**고객 호스팅 볼륨 정품 인증 가이드**

**Windows 7 및 Windows Server 2008 R2**

Microsoft Corporation

게시일: 2009년 6월

요약

Microsoft® 볼륨 정품 인증은 볼륨 라이선스 고객이 볼륨 라이선스 미디어 정품 인증 프로세서를 자동화하고 관리하는 것을 돕습니다. 볼륨 라이선스 고객과 Microsoft 파트너 프로그램, MSDN® 및 Microsoft TechNet과 같은 특별 프로그램 가입자는 볼륨 라이선스 소프트웨어와 미디어를 사용할 수 있습니다. 이 가이드는 키 관리 서비스를 사용하여 Windows® 7 및 Windows Server® 2008 R2 운영 체제의 정품 인증 버전을 배포하려는 조직의 IT 전문가를 위한 것입니다.

이 문서와 여기에서 참조하는 모든 문서는 정보 제공만을 목적으로 하며 Microsoft는 이 문서에 있는 내용에 대해 어떠한 명시적 또는 암시적 보증도 하지 않습니다. URL 및 기타 인터넷 웹 사이트 참조를 포함하여 본 문서의 정보는 사전 통지 없이 변경될 수 있습니다. 이 문서를 사용하여 생기는 위험성이나 결과는 전적으로 사용자가 책임을 집니다. 특별한 언급이 없는 경우, 본 문서에서 예시하는 회사, 조직, 제품, 도메인 이름, 전자 메일 주소, 로고, 사람, 장소 및 이벤트는 가상으로 만들어진 것입니다. 실제 회사, 조직, 제품, 도메인 이름, 전자 메일 주소, 로고, 사람, 장소 또는 이벤트와 연관시키려는 어떠한 의도도 없으며 그렇게 해석되지 않아야 합니다. 해당하는 모든 저작권 법률을 준수하는 것은 사용자의 책임입니다. 저작권에 의해 주어지는 권리를 제한하지 않고 본 문서의 어떤 부분도 Microsoft Corporation의 명시적 서면 허가 없이는 어떠한 형태나 수단(전자, 기계, 복사, 기록 등) 또는 목적으로도 재생하거나 검색 시스템에 저장 또는 전송할 수 없습니다.

Microsoft는 본 문서에서 다루는 제품이나 서비스에 대해 특허, 특허 출원, 상표, 저작권 또는 기타 지적 재산권을 가지고 있을 수 있습니다. Microsoft와 체결한 서면 라이선스 계약서에 명시된 경우를 제외하면 본 문서를 제공한다고 해서 이러한 특허, 상표, 저작권 또는 기타 지적 재산권에 대한 라이선스가 부여되는 것은 아닙니다.

© 2009 Microsoft Corporation. All rights reserved.

Microsoft, Hyper-V, MSDN, Windows, Windows 로고, Windows NT, Windows 7, Windows Server, Windows Vista 및 Windows Web Server는 Microsoft 그룹의 상표입니다.

본 문서에 언급된 실제 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

**목차**

[소개 1](#_Toc236570557)

[KMS 이해 2](#_Toc236570558)

[최소 컴퓨터 요구 사항 2](#_Toc236570559)

[KMS 정품 인증 최소 한계 2](#_Toc236570560)

[정품 인증 대수 캐시 3](#_Toc236570561)

[KMS의 작동 방식 4](#_Toc236570562)

[KMS 정품 인증 갱신 4](#_Toc236570563)

[KMS 서비스 게시 4](#_Toc236570564)

[클라이언트의 KMS 서비스 검색 4](#_Toc236570565)

[KMS 배포 계획 5](#_Toc236570566)

[DNS 서버 구성 계획 6](#_Toc236570567)

[첫 KMS 호스트 정품 인증 6](#_Toc236570568)

[이후 KMS 호스트 정품 인증 7](#_Toc236570569)

[기존 KMS 호스트 업그레이드 7](#_Toc236570570)

[KMS 클라이언트 계획 8](#_Toc236570571)

[표준 사용자로 정품 인증 8](#_Toc236570572)

[필요한 제품 키 결정 9](#_Toc236570573)

[KMS 키 선택 9](#_Toc236570574)

[KMS 호스트 선택 10](#_Toc236570575)

[KMS 정품 인증 배포 12](#_Toc236570576)

[KMS 호스트 구성 12](#_Toc236570577)

[Slmgr.vbs 원격 실행 14](#_Toc236570578)

[원격 소프트웨어 라이선스 관리자 사용을 위한 Windows 방화벽 구성 14](#_Toc236570579)

[작업 그룹 컴퓨터를 대상으로 한 원격 작업 14](#_Toc236570580)

[DNS 구성 15](#_Toc236570581)

[SRV 레코드에 대한 기본 DNS 권한 변경 15](#_Toc236570582)

[다수의 DNS 도메인에 게시 16](#_Toc236570583)

[DNS에서 SRV 레코드 직접 만들기 17](#_Toc236570584)

[BIND 8.2 이상 DNS 서버에서 SRV 레코드 직접 만들기 17](#_Toc236570585)

[DNS에 KMS SRV 레코드 게시 해제 18](#_Toc236570586)

[KMS 호스트 설치 19](#_Toc236570587)

[KMS 클라이언트 구성 20](#_Toc236570588)

[KMS 호스트 직접 지정 20](#_Toc236570589)

[KMS 클라이언트에 대한 자동 검색 설정 20](#_Toc236570590)

[KMS 클라이언트에 접미사 항목 추가 21](#_Toc236570591)

[KMS 클라이언트 배포 21](#_Toc236570592)

[KMS 클라이언트 직접 정품 인증 21](#_Toc236570593)

[MAK 클라이언트를 KMS로 변환 및 KMS 클라이언트를 MAK로 변환 22](#_Toc236570594)

[소매 버전을 볼륨 정품 인증으로 변환 23](#_Toc236570595)

[컴퓨터 정품 재인증 24](#_Toc236570596)

# 소개

Microsoft® 볼륨 정품 인증은 IT 전문가가 Microsoft 볼륨 라이선스 프로그램과 Windows의 볼륨 라이선스 버전을 제공하는 다른 프로그램에 따라 라이선스를 취득한 Windows Vista®, Windows® 7, Windows Server® 2008 및 Windows Server 2008 R2 운영 체제를 실행하는 컴퓨터의 제품 정품 인증 프로세스를 자동화하고 관리하는 작업을 지원하는 구성 가능한 솔루션입니다.

이 가이드는 Windows 7 및 Windows Server 2008 R2 운영 체제에 대한 특별 계획, 배포 및 운영 정보를 제공합니다. 이 가이드는 KMS(키 관리 서비스)를 사용하여 조직의 볼륨 정품 인증 인프라를 호스팅하는 조직을 위한 것입니다.

**참고**   이 문서는 Windows 7 및 Windows Server 2008 R2 운영 체제에 대한 볼륨 정품 인증 가이드를 제공합니다. Windows Vista 및 Windows Server 2008 볼륨 정품 인증 계획에 대한 자세한 내용은 <http://go.microsoft.com/fwlink/?LinkID=75674>의 **볼륨 정품 인증 2.0 기술 가이드**를 참조하십시오. 이 가이드에서 두 제품 간의 상호 운용성도 다룹니다.

