

Windows Server 2008 기술 개요

간행일: 2008년 1월

© 2008 Microsoft Corporation. All rights reserved. 이 문서는 제품의 제조 단계 이전에 작성되었으므로 이 문서에 포함된 모든 세부 내용이 고객에게 제공되는 제품에 포함된 내용과 정확하게 일치한다는 것을 보증할 수 없습니다. 이 문서에 포함된 정보는 문서 발행 시에 논의된 문제들에 대한 Microsoft Corporation의 당시 관점을 나타냅니다. Microsoft는 변화하는 시장 상황에 부응해야 하므로 이 문서를 Microsoft측의 공약으로 해석해서는 안 되며 발행일 이후 소개된 어떠한 정보에 대해서도 Microsoft는 그 정확성을 보증하지 않습니다. 이 문서의 내용은 문서 인쇄 시점의 제품 정보를 나타내며 계획 목적으로만 사용되어야 합니다. 이 문서의 내용은 예고 없이 언제든지 변경될 수 있습니다. 이 백서는 오직 정보를 제공하기 위한 것입니다. Microsoft는 이 요약에서 어떠한 명시적이거나 묵시적인 보증도 하지 않습니다.

Microsoft, Active Directory, PowerShell, SharePoint, SoftGrid, Windows, Windows Media, Windows 로고, Windows Vista 및 Windows Server는 미국 및/또는 기타 국가에서 Microsoft Corporation의 등록 상표 또는 상표입니다.

다른 모든 상표는 해당 소유자의 재산입니다.

목차

[1장: 소개 8](#_Toc193104698)

[개요 8](#_Toc193104699)

[웹과 응용 프로그램 8](#_Toc193104700)

[가상화 8](#_Toc193104701)

[보안과 규격 9](#_Toc193104702)

[비즈니스 작업의 견고한 토대 9](#_Toc193104703)

[2장: Hyper-V를 이용한 서버 가상화 10](#_Toc193104704)

[소개 10](#_Toc193104705)

[Hyper-V 아키텍처 11](#_Toc193104706)

[하이퍼바이저 기반 가상화 11](#_Toc193104707)

[Hyper-V 프로세서 지원 14](#_Toc193104708)

[새 하드웨어 공유 아키텍처 16](#_Toc193104709)

[저장소 기능 17](#_Toc193104710)

[강력한 네트워킹 18](#_Toc193104711)

[유연한 역할 기반 보안 19](#_Toc193104712)

[Server Core에서의 Hyper-V 20](#_Toc193104713)

[유연한 리소스 제어 21](#_Toc193104714)

[Hyper-V 고가용성 22](#_Toc193104715)

[관리 기능 24](#_Toc193104716)

[시나리오: 인프라, 응용 프로그램 및 원격 서버 작업 통합 26](#_Toc193104717)

[주요 통합 기능 27](#_Toc193104718)

[시나리오: 소프트웨어 테스트와 개발 환경의 자동화 및 통합 29](#_Toc193104719)

[시나리오: 비즈니스 연속성 및 재해 복구 30](#_Toc193104720)

[시나리오: 동적 데이터 센터 활용 32](#_Toc193104721)

[MSC 통합 32](#_Toc193104722)

[서버를 능가하는 가상화 33](#_Toc193104723)

[요약 34](#_Toc193104724)

[3장: TS RemoteApp 기반 프레젠테이션 가상화 35](#_Toc193104725)

[소개 35](#_Toc193104726)

[터미널 서비스 RemoteApp 35](#_Toc193104727)

[터미널 서비스 36](#_Toc193104728)

[원격 데스크톱 연결 6.0 이상 36](#_Toc193104729)

[플러그 앤 플레이 장치 리디렉션 38](#_Toc193104730)

[Windows Embedded for Point of Service 장치 리디렉션 39](#_Toc193104731)

[SSO(Single Sign-On) 40](#_Toc193104732)

[TS 세션 브로커 40](#_Toc193104733)

[인쇄 기능 향상 40](#_Toc193104734)

[TS Easy Print 41](#_Toc193104735)

[라이선싱 개선 사항 41](#_Toc193104736)

[터미널 서비스 게이트웨이(TS 게이트웨이) 43](#_Toc193104737)

[TS 게이트웨이 관리 44](#_Toc193104738)

[TS 게이트웨이 기능 44](#_Toc193104739)

[터미널 서비스 웹 액세스 46](#_Toc193104740)

[향상된 웹 환경 47](#_Toc193104741)

[TS 원격 프로그램 목록의 동적 업데이트 47](#_Toc193104742)

[터미널 서비스 원격 프로그램 웹 파트 48](#_Toc193104743)

[요약 48](#_Toc193104744)

[4장: 원격 위치 48](#_Toc193104745)

[소개 48](#_Toc193104746)

[배포 및 관리 49](#_Toc193104747)

[Active Directory의 관리 효율성 향상 50](#_Toc193104748)

[RODC(읽기 전용 도메인 컨트롤러) 50](#_Toc193104749)

[읽기 전용 DNS(Domain Name System) 53](#_Toc193104750)

[Hyper-V의 서버 가상화 53](#_Toc193104751)

[원격 관리 및 보안 기능 향상 54](#_Toc193104752)

[Server Core 소개 54](#_Toc193104753)

[BitLocker 드라이브 암호화 54](#_Toc193104754)

[엔터프라이즈급 프린터 관리 55](#_Toc193104755)

[Windows PowerShell 55](#_Toc193104756)

[Windows 원격 관리 55](#_Toc193104757)

[WAN 효율성 개선 55](#_Toc193104758)

[TCP/IP 스택 56](#_Toc193104759)

[IPv6(Internet Protocol 버전 6) 지원 59](#_Toc193104760)

[서비스 품질 59](#_Toc193104761)

[SYSVOL 및 SDFR(분산 파일 시스템 복제) 60](#_Toc193104762)

[서버 메시지 블록 2.0 61](#_Toc193104763)

[요약 63](#_Toc193104764)

[5장: 보안 및 규정 준수 64](#_Toc193104765)

[소개 64](#_Toc193104766)

[고급 보안이 설정된 Windows 방화벽 65](#_Toc193104767)

[BitLocker 드라이브 암호화 67](#_Toc193104768)

[Active Directory 도메인 서비스: 감사 67](#_Toc193104769)

[AD DS 액세스 감사 67](#_Toc193104770)

[AD DS 변경 감사 68](#_Toc193104771)

[글로벌 감사 정책 69](#_Toc193104772)

[서비스 기반 AD DS 70](#_Toc193104773)

[RODC(읽기 전용 도메인 컨트롤러) 70](#_Toc193104774)

[서버 및 도메인 격리 70](#_Toc193104775)

[엔터프라이즈 PKI 71](#_Toc193104776)

[PKIView를 통한 엔터프라이즈 CA 관리 71](#_Toc193104777)

[인증서 서비스 72](#_Toc193104778)

[인증서 웹 등록 73](#_Toc193104779)

[네트워크 장치 등록 74](#_Toc193104780)

[그룹 정책으로 인증서 관리 74](#_Toc193104781)

[인증서 관련 그룹 정책 설정 75](#_Toc193104782)

[피어 트러스트 및 신뢰할 수 있는 루트 CA 저장소 관리 76](#_Toc193104783)

[신뢰할 수 있는 게시자 관리 및 원치 않는 인증서 차단 76](#_Toc193104784)

[인증서 배포 변경 77](#_Toc193104785)

[온라인 인증서 상태 프로토콜 지원 77](#_Toc193104786)

[OCSP에서 제공하는 기능 78](#_Toc193104787)

[OSCP에 대한 그룹 정책 설정 79](#_Toc193104788)

[V3 인증서 템플릿 79](#_Toc193104789)

[CNG(Cryptography Next Generation) 80](#_Toc193104790)

[Windows Server 2008의 ID 및 액세스 관리 81](#_Toc193104791)

[Active Directory Rights Management Services 82](#_Toc193104792)

[Active Directory Federation Services 83](#_Toc193104793)

[지속적인 정보 보호 84](#_Toc193104794)

[시나리오: 안전하고 쉬운 공동 작업 85](#_Toc193104795)

[페더레이션 권한 관리 요약 85](#_Toc193104796)

[기타 보안 향상 85](#_Toc193104797)

[코드 무결성 85](#_Toc193104798)

[Windows 서비스 강화 86](#_Toc193104799)

[Windows Server Core 86](#_Toc193104800)

[이동식 장치 설치 86](#_Toc193104801)

[NAP(네트워크 액세스 보호) 87](#_Toc193104802)

[네트워크 액세스 보호 소개 87](#_Toc193104803)

[NAP 아키텍처 88](#_Toc193104804)

[NAP 구성 요소 88](#_Toc193104805)

[클라이언트 컴퓨터 상태 91](#_Toc193104806)

[NAP 관리 서버 91](#_Toc193104807)

[NPS(네트워크 정책 서버) 92](#_Toc193104808)

[예: NAP 적용 작동 방식 92](#_Toc193104809)

[NAP 적용 방법 94](#_Toc193104810)

[요약 96](#_Toc193104811)

[6장: 웹 및 응용 프로그램 96](#_Toc193104812)

[소개 96](#_Toc193104813)

[IIS(인터넷 정보 서비스) 7.0 97](#_Toc193104814)

[모듈 방식의 디자인 97](#_Toc193104815)

[확장성 증가 97](#_Toc193104816)

[분산 구성 98](#_Toc193104817)

[관리 도구 99](#_Toc193104818)

[새 IIS 관리자 100](#_Toc193104819)

[진단 및 문제 해결 101](#_Toc193104820)

[WAS(Windows Process Activation Service) 103](#_Toc193104821)

[WSRM(Windows 시스템 리소스 관리자) 104](#_Toc193104822)

[이벤트 인프라 104](#_Toc193104823)

[Windows Server 2008 및 Windows Vista의 이벤트 104](#_Toc193104824)

[이벤트를 보는 새로운 방법 105](#_Toc193104825)

[XML 구조 105](#_Toc193104826)

[이벤트 구독 106](#_Toc193104827)

[다시 시작 관리자 106](#_Toc193104828)

[Microsoft .NET Framework 3.0 107](#_Toc193104829)

[WCF(Windows Communication Foundation) 108](#_Toc193104830)

[WPF(Windows Presentation Foundation) 108](#_Toc193104831)

[Windows WF(Workflow Foundation) 109](#_Toc193104832)

[Windows CardSpace 109](#_Toc193104833)

[Service Trace Viewer Tool(SvcTraceViewer.exe) 109](#_Toc193104834)

[PHP 지원 109](#_Toc193104835)

[인증서 서비스 110](#_Toc193104836)

[Windows Media Services 110](#_Toc193104837)

[요약 111](#_Toc193104838)

[7장: 서버 관리 111](#_Toc193104839)

[소개 111](#_Toc193104840)

[초기 구성 작업 112](#_Toc193104841)

[서버 관리자 콘솔 115](#_Toc193104842)

[서버에 설치되어 있는 역할, 역할 서비스 및 기능 관리 115](#_Toc193104843)

[서버 역할과 역할 서비스란 무엇인가? 115](#_Toc193104844)

[기능이란 무엇인가? 116](#_Toc193104845)

[서버 관리자 마법사 119](#_Toc193104846)

[서버 관리자 명령줄 도구 121](#_Toc193104847)

[Windows PowerShell 122](#_Toc193104848)

[일관성 및 사용의 용이성 122](#_Toc193104849)

[대화형 및 스크립팅 환경 122](#_Toc193104850)

[개체 지향 및 .NET Framework 123](#_Toc193104851)

[그룹 정책 기본 설정 123](#_Toc193104852)

[기본 설정과 정책 설정 124](#_Toc193104853)

[그룹 정책 기본 설정 항목 126](#_Toc193104854)

[그룹 정책 기본 설정 기능 129](#_Toc193104855)

[대상 제어 130](#_Toc193104856)

[그룹 정책 기본 설정 배포 130](#_Toc193104857)

[그룹 정책 기본 설정의 이점 131](#_Toc193104858)

[Windows 원격 관리(WS-Management) 132](#_Toc193104859)

[Windows 원격 셸 133](#_Toc193104860)

[Server Core 133](#_Toc193104861)

[비 응용 프로그램 플랫폼 134](#_Toc193104862)

[엔터프라이즈급 인쇄 관리 135](#_Toc193104863)

[프린터 관리 135](#_Toc193104864)

[Active Directory에서 프린터 나열 및 제거 136](#_Toc193104865)

[그룹 정책을 사용한 프린터 배포 136](#_Toc193104866)

[프린터 문제 해결 136](#_Toc193104867)

[주요 이점 137](#_Toc193104868)

[Windows 배포 서비스 137](#_Toc193104869)

[Windows 배포 서비스의 향상된 기능 137](#_Toc193104870)

[새 Active Directory 도메인 서비스 설치 마법사 138](#_Toc193104871)

[다시 시작 가능 AD DS(Active Directory 도메인 서비스) 139](#_Toc193104872)

[Active Directory 도메인 서비스 스냅숏 뷰어 141](#_Toc193104873)

[요약 142](#_Toc193104874)

[8장: 고가용성 142](#_Toc193104875)

[소개 142](#_Toc193104876)

[장애 조치 클러스터링 143](#_Toc193104877)

[장애 조치 클러스터링의 새 기능 144](#_Toc193104878)

[대용량을 위한 향상된 확장성 144](#_Toc193104879)

[장애 조치 클러스터의 향상된 기능 144](#_Toc193104880)

[향상된 안정성 145](#_Toc193104881)

[저장소 통합 146](#_Toc193104882)

[네트워킹 및 보안 147](#_Toc193104883)

[클러스터링과 Hyper-V 148](#_Toc193104884)

[네트워크 부하 분산 149](#_Toc193104885)

[Windows 백업 150](#_Toc193104886)

[새 백업 기능 150](#_Toc193104887)

[Windows 안정성 및 성능 모니터 151](#_Toc193104888)

[새 모니터링 기능 151](#_Toc193104889)

[정책 기반 서비스 품질 153](#_Toc193104890)

[요약 153](#_Toc193104891)

[9장: 요약 154](#_Toc193104892)

# 1장: 소개

## 개요

웹 및 가상화 기술이 적용된 Microsoft® Windows Server® 2008은 조직의 서버 인프라에 향상된 신뢰성과 유연성을 제공하도록 설계되었습니다. 새로운 가상화 도구, 웹 기술 그리고 향상된 보안 기능이 시간을 절약하고 비용을 절감해 주며 동적 데이터 센터를 위한 플랫폼을 제공합니다. IIS 7.0(Internet Information Server 7.0), Windows Server Manager, Windows Server PowerShell 등의 강력한 새 도구들을 이용하여 서버 제어 기능을 향상시키고 웹, 구성 및 관리 작업을 간소화할 수 있습니다. NAP(네트워크 액세스 보호)나 RODC(읽기 전용 도메인 컨트롤러)와 같이 향상된 고급 보안 및 신뢰성 기능은 운영 체제를 강화하고 서버 환경을 보호함으로써 강력한 비즈니스 토대의 구축을 지원합니다.

## 웹과 응용 프로그램

Windows Server 2008은 조직이 사용자에게 풍부한 웹 기반 환경을 효율적이고 효과적으로 제공하기 위해 이용할 수 있는 강력한 웹 응용 프로그램 및 서비스 플랫폼입니다.

Windows Server 2008의 구성 요소인 IIS 7.0(Internet Information Server 7.0)에서는 관리 및 진단 기능이 향상되고 개발 및 응용 프로그램 도구가 개선되었으며 인프라 비용도 낮아졌습니다. 또한 응용 프로그램 호스팅 범위가 확장된 완벽한 모듈식 확장형 웹 서버로써, 고객의 중요한 과제를 해결하는 데 탁월한 호환성을 제공합니다.

Microsoft Windows Media® Services는 인터넷 또는 인트라넷에서 라이브 또는 주문형 오디오와 비디오 콘텐츠를 스트리밍할 수 있는 강력한 플랫폼입니다. 이는 관리 편의성, 사용자 지정 및 확장성을 제공하는 플랫폼에서 개인 설정된 신속한 콘텐츠 전달을 위해 가장 빠른 스트리밍 성능과 동적 프로그래밍 기능을 제공합니다.

## 가상화

서버 가상화 기술이 구현된 Windows Server 2008을 통해 조직은 비용을 절감하고 하드웨어 사용률을 높이며 인프라를 최적화하고 서버 가용성을 개선할 수 있습니다. Windows Server Hyper-V™를 탑재한 서버 가상화는 64비트 하이퍼바이저 기반 플랫폼을 이용하여 신뢰성과 확장성을 높였습니다. Hyper-V는 서버 통합으로 하드웨어 리소스를 최적화하는 데 유용합니다. 또한 장애 조치 클러스터링과 같은 Windows Server 2008 플랫폼의 구성 요소를 이용하여 규정을 위반한 가상 컴퓨터를 격리할 수 있는 고가용성 및 NAP(네트워크 액세스 보호)를 제공합니다.

또 다른 가상화 형식인 프레젠테이션 가상화는 응용 프로그램 프레젠테이션 계층 또는 사용자 인터페이스를 호스트 운영 체제로부터 분리하는 기능입니다. Windows Server 2008의 Terminal Services 게이트웨이 및 Terminal Services RemoteApp에서는 클라이언트 컴퓨터의 원격 응용 프로그램 통합을 이용한 중앙 집중식 응용 프로그램 액세스가 가능하며 웹 브라우저에서 동일한 원격 프로그램들을 간편하게 액세스할 수 있습니다. 또한 터미널 서비스는 방화벽을 거쳐 원격 터미널과 응용 프로그램에 액세스할 수 있는 방법을 제공합니다. 자세한 내용은 3장: Terminal Services RemoteApp를 이용한 프레젠테이션 가상화를 참조하십시오.

## 보안과 규격

Windows Server 2008은 가장 안전한 Windows 서버 제품입니다. 강화된 운영 체제를 비롯하여 네트워크 액세스 보호, 통합 권한 관리, 읽기 전용 도메인 컨트롤러 등의 보안 혁신을 통해 뛰어난 수준의 조직 데이터 보호 기능을 제공합니다. Windows Server 2008에는 보안 및 규정 준수 기능 향상, 보다 고급화된 암호화 기능 그리고 감사 및 시작 단계 보안을 강화하는 도구들이 들어 있습니다. 조직은 권한 관리 서비스 및 BitLocker™를 통해 데이터 도난을 방지할 수 있습니다.

Windows 서비스 강화 기능을 사용하면 중요한 서버 서비스가 파일 시스템, 레지스트리 또는 네트워크에 대한 비정상적 조작으로 인해 훼손되지 못하도록 함으로써 시스템을 더욱 안전하게 유지할 수 있습니다. Windows Server 2008 운영 체제에서는 NAP(네트워크 액세스 보호), RODC(읽기 전용 도메인 컨트롤러), PKI(공개 키 인프라) 기능 향상, 향상된 필터링 기능이 포함된 새 Windows 방화벽, 차세대 암호화 지원 등을 통해 보안 성능도 향상되었습니다.

더 나아가 완벽하게 통합된 통합 권한 관리 서비스 솔루션을 제공합니다. 따라서 조직은 권한 관리 프레임워크를 간편하게 확장함으로써 조직 외부의 사용자들을 위한 추가 사용자 계정 유지 관리 비용을 들이지 않고 파트너들이 중요한 정보를 안전하게 공유하도록 할 수 있습니다.

## 비즈니스 작업의 견고한 토대

Windows Server 2008은 현재까지 출시된 Windows Server 운영 체제 가운데 가장 유연하고 강력한 버전입니다. Server Core, PowerShell, Windows 배포 서비스, 향상된 네트워킹 및 클러스터링 기술 등의 새로운 기술과 기능이 통합된 Windows Server 2008은 모든 작업 및 응용 프로그램 요구 사항에 가장 적합하고 믿을 수 있는 Windows 플랫폼을 제공합니다.

서버 관리자는 서버 역할과 기능 추가, 제거 및 구성을 단일 MMC(Microsoft Management Console)에 통합합니다. WDS(Windows 배포 서비스)는 Windows Server 2008에서 협력 작업을 통해 간소화되고 안전하며 신속한 Windows 운영 체제를 클라이언트와 서버에 배포하는 구성 요소 제품군입니다. WDS는 네트워크 기반 설치를 이용하므로 관리자가 각 컴퓨터에서 직접 작업하거나 CD 또는 DVD와 같은 이동식 미디어에서 Windows 구성 요소를 설치할 필요가 없습니다. IT 전문가는 Windows PowerShell 명령줄 셸 및 스크립팅 언어를 이용하여 자주 수행하는 작업을 자동화하고 시스템 관리를 더욱 원활하게 제어하며 지사 사무실과 같은 원격 위치에서도 자동화를 가속화할 수 있습니다. PowerShell은 기존 스크립팅 솔루션과의 호환성을 유지함으로써 기존의 투자를 보호합니다.

Server Core는 선택한 역할에 필요한 하위 시스템만을 포함하는 새로운 설치 옵션으로, 패치와 서비스의 필요성을 줄인 보다 믿을 수 있고 안전한 서버를 생성할 수 있습니다.

Windows Server 2008에는 차세대 TCP/IP 스택이라고 알려진 TCP/IP 프로토콜 스택이 새롭게 구현되어 있습니다. 차세대 TCP/IP 스택은 TCP/IP 스택의 완벽한 재설계를 통해 오늘날과 같이 다양한 네트워킹 환경과 기술의 연결성 및 성능 요구를 충족합니다.

장애 조치 클러스터(이전의 서버 클러스터)는 함께 작동하여 응용 프로그램과 서비스의 가용성을 향상시키는 독립 컴퓨터의 그룹입니다. Windows Server 2008에서는 장애 조치 클러스터의 성능 향상으로 클러스터를 간소화하여 보안성과 안정성을 더 간편하게 높일 수 있습니다.

# 2장: Hyper-V를 이용한 서버 가상화

## 소개

오늘날의 데이터 센터는 다양한 서버, 운영 체제 및 응용 프로그램이 수많은 데스크톱 및 모바일 클라이언트와 상호 작용하는 복잡한 환경입니다. IT 부서는 이와 같이 다양하고 업무상 중요한 기술들을 관리 및 지원하는 동시에 비용을 절감하고 신뢰성과 보안성을 유지해야 한다는 압력을 점점 더 많이 받고 있습니다. 서버 가상화 기술 배포를 통해 중앙 집중식 관리 환경에서 분산된 서버들을 가상 컴퓨터(VM)로 이전하는 것은 이러한 과제를 해결하기 위해 많이 사용되고 있는 옵션입니다.

가상화는 IT 비용을 절감하고 네트워크 관리를 중앙에 집중시키며 네트워크 보안성을 높이고 서버 가용성을 개선하고 하드웨어 사용률을 높이는 데 도움이 됩니다.

Windows Server 2008에는 타사 소프트웨어를 구입하지 않고도 가상화의 이점을 충분히 활용할 수 있는 강력한 가상화 및 네트워크 관리 도구인 Hyper-V가 포함됩니다. 가상 컴퓨터는 사용 가능한 하드웨어를 활용할 수 있는 뛰어난 성능을 제공하고, Microsoft와 그 파트너들은 다양한 운영 체제(Windows, Linux, Xen 기반 Linux 등)를 이용하는 데 따른 상호 운용성 문제를 한 번에 해결할 수 있도록 지원하며, IT 부서들은 유연하고 강력한 도구를 사용하여 가상 리소스와 실제 리소스를 둘 다 관리할 수 있습니다.

이 장에서는 Microsoft 데스크톱과 데이터 센터 간 가상화 전략의 주요 구성 요소인 Hyper-V에 대해 소개합니다. Hyper-V의 새로운 기능과 향상된 기능이 서버 통합, 비즈니스 연속성/재해 복구 관리, 테스트와 개발, 동적 데이터 센터 등의 일반적인 시나리오에서 엔터프라이즈 고객의 고충을 어떻게 해소하는지 설명합니다. 또한 이러한 장점을 활용하여 소규모 지사 사무실의 고유한 요구를 만족시키는 방법에 대해서도 설명합니다.

가상화는 널리 채택되고 있는 솔루션입니다. 조직의 80퍼센트가 가상화를 이용하거나 평가하고 있으며 서버 통합, 중앙 집중식 관리 및 기타 비용 절감을 위해 가상화의 장점을 검토하고 있습니다. 이러한 이점이 비용을 절감해 주므로 기업은 상당한 작업을 가상화하고, 그들의 관리 도구와 보다 잘 통합되는 더욱 강력하고 유연한 가상화 솔루션을 원합니다. 64비트 방식의 멀티 프로세서 멀티 코어 서버가 광범위하게 채택되고 있어 더욱 강력해진 처리 성능을 보다 잘 활용할 수 있는 가상 컴퓨터에 대한 요구가 커지고 있습니다.

이러한 요구를 만족시키기 위해 Microsoft는 차세대 64비트 가상화 기술인 Hyper-V를 개발하여 실제 구성 요소와 가상 구성 요소 모두를 완벽하게 관리하고 속도를 향상시킬 수 있게 되었습니다. 이 기술은 믿을 수 있는 동적 가상화 기능을 통해 유연성을 발휘하는 플랫폼을 제공합니다.

## Hyper-V 아키텍처

### 하이퍼바이저 기반 가상화

Hyper-V는 64비트 하이퍼바이저를 사용하여 설계되었습니다. 하이퍼바이저는 운영 체제와 하드웨어 사이에 있는 일종의 소프트웨어입니다. 하이퍼바이저를 통해 복수의 가상 컴퓨터(VM)는 충돌 없이 실제 메모리와 CPU 리소스에 액세스합니다. Hyper-V 하이퍼바이저는 Intel VT 및 AMD “Pacifica” 기술 탑재 프로세서를 포함한 가상화 인식 하드웨어와 결합하여 게스트 운영 체제에 뛰어난 성능 및 무제한에 가까운 확장성을 제공합니다.

#### 하드웨어 가상화

Hyper-V 하이퍼바이저는 Intel VT 및 AMD “Pacifica” 기술이 적용되었으므로 복수의 운영 체제를 가상화하는 작업 중 상당 부분을 시스템 하드웨어에서 수행하기 때문에 가상화 스택 및 하이퍼바이저가 수행할 부분이 줄어듭니다.

하드웨어의 소프트웨어 에뮬레이션 기반 가상화 플랫폼은 하드웨어 요청을 가상화 환경과 호환되는 형식으로 즉석에서 변환하기 때문에 게스트 운영 체제가 자주 중단되는 문제가 있습니다. Intel VT 및 AMD “Pacifica” 하드웨어 기술은 가상화 확장을 x86 아키텍처에 통합하므로 이와 같은 즉석 변환이 거의 필요 없습니다. 이로 인해 VT 및 “Pacifica”용으로 설계된 가상화 플랫폼의 비용 부담을 줄여 가상 컴퓨터의 효율성을 높일 수 있습니다. 하드웨어 가상화 기능과 Hyper-V의 소프트웨어 가상화 구성 요소 간의 이러한 공동 작업으로 탁월한 성능의 가상화 플랫폼이 탄생됩니다.

#### 64비트 아키텍처

Hyper-V 하이퍼바이저는 64비트 설계입니다. Hyper-V는 Windows Server 2008 64비트 버전에서 실행해야 하며 가상 컴퓨터에 무제한에 가까운 확장성을 제공합니다. Hyper-V의 64비트 아키텍처는 32비트 아키텍처를 기반으로 한 가상화 플랫폼보다 훨씬 큰 메모리 용량을 처리할 수 있으므로 Hyper-V 호스트 서버는 최대 1TB의 실제 RAM을 수용할 수 있습니다.

Hyper-V를 기반으로 호스팅되는 가상 컴퓨터에는 각각 최대 64GB RAM을 할당할 수 있습니다. 이 장의 뒷부분에서 설명하게 될 Hyper-V의 동적 하드웨어 할당을 통해 가상 컴퓨터별로 필요한 리소스 요구에 따라 서로 다른 용량의 RAM을 최대 64GB까지 할당할 수 있습니다. 따라서 더 많은 작업을 가상화할 수 있으므로 조직은 복수의 게스트 운영 체제 및 VM을 호스팅하는 기능을 최대한 활용할 수 있습니다. 리소스 할당이 이처럼 유연하기 때문에 복수의 게스트 운영 체제를 단일 Hyper-V 호스트에 통합하면서도 각 운영 체제의 효율성은 거의 저하되지 않게 할 수 있습니다.

#### 64비트 게스트 운영 체제 지원

Hyper-V에 사용되는 64비트 하이퍼바이저는 32비트와 64비트 게스트 운영 체제를 둘 다 지원합니다. 32비트 버전과 64비트 버전 중 하나에서만 사용할 수 있는 응용 프로그램도 있습니다. 예를 들어, LOB 응용 프로그램은 32비트 버전에서만 사용할 수 있으며, Microsoft Exchange Server 2007은 64비트 응용 프로그램으로만 사용 가능합니다. 32비트와 64비트 가상 컴퓨터를 동일한 Hyper-V 서버에서 함께 실행할 수 있습니다. 32비트와 64비트 가상 컴퓨터를 모두 수용할 수 있는 유연성은 Hyper-V 하이퍼바이저의 주요 이점입니다. 64비트 하이퍼바이저는 조직이 원하는 향후의 모든 확장 경로를 지원하는 가상화 토대를 제공합니다.

#### 운영 체제 분할

Hyper-V는 파티션을 이용하는 복수의 VM에 호스트 시스템 하드웨어 리소스를 할당합니다. 파티션이란 단일 운영 체제 기반의 호스트 서버를 논리적으로 분리한 것입니다. 상위 파티션에는 하위 파티션의 메모리와 가상 장치를 관리하는 가상화 스택이 포함됩니다. 하위 파티션을 가상 컴퓨터라고 합니다. Hyper-V를 탑재하면 상위 파티션을 하나만 구성할 수 있다는 제약이 있으며(Windows Server 2008 x64의 인스턴스 또는 Windows Server 2008 x64의 Server Core 설치), 하위 파티션은 무제한으로 구성할 수 있습니다.

상위 파티션은 Hyper-V 호스트 서버에 연결된 키보드, 마우스 및 비디오 디스플레이에 대한 소유권을 가집니다. 또한 가상화 환경의 전반적인 관리를 원활하게 하는 WMI(Windows Management Instrumentation) 공급자를 포함합니다. 호스트 시스템 하드웨어에 필요한 IHV(독립 하드웨어 공급업체) 드라이버도 상위 파티션에 포함됩니다. 하위 파티션은 가상 컴퓨터와 연결된 운영 체제, 응용 프로그램 및 데이터 파일의 논리적 컨테이너가 됩니다. 하위 파티션은 호스트 서버 하드웨어에 제한적으로 액세스할 수 있으며, 이 하드웨어에 액세스하려면 이 장의 뒷부분에서 설명할 VMBus라는 하드웨어 공유 모델을 경유해야 합니다.

#### 마이크로커널화된 하이퍼바이저 아키텍처

Hyper-V 하이퍼바이저는 마이크로커널 운영 체제와 동일한 설계 원칙을 구현합니다. 운영 체제 드라이버를 비롯하여 공격에 노출된 기타 구성 요소가 권한이 낮은 수준에서 실행된다는 것은 구성 요소의 오작동 또는 공격이 커널 손상을 거의 또는 전혀 일으키지 않음을 의미합니다. Hyper-V 하이퍼바이저는 유사한 설계 방식을 채택하여 어떠한 자체 드라이버도 통합하지 않는 최소한의 TCB(Trusted Computing Base) 권한을 취득합니다(드라이버는 상위 및 하위 파티션에 들어 있음). 하드웨어 드라이버를 하이퍼바이저 코드 베이스에 통합하는 모놀리식 하이퍼바이저 기반의 가상화 플랫폼과 비교할 때, 이와 같이 마이크로커널화된 하이퍼바이저 아키텍처는 가상 컴퓨터를 더욱 안정적이고 안전하게 실행할 수 있는 토대를 제공합니다. 아래 그림은 Windows Server 가상화 아키텍처를 묘사한 것입니다.

##### 

그림 1: Hyper-V 아키텍처

### Hyper-V 프로세서 지원

현대의 서버 하드웨어는 다양한 프로세서 구성 옵션을 제공합니다. 서버 마더보드의 여러 소켓에 복수의 코어를 가진 프로세서를 장착할 수 있습니다. Hyper-V 프로세서 성능은 사용 가능한 프로세서 코어의 수와 속도에 따라 확장 가능합니다. 예를 들어, 듀얼 코어 프로세서를 2개의 소켓에 장착하면 Hyper-V에는 4개의 프로세서 코어가 생기는 것입니다.

Hyper-V가 사용할 수 있는 프로세서 소켓의 수는 설치된 Windows Server 2008 버전에 따라 다릅니다. 아래 표는 프로세서 지원 예입니다.

표 1: 프로세서 구성 및 운영 체제 버전별 프로세서 지원 예

|  |  |  |
| --- | --- | --- |
| **프로세서 구성** | **상위 파티션 운영 체제** | **결과** |
| 소켓 2개에 듀얼 코어 프로세서 장착 | Windows Server 2008 Standard x64 | * 상위 파티션은 프로세서 코어 4개를 사용합니다. * 각 하위 파티션에는 최대 4개의 논리 프로세서가 지정될 수 있습니다. |
| 소켓 8개에 듀얼 코어 프로세서 장착 | Windows Server 2008 Standard x64 | * 상위 파티션은 프로세서 코어 16개를 사용합니다. * 각 하위 파티션에는 최대 4개의 논리 프로세서가 지정될 수 있습니다. |
| 소켓 2개에 쿼드 코어 프로세서 장착 | Windows Server 2008 Enterprise x64 | * 상위 파티션은 프로세서 코어 8개를 사용합니다. * 각 하위 파티션에는 최대 4개의 논리 프로세서가 지정될 수 있습니다. |
| 소켓 16개에 듀얼 코어 프로세서 장착 | Windows Server 2008 Enterprise x64 | * 상위 파티션은 프로세서 코어 8개를 사용합니다. * 각 하위 파티션에는 최대 4개의 논리 프로세서가 지정될 수 있습니다. |

참고:

1. Windows Server 2008 Standard Edition x64는 최대 4개의 프로세서 소켓을 지원합니다.
2. Windows Server 2008 Enterprise Edition x64는 최대 8개의 프로세서 소켓을 지원합니다.
3. Windows Server 2008 Datacenter Edition x64는 Hyper-V와 결합하여 최대 16개의 프로세서 소켓을 지원합니다.

Hyper-V는 프로세서 코어를 가상 컴퓨터에 논리적 프로세서로 제공합니다. 소켓 4개에 쿼드 코어 프로세서를 장착한 서버는 16개의 프로세서 코어를 갖게 되는 것입니다. 이 16개 프로세서 코어는 가상 컴퓨터에 논리 프로세서로 나타날 수 있습니다. 각 가상 컴퓨터에 최대 4개의 논리 프로세서를 구성할 수 있습니다. 각 논리 프로세서는 그 논리 프로세서에 대한 가상 컴퓨터의 컴퓨팅 부하를 호스트 서버의 실제 프로세서에서 실행되는 스레드로 변환합니다.

위의 표는 여러 가지 구성 옵션과 각 구성에서 해당 결과에 따른 프로세서 지정 옵션을 나타낸 것입니다. 하위 파티션에 설치된 운영 체제는 그 운영 체제가 사용할 수 있는 논리 프로세서의 수를 결정합니다.

### 새 하드웨어 공유 아키텍처

#### VMBus

Hyper-V는 VMBus라는 파티션 간의 통신 채널을 기반으로 한 새 하드웨어 공유 아키텍처를 통합합니다. VMBus는 메모리 버스 및 파티션 사이의 고속 지점 간 통신 메커니즘으로써, 호스트와 VM이 서로 통신하는 데 사용됩니다. 앞에서 설명한 것처럼, 하이퍼바이저는 호스트 시스템과 VM 사이의 상호 작용뿐 아니라 호스트 서버의 메모리와 프로세서 간 상호 작용을 관리합니다. 디스크, 네트워킹, 입력/출력 및 비디오 하드웨어 상호 작용은 VMBus에 의해 관리됩니다.

#### VSP(가상화 서비스 공급자)

VSP(가상화 서비스 공급자)는 상위 파티션에 위치하고, 하위 파티션에 있는 VM을 대신하여 호스트 서버 하드웨어와 상호 작용합니다. VSP는 멀티플렉서 역할을 수행하므로 복수의 하위 파티션이 하드웨어를 공유할 수 있습니다. 예를 들어, 가상 컴퓨터가 10대이고 실제 네트워크 어댑터는 1개뿐인 Hyper-V 호스트에서 상위 파티션의 VSP는 이 모든 가상 컴퓨터가 동일한 NIC를 성공적으로 안전하게 공유할 수 있도록 합니다. Hyper-V에는 스토리지, 네트워킹, 입력 및 비디오를 위한 VSP가 있습니다.

#### VSC(가상화 서비스 클라이언트)

VSC(가상화 서비스 클라이언트)는 VMBus를 통해 상위 파티션의 VSP에 정보를 전달함으로써 호스트 서버 하드웨어에 간접적으로 액세스하는 게스트 운영 체제의 드라이버입니다. VSC는 고유 가상 장치(에뮬레이트된 장치가 아니라는 의미로, 뒤에서 자세히 설명)이며 VMBus를 통해 상위 파티션의 해당 VSP(저장소, 네트워킹, 입력 또는 비디오)와 통신합니다. 상위 파티션에서 실행되는 VSP 집합은 하나입니다. 하위 파티션은 자체 VSC 집합을 실행하며, 각각 상위 파티션의 해당 VSP와 통신합니다.

Hyper-V에는 Microsoft Virtual Server 2005에 사용되는 VM 추가 기능을 대신하는 통합 구성 요소가 포함되어 있습니다. Microsoft Virtual Server 2005의 VM 추가 기능은 가상화 인식 소프트웨어 구성 요소 패치를 게스트 운영 체제에 적용함으로써 게스트 운영 체제의 성능을 향상시키고 Microsoft Virtual Server 관리 인터페이스로부터 게스트 완전 차단과 같은 기능을 지원하는 통합 구성 요소를 제공하는 데 사용되었습니다. 하드웨어 지원 가상화가 있으면 게스트 운영 체제 패치는 더 이상 필요 없습니다. 통합 구성 요소가 Hyper-V에서 이 작업을 수행합니다.

#### 가상 장치

Hyper-V의 VMBus 아키텍처를 통해 게스트 운영 체제, 즉 가상 장치에 새로운 유형의 하드웨어를 도입할 수 있습니다. 이 장치는 실제 장치에 매핑되면서 실제 장치를 에뮬레이트하지는 않는 가상의 장치를 의미합니다. 에뮬레이트된 장치는 실제 장치의 소프트웨어를 정확하게 재현합니다. 예를 들어, 에뮬레이트된 디스크 컨트롤러의 경우 게스트 운영 체제에서 실제 디스크 컨트롤러와 구분되지 않습니다. 즉, 게스트 운영 체제에도 실제 운영 체제와 같은 제약 조건이 주어집니다.

가상 장치는 게스트 운영 체제를 위한 통합 구성 요소 패키지에서 이용 가능한 VSC를 포함한 모든 게스트 운영 체제에서 사용할 수 있습니다. 일반적으로 Windows 2000 Server 이상을 기반으로 하는 게스트 운영 체제는 가상 장치를 사용할 수 있습니다. 아래 표는 지원되는 게스트 운영 체제에 대한 가상 장치 지원을 열거한 것입니다.

표 2: 가상 장치 가용성

|  |  |
| --- | --- |
| **게스트 운영 체제** | **가상화된 장치 유형** |
| Windows Server 2008, Windows Server® 2003 R2, Windows Vista® SP1, Windows® XP SP3  참고: Windows Vista SP1 및 Windows XP SP3의 가상 장치 지원은 Hyper-V 릴리스에서 제공됩니다. | 가상 |
| 기타 Windows 운영 체제 | 에뮬레이트됨 |
| SUSE Linux Enterprise 10 | 가상 |
| 기타 Linux 운영 체제 | 에뮬레이트됨 |

### 저장소 기능

Hyper-V에는 가상 컴퓨터 저장소 하드웨어와 관련된 여러 가지 기능이 새로 추가되었습니다. Microsoft Virtual Server에서 가상 컴퓨터의 파일 콘텐츠는 하나 이상의 VHD(가상 하드 드라이브) 파일에 저장됩니다. 호스트 운영 체제는 이 VHD 파일을 액세스 가능한 파일 시스템(일반적으로 내부 하드 드라이브 저장소) 또는 SAN(저장소 영역 네트워크)에서 유지 관리합니다. Hyper-V는 게스트 운영 체제에 대한 새로운 저장소 액세스 방법을 지원합니다.

#### 가상 컴퓨터의 Pass-Through 디스크 액세스

가상 컴퓨터는 Pass-Through 디스크 액세스를 통해 VHD 파일을 사용하지 않고 쓰기 가능한 파일 시스템에 직접 액세스할 수 있습니다. 예를 들어, SQL Server® 데이터베이스를 포함하는 Windows Server 2008 기반 가상 컴퓨터에서 Pass-Through 디스크 액세스를 통해 iSCSI 또는 파이버 채널 SAN에 있는 데이터베이스 파일에 액세스할 수 있습니다. 이 가상 컴퓨터가 Hyper-V 호스트 서버에 직접 연결된 디스크의 파티션에 액세스하도록 구성할 수도 있습니다.

Pass-Through 디스크 액세스를 이용하면 대개 VHD 형식으로 암호화되어 있는 데이터를 비 가상 시스템에서 액세스할 수 있는 파일 시스템에서 조작 가능하도록 만들 수 있습니다. 이와 같은 저장소 구성을 위한 추가 옵션으로 Hyper-V 사용 시나리오에 유연성을 더할 수 있습니다. 예를 들어, 가상 SQL Server가 Pass-Through 디스크 액세스를 사용하여 데이터베이스 파일을 SAN에 저장함으로써 보고 응용 프로그램도 이러한 파일에 액세스할 수 있습니다. 또는 가상 IIS 7.0 웹 서버가 Pass-Through 디스크 액세스를 사용하여 웹 콘텐츠를 SAN에 저장함으로써 콘텐츠 인덱싱 응용 프로그램 또한 이러한 파일에 액세스할 수 있습니다.

#### 새 저장 장치 컨트롤러 아키텍처

Hyper-V에 사용되는 VMBus 아키텍처는 가상 컴퓨터용 가상 저장 장치 컨트롤러를 제공합니다. 가상 저장 장치 컨트롤러당 최대 255개의 VHD를 지원하며, 가상 컴퓨터당 지원되는 컨트롤러 수에는 제한이 없습니다.

가상 장치를 지원하지 않는 게스트 운영 체제는 에뮬레이트된 IDE 컨트롤러를 사용하여 저장소에 액세스합니다. Microsoft Virtual Server 2005에서 에뮬레이트된 SCSI 컨트롤러는 제거되었습니다. 이것은 에뮬레이트된 IDE 컨트롤러가 수정되어 이전의 제약 사항을 해소할 수 있게 되었기 때문입니다. Hyper-V에서 새로 에뮬레이트된 IDE 컨트롤러는 Microsoft Virtual Server 2005의 에뮬레이트된 SCSI 컨트롤러와 동일한 기능을 갖고 있습니다.

### 강력한 네트워킹

#### VLAN 지원

Windows Server 가상화는 가상 컴퓨터를 통해 송수신되는 네트워크 트래픽을 제어하고 보안을 유지하기 위해 가상 스위치를 사용합니다. Hyper-V 가상 스위치를 실제 네트워크 VLAN(가상 LAN) 태그와 연결하여 그 가상 스위치를 통해 특정 VLAN에 대한 네트워크 통신을 제한할 수 있습니다. 복수의 Hyper-V 가상 스위치를 실제 네트워크 어댑터 한 개와 연결할 수 있습니다. Hyper-V의 VLAN 지원으로 가상 컴퓨터와 특정 VLAN의 네트워크 통신을 제한함으로써 가상 컴퓨터에 대한 네트워크 보안성을 높일 수 있습니다.

#### PXE 부팅

Hyper-V의 가상 네트워크 카드는 PXE(Pre-boot Execution Environment) 부팅을 지원합니다. 고객은 이 네트워크 부팅을 이용하여 실제 서버와 동일한 방법으로 가상 컴퓨터를 구축할 수 있습니다. 이 기능을 이용하려면 호스트 네트워크에 PXE 인프라가 있어야 합니다.

#### 가상 컴퓨터 NAP 지원

Hyper-V는 Windows Server 2008의 NAP(네트워크 액세스 보호) 기능과 함께 비호환 가상 컴퓨터가 조직 네트워크에 액세스하거나 문제를 일으키지 않도록 예방합니다. NAP는 컴퓨터 상태 요구 사항을 구성 및 적용하고, 비호환 컴퓨터이면 업데이트 또는 수정한 후 기업 네트워크에 연결할 수 있게 합니다. NAP를 통해 관리자는 소프트웨어 요구 사항, 보안 업데이트 요구 사항 그리고 조직 네트워크에 연결된 컴퓨터에 필요한 구성 설정 등을 정의한 상태 정책을 구성할 수 있습니다.

NAP는 클라이언트 컴퓨터의 상태를 평가하고 비호환 컴퓨터의 네트워크 액세스를 제한하는 방법으로 상태 요구 사항을 적용합니다. 클라이언트와 서버의 구성 요소는 비호환 컴퓨터의 개선을 보조하여 컴퓨터가 무제한으로 네트워크에 액세스할 수 있게 합니다. 컴퓨터가 비호환인 것으로 판단되면 네트워크 액세스가 거부되거나 즉시 패치를 실행하여 호환 컴퓨터로 만듭니다.

NAP 적용 방법은 NAP와 결합하여 상태 정책을 적용하는 네 가지 네트워크 액세스 기술을 지원합니다. 즉, IPSec(인터넷 프로토콜 보안) 적용, 802.1X 적용, 라우팅 및 원격 액세스를 위한 VPN(가상 사설망) 적용 그리고 DHCP(Dynamic Host Configuration Protocol) 적용입니다.

NAP의 이점은 조직 환경의 실제 컴퓨터에 적용되는 것과 동일한 방식으로 가상 컴퓨터에 적용됩니다. NAP의 더욱 포괄적인 적용 범위에 대해서는 5장 보안 및 정책 적용을 참조하십시오.

### 유연한 역할 기반 보안

역할 기반 보안을 사용하면 복수의 가상 컴퓨터를 실행하는 Hyper-V 환경에서 하나 이상의 가상 컴퓨터에 대한 관리 액세스 권한을 제한할 수 있습니다. Hyper-V는 Windows Server 2008 권한 부여 관리자를 이용하여 역할 권한을 할당합니다. 예를 들어, 관리 역할은 조직 내 마케팅 부서의 데이터베이스 관리자일 수도 있습니다. 가상화되지 않은 구성으로 전용 데이터베이스 서버를 실행하는 경우에는 데이터베이스 관리자에게 조직 내 다른 서버들은 제외하고 데이터베이스 서버에 대한 액세스 권한만 할당할 수 있습니다.

그러나 가상화되지 않은 서버는 사용률이 낮은 경우가 많기 때문에 조직들은 이전에 전용 서버에 배포했던 작업을 통합 서버에 결합시키고 있습니다. 앞의 예에서는 마케팅 데이터베이스 서버를 다른 데이터베이스 및 응용 프로그램을 실행하는 서버에 통합할 수 있을 것입니다. 이러한 통합은 서버 보안 유지를 어렵게 만들기 때문에, 복수의 관리자에게 호스트 서버에 대한 관리 액세스 권한 또는 기타 VM에 대한 관리 액세스 권한 없이 필수 VM에 필요한 액세스 수준만 할당해야 합니다. 이 예제에서 마케팅 데이터베이스 관리자는 마케팅 데이터베이스 VM만 액세스 및 관리할 수 있습니다.

Hyper-V에서는 마케팅 데이터베이스와 같은 작업에 자체 가상 컴퓨터를 할당할 수 있습니다. 가상 컴퓨터는 분산된 실제 서버와 동일한 보안 경계를 나타내므로 마케팅 데이터베이스 관리자에게는 조직 내 호스트 또는 다른 가상 서버에 대한 관리 권한을 부여하지 않고 마케팅 데이터베이스를 호스팅한 가상 서버에 대한 관리 액세스 권한을 할당할 수 있습니다.

Hyper-V의 이 기능으로 더욱 간편하고 유연하게 서버를 통합할 수 있습니다.

### Server Core에서의 Hyper-V

Hyper-V를 Server Core에 하나의 역할로 설치할 수 있습니다. Server Core는 다음 서버 역할이 여러 개 실행될 수 있는 환경을 제공합니다.

* Hyper-V
* DHCP(Dynamic Host Configuration Protocol) 서버
* DNS(Domain Name System) 서버
* 파일 서버
* AD DS(Active Directory® Directory Services)
* Active Directory LDS(Lightweight Directory Services)
* Windows Media Services
* 인쇄 서버
* IIS 7.0

Server Core에서 Hyper-V를 실행하면 다음과 같이 부가적인 보안 및 성능 상 이점이 있습니다.

* 공격 위험 감소 - Server Core는 DLL 및 시스템 구성 요소를 최소한으로 사용하기 때문에 공격과 손상의 기회도 줄어듭니다. 자주 공격 목표가 되곤 하는 Internet Explorer와 같은 응용 프로그램은 Windows Server 2008의 Server Core 설치에는 제공되지 않습니다.
* 소프트웨어 업데이트 요구 사항 감소 - Server Core가 제공하는 서버 역할 집합이 감소되었습니다. 서버에서 사용할 수 없는 역할은 소프트웨어 업데이트를 통해 유지 관리할 필요가 없기 때문에 Server Core에서는 Windows Update 다운로드 용량과 횟수가 적습니다. Server Core의 또 다른 이점은 Windows Update에 필요한 재부팅 횟수가 적다는 점입니다.
* 성능 - Server Core는 메모리 요구량이 훨씬 적기 때문에 Hyper-V 실행 플랫폼 중에서 비용이 가장 저렴하게 듭니다.

MMC 3.0 기반의 Hyper-V 관리 콘솔을 이용하면 워크스테이션 또는 다른 Windows Server 2008 서버에서 가상 컴퓨터를 간편하게 생성 및 관리할 수 있으므로 Server Core는 많은 Hyper-V 설치에 이상적인 Windows Server 2008 구성이 될 수 있습니다. 이 장의 뒷부분에서 설명하게 될 WMI 공급자와 Hyper-V의 PowerShell 스크립팅 지원은 호스트 서버와 게스트 가상 컴퓨터의 스크립트 기반 관리에 강력하고 유연한 지원을 제공합니다.

Windows Server 2008의 Server Core 설치는 Hyper-V 가상 컴퓨터에 핵심 인프라 역할을 호스팅하는 데 사용할 수 있습니다. Windows Server Core 기반 소형 VM은 VM 집적도를 높이는 동시에 더욱 빠르고 간편한 마이그레이션, VM 스냅샷 및 VM 백업을 가능하게 합니다. 뿐만 아니라 Windows Server Core를 Hyper-V의 호스트 운영 체제로 사용하면 Windows Server Core의 패치 요구 사항이 감소되므로 가동 시간을 늘릴 수 있습니다. Windows Server Core와 Hyper-V는 가용성이 높은 가상 환경에 매우 적합한 조합입니다.

### 유연한 리소스 제어

Hyper-V는 실행 중인 가상 컴퓨터에 유연하고 제어 가능한 방식으로 리소스를 할당할 수 있습니다.

#### CPU 리소스 할당

Hyper-V는 유연한 CPU 리소스 할당 모델을 기반으로 실행 중인 가상 컴퓨터에 호스트 서버의 실제 CPU 리소스를 할당할 수 있습니다. 아래 표는 Hyper-V CPU 리소스 할당 계산에 사용되는 설정을 설명한 것입니다.

표 3: CPU 리소스 할당 설정

|  |  |
| --- | --- |
| **항목** | **설명** |
| 상대적 가중치 | 이 가상 컴퓨터의 리소스 요구량을 다른 모든 가상 컴퓨터와 비교하여 지정되는 상대적 가중치입니다. 상대적 가중치가 더 높은 가상 컴퓨터에는 필요에 따라 상대적 가중치가 더 낮은 다른 가상 컴퓨터로부터 추가 리소스가 동적으로 할당됩니다. 기본적으로, 모든 가상 컴퓨터는 상대적 가중치가 100으로 설정되어 있습니다. 따라서 리소스 요구량은 동일하며 이때는 우선 순위가 주어지지 않습니다. 관리자는 각 가상 컴퓨터에 1에서 10,000 사이의 상대적 가중치를 할당할 수 있습니다. 대개는 상대적 가중치만 설정하면 다른 구성이 필요하지 않습니다. |
| 할당 용량(한 CPU가 차지하는 비율) | 이 가상 컴퓨터용으로 할당된 단일 CPU 용량입니다. CPU 용량 중 사용 가능한 비율은 이 숫자보다 큽니다. |
| 최대 용량(한 CPU가 차지하는 비율) | 단일 CPU의 총 리소스 중 이 가상 컴퓨터가 언제든 사용할 수 있는 최고 비율입니다. |
| 할당 용량(시스템이 차지하는 비율) | 총 시스템 CPU 용량 중 이 가상 컴퓨터용으로 할당된 비율입니다. |
| 최대 용량(시스템이 차지하는 비율) | 총 시스템 CPU 리소스 중 이 가상 컴퓨터가 언제든 사용할 수 있는 최고 비율입니다. |
| 총 할당 용량 | 실제 컴퓨터에서 현재 실행 중인 모든 가상 컴퓨터용으로 할당된 총 CPU 용량입니다. 실제 컴퓨터에 CPU가 여러 개인 경우 이 숫자는 전체 CPU를 위해 할당된 비율을 나타냅니다. |
| 나머지 가용 용량 | 실제 컴퓨터에서 현재 실행 중인 가상 컴퓨터용으로 할당되지 않은 총 CPU 용량입니다. 실제 컴퓨터에 CPU가 여러 개인 경우 이 숫자는 전체 CPU를 위해 사용 가능한 비율을 나타냅니다. |

참고: Hyper-V는 가상 컴퓨터에 시스템 리소스를 할당하기 위한 자체 리소스 관리자를 제공합니다. WSRM(Windows 시스템 리소스 관리자)과 같은 리소스 관리자는 Hyper-V와 함께 사용할 수 없습니다.

### Hyper-V 고가용성

Hyper-V에는 장애 조치 클러스터링과 결합하여 Windows 가상화에서 실행되는 가상 컴퓨터의 고가용성을 보장하는 향상된 기능이 포함되어 있습니다. 장애 조치 클러스터링과 System Center Virtual Machine Manager를 Hyper-V와 결합하여 사용하는 관리자는 예정된 중단 시간 요구에 대해 조치를 취하고 예기치 못한 중단 시간에 대해서는 서비스 중단을 최소화하는 방법으로 대응할 수 있습니다.

Hyper-V는 다음을 통해 가상 컴퓨터의 가용성을 높입니다.

* 장애 조치 클러스터링
* 실시간 마이그레이션
* 백업

#### 클러스터링과 Hyper-V

Windows Server 2008 클러스터링은 예정되었거나 예기치 못한 네트워크 중단 시 가상 컴퓨터가 클러스터의 다른 노드로 마이그레이션할 수 있게 하여 Hyper-V에 높은 가용성을 제공합니다. 클러스터링은 Hyper-V 역할 자체를 클러스터링하거나 Hyper-V에서 실행 중인 개별 가상 컴퓨터를 클러스터링하여 구현할 수 있습니다. 전자를 호스트 클러스터링이라 하고, 후자를 게스트 클러스터링이라 합니다.

#### 호스트 클러스터링

Windows Server 2008 장애 조치 클러스터링을 사용하여 Hyper-V 역할의 가용성을 높인다는 것은 Hyper-V를 실행하는 하나 이상의 서버에 장애 조치 클러스터링 역할이 추가되며 지원되는 클러스터 구성으로 설정된다는 것을 의미합니다. 이를 호스트 클러스터링이라 합니다. 장애 조치 클러스터링에 기본적으로 필요한 것은 클러스터 노드를 위한 공유 저장소입니다. 여기에는 iSCSI 또는 파이버 채널 SAN(저장소 영역 네트워크) 등이 포함될 수 있습니다. 모든 가상 컴퓨터는 공유 저장소 영역에 저장되며, 실행 중인 가상 컴퓨터 상태는 Hyper-V 노드 중 하나에 의해 관리됩니다. 예정된 중단 시간에는 간편한 마이그레이션 기능(이 장의 뒷부분에 설명)을 사용하여 실행 중인 가상 컴퓨터를 다른 클러스터 노드로 이동할 수 있습니다. 예기치 못한 중단 시에는 중단되지 않은 클러스터 노드에서 클러스터 서비스가 가상 컴퓨터를 자동으로 다시 시작합니다. 호스트 클러스터링은 전체 Hyper-V 플랫폼 그리고 Hyper-V 서버에 호스팅된 모든 가상 컴퓨터에 높은 가용성을 제공합니다.

