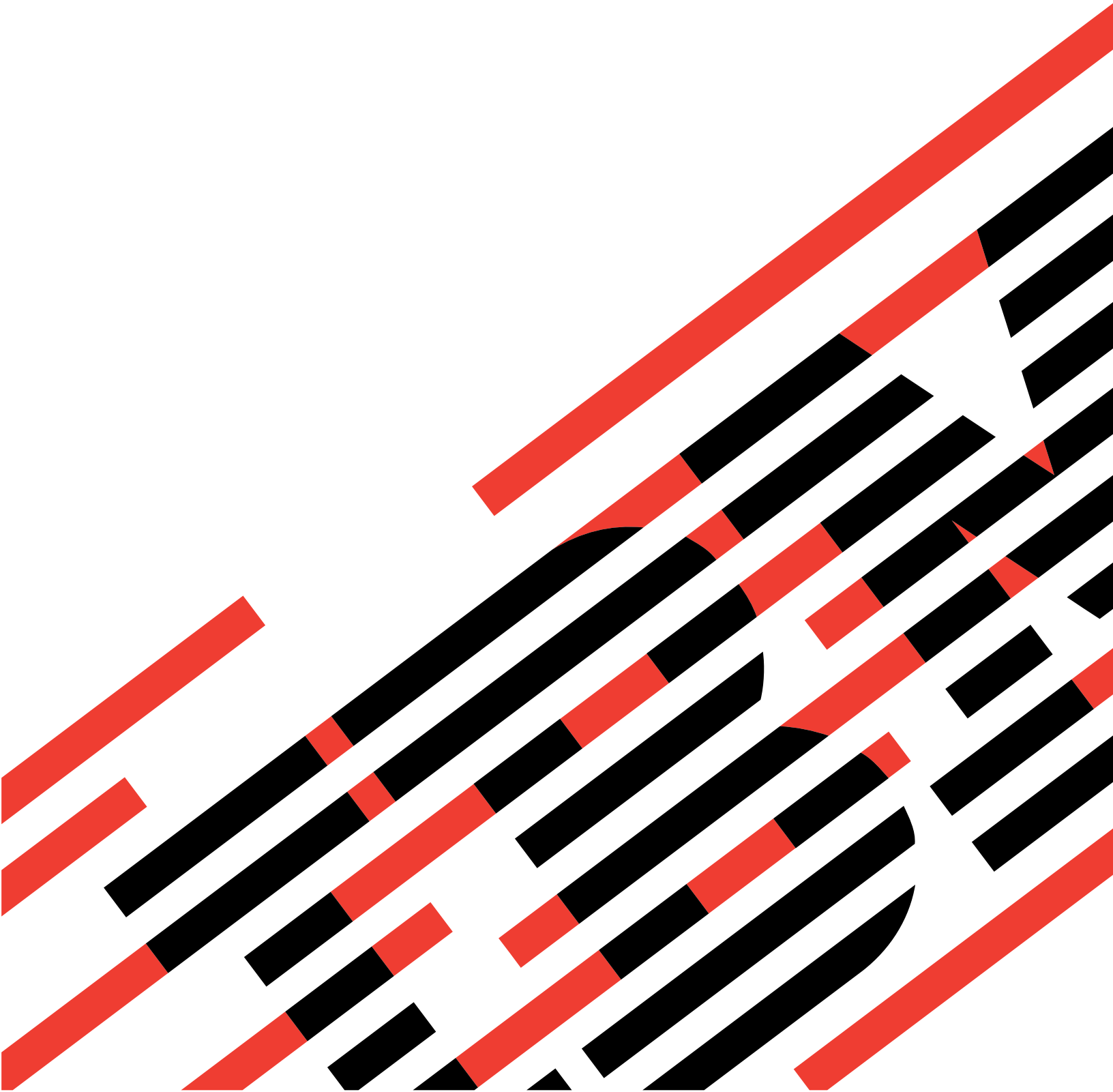
IBM

eserver

iSeries

SSL(Secure Sockets Layer)

버전 5 릴리스 3



IBM

@server

iSeries

SSL(Secure Sockets Layer)

버전 5 릴리스 3

주!

이 정보와 이 정보가 지원하는 제품을 사용하기 전에, 21 페이지의 『주의사항』의 정보를 읽으십시오.

제 5 판(2005년 8월)

이 개정판은 새 개정판에서 별도로 명시하지 않는 한 IBM Operating System/400(프로그램 번호 5722-SS1)의 버전 5, 릴리스 3, 수정 0 및 모든 후속 릴리스와 수정에 적용됩니다. 이 버전은 모든 축약 명령어 세트 컴퓨터(RISC) 모델에서 실행되는 것은 아니며 CISC 모델에서도 실행되지 않습니다.

목차

SSL(Secure Sockets Layer)

SSL(Secure Sockets Layer)은 인터넷처럼 보호되지 않는 네트워크에서 어플리케이션의 안전한 통신 세션을 가능하게 하는 산업 표준으로 현재 사용되고 있습니다. SSL 및 iSeries™ 서버 어플리케이션에 대한 자세한 정보를 보려면 다음 링크로 가십시오.

- **V5R3의 새로운 사항**
  SSL과 관련하여 사용할 수 있는 새로운 기능이나 새 정보에 대해 설명합니다.
- **SSL 시나리오**
  - SSL에 대한 새로운 추가 정보로서, SSL이 제공하는 기능과 관련된 여러 가지 예를 통해 iSeries 서버의 SSL을 쉽게 이해할 수 있도록 구성되어 있습니다.
- **SSL 개념**
  SSL 프로토콜의 몇 가지 기본 구성 원칙을 제공하는 보충 정보가 있습니다.
- **SSL 작동 계획**
  - iSeries 서버에서 SSL을 작동시키기 위한 전제조건과 여러 가지 유용한 추가 정보가 포함되어 있습니다.
- **SSL을 사용한 어플리케이션 보안**
  - iSeries 서버에서 SSL을 사용하여 보안을 유지할 수 있는 어플리케이션 리스트가 포함되어 있습니다.
- **SSL 문제 해결**
  - iSeries 서버에서 SSL 문제 해결 절차를 시작하는 방법에 대한 기본 안내서입니다.
- **SSL 관련 정보**
  - 사용자를 위한 추가 정보 자원에 대한 링크가 포함되어 있습니다.

V5R3의 새로운 사항

SSL의 현재 릴리스와 관련하여 주의해야 할 두 가지 새로운 항목이 있습니다.

1. 시나리오: SSL을 사용하여 중앙 관리 서버에 대한 클라이언트 연결 보안

   리모트 클라이언트와 iSeries 서버의 중앙 관리 서버(근거리 통신망(LAN)에 지정된 중앙 시스템) 간 연결을 보안하기 위해 SSL을 사용하는 방법을 설명하는 새로운 시나리오입니다.

2. GSKit API의 GSKit 6B 버전

   V5R3 이후 GSKit API는 GSKit 6B 버전을 기초로 합니다. 이전 릴리스에서는 GSKit 4D 버전을 기초로 하였습니다. GSKit API에 대한 자세한 정보는 여기를 클릭하십시오.

이 릴리스의 새로운 사항이나 변경사항에 대한 기타 정보를 보려면 사용자 메모 를 참조하십시오.

새로운 사항 또는 변경 사항 확인 방법

이 정보는 기술적인 변경사항을 참조할 수 있도록 다음과 같이 사용됩니다.

- » 이미지 - 새로운 정보 또는 변경 정보가 시작되는 위치를 표시합니다.

- « 이미지 - 새로운 정보 또는 변경 정보가 끝나는 위치를 표시합니다.

이 주제 인쇄

본 정보를 PDF 버전으로 보거나 다운로드할 수 있습니다. 이를 수행하려면 SSL(Secure Sockets Layer)(약 243KB)을 선택하십시오.

기타 정보

이 주제에 대한 모든 관련 정보를 보거나 인쇄할 수도 있습니다.

PDF 파일 저장

PDF를 워크스테이션에 저장하여 보거나 인쇄하려면 다음을 수행하십시오.
1. 브라우저에서 PDF를 마우스 오른쪽 버튼으로 클릭하십시오.
2. **다른 이름으로 대상 저장**을 클릭하십시오.
3. PDF를 저장하려는 디렉토리를 탐색하십시오.
4. **저장**을 클릭하십시오.

Adobe Acrobat Reader 다운로드

이 정보를 보거나 인쇄하기 위해 Adobe Acrobat Reader가 필요한 경우 Adobe 웹 사이트 (www.adobe.com/products/acrobat/readstep.html) 에서 사본을 다운로드할 수 있습니다.

시나리오

다음은 iSeries 서버에서 SSL을 작동할 때 얻는 장점을 최대화할 수 있도록 고안된 시나리오입니다.