# KMS 이해

KMS는 로컬 네트워크에서 컴퓨터를 정품 인증하므로 개별 컴퓨터를 Microsoft에 연결할 필요가 없습니다. 이를 위해 KMS는 클라이언트-서버 토폴로지를 사용합니다. KMS 클라이언트 컴퓨터는 DNS(도메인 이름 시스템) 또는 정적 구성을 사용하여 KMS 호스트 컴퓨터를 찾을 수 있습니다. KMS 클라이언트는 RPC(원격 프로시저 호출)를 사용하여 KMS에 연결합니다. KMS는 Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2 등의 운영 체제를 실행하는 컴퓨터에서 호스팅될 수 있습니다.

## 최소 컴퓨터 요구 사항

KMS 정품 인증 계획 시 네트워크는 정품 인증 최소 한계 또는 KMS가 필요한 최소 인증 컴퓨터 대수를 만족하거나 그 이상이어야 합니다. 또한 KMS 호스트가 네트워크에서 컴퓨터 수를 추적하는 방법을 이해해야 합니다.

### KMS 정품 인증 최소 한계

KMS는 물리적 컴퓨터 및 가상 컴퓨터 모두 정품 인증할 수 있습니다. KMS 정품 인증을 위한 자격 요건으로, 네트워크는 정품 인증 최소 한계를 만족해야 합니다. KMS는 이 최소 한계를 만족해야만 클라이언트 컴퓨터를 정품 인증합니다. 정품 인증 최소 한계가 만족되도록 KMS 호스트는 네트워크에서 정품 인증을 요구하는 컴퓨터의 대수를 계산합니다. Windows server 2008 또는 Windows Server 2008 R2를 실행하는 컴퓨터의 정품 인증 최소 한계는 5대입니다. Windows Vista 또는 Windows 7을 실행하는 컴퓨터의 정품 인증 최소 한계는 25대입니다.최소 한계는 물리적 컴퓨터나 가상 컴퓨터에서 실행하는 클라이언트 컴퓨터 및 서버를 포함합니다.

KMS 호스트는 KMS 클라이언트가 보내는 유효한 각 정품 인증 요구에 대한 응답으로 정품 인증을 위해 KMS 호스트에 접속한 컴퓨터 대수에 관한 정보를 제공합니다. 정품 인증 최소 한계 이하의 대수를 수신한 클라이언트는 정품 인증되지 않습니다. 예를 들어, KMS 호스트에 첫 번째로 연결하는 두 컴퓨터가 Windows 7을 실행한다면 첫 번째 컴퓨터가 1의 정품 인증 수를 수신하고 두 번재 컴퓨터가 2의 정품 인증 수를 수신합니다. 다음 컴퓨터가 Windows 7 가상 컴퓨터라면 이 컴퓨터는 3의 정품 인증 수를 수신합니다. Windows 7을 실행하는 컴퓨터는 정품 인증을 위해 25 이상의 정품 인증 수를 수신해야하기 때문에 이 중 아무 컴퓨터도 정품 인증되지 않습니다. 정품 인증 수가 너무 낮아 정품 인증되지 않는 유예 상태의 KMS 클라이언트는 현재 정품 인증 수를 얻기 위해 KMS 호스트에 2시간 마다 연결하며 최소 한계가 충족되면 정품 인증됩니다.

KMS 호스트에 연결하는 다음 컴퓨터가 Windows Server 2008 R2를 실행하고 있다면 정품 인증 수는 Windows Server 2008 R2 및 Windows 7을 실행하는 컴퓨터를 합친 값이기 때문에 4의 정품 인증 수를 수신합니다. Windows Server 2008 또는 Windows Server 2008 R2를 실행하는 컴퓨터가 5 이상의 정품 인증 수를 수신한다면 정품 인증됩니다. Windows 7을 실행하는 컴퓨터가 25 이상의 정품 인증 수를 수신한다면 정품 인증됩니다.

### 정품 인증 대수 캐시

정품 인증 최소 한계를 추적하기 위해 KMS 호스트는 정품 인증을 요구하는 KMS 클라이언트 컴퓨터의 기록을 보관합니다. KMS 호스트는 각 KMS 클라이언트 컴퓨터에 CMID(클라이언트 ID)를 부여하고 KMS 호스트는 테이블에 각 CMID를 저장합니다. 각 정품 인증 요청은 이 테이블에 30일 동안 유지됩니다. 클라이언트 컴퓨터가 정품 인증을 갱신하면 테이블에서 캐시된 CMID가 제거되고 새 기록이 만들어지며 이 때부터 다시 30일의 기간이 시작됩니다. KMS 클라이언트 컴퓨터가 30일 이내에 정품 인증을 갱신하지 않으면 KMS 호스트는 테이블에서 해당 CMID를 제거하고 정품 인증 대수를 1만큼 감소합니다.

KMS 호스트는 CMID 수가 정품 인증 최소 한계 이하로 떨어지지 않게 하기 위해 KMS 클라이언트가 필요한 CMID 수를 2배로 캐시합니다. 예를 들어, Windows 7을 실행하는 클라이언트 컴퓨터가 있는 네트워크에서 KMS 정품 인증 최소 한계는 25입니다. 이 KMS 호스트는 최근 50개의 정품 인증에 대한 CMID를 캐시합니다. Windows Server 2008 R2에 대한 KMS 정품 인증 최소 한계는 5대입니다. Windows Server 2008 R2를 실행하는 KMS 클라이언트 컴퓨터에만 접속하는 KMS 호스트는 최근 10개의 CMID를 캐시합니다. 이후 Windows 7을 실행하는 클라이언트 컴퓨터가 이 KMS 호스트에 접속하면 KMS는 더 높은 최소 한계에 대응하기 위해 캐시 크기를 50으로 증가시킵니다. KMS는 절대 캐시 크기를 줄이지 않습니다.

## KMS의 작동 방식

KMS 정품 인증에는 TCP/IP 연결이 필요합니다. 기본적으로, KMS 호스트와 클라이언트 컴퓨터는 KMS 서비스를 찾고 게시하기 위해 DNS를 사용합니다. 관리 작업이 거의 또는 전혀 필요 없는 이러한 기본 설정을 사용하거나 네트워크 구성 및 보안 요구 사항에 따라 KMS 호스트와 클라이언트 컴퓨터를 직접 구성할 수도 있습니다.

### KMS 정품 인증 갱신

KMS 정품 인증은 180일 동안 유효합니다. 이를 정품 인증 유효 기간이라고 합니다. KMS 클라이언트 컴퓨터는 정품 상태를 유지하기 위해 KMS 호스트에 180일마다 최소 한 번은 연결하여 정품 인증을 갱신해야 합니다. 기본적으로, KMS 클라이언트 컴퓨터는 정품 인증 갱신을 7일마다 시도합니다. KMS 정품 인증이 실패하면 클라이언트는 2시간마다 다시 시도합니다. 클라이언트 컴퓨터의 정품 인증이 갱신된 후에는 정품 인증 유효 기간이 다시 시작됩니다.

### KMS 서비스 게시

KMS 서비스는 DNS의 SRV(서비스) RR(리소스 레코드)를 사용하여 KMS 호스트의 위치를 저장하고 통신을 수행합니다. KMS 호스트는 KMS SRV RR을 게시하기 위해 가능한 경우 DNS 동적 업데이트 프로토콜을 사용합니다. 동적 업데이트를 사용할 수 없거나 KMS 호스트가 RR을 게시할 권리가 없는 경우, DNS 기록을 직접 게시하거나 특정 KMS 호스트에 연결하기 위해 클라이언트 컴퓨터를 구성해야 합니다.