#### 게스트 클러스터링

Hyper-V에서 실행 중인 가상 컴퓨터는 기반 호스트 운영 체제가 아닌 경우에도 클러스터링이 가능합니다. 둘 이상의 가상 컴퓨터의 게스트 운영 체제가 클러스터 리소스가 보관된 외부 공유 저장소를 액세스할 수 있도록 구성할 수 있습니다. 게스트 운영 체제가 클러스터링을 지원하는 경우에는 가상 컴퓨터가 클러스터 리소스에 대한 고가용성을 제공하도록 구성할 수 있습니다.

Hyper-V 게스트 클러스터링을 사용하여 데이터베이스, 파일 공유 그리고 네트워크 인프라 및 응용 프로그램 서비스를 포함한 다양한 리소스에 대한 고가용성을 제공할 수 있습니다. Hyper-V 게스트 클러스터링과 Windows Server 2008 네트워크 부하 분산(NLB) 서비스를 결합하여 여러 Hyper-V 호스트 서버에 고가용성과 부하 분산 기능을 제공할 수 있습니다.

네트워크 부하 분산은 네트워크 클라이언트 및 서버 응용 프로그램의 부하를 NLB 클러스터의 여러 서버에 분산하는 기능입니다. 이 기능은 작업이 증가할 때 다른 서버를 추가하여 IIS(인터넷 정보 서비스)에서 실행되는 웹 기반 응용 프로그램과 같은 상태 비저장 응용 프로그램이 확장될 수 있도록 하는 데 특히 유용합니다 NLB는 부하가 증가함에 따라 다른 서버가 추가되도록 함으로써 확장성을 제공합니다. NLB는 사용자가 오작동 서버를 쉽게 대체할 수 있도록 함으로써 안정성을 제공합니다.

#### Hyper-V 및 멀티 사이트 클러스터링

Windows Server 2008 장애 조치 클러스터링에서는 요구 대기 시간(500ms 미만) 문제가 해결되었습니다. Windows Server 2008의 요구 대기 시간은 구성 가능합니다. Windows Server 2008에서는 서브넷 상에서도 클러스터링이 가능합니다. 따라서 클러스터 노드를 지리적으로 분산된 사이트에 연결하기 위해 VLAN을 사용해야 했던 이전의 요구 사항도 없어졌습니다.

Windows Server 2008의 멀티 사이트 클러스터링 기능이 향상되어, 데이터 센터 운영 장애가 발생하는 경우 주 사이트와 지리적으로 떨어진 복구 사이트에서 조치할 수 있게 되었습니다.

Hyper-V 간편한 마이그레이션

Hyper-V의 간편한 마이그레이션 기능을 사용하면 한 Hyper-V 호스트에서 실행 중인 가상 컴퓨터를 다른 Hyper-V 호스트로 이동할 수 있습니다. 간편한 마이그레이션은 간편한 마이그레이션에 필요한 기본 공유 저장소 관리 및 리소스 재배치 기술을 제공하는 호스트 클러스터링 구성에서 지원됩니다.

간편한 마이그레이션은 세 가지 방법으로 관리할 수 있습니다. 첫째, SCVMM(System Center Virtual Machine Manager)은 실행 중인 가상 컴퓨터를 한 Hyper-V 호스트 서버에서 동일 클러스터의 다른 Hyper-V 호스트 서버로 끌어 놓기 방법을 이용하여 마이그레이션할 수 있는 GUI 인터페이스를 제공합니다. SCVMM을 사용하지 않는 경우에는 장애 조치 클러스터 관리자 MMC 콘솔을 이용하여 네트워크 중단을 최소화하면서 한 Hyper-V 호스트 서버에서 실행 중인 가상 컴퓨터를 동일 클러스터의 다른 Hyper-V 호스트 서버로 간편한 마이그레이션을 수행할 수 있습니다. 또한 Hyper-V의 WMI 공급자를 이용하면 한 Hyper-V 호스트 서버에서 실행 중인 가상 컴퓨터를 동일 클러스터의 다른 Hyper-V 호스트 서버로 간편한 마이그레이션을 스크립트화할 수 있습니다. 간편한 마이그레이션의 속도는 이동할 메모리에 포함된 정보의 양과 공유 저장 장치의 속도에 따라 달라집니다.

### 관리 기능

#### 가상 서버 마이그레이션

Microsoft Virtual Server 2005, Microsoft Virtual PC 및 Hyper-V는 개방형 VHD 형식으로 가상 컴퓨터의 파일 콘텐츠를 저장합니다. 따라서 Virtual Server 2005에서 생성된 기존의 가상 컴퓨터를 Hyper-V 호스트로 마이그레이션할 수 있습니다. 관리자는 Virtual Server 2005에서 기존의 가상 작업을 생성 및 관리할 수 있으며, 배포 후에는 가상 컴퓨터를 다시 만들 필요 없이 그 가상 컴퓨터를 Hyper-V로 직접 이동할 수 있습니다. 따라서 관리자는 가상 인프라에 대한 기존의 투자를 계속 이용하면서 점차 그 인프라를 Hyper-V로 옮길 수 있습니다.

#### WMI 공급자

Hyper-V는 WMI(Windows Management Instrumentation)를 통해 관리됩니다. Hyper-V WMI 공급자는 다음을 포함하여 Hyper-V를 전반적으로 제어하는 개체를 표시합니다.

* 서버 설정 관리
* 가상 컴퓨터 생성 및 구성
* 가상 네트워크 스위치 생성 및 구성
* 실행 중인 가상 컴퓨터의 상태 제어

뿐만 아니라 WMI 공급자는 Windows PowerShell, System Center Virtual Machine Manager 및 기타 Hyper-V 서버 관리를 위한 타사 도구와 같은 외부 스크립팅 및 관리 도구를 허용합니다.

#### 성능 카운터

Hyper-V는 상세한 성능 및 리소스 활용 카운터를 제공합니다. 이 카운터는 리소스 사용률을 전반적으로 또는 가상 컴퓨터별로 보고할 수 있습니다. 관리자는 이 성능 카운터를 이용하여 호스트 서버 리소스가 가상 컴퓨터에서 어떻게 사용되는지 확인할 수 있습니다. 이 정보는 관리자들이 Hyper-V 환경에서 성능 문제를 파악하고 Hyper-V 호스트 서버 하드웨어를 가상 컴퓨터에 효과적으로 할당하는 데 도움을 줍니다. Hyper-V 사용률 카운터 역시 비용 청구 회계용 소스 데이터를 제공할 수 있습니다.

#### 심각한 오류 알림

Hyper-V에서는 심각한 오류 알림 기능이 통합되어 중요한 상태를 인식하고 적절히 대응합니다. 예를 들어, Hyper-V 호스트 서버에 UPS(무정전 전원 공급 장치)가 연결되어 있는 경우, 정전이 되면 UPS는 상위 파티션에 전원이 끊어졌다는 신호를 보내고 예상 배터리 수명이 어느 정도인지 알립니다. Hyper-V는 이러한 심각한 오류 알림에 대해 여러 가지 방법으로 대응합니다. Hyper-V는 다음과 같은 대응책을 수행할 수 있습니다.

* 현재 상태를 저장하고 가상 컴퓨터의 전원을 끕니다.
* 게스트 운영 체제를 중단합니다.
* 상태를 저장하지 않고 가상 컴퓨터의 전원을 끕니다.
* Hyper-V 호스트가 올바로 구성된 경우 간편한 마이그레이션을 수행합니다.

#### 게스트 운영 체제 지원

사업부는 동적 데이터 센터를 기반으로 각 업무 기능에 가장 효과적인 도구를 통합합니다. 그러한 도구에는 고유한 하드웨어 또는 소프트웨어 구성이 필요할 수도 있습니다. 예를 들어, 제조 공정에 연결되어 있는 Linux 기반의 수직 응용 프로그램은 다른 영역의 Windows 기반 응용 프로그램과 공존할 수 있어야 합니다.

Hyper-V는 주요 운영 체제와 호환되는 32비트 VM뿐 아니라 Windows, Linux 및 Xen 기반 Linux를 실행하는 64비트 및 32비트 VM을 지원합니다. 과거에는 단일 응용 프로그램 기능으로 한정된 서버들을 동적 하드웨어 관리 및 장애 조치 클러스터링과 같은 고급 기능을 통합한 VM으로 교체할 수 있게 되었습니다.

#### 실행 중인 가상 컴퓨터의 핫 백업

Hyper-V는 Windows Server 2008에서 VSS(볼륨 섀도 복사본 서비스)와 상호 작용하여 실행 중인 가상 컴퓨터의 백업을 허용합니다. 따라서 VHD 파일을 다른 위치로 복사하는 데 걸리는 시간에 전체 서버를 실행 중 백업할 수 있게 된 것입니다.

#### Hyper-V 온라인 백업

Hyper-V에는 통합 VSS 작성기 구성 요소가 포함됩니다. VSS 작성기는 일관된 섀도 복사본을 제공하는 데 도움이 되는 응용 프로그램 및 서비스에 포함된 소프트웨어입니다. 응용 프로그램과 서비스가 실행 중일 때 작성기는 볼륨 섀도 복사본 서비스(일반적으로 백업 프로그램을 통해 호출)와 협력하여 섀도 복사본을 생성하는 동안에는 해당 볼륨에서 쓰기가 발생되지 않도록 합니다. 따라서 VM이 온라인 상으로 실행 중일 때 백업할 수 있습니다.

#### Hyper-V 재해 복구 준비

Hyper-V를 사용하면 가상화되지 않은 서버 및 일부 다른 제품에 비해서 재해 복구 준비를 위해 더 많은 옵션을 사용할 수 있습니다. 관리자는 실행 중인 가상 컴퓨터를 백업할 수 있으므로 가상 서버를 중단하지 않고도 가상 서버의 시스템 복구가 가능합니다. 따라서 관리자는 백업 일정을 더 유연하게 예약할 수 있습니다.

Hyper-V 호스트 서버에 장애가 생기면 호스트 서버를 수리 또는 교체할 때까지 그 호스트에 있는 모든 가상 컴퓨터를 사용할 수 없게 됩니다. 관리자가 호스트의 가상 컴퓨터를 다른 위치에 백업한 경우, 백업된 VHD 파일에는 가상 컴퓨터를 백업된 지점까지 복구하는 데 필요한 모든 정보가 들어 있습니다. 사용하지 않는 하드웨어 용량이 포함된 Hyper-V 서버가 있다면 백업된 가상 컴퓨터를 이 대체 서버로 복원하고 가상 컴퓨터를 시동하고 서비스를 복원할 수 있습니다. 이 재해 복구 방법을 테스트하여 이런 복원 방식이 보조 서비스에 영향을 미치는지 확인해야 하지만, 이것은 Hyper-V 호스트에 영향을 미치는 재해를 신속히 복구하기 위한 탁월한 선택입니다.

#### 가상 컴퓨터 스냅샷

Hyper-V는 Microsoft 볼륨 섀도 복사본 서비스와 통합되었으므로 관리자는 실행 중인 가상 컴퓨터에 대한 특정 시점의 복사본을 생성할 수 있습니다. 이는 백업 및 재해 복구 시나리오에 유용합니다. 또한 관리자가 복잡하거나 위험도가 높은 구성 변경을 구현하려는 경우 유용하며, 변경으로 인해 문제가 발생하면 롤백할 수 있는 옵션을 갖추고 있습니다. 관리자가 가상 컴퓨터의 스냅샷을 생성할 때 Hyper-V는 스냅샷이 생성되기 전에 가상 컴퓨터가 일관된 상태인지 확인합니다.

## 시나리오: 인프라, 응용 프로그램 및 원격 서버 작업 통합

가상화 기술 채택의 최대 이점은 서버 통합입니다. 기업은 관리를 간소화하고 경비를 절감하면서도신뢰성, 확장성, 보안성 등의 경쟁적 장점을 유지하고 개선해야 한다는 압력을 받고 있습니다.

Hyper-V는 데이터 센터 및 원격 위치에서의 서버 통합에 이상적이므로 조직은 하드웨어 리소스를 보다 효율적으로 사용할 수 있게 됩니다. IT 조직인 경우에는 관리 생산성을 높이고 새로운 서버를 신속하게 배포하여 변화하는 비즈니스 요구를 만족시킬 수도 있습니다.

### 주요 통합 기능

표 4: 주요 통합 기능

|  |  |
| --- | --- |
| **기능** | **설명** |
| 광범위한 게스트 운영 체제 지원 | Hyper-V에서 지원되는 게스트 운영 체제로는 Windows Server 2008(Server Core 포함), Windows Server 2003 R2 SP2, Windows Vista SP1, Windows XP Pro SP3 및 SUSE Linux Enterprise Server 10 등이 있습니다. 이러한 운영 체제는 VMBus 하드웨어 공유 이점을 활용할 수 있으며, 관련 성능의 개선 효과도 누릴 수 있습니다.  위의 운영 체제를 지원하는 것 외에도, Hyper-V에서 실행 중인 VM은 호환 가능한 하드웨어를 폭넓게 에뮬레이트할 수 있으므로 다른 많은 게스트 운영 체제가 Hyper-V VM에서 잘 작동할 수 있습니다. |
| 하드웨어 가상화 및 레거시 하드웨어 에뮬레이션 | 지원되는 게스트 운영 체제 기반 VM은 실제 존재하지 않는 가상 장치와 상호 작용합니다. 레거시 운영 체제는 특정 장치(예: Intel 21140 네트워크 어댑터)의 역할을 수행하는 에뮬레이트된 하드웨어와 상호 작용합니다. |
| P2V - 실제에서 가상으로 변환 | 실제 서버를 가상 컴퓨터로 변환합니다. |
| CPU 리소스 할당 | CPU 리소스 할당은세분화된 제어를 위해 가중치 부여 및 한정된 방식을 둘 다 지원합니다.   * 멀티스레드 기능으로 확장성을 향상시킵니다. * 각 가상 컴퓨터가 단일 호스트 프로세서 코어를 100%까지 사용할 수 있습니다. * 복수의 가상 컴퓨터가 동시에 실행되고 복수의 호스트 프로세서 코어를 사용할 수 있습니다. * 서버 유형에 관계 없이 호스팅 가능한 가상 컴퓨터의 수는 다음에 따라 달라집니다.   + 결합된 프로세서, 메모리 그리고 가상 컴퓨터가 호스트에 부여하는 I/O 부하   + 호스트 시스템에서 사용할 수 있는 프로세서, 메모리 및 I/O 용량 * Hyper-V는 작업 균형 관리를 위한 가중치 및 제약 조건을 기반으로 한 CPU 리소스 할당을 둘 다 지원합니다. * 이 가상 컴퓨터의 리소스 요구량을 다른 모든 가상 컴퓨터와 비교하여 지정되는 상대적 가중치입니다. 상대적 가중치가 더 높은 가상 컴퓨터에는 필요에 따라 상대적 가중치가 더 낮은 다른 가상 컴퓨터로부터 추가 리소스가 동적으로 할당됩니다. 기본적으로, 모든 가상 컴퓨터는 상대적 가중치가 100으로 설정되어 있습니다. 따라서 리소스 요구량은 동일하며 이때는 우선 순위가 주어지지 않습니다. * 용량 및 가중치 알고리즘은 동시에 작동합니다.   + 최대 시스템 용량에 대한 경쟁 발생 가능   + 상대적 가중치는 경쟁 과정에서 리소스 할당 방법을 표시 |
| 메모리 리소스 할당 | Hyper-V에서는 실행 중인 VM에 대한 Hot-add 메모리를 포함하여 가상 컴퓨터별로 유연한 메모리 구성이 가능합니다.   * NUMA 인식 예약 및 메모리 할당도 지원되므로 멀티 프로세서 소켓 시스템에서의 메모리 버스 경쟁이 줄어듭니다. * 비 NUMA 시스템에서는 Hyper-V가 호스트 운영 체제 스케줄러를 사용합니다. |
| PXE 부팅 | Hyper-V의 가상 네트워크 카드는 PXE(Pre-boot Execution Environment) 부팅을 지원합니다. 고객은 이 네트워크 부팅을 이용하여 실제 서버와 동일한 방법으로 가상 컴퓨터를 구축할 수 있습니다.  참고: 이 기능을 이용하려면 호스트 네트워크에 PXE 인프라가 있어야 합니다. |
| Active Directory 통합 | Active Directory에서는 네트워크의 사용자와 컴퓨터에 대한 계층 구조 정보를 위한 중앙 집중식 리포지토리를 제공하는 방법으로 동일한 디렉터리 관리 기능을 실제 컴퓨터 대신 사용되는 가상 컴퓨터에 적용할 수 있습니다. Active Directory에서는 Windows Server 2008의 관리 및 성능 개선 사항을 통합했으며, Hyper-V에서 호스팅된 가상 컴퓨터를 통해 사용할 수 있습니다.  Active Directory와의 통합으로 관리 위임 및 게스트 액세스 인증이 가능합니다. Hyper-V는 Active Directory의 그룹 정책 관리 콘솔에서 관리할 수 있는 가상 컴퓨터별 ACL을 통해 가상 컴퓨터에 대해 세분화된 관리 제어를 가능케 합니다. 이벤트 로그가 Active Directory 및 MMC(Microsoft Management Console)에 통합되었습니다. |

## 시나리오: 소프트웨어 테스트와 개발 환경의 자동화 및 통합

Hyper-V를 통해 기업은 테스트 및 개발 서버를 통합하고 가상 컴퓨터 구축을 자동화할 수 있습니다.

모든 분야의 고객은 비용을 절감하고 응용 프로그램과 인프라 설치 및 업그레이드를 가속화하는 동시에 포괄적인 품질 보증을 제공할 방법을 모색하고 있습니다. 프로덕션에 들어가기 전에 테스트 범위 목표를 달성하려면 다음과 같은 여러 가지 과제를 극복해야 합니다.

* 네트워크 운영 - 테스트 네트워크를 잘못 구성하면 프로덕션 네트워크가 불안해질 수 있습니다.
* 개발자 생산성 - 테스트 환경 구성이나 운영 체제 설치와 같이 시간이 많이 소요되는 관리 작업에 개발자 생산성이 낭비됩니다.
* 서버 운영비 및 투자 비용 - 우수한 응용 프로그램 테스트 범위에는 프로덕션 컴퓨팅 환경의 복제를 요하는데, 여기에는 인적 자원과 비싼 하드웨어가 필요합니다. 이로 인해 비용과 일정 문제에 위험을 수반할 수 있습니다.

가상 컴퓨터 기술은 30여 년 전 메인프레임 시대에 처음 발생된 이러한 과제를 해결하기 위해 개발된 것으로, 동일한 시스템에 테스트 파티션과 프로덕션 파티션을 나란히 구성할 수 있습니다. Hyper-V에서는 테스트 범위, 개발자 생산성 그리고 사용자 환경이 개선되었습니다.

또한 개발자는 Hyper-V와 같이 효율적인 도구를 이용하여 하나의 실제 서버에서 분산된 응용 프로그램을 시뮬레이트할 수 있습니다. 분산 서버 응용 프로그램의 배포와 테스트에는 일반적으로 실습 환경에서 원하는 시나리오를 시뮬레이트하도록 하드웨어와 소프트웨어 시스템을 구성하기 위해 많은 양의 하드웨어 리소스와 상당한 시간이 요구됩니다.

Hyper-V는 분산 서버 응용 프로그램 개발 시나리오에서 하드웨어 및 인적 자원 활용을 최적화하여 시간과 리소스를 절약하는 강력한 솔루션입니다. 개발자는 하나의 실제 서버에 있는 복수의 가상 컴퓨터를 이용하여 분산 서버 응용 프로그램을 간편하게 배포 및 테스트할 수 있습니다. 디스크 계층 및 가상 네트워킹과 같은 Hyper-V의 강력한 기능을 시스템 통합의 장점과 결합시킴으로써 개발자는 복잡한 네트워크 환경을 강력하고 효율적으로 시뮬레이트할 수 있습니다. 결과적으로 네트워크 구축을 위한 하드웨어, 물리적 공간 그리고 시간이 절약되는 비용 효율적인 개발 환경 솔루션이 탄생하게 됩니다.

표 5: 주요 소프트웨어 테스트 및 개발 기능

|  |  |
| --- | --- |
| **기능** | **설명** |
| 광범위한 게스트 운영 체제 지원 | Hyper-V에서 지원되는 게스트 운영 체제로는 Windows Server 2008(Server Core 포함), Windows Server 2003 R2 SP2, Windows Vista SP1, Windows XP Pro SP3 및 SUSE Linux Enterprise Server 10 등이 있습니다. 이러한 운영 체제는 VMBus 하드웨어 공유 이점을 활용할 수 있으며, 관련 성능의 개선 효과도 누릴 수 있습니다.  위의 운영 체제를 지원하는 것 외에도, Hyper-V에서 실행 중인 VM은 호환 가능한 하드웨어를 폭넓게 에뮬레이트할 수 있으므로 다른 많은 게스트 운영 체제가 Hyper-V VM에서 잘 작동할 수 있습니다. |
| 구성 라이브러리 | System Center Virtual Machine Manager와 함께 사용되는 Hyper-V에는 VM을 라이브러리에 저장하여 관리하고 필요할 때 서비스로 호출하는 기능이 포함되어 있습니다.  라이브러리 VM은 오프라인 VHD 조작을 활용하여 연결된 VM을 실행하지 않고 VM을 변경할 수 있습니다. |
| 셀프 서비스 포털 | System Center Virtual Machine Manager를 활용하는 개발자와 테스터는 관리자의 개입 없이 구성 라이브러리에서 VM을 생성 및 소멸시킬 수 있습니다. |
| VM 스냅샷 | 개발자와 테스터는 스냅샷을 이용하여 VM 시스템 구성을 "최선의" 상태로 되돌릴 수 있습니다.  프로그램 및 운영 체제를 설치, 제거 및 다시 설치하는 데 많은 시간이 걸리는 개발 및 테스트도 있습니다. Hyper-V의 스냅샷 기능을 이용하면 VM을 이전 구성으로 재설정하여 프로그램을 제거하거나 운영 체제를 다시 설치하는 수고를 덜 수 있습니다. |

## 시나리오: 비즈니스 연속성 및 재해 복구

Hyper-V를 하드웨어 플랫폼에서 응용 프로그램의 이식성 및 유연성을 요구하는 재해 복구 방법의 일부로 사용할 수 있습니다. 실제 서버를 가상 컴퓨터를 실행하는 소수의 실제 컴퓨터에 통합함으로써 재해 발생 시 손상 또는 훼손될 수 있는 물리적 자산의 수를 줄일 수 있습니다. 복구할 때는 가상 컴퓨터를 재해의 영향을 받지 않은 호스트 컴퓨터의 어느 위치에든 호스팅할 수 있으므로 복구 시간을 단축하고 조직의 유연성을 극대화할 수 있습니다.

표 6: 주요 비즈니스 연속성 및 재해 복구 기능

|  |  |
| --- | --- |
| **기능** | **설명** |
| 호스트 및 게스트 클러스터링을 통한 가용성 증가 | Hyper-V에서는 게스트 운영 체제와 호스트 컴퓨터의 클러스터링이 가능하므로 다양한 고가용성 시나리오를 구현할 수 있습니다. 호스트 컴퓨터를 클러스터링하면 서버 가용성을 비용 효율적으로 높일 수 있으므로 클러스터 내 Hyper-V 호스트에서 가상 컴퓨터에 대한 장애 조치가 가능합니다. Hyper-V 구성을 이용하면 소프트웨어 도구를 추가 구입하지 않고도 예정된 네트워크 중단 시나리오와 예기치 못한 중단 시나리오를 둘 다 효과적으로 수용할 수 있는 고가용성 가상 시스템 환경을 구현할 수 있습니다.  예를 들어, IT 관리자는 시스템 업데이트를 위해 필요한 경우 서버 다시 시작 여부를 효과적으로 예상할 수 있습니다. Hyper-V 호스트 클러스터가 올바로 구성되었다면 실행 중인 가상 컴퓨터를 네트워크 중단 없이 클러스터의 다른 호스트로 마이그레이션할 수 있습니다.  하드웨어 장애와 같은 예기치 못한 네트워크 중단 시나리오에서는 호스트에서 실행되는 가상 컴퓨터가 다음으로 이용 가능한 Hyper-V 호스트에 자동으로 마이그레이션되도록 할 수 있습니다.  게스트 클러스터링 기능을 이용하면 클러스터 인식 응용 프로그램을 Hypver-V 호스트 컴퓨터를 통해 가상 컴퓨터에서 클러스터링할 수 있습니다. |
| 실시간 백업 | Hyper-V에는 실행 중인 가상 컴퓨터와 해당 데이터를 중단 없이 백업할 수 있는 기능이 있습니다. 한 서버가 중단되면 다른 서버에서 VM을 복원하여 시작할 수 있으므로 서비스 중단이 최소화됩니다.  테이프 백업 프로세스는 Hyper-V의 가상 테이프 드라이브 기능을 활용합니다. 예를 들어, 서버가 데이터를 테이프 드라이브에 자동으로 백업하는 스크립트를 구현하는 경우에는 서버가 가상 컴퓨터로 전환된 경우에도 그 프로세스를 이용할 수 있습니다. |
| 상태 모니터링 | Hyper-V는 System Center Operations Manager와 같은 모니터링 도구와의 포괄적인 통합을 활용하여 문제가 커지기 전에 찾아서 해결합니다. |

## 시나리오: 동적 데이터 센터 활용

데이터 센터는 하드웨어 및 시설 사용률을 최적화하는 동시에 성능을 향상시키고 비즈니스 인텔리전스를 활용해야 한다는 압력을 받고 있습니다. Hyper-V는 변화하는 요구에 대처할 수 있는 민첩성과 미래를 설계하는 능력 및 유연성을 데이터 센터에 부여합니다.

데이터 센터는 64비트 멀티 프로세서 지원 및 유연한 리소스 제어와 같은 핵심 기능을 통해 상당한 리소스 요구량을 요하는 작업에서도 가상 컴퓨터를 활용할 수 있습니다.

Hyper-V는 자동 관리 동적 시스템 및 운영 대응 능력을 제공한다는 동적 데이터 센터의 비전을 실현하는 데 일조합니다. 데이터 센터는 비즈니스 프로세스를 System Center Virtual Machine Manager와 결합하여 새 응용 프로그램을 신속히 구현하고 인프라에 포함된 실제 컴퓨터에 가상 작업을 동적으로 분배함으로써 자동 관리 동적 시스템으로 진보할 수 있습니다.

### MSC 통합

Hyper-V는 DSI(Dynamic Systems Initiative)를 지원하도록 설계된 차세대 동적 관리 도구인 MSC(Microsoft System Center)와 통합되었습니다. MSC는 IT 전문가에게 IT 인프라 관리를 돕는 도구와 지식을 제공함으로써 운영 지식을 관리 도구에 구현하고 시스템에 자동 관리뿐 아니라 자체 해결 기능까지 부여합니다.

Microsoft DSI 전략의 핵심은 기업과 사내 직원들이 생산성을 높이고 변화하는 비즈니스 요구에 보다 잘 부응하도록 하는 기술을 개발 및 제공하는 것입니다. 동적 시스템 기술 전략을 구성하는 세 가지 요소가 있습니다.

1. 비즈니스 설계자, 응용 프로그램 개발자, IT 전문가, 업계 파트너와 같은 사람들의 다양한 지식을 취합하고 시스템 모델을 사용하여 이를 IT 인프라에 통합하는 작업을 위한 설계
2. 시스템에서 구성의 바람직한 상태 및 모델 상태를 파악하고 현재 고유 지식을 활용하여 시스템에 자동 관리 수준을 제공하는 지식 기반 관리
3. 시스템 리소스를 가상 서비스 풀에 통합하여 보다 뛰어난 민첩성을 확보하고 기존 인프라를 활용하기 위한 가상 인프라 가상 인프라를 활용하면 시스템이 비즈니스 우선 순위와 요구에 따라 작업을 수행하기 위해 필요한 리소스를 더욱 간편하게 신속히 추가, 제외, 이동 또는 변경할 수 있습니다.

이러한 세 가지 요소는 동적 시스템 구축의 토대입니다. 가상 인프라는 인프라의 리소스를 동원하고, 지식 기반 관리는 동적 비즈니스 요구를 만족시키기 위한 작업에 이 리소스를 투입하는 메커니즘이며, 작업을 위한 설계는 탁월한 운영 능력을 발휘하는 시스템을 구축할 수 있게 합니다.

DSI에 대한 자세한 내용은 http://www.microsoft.com/dsi/를 참조하십시오.

표 7: 동적 데이터 센터의 주요 기능

|  |  |
| --- | --- |
| **기능** | **설명** |
| 광범위한 게스트 운영 체제 지원 | Hyper-V에서 지원되는 게스트 운영 체제로는 Windows Server 2008(Server Core 포함), Windows Server 2003 R2 SP2, Windows Vista SP1, Windows XP Pro SP3 및 SUSE Linux Enterprise Server 10 등이 있습니다. 이러한 운영 체제는 VMBus 하드웨어 공유 이점을 활용할 수 있으며, 관련 성능의 개선 효과도 누릴 수 있습니다.  위의 운영 체제를 지원하는 것 외에도, Hyper-V에서 실행 중인 VM은 호환 가능한 하드웨어를 폭넓게 에뮬레이트할 수 있으므로 다른 많은 게스트 운영 체제가 Hyper-V VM에서 잘 작동할 수 있습니다. |
| 사용률 카운터 | Hyper-V 사용률 카운터를 통해서 데이터 센터는 용량 계획을 효율적으로 결정하는 데 도움이 되는 가상 서버 사용률 정보를 얻을 수 있습니다. |

## 서버를 능가하는 가상화

Hyper-V는 데스크톱에서 데이터 센터까지 모든 단계를 아우르는 완벽한 가상화 솔루션의 구성 요소입니다.

* Microsoft Virtual PC 2007 기반 데스크톱 가상화를 통해 사용자는 게스트 운영 체제를 실행할 수 있습니다. 이것은 다양한 운영 체제를 필요로 하는 개발 환경에서 수직 응용 프로그램을 테스트하는 데 주로 사용됩니다. 또한 교육자는 모든 학생에게 가상 PC 파일을 배포하여 모두가 동일한 설정에서 작업하도록 할 수 있습니다.
* Microsoft SoftGrid® 응용 프로그램 가상화 기반의 응용 프로그램 가상화는 동일한 운영 체제에서 실행되는 응용 프로그램들을 분리함으로써 충돌 가능성을 없애고 신속한 구축이 가능하도록 지원합니다. 예를 들어, 주로 레지스트리를 업데이트하는 응용 프로그램은 가상 레지스트리를 업데이트하므로 시스템은 다른 응용 프로그램을 방해하지 않고 응용 프로그램 요구 사항을 만족시킬 수 있습니다. 수동으로 구성했어야 할 사용자 지정 옵션을 포함한 응용 프로그램을 일반적인 설치 및 제거 절차를 수행하는 것보다 더 빠르게 설치 및 제거할 수 있습니다.
* Microsoft 터미널 서비스를 통한 프레젠테이션 가상화 기능으로 원격 사용자가 원격 위치에서 호스팅된 응용 프로그램 및 운영 체제에 액세스할 수 있습니다. 일반적인 사용 모델은 원격 사용자가 가정에서 또는 출장 중 사무실의 데스크톱 컴퓨터나 서버 기반 응용 프로그램에 액세스하여 로컬 파일을 조작하고 데스크톱 컴퓨터에서 하드웨어에 액세스해야 하는 응용 프로그램에 로그인하고 원격지에서는 사용할 수 없던 리소스를 사용할 수 있게 합니다. 프레젠테이션 가상화를 활용하면 용량이 적은 랩톱 컴퓨터나 호환성이 없는 다른 컴퓨터, 심지어는 운영 체제가 다른 컴퓨터를 통해서 리소스 요구량이 많은 응용 프로그램을 사용할 수 있는 또 다른 이점이 있습니다. 프레젠테이션 가상화에 대해서는 이 문서의 다음 장에서 자세히 설명합니다.

## 요약

Hyper-V는 Windows Server 2008 플랫폼을 위한 비용 효율적이고 지원 기능이 풍부한 서버 가상화 기술입니다. Microsoft가 하이퍼바이저 기반의 하드웨어 지원 가상화 기술에 가져온 변화로 가상 서버의 신뢰성과 확장성이 크게 향상되어 가장 요구가 까다로운 작업조차도 동적 가상 컴퓨터에서 실행할 수 있게 되었습니다. 시스템 관리자는 Hyper-V의 산업 표준 관리 도구를 활용하여 가상 서버와 실제 서버를 이전과 유사하게 친숙하며 폭 넓게 지원되는 인터페이스를 통해 관리할 수 있습니다.

Hyper-V를 도입한 조직은 인프라, 응용 프로그램 그리고 지사 사무실의 서버 작업을 통합할 수 있습니다. Hyper-V는 데이터 센터 및 원격 위치에서의 서버 통합에 이상적이므로 조직은 하드웨어 리소스를 보다 효율적으로 사용할 수 있게 됩니다. IT 조직인 경우에는 관리 생산성을 높이고 새로운 서버를 신속하게 배포하여 변화하는 비즈니스 요구를 만족시킬 수도 있습니다. Hyper-V를 통해 기업은 테스트 및 개발 서버 팜을 통합하고 가상 컴퓨터의 구축을 자동화할 수 있습니다. 또한 Hyper-V는 하드웨어 플랫폼에서 응용 프로그램의 이식성 및 유연성을 요구하는 재해 복구 방법의 일부로 사용할 수 있습니다. 마지막으로 Hyper-V는 변화하는 요구에 대처할 수 있는 민첩성과 미래를 설계하는 능력 및 유연성을 데이터 센터에 부여합니다.

# 3장: TS RemoteApp 기반 프레젠테이션 가상화

## 소개

TS RemoteApp(터미널 서비스 RemoteApp)는 Windows Server 2008 가상화 솔루션의 또 다른 주요 구성 요소입니다. 이것은 응용 프로그램이 사용되는 지점을 실행되는 지점과 분리하므로 클라이언트는 위치에 관계 없이 어떤 응용 프로그램이든 실행할 수 있습니다. 프레젠테이션 가상화는 다양한 클라이언트 장치에 대한 응용 프로그램 배포를 가속화 및 확장함으로써 조직의 IT 구조가 뛰어난 민첩성과 대응력을 갖도록 합니다.

Windows Server 2008은 조직이 원격 사용자들로 하여금 웹 브라우저를 사용하는 응용 프로그램에 간편하게 액세스하도록 할 수 있으며 방화벽을 거쳐 원격 터미널과 응용 프로그램에 액세스할 수 있게 하는 혁신적으로 향상된 기능을 터미널 서비스에 추가합니다. 이것은 개발 비용을 절감하며 사용자의 위치에 관계 없이 일관된 응용 프로그램 환경과 성능을 보장합니다.

## 터미널 서비스 RemoteApp

터미널 서비스를 사용하면 어느 위치에서든 Windows 기반 프로그램을 실행하는 서버 또는 전체 Windows 데스크톱에 액세스할 수 있습니다. 사용자는 터미널 서버에 연결하여 프로그램을 실행하고 그 서버의 네트워크 리소스를 사용할 수 있습니다. TS 응용 프로그램과 데이터가 데이터 센터에서 활성화되면 암호화된 키보드 및 마우스 스트로크만 네트워크로 전송됩니다.

터미널 서비스 RemoteApp는 Windows Server 2008에 새로 추가된 원격 응용 프로그램 프레젠테이션 메서드입니다. RemoteApp는 터미널 서비스 프레젠테이션 메서드를 보완하여 그 창에 있는 응용 프로그램에 액세스하는 사용자에게 전체 원격 데스크톱을 제공합니다.

TS RemoteApp에서는 사용자와 원격 응용 프로그램의 상호 작용이 크게 다릅니다. 전체 원격 데스크톱과는 달리 원격 응용 프로그램은 클라이언트 컴퓨터의 데스크톱에서 크기 조정이 가능한 창을 자체적으로 시작하여 실행합니다. 프로그램이 알림 영역 아이콘을 사용하는 경우 그 아이콘은 클라이언트의 알림 영역에 나타납니다. 팝업 창은 로컬 데스크톱으로 리디렉션되며 로컬 드라이브와 프린터는 리디렉션되어 원격 프로그램에서 사용 가능하게 됩니다. 사용자는 원격 프로그램이 데스크톱의 원격 프로그램과 함께 실행되는 다른 로컬 응용 프로그램과 다르다는 사실을 인식하지 못할 수도 있습니다.

RemoteApp는 조직 전체의 여러 데스크톱에서 개별 설치를 유지 관리하는 대신 서버에 있는 하나의 중앙 응용 프로그램만 유지 관리함으로써 관리 부담을 줄입니다. 또한 사용자 환경을 개선하여 원격 응용 프로그램을 클라이언트 컴퓨터 데스크톱과 보다 유연하게 통합할 수 있습니다.

원격 프로그램을 사용하여 프로그램을 원격 실행하려면 그 프로그램을 호스팅하는 터미널 서버가 Windows Server 2008 및 Remote Desktop Connection 6.0 이상을 기반으로 해야 합니다. 터미널 서비스 세션 또는 원격 데스크톱 세션에서 실행할 수 있는 프로그램은 모두 원격 프로그램으로 실행할 수 있습니다.

## 터미널 서비스

터미널 서비스에는 Windows Server 2008 터미널 서버에 연결할 때 최종 사용자 환경을 향상시키는 새로운 핵심 기능이 포함됩니다. 새로운 핵심 기능은 다음과 같습니다.

* 원격 데스크톱 연결 6.0 이상
* 원격 데스크톱 연결은 다음과 같은 성능 개선을 표시합니다.
  + 사용자 지정 디스플레이 해상도
  + 모니터 확장
  + 데스크톱 환경
  + 데스크톱 구성
  + 글꼴 다듬기
  + 표시 데이터 우선 순위 지정
* 미디어 플레이어 및 디지털 카메라를 위한 플러그 앤 플레이 장치 리디렉션
* Windows Embedded for Point of Service 장치 리디렉션
* SSO(Single Sign-On)
* TS 세션 브로커
* TS Easy Print
* 라이선싱 개선 사항

### 원격 데스크톱 연결 6.0 이상

터미널 서비스에 액세스하려면 원격 데스크톱 연결 6.0 이상을 사용해야 합니다. 그것은 Windows Server 2008 및 Windows Vista에 들어 있으며 Windows XP 및 Windows Server 2003을 사용하는 경우에는 무료로 다운로드할 수 있습니다.

#### 원격 데스크톱 연결 표시

원격 데스크톱 연결 6.0 이상의 소프트웨어는 해상도가 더 높은 데스크톱 컴퓨터까지 지원하도록 기능이 향상되었습니다. 데스크톱 환경 기능과 표시 데이터 우선 순위 지정 설정은 Windows Server 2008 터미널 서버에 원격으로 연결할 때 최종 사용자 환경을 개선하기 위한 것입니다.

사용자 지정 디스플레이 해상도는 16:9 또는 16:10 와이드 스크린 형식과 같은 화면 해상도 비율을 추가로 지원합니다. 예를 들어, 해상도 1680 x 1050 또는 1920 x 1200인 새로운 모니터가 지원됩니다. 지원되는 최대 해상도는 4096 x 2048입니다.

#### 모니터 확장

원격 데스크톱 연결은 복수의 모니터에서 원격 데스크톱 세션을 표시할 수 있는 모니터 확장 기능도 지원합니다.

모니터 확장에 사용되는 모니터는 다음 요구 사항을 만족해야 합니다.

* 모든 모니터는 해상도가 동일해야 합니다. 예를 들어, 1024 x 768 해상도인 2개의 모니터를 확장할 수 있습니다. 그러나 하나는 1024 x 768이고 다른 하나는 800 x 600이면 확장할 수 없습니다.
* 모든 모니터는 수평으로(즉, 나란히) 정렬해야 합니다. 클라이언트에서 복수의 모니터를 수직으로 확장하는 기능은 현재 지원되지 않습니다.
* 모든 모니터의 총 해상도가 4096 x 2048을 초과할 수는 없습니다.

#### 데스크톱 환경

RDC(원격 데스크톱 연결) 6.0 이상은 사용자의 클라이언트 컴퓨터에서 원격 컴퓨터에 있는 데스크톱을 재현합니다. 데스크톱 환경이 Windows Server 2008에 설치되어 있는 경우, 사용자는 Windows Media® Player, 데스크톱 테마, 사진 관리 등의 Windows Vista 기능을 원격 연결을 통해 이용할 수 있습니다. 대역폭 사용량이 매우 많은 경우에도 키보드와 마우스를 모니터에 표시되는 내용과 동기화하도록 하여 설계된 데스크톱 환경 기능 및 표시 데이터 우선 순위 지정 설정은 Windows Server 2008 터미널 서버에 연결하는 최종 사용자 환경을 개선합니다.

Windows Vista는 Windows® Aero™라는 시각적으로 동적인 환경을 제공합니다. Windows Aero는 다음과 같은 기능을 제공합니다.

* 반투명 창
* 축소판 그림 창 미리 보기가 가능한 작업 표시줄 단추
* 데스크톱의 3차원 스택에서 열린 창 보기

Windows Vista 클라이언트 컴퓨터가 원격 데스크톱 연결을 사용하여 Windows Server 2008 터미널 서버에 연결할 때 Windows Aero 기능을 제공하도록 Windows Server 2008 터미널 서버를 구성할 수 있습니다. 이 기능을 데스크톱 구성이라고 합니다.

Windows Vista 클라이언트 컴퓨터가 원격 데스크톱 연결을 통해 Windows Server 2008 터미널 서버에 연결할 때 데스크톱 구성을 사용할 수 있도록 하려면 Windows Vista 클라이언트 컴퓨터에 Windows Aero를 지원할 수 있는 하드웨어를 설치해야 합니다. 그러나 Windows Server 2008 터미널 서버에는 Windows Aero를 지원하는 하드웨어 구성이 필요하지 않습니다.

#### 디스플레이 데이터 우선 순위 지정

디스플레이 데이터 우선 순위 지정은 가상 채널 트래픽을 자동으로 제어하므로 디스플레이, 키보드 및 마우스 데이터는 인쇄 또는 파일 전송 등의 다른 가상 채널 트래픽보다 높은 우선 순위를 가집니다. 이 우선 순위 지정 기능은 대량 인쇄 작업과 같이 대역폭을 집중적으로 사용하는 작업으로 인해 화면 성능이 저하되는 것을 방지하기 위한 것입니다.

기본 대역폭 비율은 70:30입니다. 표시 및 입력 데이터에는 대역폭의 70퍼센트가 할당되며 클립보드, 파일 전송, 인쇄 작업 등 다른 모든 트래픽에는 나머지 30퍼센트가 할당됩니다. 터미널 서버의 레지스트리를 변경하여 표시 데이터 우선 순위 설정을 조정할 수 있습니다.

#### 글꼴 다듬기

Windows Server 2008은 특히 LCD 모니터를 사용할 때 컴퓨터 글꼴이 선명하고 부드럽게 표시되도록 하는 ClearType이라는 기술을 지원합니다.

클라이언트 컴퓨터가 원격 데스크톱 연결을 통해 Windows Server 2008 터미널 서버에 연결되면 ClearType 기능이 제공되도록 Windows Server 2008 터미널 서버를 구성할 수 있습니다. 이 기능을 글꼴 다듬기라고 합니다. 글꼴 다듬기는 클라이언트 컴퓨터가 다음 중 하나를 실행하는 경우에 사용할 수 있습니다.

* Windows Vista
* Microsoft Windows Server 2003 서비스 팩 1 및 원격 데스크톱 연결 6.0 이상의 소프트웨어
* Windows XP 서비스 팩 2 및 원격 데스크톱 연결 6.0 이상의 소프트웨어

글꼴 다듬기는 클라이언트 컴퓨터의 로컬 설정에서 원격 데스크톱 연결의 사용자 환경을 결정하는 데 유용합니다. 글꼴 다듬기를 허용하더라도 Windows Server 2008 터미널 서버의 디스플레이 설정은 변경되지 않습니다.

원격 데스크톱 연결에서 글꼴 다듬기를 사용하면 클라이언트 컴퓨터와 Windows Server 2008 터미널 서버 사이에 사용되는 대역폭이 증가합니다.

### 플러그 앤 플레이 장치 리디렉션

Windows Server 2008에서는 클라이언트측 장치를 터미널 서비스 연결로 리디렉션하는 기능이 향상 및 확장되었습니다. 사용자는 Windows 기반의 휴대용 장치, 특히 MTP(미디어 전송 프로토콜) 기반의 미디어 플레이어와 PTP(사진 전송 프로토콜) 기반의 디지털 카메라를 리디렉션할 수 있습니다. 리디렉션이 지원되면 플러그 앤 플레이 장치를 사용할 수 있습니다. 원격 프로그램 마법사에 의해 생성된 원격 데스크톱 프로토콜(.rdp) 파일은 플러그 앤 플레이 장치 리디렉션을 자동으로 활성화합니다.

터미널 서버에 대한 세션이 시작되면 리디렉션된 플러그 앤 플레이가 클라이언트 컴퓨터에 자동으로 설치됩니다. 플러그 앤 플레이 알림이 클라이언트 컴퓨터의 작업 표시줄에 나타납니다. 플러그 앤 플레이 장치의 리디렉션은 Windows Vista Enterprise 및 Windows Vista Ultimate에서 Windows Vista를 실행하는 원격 컴퓨터에 연결할 때만 사용할 수 있습니다.

리디렉션된 플러그 앤 플레이 장치가 클라이언트 컴퓨터에 설치된 경우에는 플러그 앤 플레이 장치를 세션에서 사용할 수 있습니다. 예를 들어, 디지털 카메라와 같은 Windows 기반 휴대용 장치가 리디렉션된 경우에는 원격 컴퓨터의 스캐너 및 카메라 마법사와 같은 응용 프로그램에서 직접 해당 장치에 액세스할 수 있습니다.

계단식으로 배열된 터미널 서버 연결에서는 플러그 앤 플레이 장치 리디렉션이 지원되지 않습니다. 예를 들어, 플러그 앤 플레이 장치가 로컬 클라이언트 컴퓨터에 연결되어 있으면 클라이언트가 터미널 서버(예: Server1)에 연결할 때 리디렉션하여 사용할 수 있습니다. Server1의 해당 원격 세션에서 다른 터미널 서버(예: Server2)에 연결하는 경우에는 Server2를 포함한 원격 세션에서 플러그 앤 플레이 장치를 리디렉션하여 사용할 수 없습니다.

### Windows Embedded for Point of Service 장치 리디렉션

Windows Server 2008은 Microsoft POS for .NET 1.1을 사용하는 Windows Embedded for Point of Service 장치의 리디렉션도 지원합니다. Windows Embedded for Point of Service 장치에는 다기능 POS 워크스테이션, 네트워크 부팅 가능한 “씬 클라이언트” POS 터미널, 고객 관리 정보 키오스크, 자체 계산 시스템 등이 포함됩니다. 그러나 Windows Embedded for POS 장치 리디렉션은 터미널 서버가 Windows Server 2008 32비트 버전을 실행하는 경우에만 지원됩니다.

기본적으로 Microsoft POS for .NET 장치는 **원격 데스크톱 연결**의로컬 리소스탭에서로컬 장치 및 리소스 아래 열거되는 클라이언트 컴퓨터에 표시되지 않습니다. 따라서 Microsoft POS for .NET 장치의 리디렉션이 가능하도록 하려면 터미널 서버에 연결하는 데 사용되는 원격 데스크톱 프로토콜(.rdp)을 편집해야 합니다. 다음 행을 변경 또는 추가해야 합니다. redirectposdevices:i:<값>

* <값>이 0이면 Microsoft POS for .NET 장치 리디렉션이 비활성화됩니다.
* <값>이 1이면 Microsoft POS for .NET 장치 리디렉션이 활성화됩니다.

참고: 원격 프로그램 마법사에서 생성된 .rdp 파일은 Microsoft POS for .NET 장치 리디렉션을 자동으로 활성화합니다.

Microsoft POS for .NET 1.1이 터미널 서버에서 구성되고 Windows Embedded for POS 장치 리디렉션이 클라이언트 컴퓨터의 .rdp 파일에서 활성화된 후에는 Windows Embedded for point of sale 장치를 클라이언트 컴퓨터에 연결할 수 있습니다. 그런 다음 수정된 .rdp 파일을 사용하여 클라이언트 컴퓨터를 터미널 서버에 연결할 수 있습니다. 사용자가 연결하면 Windows Embedded for POS 장치가 자동으로 터미널 서버에 설치됩니다. 플러그 앤 플레이 알림도 표시됩니다.

리디렉션된 Windows Embedded for POS 장치가 터미널 서버에 설치되면 터미널 서버에 상주하는 Windows Embedded for POS 응용 프로그램은 클라이언트 컴퓨터에 실제로 연결된 Windows Embedded for POS에 액세스할 수 있습니다.

### SSO(Single Sign-On)

도메인 계정을 가진 사용자가 암호 또는 스마트 카드를 이용하여 SSO(Single Sign-On)에서 터미널 서비스 세션에 한 번 로그온한 뒤에는 자격 증명을 입력하지 않아도 원격 서버에 액세스할 수 있습니다.

기간 업무(LOB) 응용 프로그램 배포 및 중앙 집중식 응용 프로그램 배포는 SSO를 사용하는 주요 시나리오입니다. 많은 기업이 유지 관리 비용 절감을 위해서 터미널 서버에 LOB 응용 프로그램 설치를 선호하며 터미널 서비스 원격 프로그램 또는 원격 데스크톱을 통해 이 응용 프로그램을 이용할 수 있도록 하고 있습니다. SSO를 사용하면 사용자가 원격 세션을 초기화할 때마다 자격 증명을 입력할 필요가 없으므로 보다 나은 사용자 환경을 제공할 수 있습니다.

원격 연결을 위한 SSO는 Windows Server 2008 터미널 서버에 연결된 Windows Vista 기반 컴퓨터 또는 다른 Windows Server 2008 서버에 연결된 Windows Server 2008 서버에서만 사용할 수 있습니다. 로그온에 사용되는 사용자 계정은 터미널 서버와 Windows Vista 클라이언트 모두에 대한 로그온 권한이 있어야 하며, 클라이언트 컴퓨터와 터미널 서버가 도메인에 가입되어야 합니다.

### TS 세션 브로커

TS 세션 브로커는 터미널 서비스를 위한 Microsoft 네트워크 부하 분산보다 간편한 대안을 제공하는 Windows Server 2008의 새로운 기능입니다. 이 기능은 서버의 수를 제한하지 않는 한편 2-5개 서버로 구성된 팜에 중요한 이점을 제공합니다. TS 세션 브로커를 사용하면 새로운 세션은 팜 안에서 부하가 가장 적은 서버로 분산됩니다. 이것은 성능을 최적화할 뿐 아니라, 사용자는 세션이 구성된 서버에 관한 정보를 모르더라도 기존 세션에 다시 연결할 수 있습니다. IT 관리자는 이 기능을 사용하여 각 터미널 서버의 IP(인터넷 프로토콜) 주소를 단일 DNS(Domain Name System) 항목에 매핑할 수 있습니다. 이 구성은 내결함성도 제공할 수 있습니다. 즉, 팜 서버 중 하나를 사용할 수 없게 되면 사용자는 팜에서 다음으로 부하가 가장 적은 서버에 연결됩니다.

### 인쇄 기능 향상

Windows Server 2008에서는 터미널 서비스 인쇄의 성능과 확장성이 향상되었습니다. 여기에는 리디렉션된 프린터를 원격 세션에 훨씬 신속하게 설치할 수 있다는 점과 Windows Server 2008 터미널 서버 하나가 많은 수의 리디렉션된 클라이언트 컴퓨터를 처리할 수 있다는 장점이 포함됩니다.

### TS Easy Print

Windows Server 2008에 새로 추가된 TS Easy Print는 TS RemoteApp 또는 전체 데스크톱 세션에서 클라이언트 컴퓨터에 설치된 로컬 또는 네트워크 프린터로 안전하게 인쇄할 수 있는 기능입니다. 이제는 터미널 서버에 인쇄 드라이버를 설치하지 않아도 프린터로 인쇄할 수 있습니다. TS RemoteApp 프로그램 또는 데스크톱 세션에서 인쇄하려는 경우에는 로컬 클라이언트에서 전체 프린터 속성 대화 상자(프린터 사용자 인터페이스)를 보면서 모든 프린터 기능에 액세스할 수 있습니다. IT 관리자는 여러 프린터에 리디렉션을 허용하는 대신 기본 프린터로 리디렉션되는 프린터 수를 제한하는 그룹 정책을 사용함으로써 경비를 절감하고 확장성을 개선할 수 있습니다.

### 라이선싱 개선 사항

터미널 서버 라이선싱은 Windows Server 2008의 터미널 서비스 클라이언트를 위한 클라이언트 라이선스 관리 서비스입니다. 터미널 서버 라이선싱 서비스는 터미널 서버와 함께 동작하여 터미널 서버 클라이언트에 라이선스 정책을 제공, 분류 및 시행합니다.

Windows Server 2008의 터미널 서비스 라이선싱은 사용자별 추적 및 보고, 라이선스 수동 해지, WMI 공급자에 대한 진단 및 지원 기능 개선 등과 같이 라이선싱 환경의 배포와 관리를 개선할 수 있는 새로운 기능을 포함합니다.

새로운 기능 또는 향상된 기능에는 다음이 포함됩니다.

* 터미널 서비스 장치 단위 클라이언트 액세스 라이선스 - 터미널 서비스 라이선스(TS 라이선스)는 사용자가 하나의 장치를 사용하여 조직의 서버에서 Windows 세션을 수행할 수 있도록 하는 터미널 서비스 장치 단위 클라이언트 액세스 라이선스(TS 장치 단위 CAL)를 허용합니다.
* 터미널 서비스 사용자 단위 클라이언트 액세스 라이선스 - 터미널 서비스 사용자 단위 클라이언트 액세스 라이선스(TS 사용자 단위 CAL)는 장치를 사용하는 한 사용자가 조직의 서버에서 Windows 세션을 수행하도록 허용합니다.

Windows Server 2008의 TS 라이선스에는 TS 라이선스 관리 도구를 사용하여 TS 사용자 단위 CAL 발행을 추적할 수 있는 기능이 포함되어 있습니다. 터미널 서버가 사용자 단위 라이선스 모드인 경우 여기에 연결된 사용자는 TS 사용자 단위 CAL을 갖고 있어야 합니다. 사용자에게 필요한 TS 사용자 단위 CAL이 없는 경우에는 터미널 서버가 라이센스 서버에 접촉하여 사용자 대신 CAL을 가져오게 합니다. 라이선스 서버가 사용자에게 TS 사용자 단위 CAL을 발행한 후 관리자는 TS 라이선스 관리 도구를 사용하여 CAL 발행을 추적할 수 있습니다. 또한 IT 직원은 WMI(Windows Management Instrumentation) 스크립트를 사용하여 라이선스 추적 보고서를 생성할 수 있습니다.

#### 터미널 서비스 라이선스 서버(TS 라이선스)

Windows Server 2008은 터미널 서비스 라이선스 서버도 사용합니다. 터미널 서비스 라이선스 서버는 TS 라이선스 역할 서비스가 설치된 컴퓨터입니다. 라이선스 서버는 터미널 서버 그룹을 위해 설치된 모든 TS CAL 토큰을 저장하며 발행된 라이선스 토큰을 추적합니다. 라이선스 서버 하나가 여러 터미널 서버를 동시에 관리할 수 있습니다. 클라이언트 장치에 영구적인 라이선스 토큰을 발행하려면 활성화된 라이선스 서버에 터미널 서버가 연결할 수 있어야 합니다. 설치되었지만 활성화되지 않은 라이선스 서버는 임시 라이선스 토큰만 발행합니다.

Windows Server 2008에는 다음과 같은 두 종류의 라이선스 서버(이전 명칭은 역할)가 있습니다.

* 도메인 라이선스 서버
* 포리스트 라이선스 서버(이전 명칭은 "엔터프라이즈")

TS 라이선스를 이용하려면 조직은 다음 사전 요구 사항을 만족해야 합니다.