- 시나리오: SSL을 사용하여 중앙 관리 서버에 대한 클라이언트 연결 보안

  이 시나리오에서는 iSeries Navigator 중앙 관리 서버를 사용하여 중앙 시스템 역할을 하는 iSeries 서버와 리모트 클라이언트 간 연결을 보안하기 위해 SSL을 사용하는 방법을 설명합니다.
- 시나리오: SSL을 사용하여 중앙 관리 서버에 대한 모든 연결 보안

  이 시나리오에서는 iSeries Navigator 중앙 관리 서버를 사용하여 중앙 시스템 역할을 하는 iSeries 서버에 대한 **모든** 연결을 보안하기 위해 SSL을 사용하는 방법을 설명합니다.
- 시나리오: SSL을 사용한 FTP 보안

  이 시나리오에서는 FTP 어플리케이션에 SSL을 작동시키는 방법을 설명합니다.
- 시나리오: SSL을 사용한 Telnet 보안

  이 시나리오에서는 Telnet 어플리케이션에 SSL을 작동시키는 방법을 설명합니다.
- 시나리오: iSeries SSL 성능 향상

이 시나리오에서는 iSeries 서버에서 SSL 성능을 향상시키기 위해 암호 하드웨어를 사용하는 방법을 설명합니다.

- 시나리오: 암호 하드웨어를 사용한 개인 키 보호

  이 시나리오에서는 iSeries 서버의 SSL 트랜잭션과 연관된 개인 키를 보호하기 위해 암호 하드웨어를 사용하는 방법을 설명합니다.

시나리오: SSL을 사용하여 중앙 관리 서버에 대한 클라이언트 연결 보안

상황:

사무실에 iSeries 서버가 여러 대 있는 근거리 통신망(LAN)을 갖춘 회사가 있습니다. 이 회사의 시스템 관리자인 Bob은 iSeries 서버 중 하나를 LAN의 중앙 시스템(이후 시스템 A라고 함)으로 지정했습니다. Bob은 시스템 A의 중앙 관리 서버를 사용하여 LAN에 있는 나머지 모든 엔드포인트을 관리합니다.

Bob은 회사 LAN의 외부에 있는 네트워크 연결에서 시스템 A의 중앙 관리 서버에 연결하는 문제를 걱정하고 있습니다. 출장이 잦은 Bob은 자리를 비운 동안 중앙 관리 서버에 안전하게 연결해야 합니다. 그는 회사 사무실에 없을 때 자신의 PC와 중앙 관리 서버 간의 연결 보안을 유지하려고 합니다. Bob은 자신의 PC와 시스템 A의 중앙 관리 서버에 SSL을 작동시키기로 결정했습니다. 이런 방식으로 SSL을 작동시키면 Bob은 출장 중에 중앙 관리 서버로 안전하게 연결할 수 있습니다.

목적

Bob은 자신의 PC와 중앙 관리 서버 간의 연결 보안을 원합니다. 그러나 시스템 A의 중앙 관리 서버와 LAN에 있는 엔드포인트 간 연결을 위한 추가 보안은 필요로 하지 않습니다. 회사 사무실에서 근무하는 다른 직원들도 중앙 관리 서버에 연결하기 위해 추가 보안이 필요하지 않습니다. Bob의 계획은 자신의 클라이언트 연결에 서버 인증이 사용되도록 자신의 PC와 시스템 A의 중앙 관리 서버를 구성하는 것입니다. LAN의 iSeries 서버나 다른 PC에서 중앙 관리 서버로의 연결은 SSL을 통해 보안되지 않습니다.

세부사항

다음 표는 PC 클라이언트의 SSL 작동 가능 또는 작동 불가능에 따라 사용되는 인증 유형을 보여줍니다.

표 1. 클라이언트와 중앙 관리 서버 간 SSL 보안 연결에 필요한 요소

Bob PC의 SSL 상태	시스템 A의 중앙 관리 서버에 지정한 인증 레벨	SSL 연결 작동 가능?
SSL Off	모두	아니오
SSL On	모두	예(서버 인증)

서버 인증은 Bob의 PC가 중앙 관리 서버의 인증서를 인증함을 의미합니다. Bob의 PC는 중앙 관리 서버에 연결할 때 SSL 클라이언트 역할을 합니다. 중앙 관리 서버는 SSL 서버로 작동하며 ID를 증명해야 합니다. 중앙 관리 서버는 Bob의 PC가 신뢰하는 CA(Certificate Authority)에서 발행한 인증서를 제공함으로써 ID를 증명합니다.

전제조건 및 가정

Bob은 자신의 PC와 시스템 A의 중앙 관리 서버 간 연결을 보안하기 위해 다음과 같은 관리 및 구성 타스크를 수행해야 합니다.

1. 시스템 A가 SSL의 전제조건을 충족시킵니다(SSL 전제조건 참조)
2. OS/400® V5R3 이상 버전을 시스템 A에 설치합니다. 시스템 A에서 OS/400 V5R1을 실행할 경우 다음과 같은 OS/400(5722-SS1)용 수정 프로그램(PTF)을 설치하십시오.
   a. SI01375
   b. SI01376
   c. SI01377
   d. SI01378
   e. SI01838
3. iSeries Navigator PC 클라이언트에서는 V5R3 이상 버전의 Windows®용 iSeries Access가 실행됩니다.
4. iSeries 서버에 대한 CA(Certificate Authority)를 확보하십시오.
5. 시스템 A에 대해 CA에서 서명한 인증서를 작성하십시오.
6. CA와 인증서를 시스템 A로 송신하고 키 데이터베이스로 가져오십시오.
7. 중앙 관리 서버 ID를 사용하여 인증서를 할당하십시오.
   a. 시스템 A에서 IBM® 디지털 인증 관리자를 시작하십시오. Bob은 인증서를 가져오거나 작성하고 그렇지 않으면 지금 자신의 인증 시스템을 설정하거나 변경합니다. 인증 시스템 설정 방법에 대한 정보는 디지털 인증 관리자 사용을 참조하십시오.
   b. **인증서 저장소 선택**을 클릭하십시오.
   c. ***SYSTEM**을 선택하고 **계속**을 클릭하십시오.
   d. *SYSTEM의 **인증서 저장소 암호**를 입력하고 **계속**을 클릭하십시오. 메뉴가 다시 로드되면 **어플리케이션 관리**를 펼치십시오.
   e. **인증서 지정 갱신**을 클릭하십시오.
   f. **서버**를 선택하고 **계속**을 클릭하십시오.
   g. **중앙 관리 서버**를 선택하고 **인증서 지정 갱신**을 클릭하십시오. 그렇게 하면 Windows용 iSeries Access 클라이언트의 ID를 설정하기 위해 중앙 관리 서버가 사용할 인증서가 할당됩니다.
   h. **신규 인증서 지정**을 클릭하십시오. DCM이 확인 메세지와 함께 **인증서 지정 갱신** 페이지에 다시 로드됩니다.
   i. **완료**를 클릭하십시오.
8. iSeries Navigator를 설정하십시오.
   a. 선택적으로 PC 클라이언트에 iSeries Navigator용 SSL 구성요소를 설치하십시오.
   b. CA를 PC 클라이언트에 다운로드하십시오.

구성 단계

Bob은 시스템 A의 중앙 관리 서버에 대한 PC 클라이언트 연결을 SSL로 보안하기 위해 다음 단계를 완료해야 합니다.

1. 1단계: iSeries Navigator 클라이언트에 대한 SSL 비활성화
2. 2단계: 중앙 관리 서버에 대한 인증 레벨 설정
3. 3단계: 시스템 A의 중앙 관리 서버 다시 시작
4. 4단계: iSeries Navigator 클라이언트에 대한 SSL 활성화
5. 선택적 단계: iSeries Navigator 클라이언트에 대한 SSL 비활성화

자세한 구성 단계를 보려면 SSL을 사용하여 중앙 관리 서버에 대한 클라이언트 연결 보안을 참조하십시오.

구성 세부사항: SSL을 사용하여 중앙 관리 서버에 대한 클라이언트 연결 보안

다음 정보에서는 시나리오: SSL을 사용하여 중앙 관리 서버에 대한 클라이언트 연결 보안을 읽은 것으로 간주합니다. 이 시나리오에서 iSeries 서버는 회사의 근거리 통신망(LAN)에 있는 중앙 시스템으로 지정됩니다. Bob은 회사 네트워크의 엔드포인트을 관리하기 위해 중앙 시스템의 중앙 관리 서버(여기에서는 시스템 A라고 함)를 사용합니다. 다음 정보는 중앙 관리 서버에 대한 외부 클라이언트 연결 보안에 필요한 단계를 수행하는 방법을 설명합니다. Bob을 따라 수행하면 시나리오 구성 단계가 완료됩니다.

Bob은 중앙 관리 서버에 SSL을 작동하기 전에 필수 프로그램을 설치하고 iSeries 서버에 디지털 인증서를 설정해야 합니다. 계속하기 전에 이 시나리오에 대한 전제조건 및 가정을 참조하십시오. 전제조건이 충족되면 다음 프로시듀어를 완료하여 중앙 관리 서버에 SSL을 작동시킬 수 있습니다.

1단계: iSeries Navigator 클라이언트에서 SSL 비활성화

1. iSeries Navigator에서 **연결**을 펼치십시오.
2. 시스템 A를 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
3. **보안 소켓** 탭을 클릭하고 **연결에 SSL 사용**을 선택 취소하십시오.
4. iSeries Navigator를 나간 다음 다시 시작하십시오.

iSeries Navigator의 중앙 관리 컨테이너에서 패드 로크가 사라져서 연결이 보안되지 않음을 나타냅니다. 이는 더 이상 Bob의 클라이언트와 회사의 중앙 시스템 사이에 SSL 보안 연결이 없음을 뜻합니다.

