 2003 R2의 제품 지원 기간

Microsoft 제품 지원 기간 검색

제품 이름 

▼ 좀 더 많은 검색 옵션 보기

검색

릴리스된 제품	지원 시작일	일반 지원 종료 날짜	연장 지원 종료 날짜	서비스 팩 지원 종료 날짜	메모
Windows Server 2003 R2 Datacenter Edition (32-Bit x86)	2006-03-05	2010-07-13	2015-07-14	2009-04-14	
Windows Server 2003 R2 Datacenter Edition with Service Pack 2	2007-03-13	메모 참조	메모 참조		지원은 다음 버전 서비스 팩 릴리스 24개월 후 혹은 제품 지원 기간의 마지막 기간 중 먼저 적용되는 시기에 종료됩니다. 보다 자세한 내용은 서비스 팩 지원 정책 을 참고하시기 바랍니다.
Windows Server 2003 R2 Datacenter x64 Edition	2006-03-05	2010-07-13	2015-07-14	2009-04-14	
Windows Server 2003 R2 Datacenter x64 Edition with Service Pack 2	2007-03-13	메모 참조	메모 참조		지원은 다음 버전 서비스 팩 릴리스 24개월 후 혹은 제품 지원 기간의 마지막 기간 중 먼저 적용되는 시기에 종료됩니다. 보다 자세한 내용은 서비스 팩 지원 정책 을 참고하시기 바랍니다.
Windows Server 2003 R2 Enterprise Edition (32-Bit x86)	2006-03-05	2010-07-13	2015-07-14	2009-04-14	
Windows Server 2003 R2 Enterprise x64 Edition	2006-03-05	2010-07-13	2015-07-14	2009-04-14	
Windows Server 2003 R2 Standard Edition (32-bit x86)	2006-03-05	2010-07-13	2015-07-14	2009-04-14	
Windows Server 2003 R2 Standard x64 Edition	2006-03-05	2010-07-13	2015-07-14	2009-04-14	

※출시 날짜와 종료 날짜에 대한 미묘한 차이가 발생하는 것은 종료 날짜에 대한 정의 때문입니다. 기술 지원 종료일 다음 분기의 두번째 화요일에 맞춰져 있습니다. Windows Server 2003 R2의 경우 10년이 지난 2015년 3월 5일 이후, 다음 분기의 두번째 화요일인 2015년 7월 14일이 되게 됩니다. 이는 업데이트 출시 주기와 맥락을 같이 합니다.

Windows Server 2003 EOS가 귀사에 미치는 영향

2015년 7월 14일부터 Windows Server 2003 모든 버전에 대해 보안 패치와 핫픽스 제공이 중단되기 때문에 Windows Server 2003을 실행하는 PC는 보안 위협에 더욱 취약해지며 서버 워크로드에 대한 관리 및 지원 비용도 증가하게 됩니다.

지원 종료 후 Windows Server 2003을 실행하면 비즈니스 위험이 가중됩니다.

지원되지 않는 소프트웨어를 실행하면 비즈니스가 더 큰 위험에 노출됩니다. 예를 들면 다음과 같습니다.

- **보안 위험.** 중요한 Windows Server 2003 보안 업데이트가 중단되면 서버 인프라는 유해한 바이러스, 스파이웨어 및 기타 악성 소프트웨어에 취약해져 비즈니스 데이터 및 정보가 유출되거나 손상될 수 있습니다. Windows Server 2003 자체가 지원되지 않으면 바이러스 백신 소프트웨어를 실행하더라도 완전한 보호는 어렵습니다.
- **호환성 문제.** 소프트웨어 및 하드웨어 공급업체들도 대부분 Windows Server 2003 기반의 자사 제품에 대한 지원을 중단할 것입니다.
- **지원 문제.** 안타깝지만 문제가 발생하더라도 Microsoft의 온라인 및 전화 기술 지원을 통해 귀사 또는 귀사의 IT 파트너를 지원할 수 없게 됩니다.
- **연속성 문제.** 지원 종료, 지원되는 소프트웨어 부재, 그리고 Windows Server 2003 기반의 하드웨어 노후화 등으로 인해 시스템 장애 및 비즈니스 중단의 위험이 증가합니다.

시스템을 업그레이드
하면 라이선스의
가치를 극대화할 수
있고 라이선스 관리를
간소화할 수 있습니다.

Microsoft 소프트웨어
보증은 최신 Microsoft
소프트웨어에 항상
액세스할 수 있도록
보장하는 가장 비용
효율적인 방법입니다.

"공격자들은 Windows XP 및 Windows Server 2003 취약점을 수집해 두고 공식 지원이 종료 될 때까지 기다렸다가 상당수의 Windows XP 및 Windows Server 2003 OS 설치 기반에 이를 악용할 수 있습니다. 이전 버전의 소프트웨어를 사용하면 이미 뒤엎힌 보안 환경에 불필요한 복잡성 계층만 늘어날 뿐입니다. 아직 Windows XP와 Windows Server 2003을 사용 중인 기업이 위험을 완화하기 위해 취할 수 있는 실질적 조치는 최신 솔루션으로 업그레이드하고 적시에 패치를 적용하고 맬웨어 차단 및 검색 소프트웨어를 실행하는 것입니다." Trend Micro^[1]

^[1] <http://blog.trendmicro.com/exploit-windows-xpserver-2003-demonstrates-importance-software-upgrades/>

Windows Server 2012로 업그레이드 해야 하는 가장 중요한 이유

Windows Server 2012를 이용하여 클라우드에 최적화된 IT로 전환하면 이미 투자한 기술과 솔루션을 그대로 활용할 수 있기 때문에 친숙하고 일관적인 플랫폼을 구축할 수 있습니다.

비용 절감 및 효율성 증가.

Windows Server 2012는 가동 시간을 극대화하고 장애와 중단 시간을 최소화하는 업계 표준 하드웨어의 성능과 안정성으로 새로운 차원의 비용 절감과 효율성을 제공합니다.

업무 유형의 현대화 지원.

Windows Server 2012는 관리를 간소화하고 보안, 제어, 규정 준수를 유지하면서도 데이터 및 응용 프로그램에 대한 유연한 액세스를 구현합니다.

종합적인 클라우드 플랫폼.

Windows Server 2012는 가상화, 확장성, 성능 및 연결 구현을 통해 종합적인 클라우드 플랫폼을 제공합니다.

바로 지금, Windows Server 2003의 마이그레이션 계획을 세우십시오.

Windows Server 2003 마이그레이션에 대한 관심에 감사드립니다.

Windows Server 2003 마이그레이션 계획을 지금 세울 경우 귀사는 지원 날짜가 만료된 소프트웨어 사용과 관련된 위험과 높은 지원 비용 발생을 방지할 수 있는 유리한 입장에 서게 됩니다. 최신 서버 운영 체제는 Microsoft 환경과 혁신의 이점을 구현하여 서버 기반 워크로드를 지원합니다. 예를 들어 Windows Server 2012의 향상된 성능 및 가상화 기술은 서버 통합을 통해 상당한 비용 절감 효과뿐만 아니라 보안 개선, 고성능 스토리지, 지점 성능 개선도 실현할 수 있습니다. 기업은 Windows Server 2012가 구현하는 클라우드 기반 플랫폼의 비즈니스 및 경제적 이점도 누리게 됩니다.

Microsoft의 장점

귀사에 최적인 제품을 이용할 수 있는 유연성

Microsoft의 기술은 현재 최고의 통합성과 개방성 및 상호 운용성을 제공합니다. Microsoft는 클라우드를 중심으로 변화해왔지만 우리의 기술을 귀사의 데이터 센터에 배포하거나 귀사가 파트너와 함께 호스팅할 수 있는 유연성은 여전히 있습니다.

귀사의 성공 지원에 대한 Microsoft의 약속

Microsoft와 함께하십시오. 신뢰할 수 있는 서비스 전문가들로 구성된 고객관리 팀과 파트너가 최신 기업 기술 혁신을 활용할 수 있도록 지원합니다.

친숙한 기술

Microsoft의 기술은 누구나 사용하기 쉽고 IT 전문가가 쉽게 관리할 수 있으며 기업 솔루션의 신속한 개발도 지원합니다.

Microsoft의 약속은 단순합니다.

귀사의 최종 사용자 컴퓨팅 환경을 현대화하여 완전히 새로운 수준의 기업 가치를 경험하실 수 있도록 지원하겠습니다.

Windows Server 2012를 통한 서버 플랫폼의 현대화

서버 현대화는 최신 서버 운영 체제 발전을 최대한 활용할 수 있는 절호의 기회입니다. 최근 조사에 따르면 Windows Server 2012의 조기 도입 고객들은 비용 절감에서부터 가용성 증대, 기업의 새로운 서비스의 출시 기간 단축, 생산성 향상에 이르기까지 조직 전체에 걸쳐 커다란 혜택을 누리고 있는 것으로 보고되었습니다.

데이터 센터 현대화의 실제적 이점

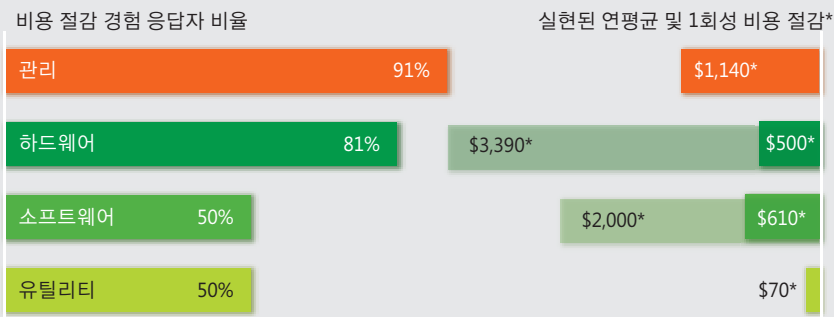
Windows Server 2012는 보다 유연하고 확장이 용이하며 안정적인 기업 인프라 혁신을 위해 현대화된 제품 및 서비스 플랫폼을 제공합니다.

- **가상화를 넘어서는 인프라.** Windows Server 2012는 가상화를 넘어서는 동적 다중 테넌트 인프라를 구현하며 클라우드 서비스 구현 및 연결을 위해 최대한의 유연성을 제공합니다.
- **단일 서버로 다중 서버와 동일한 성능 구현.** Windows Server 2012는 연속해서 사용할 수 있고 관리하기 쉬운 다중 서버 플랫폼을 혁신적인 효율성과 함께 유비쿼터스 자동화와 통합하여 뛰어난 경제성을 실현합니다.
- **어떤 클라우드에서도 모든 응용 프로그램에 액세스 가능.** Windows Server 2012는 일관된 도구집합과 프레임워크를 사용하여 응용 프로그램과 웹사이트를 온프레미스, 클라우드 및 하이브리드 환경에 구축하고 배포할 수 있는 광범위하고 확장성이 뛰어나며 탄력적인 서버 플랫폼입니다.
- **현대적인 업무 유형 실현 가능.** 관리를 간소화하고 보안, 제어, 규정 준수 유지를 지원하는 Windows Server 2012는 IT 관리자에게 풍부한 사용자 경험과 함께 사실상 모든 곳, 모든 장치의 데이터와 응용 프로그램에 대한 유연한 액세스를 제공할 수 있는 능력을 부여합니다.

총소유비용 절감

조기 도입한 56개 조직의 TCO 결과, 2012년 4월 ~ 10월

* 참고: 모든 비용 절감은 프로세서당 기준.
연한 색으로 표시된 부분은 1회성 절감액.



데이터센터의 간편하고 경제적인 라이선싱

Windows Server 2012 데이터센터를 이용하면 같은 라이선스로 무제한의 가상 컴퓨터를 관리할 수 있는 능력도 갖추게 됩니다. 이 기능은 놀라운 라이선싱 경제성을 제공하며 추후 확장이 필요할 때에도 라이선스를 추가할 필요가 없습니다. 또한 데이터센터 라이선싱은 각각의 가상 컴퓨터를 추적할 필요가 없기 때문에 까다로운 규정 준수 문제도 덜어줍니다.

Windows Server 2012의 새로운 기능

서버 가상화

Windows Server 2012는 더 많은 기능과 뛰어난 확장성 및 기본 신뢰성 메커니즘 추가를 통해 Hyper-V 가치 제시 영역을 확장합니다.

네트워킹

Windows Server 2012는 보다 효율적이고 비용 효과적인 네트워킹 관리를 촉진하면서도 네트워킹 복잡성을 완화하는 일련의 새로운 기능을 제공합니다.

원격 액세스

Windows Server 2012는 응용 프로그램과 데이터 및 전체 데스크톱 환경에 보다 안전하고도 효율적으로 원격 액세스할 수 있는 여러 방법을 제공합니다.

인증 및 보안

Windows Server 2012를 통해 관리자는 적절한 보안과 액세스를 보장할 수 있도록 사용자, 리소스, 장치를 더욱 쉽게 구성 및 관리하고 모니터링할 수 있습니다.

스토리지 및 가용성

Windows Server 2012는 운영 비용을 관리하고 자본 지출을 통제하는 동시에 주문형 용량 구현 사이의 균형을 유지할 수 있습니다.

서버 관리

통합 플랫폼인 Windows Server 2012는 종합적인 다중 서버 관리 용이성을 통해 탁월한 총소유비용을 가능케 합니다.

웹 및 응용 프로그램 플랫폼

Windows Server 2012는 뛰어난 유연성을 바탕으로 온프레미스와 클라우드 환경 모두에서 웹 기반 응용 프로그램을 호스팅하여 사설 클라우드 구축 및 관리와 주요 응용 프로그램 실행에 필요한 유연성, 확장성 및 호환성을 모두 갖춘 최고의 서버 플랫폼으로 자리를 잡았습니다.

Windows Server 2012 백서

IT 인프라에 관해 요구되는 메시지는 분명합니다. 기업들은 근본적으로 비즈니스와 IT 과제를 해결할 수 있는 일관성 있고 통합적인 접근 방식을 원합니다. 또한 온프레미스와 사설 클라우드, 공용 클라우드 환경에 배포할 수 있는 새로운 응용 프로그램과 서비스를 최대한 활용하기를 원합니다. Windows Server®를 잇는 버전인 Windows Server 2012는 더욱 뛰어난 역동성과 가용성 및 비용 효율성을 갖춘 서버 플랫폼으로서 클라우드를 통해 중소기업부터 대기업에 이르는 모든 기업의 IT를 최적화하는 데 적합한 제품입니다.

Windows Server 2012 백서는 www.microsoft.com/ko-kr/server-cloud/products/windows-server-2012-r2에서 확인할 수 있습니다.

Windows Server 2012로 경쟁에서 앞서 가십시오

과거

현재



오늘날의 기술 환경은 5년 또는 10년 전과 비교해보면 정말 놀랍습니다. 오늘날 우리가 처리하는 데이터의 유형과 볼륨은 가히 폭발적이며 서버 성능은 비교할 수 없이 탁월하고 모바일 장치는 과거의 데스크톱 PC보다도 높은 수준의 고급 기능을 갖추고 있습니다.

Windows Server 2012 R2는 새로운 강력한 서버를 이용하거나 직원들이 어디서나 업무를 볼 수 있도록 중소 규모의 기업들이 현재와 미래의 기술을 최대한 활용할 수 있도록 지원합니다. Windows Server 2012 R2로 지금 업그레이드하여 향후 경쟁에서 앞서 나가십시오.

서버 통합

비즈니스 발전 속도에 맞춰 서버 하드웨어 투자 효과를 극대화 하십시오.



실제: 대부분의 기업은 오늘날의 고급 서버 하드웨어 용량의 극히 일부만을 사용하고 있습니다.

업그레이드 필요성: 업계 최고의 가상화 플랫폼을 통해 동일한 서버에서 더 많은 응용 프로그램을 실행할 수 있습니다.

핵심 기술: Hyper-V.

Windows Server 2012 R2의 가상화 기능은 동일한 서버에 더 많은 응용 프로그램을 추가하기 때문에 하드웨어 투자의 효과를 극대화하고 IT 유지보수 비용, 전기 요금 등의 관련 비용을 줄일 수 있습니다.

서버 통합은 가상화가 제공하는 수많은 기능 중 극히 일부분에 불과하며 Windows Server 가상화를 완료하면 다양한 추가 이점들을 활용할 수 있습니다.

실시간 마이그레이션 및 실시간 복제와 같은 혁신적 기능은 시스템 중단 시간 없이 소프트웨어 업그레이드를 지원하고 응용 프로그램 문제를 해결하기 때문에 가동 중단을 감소시킵니다.

재해 복구

신속하게 시스템 장애를 복구하고 보다 빨리 온라인을 다시 연결할 수 있는 능력을 갖춰 예기치 못한 상황에 언제든지 대응할 수 있다는 확신을 가지십시오.



실제: 시스템 사고 발생 후 40퍼센트의 기업이 복구에 실패합니다.^[2]

업그레이드 필요성: 비즈니스 연속성을 극적으로 개선하고 시스템 장애 발생 시 데이터 손실 위험을 크게 줄일 수 있습니다.

핵심 기술: Hyper-V 복제.

시스템이 다운되는 이유는 정전, 침입, 화재 등 매우 다양합니다. Windows Server 2012에 도입된 Hyper-V 복제는 공통 광대역 연결을 통해 가상 컴퓨터를 다른 위치로 자동 복제하여 데이터 손실을 줄이고 빠르게 복구할 수 있는 비용 효율적인 방법을 제공합니다.