* IT 직원은 Windows Server 2008을 실행하는 서버에 TS 라이선스 역할 서비스를 설치해야 합니다.
* TS 사용자 단위 CAL 추적 및 보고는 터미널 서버와 라이선스 서버가 도메인의 구성원인 도메인 참여 시나리오에서만 지원되며 작업 그룹 모드에서는 지원되지 않습니다. Active Directory® 도메인 서비스는 사용자 단위 모드에서 라이선스 추적에 사용됩니다. Active Directory 도메인 서비스는 Windows Server 2008 기반일 수도 있고 Windows Server 2003 기반일 수도 있습니다. *참고*: Active Directory 도메인 서비스 스키마에는 TS 사용자 단위 CAL 추적 및 보고를 구현하기 위한 업데이트가 필요하지 않습니다.
* Windows Server 2008을 실행하는 터미널 서버는 Windows Server 2003을 실행하는 라이선스 서버와 통신하지 않습니다. 그러나 Windows Server 2003을 실행하는 터미널 서버는 Windows Server 2008 라이선스 서버와 통신할 수 있습니다.

#### 사용자 단위 추적 및 보고

Windows Server 2008 이전까지는 사용자 단위 라이선스가 발행되지 않았습니다. 이전에는 사용자 단위 라이선스 사용이 최종 사용자 사용권 계약(EULA) 또는 기타 라이선스 계약과 일치하는지 추적하기가 쉽지 않았습니다. Windows Server 2008부터는 IT 그룹이 사용률을 간편하게 추적하고 사용자 단위 라이선스 발행 보고서를 생성할 수 있습니다. 보고서는 라이선스 관리자 UI뿐 아니라 WMI 공급자를 통해서도 액세스할 수 있습니다.

*참고*: 사용자 단위 라이선스는 추적만 할 수 있을 뿐 시행할 수는 없습니다.

#### 라이선스 해지

라이선스를 해지하고 다른 곳에서 즉시 사용할 수 있게 하려는 고객도 있었지만 이전에는 클라이언트에게 발행된 라이선스를 해지할 수 없었습니다. 발행된 라이선스는 52-89일 사이의 임의의 기간 후 자동으로 만료되어 사용 가능한 라이선스 풀의 일부가 되었습니다. Windows Server 2008에서는 라이선스를 해지하여 즉시 사용 가능한 상태로 만들 수 있습니다\*. Windows Server 2008의 라이선스 관리자 UI 또는 새 WMI 공급자를 통해 IT 전문가는 특정 클라이언트 컴퓨터에 발행된 장치 단위 CAL을 선택하여 해지할 수 있습니다.

\**참고*: 한 번에 특정 CAL 버전의 20%만 해지할 수 있습니다.

## 터미널 서비스 게이트웨이(TS 게이트웨이)

터미널 서비스 게이트웨이는 권한 있는 원격 사용자가 인터넷을 통해 기업 네트워크의 터미널 서버와 워크스테이션에 연결할 수 있도록 하는 터미널 서비스 역할입니다. 따라서 조직은 선택된 서버와 워크스테이션을 원격 사용자나 출장 중인 직원이 VPN 연결 없이 간편하고 안전하게 사용하도록 만들 수 있습니다.

TS 게이트웨이의 주요 이점은 다음과 같습니다.

* 원격 사용자는 VPN(가상 사설망)을 복잡하게 연결하지 않고 인터넷에서 기업 네트워크의 리소스에 안전하게 연결할 수 있습니다. 사용자가 VPN을 통해 전체 기업 네트워크에 연결하는 대신 선택된 서버와 워크스테이션에만 액세스할 수 있게 함으로써 더욱 안전한 모델을 제공합니다.
* 클라이언트 구성 없이 HTTPS 프로토콜의 보안성과 가용성을 이용하여 터미널 서비스를 제공합니다.
* 관리자가 네트워크의 특정 리소스에 대한 액세스를 제어할 수 있는 포괄적인 보안 구성 모델을 제공합니다.
* 사용자는 방화벽과 NAT(네트워크 주소 변환기)를 통해 터미널 서버와 원격 워크스테이션에 원격으로 연결할 수 있습니다.
* TS 게이트웨이는 일반적으로 포트 3389를 통해 전송된 모든 RDP 트래픽을 HTTP SSL(Secure Sockets Layer) 터널을 사용하여 포트 443으로 전송합니다. 즉, 사용자의 클라이언트 컴퓨터와 TS 게이트웨이 사이의 모든 트래픽이 인터넷 전송 과정에서 암호화됩니다.

### TS 게이트웨이 관리

TS 게이트웨이 관리 스냅인 콘솔 관리자는 사용자가 네트워크를 통해 리소스에 연결하기 위해 준수해야 할 정책을 구성할 수 있습니다. TS 게이트웨이 관리 스냅인 콘솔은 관리자가 TS 게이트웨이 이벤트를 모니터링하는 데 유용한 도구를 제공합니다. 사용자는 TS 게이트웨이 관리를 사용하여 모니터링하려는 TS 게이트웨이 서버에 대한 연결 시도 실패와 같은 이벤트를 지정할 수 있습니다. 이 이벤트가 발생하면 이벤트 뷰어를 사용하여 해당 이벤트를 모니터링할 수 있습니다.

또한 TS 게이트웨이 관리를 통해 IT 직원은 활성화된 사용자 연결에 대한 세부 정보를 확인하고 최대 연결 제한을 설정하며 TS 게이트웨이 서버를 통한 네트워크 리소스 액세스를 제어하기 위한 다른 조치를 취할 수 있습니다.

조직은 터미널 서비스 게이트웨이를 사용함으로써 원격 사용자가 VPN 연결을 설치 및 구성하지 않고도 안전하고 간편하게 네트워크의 서비스와 워크스테이션에 액세스하도록 할 수 있습니다. 또한 포괄적인 보안 기능을 통해 관리자는 특정 리소스에 대한 액세스를 제어할 수 있습니다.

### TS 게이트웨이 기능

Windows Server 2008의 TS 게이트웨이는 관리를 간소화하고 보안성을 개선하기 위한 여러 가지 새로운 기능을 제공합니다.

#### CAP(연결 권한 부여 정책)

관리자는 CAP(연결 권한 부여 정책)를 이용하여 TS 게이트웨이 서버에 액세스할 수 있는 사용자, 사용자 그룹 및 컴퓨터 그룹(선택적)을 지정할 수 있습니다. TS 게이트웨이 관리를 통해 CAP가 생성됩니다. CAP는 기업 네트워크의 원격 컴퓨터에 대한 액세스를 더 높은 수준으로 제어함으로써 관리를 간소화하고 보안성을 개선합니다.

CAP를 사용하는 관리자는 사용자, 사용자 그룹 또는 컴퓨터 그룹이 TS 게이트웨이 서버에 대한 특정 액세스 조건을 만족하도록 요구할 수 있습니다. 각 CAP마다 구체적인 조건을 열거할 수 있습니다. 예를 들어, 관리자는 스마트 카드 사용과 같은 연결 요구 사항을 지정할 수 있으며, 기업 네트워크의 리소스에 연결할 수 있는 특정 사용자 그룹, 사용자가 연결할 수 있는 특정 리소스, 특정 사용자 그룹 구성원 요구 사항 등을 정의할 수 있습니다. 사용자는 자신의 그룹 이름을 포함한 CAP에 지정된 조건을 만족하는 경우에만 TS 게이트웨이 서버에 액세스할 수 있습니다.

#### 리소스 그룹 및 RAP(리소스 권한 부여 정책)

CAP를 정의한 후에는 리소스 그룹을 생성하고 TS 게이트웨이 서버에서 네트워크의 특정한 원격 컴퓨터에 대한 사용자 액세스를 허용하는 RAP(리소스 권한 부여 정책)를 정의해야 합니다. CAP와 RAP는 TS 게이트웨이 관리 콘솔을 사용하여 생성 및 관리됩니다.

관리자는 리소스 그룹을 사용하여 사용자가 액세스할 수 있는 원격 컴퓨터 그룹을 정의할 수 있습니다. RAP를 이용하면 리소스 그룹에 대한 사용자 액세스를 관리할 수 있습니다. TS 게이트웨이 서버를 통해서 네트워크에 연결하는 사용자는 적어도 하나의 RAP에 명시된 조건을 만족하는 경우에만 네트워크 상의 특정 원격 컴퓨터에 대한 액세스가 허용됩니다. 리소스 그룹을 수동으로 생성하는 대신 Active Directory 디렉터리 서비스에서 보안 그룹을 정의하여 액세스 조건 관리에 사용할 수 있습니다.

네트워크 상의 올바른 원격 컴퓨터에 올바른 사용자가 액세스하도록 하려면 관리자는 리소스 그룹을 신중하게 계획하고 생성해야 합니다. 각 리소스 그룹에 어떤 사용자가 액세스할 수 있는지 확인하기 위한 평가가 필요합니다. 그런 다음에는 필요에 따라 사용자 액세스를 허용하기 위해 하나 이상의 RAP를 생성해야 합니다.

#### 모니터링 기능

TS 게이트웨이 관리는 TS 게이트웨이를 통해 클라이언트에서 네트워크 상의 원격 컴퓨터로 활성 연결에 대한 정보를 볼 수 있는 기능을 제공합니다. 이 정보에는 클라이언트의 IP 주소, 클라이언트에 로그온한 사용자의 이름, 클라이언트가 연결된 원격 컴퓨터의 이름 그리고 연결이 유휴 상태인 시간(그러한 경우) 등이 포함됩니다. 또한 관리자는 모니터링하려는 이벤트를 지정한 후 이벤트 뷰어를 사용하여 이 이벤트를 모니터링할 수도 있습니다.

#### NAP(네트워크 액세스 보호)와의 통합

TS 게이트웨이는 NAP(네트워크 액세스 보호)와의 통합으로 Windows Server 2008의 보안성을 높입니다. IT 전문가는 TS 게이트웨이 서버와 클라이언트가 NAP를 이용하도록 구성할 수 있습니다. 그런 시나리오에서 네트워크 보안 요구 사항을 만족하지 않는 컴퓨터를 사용하여 터미널 서버에 액세스하려는 원격 사용자는 TS 게이트웨이에 의해 터미널 서버 액세스를 거부 당하게 됩니다.

NAP는 상태 정책을 만들고 적용하며 수정하는 기술로, Windows Vista 및 Windows Server 2008에 포함되어 있습니다. 시스템 관리자는 TS 게이트웨이 서버에 연결하는 터미널 서비스 클라이언트에 대해 NAP를 사용하여 상태 요구 사항을 시행할 수 있습니다. NAP를 사용하는 IT 직원은 터미널 서비스 클라이언트가 TS 게이트웨이 서버를 통해 기업 네트워크의 컴퓨터에 연결하기 전에 조직의 상태 정책 요구 사항을 만족하는지 확인하는 데 도움을 줄 수 있습니다. NAP에 대한 자세한 내용은 5장: 보안 및 규정 준수를 참조하십시오.

*참고*: TS 터미널에는 NAP 기술이 적용되지 않습니다.

## 터미널 서비스 웹 액세스

TS 웹 액세스(터미널 서비스 웹 액세스)는 사용자가 다른 소프트웨어를 설치하지 않고도 웹 브라우저에서 터미널 서비스 RemoteApp 프로그램을 사용할 수 있도록 관리자가 설정하는 터미널 서비스 역할입니다. 사용자는 TS 웹 액세스를 통해 웹 사이트를 방문하여 사용 가능한 응용 프로그램 목록에 액세스할 수 있습니다. 목록에 나열된 프로그램 중 하나를 시작하면 이 응용 프로그램을 호스팅하는 Windows Server 2008 기반 터미널 서버에서 그 사용자에 대한 터미널 서비스 세션이 자동으로 시작됩니다. 이 웹 인터페이스는 현재 사용 가능한 모든 원격 응용 프로그램을 보여주는 중앙 집중식 메뉴를 사용자에게 제공합니다. 원격 응용 프로그램을 실행하려면 메뉴에서 프로그램을 선택하기만 하면 됩니다.

TS 웹 액세스를 Windows Server 2008 웹 서버에 설치한 후 사용자는 TS 웹 액세스 서버에 연결하여 하나 이상의 Windows Server 2008 기반 터미널 서버에서 사용 가능한 원격 프로그램에 액세스할 수 있습니다. TS 웹 액세스의 이점은 다음과 같습니다.

* 사용자는 인터넷 또는 인트라넷을 통해 웹 사이트에서 원격 프로그램에 액세스할 수 있습니다. 원격 프로그램을 시작하려면 프로그램 아이콘을 클릭하기만 하면 됩니다.
* 원격 프로그램을 사용할 때는 로컬 컴퓨터에서 실행할 때처럼 나타납니다.
* 사용자가 동일한 터미널 서버에서 실행되고 있는 하나 이상의 원격 프로그램을 열면 그 프로그램들은 동일한 터미널 서비스 세션에서 실행됩니다.
* TS 웹 액세스를 사용하면 관리 오버헤드를 크게 줄일 수 있습니다. 프로그램을 중앙 위치에서 쉽게 배포할 수 있습니다. 프로그램은 클라이언트 컴퓨터가 아닌 터미널 서버에서 실행되므로 서버 유지 관리가 더욱 간편합니다.
* TS 웹 액세스는 최소한의 구성으로 동작하는 솔루션을 제공합니다. TS 웹 액세스 웹 페이지에는 사용자 지정된 웹 페이지 또는 Windows SharePoint® Services 사이트에 통합할 수 있는 사용자 지정 가능한 웹 파트가 포함됩니다.
* 그룹 정책 소프트웨어 배포를 사용하여 원격 프로그램을 배포한 경우 터미널 서비스 원격 프로그램 웹 파트에 나타나는 사용 가능한 프로그램 목록을 개별 사용자에 맞게 사용자 지정할 수 있습니다.
* 또한 TS 웹 액세스를 사용하여 전체 데스크톱에 대한 액세스를 제공할 수도 있습니다.

TS 웹 액세스를 사용하면 관리 오버헤드가 줄어듭니다. 중앙 위치에서 쉽게 프로그램에 액세스할 수 있습니다. 프로그램은 클라이언트 컴퓨터가 아닌 터미널 서버에서 실행되므로 IT 직원은 단일 지점에서 응용 프로그램을 유지 관리 및 업데이트할 수 있습니다.

### 향상된 웹 환경

TS 웹 액세스는 터미널 서비스의 이전 버전에 비해 크게 개선된 웹 환경을 제공합니다. 이러한 개선에는 다음이 포함됩니다.

* TS 웹 액세스를 사용하면 원격 프로그램을 시작하기 위해 RDC(원격 데스크톱 연결) 클라이언트를 시작할 필요가 없습니다. 대신 웹 페이지에 액세스한 후 프로그램 아이콘을 클릭하기만 하면 됩니다.
* 원격 프로그램은 로컬 데스크톱에서 실행하는 것처럼 보입니다.
* 사용자가 동일한 터미널 서버의 여러 프로그램을 시작한 경우 그 프로그램들은 모두 동일한 터미널 서비스 세션에서 실행됩니다.
* 따라서 TS 웹 액세스에 액세스하기 위해 별도로 ActiveX® 컨트롤을 다운로드할 필요가 없습니다. 대신 RDP 클라이언트 버전 6.0 이상에는 필요한 ActiveX 컨트롤이 포함되어 있습니다.

### TS 원격 프로그램 목록의 동적 업데이트

TS 웹 액세스가 배포되면 터미널 서비스 원격 프로그램 웹 파트에 나타나는 원격 프로그램 목록이 동적으로 업데이트됩니다. 이 목록은 단일 터미널 서버의 허용 목록으로 채워집니다.

관리자는 원격 프로그램 목록을 채우는 데 사용될 데이터 소스를 지정할 수 있습니다. 데이터 소스가 단일 터미널 서버인 경우에는 그 서버의 허용 목록에서 웹 액세스가 가능하도록 구성된 모든 원격 프로그램으로 웹 파트가 채워집니다. 웹 파트에 표시되는 프로그램 목록은 현재 사용자에게만 해당되는 것이 아닙니다.

동적으로 업데이트되는 프로그램 목록과 원격 프로그램 데이터 소스를 지정할 수 있는 기능을 이용하여 웹을 통한 원격 프로그램 배포를 간소화할 수 있습니다. 터미널 서버가 하나뿐인 경우에는 터미널 서버 데이터 소스를 이용하여 프로그램을 간단히 배포할 수 있습니다. 터미널 서비스의 이전 버전에서는 원격 프로그램 목록으로 웹 사이트를 동적 업데이트할 수 있는 메커니즘이 지원되지 않았습니다.

### 터미널 서비스 원격 프로그램 웹 파트

TS 웹 액세스는 사용자 지정 가능한 터미널 서비스 원격 프로그램 웹 파트를 제공하며, 여기에 원격 프로그램 목록이 표시됩니다. 다음 중 한 가지 방법을 사용하여 웹 파트를 배포할 수 있습니다.

* TS 웹 액세스 웹 페이지의 일부로 원격 프로그램 웹 파트를 배포합니다. (이것이 간편한 기본 솔루션입니다.)
* 사용자 지정된 웹 페이지의 일부로 웹 파트를 배포합니다.

TS 웹 액세스는 유연하고 간편한 솔루션을 제공합니다. 제공된 TS 웹 액세스 웹 페이지와 웹 파트를 이용하여 TS 웹 액세스 사이트를 신속 간편하게 구현할 수 있으며, 사용자는 웹 페이지를 이용하여 TS 웹 액세스를 배포할 수 있습니다.

## 요약

Microsoft는 Windows Server 2008의 터미널 서비스를 통해 가장 강력한 프레젠테이션 가상화 플랫폼을 내놓았습니다. 터미널 서비스는 터미널 서비스를 사용하여 배포 및 관리되는 응용 프로그램에 대한 관리자와 사용자의 환경을 획기적으로 개선하는 여러 가지 새로운 기능을 제공합니다. Windows Server 2008은 중앙에서 관리되는 응용 프로그램과 리소스를 "어느 위치에서나 액세스"할 수 있도록 보안성이 향상되고 관리하기 간편한 플랫폼을 제공하여 터미널 서비스의 성능을 개선합니다.

TS RemoteApp를 이용한 프레젠테이션 가상화를 통해 원격 연결을 간소화함으로써 웹 페이지에서 다양한 응용 프로그램에 액세스하고 로컬 데스크톱과 원활하게 통합할 수 있도록 하여 원격 작업자의 효율을 개선합니다. 터미널 서비스 프레젠테이션 가상화는 조직이 중요한 지적 재산을 안전하게 보호하는 데 도움이 됩니다. 또한 응용 프로그램과 데이터를 데스크톱에서 제거하여 규정 준수를 용이하게 합니다.

# 4장: 원격 위치

## 소개

기업은 고객에게 더 가까이 가려 하고, 작업자는 중앙 위치에서 지사 사무실 같은 원격 위치로 점점 옮겨가고 있습니다. 원격 위치의 수가 점점 증가하는 가운데 이에 대한 IT 관리 요구 및 보안 과제 역시 증가하고 있습니다. Microsoft는 빠른 속도로 증가하는 이 분야의 인력을 비롯하여 지사 사무실 고유의 과제를 해결하기 위한 새로운 솔루션의 필요성을 인식하고 있습니다.

원격 위치에는 IT 직원이 거의 또는 전혀 없기 때문에 이 위치의 서버들은 IT 관리자에게 여러 가지 우려를 주고 있습니다. 서버에서 실행되는 소프트웨어는 속도가 느린 WAN 연결을 효과적으로 이용함으로써 전체 대역폭을 소모하지 않고 중요한 데이터 전송 속도를 늦추지 않으며 원격 위치의 사용자들에게도 성능 저하가 없는 응용 프로그램 환경을 제공해야 합니다. 서버의 물리적 보안을 항상 보장할 수는 없기 때문에 보안은 원격 위치에서 더욱 큰 관심사가 되었습니다. IT 직원 대부분이 현장에 없기 때문에 중앙 집중식 관리뿐 아니라 원격 관리와 배포까지 제공하는 서버 솔루션이 선호됩니다.

Microsoft는 Microsoft Windows Server 2003 R2에서 이러한 과제를 해결하기 시작했습니다. Windows Server 2008에는 관리자가 원격 위치를 보다 잘 제어하고 원격 사이트와 조직의 중앙 네트워크 및 데이터에 대한 보호 수준을 향상시킬 수 있는 다양한 기능이 추가되었습니다. 또한 조직 고유의 요구를 만족시킬 필요가 있는 IT 전문가를 위해 더욱 뛰어난 유연성을 제공합니다.

Windows Server 2008이 원격 위치에 제공할 수 있는 주요 이점은 다음 세 가지 범주로 구분할 수 있습니다.

* 원격 서버 배포와 관리의 효율성 개선
* 지사 사무실과 같은 원격 위치의 보안 위험 감소
* WAN 통신 및 대역폭 활용의 효율성 개선

Windows Server 2008은 주요 서버 역할에 대한 배포 간소화와 관리 효율성 개선, 보안성 강화, 성능을 최적화하고 서비스 연속성을 제공하는 아키텍처 등을 통해 다양한 신규 기능과 기능 향상으로 원격 위치의 근본적인 요구를 해결합니다.

## 배포 및 관리

원격 위치의 서버, 서비스 및 보안 관리는 IT 전문가의 과제입니다. Windows Server 2008은 지사 사무실에 있는 서버의 원격 배포와 관리를 간소화합니다. 다음을 포함한 여러 가지 새로운 기능과 기능 향상이 지사 사무실의 요구와 우려를 직접 해결합니다.

* Active Directory의 관리 효율성 향상
* RODC(읽기 전용 도메인 컨트롤러) 도입
* BitLocker
* 역할 구분
* Server Core

### Active Directory의 관리 효율성 향상

Windows Server 2008의 AD DS(Active Directory 도메인 서비스)에는 도메인 서비스 관리를 간소화하고 관리자가 원격 위치의 요구를 더욱 유연하게 해결할 수 있는 기능 향상이 포함되어 있습니다. 기본적인 몇 가지 관리 기능 향상은 다음과 같습니다.

* AD DS 설치 프로세스를 간소화하는 업데이트된 AD DS 설치 마법사
* AD DS 관리에 사용되는 MMC(Microsoft Management Console) 기능 변경
* 도메인 컨트롤러의 새 설치 옵션
* AD DS의 인터페이스 및 관리 옵션 향상
* 기업 네트워크 전체에서 도메인 컨트롤러를 검색할 수 있는 도구 기능 향상

Windows Server 2008에 제공되는 이 AD DS 인터페이스 기능 향상은 초기 배포를 합리화하고 지사 사무실에서의 서버 관리를 간소화함으로써 IT 관리 시간을 단축할 것입니다.

### RODC(읽기 전용 도메인 컨트롤러)

RODC(읽기 전용 도메인 컨트롤러)는 Windows Server 2008 운영 체제에 새로 추가된 도메인 컨트롤러 유형입니다. RODC를 이용하면 빠르고 믿을 수 있으며 강력한 인증 서비스를 필요로 하는 지사 사무실에서 보다 안전하게 도메인 컨트롤러를 배포할 수 있습니다.

RODC는 주로 원격 위치 및 지사 사무실 환경에서 배포하도록 설계되었습니다. 원격 사이트에는 비교적 사용자 수가 적고 물리적 보안 수준이 낮으며 허브 사이트 연결을 위한 네트워크 대역폭이 비교적 부족하고 로컬 IT 지식 기반도 취약한 경우가 많습니다. 실제 보안 수준이 적절치 않다는 점이 RODC의 배포를 고려하게 되는 가장 일반적인 이유입니다. 그러나 조직은 특수한 관리 요구를 위해 RODC 배포를 선택할 수도 있습니다.

원격 위치는 속도가 느린 WAN 링크를 통해 연결된 사용자에게 Active Directory 도메인 서비스를 제공해야 하는 네트워크 관리자에게 여러 가지 과제를 부여합니다. 로컬 도메인 컨트롤러가 없기 때문에 WAN 링크의 제한으로 인해 로그온, 그룹 정책 처리 및 네트워크 서비스 액세스에 지연이 발생할 수 있습니다. 한편 원격 위치에서 도메인 컨트롤러 배포 및 유지 관리를 지원할 로컬 IT 직원이 현장에 없고 서버의 물리적 보안이 보장되지 않는 경우에는 중대한 문제가 될 수 있습니다. RODC는 다음 기능을 통해 이러한 문제를 해결합니다.

* 읽기 전용 Active Directory 데이터베이스
* 단방향 복제
* 자격 증명 캐싱
* 관리자 역할 분리
* 새 MMC 스냅인 기능

#### 읽기 전용 Active Directory 데이터베이스

RODC는 쓰기 가능한 도메인 컨트롤러가 보유한 Active Directory 개체와 특성 중에서 계정 암호를 제외한 모든 것을 갖고 있습니다. 그러나 RODC에 저장된 복제본을 변경하는 것은 불가능합니다. 이것은 지사 사무실에서 발생할 수 있는 변경으로 인해 포리스트가 손상되지 않도록 하기 위한 것입니다. 디렉터리에 대한 읽기 액세스를 요청하는 로컬 응용 프로그램은 액세스 권한을 취득할 수 있습니다. 읽기 액세스를 요청하는 LDAP(Lightweight Directory Application Protocol) 응용 프로그램은 일반적으로 허브 사이트에 있는 쓰기 가능한 도메인 컨트롤러로 안내하는 LDAP 추천 응답을 받게 됩니다.

#### 단방향 복제

변경 사항은 RODC에 직접 작성되지 않으므로 RODC에서는 변경이 발생될 수 없습니다. 따라서 복제 파트너인 쓰기 가능한 도메인 컨트롤러는 RODC에서 변경 사항을 가져올 필요가 없습니다. 결과적으로 허브에 있는 브리지헤드 서버의 작업 부하와 복제를 모니터링할 필요성이 줄어듭니다. RODC 단방향 복제는 AD DS와 DFS(분산 파일 시스템) 복제에 모두 적용됩니다. RODC는 AD DS와 DFS 복제 변경에 대해 정상적인 인바운드 복제를 수행합니다. WAN 링크를 이용하여 중앙 서버에 연결하는 지사 사무실에서는 Windows Server 2008에서 단방향 복제를 통해 원격 위치와 허브 사이트 사이의 대역폭 사용을 최적화할 수 있습니다.

#### 자격 증명 캐싱

자격 증명 캐싱은 사용자 또는 컴퓨터 자격 증명의 저장소입니다. 자격 증명이란 보안 원칙(사용자 및 컴퓨터 계정)과 연결된 소규모의 암호 집합입니다. 기본적으로 RODC는 사용자 또는 컴퓨터 자격 증명을 저장하지 않습니다. 그러나 RODC의 컴퓨터 계정과 각 RODC가 가진 Kerberos TGT(Ticket-Granting Ticket)(*krbtgt)* 계정은 예외입니다. 관리자는 RODC의 다른 자격 증명 캐싱을 명시적으로 허용해야 합니다.

RODC는 지사 사무실을 위한 KDC(키 배포 센터)로 보급되고 있습니다. RODC는 TGT(Ticket-Granting Ticket) 요청에 서명하거나 요청을 암호화할 때 쓰기 가능한 도메인 컨트롤러에서 KDC가 사용하는 것과 다른 krbtgt 계정과 암호를 사용합니다.

계정 인증이 성공하면 RODC는 허브 사이트에서 쓰기 가능한 도메인 컨트롤러와 접촉을 시도하고 필요한 자격 증명 사본을 요청합니다. 쓰기 가능한 도메인 컨트롤러는 요청이 RODC에서 수신되고 있음을 인식하고 그 RODC에 유효한 암호 복제 정책을 확인합니다.

암호 복제 정책은 사용자 또는 컴퓨터의 자격 증명을 쓰기 가능한 도메인 컨트롤러에서 RODC로 복제할 수 있는지 여부를 결정합니다. 암호 복제 정책이 이를 허용하는 경우 쓰기 가능한 도메인 컨트롤러는 자격 증명을 RODC로 복제하며 복제된 자격 증명은 RODC의 캐시에 저장됩니다.

자격 증명이 RODC 캐시에 저장된 후 RODC는 자격 증명이 변경될 때까지 그 사용자의 로그온 요청을 직접 처리합니다. RODC의 krbtgt 계정을 사용하여 TGT에 서명하면 RODC는 해당 자격 증명의 캐시 복사본이 있음을 인식하게 됩니다. 다른 도메인 컨트롤러가 TGT에 서명한 경우 RODC는 쓰기 가능한 도메인 컨트롤러에 요청을 전달합니다.

자격 증명 캐싱을 RODC 인증을 받은 사용자로만 제한함으로써 RODC 훼손에 따른 자격 증명 노출 위험도 줄어듭니다. 이것은 일반적으로 소수의 도메인 사용자 하위 집합만이 특정 RODC의 캐시에 자격 증명을 저장하기 때문입니다. 따라서 RODC가 훼손되면 캐시에 저장된 자격 증명만 훼손될 것입니다.

자격 증명 캐싱을 사용하지 않는다면 노출을 더욱 제한할 수 있겠지만, 이 경우에는 모든 인증 요청을 속도가 더 느린 WAN 링크를 통해 쓰기 가능한 도메인 컨트롤러에 전달하는 결과가 될 것입니다. 관리자는 사용자의 자격 증명을 RODC 캐시에 저장하도록 기본 암호 복제 정책을 수정할 수 있습니다.

RODC가 배포되면 그 복제 파트너가 될 암호 복제 정책을 쓰기 가능한 도메인 컨트롤러에 구성해야 합니다. 암호 복제 정책은 ACL(액세스 제어 목록)의 역할을 합니다. 이것은 RODC가 암호를 캐시에 저장하도록 허용해야 하는지 여부를 결정합니다. RODC가 인증된 사용자 또는 컴퓨터 로그온 요청을 수신한 후에는 암호 복제 정책을 참조하여 해당 계정의 암호를 캐시에 저장해야 하는지 여부를 결정합니다. 동일한 계정으로 다음에 다시 로그온할 때부터는 더욱 효율적으로 처리할 수 있습니다.

암호 복제 정책은 캐싱이 허용된 계정과 캐싱이 명시적으로 거부된 계정을 나열합니다. 캐싱이 허용된 사용자와 컴퓨터 계정 목록이라 해도 RODC가 그 계정의 암호를 반드시 캐시에 저장했다고 할 수는 없습니다. 예를 들어, 관리자는 RODC에서 캐시에 저장해야 할 계정을 미리 지정할 수 있습니다. 이와 같이 RODC는 허브 사이트와의 WAN 링크가 오프라인인 경우라도 이들 계정의 자격 증명이 캐시에 저장되었다면 인증할 수 있습니다.

#### 관리자 역할 분리

RODC의 로컬 관리자 역할을 어떤 도메인 사용자에게든 위임할 수 있습니다. 이때 그 도메인 사용자에게 반드시 해당 도메인 또는 다른 도메인 컨트롤러에 대한 사용자 권한을 허용할 필요는 없습니다. 이를 통해 로컬 지사 사용자는 RODC에 로그온하여 드라이버 업그레이드와 같은 서버 유지 관리 작업을 수행할 수 있습니다. 그러나 지사 사무실의 사용자는 다른 도메인 컨트롤러에 로그온하거나 도메인의 다른 관리 작업을 수행할 수는 없습니다. 이와 같이 지사 사무실의 사용자에게 도메인의 나머지 부분에 대한 보안을 훼손하지 않고 지사 사무실의 RODC를 효과적으로 관리할 권한을 위임할 수 있습니다. 관리자 역할 분리는 유연한 관리 모델을 제공하는 한편 보안성을 높입니다. 이것은 로컬 제어 또는 유지 관리가 어느 정도 필요하지만 중앙 네트워크와 서버를 보호해야 하는 지사 사무실에 특히 적합합니다.

#### 새 MMC 스냅인 기능

Windows Server 2008의 Active Directory 사이트 및 서비스 스냅인 도구 모음과 동작메뉴에는 찾기 명령이 있습니다. 이 명령을 이용하면 도메인 컨트롤러가 있는 사이트를 찾을 수 있습니다. 이것은 지사 사무실과 허브에 있는 도메인 컨트롤러 간의 복제 문제를 해결하는 데 유용합니다.

도메인 컨트롤러의 속성 시트에는 RODC 관리에 유용한 암호 복제 정책 탭이 있습니다. 관리자는 이 탭에서고급 버튼을 클릭하여 다음을 확인할 수 있습니다.

* RODC에 전송된 암호
* 현재 RODC에 저장되어 있는 암호
* 현재 보안 그룹에 정의되어 있지 않은 허용되거나 거부된 복제 항목인 암호를 포함하여 RODC에 인증된 암호 - 관리자는 누가 RODC를 사용하고 있는지 확인하면서 암호 복제를 허용할지 거부할지를 결정할 수 있습니다.

### 읽기 전용 DNS(Domain Name System)

DNS(Domain Name System) 서버 서비스를 RODC에 설치할 수 있습니다. RODC는 ForestDNSZones와 DomainDNSZones를 비롯하여 DNS가 사용하는 모든 응용 프로그램 디렉터리 파티션을 복제할 수 있습니다. DNS 서버가 RODC에 설치된 경우 클라이언트는 다른 DNS 서버를 쿼리할 때처럼 이름 확인을 위해 이 서버를 쿼리할 수 있습니다. 이 방법을 통해 지사의 클라이언트는 속도가 느린 WAN 링크로 이름 확인 요청을 전송하지 않고도 고속 로컬 LAN에서 이름을 확인할 수 있습니다.

그러나 RODC의 DNS 서버는 클라이언트 업데이트를 직접 지원하지는 않습니다. 결과적으로 RODC는 RODC가 호스팅하는 Active Directory 통합 영역에 대한 NS(이름 서버) 리소스 레코드를 등록하지 않습니다. 클라이언트가 RODC에 대한 DNS 레코드 업데이트를 시도하면 서버는 쓰기 가능한 도메인 컨트롤러를 추천합니다. 그러면 클라이언트는 추천 받은 DNS 서버에 대한 업데이트를 시도할 수 있습니다. 백그라운드에서는 RODC의 DNS 서버가 업데이트가 이루어진 DNS 서버로부터 업데이트된 레코드의 복제를 시도하게 됩니다. 이 복제 요청은 단일 개체, 즉 DNS 레코드에만 적용됩니다. 변경된 영역 또는 도메인 데이터의 전체 목록은 이 특수한 단일 개체 복제 요청 과정에서 복제되지 않습니다.

### Hyper-V의 서버 가상화

조직은 Windows Server 2008 가상화 솔루션인 Hyper-V를 이용하여 하드웨어 사용률을 극대화하고 작업 부하를 통합하고 관리비를 절감함으로써 서버를 통합하고 서버 소유 비용을 줄일 수 있습니다. Hyper-V는 실제 서버 수가 더 적거나 심지어 하나인 경우에도 원격 인프라의 응용 프로그램과 서비스를 실행하는 서버를 통합하는 동시에 서로 다른 운영 체제 환경의 분리를 유지할 수 있습니다. IT 전문가는 이미 친숙한 관리 인터페이스를 사용하여 가상화된 서버를 중앙 허브 사이트에서 원격 관리할 수 있습니다. 보다 포괄적인 가상화 개념에 대해서는 2장 Hyper-V를 이용한 서버 가상화를 참조하십시오.

## 원격 관리 및 보안 기능 향상

Windows Server 2008은 원격 위치의 서버 관리를 담당하는 IT 전문가에게 보안성이 향상되고 원격 관리 기능이 개선된 여러 가지 새로운 기능을 제공합니다.

### Server Core 소개

Windows Server 2008부터, 관리자는 Windows Server 설치 시 원치 않는 기능은 제외하고 필요한 특정 기능만 최소로 설치할 수 있게 되었습니다. Server Core는 지사 사무실과 같은 원격 위치에 공통으로 배포된 일반 인프라 역할을 실행하기 위한 환경을 제공합니다. Windows Server 2008 관리자는 Server Core 설치를 사용하여 원격 사무실 서버에 필요한 특정 기능만 제공함으로써 원격 서버의 관리를 간소화하고 보안 위험을 줄일 수 있습니다. Server Core에 대해서는 이 문서의 서버 관리 장에서 자세히 설명합니다.

### BitLocker 드라이브 암호화

BitLocker 드라이브 암호화는 Windows Server 2008에 새로 추가된 중요한 보안 기능으로 원격 위치의 서버를 보호하는 데 유용합니다. Windows Vista Enterprise 및 Windows Vista Ultimate 버전에서 클라이언트 컴퓨터와 로밍 사용자의 모바일 컴퓨터를 보호하는 데 사용할 수도 있습니다. BitLocker는 디스크 드라이브의 내용을 암호화합니다. 이것은 다른 운영 체제를 실행하거나 다른 소프트웨어 도구를 실행하는 사람이 파일 및 시스템 보호 기능을 차단하거나 보호된 드라이브에 저장된 파일을 오프라인 상태에서 보는 등의 행위를 하지 못하도록 합니다.

BitLocker는 두 가지 중요한 하위 기능인 시스템 볼륨 암호화와 초기 부팅 구성요소에 대한 무결성 검사를 함께 수행하여 데이터 보호 기능을 개선합니다. 초기 부팅 구성 요소에 대한 무결성 검사를 통해, 그 구성 요소가 변조되지 않고 암호화된 드라이브가 원래 컴퓨터에 있는 경우에만 데이터 암호가 해독되도록 할 수 있습니다.

BitLocker는 사용자가 ATM 카드 PIN과 유사한 PIN을 제공할 때까지 또는 입력 데이터를 포함한 USB 플래시 드라이브를 삽입할 때까지 정상적인 부팅 프로세스를 차단할 수 있는 옵션을 제공합니다. 새로 추가된 이 보안 수단은 다단계 인증 및 보증 방식을 제공하므로 정확한 PIN을 입력하거나 USB 플래시 드라이브를 삽입하기 전에는 컴퓨터를 다시 시작하거나 최대 절전 모드에서 재개할 수 없습니다.

또한 BitLocker는 향상된 복구 옵션을 제공합니다. BitLocker의 재해 복구 콘솔은 데이터 검색이 가능하도록 하기 위해 초기 부팅 구성 요소에 통합되었습니다. 기본 설정의 BitLocker에는 사용자 작업이 필요하지 않으며, 활성화 자체도 원거리에서 자동으로 수행할 수 있습니다. BitLocker는 안전하고 쉽게 관리할 수 있는 데이터 보호 솔루션을 기업에 제공합니다.

BitLocker는 컴퓨터 분실, 도난 또는 폐기 시에도 데이터 도난 또는 노출 위험을 막을 수 있습니다. 지사 사무실의 경우에는 서버의 실질적인 보안이 항상 보장되는 것이 아니므로 이 기능이 중요합니다. 스왑 및 최대 절전 모드 파일을 포함한 전체 시스템 볼륨이 암호화되므로 원격 위치의 원격 서버에 더욱 뛰어난 보안성을 제공합니다.

### 엔터프라이즈급 프린터 관리

Windows Server 2008은 관리자가 단일 인터페이스에서 조직 내의 모든 프린터와 지사 사무실과 같은 원격 위치의 프린터까지 관리 및 모니터링하고 문제를 해결할 수 있는 MMC 스냅인인 인쇄 관리 스냅인을 제공합니다. 이것은 현장 관리 작업을 수행할 IT 직원이 거의 없거나 전혀 없는 원격 위치의 장치들을 중앙에서 원활히 관리할 수 있도록 합니다. 인쇄 관리 스냅인에 대한 포괄적인 설명은 7장 서버 관리를 참조하십시오.

### Windows PowerShell

Windows PowerShell 명령줄 셸 및 스크립트 언어는 IT 전문가가 공통적인 작업을 자동화하는 데 유용합니다. 새로운 관리 중심 스크립트 언어, 120개 이상의 표준 명령줄 도구, 일관성 있는 구문과 유틸리티를 제공하는 Windows PowerShell을 사용하면 지사 사무실과 같은 원격 위치에서도 IT 전문가가 훨씬 쉽게 시스템 관리를 제어하고 자동화를 가속화할 수 있습니다. PowerShell에 대한 포괄적인 설명은 7장 서버 관리를 참조하십시오.

### Windows 원격 관리

Windows 원격 관리는 원격 위치에 있는 서버를 낮은 대역폭에서 쉽게 관리할 수 있는 스크립팅 가능한 방식을 제공합니다. Windows Remote Manager는 Microsoft에서 구현한 WS-Management 프로토콜입니다. 표준 SOAP을 기반으로 하는 이 프로토콜은 하드웨어와 운영 체제의 상호 운용을 가능케 합니다. 관리자는 Windows 원격 관리 스크립트 개체, Windows 원격 관리 명령줄 도구 또는 Windows 원격 셸 명령줄 도구를 사용하여 지사 사무실에 있는 원격 컴퓨터로부터 관리 데이터(디스크, 네트워크 어댑터, 서비스 또는 프로세스와 같은 개체에 대한 정보)를 입수할 수 있습니다. Windows 원격 관리에 대한 포괄적인 설명은 5장: 보안 및 규정 준수를 참조하십시오.

## WAN 효율성 개선

지사 사무실을 관리하는 관리자의 과제는 사용 가능한 대역폭을 최적화하고 원격 사이트에 있는 작업자의 생산성을 개선하는 것입니다. Windows Server 2008에는 원격 위치의 이 중대한 요구를 만족시킬 새로운 기능과 개선이 추가되었습니다.

### TCP/IP 스택

Windows Server 2008에는 차세대 TCP/IP 스택이라고 알려진 TCP/IP 프로토콜 스택이 새롭게 구현되었습니다. 차세대 TCP/IP 스택은 인터넷 프로토콜 버전 4(IPv4) 및 6(IPv6)의 TCP/IP 기능을 완전히 재설계한 것으로 다양한 네트워킹 환경과 기술의 연결성 및 성능 요구를 만족합니다. 다음 기능이 새로 추가되었거나 개선되었습니다.

* 수신 창 자동 조정 및 복합 TCP - 사용 가능한 네트워크 대역폭의 가용성을 더욱 개선합니다.
* 고손실 환경을 위한 기능 향상 - 더욱 일관되고 신뢰할 수 있는 연결성을 보장하는 데 유용합니다.
* IPv4에 대한 인접 라우터 연결 불가 감지 - 네트워크 노드를 사용할 수 없게 되었을 때 감지 및 복구 기능을 개선합니다.
* 이전에는 실행되지 않던 게이트웨이가 다시 온라인 상태가 되어 처리 속도가 빨라졌음을 컴퓨터에서 확인할 수 있도록 실행되지 않는 게이트웨이 감지 기능 변경
* PMTU 블랙 홀 라우터 감지 - 연결이 끊어지는 것을 방지하는 데 유용합니다.
* 컴파트먼트 라우팅 - VPN 연결 시나리오에서 트래픽이 가장 효율적으로 라우팅되도록 합니다.
* 네트워크 진단 프레임워크 지원 - 사용자가 네트워크 연결을 복원하고 관련 문제점을 해결하는 데 유용한 확장 가능한 아키텍처를 제공합니다.
* Windows 필터링 플랫폼 - ISV(독립 소프트웨어 공급업체)가 TPC/IP 프로토콜 스택의 여러 계층과 운영 체제 전체에서 필터링을 수행함으로써 방화벽, 바이러스 백신 소프트웨어, 진단 소프트웨어 및 기타 응용 프로그램과 서비스를 생성할 수 있도록 API를 제공하는 새로운 아키텍처입니다.
* 명시적 정체 알림 - 정체된 라우터의 문제점을 해결하고 전체적인 처리량을 더욱 개선할 수 있습니다.

이러한 기능 향상은 대체로 속도가 느리고 신뢰성도 낮은 편인 WAN 링크를 통해 허브 사이트에 연결된 원격 위치의 일반적인 문제들을 완화하는 데 도움이 됩니다.

Windows Server 2008 네트워킹에 사용되는 향상되고 개선된 TCP/IP 스택은 네트워크 연결을 자동 조정하여 처리량을 극대화함으로써 성능을 개선합니다. 또한 기가비트급 네트워크와 차세대 인터넷 프로토콜에 대한 최적화된 지원을 통해 증가하는 IT 인프라 요구를 해결함으로써 확장성을 높입니다. Windows Server 2008 네트워킹은 완벽하게 통합된 네트워크 보안 기능을 통해 보안성을 향상시킵니다. 원격 위치의 경우에는 전송 시간을 단축하고 일반적으로 WAN 연결과 관련된 지연 문제를 줄임으로써 작업 생산성을 개선합니다.

#### 수신 창 자동 조정

TCP 수신 창 크기는 TCP 연결에서 수신되는 데이터를 저장하는 데 사용되는 수신 호스트의 메모리 버퍼에 있는 바이트의 양입니다. 차세대 TCP/IP 스택은 네트워크의 현재 상태에 따라 연결을 위한 최대 수신 창 크기의 값을 정확히 결정할 수 있도록 수신 창 자동 조정 기능을 지원합니다. 수신 창 자동 조정에서는 대역폭 지연에 따른 영향(대역폭을 연결 대기 시간으로 곱한 값) 및 응용 프로그램 검색 속도를 측정하여 연결당 최적의 수신 창 크기를 결정합니다. 그런 다음에는 최대 수신 창 크기를 규칙적으로 자동 조정합니다.

TCP 피어의 처리량이 개선됨에 따라 데이터 전송 과정에서 네트워크 대역폭 활용률이 높아집니다. 모든 응용 프로그램이 TCP 데이터 수신을 위해 최적화되어 있다면 전체적인 네트워크 활용률이 상당히 높아져서 LAN을 비롯하여 원격 위치를 허브에 연결하는 WAN에서도 이용 가능한 대역폭을 더욱 효율적으로 사용할 수 있습니다.

#### 복합 TCP

수신 창 자동 조정은 수신측 처리 속도를 최적화하는 반면, 차세대 TCP/IP 스택의 복합 TCP(CTCP)는 발신측 처리 속도를 최적화합니다. 이러한 특성이 함께 작용하여 링크 활용률을 높이고 대역폭 지연에 따른 영향이 큰 연결을 위해 중대한 성능 상의 이점을 제공합니다.

CTCP는 수신 창 크기가 크고 대역폭 지연에 따른 영향(연결 대역폭을 그 지연 시간으로 곱한 값)이 큰 TCP 연결에 사용됩니다. 이것은 한 번에 전송되는 데이터 양을 크게 높이면서도 그 동작이 다른 TCP 연결에 나쁜 영향을 미치지 않도록 합니다.

예를 들어, Microsoft 내부에서 수행된 테스트에서 왕복 시간(RTT) 50밀리초인 초당 1기가비트 연결의 경우 대용량 파일의 백업 시간이 거의 절반으로 줄었습니다. 대역폭 지연에 따른 영향이 더 큰 연결도 보다 나은 성능을 보일 수 있습니다.

#### 고손실 환경을 위한 성능 향상

차세대 TCP/IP 스택은 대기 시간이 길거나 신뢰성이 떨어질 수 있는 WAN 링크를 통해 허브 사이트에 연결된 지사 사무실과 같은 고손실 환경에서 처리 속도를 최적화하기 위해 다음과 같은 RFC(Request for Comments)를 지원합니다.

* RFC 2582 - TCP의 빠른 복구 알고리즘으로 NewReno 수정: 데이터 창에서 복수의 세그먼트가 손실되고 보낸 사람은 데이터가 수신되었다는 부분 승인을 수신하면 NewReno 알고리즘은 보낸 사람이 전송 속도를 높일 수 있는 방식을 변경하여 처리 속도를 높입니다.
* RFC 2883 - TCP에 대한 선택적 승인(SACK) 옵션 확장: RFC 2018에 정의된 SACK를 이용하면 받는 사람은 수신 데이터 중 최대 4개의 비연속 블록을 표시할 수 있습니다. RFC 2883은 중복 패킷을 승인하기 위한 SACK TCP 옵션의 추가 사용에 대해 정의합니다. 그러면 SACK 옵션을 포함하는 TCP 세그먼트를 받는 사람은 세그먼트가 불필요하게 전송되었을 때를 확인하고 향후의 재전송을 방지하기 위한 조치를 취할 수 있습니다. 재전송 횟수를 줄이면 전체적인 처리 속도가 빨라집니다.
* RFC 3517 - TCP에 대한 보존적인 선택적 승인(SACK) 기반의 손실 복구 알고리즘: Windows Server 2003과 Windows XP는 어떤 TCP 세그먼트가 대상 지점에 도착하지 않았는지 확인하는 데에만 SACK 정보를 사용하는 반면, RFC 3517은 중복 승인이 수신된 경우 손실 복구를 위해 SACK 정보를 사용하는 방법을 정의하고 SACK 연결이 활성화되면 빠른 복구 알고리즘을 제공합니다. 차세대 TCP/IP 스택은 연결별로 SACK 정보를 계속 추적하며 수신되는 승인과 중복된 승인을 모니터링하여 세그먼트가 대상 지점에서 수신되지 않을 때 더욱 신속히 복구합니다.
* RFC 4138 - F-RTO(Forward RTO-Recovery): TCP 및 SCTP(Stream Control Transmission Protocol)에 대한 의사 재전송 시간 제한을 감지하기 위한 알고리즘: F-RTO(Forward-Retransmission Timeout) 알고리즘은 TCP 세그먼트의 불필요한 재전송을 방지합니다. 왕복 시간(RTT)이 갑자기 또는 일시적으로 증가하는 경우 TCP 세그먼트가 불필요하게 재전송되는 일이 발생할 수 있습니다. F-RTO 알고리즘을 이용하면 무선 클라이언트가 한 무선 AP(액세스 포인트)에서 다른 AP로 로밍하는 경우와 같이 RTT가 갑자기 또는 일시적으로 증가한 상황에서 F-RTO는 불필요한 세그먼트 재전송을 방지하고 더욱 신속하게 정상 전송 속도를 회복할 수 있습니다.

이러한 성능 향상 덕분에 더욱 빠르고 일관성 있는 커뮤니케이션이 이루어져 WAN 링크를 통해 연결된 지사 사무실의 사용자와 컴퓨터에서 커뮤니케이션과 관련된 문제가 줄어듭니다.

#### 실행되지 않는 게이트웨이 감지 기능 변경

Windows Server 2003과 Windows XP의 TCP/IP에서 실행되지 않는 게이트웨이 감지는 장애 조치 기능을 제공하지만, 실행되지 않는 게이트웨이를 재시도하여 다시 사용 가능하게 되었는지 확인하기 위한 장애 복구 기능은 제공하지 않습니다. 차세대 TCP/IP 스택은 이전에 감지된 실행되지 않는 게이트웨이를 사용하여 TCP 트래픽 전송을 주기적으로 시도함으로써 실행되지 않는 게이트웨이에 대한 장애 복구 기능을 제공합니다. 실행되지 않는 게이트웨이를 통해 TCP 트래픽이 성공적으로 전송된 경우 차세대 TCP/IP 스택은 기본 게이트웨이를 이전에 감지된 실행되지 않는 게이트웨이로 전환합니다. 기본 게이트웨이로의 장애 복구는 기본 게이트웨이를 사용하여 트래픽을 대상 지점에 전송함으로써 처리 속도를 높입니다. 지사 사무실의 경우에는 오프라인이었던 지사 사무실과 허브 링크 사이의 커뮤니케이션을 더 빠른 속도의 기본 링크로 전환시켜 데이터 전송 속도가 더욱 빨라지게 만들 수 있습니다.

#### PMTU 블랙 홀 라우터 감지 기능 변경

RFC 1191에 정의된 PMTU(Path Maximum Transmission Unit)를 검색하려면 다음 링크의 MTU를 포함한 라우터로부터 ICMP(Internet Control Message Protocol) 대상에 연결할 수 없음-조각화 필요 및 DF(조각화 안 함) 세트 메시지를 수신해야 합니다. 그러나 조각화할 수 없는 패킷을 중간 라우터에서 자동으로 삭제하는 경우도 있습니다. 이러한 라우터를 블랙 홀 PMTU 라우터라고 합니다. 또한 중간 라우터는 방화벽 규칙에 따라 ICMP 메시지를 삭제할 수도 있습니다. 블랙 홀 PMTU 라우터 때문에 TCP 연결 제한 시간이 초과되어 종료될 수 있습니다.

PTMU 블랙 홀 라우터 감지 기능은 대용량 TCP 세그먼트가 재전송될 때 이를 감지한 다음 ICMP 오류 메시지 수신을 이용하는 대신 연결을 위해 PMTU를 자동으로 조정합니다. Windows Server 2003 및 Windows XP에서는 PMTU 블랙 홀 라우터 감지가 기본적으로 비활성화되는데, 그 이유는 이 기능이 활성화되면 특정 네트워크 세그먼트에 대해 수행되는 최대 재전송 횟수가 증가하기 때문입니다. 차세대 TCP/IP 스택은 TCP 연결 종료를 방지하기 위해 PMTU 블랙 홀 라우터 감지를 기본적으로 활성화하여 지사 사무실 사용자와 컴퓨터의 연결 중단이 줄어들도록 합니다.

### IPv6(Internet Protocol 버전 6) 지원

Windows Server 2008 및 Windows Vista에서는 IPv6이 설치되고 기본적으로 활성화됩니다. IPv6 설정은 Internet Protocol 버전 6(TCP/IPv6) 구성 요소의 속성 및 Netsh 인터페이스 IPv6 컨텍스트의 명령을 통해서 구성할 수 있습니다. Windows Server 2008 및 Windows Vista의 IPv6은 제거할 수는 없지만 비활성화할 수는 있습니다.

차세대 TCP/IP 스택은 IPv4와 IPv6 구현에서 공통의 전송(TCP 및 UDP) 및 프레임 계층을 공유하는 이중 IP 계층 아키텍처를 지원합니다. 차세대 TCP/IP 스택은 기본적으로 IPv4와 IPv6을 둘 다 활성화합니다. IPv6 지원을 위해 별도의 구성 요소를 설치할 필요는 없습니다.

### 서비스 품질

Windows Server 2003 및 Windows XP에서는 GQoS(Generic QoS) API를 통해서 응용 프로그램이 QoS(서비스 품질) 기능을 사용할 수 있습니다. GQoS API를 사용한 응용 프로그램은 우선순위가 지정된 전달 기능에 액세스했습니다. Windows Server 2008 및 Windows Vista에는 기업과 가정에서 네트워크 트래픽을 관리할 수 있는 새로운 기능이 추가되었습니다.

#### 기업 네트워크에 대한 정책 기반의 QoS

Windows Server 2008 및 Windows Vista의 QoS 정책을 통해 IT 직원은 나가는 네트워크 트래픽의 전송 속도에 우선 순위를 정하거나 관리할 수 있습니다. IT 직원은 특정 응용 프로그램 이름, 특정 소스 및 대상 IP 주소, 특정 소스 및 대상 TCP 또는 UDP 포트로 설정을 제한할 수 있습니다. QoS 정책 설정은 사용자 구성 또는 컴퓨터 구성 그룹 정책 설정의 일부이며 그룹 정책 개체 편집기를 사용하여 구성합니다. 이 설정은 그룹 정책 관리 콘솔을 사용하여 Active Directory 도메인 서비스 컨테이너(도메인, 사이트 및 조직 구성 단위)에 연결됩니다.

대역폭 사용을 관리하기 위해 아웃바운드 트래픽의 스로틀 속도로 QoS 정책을 구성할 수 있습니다. 스로틀 기능을 사용함으로써, QoS 정책은 총 아웃바운드 네트워크 트래픽을 지정된 속도로 제한할 수 있습니다. 우선 순위 전달을 지정하기 위해 트래픽은 DSCP(Differentiated Services Code Point) 값으로 표시됩니다. 네트워크 인프라에서 라우터 또는 무선 액세스 포인트는 우선 순위에 따른 전달을 위해 DSCP 표시된 패킷을 서로 다른 큐에 배치할 수 있습니다. DSCP 표시와 스로틀 기능을 함께 사용하여 트래픽을 효과적으로 관리할 수 있습니다. 스로틀 기능과 우선 순위 표시는 모두 네트워크 계층에서 설정하므로, 응용 프로그램 자체는 수정하지 않아도 됩니다.

네트워크 관리자는 서비스 품질 정책을 사용하여 허브 사이트의 서버에 연결된 지사 사무실의 특정 사용자와 그룹에서 전송되는 네트워크 트래픽의 우선 순위를 지정할 수 있습니다. 이것은 최대 부하 시점에 사용 가능한 네트워크 대역폭을 보다 잘 이용하므로 처리 속도를 높이고 사용 경험을 개선하며 지연을 줄여 전체적인 생산성을 향상시킬 수 있습니다.

### SYSVOL 및 SDFR(분산 파일 시스템 복제)

데이터를 계속 업데이트하고 원격 서버와 동기화하는 것은 지사 사무실 시나리오를 관리하는 IT 전문가의 과제입니다. Windows Server 2008는 이 프로세스를 간소화할 수 있는 새로운 복제 기능을 제공합니다.