2단계: 중앙 관리 서버에 대한 인증 레벨 설정

1. iSeries Navigator에서 **중앙 관리**를 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
2. **보안** 탭을 클릭하고 **SSL(Secure Sockets Layer) 사용**을 선택하십시오.
3. 인증 레벨에 **모두**를 선택하십시오(V5R3 이상의 Windows용 iSeries Access에서 사용할 수 있음).
4. **확인**을 클릭하여 이 값을 중앙 시스템에 설정하십시오.

3단계: 중앙 시스템에서 중앙 관리 서버 다시 시작

1. iSeries Navigator에서 **연결**을 펼치십시오.
2. **시스템 A**에서 **네트워크 --> 서버**를 펼치고 **TCP/IP**를 선택하십시오.
3. **중앙 관리**를 마우스 오른쪽 버튼으로 클릭하고 **중단**을 선택하십시오. 중앙 시스템 보기가 접히고 서버에 연결되지 않았음을 설명하는 메세지가 표시됩니다.

4. 중앙 관리 서버가 중단되었으면 **시작**을 클릭하여 다시 시작하십시오.

4단계: iSeries Navigator 클라이언트에 대한 SSL 활성화

1. iSeries Navigator에서 **연결**을 펼치십시오.
2. 시스템 A를 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
3. **보안 소켓** 탭을 클릭하고 **연결에 SSL(Secure Sockets Layer) 사용**을 선택하십시오.
4. iSeries Navigator를 나간 다음 다시 시작하십시오.

iSeries Navigator의 중앙 관리 서버의 옆에 패드 로크가 나타납니다. 이는 Bob의 클라이언트와 회사의 중앙 시스템 사이에 SSL 보안 연결이 활성화되었음을 뜻합니다.

주: 이 프로시듀어는 하나의 PC와 중앙 관리 서버 간 연결만 보안합니다. 엔드포인트에서 중앙 관리 서버로의 연결뿐 아니라 중앙 관리 서버에 대한 다른 클라이언트 연결도 보안되지 않습니다. 다른 클라이언트를 보안하려면 전제조건을 충족시키는지 확인하고 4단계를 반복하십시오. 중앙 관리 서버와의 다른 연결을 보안하려면 시나리오: SSL을 사용하여 중앙 관리 서버에 대한 모든 연결 보안을 참조하십시오.

선택적 단계: iSeries Navigator 클라이언트에 대한 SSL 비활성화

Bob이 회사 사무실에서 근무하고 자신의 PC 성능에 영향을 미치는 SSL 연결을 원하지 않을 경우 다음 단계를 수행하면 SSL을 쉽게 비활성화할 수 있습니다.

1. iSeries Navigator에서 **연결**을 펼치십시오.
2. **중앙 관리**를 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
3. **보안 소켓** 탭을 클릭하고 **연결에 SSL 사용**을 선택 취소하십시오.
4. iSeries Navigator를 나간 다음 다시 시작하십시오.

iSeries Navigator의 중앙 관리 서버에서 패드 로크가 사라져서 연결이 보안되지 않음을 나타냅니다. 이는 더 이상 Bob의 PC 클라이언트와 시스템 A의 중앙 관리 서버 사이에 SSL 보안 연결이 없음을 뜻합니다.

다른 SSL 시나리오로 연결되는 링크에 대해서는 시나리오를 참조하십시오.

시나리오: SSL을 사용하여 중앙 관리 서버에 대한 모든 연결 보안

상황:

회사는 리모트 위치(엔드포인트)에 iSeries 서버가 여러 대 있는 광역 네트워크(WAN)를 방금 설치했습니다. 엔드포인트은 본사에 있는 하나의 iSeries 서버(중앙 시스템)에 의해 중앙에서 관리됩니다. Tom은 회사의 보안 전문가입니다. Tom은 회사 중앙 시스템의 중앙 관리 서버 및 모든 엔드포인트 서버와 클라이언트 간의 모든 연결을 보안하는 데 SSL을 사용하려고 합니다.

세부사항

Tom은 SSL을 사용하여 중앙 관리 서버에 대한 모든 연결을 **안전하게** 관리할 수 있습니다. 중앙 관리 서버에 SSL을 사용하기 위해 Tom은 중앙 시스템에 액세스할 때 사용하는 PC에서 Windows용 iSeries Access와 iSeries Navigator를 보안해야 합니다.

Tom은 두 가지 인증 레벨 중에서 선택합니다.

서버 인증

엔드포인트 시스템 서버 인증서의 인증을 제공합니다. 엔드포인트 시스템에 연결될 때 중앙 시스템이 SSL 클라이언트의 역할을 합니다. 엔드포인트 시스템은 SSL 서버의 역할을 하며, 중앙 시스템이 신뢰하는 인증 기관에서 발행한 인증서를 제공하여 ID를 증명해야 합니다. 모든 엔드포인트 시스템에는 신뢰할 수 있는 CA에서 발행한 유효한 인증서가 필요합니다.

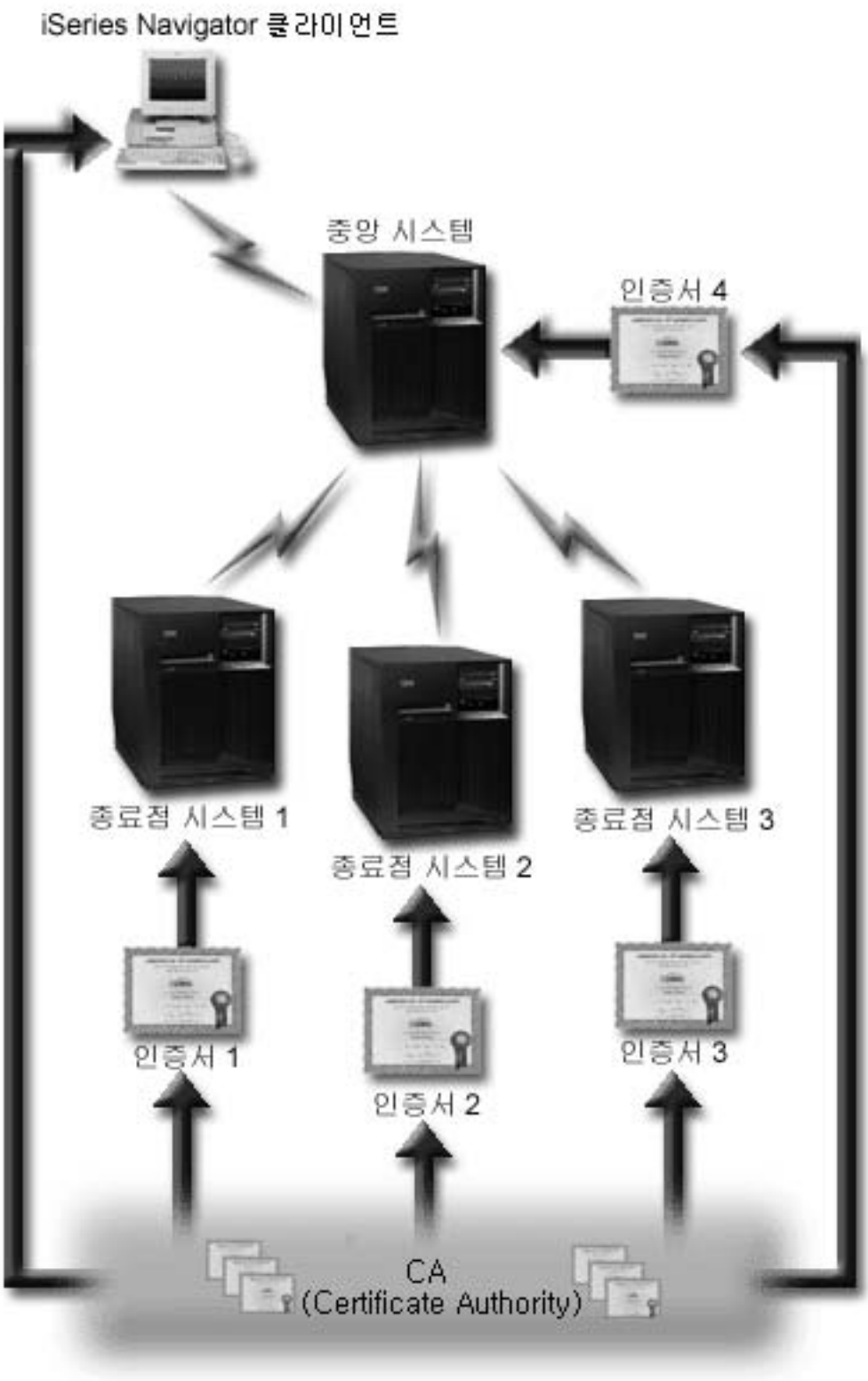
클라이언트 및 서버 인증

중앙 시스템 및 엔드포인트 시스템 모두의 인증서를 제공합니다. 이 인증은 서버 인증 레벨보다 강력한 보안 레벨입니다. 다른 어플리케이션에서는 이것을 클라이언트 인증이라고 하며, 이 인증을 통해 클라이언트가 신뢰할 수 있는 유효한 인증서를 제공해야 합니다. 중앙 시스템(SSL 클라이언트)이 엔드포인트 시스템(SSL 서버)에 연결을 시도할 때 중앙 시스템과 엔드포인트 시스템은 인증 기관의 신뢰성을 위해 서로의 인증서를 인증합니다.

