보안, 유연성, 민첩성의 보완으로 비밀번호 관리 강화

IBM Redbooks 솔루션 가이드

직원이 매일같이 관리해야 하는 무수히 많은 로그인 정보 및 비밀번호가 끊임없이 불만을 초래하고 업무 생산성을 떨어뜨리고 있습니다. 각종 애플리케이션의 로그인 정보를 기억해야 합니다. 이 애플리케이션 중 상당수는 사용자 이름과 비밀번호, 비밀번호 복잡성 요구사항, 비밀번호 변경 의무 주기 등이 저마다 다릅니다. 비즈니스 애플리케이션이 추가될 때마다 직원이 관리해야 하는 로그인 정보 수도 증가합니다. 헬프 데스크는 사라졌거나 잊어버린 로그인 정보를 복원하는 절차를 되풀이하곤 합니다. 이러한 요인이 복합적으로 작용하면서 보안 위험이 가중되고 헬프 데스크 비용도 감당하기 어려울 정도로 치솟게 됩니다.

IBM® Security Access Manager for Enterprise Single Sign-On을 사용하면 중앙에서 관리하는 단일 솔루션을 통해 이러한 심각한 보안 , 생산성, 컴플라이언스 문제를 해결할 수 있습니다. 그림 1은 이 솔루션을 개괄적으로 보여 줍니다.

그림 1. IBM Security Access Manager for Enterprise Single Sign-On 개요

알고 계십니까?

사용자는 다수의 비밀번호를 기억해야 한다는 것에 자주 불만을 제기하며, 컴퓨터 보안에서 발생하는 대표적인 허점 중 하나가 안전하지 않은 비밀번호 선택입니다. 안전하지 않은 비밀번호 또는 부실한 비밀번호 관리로 인한 보안 사고가 심심찮게 일어납니다. IBM Security Access Manager for Enterprise Single Sign-On 솔루션은 중앙 집중식 비밀번호 관리 및 셀프 서비스, 유연성 있는 강력 인증 메커니즘, 공유 및 가상 워크스테이션 사용 기능을 제공하며 특별한 가치를 선사합니다.

비즈니스 가치 및 솔루션 개요

IBM Security Access Manager for Enterprise Single Sign-On으로 비밀번호의 딜레마를 해결할 수 있습니다. 사용자는 하나의 비밀번호만 기억하면 되고 더 이상 모든 업무용 애플리케이션에서 일일이 강력한 비밀번호를 사용할 필요 없습니다. 한 번만 인증하면 IBM Security Access Manager for Enterprise Single Sign-On이 나머지를 해결합니다. IBM Security Access Manager for Enterprise Single Sign-On은 다음과 같은 주요 비즈니스 가치를 제공합니다.

- 매우 안전한 방식으로 비밀번호 관리

  IBM Security Access Manager for Enterprise Single Sign-On은 비밀번호 관련 애플리케이션과 데이터를 보호합니다. AES(Advanced Encryption Standard), 3중 DES(Triple Data Encryption Standard) 등 이용 가능한 가장 강력한 암호화 기술을 적용합니다. IBM Security Access Manager for Enterprise Single Sign-On은 FIPS(Federal Information Processing Standard) 140-2를 준수하므로 정부 기관, 병원, 기타 기관에 요구되는 까다로운 개인 정보 보호 및 보안 규정도 지킬 수 있습니다. IBM Security Access Manager for Enterprise Single Sign-On은 더 강력한 보안을 위해 2차 인증도 제공합니다. 사용자 또는 시스템에 따라 여러 보안 기능을 복합적으로 사용할 수 있습니다. 이와 같이 다중 보안 기능이 있을 경우 IBM Security Access Manager for Enterprise Single Sign-On에서 십분 활용할 수 있습니다.