#### DSFR 소개

DFSR(Distributed File System Replication) 서비스는 복수의 서버에서 폴더를 계속 동기화시키는 데 사용되는 복수 마스터 복제 엔진입니다. 데이터를 여러 서버로 복제하면 데이터 가용성이 높아지며 원격 사이트의 사용자가 빠르고 안전하게 파일에 액세스할 수 있습니다. DFSR은 RDC(원격 차등 압축)라는 압축 알고리즘을 사용합니다. RDC는 대역폭이 제한된 네트워크에서 파일을 효율적으로 업데이트하는 데 사용할 수 있는 프로토콜입니다. RDC는 파일에서 데이터 삽입, 제거 및 재배치를 감지하여 파일이 업데이트될 때 DFSR이 변경 사항만 복제할 수 있도록 합니다. DFSR은 분산 파일 시스템 및 공유 시스템 볼륨 데이터를 복제하는 데 사용됩니다. 대부분의 파일 유형에서 RDC와 DFSR은 데이터 동기화를 유지 관리하는 데 필요한 대역폭을 크게 줄일 수 있습니다.

#### SYSVOL 및 DFSR

Windows Server 2008에서 DFSR은 도메인 정보를 저장하는 데 사용되는 공유 시스템 볼륨(SYSVOL)을 복제합니다. 이것은 여러 가지 이점을 제공합니다. DFSR은 Windows Server 2008 도메인 기능 수준에서 자동으로 활성화됩니다. 그러면 SYSVOL은 원격 차등 압축의 이점을 이용하여 대역폭 활용률을 줄이게 됩니다.

주문형 복제는 Windows Server 2008에 새로 추가된 기능으로, 필요한 파일만 복제하고 필요하지 않은 데이터는 지사 사무실 서버에서 제거합니다. 주문형 복제는 크기별 또는 마지막 액세스 시간별로 구성할 수 있습니다. Windows Server의 이전 버전에서는 속도가 느린 WAN 링크를 통해 연결된 사이트 간의 대기 시간으로 인해 암호 재설정과 같은 항목에 동기화 문제가 발생할 수도 있습니다. 주문형 복제 기능을 사용하여 이 문제를 예방할 수 있습니다.

Windows Server 2008에서 DFSR과 주문형 복제를 결합하여 필요한 SYSVOL 복제를 제공하고 대역폭 활용률을 보존하며 지사 사무실에 불필요한 데이터 저장소를 줄일 수 있습니다.

### 서버 메시지 블록 2.0

SMB(서버 메시지 블록)는 Windows 기반 컴퓨터의 기본적인 파일 공유 프로토콜이며 CIFS(Common Internet File System)의 확장입니다. Windows Server 2008에는 클라이언트측 캐시 기능 향상 및 개선된 파일 복사 성능을 제공하는 SMB 버전 2.0이 포함됩니다.

클라이언트와 서버 간의 데이터 전송으로 인한 지연 때문에 WAN 링크 상에서 응용 프로그램 사용을 시도하는 사용자의 대기 시간이 길어질 수 있습니다. 프로토콜의 효율을 높아져도 대기 시간을 완전히 없앨 수는 없지만, 그로 인한 영향을 최소화하고 지사 사무실 작업자에게 보다 나은 사용자 환경을 제공할 수는 있습니다. SMB 2.0은 SMB 1.0에 비해 많은 개선이 이루어졌으며 대기 시간도 줄어들었습니다.

Windows에는 SMB 클라이언트와 SMB 서버가 포함됩니다. SMB 버전 1.0은 원래 Microsoft LAN Manager 및 Windows for Workgroups와 같은 초기의 Windows 기반 네트워크 운영 체제를 위해 설계되었습니다. Windows Server 2008 및 Windows Vista의 SMB에는 오늘날의 네트워킹 환경에 맞게 재설계되고 차세대 파일 서버의 요구를 만족시키는 새로운 버전인 SMB 2.0이 포함되어 있습니다.

SMB 2.0은 같은 패킷 내에서 여러 SMB 명령을 보낼 수 있도록 지원합니다. 이를 통해 SMB 1.0의 일반적인 문제로 알려진 SMB 클라이언트와 서버 간 전송 패킷 수를 줄여 클라이언트와 서버가 통신해야 하는 횟수를 줄일 수 있습니다. 또한 SMB 2.0은 SMB 1.0에 비해 훨씬 큰 용량의 버퍼 크기를 지원하여 보다 적은 수의 패킷으로 더 많은 데이터를 전송할 수 있도록 합니다.

다른 모든 기술과 마찬가지로 SMB 2.0에서도 확장성이 중요한 구성 요소입니다. SMB 2.0은 이전 버전의 제한을 사용하지 않습니다. 예를 들어, 서버가 사용할 수 있는 파일 공유 수와 함께 서버에서 동시에 열 수 있는 파일 핸들 수가 늘어났습니다. 확장성과 함께 가용성도 중요한 구성 요소 중 하나입니다. SMB 2.0은 네트워크 가용성이 일시적으로 중단되더라도 상태를 유지할 수 있는 견고한 핸들을 지원함으로써 가용성을 향상시킵니다. 이를 통해 사용자는 연결 상태를 유지할 수 있으며 불안정한 링크를 통해서도 데이터를 전송할 수 있는 횟수가 늘어납니다.

SMB 2.0의 여러 가지 향상된 기능으로 데이터 전송 시간도 단축되었습니다. Windows Vista(기본적으로 SMB 2.0 지원)에서 수행된 몇 가지 성능 비교 통계를 다음 그래프에서 설명합니다.

다음 그림은 네트워크 대역폭의 사용률이 높을수록 SMB 1.0에 비해 SMB 2.0을 사용하여 파일을 다운로드 및 업로드할 때 LAN을 통한 전송 속도가 빨라짐을 보여 줍니다.

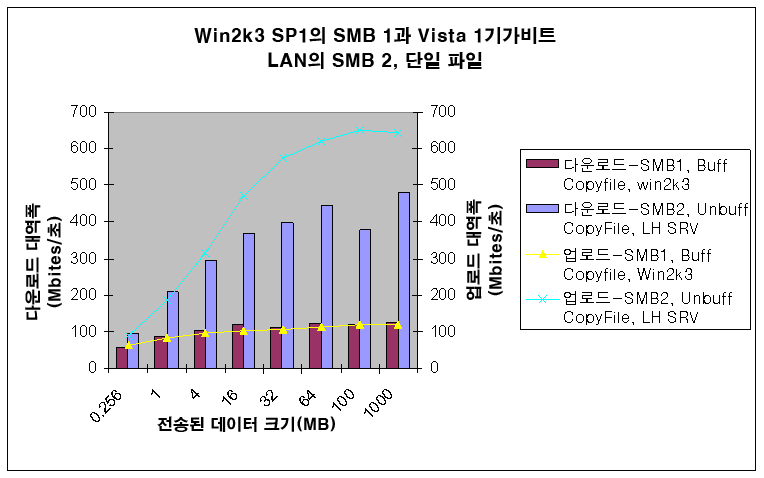


그림 2: LAN 연결을 통한 SMB 2.0과 SMB 1.0 비교

다음 그림은 네트워크 대역폭의 사용률이 높을수록 SMB 1.0에 비해 SMB 2.0을 사용하여 파일을 다운로드 및 업로드할 때 WAN을 통한 전송 속도가 빨라짐을 보여 줍니다.

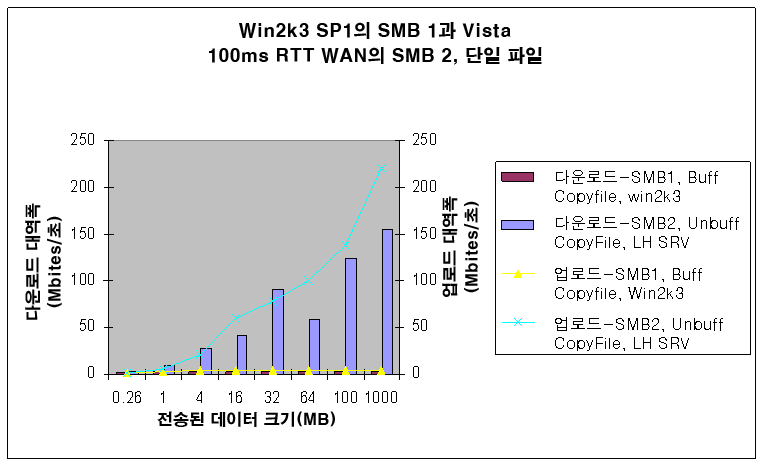


그림 3: WAN 연결을 통한 SMB 2.0과 SMB 1.0 비교

원격 위치 시나리오에서 SMB는 대역폭 사용을 최적화하고 원격 작업자와 조직의 중앙 네트워크 간 연결을 향상시키는 Windows Server 2008 주요 구성 요소 중 하나입니다.

## 요약

Windows Server 2008은 IT 관리자가 지점 위치에서 서버를 보다 효율적으로 배포 및 관리하고, 증가하는 보안 요구에 대처하며, 계속해서 늘어 가는 기업 WAN에 대한 대역폭 요구 사항을 보다 잘 충족시킬 수 있도록 하기 위해 설계된 새로운 도구와 기능을 제공합니다.

새로운 관리 도구는 지점 위치에서 Active Directory 도메인 서비스를 배포 및 관리하는 작업을 간소화하고, 읽기 전용 도메인 컨트롤러는 원격 위치에서 도메인 컨트롤러 기능을 사용할 수 있는 보다 안전한 방법을 제공합니다. Windows Server 2008의 Windows BitLocker 드라이브 암호화는 지점 서버 또는 원격 작업자 랩톱의 중요한 데이터를 위해 새로운 보안 옵션을 선보였습니다. 조직에서는 새로운 Server Core 설치 옵션을 사용하여 지점에 관리가 간소화되고 보안이 향상된 주요 서버 기능을 제공할 수 있습니다.

# 5장: 보안 및 규정 준수

## 소개

Windows Server 2008은 정책 기반 보안 기능을 통해 향상된 관리 효율성과 보안 준수를 제공합니다. 간소화된 관리 인터페이스를 통해 관리자는 보안 및 정책 관련 기능을 쉽게 제어하여 관리 시간은 단축시키면서 보안은 강화할 수 있습니다. Windows Server 2008에는 보안 및 규정 준수를 향상시키는 여러 가지 기능이 있습니다. 몇 가지 주요한 향상 기능은 다음과 같습니다.

* 방화벽 향상 - 새로운 "고급 보안이 설정된 Windows 방화벽"은 여러 가지 향상된 보안 기능을 제공합니다.
* 데이터 암호화 및 보호 - BitLocker는 디스크 드라이브를 암호화하여 중요한 데이터를 보호합니다.
* RODC(읽기 전용 도메인 컨트롤러) - RODC는 실제 보안 수준이 낮을 수 있는 원격 사이트에 설치 가능한 새로운 유형의 도메인 컨트롤러입니다.
* 서버 및 도메인 격리 - 인증된 컴퓨터와 권한이 부여된 컴퓨터로만 액세스를 제한하도록 서버 및 도메인 리소스를 격리시킬 수 있습니다.
* 인증서 향상 - 엔터프라이즈 PKI는 인증서 관리 작업을 간소화하며 향상된 모니터링 기능과 새로운 웹 등록 제어 기능을 제공합니다.
* 향상된 클라이언트 상태 - NAP(네트워크 액세스 보호)를 통해 관리자는 클라이언트의 네트워크 액세스를 허용하기 전에 상태 및 보안 요구 사항을 구성하고 적용할 수 있습니다.
* 암호화 도구 - Next Generation Cryptology는 유연한 암호화 개발 플랫폼을 제공합니다.
* 사용자 ID 관리 - ID 및 액세스 솔루션은 조직에서 사용자 ID와 액세스 권한을 관리할 수 있도록 하기 위해 설계된 일련의 플랫폼 기술입니다.
* 페더레이션 권한 관리 - 페더레이션 공동 작업은 안전한 방식으로 중요한 정보를 외부 사용자와 공유하는 작업을 간소화합니다.
* 파일 시스템 암호화 - 중요한 보안 기능인 파일 시스템 암호화는 사용자 수준의 파일 및 폴더 암호화에 유용합니다. 네트워크 파일 및 폴더 암호화를 수행할 때 이 기능을 통해 관리자는 스마트 카드에 파일 시스템 암호화 키를 저장할 수 있습니다.

이와 같이 향상된 기능으로 관리자는 조직의 보안 수준을 높이고 보안 관련 구성 및 설정의 관리와 배포를 간소화할 수 있습니다.

## 고급 보안이 설정된 Windows 방화벽

Windows Server 2008의 고급 보안이 설정된 Windows 방화벽은 기술 간의 충돌과 조정 오버헤드를 줄여 줍니다. 고급 보안이 설정된 Windows 방화벽은 중앙 집중식 방화벽 필터링 및 연결 보안 규칙을 제공합니다. 이 방화벽은 네트워크에 있는 악의적인 사용자와 프로그램에 대한 차단 수준을 제공하기 위해 관련 구성 및 현재 실행되고 있는 응용 프로그램에 따라 네트워크 트래픽을 허용하거나 차단하는 상태 저장 호스트 기반 방화벽입니다. Windows 방화벽의 고급 보안 기능은 다음과 같습니다.

* 들어오는 트래픽 및 나가는 트래픽 모두에 대해 지원
* 로컬 및 원격 방화벽 구성을 위한 새로운 MMC(Microsoft Management Console) 스냅인
* 통합된 방화벽 필터링 및 IPSec(인터넷 프로토콜 보안) 보호 설정
* 여러 가지 새로운 방화벽 예외 구성 방식

#### 들어오는 트래픽 및 나가는 트래픽 모두에 대해 지원

현재 Windows 방화벽은 들어오는 트래픽을 가로채서 요청에 대한 응답으로 전송된 트래픽(요청된 트래픽) 또는 허용된 대로 지정된 요청하지 않은 트래픽(예상된 트래픽)에 해당하지 않는 요청하지 않은 들어오는 트래픽을 모두 삭제할 수 있도록 방화벽 사용을 지원합니다. 이는 방화벽 기능의 주요 구성 요소로, 요청하지 않은 들어오는 트래픽을 통해 퍼지는 네트워크 수준의 바이러스 및 웜으로 컴퓨터가 감염되지 않게 해 줍니다.

Windows Server 2008에 포함된 Windows 방화벽 고급 보안 기능의 특징은 방화벽을 통해 들어오는 트래픽과 나가는 트래픽을 모두 차단할 수 있다는 점입니다. 예를 들어, 네트워크 관리자는 특정 포트(예: 바이러스 소프트웨어가 사용하는 것으로 알려진 포트) 또는 중요하거나 원치 않는 콘텐츠를 포함하는 특정 주소로 전송되는 모든 트래픽을 차단하도록 새 Windows 방화벽(일련의 예외 포함)을 구성할 수 있습니다. Windows Server 2008에서 Windows 방화벽의 기본 동작은 다음과 같습니다.

* 요청하지 않았거나 구성된 예외와 일치하지 않는 경우 들어오는 트래픽을 모두 차단합니다.
* 구성된 예외와 일치하지 않는 경우 나가는 트래픽을 모두 허용합니다.

#### 이와 같은 추가 지원은 바이러스로 감염된 컴퓨터로부터 네트워크와 다른 시스템을 보호해 줍니다.

#### GUI 구성을 위한 새로운 MMC 스냅인

이제 Windows 방화벽은 "고급 보안이 설정된 Windows 방화벽"이라는 MMC 스냅인으로 구성됩니다. 이 스냅인을 사용하여 네트워크 관리자는 로컬 및 원격 컴퓨터에서 Windows 방화벽에 대한 설정을 구성할 수 있습니다(현재 Windows 방화벽의 경우 원격 데스크톱 연결 없이는 구성할 수 없음). 또한 관리자는 새로운 Windows 방화벽 고급 설정의 명령줄 구성에 대한 netsh advfirewall 컨텍스트에서 명령을 사용할 수 있습니다.

#### 통합된 방화벽 및 IPSec 설정

IPSec는 IP 트래픽에 대해 암호화 보호를 제공하기 위한 일련의 인터넷 표준입니다. 이전 버전의 Windows Server에서 Windows 방화벽과 IPSec는 별도로 구성되었습니다. Windows에서 호스트 기반 방화벽과 IPSec는 들어오는 트래픽을 차단하거나 허용할 수 있으므로 겹치거나 충돌하는 방화벽 예외 및 IPSec 규칙을 만들 수 있습니다. 새로운 Windows 방화벽은 같은 GUI와 명령줄 명령을 사용하는 두 네트워크 서비스의 구성을 결합했습니다. 이러한 방화벽과 IPSec 설정의 통합은 IPSec 설정 구성도 간소화합니다.

#### 여러 가지 방화벽 예외 구성 방식

Windows Server 2008의 고급 보안 기능을 통해 관리자는 다음과 같은 여러 가지 새로운 방식으로 방화벽 예외를 구성할 수 있습니다.

* IP 프로토콜 번호에 대해 예외를 구성할 수 있습니다. 새로운 Windows 방화벽을 통해 관리자는 이름별로 프로토콜을 선택하거나 수동으로 원하는 트래픽에 대해 IPv4 프로토콜또는 IPv6 다음 머리글필드에 값을 입력할 수 있습니다.
* 소스 및 대상에 대해 예외를 구성할 수 있습니다. 관리자는 들어오는 트래픽과 나가는 트래픽 모두에 대해 소스 및 대상 TCP 또는 UDP 포트를 구성하여 허용되거나 차단되는 TCP 및 UDP 트래픽의 유형을 보다 세밀하게 정의할 수 있습니다.
* 전체 또는 다중 포트에 대해 예외를 구성할 수 있습니다. 또한 관리자는 모든 TCP 또는 모든 UDP 트래픽에 대해 TCP 또는 UDP 포트를 모두 지정하거나 쉼표로 구분된 다중 포트 목록을 지정할 수 있습니다.
* 특정 유형의 인터페이스에 대해 예외를 구성할 수 있습니다.관리자는 예외를 모든 인터페이스에 적용할지 아니면 LAN, 원격 액세스, 무선 인터페이스 등 특정 유형의 인터페이스에 적용할지 지정할 수 있습니다.
* 유형 및 코드별로 ICMP 및 ICMPv6(ping) 트래픽에 대해 예외를 구성할 수 있습니다. Windows Server 2008의 Windows 방화벽에는 공통 예외로 간주되는 ICMP 및 ICMPv6 메시지 집합이 미리 정의되어 있으며 관리자는 ICMP 또는 ICMPv6 메시지 유형 및 코드 필드 값을 지정하여 새로운 ICMP 또는 ICMPv6 메시지를 추가할 수 있습니다. 예를 들어, 관리자가 "ICMPv6 패킷이 너무 큼" 메시지에 대해 예외를 만들려는 경우 수동으로 ICMPv6 유형 2 및 코드 0에 대해 예외를 만들 수 있습니다.
* 서비스에 대해 예외를 구성할 수 있습니다. 관리자는 예외를 모든 프로세스에 적용할지, 서비스에만 적용할지, 서비스 이름별로 특정 서비스에 적용할지 지정할 수도 있으며 서비스에 대한 짧은 이름을 입력할 수도 있습니다. 예를 들어, 관리자가 예외를 컴퓨터 브라우저 서비스에만 적용하도록 구성하려는 경우 컴퓨터에서 실행되는 서비스의 목록에서 컴퓨터 브라우저 서비스를 선택할 수 있습니다.

Windows Server 2008에 포함된 새로운 Windows 방화벽은 바이러스 소프트웨어에서 사용하는 것으로 알려진 포트 또는 중요하거나 원치 않는 콘텐츠를 포함하는 특정 주소로 나가는 트래픽을 가로채서 조직 내에 바이러스가 퍼지지 않도록 하고 주요 시스템을 보호할 수 있습니다. 새로운 고급 보안이 설정된 Windows 방화벽 MMC 스냅인을 통해 관리자는 로컬 및 원격 시스템에서 Windows 방화벽과 IPSec 설정을 모두 쉽게 구성할 수 있습니다. 소개된 여러 가지 새로운 방식으로 Windows 방화벽 예외를 구성할 수 있으므로 관리자는 새로운 보안 위협에 유연하게 대처할 수 있습니다. 이러한 향상된 기능은 Windows Server 2008에 포함된 Windows 방화벽의 보안을 강화하고 관리를 용이하게 해 줍니다.

## BitLocker 드라이브 암호화

BitLocker 드라이브 암호화는 서버, 워크스테이션 및 모바일 컴퓨터를 보호할 수 있도록 해 주는 Windows Server 2008의 새로운 주요 보안 기능입니다. 이 기능은 클라이언트 컴퓨터 및 모바일 컴퓨터 보호를 위해 Windows Vista Enterprise 및 Windows Vista Ultimate 버전에서도 제공됩니다. BitLocker는 디스크 드라이브의 내용을 암호화합니다. 이를 통해 병렬 운영 체제를 실행하거나 기타 악의적인 소프트웨어 도구를 실행하는 자가 파일 및 시스템 보호를 손상시키거나 보호된 드라이브에 저장되어 있는 파일을 오프라인에서 보지 못하도록 할 수 있습니다. BitLocker의 보다 포괄적인 적용 범위에 대해서는 4장 "지점"에서 확인할 수 있습니다.

## Active Directory 도메인 서비스: 감사

Windows Server 2008에서 관리자는 Active Directory 개체에 대한 액세스를 감사하는 추가 옵션을 사용할 수 있습니다. 새 감사 정책 하위 범주(디렉터리 서비스 변경)는 만들기, 수정, 이동, 삭제 취소 등의 Active Directory 개체 변경을 감사하고 변경 내용이 적용된 경우 이전 특성 값과 새 특성 값을 기록합니다.

참고: 디렉터리 서비스 액세스 감사는 개체 액세스 감사와 같은 방식으로 적용됩니다. 단, AD DS 개체에만 적용되며 파일 시스템 개체 및 레지스트리 개체에는 적용되지 않습니다.

### AD DS 액세스 감사

Windows 2000 Server 및 Windows Server 2003에는 유일한 감사 정책으로 디렉터리 서비스 액세스 감사가 있었습니다. 이 정책은 디렉터리 서비스 이벤트 감사의 사용 여부를 제어했습니다. Windows Server 2008에서 이 정책은 다음과 같은 네 가지 하위 범주로 분류됩니다.

* 디렉터리 서비스 액세스
* 디렉터리 서비스 변경
* 디렉터리 서비스 복제
* 세부 디렉터리 서비스 복제

글로벌 감사 정책인 디렉터리 서비스 액세스 감사는 디렉터리 서비스 이벤트 감사의 사용 여부를 제어합니다. 이 보안 설정에 따라 디렉터리의 개체에 대해 특정 작업이 수행될 때 이벤트가 보안 로그에 기록되는지 여부가 결정됩니다. 관리자는 개체에 대한 SACL(시스템 액세스 제어 목록)을 수정하여 감사할 작업을 제어할 수 있습니다. AD DS 개체에 대한 SACL은 해당 개체의 속성 대화 상자에 있는 **보안** 탭에서 설정할 수 있습니다. Windows Server 2008에서 이 정책은 기본적으로 사용됩니다.

기본 도메인 컨트롤러 정책을 수정하여 이 정책 설정을 정의한 경우 관리자는 성공 감사, 실패 감사, 감사 안 함 중에서 지정할 수 있습니다. 성공 감사는 사용자가 SACL이 지정된 AD DS 개체에 성공적으로 액세스한 경우 감사 항목을 생성합니다. 실패 감사는 사용자가 SACL이 지정된 AD DS 개체에 액세스하지 못한 경우 감사 항목을 생성합니다. Windows 2000 Server 및 Windows Server 2003에서 감사 이벤트는 ID 번호가 566인 보안 로그에 표시되었습니다. Windows Server 2008에서는 감사 정책 하위 범주 중 하나인 디렉터리 서비스 액세스가 계속해서 같은 이벤트를 생성합니다. 단, 이벤트 ID 번호가 4662로 변경되었습니다.

### AD DS 변경 감사

새로운 감사 하위 범주 중 하나인 디렉터리 서비스 변경은 AD DS의 개체 변경을 감사할 수 있도록 해 줍니다. 감사할 수 있는 변경 유형은 개체에 대해 수행되는 만들기, 수정, 이동 및 복원 작업입니다. 이러한 작업으로 생성되는 이벤트는 보안 로그에 표시되며 이전 특성 값과 현재 특성 값을 포함합니다.

이 새로운 정책 하위 범주로 AD DS에서의 감사에 다음과 같은 기능이 추가되었습니다.

* 개체의 특성에 대해 수정 작업이 성공적으로 수행되는 경우 AD DS는 이전 특성 값과 현재 특성 값을 기록합니다. 이 특성이 여러 값을 사용하는 경우 수정 작업으로 인해 변경된 값만 기록됩니다.
* 새 개체가 만들어진 경우 만들 때 채워진 특성의 값만 기록됩니다. 만들기 작업 중 특성이 추가된 경우 해당하는 새 특성 값이 기록됩니다. 대부분의 경우 AD DS는 특성에 기본값을 지정합니다(예: sAMAccountName). 이러한 시스템 특성의 값은 기록되지 않습니다.
* 개체가 도메인 내에서 이동된 경우 이전 위치와 새 위치가 고유 이름 형식으로 기록됩니다. 개체가 다른 도메인으로 이동된 경우 대상 도메인의 도메인 컨트롤러에 만들기 이벤트가 생성됩니다.
* 개체가 복원된 경우 개체가 이동된 위치가 기록됩니다. 또한 복원 작업 중 특성이 추가, 수정 또는 삭제된 경우 해당 특성의 값이 기록됩니다.

개체가 삭제된 경우 변경 감사 이벤트가 생성되지 않습니다. 단, 디렉터리 서비스 액세스 하위 범주가 사용된 경우 감사 이벤트가 생성됩니다.

디렉터리 서비스 변경이 사용되면 AD DS는 관리자가 감사를 위해 설정한 개체가 변경된 경우 보안 이벤트 로그에 이벤트를 기록합니다. 다음 표에서는 이러한 이벤트를 설명합니다.

표 8: AD DS 이벤트 기록

|  |  |  |
| --- | --- | --- |
| **이벤트 ID** | **이벤트 유형** | **이벤트 설명** |
| 5136 | 수정 | 이 이벤트는 디렉터리에서 특성이 성공적으로 수정된 경우 기록됩니다. |
| 5137 | 만들기 | 이 이벤트는 디렉터리에 새 개체가 만들어진 경우 기록됩니다. |
| 5138 | 복원 | 이 이벤트는 디렉터리에서 개체가 복원된 경우 기록됩니다. |
| 5139 | 이동 | 이 이벤트는 도메인 내에서 개체가 이동된 경우 기록됩니다. |

### 글로벌 감사 정책

감사 정책을 사용하여 서버에서의 모든 이벤트 및 응용 프로그램 사용을 추적하고 감사할 수 있으며, 관리자는 조직 내 컴퓨터에서 감사 정책을 구성, 생성, 백업 및 복원할 수도 있습니다.

글로벌 감사 정책인 디렉터리 서비스 액세스 감사를 사용하면 모든 디렉터리 서비스 정책 하위 범주를 사용할 수 있습니다. 보안 설정\로컬 정책\감사 정책 아래의 기본 도메인 컨트롤러 그룹 정책에서 이 글로벌 감사 정책을 설정할 수 있습니다. Windows Server 2008에서 이 글로벌 감사 정책은 기본적으로 사용됩니다. 따라서 디렉터리 서비스 변경하위 범주도 기본적으로 사용됩니다. 이 하위 범주는 액세스 이벤트만 감사하도록 설정되어 있습니다. 단, 두 감사 하위 범주는 서로 독립적으로 작동합니다. 관리자는 디렉터리 서비스 액세스를 사용하지 않도록 선택하여 이전과 마찬가지로 디렉터리 서비스 변경 하위 범주가 사용된 경우 생성되는 변경 이벤트만 기록되도록 설정할 수도 있습니다.

Windows 2000 Server 및 Windows Server 2003에서는 디렉터리 서비스 액세스 감사 정책을 통해서만 Active Directory 감사를 제어할 수 있었습니다. 이 제어로 생성된 이벤트는 이전 값과 수정된 새 값을 표시하지 않았습니다. 새로운 감사 정책 하위 범주 중 하나인 디렉터리 서비스 변경을 사용하면 디렉터리에 대해 성공한 변경이 이전 특성 값 및 현재 특성 값과 함께 기록됩니다. 개체 특성이 어떻게 변경되었는지 확인할 수 있으면 이벤트 로그를 개체 수명 동안 발생하는 변경에 대한 추적 메커니즘으로 보다 유용하게 사용할 수 있으며 필요에 따라 이전 특성 값으로 되돌릴 수도 있습니다.

## 서비스 기반 AD DS

Windows Server 2008에서 AD DS(Active Directory 도메인 서비스)는 서비스 기반이므로 MMC(Microsoft Management Console) 스냅인 또는 명령줄을 사용하여 중지하고 시작할 수 있습니다. 서비스 기반 AD DS는 오프라인 작업(예: 오프라인 조각 모음 또는 정식 복원) 수행에 필요한 시간을 단축시켜 관리 작업을 간소화합니다. 또한 AD DS 유지 관리를 수행하는 동안 도메인 컨트롤러에서 실행되는 다른 서비스를 활성 상태로 유지시켜 가용성을 향상시킵니다. 중지된 도메인 컨트롤러에 특별히 바인딩된 클라이언트는 검색을 통해 간단하게 다른 도메인 컨트롤러에 연결됩니다.

## RODC(읽기 전용 도메인 컨트롤러)

RODC(읽기 전용 도메인 컨트롤러)는 Windows Server 2008 운영 체제에서 사용할 수 있는 새로운 유형의 도메인 컨트롤러로, 원격 위치에서의 배포를 위해 설계되었습니다. RODC는 본 설명서의 "원격 위치" 섹션에서 자세히 설명됩니다.

## 서버 및 도메인 격리

Microsoft Windows 기반 네트워크에서 관리자는 인증된 컴퓨터와 권한이 부여된 컴퓨터로만 액세스를 제한하도록 서버 및 도메인 리소스를 논리적으로 격리시킬 수 있습니다. 예를 들어, 컴퓨터가 보안 통신에 대한 일련의 공통 요구 사항을 공유하는 기존의 실제 네트워크 안에 논리 네트워크를 만들 수 있습니다. 이와 같이 논리적으로 격리된 네트워크에 있는 각 컴퓨터는 연결 설정을 위해 격리된 네트워크의 다른 컴퓨터에 인증 자격 증명을 제공해야 합니다.

이러한 격리를 통해 권한이 부여되지 않은 컴퓨터와 프로그램이 리소스에 부적절하게 액세스하지 못하도록 할 수 있습니다. 격리된 네트워크에 포함되지 않은 컴퓨터로부터의 요청은 무시됩니다.

네트워크 보호에 사용할 수 있는 격리의 두 가지 유형은 다음과 같습니다.

* 서버 격리 - 서버 격리 시나리오에서 특정 서버는 IPSec 정책을 사용하여 다른 컴퓨터의 인증된 통신만 수락하도록 구성됩니다. 예를 들어, 웹 응용 프로그램 서버에서만 연결을 수락하도록 데이터베이스 서버를 구성할 수 있습니다.
* 도메인 격리 - 도메인을 격리시키기 위해 관리자는 Active Directory 도메인 구성원 자격을 사용하여 도메인 구성원 컴퓨터가 다른 도메인 구성원 컴퓨터의 인증 및 보호된 통신만 수락하도록 할 수 있습니다. 격리된 네트워크는 도메인에 속한 컴퓨터로만 구성됩니다. 도메인 격리는 IPSec 정책을 사용하여 모든 클라이언트 및 서버 컴퓨터 등의 도메인 구성원 간에 전송된 트래픽을 보호합니다.

서버 및 도메인 격리를 통해 중요한 특정 서버 및 데이터를 보호하고, 관리되지 않거나 악의적인 컴퓨터 및 사용자로부터 관리되는 컴퓨터를 보호할 수 있습니다.

## 엔터프라이즈 PKI

Windows Server 2008 및 Windows Vista 운영 체제에서는 PKI(공개 키 인프라)에 대해 여러 가지 기능이 향상되었습니다. Windows PKI의 모든 측면에서 관리 효율성이 향상되었으며 인증서 해지 서비스가 새롭게 설계되었고 등록에 대한 공격 위험이 감소되었습니다. PKI의 향상된 기능은 다음과 같습니다.

* PKIView를 통한 보다 간단해진 관리
* 인증서 웹 등록
* 네트워크 장치 등록 서비스
* 인증서 정책 설정
* 인증서 배포 변경
* OCSP(온라인 인증서 상태 프로토콜) 지원
* 그룹 정책으로 인증서 관리

Windows Server 2008의 이러한 향상된 기능은 조직의 PKI 환경을 관리하는 IT 전문가에게 새로운 옵션과 기능을 제공합니다.

### PKIView를 통한 엔터프라이즈 CA 관리

처음에는 Microsoft Windows Server 2003 Resource Kit에 PKI 상태 도구로 포함되었던 PKIView는 Windows Server 2008용 MMC(Microsoft Management Console) 스냅인입니다. PKIView는 CA의 성능 상태를 분석하고 AD CS에 게시된 CA 인증서의 세부 정보를 확인하는 데 사용됩니다. PKIView는 Windows Server 2008의 코어 운영 체제에 속하므로 PKIView를 사용하려는 관리자는 서버 설치 후 MMC에 PKIView를 추가하기만 하면 됩니다. 그러면 CA의 성능 상태를 분석하고 AD CS에 게시된 CA 인증서의 세부 정보를 확인하는 데 PKIView를 사용할 수 있습니다.

PKIView는 네트워크 PKI 환경의 상태 뷰를 제공합니다. 모든 CA 및 이에 대한 현재 성능 상태 뷰가 제공되면 관리자는 보다 쉽고 효율적으로 CA 계층을 관리하고 CA 오류를 해결할 수 있습니다. 특히 PKIView는 AIA(기관 정보 액세스) 위치 및 CRL 배포 지점의 유효성 또는 액세스 가능성을 나타냅니다.

선택한 CA 각각에 대해 PKIView는 다음과 같이 트리에 CA 성능 상태를 나타냅니다.

표 9: PKIView CA 성능 상태

| **표시기** | **CA 상태** |
| --- | --- |
| 물음표 | CA 성능 상태 평가 |
| 녹색 표시기 | CA에 문제가 없습니다. |
| 노란색 표시기 | CA에 단순한 문제가 있습니다. |
| 빨간색 표시기 | CA에 심각한 문제가 있습니다. |
| CA 아이콘에 빨간색 십자가 표시 | CA가 오프라인 상태입니다. |

PKIView 스냅인이 MMC에 추가되면 관리자는 다음과 같은 세 개의 창을 확인할 수 있습니다.

* 트리 - 이 창은 네트워크의 PKI 계층을 트리 형식으로 표시합니다. 엔터프라이즈 PKI 노드 아래의 각 노드는 하위 CA를 자식 노드로 표시하는 CA를 나타냅니다.
* 결과 - 트리에서 CA를 선택하면 이 창에 하위 CA, CA 인증서, CRL 배포 지점 및 AIA 위치의 목록이 표시됩니다. 트리에서 콘솔 루트를 선택하면 결과 창에 모든 루트 CA가 표시됩니다. 결과 창에는 다음과 같은 세 개의 열이 있습니다.
  + 이름 - 엔터프라이즈 PKI 노드를 선택하면 엔터프라이즈 PKI 노드 아래에 있는 루트 CA의 이름이 표시됩니다. 트리에서 CA 또는 하위 CA를 선택하면 CA 인증서, AIA 위치 및 CDP의 이름이 표시됩니다.
  + 상태 - CA 상태(선택한 CA와 연관되어 있는 아이콘으로도 트리에 표시됨)나 CA 인증서, AIA 위치 또는 CDP의 상태(정상 및 다운로드할 수 없음과 같은 상태 텍스트 설명으로 표시됨)를 간략하게 설명합니다.
  + 위치 - 인증서 각각에 대한 AIA 위치 및 CDP(프로토콜 및 경로)를 보여 줍니다. file://, HTTP:// 및 LDAP://를 예로 들 수 있습니다.
* 작업 - 이 창은 동작**,** 보기및 도움말 메뉴를 사용하는 것과 같은 기능을 제공합니다.

트리 또는 결과 창에서 선택한 항목에 따라 사용자는 작업 창의 AIA 및 CRL 정보를 비롯하여 CA와 CA 인증서의 세부 정보를 볼 수 있습니다. 또한 엔터프라이즈 PKI 구조를 관리하고 CA 인증서 또는 CRL을 수정하거나 변경할 수 있습니다.

### 인증서 서비스

인증서 서비스는 공개 키 기술을 기반으로 한 소프트웨어 보안 시스템에 사용되는 인증서를 발급 및 관리할 수 있도록 사용자 지정 가능 서비스를 제공합니다. Windows Vista 및 Windows Server 2008에는 인증서 서비스에 대한 새 기능의 도입과 더불어, 새 COM 등록 제어, 새 등록 DLL 및 공개 키 인프라 통신 프로토콜인 SCEP(단순 인증서 등록 프로토콜)가 도입되었습니다.

### 인증서 웹 등록

Windows Server 2008의 인증서 웹 등록 지원은 여러 가지 측면에서 변경되었습니다. 일례로, 이전 ActiveX 등록 컨트롤이 Windows Vista 및 Windows Server 2008에서는 새로운 COM 등록 컨트롤로 바뀌었습니다.

인증서 웹 등록은 Windows 2000 운영 체제 이후 제공되었으며, 도메인에 가입되지 않았거나 네트워크에 직접 연결되지 않은 사용자 및 컴퓨터를 비롯하여 타사 운영 체제 사용자를 위해 인증서를 발급하고 갱신해야 하는 조직에 등록 메커니즘을 제공하기 위해 설계되었습니다. 이러한 사용자는 CA(인증 기관)의 자동 등록 메커니즘이나 인증서 요청 마법사를 사용하는 대신, Windows 기반 CA에서 제공하는 웹 등록 지원을 사용하여 인터넷 또는 인트라넷 연결을 통해 신규 및 갱신된 인증서를 요청하고 얻을 수 있습니다.

#### 변경된 기능

이전 등록 컨트롤이었던 XEnroll.dll은 Windows Vista 및 Windows Server 2008에서 제거되었으며 대신 CertEnroll.dll이 새로운 등록 컨트롤로 소개되었습니다. 웹 등록 프로세스는 본질적으로 이전과 동일하지만, 이러한 등록 컨트롤 변경은 Windows Vista 또는 Windows Server 2008을 실행하는 사용자나 컴퓨터가 이전 버전의 Windows에 설치된 웹 등록 페이지에서 인증서를 요청하려고 할 때 호환성에 영향을 줄 수 있습니다.

Windows Server 2008 CA는 Windows XP 및 Windows Server 2003 클라이언트를 실행하는 사용자의 인증서 웹 등록 요청을 점차적으로 지원할 예정입니다. 사용자가 Windows XP, Windows Server 2003 또는 Windows 2000 기반 컴퓨터에서 Windows Server 2008 웹 등록 페이지를 통해 인증서를 등록하려고 하면 웹 등록 페이지에서는 이를 감지하여 클라이언트에 로컬로 설치된 Xenroll.dll을 사용합니다. 단, 다음과 같은 클라이언트 동작은 이전 버전의 Windows에서와 다릅니다.

* Windows Vista는 고유한 등록 에이전트 기능을 제공하므로 Windows Server 2008의 웹 등록에서는 등록 에이전트 기능(스마트 카드 등록 스테이션이라고도 함)이 제거되었습니다. 사용자가 Windows Server 2008 웹 등록을 사용하는 다른 클라이언트를 대신하여 등록을 수행해야 하는 경우 Windows Vista를 실행하는 컴퓨터를 등록 스테이션으로 사용해야 합니다. 또는 웹 등록이 설치된 Windows Server 2003 기반 서버를 사용하고 해당 서버를 등록 에이전트로 사용하여 Windows Server 2008 CA를 통해 인증서를 등록할 수도 있습니다.
* Internet Explorer 버전 6.x 이상 또는 Netscape 8.1 브라우저 사용자만 웹 등록 페이지를 통해 직접 인증서 요청을 제출할 수 있습니다. 다른 웹 브라우저 사용자도 웹 등록 페이지를 통해 등록 요청을 제출할 수 있기는 하지만, 먼저 웹 등록 페이지를 통해 제출할 PKCS#10 요청을 미리 생성해야 합니다.
* 인증서 웹 등록은 Suite B를 준수하는 인증서의 발급을 지원하기 위해 Windows Server 2008에 소개된 버전 3.0 인증서 템플릿과 함께 사용할 수 없습니다.
* Internet Explorer는 로컬 컴퓨터의 보안 컨텍스트에서 실행할 수 없으므로 사용자는 더 이상 웹 등록을 통해 컴퓨터 인증서를 요청할 수 없습니다.

### 네트워크 장치 등록

NDES(네트워크 장치 등록 서비스)는 Microsoft의 SCEP(단순 인증서 등록 프로토콜) 구현으로, MSCEP(Microsoft 단순 인증서 프로토콜) 호출에 사용됩니다. SCEP는 다른 방식으로는 네트워크에서 인증을 받을 수 없는 라우터, 스위치 등의 네트워크 장치에서 실행 중인 소프트웨어가 CA(인증 기관)의 x509 인증서를 등록할 수 있도록 해 주는 PKI(공개 키 인프라) 통신 프로토콜입니다. MSCEP(Microsoft SCEP)는 Windows의 SCEP 구현입니다.

MSCEP는 IIS(인터넷 정보 서비스)에서 ISAPI(인터넷 서버 응용 프로그래밍 인터페이스) 필터로 작동하여 다음 기능을 수행합니다.

* 일회용 등록 암호를 생성하여 관리자에게 제공
* 네트워크 장치에서 실행되는 소프트웨어를 대신하여 SCEP 등록 요청 수신 및 처리
* CA에서 대기 중인 요청 검색

Windows Server 2003에서 MSCEP는 CA와 같은 컴퓨터에 설치되어야 하는 Windows Server 2003 Resource Kit 추가 기능이었습니다. Windows Server 2008에서 MSCEP는 운영 체제에 속하므로 CA와 다른 컴퓨터에 설치될 수 있습니다.

NDES 및 SCEP를 통해 조직은 라우터, 스위치 등의 네트워크 장치를 인증할 수 있도록 하여 보안을 강화할 수 있습니다.

### 그룹 정책으로 인증서 관리

응용 프로그램이 신뢰할 수 있는 소스로부터 온 것인지 확인하기 위해 소프트웨어 서명을 사용하는 소프트웨어 게시자와 응용 프로그램 개발자가 늘어나고 있습니다. 하지만 아직 다수의 사용자들은 설치한 응용 프로그램과 연관된 인증서를 이해하지 못하거나 주의를 기울이지 않고 있습니다. X.509 공개 키 인프라가 점차적으로 신뢰의 기반으로 널리 사용되면서 인증서 경로 검색 및 경로 유효성 검사를 관리하는 데 추가 옵션을 필요로 하는 조직이 많아지고 있습니다. Windows Server 2008 그룹 정책의 인증서 설정을 통해 관리자는 조직의 보안 요구에 따라 인증서 유효성 검사 설정을 관리하고 중앙 위치에서 도메인의 모든 컴퓨터에 대한 인증서 설정을 관리할 수 있습니다.

예를 들어, 특정 중개 CA(인증 기관) 인증서가 만료되고 클라이언트가 자동으로 새 인증서를 검색할 수 없는 경우 관리자는 그룹 정책을 통해 이러한 인증서를 클라이언트 컴퓨터에 배포할 수 있게 되었습니다. 관련된 다른 시나리오로는, 관리자들이 사용자가 승인되지 않은 게시자 인증서로 서명된 응용 프로그램을 설치하지 않도록 하려는 경우를 들 수 있습니다.

이 기능은 하나 이상의 Windows 기반 CA를 사용하는 PKI(공개 키 인프라)를 가지며 그룹 정책을 통해 클라이언트 컴퓨터를 관리하는 조직에 적용됩니다.

그룹 정책의 인증서 유효성 검사 설정을 사용하여 다음을 수행할 수 있습니다.

* 보안 설계자가 인증서 기반 신뢰 사용을 향상시킬 수 있습니다.
* 보안 관리자가 환경에서 PKI 사용 응용 프로그램을 관리할 수 있습니다.

인증서 신뢰 관련 그룹 정책 설정을 사용하려면 조직 내 사용자와 컴퓨터의 인증서 요구 사항 및 해당 인증서에 대해 사용자와 컴퓨터에 부여할 제어 수준을 신중하게 계획하여 결정해야 합니다. 관리자는 사용자가 인증서의 중요성과 인증서 관리 소홀로 인한 위험을 파악하고 인증서를 적절하게 관리하는 방법을 이해할 수 있도록 이러한 설정을 사용할 때 명확하고 효율적인 교육을 실시하여 사용자를 도울 수 있습니다.

### 인증서 관련 그룹 정책 설정

이전 버전의 Windows 운영 체제에는 인증서 유효성 검사에 대해 이러한 종류의 제어 기능을 구현하는 설정이 거의 없었습니다. 인증서 관련 그룹 정책 설정은 컴퓨터 구성\Windows 설정\보안 설정\공개 키 정책 아래의 그룹 정책 개체 편집기에서 확인할 수 있습니다**.** 다음 정책 옵션은 인증서 경로 유효성 검사 설정 속성 시트의 별도 탭에서 관리할 수 있습니다.

* 저장소
* 신뢰할 수 있는 게시자
* 네트워크 검색
* 해지

또한 클라이언트에 다른 유형의 인증서를 배포하는 데 사용할 수 있도록 다음과 같은 네 개의 새로운 정책 저장소가 공개 키 정책에 추가되었습니다.

* 중개 인증 기관
* 신뢰할 수 있는 게시자
* 신뢰할 수 없는 인증서
* 신뢰할 수 있는 사용자

이러한 새 정책 저장소는 Windows Server 2003에 제공된 엔터프라이즈 신뢰 및 신뢰할 수 있는 루트 인증 기관 저장소와 함께 사용됩니다. 이와 같은 경로 유효성 검사 설정 및 인증서 저장소를 사용하여 다음과 같은 작업을 완료할 수 있습니다.

* 피어 트러스트 및 신뢰할 수 있는 루트 인증서 저장소 관리
* 신뢰할 수 있는 게시자 관리
* 정책에 따라 신뢰할 수 없는 인증서 차단
* 인증서 관련 데이터 검색 관리
* CRL 및 OCSP(온라인 인증서 상태 프로토콜) 응답에 대한 만료 시간 관리
* 인증서 배포

### 피어 트러스트 및 신뢰할 수 있는 루트 CA 저장소 관리

인증서 경로 유효성 검사 설정 대화 상자의 저장소 탭에서 관리자는 사용자가 신뢰할 수 있는 루트 인증서 및 피어 트러스트 인증서를 관리할 수 있도록 조정할 수 있습니다. 이 제어 기능을 통해 사용자가 루트 또는 피어 트러스트를 결정할 수 없도록 할 수도 있고 사용자가 피어 트러스트에 대해 관리할 수 있는 특정 인증서 용도(예: 서명 및 암호화)의 수를 제어할 수도 있습니다.

또한 저장소 탭에서 관리자는 도메인에 가입된 컴퓨터의 사용자가 엔터프라이즈 루트 CA만 신뢰할 수 있는지 아니면 엔터프라이즈 루트 CA와 타사 루트 CA를 모두 신뢰할 수 있는지 지정할 수 있습니다. 이에 반해, 관리자가 선택한 신뢰할 수 있는 루트 인증서를 도메인의 컴퓨터에 배포해야 하는 경우 신뢰할 수 있는 루트 인증서 저장소에 신뢰할 수 있는 루트 인증서를 복사하는 방식으로 작업을 수행할 수 있습니다. 그러면 다음 번에 도메인 정책이 새로 고쳐질 때 배포된 내용이 해당 인증서 저장소에 전파됩니다.

인증서가 점차 다양하게 사용되고 이러한 인증서를 인식하도록 할지 여부를 결정하는 것이 중요해지면서, 인증서 신뢰를 관리하고 도메인의 사용자가 조직의 신뢰할 수 있는 루트 인증서 집합을 구성하지 못하도록 하려는 조직도 있습니다.

### 신뢰할 수 있는 게시자 관리 및 원치 않는 인증서 차단

인증서 경로 유효성 검사 설정 대화 상자의 신뢰할 수 있는 게시자탭에서관리자는 신뢰할 수 있는 게시자로부터 온 것으로 수락할 수 있는 인증서를 제어할 수 있습니다. 전사적으로 신뢰할 수 있는 게시자 정책 옵션을 지정하면 조직은 Authenticode 인증서를 사용자와 관리자가 모두 관리할 수 있는지, 관리자만 관리할 수 있는지 아니면 엔터프라이즈 관리자만 관리할 수 있는지 결정할 수 있습니다.

관리자는 특정 인증서를 신뢰할 수 없는 인증서 저장소에 추가하여 이러한 인증서가 조직에서 사용되지 않도록 할 수도 있습니다. 네트워크 관리자가 바이러스 및 기타 악의적인 소프트웨어의 조직 환경 침투를 막는 작업을 담당했듯이 나중에는 관리자가 특정 인증서의 사용을 차단하고자 할 수 있습니다. 조직의 고유 CA에서 발급된 인증서는 해지할 수 있으며 이 경우 해당 인증서는 인증서 해지 목록에 추가됩니다. 외부 CA에서 발급된 인증서는 해지할 수 없습니다. 단, 이러한 인증서가 신뢰할 수 없는 인증서인 경우 신뢰할 수 없는 인증서 저장소에 추가하여 차단할 수 있습니다. 이러한 인증서는 다음 번에 그룹 정책이 새로 고쳐질 때 도메인에 속한 각 컴퓨터의 신뢰할 수 없는 인증서 저장소에 복사됩니다.

### 인증서 배포 변경

자동 등록, 인증서 요청 마법사, 웹 등록 등의 여러 메커니즘을 사용하여 사용자 및 컴퓨터 인증서를 배포할 수 있습니다. 하지만 여러 대의 컴퓨터에 다른 유형의 인증서를 배포하는 작업은 어려울 수 있습니다. Windows Server 2003에서는 그룹 정책을 사용하여 신뢰할 수 있는 루트 CA 인증서와 엔터프라이즈 신뢰 인증서를 배포할 수 있었습니다.

Windows Server 2008에서는 다음과 같은 유형의 인증서를 그룹 정책의 적절한 인증서 저장소에 배치하여 모두 배포할 수 있습니다.

* 신뢰할 수 있는 루트 CA 인증서
* 엔터프라이즈 신뢰 인증서
* 중개 CA 인증서
* 신뢰할 수 있는 게시자 인증서
* 신뢰할 수 없는 인증서
* 신뢰할 수 있는 사용자(피어 트러스트 인증서)

이를 통해 관리자는 조직 내 사용자와 컴퓨터에 점점 다양해지는 인증서를 효율적인 방식으로 배포할 수 있습니다.

### 온라인 인증서 상태 프로토콜 지원

인증 기관에서 발급된 인증서를 관리하는 과정에는 인증서 해지가 필요합니다. 인증서 상태를 전달하는 가장 일반적인 방식은 CRL(인증서 해지 목록)을 배포하는 것입니다. 기존의 CRL을 사용하는 것이 최적의 솔루션이 아닌 경우 Windows Server 2008의 OCSP(온라인 인증서 상태 프로토콜) 지원을 통해 해지 상태 정보를 관리하고 배포할 수 있습니다.

#### OCSP에서 지원하는 기능

온라인 인증서 상태 프로토콜 응답 및 CRL 사용은 인증서 유효성 검사 정보를 전달하는 가장 일반적인 두 가지 방식입니다. 주기적으로 배포되며 해지되었거나 일시 중단된 모든 인증서의 정보를 포함하는 CRL과 달리, 온라인 응답자는 단일 인증서의 상태 정보에 대해서만 클라이언트와 요청을 주고 받습니다. 요청당 검색되는 데이터의 양은 해지되었을 수 있는 인증서 수에 관계없이 일정하게 유지됩니다.

여러 가지 경우에 온라인 응답자는 인증서 해지 목록을 사용하는 것보다 효율적으로 인증서 상태 요청을 처리할 수 있습니다. 이러한 경우의 예는 다음과 같습니다.

* 클라이언트가 원격으로 네트워크에 연결하며 대용량 CRL을 다운로드할 필요가 없고 대용량 CRL 다운로드에 필요한 초고속 연결을 사용하지 않을 경우
* 네트워크가 해지 확인 활동에서 높은 사용량을 처리해야 하는 경우(예: 많은 수의 사용자가 로그온하거나 서명된 전자 메일 메시지를 동시에 보내는 경우)
* 조직이 타사 CA에서 발급된 인증서의 해지 데이터를 배포하기 위해 효율적인 방식을 필요로 하는 경우
* 조직이 해지되었거나 일시 중단된 모든 인증서 정보를 제공하는 대신 개별 인증서 상태 요청 확인에 필요한 해지 확인 데이터만 제공하려는 경우

Windows Server 2008의 OCSP 지원에는 다음 내용이 포함됩니다.

* 웹 프록시 캐싱 - 온라인 응답자 웹 프록시 캐시는 온라인 응답자용 서비스 인터페이스입니다. 이는 IIS(인터넷 정보 서비스)가 호스팅하는 ISAPI(인터넷 서버 API) 확장으로 구현됩니다.
* Nonce 및 비 Nonce 요청 지원 - Nonce 및 비 Nonce 요청에 대한 구성 옵션을 사용하여 OCSP 응답의 재생 공격을 막을 수 있습니다.
* Windows 설치 통합 - Windows Server 역할 관리 도구를 사용하여 온라인 응답자를 설치할 수 있습니다.
* 고급 암호화 지원 - 암호화 작업에 ECC(Elliptic Curve Cryptography) 및 SHA-256 암호화를 사용하도록 OCSP 응답자를 구성할 수 있습니다.
* 미리 구성된 OCSP 인증서 템플릿 - Windows Server 2008에서 제공하는 OCSP 인증서 템플릿을 사용하여 OCSP 응답자 배포가 간소화되었습니다.
* Kerberos 프로토콜 통합 - 로그온 시 신속하게 서버 인증서의 유효성을 검사하기 위해 Kerberos 암호 인증과 함께 OCSP 요청 및 응답을 처리할 수 있습니다.

Microsoft 온라인 응답자는 RFC 2560(OCSP)을 기반으로 하며 이를 준수합니다. 따라서 온라인 응답자의 인증서 상태 응답은 OCSP 응답을 참조하는 경우가 많습니다.

### OCSP에서 제공하는 기능

온라인 응답자 서비스의 중요한 새로운 기능 집합으로 다음 두 가지를 들 수 있습니다.

* 온라인 응답자 - OCSP 서비스가 설치된 단일 컴퓨터에서 제공하는 기본적인 온라인 응답 기능
* 응답자 배열 - 온라인 응답자를 호스팅하고 인증서 상태 요청을 처리하는 다중 연결 컴퓨터

온라인 응답자는 OCSP 서비스가 실행되고 있는 컴퓨터입니다. CA를 호스팅하는 컴퓨터를 온라인 응답자로 구성할 수도 있지만 CA와 온라인 응답자를 별도의 컴퓨터에서 유지 관리하는 것이 좋습니다. 단일 온라인 응답자는 하나의 CA 또는 여러 CA에서 발급된 인증서에 대한 해지 상태 정보를 제공할 수 있습니다. 둘 이상의 온라인 응답자에서 CA 해지 정보를 지원할 수 있습니다.

S/MIME(Secure/Multipurpose Internet Mail Extensions), SSL(Secure Sockets Layer), EFS(파일 암호화 시스템), 스마트 카드 등 X.509 인증서를 사용하는 응용 프로그램은 인증, 서명 또는 암호화 작업을 수행하는 데 사용될 때마다 인증서 상태의 유효성을 검사해야 합니다. 인증서 상태 및 해지 확인은 다음을 기반으로 인증서 유효성을 검사합니다.

* 시간 - 인증서는 사용 기간이 지정된 상태로 발급되며, 인증서 만료 날짜에 도달하지 않았고 이 날짜 전에 인증서가 해지되지 않은 경우 유효한 것으로 간주됩니다.
* 해지 상태 - 키 손상, 일시 중단 등 여러 가지 이유로 만료 날짜 전에 인증서를 해지할 수 있습니다.

