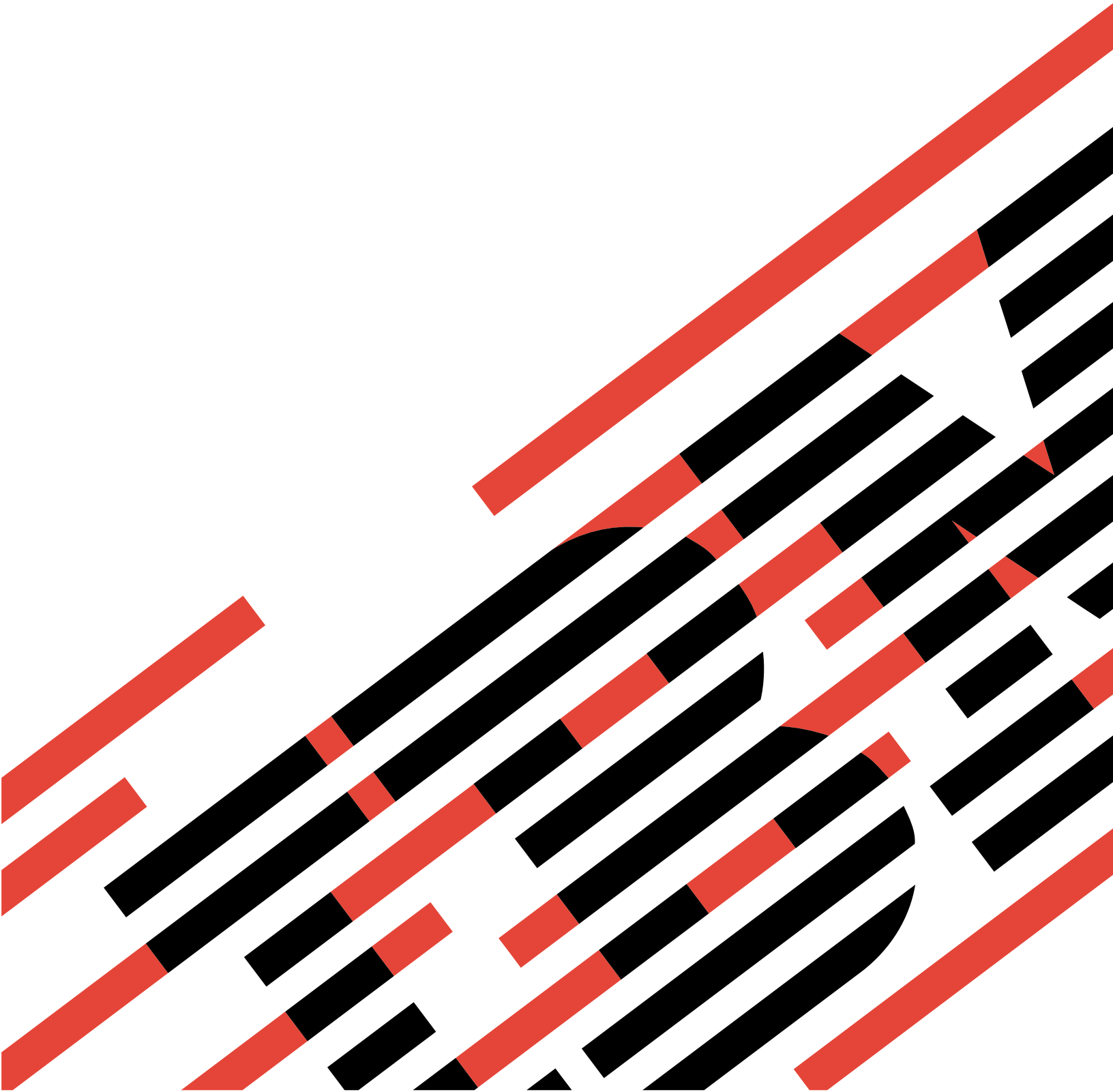
IBM

eserver

iSeries

SSL(Secure Sockets Layer)



IBM

@server

iSeries

SSL(Secure Sockets Layer)

목차

제 1 부 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.

- **V5R2의 새로운 사항**
  - SSL과 관련이 있는 새로운 기능이나 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**
  - 보안 소켓층 프로토콜의 기본적인 빌딩 블록을 제공하는 추가 정보가 포함되어 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.