Windows Server 2012 R2는 비즈니스 요건에 따라 복제 간격을 15분이나 5분, 30초 등으로 맞춤 지정할 수 있는 유연성을 더했습니다. 또한 추가 서버에도 복제할 수 있도록 다중 노드 Hyper-V 복제 기능 도입으로 안정성을 더욱 높였습니다.

유연하고 비용 효율적인 스토리지

기존 솔루션보다 훨씬 저렴한 비용으로 비즈니스 요건에 맞게 데이터 스토리지를 빠르게 확장하십시오.



실제: 기존의 스토리지 구현에 드는 비용은 일반적인 중소 기업의 IT 전체 1년 예산에 맞먹습니다.

업그레이드 필요성: 많은 비용을 들이지 않아도 필요한 스토리지를 필요한 때에 직원들에게 제공할 수 있습니다.

핵심 기술: 스토리지 공간.

대부분의 기업이 확장 볼륨과 문서 및 이메일부터 동영상과 소셜 미디어에 이르는 오늘날의 다양한 유형의 데이터를 저장해야 합니다. Windows Server 2012 R2에 포함된 스토리지 공간 기능은 직원들에게 “적시에 충분하게” 스토리지를 할당하고 이를 필요에 따라 빠르게 확대 및 축소시키는 비용 효율적인 솔루션을 제공합니다.

Windows Server 2012 R2에는 저렴한 업계 표준 하드웨어를 사용하면서 스토리지 성능을 극적으로 향상시키는 스토리지 티어링 기능을 새로 도입하였습니다.

^[2] 미연방재난관리국. fema.gov

일관된 사용자 환경

기업에서 사용하는 모든 PC와 모바일 장치에 일관되고 잘 관리된 사용 환경을 제공합니다.



실제: 많은 기업들이 직원들의 다양한 모바일 장치의 관리에 어려움을 겪고 있습니다.

업그레이드 필요성: PC와 모바일 장치의 간편한 관리와 함께 일관된 모바일 환경을 제공할 수 있습니다.

핵심 기술: Windows Server Essentials Experience 및 Office 365.

Windows Server 2012 R2 스탠드 및 데이터센터 에디션은 Windows Server Essentials Experience의 많은 장점들을 갖추고 있습니다. 단일 인터페이스에서 직원들의 연결 데스크톱과 모바일 장치를 쉽게 백업, 배포 및 관리할 수 있는 단순화된 관리 보드도 그 중 하나입니다.

간편한 원격 액세스

안전하게 데이터를 보호하면서도 직원들에게 어느 곳에서든 일할 수 있는 유연성을 제공하십시오.



실제: 직원들은 어디서든 데이터에 액세스하기를 원하는 한편 회사는 데이터의 안전한 보호를 원합니다.

업그레이드 필요성: 서버상의 민감한 데이터를 안전하게 보호하면서도 어느 곳에서든 액세스가 가능합니다.

핵심 기술: RDS로 작동하는 가상 데스크톱 인프라(VDI).

직원들은 PC나 모바일 장치를 이용하여 집이나 사무실, 혹은 이동 중 어느 곳에서든 응용 프로그램과 데이터에 액세스할 수 있는 유연성을 원합니다. 그러나 노트북과 모바일 장치는 분실이나 도난이 자주 발생하기 때문에 민감한 기업 데이터가 위험해질 수 있습니다.

Windows Server 원격 데스크톱 서비스(RDS)로 작동하는 가상 데스크톱 인프라(VDI)를 이용하면 직원들은 원격으로 응용 프로그램에 액세스할 수 있고 기업은 서버 데이터를 안전하게 지킬 수 있습니다.

Windows Server 2012 R2 VDI/RDS는 사용자 환경과 관리 기능을 계속 강화합니다. 이 서비스의 새로운 기능은 성능과 확장성 개선을 위해 스토리지 티어링과 데이터 복제 등의 핵심 플랫폼 기능을 최대한 활용할 수 있도록 지원합니다.

Windows Server 2012 R2 출시와 함께 기업 데스크톱과 Windows, Windows RT, iOS, OS X 및 Android 장치의 응용 프로그램에 쉽게 액세스할 수 있는 Microsoft 원격 데스크톱 응용 프로그램도 출시했습니다.

지금 업그레이드하십시오!

Microsoft 파트너에게 문의하거나 다음 사이트에서 보다 자세한 내용을 확인하십시오.
<http://www.microsoft.com/windowsserver2012r2>

Windows Server 버전별 기능 비교

Windows Server는 기업의 IT 인프라가 오늘날 컴퓨팅 환경의 가장 까다로운 요건을 충족시킬 수 있도록 IT 운영 상의 혁신을 돕습니다. 경쟁에서의 성공에 필요한 기능을 제공하는 서버 운영 체제를 선택할 경우 장기적으로 회사에 커다란 가치와 성공을 제공할 것입니다.

기능	Windows Server 2003 R2	Windows Server 2008 R2	Windows Server 2012 R2
기업 확장성 및 성능	●	●	●
Hyper-V 네트워크 가상화	○	○	●
가상 데스크톱 인프라	○	●	●
웹 및 응용 프로그램 서버	●	●	●
ASP.NET 지원 및 관리	●	●	●
다중 테넌트, 고밀도 웹사이트	○	●	●
저비용, 고가용성 SMB 3.0 파일 스토리지	○	○	●
Windows PowerShell 3.0	○	●	●
지점 지원	●	●	●
BranchCache의 지점 가용성 및 확장성 개선	○	●	●
하이브리드 응용 프로그램	○	●	●
동적 액세스 제어	○	○	●
FAX 서버	●	●	●
파일 및 프린트 서버	●	●	●
Windows 배포 서비스 및 Windows Server 업데이트 서비스	○	●	●

○ 비 지원 기능
● 부분적 지원 기능
● 지원 기능

보안에 강한 Enterprise OS, Windows Server 2012

- Windows Server 2003 VS Windows Server 2012 R2

- 13 Windows Server 2003과 Windows Server 2012 R2의 기본 구조(Architecture) 차이
- 19 웹 서버(IIS, Internet Information Service)의 변화
- 29 엔드포인트/클라이언트 보안(Endpoint 보안) 및 모바일 연결성 제공
- 34 클라우드 시대에 적절한 ID(Identity) 및 보안 권한 관리



Windows Server 2003과 Windows Server 2012 R2의 기본 구조(Architecture) 차이

Windows Server 2003(5.2.3790)과 Windows Server 2012 R2(6.3.9600)의 근본적인 차이는 운영 체제 핵심인 커널에 대한 보안이 기본적으로 적용되어 있는지에 대한 부분입니다.

Windows Server 2008부터 제공되고 있는 커널 버전 6에서부터 커널 버전 5에 비해 보안에 대한 기술이 대폭 향상 및 탑재되어 운영 체제의 기본 보안을 강화시켜 주고 있습니다.

커널 버전 5와 커널 버전 6에 대한 기본 보안 구조의 차이는 아래와 같습니다.

• 64비트 버전에 대한 커널 패치 보호

Windows 커널을 허가되지 않은 프로그램이 패치하는 것을 방어합니다. 지원되지 않는 방법론을 통해 운영 체제의 커널을 수정하게 되면, 운영 체제 안정성에 막대한 영향을 끼칠 수 있습니다. 커널 패치 보호 기술을 통해, 허가된 형태의 방법을 이용해서 운영 체제의 커널을 패치할 수 있게 합니다.

• 힙 관리자(Heap Manager)의 보안 강화

메타데이터 인코딩 차단, 블록 헤더의 무결성 확인 등 힙 관리자의 보안을 강화하였습니다.

• 레지스트리의 보안 강화

운영 체제의 주요한 정보가 담긴 HKEY_LOCAL_MACHINE에 대한 사용 권한 강화를 통해 보안을 강화하였으며, 기존 응용 프로그램과의 호환성을 위하여, 레지스트리 가상화를 지원합니다.

• 코드 무결성

• 데이터 실행 보호(DEP, Data Execution Protection)

응용 프로그램이 사용 중인 메모리가 아닌, 다른 메모리 영역을 비정상적으로 사용할 경우, 응용 프로그램을 종료하여, 시스템 메모리를 보호합니다. 더불어, 메모리 영역에 대해 실행 가능한지 여부에 대한 지정을 할 수 있게 합니다.

• ASLR(Address Space Layout Randomization)

운영 체제의 사용자 모드에서 실행 가능한 이미지(.exe, .dll)가 로딩될 경우, 할당되는 메모리 영역을 랜덤하게 지정하여, 메모리 영역을 미리 알고 공격하는 형태를 무력화합니다.

• Windows 리소스 보호

운영 체제의 주요 파일 및 영역에 대한 운영 체제의 기본 보호가 동작하여, 비정상적 운영 체제 수정시 이를 원상 복구합니다. 이를 통해 운영 체제의 안정성을 향상시킵니다.

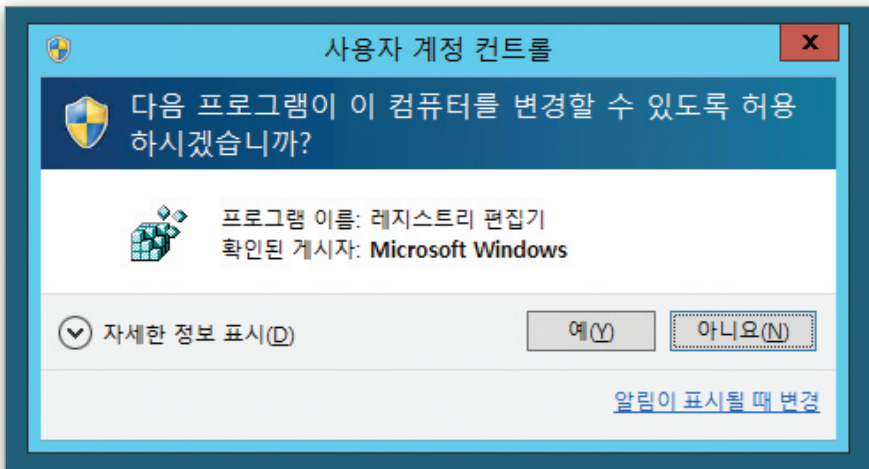
• Windows 서비스 기본 보안 강화

서비스 별 사용 권한을 보다 세분화하고, 서비스별 보안 ID(SID)를 배정, 서비스에 대한 사용 권한 및 보안 관리가 가능하게 합니다. 또한 기존 Windows Server 2003의 경우, 운영 체제의 세션 정보와 로그인한 사용자의 세션 정보가 동일하여, 사용자가 운영 체제에 대한 부분과 기본 교신이 가능했던 부분을 고립화하여 운영 체제와 관리자를 세션적으로 분리하게 됩니다.

• Windows Integrity 메커니즘

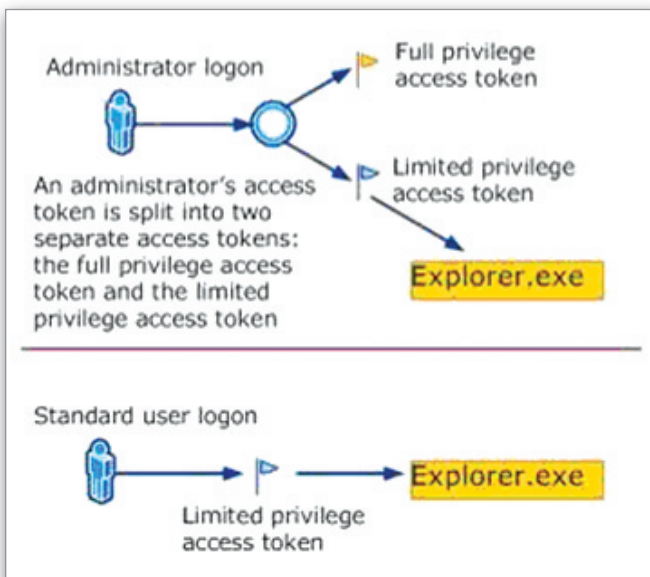
기본적으로 운영 체제와 함께 제공되어, 강화된 보안 레벨을 보장해 주는 기술과 더불어, Windows Server에는 잘못된 설정, 악성 코드, 나아가 보안이라는 영역에서 중요하게 여기는 사용 권한에 대한 보안 처리 구조가 있습니다. 바로 사용자 계정 컨트롤이 이에 해당됩니다. 커널 버전 5와 커널 버전 6의 차이중 가장 눈에 띄는 부분이며, 운영 체제의 안전한 운영 및 방어를 위해서 꼭 필요한 기술입니다.

<그림 01-01> 사용자 계정 컨트롤



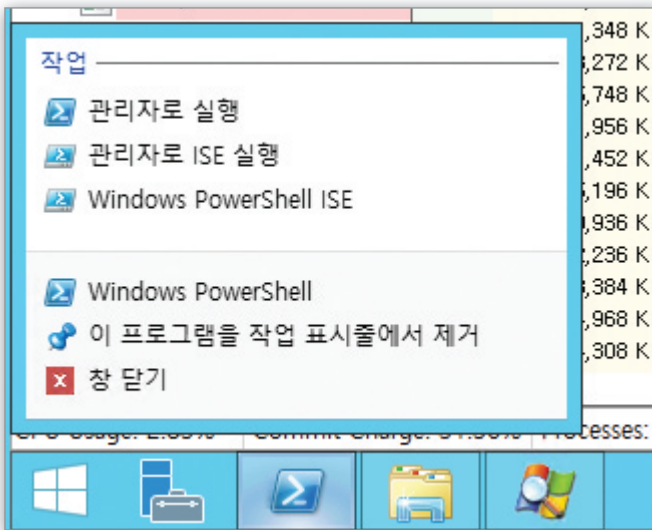
먼저, 우리에게 UAC(User Account Control)로 잘 알려진 기술은 관리자가 시스템을 접근했을 경우, 기본적인 권한을 일반 사용자로 할당받을 지, 관리자 권한으로 할당받을 지에 대한 구분을 제공합니다.

<그림 01-02> UAC의 기본 아키텍처



관리자 권한으로 접근되는 Windows Server 2003의 경우, 실행되는 모든 프로세스는 기본적으로 관리자 권한으로 실행되므로, 실수로 실행된 프로세스는 물론 악성 코드까지도 시스템에 악영향을 줄 수 있게 됩니다. Windows Server 2012 R2 서버 운영 체제에서는 UAC 기술이 기본 탑재되어 있으므로, 최소 보안을 향상시켜, 필요시 관리자 권한을 요구할 수 있는 형태로 동작합니다.

<그림 01-03> 관리자 권한으로 실행



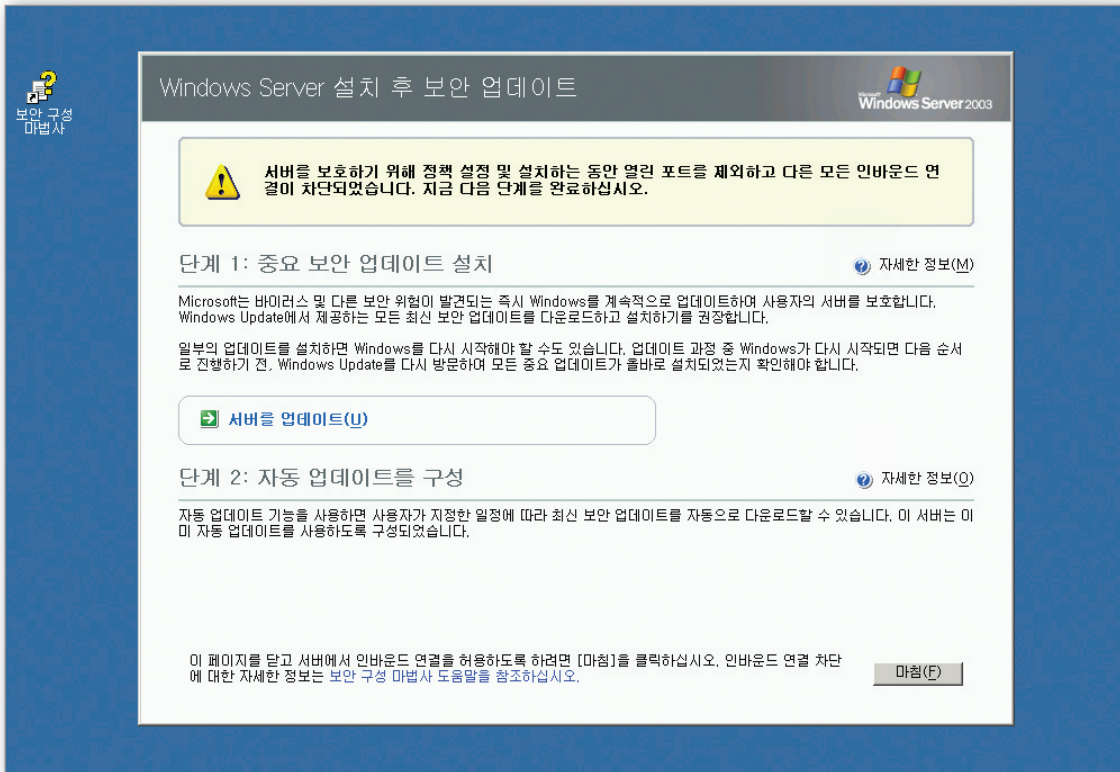
시스템에 대한 비인지 권한 탈취가 시도되는 경우이더라도, 기본 권한이 사용자에게 머물러 있기에, UAC 구조를 정상적으로 통과하지 않는 한, 시스템 전반에 대한 악성 코드 실행을 할 수 없습니다.