인증서 해지 목록에는 해지한 CA에서 발급된 모든 인증서의 일련 번호가 포함됩니다. 클라이언트가 인증서 해지 상태를 확인하려면 CA에 의해 해지된 모든 인증서의 정보를 포함하는 CRL을 다운로드해야 합니다.

### OSCP에 대한 그룹 정책 설정

OCSP 및 CRL 데이터 사용 관리를 향상시키기 위해 여러 가지 그룹 정책 설정이 추가되었습니다. CRL에도 인증서와 마찬가지로 만료 날짜가 지정됩니다. 업데이트가 게시되거나 액세스 가능한 상태가 되기 전에 만료 날짜가 경과한 경우 온라인 응답자가 있어도 인증서 체인 유효성 검사를 실패할 수 있습니다. 온라인 응답자는 만료된 CRL의 데이터를 사용하기 때문입니다. 네트워크 상태로 인해 업데이트된 CRL의 적시 게시 및 수신이 지연될 수 있는 경우 관리자는 이러한 그룹 정책 설정을 사용하여 기존 CRL 또는 OCSP 응답의 만료 시간을 연장할 수 있습니다.

CRL 및 OCSP 응답 수명을 연장하려면인증서 경로 유효성 검사 설정(컴퓨터 구성 **>** Windows 설정 **>** 보안 설정>공개 키 정책)의 해지탭으로 이동하여 다음 두 가지 옵션을 구성하면 됩니다.

* 모든 CRL 및 OCSP 응답이 해당 수명보다 오랫동안 유효하도록 허용
* 유효 기간을 확장할 수 있는 기본 시간

**해지** 탭의 각 옵션을 통해 OCSP 응답이 CRL에 포함된 정보로 재정의되도록 할 수 있습니다. 그러면 클라이언트가 해지 상태를 포함하지 않는 CRL을 가진 경우 로컬 CRL에 인증서를 추가하여 해지된 인증서가 유효한 상태로 확인되도록 설정할 수 있습니다. 이 옵션은 권장되지 않지만 로컬 관리자가 변경한 해지 내용이 CA 관리자의 변경 확인 전까지 최종 확정되지 않는 상황에서는 유용할 수 있습니다.

### V3 인증서 템플릿

인증서 템플릿은 엔터프라이즈 인증 기관을 사용하는 관리 Active Directory 환경에서 인증서 등록을 구현할 수 있는 실용적인 방법을 제공합니다. CA 관리자는 엔터프라이즈 CA에서 등록된 인증서에 대한 청사진을 정의할 수 있습니다. 최초로 Windows 2000 Server에서 정적 V1 인증서 템플릿이 소개되었습니다. Windows Server 2003에서는 V2 인증서 템플릿에 사용자 지정이 도입되었고, Windows Server 2008에서는 더 많은 인증서 템플릿과 인증서 템플릿 속성을 사용할 수 있게 되었습니다. Windows Server 2008의 새로운 인증서 템플릿 유형을 V3 템플릿이라고 합니다.

V3 템플릿은 Windows Server 2008에 소개된 최신 암호화 알고리즘을 활용할 수 있습니다. V3 인증서 템플릿을 사용하여 관리자는 클라이언트와 CA 간의 CA 관련 통신이 가장 안전한 방식으로 수행되도록 할 수도 있습니다. 또한 Windows Server 2008은 클라이언트가 Kerberos 인증을 사용하여 인증서 원본의 유효성을 검사할 수 있도록 완전히 새로운 기본 템플릿을 소개합니다.

기본 운영 체제의 종속성으로 인해 Windows Server 2008 템플릿은 Windows Server 2008에서도 실행되고 있는 CA에만 지정될 수 있습니다. 또한 Windows Vista 클라이언트 컴퓨터와 Windows Server 2008 컴퓨터만 V3 인증서 템플릿을 등록할 수 있습니다.

표 10

|  |  |  |
| --- | --- | --- |
| **템플릿** | **템플릿 수정에 필요한 Windows 버전** | **템플릿을 지정할 수 있는 CA의 Windows 버전** |
| V1 템플릿 | 해당 없음(V1 이후의 템플릿은 정적 템플릿임) | Windows 2000 Enterprise Edition  Windows Server 2003 Enterprise Edition  Windows Server 2008 |
| V2 템플릿 | Windows Server 2003  Windows XP  Windows Server 2008 | Windows Server 2003 Enterprise Edition  Windows Server 2008 Enterprise Edition |
| V3 템플릿 | Windows Server 2008 | Windows Server 2008 |

Windows Server 2008과 Windows Vista에서 중요한 변화 중 하나는 CNG(Cryptography Next Generation)가 추가된 것입니다. CNG는 Suite-B 알고리즘을 지원하여 암호화와 서명 인증서에 대체 및 사용자 지정 암호화 알고리즘을 사용할 수 있도록 합니다.

### CNG(Cryptography Next Generation)

CNG(Cryptography Next Generation)는 IT 전문가가 AD CS(Active Directory 인증서 서비스), SSL(Secure Sockets Layer), IPSec(인터넷 프로토콜 보안) 등 암호화 관련 응용 프로그램에서 사용자 지정 암호화 알고리즘을 생성, 업데이트 및 사용할 수 있도록 유연한 암호화 개발 플랫폼을 제공합니다. CNG는 미 정부의 Suite B 암호화 알고리즘을 구현합니다. 여기에는 암호화, 디지털 서명, 키 교환 및 해싱에 대한 알고리즘이 포함됩니다.

CNG는 암호화 키 만들기, 저장, 검색 등의 기본적인 암호화 작업을 수행하는 데 사용되는 일련의 API를 제공합니다. 또한 추가 암호화 공급자 설치 및 사용을 지원합니다. CNG를 통해 조직 및 개발자는 고유 암호화 알고리즘을 사용하거나 표준 암호화 알고리즘을 구현할 수 있습니다. Windows Server 2008 및 Windows Vista에서 지원하는 CNG에는 다음과 같은 기능이 있습니다.

* CNG를 통해 고객은 고유 암호화 알고리즘을 사용하거나 표준 암호화 알고리즘을 구현할 수 있습니다. 또한 고객은 새 알고리즘을 추가할 수 있습니다.
* CNG는 커널 모드로 암호화를 지원합니다. 완벽한 암호화 기능을 지원하기 위해 커널 모드와 사용자 모드에서 같은 API가 사용됩니다. CNG를 사용하는 프로세스를 시작할 때 외에도 SSL/TLS(Secure Sockets Layer/전송 계층 보안) 및 IPSec가 커널 모드로 작동합니다.
* CNG 계획에는 공통 기준 평가와 함께 FIPS(Federal Information Processing Standards) 140-2 level-2 인증서를 얻는 과정이 포함됩니다.
* CNG는 보안 프로세스에 오래된 키를 사용하고 저장하여 공통 기준 요구 사항을 준수합니다.
* CNG는 CryptoAPI 1.0 알고리즘의 현재 집합을 지원합니다.
* CNG는 ECC(Elliptic Curve Cryptography) 알고리즘을 지원합니다. 미 정부의 Suite B 작업에는 여러 ECC 알고리즘이 필요합니다.
* TPM(신뢰할 수 있는 플랫폼 모듈)을 사용하는 컴퓨터는 TPM에 키를 격리하고 저장할 수 있습니다.

CNG는 CryptoAPI 1.0 알고리즘의 현재 집합과 함께 ECC(Elliptic Curve Cryptography) 알고리즘도 지원합니다. 미 정부의 Suite B 작업에는 여러 ECC 알고리즘이 필요합니다.

Suite B에 대한 자세한 내용은 http://www.nsa.gov/ia/industry/crypto\_suite\_b.cfm을 참조하십시오.

## Windows Server 2008의 ID 및 액세스 관리

사용자 ID 관리는 오늘날 여러 비즈니스에서 가장 중요한 요소 중 하나입니다. 사용자는 유형이 다른 장치를 사용하여 회사 네트워크의 여러 시스템과 리소스에 액세스해야 합니다. 이러한 시스템은 대부분 상호 통신이 불가능하므로 같은 사용자에 대해 여러 ID가 사용될 수 밖에 없습니다. 따라서 이와 같이 중복되는 ID를 관리하는 작업은 복잡하고 시간이 많이 걸리며 오류와 체계화되지 못한 사용자 암호 관리를 야기하여 보안 위험을 높입니다.

Microsoft IDA(ID 및 액세스) 솔루션은 조직이 사용자 ID 및 관련 액세스 권한을 관리할 수 있도록 하기 위해 설계된 일련의 플랫폼 기술 및 제품입니다. 보안 및 사용의 용이성에 초점이 맞추어진 이들 솔루션은 기업이 생산성을 높이고 IT 비용을 절감하고 ID 및 액세스 관리의 복잡성을 제거할 수 있도록 해 줍니다. Microsoft ID 및 액세스 솔루션은 다음과 같은 다섯 가지 고유 영역으로 분류됩니다.

* ID 관리 - ID 및 액세스 관리를 자동화합니다.
* 정보 보호 - 위치에 관계없이 기밀 데이터를 보호합니다.
* 페더레이션 ID - 조직 경계에 구애 받지 않고 안전하게 공동 작업을 수행합니다.
* 디렉터리 서비스 - 사용자 및 장치 관리를 간소화합니다.
* 강력한 인증 - 최신 암호화 표준과 혁신적인 인증서 관리를 통합하여 보안 액세스를 사용자 이름 및 암호 이상으로 확대합니다.

Microsoft Windows Server 2008은 포괄적으로 통합된 ID 및 액세스 플랫폼을 제공합니다. Microsoft IDA 플랫폼은 Active Directory를 기반으로 구축되었으며 전체 조직이 조직 내외부의 사용자와 쉽게 공동 작업을 수행하면서 중요한 정보를 보호하는 데 기여할 수 있도록 IT 전문가, 개발자 및 정보 근로자에게 친숙한 인터페이스를 제공합니다. Windows 환경의 통합된 지원은 쉽게 사용할 수 있는 파트너 솔루션과 함께 다른 유형의 환경 지원으로 확대될 수 있습니다. 이러한 플랫폼 기능은 각각 여러 키 구성 요소를 가지는 다음과 같은 세 가지 서비스 범주로 분류됩니다.

* 디렉터리 서비스
  + RODC(읽기 전용 도메인 컨트롤러)
  + AD FS(Active Directory Federation Services)
  + 디렉터리 서비스 감사
  + 서비스 기반 AD DS(Active Directory 도메인 서비스)
* 정보 보호
  + 페더레이션 공동 작업
  + BitLocker
  + 페더레이션 권한 관리
* 강력한 인증
  + 암호화 API
  + V3 인증서 템플릿
  + PKI(공개 키 인프라)

### Active Directory Rights Management Services

Windows Server 2008 AD RMS(Rights Management Services)(Windows RMS에서 변경됨)는 중요한 정보를 보호하는 데 있어 핵심 요소입니다. Windows Server 2008이 릴리스되기 전에는 RMS 보호 문서를 회사 네트워크 외부 사용자와 공유하려는 경우 이 수신자가 자체 조직 내에 호환되는 RMS 서버를 갖추고 있어야 했습니다. 또는 외부 사용자에게 회사 네트워크 *내부*의 Active Directory 계정을 부여해야 했습니다. 이는 해결하기 힘든 관리 및 보안 문제를 야기하는 프로세스입니다. Microsoft 공동 작업 플랫폼인 Microsoft Office SharePoint Server 2007도 사용자의 Active Directory 프로필을 기반으로 문서에 동적으로 RMS 보호를 적용하는 기능을 갖추고 있었지만 마찬가지로 로컬 Active Directory 계정을 사용해야 했습니다.

이제 Windows Server 2008을 통해 보다 포괄적이면서도 관리가 쉬운 새로운 방식으로 중요한 정보를 보호할 수 있습니다. Windows Server 2003에서 AD FS(Active Directory Federation Services)를 사용하는 조직은 다른 조직과 페더레이션 트러스트 관계를 설정할 수 있습니다. 한 번 로컬 도메인에 로그인한 사용자는 ID 및 액세스 페더레이션을 통해 파트너 도메인에 대한 액세스 권한을 얻게 됩니다. AD RMS는 Windows Server 2008에서 AD FS와 통합되어 있으므로 이제 페더레이션 트러스트를 통해 AD RMS는 로컬로 로그인하거나 자체적으로 AD RMS 서버를 설치하지 않은 외부 사용자에게 적절한 RMS 권한을 부여할 수 있습니다.

이 시나리오를 "보안 페더레이션 공동 작업"이라고 합니다. 본질적으로 RMS 보호 정보를 공유하려는 회사 내 관리자는 더 이상 외부 사용자에 대해 별도의 사용자 이름과 암호를 관리할 필요가 없습니다. 또한 외부 사용자는 여러 ID를 기억해야 하는 번거로움 없이 SSO(Single Sign-On)만으로 RMS 보호 콘텐츠에 액세스할 수 있게 되었습니다. 즉, 파트너든, 공급자든, 고객이든 누구와도 기밀 정보를 안전하게 공유하는 작업이 훨씬 쉬워졌습니다. 외부 사용자가 인증되면 자동으로 RMS는 외부 사용자가 공동으로 작업할 수 있도록 적절한 모든 라이선스와 조직의 중요한 내부 콘텐츠를 제공합니다. 관리자는 여러 파트너 관계에 적용할 수 있는 템플릿을 정의하는 권한을 비롯하여 이러한 외부 사용자가 보호된 콘텐츠를 사용하는 방법을 세밀하게 제어할 수 있는 권한을 얻게 됩니다.

Windows Server 2008에서 AD FS와 AD RMS는 다른 도메인의 사용자가 로컬 Active Directory 프로필이 아닌 페더레이션 ID를 기반으로 문서를 안전하게 공유할 수 있도록 함께 작업합니다. 이를 통해 사용자를 인증하고 사용자의 콘텐츠 액세스를 제어하는 AD FS 클레임을 해석할 수 있습니다. 외부 사용자가 로컬 Active Directory 도메인에 로그인하면 이 사용자에게 부여될 인증서 및 액세스 권한을 포함하는 페더레이션 클레임이 제공됩니다.

이는 외부 사용자에 대한 섀도 계정을 유지 관리할 필요 없이 해당 사용자에게 RMS 보호 콘텐츠에 대한 Single Sing-On 액세스 권한을 제공하는 강력한 새 콘텐츠 공유 시나리오(페더레이션 문서 공동 작업)를 만듭니다. 두 엔터티가 페더레이션 트러스트 관계를 설정하면 사용자는 같은 도메인에 있는 것처럼 보호 콘텐츠를 공유하고 사용할 수 있습니다. 리소스 공급자 측 관리자는 사용자 ID를 개별적으로 관리하지 않고도 특정 종류의 콘텐츠에 액세스할 수 있는 권한을 가진 사용자를 세밀하게 제어할 수 있습니다.

### Active Directory Federation Services

AD FS(Active Directory Federation Services)는 Windows Server 2008에서 서버로 사용되어, 여러 플랫폼에서 작동할 수 있는 확장성이 뛰어나고 안전한 ID 액세스 솔루션을 제공합니다. AD FS는 사용자 계정과 응용 프로그램이 다른 네트워크나 조직에 있는 경우에도 내외부 네트워크의 브라우저 기반 클라이언트에, 인터넷에 연결되어 있는 보호된 응용 프로그램에 대한 액세스 권한을 제공합니다.

일반적인 시나리오에서 응용 프로그램과 사용자 계정은 서로 다른 네트워크에 있습니다. 사용자는 응용 프로그램에 액세스하려고 할 때 보조 자격 증명을 입력해야 합니다. 하지만 AD FS를 사용하면 보조 계정이 필요하지 않습니다. 대신 신뢰 관계를 사용하여 사용자의 디지털 ID와 신뢰할 수 있는 파트너에 대한 액세스 권한을 추정할 수 있습니다. 페더레이션 환경에서 각 조직은 이전과 마찬가지로 고유 ID를 관리할 수 있지만 이전보다 안전한 방식으로 다른 조직의 ID를 추정하고 수락할 수 있습니다.

여러 조직에 페더레이션 서버를 배포하여 신뢰할 수 있는 파트너 조직 간의 B2B 트랜잭션을 원활하게 진행할 수 있습니다. 인터넷에서 액세스할 수 있는 리소스를 소유하고 관리하는 조직은 AD FS 페더레이션 서버 및 신뢰할 수 있는 파트너의 보호된 리소스에 대해서만 액세스를 관리하는 AD FS 사용 웹 서버를 배포할 수 있습니다.

AD FS에는 페더레이션 파트너 간의 트러스트 관계를 쉽게 설정할 수 있도록 해 주는 정책 가져오기/내보내기 기능이 있습니다. 멤버 자격 공급자는 페더레이션 파트너의 사용자를 위해 Windows SharePoint Services 및 RMS에 대한 역할 기반 권한 부여를 허용합니다. 관리자는 그룹 정책을 통해 페더레이션 서비스 배포를 제어할 수 있습니다. 여러 인증서 해지 확인 설정에 대한 지원도 제공됩니다.

또한 사용자 계정을 소유하고 관리하는 조직은 로컬 사용자를 인증하며 보안 토큰을 만드는 AD FS 페더레이션 서버를 배포할 수 있습니다. 리소스 조직의 페더레이션 서버는 권한 부여를 결정하는 데 이러한 보안 토큰을 사용할 수 있습니다.

### 지속적인 정보 보호

Windows Server 2008의 AD RMS는 여러 응용 프로그램 및 플랫폼에서 작동하면서 콘텐츠 위치와 관련된 순서에 따라 완벽하게 통합된 사용 권한 및 암호화를 제공합니다. 문서, 스프레드시트, 인트라넷 웹 사이트 및 전자 메일 메시지 보호에도 사용될 수 있습니다. 또한 개발자가 RMS를 사용하지 않는 응용 프로그램에 RMS 기능을 통합할 때 필요한 도구를 제공합니다. 조직에서는 즉시 적용 가능한 사용자 지정 사용 권한 템플릿을 만들 수도 있습니다.

AD RMS 서버와 클라이언트 시스템은 사용자 권한 부여부터 시작하여 첫 번째 위치에 있는 콘텐츠에 RMS 권한을 적용하는 프로세스를 시작합니다. RMS 서버가 사용자에게 권한 계정 인증서를 발급하면 해당 사용자는 콘텐츠를 보호할 수 있습니다. RMS 문서 보호를 사용하는 방법은 간단합니다. RMS 기능은 Microsoft Office Word 및 Microsoft Office Excel과 같은 Microsoft 생산 응용 프로그램에서 기본 제공됩니다. RMS 서버는 권한 정보와 콘텐츠를 결합하여 무단 액세스가 발생하지 않도록 콘텐츠를 암호화합니다. 사용자가 보호된 문서를 보거나 사용하려는 경우 RMS 서버는 알림을 표시한 후 사용자의 권한을 확인하고 암호화를 해독할지, 라이선스가 적절히 사용되고 있는지 확인합니다.

Windows Server 2008 릴리스 전 RMS 보호 콘텐츠에 액세스하려는 외부 사용자에게는 로컬 사용자 계정이 있어야 했습니다. 하지만 이제 더 이상 로컬 사용자 계정이 필요하지 않으며 이에 따라 외부 계정 관리가 간소화되었습니다.

### 시나리오: 안전하고 쉬운 공동 작업

Microsoft 페더레이션 권한 관리 솔루션을 사용하면 공유 콘텐츠를 통해 안전하게 공동 작업을 수행하는 것이 보다 쉬워지며 조직의 중요한 데이터 보호 수준이 강화됩니다. 일반적인 공동 작업 시나리오는 다른 조직의 사원과 기밀 정보를 공유해야 하는 회사에 적용됩니다. 예를 들어, Contoso는 신제품을 디자인하여 Fabrikam의 엔지니어에게 제품 사양 검토를 맡기고 생산 계획을 구상하려고 합니다. 제품 사양은 기밀이므로 Contoso는 엔지니어에게 읽기 권한만 제공하고 변경, 복사, 인쇄 또는 전달 권한은 부여하지 않고자 합니다.

이 경우 Contoso는 Office Word 2007의 통합된 RMS 기능을 사용하여 적절한 권한을 쉽게 적용할 수 있습니다. 두 회사가 Windows Server 2008의 AD FS를 사용하는 경우 페더레이션 트러스트 관계를 설정할 수 있습니다. Contoso는 이전과 동일한 방식으로 RMS 권한을 적용하면 되지만 Fabrikam 사원에게 로컬 Active Directory ID를 제공할 필요가 없습니다. 사원이 Fabrikam의 도메인에 로그인하면 사원에게 페더레이션 사용자 권한이 부여된 후 Contoso의 AD RMS 서버에서 해석할 수 있는 AD FS 클레임이 제공됩니다.

### 페더레이션 권한 관리 요약

공동 작업에 있어 보안 정책을 위반하지 않고 정보를 공유하는 것은 쉽지 않습니다. Windows Server 2008에 포함된 RMS 기술은 AD FS 개발과 함께 공동 작업을 안전하게 수행하는 데 큰 향상을 가져왔습니다. 이제 AD RMS와 AD FS의 통합으로 회사들은 이전보다 더 쉽고 안전하게 정보를 공유할 수 있게 되었습니다. RMS와 Office SharePoint Server 2007을 사용하여 AD FS 클레임을 해석하면 관리자는 불필요한 Active Directory 저장소를 유지 관리하면서 겪었던 보안 및 관리 문제로부터 벗어날 수 있습니다.

AD RM을 통해 문서, 데이터 및 전자 메일이 무단으로 사용되지 않도록 할 수 있습니다. RMS는 문서 소유자가 권한이 부여된 사용자를 식별하고 문서 사용 제한을 관리할 수 있도록 해 줍니다.

## 기타 보안 향상

Windows Server 2008에는 조직이 서버 및 네트워크의 보안을 강화시킬 수 있도록 지원하는 여러 가지 향상된 기능이 있습니다.

### 코드 무결성

코드 무결성은 운영 체제 실행 파일 및 DLL을 모두 서명하여 운영 체제가 실행 중일 때 운영 체제 파일을 보호할 수 있도록 해 줍니다. 그러면 파일이 메모리로 로드될 때 이러한 서명의 유효성이 검사됩니다.

### Windows 서비스 강화

Windows Server 2008은 비즈니스 응용 프로그램 및 서비스 실행에 사용할 강력한 기반을 제공하기 위해 운영 체제를 강화하고 환경을 보호합니다. Windows 서비스 강화 기능을 사용하면 중요한 Windows 서비스가 파일 시스템, 레지스트리 또는 네트워크에서 비정상적인 활동에 사용되지 못하도록 하여 시스템을 안전하게 유지할 수 있습니다. Windows 서비스 강화 기능을 사용하면 기본적으로 보다 적은 수의 서비스가 실행되며 서비스 계정에 부여되는 사용 권한도 적고 네트워크 액세스가 제한됩니다.

또한 Windows Server 2008에서는 커널 수준에서 실행해야 하는 코드의 양을 줄여 커널 모드 서비스에 대한 보호를 강화합니다. 예를 들어, 이전에는 커널 모드 코드와 사용자 모드 코드에서 모두 사용되는 몇몇 프린터 드라이버가 있었습니다. 서비스 강화를 통해 프린터 드라이버가 사용자 모드 계층으로 옮겨지면서 이제는 드라이버 자체에 커널 코드가 없습니다. 서비스 강화 기능은 필요한 최소 권한으로 서비스가 실행되도록 하여 시스템 보안을 향상시킵니다.

Windows 서비스 강화 기능은 중요한 Windows 서비스가 파일 시스템, 레지스트리 또는 네트워크에서 비정상적인 활동에 사용되지 않도록 합니다. 서비스 강화 기능은 플랫폼 침입 위험을 감소시킵니다.

### Windows Server Core

Server Core는 불필요한 기능 없이 특정 기능만 포함하는 최소한의 Windows Server 설치입니다. Server Core는 본 설명서의 "서버 관리" 섹션에서 설명됩니다.

### 이동식 장치 설치

Windows Server 2008은 USB 드라이브와 같은 이동식 장치로 데이터를 복사하지 못하도록 하는 방법을 제공합니다. 키보드, 마우스 또는 USB 드라이브에 대한 제어 권한을 결정하도록 그룹 정책 설정을 구성할 수 있습니다. 관리자는 다음을 비롯하여 이동식 장치 사용 방법을 유연하게 결정할 수 있습니다.

* 사용자가 장치를 설치하지 못하도록 합니다.
* 사용자가 "승인" 목록에 있는 장치만 설치할 수 있도록 합니다. 사용자는 이 목록에 있는 장치를 설치할 수 없습니다.
* 사용자가 "거부" 목록에 있는 장치를 설치하지 못하도록 합니다. 사용자는 이 목록에 없는 장치를 설치할 수 있습니다.
* 이동식 장치 사용자나 CD 및 DVD 버너, 플로피 디스크 드라이브, 외장 하드 드라이브 및 휴대용 장치(예: 미디어 플레이어, 스마트 폰 또는 Pocket PC 장치) 사용자에 대한 읽기 또는 쓰기 액세스 권한을 거부합니다.

사용자가 설치할 수 있는 장치를 제한하면 데이터 도난 위험을 줄일 수 있고, 사용자가 지원 센터의 교육을 받았으며 지원 자격을 갖춘 장치만 설치하도록 함으로써 지원 비용을 절감할 수 있습니다.

## NAP(네트워크 액세스 보호)

간단히 말해, NAP(네트워크 액세스 보호)는 규정을 준수하지 않는 컴퓨터가 조직의 네트워크에 액세스하여 네트워크를 손상시키지 않도록 해 줍니다. 클라이언트의 회사 네트워크 연결을 허용하기 전에 NAP를 사용하여 클라이언트 상태 요구 사항을 구성 및 적용하고 규정을 준수하지 않는 클라이언트 컴퓨터를 업데이트하거나 업데이트를 관리할 수 있습니다. NAP는 Microsoft 이외의 회사에서 자체 소프트웨어를 NAP 플랫폼에 통합할 수 있도록 일련의 API를 제공하기도 합니다. NAP API를 사용하여 소프트웨어 개발자와 공급업체는 추가 규정 준수 검증 및 적용 메커니즘으로 NAP의 기능을 사용자 지정할 수 있습니다.

### 네트워크 액세스 보호 소개

대부분의 조직은 네트워크에 배포할 수 있는 하드웨어와 소프트웨어의 유형을 지정하는 네트워크 정책을 만듭니다. 이러한 정책에는 네트워크에 연결하기 전에 클라이언트 컴퓨터를 구성하는 방법에 대한 규칙이 자주 포함됩니다. 예를 들어, 클라이언트 컴퓨터에서 최신 바이러스 백신 업데이트가 설치된 바이러스 백신 소프트웨어를 반드시 실행하도록 하고 조직의 네트워크에 연결하기 전에 클라이언트 컴퓨터에 소프트웨어 방화벽을 설치하여 사용하도록 하는 조직이 많습니다. 조직의 네트워크 정책에 따라 구성된 클라이언트 컴퓨터는 상태 정책을 준수하는 것으로 간주되고 조직의 네트워크 정책에 따라 구성되지 않은 컴퓨터는 상태 정책을 준수하지 않는 것으로 간주됩니다.

NAP는 관리자가 NPS(네트워크 정책 서버)를 사용하여 클라이언트 컴퓨터 상태를 정의하는 정책을 만들도록 해 줍니다. 또한 NAP는 조직에서 정의한 클라이언트 상태 정책을 적용합니다. 이는 컴퓨터 바이러스 등 클라이언트 컴퓨터로 인해 발생할 수 있는 유해한 요소로부터 네트워크를 보호합니다. NAP는 클라이언트가 클라이언트 상태 정책을 준수하도록 자동 업데이트 관리를 통해 NAP 가능 클라이언트 컴퓨터를 자동으로 업데이트할 수도 있습니다. 또한 NAP는 클라이언트 컴퓨터가 조직의 네트워크에 연결할 때는 규정을 준수하지만 연결되어 있는 상태에서 규정을 준수하지 않는 상황이 발생하지 않도록 하기 위해 클라이언트 컴퓨터 상태를 지속적으로 검색합니다.

NAP를 배포하려면 Windows Server 2008을 실행하고 있는 서버가 필요합니다. 또한 클라이언트 컴퓨터에서 Windows Vista, Windows Server 2008, Windows Server 2003 SP1 또는 Windows XP용 네트워크 액세스 보호 클라이언트가 설치된 Windows® XP 서비스 팩 2(SP2)가 실행되고 있어야 합니다.

### NAP 아키텍처

NAP 아키텍처는 다음 그림과 같이 클라이언트와 서버 구성 요소로 이루어집니다.

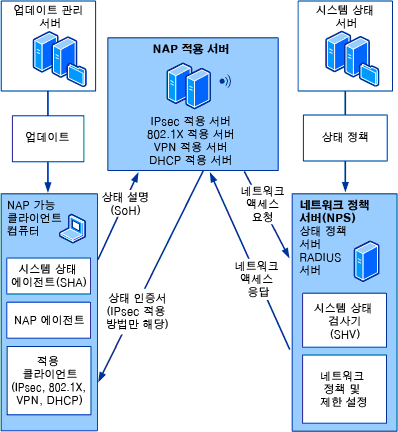


그림 4: NAP 아키텍처 클라이언트와 서버 구성 요소

### NAP 구성 요소

NAP는 여러 클라이언트와 서버 구성 요소로 이루어집니다. NAP 적용 방법 또는 IT 담당자가 선택한 방법에 따라 모든 NAP 배포에 사용되는 공통 NAP 구성 요소도 있고 특정 배포에만 사용되는 구성 요소도 있습니다.

NAP 적용 방법은 상태 정책 적용을 위해 NAP와 함께 사용되는 네 가지 네트워크 액세스 기술 즉, IPSec(인터넷 프로토콜 보안) 적용, 802.1X 적용, 라우팅 및 원격 액세스를 위한 VPN(가상 사설망) 적용, DHCP(Dynamic Host Configuration Protocol) 적용입니다.

#### 공통 NAP 구성 요소

공통 NAP 구성 요소는 클라이언트와 서버 구성 요소로 이루어집니다. NAP 가능 클라이언트란 NAP 구성 요소가 설치되어 있으며 네트워크 정책 서버로 상태 설명 목록을 보내 성능 상태를 확인할 수 있는 컴퓨터입니다.

#### 공통 클라이언트 구성 요소

공통 NAP 클라이언트 구성 요소는 다음과 같습니다.

* SHA(시스템 상태 에이전트) - SHA(시스템 상태 에이전트)는 NPS가 SHA에서 모니터링하는 설정이 최신이며 올바르게 구성되었는지 여부를 확인할 수 있도록 클라이언트 컴퓨터의 규정 준수 상태를 모니터링하고 보고합니다. 예를 들어, Microsoft SHA는 Windows 방화벽 사용 여부와 바이러스 백신 소프트웨어 설치, 사용 및 업데이트 여부를 확인하기 위해 상태를 모니터링할 수 있습니다. 추가 기능을 제공하는 다른 회사의 SHA를 사용할 수도 있습니다.
* SoH(상태 설명) - 상태 설명은 성능 상태를 인증하는 시스템 상태 에이전트의 선언입니다. 시스템 상태 에이전트는 상태 설명을 만들어 NAP 에이전트로 보냅니다.
* NAP 에이전트 - NAP 에이전트는 상태 정보를 수집 및 관리합니다. 또한 NAP 에이전트는 SHA의 상태 설명을 처리하고 설치된 적용 클라이언트에 클라이언트 상태를 보고합니다. NAP 클라이언트의 전체 성능 상태를 나타내기 위해 NAP 에이전트는 SoH 목록을 사용합니다.
* NAP EC(NAP 적용 클라이언트) - NAP를 사용하려면 클라이언트 컴퓨터에 하나 이상의 NAP 적용 클라이언트가 설치되어 사용되어야 합니다. 개별 NAP 적용 클라이언트는 적용 방법에 따라 다릅니다. NAP 적용 클라이언트는 네트워크에 대한 액세스를 요청하고, NPS 서버에 클라이언트 컴퓨터의 성능 상태를 전달하며, NAP 클라이언트 아키텍처의 다른 구성 요소에 제한된 클라이언트 컴퓨터 상태를 전달합니다.

#### 공통 서버 구성 요소

공통 NAP 서버 구성 요소는 다음과 같습니다.

* 상태 정책 - NPS 정책은 네트워크 액세스를 요청하는 클라이언트 컴퓨터에 대한 상태 요구 사항 및 적용 설정을 정의합니다. NPS는 NAP 적용 클라이언트가 보낸 SoH 목록을 포함하는 RADIUS 액세스 요청 메시지를 처리하여 NAP 관리 서버로 전달합니다.
* NAP 관리 서버 - NAP 관리 서버 구성 요소는 클라이언트 측의 NAP 에이전트와 유사한 처리 기능을 제공합니다. NPS를 통해 NAP 적용 서버로부터 SoH 목록을 받아서 각 SoH를 적절한 SHV에 배포합니다. 그런 다음, SHV로부터 SoH 응답 결과를 수집하여 NPS에 평가용으로 전송합니다.
* SHV(시스템 상태 검사기) - SHV는 SHA에 상응하는 서버 소프트웨어입니다. 클라이언트에서 각 SHA의 NPS에는 해당하는 SHV가 있습니다. SHV는 클라이언트 컴퓨터의 해당 SHA가 만든 SoH를 확인합니다.
  + 해당 정책 서버(필요한 경우) 및 업데이트 관리 서버와 함께 SHA와 SHV는 서로 대응됩니다.
  + SHA가 설치된 적이 없거나 손상 또는 제거된 경우와 같이 SoH가 수신되지 않은 것으로 SHV에 감지될 수도 있습니다. SoH가 정의된 정책을 충족하는지에 관계없이, SHV는 NAP 관리 서버에 SoHR(상태 설명 응답) 메시지를 보냅니다.
  + 하나의 네트워크에 두 종류 이상의 SHV가 있을 수도 있습니다. 이 경우 NPS 서버는 모든 SHV의 출력을 조정하고 비규격 컴퓨터의 액세스를 제한할지 여부를 결정해야 합니다. 따라서 환경에 대한 상태 정책을 정의하고 다른 SHV가 상호 작용하는 방식을 평가할 때는 주의해서 계획해야 합니다.
* NAP ES(NAP 적용 서버) - NAP 적용 서버에는 사용 중인 NAP 적용 방법에 해당하는 NAP EC가 지정되어 있습니다. 이 서버는 NAP EC에서 SoH 목록을 받은 후 평가를 위해 NPS에 전달합니다. 그 응답을 기반으로, NAP 가능 클라이언트에 제한된 또는 제한되지 않은 네트워크 액세스 권한을 제공하거나 네트워크 액세스 권한을 제공하지 않습니다. NAP 적용 유형에 따라, NAP ES는 인증 기관(IPSec 적용), 인증 스위치 또는 무선 액세스 지점(802.1x 적용), 라우팅 및 원격 액세스 서버(VPN 적용) 또는 DHCP 서버(DHCP 적용)일 수 있습니다.
* 정책 서버 - 정책 서버는 시스템 상태에 대한 요구 사항을 평가하는 데 사용되는 정보를 제공하기 위해 SHV와 통신하는 소프트웨어 구성 요소입니다. 예를 들어 바이러스 백신 서명 서버와 같은 정책 서버는 클라이언트 바이러스 백신 SoH의 유효성 검사를 위해 현재 서명 파일의 버전을 제공할 수 있습니다. 정책 서버에 해당하는 SHV가 있지만 모든 SHV에 정책 서버가 필요한 것은 아닙니다. 예를 들어 SHV는 NAP 가능 클라이언트가 로컬 시스템 설정에서 호스트 기반 방화벽이 사용되도록 설정되어 있는지 확인하게 할 수 있습니다.
* 업데이트 관리 서버 - 업데이트 관리 서버는 SHA가 비규격 클라이언트 컴퓨터를 규격 상태로 만드는 데 사용할 수 있는 업데이트를 호스팅합니다. 예를 들어 업데이트 관리 서버는 소프트웨어 업데이트를 호스팅할 수 있습니다. 상태 관리 정책에서 NAP 클라이언트 컴퓨터에 최신 소프트웨어 업데이트가 설치되어 있도록 요구할 경우 NAP EC는 이러한 업데이트가 없는 클라이언트의 네트워크 액세스를 제한합니다. 클라이언트가 상태 관리 정책을 준수하는 데 필요한 업데이트를 받으려면 업데이트 관리 서버가 제한된 네트워크 액세스 권한으로 클라이언트에 액세스할 수 있어야 합니다.
* SoHR(상태 설명 응답) - 해당 SHV에서 클라이언트 SoH가 상태 정책을 준수하는지 평가된 후에, 평가 결과가 포함된 상태 설명 응답이 생성됩니다. SoHR은 SoH의 경로를 역으로 이동하여 클라이언트 컴퓨터 SHA로 다시 전송됩니다. 클라이언트 컴퓨터가 비규격으로 간주될 경우 SoHR에는 클라이언트 컴퓨터 구성이 상태 요구를 준수하도록 하기 위해 SHA가 사용하는 업데이트 관리 지침이 포함됩니다.

각 유형의 SoH에 시스템 상태에 대한 다른 종류의 정보가 포함되어 있는 것처럼, 각 SoHR 메시지에는 상태 요구를 준수하는 방법에 대한 정보가 포함되어 있습니다.

### 클라이언트 컴퓨터 상태

NAP에서는 상태를 클라이언트에 제한없는 네트워크 액세스 권한 또는 제한된 액세스 권한이 부여되는지, 아니면 네트워크 액세스 권한이 부여되지 않는지를 확인하는 데 사용되는 클라이언트 컴퓨터에 대한 정보로 정의합니다. NAP는 클라이언트 컴퓨터의 상태를 평가한 후 구성된 상태 정책에 요구되는 상태와 비교합니다.

상태 측정에 대한 예에는 다음이 포함될 수 있습니다.

* Windows 방화벽의 작동 상태 - 방화벽이 사용되도록 설정되어 있습니까, 아니면 그렇지 않습니까?
* 바이러스 백신 서명의 업데이트 상태 - 바이러스 백신 서명이 사용 가능한 가장 최근의 서명입니까?
* 보안 업데이트의 설치 상태 - 가장 최근의 보안 업데이트가 클라이언트에 설치되어 있습니까?

클라이언트 컴퓨터의 상태가 NAP 클라이언트 구성 요소에 의해 발행된 SoH(상태 설명) 목록에 캡슐화됩니다. NAP 클라이언트 컴퓨터는 클라이언트가 규격 클라이언트인지와 제한없는 네트워크 액세스 권한이 부여될 수 있는지를 평가하기 위해 SoH 목록을 NAP 서버 구성 요소로 보냅니다.

NAP를 사용하여 관리자는 상태 정책을 지속적으로 준수하도록 하고, 비규격 컴퓨터가 상태 정책을 준수하는 것으로 확인될 때까지 해당 컴퓨터의 액세스를 제한할 수 있습니다. NAP 용어적 개념에 따르면 컴퓨터가 조직의 정의된 상태 요구를 충족하는지 확인하는 것을 상태 정책 유효성 검사라고 합니다. NPS는 NAP에 대한 상태 정책 유효성 검사를 수행합니다.

### **NAP 관리 서버**

NAP 관리 서버 구성 요소는 클라이언트 측의 NAP 에이전트와 비슷한 처리 기능을 제공합니다. NPS를 통해 NAP 적용 서버로부터 SoH 목록을 받아서 각 SoH를 적절한 SHV에 배포합니다. 그런 다음, SHV로부터 SoH 응답 결과를 수집하여 NPS에 평가용으로 전송합니다.

### NPS(네트워크 정책 서버)

이전 버전의 Windows에서 NPS(네트워크 정책 서버)는 IAS(인터넷 인증 서비스)로 지칭되었습니다. 현재 NPS는 IPSec(인터넷 프로토콜 보안) 적용, 802.1X 적용, 라우팅 및 원격 액세스에 대한 VPN(가상 사설망) 적용, DHCP(Dynamic Host Configuration Protocol) 적용의 네 가지 NAP 적용 방법에 대해 NAP 정책 서버로 작동하는 기능을 비롯하여 여러 가지 기능을 제공합니다.

사용자가 NPS를 NAP 정책 서버로 구성하면 NPS는 네트워크에 연결하거나 네트워크에서 통신하려고 하는 NAP 가능 클라이언트 컴퓨터가 보낸 상태 설명 목록을 평가합니다. IT 관리자는 SHV(시스템 상태 검사기), SHV 템플릿 및 클라이언트 컴퓨터가 조직의 상태 요구에 맞게 구성을 업데이트할 수 있도록 하는 업데이트 관리 서버 그룹을 비롯한 NAP 정책을 NPS에 구성합니다.

NPS는 Microsoft에서 구현한 RADIUS(Remote Authentication Dial-In User Service) 서버 및 프록시이기도 합니다. RADIUS 서버로서 NPS는 802.1X 무선 및 인증 스위치, 원격 액세스 전화 접속 및 VPN(가상 사설망) 연결을 비롯한 다양한 유형의 네트워크 액세스에 대해 중앙 집중식 연결 인증, 권한 부여 및 회계 작업을 수행합니다. RADIUS 프록시로서 NPS는 다른 RADIUS[[1]](#footnote-2) 서버에 인증 및 계정 지정 메시지를 전달합니다.

### 예: NAP 적용 작동 방식

위에서 설명한 것처럼 NAP는 클라이언트 컴퓨터의 상태를 모니터링 및 평가하고, 클라이언트 컴퓨터가 비규격으로 간주될 경우 네트워크 액세스를 제한하여 상태 요구를 적용합니다. 클라이언트 및 서버 구성 요소는 비규격 클라이언트 컴퓨터가 제한없는 네트워크 액세스 권한을 얻을 수 있도록 해당 컴퓨터의 업데이트 관리를 지원합니다. NAP가 제대로 작동하려면 다음과 같은 몇 가지 핵심 프로세스가 필요합니다.

* 정책 유효성 검사
* NAP 적용 및 네트워크 제한
* 업데이트 관리
* 규정 준수를 위한 지속적인 모니터링

#### 정책 유효성 검사

NPS를 사용하여 관리자는 NAP가 클라이언트 컴퓨터 구성을 검색 및 적용하고 업데이트 상태를 관리할 수 있도록 하는 SHV를 사용하여 클라이언트 상태 정책을 만들 수 있습니다.

Windows 시스템 상태 에이전트 및 Windows 시스템 상태 검사기는 NAP 가능 컴퓨터에 다음 설정을 적용합니다. 클라이언트 컴퓨터는 다음과 같습니다.

* 방화벽 소프트웨어가 설치되고 사용 가능하게 설정되어 있습니다.
* 바이러스 백신 소프트웨어가 설치 및 실행되고 있습니다.
* 현재 바이러스 백신 업데이트가 설치되어 있습니다.
* 바이러스 백신 소프트웨어가 설치 및 실행되고 있습니다.
* 현재 바이러스 백신 업데이트가 설치되어 있습니다.
* Microsoft Update 서비스가 사용 가능하게 설정되어 있습니다.

또한 NAP 가능 클라이언트 컴퓨터가 Windows Update 에이전트를 실행하고 있으며 WSUS(Windows Server Update Service) 서버에 등록되어 있으면 NAP는 MSRC(Microsoft 보안 대응 센터)의 보안 심각도 등급과 일치하는 네 가지 값 중 하나를 기반으로 최신 소프트웨어 보안 업데이트가 설치되어 있는지 확인할 수 있습니다. 다음과 같은 네 가지 심각도 등급이 있습니다.

* 위험 - 사용자 작업 없이 인터넷 웜 프로그램을 작동시킬 수 있는 보안 취약 수준
* 중요 - 사용자 데이터의 기밀성, 무결성 또는 가용성, 처리 리소스의 무결성 또는 가용성을 침해할 수 있는 보안 취약 수준
* 보통 - 기본 구성, 감사 또는 침투 어려움과 같은 요인으로 인해 보안 침해 가능성이 상당 수준 완화
* 낮음 - 침투가 상당히 어렵거나 그 영향력이 최소인 보안 취약 수준

#### NAP 적용 및 네트워크 제한

비규격 클라이언트 컴퓨터의 네트워크에 액세스를 거부하거나 제한된 네트워크에 대한 액세스만 허용하도록 NAP를 구성할 수 있습니다. 제한된 네트워크에는 비규격 NAP 클라이언트가 상태 요구에 맞게 구성을 업데이트할 수 있도록 HRA(상태 등록 기관) 서버 및 업데이트 관리 서버와 같은 핵심 NAP 서비스가 포함되어야 합니다. NAP 적용 설정을 사용하여 IT 직원은 비규격 클라이언트의 네트워크 액세스를 제한하거나 NAP 가능 클라이언트 컴퓨터의 상태를 확인하고 로깅할 수 있습니다.

사용자는 다음 설정을 사용하여 액세스를 제한하거나, 액세스 제한을 지연시키거나, 액세스를 허용하도록 선택할 수 있습니다.

* 적용 안 함 - 기본 설정입니다. 정책 조건과 일치하는 클라이언트는 네트워크 상태 요구를 충족하는 것으로 간주되며 연결 요청이 인증되거나 허가될 경우 네트워크에 대해 제한없는 액세스 권한이 부여됩니다. NAP 가능 클라이언트 컴퓨터의 상태 준수 여부가 로깅됩니다.
* 적용 - 정책 조건과 일치하는 클라이언트는 네트워크 상태 요구를 충족하지 않는 것으로 간주되며 제한된 네트워크에 배치됩니다.
* 나중에 적용 - 정책 조건과 일치하는 클라이언트에 일시적으로 제한없는 액세스 권한이 부여됩니다. NAP 적용은 지정된 날짜 및 시간이 될 때까지 지연됩니다.

#### 업데이트 관리

제한된 네트워크에 있는 비규격 클라이언트 컴퓨터는 업데이트 관리가 필요할 수 있습니다. 업데이트 관리란 현재의 상태 요구를 만족하도록 클라이언트 컴퓨터를 업데이트하는 과정을 말합니다. 예를 들어 제한된 네트워크에 비규격 클라이언트 컴퓨터가 오래된 서명을 업데이트할 수 있도록 최신 바이러스 서명을 제공하는 FTP(File Transfer Protocol) 서버가 포함되어 있을 수 있습니다.

관리자는 NPS 상태 정책의 NAP 설정을 사용하여 자동 업데이트 관리를 구성할 수 있습니다. 그러면 NAP 클라이언트 구성 요소는 비규격 상태인 클라이언트 컴퓨터의 업데이트를 자동으로 시도합니다.

#### 규정 준수를 위한 지속적인 모니터링

NAP는 네트워크에 이미 연결되어 있는 규격 클라이언트 컴퓨터에 상태 규정을 적용할 수 있습니다. 이 기능은 상태 정책이 변경되고 클라이언트 컴퓨터의 상태가 변경될 때 네트워크가 보호되도록 해 줍니다. 예를 들어 상태 정책이 Windows 방화벽을 켤 것을 요구하지만 사용자가 실수로 끈 경우 NAP는 클라이언트 컴퓨터를 비규격 상태로 결정할 수 있습니다. 그러면 NAP는 Windows 방화벽이 다시 켜질 때까지 해당 클라이언트 컴퓨터를 제한된 네트워크에 둡니다. 자동 업데이트 관리가 사용되도록 설정하면 NAP 클라이언트 컴퓨터는 사용자 개입 없이 Windows 방화벽을 자동으로 설정할 수 있습니다.

### NAP 적용 방법

NAP는 다음 네트워크 기술에 대한 상태 정책을 적용합니다.

* IPSec(인터넷 프로토콜 보안)으로 보호되는 트래픽
* 802.1X 포트 기반 유선 및 무선 네트워크 액세스 프로토콜
* 라우팅 및 원격 액세스 기능이 설치된 VPN(가상 사설망)
* DHCP(Dynamic Host Configuration Protocol) IPv4 주소 임대 및 갱신

다음 섹션에서는 이러한 적용 방법에 대해 설명합니다.

#### IPSec 통신에 대한 NAP 적용

IPSec으로 보호된 트래픽에 대한 NAP 적용은 상태 인증서 서버, HRA(상태 등록 기관) 서버, NPS 서버 및 IPSec 적용 클라이언트와 함께 배포됩니다. NAP 클라이언트가 규격으로 확인되면 상태 인증서 서버는 X.509 인증서를 발급합니다. 인증된 클라이언트가 인트라넷에 있는 다른 NAP 클라이언트와 IPSec으로 보호되는 통신을 시작하면 이러한 인증서를 사용하여 NAP 클라이언트가 인증됩니다.

IPSec 적용은 네트워크의 통신을 규격 클라이언트로 한정하고 가장 강력한 형식의 NAP 적용을 제공합니다. 이 적용 방법은 IPSec을 사용하므로 관리자는 보호되는 통신에 대한 요구를 IP 주소 기준 또는 TCP/UDP 포트 번호 기준으로 정의할 수 있습니다.

#### 802.1X에 대한 NAP 적용

802.1X 포트 기반 네트워크 액세스 제어에 대한 NAP 적용은 NPS 서버 및 EAPHost(Extensible Authentication Protocol Host) 적용 클라이언트 구성 요소와 함께 배포됩니다. 802.1X 포트 기반 적용을 사용할 경우 NPS 서버는 802.1X 인증 스위치나 802.1X 규격 무선 액세스 지점이 비규격 802.1X 클라이언트를 제한된 네트워크에 배치하도록 합니다. NPS 서버는 액세스 지점이 연결에 IP 필터나 가상 LAN 식별자를 적용하도록 하여 클라이언트의 네트워크 액세스를 제한된 네트워크로 제한합니다. 802.1X 적용은 802.1X 가능 네트워크 액세스 장치를 통해 네트워크에 액세스하는 모든 컴퓨터에 강력한 네트워크 제한을 제공합니다.

#### VPN에 대한 NAP 적용

VPN에 대한 NAP 적용은 VPN 적용 서버 구성 요소와 VPN 적용 클라이언트 구성 요소와 함께 배포됩니다. VPN 서버는 VPN에 대한 NAP 적용을 사용하여, 클라이언트 컴퓨터가 원격 액세스 VPN 연결을 사용하여 네트워크에 연결하려고 할 때 상태 정책을 적용할 수 있습니다. VPN 적용은 클라이언트 상태 요구를 충족하지 않는 원격 액세스 VPN 연결을 통해 네트워크 액세스하는 모든 컴퓨터의 네트워크 액세스를 제한하는 강력한 기능을 제공합니다. VPN 적용은 Windows Server 2003 및 ISA(Internet Security and Acceleration) Server 2004에 제공되는 네트워크 액세스 격리 제어와는 다릅니다.

#### DHCP에 대한 NAP 적용

DHCP 적용은 DHCP NAP 적용 서버 구성 요소, DHCP 적용 클라이언트 구성 요소 및 NPS와 함께 배포됩니다. DHCP 서버 및 NPS는 DHCP 적용을 사용하여, 컴퓨터가 IPv4(IP 버전 4) 주소를 임대하거나 갱신하려고 할 때 상태 정책을 적용할 수 있습니다. NPS 서버는 DHCP 서버가 제한된 IP 주소 구성을 지정하도록 하여 클라이언트 네트워크 액세스를 제한된 네트워크로 제한합니다. 그러나 클라이언트 컴퓨터가 정적 IP 주소로 구성되었거나 제한된 IP 주소 구성을 회피하도록 구성된 경우 DHCP 적용은 효과가 없습니다. DHCP 메시지에 저장되어 있는 상태 유효성 검사 데이터는 다른 컴퓨터에서 볼 수 있습니다. DHCP 적용 클라이언트는 DHCP 서버가 요청할 때만 SoH 목록을 보냅니다.

#### 여러 방식 조합

이러한 각 NAP 적용 방법은 각기 다른 이점을 갖습니다. 관리자들은 적용 방법을 조합하여 이러한 다양한 방법의 이점을 적절히 얻을 수 있습니다. 그러나 여러 가지 NAP 적용 방법을 배포하면 NAP 구현을 관리하는 것이 더 복잡해질 수 있습니다.

또한 NAP 프레임워크는 Microsoft가 아닌 타 회사에서 해당 소프트웨어를 NAP 플랫폼에 통합할 수 있도록 하는 API 제품군을 제공합니다. 소프트웨어 개발자와 공급업체는 NAP API를 사용하여 상태의 유효성을 검사하고 비규격 클라이언트의 업데이트 관리를 수행하는 종단 간 솔루션을 제공할 수 있습니다.

## 요약

조직에서는 Windows Server 2008을 사용하여 네트워크 액세스 보호와 같은 정책 기반 보안 기능을 통해 향상된 보안 이점을 얻을 수 있습니다. RODC와 같은 Active Directory의 보안 관련 기능 향상과 새로운 감사 옵션은 엔터프라이즈 PKI 기능 향상과 조합되어 관리자들이 원격 위치에서도 보다 쉽게 조직의 보안을 유지하고 보안 이벤트를 감사할 수 있도록 합니다. Windows BitLocker 드라이브 암호화와 같은 운영 체제의 다른 기능과 새로운 Windows 방화벽 기능은 시스템을 보다 안전하게 만들어 줍니다. Windows Server 2008은 보다 안전한 서버 플랫폼 및 네트워크 환경을 원하는 조직에 적합합니다. Windows Server 2008의 ID 및 액세스 기능은 향상된 통합 권한 관리 기능과 결합되어 사용자 ID와 액세스 권한을 관리하고 민감한 콘텐츠를 외부 사용자와 공유하는 작업을 간소화합니다.

# 6장: 웹 및 응용 프로그램

## 소개

Microsoft Windows Server 2008은 서버 또는 웹에서 응용 프로그램 및 서비스를 개발하고 안전하게 호스팅하기 위한 안전하면서 관리가 용이한 플랫폼을 제공합니다. 새로운 기능에는 간소화된 응용 프로그램 및 서비스 관리, 보다 빠른 배포, 향상된 보안, 성능 및 확장성 향상 등이 포함됩니다. Windows Server 2008은 이러한 향상된 기능을 제공하면서, 관리자가 응용 프로그램 및 서비스에서 핵심 운영 체제 리소스가 어떻게 활용되고 있는지를 보다 잘 제어하고 확인할 수 있도록 합니다. 주요 이점은 다음과 같습니다.

* 풍부한 웹 기반 환경을 효율적이고 효과적으로 제공
* 모듈 방식 아키텍처 및 완전한 사용자 지정형 설치를 통해 웹 서버 공격 지점, 서버 규격 및 패치 감소
* 새 웹 사이트의 자동 샌드박싱(sandboxing)을 통해 웹 사이트 및 응용 프로그램의 안정성 및 보안 향상
* 새로 배포된 구성 시스템을 활용하여 *코*드 및 콘텐츠와 함께 XCopy 배포
* 강력한 새 관리 도구를 사용한 보다 쉬운 관리
* 작동 중단을 최소화하고 오류 복구를 가속화하는 진단 및 문제 해결 도구 개선
* 다음을 지원하는 통합된 .NET Framework 3.0
  + WCF(Windows Communication Foundation)
  + WPF(Windows Presentation Foundation)
  + Windows WF(Workflow Foundation)
  + WCS(Windows CardSpace)
* 일반적인 타사 웹 응용 프로그램을 실행하기 위한 통합 PHP 지원
* 인터넷이나 인트라넷을 통해 라이브 또는 주문형 오디오 및 비디오 콘텐츠를 스트리밍할 수 있는 강력한 플랫폼
* 비즈니스 프로세스를 향상시키고 팀 생산성을 향상시키도록 디자인된 공동 작업 기술 및 웹 기반 응용 프로그램 플랫폼

## IIS(인터넷 정보 서비스) 7.0

Windows Server 2008은 IIS(인터넷 정보 서비스) 7.0, ASP.NET, Windows Communication Foundation 및 Windows SharePoint Services를 통합하는 웹 게시용 통합 플랫폼을 제공합니다. IIS 7.0은 기존 IIS 웹 서버에서 가장 획기적으로 향상된 제품으로, 웹 플랫폼 기술 통합에서 핵심적인 역할을 담당할 것입니다. IIS 7.0의 주요 이점으로는 보다 효율적인 운영과 관리 기능, 향상된 보안 및 지원 비용 절감 등이 있습니다. 이러한 기능은 웹 솔루션을 위한 일관된 단일 개발 및 관리 모델을 제공하는 통합 플랫폼을 만들도록 도와 줍니다.