제 1 장 V5R2의 새로운 사항

iSeries용 2058 Cryptographic Accelerator는 V5R2M0에서 사용할 수 있는 옵션입니다. 이러한 암호화 하드웨어 옵션은 iSeries 서버의 SSL 성능을 향상시키기 위해 설계된 것입니다. 이 옵션에 대한 자세한 정보는 암호화 하드웨어를 참조하십시오.

신규 GSKit(Global Secure Kit) API(Application Programming Interface)

신규 OS/400® GSKit(Global Secure Toolkit) API를 `gsk_secure_soc_startInit()`와 같이 사용할 수 있습니다. 자세한 정보는 GSKit(Global Secure ToolKit) API를 참조하십시오.

이 릴리스의 새로운 사항이나 변경 사항에 대한 기타 정보는 사용자 메모 를 참조하십시오.

새로운 사항 또는 변경 사항 확인 방법

기술적인 변경 사항이 있는 위치를 쉽게 확인할 수 있도록 본 정보에서는 다음 항목을 사용합니다.

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

제 2 장 이 주제 인쇄

본 정보를 PDF 버전으로 보거나 다운로드할 수 있습니다. PDF 버전을 보거나 다운로드하려면 SSL을 사용한 어플리케이션 보안(약 215KB 또는 34 페이지)을 선택하십시오.

기타 정보

이 주제에 대한 모든 관련 정보를 보거나 인쇄할 수도 있습니다.

PDF 파일 저장

PDF를 워크스테이션에 저장하여 보거나 인쇄하려면 다음과 같이 하십시오.

1. 브라우저에서 PDF를 마우스 오른쪽 버튼으로 클릭하십시오.
2. **다른 이름으로 대상 저장**을 클릭하십시오.
3. PDF를 저장할 디렉토리로 이동하십시오.
4. **저장**을 클릭하십시오.

Adobe Acrobat Reader 다운로드

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

제 3 장 SSL 시나리오

»

다음 시나리오는 iSeries 서버에서 SSL의 이점을 최대한 활용하기 위한 것입니다.

- 시나리오: SSL을 사용한 중앙 관리 보안
- 시나리오: SSL을 사용한 FTP 보안
- 시나리오: SSL을 사용한 Telnet 보안
- 시나리오: iSeries SSL 성능 확장
- 시나리오: 암호화 하드웨어를 사용한 개인 키 보호

«

SSL 시나리오: SSL을 사용한 중앙 관리 보안

»

상황

회사에서 WAN(Wide Area Network)을 설치했으며 여기에는 여러 대의 iSeries 서버(종료점 시스템)가 포함되어 있을 뿐 아니라 홈 오피스의 iSeries 서버 한 대가 중앙으로 관리를 합니다. 이 회사의 보안 담당자인 Tom은 자신의 홈 오피스에 있는 iSeries 서버(중앙 시스템)에 연결하기 위해 iSeries Navigator 클라이언트의 중앙 관리 기술을 사용합니다. 또한 SSL을 사용하여 중앙 시스템과 모든 종료점 서버 간에 보안을 유지하려고 합니다.

세부사항

iSeries Navigator의 중앙 관리 기술을 사용하면 하나의 중앙 시스템을 통해 여러 시스템을 관리할 수 있습니다. 또한 중앙 관리 기술과 SSL을 사용할 경우 시스템을 **안전하게** 관리할 수 있습니다. 중앙 관리 기술과 SSL을 사용하기 위해서는 중앙 관리를 실행할 PC에서 Windows®용 iSeries Access 및 iSeries Navigator를 위한 보안을 유지해야 합니다.

중앙 관리 환경에서 사용할 수 있는 인증 레벨에는 다음의 두 가지가 있습니다.