- 헬프 데스크 비용 절감, 업무 생산성 향상

  IBM Security Access Manager for Enterprise Single Sign-On은 셀프 서비스 비밀번호 초기화 기능을 제공하므로 비밀번호 분실이나 계정 잠김에 따른 비용 및 생산성 저하 문제를 최소화하거나 해결할 수 있습니다. 비밀번호를 잊어버리거나 입력 오류 횟수 초과로 인해 계정이 잠기면 이를 처리하는 헬프 데스크의 부담이 늘어납니다. IBM Security Access Manager for Enterprise Single Sign-On은 구성 가능한 기능을 제공하여 사용자가 각종 보안 요구사항에 따라 스스로 비밀번호를 관리할 수 있게 합니다. 사용자가 대화형 메뉴를 통해 직접 비밀번호 변경, 초기화, 계정 잠금 및 잠금 해제를 수행하는 것을 구성 가능한 정책에 따라 사용자 정의하고 허용 또는 차단할 수 있습니다. IBM Security Access Manager for Enterprise Single Sign-On를 도입한 기업은 비밀번호 및 계정 서비스를 헬프 데스크, 사용자 또는 둘 다에게 맡길 것인지 유연성 있게 결정할 수 있습니다. 비밀번호 초기화 기능을 사용하면 IBM Security Access Manager for Enterprise Single Sign-On 비밀번호를 초기화하여 데스크탑 환경에 대한 액세스 권한을 다시 취득할 수 있습니다. 애플리케이션별 비밀번호는 초기화하지 않습니다.

- 감사 및 리포팅을 통해 컴플라이언스 입증

  IBM Security Access Manager for Enterprise Single Sign-On은 전사적 범위의 데스크탑을 대상으로 세부적인 사용자 활동을 감사하고 리포팅하는 기능을

기본적으로 제공합니다. 사용자의 애플리케이션 로그인 및 로그아웃을 포함한 감사 이벤트를 기록할 수 있습니다. 감사 메커니즘을 사용자 정의하여 사용자 활동과 관련된 다른 정보도 수집할 수 있습니다. 몇 가지 리포트가 기본적으로 포함되어 있지만, 모든 감사 데이터가 쿼리 가능한 하나의 관계형 데이터베이스에 있으므로 사용자 정의 리포트도 생성 가능합니다.

- 편리한 배치

  웹 기반 관리 콘솔, 강력한 디렉토리 통합, 배치하기 편리한 클라이언트측 소프트웨어를 사용하여 효과적으로 IBM Security Access Manager for Enterprise Single Sign-On을 구현하고 관리할 수 있습니다. 중앙의 웹 관리 콘솔(AccessAdmin)에서 모든 관리 기능을 수행합니다. 관리자는 AccessStudio 애플리케이션의 포인트 앤 클릭 마법사를 통해 프로파일 구성 작업을 차례로 수행할 수 있습니다. 관리자는 웹 브라우저를 통해 서버에 연결할 수 있는 어디서든 AccessAdmin 콘솔에 액세스하면 됩니다. IBM Security Access Manager for Enterprise Single Sign-On은 디렉터리 스키마 또는 사용자 저장소의 기타 설정을 변경할 필요 없이 기존 사용자 저장소를 사용합니다.

- 우수한 성능

  IBM Security Access Manager for Enterprise Single Sign-On은 모든 전용, 공유, 로밍 데스크탑 환경에서 최고의 속도를 실현합니다. 사용자에게 애플리케이션에 대한 SSO(single sign-on) 환경을 제공할 때 최소한의 자원만 사용합니다. IBM Security Access Manager for Enterprise SingleSign-On은 이벤트별로 자원을 사용하므로 클라이언트와 네트워크에 미치는 영향이 최소화됩니다. 추가적인 하드웨어나 소프트웨어는 필요 없습니다.

- 전사적 ID 관리 시스템과의 통합

  IBM Security Access Manager for Enterprise Single Sign-On Provisioning Bridge는 신임 정보 배포 프로세스를 자동화함으로써 IBM Security Access Manager for Enterprise Single Sign-On의 효용을 확대합니다. IBM Security Access Manager for Enterprise Single Sign-On Provisioning Bridge는 API 라이브러리를 활용하여 ID 관리 소프트웨어에서 자동으로 IBM Security Access Manager for Enterprise Single Sign-On 사용자 신임 정보를 프로비저닝할 수 있도록 지원합니다. 그러면 애플리케이션의 사용자 이름 또는 비밀번호가 사용자에게 투명한 방식으로 관리되므로 사용자가 일일이 기억할 필요 없습니다.

  사용자가 어떤 애플리케이션의 사용자 이름과 비밀번호를 알아야 할 경우 신임 정보 저장소(Wallet)에서 그 정보를 확인하면 됩니다. 이러한 액세스는 IBM Security Access Manager for Enterprise Single Sign-On에 인증된 경우에 한해 가능합니다. AccessAgent가 있는 워크스테이션을 사용할 수 없다면 AccessAssistant 웹 브라우저 기반 인터페이스를 통해 그 정보를 얻을 수 있습니다. IBM Security Access Manager forEnterprise Single Sign-On은 ID 관리 소프트웨어와 통합되지 않은 경우에도 이러한 구성요소를 통해 우수한 가용성과 보안을 자랑하는 비밀번호 확인 프로세스를 지원합니다.