기타 어플리케이션과 달리 중앙 관리는 신뢰할 수 있는 그룹의 유효성 리스트라고 하는 유효성 리스트를 통해서도 인증을 제공합니다. 일반적으로 유효성 리스트는 사용자 ID와 같이 사용자를 식별하는 정보 및 암호, 개인 ID 번호, 디지털 인증서와 같은 인증 정보를 저장합니다. 이 인증 정보는 암호화되어 있습니다.

서버 인증이 대개는 SSL 세션 작동 중에 발생하므로 대부분의 어플리케이션은 서버와 클라이언트 인증을 모두 작동하도록 지정하지 않습니다. 많은 어플리케이션에 클라이언트 인증 구성 옵션이 포함되어 있습니다. 중앙 관리는 네트워크에서 중앙 시스템이 담당하는 이중 역할로 인해 클라이언트 인증 대신에 ″서버 및 클라이언트 인증″이라는 용어를 사용합니다. PC 사용자가 중앙 시스템에 연결되고 SSL이 작동된 경우 중앙 시스템은 서버 역할을 합니다. 그러나 중앙 시스템이 엔드포인트 시스템에 연결되면 중앙 시스템은 클라이언트 역할을 합니다. 다음 그림은 중앙 시스템이 네트워크에서 서버와 클라이언트로서 어떻게 작동하는지를 보여줍니다.

주: 이 그림에서 인증 기관과 연관된 인증서는 중앙 시스템과 모든 엔드포인트 시스템의 키 데이터베이스에 저장되어야 합니다.


iSeries Navigator 클라이언트
중앙 시스템
인증서 4
종료점 시스템 1
종료점 시스템 2
종료점 시스템 3
인증서 1
인증서 2
인증서 3
CA
(Certificate Authority)

전제조건 및 가정

Tom은 중앙 관리 서버에 대한 모든 연결을 보안하기 위해 다음과 같은 관리 및 구성 타스크를 수행해야 합니다(이미지 SSL 보안 중앙 관리 WAN 참조).

1. 중앙 시스템이 SSL의 전제조건을 충족시킵니다(SSL 전제조건 참조).
2. 중앙 시스템과 모든 엔드포인트 iSeries 서버에서는 V5R2 이상의 OS/400 버전이 실행됩니다. 중앙 시스템과 엔드포인트에서 OS/400 V5R1이 실행될 경우 다음과 같은 OS/400(5722-SS1)용 수정 프로그램(PTF)을 설치하십시오.
   a. SI01375
   b. SI01376
   c. SI01377
   d. SI01378
   e. SI01838
3. iSeries Navigator PC 클라이언트에서는 V5R2 이상의 Windows용 iSeries Access가 실행됩니다. 클라이언트가 V5R1을 사용하는 경우 Windows용 iSeries Access V5R1(5722-XE1)용 서비스 팩 PTF SI01907 이상을 설치하십시오.
4. iSeries 서버에 대한 CA(Certificate Authority)를 확보하십시오.
5. SSL 작동 중앙 관리 서버가 관리하는 각 iSeries 서버에 대해 CA에서 서명한 인증서를 작성하십시오.
6. CA 및 인증서를 각 iSeries 서버에 송신하고 키 데이터베이스로 가져오십시오.
7. iSeries Navigator가 사용하는 모든 엔드포인트 서버에 대한 중앙 관리 어플리케이션 ID와 어플리케이션 ID를 사용하여 인증서를 할당하십시오.
   a. 중앙 서버에서 IBM 디지털 인증 관리자를 시작하십시오. 인증서를 확보 또는 작성해야 하거나 인증 시스템을 설정 또는 변경해야 하는 경우에는 지금 처리하십시오. 인증 시스템 설정에 대한 정보는 디지털 인증 관리자 사용을 참조하십시오.
   b. **인증서 저장소 선택**을 클릭하십시오.
   c. ***SYSTEM**을 선택하고 **계속**을 클릭하십시오.
   d. *SYSTEM의 **인증서 저장소 암호**를 입력하고 **계속**을 클릭하십시오. 메뉴가 다시 로드되면 **어플리케이션 관리**를 펼치십시오.
   e. **인증서 지정 갱신**을 클릭하십시오.
   f. **서버**를 선택하고 **계속**을 클릭하십시오.
   g. **중앙 관리 서버**를 선택하고 **인증서 지정 갱신**을 클릭하십시오. 사용하려는 중앙 관리 서버에서 인증서를 지정합니다.
   h. **신규 인증서 지정**을 클릭하십시오. DCM이 확인 메세지와 함께 **인증서 지정 갱신** 페이지에 다시 로드됩니다.
   i. **완료**를 클릭하십시오.
   j. iSeries Navigator가 사용하는 모든 엔드포인트 서버에 대해 이 절차를 반복하십시오.
8. iSeries Navigator를 설정하십시오.

a. 선택적으로 PC 클라이언트에 iSeries Navigator용 SSL 구성요소를 설치하십시오.

b. CA를 PC 클라이언트에 다운로드하십시오.

구성 단계

Tom은 중앙 관리 서버에서 SSL을 작동하기 전에 필수 프로그램을 설치하고 중앙 시스템에 디지털 인증을 설정해야 합니다. 계속하기 전에 이 시나리오에 대한 전제조건 및 가정을 참조하십시오. 전제조건이 충족되면 다음 프로시듀어를 완료하여 중앙 관리 서버로의 모든 연결을 보안할 수 있습니다.

주: iSeries Navigator에 SSL이 작동되도록 설정한 경우 Tom은 SSL을 작동 불가능하게 한 후 중앙 관리 서버에서 SSL을 작동시켜야 합니다. 중앙 관리 서버가 아니라 iSeries Navigator에 SSL이 작동되도록 설정한 경우 iSeries Navigator가 중앙 시스템에 연결되지 않습니다.

- 1단계: 서버 인증을 위한 중앙 시스템 구성
- 2단계: 서버 인증을 위한 엔드포인트 시스템 구성
- 3단계: 중앙 시스템에서 중앙 관리 서버 다시 시작
- 4단계: 모든 엔드포인트 시스템에서 중앙 관리 서버 다시 시작
- 5단계: iSeries Navigator 클라이언트에 대한 SSL 활성화
- 6단계: 클라이언트 인증을 위한 중앙 시스템 구성
- 7단계: 클라이언트 인증을 위한 엔드포인트 시스템 구성
- 8단계: 엔드포인트 시스템에 유효성 리스트 복사
- 9단계: 중앙 시스템에서 중앙 관리 서버 다시 시작
- 10단계: 모든 엔드포인트 시스템에서 중앙 관리 서버 다시 시작

확장된 구성 단계를 보려면 구성 세부사항: SSL을 사용하여 중앙 관리 서버에 대한 모든 연결 보안을 참조하십시오.

구성 세부사항: SSL을 사용하여 중앙 관리 서버에 대한 모든 연결 보안

다음 정보에서는 시나리오: SSL을 사용하여 중앙 관리 서버에 대한 모든 연결 보안을 읽은 것으로 간주합니다. 중앙 관리 서버에 대한 모든 연결 보안에 필요한 단계를 수행하는 방법을 이해할 수 있습니다. Tom을 따라 수행하면 시나리오가 완료됩니다.

Tom은 중앙 관리 서버에 SSL을 작동하기 전에 필수 프로그램을 설치하고 iSeries 서버에 디지털 인증서를 설정해야 합니다. 계속하기 전에 이 시나리오에 대한 전제조건 및 가정을 참조하십시오. 전제조건이 충족되면 다음 프로시듀어를 완료하여 중앙 관리 서버로의 모든 연결을 보안할 수 있습니다.

주: iSeries Navigator에 SSL이 작동되도록 설정한 경우 Tom은 SSL을 작동 불가능하게 한 후 중앙 관리 서버에서 SSL을 작동시켜야 합니다. 중앙 관리 서버가 아니라 iSeries Navigator에 SSL이 작동되도록 설정한 경우 iSeries Navigator가 중앙 시스템에 연결되지 않습니다.

1단계: 서버 인증을 위한 중앙 시스템 구성

SSL을 사용하면 iSeries Navigator 클라이언트와 중앙 시스템 간의 전송 보안 뿐만 아니라 중앙 시스템과 엔드포인트 시스템 간의 전송 보안을 유지할 수 있습니다. SSL은 인증서의 전송과 인증 그리고 자료 암호화를 제공합니다. SSL 연결은 SSL 작동 가능 중앙 시스템과 SSL 작동 가능 엔드포인트 시스템 간에서만 이루어질 수 있습니다. Tom은 클라이언트 인증을 구성하기 전에 서버 인증을 구성해야 합니다.

1. iSeries Navigator에서 **중앙 관리**를 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
2. **보안** 탭을 클릭하고 **SSL(Secure Socket Layer) 사용**을 선택하십시오.
3. **서버**를 인증 레벨로 선택하십시오.
4. **확인**을 클릭하여 이 값을 중앙 시스템에 설정하십시오.

   주: 서버 인증을 위한 엔드포인트 시스템의 구성이 완료될 때까지 중앙 관리 서버를 다시 시작하지 **마십시오.**
5. 서버 인증을 위한 엔드포인트 시스템 구성

2단계: 서버 인증을 위한 엔드포인트 시스템 구성

Tom이 서버 인증을 위해 중앙 시스템을 구성했으면 서버 인증을 위해 엔드포인트 시스템을 구성해야 합니다. 다음 타스크를 완료합니다.