서버 인증

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

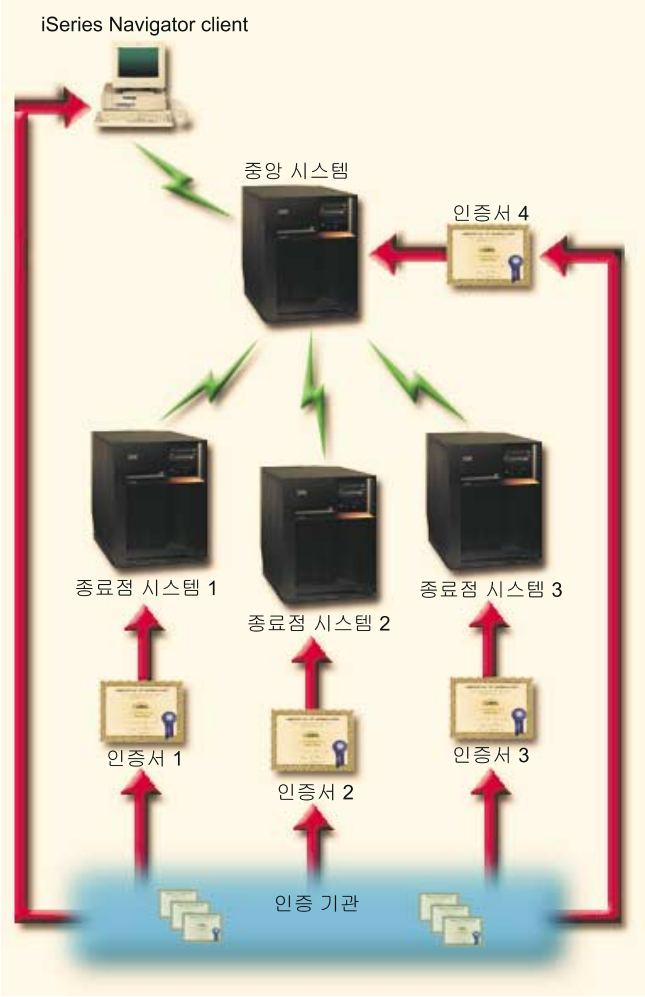
클라이언트 및 서버 인증

중앙 시스템 및 종료점 시스템 모두의 인증서를 제공합니다. 이 인증서가 서버 인증 레벨보다 더 강력한 보안 레벨로 간주됩니다. 다른 어플리케이션에서는 이것을 클라이언트 인증이라고 하며, 이 인증을 통해 클라이언트가 신뢰할 수 있는 유효한 인증서를 제공해야 합니다. 중앙 시스템(SSL 클라이언트)이 종료점 시스템(SSL 서버)에 연결을 시도할 때 중앙 시스템과 종료점 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.

일반적으로 대부분의 어플리케이션에서는 서버와 클라이언트의 인증 작동을 동시에 지정하지 않습니다. 이것은 서버 인증이 거의 SSL 세션 작동 중에 발생하기 때문입니다. 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 SSL을 작동시킬 수 있으면 중앙 시스템은 서버의 역할을 하지만 중앙 시스템이 종료점 시스템에 연결되면 클라이언트의 역할을 합니다. 다음 그림은 중앙 시스템이 네트워크에서 서버와 클라이언트로서 어떻게 작동하는지를 보여줍니다.

주: 이 그림에서 인증 기관과 연관된 인증서는 반드시 중앙 시스템 및 모든 종료점 시스템의 키 데이터베이스에 저장되어 있어야 합니다.



전제조건 및 가정

SSL 작동 중앙 관리가 제대로 작동하기 위해서는 다음의 관리 및 구성 타스크(SSL 보안 중앙 관리 WAN 이미지 참조)를 수행해야 합니다.

1. 중앙 관리와 함께 사용되는 iSeries 서버가 SSL에 대한 전제조건을 만족합니다(SSL 전제조건 참조).
2. 중앙 시스템과 모든 종료점 iSeries 서버가 OS/400 V5R2를 실행합니다. V5R1을 사용하는 경우 다음 OS/400(5722-SS1)용 수정 프로그램(PTF)을 설치하십시오.
   a. SI01375
   b. SI01376
   c. SI01377
   d. SI01378
   e. SI01838

3. iSeries Navigator PC 클라이언트가 Windows용 iSeries Access V5R2를 실행합니다. 클라이언트가 V5R1을 사용하는 경우 Windows용 iSeries Access V5R1(5722-XE1)용 서비스 팩 PTF SI01907 이상을 설치하십시오. 자세한 정보는 V5R1 Information Center, ″Securing Management Central″ 페이지를 참조하십시오.
4. iSeries 서버에 대한 CA(Certificate Authority)를 확보하십시오.
5. SSL 작동 중앙 관리 서버에서 관리하게 될 각 iSeries 서버에 대해 CA에서 서명한 인증서를 작성하십시오.
6. CA 및 인증서를 각 iSeries 서버에 송신하고 키 데이터베이스로 가져오십시오.
7. 중앙 관리 어플리케이션 및 iSeries Navigator에서 사용하는 모든 종료점 서버에 대한 어플리케이션 인증서를 지정하십시오.
   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. 이렇게 하면 Windows용 iSeries Access 클라이언트의 ID 설정을 위해 사용할 중앙 관리 서버에 인증서가 지정됩니다.
   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 종료점 서버에 대해 이 절차를 반복하십시오.
8. iSeries Navigator를 설정하십시오.
   a. iSeries Navigator용 SSL 구성요소를 설치하십시오(선택적).
   b. CA를 작성한 시스템에서 CA를 다운로드하십시오.

