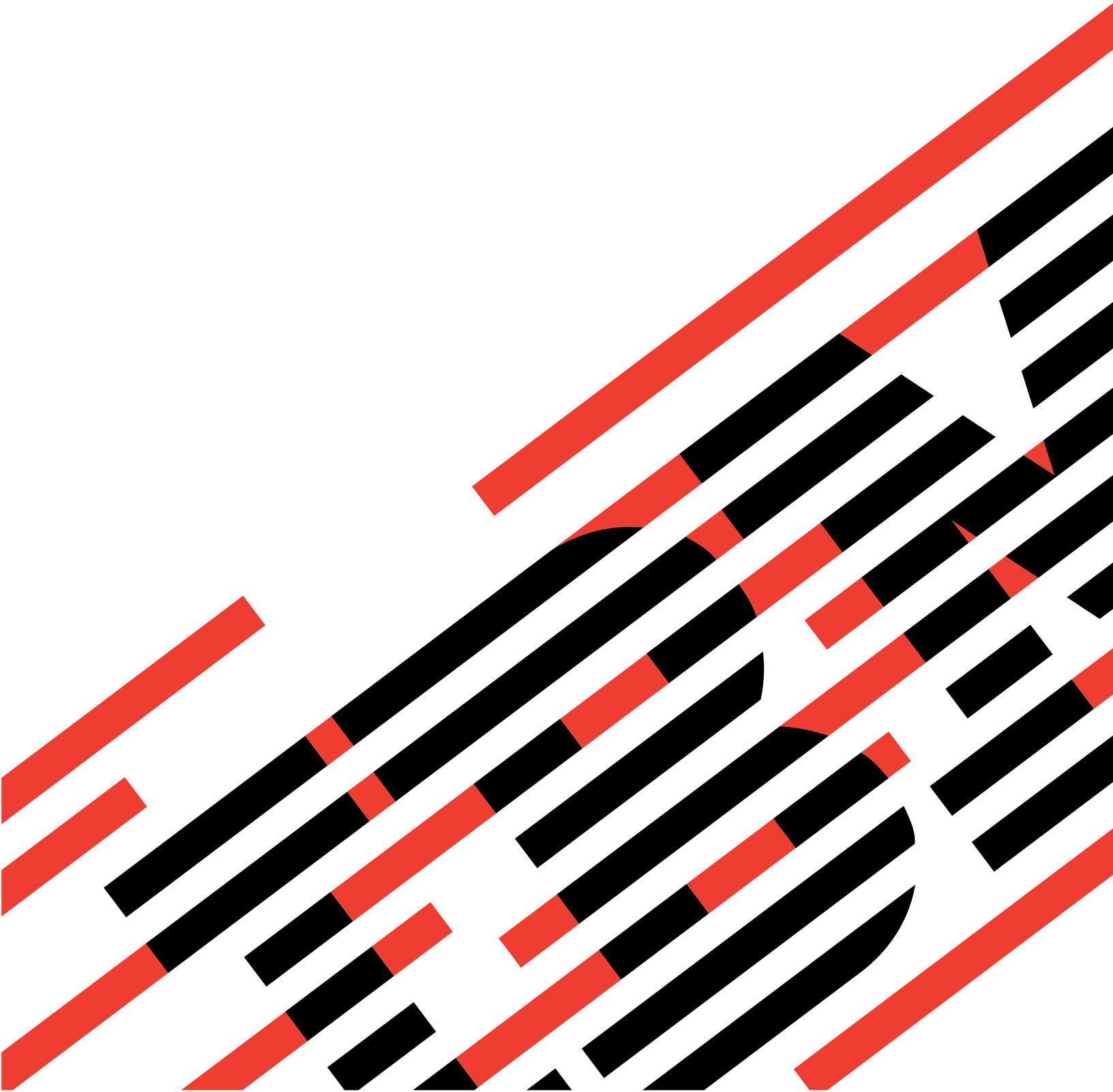
IBM

eserver

iSeries

安全套接字层（SSL）



IBM

@server

iSeries

安全套接字层（SSL）

目录

第 1 部分 安全套接字层（SSL）

“安全套接字层”（SSL）已经成为允许应用程序在不受保护的网络（如因特网）上进行安全通信会话的业界标准。使用以下链接查找关于 SSL 和 iSeries™ 服务器应用程序的更多信息:

- **V5R2 的新增功能**
  记录了关于 SSL 可用的新功能或新信息。
- **SSL 方案**
  是对 SSL 信息的新补充，且设计的目的在于通过提供 SSL 如何工作的可能示例，来提高您对 iSeries 服务器上 SSL 的理解。
- **SSL 概念**
  包括提供“安全套接字层”协议的一些基本构件的补充信息。
- **SSL 启用计划**
  包括在 iSeries 服务器上启用 SSL 的先决条件，也包括一些有用的技巧。
- **用 SSL 保护应用程序**
  包括一个应用程序列表，可以用 iSeries 服务器上的 SSL 来保护。
- **SSL 故障诊断**
  提供有关如何开始进行 iSeries 服务器上的 SSL 故障诊断程序的基本指南。
- **SSL 的相关信息**
  包括要使用的附加信息资源的链接。