<그림 01-04> 사용 권한이 분리된 서버의 프로세스 (High, Medium, Low)

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

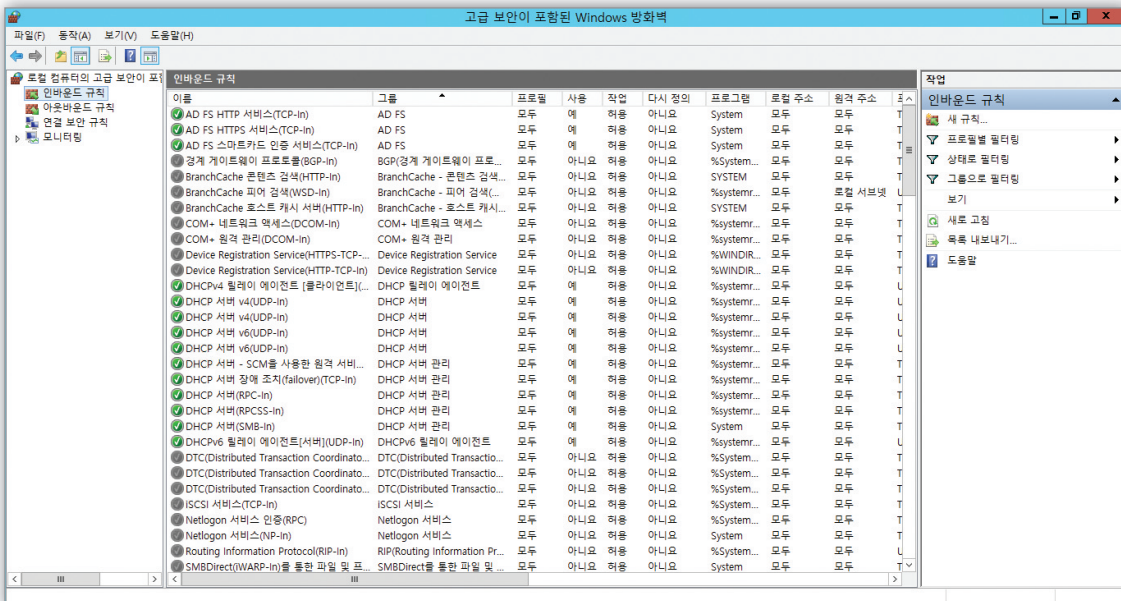
운영 체제에 대한 접근을 제어할 수 있는 방화벽(Firewall)에 대한 동작 방식도 차이가 납니다. **Windows Server 2003**의 초기 출시 버전의 경우에는 별도의 Windows 방화벽이 존재하지 않아, 설치 후, 추가적인 보안 업데이트를 반영하기 전에 공격을 받을 수 있었습니다. 보안 강화를 주 목적으로 한 서비스팩 2(Service Pack 2)가 반영된 설치 이미지를 이용했을 경우, 운영 체제 설치 후, 한시적으로 Windows 방화벽이 동작하여, 시스템에 대한 접근을 막아 주지만, 이후 기본적인 방화벽은 사용되지 않는 상태로 변경됩니다.

<그림 01-05> Windows Server 2003 서비스팩2 설치 초기 화면, 이 단계에서만 기본 방화벽이 동작



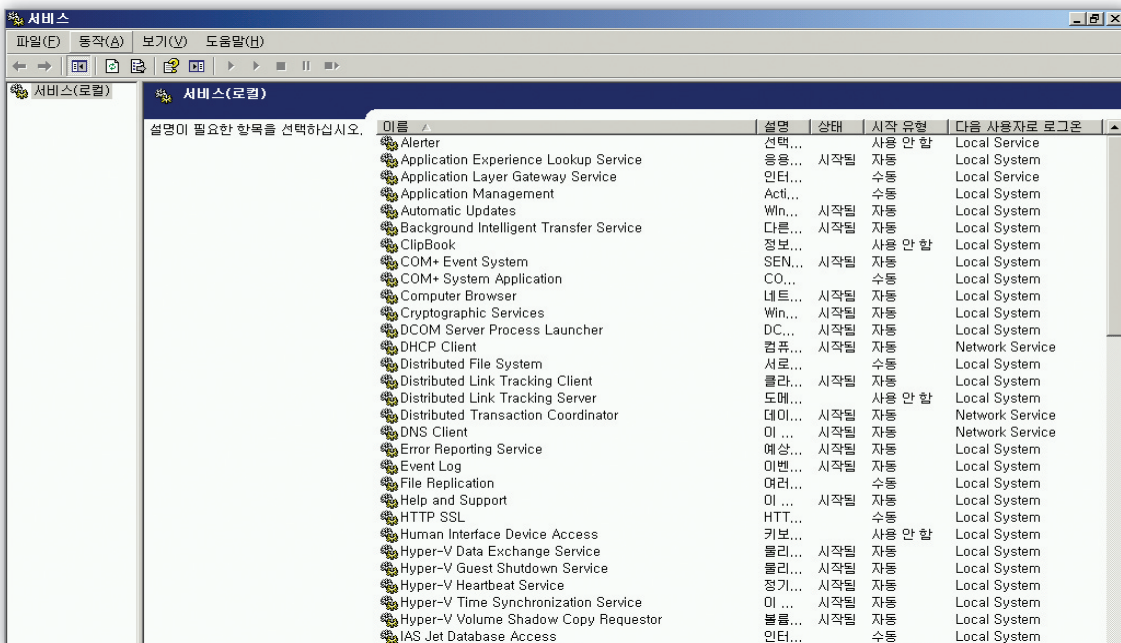
Windows Server 2012 R2의 경우에는 Windows 방화벽이 단순히 시스템에 대한 접근을 차단하고 있는 상태만이 아니라, 원하는 서비스 및 포트에 대한 제어가 가능하고, IPSec(IP 보안) 기술과 연계되어, 인증 및 전송 암호화에 대한 처리 역시 가능합니다. 관리자가 인지하지 못한 채, Windows 방화벽 서비스가 종료될 경우, 운영 체제에 대한 네트워크 처리를 일시적으로 차단시켜, 시스템에 대한 원격 공격을 불가능하게 합니다.

<그림 01-06> Windows Server 2012 R2의 고급 보안이 포함된 Windows 방화벽

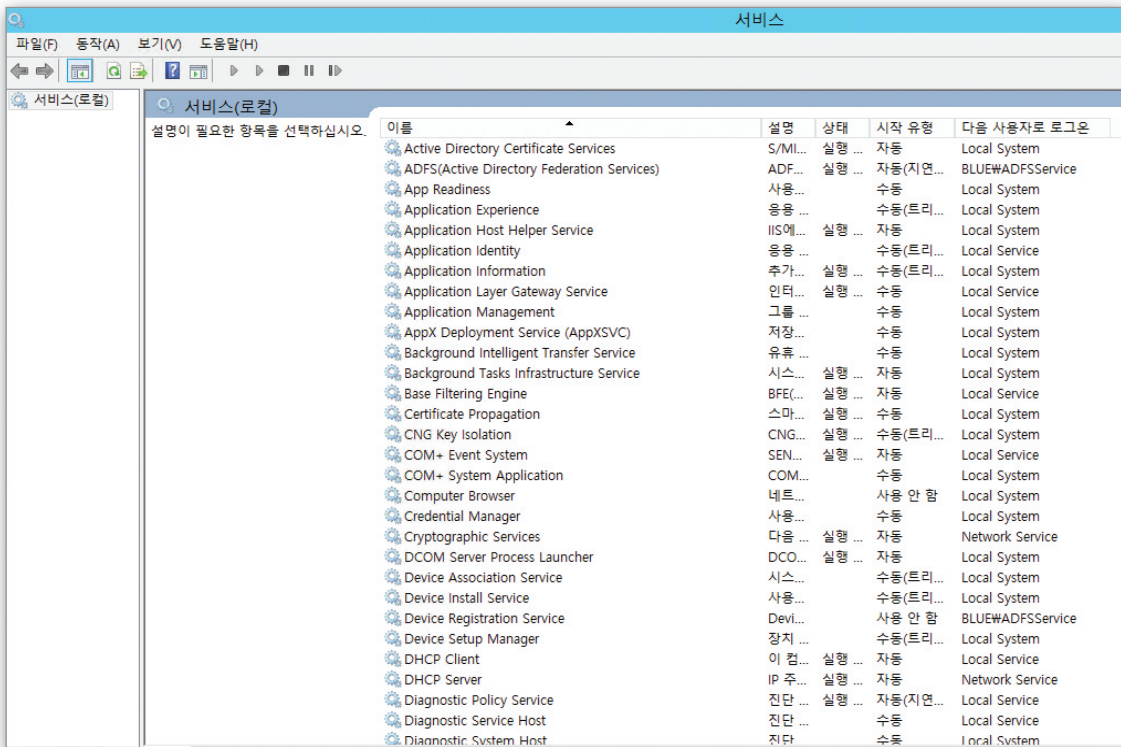


운영 체제의 다양한 서비스에 대한 기본 권한 역시 Windows Server 2012 R2가 보다 세분화되고 최소한의 형태로 제한적입니다. 로컬 시스템(Local System), 로컬 서비스(Local Service), 네트워크 서비스(Network Service)로 구분(높은 권한 순)된 서비스의 기본 계정 역시, 보다 제한적인 권한으로 동작할 수 있도록 Windows Server 2012 R2가 설계되어 있습니다.

<그림 01-07> Windows Server 2003 서비스의 기본 계정, 대부분 Local System으로 동작

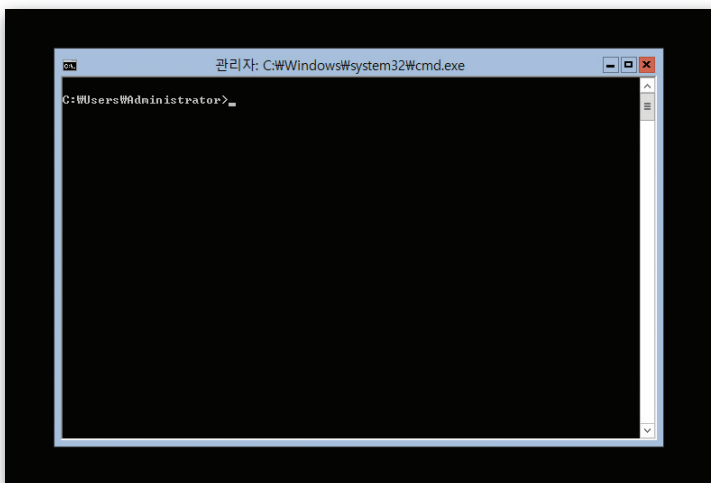


<그림 01-08> Windows Server 2012 R2의 세분화된 서비스 기본 계정



Windows Server 2008부터 서버에 대한 설치 역시, 전체 설치 버전(Full GUI)과 서버 코어(Server Core)로 제공하여, 필요 인프라스트럭처에 대한 리소스 사용량 감소 및 시스템 구성 요소 설치를 줄여, 외부에서 시스템을 접근할 수 있는 노출 지점을 최소화할 수 있습니다. 이는 기본적인 보안 수준을 손쉽게 상승시킬 수 있는 방안을 의미합니다.

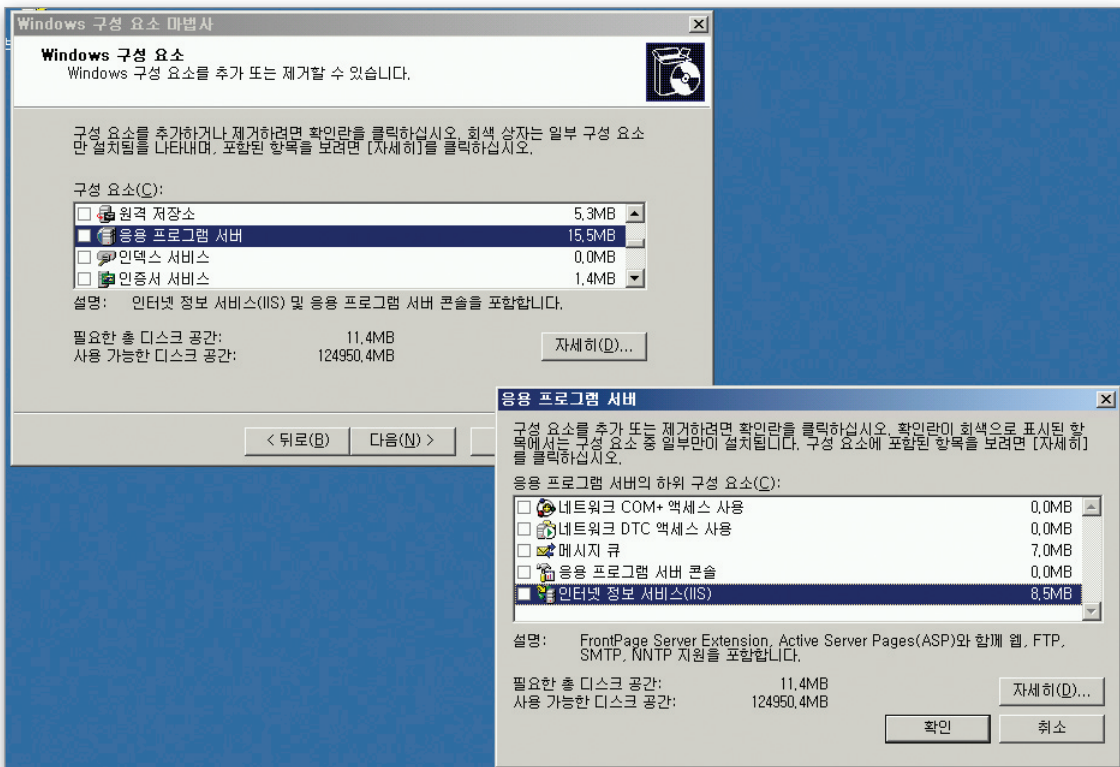
<그림 01-09> Windows Server 2012 R2 서버 코어



웹 서버(IIS, Internet Information Service)의 변화

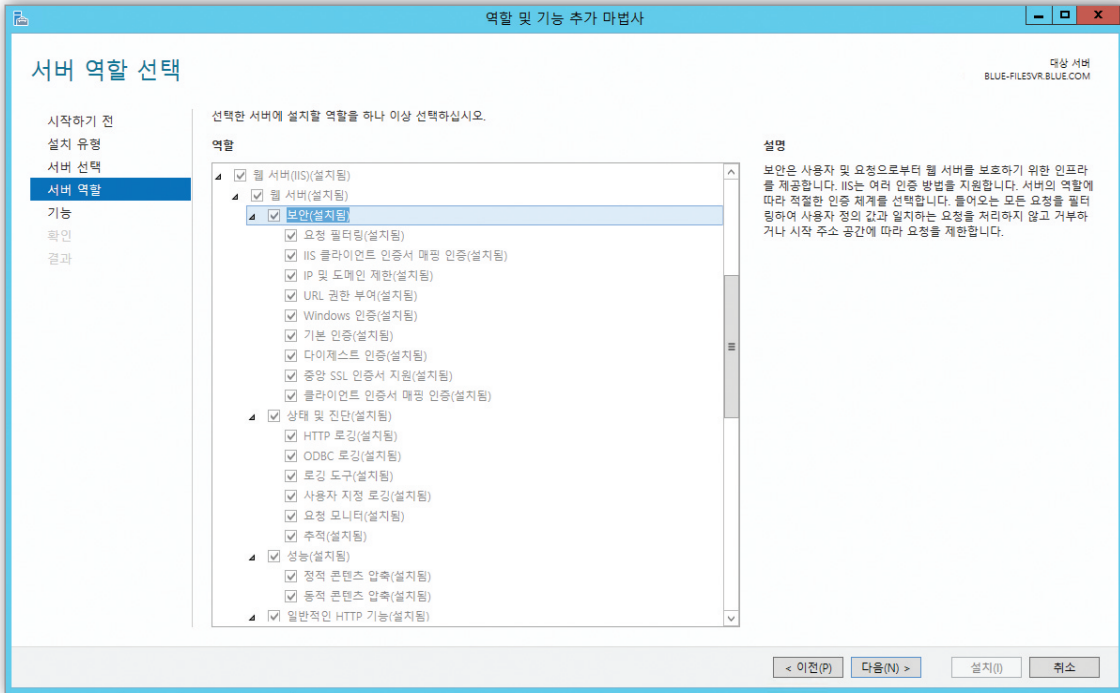
Windows Server 2003의 IIS 6.0 버전과 Windows Server 2012 R2의 IIS 8.0 버전의 큰 차이는 보안 및 성능에 대한 부분입니다.