      주: Windows용 iSeries Access 클라이언트의 키 데이터베이스에 없는 CA 인증서를 선택하는 경우 SSL을 사용할 수 있도록 데이터베이스에 해당 인증서를 추가해야 합니다.

구성 단계

중앙 관리에서 SSL을 작동시키려면 먼저 iSeries 서버에 필수 프로그램을 설치하고 디지털 인증서를 설정해야 합니다. 계속하기 전에 이 시나리오에 대한 전제조건 및 가정을 참조하십시오. 모든 전제조건을 만족시켰으면 중앙 관리용 SSL을 작동시키기 위한 다음 절차를 완료할 수 있습니다.

주: SSL이 iSeries Navigator용으로 작동되는 경우 SSL을 중앙 관리용으로 작동시키려면 먼저 SSL을 작동 불가능하게 해야 합니다. SSL이 iSeries Navigator용으로 작동하고 중앙 관리용으로 작동하지 않을 때 iSeries Navigator가 중앙 관리의 중앙 시스템으로 연결을 시도하면 오류가 발생합니다.

서버 인증의 경우(필수)

1. 서버 인증을 위한 중앙 시스템 구성
2. 서버 인증을 위한 종료점 시스템 구성

클라이언트 인증의 경우(선택적)

주: 서버 인증이 구성되기 전에는 클라이언트 인증 구성을 완료할 수 없습니다.

1. 클라이언트 인증을 위한 중앙 시스템 구성
2. 클라이언트 인증을 위한 종료점 시스템 구성

서버 인증을 위한 중앙 시스템 구성

SSL을 사용하면 iSeries Navigator 클라이언트와 중앙 시스템 간의 전송 보안 뿐만 아니라 중앙 시스템과 종료점 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 종료점 시스템 간에서만 이루어질 수 있습니다. 클라이언트 인증을 수행하려면 먼저 서버 인증을 설정해야 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. 인증 레벨에 해당되는 **서버**를 선택하십시오.
4. **확인**을 클릭하여 이 값을 중앙 시스템에 설정하십시오.

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

서버 인증을 위한 종료점 시스템 구성

중앙 시스템에서 서버 인증을 위해 SSL이 작동되도록 한 후에는 모든 종료점 시스템에서도 서버 인증을 위해 SSL이 작동되도록 해야 합니다. 종료점 시스템에서 SSL과 서버 인증을 사용하도록 구성하려면 다음 타스크를 완료하십시오.

1. **중앙 관리** 보기를 펼치십시오.
2. **다음과 같이 종료점 시스템의 시스템 값을 비교하고 갱신하십시오.**
   a. **종료점 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 옵션은 체크하지 마십시오.
   c. **시스템 그룹 --> 신규 시스템 그룹**을 마우스 오른쪽 버튼으로 클릭하십시오.

d. SSL을 사용하여 연결할 모든 종료점 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.

- 보안 소켓층 사용이 **예**로 설정되어 있는지 확인하십시오.
- SSL 인증 레벨이 **서버**로 설정되어 있는지 확인하십시오.

이러한 값은 중앙 시스템에서 서버 인증을 위한 중앙 시스템 구성 절차에서 설정됩니다.

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

j. **비교 및 갱신** 프로세스가 완료될 때까지 기다렸다가 중앙 관리 서버를 다시 시작하십시오. 비교 및 갱신 프로세스가 완료되기 까지는 일정 시간(몇 분)이 소요됩니다.