第 1 章 V5R2 的新增功能

iSeries 的 “2058 加密加速器” 在 V5R2MO 上是可用选件。此加密硬件选件是为改进 iSeries 服务器的 SSL 性能而设计的。参阅加密硬件以获取关于此选件的更多信息。

新 Global Secure Kit（GSKit）应用程序编程接口（API）

可以使用新 OS/400® Global Secure Toolkit（GSKit）API: `gsk_secure_soc_startInit()`。参阅 Global Secure ToolKit（GSKit）API 以获取更多信息。

要查找关于本发行版的新增功能或更改的其它信息，参阅用户备忘录

。

如何查看新增功能或更改内容

为帮助您了解哪些地方做了技术更改，使用以下信息:

- 
  图像，标记了新的或更改了的信息开始位置。
- 图像，标记了新的或更改了的信息结束位置。

第 2 章 打印本主题

可以查看或下载此信息的 PDF 版本。为此，选择用 SSL 保护应用程序（大约 215KB 或 34 页）。

其它信息

还可查看或打印本主题的任何相关信息。

保存 PDF 文件

要将 PDF 保存在工作站上以便进行查看或打印，遵循以下步骤:

1. 在浏览器中右键单击 PDF。
2. 单击**将目标另存为**。
3. 浏览至希望保存 PDF 的目录。
4. 单击**保存**。

下载 Adobe Acrobat Reader

如果需要 Adobe Acrobat Reader 以查看或打印此信息，可以从 Adobe Web 站点（www.adobe.com/products/acrobat/readstep.html）  下载副本。

第 3 章 SSL 方案

以下方案设计旨在帮助您尽量增大在 iSeries 服务器上启用 SSL 的益处:

- 方案: 用 SSL 保护中央管理
- 方案: 用 SSL 保护 FTP
- 方案: 用 SSL 保护 Telnet
- 方案: 提高 iSeries SSL 性能
- 方案: 用加密硬件保护专用密钥

SSL 方案: 用 SSL 保护中央管理

情况

某公司刚刚建立了一个广域网（WAN），它包括在远程位置（端点系统）的几个 iSeries 服务器，由一台位于总公司的 iSeries 服务器进行中心管理。此公司的安全性专家 Tom 使用 “iSeries 导航器” 客户机的 “中央管理” 技术，连接到总公司 iSeries 服务器（中央系统）。Tom 打算用 SSL 来保护中央系统和所有端点服务器之间的连接。

详细信息

使用 iSeries 导航器的中央管理技术，Tom 可以通过单个中央系统管理多个系统。通过将 SSL 和 “中央管理” 配合使用，Tom 可以**安全地**管理那些系统。要将 SSL 与 “中央管理” 配合使用，Tom 必须保护运行 “中央管理” 的 PC 机上的 iSeries Access Windows® 版和 “iSeries 导航器”。

在 “中央管理” 环境下，Tom 具有两个认证级别:

服务器认证

提供端点系统服务器证书的认证。当连接到端点系统时，中央系统就充当 SSL 客户机的角色。端点系统充当 SSL 服务器的角色，而且必须提供中央系统所信任的 “认证中心” 发出的证书，以此证明端点系统的身份。对于每个端点系统，必须有由可信的 CA 发出的有效证书。