- 키오스크 시스템 및 가상 데스크탑에서도 SSO 지원

  다른 사용자와의 워크스테이션 공유를 허용하면 편리하지만 위험도 수반합니다. 사용자가 로그오프하지 않고 키오스크를 떠나는 바람에 기밀 데이터가 노출되는 경우가 많습니다. IBM Security Access Manager for Enterprise Single Sign-On은 비활성 세션 종료 및 애플리케이션 종료를 자동화하는 기능으로 이러한 위협 요인을 해결합니다. RFID(radio frequency identification) 근접 키 또는 스마트 카드 제거를 통해

사용자 부재 시 자동 로그아웃하는 기능도 이 자동화의 범위에 포함됩니다.

IBM Security Access Manager for Enterprise Single Sign-On은 로밍 데스크탑 구현에 대해서도 강력한 세션 관리를 지원합니다. Microsoft Windows Terminal Services, Citrix XenApps와 같은 기술을 적용하며 공유 데스크탑 또는 키오스크 시스템과 전용 데스크탑을 사용합니다. 사용자는 편리하고 안전하게 여러 워크스테이션을 로밍할 수 있습니다. IBM Security Access Manager for Enterprise Single Sign-On은 VMware View와 같은 VDI(virtual desktop infrastructure) 기술도 보호합니다. 뿐만 아니라 IBM Security Access Manager for Enterprise Single Sign-On은 로밍 데스크탑 모드 및 Web Workplace를 통해 씬 클라이언트 액세스와 클라이언트 없는 액세스도 지원합니다.

솔루션 아키텍처

IBM Security Access Manager for Enterprise Single Sign-On은 한 번만 사용자를 인증하면 이후 사용자 신임 정보의 인식 및 처리를 자동으로 해결하는 계층을 추가하는 방법으로 SSO 기능을 제공합니다.

그림 1과 같이 IBM Security Access Manager for Enterprise Single Sign-On은 다음 아키텍처 구성요소로 나눌 수 있습니다.

- 인증 요소

  IBM Security Access Manager for Enterprise Single Sign-On은 사용자 인증을 위해 다양한 인증 요소를 지원합니다. 표준 사용자 이름 및 비밀번호 기반 인증 외에도 근접성 또는 출입증을 통한 사용자 인증도 가능합니다. 예를 들면 액티브/패시브 RFID, 지문 인식, SMS(Short Message Service)나 OTP(one-time password) 토큰 기반 OTP, USB 토큰 등이 있습니다.

- AccessAgent

  AccessAgent는 모든 Windows 데스크탑 엔드포인트, Windows Server Terminal Services 세션, VMware vSphere 가상 데스크탑 인터페이스 세션, Citrix XenApp Presentation Server 세션에서 실행됩니다. AccessAgent는 사용자 인증을 담당합니다. Windows와 AccessProfile에 정의된 애플리케이션에 대한 SSO를 자동화할 수 있습니다. AccessAgent는 Windows GINA(Graphical Identification and Authentication) 동적 링크 라이브러리(DLL) 체인을 확장하여 셀프 서비스 또는 강력 인증 기능을 추가로 제공할 수 있습니다.

- Identity Wallet

  Identity Wallet(또는 Wallet)은 SSO에 필요한 사용자 신임 정보를 저장합니다. 사용자 인증이 성공하면 IBM IMS™ Server에서 AccessAgent로 로드되므로, 엔드포인트와 컴퓨터 네트워크의 연결이 끊긴 상태에서도 사용 가능합니다. Identity Wallet은 신임 정보의 변조 또는 도용을 방지하기 위해 강력 암호화 메커니즘을 사용하여 암호화됩니다.

- IMS Server

  IMS Server는 사용자 데이터, AccessProfile, Identity Wallet, 시스템 프로파일의 중앙 저장소입니다. IMS Server는 사용자와 정책을 관리할 수 있는 웹 기반 인터페이스를 제공합니다.

사용 시나리오

이 시나리오에서는 한 의료 서비스 기업이 여러 곳의 독립적 진료소를 운영하고 각 진료소는 자체 건물에서 예방 치료, 심장 수술, 외래 진료를 실시합니다. 이 회사에서 직접 채용한 다수의 의료진과 지원 인력 그리고 회사와 계약한 소그룹의 독립 외과의가 일하고 있습니다.