<그림 02-01> Windows Server 2003 IIS 6 설치



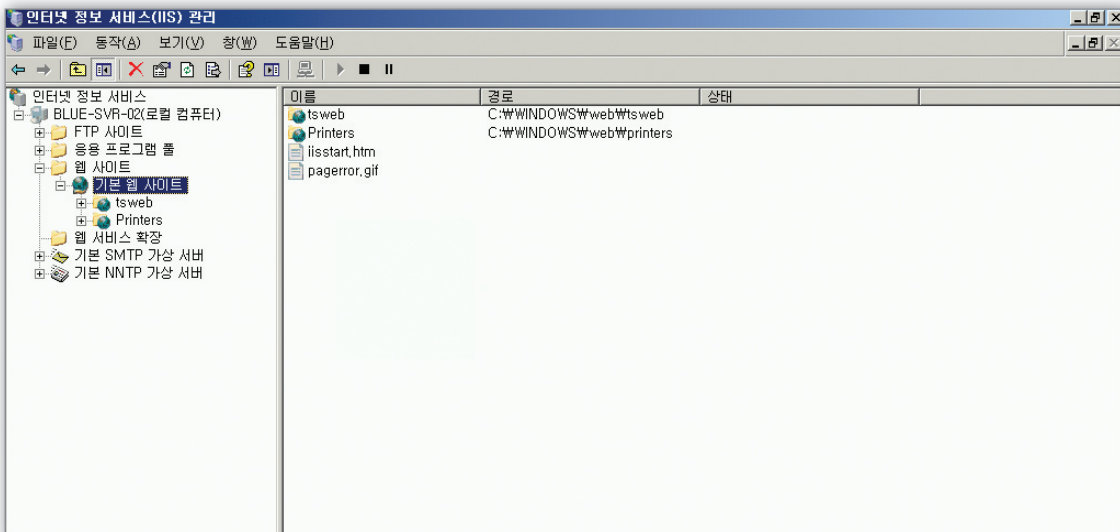
Windows Server 2003의 경우에는 IIS에 대한 설치가 단일 구조로 설계되어 있기에, 필요한 모듈별 설치가 불가능했습니다.

<그림 02-02> Windows Server 2012 R2 IIS 8 설치

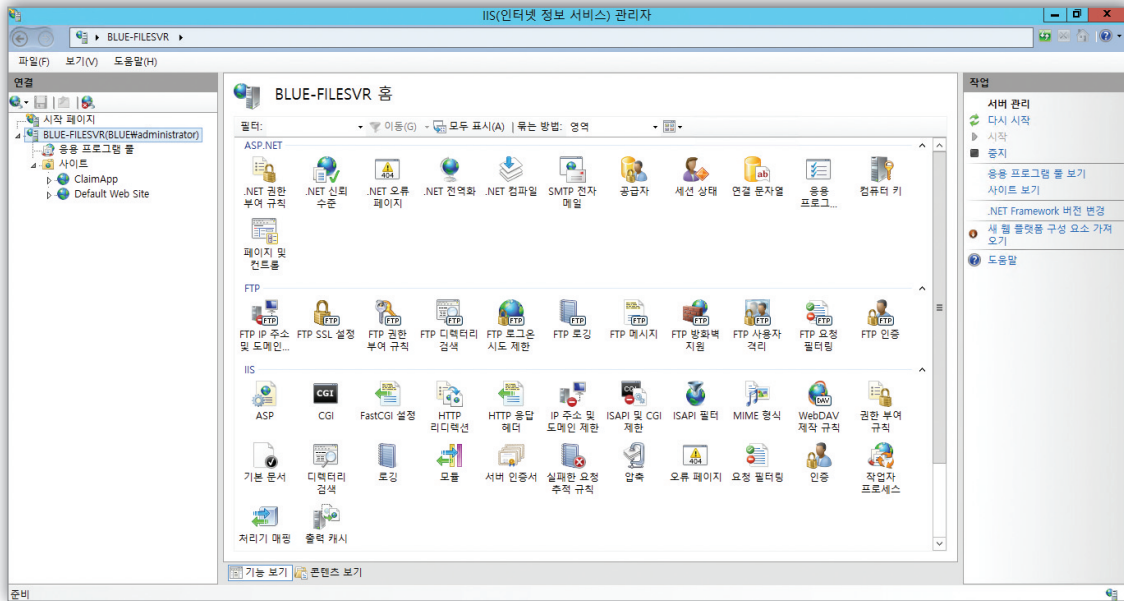


Windows Server 2012 R2의 경우에는 IIS에 대한 설치 구조를 50여개의 모듈로 구분하여, 운영 조직과 관리자가 필요한 부분에 대해서만 설치 가능함과 동시에 보안, 역시 강화할 수 있습니다.

<그림 02-03> Windows Server 2003 IIS 6 관리 도구

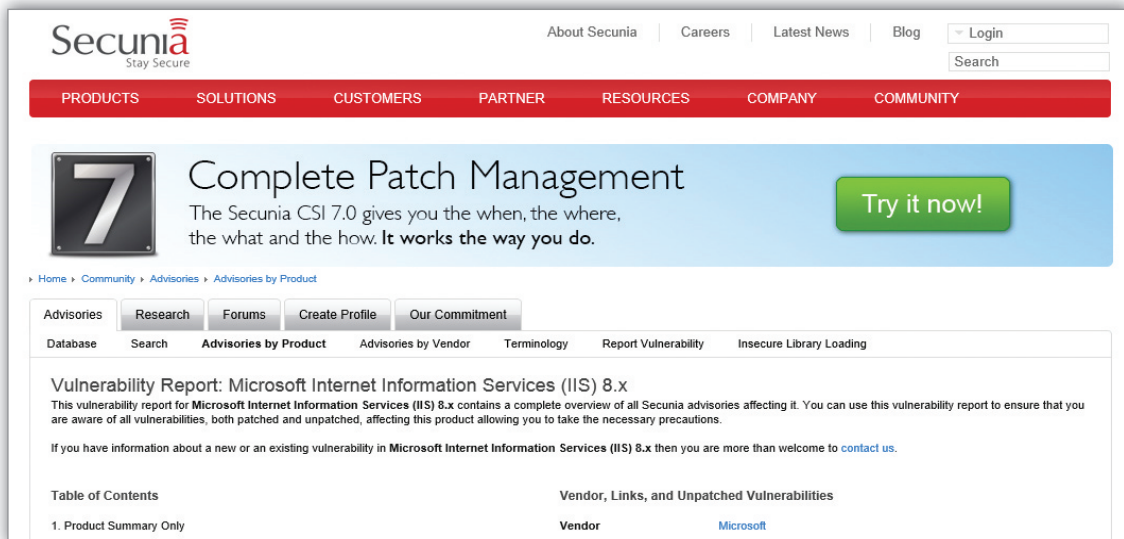


<그림 02-04> Windows Server 2012 R2 IIS 8 관리 도구, 모듈별로 설정 분리



보안에 대한 취약점을 권고하고, 이에 대한 대비책으로 알려진 Secunia(<http://www.secunia.com>)의 보안 권고를 살펴보면, IIS 8 버전에는 별도의 보안 권고가 없으며, IIS 6 버전에는 11개의 취약점 및 권고가 제공되고 있습니다. 이기종에서 사용되는 Apache Tomcat 7 버전에는 15개의 권고 및 33개의 취약점이 보여 집니다. 이미 10년이 된 Windows Server 2003의 IIS 6도 이기종과 비교하여 훌륭한 웹 서버 보안을 보여 주지만, Windows Server 2012 R2의 IIS는 아직까지 별도의 보안 취약점이 발견되지도 않았습니다.

<그림 02-05> Windows Server 2012 R2, IIS 8 버전의 보안



<그림 02-06> Windows Server 2003, IIS 6 버전의 보안

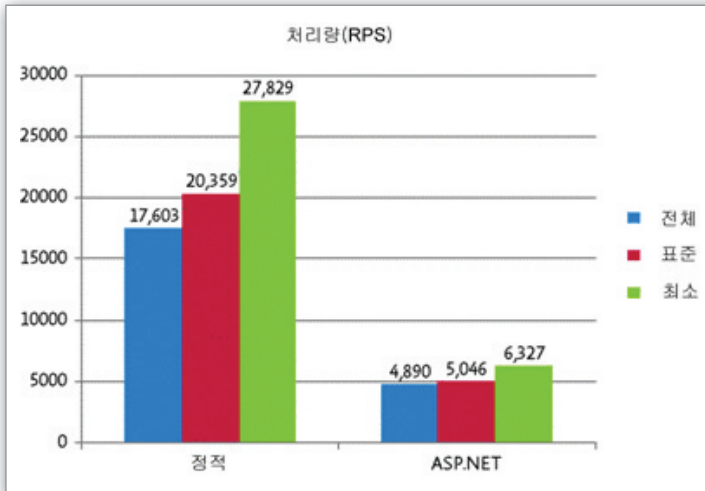
The screenshot shows the Secunia website interface. At the top, there is a navigation bar with links for 'About Secunia', 'Careers', 'Latest News', 'Blog', and a 'Login' button. Below this is a red navigation bar with links for 'PRODUCTS', 'SOLUTIONS', 'CUSTOMERS', 'PARTNER', 'RESOURCES', 'COMPANY', and 'COMMUNITY'. The main content area features a large banner for 'Complete Patch Management' with a 'Try it now!' button. Below the banner, there is a breadcrumb trail: 'Home > Community > Advisories > Advisories by Product'. The 'Advisories' tab is selected, and the 'Advisories by Product' link is highlighted. The main heading is 'Vulnerability Report: Microsoft Internet Information Services (IIS) 6'. The text below states: '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.' It also includes a link to 'contact us' if the user has information about a new or existing vulnerability. A 'Table of Contents' is provided on the left, and a 'Vendor, Links, and Unpatched Vulnerabilities' table is on the right. The table shows the vendor as 'Microsoft' and the product link as 'N/A'.

<그림 02-07> Apache Tomcat 7 버전의 보안

The screenshot shows the Secunia website interface, similar to the previous one. The main heading is 'Vulnerability Report: Apache Tomcat 7.x'. The text below states: '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.' It also includes a link to 'contact us' if the user has information about a new or existing vulnerability. A 'Table of Contents' is provided on the left, and a 'Vendor, Links, and Unpatched Vulnerabilities' table is on the right. The table shows the vendor as 'Apache Software Foundation', the product link as 'View Here (Link to external site)', and the affected by as '15 Secunia advisories' and '33 Vulnerabilities'.

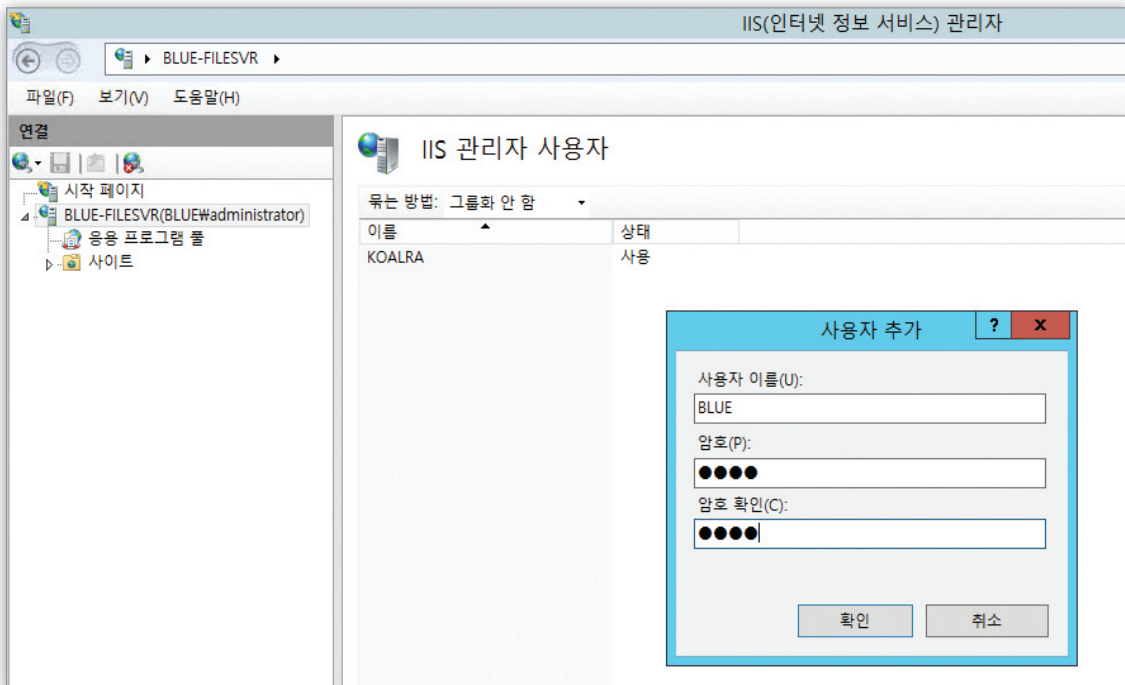
Windows Server 2003 IIS 6과 Windows Server 2012 R2 IIS 8에 대한 성능 차이는 모듈로 구분된 기본 구조와 더불어 NUMA(Non Uniform Memory Access) 기술이 IIS에서 기본 사용되고 있기에, 더 많은 사이트를 단일 서버에서 운영할 수 있으며, Microsoft.com에서는 이미 몇십만개의 사이트를 단일 서버에서 운영한 결과를 보여 주고 있습니다.

<그림 02-08> 동일 클라이언트가 100개일 때, 전체/표준/최소 설치 시 처리량에 대한 비교



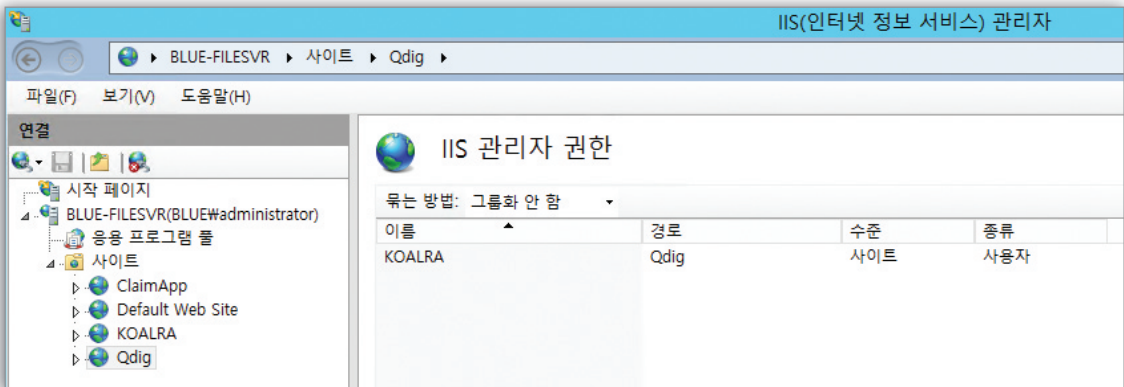
웹 서버를 서비스하는 서버의 하드웨어적인 성능이 높아져 감에 따라, 보다 많은 사이트를 하나의 서버에서 호스팅할 수 있게 되었습니다. 모든 사이트가 단일 관리자에 의해서 관리되는 경우보다, 여러 조직 혹은 외부 고객이나 관리자에 의해서 관리되는 경우, 해당 서버에 대한 인증 및 보안 관리가 Windows Server 2003 IIS 6에서는 쉽지 않은 형태였습니다.

<그림 02-09> IIS 보안 영역에 사용자 생성 및 관리



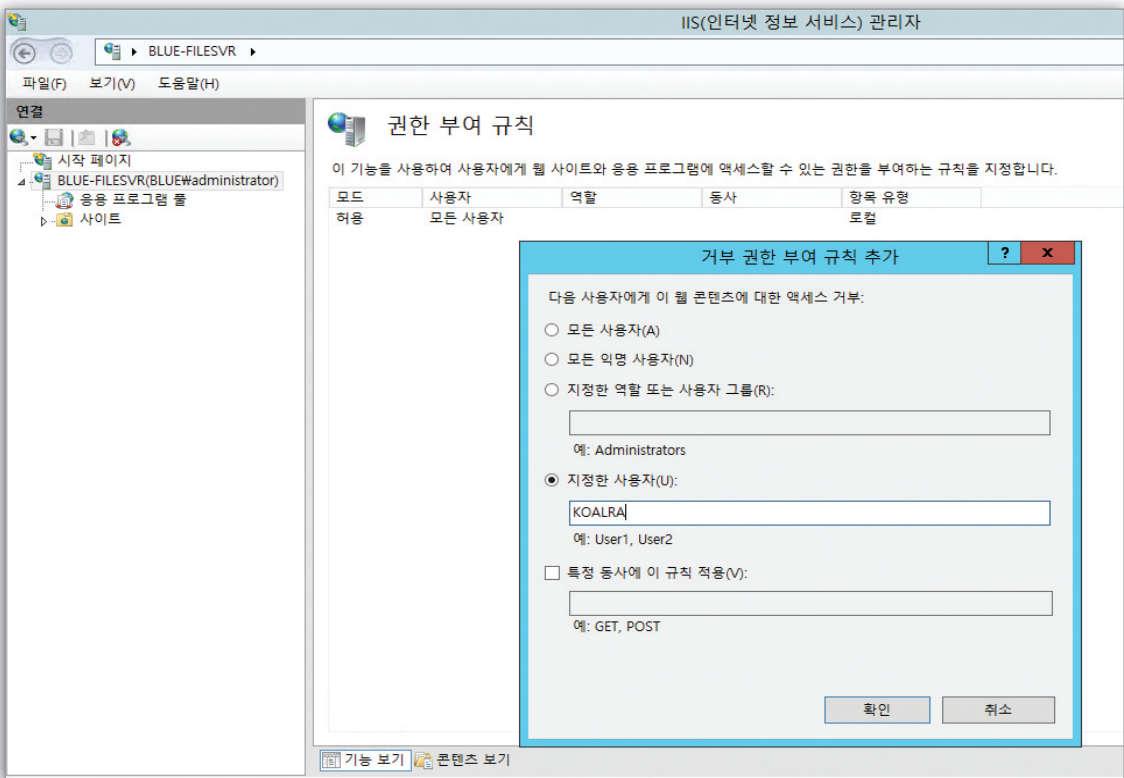
IIS 7부터, IIS에 대한 인증을 기본적으로 Windows 인증을 사용함과 동시에 IIS에서 별도의 사용자를 선언하여, Windows 보안 영역(Security Context)와 분리할 수 있게 되었습니다.