3. **중앙 시스템에서 중앙 관리 서버 다시 시작**

a. iSeries Navigator에서 **연결**을 펼치십시오.

b. 중앙 시스템 보기를 펼치십시오.

c. **네트워크 --> 서버**를 펼치고 **TCP/IP**를 선택하십시오.

d. **중앙 관리**를 마우스 오른쪽 버튼으로 클릭하고 **중단**을 선택하십시오. 중앙 시스템 보기가 접히고 더 이상 서버에 연결되어 있지 않은 것으로 메세지가 표시됩니다.

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

4. **모든 종료점 시스템에서 중앙 관리 서버 다시 시작**

a. 다시 시작할 종료점 시스템을 펼치십시오.

b. **네트워크 --> 서버**를 펼치고 **TCP/IP**를 선택하십시오.

c. **중앙 관리**를 마우스 오른쪽 버튼으로 클릭하고 **중단**을 선택하십시오.

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

e. 각 종료점 시스템에 대해 이 절차를 반복하십시오.

5. **iSeries Navigator 클라이언트에 대한 SSL 활성화**

a. iSeries Navigator에서 **연결**을 펼치십시오.

b. 중앙 시스템을 마우스 오른쪽 버튼으로 클릭하고 **등록 정보**를 선택하십시오.

c. **보안 소켓** 탭을 클릭하고 **연결에 SSL(Secure Sockets Layer) 사용**을 선택하십시오.

d. iSeries Navigator를 나간 다음 다시 시작하십시오.

서버 인증을 위한 구성을 완료했으면 다음의 선택적 클라이언트 인증 절차를 수행할 수 있습니다.

- 클라이언트 인증을 위한 중앙 시스템 구성
- 클라이언트 인증을 위한 종료점 시스템 구성

클라이언트 인증은 종료점 시스템과 중앙 시스템에 인증 기관과 신뢰할 수 있는 그룹에 대한 유효성을 제공합니다.

클라이언트 인증을 위한 중앙 시스템 구성

중앙 시스템(SSL 클라이언트)이 SSL을 사용하여 종료점 시스템(SSL 서버)에 연결하려고 할 때 중앙 시스템과 종료점 시스템은 클라이언트 인증을 통해 서로의 인증서를 인증합니다(중앙 관리에서는 인증 기관 및 신뢰할 수 있는 그룹 인증이라고 함).

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

클라이언트 인증을 위한 종료점 시스템 구성

1. **종료점 시스템의 시스템 값 비교 및 갱신**

   주: V4R5를 실행하는 종료점 iSeries 서버에는 이 타스크가 적용되지 않습니다. V4R4 레드북, ″Management Central: A Smart Way to Manage AS/400® Systems  ″를 참조하십시오.

   a. **종료점 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 옵션은 체크하지 마십시오.

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

   d. SSL을 사용하여 연결할 모든 종료점 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 다음을 확인하십시오.

      - 보안 소켓층 사용이 **예**로 설정되었는지 확인하십시오.
      - SSL 인증 레벨이 **클라이언트 및 서버**로 설정되었는지 확인하십시오.

      이러한 값은 중앙 시스템에서 클라이언트 인증을 위한 중앙 시스템 구성 절차에서 설정됩니다. 각 값의 옆에 있는 **갱신** 상자를 체크하십시오.

   i. 신규 시스템 그룹에 포함된 종료점 시스템에 이러한 값을 설정하려면 **확인**을 클릭하십시오.

2. **종료점 시스템에 유효성 리스트 복사**
   a. iSeries Navigator에서 **중앙 관리 --> 정의**를 펼치십시오.
   b. **패키지**를 마우스 오른쪽 버튼으로 클릭하고 **신규 정의**를 선택하십시오.
   c. **신규 정의** 창에서 다음과 같이 하십시오.
      - **이름:** 정의명을 입력하십시오.
      - **소스 시스템:** 중앙 시스템명을 선택하십시오.
      - **선택한 파일 및 폴더:** 이 필드를 클릭하고 /QSYS.LIB/QUSRSYS.LIB/QYPSVLDL.VLDL을 입력하십시오.
   d. **옵션** 탭을 클릭하고 **기존 파일을 송신할 파일로 대체**를 선택하십시오.
   e. **고급**을 클릭하십시오
   f. **고급 옵션** 창에서 복원 시 오브젝트 차이를 허용하려면 **예**를 지정하십시오.
   g. 정의 리스트를 화면정리하고 신규 패키지를 표시하려면 **확인**을 클릭하십시오.
   h. 신규 패키지를 마우스 오른쪽 버튼으로 클릭하고 **송신**을 선택하십시오
   i. **송신** 대화 상자: 신뢰할 수 있는 그룹만 추가하고 다른 그룹은 제거한 다음 **확인**을 클릭하십시오. 신뢰할 수 있는 그룹은 이 절차의 1단계에서 정의한 시스템 그룹입니다.