이 기업은 재무 데이터 및 비공개 고객 데이터(환자, 연구 파트너, 제휴 병원 등)를 관리합니다. 대부분의 기록이 SAP 시스템에서 전자 형식으로 보존되어 있습니다. 또한 사내 및 사외(환자 및 외부 파트너) 커뮤니케이션을 위해 전 직원 대상의 이메일 발송이 가능합니다.

그림 2는 개별 네트워크 영역 간 주요 통신 회선을 포함하여 이 의료 서비스 기업의 아키텍처 다이어그램을 보여 줍니다.

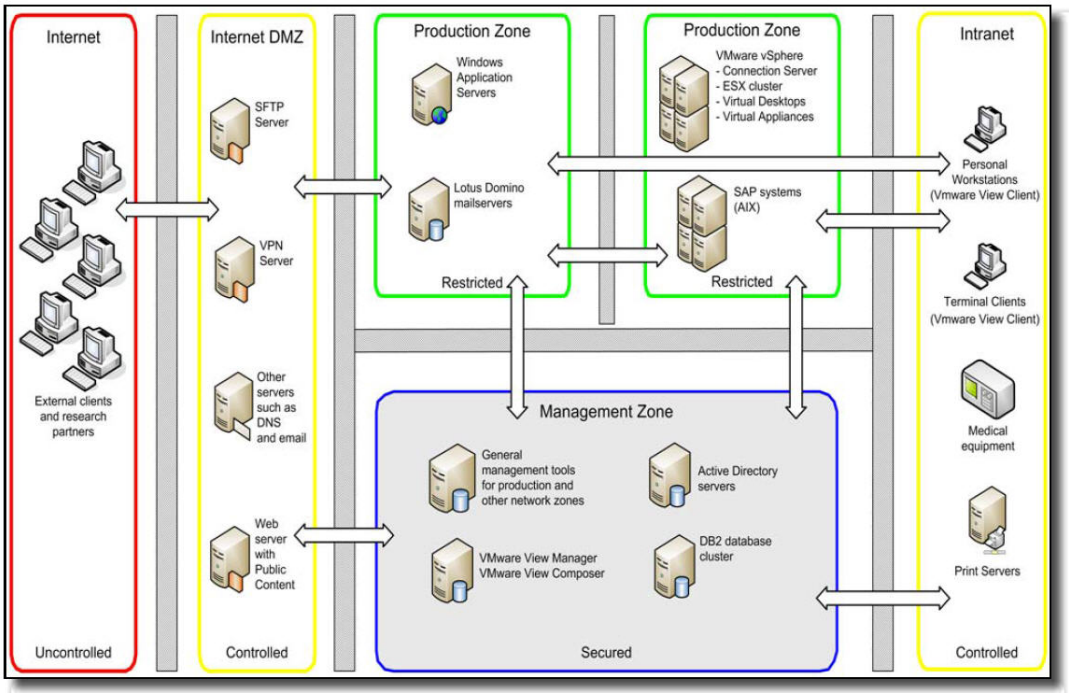

그림 2. 이 의료 서비스 기업의 현재 아키텍처 개요

이 기업은 단기적으로 다음 비즈니스 목표를 달성하려 합니다.

- 우수한 개인별 맞춤 의료 서비스를 제공하여 환자 진료의 품질과 가용성 그리고 만족도 향상
- 모든 환자 관련 정보의 보호 강화, 컴플라이언스 요건, 새로운 기술, 폭발적인 데이터 증가에 따른 각종 보안 위험 해결
- HIPAA(Health Insurance Portability and Accountability Act), PCI-DSS(Payment Card Industry Data Security Standard)와 같은 개인정보보호법 및 산업 규정에 대한 종합적인 컴플라이언스 관리 및 입증

이 기업은 전반적으로 완성된 보안 솔루션을 구축하여 정보 유출을 방지하고 환자에게 영향을 미칠 모든 활동에 대해 신뢰할 만한 인증 체계를 구축하고 개별적인 추적 및 책임 소재 규명을 지원하려 합니다.

IBM Security Access Manager for Enterprise Single Sign-On의 기본적인 구현을 위해 다음 구성요소를 배치합니다.

- 중앙 사용자 저장소 또는 디렉토리

  중앙 사용자 저장소는 Active Directory, Novell, 일반 LDAP(Lightweight Directory Access Protocol)와 같이 지원되는 여러 저장소 중 하나를 사용하면 됩니다. IBM Security Access Manager for Enterprise Single Sign-On 구성요소를 설치하기 전에 중앙 사용자 저장소가 마련되어야 합니다. 이 의료 서비스 기업의 환경에서는 그림 2와 같이 Active Directory가 중앙 사용자 저장소입니다.