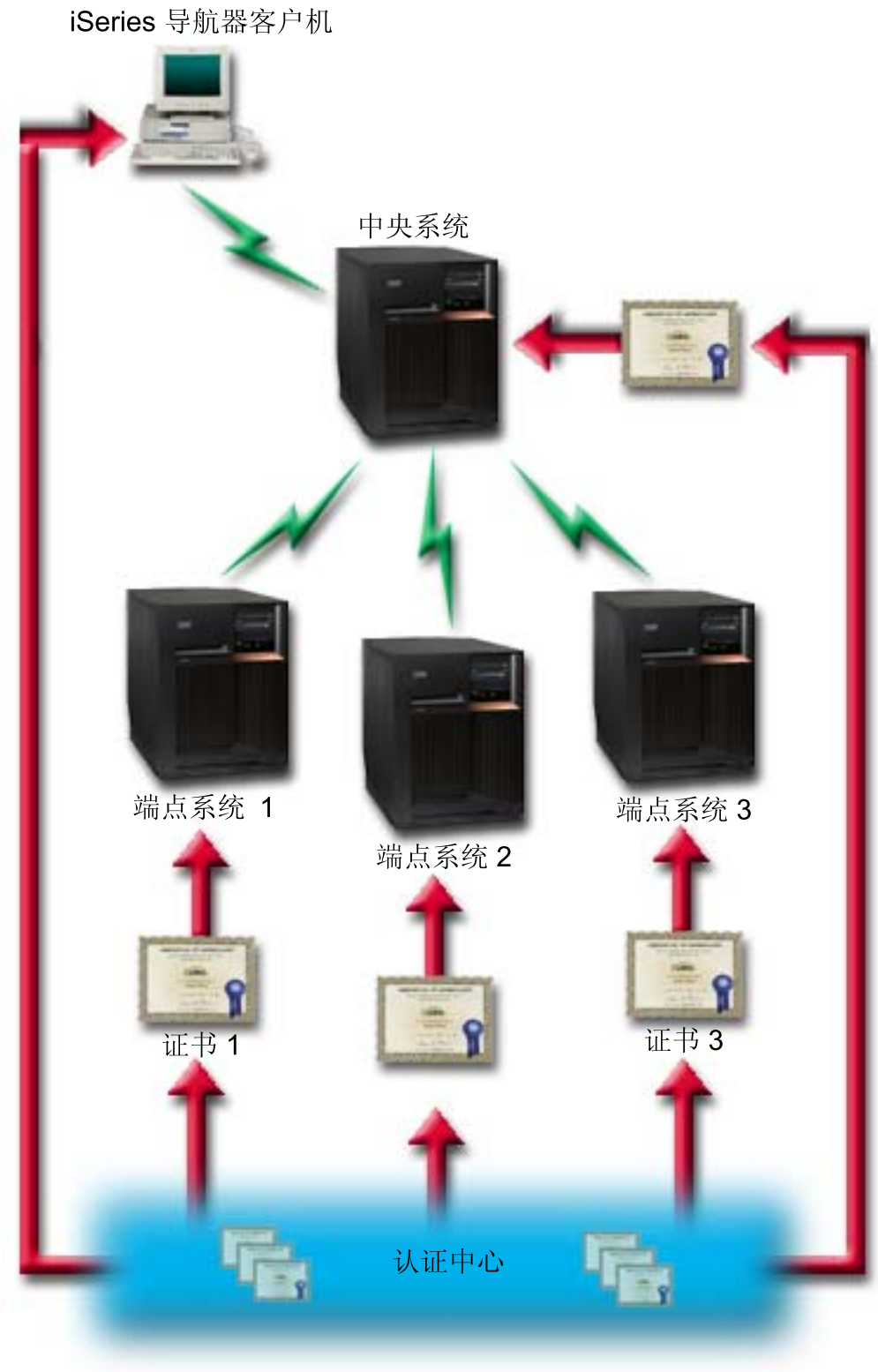
客户机和服务器认证

同时提供中央系统和端点系统证书的认证。它被认为是一种比服务器认证级别更强的安全级别。在其它应用程序中，它被称为是客户机认证，其中客户机必须提供有效可信的证书。当中央系统（SSL 客户机）试图与某端点系统（SSL 服务器）建立连接时，中央系统和端点系统互相鉴定对方的证书以证明授权的真实性。

与其它应用程序不同，“中央管理” 还通过一份验证列表（称作 “可信组” 验证列表）来提供认证。通常，验证列表存储识别用户的信息（如用户标识）和认证信息（如密码、个人识别号码或数字证书）。这些认证信息都是加密的。

| 大多数应用程序通常不指定同时启用服务器认证和客户机认证。这是因为服务器认证几乎总是在 SSL 会话启用
| 期间进行。许多应用程序具有客户机认证配置选项。由于中央系统在网络中起双重作用，因此“中央管理”使
| 用“服务器和客户机认证”这个术语而不是客户机认证。当 PC 机用户连接到中央系统并且 SSL 已启用时，
| 中央系统充当服务器的角色；而当中央系统连接到端点系统时，它又充当客户机的角色。以下图表显示了中央
| 系统在网络中是如何同时充当服务器和客户机的。

注: 在此图表中，与“认证中心”关联的证书必须存储在中央系统和所有端点系统的密钥数据库中。



先决条件和假设

Tom 必须执行以下的管理和配置任务（参阅图像 SSL 保护的中央管理 WAN），以便使启用 SSL 的“中央管理”工作:

1. 与“中央管理”配合使用的 iSeries 服务器可满足 SSL 的先决条件（参阅 SSL 的先决条件）。
2. 中央系统和所有端点的 iSeries 服务器运行 OS/400 的 V5R2。如果是在 V5R1 环境下，则安装以下 OS/400（5722-SS1）的修正（PTF）:
   a. SI01375
   b. SI01376
   c. SI01377
   d. SI01378
   e. SI01838
3. “iSeries 导航器”PC 客户机运行 iSeries Access Windows 版的 V5R2。如果客户机在 V5R1 环境下，则安装 iSeries Access Windows 版（5722-XE1）的 V5R1 PTF SI01907（或更高版本）服务包。参阅 V5R1 Information Center, ″Securing Management Central″ 页面，以获取更多的信息。
4. 获取 iSeries 服务器的“认证中心”（CA）。
5. 创建由 CA 签署的证书，以使每台 iSeries 服务器都由启用 SSL 的“中央管理服务器”来管理。
6. 将 CA 和证书发送到每台 iSeries 服务器，并将其导入到密钥数据库。
7. 用“中央管理”应用程序标识和“iSeries 导航器”所使用的所有端点服务器的应用程序标识来指定证书:
   a. 启动中央服务器上的“IBM® 数字证书管理器”。如果 Tom 需要获取或创建证书，或另外设置或更改他的证书系统，则现在就进行（参阅使用数字证书管理器以获取有关设置证书系统方面的信息）。
   b. 单击**选择证书存储库**。
   c. 选择 ***SYSTEM** 并单击**继续**。
   d. 输入 *SYSTEM **证书存储库密码**，并单击**继续**。当重新装入菜单时，展开**管理应用程序**。
   e. 单击**更新证书指定**。
   f. 选择**服务器**并单击**继续**。
   g. 选择**中央管理服务器**，并单击**更新证书指定**。这就将证书指定给了“中央管理”服务器来使用，以便建立 iSeries Access Windows 版客户机身份。
   h. 单击**指定新证书**。得到确认信息后，DCM 重新装入到**更新证书指定**页面。
   i. 单击**完成**。
   j. 对“iSeries 导航器”所使用的所有端点服务器重复此过程。
8. 设置“iSeries 导航器”:
   a. 选择性地安装“iSeries 导航器”的 SSL 组件。
   b. 从创建 CA 的系统上下载 CA。

   注: 如果 Tom 从某个 CA 选择了证书，而该 CA 的证书不在 Tom 的 iSeries Access Windows 版客户机密钥数据库中，那么为了使用 SSL 他就需要将该证书添加到密钥数据库。

配置步骤

Tom 可以在“中央管理”上启用 SSL 之前，他必须安装先决条件程序并在 iSeries 服务器上设置数字证书（继续之前参阅本方案的先决条件和假设）。满足了这些先决条件之后，他可以通过完成以下的步骤来启用“中央管理”的 SSL。

| **注**: 如果为“iSeries 导航器”启用 SSL，则在启用“中央管理”的 SSL 之前，Tom 必须禁用 SSL。如果只是对“iSeries 导航器”启用 SSL，而不是对“中央管理”启用它，那么通过“iSeries 导航器”来连接“中央管理”中央系统的尝试将会失败。

| **对于服务器认证（必需）**:

| 1. 配置中央系统以进行服务器认证
| 2. 配置端点系统以进行服务器认证

| **对于客户机认证（可选）**:

| **注**: 只有服务器认证配置之后，才可能完成客户机认证配置。

| 1. 配置中央系统以进行客户机认证
| 2. 配置端点系统以进行客户机认证

| 配置中央系统以进行服务器认证

| SSL 允许 Tom 保护在中央系统与端点系统之间的传输，以及“iSeries 导航器”客户机与中央系统之间的传输。SSL 提供证书的传送和认证及数据的加密。SSL 连接只可以存在于启用 SSL 的中央系统和启用 SSL 的端点系统之间。Tom 必须在他可以进行客户机认证之前，进行服务器认证设置。

| 1. 在 iSeries 导航器中，右键单击**中央管理**，然后选择**特性**。
| 2. 单击**安全性**选项卡，然后选择**使用安全套接字层（SSL）**。
| 3. 选择**服务器**作为认证级别。
| 4. 单击**确定**以在中央系统上设置此值。

| **注**: 完成服务器认证的端点系统配置之前，**不要**重新启动“中央管理服务器”。

| 5. 配置端点系统以进行服务器认证。

| 配置端点系统以进行服务器认证

| Tom 在对服务器认证启用中央系统上的 SSL 之后，需要为服务器认证启用所有端点系统上的 SSL。为配置端点系统以使用 SSL 和服务器认证，他完成了以下任务:

| 1. 展开**中央管理**视图。
| 2. **比较并更新端点系统的系统值**:
| a. 在**端点系统**下，右键单击中央系统并选择**库存 —> 收集**。
| b. 选中收集对话框中的**系统值**选项，以便收集中央系统的系统值库存。不选其它任何选项。
| c. 右键单击**系统组 —> 新建系统组**。
| d. 定义包括使用 SSL 要连接的所有端点系统的新系统组。
| e. 要显示新组，展开系统组列表。
| f. 收集完成之后，右键单击新系统组并选择**系统值 —> 比较并更新**。
| g. 验证中央系统是否在**模型系统**区显示。
| h. 选择**中央管理**类别并验证以下值，选中各项旁边的框:
| • “使用安全套接字层”是否设置为**是**。
| • SSL 认证级别是否设置为**服务器**。
| 在配置中央系统以进行服务器认证的过程中，在中央系统上设置这些值。
| i. 单击**确定**以便在新系统组的端点系统上设置这些值。