      주: 중앙 시스템은 항상 소스 시스템이므로 중앙 시스템에서는 **송신** 타스크가 실패합니다. **송신** 타스크는 모든 종료점 시스템에서 성공적으로 완료되어야 합니다.
3. **중앙 시스템에서 중앙 관리 서버 다시 시작**
   a. iSeries Navigator에서 **연결**을 펼치십시오.
   b. 중앙 시스템을 펼치십시오.
   c. **네트워크 --> 서버**를 펼치고 **TCP/IP**를 선택하십시오.
   d. **중앙 관리**를 마우스 오른쪽 버튼으로 클릭하고 **중단**을 선택하십시오. 중앙 시스템 보기가 접히고 더 이상 서버에 연결되어 있지 않은 것으로 메세지가 표시됩니다.
   e. 중앙 관리 서버가 중단되었으면 **시작**을 클릭하여 다시 시작하십시오.
4. **모든 종료점 시스템에서 중앙 관리 서버 다시 시작**

   주: 각 종료점 시스템에 대해 이 절차를 반복하십시오.
   a. 다시 시작할 종료점 시스템을 펼치십시오.
   b. **네트워크 --> 서버**를 펼치고 **TCP/IP**를 선택하십시오.
   c. **중앙 관리**를 마우스 오른쪽 버튼으로 클릭하고 **중단**을 선택하십시오.
   d. 중앙 관리 서버를 중단한 후 **시작**을 클릭하여 다시 시작하십시오.

제 4 장 SSL 개념

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

다음에 나오는 개념 정보를 통해 SSL과 iSeries 서버 간의 관계를 보다 잘 이해할 수 있을 것입니다.

- 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 것입니다. SSL은 원래 웹 브라우저 및 서버 통신의 보안을 위해 개발된 것이지만 TELNET 및 FTP와 같은 다른 어플리케이션에서도 SSL을 사용할 수 있도록 기본 스펙이 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 종료점 간에서 자료의 흐름을 제어합니다.

핸드쉐이크 프로토콜은 SSL 세션의 하나의 종료점이나 두 개의 종료점을 각각 인증하고, 해당 SSL 세션의 자료를 암호화하고 암호를 해독하기 위한 키를 생성할 때 사용할 수 있는 고유 대칭 키를 설정합니다. SSL은 비대칭 암호, 디지털 인증서 및 SSL 핸드쉐이크 흐름을 사용하여 SSL 세션의 하나의 종료점이나 두 개의 종료점을 각가 인증합니다. 일반적으로는 서버를 인증하며 선택적으로 클라이언트를 인증합니다. 인증 기관에서 발행한 디지털 인증서는 연결의 종료점마다 SSL을 사용해서 각 종료점이나 어플리케이션에 지정됩니다.