- IMS Server

  IMS Server는 Java 기반 애플리케이션이며, 각자의 IBM WebSphere® Application Server의 인스턴스에서 실행됩니다. Windows 서버 플랫폼에 소프트웨어로 설치되거나 패키지 가상 어플라이언스에 통합될 수 있습니다. 그림 2와 같이 IMS Server는 관리 영역에 배치됩니다.

- IMS 데이터베이스

  IMS 데이터베이스는 IBM Security Access Manager for Enterprise Single Sign-On을 위한 모든 구성, 정책과 사용자 데이터를 저장합니다. 이 데이터베이스는 기존 데이터베이스 서버에서 생성하거나 IMS Server와 동일한 시스템에 설치할 수 있습니다. IBM DB2®, Microsoft SQL, Oracle과 같은 데이터베이스를 지원합니다. 이 의료 서비스 기업의 환경에서는 그림 2와 같이 기존 DB2 데이터베이스를 사용합니다.

- AccessAgent

  AccessAgent는 IBM Security Access Manager for Enterprise Single Sign-On으로 관리할 각 클라이언트 시스템, Windows Terminal Server, VMware Virtual Desktop, Citrix XenApp 서버에 설치합니다.

- AccessStudio

  AccessStudio는 AccessProfile을 생성하는 데 사용하는 관리 도구입니다. 단 하나의 워크스테이션에, 주로 한 명 이상의 IMS Server 관리자가 사용하는 워크스테이션에 설치해야 합니다. AccessStudio는 AccessAgent를 필요로 하므로 AccessStudio를 설치하기에 앞서 동일한 워크스테이션에 AccessAgent를 설치합니다.

이 기업은 기본 인프라 구성요소를 배치한 후 다음 기능을 구현합니다.

- 비밀번호 셀프 서비스

  이 의료 서비스 기업의 사용자는 Microsoft Windows 비밀번호를 잊어버린 경우 IT 지원 데스크에 연락해야 합니다. 그러면 지원 데스크의 담당자가 필수 보안 점검을 수행한 다음 사용자를 대신하여 비밀번호를 초기화합니다. IBM Security Access Manager for Enterprise Single Sign-On은 비밀번호 셀프 서비스 기능을 통해 이 문제를 해결합니다. IMS Server에 연결 가능한 사용자는 직접 비밀번호를 초기화할 수 있습니다.

  사용자는 IBM Security Access Manager for Enterprise Single Sign-On의 비밀번호 셀프 서비스 기능을 통해 어떤 워크스테이션에서도 시도-응답(challenge-response) 프로세스를 거쳐 기본 인증을 초기화할 수 있습니다. 기본 인증 방식은 IBM Security Access Manager for Enterprise Single Sign-On 비밀번호 또는 데스크탑 비밀번호가 될 수 있습니다. 모든 질문은 사용자 정의 및 구성 가능합니다. IBM Security Access

Manager for Enterprise Single Sign-On 비밀번호 셀프 서비스가 구성된 경우(추가적인 구성요소의 설치 불필요) 사용자는 기술 지원 팀에 연락하지 않아도 됩니다. 그리고 관리자가 비밀번호를 초기화할 때까지 기다릴 필요도 없습니다. 즉 사용자는 AccessAgent의 등록 단계에서 설정했던 2차 본인 확인 정보를 제시합니다. 비밀번호 셀프 서비스 기능을 사용하기 위해 추가적인 구성요소를 설치할 필요 없습니다.

- RFID를 사용하는 강력 인증

  이 의료 서비스 기업은 의료진에게 안전하고 *빠른 사용자 전환* 기능을 제공하려 합니다. 병원 내 각처에 배치된 공유 터미널 클라이언트의 사용자에게는 더 빠르고 편리한 시스템 로그온 방법이 필요합니다. 의료진은 다음 환자를 진료하기에 앞서 현재 환자의 기록에 몇 가지 간단한 소견을 추가하여 업데이트해야 합니다. 또한 매일 가상 데스크탑 환경에 액세스하기 위해 수 차례 사용자 이름과 (복잡한) 비밀번호를 입력해야 하므로, 이는 불만 요인으로 작용하고 있습니다. 이 고객은 이 문제의 해결에 나서되 보안의 절충은 허용하지 않을 것입니다.