**참고**네트워크의 복잡성 및 토폴로지에 따라 DNS 변경을 모든 DNS 호스트에 전달하려면 시간이 걸릴 수도 있습니다.

### 클라이언트의 KMS 서비스 검색

기본적으로, KMS 클라이언트는 KMS 서비스 정보에 대한 DNS를 쿼리합니다. KMS 클라이언트는 DNS에 KMS 서비스 정보를 처음으로 쿼리할 때 DNS가 반환한 SRV RR 목록에서 KMS 호스트를 무작위로 선택합니다.

SRV RR을 포함한 DNS 서버 주소는 KMS 클라이언트에 접미사 항목으로 나열될 수 있는데 이는 하나의 DNS 서버와 다른 중요 DNS를 가진 KMS 클라이언트에서 KMS에 대한 SRV RR의 광고를 할 수 있게 합니다.

우선 순위와 가중치 매개 변수는 KMS에 대한 **DnsDomainPublishList** 레지스트리 값에 추가될 수 있습니다. KMS 호스트 우선 순위 그룹과 각 그룹 내 가중치를 정함으로써 클라이언트가 처음으로 시도해야 하는 KMS 호스트를 정할 수 있고 여러 KMS 호스트 사이의 트래픽 균형을 조정할 수 있습니다. Windows 7 및 Windows Server 2008 R2에서만 우선 순위와 가중치 매개 변수를 제공합니다.

클라이언트가 선택한 KMS 호스트가 응답하지 않으면 KMS 클라이언트는 SRV RR 목록에서 이 KMS 호스트를 제거하고 목록의 다른 KMS 호스트를 무작위로 선택합니다. KMS 호스트가 응답하면 KMS 클라이언트는 KMS호스트 이름을 캐시하고 이후 정품 인증과 갱신 시도에 이 호스트를 사용합니다. 캐시된 KMS 호스트가 다음 번 갱신 때 응답하지 않으면 KMS 클라이언트는 KMS SRV RR을 얻기 위해 DNS에 쿼리하여 새 KMS 호스트를 검색합니다.

기본적으로, 클라이언트 컴퓨터는 정품 인증을 위해 TCP 포트 1688(이 기본 포트를 변경할 수 있음)을 통해 익명 RPC를 사용하여 KMS 호스트에 연결합니다. KMS 호스트와 TCP 세션을 수립하고 나면 클라이언트가 단일 요청 패킷을 보냅니다. KMS 호스트는 정품 인증 대수로 응답합니다. 대수가 해당 운영 체제에 대한 정품 인증 최소 한계를 만족하거나 그 이상이면 클라이언트가 정품 인증하고 세션이 종결됩니다. KMS 클라이언트는 갱신 요청에도 이와 동일한 프로세스를 사용합니다. 각 방향의 통신은 250바이트입니다.

## KMS 배포 계획

KMS 서비스에는 전용 서버가 필요하지 않습니다. KMS 서비스는 AD DS(Active Directory® 도메인 서비스) 도메인 컨트롤러와 RODC(읽기 전용 도메인 컨트롤러) 등의 다른 서비스와 함께 호스팅할 수 있습니다. KMS 호스트는 Windows Server 2003을 포함하여 모든 지원되는 Windows 운영 체제를 실행하는 물리적 컴퓨터나 가상 컴퓨터에서 실행할 수 있습니다. Windows Server 2008 R2를 실행하는 KMS 호스트는 볼륨 정품 인증을 지원하는 모든 Windows 운영 체제를 정품 인증할 수 있지만 Windows 7을 실행하는 KMS 호스트는 Windows 7 및 Windows Vista를 실행하는 컴퓨터만 정품 인증할 수 있습니다. 하나의 KMS 호스트로 KMS 클라이언트를 무제한 지원할 수 있지만 장애 조치를 위해 최소 두 개 이상의 KMS 호스트를 두는 것이 좋습니다. 대부분의 조직은 전체 인프라를 두 개의 KMS 호스트만으로 운영할 수 있습니다.

**참고**KMS는 Windows Server 2003에 자동으로 포함되지 않습니다. Windows Server 2003을 실행하는 컴퓨터에 KMS를 호스트하려면 다음 사이트 중 하나에서 KMS를 다운로드하고 설치하십시오.

* x86 기반 컴퓨터의 경우, <http://go.microsoft.com/fwlink/?LinkID=82964>의 **Windows Server 2003 SP1 이상용 키 관리 서비스 1.1 (x86)**를 참조하십시오.
* x64 기반 컴퓨터의 경우, <http://go.microsoft.com/fwlink/?LinkId=83041>의 **Windows Server 2003 SP1 이상용 키 관리 서비스 1.1 (x64)**를 참조하십시오.

### DNS 서버 구성 계획

기본 KMS 자동 게시 기능은 SRV RR 및 DNS 동적 업데이트 프로토콜 지원이 필요합니다. KMS 클라이언트의 기본 동작과 KMS SRV RR 게시는 Microsoft 소프트웨어를 실행하는 DNS 서버나 SRV RR(IETF(Internet Engineering Task Force) RFC(Request For Comments) 2782당)과 동적 업데이트(RFC(Request For Comments) 2136당)를 지원하는 다른 DNS 서버에서 지원됩니다. 예를 들어, BIND(Berkeley Internet Domain Name) 버전 8.x 및 9.x는 SRV 레코드와 동적 업데이트를 모두 지원합니다.

DNS 서버에서 SRV, A(인터넷 프로트콜 버전 4 또는 IPv4) 및 AAAA(인터넷 프로토콜 버전 6 또는 IPv6) RR을 만들고 업데이트하는 데 필요한 자격 증명을 갖도록 KMS 호스트를 구성해야 합니다. 아니면 레코드를 직접 만들어야 합니다. KMS 호스트에 필요한 자격 증명을 부여하는 좋은 방법은 AD DS에서 보안 그룹을 만들고 모든 KMS 호스트를 이 그룹에 추가하는 것입니다. Microsoft 소프트웨어를 실행하는 DNS 서버에서 이 보안 그룹에 KMS SRV RR을 포함할 각 DNS 도메인의 \_VLMCS.\_TCP 레코드에 대해 완전한 권한을 부여해야 합니다.

### 첫 KMS 호스트 정품 인증

네트워크에 있는 KMS 호스트는 KMS 키를 설치하고 Microsoft를 통해 정품 인증해야 합니다. KMS 키를 설치하면 KMS 호스트에서 키 관리 서비스를 이용할 수 있게 됩니다. KMS 설치 후 전화나 온라인으로 KMS 호스트 정품 인증을 완료하십시오. 이 최초 정품 인증 후에는 KMS 호스트가 Microsoft와 정보를 교류하지 않습니다.

KMS 키는 KMS 호스트에만 설치되고 개별 KMS 클라이언트에는 절대 설치되지 않습니다. Windows 7 및 Windows Server 2008 R2는 KMS 클라이언트 컴퓨터에 KMS 키가 실수로 설치되는 것을 방지하기 위한 안전 장치를 가지고 있습니다. 사용자가 KMS 키를 설치할 때마다 그림 1의 경고가 나타납니다.



그림 1. KMS 키 설치

### 이후 KMS 호스트 정품 인증

각 KMS 키는 최대 6개의 KMS 호스트에 설치될 수 있으며 이는 물리적 컴퓨터나 가상 컴퓨터일 수 있습니다. KMS 호스트 정품 인증 후 동일 호스트는 동일 키로 최대 9번 이상 다시 정품 인증할 수 있습니다.