<그림 02-10> IIS내 사이트에 관리자 권한 부여



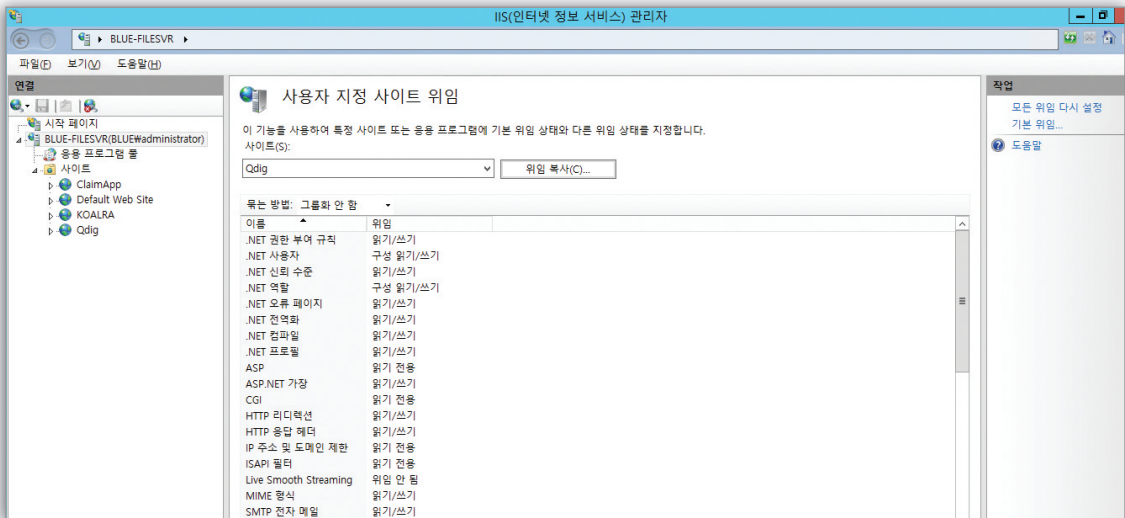
IIS에서 별도의 사용자를 선언한 후, 관리자별로 관리할 사이트를 지정할 수 있고, 해당 사용자는 지정된 사이트 이외에는 관리할 수 없습니다. (인증 처리 불가)

<그림 2-11> IIS에서 생성된 사용자에게 대한 사이트나 디렉터리에 권한 부여



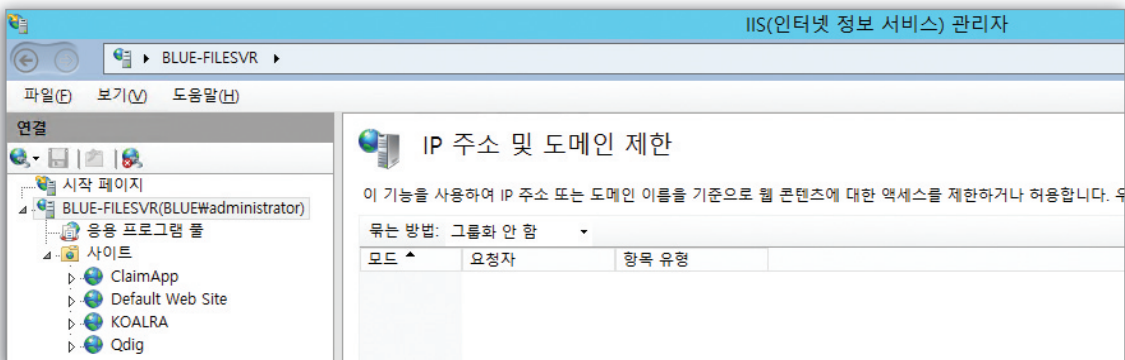
IIS내 사용자는 관리 용도 이외에도 필요 시 웹 사이트 내 가상 디렉터리나 응용 프로그램에 별도의 권한을 부여, 차단할 수 있게 사용할 수 있습니다.

<그림 02-12> IIS의 모듈별 사용자 위임



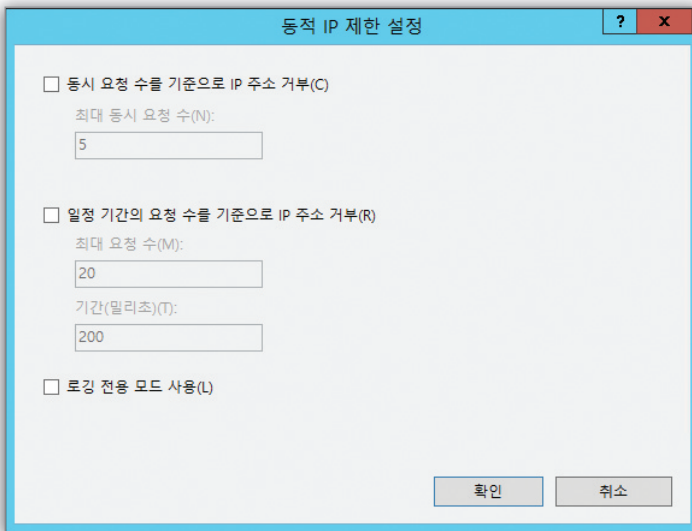
IIS의 특정 모듈에 대해서 중앙 관리 정책을 가지고 있거나, 보안/성능상의 이유로 수정을 불가능하게 지정, 혹은 설정 확인만 하고자 할 경우, 기존 IIS 6는 단일 구조로 설계되어 있으므로, 별도의 기능 차단이 불가능합니다. IIS 7 이후부터, 모듈별 위임 기술이 탑재되어, 중앙 관리자는 사이트 별로 특정 모듈에 대해 권한을 부여하거나, 읽기 전용으로 확인만 가능, 혹은 아예 확인조차 할 수 없도록 모듈을 감출 수 있게 제공합니다.

<그림 02-13> IP 주소 및 도메인 제한을 통한 보안 강화



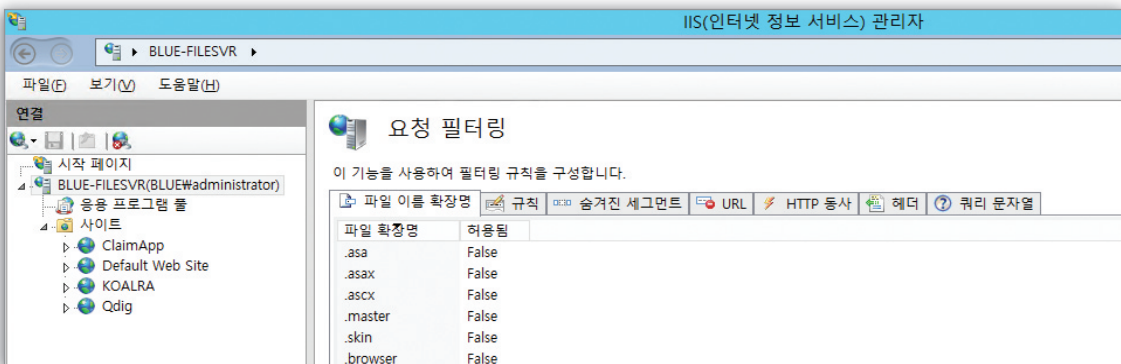
웹 서버를 향한 여러 공격 방식에 대해 네트워크 영역에서 장비를 이용해서 방어하는 형태도 사용할 수 있지만, 추가적으로 운영 체제의 주요 방어 기술 역시 중요합니다. IIS 7부터 IP 주소 및 도메인 제한을 이용하여 특정 IP 주소 및 도메인을 운영 체제 레벨에서 방어할 수 있습니다.

<그림 02-14> IP 주소 및 도메인 제한 기술 내 동적 적용



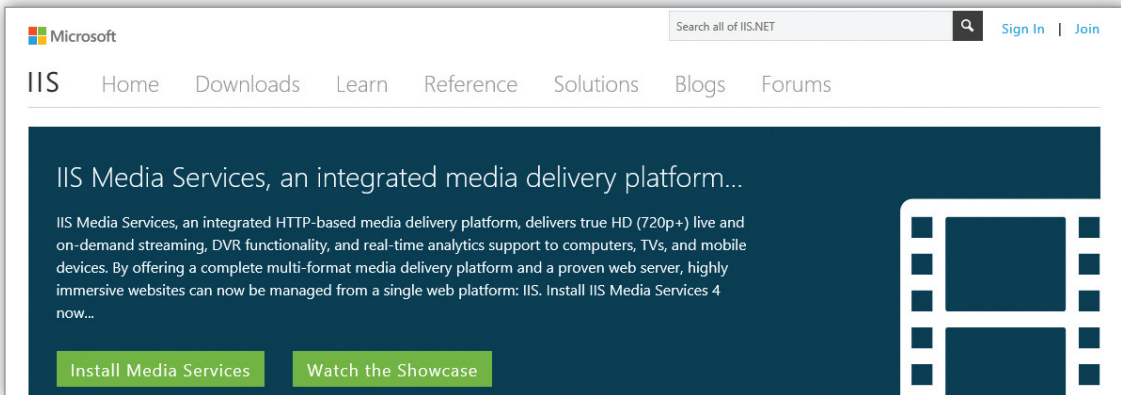
IP 주소 및 도메인 제한 기술에는 동적 제한 기술도 기본 내장되어 있어, 동시 요청을 서버에 전송하여 서버를 공격하거나, 이를 조금 더 고급화하여, 일정 시간 내에 요청 수를 기준으로 방어를 활성화할 수 있습니다.

<그림 02-15> URLScan 기술에 기반한 요청 필터링



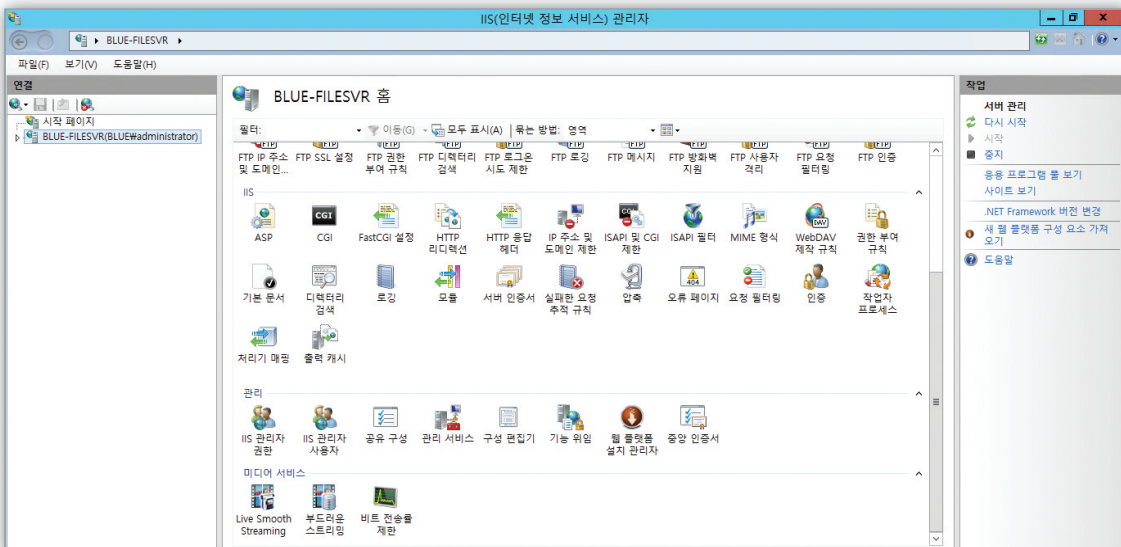
웹 서버로 요청되는 여러 서비스들에 대해서 확장명, 규칙, 숨겨진 세그먼트, URL, HTTP 동사, 헤더, 쿼리 문자열로 필터링할 수 있는 URLScan 기술을 기본적으로 탑재하여, 서버에 대한 요청 보안 역시, 기본적으로 동작시킬 수 있습니다.

<그림 02-16> IIS 미디어 서비스



디바이스 시대에 따른 다양한 클라이언트 환경 역시, IIS의 변화를 이끌었는데, 미디어 서비스에 대한 기본 기능 탑재도 이와 함께 하게 됩니다. Windows Server 2003 시절에는 미디어 서비스라는 별도의 서비스를 Windows Server에 설치하여 제공하였고, 해당 서비스에서 제공되는 미디어 유형 역시 제한도 존재하였지만, IIS의 미디어 기술 확장을 사용하면, 동영상의 비트 전송률(Bit Rate)을 확인하여, 이에 적절한 대역폭 제공과 실시간 부드러운 스트리밍(Smooth Streaming)까지 적용할 수 있습니다.

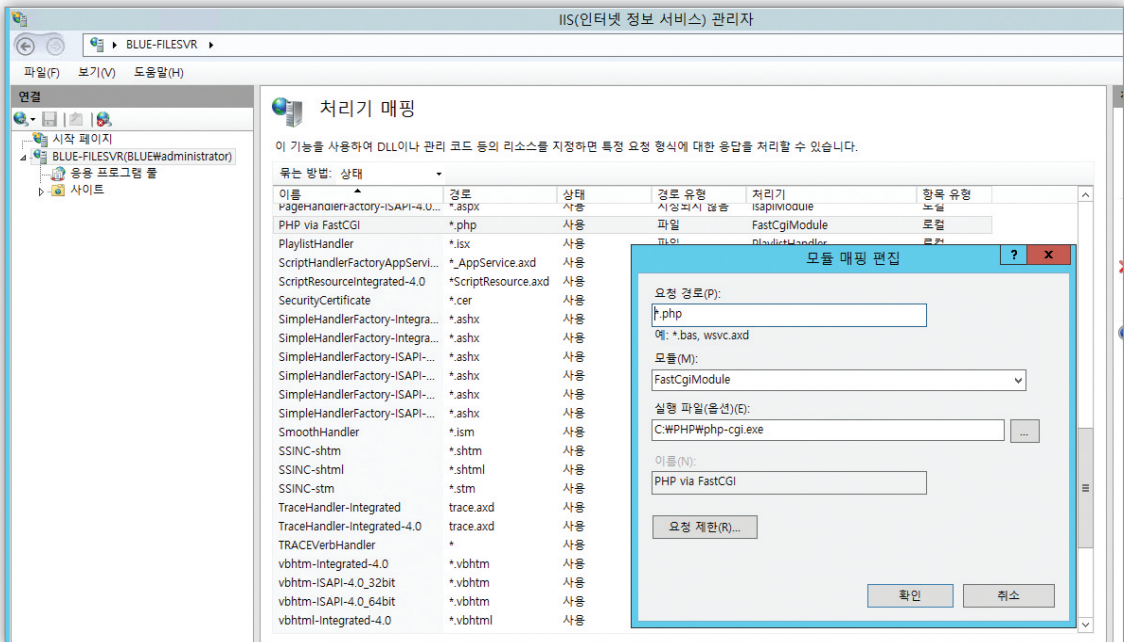
<그림 02-17> IIS 미디어 서비스



자세한 사항은 <http://www.iis.net/media>를 참고하면 좋습니다.

또한, IIS 7부터 Zend Technologies와 협력한 FastCGI 모듈을 통해 확장된 응용 프로그램 프레임 워크는 PHP 프레임워크를 제공합니다.

<그림 02-18> IIS 8, FastCGI를 통한 PHP 설정



이를 통해 다른 플랫폼을 주로 사용했던 PHP에 대해서도 Windows 플랫폼 및 기술과 동일한 형태로 성능 및 환경을 서비스 할 수 있습니다.