디지털 인증서는 신뢰할 수 있는 인증 기관(CA)에서 디지털로 서명한 몇 가지의 식별 정보 및 공용키로 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 종료점은 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 종료점 사이에 초기 SSL 세션이 설정되면 두 종료점과 어플리케이션에 대한 SSL 세션 정보가 보안 메모리에 캐시되어 후속 SSL 세션의 작동 속도를 높일 수 있습니다. SSL 세션이 재개되면 두 종료점은 공용 키나 개인 키를 사용하지 않고도 각각 고유 정보에 액세스할 수 있음을 인증하기 위해 단축 핸드쉐이크 흐름을 사용합니다. 양쪽 모두가 고유 정보에 액세스할 수 있음이 입증되면 새로운 대칭 키가 설정되고 SSL 세션이 ″재개″됩니다. TLS 버전 1.0과 SSL 버전 3.0 세션에서는 24시간이 지나면 캐시된 정보가 보안 메모리에서 삭제됩니다. V5R2M0의 경우 암호화 하드웨어를 사용하면 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 3.0으로 결정되지 않을 경우 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 2.0으로 결정되지 않으면 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, Inc.의 BSAFE 3.0을 사용하며 BSAFE 3.0에는 많은 수정 프로그램(timing attack 관련)과 SHA-1 해싱 알고리즘이 포함됩니다. SHA-1 해싱 알고리즘은 MD5 해싱 알고리즘 보다 안전한 것으로 간주됩니다. SHA-1을 사용할 경우 SSL 버전 3.0이 MD5 대신에 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 3.0과 비교해 볼 때 TLS(Transport Layer Security) 버전 1.0은 업계 표준 최신 SSL 프로토콜입니다. 그 스펙은 IETF(Internet Engineering Task Force)의 RFC 2246, ″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 3.0에서 사용하는 MAC(Message Authentication Code)보다 안전한 것으로 알려져 있습니다.
- **향상된 PRF(Psuedorandom Function)**
  - PRF는 키 자료의 생성에 사용됩니다. TLS에서는 PRF가 HMAC로 정의됩니다. PRF는 보안을 보장하는 방식으로 두 개의 해시 알고리즘을 사용합니다. 그 중 하나의 알고리즘이 노출되더라도 두 번째 알고리즘이 노출되지 않으면 자료는 안전합니다.
- **개선된 완료 메세지 확인**
  - TLS 버전 1.0과 SSL 버전 3.0 모두 교환된 메세지가 변경되지 않았다는 것을 인증하는 완료 메세지를 두 종료점에 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 간에서 반드시 교환시켜야 하는 인증 유형을 지정합니다.
- **특정 경고 메세지**
  - TLS는 두 개의 세션 종료점 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. 이어서 SSL 핸드쉐이크가 완료되면 통신 링크의 한쪽 끝이나 양 끝이 인증되고 자료의 암호화와 해독을 위한 고유 키가 생성됩니다. 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(기본)
- IBM HTTP Server(Apache로 구동)
- FTP 서버
- Telnet 서버
- 중앙 관리 종료점 시스템
- 디렉토리 서비스(LDAP)

제 5 장 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 서버에서 DCM을 사용하려는 경우 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. V5R2M0 릴리스부터는 다음의 암호화 하드웨어 옵션을 iSeries 서버와 함께 사용할 수 있습니다.
  - 2058 Cryptographic Accelerator(하드웨어 피처 코드 4805)
  - 4758 Cryptographic Coprocessor(하드웨어 피처 코드 4801 또는 4802)

  암호화 하드웨어를 설치하려면 옵션 35, Cryptographic Service Provider도 설치해야 합니다.

Windows용 iSeries Access 또는 IBM Toolbox for Java 구성요소에서 SSL을 사용하려는 경우에도 iSeries Client Encryption 제품, 5722-CE3(128비트)을 설치해야 합니다. Windows용 iSeries Access에서는 이 제품이 있어야만 보안 연결을 설정할 수 있습니다.

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.

제 6 장 SSL을 사용한 어플리케이션 보안

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

- iSeries용 IBM HTTP Server(기본)
- iSeries용 IBM HTTP Server(Apache로 구동)
- FTP 서버
- Telnet 서버
- DRDA®(분산 관계형 데이터베이스 구조) 및 분산 자료 관리(DDM) 서버
- 중앙 관리
- 디렉토리 서비스 서버(LDAP)
- 기업망 ID 맵핑(EIM)
- iSeries Navigator를 포함한 Windows용 iSeries Access 어플리케이션
- 어플리케이션 프로그래밍 인터페이스(API)의 Windows용 iSeries Access 세트에 기록된 어플리케이션
- Developer Kit for Java를 사용하여 개발한 프로그램 및 IBM Toolbox for Java를 사용하는 클라이언트 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.

제 7 장 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.

위에 열거한 사항들을 확인했음에도 iSeries 서버에서 SSL 관련 문제가 계속 발생하면 다음 옵션을 시도할 수 있습니다.

- 해당 오류에 대한 추가 정보를 찾을 수 있도록 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 표에서는 서버 작업 기록부에 표시되는 -93을 상수 SSL_ERROR_SSL_NOT_AVAILABLE에 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 어플리케이션의 경우 이 API를 사용하여 이 문장이 포함되어 있는 작업 기록부에 메세지를 출력하고 있습니다.

  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.SSL

| 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.

제 8 장 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
- JSSL에 대한 간단한 설명과 JSSL 사용 방법이 포함되어 있는 (JSSL)Java Secure Socket Layer 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.

«

Printed in U.S.A