조직에 6개 이상의 KMS 호스트가 필요한 경우, 예외를 요청하기 위해 정품 인증 콜 센터로 전화하여 조직이 가지고 있는 KMS 키에 대해 추가 정품 인증을 요청할 수 있습니다. 자세한 내용은 볼륨 라이선스 웹 사이트 <http://go.microsoft.com/fwlink/?LinkID=73076>를 참조하십시오.

### 기존 KMS 호스트 업그레이드

Windows Server 2003, Windows Vista 또는 Windows Server 2008을 실행하는 KMS 호스트는 Windows 7 및 Windows Server 2008 R2를 실행하는 KMS 클라이언트를 지원하기 위해 구성될 수 있습니다. Windows Vista 및 Windows Server 2008을 위해 확장된 KMS 클라이언트를 지원하는 파일을 가진 패키지가 있는 KMS 호스트를 업데이트해야 합니다. 이 패키지는 Microsoft 다운로드 센터 <http://www.microsoft.com/downloads>나 Windows Update 및 WSUS(Windows Server Update Services)에서 사용 가능합니다. KMS 호스트에 이 패키지가 설치되면 Windows 7 및 Windows Server 2008 R2를 지원하기 위해 설계된 KMS 키는 이 가이드 처음 부분에서 설명한 것처럼 설치되고 정품 인증됩니다. 새 Windows 운영 체제 버전을 지원하는 KMS 키는 KMS 클라이언트로 작용하는 Windows의 이전 볼륨 라이선스 버전에 대한 지원도 제공합니다.

Windows Server 2003 KMS 호스트 업데이트의 경우, 모든 필요한 파일은 KMS 1.2 다운로드 가능 패키지에 포함되어 있으며 이는 Microsoft 다운로드 센터 <http://www.microsoft.com/downloads>에서 사용 가능합니다.

### KMS 클라이언트 계획

기본적으로, Windows Vista, Windows 7, Windows Server 2008 및 Windows Server 2008 R2의 볼륨 라이선스 버전을 실행하는 컴퓨터는 KMS 클라이언트이며 추가 구성이 필요 없습니다. KMS 클라이언트는 DNS에 KMS 서비스를 게시하는 SRV RR을 쿼리하여 KMS 호스트의 위치를 자동으로 찾을 수 있습니다. 네트워크 환경에서 SRV RR을 사용하지 않는 경우, 특정 KMS 호스트르 사용하도록 KMS 클라이언트를 직접 구성할 수 있습니다.

KMS 클라이언트를 직접 구성하려면, 이 가이드 후반부의 "KMS 호스트 직접 지정" 부분의 단계를 따르십시오.

### 표준 사용자로 정품 인증

Windows 7 및 Windows Server 2008 R2는 정품 인증을 위해 관리자 권한이 필요 없습니다. 그러나 이 변경은 표준 사용자 계정으로 정품 인증된 상태의 Windows 7 또는 Windows Server 2008 R2를 제거하는 것은 허락하지 않습니다. 관리자 계정은 다른 정품 인증 또는 "라이선스 초기화"와 같은 라이선스 관련 작업을 위해 필요합니다.

# 필요한 제품 키 결정

Windows 7 및Windows Server 2008 R2 운영 체제는 다양한 버전이 있습니다. 볼륨 정품 인증을 간소화하고 조직에 필요한 제품 키의 수를 줄이기 위해 Microsoft는 제품 키를 개별 제품 요소가 아니라 제품 그룹에 적용시키는 *제품 키 그룹*을 만들었습니다.

## KMS 키 선택

KMS의 경우, 제품 키는 제품 그룹과 연관되며 해당하는 제품 그룹 내의 Windows 버전과 제품 계층 내 다른 하위 버전도 정품 인증할 수 있습니다. 계층에서 첫 단계이면서 가장 포괄성이 낮은 계층은 클라이언트 볼륨 라이선스 제품 그룹이고 서버 그룹 C는 KMS 계층에서 가장 포괄성이 높은 그룹입니다.

이 계층은 Windows Vista 및 Windows Server 2008 볼륨 라이선스 버전 및 제품 키 그룹으로 확장합니다. Windows 7 및 Windows Vista 모두에 대한 클라이언트 VL용 KMS 키에 액세스할 수 있는 고객을 의미하는개별 KMS 키는 각 제품 키 그룹에 대해 발급됩니다. 고객이 Windows의 여러 버전 및 세대를 정품 인증하기 위해 단일 KMS 키를 가질 수 있음을 의미하는 새 Windows 제품용 KMS 키는 이전 세대도 정품 인증합니다. 표 1는 제품 그룹 간의 상관 관계를 보여줍니다.

표 1 제품 그룹 상관 관계

| 볼륨 라이선스 제품 키 그룹 | Windows 버전(Windows 7 및 Windows Server 2008 R2) | Windows 버전(Windows Vista 및 Windows Server 2008) |
| --- | --- | --- |
| 클라이언트 VL | * Windows 7 Professional
* Windows 7 Enterprise
 | * Windows Vista Business
* Windows Vista Enterprise
 |
| 서버 그룹 A | * Windows Web Server® 2008 R2
* Windows Server 2008 R2 HPC Edition
* Windows HPC Server 2008 R2
 | * Windows Web Server 2008
* Windows Compute Cluster Server 2008
 |
| 서버 그룹 B | * Windows Server 2008 R2 Standard
* Windows Server 2008 R2 Enterprise
 | * Windows Server 2008 Standard
* Windows Server 2008 Enterprise
* Hyper-V™ 없는 버전 포함
 |
| 서버 그룹 C | * Windows Server 2008 R2 Datacenter
* Itanium 기반 시스템용 Windows Server 2008 R2
 | * Windows Server 2008 Datacenter
* Itanium 기반 시스템용 Windows Server 2008
* Hyper-V 없는 버전 포함
 |

## KMS 호스트 선택

이 가이드에서 앞서 언급한 것처럼, KMS는 물리적 컴퓨터나 가상 컴퓨터의 클라이언트 또는 서버 운영 체제에 호스팅될 수 있습니다. KMS 호스트 시스템을 선택하는 경우, KMS로 정품 인증할 운영 체제 버전을 고려하십시오. Windows 7에서 호스팅되는 KMS는 클라이언트 운영 체제만 정품 인증할 수 있지만 Windows Server 2008 R2에서 호스팅되는 KMS는 클라이언트와 서버 컴퓨터 모두를 정품 인증할 수 있습니다. 이 계층 설명은 표 2를 참조하십시오.