<그림 02-19> PHP 사이트에 부하가 걸렸을 경우, 처리 모듈이 다수의 프로세스로 확장 처리

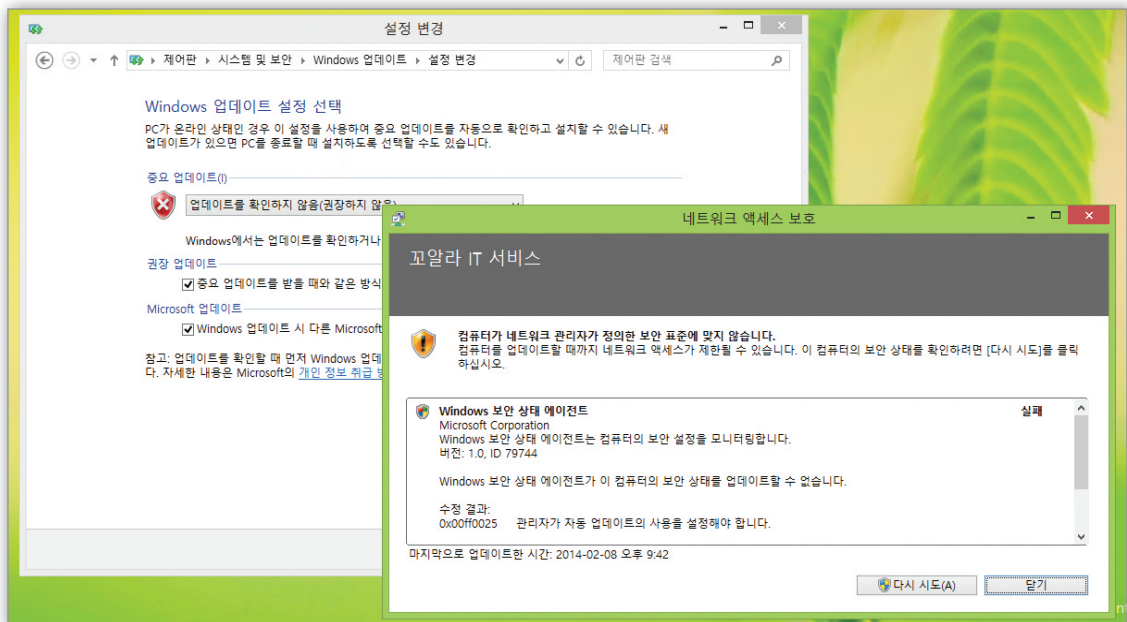
프로세스		성능	사용자	세부 정보	서비스
이름	상태	100% CPU	41% 메모리		
앱 (4)					
▶ Internet Explorer		0%	13.6MB		
▶ Windows 명령 처리기		0%	0.5MB		
▶ Windows 탐색기		0%	41.5MB		
▶ 작업 관리자		7.9%	7.5MB		
백그라운드 프로세스 (15)					
CGI / FastCGI(32비트)		3.5%	2.2MB		
CGI / FastCGI(32비트)		6.5%	2.2MB		
CGI / FastCGI(32비트)		5.6%	2.2MB		
CGI / FastCGI(32비트)		1.0%	2.2MB		
CGI / FastCGI(32비트)		22.2%	2.7MB		
IIS Worker Process		8.3%	18.2MB		

엔드포인트/클라이언트 보안(Endpoint 보안) 및 모바일 연결성 제공

모바일 디바이스 시대에는 이제 정적인 클라이언트 관리 환경이 아닌, 동적이면서 실시간으로 적용되는 클라이언트 보안 관리가 필수적이 되었습니다.

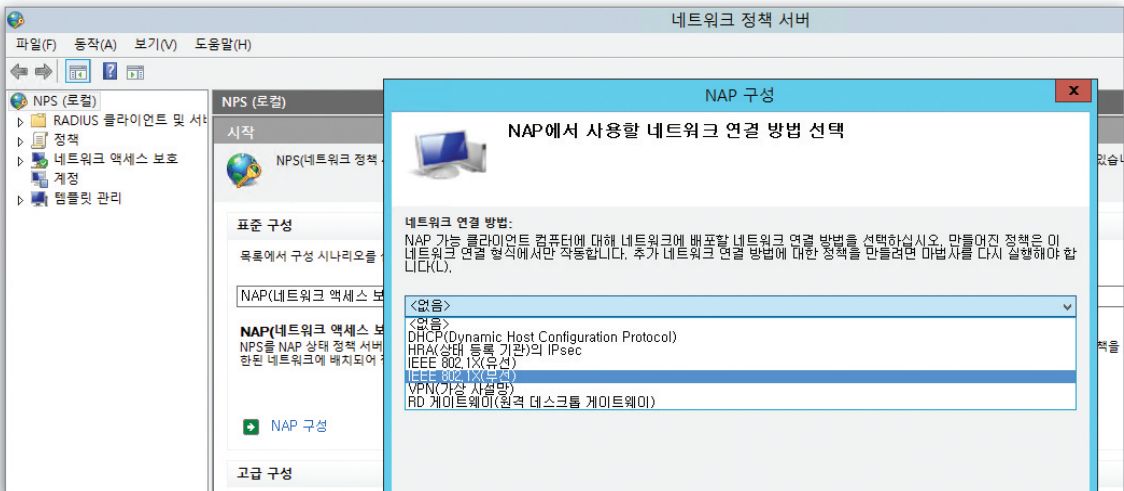
일반적으로 조직에서는 클라이언트 보안을 로그인 시, 혹은 최초 조직에 디바이스를 가져왔을 경우에 검사한 후, 이를 네트워크에 연결하게 됩니다. 이후 네트워크에서 비정상적인 동작을 감지하여 적절하게 네트워크를 격리하거나, 치료할 수 있는 기술에서 이제 고민할 시점이 되었습니다.

<그림 03-01> 네트워크 액세스 보호



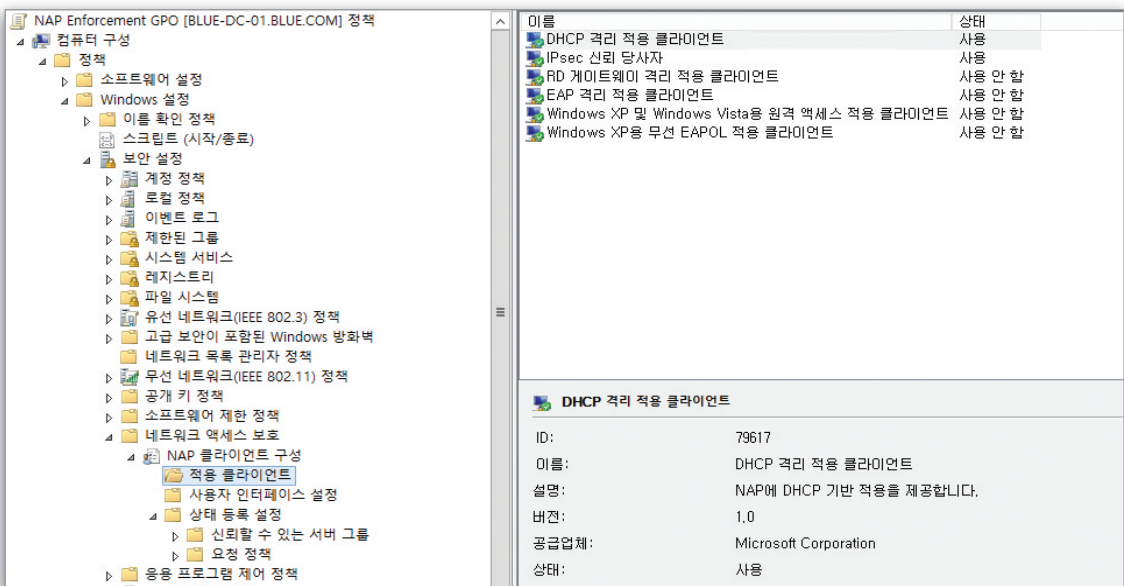
네트워크 액세스 보호(NAP, Network Access Protection)을 통해 Windows 클라이언트의 보안 상태를 실시간으로 감지하고, 문제 발생시 네트워크를 격리할 수 있습니다.

<그림 03-02> Windows Server 2012 R2 네트워크 정책 서버



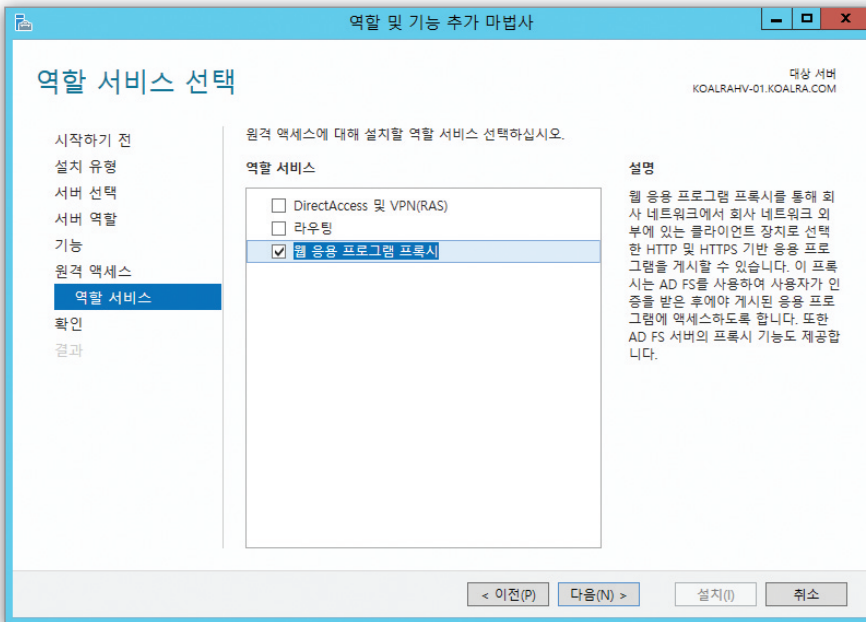
Windows Server 2012 R2의 네트워크 정책 서버를 통해, DHCP, IPsec, 유/무선에 대한 802.1X, VPN, 원격 데스크톱 게이트웨이 시나리오에 대한 NAP을 적용할 수 있습니다. 적용 시나리오는 조직의 보안 요구 사항에 적합할 수 있도록, 복수로 적용하여 보다 높은 보안 수준에 맞출 수 있습니다. 클라이언트 구성에 대한 중앙 관리 역시, 액티브 디렉터리(Active Directory)의 그룹 정책을 통해 손쉽게 구성할 수 있습니다.

<그림 03-03> NAP 그룹 정책



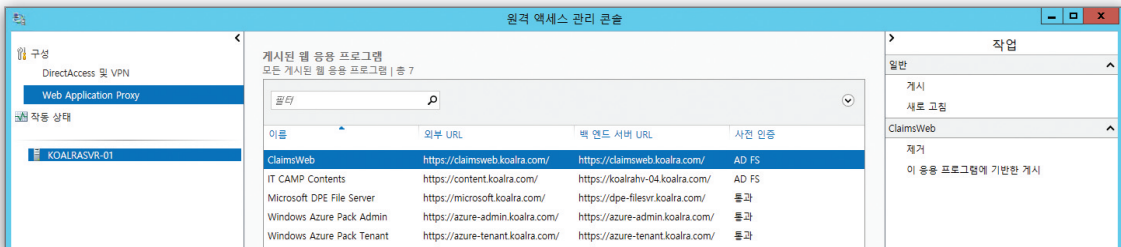
조직 내부 네트워크 환경이 아닌, 인터넷 환경에서 업무를 하게 되는 모바일 디바이스에 대해서 안전하게 조직 네트워크에 대한 접근성 및 서버 기기도 검토해야 할 대상입니다.

<그림 03-04> 웹 응용 프로그램 프록시 설치



Windows Server 2012 R2에서는 웹 응용 프로그램 프록시(WAP, Web Application Proxy) 기술을 제공하여, 외부로 게시해야 할 내부 기간계 웹 사이트에 대해서 안전한 외부 접근성을 제공합니다.

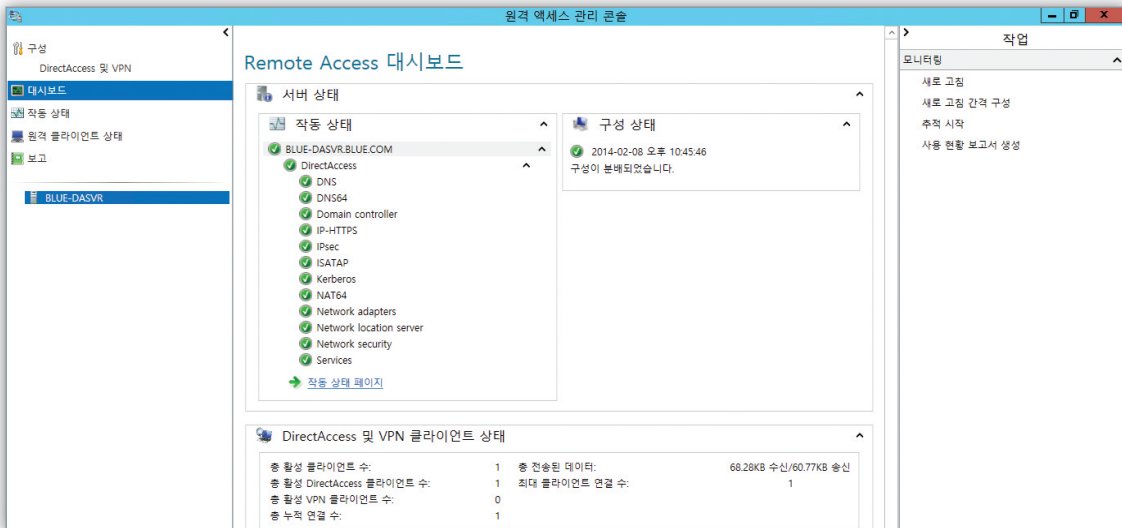
<그림 03-05> WAP을 통한 내부 인프라 게시



WAP을 이용하게 되면, Windows Server 2012 R2가 내부의 리소스에 대해서 외부로 제공하는 서비스와 더불어, 사전 인증에 대한 부분을 페더레이션 서비스로 먼저 처리하여, 인증을 넘겨줄지, 아니면 기존과 동일하게 내부에서 처리할지에 대한 부분도 세분화시킬 수 있습니다. 내부 리소스에 대한 HTTPS의 게시는 Windows Server 2012 R2만으로도 이제 가능해 졌으며, WAP을 통하여 클라우드 폴더, 디바이스 등록 서비스 등도 제공됩니다.

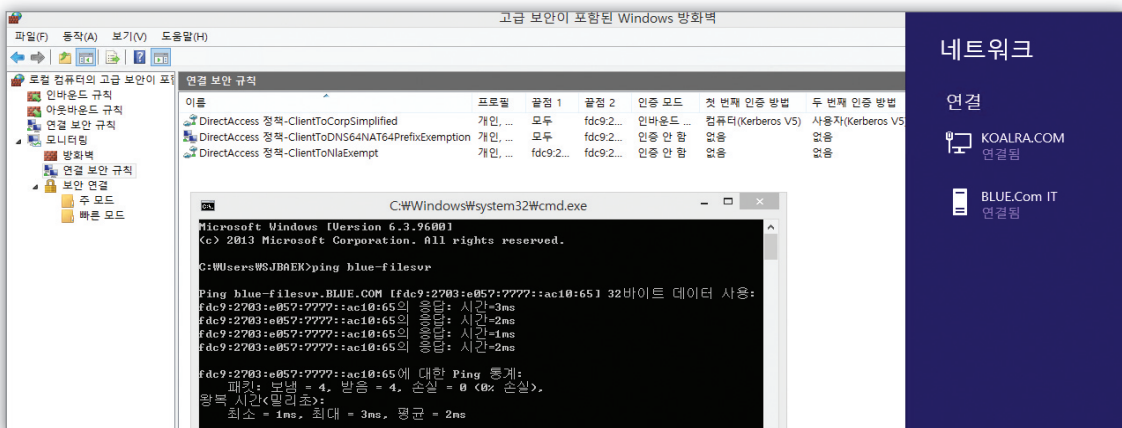
Windows 클라이언트와 인터넷 환경에서 조직의 네트워크에 연결될 때, 일반적으로는 VPN 기술을 떠올리곤 합니다. VPN의 경우에는 클라이언트에 별도의 소프트웨어를 설치하고, 이에 대한 설정을 반영해야 하며, 이 경우 사용자의 실수, 혹은 인터넷 환경에서 제공하는 프로토콜 설정에 따라 접근이 되지 않을 수 있습니다. Windows Server의 DirectAccess 기술을 활용하면, 중앙에서 조직 네트워크 접근에 대한 설정을 반영할 수 있으며, 클라이언트는 조직 네트워크에 있지 않을 경우, 자동으로 이를 감지하여 DirectAccess 서버에 접속하게 됩니다.

<그림 03-06> Windows Server 2012 R2 DirectAccess



VPN과는 달리 DirectAccess는 인터넷에서 접근 중인 클라이언트에 대해, 조직 내부에서 접근이 가능한 양방향 접속을 연결하게 되기 때문에, 관리자는 규정에 대한 강제 반영, 클라이언트에 대한 연결이 자유롭습니다. 더불어, 클라이언트에서는 Teredo, IPHTTPS 등 다양한 인터넷 접속 환경에서 가장 최적의 접속 방식을 선택해 연결하게 됩니다.