### 모듈 방식의 디자인

IIS 7.0 코어 웹 서버에서는 몇 가지 기본 기능이 IIS 6.0과 다르게 변경되었습니다. 이전 버전의 IIS에서는 모든 기능이 기본으로 제공되었습니다. IIS 7.0은 40개가 넘는 개별 기능 모듈로 구성되어 있습니다. 모듈의 절반만 기본적으로 설치되며 관리자는 선택한 기능 모듈을 선택적으로 설치하거나 제거할 수 있습니다. 이러한 모듈 방식을 통해 관리자는 필요한 옵션만 설치할 수 있으며 관리 및 업데이트가 필요한 기능 수를 제한하여 시간을 절감할 수 있습니다.

처리 방식도 일부 변경되었습니다. 네이티브 코드와 관리되는 코드는 단일 요청 파이프라인을 통해 처리됩니다. 또한 새로운 작업자 프로세스 웹 코어는 요청 파이프라인의 모든 알림 이벤트에 액세스할 수 있도록 합니다. 높은 통합 수준 때문에 모든 유형의 웹 콘텐츠에 기존 ASP.NET 기능(예: 폼 기반 인증 또는 URL 권한 부여)을 사용할 수 있습니다.

그 결과 불필요한 소프트웨어가 실행되지 않으므로 공격 가능 범위가 크게 줄어들며, 관리되는 코드 모듈을 만들어 IIS 7.0 코어 기능을 쉽게 확장할 수 있습니다.

### 확장성 증가

이전 버전에서는 코어 웹 서버의 기본 제공 기능을 확장하거나 교체할 경우 문제가 있었습니다. IIS 7.0을 사용하여 개발자는 .Net에서 만든 사용자 지정 인증 모음과 같이 기능을 확장하는 관리되는 코드 모듈을 만들 수 있습니다. IIS 7.0은 코어 서버 모듈 작성에 새로운 Win32® API를 사용합니다. ISAPI 필터 및 확장이 IIS 7.0에서도 계속 지원되지만, 코어 서버 모듈은 ISAPI(Internet Server Application Programming Interface) 필터 및 확장을 대신할 수 있는 강력하고 유용한 기능입니다. 모든 IIS 코어 서버 기능은 새로운 IIS 7.0 Win32 모듈 API를 사용하여 별도의 기능 모듈로 개발되었기 때문에 관리자와 개발자는 원할 경우 IIS 기능 모듈을 추가하거나 제거하거나 바꿀 수도 있습니다.

모듈은 네이티브 코드(C/C++) 및 관리되는 코드(예: .NET Framework를 사용하는 C# 및 Visual Basic® 2005와 같은 언어) 둘 다로 개발할 수 있습니다. IIS 7.0의 통합 요청 처리 파이프라인은 관리되는 코드 모듈(IHttpModule) 및 처리기(IHttpHandler)에 대한 알림을 제공할 수 있으며, 관리되는 코드 모듈에서 파이프라인의 모든 요청에 대해 요청 파이프라인의 모든 이벤트에 액세스할 수 있도록 합니다. 결과적으로 IHttpModule 인터페이스나 IHttpHandler 인터페이스를 구현하여 클라이언트 요청을 필터링하고 URL을 조작하는 관리되는 코드 모듈 및 처리기를 통해 파이프라인의 이벤트를 보다 강력하게 제어할 수 있습니다. 또한 IIS 7.0에서는 구성, 스크립팅, 이벤트 로깅 및 관리 도구 기능 모음을 확장할 수 있으므로 소프트웨어 개발자는 웹 서버 확장을 구축할 수 있는 완전한 서버 플랫폼을 사용할 수 있게 됩니다.

### 분산 구성

IIS 7.0에서는 IIS 설정의 분산 구성을 통해 구성 데이터를 저장하고 액세스하는 방식이 크게 향상되었습니다. 이를 통해 관리자는 코드 및 콘텐츠와 함께 저장되는 파일에 IIS 구성 설정을 지정할 수 있습니다. 이제 구성 설정을 단일 파일에 지정하여 선택한 웹 사이트 기능이나 웹 응용 프로그램의 관리 책임을 다른 사람에게 위임하고 간단한 XCopy 배포를 사용할 수 있습니다.

#### 분산 구성을 허용하는 변경

메타베이스라고 하는 IIS 6.x의 중앙 관리형 구성 저장소는 더 이상 없습니다. IIS 7.0에서는 분산 XML 구성 파일 계층을 기반으로 하는 새로운 위임형 구성 시스템을 제공합니다. 이 계층은 서버 수준의 구성 기본값이 포함된 전역 applicationHost.config 파일과 응용 프로그램의 디렉터리 구조 내의 분산 Web.config 파일로 구성됩니다. 이러한 파일은 ASP.NET 응용 프로그램 프레임워크에서 이동 가능한 방식으로 응용 프로그램 설정을 저장하는 데 사용하는 것과 동일한 Web.config 파일입니다. 따라서 강력하게 구성된 명확한 XML 지시문을 사용하여 IIS 및 ASP.NET 구성을 나란히 저장할 수 있습니다. 이를 통해 일반 API 모음을 사용하여 액세스할 수 있고 일관된 형식으로 저장되는 모든 웹 플랫폼 구성 설정에 대한 단일 구성 저장소가 가능해 집니다. IIS 7.0 구성 시스템은 완전하게 확장 가능하므로 개발자는 IIS 구성과 동일한 수준 및 우선 순위를 갖는 사용자 지정 구성을 포함하도록 구성 저장소를 확장할 수 있습니다.

이전에는 응용 프로그램이 올바르게 작동하려면 먼저 IIS 응용 프로그램 설정을 컴퓨터 수준의 메타베이스 리포지토리에서 명시적으로 구성해야 했습니다. 응용 프로그램은 분산 Web.config 파일을 사용하여 디렉터리 구조 내에 필요한 서버 구성을 캡슐화합니다. 이를 통해 배포가 크게 간소화되었으며, 독립형 응용 프로그램을 대상 서버의 응용 프로그램 디렉터리에 간단히 복사하고 원하는 설정으로 즉시 실행할 수 있습니다.

IIS 7.0은 %windir%\system32\inetsrv 디렉터리에 ApplicationHost.config를 저장합니다. 이 파일에는 다음과 같은 두 가지 주요 구성 섹션 그룹이 있습니다.

* system.applicationHost
* system.WebServer

system.applicationHost 섹션 그룹에는 사이트, 응용 프로그램, 가상 디렉터리 및 응용 프로그램 풀에 대한 구성이 포함되어 있습니다. system.WebServer 섹션 그룹에는 전역 웹 기본값을 비롯한 기타 모든 설정에 대한 구성이 포함되어 있습니다.

#### XCopy 배포

분산 구성에서는 IIS 구성 설정을 Web.config 파일에 저장할 수 있으므로, XCopy를 사용하여 여러 웹 서버에서 응용 프로그램을 보다 쉽게 복사할 수 있으며 비용이 많이 들고 오류가 발생하기 쉬운 복제, 수동 동기화 및 추가 구성 작업을 수행하지 않아도 됩니다. 따라서 응용 프로그램을 개발 시스템에서 테스트 시스템으로, 다시 프로덕션 시스템으로 이동할 때 특정 사이트나 응용 프로그램에 대한 구성 설정을 시스템 간에 보다 쉽게 복사할 수 있습니다. XCopy 배포 기능을 사용할 경우 응용 프로그램 개발자는 시스템 관리자를 따로 두지 않고도 응용 프로그램의 구성을 변경할 수 있으므로 전반적으로 TCO 절감 효과가 있습니다. 또한 XCopy 배포가 간편하므로 시스템 관리자가 시스템 간에 사이트를 쉽게 이동할 수 있습니다.

### 관리 도구

IIS 7.0에는 업데이트되고 개정된 다음과 같은 IIS 관리용 도구가 포함되어 있습니다.

* + 새로운 그래픽 관리 인터페이스를 포함하는 IIS 관리자
  + 강력한 새 명령줄 도구인 appcmd.exe로 바뀐 명령줄 스크립트
  + 설정을 직접 편집할 수 있는 .NET Framework 2.0 구성 저장소 기반의 구성 저장소
  + CIM 개체 관리자와 관리되는 개체 간의 중개자로 작동하는 소프트웨어 구성 요소인 WMI 공급자. 이 구성 요소를 통해 VBScript(Visual Basic Scripting Edition) 및 JScript 기록기에 대한 구성 및 서버 상태 정보에 액세스할 수 있습니다.
  + WMI 공급자가 노출하는 것과 동일한 정보를 보다 간단한 API(응용 프로그래밍 인터페이스)로 노출하는 관리되는 인터페이스인 Microsoft.Web.Administration. 개발자는 Microsoft.Web.Administration을 사용하여 IIS 7.0의 모든 기능을 제어하고 읽을 수 있습니다.

또한 Windows Server 2008에는 IIS 6.0을 원격으로 관리하도록 지원하고 FTP 사이트를 관리하기 위한 IIS 6.0 MMC 스냅인이 제공됩니다. IIS 6.0 관리 도구 및 웹 서버 구성 요소는 별도로 설치할 수 있습니다.

Windows Server 2008의 새로운 관리 도구는 새로운 IIS 7.0 분산 구성을 완전히 지원하며 관리자 이외의 사용자에게 사이트 및 응용 프로그램 구성에 액세스하는 권한을 위임할 수 있도록 합니다(아래의 위임 관리 섹션 참조).

### 새 IIS 관리자

IIS 7.0의 새 관리 유틸리티인 IIS 관리자는 웹 서버 관리를 위한 보다 효율적인 도구입니다. 이 유틸리티는 IIS 및 ASP.NET 구성 설정, 사용자 데이터 및 런타임 진단 정보를 지원합니다. 새로운 IIS 관리자 인터페이스는 HTTP를 통한 원격 관리를 지원하므로, 방화벽에서 DCOM 또는 기타 관리 포트를 열어 두지 않고도 통합된 로컬 및 원격 관리가 가능합니다.

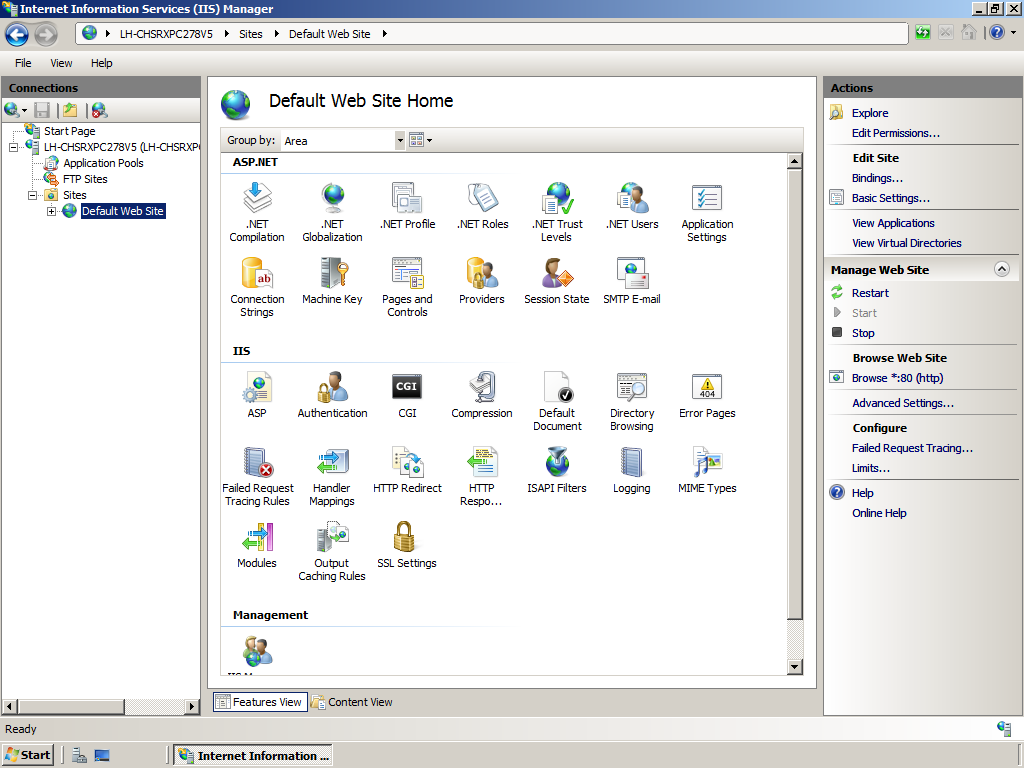


그림 5: 새 IIS 관리 화면

또한 IIS 관리자에서 관리자들은 관리 제어 권한을 개발자나 콘텐츠 소유자에게 위임할 수 있습니다. IIS 관리자에는 그 밖에 다음과 같은 주요 기능이 있습니다.

* + .NET Framework를 사용하여 새 UI 기능을 플러그 인하기 위한 풍부한 확장 가능 프레임워크
  + 위임 관리를 위한 Windows 및 비 Windows 자격 증명 지원
  + 새 UI 모듈을 클라이언트에 자동으로 다운로드하여 설치
  + HTTP/SSL을 통한 원격 관리

웹 서버, 웹 사이트 및 웹 응용 프로그램을 관리 및 운영할 수 있는 새로운 명령줄 도구 appcmd.exe도 포함되어 있습니다. 이 명령줄 인터페이스는 관리자의 일반적인 관리 웹 서버 작업을 간소화합니다. 예를 들어 500밀리초 이상 대기해야 하는 웹 서버 요청을 나열하기 위해 appcmd.exe를 사용할 수 있습니다. 이 정보는 성능이 나쁜 응용 프로그램 문제를 해결하는 데 사용될 수 있습니다. appcmd.exe의 출력은 추가 처리를 위해 다른 명령에 파이핑될 수 있습니다.

#### 위임 관리

IIS 7.0의 분산 구성은 웹 사이트를 호스팅하거나 관리하는 사용자가 개발자나 콘텐츠 소유자에게 다양한 수준의 관리 제어 권한을 위임하여 소유 비용 및 관리자 작업 부하를 줄일 수 있도록 합니다. 예를 들어 응용 프로그램 개발자가 웹 사이트에 사용되는 기본 문서나 기타 속성을 구성 및 유지 관리할 수 있도록 해당 웹 사이트에 대한 관리 제어 권한을 위임할 수 있습니다. 관리자는 다른 사람이 변경할 수 없도록 특정 구성 설정을 잠글 수도 있습니다. 이 기능을 통해 웹 사이트에 대한 관리 액세스 권한을 위임 받은 콘텐츠 개발자가 스크립트 실행을 방지하는 보안 정책을 무시하지 않도록 할 수 있습니다. 위임은 매우 구체적으로 수행될 수 있습니다. 즉, 관리자는 사례별로 위임할 기능을 정확히 결정할 수 있습니다.

#### Microsoft.Web.Administration

IIS 7.0에는 새로운 웹 서버용 관리 API인 Microsoft.Web.Administration도 제공됩니다. 이 기능을 사용하면 XML 구성 파일을 조작하여 구성 설정을 편집할 수 있습니다. 아울러 서버, 서버 속성 및 서버 상태를 관리할 수 있는 개체도 제공됩니다. 이 API는 IIS 구성 파일 계층의 구성 속성을 프로그래밍 방식으로 읽고 쓰며, 이전 버전의 IIS의 WMI 스크립트에서 액세스할 수 있던 것과 동일한 데이터를 프로그래밍 방식으로 사용할 수 있도록 합니다.

### 진단 및 문제 해결

IIS 7.0은 기본 제공된 진단 및 추적 지원보다 더 쉽게 웹 서버의 문제를 해결할 수 있도록 하며, 관리자가 웹 서버에 대한 자세한 실시간 진단 정보를 볼 수 있도록 합니다. 진단 및 문제 해결 기능은 개발자나 관리자가 서버에서 실행 중인 요청을 확인할 수 있도록 하며, 자세한 추적 로그를 통해 재현하기 어려운 오류 조건을 필터링하고 오류를 자동으로 추적할 수 있도록 합니다.

#### 자세한 오류 메시지

IIS 7.0은 좀 더 자세하고 실용적인 오류 메시지를 제공하여 문제 해결을 간소화합니다. IIS 7.0의 새로운 사용자 지정 오류 모듈을 사용하여 자세한 오류 정보를 브라우저로 다시 보낼 수 있습니다. 기본 위치는 로컬 호스트이지만 다른 원격 클라이언트로 오류 정보를 보내도록 구성할 수도 있습니다. 관리자는 이제 간단한 오류 코드 대신, 요청에 대한 자세한 정보, 오류를 유발했을 수 있는 잠재적인 문제점 및 제안되는 오류 수정 방법을 확인할 수 있습니다.

#### RSCA(Runtime Status and Control API)

IIS 7.0의 문제 해결 지원을 향상시키는 가장 중요한 기능 중 하나는 IIS 7.0에서 서버에 대한 자세한 런타임 정보를 제공하도록 디자인된 RSCA(Runtime Status and Control API)입니다. RSCA를 사용하면 사이트, 응용 프로그램 풀, .NET Framework 응용 프로그램 도메인 및 실행 중인 요청을 비롯한 다양한 엔터티를 검사하고 관리할 수 있습니다. 이 정보를 사용하여 관리자나 개발자는 서버 리소스 사용량을 분석하고 웹 응용 프로그램 문제를 해결할 수 있습니다.

예를 들어 RSCA 및 IIS 7.0 관리 도구를 사용하여 관리자는 100%의 CPU를 소비하는 작업자 프로세스에서 실행되고 있는 요청이나 특정 사이트에 대해 로드된 응용 프로그램 도메인을 알 수 있습니다. 또한 RSCA는 서버에서 현재 실행되고 있는 요청을 실시간으로 공개합니다. RSCA 데이터는 WMI 공급자 및 관리되는 API(Microsoft.Web.Administration)에서 사용할 수 있습니다. IIS 관리자 명령줄 도구(appcmd.exe)를 통해서도 이러한 데이터를 표시할 수 있습니다.

#### 실패한 요청 추적

IIS 7.0에는 요청 및 응답 경로를 아우르는 자세한 추적 이벤트가 포함되어 있으므로 개발자 및 관리자는 기존 페이지 수준 코드로, 다시 응답에 이르기까지 IIS 요청 처리 파이프라인을 따라 이동하면서 요청을 추적할 수 있습니다. 이러한 자세한 추적 이벤트를 통해 개발자는 요청 경로와 요청의 결과로 발생한 오류 정보뿐만 아니라 경과 시간, 모든 유형의 오류를 해결하는 데 도움이 될 수 있는 기타 디버깅 정보를 이해할 수 있습니다.

서버에 대한 요청이 실패하거나 요청 처리가 너무 오래 걸리면 관리자는 해당 요청에 대한 추적 이벤트를 캡처하고 발생 시 추적 이벤트를 로깅하는 실패한 요청 추적 규칙을 정의할 수 있습니다. 요청에 대해 할당된 시간 간격이 초과될 때까지 요청이 처리되지 않았거나 응답에 대해 지정된 HTTP 상태 및 하위 상태 코드 조합이 생성된 경우, 추적 로그에 이벤트가 기록됩니다. 이벤트 세부 수준에 따라 추적 로그의 기록 여부가 결정될 수도 있습니다. 추적 로그에는 실패한 요청에 해당하는 정보만 포함되어 있습니다. 관리자는 더 이상 실패한 특정 요청에 대해 필요한 정보를 찾기 위해 모든 요청이 들어 있는 대규모 로그 파일을 검색하지 않아도 됩니다. 새로운 XSL 시트는 웹 응용 프로그램에서 발생할 수 있는 다양한 문제점의 진단을 돕기 위해 여러 횡단면으로 데이터를 표시하도록 디자인되었습니다.

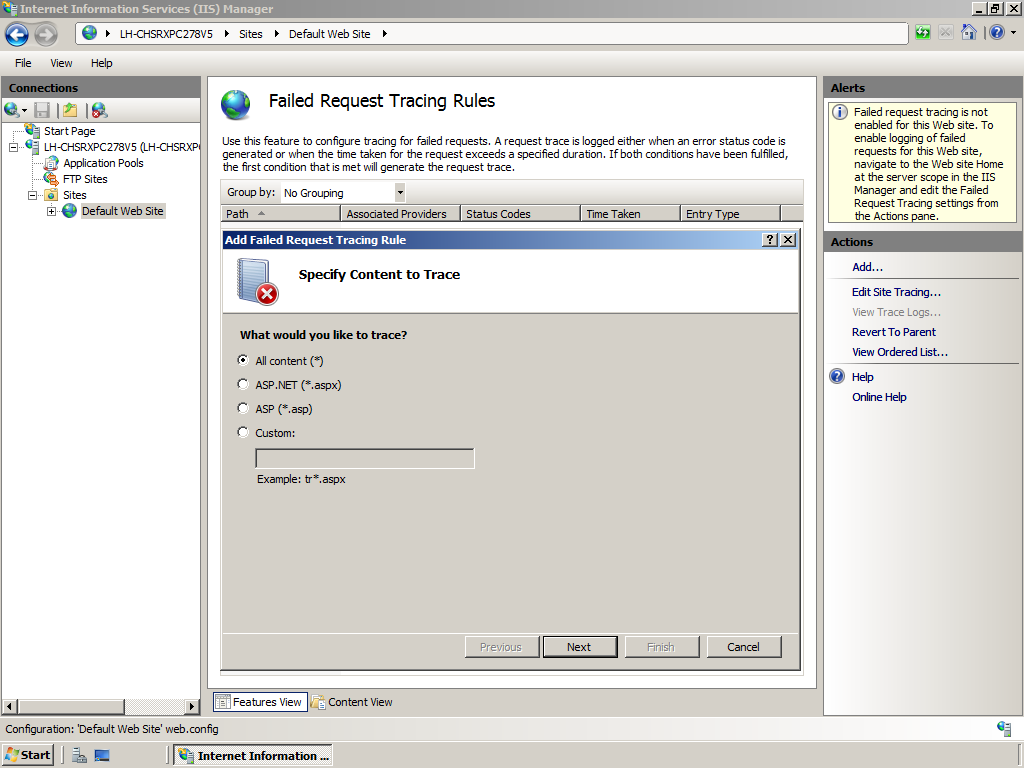


그림 6: 실패한 요청 추적 규칙 화면

## WAS(Windows Process Activation Service)

여러 프로토콜을 통한 WCF(Windows Communication Foundation) 서비스의 개발 및 호스팅을 향상시키기 위해(아래의 “WCF(Windows Communication Foundation)” 참조), Windows Server 2008에는 임의 프로토콜 수신기의 플러그형 활성화를 지원하는 WAS(Windows Process Activation Service)가 포함되어 있습니다. WAS는 모든 유형의 메시지 활성화 응용 프로그램에 지능형 리소스 관리, 요청 시 프로세스 활성화, 상태 모니터링, 자동 실패 검색 및 재생 기능을 제공합니다. WAS는 IIS 6.0 요청 처리 모델을 기반으로 합니다.

WAS는 WWW 서비스 대신 응용 프로그램 풀 구성 및 작업자 프로세스를 사용하므로, 응용 프로그램은 HTTP 및 비 HTTP 사이트 둘 다에 대해 동일한 구성과 프로세스 모델을 사용할 수 있습니다. WAS는 WWW 서비스와는 별도로 실행되어, NET.TCP와 같은 수신기를 통해 웹 서비스를 관리할 수 있습니다. 이 기능은 HTTP.sys에서 HTTP 요청을 수신 대기할 필요가 없는 응용 프로그램에 유용합니다.

## WSRM(Windows 시스템 리소스 관리자)

관리자는 Windows 시스템 리소스 관리자를 사용하여 CPU 및 메모리 리소스가 응용 프로그램, 서비스 및 프로세스에 할당되는 방식을 제어할 수 있습니다. 이러한 방식으로 리소스를 관리하면 시스템 성능이 향상되고 응용 프로그램, 서비스 또는 프로세스가 나머지 시스템과 충돌할 가능성도 줄어듭니다. 또한 컴퓨터에서 실행되는 응용 프로그램 및 서비스 사용자에게 보다 일관되고 예측 가능한 환경이 제공됩니다.

WSRM은 Equal\_Per\_IISAppPool 및 Equal\_Per\_Session.Conditional을 비롯한 기본 제공 정책을 통해 리소스 관리를 웹 풀 및 세션과 통합합니다. WSRM의 정책은 클러스터 구성에서 실행될 경우 응답 하드웨어 Hot-add 변경 또는 클러스터 변경의 다른 리소스 할당으로 자동 전환됩니다.

또한 WSRM은 회계와 관련된 많은 기능을 추가로 제공합니다. SQL Server 2005를 사용할 경우 관리자는 SQL 기반 계정 엔진을 사용하여 비용 부과 및 기타 비용 기반 모델에 전달될 수 있는 표준 형식의 리소스 사용량 통계를 캡처할 수 있습니다(x86 기반 및 x64 기반 서버만 해당). 뿐만 아니라 WSRM을 사용하면 여러 WSRM 관리 시스템의 회계 데이터를 통합된 단일 데이터베이스에 저장할 수 있으므로 비용 부과 및 회계를 위해 여러 서버에서 데이터를 수집하기 위한 프런트 엔드 웹 기반 도구를 작성할 필요가 없습니다. WSRM은 또한 회계 데이터를 SQL Server 2005 데이터베이스에 직접 저장할 수 있도록 지원합니다.

이전 버전의 WSRM은 별도의 WSRM CD로 배포되었으며 별도의 설치 과정을 통해 설치해야 했습니다. Windows Server 2008에서는 WSRM이 설치 미디어에 포함되어 있으며, 다른 기본 제공 선택적 구성 요소와 마찬가지로 선택적 구성 요소 대화 상자를 통해 설치하거나 제거할 수 있습니다. WSRM은 모든 버전의 Windows Server 2008에서 사용할 수 있으며 Windows Server 2008을 지원하는 모든 컴퓨터에서 실행됩니다.

## 이벤트 인프라

### **Windows Server 2008 및 Windows Vista의 이벤트**

Windows Server 2008에는 이전 버전의 이벤트 및 추적 문제를 극복한 새로운 이벤트 처리 아키텍처를 제공합니다. 여기서는 이벤트 로그의 제한된 확장성(모든 로그의 총 크기를 사용 가능한 메모리 양으로 제한), 이벤트 게시 성능(활성 도메인 컨트롤러에 게시할 수 있는 이벤트 수 제한) 및 추적 이벤트의 제한된 보안 등의 문제가 해결되었습니다.

이벤트 6.0은 이벤트 로그 서비스 및 이벤트 뷰어를 대신합니다. Windows 이벤트는 추가 검토를 위해 로그 파일에 보관되는 이벤트를 특수하게 처리하도록 디자인되었으며 IPC 및 알림 메커니즘과 같은 임시 이벤트에는 적합하지 않습니다.

### **이벤트를 보는 새로운 방법**

새 이벤트 뷰어는 완전히 다시 작성되었으며 MMC(Microsoft Management Console) 3.0 내에서 작동하므로 모양도 달라졌습니다. 이전 버전과 마찬가지로 트리 창과 이벤트 목록이 제공됩니다. Windows 로그 노드 아래에 제공되는 친숙한 응용 프로그램, 시스템 및 보안 로그에도 여전히 액세스할 수 있습니다. 새 노드도 일부 추가되었습니다. 이벤트 목록 아래에는 미리 보기 창이 있습니다. 여기에는 포커스가 있는 이벤트의 속성이 표시됩니다. 하나 이상의 로그 파일에 대해 이벤트를 수집할 수 있으며 이벤트는 특정 ID, 심각도 수준 또는 시간 프레임에 초점을 둘 수 있습니다. 관리자는 새로운 인터페이스를 사용하여 이벤트 속성을 보기 위해 이벤트를 두 번 클릭할 필요가 없으며 목록과 이벤트 속성 대화 상자를 모두 보기 위해 여러 창에서 작업할 필요가 없습니다.

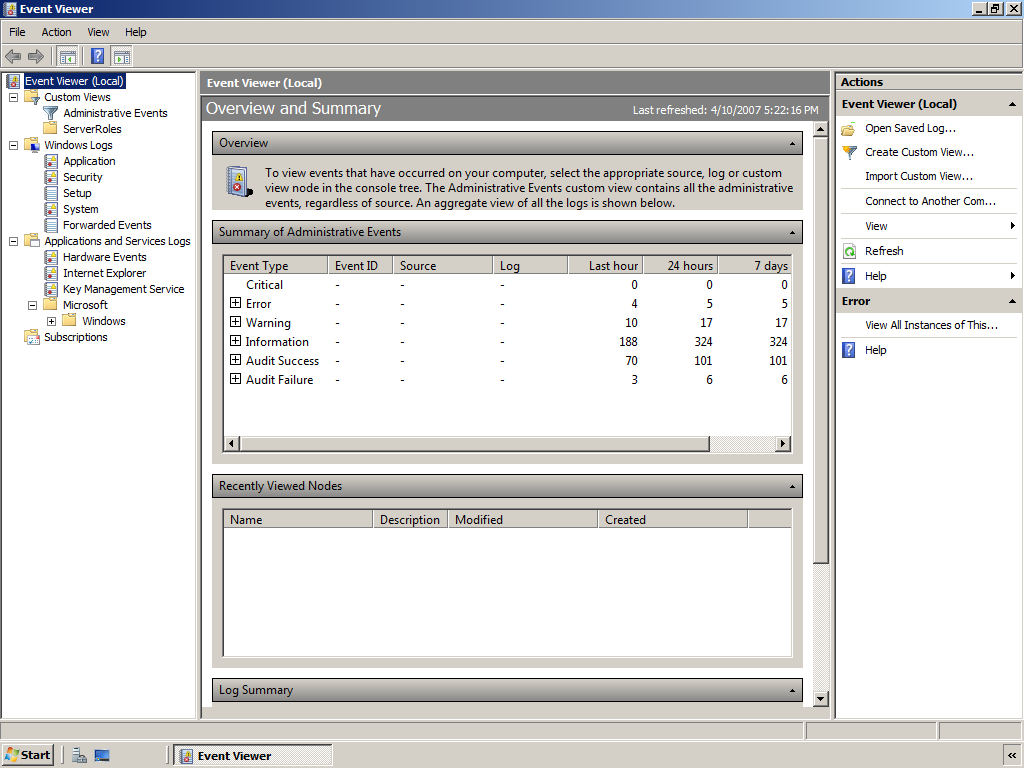


그림 7: 새 이벤트 뷰어 화면

### **XML 구조**

새 이벤트 로그는 잘 정의된 구조로 이루어져 있습니다. 이벤트는 게시된 스키마가 있는 XML을 사용하여 외부적으로 표시됩니다. 따라서 오류가 있는 이벤트를 걸러 내고 관심 있는 이벤트를 수집하는 쿼리를 만들 수 있습니다. 내부적으로 이벤트는 이진 형식으로 저장되므로 압축성, 안정성 및 검색 성능을 적절히 균형 있게 제공합니다.

XML이 사용되므로 XPath가 이벤트 쿼리 언어의 기반이 됩니다. 새 작업 스케줄러 통합 기능에서 확인할 수 있는 것처럼 구조화된 이벤트를 사용하면 자동화가 가능해 집니다. 이벤트 로그 명령줄 유틸리티에 제공되는 간단한 XPath 식을 통해 단일 로그에서 이벤트를 선택할 수 있으며, 간단하지만 강력한 XML 기반 쿼리 언어를 사용하여 로그 또는 외부 이벤트 아카이브에서 이벤트를 선택하고 표시되지 않도록 할 수 있습니다.

### **이벤트 구독**

관리자는 이벤트 뷰어를 사용하여 하나의 로컬 또는 원격 컴퓨터의 이벤트를 볼 수 있지만 문제를 해결하기 위해서는 여러 컴퓨터에 있는 여러 로그에 저장되어 있는 이벤트 모음을 검토해야 할 수 있습니다. Windows Server 2008 및 Windows Vista에는 여러 원격 컴퓨터의 이벤트 복사본을 수집한 후 로컬로 저장하는 기능이 있습니다. 수집할 이벤트를 지정하기 위해 관리자는 이벤트 구독을 만듭니다. 구독은 수집할 이벤트와 로컬로 저장할 로그를 정확히 지정합니다. 구독이 활성화되고 이벤트가 수집되면 전달된 이벤트를 로컬로 저장된 이벤트처럼 조작할 수 있습니다.

Windows Server 2008의 새 이벤트 기능을 사용하여 서버 및 응용 프로그램 관리자는 응용 프로그램을 보다 쉽게 모니터링하고, 분석을 위해 로깅된 데이터를 수집하고, 발생한 문제를 해결할 수 있습니다.

## 다시 시작 관리자

Windows Server 2008의 다시 시작 관리자 API는 설치나 업데이트를 완료하는 데 필요한 시스템 다시 시작 횟수를 없애거나 줄일 수 있습니다. 다시 시작 관리자는 중요한 시스템 서비스만 종료한 후 다시 시작하고 차단 DLL 및 리소스를 언로드합니다. 이를 통해 사용 중인 파일이 사용 가능하게 해제되며 설치 작업을 완료할 수 있습니다.

중요한 시스템 서비스, Windows Installer, Window Update 에이전트 또는 WMI(Windows Management Instrumentation)에서 소유하는 파일이나 리소스의 업데이트를 수행하려면 시스템을 다시 시작해야 합니다. 중요한 시스템 서비스에는 smss.exe, csrss.exe, winit.exe, logonui.exe, lsass.exe, services.exe, winlogon.exe, csrss.exe, RPCSS가 있는 svchost.exe 및 Dcom/PnP가 있는 svchost.exe가 포함됩니다.

다시 시작 관리자는 다음 순서로 응용 프로그램을 중지합니다.

1. GUI 응용 프로그램
2. 콘솔 응용 프로그램
3. Windows 서비스
4. Windows 탐색기

다시 시작 관리자는 다시 시작되도록 등록된 응용 프로그램을 중지 순서와는 반대로 다시 시작합니다.

다시 시작 관리자 DLL은 표준 또는 사용자 지정 설치 관리자에 의해 로드될 수 있는 공용 C 인터페이스를 내보냅니다. 응용 프로그램의 설치 또는 업데이트 중에, 설치 관리자는 다시 시작 관리자를 사용하여 현재 사용 중이기 때문에 업데이트할 수 없는 파일을 확인할 수 있습니다. 다시 시작 관리자는 현재 해당 파일을 사용 중인 중요하지 않은 서비스나 응용 프로그램을 종료한 후 다시 시작할 수 있습니다.

개발자는 다시 시작 관리자가 다음을 기반으로 하는 응용 프로그램이나 서비스를 종료한 후 다시 시작하도록 하는 설치 관리자를 작성할 수 있습니다.

* + 사용 중인 파일
  + 프로세스 ID(PID)
  + Windows 서비스의 약식 이름

사용 중인 것으로 확인되어 업데이트에 의해 간단히 삭제 및 대체될 수 없으며 다시 시작 관리자에 등록될 수 있는 파일. 그런 후 해당 파일을 사용 중인 응용 프로그램이나 서비스를 안전하게 종료한 후 다시 시작할 수 있습니다.

다시 시작 횟수를 최소화하면 응용 프로그램 중단이 줄어들고 시스템 가동 시간이 증가합니다.

## Microsoft .NET Framework 3.0

Microsoft .NET Framework 버전 3.0(이전의 WinFX®)은 Windows용 관리되는 코드 프로그래밍 모델입니다. 이 프로그램은 공용 언어 런타임 2.0을 포함하며 시각적으로 뛰어난 작업 환경, 기술 범위 간 커뮤니케이션, ID 관리 및 광범위한 비즈니스 프로세스 지원을 전달하는 응용 프로그램을 구축하기 위한 신기술을 조합해서 제공합니다.

.NET Framework 3.0의 추가 기능에는 다음이 포함됩니다.

* WCF(Windows Communication Foundation)
* WPF(Windows Presentation Foundation)
* Windows WF(Workflow Foundation)
* WCS(Windows CardSpace)(이전의 InfoCard)

Microsoft .NET Framework 3.0은 Windows Server 2008에는 응용 프로그램 서버 역할의 일부로 제공되고 Windows Vista에도 구성 요소로 포함되어 있습니다. 아울러 Windows XP 서비스 팩 2 및 Windows Server 2003 서비스 팩 1에서도 사용할 수 있습니다.

Microsoft .NET Framework 3.0은 .NET Framework 2.0을 보강한 제품군으로 .NET Framework 2.0의 추가 릴리스입니다. 따라서 소프트웨어가 개정되는 세대형 릴리스와는 다릅니다. Microsoft .NET Framework 3.0은 이전 .NET Framework의 코어 런타임 구성 요소를 사용하며, .NET Framework 2.0에서 만든 응용 프로그램과 호환됩니다.

### WCF(Windows Communication Foundation)

WCF(Windows Communication Foundation)는 연결된 시스템을 구축 및 실행하기 위한 .NET Framework 기술 모음입니다. WCF는 기존 Microsoft 연결 기술의 기능을 통합 및 확장하며, 기본 통신 프로토콜과는 독립되는 단일 프로그래밍 모델을 제공합니다. WCF 응용 프로그램은 개방형 표준 및 프로토콜을 사용하여 다른 기술과 상호 운용될 수 있습니다. Windows Communication Foundation에서 지원되는 고급 웹 서비스는 상호 운용성과 함께 안전하고 믿을 수 있는 트랜잭션 메시지를 제공합니다. Microsoft .NET Framework에서 구축된 Windows Communication Foundation의 서비스 지향 프로그래밍 모델은 연결된 시스템의 개발을 간소화합니다. Windows Communication Foundation은 Windows XP 및 Windows Server 2003뿐만 아니라 Windows Server 2008 및 Windows Vista에서 사용할 수 있습니다.

Windows Communication Foundation은 기존 연결 기술의 뛰어난 특성을 조합 및 확장하여 통합된 개발 및 런타임 환경을 제공하는 차세대 연결 기술을 나타냅니다. 이 프로그램은 다음 기술을 대신하는 간단한 API와 일관되며 직관적인 프로그래밍 모델을 제공합니다.

* 효율적인 RPC(원격 프로시저 호출) 기능에 대한 DCOM 및 .NET Remoting 지원
* 쉽게 구성할 수 있으며 상호 운용 가능한 웹 서비스에 대한 ASMX(ASP.NET Web Services) 지원
* 동기화, 분산 트랜잭션, 기본 보안 및 분산 COM+ 서비스에 대한 .NET Framework 엔터프라이즈 서비스 지원
* 보안, 안정적인 메시지 및 분산 트랜잭션 지정을 비롯하여 WS-\* 지정으로 통칭되는 개방형 웹 서비스 표준에 대한 WSE(Web Services Enhancements) 지원
* MSMQ 또는 .NET Framework System.Messaging 네임스페이스 기술과 호환되는 큐 메시지

IIS 7.0에는 WCF의 메시지를 보고 필터링하고 관련 문제를 해결하며, IIS 설정, 사용자 데이터 및 진단을 관리하기 위한 새로운 관리 인터페이스가 있습니다.

### WPF(Windows Presentation Foundation)

WPF는 컴퓨터의 전체 성능을 활용하면서 Windows Vista 및 Windows Server 2008에서 응용 프로그램을 구축하기 위한 토대와 응용 프로그램 UI, 문서 및 미디어 콘텐츠를 아우르는 고품질 환경을 제공합니다. 또한 태블릿 및 기타 입력 형식을 지원하며, 보다 현대적인 이미지 및 인쇄 파이프라인, 뛰어난 액세스 기능 및 UI 자동화 인프라, 데이터 중심 UI 및 가상화, 응용 프로그램 환경을 Windows 셸에 연결하는 통합 지점으로서의 기능도 제공합니다.

### Windows WF(Workflow Foundation)

Windows Workflow Foundation은 Windows에서 워크플로 사용 응용 프로그램을 빠르게 구축할 수 있도록 하는 프로그래밍 모델, 엔진 및 도구입니다. 이 프로그램은 Visual Studio® 2005용 In Process 워크플로 엔진, API 및 디자이너로 구성되어 있습니다. Windows Workflow Foundation은 Windows 클라이언트 버전과 서버 버전 둘 다에서 사용할 수 있습니다. Windows Workflow Foundation은 LOB(기간 업무) 응용 프로그램 내 워크플로, 사용자 인터페이스 페이지 흐름, 문서 중심 워크플로, 휴먼 워크플로, 서비스 지향 응용 프로그램을 위한 복합 워크플로, 비즈니스 규칙 중심 워크플로, 시스템 관리용 워크플로를 비롯한 다양한 시나리오에서 시스템 워크플로 및 휴먼 워크플로를 모두 지원합니다.

### Windows CardSpace

Windows CardSpace™는 사용자들이 디지털 ID의 교환을 보다 잘 관리하고 안전하게 제어하도록 도와 주는 Microsoft Windows의 신기능입니다. 이 기능은 사용자와 중요한 데이터를 일반적인 피싱 및 사기 공격으로부터 보호하며 자신의 디지털 ID 정보를 교환할 상대방을 보다 안전하게 결정할 수 있도록 도와 주는 환경을 제공합니다. Windows CardSpace™는 Windows Vista에는 기본으로 제공되며 Windows XP 및 Windows Server 2003의 경우 다운로드 버전으로 사용할 수 있는 .NET Framework 3.0의 일부로 제공됩니다.

### Service Trace Viewer Tool(SvcTraceViewer.exe)

WCF(Windows Communication Foundation) Service Trace Viewer Tool은 관리자가 WCF에 의해 생성된 진단 추적을 분석할 수 있도록 도와 줍니다. 서비스 추적 뷰어는 사용자들이 WCF 서비스 문제를 진단하고 복구하고 확인할 수 있도록 로그에서 추적 메시지를 쉽게 병합하고 보고 필터링할 수 있게 합니다. 진단 추적은 응용 프로그램 작동 중에 발생하는 상황에 대한 정보를 제공하며 중간 지점을 따라 이동하면서 소스에서 대상까지 작업을 따라갈 수 있습니다.

## PHP 지원

PHP는 다수의 웹 개발자가 사용하는 소스 개방형 스크립팅 언어입니다. Windows Server 2008에는 운영 체제에서 PHP 스크립팅 언어를 실행할 수 있도록 하여 PHP 기반 웹 사이트 및 응용 프로그램이 IIS 7.0 웹 서버에 호스팅될 수 있도록 하는 기능이 포함되어 있습니다.

IIS 7.0에는 FastCGI 기능 모듈도 포함되어 있습니다. FastCGI는 CGI에 대한 개방형 확장으로, 고성능을 제공하고 언어 독립적이며 확장성이 뛰어납니다. FastCGI 확장은 Server Core에 기본으로 제공되며 IIS 7.0에서 향상된 성능과 안정성을 가져다 주는 PHP와 같은 응용 프로그램 프레임워크를 가능하게 합니다. IIS 7.0에서는 ASP, ASP.NET, XML 및 PHP를 지원하여 조직에서 원하는 언어로 유연하게 응용 프로그램을 작성하고 요구에 가장 적합한 플랫폼에 응용 프로그램을 호스팅할 수 있도록 합니다.

## 인증서 서비스

인증서 서비스는 많은 인스턴스에서 인증 및 응용 프로그램에 대한 보안 액세스를 제공하기 위해 사용되는 인증서를 발급하고 관리하기 위한 강력한 사용자 지정 가능 서비스를 제공합니다. Windows Vista 및 Windows Server 2008에는 인증서 서비스에 대한 새 기능의 도입과 더불어, 새 COM 등록 제어, 새 등록 DLL 및 공개 키 인프라 통신 프로토콜인 SCEP(단순 인증서 등록 프로토콜)가 도입되었습니다. 이러한 변경 내용과 향상된 기능은 5장: 보안 및 규정 준수에서 자세히 설명합니다.

## Windows Media Services

Windows Media Services는 인터넷이나 인트라넷을 통해 라이브 또는 주문형 오디오 및 비디오 콘텐츠를 스트리밍할 수 있는 강력한 플랫폼입니다. Windows Media Services에서는 클라이언트에 콘텐츠를 전달하도록 여러 Windows Media 서버를 구성 및 관리할 수 있습니다.

Windows Media Services는 초고속 스트리밍 환경, 개인 설정된 콘텐츠의 즉석 전달을 위한 동적 프로그래밍, 쉬운 관리, 사용자 지정 및 확장성을 보장하는 강력한 플랫폼을 제공합니다.

Windows Media Services의 빠른 스트리밍 기능은 결과적으로 버퍼링 시간을 없애고, 네트워크 연결 중에 재생이 중단될 가능성을 줄여 줍니다. 빠른 시작, 빠른 캐시, 빠른 복구 및 빠른 다시 연결과 같은 기능은 무선 및 위성과 같이 지연이 자주 발생하는 네트워크에서도 최소의 버퍼링 및 작동 중단으로 콘텐츠를 스트리밍하여 중단 없는 시청 환경을 제공합니다.

Windows Media Services는 동적 콘텐츠 프로그래밍을 가능하게 하므로 조직이 콘텐츠를 즉석에서 업데이트하고 개인에 맞게 설정하여 사용자에게 가장 적합한 환경을 제공할 수 있습니다. 이러한 프로그램 기능에는 다음이 포함됩니다.

* 디지털 미디어 콘텐츠를 즉석에서 자동으로 프로그래밍 및 업데이트합니다.
* 주문형 또는 라이브 브로드캐스트 중에 시청을 중단시키지 않으면서 프로그램을 변경하고, 클립 순서를 변경하고, 광고 및 새 클립을 삽입합니다.
* 타사 광고 서버와 쉽게 통합될 수 있는 리드인 또는 삽입 광고를 비롯한 다양한 광고 종류로 수익을 창출합니다. 고급 보고 기능을 통해 광고가 시청된 방식과 시기를 추적합니다.
* 개별 대상 그룹에 맞게 개인 설정된 재생 목록을 자동으로 생성하여 각 사용자에게 보다 적절하고 유용한 스트리밍 콘텐츠를 만듭니다.

이제 Windows Server 2008을 사용하여 관리자들은 Windows Server 2008의 Server Core 설치에서 스트리밍 미디어 서비스 역할을 수행하는 데 필요한 Windows Media Services용 서비스를 설치할 수 있습니다.

## 요약

IIS 7.0의 다양한 구조적 변화로 인해 보다 유연한 웹 응용 프로그램 시스템이 생성되었습니다. GUI 인터페이스와 appcmd.exe 명령줄 도구를 통해 IIS 구성에 액세스할 수 있게 되면서 기본적인 기술을 갖고 있는 초보 웹 서버 관리자와 스크립팅 도구를 사용하여 여러 서버를 관리하는 전문적인 관리자 모두 효과적인 도구를 사용할 수 있게 되었습니다. IIS의 추적 및 문제 해결 구성 요소는 관리자 및 응용 프로그램 개발자가 오작동하는 페이지 및 코드를 격리할 수 있도록 도와 주는 유용하고 상세한 정보를 제공합니다. IIS 7.0의 모듈화된 기능과 세부 관리 모델은 서버 관리자가 필요한 서버를 정확하게 만들 수 있도록 하며 사이트 및 콘텐츠 관리자에 필요한 수준의 액세스만 허용할 수 있도록 함으로써 Windows Server 2008이 호스팅 웹 및 서버 응용 프로그램을 위한 최상의 제품으로 자리 잡는 데 일조했습니다. .NET 3.0의 기능과 WCF(Windows Communication Foundation), WPF(Windows Presentation Foundation), Windows WF(Workflow Foundation) 및 Windows CardSpace의 통합된 기능은 Windows Server 2008을 웹 및 서버 응용 프로그램을 구축할 수 있는 풍부하고 강력한 응용 프로그램 개발 및 지원 플랫폼으로 만들어 줍니다. Windows Media Services는 인터넷 및 인트라넷을 통해 라이브 또는 주문형 오디오 및 비디오 콘텐츠를 스트리밍할 수 있는 다재다능한 플랫폼입니다.

# 7장: 서버 관리

## 소개

Windows Server 2008은 엔터프라이즈에서 단일 서버 및 여러 서버의 관리를 향상시키기 위한 다양한 도구, 기술 및 설치 옵션을 제공합니다. 단일 서버 관리 시, 서버 관리자는 IT 전문가에게 서버 역할, 역할 서비스 및 기능을 추가, 제거 및 구성하기 위한 통합된 작업 환경을 제공하는 단일화된 MMC(Microsoft Management Console)입니다. 또한 서버 관리자는 서버 역할을 기반으로 하는 핵심 관리 작업을 노출하고 고급 관리 도구에 액세스할 수 있도록 하여 지속적인 서버 관리, 모니터링 및 작업에 대한 포털로도 작동합니다.

IIS(인터넷 정보 서비스), 터미널 서버 및 Active Directory와 같은 서버 역할에 대한 작업을 자동화하도록 특수하게 디자인된 새로운 명령줄 셸 및 스크립팅 언어를 제공하면서 기존 스크립트 투자도 활용하는 Windows PowerShell을 사용하여 여러 서버의 관리를 자동화할 수 있습니다.

IT 전문가는 Windows Remote Shell 도구를 사용하여 원격 서버의 WinRM(Windows 원격 관리) 및 WMI(Windows Management Instrumentation) 개체를 통해 서버를 원격으로 관리하거나 관리 데이터를 가져올 수 있습니다. Windows Remote Management는 Microsoft에서 구현한 DMTF(Distributed Manager Task Force) 표준 관리용 웹 서비스(WS-Management)인 새로운 원격 액세스 프로토콜입니다.

Server Core는 특정 서버 역할에 대한 최소 설치 옵션을 제공하는 Windows Server 2008의 새 기능으로, 서버 규격 및 공격 범위를 줄여 관리 및 유지 관리 요구를 줄여줍니다. 이 장에서는 이러한 도구와 기술을 소개하고 Windows Server 2008의 관리 효율을 향상시키는 방법을 설명합니다.

WDS(Windows 배포 서비스)는 네트워크 기반 설치를 지원하여 Windows 운영 체제의 배포를 간소화하여 시간을 절약하는 구성 요소 제품군입니다.

## 초기 구성 작업

네트워크 구성과 같이 사용자 개입이 필요한 구성 작업에 의해 설치 프로세스가 더 이상 중단되지 않으므로 Windows Server 2008의 설치가 간소화됩니다. 이제 이러한 작업과 대화 상자는 기본 설치가 끝난 후에 진행되므로 관리자가 설치가 끝날 때까지 앉아 개입할 필요가 없습니다.

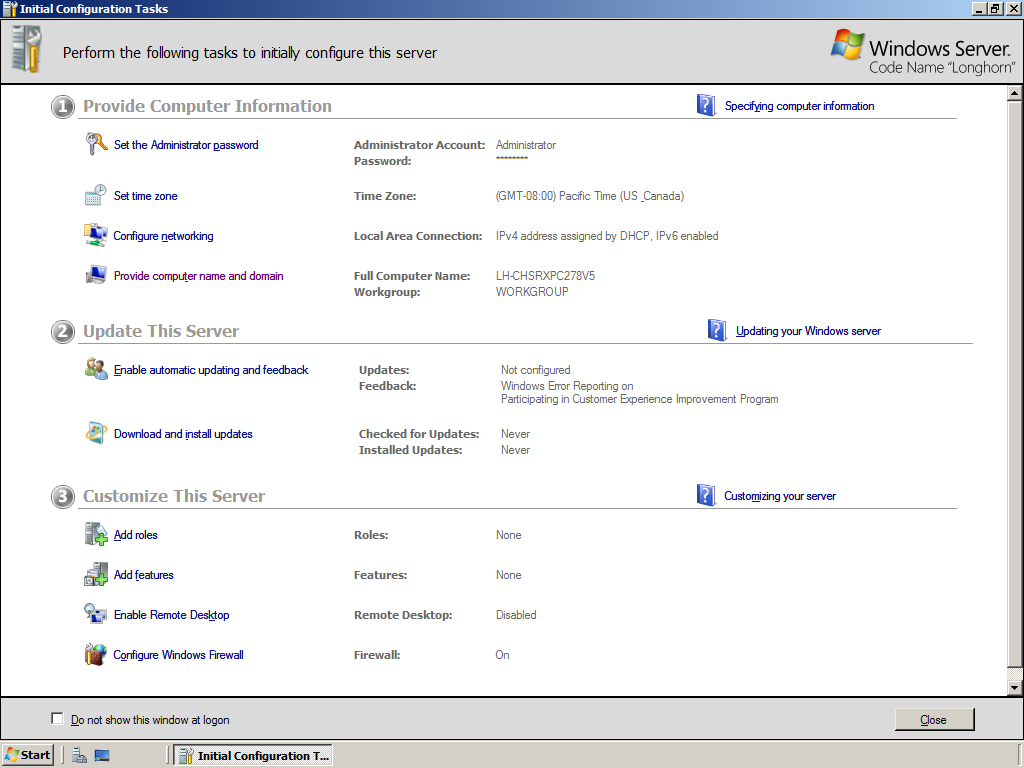


그림 8: 초기 구성 작업 창

초기 구성 작업 창은 관리자가 새 서버를 구축하고 설정할 수 있도록 도와 주는 Windows Server 2008의 새 기능입니다. 여기에는 Administrator 암호 설정, 서버 보안을 향상시키기 위한 Administrator 계정 이름 변경, 기존 도메인에 서버 가입, Windows Update 및 Windows 방화벽 설정 등의 작업이 포함됩니다.

#### 초기 구성의 기본 설정

다음 표에서는 Windows Server 2008 설치 프로세스에 의해 구성된 기본 설정 일부를 보여 줍니다. 초기 구성 작업 창에서 사용할 수 있는 명령을 사용하여 관리자는 이러한 기본값을 수정할 수 있습니다.

표 11: AD DS 초기 구성 기본 설정

|  |  |
| --- | --- |
| **설정** | **기본 구성** |
| Administrator 암호 | Administrator 계정 암호는 기본적으로 비어 있습니다. |
| 컴퓨터 이름 | 컴퓨터 이름은 설치 중에 임의로 지정됩니다. 관리자는 초기 구성 작업 창의 명령을 사용하여 컴퓨터 이름을 수정할 수 있습니다. |
| 도메인 구성원 자격 | 컴퓨터는 기본적으로 도메인에 가입되어 있지 않으며 WORKGROUP이라는 작업 그룹에 가입되어 있습니다. |
| Windows Update | Windows Update는 기본적으로 꺼져 있습니다. |
| 네트워크 연결 | 모든 네트워크 연결은 DHCP를 사용하여 자동으로 IP 주소를 획득하도록 설정됩니다. |
| Windows 방화벽 | Windows 방화벽은 기본적으로 켜져 있습니다. |
| 설치된 역할 | 역할이나 기능은 기본적으로 설치되어 있지 않습니다. |

#### 초기 구성 작업의 이점

초기 구성 작업창은 관리자가 서버를 구성하고 엔터프라이즈의 운영 체제 설치와 서버 배포 간에 소요되는 시간을 단축하도록 도와줍니다. 또한 관리자가 관리자 계정, 도메인 정보 및 네트워크 설정과 같이 이전에는 Windows Server 2003 설치 프로그램에서 구성했던 운영 체제 설정을 논리적 방식으로 지정할 수 있도록 합니다.

Windows Server 2008 이전의 Windows Server급 운영 체제 설치 프로그램은 관리자가 관리자 계정, 도메인 및 네트워크 정보를 제공할 수 있도록 일시 중지되었습니다. 사용자 의견에 이 프로세스로 인해 운영 체제 및 서버 배포가 지연되었음이 표시됩니다. 초기 구성 작업 창에서 관리자는 설치가 완료될 때까지 이러한 작업을 연기할 수 있으므로 작업 중단을 줄이고 전체적인 배포를 보다 빠르게 진행할 수 있습니다.

## 서버 관리자 콘솔

Windows Server 2008에서는 새로운 서버 관리자 콘솔을 사용하여 조직에서 수행되는 여러 서버 역할 설치, 관리 및 보안 유지 작업을 용이하게 진행하도록 합니다. 서버 관리자는 구조, 제약 조건, 구성 및 모범 사례를 비롯하여 소프트웨어에서 복잡한 IT 서비스 및 시스템을 모델링하는 데 사용되는 SML(Service Modeling Language) 플랫폼 위에서 구축되었습니다. 서버 관리자는 SML 플랫폼이 제공하는 모델 기반 관리 인프라를 활용합니다. 서버 관리자 역할은 다음 작업을 위한 통합된 단일 콘솔을 제공합니다.

* 서버의 구성 및 시스템 정보 관리
* 서버 상태 표시
* 서버 역할 구성의 문제점 식별

### 서버에 설치되어 있는 역할, 역할 서비스 및 기능 관리

서버 관리자를 사용하여 설치한 역할 및 기능은 기본적으로 보안이 유지됩니다. 관리자는 기본 설정을 변경하려는 경우가 아니면, 역할 설치나 제거 이후에 보안 구성 마법사를 실행할 필요가 없습니다.