표 2. KMS 계층

| 제품 키 그룹 | KMS를 호스팅할 수 있는 운영 체제(KMS 키로 KMS 호스트 정품 인증) | 이 KMS 호스트로 정품 인증되는 Windows 제품 버전 |
| --- | --- | --- |
| Windows 7용 클라이언트 VL | * Windows Vista
* Windows 7
* Windows Server 2003 1.2용 KMS
 | * Windows 7 Professional
* Windows 7 Enterprise
* Windows Vista Business
* Windows Vista Enterprise
 |
| Windows Server 2008 R2용 서버 그룹 A | * Windows Server 2003 1.2용 KMS
* Windows Web Server 2008
* Windows Web Server 2008 R2
* Windows HPC Server 2008
* Windows HPC Server 2008 R2
 | 이전 이상 포함:* Windows Web Server 2008 R2
* Windows Web Server 2008
* Windows HPC Server 2008 R2
* Windows HPC Server 2008
 |
| Windows Server 2008 R2용 서버 그룹 B | 이전 이상 포함:* Windows Server 2008 R2 Standard
* Windows Server 2008 R2 Enterprise
* Windows Server 2008 Standard
* Windows Server 2008 Enterprise
 | 이전 이상 포함:* Windows Server 2008 R2 Standard
* Windows Server 2008 R2 Enterprise
* Windows Server 2008 Standard
* Windows Server 2008 Enterprise
 |
| 서버 그룹 C | 이전 이상 포함:* Windows Server 2008 R2 Datacenter
* Windows Server 2008 Datacenter
* Itanium 기반 시스템용 Windows Server 2008
 | 이전 이상 포함:* Windows Server 2008 R2 Datacenter
* Windows Server 2008 Datacenter
* Itanium 기반 시스템용 Windows Server 2008
 |

# KMS 정품 인증 배포

KMS 정품 인증은 관리자의 개입을 최소화시킨 인증 방식입니다. 네트워크 환경에 DDNS(동적 도메인 이름 시스템)가 있고 컴퓨터가 서비스를 자동으로 게시할 수 있는 경우, 최소한의 개입만으로 KMS 호스트를 배포할 수 있습니다. 조직에 둘 이상의 KMS 호스트가 있거나 네트워크가 DDNS를 지원하지 않는 경우, 추가 구성 작업이 필요할 수도 있습니다.

경고   이 단원에 나오는 일부 절차에는 레지스트리 변경이 필요합니다. 레지스트리 편집기를 사용하거나 다른 방법을 이용하여 레지스트리를 잘못 수정하는 경우 문제가 발생할 수 있으며 이러한 문제는 운영 체제를 다시 설치해야 해결될 수도 있습니다. Microsoft는 이러한 문제의 해결을 보장하지 않습니다. 레지스트리 수정에 따른 모든 위험은 사용자의 책임입니다.

본 단원의 나머지 부분에서는 다음과 같은 중요 작업을 설명합니다.

* KMS 호스트 구성
* DNS 구성
* KMS 호스트 설치
* KMS 클라이언트 구성

## KMS 호스트 구성

SL 관리자(Slmgr.vbs)라고도 하는 소프트웨어 라이선스 관리자는 볼륨 정품 인증 정보를 구성하고 검색하는 데 필요한 스크립트입니다. 이 스크립트는 대상 컴퓨터에서 로컬로 실행하거나 다른 컴퓨터에서 원격으로 실행할 수 있지만, 승격된 명령 프롬프트에서 실행해야 합니다. 표준 사용자가 Slmgr.vbs를 실행하면 일부 라이선스 데이터가 누락되거나 올바르지 않을 수도 있습니다. 이 경우에는 많은 작업이 금지됩니다.

Slmgr.vbs는 Wscript.exe 또는 Cscript.exe를 사용할 수 있고, 사용할 스크립트 엔진을 지정할 수 있습니다. 스크립트 엔진을 지정하지 않으면 Slmgr.vbs가 기본 스크립트 엔진인 Wscript.exe를 사용하여 실행됩니다.

**참고**KMS에는 KMS 호스트에서 방화벽 예외가 필요합니다. 기본 TCP 포트를 사용하는 경우, Windows 방화벽에서 **KMS 트래픽** 예외를 적용하십시오. 다른 방화벽을 사용하는 경우, TCP 포트 1688을 여십시오. 기본 포트 이외 포트를 사용하는 경우, 방화벽에서 사용자 지정 TCP 포트를 여십시오.

변경 내용이 적용되려면 소프트웨어 라이선스 서비스를 다시 시작해야 합니다. 소프트웨어 라이선스 서비스를 다시 시작하려면 MMC(Microsoft 관리 콘솔) 서비스 스냅인을 사용하거나 승격된 명령 프롬프트에서 다음 명령을 실행할 수 있습니다.

net stop sppsvc && net start sppsvc

Slmgr.vbs에는 최소 하나 이상의 매개 변수가 필요합니다. 스크립트를 매개 변수 없이 실행하는 경우, 도움말 정보가 표시됩니다. 표 3에 Slmgr.vbs 명령줄 옵션과 각 옵션에 대한 설명을 수록했습니다. 표 3에 있는 대부분의 매개 변수는 KMS 호스트를 구성합니다. 그러나 /sai 및 /sri 매개 변수는 호스트에 연결한 후에 KMS 클라이언트로 전달됩니다. Slmgr.vbs의 일반적 구문은 다음과 같습니다.

slmgr.vbs /parameter

표 3. Slmgr.vbs 매개 변수

| 매개 변수 | 설명 |
| --- | --- |
| /sprt PortNumber | KMS 호스트에서 TCP 통신 포트를 설정합니다. PortNumber에 사용할 TCP 포트 번호를 기입합니다. 기본 설정은 **1688**입니다. |
| /cdns | KMS 호스트에 의한 자동 DNS 게시를 해제합니다. |
| /sdns | KMS 호스트에 의한 자동 DNS 게시를 설정합니다. |
| /cpri | KMS 호스트 프로세스의 우선 순위를 낮춥니다. |
| /spri | KMS 호스트 프로세스의 우선 순위를 **기본**으로 설정합니다. |
| /sai ActivationInterval | KMS 호스트를 찾지 못하는 경우 KMS 클라이언트가 정품 인증을 받으려는 요청 빈도를 변경합니다. ActivationInterval에 분 단위의 시간을 넣습니다. 기본 설정은 **120**입니다. |
| /sri RenewalInterval | KMS 클라이언트가 KMS 호스트에 접속하여 정품 인증을 갱신하려는 요청 빈도를 변경합니다. RenewalInterval에 분 단위의 시간을 넣습니다. 기본 설정은 **10080**(7일)입니다. 이 설정은 로컬 KMS 클라이언트 설정보다 우선합니다. |
| /dli | KMS 호스트로부터 현재 KMS 정품 인증 수를 가져옵니다. |

Slmgr.vbs 원격 실행

Slmgr.vbs를 원격으로 실행하려면 관리자가 추가 매개 변수를 제공해야 합니다. 대상 컴퓨터의 컴퓨터 이름을 비롯하여 대상 컴퓨터에서 로컬 관리자 권한을 가진 사용자 계정의 사용자 이름 및 암호를 포함시켜야 합니다. 사용자 이름과 암호를 지정하지 않고 원격으로 실행하면 스크립트가 스크립트를 실행하는 사용자의 자격 증명을 사용합니다.

다음 구문은 Slmgr.vbs를 원격으로 실행하는 데 필요한 추가 매개 변수를 보여줍니다.

slmgr.vbs TargetComputerName [username] [password] /parameter [options]

### 원격 소프트웨어 라이선스 관리자 사용을 위한 Windows 방화벽 구성

Slmgr.vbs는 WMI(Windows Management Instrumentation)를 사용하므로, 관리자가 WMI 트래픽이 허용되도록 Windows 방화벽을 구성해야 합니다.

* 단일 서브넷의 경우, Windows 방화벽에서 **WMI(Windows Management Instrumentation)** 예외를 허용합니다.
* 여러 서브넷에 걸쳐 WMI 트래픽을 허용하려면 **WMI(Windows Management Instrumentation)(ASync-In)**, **Windows Management Instrumentation(WMI)(DCOM-In)** 및 **WMI(Windows Management Instrumentation)(WMI-In)**에 대한 연결을 허용합니다. 이와 함께 해당 범위에서 원격 액세스를 허용합니다. 관리 도구 폴더인 고급 보안과 함께 Windows 방화벽을 사용하여 이러한 설정을 구성합니다.