  이 의료 서비스 기업은 모든 공유 터미널 클라이언트에 RFID 출입증리더를 배치하는 방법을 선택했습니다. 의료진은 이 기능을 사용하여 RFID 출입증을 SSO 사용자 이름 및 비밀번호와 연결할 수 있습니다. 의료진이 매일 한 번씩 RFID 출입증과 비밀번호를 제시하도록 정책이 설계되었습니다. 그러면 남은 일과에서는 리더기에 RFID 출입증을 갖다대면 자동으로 SSO Wallet에 로그온됩니다.

- 로밍 데스크탑 구현

  사용자가 반공용 구역의 공유 워크스테이션에서 비밀번호 또는 RFID 출입증을 사용하여 로그온하면 자동으로 이 사용자의 Virtual Desktop과 연결됩니다. 이 Virtual Desktop에 사용자를 로그온하는 프로세스는 안전하고 변조 불가한 방법으로 이루어져야 합니다.

  Virtual Desktop에 로그온한 사용자는 인증 신임 정보를 제공하지 않고도 애플리케이션을 사용할 수 있어야 합니다. 마치 이 애플리케이션이 연결의 시작점이 공유 워크스테이션에 실행되는 것처럼 작동해야 합니다. 사용자가 공유 워크스테이션에서 로그오프하더라도 로밍 가상 데스크탑과 그 애플리케이션은 계속 가상 인프라에서 실행되어야 합니다. 공유 워크스테이션 비활성 정책은 최대한 엄격하게 설정함으로써 유휴 상태 Virtual Desktop 세션에 대한 무단 액세스를 차단해야 합니다. 비활성 세션은 자동으로 종료해야 합니다.

  의료진은 분산 배치된 워크스테이션에서 RFID 출입증을 통해 자동으로 로그온하고 VMware ESXi Server에서 호스팅되는 가상 데스크탑에 연결합니다. 그림 3은 목표로 삼은 솔루션 구성요소 아키텍처를 보여 줍니다.