1. **중앙 관리**를 펼치십시오.
2. 엔드포인트 시스템의 시스템 값을 비교하고 갱신하십시오.
   a. **엔드포인트 시스템** 아래에서 중앙 시스템을 마우스 오른쪽 버튼으로 클릭하고 **명세 --> 수집**을 선택하십시오.
   b. 중앙 시스템에 대한 시스템 값 명세를 수집하려면 수집 대화 상자에서 **시스템 값** 옵션을 체크하십시오. 다른 옵션을 선택 취소하십시오.
   c. **시스템 그룹 --> 신규 시스템 그룹**을 마우스 오른쪽 버튼으로 클릭하십시오.
   d. SSL을 사용하여 연결할 모든 엔드포인트 시스템이 포함되어 있는 신규 시스템 그룹을 정의하십시오.
   e. 신규 그룹을 표시하려면 시스템 그룹 리스트를 펼치십시오.
   f. 수집을 완료한 다음 신규 시스템 그룹을 마우스 오른쪽 버튼으로 클릭하고 **시스템 값 --> 비교 및 갱신**을 선택하십시오.
   g. 중앙 시스템이 **모델 시스템** 필드에 표시되는지 확인하십시오.
   h. **중앙 관리** 범주를 선택하고 다음에 나오는 값의 옆에 있는 상자에서 체크 상태를 확인하십시오.
      - **SSL 사용**에 **예**를 지정하십시오.
      - SSL 인증 레벨에 **서버**를 지정하십시오.

      서버 인증을 위한 중앙 시스템 구성 프로시듀어 도중 중앙 시스템에 이들 값을 설정합니다.
   i. 신규 시스템 그룹에 포함된 엔드포인트 시스템에서 이러한 값을 설정하려면 **확인**을 클릭하십시오.
   j. **비교 및 갱신** 프로세스가 완료될 때까지 기다린 후 중앙 관리 서버를 다시 시작하십시오. 비교 및 갱신 프로세스가 완료되기 까지는 일정 시간(몇 분)이 소요됩니다.

3단계: 중앙 시스템에서 중앙 관리 서버 다시 시작

1. iSeries Navigator에서 **연결**을 펼치십시오.
2. 중앙 시스템 보기를 펼치십시오.
3. **네트워크 --> 서버**를 펼치고 **TCP/IP**를 선택하십시오.
4. **중앙 관리**를 마우스 오른쪽 버튼으로 클릭하고 **중단**을 선택하십시오. 중앙 시스템 보기가 접히고 서버에 연결되지 않았음을 설명하는 메세지가 표시됩니다.
5. 중앙 관리 서버가 중단되었으면 **시작**을 클릭하여 다시 시작하십시오.

4단계: 모든 엔드포인트 시스템에서 중앙 관리 서버 다시 시작

1. 다시 시작할 엔드포인트 시스템을 펼치십시오.
2. **네트워크 --> 서버**를 펼치고 **TCP/IP**를 선택하십시오.
3. **중앙 관리**를 마우스 오른쪽 버튼으로 클릭하고 **중단**을 선택하십시오.
4. 중앙 관리 서버를 중단한 후 **시작**을 클릭하여 다시 시작하십시오.
5. 각 엔드포인트 시스템에 대해 이 절차를 반복하십시오.

5단계: iSeries Navigator 클라이언트에 대한 SSL 활성화

1. iSeries Navigator에서 **연결**을 펼치십시오.
2. 중앙 시스템을 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
3. **보안 소켓** 탭을 클릭하고 **연결에 SSL(Secure Sockets Layer) 사용**을 선택하십시오.
4. iSeries Navigator를 나간 다음 다시 시작하십시오.

6단계: 클라이언트 인증을 위한 중앙 시스템 구성(선택적 단계)

Tom이 서버 인증을 위한 구성을 완료했으므로 다음과 같은 클라이언트 인증 프로시듀어를 선택적으로 수행할 수 있습니다. 클라이언트 인증은 엔드포인트 시스템과 중앙 시스템 모두에 인증 기관과 신뢰할 수 있는 그룹의 유효성을 제공합니다. 중앙 시스템(SSL 클라이언트)이 SSL을 사용하여 엔드포인트 시스템(SSL 서버)에 연결하려고 하면 중앙 시스템과 엔드포인트 시스템은 클라이언트 인증을 통해 서로의 인증서를 인증합니다. 이를 인증 기관 및 신뢰할 수 있는 그룹 인증이라고도 합니다.

주: 서버 인증을 구성한 경우에만 클라이언트 인증 구성을 완료할 수 있습니다.

1. iSeries Navigator에서 **중앙 관리**를 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.
2. **보안** 탭을 클릭하고 **SSL(Secure Sockets Layer) 사용**을 선택하십시오.
3. 인증 레벨에 해당되는 **클라이언트와 서버**를 선택하십시오.
4. **확인**을 클릭하여 이 값을 중앙 시스템에 설정하십시오.

   주: 모든 엔드포인트 시스템이 클라이언트 및 서버 인증과 함께 SSL을 사용하도록 구성될 때까지는 중앙 관리 서버를 다시 시작하지 **마십시오**.
5. 클라이언트 인증을 위한 엔드포인트 시스템 구성

7단계: 클라이언트 인증을 위한 엔드포인트 시스템 구성(선택적 단계)

1. 엔드포인트 시스템의 시스템 값 비교 및 갱신

   주: V4R5를 실행하는 엔드포인트 iSeries 서버에는 이 타스크가 적용되지 않습니다.

   a. **엔드포인트 시스템** 아래에서 중앙 시스템을 마우스 오른쪽 버튼으로 클릭하고 **명세 --> 수집**을 선택하십시오.

   b. 중앙 시스템에 대한 시스템 값 명세를 수집하려면 수집 대화 상자에서 **시스템 값** 옵션을 체크하십시오. 다른 옵션을 선택 취소하십시오.

   c. **시스템 그룹 --> 신규 시스템 그룹**을 마우스 오른쪽 버튼으로 클릭하십시오.

   d. SSL을 사용하여 연결할 모든 엔드포인트 시스템이 포함되어 있는 신규 시스템 그룹을 정의하십시오.

   e. 신규 그룹을 표시하려면 시스템 그룹 리스트를 펼치십시오.

   f. 수집을 완료한 다음 신규 시스템 그룹을 마우스 오른쪽 버튼으로 클릭하고 **시스템 값 --> 비교 및 갱신**을 선택하십시오.

   g. **중간 시스템**이 **모델 시스템** 필드에 표시되는지 확인하십시오.

   h. **중앙 관리** 범주를 선택하고 다음을 확인하십시오.

      - **SSL 사용**에 **예**를 지정하십시오.
      - SSL 인증 레벨에 **클라이언트 및 서버**를 지정하십시오.

      클라이언트 인증을 위한 중앙 시스템 구성 프로시듀어 도중 중앙 시스템에 이들 값을 설정합니다. 각 값의 옆에 있는 **갱신** 상자를 체크하십시오.

   i. 신규 시스템 그룹에 포함된 엔드포인트 시스템에서 이러한 값을 설정하려면 **확인**을 클릭하십시오.

8단계: 엔드포인트 시스템에 유효성 리스트 복사

1. 다음 단계는 사용자의 중앙 시스템이 V5R3 이상이라고 가정합니다. iSeries Navigator에서 **중앙 관리 --> 정의**를 펼치십시오.
2. **패키지**를 마우스 오른쪽 버튼으로 클릭하고 **신규 정의**를 선택하십시오.
3. **신규 정의** 창에서 다음과 같이 하십시오.
   - **이름:** 정의명을 입력하십시오.
   - **소스 시스템:** 중앙 시스템명을 선택하십시오.
   - **선택한 파일 및 폴더:** 필드를 클릭하고 /QSYS.LIB/QMGTC2.LIB/QYPSVLDL.VLDL을 입력하십시오.
4. **옵션** 탭을 클릭하고 **기존 파일을 송신할 파일로 대체**를 선택하십시오.
5. **고급**을 클릭하십시오
6. **고급 옵션** 창에서 복원 시 오브젝트 차이를 허용하려면 **예**를 지정하십시오.
7. 정의 리스트를 화면정리하고 신규 패키지를 표시하려면 **확인**을 클릭하십시오.
8. 신규 패키지를 마우스 오른쪽 버튼으로 클릭하고 **송신**을 선택하십시오
9. **송신** 대화: **시스템 그룹을 신뢰 그룹으로** 펼치고 **사용할 수 있는 시스템 및 그룹** 리스트에 위치시키십시오. 개별적으로 V5R3 이상의 모든 시스템을 **선택한 시스템 및 그룹** 리스트로 추가하십시오. **선택한 시스템 및**

그룹 리스트에서 다른 모든 시스템을 제거하고 **확인**을 클릭하십시오. 신뢰 그룹은 7장: 클라이언트 인증에 대한 구성 엔드포인트 시스템의 1.c에서 정의한 시스템 그룹입니다.

주: 중앙 시스템은 항상 소스 시스템이므로 중앙 시스템에서는 **송신** 타스크가 실패합니다. **송신** 타스크는 모든 엔드포인트 시스템에서 성공적으로 완료되어야 합니다.