j. 等**比较并更新**进程完成之后，重新启动“中央管理服务器”。这可能要花几分钟。

3. **在中央系统上重新启动“中央管理”服务器**:
   a. 在“iSeries 导航器”中，展开**我的连接**。
   b. 展开中央系统视图。
   c. 展开**网络 —> 服务器**并选择 **TCP/IP**。
   d. 右键单击**中央管理**并选择**停止**。中央系统视图停止，显示一条消息，说明不再与服务器相连接。
   e. “中央系统”服务器停止后，单击**启动**以重新启动服务器。
4. **重新启动所有端点系统上的“中央管理”服务器**:
   a. 展开要重新启动的端点系统。
   b. 展开**网络 —> 服务器**并选择 **TCP/IP**。
   c. 右键单击**中央管理**并选择**停止**。
   d. “中央系统”服务器停止后，单击**启动**以重新启动服务器。
   e. 为每个端点系统重复此过程。
5. **激活“iSeries 导航器”客户机的 SSL**:
   a. 在“iSeries 导航器”中，展开**我的连接**。
   b. 右键单击中央系统，然后选择**特性**。
   c. 单击**安全套接字**选项卡并选择**对连接使用安全套接字层（SSL）**。
   d. 退出“iSeries 导航器”并重新启动它。

既然 Tom 完成了服务器认证的配置，他就可以执行以下可选的客户机认证步骤:

- 配置中央系统以进行客户机认证
- 配置端点系统以进行客户机认证

客户机认证提供“认证中心”的验证，且对端点系统和中央系统提供可信组。

配置中央系统以进行客户机认证

当中央系统（SSL 客户机）尝试使用 SSL 连接到某端点系统（SSL 服务器）时，通过客户机认证（在“中央管理”中称为“认证中心”与“可信组”的认证），中央系统和端点系统互相鉴定对方的证书。

1. 在“iSeries 导航器”中，右键单击**中央管理**并选择**特性**。
2. 单击**安全性**选项卡并选择**使用安全套接字层（SSL）**。
3. 对认证级别选择**客户机和服务器**。
4. 单击**确定**以在中央系统上设置此值。

   注: 将所有端点系统配置为同时使用 SSL 与客户机和服务器认证之前，**不要**重新启动“中央管理服务器”。
5. 配置端点系统以进行客户机认证。

配置端点系统以进行客户机认证

1. **比较并更新端点系统的系统值**:

   注: 这个任务对任何运行 V4R5 的端点 iSeries 服务器不起作用。参阅 V4R4 红皮书 “Management Central: A Smart Way to Manage AS/400® Systems

   ”。

a. 在**端点系统**下，右键单击中央系统并选择**库存 —> 收集**。
b. 选中收集对话框上的**系统值**选项，以便收集中央系统的系统值库存。不选其它任何选项。
c. 右键单击**系统组 —> 新建系统组**。
d. 定义包括使用 SSL 要连接的所有端点系统的新系统组。
e. 要显示新组，展开系统组列表。
f. 收集完成之后，右键单击新建系统组并选择**系统值 —> 比较并更新**。
g. 验证中央系统是否显示在**模型系统**区。
h. 选择**中央管理**类别并验证以下内容:
   - “使用安全套接字层”是否设置为**是**。
   - SSL 认证级别是否设置为**客户机和服务器**。

   在配置中央系统以进行客户机认证的过程中，在中央系统上设置这些值。选中每个值旁的**更新**框。
i. 单击**确定**以在新系统组的端点系统上设置这些值。

2. **将验证列表复制到端点系统**:
   a. 在“iSeries 导航器”中，展开**中央管理 —> 定义**。
   b. 右键单击**软件包**，并选择**新建定义**。
   c. 在**新建定义**窗口，进行以下操作:
      - **名称**: 输入定义的名称。
      - **源系统**: 选择中央系统的名称。
      - **选定的文件和文件夹**: 单击字段，并输入 /QSYS.LIB/QUSRSYS.LIB/QYPSVLDL.VLDL。
   d. 单击**选项**选项卡，并选择**用将要发送的文件替换现有的文件**。
   e. 单击**高级**。
   f. 在**高级选项**窗口，指定**是**以允许恢复对象差别。
   g. 单击**确定**以刷新定义列表并显示新软件包。
   h. 右键单击新软件包，然后选择**发送**。
   i. 在**发送**对话框中: 添加可信组，除去任何其它的组，然后单击**确定**。“可信组”是您在此过程的“步骤 1”中所定义的系统组。

      注: 在中央系统中**发送**任务通常会失败，因为中央系统通常是源系统。**发送**任务可在所有端点系统上成功完成。

3. **在中央系统上重新启动“中央管理”服务器**:
   a. 在“iSeries 导航器”中，展开**我的连接**。
   b. 展开中央系统。
   c. 展开**网络 —> 服务器**并选择 **TCP/IP**。
   d. 右键单击**中央管理**并选择**停止**。中央系统视图折叠，显示出一条消息，说明您不再和服务器相连接。
   e. “中央系统”服务器停止后，单击**启动**以重新启动服务器。