### 서버 역할과 역할 서비스란 무엇인가?

서버 역할이란 서버의 기본 기능을 나타냅니다. 관리자는 전체 서버에 단일 역할을 전담하거나 단일 컴퓨터에 여러 서버 역할을 설치하도록 선택할 수 있습니다. 각 역할에는 하나 이상의 역할 서비스가 포함되거나 선택적으로 설치 가능한 역할 요소가 포함될 수 있습니다. Windows Server 2008에서는 다음 역할을 사용할 수 있으며 이러한 기능은 서버 관리자를 사용하여 설치 및 관리할 수 있습니다.

* Active Directory 인증서 서비스
* Active Directory 도메인 서비스
* Active Directory Federation Services
* AD LDS(Active Directory Lightweight Directory Services)
* Active Directory Rights Management Services
* 응용 프로그램 서버
* DHCP 서버
* DNS 서버
* 팩스 서버
* 파일 서비스
* 네트워크 정책 및 액세스 서비스
* 인쇄 서비스
* 터미널 서비스
* UDDI(Universal Description, Discovery, and Integration) 서비스
* 웹 서버(IIS)
* Windows 배포 서비스
* Windows SharePoint Services

### 기능이란 무엇인가?

기능이라는 말은 일반적으로 서버의 기본 기능을 나타내지 않으며 서버의 보조 또는 지원 기능을 나타냅니다. 즉, 관리자는 기능을 서버의 기본 기능으로서 설치한다기 보다, 설치된 역할의 기능을 확장하기 위해 설치합니다. 예를 들어 장애 조치 클러스터링은 관리자가 파일 서버와 같은 특정 역할을 설치한 후에 파일 서버 역할을 보다 풍부하게 만들기 위해 선택적으로 설치할 수 있는 기능입니다. Windows Server 2008에서는 다음 기능을 사용할 수 있으며 이러한 기능은 서버 관리자를 사용하여 설치할 수 있습니다.

* BitLocker 드라이브 암호화
* BITS 서버 확장
* 연결 관리자 관리 키트
* 데스크톱 환경
* 장애 조치 클러스터링
* 그룹 정책 관리 콘솔
* 인터넷 인쇄 클라이언트
* iSNS(인터넷 저장소 이름 서버)
* LPR 포트 모니터
* 메시지 큐
* Microsoft .NET Framework 3.0 기능
* 다중 경로 I/O
* 네트워크 부하 분산
* 피어 이름 확인 프로토콜
* qWave(Quality Windows Audio Video Experience)
* 복구 디스크
* 원격 지원
* 원격 서버 관리 도구
* 이동식 저장소 관리자
* RPC Over HTTP 프록시
* NFS용 서비스
* 단순 TCP/IP 서비스
* SMTP 서버
* SNMP 서비스
* SAN에 대한 저장소 관리자
* UNIX 기반 응용 프로그램에 대한 하위 시스템
* 텔넷 클라이언트
* 텔넷 서버
* TFTP 클라이언트
* Windows 내부 데이터베이스
* WINS(Windows Internet Name Service)
* Windows PowerShell
* Windows 프로세스 활성화 서비스
* Windows Server 백업
* Windows 시스템 리소스 관리자
* 무선 네트워킹

서버 관리자 콘솔의 계층적 창에는 관리자가 특정 역할을 관리하기 위해 콘솔을 열거나, 문제 해결 도구를 시작하거나, 백업 및 재해 복구 옵션을 찾는 데 사용할 수 있는 확장 가능한 노드가 포함되어 있습니다. 서버 관리자는 다양한 관리 인터페이스와 도구를 통합된 관리 콘솔에 결합하여 관리자들이 여러 인터페이스, 도구 및 대화 상자 간을 이동하지 않고도 일반적인 관리 작업을 완료할 수 있도록 합니다.

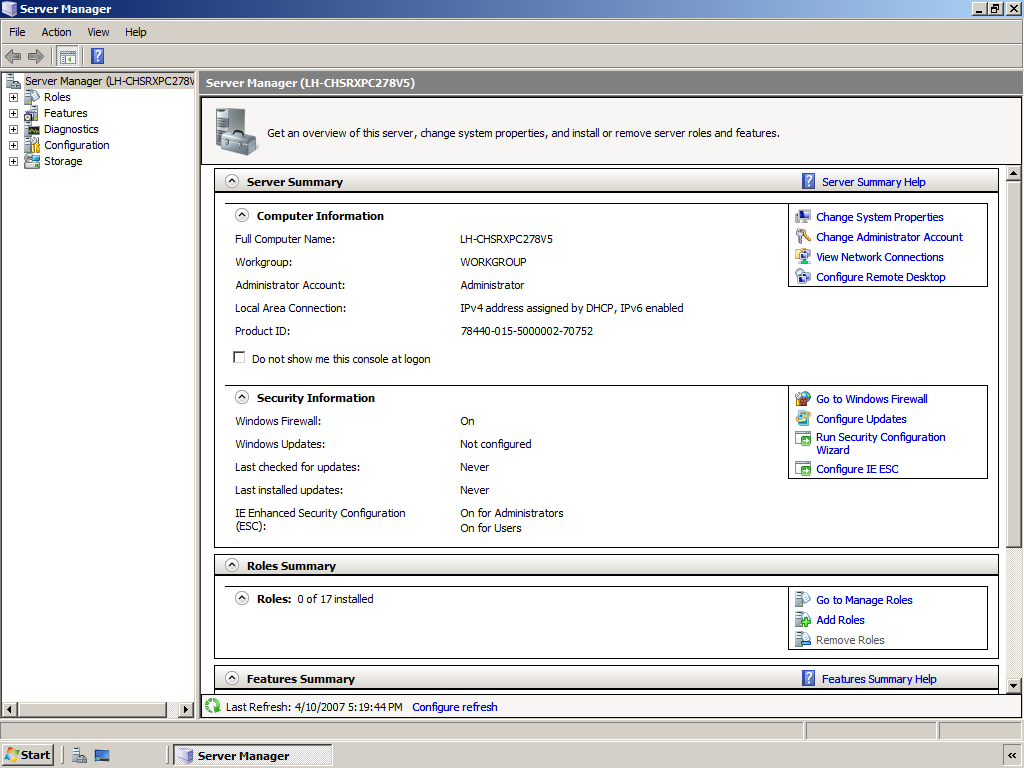


그림 9: 서버 관리자 주 창

서버 관리자 콘솔의 주 창은 다음과 같은 네 가지 축소 가능 섹션으로 구성되어 있습니다.

* 서버 요약 - 서버 요약에는 시스템 정보와 보안 요약의 두 하위 섹션이 포함되어 있습니다. 시스템 정보에는 컴퓨터 이름, 도메인, 로컬 관리자 계정 이름, 네트워크 연결 및 운영 체제의 제품 ID가 표시됩니다. 시스템 정보 하위 섹션의 명령을 사용하여 이 정보를 편집할 수 있습니다..
* 보안 요약 - 보안 요약에는 Windows Update 및 Windows 방화벽 상태가 표시됩니다. 또한 컴퓨터의 업데이트를 마지막으로 확인한 시간과 업데이트가 설치된 시간이 표시됩니다. 보안 요약 하위 섹션의 명령을 사용하여 관리자는 이러한 설정을 편집하거나 고급 옵션을 볼 수 있습니다.
* 역할 요약 - 역할 요약에는 서버에 설치되어 있는 역할을 나타내는 테이블이 포함되어 있습니다. 이 섹션의 명령을 사용하여 관리자는 역할을 추가 또는 제거하거나, 특정 역할을 관리할 수 있는 콘솔을 열 수 있습니다.
* 기능 요약 - 기능 요약에는 서버에 설치되어 있는 기능을 나타내는 테이블이 표시됩니다. 이 섹션의 명령을 사용하여 기능(예: BitLocker, Windows Backup, SMTP 등)을 추가하거나 제거할 수 있습니다.
* 리소스 및 지원 - 리소스 및 지원에는 해당 서버가 사용자 의견 프로그램인 Windows Server 사용자 환경 개선 프로그램(CEIP) 및 Windows 오류 보고에 참여하는 방식을 보여 줍니다. 모든 Microsoft 고객에게 Microsoft 제품의 디자인과 개발에 기여할 수 있도록 하기 위해 CEIP를 만들었습니다. CEIP는 고객이 Microsoft 제품을 사용하는 방식과 고객에게 발생한 문제점에 대한 정보를 수집합니다. 또한 리소스 및 지원 섹션은 화제의 뉴스그룹에 참가하거나 추가 지원 및 연구 항목을 찾을 수 있는 시작점으로도 디자인되었습니다. 이 섹션은 Windows Server TechCenter: <http://go.microsoft.com/fwlink/?LinkID=50945>에서 온라인으로 사용할 수 있습니다.

Windows Server 2008의 서버 관리자 콘솔 통합 관리 인터페이스는 서버 구성 및 설치된 역할의 관리를 간소화합니다.

### 서버 관리자 마법사

서버 관리자의 마법사는 이전 버전의 Windows Server와 비교할 때 배포 시간을 단축하여 엔터프라이즈의 서버 배포 작업을 능률화합니다. 이제 역할 구성이나 제거, 여러 역할 정의와 같은 가장 일반적인 구성 작업은 서버 관리자 마법사를 사용하여 단일 세션에서 완료할 수 있습니다. Windows Server 2008은 사용자가 서버 관리자 마법사를 따라 작업을 진행할 때 종속성 확인을 수행하여 선택한 서버에 필요한 모든 필수 역할 서비스가 설치되어 있는지와 다른 역할이나 역할 서비스에 필요한 역할 서비스가 제거되지 않았는지 확인합니다. Windows Server 2008에는 다음과 같은 역할 마법사가 포함되어 있습니다.

#### 역할 추가 마법사

먼저 역할 추가 마법사를 사용하여 한 번에 여러 개의 역할을 서버에 추가할 수 있습니다. 이 마법사는 역할 간 종속성을 자동으로 확인하고 선택한 각 역할에 대해 필요한 모든 역할 및 역할 서비스가 설치되어 있는지 확인합니다. 터미널 서비스 및 AD CS(Active Directory 인증서 서비스)와 같은 일부 역할의 경우 역할 추가 마법사를 사용하면 역할 구성 방법을 설치 프로세스의 일부로 지정할 수 있는 구성 페이지도 제공됩니다.



그림 10: 역할 추가 마법사의 서버 역할 선택 페이지

#### 역할 서비스 추가 마법사

파일 서비스, 터미널 서비스 및 Active Directory 인증서 서비스와 같은 대부분의 역할은 여러 개의 하위 요소로 구성되어 있습니다. 이러한 하위 요소는 서버 관리자 인터페이스에서 역할 서비스로 식별됩니다. 이러한 복잡한 역할 중 하나가 설치되면 관리자는 역할 서비스 추가 마법사를 사용하여 역할에 역할 서비스를 추가할 수 있습니다. 역할 서비스 추가 마법사를 여는 명령은 서버 관리자 콘솔의 각 역할 홈 페이지에 있습니다.

#### 기능 추가 마법사

기능 추가 마법사를 사용하여 단일 세션에서 하나 이상의 기능을 컴퓨터에 설치할 수 있습니다. 기능은 하나 이상의 역할 기능을 지원 또는 확장하거나, 설치되어 있는 역할에 관계없이 서버 자체의 기능을 향상시키는 소프트웨어 프로그램입니다. 기능의 예로 Windows PowerShell을 들 수 있습니다. 기능 추가 마법사를 여는 명령은 초기 구성 작업 창의 이 서버 사용자 지정영역과 서버 관리자 콘솔 창의 기능 요약 섹션에 포함되어 있습니다.

#### 역할 제거 마법사

역할 제거 마법사는 서버에서 하나 이상의 역할을 제거하는 데 사용할 수 있습니다. 이 마법사는 역할 간의 종속성을 자동으로 확인하고 필요한 역할 및 해당 역할에 대한 역할 서비스가 제거되지 않도록 합니다. 역할 제거 마법사 프로세스는 서버에 남아 있는 역할에 필요한 역할이나 역할 서비스가 실수로 제거되지 않도록 합니다.

#### 역할 서비스 제거 마법사

역할 서비스 제거 마법사를 사용하여 설치된 역할에서 역할 서비스를 제거할 수 있습니다. 역할 서비스 제거 마법사를 여는 명령은 서버 관리자 콘솔의 각 역할 홈 페이지에 있습니다.

#### 기능 제거 마법사

기능 제거 마법사를 사용하여 관리자는 단일 세션에서 컴퓨터에 있는 하나 이상의 기능을 제거할 수 있습니다. 기능 제거 마법사를 여는 명령은 초기 구성 작업 창의 이 서버 사용자 지정영역과 서버 관리자 콘솔의 기능 요약 섹션에 포함되어 있습니다.

#### 효율적인 설치

서버 관리자의 마법사는 역할, 역할 서비스 및 기능을 설치하거나 구성하거나 제거하는 데 필요한 시간을 단축하여 엔터프라이즈에 서버를 배포하는 작업을 간소화합니다. 이전 버전의 Windows Server에서는 사용자가 서버 구성, 서버 관리 또는 Windows 구성 요소 추가/제거를 통해 서버 역할이나 기타 소프트웨어를 추가하거나 제거해야만 했습니다. 종속성 확인 기능이 제한되었으며, 관리자는 Windows 구성 요소 추가/제거를 사용하여 한 번에 한 역할만 설치할 수 있었습니다. 더 많은 역할을 추가하려면 먼저 각 역할의 설치를 끝냈어야 합니다.

서버 관리자의 마법사 모음을 통해 관리자는 단일 세션 내에서 여러 역할을 추가, 제거 또는 확장할 수 있습니다. 한 서버 관리자 마법사에서 단일 세션이 끝났을 때 서버의 배포 준비가 완료될 수 있습니다. 역할 구성은 기본적으로 권장되는 보안 설정으로 구성되므로, 보안 기본값을 수정할 필요가 있는 경우가 아니면 역할이나 기능을 설치한 후에 보안 구성 마법사를 실행할 필요가 없습니다.

### 서버 관리자 명령줄 도구

서버 관리자는 Windows Server 2008이 실행되는 컴퓨터에서 수행되는 역할 및 기능 배포를 자동화하는 명령줄 도구인 ServerManagerCmd.exe를 제공합니다. 이 명령줄 도구를 사용하여 역할, 역할 서비스 및 기능을 설치 및 제거할 수 있습니다. 또한 ServerManagerCmd.exe 매개 변수는 컴퓨터에 설치되어 있거나 설치할 수 있는 모든 역할, 역할 서비스 및 기능 목록을 표시할 수 있습니다. 서버 관리자 명령줄 인터페이스를 통한 설치에서는 매개 변수를 지정하여 명령 인스턴스당 하나의 역할, 역할 서비스 또는 기능을 설치하거나 제거할 수 있습니다. ServerManagerCmd.exe는 XML 응답 파일과 함께 사용하여 반복되는 자동 설치를 보다 빠르게 진행하거나 여러 역할이나 기능을 추가 또는 제거할 수 있습니다.

## Windows PowerShell

Microsoft Windows PowerShell 명령줄 셸 및 스크립팅 언어는 IT 전문가가 일반 작업을 자동화하도록 도와줍니다. 새로운 관리 중심 스크립트 언어, 120개 이상의 표준 명령줄 도구, 일관성 있는 구문과 유틸리티를 제공하는 Windows PowerShell을 사용하면 IT 전문가는 훨씬 쉽게 시스템 관리를 제어하고 자동화를 가속화할 수 있습니다. Windows PowerShell은 기존 IT 인프라 및 기존 스크립트 투자를 활용할 수 있으므로 채택 및 사용이 용이합니다. 또한 사용자가 터미널 서버와 같은 서버 역할을 배포할 수 있을 뿐만 아니라 서버 관리 및 운영 작업을 자동화할 수 있도록 합니다.

### 일관성 및 사용의 용이성

시스템 관리는 복잡한 작업일 수 있으며 일관된 인터페이스가 있는 도구를 사용하면 프로세스의 본질적인 복잡성을 보다 쉽게 제어할 수 있습니다. Windows PowerShell 명령 및 구문의 일관성은 타고난 기능 중 하나로, 관리 작업을 완료하고 스크립트를 작성하는 데 필요한 시간을 단축해 줍니다.

모든 명령은 표준 명명 규칙을 따르며 직관적 유틸리티(예: -sort, -where, -list) 모음을 함께 사용할 수 있으므로 PowerShell 작업을 보다 효율적으로 처리할 수 있습니다. 모든 명령 및 PowerShell 스크립팅 언어는 시스템 관리에 주안점을 두는 이해하기 쉬운 동사-명사 구문(예: get-eventlog, stop=process)을 따릅니다. 또한 Windows PowerShell은 레지스트리 및 인증서 저장소와 같은 시스템 데이터를 탐색하는 기능을 비롯하여 시스템 관리 저장소를 파일 시스템(예: dir //HKLB; cd \\HKJLM)처럼 간편하게 탐색할 수 있도록 합니다.

### 대화형 및 스크립팅 환경

Windows PowerShell은 명령줄 셸과 스크립팅 언어를 통합하여 관리자들이 시스템 관리 작업을 효율적으로 수행하고 자동화할 수 있도록 합니다. Windows PowerShell은 스트립팅 언어와 정확히 동일한 구문을 갖는 cmdlet(명령줄 도구)를 제공하여 Windows 명령 프롬프트 및 WSH(Windows 스크립트 호스트)를 향상시킵니다. Windows PowerShell 명령 프롬프트에 입력하는 명령은 여러 서버에서 작업을 자동화하기 위해 스크립트에서 사용되는 것과 동일한 명령입니다.

PowerShell은 조직의 기존 스크립트(예: .vbs, .bat, .perl)를 지원하므로 Windows PowerShell을 채택하기 위해 스크립트를 마이그레이션하지 않아도 됩니다. 기존 Windows 기반 명령줄 도구는 Windows PowerShell 명령줄에서 실행됩니다. Windows PowerShell은 일관된 구문 및 명명 규칙을 제공하고 스크립팅 언어를 대화형 셸에 통합하여 시스템 관리 작업 자동화에 따른 복잡성과 시간을 줄여 줍니다.

### 개체 지향 및 .NET Framework

사용자들은 텍스트 명령을 입력하여 Windows PowerShell과 상호 작용하지만 Windows PowerShell은 텍스트가 아니라 개체를 기반으로 합니다. 명령의 결과로 개체가 출력됩니다. 사용자는 출력 개체를 다른 명령의 입력으로 보낼 수 있습니다. 그 결과 Windows PowerShell은 새롭고 강력한 명령줄 패러다임을 제공하게 되었습니다. 이해하기 쉬운 명령줄 도구와 유틸리티를 통해 Microsoft .NET 기술, 웹 서비스 및 개체를 사용할 수 있으므로 관리자는 시스템 관리를 보다 쉽게 제어하고 자동화할 수 있습니다. Windows PowerShell은 관리자에게 레지스트리 데이터, WMI 데이터 및 서비스 데이터와 같은 다양한 유형의 시스템 데이터를 필터링, 정렬, 그룹화 및 비교하는 향상된 기능의 새로운 데이터 및 개체 조작 유틸리티를 제공합니다. 예를 들어 PowerShell은 시스템의 사용 가능한 디스크 용량과 같은 하드웨어 구성에 대한 정보를 WMI를 통해 검색할 수 있습니다. 개체 지향 및 .NET Framework는 이러한 강력한 기능의 토대가 됩니다.

## 그룹 정책 기본 설정

많은 조직에서 IT 직원은 사용자를 위해 드라이브 및 프린터를 매핑해야 합니다. 이를 위해 담당 직원은 스크립트를 작성하고 디버깅한 후 GPO(그룹 정책 개체)를 통해 스크립트를 실행해야 합니다. 많은 다른 설정이 로그온 스크립트를 통해서도 배포됩니다. 스크립트는 자주 분산되고, 거의 문서화되지 않으며 문제 해결, 지원 및 수정하는 데 시간이 많이 소요됩니다.

조직에서는 일반적으로 관리되는 설정과 관리되지 않는 설정의 두 가지 유형으로 배포합니다. 관리되는 설정은 적용되는 정책 설정입니다. 사용자는 정책 설정을 변경할 수 없습니다. 정책 설정은 표준 구성을 적용하여 지원 비용을 절감하고 생산성 손실을 방지하도록 도와 주며 조직의 자산을 보호합니다.

관리되지 않는 설정은 기본 설정입니다. 사용자는 정책 설정과 달리 기본 설정은 변경할 수 있습니다. 조직에서는 기본 운영 체제 설정을 적용하지 않고 기본 설정을 명시적으로 배포하여 IT 환경에 보다 잘 호환되고 조직 및 조직 구성원이 컴퓨터를 사용하는 방식에 맞게 특수하게 조정된 구성을 만듭니다. 또한 사용자가 많은 설정을 변경할 수 없는 제한적인 환경에서는 사용자를 위해 일부 기본 설정을 반드시 배포해야 합니다. 조직에서는 다양한 방식으로 기본 설정을 배포하지만 가장 기본적인 설정은 기본 사용자 프로필, 레지스트리 항목(.reg) 파일 및 로그온 스크립트입니다. Windows 이미지에 기본 설정을 포함시키는 것도 일반적입니다. 그러나 기본 설정을 배포하는 데 사용되는 대부분의 방법은 분산형으로 수행되므로 다루기가 힘듭니다.

좀 더 IT 집약적인 기본 설정 배포 방법과 달리, 그룹 정책 기본 설정은 기본 설정을 배포하기 위해 그룹 정책에 중앙 집중식 시스템을 추가합니다. 이 방식은 배포를 간소화하고 구성 오류를 줄이며 IT 비용을 절감합니다. 관리자는 앞에 설명된 단계를 사용하여 매핑된 드라이브를 배포하지 않고 간단히 그룹 정책 개체를 만든 후 드라이브 맵 기본 설정 속성을 편집할 수도 있습니다.

### 기본 설정과 정책 설정

Windows Server 2008에는 GPMC(그룹 정책 관리 콘솔)에 기본 제공되는 새로운 그룹 정책 기본 설정이 포함되어 있습니다. 또한 관리자는 Windows Vista SP1(서비스 팩 1)이 실행되는 컴퓨터에 RSAT(원격 서버 관리 도구)를 설치하여 기본 설정을 구성할 수 있습니다. 현재 베타 버전으로 제공되며 Windows Server 2008 출시 직후에 출시될 예정인 RSAT는 업데이트된 GPMC를 포함합니다.

그룹 정책 기본 설정에 대한 가장 일반적인 질문은 “기본 설정이 정책 설정과 어떻게 다릅니까?”입니다. 이 개념을 이해하는 것은 그룹 정책 기본 설정을 완전히 활용하는 데 꼭 필요합니다. 다음 표에서는 두 설정 간 차이점을 요약해서 설명합니다.

표 12: 기본 설정과 설정

|  | **그룹 정책 기본 설정** | **그룹 정책 설정** |
| --- | --- | --- |
| **적용** | * 기본 설정은 적용되지 않습니다. * 사용자 인터페이스가 비활성화되지 않습니다. * 새로 고치거나 한 번 적용할 수 있습니다. | * 설정이 적용됩니다. * 사용자 인터페이스가 비활성화됩니다. * 설정이 새로 고쳐집니다. |
| **유연성** | * 레지스트리 설정, 파일 등에 대한 기본 설정 항목을 쉽게 만듭니다. * 로컬 또는 원격 컴퓨터에서 개별 레지스트리 설정이나 전체 레지스트리 분기를 가져옵니다. | * 정책 설정을 추가하기 위해 응용 프로그램 지원이 필요하며 관리 템플릿을 만들어야 합니다. * 파일, 폴더 등을 관리하기 위한 정책 설정을 만들 수 없습니다. |
| **로컬 정책** | * 로컬 그룹 정책에서 사용할 수 없습니다. | * 로컬 그룹 정책에서 사용할 수 있습니다. |
| **인식** | * 그룹 정책을 인식하지 않는 응용 프로그램을 지원합니다. | * 그룹 정책을 인식하는 응용 프로그램이 필요합니다. |
| **저장소** | * 원래 설정을 덮어씁니다. * 기본 설정 항목을 제거하면 원래 설정이 복원되지 않습니다. | * 원래 설정이 변경되지 않습니다. * 레지스트리 정책 분기에 저장됩니다. * 정책 설정을 제거하면 원래 설정이 복원됩니다. |
| **대상 및 필터링** | * 대상은 각 유형의 대상 항목에 대해 사용자 인터페이스를 사용하여 세밀하게 지정됩니다. * 개별 기본 설정 항목 수준의 대상을 지원합니다. | * 필터링은 WMI(Windows Management Instrumentation)를 기반으로 수행되며 WMI 쿼리를 작성해야 합니다. * GPO 수준의 필터링을 지원합니다. |
| **사용자 인터페이스** | * 대부분의 설정을 구성하기 위한 익숙하고 간편한 인터페이스를 제공합니다. | * 대부분의 정책 설정에 대한 대체 사용자 인터페이스를 제공합니다. |

기본 설정과 정책 설정의 기본적인 차이점은 적용입니다. 그룹 정책은 정책 설정을 엄격하게 적용합니다. 첫째, 그룹 정책은 레지스트리 정책 분기에 해당 설정을 쓰며, 각 분기에 대한 ACL(액세스 제어 목록)은 표준 사용자가 해당 정책 설정을 변경하지 못하도록 합니다.

그룹 정책 인식 응용 프로그램이나 운영 체제 기능은 관리될 수 있는 설정을 찾습니다. 정책 설정이 없으면 레지스트리의 다른 위치에서 설정을 찾습니다. 둘째, 그룹 정책 인식 응용 프로그램 및 운영 체제 기능은 일반적으로 그룹 정책에 의해 관리되는 설정에 대한 사용자 인터페이스를 사용할 수 없도록 설정하므로 사용자들은 변경할 수 없습니다. 마지막으로 그룹 정책은 정기적으로(기본적으로 90분 간격) 정책 설정을 새로 고칩니다. 이 새로 고침 간격은 그룹 정책 관리자가 구성할 수 있습니다.

그룹 정책 설정과 달리, 그룹 정책은 기본 설정을 엄격하게 적용하지 않습니다. 그룹 정책은 레지스트리의 그룹 분기에 기본 설정을 저장하지 않습니다. 대신, 응용 프로그램 또는 운영 체제 기능이 설정을 저장하는 데 사용하는 레지스트리의 같은 위치에 기본 설정을 씁니다. 이러한 방식은 다음과 같은 두 가지 결과를 가져옵니다. 첫째, 그룹 정책 기본 설정은 그룹 정책이 인식하지 못하는 응용 프로그램 및 운영 체제 기능을 지원합니다. 둘째, 그룹 정책 기본 설정을 사용할 경우 응용 프로그램 또는 운영 체제 기능에서 구성되는 설정에 대한 사용자 인터페이스가 비활성화되지 않습니다. 따라서 그룹 정책을 사용하여 기본 설정을 배포한 후에도 해당 설정을 변경할 수 있습니다. 또한 그룹 정책은 기본적으로 그룹 정책 설정과 동일한 간격으로 기본 설정을 새로 고칩니다. 그러나 관리자는 개별 기본 설정을 한 번만 적용하도록 선택하여 그룹 정책이 해당 기본 설정을 새로 고치지 못하도록 할 수 있습니다. 이렇게 하면 기본 설정을 한 번 구성한 후 사용자가 지속적으로 변경하도록 할 수 있습니다.

그룹 정책 필터링은 그룹 정책 기본 설정 항목 수준의 대상과 본질적으로 다릅니다. GPO는 WMI 필터를 사용하여 필터링되며 해당 필터는 그룹 정책이 전체 GPO에 적용될지 여부를 결정합니다. GPO 내의 개별 정책 설정은 필터링할 수 없습니다. 물론, 이 제한을 극복하기 위해 필터링 요구에 따라 GPO를 만들 수 있지만 이 경우 대량의 GPO 모음을 관리해야 할 수 있습니다. 한편, 그룹 정책 기본 설정은 항목 수준의 대상을 지원하므로 GPO 내에서 개별 기본 설정 항목을 대상으로 지정할 수 있습니다. 예를 들어 단일 GPO에 전원 정책을 구성하는 두 개의 기본 설정 항목이 포함될 수 있습니다. 첫 번째 기본 설정 항목은 데스크톱 PC를 대상으로 하고 두 번째는 모바일 PC를 대상으로 할 수 있습니다. 또한 그룹 정책 필터링을 위해 관리자는 경우에 따라 복합 WMI 쿼리를 작성해야 하지만 항목 수준 대상은 친숙한 사용자 인터페이스를 제공합니다.

### 그룹 정책 기본 설정 항목

다음 표에서는 각 그룹 정책 기본 설정 확장의 핵심 기능을 개괄적으로 소개합니다.

표 13

|  |  |
| --- | --- |
| **Windows 설정** | |
| **드라이브** **맵** | 로그온 스크립트 없이 네트워크 드라이브 매핑을 만들고, 바꾸고, 업데이트하고, 삭제할 수 있도록 합니다.  여러 드라이브 맵 기본 설정 항목을 단일 GPO 내에서 배포할 수 있습니다. 드라이브 맵 기본 설정 항목은 특정 부서, 위치 등을 대상으로 할 수 있습니다. |
| **환경** | 사용자 및 시스템 환경 변수를 관리할 수 있습니다.  단일 GPO를 사용하여 여러 다른 시나리오에 대한 변수를 구성하는 방법을 제공합니다.  파일 리포지토리의 위치는 환경 기본 설정 확장을 사용하여 정의할 수 있습니다. 그러면 경로를 하드 코딩하지 않고도 이러한 변수를 다른 기본 설정 항목에서 사용할 수 있으며, 경로가 변경될 때 단일 GPO가 업데이트되므로 다른 위치에서 경로를 찾을 필요가 없습니다. |
| **파일** | 대상 컴퓨터에서 파일을 만들고 바꾸고 업데이트하고 삭제할 수 있도록 합니다.  파일 경로에 와일드카드를 사용하여 단일 GPO를 통해 파일 그룹을 쉽게 복사할 수 있도록 합니다.  파일 기본 설정 확장은 일반적으로 사용자 프로필 폴더에 구성 파일을 복사하는 데 사용할 수 있습니다. 예를 들어 이 확장을 사용하여 IT 직원은 사용자 지정 사전 또는 응용 프로그램 파일을 각 사용자 프로필 내의 AppData 폴더에 복사할 수 있습니다. |
| **폴더** | 대상 컴퓨터에서 폴더를 만들고 바꾸고 업데이트하고 삭제하고 정리할 수 있습니다.  환경 변수는 지원되지만 폴더 경로에 와일드카드를 사용할 수는 없습니다.  폴더 기본 설정 확장은 임시 폴더를 정기적으로 정리하는 데 사용할 수 있습니다. 예를 들어 일부 응용 프로그램이 시스템 드라이브의 루트에 만드는 임시 폴더를 제거하거나 Windows 임시 폴더를 정기적으로 정리하는 데 이 확장을 사용할 수 있습니다. |
| **Ini 파일** | .ini 파일에서 개별 속성을 만들고 업데이트하고 바꾸고 삭제할 수 있습니다. |
| **네트워크 공유** | 여러 대상 컴퓨터의 네트워크 공유를 관리할 수 있습니다.  ABE(액세스 기반 열거)를 관리하여 사용자에게 액세스 권한이 없는 하위 폴더가 표시되지 않도록 하고, 사용자 제한을 구성할 수 있도록 합니다. |
| **레지스트리** | 여러 컴퓨터에서 레지스트리 설정을 만들고 바꾸고 업데이트하고 삭제하는 유연하고 손쉬운 방법을 제공합니다.  레지스트리 기본 설정 항목은 스크립트를 작성하지 않고도 설정을 배포하는 편리한 방법입니다. 예를 들어 이 항목을 사용하여 타사 응용 프로그램이나 그룹 정책이 인식하지 못하는 응용 프로그램에 대한 설정을 배포할 수 있습니다. |
| **바로 가기** | 여러 대상 사용자 및 컴퓨터에서 다음 세 가지 유형의 바로 가기를 만들고 바꾸고 업데이트하고 삭제할 수 있도록 합니다.   * 파일 시스템 개체 **-** 프로그램 및 문서에 연결되는 일반적인 바로 가기 * URL - 웹 페이지에 대한 바로 가기 * 셸 개체 - 제어판, 휴지통 등을 비롯하여 셸 네임스페이스에 나타나는 개체   바로 가기 기본 설정 확장은 바탕 화면, **시작** 메뉴, 즐겨찾기 폴더 및 빠른 시작 도구 모음을 비롯한 여러 위치에서 바로 가기를 만들 수 있도록 지원합니다. |
| **제어판 설정** | |
| **데이터 원본** | 사용자 및 컴퓨터에 대한 데이터 원본을 만들고 바꾸고 업데이트하고 삭제할 수 있도록 합니다.  사용자 데이터 원본이 사용자와 함께 컴퓨터 간에 로밍되도록 하여 배포를 획기적으로 간소화합니다.  데이터 원본 확장을 사용하면 데이터 원본 구성을 필요로 하는 업무용 응용 프로그램 관리에 따른 복잡성 및 비용이 절감됩니다. |
| **장치** | 사용자 또는 컴퓨터에 대한 특정 장치 클래스를 사용할 수 없게 설정하는 방법을 제공합니다.  예를 들어 고객 기록이나 지적 재산권과 같은 민감한 정보를 다루는 사용자는 장치 확장을 사용하여 다른 사람이 USB 포트, 플로피 디스크 드라이브 및 기타 이동식 미디어를 사용하지 못하게 설정하도록 할 수 있습니다.  장치 확장으로 사용자의 장치 설정이 금지되지는 않으며 컴퓨터에 있는 장치를 사용하거나 사용하지 않도록 설정하는 데 사용됩니다. |
| **폴더 옵션** | 다음 두 가지 유형의 항목이 지원됩니다.   * 폴더 옵션 - Windows XP 또는 Windows Vista에 대한 Windows 탐색기 폴더 옵션을 구성합니다. * 연결 프로그램 - 파일 확장명과 파일 형식 간의 연결을 구성합니다. 두 가지 시나리오가 일반적입니다. 첫째, 프로그램을 실수로 또는 악의적인 의도로 실행할 수 없도록 파일 연결을 끊을 수 있습니다(많은 전자 메일 바이러스의 실행에 파일 연결 기능이 필요함). 둘째, 파일 확장명을 다른 프로그램에 연결할 수 있습니다. |
| **인터넷 설정** | Microsoft Internet Explorer 5, Internet Explorer 6 및 Internet Explorer 7의 Internet Explorer 옵션을 구성할 수 있습니다.  인터넷 옵션 제어판에서 사용할 수 있는 대부분의 설정을 구성할 수 있습니다.  이러한 많은 설정은 엄격하게 적용되는 그룹 정책 설정으로 사용할 수 있습니다. 인터넷 설정 기본 설정 확장은 사용자가 나중에 변경할 수 있는 기본 Internet Explorer 구성을 만드는 데 사용할 수 있습니다. |
| **로컬 사용자 및 그룹** | 여러 대상 컴퓨터에 대한 로컬 사용자 계정 및 그룹을 구성할 수 있습니다. 다음과 같은 기본 설정 유형이 지원됩니다.   * 로컬 사용자 - 로컬 컴퓨터에서 사용자 계정을 만들거나 업데이트하거나 바꾸거나 삭제할 수 있습니다. 예를 들어 이 유형을 사용하여 로컬 Administrator 계정의 암호를 변경하거나 이 계정을 사용하지 못하게 설정할 수 있습니다. * 로컬 그룹 - 로컬 컴퓨터에서 그룹을 만들거나 업데이트하거나 바꾸거나 삭제할 수 있습니다. 예를 들어 이 유형을 사용하여 로그온한 사용자를 그룹에 추가하거나 그룹에서 제거할 수 있습니다. |
| **네트워크 옵션** | 다음 유형의 네트워크 연결을 구성할 수 있습니다.   * VPN 연결 - VPN(가상 사설망)의 옵션, 보안 설정 및 연결 유형 등을 구성할 수 있습니다. * DUN 연결 - 기본 전화 접속 구성 |
| **전원 옵션** | 전원 옵션 기본 설정 항목을 사용하여 Windows XP가 실행되는 컴퓨터의 전원 옵션 및 전원 구성표를 구성할 수 있습니다. 이를 통해 사용자가 나중에 필요할 때 변경할 수 있는 기본 구성을 만들 수 있습니다. |
| **프린터** | 프린터 연결 구성은 관리자가 대개 로그온 스크립트를 작성하여 수행하는 일반적인 작업입니다. 프린터 기본 설정 확장은 여러 대상 사용자 또는 컴퓨터에 대해 공유 프린터, TCP/IP 프린터 및 로컬 컴퓨터를 쉽게 만들거나 업데이트하거나 바꾸거나 삭제할 수 있도록 합니다.  기본 설정 대상을 사용하여 위치, 부서, 컴퓨터 종류 등을 기반으로 프린터 연결을 배포할 수 있습니다. |
| **국가별 옵션** | 숫자, 통화, 시간 및 날짜 형식을 비롯하여 사용자 로캘을 구성할 수 있습니다. |
| **예약된 작업** | 중앙에서 대상 사용자 및 컴퓨터의 작업을 예약할 수 있습니다. 예약된 작업 기본 설정 항목에 대한 사용자 인터페이스는 Windows의 예약된 작업에 해당합니다.  이 기본 설정 확장을 사용하면 Windows Vista의 강력한 새 작업 스케줄러를 사용하여 예약된 작업을 아주 쉽게 관리할 수 있습니다. |
| **서비스** | 다음 방식으로 서비스를 구성할 수 있습니다.   * 시작 - 시작 유형을 선택적으로 자동, 수동 또는 사용 안 함으로 변경합니다. * 서비스 작업 - 서비스를 선택적으로 시작, 중지 또는 다시 시작합니다. * 다음 계정으로 로그온 - 서비스가 사용하는 계정을 구성합니다. * 복구 - 서비스의 복구 옵션을 구성합니다. |
| **시작 메뉴** | 사용자의 **시작** 메뉴 옵션을 구성할 수 있습니다.  Windows XP 및 Windows Vista 시작 메뉴 기본 설정 항목이 모두 지원됩니다.  예를 들어 이 메뉴 옵션을 사용하여 **연결 대상** 메뉴를 항상 표시하도록 모바일 PC에 대한 **시작** 메뉴를 구성하거나 조직의 직원이 컴퓨터를 사용하는 방식을 반영하도록 **시작** 메뉴를 쉽게 구성할 수 있습니다. |

### 그룹 정책 기본 설정 기능

대부분의 그룹 정책 기본 설정 확장은 각 기본 설정 항목에 대해 다음과 같은 작업을 지원합니다.

* 만들기 - 대상 컴퓨터에서 새 항목을 만듭니다.
* 삭제 - 대상 컴퓨터에서 기존 항목을 제거합니다.
* 바꾸기 - 대상 컴퓨터에서 항목을 삭제한 후 다시 만듭니다. 그 결과 그룹 정책 기본 설정이 기본 설정 항목과 관련된 모든 기존 설정 및 파일을 대신합니다.
* 업데이트 - 대상 컴퓨터에서 기존 항목을 수정합니다.

### 대상 제어

대상 기능이 추가되었기 때문에 기본 설정은 구성 배포에 아주 유용한 도구가 되었습니다.

WMI 필터를 사용하여 GPO를 필터링할 수 있지만 필터는 전체 GPO에 영향을 줍니다. GPO의 개별 정책 설정을 필터링하려는 경우 개별 설정에 대해 별도의 GPO를 만든 후 각 GPO를 필터링하는 것이 해결 방법이 될 수 있습니다. 많은 조직에서는 이렇게 작업할 경우 수천 개까지는 아니겠지만 수백 개의 GPO가 생성되므로 유지 관리도 어렵고 성능도 크게 저하시킬 수 있습니다.

그러나 그룹 정책 기본 설정은 항목 수준의 대상을 지원합니다. 항목 수준 대상은 그룹 정책이 GPO 내의 개별 기본 설정 항목을 적용하는 사용자 및 컴퓨터를 결정합니다. 예를 들어 다양한 위치의 컴퓨터를 포괄하는 단일 GPO 내에서 여러 다른 기본 설정을 대상으로 지정할 수 있습니다.

그룹 정책 기본 설정 항목은 사용자 및 컴퓨터를 구성하기 위한 핵심 요소가 되지만 대상 항목은 제한된 사용자 및 컴퓨터를 선택하는 데 필요한 논리를 제공합니다. 다음은 관리자가 실제로 그룹 정책 대상 항목을 사용하는 방식을 보여 주는 예입니다.

* 모바일 컴퓨터 - 조직에서 VPN 연결을 구성하지만 모바일 PC에만 VPN 연결을 적용하려고 할 수 있습니다. 휴대용 컴퓨터 대상 항목을 사용하여 모바일 PC로만 기본 설정 항목을 제한할 수 있습니다.
* 성능 기반 구성 - 각 컴퓨터의 성능 특성을 기반으로 특정 설정을 구성해야 할 수 있습니다. 사용 가능한 디스크 공간이 충분한 고속 컴퓨터는 하나의 기본 설정 항목을 수신하고, 저속 컴퓨터나 사용 가능한 디스크 공간이 부족한 컴퓨터는 다른 기본 설정 항목을 수신할 수 있습니다. CPU 속도 및 디스크 속도 대상 항목을 사용하여 필요에 따라 각 기본 설정 항목을 대상으로 지정할 수 있습니다.
* 운영 체제 버전 - Windows Vista를 사용하면 일부 설정이 Windows XP와는 다른 위치에 저장됩니다. 각 운영 체제에 대해 하나씩 두 개의 기본 설정 항목이 생성될 수 있습니다. 그런 후 운영 체제 대상 항목을 사용하여 각 필터 기본 설정 항목을 대상으로 지정할 수 있습니다.
* 소프트웨어 사전 요구 사항 - 응용 프로그램 설정을 구성해야 할 수 있지만 관리자는 이 작업을 수행하기 전에 먼저 컴퓨터에 실제로 해당 응용 프로그램이 설치되어 있는지 확인하려고 할 수 있습니다. 파일 일치 및 레지스트리 일치 대상 항목을 함께 사용하여 특정 버전의 이진 파일이 있는지 확인하거나, Uninstall 레지스트리 키의 항목으로 응용 프로그램이 설치되어 있는지 확인할 수 있습니다.

### 그룹 정책 기본 설정 배포

그룹 정책 기본 설정을 사용하기 위해 서버에 서비스를 설치할 필요는 없습니다. Windows Server 2008에는 GPMC(그룹 정책 관리 콘솔)의 일부로 그룹 정책 기본 설정이 기본적으로 포함되어 있습니다. 관리자는 Windows Vista SP1이 실행되고 있는 컴퓨터에 RSAT를 설치하여 Windows Server 2003 환경에서 그룹 정책 기본 설정을 구성하고 배포할 수 있게 될 것입니다. RSAT 및 Windows Vista SP1 모두 2008년 2사분기에 출시될 예정입니다.

그룹 정책 기본 설정이 들어 있는 GPO를 만들기 위해 서비스를 설치할 필요는 없지만 기본 설정을 배포할 클라이언트 컴퓨터에 그룹 정책 기본 설정 CSE(클라이언트측 확장)를 배포해야 합니다. Microsoft에서는 별도의 다운로드로 CSE를 제공할 예정입니다. CSE는 다음 Windows 버전을 지원합니다.

* Windows XP SP2
* Windows Vista
* Windows Server 2003 SP1
* Windows Server 2008에는 이미 CSE가 포함되어 있음

### 그룹 정책 기본 설정의 이점

다음 목록에서는 그룹 정책 기본 설정 사용의 이점을 요약해서 보여 줍니다.

* IT 생산성 향상 - 그룹 정책 기본 설정은 20가지가 넘는 새로운 확장으로 그룹 정책 기능 집합을 확장하여 IT 직원이 친숙한 도구로 더 많은 작업을 수행할 수 있도록 합니다. 또한 중앙의 원본 위치에서 설정을 구성 및 배포할 수 있으므로 구성이 업데이트될 때 설정을 다시 패키지하고 다시 배포할 필요가 없습니다. 관리자는 업데이트하려는 기본 설정 항목이 들어 있는 GPO를 편집하기만 하면 됩니다. 기본 설정은 사용자 및 컴퓨터 구성을 관리할 수 있는 중앙의 위치를 제공합니다.
* 로그온 스크립트에 대한 필요성 감소 - 그룹 정책 기본 설정이 로그온 스크립트에 대한 필요성을 완전히 해소하는 것은 아니지만 필요성을 크게 줄여 줍니다. 로그온 스크립트에 의해 수행되는 가장 일반적인 작업은 프린터 설치, 네트워크 드라이브 매핑, 레지스트리 설정 구성, 파일/폴더 복사입니다.
* 구성 오류 제한 - 배포 도중 및 이후에 발생하는 구성 오류는 대개 높은 배포 비용을 초래하는 지원 요청을 유발합니다. 그룹 정책 기본 설정은 이러한 비용 절감 효과를 가져옵니다. 첫째, 기본 설정은 다른 도구보다 정밀하게 항목을 구성할 수 있도록 합니다. 둘째, 항목의 세부 정보를 몰라도 구성이 가능합니다. 대신, 그룹 정책 기본 설정은 명확하고 익숙하며 사용이 용이한 대화 상자를 사용하여 기본 설정 항목을 수집하므로 사용자는 Windows 레지스트리에 값이 저장되는 방식을 알아야 할 필요가 없습니다. 관리자는 레지스트리에 저장할 값과 저장 위치를 알아야 할 필요가 없으며, 기본 설정 항목에서 옵션을 선택하여 **시작** 메뉴 설정을 구성할 수 있습니다. 그룹 정책 기본 설정을 사용하면 대부분의 경우 기본 사용자 프로필을 사용하여 설정을 배포할 필요가 없습니다. 기본 사용자 프로필을 사용할 경우 필요한 것보다 더 많은 설정이 배포되므로 결과적으로 구성의 신뢰도가 떨어질 수 있습니다.
* 최종 사용자 만족도 향상 - 구성이 일관되고 믿을 수 있다면 생산성이 일정 수준 이상으로 유지될 수 있으므로 사용자의 만족도가 높아집니다. 또한 그룹 정책 기본 설정을 사용하여 사용자 및 컴퓨터를 구성하면 표준 사용자 계정을 사용하여 더 나은 결과를 얻을 수 있습니다. 그룹 정책 기본 설정은 기본적으로 로컬 시스템 계정을 사용하여 사용자가 구성할 수 없는 설정을 구성하도록 합니다. 관리자는 사용자 대신 이러한 설정을 구성하여 문제를 피할 수도 있습니다.
* 이미지 유지 관리 작업 최소화 - 그룹 정책 기본 설정을 최소화된 이미지(thin image) 전략과 함께 사용하면 디스크 이미지 유지 관리에 드는 시간과 비용을 크게 절감할 수 있습니다. 구성 변경을 반영하도록 이미지를 업데이트하는 대신, 일반 이미지를 배포한 후 관리자가 그룹 정책 설정을 업데이트할 수 있습니다. 이 방법은 엔지니어링 및 테스트 시간과 비용을 크게 줄여 줍니다.
* 전체 이미지 수 줄이기 - 그룹 정책 기본 설정을 씬 이미지 전략과 함께 사용하면 개발 및 유지 관리해야 하는 디스크 이미지의 수를 줄이는 데 도움이 됩니다. 복합 이미지(thick image)를 작성하면 대개 조직 내의 여러 사용자 그룹에 대한 고유 이미지가 만들어집니다. IT 부서에서는 그룹 정책 기본 설정을 사용하여 각 그룹의 일반 이미지를 작성 및 배포한 후 기본 설정 항목을 대상으로 지정하여 사용자 및 컴퓨터를 고유하게 구성할 수 있습니다.

## Windows 원격 관리(WS-Management)

지점 및 기타 위치의 원격 서버 수가 증가하면서 IT 전문가는 오프사이트 서버를 효과적으로 관리하기 위한 보다 적절한 방법이 필요하게 되었습니다. Windows 원격 관리는 원격 위치에 있는 서버를 낮은 대역폭에서 쉽게 관리할 수 있는 스크립팅 가능한 방식을 제공합니다. Windows Remote Manager는 Microsoft에서 구현한 WS-Management 프로토콜입니다. 표준 SOAP을 기반으로 하는 이 프로토콜은 하드웨어와 운영 체제의 상호 운용을 가능케 합니다. DCOM 기반 원격 액세스와 달리, Windows 원격 관리 및 WS-Management는 표준 고정 포트를 사용합니다. WS-Management는 DCOM 기반 액세스에 사용되는 동적 포트 모델과 달리, 표준 고정 포트를 사용하므로 수준 높은 보안성을 제공합니다.

관리자는 Windows 원격 관리 스크립팅 개체, Windows 원격 관리 명령줄 도구 또는 Windows 원격 셸 명령줄 도구를 사용하여 관리 데이터를 가져올 수 있습니다. 예를 들어 디스크, 네트워크 어댑터, 서비스 또는 프로세스와 같은 개체에 대한 정보를 로컬 및 원격 컴퓨터에서 가져올 수 있습니다. 컴퓨터에서 Windows 원격 관리가 포함된 Windows 운영 체제 버전이 실행되고 있는 경우 WMI(Windows Management Instrumentation)에서 관리 데이터를 제공합니다. 하드웨어 및 시스템 데이터는 비 Windows 운영 체제에서 실행되는 WS-Management 프로토콜 구현에서도 가져올 수 있습니다. WS-Management 프로토콜에 반환된 데이터는 개체가 아닌 XML 형식을 갖습니다.

### Windows 원격 셸

IT 전문가는 새로운 WinRA(Windows 원격 셸) 도구를 사용하여 서버를 원격으로 관리하거나 원격 서버의 Windows 원격 관리 및 WMI(Windows Management Instrumentation) 개체를 통해 관리 데이터를 가져올 수 있습니다. Windows 원격 셸을 통해 Windows Vista 및 Windows Server 2008 컴퓨터에서 원격으로 스크립트를 실행할 수 있습니다. WinRS는 Microsoft에서 구현한 DMTF 표준 WS-Management 원격 액세스 프로토콜을 활용합니다.

## Server Core

Windows Server 2008부터, 관리자는 Windows Server 설치 시 원치 않는 기능은 제외하고 필요한 특정 기능만 최소로 설치할 수 있게 되었습니다. Server Core는 다음 서버 역할이 여러 개 실행될 수 있는 환경을 제공합니다.

* Hyper-V
* IIS 7.0
* DHCP(Dynamic Host Configuration Protocol) 서버
* DNS(Domain Name System) 서버
* 파일 서버
* Active Directory 도메인 서비스
* AD LDS(Active Directory Lightweight Directory Services)
* Windows Media Services
* 인쇄 서버

Windows Server 2008의 Server Core 설치는 다음 옵션 기능을 지원합니다.

* 장애 조치 클러스터링
* WINS
* 네트워크 부하 분산
* UNIX 기반 응용 프로그램에 대한 하위 시스템
* 백업
* 다중 경로 IO
* 이동식 저장소 관리
* BitLocker 드라이브 암호화
* SNMP(Simple Network Management Protocol)
* 분산 파일 시스템 복제
* SNTP(Simple Network Time Protocol)

이를 위해 Server Core 설치 옵션은 서버에 대해 선택한 역할에 필요한 실행 파일 및 지원 DLL(동적 연결 라이브러리)만 설치합니다. 예를 들어 Windows 탐색기의 사용자 인터페이스(또는 "셸")는 Server Core의 일부로 설치되지 않습니다. 대신 Server Core 기반 서버를 사용할 때 기본 사용자 인터페이스는 명령 프롬프트입니다.

Server Core는 조직에 다음과 같은 이점을 제공합니다.

* 소프트웨어 유지 관리 감소 - Server Core는 설치된 서버 역할을 지원하는 데 필요한 항목만 설치하므로 소프트웨어 유지 관리 작업이 줄어듭니다. 보다 줄어든 Server Core 설치를 수행하면 업데이트 및 패치 수가 감소되므로 서버의 WAN 대역폭 사용량과 IT 직원의 관리 시간이 절약됩니다. 최소의 Server Core 설치를 사용하면 설치된 구성 요소 중에서 업데이트 또는 패치해야 하는 구성 요소 수가 줄어들며 필요한 다시 시작 수도 줄어듭니다.
* 공격 위험 감소 - 서버에서 더 적은 수의 파일이 설치 및 실행되므로 네트워크에 노출되는 공격 경로가 줄어들게 되며 결과적으로 공격 위험도 줄어듭니다. 관리자는 지정한 서버에 필요한 특정 서비스만 설치할 수 있으므로 노출 위험이 최소로만 유지됩니다.
* 필요한 다시 시작 횟수 및 디스크 공간 감소 - Server Core 설치는 필수 기능을 제공하는 데 필요한 최소 파일을 설치하므로 서버에서 더 적은 디스크 공간이 사용됩니다.

Server Core는 많은 서버를 보유하고 그 중 일부 서버가 전용 작업만 수행하면 되는 조직이나, 높은 보안성이 요구되는 환경에서 사용되도록 디자인되었습니다.

많은 Windows Server 작업에 그래픽 사용자 인터페이스를 사용할 수 없으므로 Server Core 설치 옵션을 사용할 경우, 관리자는 Server Core 컴퓨터를 관리할 원격 컴퓨터로 선택하여 Windows Server 2008이 실행되는 다른 컴퓨터의 MMC(Microsoft Management Console) 스냅인을 사용하여 Server Core 설치를 관리해야 하며, 그렇지 않은 경우 명령 프롬프트 또는 스크립팅 기술을 사용하여 서버의 로컬 관리를 수행해 본 경험이 있어야 합니다.

### 비 응용 프로그램 플랫폼

Server Core는 응용 프로그램 플랫폼이 아니며 사용자는 Server Core 설치에서 서버 응용 프로그램을 실행하거나 개발할 수 없습니다. Server Core 설치는 지원되는 서버 역할 및 관리 도구를 실행하는 데만 사용할 수 있습니다.

Server Core는 다음 두 범주로 구분될 수 있는 관리 도구 및 에이전트를 지원합니다.

* 원격 관리 도구 - 이 도구는 Server Core 설치에서 지원하는 프로토콜 중 하나를 사용하여 RPC와 같은 원격 관리 워크스테이션과 통신하므로 변경할 필요가 없습니다.
* 로컬 관리 도구 및 에이전트 - 이 도구는 어떠한 셸 또는 사용자 인터페이스에도 종속될 수 없으며 관리되는 코드도 사용할 수 없으므로 Server Core 설치에서 사용하기 위해 변경해야 할 수 있습니다.

Windows Server 2008 SDK(소프트웨어 개발 키트)에는 Server Core 설치에서 지원되는 API 목록이 포함되어 있습니다.

관리자는 서버에서 Server Core 설치 옵션을 사용하도록 선택하여 보안 위험을 줄이면서 관리 및 소프트웨어 업데이트 요구를 줄일 수 있습니다.

## 엔터프라이즈급 인쇄 관리

조직이 클수록, 네트워크 내의 프린터 수가 많아지며, IT 직원이 해당 프린터를 설치 및 관리하는 데 필요한 시간이 더 많이 들게 되므로 운영 비용이 증가합니다. Windows Server 2008에는 관리자가 단일 인터페이스에서 조직 내의 모든 프린터(원격 위치의 프린터 포함)를 관리하고 모니터링하고 문제를 해결할 수 있도록 하는 인쇄 관리 MMC 스냅인이 포함되어 있습니다.

인쇄 관리는 하나의 콘솔에서 네트워크에 있는 모든 프린터 및 인쇄 서버의 자세한 최신 상태 정보를 제공합니다. 또한 오류 상태에 있는 프린터를 쉽게 찾을 수 있도록 하며 프린터나 인쇄 서버에 대한 주의가 필요할 때 전자 메일로 알림을 보내거나 스크립트를 실행할 수도 있습니다. 웹 인터페이스를 제공하는 프린터 모델에서 인쇄 관리는 이러한 추가 데이터에 액세스할 수 있습니다. 따라서 프린터가 원격 위치에 있는 경우에도 토너 및 용지 수준과 같은 정보를 쉽게 관리할 수 있습니다.

로컬 인쇄 서버의 관리자는 프린터를 추가 및 제거할 수 있습니다. 인쇄 관리는 인쇄 서버와 동일한 서브넷에 있는 모든 프린터를 자동으로 검색하고, 적절한 프린터 드라이버를 설치하고, 큐를 설정하고, 프린터를 공유할 수 있습니다. 프린터 드라이버를 찾을 수 없는 경우가 아니면 추가 작업이 필요하지 않습니다.