V5R3 이전의 iSeries systems에서QYPSVLDL.VLDL은 QUSRSYS.LIB에 위치했지만 V5R3은 QMGTC2.LIB에 위치합니다. 따라서 V5R3 이전의 시스템인 경우 유효성 리스트를 송신하고 QUSRSYS.LIB 대신에 QMGTC2.LIB에 위치시키십시오. 다음을 수행하십시오.

a. 위에서 작성한 패키지 정의에서 마우스 오른쪽 버튼으로 클릭하고 **신규 기본 파일**을 선택하십시오.
b. 첫 번째 정의에서 구분하기 위해서 신규 이름을 정의하십시오.
c. 정의의 **일반** 탭의 **목표 경로** 열에서 /QSYS.LIB/QMGTC2.LIB/QYPSVLDL.VLDL경로를 클릭하십시오. 편집하려면 이를 허용합니다. QMGTC2를 QUSRSYS로 변경하십시오.

   주: 소스 경로가 아닌 **목표 경로**를 편집하십시오.
d. 신규 패키지 정의를 저장하려면 **확인**을 클릭하십시오.
e. 신규 패키지 정의에서 마우스 오른쪽 버튼으로 클릭하고 **송신**을 선택하십시오.
f. **송신** 대화: **시스템 그룹을 신뢰 그룹으로** 펼치고 **사용할 수 있는 시스템 및 그룹** 리스트에 위치시키십시오. 개별적으로 V5R3 이전 시스템을 **선택한 시스템 및 그룹** 리스트에 추가하십시오. **선택한 시스템 및 그룹** 리스트에서 다른 모든 시스템을 제거하고 **확인**을 클릭하십시오. **신뢰 그룹**은 7장: 클라이언트 인증에 대한 구성 엔드포인트 시스템의 1.c에서 정의한 시스템 그룹입니다.

9단계: 중앙 시스템에서 중앙 관리 서버 다시 시작

1. iSeries Navigator에서 **연결**을 펼치십시오.
2. 중앙 시스템을 펼치십시오.
3. **네트워크 --> 서버**를 펼치고 **TCP/IP**를 선택하십시오.
4. **중앙 관리**를 마우스 오른쪽 버튼으로 클릭하고 **중단**을 선택하십시오. 중앙 시스템 보기가 접히고 서버에 연결되지 않았음을 설명하는 메세지가 표시됩니다.
5. 중앙 관리 서버를 중단한 후 **시작**을 클릭하여 다시 시작하십시오.

10단계: 모든 엔드포인트 시스템에서 중앙 관리 서버 다시 시작

주: 각 엔드포인트 시스템에 대해 이 절차를 반복하십시오.

1. 다시 시작할 엔드포인트 시스템을 펼치십시오.
2. **네트워크 --> 서버**를 펼치고 **TCP/IP**를 선택하십시오.
3. **중앙 관리**를 마우스 오른쪽 버튼으로 클릭하고 **중단**을 선택하십시오.
4. 중앙 관리 서버를 중단한 후 **시작**을 클릭하여 다시 시작하십시오.

다른 SSL 시나리오로 연결되는 링크에 대해서는 시나리오를 참조하십시오.

개념

SSL 프로토콜을 사용하면 클라이언트와 서버 어플리케이션 간에 보안 연결을 설정하여 통신 세션의 각 엔드포인트 또는 두 엔드포인트의 인증을 제공할 수 있습니다. 또한 SSL은 클라이언트와 서버 어플리케이션이 교환하는 자료의 보안성 및 무결성을 제공합니다.

다음의 개념 정보를 통해 SSL과 iSeries 서버 간의 관계를 보다 잘 이해할 수 있습니다.

- SSL의 역사
- SSL 작동 방식
- 지원되는 SSL 및 TLS(Transport Layer Security) 프로토콜
- 서버 인증
- 클라이언트 인증

SSL의 역사

SSL(Secure Sockets Layer) 프로토콜은 인터넷 보안에 대한 관심이 커짐에 따라 1994년에 Netscape에서 개발한 프로토콜입니다. 처음에 SSL은 웹 브라우저와 서버 통신의 보안을 위해 개발되었습니다. 스펙은 TELNET이나 FTP와 같은 다른 어플리케이션에서 SSL을 작동할 수 있는 방식으로 설계되었습니다. SSL 및 관련 프로토콜에 대한 자세한 정보는 지원되는 SSL 및 TLS(Transport Layer Security) 프로토콜을 참조하십시오.

SSL 작동 방식

SSL은 실제로 두 개의 프로토콜입니다. 레코드 프로토콜과 핸드쉐이크 프로토콜이 그것입니다. 레코드 프로토콜은 SSL 세션의 두 엔드포인트 간에서 자료의 흐름을 제어합니다.

핸드쉐이크 프로토콜은 SSL 세션의 하나의 엔드포인트이나 두 개의 엔드포인트을 각각 인증하고, 해당 SSL 세션의 자료를 암호화하고 암호를 해독하기 위한 키를 생성할 때 사용할 수 있는 고유 대칭 키를 설정합니다. SSL은 비대칭 암호, 디지털 인증 및 SSL 핸드쉐이크 흐름을 사용하여 SSL 세션의 한 엔드포인트 또는 두 엔드포인트을 인증합니다. 보통 SSL은 서버를 인증합니다. 선택적으로 SSL은 클라이언트를 인증합니다. 인증기관에서 발행한 디지털 인증서는 연결의 엔드포인트마다 SSL을 사용해서 각 엔드포인트이나 어플리케이션에 지정됩니다.

디지털 인증은 신뢰할 수 있는 CA(Certificate Authority)에서 디지털로 서명한 공용 키와 몇 가지 식별 정보로 이루어집니다. 각 공용 키에는 연관된 개인 키가 있습니다. 개인 키는 인증서와 함께 저장되거나 인증서의 일부로 저장되지 않습니다. 서버 인증과 클라이언트 인증 모두에 있어서 인증 중인 엔드포인트은 디지털 인증서에 포함되어 있는 공용 키와 연관된 개인 키에 액세스할 수 있음을 증명해야 합니다.

SSL 핸드쉐이크 작업은 공용 키와 개인 키를 사용하는 암호 조작으로 인해 높은 성능을 필요로 합니다. 두 엔드포인트 사이에 초기 SSL 세션이 설정되면 두 엔드포인트과 어플리케이션에 대한 SSL 세션 정보가 보안 메모리에 캐시되어 후속 SSL 세션의 작동 속도를 높일 수 있습니다. SSL 세션이 재개되면 두 엔드포인트은 공용 키나 개인 키를 사용하지 않고도 각각 고유 정보에 액세스할 수 있음을 인증하기 위해 단축 핸드쉐이크 흐름을 사용합니다. 두 엔드포인트 모두 이 고유 정보에 대한 액세스 권한이 있음을 증명할 수 있으면 새로운 대칭 키가 설정되고 SSL 세션이 재개됩니다. TLS 버전 1.0과 SSL 버전 3.0 세션에서는 24시간이 지나면 캐

시된 정보가 보안 메모리에서 삭제됩니다. V5R2M0 및 후속 릴리스에서 암호 하드웨어를 사용하여 기본 CPU에 미치는 SSL 핸드쉐이크 성능의 영향을 최소화할 수 있습니다.

지원되는 SSL 및 TLS(Transport Layer Security) 프로토콜

SSL 프로토콜에는 여러 버전이 있습니다. 최신 버전인 TLS(Transport Layer Security) 프로토콜은 SSL 3.0을 기반으로 하는 IETF(Internet Engineering Task Force)의 제품입니다. OS/400은 다음과 같은 SSL 및 TLS 프로토콜 버전을 지원합니다.

- TLS 버전 1.0
- SSL 버전 3.0과 호환되는 TLS 버전 1.0

  주:

  1. SSL 버전 3.0과 호환되는 TLS 버전 1.0을 지정하는 것은 가능하면 TLS로 결정되고 아니면 SSL 버전 3.0으로 결정된다는 것을 의미합니다. SSL 버전 3.0을 조정할 수 없으면 SSL 핸드쉐이크에 실패합니다.
  2. SSL 버전 3.0 및 SSL 버전 2.0과 호환되는 TLS 버전 1.0도 지원됩니다. 이것은 프로토콜 값 **ALL**로 지정되는데 가능하면 TLS로 결정되고 아니면 SSL 버전 3.0으로 결정된다는 것을 나타냅니다. SSL 버전 3.0으로 결정되지 않을 경우 SSL 버전 2.0으로 결정됩니다. SSL 버전 2.0을 조정할 수 없으면 SSL 핸드쉐이크에 실패합니다.
- SSL 버전 3.0
- SSL 버전 2.0
- SSL 버전 2.0과 호환되는 SSL 버전 3.0

SSL 버전 3.0 대 SSL 버전 2.0

SSL 버전 3.0은 SSL 버전 2.0과 비교해 볼 때 전혀 다른 프로토콜입니다. 두 프로토콜의 주요한 차이점은 다음과 같습니다.