참고   개인 및 공용 프로필에서 Windows 방화벽 예외는 기본적으로 로컬 서브넷에서 들어오는 트래픽에만 예외를 적용합니다. 여러 서브넷에 적용되도록 예외를 확장하려면 고급 보안이 설정된 Windows 방화벽에서 예외 설정을 변경하거나 AD DS 도메인에 가입된 경우 도메인 프로필을 선택합니다.

### 작업 그룹 컴퓨터를 대상으로 한 원격 작업

관리자는 특정 작업 그룹에 속한 컴퓨터를 대상으로 Slmgr.vbs가 원격으로 작동하도록 할 수 있습니다. 이를 위해, KMS 클라이언트에서 레지스트리 하위 키 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**에 **DWORD** 값 **LocalAccountTokenFilterPolicy**를 만듭니다. 이 값을 **0x01**로 설정합니다.

## DNS 구성

다음 단원에서는 볼륨 정품 인증이 가능하도록 DNS를 구성하는 개념에 대해 설명합니다.

* 하나 이상의 KMS 호스트가 사용되는 경우 “SRV 레코드에 대한 기본 DNS 권한 변경” 단원을 참조하십시오.
* 다른 DNS 서비스를 사용하여 KMS 호스트를 찾도록 KMS 클라이언트를 활성화하려면 “여러 DNS 도메인에 게시” 단원을 참조하십시오.
* KMS 호스트에 대한 SRV 리소스 레코드를 수동으로 추가하려면 “DNS에서 SRV 레코드 직접 만들기”, “BIND 8.2 이상 DNS 서버에서 SRV 레코드 직접 만들기” 및 “DNS에 KMS SRV 레코드 게시 해제” 단원을 참조하십시오.

참고   DNS 변경은 모든 DNS 서버가 복제될 때까지 반영되지 않을 수도 있습니다.

### SRV 레코드에 대한 기본 DNS 권한 변경

하나의 KMS 호스트만 사용하는 경우, DNS에서 권한을 구성할 필요가 없을 수도 있습니다. 컴퓨터가 SRV RR을 만들고 이를 업데이트하는 것이 기본 동작입니다. 그러나 둘 이상의 KMS 호스트가 있는 경우(일반적인 경우), 다른 호스트는 SRV 기본 권한이 변경될 때까지 SRV RR을 업데이트하지 못합니다.

다음 고급 절차는 Microsoft의 자체 환경에 대한 예입니다. 세부적 단계는 조직마다 다를 수 있기 때문에 여기서는 이러한 세부적 단계를 제공하지 않으며 원하는 결과를 얻기 위한 유일한 방법도 아닙니다.

1. KMS 호스트에 사용될 AD DS에서 전역 보안 그룹을 만듭니다. 예를 들면 Key Management Service Group과 같습니다.
2. 각 KMS 호스트를 이 그룹에 추가합니다. 모든 호스트는 동일 도메인에 가입되어야 합니다.
3. 첫 번째 KMS 호스트가 만들어지면 이 호스트가 원래 SRV 레코드를 만듭니다. 첫 번째 KMS 호스트가 SRV 리소스 레코드를 만들지 못하는 경우, 조직이 기본 권한을 변경했기 때문일 수 있습니다. 이 경우, “DNS에서 SRV 레코드 직접 만들기” 단원의 설명에 따라 SRV RR을 수동으로 만듭니다.
4. SRV 그룹이 전역 보안 그룹 구성원에 의한 업데이트를 허용할 수 있는 권한을 설정합니다.

**참고** 도메인 관리자는 앞 단계의 수행 권한을 조직 관리자에게 위임할 수 있습니다. 이를 위해 AD DS에서 보안 그룹을 만들고 이 그룹에 SRV 레코드 변경 권한을 부여한 다음 대리인을 추가합니다.

### 다수의 DNS 도메인에 게시

기본적으로 KMS 호스트는 호스트가 속한 DNS 도메인에서만 등록됩니다. 네트워크 환경에 하나의 DNS 도메인만 있는 경우, 추가적인 조치가 필요하지 않습니다.

DNS 도메인 이름이 두 개 이상 있는 경우, SRV RR 게시 때 KMS 호스트가 사용할 DNS 도메인 목록을 생성할 수 있습니다. 이 레지스트리 값을 설정하면 주 DNS 접미사로 지정된 도메인에서만 게시하는 KMS의 기본 동작이 일시 중단됩니다.

KMS에 대한 **DnsDomainPublishList** 레지스트리 값에 priority 및 weight 매개 변수를 선택적으로 추가합니다. 이 기능을 사용하면 각 그룹 내에서 KMS 호스트의 우선 순위 그룹과 가중치를 결정하여 먼저 시도할 KMS 호스트를 지정하고 여러 KMS 호스트 사이에서 트래픽의 균형을 조정할 수 있습니다.

참고   DNS 변경은 모든 DNS 서버가 복제될 때까지 반영되지 않을 수도 있습니다. 변경이 너무 빈번하면(시간 < 복제 시간) 복제되지 않은 서버에서 변경이 수행되는 경우 이전 레코드가 그대로 유지될 수 있습니다.

다수의 DNS 도메인에서 KMS를 자동으로 게시하려면 레지스트리 하위 키 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform**의 다중 문자열 레지스트리 값 **DnsDomainPublishList**에 게시해야 하는 모든 KMS에 각 DNS 도메인 접미사를 추가합니다. 값을 변경한 후 소프트웨어 라이선스 서비스를 다시 시작하여 SRV RR을 만듭니다.

참고   이 키는 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL**의 Windows Vista 위치에서 변경되었습니다.

다수의 도메인에 게시하도록 KMS 호스트를 구성한 후, 레지스트리 하위 키를 내보내고 이를 추가 KMS 호스트의 레지스트리로 가져옵니다. 이 절차가 성공했는지 확인하기 위해 각 KMS 호스트에서 응용 프로그램 이벤트 로그를 확인하십시오. 이벤트 ID 12294는 KMS 호스트가 SRV RR을 성공적으로 생성했음을 나타냅니다. 이벤트 ID 12293은 SRV RR이 성공적으로 생성되지 않았음을 나타냅니다. 오류 코드의 전체 목록을 보려면 <http://technet.microsoft.com/en-us/library/cc303695.aspx>의 볼륨 정품 인증 2.0 운영 가이드를 참조하십시오.

### DNS에서 SRV 레코드 직접 만들기

해당 환경에서 DDNS를 지원하지 않는 경우, SRV RR을 수동으로 만들어 KMS 호스트를 게시해야 합니다. DDNS를 지원하지 않는 환경에서는 이벤트 로그가 실패한 DNS 게시 이벤트를 수집하지 않도록 모든 KMS 호스트에서 게시를 해제시켜야 합니다. 자동 게시를 해제시키려면 **/cdns** 명령줄 옵션과 함께 Slmgr.vbs 스크립트를 사용합니다. Slmgr.vbs 스크립트에 대한 자세한 내용은 “KMS 호스트 구성” 단원을 참조하십시오.

참고   수동으로 만들어진 SRV RR은 모든 레코드의 충돌이 방지된다면 KMS 호스트가 다른 도메인에서 자동으로 게시하는 SRV RR과 공존할 수 있습니다.