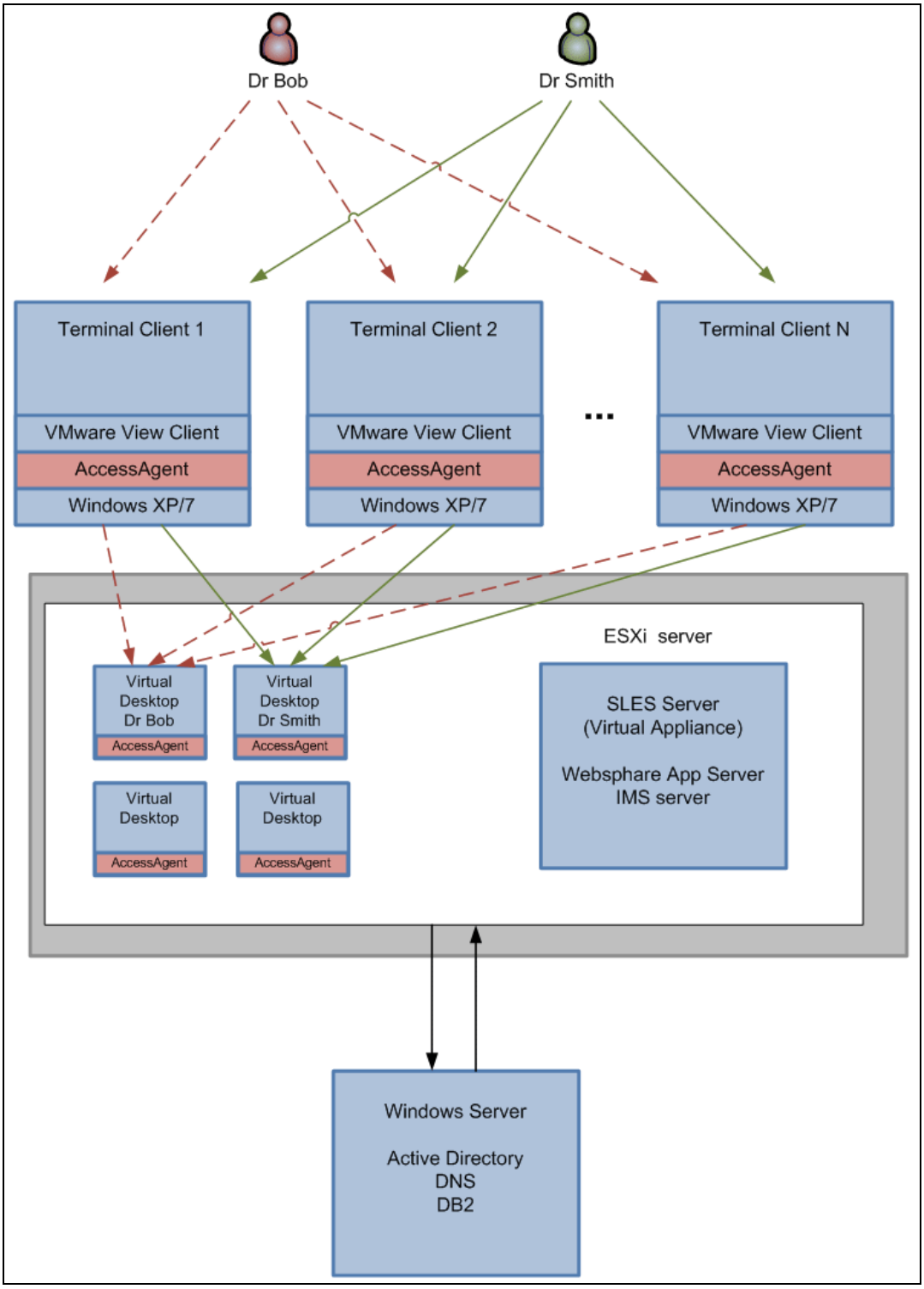

그림 3. 로밍 데스크탑 아키텍처

주문 정보

이 제품은 IBM Passport Advantage®를 통해서만 구입하실 수 있습니다. 박스(shrink-wrapped) 제품으로는 공급되지 않습니다. 자세한 주문 정보는 IBM 발표문("관련 정보" 섹션)을 참조하십시오.

관련 정보

자세한 정보는 다음 문서에서 확인하십시오.

- *Enterprise Single Sign-On Design Guide Using IBM Security Access Manager for Enterprise Single Sign-On 8.2*, SG24-7350
  http://www.redbooks.ibm.com/abstracts/sg247350.html?Open

- *BIO-key Biometric Service Provider for IBM Security Access Manager for Enterprise Single Sign-On*, REDP-4892
  http://www.redbooks.ibm.com/abstracts/redp4892.html?Open

- *A Guide to Authentication Services in IBM Security Access Manager for Enterprise Single Sign-On*, REDP-4835
  http://www.redbooks.ibm.com/abstracts/redp4835.html?Open

- *A Guide to Writing Advanced Access Profiles for IBM Tivoli Access Manager for Enterprise Single Sign-On*, REDP-4767
  http://www.redbooks.ibm.com/abstracts/redp4767.html?Open

- *Setup and Configuration for IBM Tivoli Access Manager for Enterprise Single Sign-On 8.1 for Single-Server and Cluster Environments*, REDP-4700
  http://www.redbooks.ibm.com/abstracts/redp4700.html?Open

- IBM Security Access Manager for Enterprise Single Sign-On 제품 페이지
  http://www.ibm.com/software/tivoli/products/access-mgr-esso

- IBM 발표문 및 판매 매뉴얼
  http://www.ibm.com/common/ssi/index.wss?request_locale=en

  이 페이지에서 `IBM Security Access Manager for Enterprise Single Sign-On`을 입력하고 **Search**를 클릭하십시오. 다음 페이지에서 정보 유형, 지역, 언어 또는 이 세 가지 옵션을 모두 적용하여 검색 범위를 한정하십시오.

주의사항

이 정보는 미국에서 제공되는 제품과 서비스를 대상으로 개발된 것입니다.

IBM은 이 문서에서 언급된 제품, 서비스 또는 기능을 다른 국가에서 제공하지 않을 수도 있습니다. 한국에서 사용 가능한 제품 및 서비스에 대해서는 한국 IBM 담당자에게 문의하십시오. IBM 제품, 프로그램 또는 서비스를 언급했다고 해서 해당 IBM 제품, 프로그램 또는 서비스만을 사용할 수 있다는 것을 의미하지는 않습니다. IBM의 지적 재산권을 침해하지 않고 기능상 동등한 제품, 프로그램 또는 서비스를 대신 사용할 수 있습니다. 그러나 비IBM 제품, 프로그램 또는 서비스의 운영에 대한 평가 및 검증은 사용자의 책임입니다. IBM은 이 문서에서 다루고 있는 특정 내용에 대해 특허를 보유하고 있거나 현재 특허 출원 중일 수 있습니다. 이 문서를 제공한다고 해서 특허에 대한 라이센스까지 부여하는 것은 아닙니다. 라이센스에 대한 의문사항은 다음으로 문의하십시오.