- SSL 버전 3.0 핸드쉐이크 프로토콜 흐름은 SSL 버전 2.0의 핸드쉐이크 흐름과 다릅니다.
- SSL 버전 3.0은 RSA Data Security, Incorporated의 BSAFE 3.0 구현을 사용합니다. BSAFE 3.0에는 여러 가지 타이밍 공격 수정 프로그램과 SHA-1 해싱 알고리즘이 있습니다. SHA-1 해싱 알고리즘은 MD5 해싱 알고리즘 보다 안전한 것으로 간주됩니다. SHA-1에서 SSL 버전 3.0은 MD5 대신 SHA-1을 사용하는 추가 Cipher suite를 지원할 수 있습니다.
- SSL 버전 3.0 프로토콜은 SSL 핸드쉐이크 처리 중에 발생하는 MITM(man-in-the-middle) 유형의 공격을 감소시킵니다. SSL 버전 2.0의 경우에는 MITM 공격이 예상과 달리 암호 스펙을 약화시킬 수 있습니다. 암호를 약화시키면 권한이 없는 사람이 SSL 세션 키를 해독할 가능성이 있습니다.

TLS 버전 1.0 대 SSL 버전 3.0

SSL 버전 3.0 기반의 최신 산업 표준 SSL 프로토콜은 TLS(Transport Layer Security) 버전 1.0입니다. 해당 스펙은 RFC 2246의 IETF(Internet Engineering Task Force), ″The TLS Protocol″  에 정의되어 있습니다.

TLS의 주 목적은 SSL을 보다 안전하게 만들고 프로토콜의 스펙에 더 우수한 정확성과 완벽성을 제공하는 것입니다. TLS는 SSL 버전 3.0에 비해 다음과 같은 확장 기능을 제공합니다.

- 보다 안전한 MAC 알고리즘
- 보다 세분화된 경고
- ″모호한″ 스펙 부분에 대한 보다 명확한 정의

SSL가 작동되는 모든 iSeries 서버 어플리케이션은 그 어플리케이션이 SSL 버전 3.0이나 SSL 버전 2.0만 사용하도록 특별히 요구하는 경우를 제외하고 자동으로 TLS 지원을 받습니다.

TLS는 다음과 같은 보안 개선점을 제공합니다.

- **메세지 인증을 위한 키 해싱**
  TLS는 HMAC(Key-Hashing for Message Authentication Code)를 사용하여 인터넷과 같은 개방 네트워크에서 작업할 때 레코드를 변경할 수 없도록 합니다. SSL 버전 3.0도 키 메세지 인증을 제공하지만 HMAC는 SSL 버전 3.0에 사용되는 메세지 인증 코드(MAC) 기능보다 안전합니다.
- **향상된 PRF(Psuedorandom Function)**
  PRF는 키 자료를 생성합니다. TLS에서 HMAC는 PRF를 정의합니다. PRF는 보안을 보장하는 방식으로 두 개의 해시 알고리즘을 사용합니다. 어느 한 알고리즘이 노출될 경우 두 번째 알고리즘이 노출되지 않는 한 자료는 보안 상태를 유지합니다.
- **개선된 완료 메세지 확인**
  TLS 버전 1.0과 SSL 버전 3.0 모두 교환된 메세지가 변경되지 않았다는 것을 인증하는 완료 메세지를 두 엔드포인트에 제공합니다. 그러나 TLS는 이 완료 메세지를 SSL 버전 3.0보다 안전한 PRF와 HMAC 값을 기준으로 처리합니다.
- **일관된 인증 처리**
  SSL 버전 3.0과 달리 TLS는 TLS 구현 간에 교환되어야 하는 인증서 유형을 지정합니다.
- **특정 경고 메세지**
  TLS는 두 개의 세션 엔드포인트 중 하나에서 감지된 문제를 표시하기 위해 보다 구체적인 추가 경고를 제공합니다. 또한 TLS는 어떤 경고를 언제 전송해야 할 지에 관해 문서를 작성합니다.

서버 인증

서버 인증을 사용하는 경우 클라이언트는 서버 인증서가 유효하며 클라이언트가 신뢰하는 CA(Certificate Authority)에서 서명한 것인지를 확인합니다. SSL은 비대칭 암호와 핸드쉐이크 프로토콜 흐름을 사용하여 이러한 고유 SSL 세션에만 사용할 대칭 키를 생성합니다. 이 키는 SSL 세션에서 흐르게 될 자료의 암호화와 해독에 필요한 키 세트를 생성하는 데 사용됩니다. 후속적으로 SSL 핸드쉐이크가 완료되면 통신 링크 중 한쪽 끝 또는 양 끝이 인증된 것입니다. 또한 자료를 암호화하고 해독하는 고유 키가 생성된 것입니다. 일단 핸드쉐이크가 완료되면 어플리케이션 계층 자료가 암호화되어 해당 SSL 세션을 통과합니다.

클라이언트 인증

대부분의 어플리케이션에서는 옵션을 통해 클라이언트 인증을 가능하게 할 수 있도록 합니다. 클라이언트 인증서를 사용하여 서버는 클라이언트 인증서가 유효하며 그 인증서가 서버에서 신뢰하는 인증 기관에서 서명된 것인지를 확인할 수 있습니다. 다음은 클라이언트 인증을 지원하는 iSeries 서버 어플리케이션입니다.

- IBM HTTP Server(Apache로 구동)
- FTP 서버
- Telnet 서버
- 중앙 관리 엔드포인트 시스템
- 디렉토리 서비스(LDAP)

SSL 작동 계획

iSeries 서버에서 SSL 작동을 계획할 때는 다음 사항을 고려하십시오.

- SSL 전제조건
- 원하는 디지털 인증서의 유형 및 확보 위치

SSL 전제조건

- IBM DCM(Digital Certificate Mananger), OS/400(5722-SS1)의 옵션 34
- iSeries용 TCP/IP Connectivity Utilities(5722-TC1)
- iSeries용 IBM HTTP Server(5722-DG1)
- HTTP 서버를 사용하여 DCM을 사용하려면 IBM Developer Kit for Java™(5722-JV1)가 설치되어 있어야 합니다. 그렇지 않으면 HTTP 관리 서버가 시작되지 않습니다.
- IBM Cryptographic Access Provider 제품, 5722-AC3(128비트). 이 제품의 비트 *크기*는 암호 조작에 사용할 수 있는 대칭 키에서 기밀 자료의 최대 *크기*를 나타냅니다. 대칭 키에 허용되는 자료의 *크기*는 각 국가의 수출입법에 의거하여 처리됩니다. 비트 *크기*가 클수록 연결이 더 안전합니다.
- SSL을 사용할 경우 SSL 핸드쉐이크 처리 속도를 높이기 위해 암호화 하드웨어를 설치할 수도 있습니다. 사용할 수 있는 옵션에 대한 암호 하드웨어 정보를 참조하십시오. 4758 IBM Cryptographic Coprocessor 또는4764 IBM Cryptographic Coprocessor를 설치하려면 Option 35, Cryptographic Service Provider도 설치해야 합니다.

Windows용 iSeries Access 구성요소에 SSL을 사용하려면 iSeries Client Encryption 제품 5722-CE3(128 비트)도 설치해야 합니다. Windows용 iSeries Access에서 보안 연결을 설정하려면 이 제품이 필요합니다.

주: 개인 통신 제품과 함께 제공되는 PC5250 에뮬레이터를 사용할 경우에는 클라이언트 암호화 제품을 설치할 필요가 없습니다. 개인 통신에는 고유의 내장 암호화 코드가 있습니다.

디지털 인증서

공용 디지털 인증서와 개인용 디지털 인증서의 차이점과 각각을 얻기 위한 옵션에 대한 자세한 정보는 공용 인증서 사용 대 개인용 인증서 발행을 참조하십시오.

IBM DCM (Digital Certificate Manager)은 디지털 인증서를 관리하기 위한 iSeries 서버 솔루션입니다. DCM에 대한 더 자세한 정보는 Information Center에서 DCM(Digital Certificate Manager) 사용 주제를 참조하십시오.

SSL을 사용한 어플리케이션 보안

SSL을 사용하여 다음과 같은 iSeries 서버 어플리케이션의 보안을 유지할 수 있습니다.

- 기업망 ID 맵핑(EIM)
- FTP 서버
- HTTP Server(Apache로 구동)
- Windows용 iSeries Access
- 디렉토리 서비스 서버(LDAP)
- DRDA®(분산 관계형 데이터베이스 구조) 및 분산 자료 관리(DDM) 서버
- 중앙 관리 서버
- Telnet 서버
- Websphere Application Server -- Express
- 어플리케이션 프로그래밍 인터페이스(API)의 Windows용 iSeries Access 세트에 기록된 어플리케이션
- iSeries 서버에서 지원되는 보안 소켓 API(Application Programmable Interface)를 사용하여 개발한 어플리케이션. 지원되는 API는 GSKit(Global Secure Toolkit) 및 SSL_ iSeries 기본 API입니다. GSKit 및 SSL_API에 대한 자세한 정보는 보안 소켓 API를 참조하십시오.

SSL 문제 해결

이러한 기본적인 문제 해결 정보는 iSeries 서버에서 SSL과 관련하여 발생할 수 있는 문제 리스트의 범위를 축소하여 사용자들에게 도움을 주기 위한 것입니다. 이것은 문제 해결 정보를 위한 포괄적인 자료가 아닌 단지 참고사항일 뿐입니다.

다음 사항을 모두 만족하는지 확인하십시오.