적합한 정방향 조회 영역에서 DNS 관리자를 사용하면 해당 위치에 적합한 정보를 이용하여 새로운 SRV RR이 만들어집니다. 기본적으로 KMS는 TCP 포트 1688에서 데이터를 수신하며 서비스는 \_VLMCS입니다. 표 4에는 SRV RR에 대한 예제 설정이 나와 있습니다.

표 4. SRV 리소스 레코드

| 이름 | 설정 |
| --- | --- |
| 서비스 | \_VLMCS |
| 프로토콜 | \_TCP |
| 포트 번호 | 1688 |
| 서비스를 제공하는 호스트 | KMS 호스트의 FQDN(정규화된 도메인 이름) |

### BIND 8.2 이상 DNS 서버에서 SRV 레코드 직접 만들기

조직에서 Microsoft 이외 DNS 서버를 사용하는 경우 DNS 서버가 BIND 8.2 이상과 호환되기만 한다면 필요한 SRV RR을 만들 수 있습니다. 레코드를 만들 때는 표 5의 정보들을 포함시키십시오. 표 5에 나타낸 우선 순위 및 가중치 설정은 Windows 7 및 Windows Server 2008 R2에서만 사용합니다.

표 5. SRV RR 정보

|  |  |
| --- | --- |
| 이름 | 설정 |
| 이름 | \_vlmcs.\_tcp |
| 유형 | SRV |
| 우선 순위 | 0 |
| 가중치 | 0 |
| 포트 | 1688 |
| 호스트 이름 | KMS 호스트의 FQDN |

KMS 자동 게시를 지원하도록 BIND 8.2 이상 DNS 서버를 구성하려면 KMS 호스트에서 RR 업데이트가 가능하도록 BIND 서버를 구성합니다. 예를 들어, 다음 라인을 named.conf의 영역 정의에 추가합니다.

allow-update { any; };

참고   이 서버에서 호스팅하는 모든 영역에 대해 DDNS가 허용되도록 allow-update 문을 named.conf.options에 추가할 수도 있습니다.

### DNS에 KMS SRV 레코드 게시 해제

KMS 호스트는 DNS에서 SRV RR을 생성하여 자신의 존재를 자동으로 게시합니다. KMS 호스트에 의한 자동 DNS 게시를 해제하려면 **/cdns** 명령줄 옵션과 함께 Slmgr.vbs 스크립트를 사용합니다.

Slmgr.vbs 스크립트를 사용하여 자동 DNS 게시를 해제시키는 것이 권장되지만 레지스트리에서 **DisableDnsPublishing**라고 하는 새로운 **DWORD** 값을 만들고 이 값을 **1**로 설정하여 이 작업을 수행할 수도 있습니다. 이 값은 레지스트리 하위 키 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform**에 있습니다. DNS에 KMS SRV 레코드 게시를 위한 기본 동작을 다시 사용하려면 값을 **0**으로 설정합니다.

## KMS 호스트 설치

KMS 기능을 사용하기 위해 KMS 호스트에 KMS 키를 설치하고 Microsoft 정품 인증 서비스를 이용하여 인터넷이나 전화로 호스트를 정품 인증합니다. Windows 7 또는 Windows Server 2008 R2를 실행하는 컴퓨터는 모두 KMS 호스트 역할을 할 수 있습니다.

Windows Vista, Windows Server 2003 및 Windows Server 2008도 KMS 호스트 역할을 할 수 있습니다. KMS 호스트가 정품 인증할 수 있는 KMS 클라이언트는 KMS 호스트 정품 인증에 사용되는 호스트 키에 따라 결정됩니다. KMS 호스트 키에 대한 자세한 내용은 <http://technet.microsoft.com/en-us/library/cc303276.aspx>의 볼륨 정품 인증 2.0 계획 가이드를 참조하십시오.

승격된 명령 프롬프트를 사용하여 Windows 7 또는 Windows Server 2008 R2 컴퓨터에서 KMS 키를 설치하고 정품 인증합니다.

* KMS 키를 설치하려면 명령 프롬프트에 **slmgr.vbs /ipk KmsKey**를 입력합니다.
* 온라인으로 정품 인증하려면 명령 프롬프트에 **slmgr.vbs /ato**를 입력합니다.
* 전화를 사용하여 정품 인증하려면 명령 프롬프트에 **slui.exe 4**를 입력합니다.

KMS 키 정품 인증 후, 소프트웨어 라이선스 서비스를 다시 시작합니다.

UI(사용자 인터페이스)를 사용하여 KMS 호스트 키를 설치할 때마다 Windows 7 및 Windows Server 2008 R2에 그림 2와 같은 경고가 표시됩니다. (Slmgr.vbs 스크립트를 사용하여 KMS 호스트 키를 설치하는 경우에는 사용자에게 이 경고가 표시되지 않음) 이 메시지는 관리자가 KMS 호스트로 의도하지 않은 컴퓨터에 KMS 키가 실수로 설치되는 것을 방지합니다.



그림 2. KMS 키 경고

KMS 호스트가 올바로 구성되었는지 확인하기 위해 KMS 수가 증가하는지 확인할 수 있습니다. KMS 호스트의 명령 프롬프트 창에 **slmgr.vbs /dli**를 입력하여 현재 KMS 수를 표시합니다. Applications and Services Logs 폴더에 있는 Key Management Service 로그에서 이벤트 ID 12290이 있는지 확인할 수도 있습니다. Key Management Service 로그에는 KMS 클라이언트의 정품 인증 요청이 기록됩니다. 각 이벤트에는 각 정품 인증 요청의 타임스탬프와 컴퓨터 이름이 표시됩니다.

## KMS 클라이언트 구성

이 단원에는 컴퓨터를 KMS 클라이언트로 설치하고 구성하는 개념에 대해 설명합니다. 기본적으로, Windows Vista, Windows 7, Windows Server 2008 및 Windows Server 2008 R2의 볼륨 라이선스 버전은 KMS 클라이언트입니다. 조직에서 KMS를 사용하여 정품 인증하려는 컴퓨터가 이러한 운영 체제 중 하나를 사용하고 있으며 네트워크가 DNS 자동 검색을 허용하는 경우, 더 이상의 구성이 필요하지 않습니다.

DNS를 사용하여 KMS 호스트를 검색하도록 KMS 클라이언트가 구성되었지만 DNS로부터 SRV 레코드를 수신하지 않는 경우, Windows 7 및 Windows Server 2008 R2는 이벤트 로그에 오류를 기록합니다.

### KMS 호스트 직접 지정

KMS 호스트 캐싱을 사용하여 KMS 호스트를 KMS 클라이언트에 수동으로 할당할 수 있습니다. KMS 호스트를 직접 할당하면 KMS 클라이언트에서 KMS 자동 검색이 해제됩니다. KMS 클라이언트에 KMS 호스트를 직접 할당하는 방법:

slmgr.vbs /skms <value>:<port>

여기서 value는 KMS 호스트의 KMS\_FQDN, IPv4Address, 또는 NetbiosName이고 port는 KMS 호스트의 TCP 포트입니다.

### KMS 클라이언트에 대한 자동 검색 설정

기본적으로 KMS 클라이언트는 KMS 호스트를 자동으로 검색합니다. KMS 호스트를 KMS 클라이언트에 직접 할당하여 자동 검색을 해제시킬 수 있습니다. 이 작업으로 KMS 클라이언트 캐시에서 KMS 호스트 이름도 삭제됩니다. 자동 검색이 해제된 경우, 명령 프롬프트에서 **slmgr.vbs /ckms**를 실행하여 이를 다시 사용할 수 있습니다.