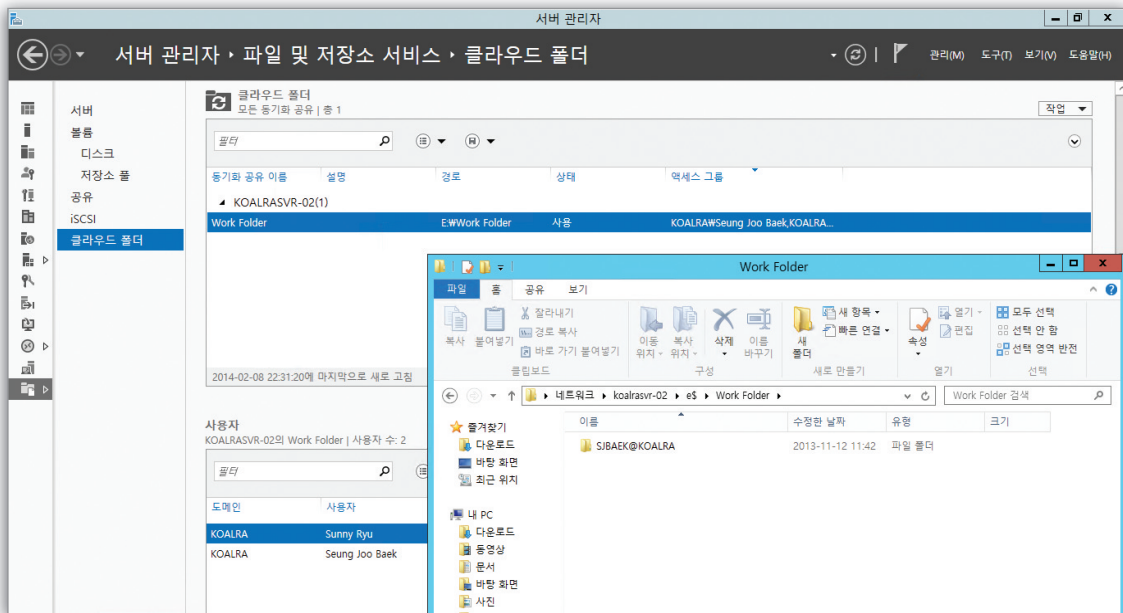
<그림 03-07> Windows 클라이언트에서 DirectAccess를 통한 접근



DirectAccess의 접근시 사용하는 인증 및 암호화 기술은 일반적으로 안전하다고 인지하는 L2TP VPN과 거의 동일한 원천 기술을 사용합니다.

마지막으로 클라우드 폴더도 관심있게 살펴볼 수 있는 기술입니다. Windows 8에서부터 디바이스의 설정을 동기화하거나, 데이터에 대한 디바이스 간 관리를 위해 Microsoft에서 제공하는 SkyDrive를 사용했다. 비즈니스 조직의 경우에는 Microsoft의 공용 클라우드가 아닌, 사내에서 제공하는 폴더 형태의 웹 드라이브를 요구했고, 이를 Windows Server 2012 R2에서 적용하였습니다.

<그림 03-08> Windows Server 2012 R2에서 구성한 클라우드 폴더



인터넷 환경에서 접속하는 디바이스의 경우 클라우드 폴더를 설정해 사내의 폴더와 안전하게 동기화할 수 있어, 데이터에 대한 보안 및 규정을 준수하면서, 편리하게 외부에서 개인의 폴더를 사용할 수 있습니다.

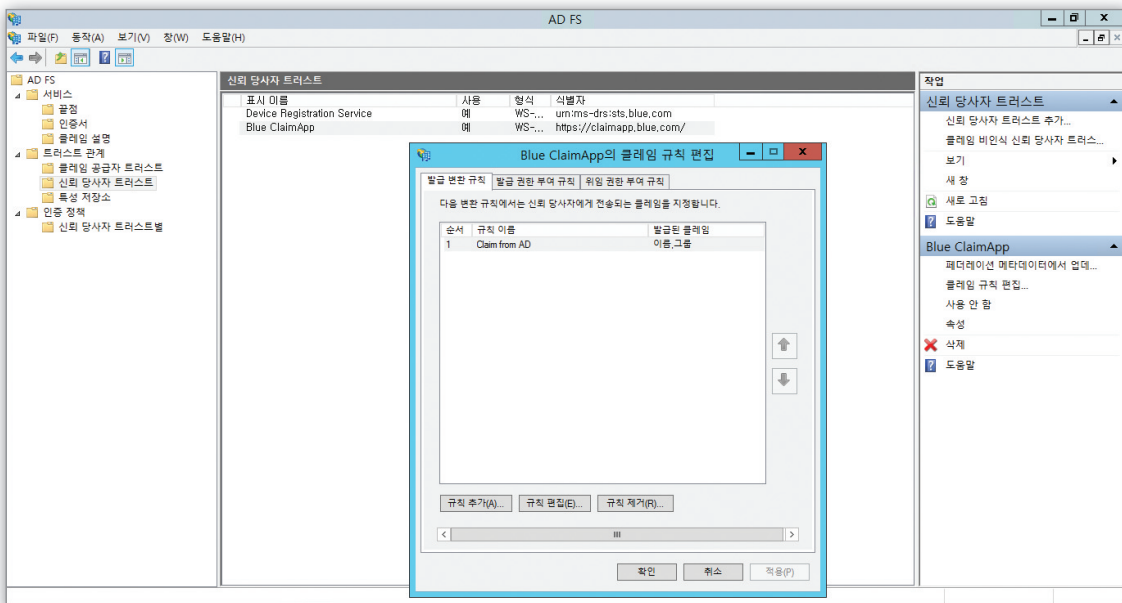
<그림 03-09> Windows 클라이언트에서 사용중인 클라우드 폴더



클라우드 시대에 적절한 ID(Identity) 및 보안 권한 관리

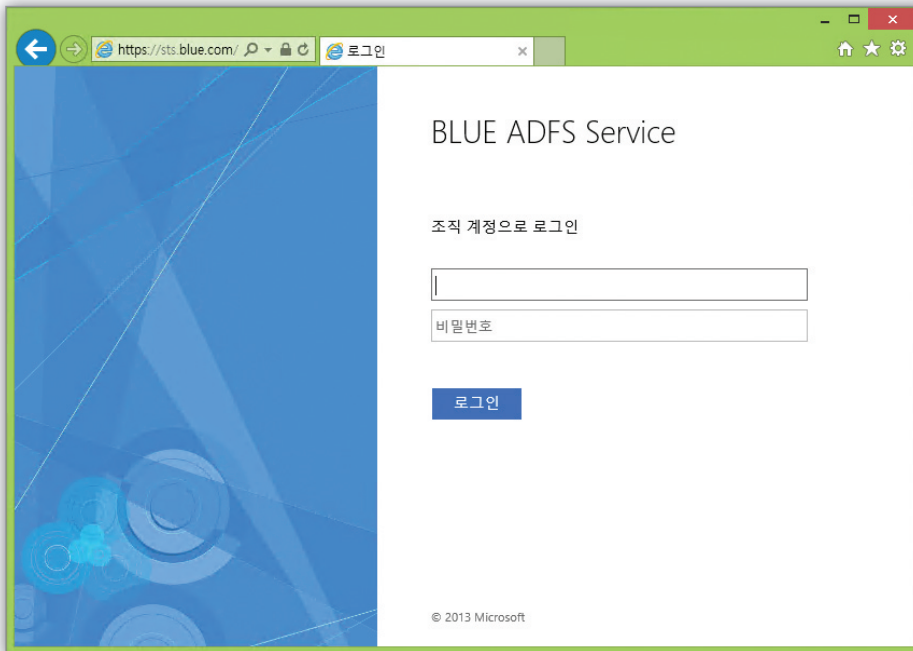
액티브 디렉터리(Active Directory)를 기본으로 하는 클라이언트 IDENTITY 관리의 LAN 환경에 국한된 형태의 조직에서만 적용이 가능합니다. 클라우드 시대에 일반적으로 사용되는 클라이언트 및 디바이스 접근 방식인 웹 환경에서는 VPN과 같은 네트워크 기술을 추가하여 LAN에 대한 접근성을 확보해야 합니다.

<그림 04-01> Windows Server 2012 R2의 액티브 디렉터리 페더레이션 서비스(AD FS)



Windows Server 2012 R2에서는 IDENTITY에 대한 인증을 클라우드 환경으로 확장할 수 있도록 페더레이션 서비스(Federation Service)를 강화하였습니다.

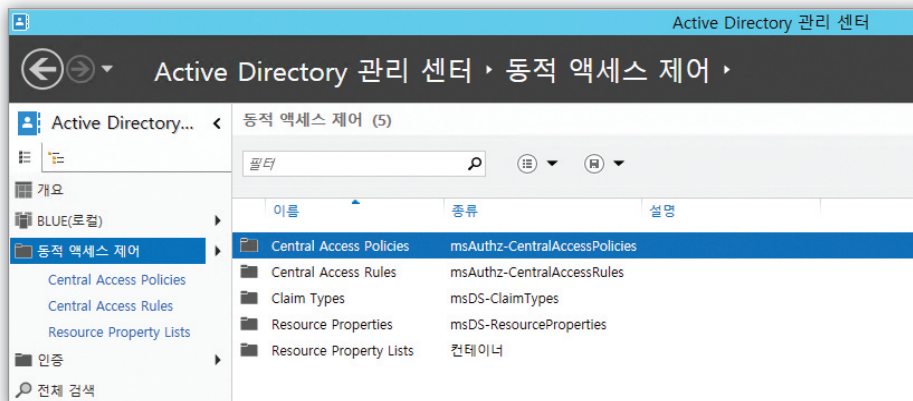
<그림 04-02> 디바이스에서 페더레이션 서비스를 접속한 경우



페더레이션 서비스와 연계된 조직내 기간제 시스템, 그리고 외부에서 서비스되고 있는 클라우드의 경우, SSO(Single Sign On) 처리를 할 수 있게 됩니다. SSO에 대한 중앙 관리 및 처리는 단일 ID를 사용하는 형태의 보안 향상 및 생산성, 나아가 보안 관계 변경 시 손쉬운 기술 변경 처리가 가능합니다.

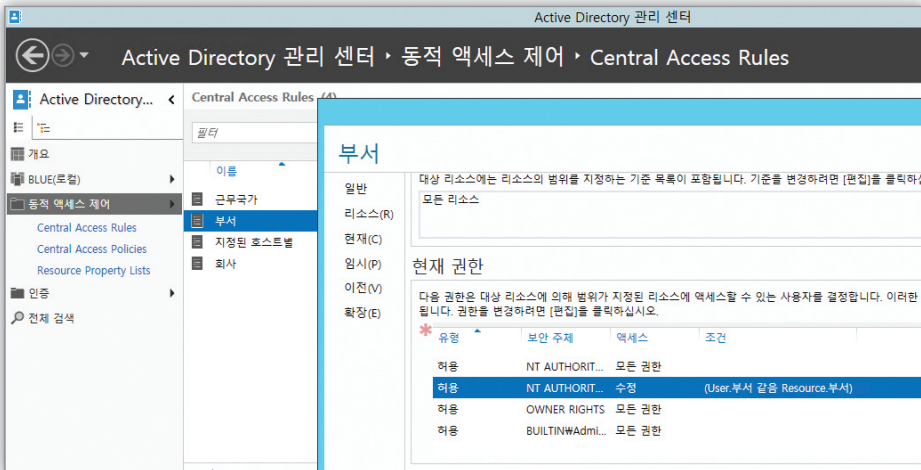
사용자 및 그룹 방식으로 관리되던 조직 내 사용 권한의 관리 역시 빨라진 비즈니스 변화에 따라 변화되어야 합니다.

<그림 04-03> 동적 액세스 제어



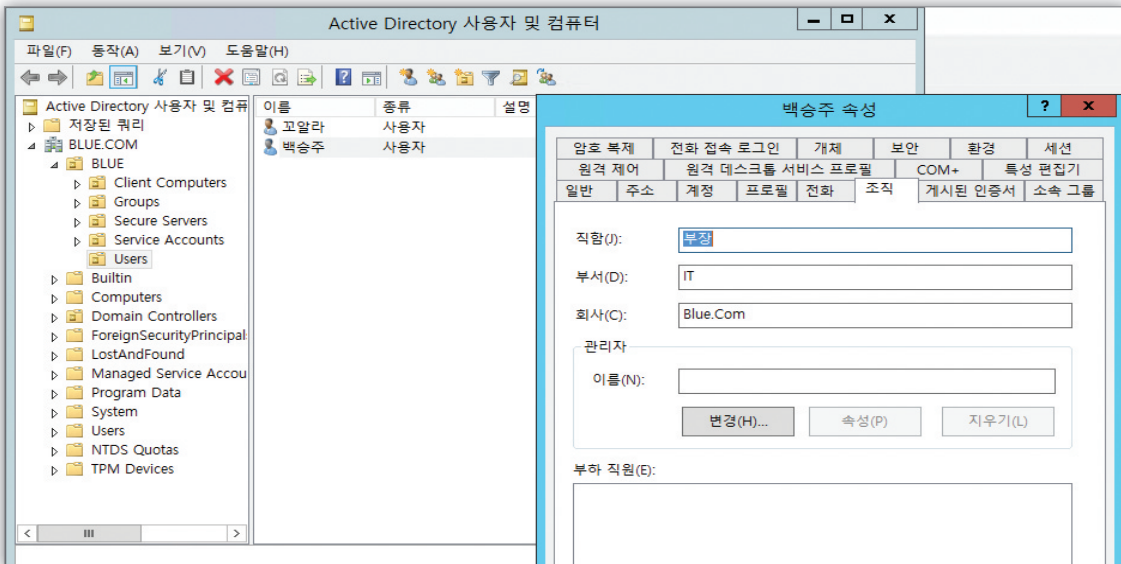
동적 액세스 제어(DAC, Dynamic Access Control)은 사용자와 그룹에 부여하던 사용 권한을 특정 조건에 따라 부여할 수 있는 기술적 기반을 제공합니다. 이러한 형태의 관리를 우리는 클레임 기반(Claim Based) 관리라고 부릅니다.

<그림 04-04> 동적 액세스 제어에서 선언한 보안 권한



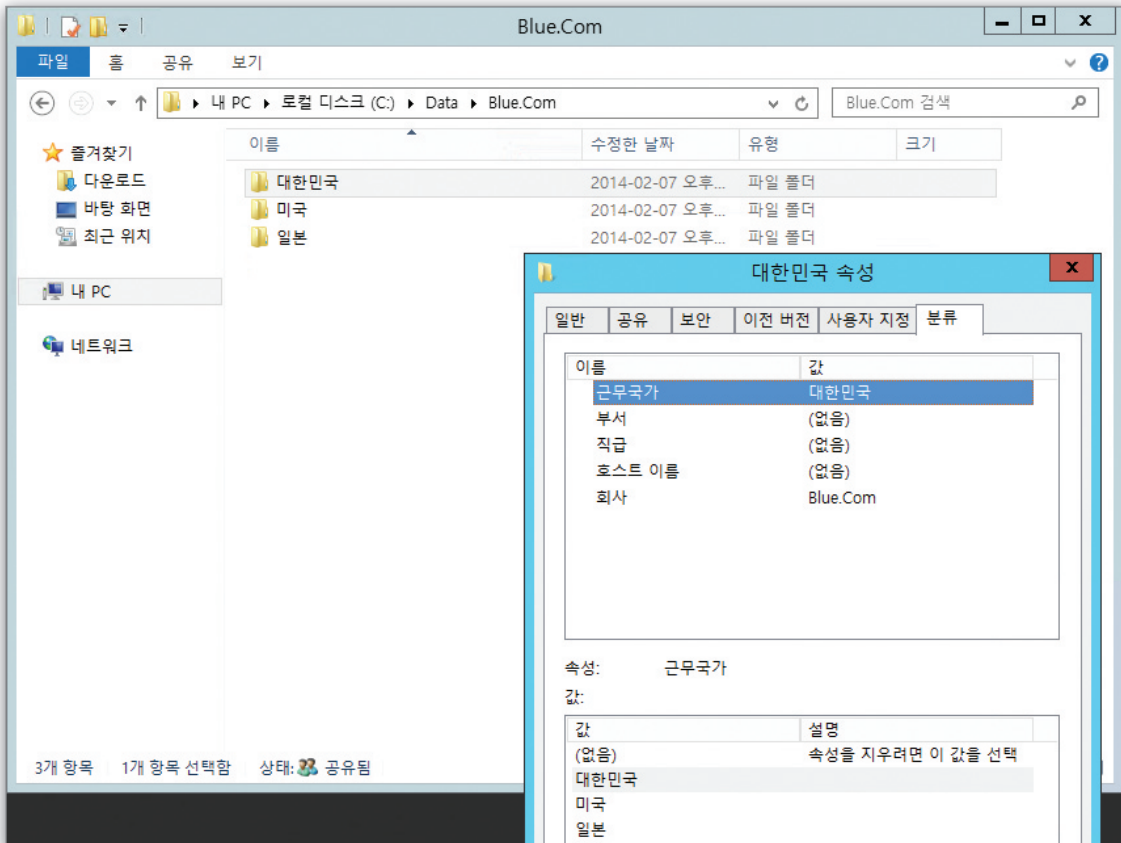
사용자 및 그룹의 특성(Attribute)에 기반한 권한을 만들고, 해당 조건이 맞을 경우, 권한을 할당하게 됩니다. 비즈니스나 조직 구조의 변화에 따라 사용자의 특성이 변경되었을 경우, 사용자는 권한을 얻거나, 잃게 됩니다.

<그림 04-05> 액티브 디렉터리의 사용자 특성



예를 들어, 사용자의 부서가 근무 국가가 대한민국으로 되어 있는 경우에, DAC를 활용하면 폴더 특성을 살펴볼 수 있습니다.