- iSeries 서버에서 SSL 전제조건을 만족합니다(SSL 전제조건 참조).
- V5R1 시스템에서 iSeries Navigator의 중앙 관리 기술을 사용하는 경우 시스템에 다음 PTF를 설치했습니다.
  - si01375
  - si01376
  - si01377
  - si01378
  - si01838
- 인증 기관 및 인증서가 유효하며 만료되지 않았습니다.

시스템에 대한 이전 명령문이 참이고 SSL 관련 문제가 계속되면 다음 옵션을 시도해 보십시오.

- 오류에 대한 자세한 정보를 찾을 수 있는 오류 표에서 서버 작업 기록부의 SSL 오류 코드를 상호 참조할 수 있습니다. 보안 소켓 오류 코드 메세지에 대한 정보에 액세스하려면 보안 소켓 API 오류 코드 메세지 페이지를 참조하십시오. 예를 들어 이 표는 서버 작업 기록부에 표시될 수 있는 -93을 상수 SSL_ERROR_SSL_NOT_AVAILABLE로 맵핑합니다.
  - 음수 리턴 코드(코드 번호 앞에 대시(-)로 표시)는 SSL_API를 사용하고 있음을 표시합니다.
  - 양수 리턴 코드는 GSKit API를 사용하고 있음을 표시합니다. 프로그래머가 오류 리턴 코드에 대한 간단한 설명을 얻을 수 있도록 프로그램에 gsk_strerror()or SSL_Strerror() API를 코딩할 수 있습니다. 일부 어플리케이션은 이 API를 사용하고 이 문단이 있는 작업 기록부로 메세지를 인쇄합니다.

  추가 정보가 필요하면 해당 오류에 대해 추측이 가능한 원인 및 회복 방법을 나타내기 위해 표에 제공되는 메세지 ID를 iSeries 서버에 표시할 수 있습니다. 이러한 오류 코드를 설명하는 추가 정보는 오류를 리턴한 개별 보안 소켓 API에서 찾을 수 있습니다.
- 다음에 나오는 두 가지 헤더 파일에는 표와 동일한 시스템 SSL 리턴 코드의 상수 이름이 포함되어 있으나 메세지 ID를 상호 참조하지는 않습니다.
  - QSYSINC/H.GSKSSL
  - ≫QSYSINC/H.QSOSSL≪

  이러한 두 개의 파일에서 시스템 SSL 리턴 코드의 이름이 상수로 남아 있더라도 하나 이상의 고유 오류가 각 리턴 코드와 연관되어 있을 수 있습니다.

iSeries 서버에 대한 자세한 문제 해결 정보는 문제 해결 및 서비스 페이지를 참조하십시오.

관련 정보

다음 소스에서 추가 SSL 정보를 찾을 수 있습니다.

IBM 소스

- JSSE에 대한 간단한 설명과 JSSE 사용 방법이 포함되어 있는 SSL 및 (JSSE) Java Secure Socket Extension 페이지
- 사용할 수 있는 Java 클래스에 대한 간단한 설명과 사용 방법이 포함되어 있는 IBM Toolbox for Java 페이지.

RFC(Request for Comments)

- RFC 2246: ″TLS Protocol Version 1.0″  - TLS 프로토콜에 대해 자세히 설명합니다.
- RFC2818: ″HTTP OVer TLS″  - 인터넷에서 TLS를 사용하여 HTTP 연결 보안을 유지하는 방법에 대해 설명합니다.

기타 소스

- SSL Protocol Version 3.0 문서  - SSL 프로토콜 버전 3.0에 대해 자세히 설명합니다.

부록. 주의사항

이 정보는 미국에서 제공되는 제품 및 서비스용으로 작성된 것입니다.

IBM은 다른 국가에서는 이 자료에 기술된 제품, 서비스 또는 기능을 제공하지 않을 수도 있습니다현재 사용할 수 있는 제품 및 서비스에 대한 정보는 한국 IBM 담당자에게 문의하십시오. 이 책에서 IBM 제품, 프로그램 또는 서비스를 언급했다는 것이 해당 IBM 제품, 프로그램 또는 서비스만을 사용할 수 있다는 것을 의미하지는 않습니다. IBM의 지적 재산권을 침해하지 않는 한, 기능상으로 동등한 제품, 프로그램 또는 서비스를 대신 사용할 수 있습니다. 그러나 비IBM 제품, 프로그램 또는 서비스의 운영에 대한 평가 및 검증은 사용자의 책임입니다.

IBM은 이 책에서 다루고 있는 특정 내용에 대해 특허를 보유하고 있거나 현재 특허 출원 중일 수 있습니다. 이 책을 제공한다고 해서 특허에 대한 라이센스까지 부여하는 것은 아닙니다. 라이센스에 대한 의문사항은 다음으로 문의하십시오.

135-270
서울특별시 강남구 도곡동 467-12, 군인공제회관빌딩
한국 아이.비.엠 주식회사
고객만족센터
전화번호: 080-023-8080

2바이트(DBCS) 정보에 관한 라이센스 문의는 한국 IBM 고객만족센터에 문의하거나 다음 주소로 서면 문의하시기 바랍니다.

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

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 일체의 보증없이 이 책을『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, 이 변경사항은 최신판에 통합됩니다. IBM은 이 책에 설명한 제품 및(또는) 프로그램을 사전 통지없이 언제든지 개선 및(또는) 변경할 수 있습니다.

이 정보에서 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.

(1) 독립적으로 작성된 프로그램과 기타 프로그램(본 프로그램 포함) 간의 정보 교환 및 (2) 교환된 정보의 상호 이용을 목적으로 정보를 원하는 프로그램 라이센스 사용자는 다음 주소로 문의하십시오.

135-270
서울특별시 강남구 도곡동 467-12, 군인공제회관빌딩
한국 아이.비.엠 주식회사
고객만족센터

이러한 정보는 해당 조항 및 조건에 따라(예를 들면, 사용료 지불 포함) 사용할 수 있습니다.

이 책에 기술된 라이센스가 있는 프로그램 및 사용 가능한 모든 라이센스가 있는 자료는 IBM이 IBM 기본 계약, IBM 프로그램 라이센스 계약(IPLA) 또는 이와 동등한 계약에 따라 제공한 것입니다.

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

비IBM 제품에 관한 정보는 해당 제품의 공급업체, 공개 자료 또는 기타 범용 소스로부터 얻은 것입니다. IBM에서는 이러한 비IBM 제품을 테스트하지 않았으므로, 이들 제품과 관련된 성능의 정확성, 호환성 또는 기타 주장에 대해서는 확신할 수 없습니다. 비IBM 제품의 성능에 대한 의문사항은 해당 제품의 공급업체에 문의하십시오.

IBM의 향후 방향 또는 의도에 관한 모든 언급은 별도의 통지없이 변경될 수 있습니다.

상표

다음 용어는 미국 또는 기타 국가에서 사용되는 IBM Corporation의 상표입니다.

DRDA
IBM
iSeries
Operating System/400
OS/400
Windows
Windows NT

Lotus®, Freelance 및 WordPro는 미국 또는 기타 국가에서 사용되는 IBM Corporation과 Lotus Development Corporation의 상표입니다.

Microsoft®, Windows, Windows NT® 및 Windows 로고는 미국 또는 기타 국가에서 사용되는 Microsoft Corporation의 상표입니다.

기타 회사, 제품 및 서비스 이름은 해당 회사의 상표 또는 서비스표입니다.

서적의 다운로드 및 인쇄 조건

귀하가 다운로드하려는 서적을 사용하는 데에는 다음의 조건이 적용되며 귀하가 이를 승인하는 경우에 해당 서적을 사용할 수 있습니다.

개인적인 사용: 일체의 소유권 표시를 하는 경우에 한하여 귀하는 이들 서적을 개인적이며 비상업적인 용도로 복제할 수 있습니다. 귀하는 IBM의 명시적인 동의없이 해당 서적에 대한 2차적 저작물 또는 그 일부를 배포, 전시 또는 작성할 수 없습니다.

상업적 사용: 일체의 소유권 표시를 하는 경우에 한하여 귀하는 이들 서적을 귀하 사업장 내에서만 복제, 배포 및 전시할 수 있습니다. 귀하는 IBM의 명시적인 동의없이 귀하의 사업장 이외에서 해당 서적의 2차적 저작물을 작성할 수 없으며 이들 서적 또는 그 일부를 복제, 배포 또는 전시할 수 없습니다.

본 계약에서 명시하지 않는 한, 본 서적 또는 본 서적에 포함된 정보, 데이터, 소프트웨어 또는 기타 지적 재산권에 대하여 다른 허가나 라이센스 또는 권리가 부여되지 않습니다.

해당 서적의 사용이 IBM에게 손해를 가져오거나, 상기 지시사항이 적절하게 준수되지 않은 것으로 IBM이 판단한 경우, IBM은 본 계약에서 부여한 서적에 대해 허가를 취소할 권리가 있습니다.

귀하는 미국 수출법 및 관련 규정을 포함하여 모든 적용 가능한 법률 및 규정을 철저히 준수하지 않는 경우 본 정보를 다운로드, 송신 또는 재송신할 수 없습니다. IBM은 이들 서적의 내용과 관련하여 어떠한 보증도 하지 않습니다. 본 서적은 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 일체의 보증없이 ″현상태대로″ 제공됩니다.

귀하는 본 사이트로부터 서적을 다운로드하거나 인쇄함으로써 본 조건에 동의한 것으로 간주됩니다.