### KMS 클라이언트에 접미사 항목 추가

SRV RR을 포함한 DNS 서버 주소를 KMS 클라이언트의 접미사 항목으로 추가함으로써 하나의 DNS 서버에서 여러 KMS 호스트를 인식시키고 다른 기본 DNS 서버를 가진 KMS 클라이언트가 이를 발견하도록 할 수 있습니다. KMS 클라이언트에서 도메인 접미사 검색 목록을 구성하기 위한 자세한 내용은 <http://support.microsoft.com/kb/275553>에서 Microsoft 도움말 및 지원 문서 “도메인 이름 시스템 클라이언트에서 도메인 접미사 검색 목록을 구성하는 방법”을 참조하십시오.

### KMS 클라이언트 배포

본 단원의 정보는 Windows AIK (Windows 자동 설치 키트)를 사용하여 Windows 운영 체제를 배포하고 정품 인증하는 볼륨 라이선스 고객에게 적용됩니다. 시스템 준비 도구(Sysprep) 또는 Slmgr.vbs 스크립트를 사용하여 KMS 클라이언트의 배포를 준비합니다.

* **Sysprep.** 이미지를 캡처하기 전에 **/generalize** 명령줄 옵션을 포함시켜 Sysprep를 실행하여 정품 인증 타이머, SID(보안 식별자) 및 기타 중요 설정을 초기화합니다. 정품 인증 타이머가 초기화되면 이미지가 배포될 때까지 이미지의 유예 기간이 만료되지 않습니다. Sysprep.exe를 실행하면 설치된 제품 키가 제거되지 않고 최소 설치 중 새 키를 입력하라는 요구를 받지 않습니다. 남은 라이선스 초기화가 없는 경우, Sysprep 작업이 완료되기는 하지만 정품 인증 타이머가 변경되지 않고 상황을 설명하는 오류가 반환됩니다.
* **Slmgr.vbs.** 내부용으로 데모 VM(가상 컴퓨터)을 구축하는 경우(조직 영업부용 가상 컴퓨터를 구축하거나 임시 교육 환경을 준비하는 경우 등), **/rearm** 명령줄 옵션과 함께 Slmgr.vbs 스크립트를 실행하면 유예 기간이 30일 연장되어 컴퓨터의 다른 부분은 그대로 유지되면서 정품 인증 타이머가 초기화됩니다. 정품 인증 타이머는 Windows 7 또는 Windows Server 2008 R2를 실행하는 컴퓨터에서 3회까지 초기화할 수 있습니다.

### KMS 클라이언트 직접 정품 인증

KMS 클라이언트는 기본적으로 사전 지정된 기간마다 정품 인증을 자동으로 시도합니다. 사용자에게 배포하기 전에 KMS 클라이언트(예를 들어, 연결되지 않은 클라이언트)를 수동으로 정품 인증하려면 제어판 시스템 항목을 이용하거나 승격된 명령 프롬프트에서 **slmgr.vbs /ato**를 실행합니다. Slmgr.vbs 스크립트는 정품 인증의 성공 또는 실패를 보고하고 결과 코드를 제공합니다. 정품 인증을 수행하려면 KMS 클라이언트가 조직 네트워크에서 KMS 호스트에 액세스할 수 있어야 합니다.

### MAK 클라이언트를 KMS로 변환 및 KMS 클라이언트를 MAK로 변환

기본적으로, Windows 7 및 Windows Server 2008 R2 운영 체제는 정품 인증에 KMS를 사용합니다. 기존 KMS 클라이언트를 MAK(복수 정품 인증 키) 클라이언트로 변경하려면 간단히 MAK를 설치하면 됩니다. 마찬가지로 MAK 클라이언트를 KMS 클라이언트로 변경하려면 다음을 실행합니다.

slmgr.vbs /ipk <KmsSetupKey>

여기서 KmsSetupKey는 표 6에 나타낸 설치 키 중 하나입니다. KMS 설치 키를 설치한 후 **cscript slmgr.vbs /ato**를 실행하여 KMS 클라이언트를 정품 인증합니다.

표 6. KMS 클라이언트 설치 키

| 운영 체제 버전 | 제품 키 |
| --- | --- |
| Windows 7 |
| Windows 7 Professional | FJ82H-XT6CR-J8D7P-XQJJ2-GPDD4 |
| Windows 7 Professional N | MRPKT-YTG23-K7D7T-X2JMM-QY7MG |
| Windows 7 Enterprise | 33PXH-7Y6KF-2VJC9-XBBR8-HVTHH |
| Windows 7 Enterprise N | YDRBP-3D83W-TY26F-D46B2-XCKRJ |
| Windows Server 2008 R2 |
| Windows Server 2008 R2 HPC Edition | FKJQ8-TMCVP-FRMR7-4WR42-3JCD7 |
| Windows Server 2008 R2 Datacenter | 74YFP-3QFB3-KQT8W-PMXWJ-7M648 |
| Windows Server 2008 R2 Enterprise | 489J6-VHDMP-X63PK-3K798-CPX3Y |
| Itanium 기반 시스템용 Windows Server 2008 R2 | GT63C-RJFQ3-4GMB6-BRFB9-CB83V |
| Windows Server 2008 R2 Standard | YC6KT-GKW9T-YTKYR-T4X34-R7VHC |
| Windows Web Server 2008 R2 | 6TPJF-RBVHG-WBW2R-86QPH-6RTM4 |

### 소매 버전을 볼륨 정품 인증으로 변환

조직이 해당 볼륨 라이선스를 취득하고 제품 사용 권한을 따르는 경우 Windows 7 Professional 및 Windows Server 2008 R2의 소매 버전을 KMS 클라이언트로 변환할 수 있습니다. Windows 7 Professional 및 모든 버전의 Windows Server 2008 R2를 소매 버전에서 KMS 클라이언트로 변환하려면 운영 체제 설치 과정에서 **제품 키** 페이지를 건너뜁니다. 설치가 완료되면 승격된 명령 프롬프트 창을 열고 다음 내용을 입력합니다.

Slmgr.vbs /ipk <SetupKey>

여기서 SetupKey는 표 6에서 Windows 7 또는 Windows Server 2008 R2 버전에 해당하는 KMS 클라이언트 설치 키입니다.

# 컴퓨터 정품 재인증

Windows 7과 Windows Server 2008 R2는 운영 체제가 설치된 컴퓨터의 하드웨어 구성을 주기적으로 점검합니다. 운영 체제가 하드웨어에서 큰 변화를 감지하면 정품 재인증이 필요합니다. 가중 요인과 임계값은 컴퓨터 하드웨어 시장의 지속적 발전에 대응하여 변화하기 때문에 이러한 값은 실제로 달라질 수 있습니다. KMS 클라이언트는 주로 하드 디스크 변경을 기준으로 정품 재인증이 필요한지 판단합니다.

KMS 정품 인증은 180일 동안 유효합니다. 이를 정품 인증 유효 기간이라고 합니다. KMS 클라이언트는 정품 상태를 유지하기 위해 KMS 호스트에 180일마다 최소 한 번은 연결하여 정품 인증을 갱신해야 합니다. 기본적으로, KMS 클라이언트 컴퓨터는 정품 인증 갱신을 7일마다 시도합니다. 클라이언트의 정품 인증이 갱신된 후에는 정품 인증 유효 기간이 다시 시작됩니다.