135-700 서울특별시 강남구 도곡동 467-12 군인공제회관빌딩 한국 아이.비.엠 주식회사

다음 단락은 현지법과 상충하는 영국이나 기타 국가에서는 적용되지 않습니다. IBM은 타인의 권리 비침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 어떠한 종류의 보증 없이 이 발행물을 "현상태대로" 제공합니다. 일부 국가에서는 특정 거래에서 명시적 또는 묵시적 보증의 면책사항을 허용하지 않으므로, 이 사항이 적용되지 않을 수도 있습니다. 이 정보에는 기술적으로 부정확한 내용이나 인쇄상의 오류가 있을 수 있습니다. 이 정보는 주기적으로 변경되며, 변경된 사항은 최신판에 통합됩니다. IBM은 이 발행물에서 설명한 제품 및/또는 프로그램을 사전 통지 없이 언제든지 개선 및/또는 변경할 수 있습니다.

이 정보에서 언급되는 비IBM의 웹 사이트는 단지 편의상 제공된 것으로, 어떤 방식으로든 이들 웹 사이트를 옹호하고자 하는 것은 아닙니다. 해당 웹 사이트의 자료는 본 IBM 제품 자료의 일부가 아니므로 해당 웹 사이트 사용으로 인한 위험은 사용자 본인이 감수해야 합니다. IBM은 귀하의 권리를 침해하지 않는 범위 내에서 적절하다고 생각하는 방식으로 귀하가 제공한 정보를 사용하거나 배포할 수 있습니다. 비IBM 제품에 관한 정보는 해당 제품의 공급업체, 공개 자료 또는 기타 범용 소스로부터 얻은 것입니다. IBM에서는 이러한 제품들을 테스트하지 않았으므로, 비IBM 제품과 관련된 성능, 호환성, 기타 주장의 정확성을 확신할 수 없습니다. 비IBM 제품의 성능에 대한 의문사항은 해당 제품의 공급업체에 문의하십시오.이 정보에는 일상의 비즈니스 운영에서 사용되는 자료 및 보고서에 대한 예제가 들어 있습니다. 이들 예제에는 개념을 가능한 완벽하게 설명하기 위하여 개인, 회사, 상표 및 제품의 이름이 사용될 수 있습니다. 이들 이름은 모두 가공의 것이며 실제 기업의 이름 및 주소와 유사하더라도 이는 전적으로 우연입니다.

본 문서에 포함된 모든 성능 데이터는 제한된 환경에서 산출된 것입니다. 따라서 다른 운영 환경에서 얻어진 결과는 상당히 다를 수 있습니다. 일부 성능은 개발 단계의 시스템에서 측정되었을 수 있으므로 이러한 측정치가 일반적으로 사용되고 있는 시스템에서도 동일하게 나타날 것이라고는 보증할 수 없습니다. 또한 일부 성능은 추정을 통해 추측되었을 수도 있으므로 실제 결과는 달라질 수 있습니다. 이 문서의 사용자는 해당 데이터를 본인의 특정 환경에서 검증해야 합니다.

저작권 라이센스:

이 정보에는 여러 운영 플랫폼에서의 프로그래밍 기법을 보여 주는 원어로 된 샘플 응용프로그램이 들어 있습니다. 귀하는 이러한 샘플 프로그램의 작성 기준이 된 운영 플랫폼의 응용프로그램 프로그래밍 인터페이스(API)에 부합하는 응용프로그램을 개발, 사용, 판매 또는 배포할 목적으로 추가 비용 없이 이들 샘플 프로그램을 어떠한 형태로든 복사, 수정 및 배포할 수 있습니다. 이러한 샘플 프로그램은 모든 조건하에서 완전히 테스트된 것은 아닙니다. 따라서 IBM은 이들 샘플 프로그램의 신뢰성, 서비스 가능성 또는 기능을 보증하거나 진술하지 않습니다.

이 문서는 2012년 12월 7일에 작성되었거나 업데이트되었습니다.

다음 방법 중 하나를 이용하여 의견을 보내주십시오.

- 온라인 **문의** 리뷰 양식:
  ibm.com/redbooks
- 이메일:
  ibmkspoe@kr.ibm.com
- 우편:
  135-700
  서울특별시 강남구 도곡동 467-12 군인공제회관빌딩
  한국 아이.비.엠 주식회사
  고객만족센터

이 백서는 **ibm.com**/redbooks/abstracts/tips0943.html에서 온라인으로 이용할 수 있습니다.

상표