4. **重新启动所有端点系统上的“中央管理”服务器**:

   注: 为每个端点系统重复此过程。
   a. 展开要重新启动的端点系统。
   b. 展开**网络 —> 服务器**并选择 **TCP/IP**。
   c. 右键单击**中央管理**并选择**停止**。

d. “中央管理”服务器停止后，单击**启动**以重新启动服务器。

第 4 章 SSL 概念

用 SSL 协议可以建立客户机和服务器应用程序之间的安全连接，这些应用程序提供通信会话的一个或两个端点的认证。SSL 还提供客户机和服务器应用程序所交换的数据的保密性和完整性。

以下提供的概念性信息可帮助您更深刻地理解 SSL 和 iSeries 服务器之间的关系:

- SSL 历史
- SSL 如何工作
- 受支持的 SSL 和“传输层安全”（TLS）协议
- 服务器认证
- 客户机认证

SSL 历史

为了满足对因特网安全性日益增长的需要，Netscape 于 1994 年开发了“安全套接字层协议”（SSL）。虽然最初开发 SSL 是为了保护 Web 浏览器和服务器通信，但以这种方式设计的规范也允许其它应用程序（如 TELNET 和 FTP）使用 SSL。参阅受支持的 SSL 和“传输层安全”（TLS） 协议以获取有关 SSL 和相关协议的更多信息。 

SSL 如何工作

SSL 实际上是两个协议，即记录协议和握手协议。记录协议控制在 SSL 会话的两个端点之间的数据流。

握手协议认证 SSL 会话的一个或两个端点，并建立一个唯一的对称密钥，用于生成该 SSL 会话数据的加密和解密密钥。SSL 使用非对称密码术、数字证书和 SSL 握手流来认证 SSL 会话的一个或两个端点。通常，服务器需要认证，而客户机可选择进行认证。一份由“认证中心”发出的数字证书，可以指定给每个端点，或指定给连接的每个端点上使用 SSL 的应用程序。

数字证书包含一个公用密钥和由可信的“认证中心”（CA）数字化签署的一些标识信息。每个公用密钥都具有一个关联的专用密钥。专用密钥不和证书存储在一起，也不作为证书的一部分存储。在服务器认证和客户机认证中，正在被鉴定的端点必须能够证明其有权访问与数字证书中包含的公用密钥关联的专用密钥。

由于加密操作使用公用密钥和专用密钥，因此 SSL 握手是强调性能的操作。建立了两个端点之间的初始 SSL 会话之后，这两个端点的 SSL 会话信息和应用程序就可以在安全内存中高速缓存，从而加速后续 SSL 会话的启用。恢复 SSL 会话时，这两个端点使用简短的握手流，以鉴定每个端点都有权访问唯一信息，而无需使用公用密钥或专用密钥。如果两个端点都能证明它们有权访问此唯一信息，那么建立新的对称密钥并“恢复”该 SSL 会话。对于 TLS 版本 1.0 和 SSL 版本 3.0 会话，高速缓存的信息在安全内存中保留的时间不会超过 24 小时。在 V5R2M0 中，通过使用加密硬件可将 SSL 握手性能对主 CPU 的影响降至最低。

受支持的 SSL 和“传输层安全”（TLS）协议

有几个已定义的 SSL 协议版本。最新版本的“传输层安全协议”（TLS）是基于 SSL 3.0 版，并是“Internet 工程任务组”（IETF）的产品。OS/400 实现支持以下 SSL 和 TLS 协议的版本:

- TLS 版本 1.0
- TLS 版本 1.0 与 SSL 版本 3.0 的兼容性

  注:

  1. 指定 TLS 版本 1.0 与 SSL 版本 3.0 的兼容性意味着如果可能的话将进行 TLS 协商，而如果该协商不可能的话，则将进行 SSL 版本 3.0 协商。如果 SSL 版本 3.0 不能协商，那么 SSL 握手将会失败。
  2. 我们还支持 TLS 版本 1.0 与 SSL 版本 3.0 和 SSL 版本 2.0 的兼容性。这用协议值 **ALL** 指定，这表示如果可能的话，将进行 TLS 协商，而如果不可能的话，则将进行 SSL 版本 3.0 协商。如果 SSL 版本 3.0 不能协商，则将协商 SSL 版本 2.0。如果 SSL 版本 2.0 不能协商，那么 SSL 握手将会失败。
- SSL 版本 3.0
- SSL 版本 2.0
- SSL 版本 3.0 与 SSL 版本 2.0 的兼容性

SSL 版本 3.0 与 SSL 版本 2.0

和 SSL 版本 2.0 相比，SSL 版本 3.0 几乎是一个完全不同的协议。这两个协议之间的一些主要区别在于:

- SSL 版本 3.0 握手协议流与 SSL 版本 2.0 握手流不同。
- SSL 版本 3.0 使用 RSA Data Security, Inc. 的 BSAFE 3.0 实现，BSAFE 3.0 包括许多定时攻击修正和 SHA-1 散列算法。SHA-1 散列算法被认为是比 MD5 散列算法更安全的算法。拥有 SHA-1 使 SSL 版本 3.0 可支持使用 SHA-1 而不是 MD5 的其它密码套件。
- SSL 版本 3.0 协议减少了 SSL 握手处理期间发生的 man-in-the-middle（MITM）类型的攻击。在 SSL 版本 2.0 中，MITM 攻击可能会削弱密码规范，虽然这未必会发生，但有这种可能。削弱密码可能会使某个未授权的人破坏 SSL 会话密钥。

TLS 版本 1.0 与 SSL 版本 3.0

基于 SSL 版本 3.0 的“传输层安全”（TLS）版本 1.0，是业界最新的标准 SSL 协议。其规范由“Internet 工程任务组”（IETF）在 RFC 2246 ″The TLS Protocol″ 中定义。 

TLS 的主要目标是使 SSL 更安全并使协议的规范更精确和完善。TLS 在 SSL 版本 3.0 的基础上，提供了这些增强内容:

- 更安全的 MAC 算法
- 更严密的警告
- “灰色区域”规范的更明确的定义

任何对 SSL 启用的 iSeries 服务器应用程序将自动获取 TLS 支持，除非该应用程序特别要求只能使用 SSL 版本 3.0 或 SSL 版本 2.0。

TLS 提供了以下安全性改进:

- **对于消息认证使用密钥散列法**
  TLS 使用“消息认证代码的密钥散列法”（HMAC），当记录在开放的网络（如因特网）上传送时，该代码”确保记录不会被更改。SSL 版本 3.0 还提供键控消息认证，但 HMAC 被认为比 SSL 版本 3.0 所使用的（消息认证代码）MAC 功能更安全。

- **增强的伪随机功能（PRF）**
  PRF 用来生成密钥数据。在 TLS 中，PRF 用 HMAC 定义。PRF 使用两种散列算法，以这种方式保证其安全性。如果任一种算法暴露了，那么只要第二种算法不暴露，数据仍然会保持安全。
- **改进的已完成消息验证**
  TLS 版本 1.0 和 SSL 版本 3.0 都对两个端点提供已完成的消息，以鉴定交换的消息没有被更改。然而，TLS 将此已完成消息基于 PRF 和 HMAC 值之上，这也比 SSL 版本 3.0 更安全。
- **一致证书处理**
  与 SSL 版本 3.0 不同，TLS 试图指定必须在两次 TLS 实现之间交换的证书类型。
- **特定警告消息**
  TLS 提供更多的特定和附加警告，以指示任一会话端点检测到的问题。TLS 还对何时应该发送某些警告进行记录。

服务器认证

通过服务器认证，客户机可确保服务器证书是有效的，并确保该证书是由客户机信任的认证中心（CA）签署的。SSL 将使用非对称密码术和握手协议流来生成一个只能用于此唯一 SSL 会话的对称密钥。此密钥用来生成一套密钥，使用这套密钥加密和解密将在 SSL 会话上流过的数据。随后，在 SSL 握手完成后，将对通信链路的一端或两端进行认证且将生成一个唯一的密钥来加密和解密数据。握手完成之后，应用层数据将在该 SSL 会话中以加密形式流动。

客户机认证

许多应用程序允许启用客户机认证选项。通过客户机认证，服务器将确保客户机证书是有效的，并确保该证书是由服务器所信任的“认证中心”签署的。以下的 iSeries 服务器应用程序支持客户机认证:

- IBM HTTP Server（原始）
- IBM HTTP Server（基于 Apache）
- FTP 服务器
- Telnet 服务器
- “中央管理”端点系统
- 目录服务（LDAP）

第 5 章 SSL 启用计划

当计划在 iSeries 服务器上启用 SSL 时，请考虑以下问题:

- SSL 的先决条件
- 想要什么类型的数字证书，从哪里可获取它们

SSL 的先决条件:

- IBM Digital Certificate Manager（DCM），OS/400（5722-SS1）的选件 34
- TCP/IP Connectivity Utilities iSeries 版（5722-TC1）
- IBM HTTP Server iSeries 版（5722-DG1）
- 如果您正在尝试用 HTTP server 来使用 DCM，请确保安装有 IBM Developer Kit for Java™ （5722–JV1），否则 HTTP 管理服务器将不会启动。
- IBM Cryptographic Access Provider 产品，5722-AC3（128 位）。此产品的位大小指示可用于加密操作的对称密钥中的秘密资料的最大大小。对称密钥允许的大小受各个国家或地区的导入和导出规则控制。位大小越大，连接越安全。
- 您可能还希望安装加密硬件以与 SSL 配合使用来加速 SSL 握手处理。从 V5R2M0 发行版起，以下的加密硬件选件可供与 iSeries 服务器配合使用:
  - 2058 加密加速器（硬件功能部件代码 4805）
  - 4758 加密协处理器（硬件功能部件代码 4801 或 4802）