인쇄 관리를 통해 Windows Server 2003 R2, Windows Vista 또는 Windows Server 2008 운영 체제가 실행되는 중앙의 컴퓨터에서 조직의 모든 프린터를 관리할 수 있습니다. Windows XP 클라이언트, x86 및 x64에서도 인쇄 관리를 사용할 수 있습니다.

### 프린터 관리

인쇄 관리를 사용하여 지점의 프린터를 비롯한 전체 엔터프라이즈의 모든 프린터를 관리할 수 있습니다. 특정 프린터의 실제 위치에 관계없이, 프린터 공유 방식을 제어하고 드라이버를 업데이트하고, 인쇄 큐를 제어하는 데 동일한 인터페이스가 사용됩니다. 또한 각 인쇄 서버의 각 프린터에 대한 개별 폴더로 이동해야 할 필요가 없습니다. 관리자는 인쇄 관리를 서버 구성 마법사 및 터미널 서비스와 함께 사용하여 지점의 로컬 인쇄 서버에서 네트워크 프린터를 자동으로 검색하고 설치할 수 있습니다. 이 기능은 지점 직원이 관리 업무를 교육 받지 못한 경우에 유용합니다.

### Active Directory에서 프린터 나열 및 제거

관리자는 Active Directory에서 프린터를 나열하여 보다 쉽게 프린터를 찾고 설치할 수 있습니다. 관리자는 인쇄 서버에 프린터를 설치한 후에 인쇄 관리를 사용하여 Active Directory에서 해당 프린터를 나열할 수 있습니다. 실제로 여러 대의 프린터를 동시에 나열할 수 있습니다. 관리자는 나열하거나 제거할 모든 프린터를 표시하도록 필터를 설정하여 모든 프린터를 동시에 쉽게 선택할 수 있습니다.

### 그룹 정책을 사용한 프린터 배포

인쇄 관리를 그룹 정책과 함께 사용하여 클라이언트 컴퓨터의 프린터 및 팩스 폴더에 프린터 연결을 자동으로 추가할 수 있습니다. 프린터 연결 설정은 Active Directory의 기존 GPO(그룹 정책 개체)에 자동으로 추가될 수 있습니다. 그룹 정책 처리가 클라이언트 컴퓨터에서 실행되면 프린터 연결 설정이 GPO와 연결된 사용자 또는 컴퓨터에 적용됩니다. 이 방법으로 배포한 프린터는 연결된 인쇄 서버가 모니터링되고 있는 동안 인쇄 관리 트리의 배포된 프린터 개체에 표시됩니다.

이러한 프린터 설치 방법은 방이나 사무실의 모든 컴퓨터가 동일한 프린터에 액세스해야 하는 실험실, 강의실 또는 지점 설정에서 유용합니다. 컴퓨터 및 프린터가 기능, 작업 그룹 또는 부서별로 구분되는 대규모 조직에서도 유용할 수 있습니다. 사용자별 연결을 사용하여 프린터 연결을 설치한 경우 해당 사용자가 어떤 컴퓨터에 로그온했는지에 관계없이 이 프린터 연결에 액세스할 수 있습니다. 컴퓨터별 연결을 사용하여 설치한 프린터 연결은 프린터 및 팩스 폴더에 표시되며 해당 컴퓨터의 모든 사용자가 사용할 수 있습니다.

### 프린터 문제 해결

인쇄 관리는 원격 위치에 있는 프린터를 비롯한 각종 프린터 문제를 식별하고 해결하는 데 도움이 될 수 있는 여러 가지 기능을 제공합니다. 관리자는 미리 정의된 필터를 설정하여 준비 상태가 아니거나 인쇄 작업이 큐에 백업된 모든 프린터를 쉽게 찾을 수 있습니다. 제조업체에 관계없이, 많은 장치는 풍부한 상태 정보를 제공하므로 인쇄 관리를 통해 관리될 수 있습니다. 관리자는 조직 내의 프린터를 면밀히 모니터링하여 용지 또는 토너 부족과 같은 문제가 발생하기 전에 조치할 수 있습니다. 프린터에 주의가 요구될 때 관리자에게 경고하도록 전자 메일 메시지 알림을 설정할 수 있습니다. 이 기능은 조직의 여러 위치에 여러 대의 프린터가 있으며 여러 명의 담당자가 프린터를 관리할 때 특히 유용합니다. 프린터나 인쇄 서버를 사용할 수 없을 때 IT 직원에게 알리는 자동화 시스템을 사용하면 문제를 보다 빠르게 해결하여 프린터 및 인쇄 서버 문제로 인한 영향을 줄일 수 있습니다.

### 주요 이점

인쇄 관리는 클라이언트 컴퓨터에 프린터를 설치할 때와 프린터를 관리 및 모니터링할 때 인쇄 관리자의 작업 시간을 크게 줄여줍니다. 인쇄 관리를 그룹 정책과 함께 사용하면 개별 컴퓨터에서 프린터 연결을 설치 및 구성할 필요 없이, 클라이언트 컴퓨터의 프린터 및 팩스 폴더에 프린터 연결을 자동으로 추가할 수 있습니다. 이렇게 하면 같은 부서에 있는 사용자나 지점에서 근무하는 모든 사용자처럼 동일한 프린터에 액세스해야 하는 다수의 사용자를 위해 효과적이면서 빠르게 프린터를 추가할 수 있습니다.

## Windows 배포 서비스

WDS(Windows 배포 서비스)는 네트워크 기반 설치를 사용하여 컴퓨터에 Windows 운영 체제를 빠르게 배포하는 간단하고 안전한 방법을 제공하기 위해 Windows Server 2008에서 함께 작동하는 구성 요소 제품군입니다. WDS는 관리자가 각 컴퓨터에서 직접 작업하거나 CD 또는 DVD 미디어에서 Windows 구성 요소를 설치할 필요성을 없애줍니다. 여기에는 IT 직원 시간을 절약하는 새롭고 향상된 많은 기능이 포함되어 있습니다. WDS의 세 가지 구성 요소는 다음 세 범주로 구성됩니다.

* 서버 구성 요소 - 이 구성 요소에는 운영 체제를 로드 및 설치할 클라이언트를 네트워크 부팅시키기 위한 PXE(Pre-Boot Execution Environment) 서버 및 TFTP(Trivial File Transfer Protocol) 서버가 포함됩니다. 또한 부팅 이미지, 설치 이미지 그리고 네트워크 부팅에 특히 필요한 파일들이 들어 있는 공유 폴더와 이미지 리포지토리도 포함됩니다.
* 클라이언트 구성 요소 - 이 구성 요소는 Windows PE(Windows 사전 설치 환경) 내에서 실행되는 그래픽 사용자 인터페이스를 포함하며 서버 구성 요소와 통신하여 운영 체제 이미지를 선택하고 설치합니다.
* 관리 구성 요소 - 이 구성 요소는 서버, 운영 체제 이미지 및 클라이언트 컴퓨터 계정을 관리하는 데 사용되는 도구 집합입니다.

### Windows 배포 서비스의 향상된 기능

Windows 배포 서비스에는 모든 Windows 배포 서비스 기능을 편리하게 관리할 수 있는 Windows 배포 서비스 MMC 스냅인이 포함되어 있습니다. WDS에는 Windows Vista 및 Windows Server 2008를 쉽게 배포하도록 특수하게 디자인된 향상된 RIS 기능 모음이 제공됩니다. Windows 배포 서비스를 사용하여 IT 직원은 다음을 수행할 수 있습니다.

* Sysprep.exe 및 Windows 배포 서비스 스냅인을 사용하여 사용자 지정 이미지 생성에 사용할 수 있는 "캡처 이미지"를 만듭니다.
* Windows 배포 서비스 캡처 마법사를 사용하여 Sysprep.exe로 준비한 이미지를 만들고 추가합니다.
* Windows 배포 서비스 스냅인을 사용하여 Windows 이미지에 무인 설치 파일을 연결합니다.
* 하나 이상의 언어 팩을 하나의 이미지에 연결하여 조직에서 지원하는 각 언어에 대해 고유한 이미지를 만들 필요가 없도록 합니다.
* Windows 배포 서비스 스냅인을 사용하여 PXE 부팅을 지원하지 않는 컴퓨터에서 사용할 "검색 이미지"를 만듭니다.

참고: 차기 버전의 BDD(Business Desktop Deployment) 2007은 Microsoft 배포입니다. 이 제품은 데스크톱 및 서버 배포를 자동화하기 위한 권장 프로세스 및 도구 집합입니다. Microsoft 배포는 대규모 배포 프로젝트와 관련된 모든 조직 역할에 대한 자세한 지침과 지원 작업을 제공합니다. Microsoft 배포는 일반적인 배포 콘솔에 데스크톱 및 서버를 배포하는 데 필요한 도구 및 프로세스와 지침 모음을 통합합니다. 이 4세대 배포 지원 프로그램은 최근에 출시된 Microsoft 배포 기술과 통합되어 이미지 생성 및 자동 설치를 한 번에 수행할 수 있도록 합니다. Microsoft 배포의 다양한 도구와 종단 간 지침은 배포 시간을 단축하고, 데스크톱 및 서버 이미지를 표준화하고, 서비스 중단을 제한하고, 배포 후 지원 센터 비용을 절감하고, 보안 및 지속적인 구성 관리를 향상시킵니다. 추가 정보는 다음 사이트에서 확인할 수 있습니다. <http://www.microsoft.com/downloads/details.aspx?familyid=3bd8561f-77ac-4400-a0c1-fe871c461a89&displaylang=en&tm>

## 새 Active Directory 도메인 서비스 설치 마법사

Windows Server 2008에는 설치 간소화를 위한 새로운 설치 마법사가 포함되어 있습니다. 새 마법사에서는 TCP/IP 및 DNS(Domain Name System) 클라이언트 설정과 같은 로컬 네트워크 설정에 대한 모든 오류 검사가 함께 그룹화됩니다. NetBIOS 이름 및 익명 액세스 권한과 같이 새 도메인 생성에만 관련된 기능은 새 도메인 선택 항목 가까이에 있습니다.

Active Directory 도메인 서비스 설치 마법사는 "/adv" 스위치를 지정하여 dcpromo를 실행하는 기능(예: dcpromo /adv)의 대체 기능인 고급 모드를 사용할 수 있도록 마법사의 시작 페이지에 새 옵션을 제공합니다 고급 모드는 보다 수준 높은 구성을 가능하게 하며, 숙련된 사용자가 다음과 같은 작업을 보다 손쉽게 제어할 수 있도록 하는 추가 옵션을 제공합니다.

* 새 도메인 트리 만들기
* 같은 도메인에 속하는 기존 도메인 컨트롤러의 백업 미디어를 사용하여 초기 복제에 따른 네트워크 트래픽 줄이기
* 설치를 위한 원본 도메인 컨트롤러 선택
* RODC(읽기 전용 도메인 컨트롤러)에 대한 암호 복제 정책 정의

이러한 변경 외에, Active Directory 도메인 서비스 설치 마법사에는 다음 표에 나와 있는 새로운 대화 상자 페이지가 있습니다.

표 14: AD DS 설치 마법사 옵션

|  |  |
| --- | --- |
| **새 마법사 페이지** | **설명** |
| 추가 옵션 | 도메인 컨트롤러 설치 중에 도메인 컨트롤러를 DNS 서버, 글로벌 카탈로그 서버 또는 RODC로도 구성하도록 지정합니다. |
| 사이트 선택 | 도메인 컨트롤러가 설치될 사이트를 지정합니다. |
| 기능 수준 설정 | 새 도메인 또는 포리스트의 설치 중에 도메인 및 포리스트 기능 수준을 설정합니다. |
| 암호 복제 정책 | RODC에 캐시가 허용되거나 거부될 계정 암호를 지정합니다. 이 페이지는 고급 모드 설치 사용 확인란을 선택한 경우에만 표시됩니다. |
| DNS 위임 만들기 | 도메인 컨트롤러 설치 유형(배포 구성 선택 페이지에 지정) 및 DNS 환경에 따라 DNS 위임을 만들기 위한 기본 옵션을 제공합니다. |

그 밖의 여러 향상된 기능이 AD DS 설치 중에 오류가 발생할 가능성을 줄여줍니다. 예를 들어 추가 도메인 컨트롤러를 설치할 때 사용자는 도메인 이름을 직접 입력할 필요 없이 도메인 트리 보기에서 도메인 이름을 선택할 수 있습니다.

Windows Server 2008에서는 AD DS의 무인 설치를 실행하기 위한 새로운 옵션을 사용할 수 있습니다. Windows Server 2003 운영 체제의 무인 설치와 달리, Windows Server 2008의 무인 설치에서는 도메인 컨트롤러 다시 시작을 묻는 메시지와 같은 사용자 인터페이스 메시지에 응답할 필요가 없습니다. 이러한 기능은 Windows Server 2008의 새로운 설치 옵션으로, 대화형 Active Directory 도메인 서비스 설치 마법사와 같이 사용자 인터페이스 옵션을 제공하지 않는 Windows Server 2008 Server Core 설치에 AD DS를 설치하는 데 필요합니다.

## 다시 시작 가능 AD DS (Active Directory 도메인 서비스)

관리자는 MMC(Microsoft Management Console) 스냅인이나 명령줄을 사용하여 Windows Server 2008에서 AD DS(Active Directory 도메인 서비스)를 중지한 후 다시 시작할 수 있습니다. 다시 시작 가능 AD DS는 서버에 업데이트를 적용하는 것과 같은 특정 작업 수행에 필요한 시간을 단축합니다. 관리자는 도메인 컨트롤러를 다시 시작할 필요 없이 Active Directory 데이터베이스의 오프라인 조각 모음과 같은 작업을 수행하기 위해 AD DS를 중지할 수도 있습니다. 서버에서 실행되고 있으며 작동을 위해 AD DS에 의존하지 않는 DHCP(Dynamic Host Configuration Protocol)와 같은 기타 서비스는 AD DS가 중지된 동안 클라이언트 요청을 충족하기 위해 그대로 사용할 수 있습니다.

AD DS를 중지하는 것은 디렉터리 서비스 복원 모드로 로그온하는 것과 비슷하지만 다시 시작 가능 AD DS는 Windows Server 2008이 실행되는 도메인 컨트롤러의 고유한 상태를 제공합니다. 이 상태는 AD DS 중지됨으로 알려져 있습니다. Windows Server 2008에서 실행되는 도메인 컨트롤러에 사용할 수 있는 세 가지 상태는 다음과 같습니다.

* AD DS 시작됨 - 이 상태에서 AD DS는 시작되어 있습니다. 클라이언트 및 서버에서 실행되는 기타 서비스의 경우 이 상태에서 실행되는 Windows Server 2008 도메인 컨트롤러가 Windows 2000 Server 또는 Windows Server 2003에서 실행되는 도메인 컨트롤러와 같습니다.
* AD DS 중지됨 - 이 상태에서 AD DS는 중지되어 있습니다. 이 모드는 고유하지만 서버는 디렉터리 서비스 복원 모드의 도메인 컨트롤러와 도메인 가입 구성원 서버 모두의 부분적인 특성을 갖습니다.
* 디렉터리 서비스 복원 모드와 마찬가지로, Active Directory 데이터베이스(Ntds.dit)는 오프라인 상태입니다. 또한 로그온을 위해 다른 도메인 컨트롤러에 연결할 수 없을 때 디렉터리 서비스 복원 모드 암호를 사용하여 로컬로 로그온할 수 있습니다.
* 구성원 서버처럼 서버는 도메인에 가입됩니다. 사용자는 도메인 로그온을 위해 다른 도메인 컨트롤러를 사용하여 대화형으로 또는 네트워크를 통해 로그온할 수 있습니다. 그러나 도메인 컨트롤러는 이 상태에서 로그온 요청을 서비스하거나 다른 도메인 컨트롤러와 복제할 수 없으므로 장기간 이 상태를 유지하면 안 됩니다. 클라이언트가 DC와의 연결을 갱신할 때 원본 DC가 백업 및 실행 중이면 해당 연결로 되돌아갑니다.
* 디렉터리 서비스 복원 모드 - 이 모드 또는 상태는 Windows Server 2003과 동일합니다.

다음 순서도는 Windows Server 2008이 실행되는 도메인 컨트롤러가 이러한 세 가지 가능한 상태 간을 전환하는 방식을 보여 줍니다.

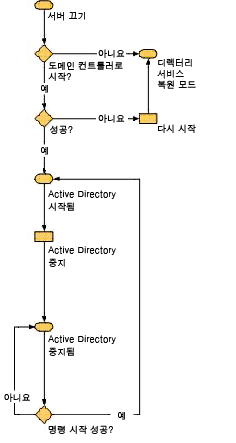


그림 11: Windows Server 2008이 실행되는 도메인 컨트롤러의 세 가지 상태

Windows Server 2008에 포함된 Active Directory 도메인 서비스의 서비스는 RODC와 같은 새 설치 옵션, 유용한 마법사 및 향상된 관리 인터페이스와 도구를 사용하여 원격 위치에 있는 도메인 컨트롤러 및 도메인 서비스의 원격 배포와 지속적인 관리를 간소화합니다.

## Active Directory 도메인 서비스 스냅숏 뷰어

Windows Server 2008에는 AD DS 스냅숏을 만드는 데 사용할 수 있는 향상된 ntdsutil 명령이 제공됩니다. 이러한 스냅숏은 만들어질 때 Active Directory의 완전한 상태를 캡처합니다. 도메인 컨트롤러를 디렉터리 서비스 복원 모드로 시작하지 않고 기존 AD DS 스냅숏을 Active Directory의 병렬 읽기 전용 인스턴스로 탑재할 수 있습니다. AD DS 스냅숏 탑재는 삭제되었거나 수정된 AD DS 개체를 복구하는 데 사용할 수 있습니다.

Windows Server 2008의 스냅숏 뷰어를 통해 관리자는 시간에 따라 작성된 AD DS 스냅숏의 개체 정보를 노출하여 실수로 삭제된 개체를 파악할 수 있습니다. 관리자는 여러 다른 스냅숏에 나타나는 개체의 다양한 상태를 비교하여 삭제된 개체를 복원하는 데 사용할 AD DS 스냅숏을 보다 잘 결정할 수 있습니다.

## 요약

Windows Server 2008에서는 엔터프라이즈에서 사용되는 단일 및 여러 서버의 관리 환경을 향상시키고 Windows 운영 체제의 배포를 간소화하는 여러 도구, 기술 및 설치 옵션을 사용할 수 있습니다.

서버 관리자는 IT 전문가에게 서버 역할, 역할 서비스 및 기능을 추가, 제거 및 구성하기 위한 포괄적인 환경을 제공하는 통합된 Microsoft Management Console입니다. 또한 서버 관리자는 서버 역할을 기반으로 하는 핵심 관리 작업을 노출하고 고급 관리 도구에 액세스할 수 있도록 하여 지속적인 서버 관리, 모니터링 및 작업에 대한 포털로도 작동합니다.

여러 대의 서버 관리는 IIS 및 Active Directory와 같이 서버 역할에 대한 관리 작업을 자동화하기 위해 특수 설계된 새로운 명령줄 셸 및 스크립팅 언어로 구성되는 Windows PowerShell을 사용하여 자동화할 수 있습니다.

관리자는 Windows Server 2008의 Server Core 설치 옵션을 사용하여 서버에 필요한 기능만 설치하여 지속적인 유지 관리 요구를 줄이고 관리를 간소화할 수 있습니다.

프린터 설치, 공유 및 관리를 위해 인쇄 관리에서 제공하는 자동화 옵션 및 중앙 집중식 제어 인터페이스는 IT 직원이 프린터를 배포하는 데 필요한 시간을 단축하고 프린터, 인쇄 서버 및 인쇄 작업의 관리를 단순화합니다.

# 8장: 고가용성

## 소개

가용성은 응용 프로그램, 서비스 또는 시스템이 제공하는 서비스 수준을 나타냅니다. 고가용성 시스템은 작동 중단을 최소화하는 적절한 수준의 서비스를 제공합니다. 예기치 않은 과도한 작동 중단은 조직에 심각한 영향을 미칠 수 있습니다. 중대한 시스템, 서비스 또는 응용 프로그램의 손실은 직원 생산성, 매출 및 파트너와 고객의 신뢰를 저해할 수 있습니다. 중대한 응용 프로그램 및 서비스의 고가용성을 유지하는 일은 IT 부서에서 최우선적으로 고려되는 측면이며, 고가용성은 Windows Server 2008의 향상된 많은 기능 중에서 핵심이 됩니다.

이 장에서는 관리를 간소화하면서 고가용성을 유지하는 데 도움이 되는 Windows Server 2008의 몇 가지 핵심 기능을 소개합니다.

* 장애 조치 클러스터링
  + 하드웨어 장애가 업무용 응용 프로그램 및 서비스의 가용성에 영향을 미치지 않도록 합니다.
  + 장애 조치 클러스터를 보다 쉽게 구현하고 이를 업무에 활용하도록 지원하는 새 기능을 제공합니다.
* 서버 관리자 콘솔
  + 사용자에게 클러스터된 서버를 만들고 관리하고 사용할 수 있는 간단한 인터페이스를 제공하여 복잡성을 줄입니다.
  + 배포 횟수 및 구성 문제 감소에 따라 지원 비용 및 구현 시간을 줄입니다.
  + 고객 환경에 맞게 기술이 조정될 수 있으므로 지리적으로 분산된 환경에서도 구현 가능하도록 기능을 향상시킵니다.
* 네트워크 부하 분산
  + 네트워크 부하 분산은 네트워크 상 클라이언트/서버 응용 프로그램의 부하를 여러 클러스터 서버에 분산합니다.
  + Windows Server 2008의 NLB에서는 네트워킹, 보안 및 관리 기능이 향상되어 가용성과 안정성이 강화되었습니다.
* 향상된 백업
  + 백업 속도 개선
  + 복원 간소화
  + 일정 기능 개선

## 장애 조치 클러스터링

장애 조치 클러스터(이전의 서버 클러스터)는 함께 작동하여 응용 프로그램과 서비스의 가용성을 향상시키는 독립 컴퓨터의 그룹입니다. 클러스터된 서버(노드라고 함)는 물리적 케이블과 소프트웨어로 연결됩니다. 클러스터 노드 중 하나가 실패하면 장애 조치라는 프로세스를 통해 클러스터의 다른 노드가 실패한 노드의 작업을 인계 받으므로 사용자는 최소의 서비스 중단만 경험하게 됩니다. 장애 조치 클러스터는 업무용 서비스 및 응용 프로그램에 대한 고가용성을 제공해야 하는 IT 전문가가 주로 사용합니다. Windows Server 2008의 장애 조치 클러스터 기능 향상을 통해 클러스터를 단순화하여 더욱 안전한 클러스터를 만들고 클러스터 안정성을 개선할 수 있게 됩니다.

### 장애 조치 클러스터링의 새 기능

#### 새 유효성 검사 마법사

고가용성의 이점을 충분히 실현하려면 서버, 네트워크 및 저장소를 비롯한 전체 구성을 주의해서 설정해야 합니다. Windows Server 2008에는 시스템, 저장소 및 네트워크 구성이 클러스터에 적합한지 확인할 수 있는 새로운 유효성 검사 마법사가 제공되므로 장애 조치 클러스터의 설치 및 구성이 간편해졌습니다. 새 유효성 검사 마법사에서 수행되는 일부 테스트에는 다음이 포함됩니다.

* 노드 테스트 - 서버에서 동일한 운영 체제 버전이 실행되고 있는지와 동일한 소프트웨어 업데이트가 있는지 확인합니다.
* 네트워크 테스트 - 계획된 클러스터 네트워크가 특정 요구(예: 네트워크 중복성을 위해 적어도 2개 이상의 별도 서브넷을 갖는지 여부)를 충족하는지 확인합니다.
* 저장소 테스트 - 모든 클러스터 노드가 모든 공유 디스크에 액세스할 수 있고 특정 요구를 만족하도록 저장소가 올바르게 구성되어 있는지 분석합니다.

### 대용량을 위한 향상된 확장성

Windows Server 2008에서는 전역 고유 식별자 또는 클러스터 저장소의 GTP(GUID 파티션 테이블) 디스크를 지원합니다. GPT 디스크는 MBR(마스터 부트 레코드) 디스크와 달리, 2TB 이상의 파티션을 포함할 수 있으며 중복성이 기본으로 제공됩니다. GPT는 디스크당 최대 128개의 파티션을 허용하고, 최대 18TB의 볼륨을 지원하고, 중복성을 위해 기본 및 백업 파티션 테이블을 허용하고, 고유한 디스크 및 파티션 ID를 지원하므로 MBR(마스터 부트 레코드) 파티션보다 더 많은 이점을 제공합니다.

### 장애 조치 클러스터의 향상된 기능

Windows Server 2008의 장애 조치 클러스터는 클러스터 배포, 관리 및 작동을 다음과 같이 향상시킵니다.

* 클러스터 설치 및 마이그레이션 향상 - 클러스터 설치 마법사는 아주 간단하므로 클러스터 설치를 한 단계 만에 완료할 수 있습니다. 이제 클러스터 설치를 완전히 스크립트로 작성할 수 있으므로 배포를 자동화할 수 있습니다. 기존 클러스터의 마이그레이션이 간단해졌습니다. Windows Server 2003이 실행되는 클러스터에서 리소스 그룹 설정을 캡처한 후 Windows Server 2008이 실행되는 클러스터에 적용할 수 있습니다.
* 관리 인터페이스 간소화 - 마법사 및 인터페이스 기능이 향상되어 관리 작업이 간단해졌으므로 관리자는 클러스터가 아닌 응용 프로그램 관리에 주력할 수 있습니다.
* 안정성 및 보안 향상으로 가용성 증가 - 클러스터가 저장소와 통신하는 방식이 향상되어 쿼럼 리소스가 더 이상 단일 장애 지점이 되지 않습니다.
* 네트워킹 및 보안성 향상 - IPv6의 통합, 레거시 NetBIOS 종속성 없이 DNS 사용, 조직에서 안정성을 높이고 안전한 배포를 이루도록 도와 주는 기타 향상된 네트워킹 기능을 통해 네트워크 성능 및 보안이 향상되었습니다.

#### 서버 관리자 콘솔

클러스터 관리의 간소화를 위해 관리자가 클러스터가 아닌 응용 프로그램 및 데이터 관리에 주력하도록 관리 인터페이스가 향상되었습니다. 새로운 인터페이스는 작업을 기반으로 하고 보다 직관적이며, 이전의 복잡했던 작업을 안내하는 마법사를 통해 지원됩니다. Windows Server 2008의 장애 조치 클러스터를 사용하여 다음 관리 및 운용 작업이 간소화되었습니다.

* 향상된 인터페이스 - 사용자 인터페이스는 작업을 기반으로 하며, 이전의 복잡했던 작업을 안내하는 마법사를 통해 지원됩니다. 이제 프린터 서버 역할과 같은 클러스터 역할의 설치 작업을 간단한 몇 단계로 처리할 수 있습니다. 새로운 클러스터 관리 도구는 구성 옵션을 직관적인 작업 기반 메뉴 옵션으로 표시하는 클러스터된 역할의 전체 보기를 제공합니다.
* 구성에 클러스터된 리소스를 빠르게 추가 - 공유 폴더의 가용성을 높이는 것과 같은 작업은 향상된 클러스터 관리 인터페이스로 보다 쉽게 수행할 수 있습니다.
* 클러스터 문제 해결 - 관리자는 클러스터 로그를 사용하지 않고도 Windows용 이벤트 추적을 사용하여 클러스터에서 발생하는 이벤트 시퀀스에 대한 정보를 쉽게 수집하고 관리하고 보고할 수 있습니다.
* 볼륨 섀도 복사본 서비스를 사용하여 백업 캡처 - 볼륨 섀도 복사본 서비스와의 완전한 통합을 통해 클러스터 구성을 보다 쉽게 백업 및 구성할 수 있습니다.
* 클러스터의 공유 폴더가 표시되는 방법 제어 - 시스템은 표시되는 공유 저장소 및 공유 폴더를 지정합니다. 따라서 클러스터에 해당하므로 다른 노드로 장애 조치될 수 있는 공유 폴더와, 단일 노드의 로컬 폴더이므로 장애 조치를 수행할 수 없는 공유 폴더를 쉽게 구분할 수 있습니다.

또한 Windows Server 2008에서는 장애 조치 클러스터에 대한 명령줄 및 WMI(Windows Management Instrumentation) 옵션을 지원합니다.

### 향상된 안정성

Windows Server 2008의 장애 조치 클러스터를 통한 클러스터 인프라 향상으로 사용자 서비스 극대화 효과를 누릴 수 있습니다. 가장 중요한 변경 내용 중 하나는 시스템이 “쿼럼”을 유지 관리하는 방식입니다. 쿼럼은 활성 상태인 노드와 대기 상태인 노드를 결정하는 클러스터의 구성 데이터베이스로써, 노드 간 통신이 중단될 경우 한 노드만 응용 프로그램과 서비스를 계속 제공하도록 하는 데 사용됩니다. 클러스터 노드 간 통신이 끊어지면 분할 브레인(split-brain) 시나리오를 방지하기 위해 시도/응답(challenge/response) 프로토콜이 시작됩니다. 통신이 끊어지면 클러스터 리소스의 소유자가 해당 클러스터와 모든 리소스의 소유자가 되므로 분할 브레인 문제가 발생하지 않습니다. 소유자는 해당 리소스를 클라이언트에서 사용할 수 있도록 만듭니다. 쿼럼 디스크를 소유하는 노드가 제대로 작동하지 않을 경우 작동하는 나머지 노드 중 하나가 장치 소유권을 갖게 됩니다.

관리자는 장애 조치 클러스터의 향상된 기능을 활용하여 이전 버전의 Windows에서 제공되던 다음 두 클러스터 모델 중 하나로 클러스터를 구성할 수 있습니다.

* 쿼럼 디스크 모델: 단일 디스크가 분할된 클러스터 중 어느 부분이 계속 작동할지를 결정할 권한을 갖습니다.
* 주 노드 집합 모델: 클러스터는 주 노드가 정상 상태이고 통신이 가능한 동안만 작동됩니다.

Windows Server 2008을 사용하는 경우 두 모델의 새로운 "하이브리드" 구조가 기본 구성으로 사용됩니다. 이를 통해 두 모델의 이점을 함께 얻을 수 있습니다. 예를 들어 두 노드 클러스터를 사용하면 쿼럼 디스크에 장애가 발생할 경우에도 클러스터가 계속 실행됩니다. 관리자는 쿼럼을 복잡하게 직접 구성할 필요가 없으며 클러스터 설치 중 모든 작업이 자동으로 수행됩니다. 이러한 새 하이브리드 모델을 사용하면 각 노드에 쿼럼 리소스의 복제본이 있으므로 쿼럼 디스크에 장애가 발생해도 클러스터 장애로 연결되지 않습니다.

### 저장소 통합

Windows Server 2008 장애 조치 클러스터의 향상된 저장소 통합 기능은 이전 버전의 서버 클러스터보다 더 나은 기능 및 안정성을 제공합니다. 주요 향상 기능에는 다음이 포함됩니다.

* 디스크 리소스의 동적 추가 - 리소스가 온라인 상태일 때 리소스 종속성을 수정할 수 있으므로 관리자는 디스크가 사용될 응용 프로그램을 중단하지 않으면서 추가 디스크를 사용 가능하게 설정할 수 있습니다.
* 데이터 저장소를 통한 성능 및 안정성 향상 - Windows Server 2008에는 영구 예약을 사용하기 위한 향상된 메커니즘과 공유 디스크 관리를 위한 새 알고리즘이 제공됩니다. SAN을 중단할 수 있는 SCSI 버스 재설정을 더 이상 사용하지 않습니다. Windows Server 2008의 장애 조치 클러스터링을 사용하면 디스크가 항상 보호되므로 볼륨이 손상될 위험이 줄어듭니다. 또한 장애 조치 클러스터는 향상된 디스크 검색 및 복구 방법, 그리고 SAS(Serial Attached SCSI), iSCSI 및 파이버 채널의 세 가지 저장소 연결 유형을 지원합니다.
* 간편한 디스크 유지 관리 - 유지 관리 모드가 획기적으로 향상되어 관리자는 클러스터 중단을 최소화하면서 디스크를 보다 쉽게 검사, 수정, 백업 또는 복원하기 위한 도구를 실행할 수 있습니다.

### 네트워킹 및 보안

Windows Server 2008의 장애 조치 클러스터를 사용하면 이전 버전과 비교할 때 네트워크 성능과 보안이 향상됩니다. 이러한 향상을 통해 사용자는 다음을 할 수 있습니다.

* 장애 조치 클러스터와 완전하게 통합되는 IPv6 사용 - 장애 조치 클러스터는 노드 간 통신과 노드와 클라이언트 간 통신에서 IPv6을 사용할 수 있도록 완전하게 지원합니다.
* 레거시 NetBIOS 종속성 없이 DNS(Domain Name System) 사용 - 이 기능은 SMB(서버 메시지 블록) 트래픽의 전송을 간소화하므로 WINS(Windows Internet Name Service) 및 NetBIOS 이름 확인 브로드캐스트가 발생하지 않습니다.
* 기타 네트워킹 기능 향상을 통한 안정성 개선 - 관리자는 네트워크 이름 리소스 및 관련된 여러 IP 주소 간을 연결하여 이러한 IP 주소 중 하나라도 사용 가능할 경우 네트워크 이름을 사용할 수 있습니다. 또한 노드는 "하트비트"를 송수신하여 각 노드가 사용 가능한지 확인할 때 신뢰도가 떨어지는 UDP(User Datagram Protocol)가 아닌 보다 믿을 수 있는 TCP(Transmission Control Protocol)를 사용합니다.
* 보안이 향상되었습니다. 장애 조치 클러스터의 향상된 보안 기능에는 다음이 포함됩니다.
  + 새 보안 모델 - Windows Server 2008은 클러스터 서비스가 LocalSystem 기본 제공 계정의 컨텍스트에서 실행되는 향상된 보안 모델을 제공합니다. 이로 인해 보안이 강화되고 계정 암호 관리가 향상됩니다.
  + 감사 - 관리자는 감사를 사용하여 클러스터에 액세스한 대상과 액세스한 시기에 대한 정보를 파악할 수 있습니다.
  + 암호화 - Windows Server 2008에서 관리자는 노드 간 통신을 암호화할 수 있습니다.
* 여러 IP 서브넷의 노드 지원 - 클러스터의 노드는 유연성을 높이기 위해 더 이상 동일한 IP 서브넷에 있지 않아도 됩니다. 이 기능은 클러스터가 사이트 복구를 위해 지리적으로 멀리 떨어진 위치로 확장될 때 특히 유용합니다.

클러스터를 사용하여 고가용성 솔루션을 제공하는 관리자의 입장에서 볼 때, Windows Server 2008은 클러스터의 배포와 관리를 간소화하고 성능 및 안정성을 향상시킵니다

## 클러스터링과 Hyper-V

Windows Server 2008 장애 조치 클러스터링은 가상 컴퓨터가 작동 중단 중에 클러스터의 다른 노드로 마이그레이션할 수 있도록 하여 Hyper-V에 고가용성을 제공합니다. 클러스터링은 Hyper-V 역할 자체를 클러스터링하거나 Hyper-V에서 실행 중인 개별 가상 컴퓨터를 클러스터링하여 구현할 수 있습니다. 전자를 호스트 클러스터링이라 하고, 후자를 게스트 클러스터링이라 합니다.

Windows Server 2008 장애 조치 클러스터링을 사용하여 Hyper-V 역할의 가용성을 높일 경우, Hyper-V가 실행되는 두 대 이상의 서버에 장애 조치 클러스터링 역할이 추가되며 이 서버들은 지원되는 클러스터 구성에 구성됩니다. 이를 호스트 클러스터링이라 합니다. Windows Server 2008 장애 조치 클러스터링에서 반드시 필요한 요소는 클러스터 노드에 대한 공유 저장소입니다. 여기에는 iSCSI 또는 파이버 채널 SAN(저장소 영역 네트워크) 등이 포함될 수 있습니다. 모든 가상 컴퓨터는 공유 저장소 영역에 저장되며 Hyper-V 노드 중 하나가 실행 중인 가상 컴퓨터를 관리합니다. 예정된 작동 중단이 발생하면 장애 조치 클러스터링 서비스는 영향 받은 가상 컴퓨터를 다른 클러스터 노드로 이동할 수 있습니다. 예기치 못한 작동 중단이 발생하면 장애 조치 클러스터링 서비스는 작동되는 클러스터 노드에서 가상 컴퓨터를 자동으로 다시 시작합니다. 호스트 클러스터링은 전체 Hyper-V 플랫폼과 Hyper-V 서버에 호스팅된 모든 가상 컴퓨터에 고가용성을 제공하므로,

예기치 못한 작동 중단을 방지하는 데 도움이 될 수 있으며 Hyper-V 호스트 유지 관리 중에 가상 컴퓨터를 계속 사용하도록 할 수 있습니다. 또한 Hyper-V 관리자가 빠른 마이그레이션 기능을 사용하여 실행 중인 가상 컴퓨터를 가용 리소스가 있는 호스트로 마이그레이션할 수 있도록 하여 데이터 센터가 동적인 작업에 대처하도록 합니다.

Hyper-V에서 실행 중인 가상 컴퓨터는 기반 호스트 운영 체제가 아닌 경우에도 클러스터링이 가능합니다. Hyper-V는 가상 컴퓨터가 iSCSI를 사용하여 외부 저장소에 액세스할 수 있도록 합니다. 둘 이상의 가상 컴퓨터의 게스트 운영 체제가 클러스터 리소스가 보관된 외부 공유 저장소를 액세스할 수 있도록 구성할 수 있습니다. 게스트 운영 체제가 클러스터링을 지원할 경우 클러스터 리소스에 대한 고가용성을 제공하도록 구성될 수 있습니다.

Hyper-V 게스트 클러스터링을 사용하여 데이터베이스, 파일, 공유, 네트워크 인프라 및 응용 프로그램 서비스를 비롯한 다양한 리소스에 대해 고가용성을 제공할 수 있습니다. Hyper-V 게스트 클러스터링과 Windows Server 2008 네트워크 부하 분산(NLB) 서비스를 결합하여 여러 Hyper-V 호스트 서버간에 고가용성과 부하 분산 기능을 제공할 수 있습니다. 예를 들어 Hyper-V 가상 컴퓨터는 웹 서버 팜이나 터미널 서비스 팜을 호스팅하는 데 사용될 수 있습니다. NLB를 통해 트래픽을 균일하게 분산시켜 단일 VM이 요청으로 과부하되지 않고, 팜 내의 개별 VM이 클라이언트 액세스를 중단하지 않고 재부팅될 수 있고, VM 템플릿을 사용하여 팜의 새 서버를 쉽게 구축할 수 있습니다.

Windows Server 2008 클러스터링은 멀티 사이트 클러스터링의 구현 시 한계점을 해소했습니다. Windows Server 2003 클러스터의 요구 대기 시간(500ms 미만) 문제가 해결되었습니다. Windows Server 2008의 요구 대기 시간은 구성 가능합니다. Windows Server 2008에서는 서브넷 상에서도 클러스터링이 가능합니다. 이제 개별 사이트를 연결하기 위해 VLAN을 사용해야 할 필요가 없습니다. Windows Server 2008의 멀티 사이트 클러스터링은 주 사이트에서 지리적으로 떨어져 있는 복구 사이트에 데이터 센터 작업을 장애 조치할 수 있도록 합니다.

## 네트워크 부하 분산

NLB(네트워크 부하 분산)는 NLB 클러스터의 여러 서버에 네트워크상 클라이언트 및 서버 응용 프로그램의 부하를 분산하는 기능입니다. NLB는 부하가 증가함에 따라 다른 서버가 추가되도록 함으로써 확장성을 제공합니다. NLB는 사용자가 오작동 서버를 쉽게 대체할 수 있도록 함으로써 안정성을 제공합니다. NLB는 일련의 서버에 클라이언트 요청을 분산해야 하는 조직에 권장됩니다. 이 기능은 작업이 증가할 때 다른 서버를 추가하여 IIS(인터넷 정보 서비스)에서 실행되는 웹 기반 응용 프로그램과 같은 상태 비저장 응용 프로그램이 확장될 수 있도록 하는 데 특히 유용합니다.

Windows Server 2008의 NLB는 그 기능이 다음과 같이 향상되었습니다.

* IPv6 지원 - NLB는 모든 통신에서 IPv6을 지원합니다.
* NDIS 6.0 지원 - NDIS 6.0은 NDIS(Network Driver Interface Specification) 라이브러리의 후속 버전입니다. NDIS는 커널 모드 네트워크 드라이버와 운영 체제 간에 표준 인터페이스를 지정합니다. NLB 드라이버는 새로운 NDIS 6.0 경량 필터 모델을 사용하도록 완전히 재구성되었습니다. NDIS 6.0은 이전 NDIS 버전과 호환됩니다. NDIS 6.0의 새 디자인은 향상된 드라이버 성능, 확장성 및 간소화된 NDIS 드라이버 모델을 제공합니다.
* WMI 기능 향상 - IPv6 및 여러 전용 IP 주소를 지원하기 위해 MicrosoftNLB 네임스페이스의 WMI 기능이 향상되었습니다.
* 향상된 DoS(서비스 거부) 공격 및 타이머 기아 보호 - NLB는 콜백 인터페이스를 사용하여 공격이 진행 중이거나 노드에 과부하가 걸렸을 때 이를 감지하고 응용 프로그램에 알릴 수 있습니다. Microsoft ISA Server 2006은 클러스터 노드에 과부하가 걸렸거나 노드가 공격 받는 경우 이 기능을 사용합니다.
* 노드당 여러 전용 IP 주소 지원 - NLB는 각 노드에 대해 여러 개의 전용 IP 주소를 정의하도록 완전히 지원합니다(이전에는 각 노드당 전용 IP 주소가 하나만 지원됨). 이를 통해 각 응용 프로그램이 자체의 전용 IP 주소를 요구하는 시나리오에서 동일한 NLB 클러스터에 여러 응용 프로그램을 호스팅할 수 있습니다. Microsoft NLB\_NodeSetting 클래스는 DedicatedIPAddresses 및 DedicatedNetMasks에 여러 개의 전용 IP 주소를 지정하여 이러한 주소를 지원합니다. 이 기능은 ISA Server 2006에서 클라이언트가 IPv4 및 IPv6 트래픽 둘 다로 구성되는 시나리오의 각 NLB 노드를 관리하기 위해 사용됩니다.

이러한 네트워크 부하 분산 기능은 새로운 업계 표준을 지원하고, 성능, 상호 운용성, 보안 및 유연성을 향상시키며, 응용 프로그램 배포 및 통합을 지원합니다.

## Windows 백업

백업은 서비스의 고가용성을 제공하도록 디자인된 Windows Server 2008의 또 다른 핵심 구성 요소입니다. 백업 기능은 해당 기능이 설치되어 있는 서버에 대한 백업 및 복구 솔루션을 제공합니다. 또한 이전 버전의 Windows 운영 체제에서 사용되던 백업 기능을 대신하는 새로운 백업 및 복구 기술을 제공합니다.

백업 기능을 사용하면 복잡한 기술을 사용하지 않고도 전체 서버를 효율적이면서 안정적으로 보호할 수 있습니다. 마법사는 자동 백업 일정을 설정하고, 필요한 경우 수동 백업을 만들고, 항목 또는 전체 볼륨을 복구할 수 있도록 도와줍니다. Windows Server 2008의 백업을 사용하여 전체 서버나 선택한 볼륨을 백업할 수 있습니다.

### 새 백업 기능

향상된 백업 기능에는 다음이 포함됩니다.

* + 새롭고 더 빨라진 백업 기술 - 백업은 볼륨 섀도 복사본 서비스 및 블록 수준의 백업 기술을 사용하여 운영 체제, 파일과 폴더 및 볼륨을 효율적으로 백업 및 복구합니다.
  + 백업 간소화 - 첫 번째 전체 백업을 만든 후에 자동으로 증분 백업이 실행되므로 마지막 백업을 수행한 이후에 저장한 데이터만 저장됩니다. 이전 버전의 백업과 달리, 관리자는 전체 및 증분 백업을 수동으로 예약할 필요가 없습니다.
  + 복원 간소화 - 백업을 선택한 후 해당 백업에서 복원할 항목을 선택하여 항목을 복원할 수 있습니다. 개별 파일 또는 전체 폴더를 복구할 수 있습니다. 이전에는 증분 백업에 항목을 저장한 경우 여러 가지 백업에서 수동으로 복원해야 했습니다. 이제 사용자는 복원하려는 항목의 백업 날짜를 선택하기만 하면 됩니다.
  + 운영 체제 복구 간소화 - 새 Windows 복구 도구를 사용하여 운영 체제를 보다 쉽게 복구할 수 있습니다. 사용자는 같은 서버로 복구할 수 있으며 하드웨어가 작동하지 않는 경우 운영 체제가 없는 새 서버로 복구할 수 있습니다.
  + DVD 미디어 지원 - 사용자는 DVD에 직접 볼륨을 수동 백업할 수 있습니다. 또한 공유 폴더 및 하드 디스크의 수동 백업도 여전히 지원됩니다. 예약된 백업은 하드 디스크에 저장됩니다.
  + 향상된 일정 - 백업에는 IT 직원에게 일별 백업을 만드는 과정을 안내하는 마법사가 포함되어 있습니다. 시스템 볼륨은 자동으로 예약된 모든 백업에 포함됩니다.

Windows Server 2008은 조직의 데이터와 네트워크에 있는 서버의 운영 체제를 모두 보호하는 고가용성 솔루션을 구축하는 데 필요한 백업 및 복구 솔루션을 제공합니다. 또한 데이터 복구를 가속화하면서 업무용 데이터가 적절히 백업되는지 확인할 필요를 없애줍니다.

## Windows 안정성 및 성능 모니터

Windows Server 2008에는 IT 전문가에게 시스템 성능 및 안정성을 쉽게 모니터링하고 평가하기 위한 도구를 제공하는 Windows 안정성 및 성능 모니터가 포함되어 있습니다. 참고: 일부 Windows Sever 2008 평가판에서는 이 기능을 “Windows 성능 진단 콘솔”로 지칭했습니다. Windows 안정성 및 성능 모니터는 성능 로그 및 경고, 서버 성능 관리자 및 시스템 모니터를 비롯하여 이전에 제공되던 일부 독립 실행형 도구의 기능을 결합한 MMC 스냅인입니다. 이 스냅인은 성능 데이터 수집 및 이벤트 추적 세션을 사용자 지정하기 위한 편리한 그래픽 인터페이스를 제공합니다. 아울러 시스템 변경 내용을 추적하고 이러한 변경 내용을 시스템 안정성의 변화와 비교하여 그 상관 관계를 그래픽으로 보여 주는 또 다른 MMC 스냅인인 안정성 모니터가 포함되어 있습니다.

Windows 안정성 및 성능 모니터는 IT 전문가와 네트워크 관리자에게 네트워크를 효과적으로 관리하는 데 필요한 성능 정보를 제공하도록 디자인된 도구입니다. 리소스 보기에서 실시간 상태를 보려면 콘솔이 Administrators 그룹의 구성원으로 실행되어야 합니다. 데이터 수집기 집합을 만들거나 로그를 구성하거나 보고서를 보려면 콘솔이 Administrators 그룹 또는 Performance Log Users 그룹의 구성원으로 실행되어야 합니다.

### 새 모니터링 기능

다음은 Windows Server 2008에 새로 도입된 Windows 안정성 및 성능 모니터의 핵심 기능입니다.

* 데이터 수집기 집합
* 로그 생성을 위한 마법사 및 템플릿
* 리소스 보기
* 안정성 모니터
* 일정을 포함한 모든 데이터 수집에 대한 통합된 속성 구성
* 사용자에게 친숙한 진단 보고서

#### 데이터 수집기 집합

데이터 수집기 집합은 데이터 수집기를 다양한 성능 모니터링 시나리오에서 사용하기 위해 재사용 가능한 요소로 그룹화하는 Windows 안정성 및 성능 모니터의 중요한 새 기능입니다. 여러 서버를 관리하는 관리자는 이 기능을 사용할 경우 데이터 수집기를 한 번 정의하고 모니터링할 정보를 지정한 후 여러 서버에서 사용할 수 있으므로 시간을 절약할 수 있습니다. 데이터 수집기 그룹을 데이터 수집기 집합으로 저장하면 단일 속성 변경을 통해 일정과 같은 작업을 전체 집합에 적용할 수 있습니다. Windows 안정성 및 성능 모니터에는 시스템 관리자가 서버 역할 또는 모니터링 시나리오와 관련된 성능 데이터의 수집을 바로 시작할 수 있도록 도와주는 기본 데이터 수집기 집합 템플릿도 포함되어 있습니다.

#### 로그 생성을 위한 마법사 및 템플릿

이제 로그 파일에 카운터를 추가하고 시작, 중지 및 기간을 예약하는 작업을 간소화된 마법사 인터페이스를 통해 수행할 수 있습니다. 시스템 관리자는 이 구성을 템플릿으로 저장하여 모든 컴퓨터에서 구성 단계를 진행할 필요 없이 나머지 컴퓨터에서 동일한 로그를 수집할 수 있습니다. 이제 성능 로그 및 경고 기능은 Windows 안정성 및 성능 모니터에 통합되었으므로 데이터 수집기 집합에서 사용할 수 있습니다.

#### 리소스 보기

새로운 리소스 보기 화면이 Windows 안정성 및 성능 모니터의 홈 페이지로 표시됩니다. 이 보기는 CPU, 디스크, 네트워크 및 메모리 사용량의 그래픽 개요를 실시간으로 제공합니다. 시스템 관리자는 이러한 모니터링되는 각 요소를 확장하여 어떤 프로세스에서 어떤 리소스가 사용되고 있는지 확인할 수 있습니다. 이전 버전의 Windows에서는 이러한 실시간 프로세스별 데이터를 작업 관리자 내에서만 사용할 수 있었습니다.

#### 안정성 모니터

안정성 모니터는 예기치 않은 문제로 인해 시스템의 안정성이 저하되었는지 여부를 반영하는 시스템 안정성 지수를 계산합니다. 시간별 안정성 지수 그래프에서 문제가 발생하기 시작한 시점을 빠르게 확인할 수 있습니다. 시스템 안정성 보고서는 문제의 근본 원인을 해결하는 데 도움이 되는 세부 정보를 제공합니다. 응용 프로그램 설치 또는 제거, 운영 체제 업데이트, 드라이버 수정 등의 시스템 변경 작업 중에 오류(응용 프로그램 오류, 하드웨어 오류 또는 운영 체제 중지)가 발생할 경우 시스템 변경 내용을 검토하여 문제 해결 전략을 빠르게 개발하고 시간 및 리소스를 절약할 수 있습니다.

#### 데이터 수집에 대한 통합된 속성 구성

일회성 데이터 수집기 집합을 만들지 또는 지속적으로 작업을 로깅하기 위한 데이터 수집기 집합을 만들지에 관계없이, 생성, 수정 및 예약 인터페이스는 동일합니다. 사용 중인 데이터 수집기 집합이 앞으로도 성능 모니터링에 유용하다고 판단될 경우 다시 만들 필요가 없으며, 다시 구성하거나 템플릿으로 저장할 수 있습니다. 이와 같이 관련 프로세스가 단순하므로 성능 정보에 대한 보다 효과적인 모니터링을 수행하면서 관리 시간을 단축할 수 있습니다.

#### 사용자에게 친숙한 진단 보고서

Windows Server 2003의 서버 성능 관리자에 익숙한 사용자는 이제 Windows Server 2008의 Windows 안정성 및 성능 모니터에서 동일한 종류의 진단 보고서를 찾을 수 있습니다. 보고서 생성에 필요한 시간도 향상되었습니다. 데이터 수집기 집합을 사용하여 수집한 데이터에서 보고서를 작성할 수 있으므로, 시스템 관리자는 서버 변경이 성능에 미친 영향을 평가하거나 보고서의 권장 결과를 검토할 수 있습니다.

## 정책 기반 서비스 품질

네트워크 관리자는 Windows Server 2008 및 Windows Vista의 QoS(서비스 품질) 정책을 사용하여 지정된 클라이언트와 서버 사이 또는 응용 프로그램 서버 사이에서 트래픽 우선 순위를 지정할 수 있습니다. 우선 순위 설정은 특정 응용 프로그램 이름, 특정 원본 및 대상 IP 주소, 특정 원본 및 대상 TCP 또는 UDP 포트를 대상으로 지정될 수 있습니다. QoS 정책 설정은 Active Directory 내 사용자 또는 컴퓨터 구성 그룹 정책 설정의 일부로 구성됩니다.

대역폭 사용을 관리하기 위해 관리자는 아웃바운드 트래픽의 스로틀 속도로 QoS 정책을 구성할 수 있습니다. 스로틀 기능을 사용함으로써, QoS 정책은 총 아웃바운드 네트워크 트래픽을 지정된 속도로 제한할 수 있습니다. 우선 순위 전달을 지정하기 위해 트래픽은 DSCP(Differentiated Services Code Point) 값으로 표시됩니다. 네트워크 인프라의 라우터 또는 무선 액세스 지점은 네트워크 구성 요소가 QoS 사용 가능한 경우 DSCP 표시 패킷을 차등 전송하기 위해 다른 큐에 배치할 수 있습니다. DSCP 표시와 스로틀 기능을 함께 사용하여 트래픽을 효과적으로 관리할 수 있습니다. 스로틀 기능과 우선 순위 표시는 모두 네트워크 계층에서 설정하므로, 응용 프로그램 자체는 수정하지 않아도 됩니다.

예를 들어 관리자는 재무 부서 직원의 경우 재무 응용 프로그램을 호스팅하는 서버로 이동하는 트래픽에 우선 순위를 두도록 QoS 정책 설정을 구성하여 사용량이 최고일 때도 그룹의 통신이 원활하게 진행되도록 합니다.

## 요약

Windows Server 2008의 장애 조치 클러스터링은 중요한 응용 프로그램 및 서비스를 제공해야 하는 조직을 위한 편리한 솔루션입니다. 새로운 구성 기능은 고가용성 장애 조치 클러스터 솔루션을 보다 쉽게 디자인하고 배포하도록 하며, 새로운 관리 인터페이스는 장애 조치 클러스터 관리를 위한 간단한 통합 인터페이스를 제공하여 복잡성과 비용을 줄입니다.

네트워크 부하 분산은 클러스터에 포함되어 있는 여러 서버에 클라이언트 트래픽을 분산하여 확장성과 가용성을 향상시킵니다. Windows Server 2008에는 클러스터 관리를 간소화하고, 조직이 클러스터 솔루션을 통해 업무용 응용 프로그램 및 서비스를 효과적으로 전달하도록 지원하는 다양한 새 기능이 포함되어 있습니다. 향상된 기능에는 IPv6 및 NDIS 6.0에 대한 지원과 ISA Server 2006의 개선된 기능이 포함됩니다.

관리자는 Windows Server 2008의 향상된 백업 및 복구 기능을 사용하여 중요한 데이터뿐만 아니라 서버 운영 체제 및 구성을 안전하고 효율적으로 보호할 수 있습니다. 마법사는 백업 및 복구를 위한 편리한 도구를 제공하여 관리 시간을 단축하고 비용을 절감합니다.

네트워크 관리자는 Windows Server 2008의 서비스 품질 정책 기능을 사용하여 지정한 클라이언트와 서버 사이 또는 응용 프로그램 서버 사이에서 트래픽의 우선 순위를 지정하여 업무용 응용 프로그램 및 서비스가 사용 가능한 대역폭 리소스를 할당 받는 순서를 지정할 수 있습니다.

# 9장: 요약

Microsoft Windows Server 2008은 차세대 Windows Server입니다. Windows Server 2008은 업무 작업을 수행하기 위한 견고한 토대를 제공하여 IT 전문가가 서버 및 네트워크 인프라를 보다 쉽게 제어하도록 합니다. 또한 운영 체제를 강화하고 네트워크 환경을 보호하여 보안을 향상시킵니다. 아울러 IT 시스템의 배포 및 유지 관리를 가속화하고 서버 및 응용 프로그램의 보다 쉬운 통합 및 가상화를 가능하게 하며 직관적인 관리 도구를 제공하여 IT 전문가에게 유연한 작업 환경을 제공합니다. 또한 Windows Server 2008은 조직에서 효율적이며 효과적으로 풍부한 웹 기반 환경을 제공할 수 있도록 하는 강력한 웹 응용 프로그램 및 서비스 플랫폼입니다. Windows Server 2008은 조직의 서버 및 네트워크 인프라에 최상의 토대를 제공합니다.

1. RADIUS는 IETF(Internet Engineering Task Force) 표준입니다. [↑](#footnote-ref-2)