<그림 04-06> 폴더에 부여된 분류



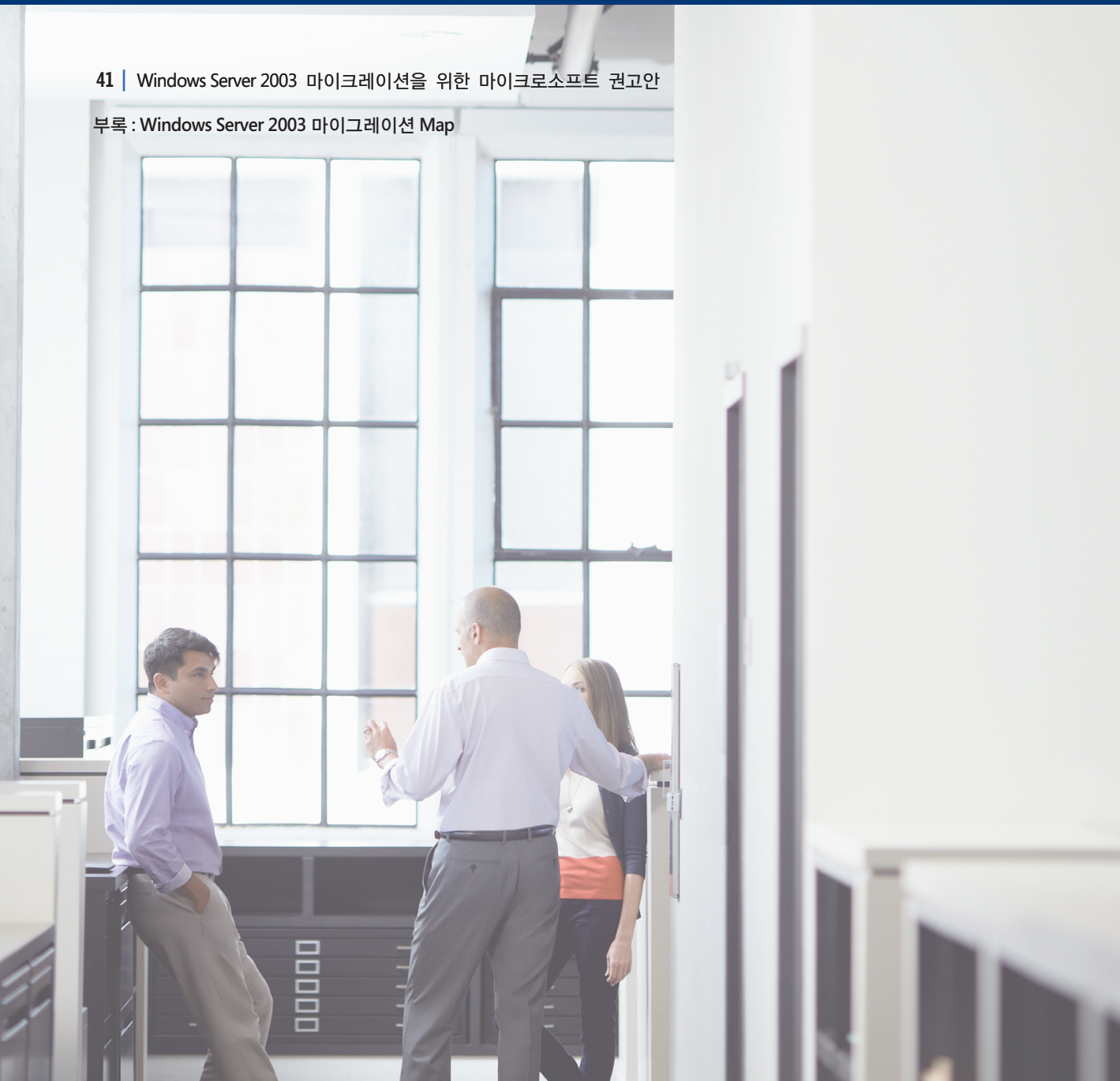
조직 내 파일 서버 폴더들에 분류가 지정되고, 해당 분류와 사용자 특성이 같은 경우만 접근이 가능한 형태입니다.

DAC에서 사용하고 있는 클레임 기반 기술은 앞서 언급한 페더레이션 서비스에서도 동일한 형태로 활용되고 있으며, 별도의 보안 그룹 관리가 아닌 개체의 특성을 사용하고 있고, 해당 특성은 비즈니스 변화시 수명을 같이 하거나, 변화되므로, 변경 즉시 보안이 적용되는 빠른 처리가 장점으로 인지되고 있습니다.

Windows Server 2003, "How to Migrate"

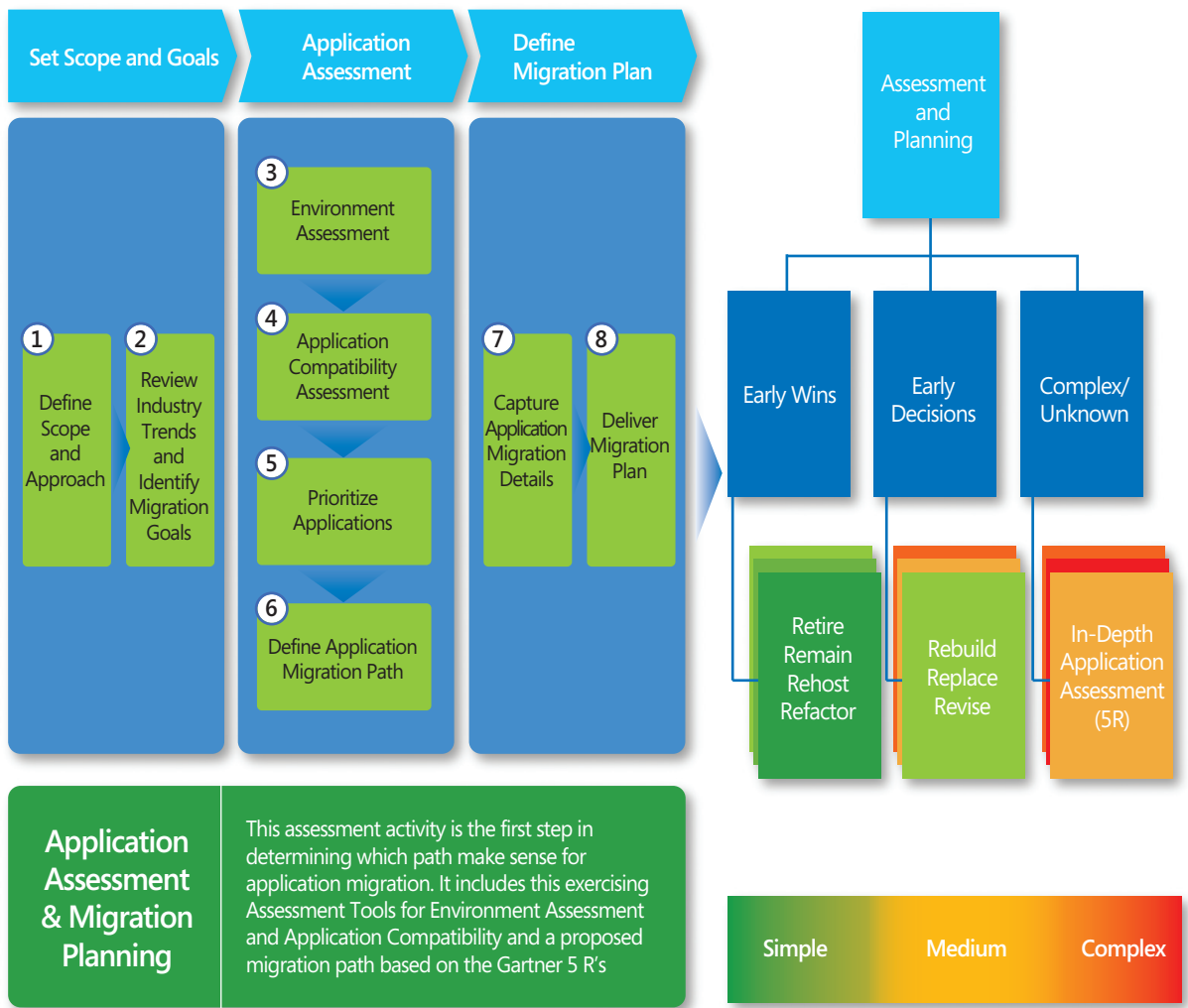
41 | Windows Server 2003 마이그레이션을 위한 마이크로소프트 권고안

부록 : Windows Server 2003 마이그레이션 Map

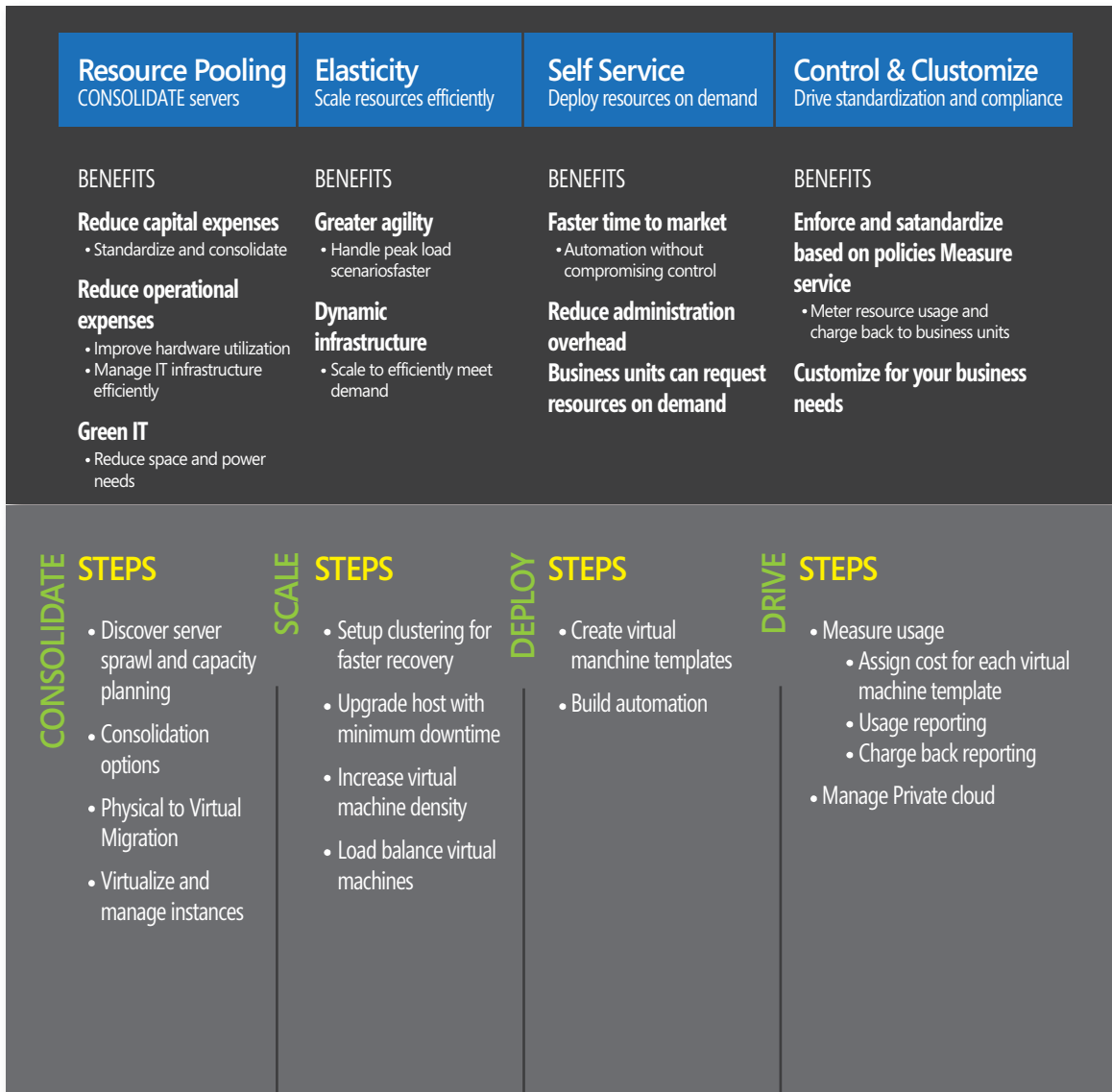


Windows Server 2003 마이그레이션을 위한 마이크로소프트 권고안

- OS의 마이그레이션은 그 자체로 끝나는 것이 아니라 해당 OS 에 설치/구성된 솔루션 또는 애플리케이션의 변경을 수반하게 됩니다. ▶성공적인 마이그레이션을 위하여 사전 진단 및 평가(Assessment)를 통해서 필요한 절차, 대상 및 계획을 수립하시기 바랍니다.
- Microsoft Services 팀이 보유한 Application Modernization 방법론 및 프로세스를 통해서 고객사에 도움을 제공할 수 있습니다.

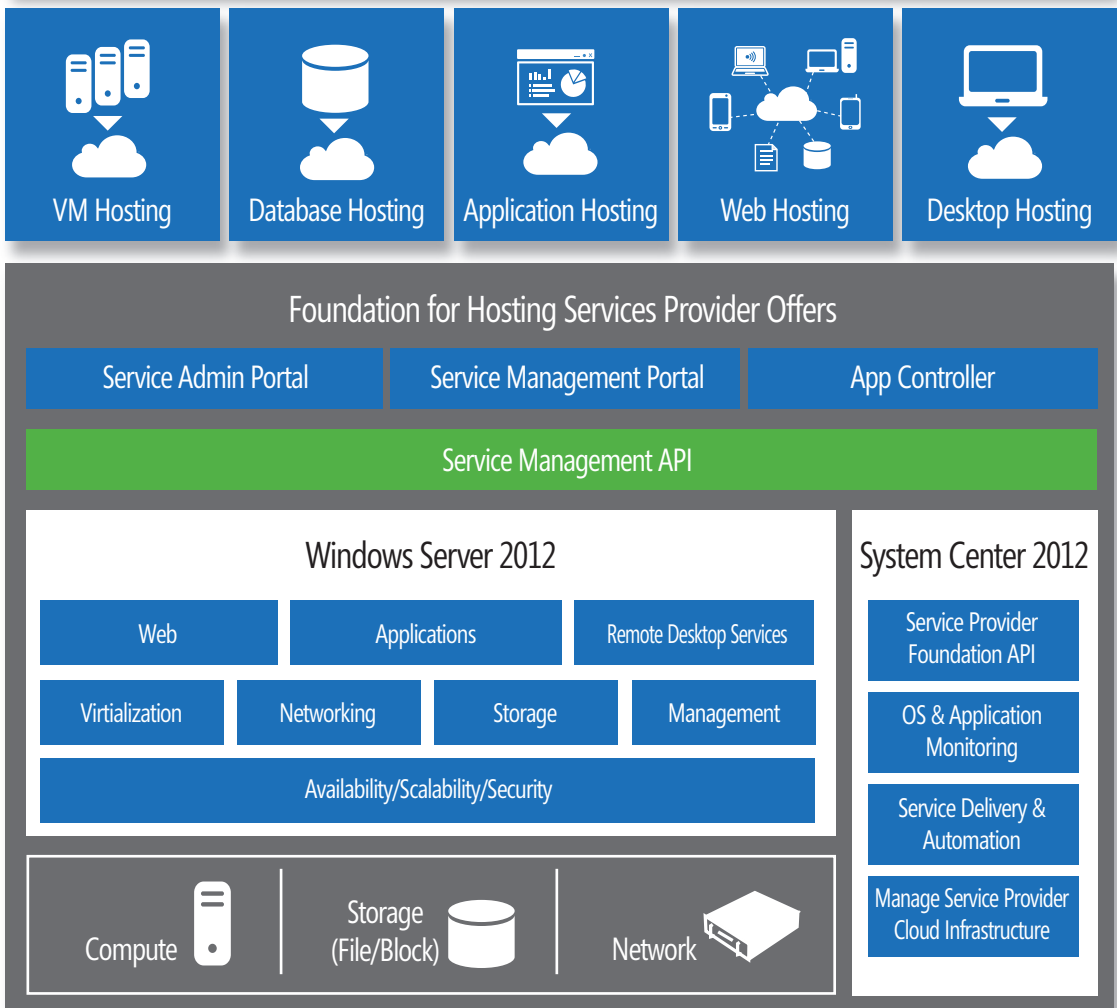


- Private Cloud 기술을 활용한 Server Consolidation 접근법을 고려하시기 바랍니다.
- 현재의 Hardware 는 Windows Server 2003을 운영하던 시대와 비교해서 성능 및 용량이 현저하게 증가하였습니다. ▶
1:1 마이그레이션은 서버 자원의 낭비를 초래할 수 있으므로 가상화 기술을 적극 활용하셔서 “Resource Flexibility, Operation Efficiency, Business Agility” 를 확보하시기 바랍니다.



- Microsoft Services 팀이 보유한 Datacenter Modernization 방법론 및 Hyper-V & System Center 솔루션을 통해서 고객 사에 도움을 제공할 수 있습니다.

Microsoft Hyper-V + System Center Capability





© 2014 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows 8 및 기타 제품명은 미국 및/또는 기타 국가에서 등록 상표 및/또는 상표입니다. 이 문서는 정보 제공 목적으로만 사용할 수 있으며 문서 발행 시점에 논의된 현안들에 대한 Microsoft Corporation의 당시 입장을 나타냅니다. Microsoft는 변화하는 시장 상황에 대응해야 하므로 본 문서 내의 정보를 Microsoft의 공약으로 해석할 수 없으며, Microsoft는 발행일 이후 제공된 어떠한 정보에 대해서도 정확성을 보증하지 않습니다. Microsoft는 이 프레젠테이션에서 일체의 명시적, 묵시적, 또는 법적인 보증도 하지 않습니다.

Microsoft