  如果希望安装加密硬件，还必须安装“选项 35”，即“加密服务提供程序”。

如果希望 SSL 与任何 iSeries Access Windows 版或者 IBM Toolbox for Java 组件配合使用，还必须安装 iSeries Client Encryption 产品，5722-CE3（128 位）。iSeries Access Windows 版需要此产品以便建立安全连接。

注: 不需要安装 Client Encryption 产品，就可使用随“个人通信”产品附带的 PC5250 仿真器。“个人通信”有其自己的内置加密代码。

数字证书

参阅使用公用证书与发出专用证书以加深理解公用数字证书和专用数字证书之间的差别以及获取它们的选择。

IBM“数字证书管理器”（DCM）是 iSeries 服务器用以管理数字证书的解决方案。要查找有关 DCM 的更多信息，参阅“信息中心”主题使用“数字证书管理器”。

第 6 章 用 SSL 保护应用程序

可以用 SSL 保护以下 iSeries 服务器应用程序:

- IBM HTTP Server iSeries 版（原始）
- IBM HTTP Server iSeries 版（基于 Apache）
- FTP 服务器
- Telnet 服务器
- 分布式关系数据库体系结构（DRDA®）和分布式数据管理（DDM）服务器
- 中央管理
- 目录服务服务器（LDAP）
- 企业身份映射（EIM）
- iSeries Access Windows 版应用程序，包括“iSeries 导航器”
- 写至应用程序编程接口（API）的 iSeries Access Windows 版集的应用程序
- 用 Developer Kit for Java 开发的程序和使用 IBM Toolbox for Java 的客户机应用程序
- 使用 iSeries 服务器上支持的安全套接字“应用程序编程接口”（API）开发的应用程序。受支持的 API 是 Global Secure Toolkit（GSKit）和 SSL_ iSeries 本地 API。参阅安全套接字 API 以获取有关 GSKit 和 SSL_API 的信息。

第 7 章 SSL 故障诊断

这种很基本的故障诊断信息旨在帮助您减少 iSeries 服务器可能遇到的关于 SSL 的问题。重要的是要知道它不是故障诊断的全部资料，而仅仅是一个指南。

验证以下叙述是否真实:

- 是否已满足 iSeries 服务器上 SSL 的先决条件（参阅 SSL 的先决条件）。
- 如果正在使用装有 V5R1 系统的 “iSeries 导航器” 的 “中央管理” 技术，则系统上是否已安装有以下 PTF:
  - si01375
  - si01376
  - si01377
  - si01378
  - si01838
- 认证中心和证书有效且证书没有过期。

如果已对系统验证了上述叙述是真实的，但依然在 iSeries 服务器上有与 SSL 相关的问题，可以尝试以下选项:

- 在错误表中可交叉引用服务器工作日志中的 SSL 错误代码以查找有关该错误的更多信息。参阅安全套接字 API 错误代码消息页面以访问有关安全套接字错误代码消息的信息。例如，此表将可能在服务器工作日志中显示的 -93 映射为常量 SSL_ERROR_SSL_NOT_AVAILABLE。
  - 负返回码（由代码数字前的短杠表示）表示您正在使用 SSL_ API。
  - 正返回码表示您正在使用 GSKit API。程序员可在其程序中编码 gsk_strerror()or SSL_Strerror() API 以获取错误返回码的简短描述。一些应用程序使用此 API 并对包含此语句的工作日志打印出一条消息。

  如果需要更详细的信息，该表中提供的消息标识可以显示在 iSeries 服务器上以说明此错误的可能原因及恢复。解释这些错误代码的其它文档可能位于返回错误的个别安全套接字 API 中。
- 以下两个头文件包含与该表相同的 “系统 SSL” 返回码的常量名称，但是没有消息标识交叉引用:
  - QSYSINC/H.GSKSSL
  - QSYSINC/H.SSL

  请记住，虽然在这两个文件中 “系统 SSL” 返回码的名称保持常量，但可能有多个错误与每个返回码关联。

要获取关于 iSeries 服务器故障诊断的更多信息，参阅故障诊断和服务页面。

第 8 章 相关信息

可在以下资源查找附加的 SSL 信息:

IBM 源

- SSL 和 Java 安全套接字扩展（JSSE）页面包括 JSSE 的简短描述及其使用方法。
- Java 安全套接字层（JSSL）页面包括 JSSL 的简短描述及其使用方法。
- IBM Toolbox for Java 页面包括可用 Java 类的简短描述及其使用方法。

请求注释文件（RFC）

- RFC 2246: ″The TLS Protocol Version 1.0″ 详细解释了 TLS 协议。
- RFC2818: ″HTTP Over TLS″ 描述了如何在因特网上使用 TLS 保护 HTTP 连接。

其它资源

- The SSL Protocol Version 3.0 文档 非常详细地解释了 SSL Protocol Version 3.0。

中国印刷